Proceedings of the International Symposium on Algebraic Number Theory

Tokyo & Nikko
September, 1955

Organized by
The Science Council of Japan
under the joint sponsorship with
The International Mathematical [illegible]

Published by
The Organizing Committee
International Symposium on
Algebraic Number Theory
Science Council of Japan
Ueno Park, Tokyo
October, 1956

CONTENTS

Short Notes

*Articles marked with * appeared in fuller detail in Journal of the Mathematical Society of Japan, vol. 7, Supplement, December, 1955.*

International Symposium on Algebraic Number Theory

Report

> The Executive Committee shall discuss the future program of conferences each year on the basis of proposals received before February 1 (in 1954 before November 1). In setting up the programs the Executive Committee must take into account the interest of the various subjects from the point of view of the actual state of science, the scientific circumstances in the countries in which the conference might take place, and what conferences have taken place in recent years....
> (*From Art. 4 of the rules on Symposia of the International Mathematical Union.*)

1. An International Symposium on Algebraic Number Theory was held in Tokyo and Nikko, Japan on September 8-13, 1955. It was attended by 64 mathematicians, of whom 10 from foreign countries: France, Germany, India and the United States of America. Professor T. Takagi, the founder of the class field theory, attended it on September 9 as Honorary Chairman of the Symposium. It was organized by an Organizing Committee under the Science Council of Japan, with Professor S. Iyanaga as Chairman, Professor Y. Akizuki as Secretary and with three foreign members nominated by the International Mathematical Union: Professors K. Chandrasekharan, C. Chevalley and S. Mac Lane. It was co-sponsored by the International Mathematical Union, whose Executive Committee approved the proposal of the Science Council of Japan to hold this Symosium, endorsed by the decision of the Japanese Government at its Cabinet meeting on October 22, 1955. Thus a financial aid was given by UNESCO through the International Council of Scientific Unions and the International Mathematical Union; it was also aided by a Society for Supporting the Symposium formed principally with representative people in the financial and industrial circles of Japan, as well as by the foreign governments and institutions concerned, which contributed towards the travel expenses of the foreign participants.

2. The Organizing Committee aimed at exchanging informations on latest research results, with a view to further developing the Algebraic

Number Theory, among the ranking mathematicians working in this field all over the world in an atmosphere of friendship and cordiality. A special emphasis was laid on possible extensions of the class field theory as well as on the interplay of the algebraic geometry and the number theory. It turned out, incidentally, that remarkable results had been obtained by a number of participants from abroad and inside Japan, concerning the generalization of the theory of complex multiplication, so that a notable progress was marked in this field on this occasion. As the papers presented by Japanese mathematicians were so numerous, only a smaller part of them could be read at the Symposium in full length. As for the selection of the papers to be read and the plan of the Symposium in general, the whole responsibility was assumed by the Organizing Committee.

3. As Japan is situated in a remote corner of the world distant from the western countries, and as this was the first symposium of its kind to be held here, this was considered by the Japanese public interested in mathematics as a particular good occasion to have contact with the ranking mathematicians from abroad. A Public Lecture Meeting by three participant mathematicians, Professors E. Artin, A. Weil and C. Chevalley was held on September 8 in response to the wish of the interested general public. The contents of these lectures were translated into Japanese and published in Japanese periodicals[1]. Moreover, the foreign participants were invited to deliver lectures and to participate in seminars in universities in various parts of Japan before their going home.

The following pages will reproduce the scientific content and the atmosphere of the Symposium.

[1] "Sugaku" (edited by the Mathematical Society of Japan) vol. 7, no. 4, 1956, and "Kagaku" (published by Iwanami Shoten, Tokyo) vol. 25, no. 12, 1955.

Staff

PRESIDENT OF THE SCIENCE COUNCIL OF JAPAN

Kaya, Seiji

OFFICERS OF THE SYMPOSIUM

Honorary Chairman	Takagi, Teiji
Chairman	Suetuna, Zyoiti

ORGANIZING COMMITTEE

Chairman	Iyanaga, Shôkichi
Secretary	Akizuki, Yasuo

Members Nominated by the International Mathematical Union

Chandrasekharan, Komaravolu

Mac Lane, Saunders   Chevalley, Claude

Members Nominated by the Science Council of Japan

Fujioka, Yoshio   Honda, Hiroto
Hukuhara, Masuo   Inada, Seisuke
Ishizawa, Sadayoshi   Kawada, Yukiyosi
Kitagawa, Tosio   Kotani, Masao
Kunugi, Kinjiro   Nozawa, Tadao
Okano, Kiyoshi   Saito, Hitoshi
Shoda, Kenjiro   Suetuna, Zyoiti
Tamagawa, Tsuneo   Tannaka, Tadao
Yoshimoto, Motosuke   Yosida, Kôsaku

PREPARATION COMMITTEE

Chairman	Shoda, Kenjiro

Members

Akizuki, Yasuo   Iyanaga, Shôkichi
Saito, Hitoshi   Suetuna, Zyoiti

RECEPTION COMMITTEE

Hukuhara, Masuo   Kunugi, Kinjiro
Nomizu, Katsumi   Yamabe, Hidehiko
Yoneda, Nobuo   Yosida, Kôsoku

EDITORIAL COMMITTEE

Iyanaga, Shôkichi   Kawada, Yukiyosi

Programme

Sept. 8 (Thursday)

10.30 - 11.30

Opening Ceremony (Conference Room, Daiichi Mutual Life Insurance Co.)

14.00 - 16.30

Public Lectures (University of Tokyo)

Speakers:

Prof. E. Artin: Theory of braids

Prof. A. Weil: On the breeding of bigger and better zeta-functions

Prof. C. Chevalley: A few remarks on mathematical journals

Sept. 9 (Friday)

9.30 - 12.00

(Conference Room, D.M.L.I.C.)

Chairman: Prof. C. Chevalley

Communications:

Prof. E. Artin: Representatives of the connected components of the idèle class group

Prof. K. Iwasawa: Galois groups acting on the multiplicative groups of local fields

Prof. A. Weil: On certain characters of idèle class groups

14.00 - 16.30

(Conference Room, D.M.L.I.C.)

Chairman: Prof. K. Shoda

Communications:

Prof. R. Brauer: Number-theoretical investigations on groups of finite order

Prof. T. Tannaka: On the generalized principal ideal theorem

Mr. T. Kubota: Density in a family of abelian extensions

Short Communications:

Prof. F. Terada: A generalization of the principal ideal theorem

Prof. K. Taketa: Über die Struktur der metabelschen Gruppen

Sept. 10 (Saturday)

9.00 - 11.45

(Conference Room, D.M.L.I.C.)

Chairman: Prof. R. Brauer

Communications:

Prof. C. Chevalley: Projective imbedding of a group variety

Mr. K. Yamazaki: Fibre spaces and sheaves in number theory

Prof. D. Zelinsky: Cohomology of function fields and other algebras

Prof. T. Nakayama (Read by Prof. Y. Kawada): A conjecture on the cohomology of algebraic number fields and the proof of its special case

Sept. 12 (Monday)

9.00 - 12.00

(Ball-room, Kanaya Hotel)

Chairman: Prof. E. Artin

Commuications:

Mr. G. Shimura: On complex multiplications

Mr. Y. Taniyama: Jacobian varieties and number fields

Prof. A. Weil: Generalization of complex multiplication

Short Communications:

Prof. E. Inaba: On cohomology groups in a field, which is complete with respect to a discrete valuation

Mr. M. Ikeda: Cohomology theory for algebras

14.00 - 16.30

(Ball-room, K. H.)

Chairman: Prof. A. Weil

Communications:

Prof. M. Deuring: On the zeta-function of an elliptic function field with complex multiplications

Mr. I. Satake: On Siegel's modular functions

Prof. K. G. Ramanathan: Units of fixed points in involutorial algebras

16.30 - 17.30

Chairman: Prof. K. Iwasawa

Short Communications:

Mr. T. Ono: On orthogonal groups over number fields

Prof. T. Tamagawa:	On some extensions of Epstein's Z-series
Prof. T. Tatuzawa:	Additive prime number theory in the totally real algebraic number field
Prof. K. Yamamoto:	Theory of arithmetic linear transformations and its application to an elementary proof of Dirichlet's theorem about the primes in an arithmetic progression
Mr. H. Morikawa:	Cycles on algebraic varieties

Sept. 13 (Tuesday)

9.00 - 12.00

(Ball-room, K. H.)

Chairman: Prof. Y. Akizuki

Communications:

Prof. J.-P. Serre:	Syzygy theory in local rings
Prof. A. Néron:	Arithmétique et classes de diviseurs sur les variétés algébriques
Prof. Y. Nakai:	Some results in the theory of the differential forms of the first kind on algebraic varieties
Mr. M. Nagata:	The theory of multiplicity in general local rings

14.00 - 16.00

(Ball-room, K. H.)

Chairman: Prof. S. Iyanaga

Short Communications:

Mr. M. Narita:	On the structure of complete local rings
Mr. S. Takahashi:	On Fermat function field
Prof. H. Kuniyoshi:	Certain subfields of rational function fields
Mr. K. Masuda:	On the arithmetic on a Galois structure
Prof. G. Azumaya:	An existence theorem of algebras
Prof. Y. Kawada:	Some remarks on class formations
Prof. M. Moriya:	Zusammenhang zwischen 2-Kohomologiegruppe und Differente
Prof. N. Nakano:	Idealtheorie in unendlichen algebraischen Zahlkörpern
Prof. T. Morishima:	On Fermat's last theorem

16.00 - 16.30

Closing Session (Ball-room, K. H.)

Participants

FRANCE

Néron, André
Assistant Professor
Department of Mathematics
University of Poitiers, Poitiers

Serre, Jean-Pierre
Assistant Professor
Department of Mathematics
University of Nancy, Nancy

GERMANY

Deuring, Max
Professor
Mathematical Institute
University of Göttingen
Göttingen

INDIA

Ramanathan, K. G.
Member
Tata Institute of Fundamental Research
Apollo Pier Road, Bombay 1

U. S. A.

Artin, Emil
Professor
Department of Mathematics
Princeton University
Princeton, N. J.

Brauer, Richard
Professor
Department of Mathematics
Harvard University
Cambridge 38, Mass.

Chevalley, Claude
Professor
Department of Mathematics
Columbia University
New York 27, N. Y.

Iwasawa, Kenkichi
Assistant Professor, University of Tokyo;
Associate Professor
Massachusetts Institute of Technology
Cambridge 39, Mass.

Weil, André
Professor
Department of Mathematics
University of Chicago
Chicago 37, Ill.

Zelinsky, Daniel
Associate Professor
College of Liberal Arts
Northwestern University
Evanston, Ill.

JAPAN

AKIZUKI, Yasuo	Professor Faculty of Science University of Kyoto, Kyoto
ASANO, Keizo	Professor Institute of Polytechnics Osaka City University, Osaka
AZUMAYA, Gorô	Professor Faculty of Science Hokkaido University, Sapporo
HATTORI, Akira	Lecturer Faculty of Science Tokyo University of Education, Tokyo
HIRAI, Atuhiro	Assistant Faculty of Science Osaka University, Osaka
HITOTUMATU, Sin	Assistant Professor Faculty of Science Rikkyo Daigaku, Tokyo
IKEDA, Masatoshi	Lecturer Faculty of Science Osaka University, Osaka
INABA, Eizi	Professor Faculty of Science Ochanomizu University, Tokyo
ITÔ, Noboru	Lecturer Faculty of Science Nagoya University, Nagoya
IWAHORI, Nagayosi	Assistant Professor College of General Education University of Tokyo, Tokyo
IYANAGA, Shôkichi	Professor Faculty of Science University of Tokyo, Tokyo
KAWADA, Yukiyosi	Professor Faculty of Science University of Tokyo, Tokyo
KAWAHARA, Yûsaku	Graduate Student Faculty of Science Nagoya University, Nagoya

KAWAI, Ryoichiro	Lecturer Faculty of Science University of Kyoto, Kyoto
KOIZUMI, Shoji	Assistant Professor Faculty of Science Tokyo University of Education, Tokyo
KUBOTA, Tomio	Assistant Faculty of Science Nagoya University, Nagoya
KUGA, Michio	Lecturer College of General Education University of Tokyo, Tokyo
KUNIYOSHI, Hideo	Assistant Professor Faculty of Science Tôhoku University, Sendai
MASUDA, Katsuhiko	Lecturer Faculty of Science and Literature Yamagata University, Yamagata
MATSUMURA, Hideyuki	Graduate Student Faculty of Science University of Kyoto, Kyoto
MORI, Shinziro	Professor Faculty of Science Hiroshima University, Hiroshima
MORIKAWA, Hisasi	Assistant Faculty of Science Nagoya University, Nagoya
MORISHIMA, Taro	Professor Tokyo College of Science, Tokyo
MORIYA, Mikao	Professor Faculty of Science Okayama University, Okayama
NAGAI, Osamu	Assistant Faculty of Science Osaka University, Osaka
NAGAO, Hirosi	Assistant Professor Institute of Polytechnics Osaka City University, Osaka
NAGATA, Masayoshi	Lecturer Faculty of Science University of Kyoto, Kyoto

NAKAI, Yoshikazu	Assistant Professor Faculty of Science University of Kyoto, Kyoto
NAKANO, Noboru	Assistant Professor Faculty of Science Hiroshima University, Hiroshima
NAKANO, Shigeo	Assistant Professor Faculty of Science University of Kyoto, Kyoto
NARITA, Masao	Assistant International Christian University, Tokyo
NISHI, Mieo	Assistant Faculty of Science University of Kyoto, Kyoto
NISHIMURA, Hajime	Lecturer Faculty of Science University of Kyoto, Kyoto
NOMIZU, Katsumi	Assistant Professor Faculty of Science Nagoya University, Nagoya
OKUGAWA, Kôtaro	Professor Faculty of Science University of Kyoto, Kyoto
ONO, Takashi	Assistant Faculty of Science Nagoya University, Nagoya
OSIMA, Masaru	Professor Faculty of Science Okayama University, Okayama
SATAKE, Ichiro	Lecturer College of General Education University of Tokyo, Tokyo
SHIMURA, Goro	Lecturer College of General Education University of Tokyo, Tokyo
SHODA, Kenjiro	Member of Japan Academy President Osaka University, Osaka
SUETUNA, Zyoiti	Member of Japan Academy Professor Faculty of Science University of Tokyo, Tokyo

TAKAHASHI, Shuichi	Assistant Faculty of Science Tôhoku University, Sendai
TAKAHASI, Mutuo	Assistant Professor Institute of Polytechnics Osaka City University, Osaka
TAKETA, Kiyosi	Professor Musashi Technical College, Tokyo
TAMAGAWA, Tsuneo	Assistant Professor Faculty of Science University of Tokyo, Tokyo
TANIYAMA, Yutaka	Assistant Faculty of Science University of Tokyo, Tokyo
TANNAKA, Tadao	Professor Faculty of Science Tôhoku University, Sendai
TATUZAWA, Tikao	Professor Faculty of Science Gakushuin University, Tokyo
TERADA, Fumiyuki	Assistant Professor Faculty of Science Tôhoku University, Sendai
TSUZUKU, Toshiro	Graduate Student Faculty of Science Nagoya University, Nagoya
UCHIYAMA, Saburô	Graduate Student Faculty of Science Tokyo Metropolitan University, Tokyo
YAMABE, Hidehiko	Assistant Professor Faculty of Science Osaka University, Osaka
YAMAMOTO, Koichi	Assistant Professor Faculty of Science Kyushu University, Fukuoka
YAMAZAKI, Keijiro	Assistant College of General Education University of Tokyo, Tokyo

Opening Ceremony

Message

Telegram of Professor H. Hopf, President of the International Mathematical Union to the Chairman of the Organizing Committee

THE INTERNATIONAL MATHEMATICAL UNION CONVEYS ITS SINCEREST WISHES FOR A FULL SUCCESS OF YOUR PRESENT COLLOQUIUM AND FOR CONTINUED PROSPERITY OF MATHEMATICS IN JAPAN.

Opening Address

By Shôkichi IYANAGA
Chairman of the Organizing Committee

First of all, I should like to welcome, on behalf of the Organizing Committee, the distinguished mathematicians who have come a long way from other countries to attend this Symposium and express my heartfelt gratitude to my colleagues and all those who have collaborated in realizing this event.

It is a policy of the International Mathematical Union to sponsor international symposia on those branches of mathematics, which are actually in a lively development, in countries where these branches are most vividly studied. I feel it a great honour to us, therefore, that our proposal to organize an International Symposium on Algebraic Number Theory was favourably considered by the Union, which is now going to be opened by this Ceremony.

In materializing the plan of this Symposium, our Organizing Committee met with some difficulties. As you are well aware, we are remote from European and American countries, and our financial resources did not permit us to invite a large number of mathematicians from such countries. We had also to restrict the number of Japanese speakers because of the limited time available for the Symposium.

We are glad, however, to see assembled here the mathematicians from all over the world well representing the present status of the science, and sincerely hope that their collaboration in our Symposium in a friendly atmosphere will bear good fruits for the future advancement of our science.

The Symposium is held under the co-sponsorship of the Science Council of Japan and the International Mathematical Union. It is helped, however, also by foreign governments and institutions as well as by private individuals and business and industrial circles in this country. I should like to mention a number of school boys and girls loving mathematics, who have contributed a part of their allowances to our Symposium. Availing myself of this opportunity, may I express our deepest gratitude to one of all of them.

Welcome Address

By Seiji KAYA

President of the Science Council of Japan

Representing all scientific circles in Japan, I sincerely wish to express my welcome to you on this occasion of the International Symposium on Algebraic Number Theory.

It is our great pleasure that the highest authorities in this field accepted our invitation in oder to make this Symposium highly fruitful and have attended from every part of the world far from Japan, and I am heartily grateful for your attendance at the meeting.

Our mathematics has an old tradition and an originality in its development. In less than one hundred years since modern mathematics of the West was introduced into Japan, it has made a remarkable development. I believe that it has made a great contribution for the world of mathematics from the international standpoint.

It really has an epoch-making significance for our mathematical circle that an International Symposium is going to be held in Japan for the first time in this field, and that distinguished scholars meet together, report to each other recent results of their studies and discuss various problems with their erudite knowledge, and I firmly believe and expect that it will render a remarkable contribution for the mathematical circles of the world.

Notwithstanding that Algebraic Number Theory, which is the main subject of the Symposium, is very difficult to understand for people who do not specialize in this field and sometimes gives them a feeling that it is unapproachable, great and sincere help has been given by UNESCO, the Japanese Government and many people at home and abroad for the Symposium, for whcih I should like to express my hearty thanks on this occasion.

As far as I know, all guests except Prof. Chevalley are visiting our country for the first time. I hope that they have personal contact with Japanese people and appreciate the Culture of Japan, for it will be of great significance in promoting cultural exchange and international friendly relations.

I heartily wish that the Symposium will achieve a great success from the cultural standpoint as well as scientific.

Address

By Zyoiti SUETUNA
Chairman of the Symposium

It is a great pleasure and honour to me to have this opportunity of saying a few words as Chairman of this International Symposium. All the mathematicians in Japan have been waiting with great expectation for the opening of the present Symposium, for this is the first international gathering of mathematicians to be held in Japan.

In taking this chair I greatly regret that Prof. Takagi has been out of health for some years and is not here with us today. His epoch-making work on the class field theory: "Über eine Theorie des relativ-Abelschen Zahlkörpers" was published in 1920 in the Journal of the College of Science, University of Tokyo. His next paper: "Über das Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörper" appeared after 2 years in the same Journal. And in 1927 Prof. Artin proved the general law of reciprocity, which he had already formulated during his investigation of L-series with general group-characters. The class field theory was thus completed. Since then the algebraic number theory made a great progress and found remarkable applications in some other branches of mathematics. It is, therefore, our great honour and sincere pleasure that the International Symposium on Algebraic Number Theory is now opened here in Tokyo.

On this occasion I should like to speak further a little about the old mathematics in Japan. About the middle of the 6th century when the

Chinese civilization was first introduced into this country, mathematics was imported from the continent together with astronomy. In the second half of the 17th century Seki Kowa, a contemporary of Newton and Leibniz, made remarkable achievements in the Japanese mathematics. Among them are the tenzan, an improvement of the Chinese algebra, and the yenri or circle-principle. He found thus, for example, the determinant sometime before Leibniz and accomplished something like what is now known as integral calculus. Since then the Japanese mathematics made a considerable development. This native mathematics of Japan, which had stood out in complete isolation, yielded however to a strong influx of the Western mathematics after the Meiji Restoration in 1868.

Here I have alluded to the old mathematics in Japan before the middle of the 19th century, because I wish now at the opening of the International Symposium first to remind you of the old tradition of mathematics in Japan and secondly to show that for the due progress of science international communication is necessary.

To all our friends—mathematicians and non-mathematicians—we can say that this kind of an international meeting, which aims at the cultural development of mankind regardless of all the political, social and racial differences, will exert not a small influence on advancement of international co-operation and peace of the world. I hope and believe that this Symposium on Algebraic Number Theory will be in every respect successful with the collaboration of all the participants.

Address

By **Claude** CHEVALLEY

Member of the Organizing Committee

I have been kindly invited to tell you a few words on behalf of the organizing committee. I was very glad to accept this invitation, because, although I had very little work to do myself, it gives me a chance to express my gratitude, and that of the other invited mathematicians, for the splendid job which was accomplished by the organizers of this Symposium in Japan, and particularly by Professor Iyanaga.

But in a mathematical conference, it is not only question of organization; there are also some mathematics involved. No conference would be a success in a country where mathematical life is not as active as it is in Japan. It has been my privilege to live here for one year and to work in close contact with the Japanese mathematicians. The intense severeness with which mathematics is studied in this country is at the same time our explanation for the already achieved results and a sure hope for the future. I would like to conclude these few remarks by paying a tribute to the young Japanese mathematicians. Although their names do not appear on committee lists or in newspaper articles, it is, after all, their devotion to science which is the surest warrant of the success of this Symposium.

Greetings

By Kenzo MATSUMURA
Minister of Education

It gave me a great pleasure to have the opportunity to say a few words of greeting at this Opening Ceremony of the International Symposium on Algebraic Number Theory.

I am particularly happy, as one of Japanese citizens as well as the Minister of Education, to see this Symposium being held in Japan for the first time in the Oriental region, for it seems to me that the selection of Japan as the site of the Conference is an indication that the standard of mathematical studies of this country has come to be in such a high estimation of the world academic circles. For this, my grateful acknowledgement goes to the International Mathematical Union, whose kind and strong recommendation has had a great deal to do with bringing this Symposium to Japan.

In my humble opinion, mathematics is the science which builds up the very foundation of scientific thinking, and its progress contributes invaluably to the promotion of many sciences and, eventually, to the welfare of mankind. Therefore, international exchange and co-operation in the field of this basic science is of utmost importance. This is why I am looking forward to this Symposium with the greatest expectation that the Symposium where a number of foremost scholars of the world are meeting together for discussion as well as friendly talks with each other will play an important role in the advancement of this field of science.

On behalf of all the people of this country let me extend my warmest welcome to the distinguished mathematicians who have come over all the way from different parts of the world to meet here. At the same time, let me also express my wishes that all of them will kindly take this opportunity for their better understanding of this country through their first-hand observation of the actual state of things in Japan, where construction is still under way.

In conclusion I wish to express my heartfelt appreciation again to the International Mathematical Union for the support accorded in organizing this Symposium in Japan and also to the Organizing Committee of this Symposium for the unselfish devotion shown in preparing this Symposium.

May I wish every success of the Symposium.

Address

By Emil ARTIN

Representing the Participants

It is a great honour for me to be given the opportunity to speak in the name of the invited guests and thus to be able to express our deeply felt gratitude to the Science Council of Japan, to the International Mathematical Union, to the Organizing Committee and to all our friends and colleagues in this country for the invitation.

In a certain sense we are not strangers here. For a long time we have found numerous friends among the Japanese mathematicians; for a long time we have had opportunity to study and to admire their work in the Japanese journals; for a long time these contacts have enabled us to come to an understanding of the Japanese culture.

Japan is the ideal country for a conference on Algebraic Number Theory. It was the great mathematician, Takagi, who created the modern concept of class field theory. His work opened a certain domain of the research in Algebraic Number Theory and most, if not all, of the later progress in this field is based on his work. We are all infinitely indebted to him.

The success of such conference depends to a large degree on whether one feels at home. And all of us immediately felt at home. I do not remember ever have I been in a foreign country where I had once such a strong and lasting feeling of sympathy and understanding as in Japan, where I felt as much of the warmth and sincerity of the people as here.

Our gratitude should be expressed especially to Prof. Iyanaga who worked relentlessly and did everything in his power to create the congenial and friendly atmosphere. We are therefore looking forward to the conference with confidence in its success and are convinced that the Science Council of Japan has made a great contribution to the advancement of our science.

Closing Address

By Kenjiro SHODA

Chairman of the Preparation Committee

I have the honour of delivering a closing address of the Opening Ceremony of this International Symposium. I sincerely wish to express my hearty thanks for the colleagues who assembled here from all over the world to take part in this international gathering for the coming four days, and earnestly hope and expect the success of the Symposium.

At the same time, I hope you will enjoy your short stay in Japan to the full extent and get something good whether it might be scenery or antiquity as you may prefer.

In closing this Ceremony I also wish to express my thanks to our guests for their kind attendance.

Closing Session

Address

By Zyoiti SUETUNA

Chairman of the Symposium

Our Symposium on Algebraic Number Theory was closed this afternoon. Many fine results were brought forward and many important discussions made during this Symposium, and I wish to express here my sincere thanks to all the participants. I hope and believe that the relationship between Japan and other countries in the field of mathematics will become closer and deeper after this Symposium.

To all our eminent guests from abroad I should like to say further a few words. The success achieved by our Symposium is due, of course, to the fact that you have come a long way to this country in the Far East to attend it. We are cordially grateful to you for your important contributions to the Symposium. As you stay longer in Japan, you will see further what Japan is and how it is like.

It was in the middle of the 6th century that the Chinese civilization was first introduced into Japan together with buddhism, and the so-called Japanese civilization has been gradually built up ever since. After the Meiji Restoration in 1868, however, the Western civilization has been introduced with overwhelming influences, so that you will observe, wherever you may go in this country, a mixture of, and sometimes a struggle between the new and the old Japan. I wish, therefore, that when you see things in Japan, you will look at them not from one point of view, but from various angles.

Address

By Seiji KAYA

President of the Science Council of Japan

First of all, may I congratulate you on having successfully completed the whole programme of the Symposium. Although I was unable to visit it during the session, I have read in newspapers about the achievements you have made, and I have just been told by Prof. Suetuna how hard you have worked for these 5 days. On behalf of the Science Council of Japan, which has been the sponsor of this Symposium, I should like to express my heartfelt thanks to you all for your collaboration and contributions.

Especially I wish to thank our distinguished guests from abroad for having come such a long way to join the Symposium. Your participation and your enlightening talks, I believe, have been, and still are a great impetus not only to those who have attended the Symposium but to all the young mathematicians in this country. I understand that many of you are going to stay for next few weeks to give lectures at various universities, and I hope that you will enjoy your tour and meeting with promising young mathematicians.

Last but not least, may I express my sincere gratitude to Prof. Suetuna who has acted as Chairman of the Symposium, Prof. Iyanaga, Chairman of the Organizing Committee, and other members of the Committee for their excellent work in organizing and operating the Symposium.

Statement by the Participants from abroad

We are deeply grateful to the Science Council of Japan, to our Japanese colleagues, and to all the authorities and personalities who have cooperated in organizing the International Conference on Number Theory. Our stay in Japan will remain in every way an unforgettable experience to every one of us.

For many years we have followed with great interest the work of the Japanese mathematical school, which now stands in the forefront of modern mathematical progress. Even before coming to Japan, we had met some Japanese mathematicians staying or traveling in foreign countries, and we were acquainted with the work of many more of them through their publications. We have found much to learn from the more intimate personal contacts which this conference has brought about. We particularly wish to record the deep impression made on us by the talent and earnestness which we have noticed in the younger generation.

It is a sad fact for Japan that a considerable proportion of the more outstanding Japanese mathematicians between the ages of 30 and 45 are now living in America; and we believe that this trend is likely to continue. Having talked to most of these men, we are convinced that it is not because of any lack of patriotism or of affection for their country that they have left it. They have done so, simply because the salaries which they would earn in Japan are not sufficient for a scientist to live decently and support a family; those who attempt to do so find it almost impossible to maintain any kind of decent living standards, and they labor under such financial worries as to affect adversely their scientific work.

In the modern world, which is dominated by science, no country, least of all Japan, can afford to lose its best scientific talents to another. We feel that we cannot show our gratitude to the country and the people of Japan in any better way than by publicly uttering the present warning and expressing our considered view that the situation requires urgent action.

We shall forever remain sincere friends of Japan; and we shall part from its shores with the heartiest wishes for its well-being and with the hope of forming ever closer ties with Japan and with our Japanese friends and colleagues in the future.

E. Artin
R. Brauer
C. Chevalley

M. Deuring
A. Néron
K. G. Ramanathan

J.-P. Serre
A. Weil
D. Zelinsky

On a Certain Type of Characters of the Idèle-Class Group of an Algebraic Number-Field

André WEIL

Notations will be the same as in my previous work on class-field theory (*Sur la théorie du corps de classes*, J. Math. Soc. Japan, 3 (1951), pp. 1–35; cf. also *Sur les "formules explicites" de la théorie des nombres premiers*, Comm. Lund (M. Riesz jubilee volume), 1952, pp. 252–265). If K is any field, K^* denotes the multiplicative group of non-zero elements of K. We consider an algebraic number-field k; k_v means its completion with respect to a valuation v; in particular, $k_\mathfrak{p}$, $k_\rho(1 \leqq \rho \leqq r_1)$, $k_\iota(r_1+1 \leqq \iota \leqq r_1+r_2)$ denote the completions of k with respect to the prime ideal $\mathfrak{p}$, to the real archimedian valuation v_ρ and to the imaginary archimedian valuation v_ι, respectively; k_ρ may be identified (canonically) with the real number-field $\mathbf{R}$, and k_ι may be identified (non-canonically) with the complex number-field $\mathbf{C}$; put $\eta_\lambda = [k_\lambda : \mathbf{R}]$. The idèle group I_k is the subgroup of $\prod k_v^*$ consisting of the $a=(a_v)$ such that almost all a_v (i.e., all except a finite number) are units. We denote by P_k the group of principal idèles, and by $C_k = I_k/P_k$ the group of idèle-classes. Each idèle $a=(a_v)$ determines in an obvious manner an ideal $\mathfrak{a}=(a)$ of k; we put:

$$\| a \| = \mathrm{N}(\mathfrak{a})^{-1} \prod_\lambda | a_\lambda |^{\eta_\lambda}.$$

Then $a \rightarrow \| a \|$ is a representation of I_k into $\mathbf{R}^*$ (in fact, into $\mathbf{R}^*_+$), taking the value 1 on P_k.

Group characters will be understood in the extended sense, i.e. as continuous representations into $\mathbf{C}^*$ (not necessarily of absolute value 1). The groups I_k, C_k will be topologized in the usual manner. A character χ of C_k may also be regarded as a character of I_k, taking the value 1 on P_k; because of the known structure of C_k, such a character can always be written as $\chi_1(a)\| a \|^\sigma$, where $\sigma \in \mathbf{R}$ and χ_1 is a character of absolute value 1.

The Hecke L-series attached to a character χ of C_k can be constructed as follows. Let $\mathfrak{f}$ be the conductor of χ; if $a=(a_v)$ is an idèle such that $a_\lambda = 1$ for $1 \leqq \lambda \leqq r_1+r_2$ and $a_\mathfrak{p}=1$ for every prime divisor $\mathfrak{p}$ of $\mathfrak{f}$, $\chi(a)$ depends only upon the ideal $\mathfrak{a}=(a)$; under those circumstances, we put $\tilde{\chi}(\mathfrak{a})=\chi(a)$. Then the L-series attached to χ is $\sum\tilde{\chi}(\mathfrak{a})\mathrm{N}\mathfrak{a}^{-s}$, the sum being extended to all integral ideals $\mathfrak{a}$ prime to $\mathfrak{f}$. We shall denote by $G(\mathfrak{f})$ the group of the fractional non-zero ideals in k whose expression in terms of prime ideals does not involve any prime divisor of $\mathfrak{f}$. We have thus attached, to every character χ of C_k with the conductor $\mathfrak{f}$, a character $\tilde{\chi}$ of $G(\mathfrak{f})$. Clearly $\tilde{\chi}$ is completely determined by its values at the prime ideals which do not divide $\mathfrak{f}$.

At the same time, χ induces on the subgroup $\prod\limits_{\lambda} k_{\lambda}^{*}$ of I_k a character of that group; if we make use of the fact that χ must be the product of a character of absolute value 1 and of a character $||a||^{\sigma}$, we see that χ, on that group, can be written as:

$$\chi((a_{\lambda}))=\prod_{\lambda}(a_{\lambda}/|a_{\lambda}|)^{-f_{\lambda}}|a_{\lambda}|^{\eta_{\lambda}(\sigma+i\varphi_{\lambda})} \qquad (1)$$

where the f_{λ} are integers and σ and the φ_{λ} are real numbers. Now denote by $k^{*}(\mathfrak{f})$ the subgroup of k^{*} consisting of all elements α/α', where α, α' are integers in k such that $\alpha\equiv\alpha'\equiv1$ mod. $\mathfrak{f}$. Then $\chi((\alpha))$ is a character of $k^{*}(\mathfrak{f})$, which coincides on $k^{*}(\mathfrak{f})$ with the character X of k^{*} given by the formula

$$\mathrm{X}(\alpha)=\prod_{\lambda}(\alpha_{\lambda}/|\alpha_{\lambda}|)^{f_{\lambda}}|\alpha_{\lambda}|^{-\eta_{\lambda}(\sigma+i\varphi_{\lambda})} \qquad (2)$$

in which α_{λ} denotes the image of α in k_{λ} (the latter being identified with $\boldsymbol{R}$ or with $\boldsymbol{C}$, as the case may be).

Conversely, assume that for some integral ideal $\mathfrak{m}$ of k we have a character ψ of the group $G(\mathfrak{m})$, and that there are integers f_{λ} and real numbers σ, φ_{λ} such that $\psi((\alpha))=\mathrm{X}(\alpha)$ for $\alpha\in k^{*}(\mathfrak{m})$, X being defined by (2). Let a be an idèle; there is a $\xi\in k^{*}$ such that, if we put $b=\xi a$, then, for every prime divisor $\mathfrak{p}$ of $\mathfrak{m}$, $b_{\mathfrak{p}}$ is a unit in $k_{\mathfrak{p}}$ and is $\equiv1$ modulo the highest power of $\mathfrak{p}$ dividing $\mathfrak{m}$; and ξ is uniquely determined in k^{*} modulo the subgroup $k^{*}(\mathfrak{m})$ of k^{*}. Now put:

$$\chi(a)=\psi((b))\prod_{\lambda}(b_{\lambda}/|b_{\lambda}|)^{-f_{\lambda}}|b_{\lambda}|^{\eta_{\lambda}(\sigma+i\varphi_{\lambda})}.$$

Our assumption on ψ implies that the right-hand side does not depend upon the choice of ξ when a is given; and one sees at once that χ is a character of I_k, taking the value 1 on P_k and satisfying (1), that its conductor $\mathfrak{f}$ divides $\mathfrak{m}$, and that the character $\tilde{\chi}$ of G $(\mathfrak{f})$ associated with χ coincides with ψ on $G(\mathfrak{m})$.

It is clear that $\alpha\rightarrow(\alpha)$ defines a homomorphism of $k^{*}(\mathfrak{m})$ into $G(\mathfrak{m})$ whose kernel is the group $E(\mathfrak{m})$ of all units ε in k such that $\varepsilon\equiv1$ mod. $\mathfrak{m}$; $E(\mathfrak{m})$ is of finite index in the group E of all units in k. Notations being as above, we see that X takes the value 1 on

$E(\mathfrak{f})$, so that, if m is the index of $E(\mathfrak{f})$ in E, χ^m takes the value 1 on E. Conversely, let the f_λ, σ, φ_λ be given; let χ be defined by (2); and assume that there is an integer $m>0$ such that χ^m is 1 on E. Then χ is 1 on a subgroup E' of E of finite index. By a theorem of Chevalley, this implies that there is an ideal $\mathfrak{m}$ such that $E'\supset E(\mathfrak{m})$; then χ is 1 on $E(\mathfrak{m})$ and therefore determines a character of the image of $k^*(\mathfrak{m})$ in $G(\mathfrak{m})$, which can then be extended to a character ψ of $G(\mathfrak{m})$, hence, for a suitable divisor $\mathfrak{f}$ of $\mathfrak{m}$, to a character $\tilde{\chi}$ of $G(\mathfrak{f})$ associated with a character χ of C_k with the conductor $\mathfrak{f}$.

A character χ of C_k is of finite order (in the group of all characters of C_k) if and only if it is 1 on the connected component of 1 in I_k, i.e. if and only if $f_\iota=0$ for all ι, $\varphi_\lambda=0$ for all λ, and $\sigma=0$; by class-field theory, such characters are those associated with the cyclic extensions of k; for such a χ, all values of $\tilde{\chi}$ are roots of unity. Our purpose is now to show that all the values of $\tilde{\chi}$ may be algebraic for certain characters χ which are not of finite order. In fact, assume that all the φ_λ are 0 and that σ is rational; then $\tilde{\chi}((\alpha))$ has algebraic values on $k^*(\mathfrak{f})$, i.e. $\tilde{\chi}$ has algebraic values on the image of $k^*(\mathfrak{f})$ in $G(\mathfrak{f})$; as that image is of finite index in $G(\mathfrak{f})$, all the values of $\tilde{\chi}$ must be algebraic. The f_λ and σ being given, a necessary and sufficient condition for the existence of such a character χ is, as we have seen, that there should be an integer m such that $\prod(\varepsilon_\lambda/|\varepsilon_\lambda|)^{mf_\lambda}=1$ for all $\varepsilon\in E$; replacing m by $2m$, this can also by written as

$$\prod_\iota(\varepsilon_\iota/\bar{\varepsilon}_\iota)^{mf_\iota}=1. \tag{3}$$

We shall say that χ is *of type* (A) if all the φ_λ are 0 and σ is rational; for such a character, the integers f_ι will be such that (3) holds, for a suitable m, for all $\varepsilon\in E$. Conversely, if the f_ι are given integers, and if there is an m such that (3) holds for all $\varepsilon\in E$, then there will be a character χ of type (A) belonging to the f_ι; and all such characters will be of the form $\chi(a)\chi_0(a)\|a\|^\rho$, where χ_0 is a character of finite order and ρ is rational.

In particular, if k is a totally imaginary quadratic extension of a totally real number-field k_0, then, by Dirichlet's theorem, the group E_0 of the units in k_0 is of finite index in E; if m is that index, ε^m must then be totally real for every $\varepsilon\in E$, so that (3) holds on E, for that value of m and for arbitrary values of the f_ι.

More generally (as Artin pointed out to me during the symposium), Minkowski's theorem on units in absolutely normal number-fields makes it possible to reduce the problem of finding all characters of type (A) of a field k to an exercise in Galois theory, and it will be enough here to state the result. Let k_0 be the maximal totally real subfield of k; then k contains at most one totally imaginary quadratic extension of k_0; for two such extensions could be written as $k_0(\sqrt{-\alpha})$, $k_0(\sqrt{-\beta})$, with α, β totally positive in k_0; then k contains the totally real field $k_0\ (\sqrt{\alpha\beta})$, which must be the same as k_0, so that the two extensions must be the same. Now let us call *trivial* those characters of type (A) which are of the form $\chi_0(a)\|a\|^\rho$, with χ_0 of finite order and ρ rational. In order for a field k to have non-trivial characters of type (A), it is necessary and sufficient that it should contain a totally imaginary quadratic extension k_1 of its maximal totally real subfield k_0; and then all such characters are of the form

$$\chi(a)=\chi_1(\mathrm{N}_{k/k_1}(a))\chi_0(a) \tag{4}$$

where χ_0 is of finite order, χ_1 is a character of type (A) of k_1, and N_{k/k_1} denotes the relative norm from I_k to I_{k_1}, which extends the relative norm of elements of k over k_1 in the obvious manner. Thus, in a certain sense, all non-trivial characters of type (A) come from totally imaginary quadratic extensions of totally real fields.

We shall say that a character χ is *of type* (A_0) if the character X of k^* associated with it according to (2) is of the form

$$\mathrm{X}(\alpha)=\pm\prod \alpha_\lambda{}^{r_\lambda}\bar{\alpha}_\lambda{}^{s_\lambda}$$

where the r_λ, s_λ are integers, and the sign may depend on α; such a character is called trivial if it is of the form $\chi_0(a)\|a\|^m$, with χ_0 of finite order and m an integer. Non-trivial characters of type (A_0) are those non-trivial characters of type (A) for which 2σ is an integer and $f_\iota\equiv 2\sigma$ mod. 2 for all ι. It is easily seen that the character χ of C_k defined by (4) is of type (A_0) if and only if the character χ_1 of C_{k_1} which appears in (4) is of type (A_0).

If χ is of type (A_0), the values taken by $\tilde{\chi}$ on the image of $k^*(\mathfrak{f})$ in $G(\mathfrak{f})$, which are the values taken by X on $k^*(\mathfrak{f})$, are all contained in the compositum of k and of its conjugates over $\mathbf{Q}$ (the rational number-field). As that image is of finite index in $G(\mathfrak{f})$, the values of $\tilde{\chi}$ on $G(\mathfrak{f})$ must all lie in a finite extension of this field. Thus:

If a character χ of the idèle-class group C_k of the field k is of type (A), the coefficients of the Hecke L-series associated with χ are algebraic numbers; if χ is of type (A_0), these coefficients all lie in a finite algebraic extension K of $\mathbf{Q}$.

It is tempting to conjecture that the converse statements are also true; but I have not examined this question. In the second statement, it would be of interest to determine the smallest field K containing all the coefficients of the L-series, i.e. containing all the values taken by $\tilde{\chi}$ on $G(\mathfrak{f})$. If N is the index in $G(\mathfrak{f})$ of the image of $k^*(\mathfrak{f})$ in $G(\mathfrak{f})$, then it is clear at any rate that all the values taken by χ^N on $G(\mathfrak{f})$ lie in the field K_0 generated by the values taken by X on k^*. The determination of K_0 amounts to an exercise in Galois theory; one should observe that K_0 need not contain k.

We now come back to the construction given above for χ when the values of χ are given on $G(\mathfrak{m})$, $\mathfrak{m}$ being a multiple of $\mathfrak{f}$. It obviously depends upon the following fact (which is equivalent to the theorem on the independence of valuations on k): If $I(\mathfrak{m})$ is the group of the idèles $a=(a_v)$ such that $a_\lambda=1$ for all λ, and $a_\mathfrak{p}=1$ for every prime divisor $\mathfrak{p}$ of $\mathfrak{m}$, then the group $P_k I(\mathfrak{m})$ is everywhere dense in I_k. It amounts to the same to say that the image of $I(\mathfrak{m})$ in C_k is everywhere dense in C_k. This implies that a character of C_k is completely determined by its values on $I(\mathfrak{m})$. We shall denote by $I'(\mathfrak{m})$ the compact subgroup of $I(\mathfrak{m})$ consisting of the idèles $a \in I(\mathfrak{m})$ such that $(a)=1$; then $I(\mathfrak{m})/I'(\mathfrak{m})$ is discrete and may be identified with $G(\mathfrak{m})$.

Let φ be any representation of C_k into a complete topological group Γ; as usual, we make no distinction between φ and the corresponding representation of I_k into Γ. Assume that there is an $\mathfrak{m}$ such that $\varphi=1$ on $I'(\mathfrak{m})$. Then φ determines a representation $\tilde{\varphi}$ of $G(\mathfrak{m})$ into Γ, and φ is uniquely determined by $\tilde{\varphi}$ since the image of $I(\mathfrak{m})$ in C_k is everywhere dense. We may now ask, conversely, whether, if a representation $\tilde{\varphi}$ of $G(\mathfrak{m})$ into Γ is given, it determines a representation φ of C_k into Γ. This will be so if and only if the representation into Γ of the image of $I(\mathfrak{m})$ in C_k which is determined by $\tilde{\varphi}$ is continuous for the topology induced on that image by the topology of C_k; for then it will be uniformly continuous, and can be extended by continuity. This is easily seen to amount to the following condition. To every neighborhood V of the neutral element in Γ, there must be an integer N and an $\varepsilon>0$ such that we have $\tilde{\varphi}((\alpha)) \in V$ for every $\alpha \in k^*(\mathfrak{m}^N)$ which satisfies the conditions $|\alpha_\lambda - 1| \leqq \varepsilon$ for all λ.

Now let χ be a character of C_k of type (A_0); then $\tilde{\chi}$ takes its values in a subfield K of $\mathbf{C}$, of finite degree over $\mathbf{Q}$. If $\mathfrak{m}$ is any multiple of the conductor of χ, we have, for $\alpha \in k^*(\mathfrak{m})$ and $\alpha_\rho>0$ for all ρ:

$$\tilde{\chi}((\alpha))=X(\alpha)=\prod_\lambda \alpha_\lambda{}^{r_\lambda}\bar{\alpha}_\lambda{}^{s_\lambda}.$$

Let w be any valuation of K, and let K_w be the completion of K with respect to w; the above criterion shows that $\tilde{\chi}$ determines a representation χ_w of C_k into K_w^*, satisfying $\chi_w(a)=\tilde{\chi}((a))$ for $a \in I(\mathfrak{m})$, provided *either* w is a valuation at infinity *or* w is attached to an ideal $\mathfrak{P}$ and we take $\mathfrak{m}=p\mathfrak{f}$, where p is the rational prime which is a multiple of $\mathfrak{P}$. As K is embedded in $\mathbf{C}$, we may of course take for w the valuation w_0 induced by the ordinary absolute value on $\mathbf{C}$; then $\chi_{w_0}=\chi$. Other valuations of K at infinity determine characters of C_k in the usual sense, i.e. representations of C_k into $\mathbf{C}$; the corresponding L-series are the conjugates over $\mathbf{Q}$ of the series attached to the given χ.

On the other hand, for each prime ideal $\mathfrak{P}$ in K, we get a representation $\chi_{\mathfrak{P}}$ of C_k into $K_{\mathfrak{P}}^*$, invariantly associated with χ. As the connected component of 1 in the group $K_{\mathfrak{P}}^*$ is $\{1\}$, $\chi_{\mathfrak{P}}$ takes the value 1 on the connected component of 1 in C_k. As C_k is the direct product of its maximal compact subgroup and of a group isomorphic to $\mathbf{R}$, and as $\chi_{\mathfrak{P}}$ takes the value 1 on the latter group, $\chi_{\mathfrak{P}}$ must map C_k onto a compact subgroup of $K_{\mathfrak{P}}^*$ and therefore onto a subgroup of the group $U_{\mathfrak{P}}$ of units in $K_{\mathfrak{P}}$. Now let ω be any character of the compact group $U_{\mathfrak{P}}$; as $U_{\mathfrak{P}}$ is the projective limit of finite groups, ω must be of finite order; therefore $\omega\circ\chi_{\mathfrak{P}}$ is a character of finite order of C_k, which, by class-field theory, determines a cyclic extension k' of k. If, for a given χ and $\mathfrak{P}$, we make all possible choices of ω, these cyclic extensions will generate a certain abelian extension $k(\chi, \mathfrak{P})$ of k; the compositum of these for all $\mathfrak{P}$ will be an abelian extension $k(\chi)$ of k which is thus invariantly attached to χ.

If χ is of finite order n, its values on I_k (not merely those on some $I(\mathfrak{m})$) are n-th roots of unity; then, for every w, χ_w is the transform of χ by an isomorphism into K_w^* of the multiplicative group of the n-th roots of unity; in that case, $k(\chi)$ is the cyclic extension attached to χ by class-field theory. In all other cases $k(\chi)$ will be an infinite extension of k. If χ is the trivial character $\chi(a)=||a||$, $k(\chi)$ is the maximal cyclotomic extension of k; more generally, if χ is any trivial character of type (A_0), $k(\chi)$ will be contained in the maximal cyclotomic extension of a cyclic extension of k of finite degree.

As to the non-trivial characters of type (A_0), some of them arise in connection with the theory of abelian varieties with complex multiplication; in fact, all the characters of type (A_0) can be expressed in terms of those which arise in that manner and of the trivial ones. Taniyama has proved that the L-series attached to the characters of type (A_0) belonging to abelian varieties with complex multiplication are precisely those which occur in the zeta-functions of such varieties; and his recent work (done since the symposium) has shown that the fields generated by the points of finite order on these varieties are closely related to the fields $k(\chi)$ defined above. For more general results, including these as rather special cases, the reader must be referred to his forthcoming publications; all that can be said here is that they tend to emphasize the importance of the characters which we have discussed and of their remarkable properties.

UNIVERSITY OF CHICAGO

On the Theory of Complex Multiplication

André WEIL

I shall concentrate chiefly on those aspects of my work which have not been duplicated by the parallel and independent investigations of Shimura and of Taniyama. A preliminary account of their results, which are more complete than my own in several important respects, appears in this same volume; it is understood that they will later give a full exposition of the whole theory.

We need the concept of *polarized variety*; the word "polarization" is chosen so as to suggest an analogy with the concept of "oriented manifold" in topology. Let V be a complete non-singular variety; X being a divisor on V, denote by $C(X)$ the class of all the divisors X' such that there are two integers m, m', both >0, for which $m'X'$ is algebraically equivalent to mX. We say that the class $C(X)$ determines a *polarization of* V if it contains at least one ample complete linear system, or in other words if there exists a projective embedding of V for which the hyperplane sections belong to $C(X)$. Thus a polarized variety may be regarded as a variety with a distinguished class of projective embeddings. The class $C(X)$ is uniquely determined by any divisor in it; every divisor in $C(X)$ will be called a polar divisor of V for the polarization determined by that class. It is clearly the same to say that a variety is polarizable or that it is projectively embeddable.

Let V be a variety, defined over a field k. Let X be a divisor on V, defining a polarization of V. If the smallest field containing k, over which X is rational, is not algebraic over k, then X belongs to an algebraic family, defined over an algebraic extension of k, and may be replaced by a member of that family, algebraically equivalent to X and algebraic over k. Thus we may assume that X itself is algebraic over k. Call Y the sum of all conjugates of X over k; if p is the characteristic, then, for a suitable m, $p^m Y$ will be rational over k; and one sees immediately that it determines a polarization of V, although not necessarily the same as the original one. We say that a *polarized* variety V is defined over k if V is defined over k and if there is on V a polar divisor which is rational over k; this amounts to saying that V has a projective embedding which is defined over k.

As an important example, we mention the case of the jacobian variety J of a curve Γ; the canonical divisor Θ on J (canonical, that is to say, up to a translation) determines a polarization of J which will be called its *canonical polarization*. A classical result, due to Torelli, and for which it would be worth while to give a modernized proof covering the abstract case, asserts that two curves are isomorphic if and only if their canonically polarized jacobians are isomorphic.

Let A be an abelian variety; we denote by A^* its dual, and by Cl the canonical homomorphism of $\mathcal{G}_a(A)$ onto A^*, with the kernel $\mathcal{G}_l(A)$. Every divisor X on A determines a homomorphism φ_X of A into A^*, defined by $\varphi_X u = \mathrm{Cl}\,(X_u - X)$. If $p=0$, the degree $\nu(\varphi_X)$ of φ_X is always the square of an integer. If $X \succ 0$, $\nu(\varphi_X)$ is >0, i.e. φ_X is surjective, if and only if there is an $m>0$ such that mX determines an ample complete linear system on A, i.e. if and only if X determines a polarization of A. Conversely, let A be polarized; then every polar divisor X on A determines a homomorphism φ_X of A onto A^*; in the extension $\mathcal{H}(A, A^*)\otimes\mathbf{Q}$ by $\mathbf{Q}$ of the group of homomorphisms of A into A^*, φ_X is uniquely determined by the polarization of A up to a positive rational factor. If ψ is a homomorphism of A^* onto A such that $\psi\varphi_X$ is of the form $m\delta_A$, then $\psi^{-1}(X)$ determines a polarization of A^* which is canonically associated with that of A. In the case $p=0$, there will be a polar divisor X on A such that every polar divisor is algebraically equivalent to a multiple mX of X; such a divisor will be called *basic*; if, for such a divisor X, we put $\nu(\varphi_X)=r^2$, r is called the *rank* of the polarized variety A.

As usual, if A, B are abelian varieties, $\mathcal{H}(A, B)$ will denote the additive group of homomorphisms of A into B, $\mathcal{H}_0(A, B)$ its extension by $\mathbf{Q}$ (i.e. the vector-space $\mathcal{H}(A, B)\otimes\mathbf{Q}$ over $\mathbf{Q}$), $\mathcal{A}(A)$ the ring of endomorphisms of A, $\mathcal{A}_0(A)$ its extension by $\mathbf{Q}$. If $\lambda\in\mathcal{H}_0(A, B)$ and $\nu(\lambda)\neq 0$ (which implies that A, B have the same dimension, since the "degree" $\nu(\lambda)$ of λ is not defined otherwise), then λ^{-1} is defined and is in $\mathcal{H}_0(B, A)$. If λ is a homomorphism of A into B, its transpose ${}^t\lambda$ is the homomorphism of B^* into A^* defined by ${}^t\lambda(\mathrm{Cl}\,Z)=\mathrm{Cl}\,(\lambda^{-1}(Z))$ for every $Z\in\mathcal{G}_a(B)$; this extends to an isomorphism of $\mathcal{H}_0(A, B)$ onto $\mathcal{H}_0(B^*, A^*)$.

If A is a polarized abelian variety, and X is a polar divisor of A, put, for every $\alpha\in\mathcal{A}_0(A)$, $\alpha'=\varphi_X^{-1}\cdot{}^t\alpha\cdot\varphi_X$; then $\alpha\rightarrow\alpha'$ is an involutory antiautomorphism of the algebra $\mathcal{A}_0(A)$, canonically attached to the polarization of A. The trace σ being defined on $\mathcal{A}_0(A)$ as usual, we have $\sigma(\alpha\alpha')>0$ for every $\alpha\neq 0$ in $\mathcal{A}_0(A)$. If A is the (canonically polarized) jacobian of a curve, then $\alpha\rightarrow\alpha'$ is no other than the so-called "Rosati antiautomorphism".

Let λ be a homomorphism of an abelian variety A onto an abelian variety B of the same dimension; if Y is a divisor on B, and if we put $X=\lambda^{-1}(Y)$, we have $\varphi_X={}^t\lambda\cdot\varphi_Y\cdot\lambda$; in particular, if Y determines a polarization on B, so does X on A. If A is polarized and X is a polar divisor of A, and if α is an automorphism of the non-polarized A, then it will be an automorphism of the polarized A if and only if there are integers m, m', both >0, such that $m\varphi_X=m'{}^t\alpha\cdot\varphi_X\cdot\alpha$; taking degrees on both sides, we get $m=m'$. But this may be written as $\alpha'\alpha=\delta_A$ and implies $\sigma(\alpha'\alpha)=\sigma(\delta_A)$. As $\sigma(\alpha'\alpha)$ is a positive non-degenerate quadratic form on $\mathcal{A}_0(A)$, and the additive group of $\mathcal{A}(A)$ is finitely generated, this shows that the group of automorphisms of a polarized abelian variety is finite (a result originally due to Matsusaka, whose proof, based on a different idea, is to appear shortly).

From now on, A will be a polarized abelian variety of dimension n; we usually write $\mathcal{A}$, $\mathcal{A}_0$ instead of $\mathcal{A}(A)$, $\mathcal{A}_0(A)$; on $\mathcal{A}_0$, we have the trace σ and the antiautomorphism $\alpha\rightarrow\alpha'$. For every prime l, not equal to the characteristic, $\mathcal{A}$ has a faithful representation R_l of trace σ by endomorphisms of a free module of rank $2n$ over the l-adic integers; this can be extended to a representation R_l of $\mathcal{A}_0$ by endomorphisms of a vector-space of dimension $2n$ over l-adic numbers. If the characteristic is 0, $\mathcal{A}$ has a faithful representation R of trace σ by endomorphisms of a free abelian group of rank $2n$ (viz., the fundamental group of the complex torus defined by A under any embedding of its field of definition into $\mathbf{C}$); this can be extended to a representation R of $\mathcal{A}_0$ in a vector-space of dimension $2n$ over $\mathbf{Q}$; and the representations R_l can be derived from R by extending the group (resp. the vector-space) on which R operates by the ring of l-adic integers (resp. by the l-adic number-field). Moreover, $\mathcal{A}$ may also be considered as operating on the Lie algebra of A, i.e. on the tangent vector-space to A at 0; if $p=0$, this can be extended to a representation R_0 of $\mathcal{A}_0$ by endomorphisms of a vector-space of dimension n over any common field of definition for A and its endomorphisms. By embedding such a field into $\mathbf{C}$, one finds that R decomposes over $\mathbf{C}$ into R_0 and the imaginary conjugate representation $\bar{R}_0$; if we call σ_0 the trace of R_0, we have $\sigma=\sigma_0+\bar{\sigma}_0$.

Let $\varepsilon_1,\cdots,\varepsilon_h$ be orthogonal idempotents in $\mathcal{A}_0$, i.e. elements such that $\varepsilon_i^2=\varepsilon_i$ for all i and $\varepsilon_i\varepsilon_j=0$ for $i\neq j$; put $\varepsilon_0=\delta_A-\sum\varepsilon_i$; we can write $\varepsilon_i=\alpha_i/m$, where m is an integer and $\alpha_0,\cdots,\alpha_h$ are in $\mathcal{A}$. Call

A_i the image of A by α_i; then it is easy to see that A is isogenous to $A_0\times\cdots\times A_h$, and that $\sigma(\varepsilon_i)=2\dim(A_i)$.

Let C be a semi-simple commutative subalgebra of $\mathcal{A}_0$; in terms of suitable orthogonal idempotents $\varepsilon_1,\cdots,\varepsilon_h$, it can be written as $C=\sum K_i\varepsilon_i$, where the K_i are fields. As $\mathcal{A}_0$ has faithful representations with the rational-valued trace σ, C has representations of the same type; this implies that, if $\xi=\sum\xi_i\varepsilon_i$ is in C, with $\xi_i\in K_i$ for $1\leqq i\leqq h$, we have $\sigma(\xi)=\sum\nu_i\operatorname{Tr}(\xi_i)$, where Tr is the ordinary trace (taken in K_i over $\mathbf{Q}$ for each i) and the ν_i are integers >0. If the A_i are defined as above, we have $2\dim(A_i)=\sigma(\varepsilon_i)=\nu_i[K_i:\mathbf{Q}]$, hence $\sum\nu_i[K_i:\mathbf{Q}]\leqq 2n$. Assume now that $\sum[K_i:\mathbf{Q}]\geqq 2n$; then the latter inequality must be an equality, and we must have $\nu_i=1$ for all i. That being so, a representation of $\mathcal{A}_0$ of trace σ is equivalent (over an algebraically closed field) to one in which all elements of C appear as diagonal matrices and in which the diagonal elements corresponding to some element of C are all distinct; then the commutor C' of C in $\mathcal{A}_0$ is also represented by diagonal matrices, which implies that it is commutative and semi-simple; what we have said about C can now also be applied to C', and it easily follows from this that $C'=C$.

In particular (as Shimura also proved), if $\mathcal{A}_0$ contains a field K of degree $\geqq 2n$, K must be of degree $2n$, must contain δ_A and the center of $\mathcal{A}_0$, and is a maximal commutative subalgebra of $\mathcal{A}_0$. When that is so, A must be isogenous to a product $B\times\cdots\times B$, where B is simple; in fact, if this were not so, $\mathcal{A}_0$ would be the direct sum of algebras $\mathcal{A}_0(A_i)$, the A_i being proper subvarieties of A, at least one of which would have to contain a field isomorphic to K, while we have just shown that $\mathcal{A}_0(A_i)$ cannot contain a field of degree $>2\dim(A_i)$. Assume now that A is isogenous to a product $B\times\cdots\times B$ of r factors B of dimension m, so that $n=rm$; then $\mathcal{A}_0$ is the ring of matrices of order r over the division-algebra $\mathcal{B}_0=\mathcal{A}_0(B)$. Call k the center of $\mathcal{B}_0$, which we identify with the center of $\mathcal{A}_0$, so that $K\supset k$; call ν the degree of k, ρ^2 the dimension of $\mathcal{B}_0$ as a vector-space over k. As K is of degree $2n/\nu$ over k and is maximally commutative in $\mathcal{A}_0$, it is known that $\mathcal{A}_0$, as a vector-space over k, must be of dimension $(2n/\nu)^2$; this gives $r\rho=2n/\nu$, hence $2m=\rho\nu$; therefore a maximal subfield of $\mathcal{B}_0$, containing k, is of degree $2m$. If now we assume that $p=0$, $\mathcal{B}_0$ must have a faithful representation by rational matrices of order $2m$; as it is known that the order of such a representation must be a multiple of $\nu\rho^2$, this gives $\rho=1$, $\mathcal{B}_0=k$. Moreover, any polarization of B determines an automorphism $\xi\to\xi'$ of k, of order 1 or 2, such that $\operatorname{Tr}(\xi\xi')\geqq 0$; if k_0 consists of the elements of k invariant under that automorphism, this implies that k_0 must be a totally real field, and that k is either k_0 or a totally imaginary quadratic extension of k_0. As before, call R_0 the representation of $\mathscr{A}_0$ determined by the Lie algebra of A; call S_0 the representation of $\mathscr{B}_0$ which is similarly defined; then the representation of k of trace $\mathrm{Tr}_{k/Q}$ decomposes into S_0 and $\bar{S}_0$; this implies that $k \neq k_0$ and that S_0 is the direct sum of m one-dimensional representations of $\mathscr{B}_0$, i.e. of m isomorphisms φ_λ of k into the universal domain, inducing on k_0 all its distinct isomorphisms into the algebraic closure $\bar{\mathbf{Q}}$ of $\mathbf{Q}$. Moreover, R_0 induces on k the representation $(n/m)S_0$; this implies that R_0 induces on K the sum of the one-dimensional representations $\varphi_{\lambda i}(1 \leqq \lambda \leqq m,\ 1 \leqq i \leqq n/m)$, where, for each λ, the $\varphi_{\lambda i}$ are all the isomorphisms of K into $\bar{\mathbf{Q}}$ which induce φ_λ on k.

Still assuming $p=0$, consider now any field K of degree $2n$ containing a totally imaginary quadratic extension k of a totally real field k_0, the latter being of degree m. Let the ψ_λ be all the isomorphisms of k_0 into $\bar{\mathbf{Q}}$; for each λ, let φ_λ be an isomorphism of k into $\bar{\mathbf{Q}}$, inducing ψ_λ on k_0, and let the $\varphi_{\lambda i}$, for $1 \leqq i \leqq n/m$, be all the isomorphisms of K into $\bar{\mathbf{Q}}$ which induce φ_λ on k. We ask for the abelian varieties A of dimension n such that $\mathscr{A}_0(A)$ contains a field isomorphic to K and that R_0 induces on K a representation which is the sum of the $\varphi_{\lambda i}$. Taking $\mathbf{C}$ as universal domain, it is easily seen that A is uniquely defined by these conditions up to an isogeny over $\mathbf{C}$ and that it can be constructed as follows. Consider the mapping $\xi \rightarrow (\varphi_{\lambda i}(\xi))$ of K into $\mathbf{C}^n$; let M be the image under that mapping of a "module" $\mathfrak{m}$ in K, i.e. of a free abelian subgroup of rank $2n$ of the additive group of K; then the complex torus $\mathbf{C}^n/M$ defines an abelian variety A with the required properties. If $(\xi_1, \cdots, \xi_{n/m})$ is a basis for K considered as a vector-space over k, we may in particular take $\mathfrak{m} = \sum \xi_i \mathfrak{n}$, where $\mathfrak{n}$ is a module in k; then one finds that A is the product of n/m varieties B of dimension m. This shows that A cannot be simple unless $n=m$.

By a *CM-extension* of a totally real field K_0 of degre n over $\mathbf{Q}$, we shall understand a system $(K; \{\varphi_\lambda\})$ consisting of a totally imaginary quadratic extension K of K_0 and of n isomorphisms φ_λ of K into $\bar{\mathbf{Q}}$, inducing on K_0 all the isomorphisms of K_0 into $\bar{\mathbf{Q}}$. If we consider $\bar{\mathbf{Q}}$ as embedded in $\mathbf{C}$, K can then be written as $K_0(\zeta)$, where ζ is such that $-\zeta^2$ is a totally positive element of K_0 and that all the $\varphi_\lambda(\zeta)$ have a positive imaginary part; ζ is uniquely determined by that condition up to a totally positive factor in K_0; conversely, the CM-extension $(K; \{\varphi_\lambda\})$ is uniquely determined by K_0 and ζ and will also be written as $K_0((\zeta))$. The CM-extension $K_0((\zeta))$ will be called *primitive* if it cannot be written as $K_0((\zeta_1))$ with ζ_1^2 lying in a proper subfield of K_0; $K_0((\zeta))$ is primitive if and only if there is no conjugate ζ' of ζ over $\mathbf{Q}$, other than ζ, such that ζ'/ζ is a totally positive algebraic number. The proof given above shows that every CM-extension of a totally real field of degree n determines a "category" of mutually isogenous abelian varieties of dimension n, and that the latter are simple if and only if the former is primitive.

In consequence, it seems reasonable to deal first with the simple abelian varieties belonging to primitive CM-extensions, even though some important results have already been obtained by Taniyama for more general cases. From now on, let $(k; \{\varphi_\lambda\})$ be a primitive CM-extension, given once for all, of a totally real field k_0 of degree n; we consider the abelian varieties A of dimension n which belong to it in the sense described above. This means that there is an isomorphism φ of k onto $\mathcal{A}_0(A)$ such than $R_0\circ\varphi$ decomposes into the sum of the φ_λ. As $(k; \{\varphi_\lambda\})$ is primitive, it is easily seen that φ is uniquely determined by this condition, so that it may be used to identify k with $\mathcal{A}_0(A)$; this identification will be made from now on. Then the ring $\mathcal{A}(A)$ is identified with a subring $\mathfrak{r}$ of the ring $\mathfrak{o}$ of all integers in k. If K is a field of definition for A and for all the endomorphisms of A, k will have a representation of trace $\sum\varphi_\lambda$ by matrices of order n over the field K. One finds that, for k to have such a representation, it is necessary and sufficient that K should contain the field k_t generated over $\mathbf{Q}$ by the values taken by that trace on k. Conversely, if K is a field of definition for A, containing k_t, it must be a field of definition for all the endomorphisms of A. One should observe that k_t need not contain k.

We now consider *polarized* abelian varieties belonging to a given CM-extension. The rank of such a variety, for $p=0$, has been defined above as the integer $r=\nu(\varphi_X)^{1/2}$ if X is a basic polar divisor. By using the representation of our varieties as complex toruses when $\boldsymbol{C}$ is taken as universal domain, one finds that, *for a given CM-extension* $(k; \{\varphi_\lambda\})$, *a given ring of endomorphisms* $\mathfrak{r}$, *and a given value of the rank* r, *there is at most a finite number of distinct types of polarized abelian varieties* with respect to isomorphism over the universal domain.

If A is such a variety, its group of automorphisms is the multiplicative group of the roots of unity in $\mathfrak{r}$. Call ω a generator of that group, and N its order. Let K be a field of definition for the polarized variety A and for its automorphism ω; let X be a positive polar divisor on A, of which we may assume that it is rational over K and that it determines an ample complete linear system; after replacing X, if necessary, by the sum of its transforms by the N automorphisms of A, we may also assume that it is invariant by ω. Now identify A with its image under the projective embedding of A defined by the complete linear system determined by X; then ω is induced on A by an automorphism Ω of the ambient projective space which leaves invariant the hyperplane H_0 such that $H_0 \cdot A = X$. If we take the homogeneous coordinates $(X_0, \cdots, X_m)$ in that space so that H_0 is defined by $X_0 = 0$, Ω will appear as a linear substitution:

$$(X_0, X_1, \cdots, X_m) \to (X_0, \sum_{i=0}^{m} c_{1i} X_i, \cdots, \sum_{i=0}^{m} c_{mi} X_i).$$

For any $r \geqq m$, let the $P_{r\nu}$ be a base for the space of homogeneous polynomials of degree rN in the X_i which are invariant under that substitution; let U_r be the locus of the point $\Phi(x)$ with the homogeneous coordinates $P_{r\nu}(x)$, in a projective space of suitable dimension, when x is a generic point of the ambient space of A. By adjoining the N-th roots of unity, if necessary, to the groundfield, and writing the substitution Ω in diagonal form, one shows that all the varieties U_r are isomorphic to one another. Call U any one of them; call V the image of A in U by Φ, and call F the mapping of A onto V induced by Φ; we say that V, together with the mapping F, is the quotient of A by the group generated by ω.

Now, for each one of the finitely many types of varieties belonging to given data $(k; \{\varphi_\lambda\})$, $\mathfrak{r}$, r, we can construct a representative A by means of a complex torus. A variety A obtained by this method need of course not be defined over an algebraic number-field. However, I have given (in a paper just published in the *Amer. J. of Math*[1].) a criterion for a variety, defined over a field K_1, to be isomorphic to a variety defined over a subfield K_0 of K_1; by using this criterion, it is easily seen that, for each type of varieties belonging to the given data, there is a representative which is defined over an algebraic number-field. As this is only a special case of some important unpublished results of T. Matsusaka on the field of moduli of a polarized abelian variety, I need not give more details here; however, it will be worthwhile to consider more closely the case in which A is defined over an algebraic number-field, even though Matsusaka's results could also be applied to that case. Let therefore A be a

[1] A. Weil, The field of definition of a variety, Amer. J. of Math., 78 (1956), pp. 509-524.

polarized abelian variety belonging to the given data and defined over an algebraic number-field which we may assume to be a finite Galois extension K of k_t. Let K_0 be the field of the elements of K which are invariant under all those automorphisms of K over k_t which transform A into a variety isomorphic to A; the degree of K_0 over k_t is at most equal to the number of possible types of varieties belonging to the given data. Let σ be an automorphism of K over K_0; there is an isomorphism α_σ of A onto A^σ, uniquely determined up to an automorphism of A and algebraic over K; therefore every conjugate of α_σ over K is of the form $\alpha_\sigma\omega^\nu$. Call V the quotient of A by its group of automorphisms, and F the canonical mapping of A onto V; then there is an isomorphism β_σ of V onto V^σ, uniquely determined by the condition $\beta_\sigma\circ F=F^\sigma\circ\alpha_\sigma$; it must be the same as its conjugates over K, and is therefore defined over K; and we have $\beta_{\tau\sigma}=\beta_\tau^\sigma\circ\beta_\sigma$ for any two automorphisms τ, σ of K over K_0. Applying the results of the paper quoted above, we conclude from this that there is a variety V_0 defined over K_0 and an isomorphism φ of V_0 onto V, defined over K, such that $\beta_\sigma=\varphi^\sigma\circ\varphi^{-1}$. Let now A_1 be any variety, isomorphic to A, defined over an algebraic number-field K_1 containing k_t. If K_1 does not contain K_0, there must be an automorphism τ of the field of all algebraic numbers over K_1 which does not leave invariant all elements of K_0; then, if α_1 is an isomorphism of A onto A_1, its transform by τ is an isomorphism of A^τ onto A_1, so that A and A^τ must be isomorphic; but this contradicts the definition of K_0. Therefore we have $K_1\supset K_0$. If now V_1 is the quotient of A_1 by its group of automorphisms, F_1 the canonical mapping of A_1 onto V_1, β_1 the isomorphism of V onto V_1 such that $\beta_1\circ F=F_1\circ\alpha_1$, and σ any automorphism of KK_1 over K_1, we have $\beta_1^\sigma=\beta_1\circ\beta_\sigma^{-1}$, hence $(\beta_1\varphi)^\sigma=\beta_1\varphi$, which shows that $\beta_1\varphi$ is an isomorphism of V_0 onto V_1, defined over K_1.

Call z a generic point of A over K, and w the corresponding point on V_0, i.e. $w=\varphi^{-1}(F(z))$. To each primitive N-th root of unity ε, we can associate the set of those functions θ on A, defined over $\overline{\mathbf{Q}}$, which satisfy $\theta(\omega z)=\varepsilon\theta(z)$; for each such function, there is a function f on V_0 such that $f(w)=\theta(z)^N$; call $\mathcal{F}_\varepsilon$ the set consisting of those functions f on V_0. If $f\in\mathcal{F}_\varepsilon$, and ε^ν is another primitive N-th root of unity, ν being an integer prime to N, then $\mathcal{F}_{\varepsilon^\nu}$ consists of the functions $f^\nu h^N$, where h runs through the set of all functions on V_0, defined over $\overline{\mathbf{Q}}$; also, if an automorphism of $\overline{\mathbf{Q}}$ over K_0 maps ε onto ε^ν, it will transform the functions in $\mathcal{F}_\varepsilon$ into the functions in $\mathcal{F}_{\varepsilon^\nu}$. We say that V_0, together with the sets of functions $\mathcal{F}_\varepsilon$, is the *Kummer variety* attached to the given type of abelian varieties (for a more general definition, valid for arbitrary polarized abelian varieties, we refer the reader to a forthcoming publication by Matsusaka); and we say that this Kummer variety is defined over K_0. It is clear that a type of abelian varieties is completely determined by its Kummer variety.

We can now formulate the basic problems of complex multiplication for *simple* abelian varieties:

I. *Characterize the fields* K_0 *for the types of abelian varieties belonging to given data* $(k; \{\varphi_\lambda\})$, $\mathfrak{r}$ *and* r.

II. For each such type, *characterize the fields generated over* K_0 *by the images on* V_0 *of the points of finite order on a variety* A *of that type.*

III. *Determine the zeta-function of any abelian variety of the given type, over a field of definition of that variety containing* k_t *and therefore* K_0.

For $n=1$, the complete solution of problems (I) and (II) is given by the classical theory of complex multiplication, and problem (III) was solved recently by Deuring. For arbitrary n, Taniyama has now solved a problem which includes the general case of (III) as a special case; the independent and overlapping investigations of Shimura, Taniyama and myself give the solution of (I) and (II) in the case $\mathfrak{r}=\mathfrak{o}$; and one may hope that the general case will not offer insurmountable difficulties any more. The basic tool here is Shimura's theory of reduction modulo a prime ideal, by means of which our problems can be reduced to problems on abelian varieties over finite fields. I shall sketch briefly the main ideas involved here.

As above, let A be a variety of one of the given types, defined over a field K containing k_t. Shimura's theory shows that, for almost all prime ideals $\mathfrak{P}$ in K (i.e., for all except a finite number), one can reduce A and its endomorphisms modulo $\mathfrak{P}$, obtaining an abelian variety $A(\mathfrak{P})$ of dimension n defined over the finite field with $N(\mathfrak{P})$ elements and an isomorphism of $\mathfrak{r}=\mathcal{A}(A)$ into $\mathcal{A}(A(\mathfrak{P}))$. Then the Frobenius endomorphism of $A(\mathfrak{P})$ (induced by the automorphism of the universal domain which raises every element to its $N(\mathfrak{P})$-th power) commutes with every element of the image of $\mathfrak{r}$ in $\mathcal{A}(A(\mathfrak{P}))$, since such an element is an endomorphism of $A(\mathfrak{P})$ which is defined over the field with $N(\mathfrak{P})$ elements. By the results proved above, this implies that the Frobenius endomorphism can be identified with an element π of the field $k=\mathcal{A}_0(A)$, and more precisely with an integer in k (not necessarily in $\mathfrak{r}$). The mapping $\mathfrak{P}\to\pi$ determines the zeta-function of A over K; and Taniyama has shown that a more detailed study of the properties of this mapping leads directly to an expression of the zeta-function *in terms of Hecke L-functions attached to characters of type* (A_0) *of the field* K (cf. p. 4 of this volume); as could be expected, these are characters which come from the quadratic extension k of the totally real k_0 (in the sense of formula (4), p. 4). In fact, the connection between characters "of type (A_0)" and abelian varieties with complex multiplication appears to be so close that it can hardly be accidental; and any future arithmetical interpretation of the characters of type (A_0), corresponding to the interpretation given by class-field theory for the characters of finite order of the idèle-class group, ought to take complex multiplication into account.

As to problems (I) and (II), I will consider only the case $\mathfrak{r}=\mathfrak{o}$. The method sketched below could perhaps be applied without substantial changes to a ring $\mathfrak{r}$ such that $\mathfrak{r}=\bar{\mathfrak{r}}$ and that the classes of ideals in $\mathfrak{r}$ which belong properly to $\mathfrak{r}$ (i.e. which consist of ideals $\mathfrak{m}$ such that, in Dedekind's notation, $\mathfrak{m}:\mathfrak{m}=\mathfrak{r}$) form a group. If $n=1$, all the subrings of $\mathfrak{o}$ have these properties; for $n>1$, it does not seem to be known whether any proper subring of $\mathfrak{o}$ has them; in order to treat the general case of problems (I) and (II), one will presumably have to rely more heavily upon the l-adic representations R_l than is done here.

We first have to look more closely into the relation between k and k_t. Taking $\mathbf{C}$ as universal domain, and taking k to be embedded in it, call k' the compositum of k and all its conjugates over $\mathbf{Q}$; call G the Galois group of k' over $\mathbf{Q}$; call H, H_t the subgroups of G corresponding respectively to the subfields k, k_t of k'; call σ the automorphism $\xi\rightarrow\bar{\xi}$ of k'. Call S the set of those automorphisms of k' over $\mathbf{Q}$ which induce on k one of the isomorphisms φ_λ. Thus S is the union of cosets with respect to H, i.e. we have $HS=H$: we have $G=S\smile S\sigma$; more generally, if σ' is any transform of σ by an inner automorphism of G, we have $G-S=S\sigma'=\sigma'S$. The assumption that $(k;\{\varphi_\lambda\})$ is primitive amounts to saying that H consists of all the elements γ of G such that $\gamma S=S$. On the other hand, H_t consists of the elements γ' of G such that $S\gamma'=S$. The subgroup of G corresponding to k_0 is $H\smile H\sigma$; and one finds that $H_t\smile\sigma H_t$ is a group, corresponding to a totally real subfield of k' of which k_t is a totally imaginary quadratic extension. Write S as the union of distinct cosets $\mu^{-1}H_t$ with respect to H_t; for each μ, let ψ_μ be the isomorphism of k_t into k' induced by μ on k_t. Then $(k_t;\{\psi_\mu\})$ is a primitive CM-extension, and the relation between $(k;\{\varphi_\lambda\})$ and $(k_t;\{\psi_\mu\})$ is symmetric. This suggests that one should look for a relation between the categories of abelian varieties belonging to these CM-extensions; as to what this may be, I have no conjecture to offer.

Before coming back to our problems, we must also observe that, for any abelian varieties A and B, $\mathcal{H}(A, B)$ is a right $\mathcal{A}(A)$-module and a left $\mathcal{A}(B)$-module. If φ is an isomorphism of a commutative subring C of $\mathcal{A}(A)$ onto a subring of $\mathcal{A}(B)$, and if one considers only those $\lambda \in \mathcal{H}(A, B)$ for which $\lambda\gamma = \varphi(\gamma)\lambda$ for all $\gamma \in C$, the distinction between right and left is not necessary. In particular, consider two abelian varieties A, A' of dimension n, belonging as above to the primitive CM-extension $(k; \{\varphi_\lambda\})$. Then they are isogenous; and, by considering the operation of $\mathcal{H}(A, A')$ on the Lie algebra of A, one sees that $\alpha\xi = \xi\alpha$ for all $\alpha \in \mathcal{H}_0(A, A')$ and all $\xi \in k$. Thus $\mathcal{H}_0(A, A')$ is a vector-space over k; as such, it is clearly of dimension 1; and $\mathcal{H}(A, A')$ is a module over the ring generated in k by $\mathcal{A}(A)$ and $\mathcal{A}(A')$. If now we assume that $\mathcal{A}(A) = \mathcal{A}(A') = \mathfrak{o}$, then $\mathcal{H}(A, A')$ is an $\mathfrak{o}$-module, isomorphic to an $\mathfrak{o}$-ideal whose class is uniquely determined; if α is a non-zero element of $\mathcal{H}_0(A, A')$, and if $\mathfrak{a}$ is the set of the $\xi \in k$ such that $\xi\alpha \in \mathcal{H}(A, A')$, $\mathfrak{a}$ is an ideal in that class. If we take $\alpha \in \mathcal{H}(A, A')$, we have $1 \in \mathfrak{a}$, so that $\mathfrak{a}^{-1}$ is an ideal in $\mathfrak{o}$.

In particular, the dual A^* of A is isogenous to A; and, if A is polarized and Y is a basic divisor on A, φ_Y is in $\mathcal{H}(A, A^*)$. If we assume A to have $\mathfrak{o}$ as its ring of endomorphisms, the same will be true of A^*, and the set of the $\xi \in k$ such that $\xi\varphi_Y \in \mathcal{H}(A, A^*)$ will be an $\mathfrak{o}$-ideal in k. One finds, in fact, that it can be written as $\mathfrak{f}_0^{-1}\mathfrak{o}$, where $\mathfrak{f}_0$ is an ideal in the ring of integers of k_0, and that the rank r of A is $r = N(\mathfrak{f}_0)$. When that is so, we say that A belongs to $\mathfrak{f}_0$; it is clear that all the conjugates of A over k_t will belong to $\mathfrak{f}_0$. Thus, in discussing our problems (I) and (II) for $\mathfrak{r} = \mathfrak{o}$, we may confine our attention to those types which belong to $(k; \{\varphi_\lambda\})$, $\mathfrak{r} = \mathfrak{o}$ and a fixed $\mathfrak{f}_0$.

Let A, A' be two such varieties; let Y, Y' be basic divisors on A, A'; if $\alpha \in \mathcal{H}(A, A')$, and if we put $Z = \alpha^{-1}(Y')$, $\varphi_Y^{-1}\varphi_Z$ will be in k; one finds that in fact it must be a totally positive integer; call it $f(\alpha)$. Take an $\alpha \neq 0$ in $\mathcal{H}_0(A, A')$, so that we can write $\mathcal{H}(A, A') = \mathfrak{a}\alpha$, where $\mathfrak{a}$ is an $\mathfrak{o}$-ideal in k; then one finds that there is a totally positive $\rho \in k_0$ such that $\rho\mathfrak{a}\bar{\mathfrak{a}} = \mathfrak{o}$ and that $f(\xi\alpha) = \rho\xi\bar{\xi}$ for all $\xi \in \mathfrak{a}$. One may call this a positive hermitian form on $\mathfrak{a}$. The form $\rho\xi\bar{\xi}$, defined on $\mathfrak{a}$, and the form $\rho_1\xi\bar{\xi}$, defined on an ideal $\mathfrak{a}_1$, will be called equivalent if there is a $\lambda \in k$ such that $\mathfrak{a}_1 = \lambda^{-1}\mathfrak{a}$ and $\rho_1 = \rho\lambda\bar{\lambda}$; the class determined for this equivalence relation by the form $\rho\xi\bar{\xi}$ on $\mathfrak{a}$ will be denoted by $(\mathfrak{a}; \rho)$. That being so, the class of the form $f(\xi\alpha)$ on the ideal $\mathfrak{a}$ determined by $\mathcal{H}(A, A')=\mathfrak{a}\alpha$ is independent of the choice of α and will be denoted by $\{A': A\}$; A and A' are isomorphic if and only if this class is $(\mathfrak{o}\,; 1)$. On the classes of forms, we define a group law by putting

$$(\mathfrak{a}\,;\ \rho)\cdot(\mathfrak{a}'\,;\ \rho')=(\mathfrak{a}\mathfrak{a}'\,;\ \rho\rho').$$

Then, if A, A', A'' all belong to the same type, we have:

$$\{A''\colon A\}=\{A''\colon A'\}\cdot\{A'\colon A\};$$

and, if τ is any automorphism of $\overline{\mathbf{Q}}$ over k_t, we have $\{A'^{\tau}\colon A^{\tau}\}=\{A'\colon A\}$. It immediately follows from this that every field K_0 occurring in problem (I) for $\mathfrak{r}=\mathfrak{o}$ is abelian over k_t, with a Galois group which is isomorphic to a subgroup of the group of classes of forms $(\mathfrak{a};\ \rho)$.

Take a field of definition K for A, A' and their endomorphisms and homomorphisms; again by Shimura's theory, we can reduce all of these modulo almost all prime ideals in K. For such a prime $\mathfrak{P}$, $\mathcal{H}(A, A')$ is mapped isomorphically onto its image in $\mathcal{H}(\mathfrak{P})=\mathcal{H}(A(\mathfrak{P}), A'(\mathfrak{P}))$ and may be identified with that image; similarly we can identify $\mathcal{H}_0(A, A')$ with its image in the extension of $\mathcal{H}(\mathfrak{P})$ by $\mathbf{Q}$. One sees at once that an element of the latter set is in $\mathcal{H}_0(A, A')$ if and only if it commutes with all elements of k. Now put $\mathcal{H}'=\mathcal{H}(\mathfrak{P})\frown\mathcal{H}_0(A, A')$; this is clearly an $\mathfrak{o}$-module containing $\mathcal{H}(A, A')$; we show that $\mathcal{H}'=\mathcal{H}(A, A')$. In fact, assume that this is not so; as both are $\mathfrak{o}$-modules, there will be a ξ in k and not in $\mathfrak{o}$ such that $\xi\mathcal{H}(A, A')\subset\mathcal{H}'$. But (e.g. by using a representation of A, A' as complex toruses over $\mathbf{C}$) one can see that there are elements α_i of $\mathcal{H}(A, A')$ and elements α'_i of $\mathcal{H}(A', A)$ such that $\delta_A=\sum\alpha'_i\alpha_i$ (this is a special case of the fact that, if A, A', A'' are three varieties of the given type, $\mathcal{H}(A, A'')$ is no other than the tensor-product, taken over $\mathfrak{o}$, of the $\mathfrak{o}$-modules $\mathcal{H}(A, A')$ and $\mathcal{H}(A', A'')$). This gives $\xi=\sum\alpha'_i\cdot(\xi\alpha_i)$, so that ξ must be an endomorphism of $A(\mathfrak{P})$, which is absurd.

Now let $\mathfrak{p}_t$ be a prime ideal in k_t; we assume that it is not ramified in K_0 and also that it has in a suitable field K a non-exceptional prime divisor $\mathfrak{P}$, i.e. one modulo which one can reduce A, all its conjugates over k_t, and the endomorphisms and homomorphisms of these varieties. Put $q=N(\mathfrak{p}_t)$. Take for A' the transform of A by an automorphism τ of $\overline{\mathbf{Q}}$ over k_t which induces on K_0 the Frobenius substitution for $\mathfrak{p}_t$. By what we have seen above, the Frobenius homomorphism of $A(\mathfrak{P})$ onto $A'(\mathfrak{P})$, induced by the automorphism $x\to x^q$ of the universal domain, will be the image of an element ϖ of $\mathcal{H}(A, A')$; and we have $f(\varpi)=q$. Then, if we put $\mathcal{H}(A, A')=\mathfrak{q}^{-1}\varpi$, $\mathfrak{q}$ is an ideal in $\mathfrak{o}$, such that $\mathfrak{q}\bar{\mathfrak{q}}=q\mathfrak{o}$, and we have $\{A'\colon A\}=(\mathfrak{q}^{-1};\ q)$.

By class-field theory, an abelian extension is completely determined by the knowledge of the Frobenius substitution for almost all prime ideals; therefore (I) will be solved if we determine the correspondence $\mathfrak{p}_t \to \mathfrak{q}$. Let m be a multiple of the order of the Frobenius substitution for $\mathfrak{p}_t$ in K_0; then τ^m transforms A into a variety A_1 isomorphic to A. Call α_1 an isomorphism of A onto A_1; this is uniquely determined up to an automorphism, i.e. up to a root of unity. Then the automorphism $x \to x^{q^m}$ of the universal domain induces a homomorphism of $A(\mathfrak{P})$ onto $A_1(\mathfrak{P})$, which, as above, may be identified with an element of $\mathcal{H}(A, A_1)$; this can be written as $\pi\alpha_1$ with $\pi \in \mathfrak{o}$; π is uniquely determined up to a root of unity. Proceeding as above, we find that $\pi\bar{\pi}=q^m$ and that $\pi\mathfrak{o}=\mathfrak{q}^m$. One should observe that, if $N(\mathfrak{P})=q^h$ and m is a multiple of h, then $A_1(\mathfrak{P})=A(\mathfrak{P})$, so that in that case α_1 can be determined uniquely by prescribing that it should reduce to the identity mapping on $A(\mathfrak{P})$; then π also is completely determined. Now, in order to find $\mathfrak{q}$, it is enough to determine the prime ideal decomposition of π in a suitable field for some suitable choice of m, e.g. for $m=h$. *But this has been done by Taniyama* (cf. § 3 of his contribution to this volume). The conclusion is that, for almost all $\mathfrak{p}_t$, we have

$$\mathfrak{q}=\prod_{\mu} \psi_\mu(\mathfrak{p}_t)$$

provided of course ideals in subfields of k' (the smallest Galois extension of $\mathbf{Q}$ containing k) are identified in the customary way with the ideals they generate in k'.

This formula contains the solution of problem (I) for $\mathfrak{r}=\mathfrak{o}$. One should observe that, while the prime ideal decomposition of π, together with the relation $\pi\bar{\pi}=q^m$, determines π up to a root of unity, this is not enough for the calculation of the zeta-function, where a more precise result (also contained in Taniyama's work) is required.

For $\mathfrak{r}=\mathfrak{o}$, problem (II) can be treated by an entirely similar method. We consider the pairs (A, a), where A is an abelian variety of one of the types discussed above, and a is a point of finite order on A. If $\mathfrak{n}$ is the ideal in $\mathfrak{o}$, consisting of those ξ for which $\xi a=0$, we say that a belongs to $\mathfrak{n}$. The type of the pair (A, a) will be considered as given by the type of A, i.e. by the data $(k; \{\varphi_\lambda\})$, $\mathfrak{r}=\mathfrak{o}$ and $\mathfrak{f}_0$, and by the ideal $\mathfrak{n}$ in $\mathfrak{o}$. Consider two such pairs (A, a) and (A', a'). If we write, as above, $\mathcal{H}(A, A')=\mathfrak{a}\alpha$ and $f(\xi\alpha)=\rho\xi\bar{\xi}$, there will be an element ξ_0 of $\mathfrak{a}$ such that $\xi_0\alpha$ maps a onto a'; it is determined uniquely modulo $\mathfrak{a}\mathfrak{n}$ and is such that $\xi_0\mathfrak{o}+\mathfrak{a}\mathfrak{n}=\mathfrak{a}$. That being so, we define an equivalence relation between triplets $\mathfrak{a}$, ρ, ξ_0, where $\mathfrak{a}$, ρ

are as before and ξ_0 is such that $\xi_0\mathfrak{o}+\mathfrak{a}\mathfrak{n}=\mathfrak{a}$, by defining two triplets $\mathfrak{a}$, ρ, ξ_0 and $\mathfrak{a}'$, ρ', ξ_0' to be equivalent if there is a $\lambda \in k$ such that $\mathfrak{a}'=\lambda^{-1}\mathfrak{a}$, $\rho'=\rho\lambda\bar{\lambda}$ and $\xi_0'\equiv\lambda^{-1}\xi_0$ mod. $\mathfrak{a}'\mathfrak{n}$; and we denote by $(\mathfrak{a}; \rho; \xi_0)$ the class of such a triplet. Then the class of the triplet $\mathfrak{a}$, ρ, ξ_0 attached as above to the two pairs (A, a) and (A', a') is independent of the choice of α; it will be denoted by $\{(A', a'\} : (A, a)\}$; the two pairs are isomorphic if and only if the class is $(\mathfrak{o}; 1; 1)$. A group law between equivalence classes is defined by putting

$$(\mathfrak{a}; \rho; \xi_0)\cdot(\mathfrak{a}'; \rho'; \xi_0')=(\mathfrak{a}\mathfrak{a}'; \rho\rho'; \xi_0\xi_0').$$

Proceeding as above, one finds that the Frobenius substitution for $\mathfrak{p}_t$, in the field generated over K_0 by the image of the point a on V_0, is $(\mathfrak{q}^{-1}; q; 1)$. This solves problem (II).

UNIVERSITY OF CHICAGO

On Complex Multiplications

Goro SHIMURA

It is well known that the theory of class-fields over imaginary quadratic fields can be described in terms of the complex multiplication of elliptic functions. In the classical treatment of this theory as well as in the purely algebraic treatment by M. Deuring ([1]), the congruence relation on elliptic functions, which was first given by L. Kronecker, has played a central role. If one obtains some similar relation on abelian functions of higher dimension, then one can study the arithmetic of such abelian functions particularly in connection with class-field theory. In the present paper we shall give some results in this direction. Using the notion of reduction modulo $\mathfrak{p}$ of algebraic varieties, we obtain a certain congruence relation for an abelian variety A of dimension n whose endomorphism-ring contains a subring isomorphic to the ring of integers of an algebraic number-field K of degree $2n$. By means of this congruence relation we can prove that a field of definition for such an abelian variety A always contains a certain class-field over K_0 and that the fields generated by division points on A contain class-fields over K_0, corresponding to the ideal-groups determined by some relations which we can write down, where K_0 denotes a certain algebraic number-field determined by K and some isomorphisms of K.

1. Let A be an abelian variety defined over a field k. We shall denote by $\mathscr{A}(A)$ the ring of all endomorphisms of A. Let K be an algebraic number-field of degree $2n$ and R the ring of all integers in K. By an *abelian variety having R as operator-domain,* we shall understand a pair (A, ι) of an abelian variety A of dimension n and an isomorphism ι of R into $\mathscr{A}(A)$. We shall denote simply by A such a pair (A, ι) if there is no fear of misunderstanding. Let (A', ι') be another abelian variety having R as operator-domain. We shall understand by an *R-homomorphism of A into A'* a homomorphism λ of A into A' such that $\lambda\iota(\mu)x = \iota'(\mu)\lambda x$ for every $\mu \in R$ and every $x \in A$. We shall say that (A, ι) is defined over a field k if k is a field of definition for A and for every element of $\iota(R)$.

Now let $\mathfrak{a}$ be an ideal of R other than the zero-ideal. We shall denote by $\mathfrak{g}(\mathfrak{a}, A)$ the set of all points t of A such that $\iota(\mu)t=0$ for every $\mu \in \mathfrak{a}$. We shall call an element t in $\mathfrak{g}(\mathfrak{a}, A)$ a *primitive element in* $\mathfrak{g}(\mathfrak{a}, A)$ if $\iota(\mu)t=0$ implies $\mu \in \mathfrak{a}$. Such an element exists if $\mathfrak{a}$ is prime to the characteristic of the ground field k. Let (A', ι') be an abelian variety having R as operator-domain and λ an R-homomorphism of (A, ι) into (A', ι'), both defined over k. We shall call λ an $\mathfrak{a}$-*multiplication of A onto A'* if the following condition is satisfied: if x is a generic point of A over k, then the field $k(\lambda x)$ is the composite of all the fields $k(\iota(\mu)x)$ such that $\mu \in \mathfrak{a}$. We shall call (A', ι') an $\mathfrak{a}$-*transform of A* if there exists an $\mathfrak{a}$-multiplication of A onto A'. For every ideal $\mathfrak{a}$ of R, there exist an $\mathfrak{a}$-transform A' of A and an $\mathfrak{a}$-multiplication λ of A onto A'; the kernel of λ is equal to $\mathfrak{g}(\mathfrak{a}, A)$. One may consider an $\mathfrak{a}$-multiplication an "ideal number" which makes $\mathfrak{a}$ principal. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of R. Then, an $\mathfrak{a}$-transform of A and a $\mathfrak{b}$-transform of A are R-isomorphic to each other if and only if $\mathfrak{a}$ and $\mathfrak{b}$ belong to the same ideal-class. Let c be an ideal-class of K. We shall call A' a *c-transform of A* if A' is an $\mathfrak{a}$-transform of A for an ideal $\mathfrak{a}$ in c. We can easily prove the following proposition.

PROPOSITION 1. *Let c be an ideal-class of K and A' a c-transform of A. Let* $\mathfrak{m}$ *be an ideal of R and t a primitive element in* $\mathfrak{g}(\mathfrak{m}, A)$. *If* $t' \in \mathfrak{g}(\mathfrak{m}, A')$, *then there exist an ideal* $\mathfrak{a}$ *in c and an* $\mathfrak{a}$-*multiplication* $\lambda_{\mathfrak{a}}$ *of A onto A' such that* $t'=\lambda_{\mathfrak{a}}t$; *t' is primitive in* $\mathfrak{g}(\mathfrak{m}, A')$ *if and only if* $\mathfrak{a}$ *is prime to* $\mathfrak{m}$. *If t' is primitive in* $\mathfrak{g}(\mathfrak{m}, A')$, *the ideal-class of* $\mathfrak{a}$ *modulo* $\mathfrak{m}$ *is uniquely determined by t'.*

Let σ be an isomorphism of the ground field k onto a field k^σ. Then we have an abelian variety A^σ defined over k^σ, the transform of A by σ. Let μ be an element of R and W the graph of $\iota(\mu)$. The transform W^σ of W by σ is a subvariety of $A^\sigma \times A^\sigma$; there exists an endomorphism of A^σ having W^σ as its graph; denote by $\iota^\sigma(\mu)$ that endomorphism. Then the mapping $\mu \rightarrow \iota^\sigma(\mu)$ gives an isomorphism of R into $\mathcal{A}(A^\sigma)$; thus we obtain an abelian variety having R as operator-domain (A^σ, ι^σ) defined over k^σ. When k has a prime characteristic p, we obtain an isomorphism σ of k, for any power $q=p^f$ of p, defined by $z^\sigma=z^q$ for every z in k. In this situation, we shall denote (A^σ, ι^σ) simply by A^q.

2. Let k be a field with a discrete valuation and $\mathfrak{o}$ be its valuation ring; denote by $\mathfrak{p}$ the maximal ideal of $\mathfrak{o}$ and by κ the residue field $\mathfrak{o}/\mathfrak{p}$. Let V be a variety in the projective N-space P^N, defined over k and $\mathfrak{A}$ the set of all polynomials $F(X)$ in $\mathfrak{o}[X_0, \cdots, X_N]$ such that $F(x)=0$ for every (x) on V. Let $\bar{P}^N$ be the projective

N-space defined over κ and denote by $\bar{V}$ the algebraic set in $\bar{P}^N$ defined by the equations $\bar{F}(X)=0$ for $F\in\mathfrak{A}$ where $\bar{F}$ denotes the class of F modulo $\mathfrak{p}$. If $\bar{V}$ has the only one component and that component has the multiplicity one ([3] p. 148), we say that V is $\mathfrak{p}$-*simple* and call $\bar{V}$ *the variety obtained from* V *by reduction modulo* $\mathfrak{p}$. In [3], we have given a theory of reduction modulo $\mathfrak{p}$ of algebraic varieties thus defined. As shown there, we can define reduction of an abstract variety. We shall use the same terminologies and notations as in [3].

Let V and W be two $\mathfrak{p}$-simple varieties defined over k; denote by $\bar{V}$ and by $\bar{W}$ the varieties obtained from V and W by reduction modulo $\mathfrak{p}$, respectively. Then $\bar{V}$ and $\bar{W}$ are abstract varieties defined over κ. Let f be a rational mapping of V into W, defined over k; denote by T the graph of f. Let ξ be a point on $\bar{V}$. We shall say that f *is defined at* ξ if there exists a point η on $\bar{W}$ such that, for some representatives V_α, W_λ, $T_{\alpha\lambda}$, ξ_α and η_λ of V, W, T, ξ and η, we have $\xi_\alpha\times\eta_\lambda\in\bar{T}_{\alpha\lambda}$ and the projection from $T_{\alpha\lambda}$ to V_α is regular at ξ_α (namely, if $x_\alpha\times y_\lambda$ is generic on $T_{\alpha\lambda}$ over k, the coordinates of y_λ are all contained in the specialization-ring $[x_\alpha\rightarrow\xi_\alpha]$).

Now let A be an abelian variety defined over k. Denote by f the rational mapping of $A\times A$ into A such that $f(x,y)=x+y$ for $x\in A$, $y\in A$ and by g the rational mapping of A into A such that $g(x)=-x$ for $x\in A$. We shall say that A *has no defect for* $\mathfrak{p}$ if the following conditions (1–4) are satisfied. (1) A *is* $\mathfrak{p}$-*simple*. Denote by $\bar{A}$ the variety obtained from A by reduction modulo $\mathfrak{p}$. (2) A *is* $\mathfrak{p}$-*complete*. (If A is a subvariety of a projective space, this is always satisfied.) (3) f *is everywhere defined on* $\bar{A}\times\bar{A}$. (4) g *is everywhere defined on* $\bar{A}$. If A has no defect for $\mathfrak{p}$, the variety $\bar{A}$ obtained from A by reduction modulo $\mathfrak{p}$ becomes an abelian variety defined over κ, in a natural manner. We shall call $\bar{A}$ *the abelian variety obtained from* A *by reduction modulo* $\mathfrak{p}$.

Let A and B be two abelian varieties defined over k, having no defect for $\mathfrak{p}$; denote by $\bar{A}$ and by $\bar{B}$ the abelian varieties obtained from A and from B by reduction modulo $\mathfrak{p}$, respectively. Denote by $\mathscr{H}(A,B;k)$ the set of all homomorphisms of A into B, defined over k, and by $\mathscr{H}(\bar{A},\bar{B};\kappa)$ the set of all homomorphisms of $\bar{A}$ into $\bar{B}$, defined over κ. Then, for every $\lambda\in\mathscr{H}(A,B;k)$, there exists a uniquely determined element $\bar{\lambda}\in\mathscr{H}(\bar{A},\bar{B};\kappa)$ such that the graph of λ is the variety obtained from the graph of λ by reduction modulo $\mathfrak{p}$. The correspondence $\lambda \rightarrow \bar{\lambda}$ defines an isomorphism of the additive group $\mathscr{H}(A, B; k)$ into the additive group $\mathscr{H}(\bar{A}, B; \kappa)$. If $A=B$, this isomorphism is a ring-isomorphism.

Now as in 1, let R be the ring of integers in an algebraic number-field K and (A, ι) an abelian variety having R as operator-domain, defined over k. Suppose that A has no defect for $\mathfrak{p}$; denote by $\bar{A}$ the abelian variety obtained from A by reduction modulo $\mathfrak{p}$. Let μ be an element of R; put $\iota(\mu)=\mu_A$ and denote by $\bar{\mu}_A$ the corresponding endomorphism of $\bar{A}$. Then the mapping $\bar{\iota}$ of R into $\mathscr{A}(\bar{A})$ defined by $\bar{\iota}(\mu)=\bar{\mu}_A$ is an isomorphism. Hence we obtain an abelian variety having R as operator-domain $(\bar{A}, \bar{\iota})$; we denote it also by $\bar{A}$ and call *the abelian variety having R as operator-domain obtained from (A, ι) by reduction modulo* $\mathfrak{p}$. Let c be an ideal-class of K and A' a c-transform of A, defined over k; let $\mathfrak{a}$ be an ideal in c and $\lambda_{\mathfrak{a}}$ an $\mathfrak{a}$-multiplication of A onto A' defined over k. Suppose that A' has no defect for $\mathfrak{p}$. Then $\bar{A}'$ is a c-transform of $\bar{A}$ and $\bar{\lambda}_{\mathfrak{a}}$ is an $\mathfrak{a}$-multiplication of $\bar{A}$ onto $\bar{A}'$. Let $\mathfrak{m}$ be an ideal of R which is prime to the characteristic of the residue field κ. Let t be a primitive element in $\mathfrak{g}(\mathfrak{m}, A)$ and suppose that t is rational over k. Then the point $\bar{t}$ obtained from t by reduction modulo $\mathfrak{p}$ is a primitive element in $\mathfrak{g}(\mathfrak{m}, \bar{A})$.

If A is an abelian variety defined over an algebraic number-field, then A has no defect for all but a finite number of prime divisors of that field.

Let V be a $\mathfrak{p}$-simple variety defined over k and denote by $\bar{V}$ the variety obtained from V by reduction modulo $\mathfrak{p}$. Let f be a function on V defined over k and denote by $\bar{f}$ the generalized function on $\bar{V}$ obtained from f by reduction modulo $\mathfrak{p}$ ([3] pp. 167–168). We shall say that f is $\mathfrak{p}$-*finite* if $\bar{f} \neq \infty$. Let ω be a differential form on V defined over k. We shall say tat ω is $\mathfrak{p}$-*finite* if ω is written in a form $\omega=\sum_{(i)} f_{(i)} dg_{i_1} \cdots dg_{i_r}$ where the $f_{(i)}$ and the g_i are $\mathfrak{p}$-finite functions on V defined over k. We can prove that the differential form $\bar{\omega}=\sum_{(i)} \bar{f}_{(i)} d\bar{g}_{i_1} \cdots d\bar{g}_{i_r}$ on $\bar{V}$ does not depend upon the choice of the $f_{(i)}$ and the g_i. We shall call $\bar{\omega}$ *the differential form obtained from ω by reduction modulo* $\mathfrak{p}$. If ω is of the first kind, and if $\bar{V}$ is a complete non-singular variety then $\bar{\omega}$ is of the first kind.

3. Let E be a complete non-singular curve of genus one, defined over a field k, having a rational point over k. Then E becomes an abelian variety of dimension one, defined over k. We shall understand by an *elliptic curve defined over a field* k, an abelian variety of dimension one, defined over k.

Let Φ be an imaginary quadratic field, R the ring of integers in Φ. Then there exists an elliptic curve E defined over an algebraic number-field k such that $\mathcal{A}(E)$ is isomorphic to R. Let ω be a differential form of the first kind on E. If $\mu_0 \in \mathcal{A}(E)$, there exists a number μ such that $\delta\mu_0\omega = \mu\omega$, where $\delta\mu_0$ denotes the differential of the rational mapping μ_0. The correspondence $\mu \rightarrow \mu_0$ is an isomorphism of R onto $\mathcal{A}(E)$; this isomorphism does not depend upon the choice of ω; denote it by ι. Thus we obtain an abelian variety having R as operator-domain (E, ι); we denote it also by E.

THEOREM 1. *Notations being as above, suppose that k contains Φ. Let $\mathfrak{p}$ be a prime ideal of R and $\mathfrak{P}$ a prime divisor of $\mathfrak{p}$ in k. Suppose that E has no defect for $\mathfrak{P}$ and denote by $\bar{E}$ the elliptic curve having R as operator-domain, obtained from E by reduction modulo $\mathfrak{P}$. Denote by π the rational mapping of $\bar{E}$ onto $\bar{E}^{N\mathfrak{p}}$ such that $\pi\bar{t} = \bar{t}^{N\mathfrak{p}}$ for every $\bar{t} \in \bar{E}$. Then $\bar{E}^{N\mathfrak{p}}$ is a $\mathfrak{p}$-transform of $\bar{E}$; and π is a $\mathfrak{p}$-multiplication of $\bar{E}$ onto $\bar{E}^{N\mathfrak{p}}$.*

This theorem is an algebro-geometric formulation of Kronecker's congruence relation on elliptic functions ([2] XI, § 14), though our theorem is concerned only with a singular modulus. From this we can derive the law of reciprocity for Strahl-class-fields over imaginary quadratic fields, with no use of the general class-field theory. Moreover we can determine the ramification in case where the conductor is prime to 2.

4. As in 1, let K be an algebraic number-field of degree $2n$ and R the ring of all integers in K. Let (A, ι) be an abelian variety having R as operator-domain defined over the field of complex numbers. Let K^* be the smallest normal extension of the rational number field Q containing K; denote by G the Galois group of the extension K^*/Q and by H the subgroup of G corresponding to K. Denote by $D(A)$ the set of all invariant differential forms on A of degree one. Let μ be an element of R and denote by $\delta\mu$ the differential of the rational mapping $\iota(\mu)$. Then $\delta\mu$ defines a linear endomorphism of the linear space $D(A)$. We can find n elements $\sigma_1, \cdots, \sigma_n$ in G such that $\mu^{\sigma_1}, \cdots, \mu^{\sigma_n}$ are the characteristic roots of the linear endomorphism $\delta\mu$ for every $\mu \in R$. We shall say that A has the *type* $(K, \sigma_1, \cdots, \sigma_n)$ if the situation

is as above. We can prove that if there exists an abelian variety of the type $(K, \sigma_1, \cdots, \sigma_n)$, there exists one defined over an algebraic number-field of a finite degree. Now, notations being as above, denote by H_0 the subgroup of G consisting of all the elements σ such that $\bigcup_{j=1}^{n} H\sigma_j\sigma = \bigcup_{j=1}^{n} H\sigma_j$. Then we can find elements $\tau_1, \cdots, \tau_s$ in G such that $\bigcup_{j=1}^{n} \sigma_j^{-1}H = \bigcup_{i=1}^{s} H_0\tau_i$ and $n[H:1] = s[H_0:1]$. Denote by K_0 the subfield of K^* corresponding to H_0; then we have $[K_0:Q] = 2s$. For this field K_0, the following proposition holds.

PROPOSITION 2. *Notations being as above, let (A, ι) be an abelian variety having R as operator-domain, of the type $(K, \sigma_1, \cdots, \sigma_n)$ defined over an algebraic number-field k of a finite degree. Then k contains K_0. Furthermore, let σ be an isomorphism of k. Then (A^σ, ι^σ) is a c-transform of (A, ι) for some ideal-class c of K if and only if σ fixes every element of K_0.*

Now we have a congruence relation on the abelian variety A.

THEOREM 2. *Notations being as in Proposition 2, let $\mathfrak{p}$ be a prime ideal of K_0 which is of the absolute degree one and $\mathfrak{P}$ a prime divisor of $\mathfrak{p}$ in k; put* $\mathrm{N}\mathfrak{p} = p$. *Suppose that p is unramified in K^* and A has no defect for $\mathfrak{P}$. Denote by A the abelian variety having R as operator-domain obtained from A by reduction modulo $\mathfrak{P}$. Denote by π the rational mapping of $\bar{A}$ onto $\bar{A}^p$ such that $\pi\bar{t} = \bar{t}^p$ for every $\bar{t} \in \bar{A}$. Then $\bar{A}^p$ is a $\mathfrak{p}^{\tau_1} \cdots \mathfrak{p}^{\tau_s}$-transform of $\bar{A}$ and π is a $\mathfrak{p}^{\tau_1} \cdots \mathfrak{p}^{\tau_s}$-multiplication of $\bar{A}$ onto $\bar{A}^p$.*

By this theorem we obtain the following result.

THEOREM 3. *Let the notations be as in Proposition 2. Then,*

1) *k contains the class-field $K_{(1)}$ over K_0 which corresponds to the ideal-group $H_{(1)}$ consisting of all ideals $\mathfrak{a}$ in K_0 such that $\mathfrak{a}^{\tau_1} \cdots \mathfrak{a}^{\tau_s}$ is principal in K;*

2) *let $\mathfrak{m}$ be an ideal of R and t a primitive element in $\mathfrak{g}(\mathfrak{m}, A)$; then the field $k(t)$ contains the class-field $K_{\mathfrak{m}}$ over K_0 which corresponds to the ideal-group $H_{\mathfrak{m}}$ consisting of all ideals $\mathfrak{a}$ in K_0 such that $\mathfrak{a}^{\tau_1} \cdots \mathfrak{a}^{\tau_s}$ belongs to the Strahl modulo $\mathfrak{m}$ in K.*

The field $K_{(1)}$ and $K_{\mathfrak{m}}$ are represented by means of Chow-points as follows. Supposing that A is a variety in a projective space P^N, let $\{A_1, \cdots, A_r\}$ be the set of all the conjugates A' of A over K_0 such that A' is R-isomorphic to A. Denote by (a) the Chow-point of the cycle $A_1 + \cdots + A_r$ in P^N. Then we have $K_{(1)} = K_0(a)$. Let $\{t_1, \cdots, t_u\}$ be the set of all the conjugates t' of t over K_0 such that there exists an isomorphism σ of $k(t)$ for which we have $A^\sigma=A_i$ for some i and $t^\sigma=t'=\lambda_\mathfrak{a}t$ where $\mathfrak{a}$ is an ideal belonging to the Strahl modulo $\mathfrak{m}$ and $\lambda_\mathfrak{a}$ is an $\mathfrak{a}$-multiplication of A onto A^σ. Denote by (m) the Chow-point of the cycle $t_1+\cdots+t_n$ in P^N. Then we have $K_\mathfrak{m}=K_0(a, m)$.

Now we shall sketch the proofs of Theorem 2 and Theorem 3. Let $\mathfrak{p}$ and $\mathfrak{P}$ be as in Theorem 2. It is easy to see that $\mathfrak{p}^{\tau_1}\cdots\mathfrak{p}^{\tau_s}$ is really an ideal of K and $\mathrm{N}_{K/Q}(\mathfrak{p}^{\tau_1}\cdots\mathfrak{p}^{\tau_s})=p^n$. We can find n invariant differential forms $\omega_1,\cdots,\omega_n$ on A such that $\delta\mu\omega_i=\mu^{\sigma_i}\omega_i$ $(1\leqq i\leqq n)$ for every $\mu\in R$. Moreover we can take the ω_i in such a way that they are $\mathfrak{P}'$-finite and the forms $\bar\omega_i$ obtained from the ω_i by reduction modulo $\mathfrak{P}'$ form a basis of the linear space of linear differential forms on A, where $\mathfrak{P}'$ denotes a prime divisor of $\mathfrak{P}$ in a field of definition for the ω_i. If μ is contained in $\mathfrak{p}^{\tau_1}\cdots\mathfrak{p}^{\tau_s}$, then μ^{τ_i} is divisible by $\mathfrak{P}$ for every i. Hence we have $\delta\bar\mu\bar\omega_i=\bar\mu^{\sigma_i}\bar\omega=0$ $(1\leqq i\leqq n)$ for every $\mu\in\mathfrak{p}^{\tau_1}\cdots\mathfrak{p}^{\tau_s}$ where a letter with a bar denotes an object obtained from the corresponding one by reduction modulo $\mathfrak{P}'$. This shows that $\delta\bar\mu=0$ for every $\mu\in\mathfrak{p}^{\tau_1}\cdots\mathfrak{p}^{\tau_s}$. Therefore, if $\bar x$ is a generic point of $\bar A$ over the residue field κ of $\mathfrak{P}$, we have $\kappa(\bar\mu\bar x)\subset\kappa(\bar x^p)$ for every μ in $\mathfrak{p}^{\tau_1}\cdots\mathfrak{p}^{\tau_s}$. From this we obtain Theorem 2.

Let $\mathfrak{m}$ and t be as in Theorem 3. Let k^* be a finite normal extension of K_0 such that $k^*\supset kK^*(t)$ and that every homomorphism of A into any conjugates of A over K_0 is defined over k^*. Denote by G^* the Galois group of the extension k^*/K_0. If σ is an element of G^*, then t^σ is a primitive element in $\mathfrak{g}(\mathfrak{m}, A^\sigma)$. By Proposition 2, A^σ is a c-transform of A for some ideal-class c of K. Then, by Proposition 1, there exist an ideal $\mathfrak{a}$ in c and an $\mathfrak{a}$-multiplication $\lambda_\mathfrak{a}$ of A onto A^σ such that $t^\sigma=\lambda_\mathfrak{a}t$. The correspondence $\sigma\rightarrow\mathfrak{a}$ defines a homomorphism of G^* into the group of ideal-classes modulo $\mathfrak{m}$ in K. Denote by N^* the kernel of that homomorphism and by $K_\mathfrak{m}$ the subfield of k^* corresponding to N^*. Then $K_\mathfrak{m}$ is an abelian extension of K_0. If an element σ of G^* fixes every element of $k(t)$, then σ is contained in N^* as we have $A^\sigma=A$, $t^\sigma=t$. This shows that $K_\mathfrak{m}$ is a subfield of $k(t)$. Now let $\mathfrak{p}$ be a prime ideal of K_0 satisfying the following conditions: i) $\mathfrak{p}$ is of the absolute degree one, ii) $\mathrm{N}\mathfrak{p}=p$ is unramified in k^*, iii) the A^σ for all $\sigma\in G^*$ have no defect for every prime divisor of $\mathfrak{p}$ in k^*. Let $\mathfrak{P}$ be a prime divisor of $\mathfrak{p}$ in k^* and σ a Frobenius substitution of $\mathfrak{P}$; then σ induces $\left(\dfrac{K_\mathfrak{m}/K_0}{\mathfrak{p}}\right)$ in $K_\mathfrak{m}$. For this σ, we obtain an ideal $\mathfrak{a}$ and an $\mathfrak{a}$-multiplication $\lambda_\mathfrak{a}$ of A onto

A^{σ} such that $t^{\sigma}=\lambda_{\mathfrak{a}}t$. Denoting by bars over letters the objects obtained by reduction modulo $\mathfrak{P}$, we have $\bar{A}^{\sigma}=\bar{A}^{p}$ and $\bar{t}^{\sigma}=\bar{\lambda}_{\mathfrak{a}}\bar{t}$. On the other hand, by Theorem 2, we have $\bar{t}^{\sigma}=\bar{t}^{p}=\pi\bar{t}$ where π denotes the $\mathfrak{p}^{\tau_1}\cdots\mathfrak{p}^{\tau_s}$-multiplication of $\bar{A}$ onto $\bar{A}^{p}$ as in that theorem. Now if $\mathfrak{p}$ is prime to $N\mathfrak{m}$, $\bar{t}$ is a primitive element in $\mathfrak{g}(\mathfrak{m}, \bar{A})$. By Proposition 1, the relation $\bar{\lambda}_{\mathfrak{a}}\bar{t}=\pi\bar{t}$ implies that $\mathfrak{a}$ and $\mathfrak{p}^{\tau_1}\cdots\mathfrak{p}^{\tau_s}$ belong to the same ideal-class modulo $\mathfrak{m}$. Thus we have proved that a prime ideal $\mathfrak{p}$ of the absolute degree one is contained in $H_{\mathfrak{m}}$ if and only if $\left(\frac{K_{\mathfrak{m}}/K_0}{\mathfrak{p}}\right)$ is equal to the identity with a finite number of exceptions. By a result of class-field theory, we have 2) of Theorem 3.

UNIVERSITY OF TOKYO

REFERENCES

[1] M. Deuring, Die Struktur der elliptischen Funktionenkörper und die Klassenkörper der imaginären quadratischen Zahlkörper, Math. Ann., **124** (1952), pp. 393–426.

[2] L. Kronecker, Zur Theorie der elliptischen Funktionen, Werke IV.

[3] G. Shimura, Reduction of algebraic varieties with respect to a discrete valuation of the basic field, Amer. Journ. of Math., **77** (1955), pp. 134–176.

Jacobian Varieties and Number Fields[1]

Yutaka TANIYAMA[2]

Introduction.

The classical theory of complex multiplication solves the problem of construction of abelian extensions of imaginary quadratic fields. Apart from this classical theory, E. Hecke [2] [3] has treated successfully the problem of unramified abelian extensions of certain imaginary biquadratic fields by means of Hilbert modular functions.

The main purpose of this work is to develop a theory comprizing both classical theory of complex multiplication and the theory of Hecke, by the method of algebraic geometry.

By the way, an arithmetic characterization of endomorphisms π of an abelian variety with sufficiently many complex multiplications is obtained. By means of this result we can prove in the affirmative the conjecture of Hasse on zeta functions of abelian varieties, and of curves, in certain singular cases. On this subject, we have some known results in special cases. A. Weil [14] proved namely that the zeta function of a curve defined by $ax^n+by^m+c=0$ over a certain algebraic number field k can be expressed by the zeta function of k and L-functions with "Grössencharaktere". M. Deuring [1] proved analogous result for singular elliptic curves. The result in this paper contains that of Deuring, and of Weil in case n, m are different prime numbers.

The same problem of construction of abelian extensions of algebraic number fields was also treated by G. Shimura and A. Weil (cf. these proceedings pp. 23–30 and pp. 9–22). A. Weil pointed out

[1] The following exposition is somewhat different from the text presented to the symposium. The main differences are as follows.

i) The part in which special emphasis was made on jacobian varieties is omitted, as this part contained a mistake.

ii) The part concerning Galois theory of the field K' is revised and simplified.

iii) Some results in § 3, especially Proposition 3, are generalized to contain the case where $[R_0 : Q] < g$.

iv) In § 5, existence theorem of Lefschetz is added.

[2] This study was done with the help of subsidy from the Ministry of Education (1954, n° 10429).

moreover some important properties of characters of idèle class groups in connection with the zeta functions of abelian varieties (cf. these proceedings pp. 1–7). The complete exposition of the problem comprising the ideas and results of G. Shimura, A. Weil and myself will be published elsewhere in a joint paper of G. Shimura and myself.

Recently I have obtained a second proof of Hasse's conjecture in case of complex multiplications as a corollary of a theorem on characters of idèle class groups, which is in close connection with the properties pointed out by A. Weil. This will be exposed in a forthcoming paper of mine. Here I wish to express my hearty thanks to Professor A. Weil for his kind discussions and valuable suggestions on these subjects during and since the symposium and also to Professor S. Iyanaga for his constant encouragement.

Notations and terminologies.

The varieties considered in this paper are always supposed to be in some projective space or in a product of projective spaces. Except for this, we use mainly the terminologies as in Weil's books [8], [9], [10] and Shimura's paper [7].

Q denotes as usual the rational number field, **C** the complex number field. σ_0 denotes the complex conjugate automorphism of **C**: $\sigma_0\mu=\mu$ for μ in **C**. Algebraic number fields are always supposed to be in **C**. By the *Galois closure* of an algebraic number field we understand the smallest absolutely normal field containing that field. N denotes always absolute norm. For any field k, $\bar{k}$ denotes the algebraic closure of k.

A, A′, B mean always abelian varieties. The dimensions of A, A′ are always supposed to be equal and are denoted by g. As in Weil's book [10], $\mathcal{A}(\mathrm{A})$ denotes the ring of endomorphisms of A, $\mathcal{H}(\mathrm{A}, \mathrm{B})$ denotes the module of homomorphisms of A into B. $\mathcal{A}_0(\mathrm{A})$, $\mathcal{H}_0(\mathrm{A}, \mathrm{B})$ denote the tensor products $\mathcal{A}(\mathrm{A})\otimes\mathbf{Q}$, $\mathcal{H}(\mathrm{A}, \mathrm{B})\otimes\mathbf{Q}$ respectively. x denotes always a generic point of A. The field over which x is a generic point will be clear from the context, so that we shall need no reference to it. For any λ in $\mathcal{H}(\mathrm{A}, \mathrm{B})$, $\nu(\lambda)$ denotes the degree $[k(x) : k(\lambda x)]$ if this degree is finite, and otherwise we put $\nu(\lambda)=0$, where k is a common field of definition of A, B, λ. In case $\nu(\lambda)\neq 0$, $\nu_i(\lambda)$ denotes the inseparability degree of $k(x)$ over $k(\lambda x)$. Let A be defined over k and R be a subring of $\mathcal{A}(\mathrm{A})$. Then k_{R} denotes the smallest field containing k, over which all endomorphisms μ in R are rational.

Let a be any point on A. In case A is defined over a finite field k of $q=p^f$ elements, we denote by a^{p^h} the isomorphic image of a by the isomorphism $\xi \to \xi^{p^h}$ of the universal domain. Then the mapping $a \to a^q$ for all a on A determines an endomorphism of A, which is denotes by π_A, or $\pi_A(k)$.

Now, let k be a field and v a discrete valuation of k, and $\mathfrak{P}$ the maximal ideal of the valuation ring $\mathfrak{O}$ of v. Then we use the symbol $\sim$ to denote the object obtained from an object of the same kind by the reduction mod. $\mathfrak{P}$. For example, $\tilde{A}$ denotes the variety obtained from A mod. $\mathfrak{P}$. The use of symbol $\tilde{A}$ indicates implicitely that this variety is also an abelian variety. $\tilde{k}$ denotes therefore the residue field $\mathfrak{O}/\mathfrak{P}$. We do not use the symbol $\sim$ in "degenerate case".

Finally, let A be defined over an algebraic number field k of finite degree, and $\mathfrak{P}$ a "non-exceptional" prime ideal in k for A (cf. below Prop. 1, § 1). If there is an endomorphism in $\mathcal{A}(A)$ from which $\pi_{\tilde{A}}(\tilde{k})$ is obtained by the reduction mod. $\mathfrak{P}$, then we denote this endomorphism by $\pi_{\mathfrak{P}}$.

§ 1. Preliminaries from reduction theory.

Let V be a variety defined over a field k and $\mathfrak{B}$ a set of normalized discrete valuations v on k. $(\alpha)=(\alpha_1, \cdots, \alpha_r)$ being a finite set of non-zero elements in k, we denote by $\mathfrak{B}(\alpha)$ the set of all v's in $\mathfrak{B}$ such that $v(\alpha_i)=0$ for $i=1, \cdots, r$. If an assertion holds for all v's in some union of $\mathfrak{B}(\alpha)$'s, we say that it holds for *almost all* v in $\mathfrak{B}$. Therefore, when k is an algebraic number field of finite degree and $\mathfrak{B}$ is the set of all normalized discrete valuations of k, "almost all" means "all but a finite number of".

Let V_1, V_2 be two non-singular varieties and Z be the graph of a mapping f of V_1 into V_2, everywhere defined on V_1. Let V_1, V_2, f be defined over k. Then, Shimura's theory [7] shows, together with the arithmetic on algebraic varieties (Weil, [13]), that, for almost all v, $\tilde{V}_1, \tilde{V}_2$ are non-singular varieties and $\tilde{f}$ is a mapping, everywhere defined over $\tilde{V}_1$ with graph $\tilde{Z}$. From this we see

PROPOSITION 1. Let A be an abelian variety defined over k, and $\mathfrak{B}$ be arbitrary. Then, for almost all v in $\mathfrak{B}$, $\tilde{A}$ is an abelian variety such that $a \to \tilde{a}$ is a homomorphism of A onto $\tilde{A}$. This homomorphism induces an isomorphism of the group of all points on A with finite orders prime to the characteristic of the residue field $\tilde{k}$. If, especially, A is a jacobian variety of a non-singular curve C of genus g with a canonical mapping φ, all defined over k, then, for almost all v in $\mathfrak{V}$, $\tilde{A}$ is a jacobian variety of the non-sigular curve $\tilde{C}$ with the same genus g, and $\tilde{\varphi}$ is a canonical mapping of $\tilde{C}$ into $\tilde{A}$. Moreover, let A, B be two abelian varietes defined over k. Then, for almost all v in $\mathfrak{V}$, $\tilde{\lambda}$ is a homomorphism of $\tilde{A}$ onto $\tilde{B}$ for all λ in $\mathcal{H}(A, B)$, and $\lambda \to \tilde{\lambda}$ is an isomorphism of $\mathcal{H}(A, B)$ into $\mathcal{H}(\tilde{A}, \tilde{B})$. The same holds especially for the ring $\mathcal{A}(A)$.

We call v *non-exceptional* for A, if $\tilde{A}$ is abelian variety and $\mu \to \tilde{\mu}$ is an isomorphism of $\mathcal{A}(A)$ into $\mathcal{A}(\tilde{A})$, and non-exceptional for (A, B) if v is non-exceptional for A and for B and $\lambda \to \tilde{\lambda}$ is an isomorphism of $\mathcal{H}(A, B)$ into $\mathcal{H}(\tilde{A}, \tilde{B})$. We call v *exceptional* if it is not non-exceptional.

The linear differentials of the first kind on A are just the linear differentials invariant under translations on A, and they form a vector space D(A) of dimension g over the universal domain. Let λ be in $\mathcal{H}(A, B)$. Then, λ induces a linear transformation $\delta\lambda$ of D(B) into D(A). We denote by $S(\lambda)$ the representation-matrix of $\delta\lambda$ with basis of D(B) and of D(A). Especially, the ring $\mathcal{A}(A)$ has an anti-representation $\mu \to S(\mu)$ as a linear transformation of D(A). Let now v be non-exceptional for A. Then, the invariant property of a differential ω in D(A) shows that if ω is defined at one point of $\tilde{A}$, then it is everywhere defined on $\tilde{A}$, i.e. $\tilde{\omega}$ belongs to $D(\tilde{A})$. Thus, for any $\omega \neq 0$ rational over k, we can find an α in k such that $\widetilde{\alpha\omega}$ belongs to D(A) and is not 0. This shows that there is a basis $(\omega)=(\omega_1, \cdots, \omega_g)$ of D(A) such that $(\tilde{\omega})=(\tilde{\omega}_1, \cdots, \tilde{\omega}_g)$ forms a basis of $D(\tilde{A})$. Conversely, for any basis (ω) of D(A), $(\tilde{\omega})$ forms a basis of $D(\tilde{A})$ for almost all non-exceptional v. Moreover, we have clearly

PROPOSITION 2. Let A, B and all λ in $\mathcal{H}(A, B)$ be defined over k, and (ω), (η) be basis of D(A), D(B) respectively, rational over k. Let v be a non-exceptional valuation of k for (A, B) such that $(\tilde{\omega})$, $(\tilde{\eta})$ form basis of $D(\tilde{A})$, $D(\tilde{B})$ respectively. Then we have $\widetilde{S(\lambda)}=\tilde{S}(\tilde{\lambda})$ for any λ in $\mathcal{H}(A, B)$, where S, $\tilde{S}$ denote the representations of $\mathcal{H}(A, B)$, $\mathcal{H}(\tilde{A}, \tilde{B})$ with basis (ω), (η) and $(\tilde{\omega})$, $(\tilde{\eta})$ respectively. The same results hold especially for anti-representations S, $\tilde{S}$ of $\mathcal{A}(A)$, $\mathcal{A}(\tilde{A})$ with basis (ω), $(\tilde{\omega})$ respectively.

COROLLARY. In the same situation, $\widetilde{S(\lambda)}=0$ (i.e. $S(\lambda)\equiv 0 \bmod. v$) if and only if $\tilde{k}(\tilde{x}^p)\supset\tilde{k}(\tilde{\lambda}\tilde{x})$, p being the characteristic of k.

§ 2. Isogeneous abelian varieties.

We recall first some basic properties of abelian varieties (cf. Weil [10]). Two abelian varieties A, A′ (of the same dimension g) are called *isogeneous* if there is a homomorphism of A onto A′. This is an equivalence relation, by which we classify all abelian varieties into categories. We call A *simple* if the category of A is simple. Let A, A′ be isogeneous. Then, the relation $\mu^*\lambda=\lambda\mu$ determines an isomorphism $\mu\rightarrow\mu^*$ of the algebra $\mathcal{A}_0(A)$ (over $\mathbf{Q}$) onto the algebra $\mathcal{A}_0(A')$. For a subring R of $\mathcal{A}(A)$, we denote by R^* the image of R by this isomorphism. l being a prime number different from the characteristic p of the universal domain, we denote by M_l the l-adic representation of $\mathcal{H}(A, B)$ or of $\mathcal{A}(A)$ (cf. Weil [10] n° 31). For $\mathcal{A}(A)$ this representation is of degree $2g$ and faithfull. For any μ in $\mathcal{A}(A)$, the characteristic equation of $M_l(\mu)$ is the same for all $l\neq p$, and has rational integral coefficients with the constant term $\nu(\mu)$. Thus, each element of $\mathcal{A}_0(A)$ is of degree at most $2g$ over $\mathbf{Q}$. On the other hand, if A is simple, $\mathcal{A}_0(A)$ is a division algebra, and $\mathcal{A}_0(A\times\cdots\times A)$ is a matrix algebra over $\mathcal{A}_0(A)$. If A, B are simple and not isogeneous, $\mathcal{H}_0(A, B)=0$. Hence in general if $\mathcal{A}_0(A)$ contains a field R_0 of degree $2g$, A must be isogeneous to $B\times\cdots\times B$, B being simple, and the commutor of R_0 in $\mathcal{A}_0(A)$ is R_0 itself.

Now, let R be a subring of $\mathcal{A}(A)$ and k be a field of definition for A and for all μ in R. Then, for any left ideal $\mathfrak{a}$ of R, there exists an abelian variety B, and a $\lambda_{\mathfrak{a}}$ in $\mathcal{H}(A, B)$, both defined over k, with the property: $k(\lambda_{\mathfrak{a}}x)=\bigcup_{\mu\in\mathfrak{a}}k(\mu x)$. Indeed, $(\mu_1,\cdots,\mu_r)$ being a set of generators of R, we can take as B the locus of $\mu_1x\times\cdots\times\mu_rx$ in $A\times\cdots\times A$, and as $\lambda_{\mathfrak{a}}$ the homomorphism defined by $\lambda_{\mathfrak{a}}x=\mu_1x\times\cdots\times\mu_rx$. Clearly, B and $\lambda_{\mathfrak{a}}$ are determined by $\mathfrak{a}$ up to isomorphisms, and the kernel of $\lambda_{\mathfrak{a}}$ is the group $\mathfrak{g}_{\mathfrak{a}}$ of all points a such that $\mu a=0$ for all μ in $\mathfrak{a}$. Moreover, if R_1 is a subring of $\mathcal{A}(A)$ containing R, and $\mathfrak{a}_1$ is the left R_1-ideal $R_1\mathfrak{a}$, then we can take $\lambda_{\mathfrak{a}}$ as $\lambda_{\mathfrak{a}_1}$. It is clear that, if v is a non-exceptional discrete valuation of k for A, then $\tilde{B}$ is also an abelian variety and $\tilde{\lambda}_{\mathfrak{a}}$ is a homomorphism of $\tilde{A}$ onto $\tilde{B}$, which can be written as $\lambda_{\tilde{\mathfrak{a}}}$.

If μ is in the right order of the left ideal $\mathcal{A}(A)\mathfrak{a}$ in $\mathcal{A}_0(A)$, then the relation $\mu^*\lambda_{\mathfrak{a}}=\lambda_{\mathfrak{a}}\mu$ determines μ^* in $\mathcal{A}(B)$. If $R_0=R\otimes\mathbf{Q}$ is semi-simple, $\mu\rightarrow\mu^*$ induces an isomorphism on R. Assume now that $\mathfrak{a}$ contains an element α such that $\nu(\alpha)\neq0$. Then A and B are isogeneous, $\mu\rightarrow\mu^*$ is an isomorphism of $\mathcal{A}_0(A)$ onto $\mathcal{A}_0(B)$ and $\mathcal{A}(B)$ contains the isomorphic image of the right order of $\mathcal{A}(A)\mathfrak{a}$. If then

$\mathfrak{b}$ is a left ideal in $\mathcal{A}(\mathrm{A})$ with this right order of $\mathcal{A}(\mathrm{A})\mathfrak{a}$ as its left order, we have $\lambda_{\mathfrak{a}\mathfrak{b}}=\varepsilon\lambda_{\mathfrak{b}}{}^{*}\lambda_{\mathfrak{a}}$ with an isomorphism ε. Note that if $\mathfrak{a}=(\alpha)$ is principal, we have $\lambda_{\mathfrak{a}}=\eta\alpha$ with an isomorphism η.

If especially R is the principal order of a subfield R_0 (of $\mathcal{A}_0(\mathrm{A})$) of degree d, then we can prove easily

$$\nu(\lambda_{\mathfrak{a}})=(\mathrm{N}\mathfrak{a})^{2g/d},$$

where $\mathrm{N}\mathfrak{a}$ denotes the absolute norm of $\mathfrak{a}$ in the field R_0. Let furthermore R be the principal order of a field R_0 of degree $2g$, and B be isogeneous to A. Assume that R^* is contained in $\mathcal{A}(\mathrm{B})$ for some λ in $\mathcal{H}(\mathrm{A},\mathrm{B})$, with $\nu_{\iota}(\lambda)=1$, and denote by $\mathfrak{h}$ the kernel of λ. Then our assumption implies that $\mu\mathfrak{h}\subset\mathfrak{h}$ for any μ in R. Denote by $\mathfrak{a}$ an ideal in R consisting of all μ in R such that $\mu(\mathfrak{h})=0$, then the kernel of $\lambda_{\mathfrak{a}}$ is $\bigcup_{\mu\in\mathrm{R}}\mu\mathfrak{h}$, hence it is equal to $\mathfrak{h}$. Thus we see that λ can be written as $\lambda_{\mathfrak{a}}$. On the other hand, if A is simple and $\mathrm{R}=\mathcal{A}(\mathrm{A})$ is the principal order of the field $\mathcal{A}_0(\mathrm{A})$ of degree $2g$, then we have clearly $\mathcal{A}(\mathrm{B})\subset\mathrm{R}^*$ for any λ. If $\mathcal{A}(\mathrm{B})$ is also the principal order of $\mathcal{A}_0(\mathrm{B})$, this shows that $\mu\rightarrow\mu^*$ induces an isomorphism of $\mathcal{A}(\mathrm{A})$ onto $\mathcal{A}(\mathrm{B})$. Hence in this case, every λ in $\mathcal{H}(\mathrm{A},\mathrm{B})$ with $\nu_{\iota}(\lambda)=1$ must be of the form $\lambda_{\mathfrak{a}}$.

§ 3. Ideal decomposition of the endomorphism π.

Let A be defined over k, and put $k_1=k_{\mathcal{A}(\mathrm{A})}$. For any automorphism σ of $\bar{k}_1$, A^σ is also an abelian variety and $\mu\rightarrow\mu^\sigma$ gives an isomorphism of $\mathcal{A}(\mathrm{A})$ onto $\mathcal{A}(\mathrm{A}^\sigma)$, which is an automorphism of $\mathcal{A}(\mathrm{A})$ if σ fixes all elements of k. From this we see that k_1 is a finite algebraic normal extension of k, and its Galois group over k operates faithfully on $\mathcal{A}(\mathrm{A})$.

Assume now the characteristic of k to be zero. Let (ω) be a basis of D(A), rational over k. Denote by $\mathrm{S}(\mu)$, $\mathrm{S}^\sigma(\mu^\sigma)$ the (faithfull) anti-representation of $\mathcal{A}_0(\mathrm{A})$, $\mathcal{A}_0(\mathrm{A}^\sigma)$ with basis (ω), (ω^σ) respectively. Given a commutative semi-simple subalgebra R_0 of $\mathcal{A}_0(\mathrm{A})$, $\mathrm{S}(\mu)$ can clearly be transformed in $\bar{k}$ into diagonal forms $\mathrm{S}_1(\mu)$ simultaneously for all μ in R_0. If especially R_0 is a field, diagonal elements of $\mathrm{S}_1(\mu)$ must be of the form $\sigma_1\iota\mu,\cdots,\sigma_j\iota\mu, 0,\cdots, 0$, where ι is an isomorphism of R_0 into C and $\sigma_1,\cdots,\sigma_j$ are isomorphisms of the field $\iota\mathrm{R}_0$ into C, determined uniquely by A, R_0 and ι. Denote by K' the Galois closure of $\iota\mathrm{R}_0$, by G the Galois group of K' over Q and by H the subgroup of G corresponding to $\iota\mathrm{R}_0$. We consider σ_i as an element in G. Then the set H^* of all σ in G such that $\sum_{i=1}^{j}\sigma\sigma_i H=\sum_{i=1}^{j}\sigma_i H$

is a subgroup of G (uniquely determined by A and R_0). Denote by K^* the subfield of K' corresponding to H^*. Then we can find $\tau_1, \cdots, \tau_s$ in G for which $\sum_{i=1}^{j} \sigma_i H = \sum_{i=1}^{s} H^* \tau_i$ holds. Put $\mathrm{R} = \mathrm{R}_0 \frown \mathcal{A}(\mathrm{A})$, then we see that k_{R} always contains K^*, as we have clearly $S^{\sigma}(\mu^{\sigma}) = \sigma[S(\mu)]$ for any μ in $\mathcal{A}_0(\mathrm{A})$.

Here we shall recall some properties of endomorphisms π (cf. Weil [9], [10]). Let C be a non-singular curve of genus g, J a jacobian variety of C and φ a canonical mapping of C into J, all defined over the finite field k of $q = p^f$ elements. Then, the zeta-function $\mathrm{Z}(u)$ of C over k is of the form $[(1-u)(1-qu)]^{-1} \prod_{i=1}^{2g} (1 - \varpi_i u)$, where $\varpi_1, \cdots, \varpi_{2g}$ are characteristic roots of $\mathrm{M}_l(\pi_{\mathrm{J}})$ for $l \neq p$. The "Riemann hypothesis" shows now that $|\varpi_i| = q^{1/2}$ for $i = 1, \cdots, 2g$. The same holds for general abelian variety A and π_{A} if k is large enough, as, in case A is simple, there is a homomorphism of a jacobian onto A, and in general case, as π_{A} belongs to the centre of $\mathcal{A}(\mathrm{A})$, which is isomorphic to the direct sum of centres of $\mathcal{A}(\mathrm{B})$'s, B being simple. However, as $\pi_{\mathrm{A}}(k') = \pi_{\mathrm{A}}(k)^i$ if $[k' : k] = i$, we have $|\varpi_i| = q^{1/2}$ for any field of definition k of A.

Now, A and k being as above, let R_0 be a subfield of $\mathcal{A}_0(\mathrm{A})$. Assume that $\mathrm{R} = \mathrm{R}_0 \frown \mathcal{A}(\mathrm{A})$ is the principal order of R_0. By the definition of $\lambda_{\mathfrak{a}}$, $\mathrm{S}(\lambda_{\mathfrak{a}}) = 0$ if and only if $k_{\mathrm{R}}(x^p) \supset k_{\mathrm{R}}(\mu x)$ for all μ in $\mathfrak{a}$, where $\mathfrak{a}$ is an ideal of R and x denotes a generic point of A over k_{R}. Hence there is the largest ideal $\mathfrak{Q}$ in R such that $\mathrm{S}(\lambda_{\mathfrak{Q}^r}) = 0$ with some natural number r. Clearly, $\mathfrak{Q}$ contains no multiple factor. Assume now some power π_{A}^h of π_{A} belongs to R. Then $\mathfrak{Q}$ divides π_{A}^h by definition. Conversely, for any ν in $\mathfrak{Q}$, we have $\mathrm{S}(\nu^r) = 0$, that is, $k_{\mathrm{R}}(x^p) \supset k_{\mathrm{R}}(\nu^r x)$, and by induction, $k_{\mathrm{R}}(\pi_{\mathrm{A}}^h x) = k_{\mathrm{R}}(x^{p^{fh}}) \supset k_{\mathrm{R}}(\nu^{rfh} x)$, which shows that π_{A}^h divides $\mathfrak{Q}^{rfh}$. Hence, if we denote by $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ all the different prime factors of π_{A}^h in R, we have $\mathfrak{Q} = \mathfrak{p}_1 \cdots \mathfrak{p}_s$. Remark that if $\mathrm{S}(\mu)$ is diagonal for all μ in R, this $\mathfrak{Q}$ can be characterized as the largest ideal such that $\mathrm{S}(\lambda_{\mathfrak{Q}}) = 0$.

On the other hand, for arbitrary ground field k, the algebra $\mathcal{A}_0(\mathrm{A})$ has an involutorial anti-automorphism $\mu \rightarrow \mu'$ such that the trace of $\mathrm{M}_l(\mu\mu')$ is positive for any $\mu \neq 0$ in $\mathcal{A}_0(\mathrm{A})$ (and for any $l \neq$characteristic of k) (cf. Weil [10]). Then, if an subfield R_0 of $\mathcal{A}_0(\mathrm{A})$ is invariant by $\mu \rightarrow \mu'$ as a whole, we have $\iota\mu' = \overline{\iota\mu}$ for each isomorphism ι of R_0 into C and for $\mu \in R_0$, (cf. Morikawa [6]). Thus, $\iota\mathrm{R}_0$ is either a totally real field or a totally imaginary quadratic extension of a totally real field.

We now prove the following

PROPOSITION 3. Let A be defined over an algebraic number field k' of finite degree. Let R_0 be a subfield of $\mathscr{A}_0(\mathrm{A})$, and put $\mathrm{R}=\mathrm{R}_0\frown\mathscr{A}(\mathrm{A})$, $K=\iota\mathrm{R}_0$. Assume that $k'=k'_{\mathrm{R}}$, that k' is absolutely normal, and contains K'. Assume furthermore that, for any non-exceptional $\mathfrak{P}'$ in k', the endomorphism $\pi_{\mathfrak{P}'}$ exists and belongs to R. Denote by $\sigma_1,\cdots,\sigma_r$ all the different isomorphisms among $\sigma_1,\cdots,\sigma_j$, determined by A, R_0 and ι. Then, we have the following ideal decomposition:

$$(\iota\pi_{\mathfrak{P}'})=\mathrm{N}_{k'/K}(\sigma_1^{-1}\mathfrak{P}'\cdots\sigma_r^{-1}\mathfrak{P}')$$

in $\iota\mathrm{R}_0$, where σ_i are supposed to be extended to k'. Moreover $[K:\mathrm{Q}]=2r$ and $\sigma_1,\cdots,\sigma_r$, $\sigma_0\sigma_1,\cdots,\sigma_0\sigma_r$ give all the $2r$ isomorphisms of K into C.

PROOF. (Note that $\mathrm{S}(\mu)$ can be transformed simultaneously into diagonal forms $\mathrm{S}_1(\mu)$ in k' for all μ in R, as $k'\supset K'$.)

At first we assume that R is the principal order. The condition $S_1(\nu)\equiv0$ mod. $\mathfrak{P}'$ for ν in R is equivalent to $\iota\nu\equiv0$ mod. $\sigma_i^{-1}(\mathfrak{P}')$ $i=1,\cdots,r$. Then, as was seen above, the prime ideal $\mathfrak{p}_i$ in K divisible by $\sigma_i^{-1}(\mathfrak{P}')$ are all the prime divisors of $\iota\pi_{\mathfrak{P}'}$ in $\iota\mathrm{R}_0$. If $\mathfrak{P}'$ is of the first degree, then $\iota\pi_{\mathfrak{P}'}\cdot\iota\pi_{\mathfrak{P}'}=p$. If moreover $\mathfrak{P}'$ is unramified over Q, then $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ are all different, hence $(\iota\pi_{\mathfrak{P}'})=\mathfrak{p}_1\cdots\mathfrak{p}_r$ and $p=\mathfrak{p}_1\cdots\mathfrak{p}_r\cdot\mathfrak{p}_1\cdots\mathfrak{p}_r$. This shows that $[K:\mathrm{Q}]=2r$ and $\sigma_1,\cdots,\sigma_r$, $\sigma_0\sigma_1,\cdots,\sigma_0\sigma_r$ are all the isomorphisms of K. Then, for general $\mathfrak{P}'$, the relation $\prod_{i=1}^{r}[\mathrm{N}_{k'/K}(\sigma_i^{-1}\mathfrak{P}')\cdot\mathrm{N}_{k'/K}(\sigma_i^{-1}\mathfrak{P}')]=\mathrm{N}\mathfrak{P}'=(\iota\pi_{\mathfrak{P}'})(\iota\pi_{\mathfrak{P}'})$ proves our proposition in this case.

In case of general order R, we take an ideal $\mathfrak{a}$ of the principal order, contained in R, and put $\mathrm{B}=\lambda_{\mathfrak{a}}\mathrm{A}$. Then $\mu\rightarrow\mu^*$ induces an isomorphism on R_0 and maps the principal order of R_0 into $\mathscr{A}(\mathrm{B})$. B, R_0^*, ι' have the same system $\sigma_1,\cdots,\sigma_j$ as A, R_0, ι for ι' defined by $\iota'\mu^*=\iota\mu$, because non-zero characteristic roots of $\mathrm{S}(\mu)$ and of $\mathrm{S}(\mu^*)$ are equal. As $\lambda_{\mathfrak{a}}$ is defined over k, $\pi^*_{\mathfrak{P}'}$ is just the $\pi_{\mathfrak{P}'}$ for B. Then the above result, applied to $\pi^*_{\mathfrak{P}}$, completes the proof.

Now assume that R_0 is of degree $2g$. Then $r=j=g$. Let k be any field of definition of A and k' be an overfield of k satisfying the condition of Prop. 3. For non-exceptional $\mathfrak{P}$ in k_{R}, $\pi_{\mathfrak{P}}$ belongs to the commutor of R_0, hence to R_0 itself. Let $\mathfrak{P}'$ be an prime divisor of $\mathfrak{P}$ in k', and put $\mathrm{N}_{k'/k_{\mathrm{R}}}\mathfrak{P}'=\mathfrak{P}^d$, $\mathrm{N}_{k_{\mathrm{R}}/K^*}\mathfrak{P}=\mathfrak{p}^f$. Then, by Prop. 3, we have $(\iota\pi_{\mathfrak{P}})^d=(\iota\pi_{\mathfrak{P}'})=\mathrm{N}_{k'/K}(\sigma_1^{-1}\mathfrak{P}'\cdots\sigma_g^{-1}\mathfrak{P}')=(\tau_1^{-1}\mathfrak{p}\cdots\tau_s^{-1}\mathfrak{p})^{df}$, as $\sum\sigma_iH=\sum H^*\tau_j$. Hence we have

COROLLARY 1. Assume that R_0 is of degree $2g$. Then, for non-exceptional $\mathfrak{P}$ in k_{R}, with relative degree f over K^*, we have

$$(\iota\pi_{\mathfrak{P}})=(\tau_1^{-1}\mathfrak{p}\cdots\tau_s^{-1}\mathfrak{p})^f,$$

where prime ideal $\mathfrak{p}$ in K^* is considered as an ideal in K'.

COROLLARY 2. Under the same assumption as in Cor. 1, all conjugates of $\mathrm{N}_{k'/K}(\sigma_1^{-1}\beta\cdots\sigma_g^{-1}\beta)$ have the same absolute values $|\mathrm{N}\beta|^{1/2}$ for any β in k'.
(This Cor. is evident, as we have $(\rho\iota\pi_{\mathfrak{P}})\cdot(\sigma_0\rho\iota\pi_{\mathfrak{P}})=\mathrm{N}\mathfrak{P}$ for any isomorphism ρ of K.)

Notations being as above, we make furthermore the assumption:

(A) R_0 is a field of degree $2g$, and there is no not-identical isomorphism σ of K over some imaginary subfield of it such that $\sum_{i=1}^{g}\sigma_i H\sigma=\sum_{i=1}^{g}\sigma_i H$.

Now, let $\mathfrak{p}$ be a prime ideal of the first degree in K^* such that $p=\mathrm{N}\mathfrak{p}$ is unramified in K' and that a prime divisor $\mathfrak{P}$ of $\mathfrak{p}$ in k_{R} is non-exceptional. Then, as $p=\prod\tau_i^{-1}\mathfrak{p}\cdot\overline{\prod\tau_i^{-1}\mathfrak{p}}$, $\prod\tau_i^{-1}\mathfrak{p}$ is not a real ideal. Moreover, for any σ in G, not belonging to H, we have $\sigma(\prod\tau_i^{-1}\mathfrak{p})\neq\prod\tau_i^{-1}\mathfrak{p}$. Indeed, if this is not the case, we should have $\sum\sigma\tau_i^{-1}H^*=\sum\tau_i^{-1}H^*$, hence $\sum\sigma_i H\sigma=\sum\sigma_i H$, and $\prod\tau_i^{-1}\mathfrak{p}$ should be real, a contradiction. This shows that $\iota\pi_{\mathfrak{P}}^h$ generates K for any $h\neq 0$. As $\tilde{\pi}_{\mathfrak{P}}^h$ belongs to the centre of $\mathcal{A}_0(\tilde{\mathrm{A}})$ for some h, we see that $\mathcal{A}_0(\tilde{\mathrm{A}})=\tilde{\mathrm{R}}_0$. Thus, $\tilde{\mathrm{A}}$, and a fortiori A, must be simple. Moreover, for any not-identical automorphism σ of K, we see that $\sum\sigma_i\sigma H\neq\sum\sigma_i H$. This last assertion shows that, any automorphism $\mu\rightarrow\mu^\alpha$ of R_0 is the identity if and only if $\mathrm{S}(\mu)$ and $\mathrm{S}(\mu^\alpha)$ have the same characteristic roots. From this we see especially that $k_{\mathrm{R}}=k^{\smile}K^*$, as $k_{\mathrm{R}}\supset k^{\smile}K^*$ in general.

§4. Zeta functions.

In this § we assume that A is defined over an algebraic number field k of finite degree, and that $\mathcal{A}_0(\mathrm{A})$ contains a subfield R_0 of degree $2g$. We assume furthermore that k contains K' and $k=k_{\mathrm{R}}$, where $\mathrm{R}=\mathrm{R}_0\frown\mathcal{A}(\mathrm{A})$.

At first, we assume that R is the principal order of R_0. For an ideal $\mathfrak{a}$ in R, we call "$\mathfrak{a}$ *division-point*" on A a point a such that $\mu a=0$ for all μ in $\mathfrak{a}$.

The number of such points is just $\mathrm{N}\mathfrak{a}$. We call a $\mathfrak{a}$ division-point b *proper* if it is no $\mathfrak{b}$ division-point for any $\mathfrak{b}\supsetneqq\mathfrak{a}$, that is, $\mu b=\nu b$ implies $\mu\equiv\nu$ mod. $\mathfrak{a}$. Let b be fixed one proper $\mathfrak{a}$ division-point. Then all proper $\mathfrak{a}$ division-points can be written as μb with μ in R prime to $\mathfrak{a}$, and conversely. Especially, for any isomorphism σ of $k(b)$ over k, $b^\sigma=\mu_\sigma b$ with some μ_σ in R, as $k=k_{\mathrm{R}}$. This shows that

b^σ is rational over $k(b)$, that is, $k(b)$ is normal over k. Denote then by $\mathfrak{G}$ the Galois group of $k(b)$ over k. Moreover, for any σ in $\mathfrak{G}$, the class of μ_σ mod. $\mathfrak{a}$ is determined uniquely by σ, hence we denote it by $[\sigma]$. Notice that $[\sigma]=1$ if and only if σ is identity. As μ_σ is rational over k, $\sigma\rightarrow[\sigma]$ is an isomorphism of $\mathfrak{G}$ into the prime residue class group mod. $\mathfrak{a}$ in R, which shows that $k(b)$ is abelian over k. Therefore, $k(b)$ is contained in some "Strahlklassenkörper" mod. F over k, here F can be assumed to be a natural number divisible by $\mathfrak{a}$.

Let now $\mathfrak{P}$ be a non-exceptional prime ideal in k, prime to F, and denote by $\sigma_{\mathfrak{P}}$ the Frobenius automorphism of $\mathfrak{P}$ in $\mathfrak{G}$. Then we have $\widetilde{b^{\sigma_{\mathfrak{P}}}}=\widetilde{\pi_{\mathfrak{P}}}\tilde{b}$. Then Prop. 1, § 1 shows that $b^{\sigma_{\mathfrak{P}}}=\pi_{\mathfrak{P}}b$, as the order of b is prime to N$\mathfrak{P}$. Put $\pi_{\mathfrak{B}}=\pi_{\mathfrak{P}_1}\cdots\pi_{\mathfrak{P}_r}$ for an ideal $\mathfrak{B}=\mathfrak{P}_1\cdots\mathfrak{P}_r$ prime to any exceptional $\mathfrak{P}$. If moreover $\mathfrak{B}$ is prime to F, denote by $\sigma_{\mathfrak{B}}$ the Artin-simbol of $\mathfrak{B}$ in $\mathfrak{G}$. Then the above result shows $b^{\sigma_{\mathfrak{B}}}=\pi_{\mathfrak{B}}b$, that is, $[\sigma_{\mathfrak{B}}]\ni\pi_{\mathfrak{B}}$. Hence, if β in k belongs to the "Strahl" mod. F, we have $\pi_{(\beta)}\equiv1$ mod. $\mathfrak{a}$. But we have in general $(\iota\pi_{\mathfrak{B}})=\mathrm{N}_{k/K}(\sigma_1^{-1}\mathfrak{B}\cdots\sigma_g^{-1}\mathfrak{B})$, so especially for β in k,

$$(\iota\pi_{(\beta)})=\varepsilon(\beta)\mathrm{N}_{k/K}(\sigma_1^{-1}\beta\cdots\sigma_1^{-1}\beta),$$

where $\varepsilon(\beta)$ is a unit in K. As $|\sigma\varepsilon(\beta)|=1$ for any σ in G by Cor. 2 of Prop. 3, $\varepsilon(\beta)$ must be a root of unity in K. Now, if $\beta\equiv1$ mod. F, then $\pi_{(\beta)}\equiv1$ mod. $\mathfrak{a}$, so $\varepsilon(\beta)\equiv1$ mod. $\mathfrak{a}$. This being true for any $\mathfrak{a}$, we assume here that $\mathfrak{a}$ is prime to twice the discriminant of K. Then we have $\varepsilon(\beta)=1$ for $\beta\equiv1$ mod. F. Thus *the symbol* $\chi(\mathfrak{B})=\iota\pi_{\mathfrak{B}}/|\iota\pi_{\mathfrak{B}}|$ *is a "Grössencharakter"* in k (cf. Hecke [4]). Similarly we see that $\chi^\sigma(\mathfrak{B})=\sigma\iota\pi_{\mathfrak{B}}/|\sigma\iota\pi_{\mathfrak{B}}|$ is also a "Grössencharakter" for any σ in G.

The case where R is not the principal order can be treated just as in the second half of the proof of Prop. 3. Then, as the characteristic roots of $\mathrm{M}_l(\pi_{\mathfrak{P}})$ and of $\mathrm{M}_l(\pi_{\mathfrak{P}}^*)$ are equal, we have the same conclusion in this case also.

Now, let B^g be an abelian variety defined over the finite field κ of $q=p^f$ elements. Denote by κ_n the finite field of q^n elements, and by N_n the number of rational points of A over κ_n. Then the zeta function $\mathrm{Z}(u)$ of B is defined by $\dfrac{d}{du}\log\mathrm{Z}(u)=\sum_{n=1}^{\infty}\mathrm{N}_n u^{n-1}$ (cf. Weil [12]). Clearly, N_n is the number of (π_{B}^n-1) division-points. As π_{B}^n-1 is prime to π_{B}, we have $\nu_i(\pi_{\mathrm{B}}^n-1)=1$ for any n. Thus $\mathrm{N}_n=\nu(\pi_{\mathrm{B}}^n-1)=\prod_{i=1}^{2g}(\varpi_i^n-1)$, where $\varpi_1,\cdots,\varpi_{2g}$ are characteristic roots of $\mathrm{M}_l(\pi_{\mathrm{B}})$ for $l\neq p$. From this we see, by a simple calculation, that

$$Z(u)=\prod_{\nu=0}^{2g}[\prod_{i_1\cdots i_\nu}(1-\varpi_{i_1}\cdots\varpi_{i_\nu}u)]^{(-1)^{\nu+1}},$$

where $i_1,\cdots,i_\nu$ run over all combinations of $1,\cdots,2g$.

Coming back to original A defined over k, let $Z_{\mathfrak{P}}(s)$ be the zeta function of $\tilde{A}$ (mod. $\mathfrak{P}$) over $\tilde{k}$, with $(N\mathfrak{P})^{-s}=u$. We define as usual the zeta function of A over k by

$$\zeta_A(s)=\prod_{\mathfrak{P}} Z_{\mathfrak{P}}(s),$$

where $\mathfrak{P}$ runs over all non-exceptional $\mathfrak{P}$'s for A. Then we have proved,

THEOREM 1. *The zeta function* $\zeta_A(s)$ *of* A *has the form:*

$$\zeta_A(s)=\Psi(s)\prod_{\nu=0}^{2g}[\prod_{i_1\cdots i_\nu}L(s-\frac{\nu}{2},\chi_{i_1\cdots i_\nu})]^{(-1)^\nu},$$

where $L(s,\chi_{i_1\cdots i_\nu})$ *are L-functions of* k *with "Grössencharaktere"* $\chi_{i_1\cdots i_\nu}=\chi^{\sigma_{i_1}}\cdots\chi^{\sigma_{i_\nu}}$, Ψ *is a product of rational functions of* q^{-s} *for a finite number of* $q=N\mathfrak{P}$, *and* $\sigma_{i_1},\cdots,\sigma_{i_\nu}$ *run over all combinations of isomorphisms of* K.

We have similarly,

THEOREM 1′. *Let* C *be a non-singular curve. Assume that* C *and a jacobian variety* J *of* C *and a canonical mapping* φ *of* C *into* J *are defined over* k, *and that* J, k *satisfy the conditions of this* §. *Then the zeta function* ζ_C *of* C *(defined similarly as* ζ_A*) has the form:*

$$\zeta_C(s)=\Psi(s)\zeta(s)\zeta(s-1)\prod_{i=1}^{2g}L(s-\tfrac{1}{2},\chi_i)^{-1},$$

where L *and* Ψ *are as in Theorem 1, and* $\zeta(s)$ *is the zeta function of* k.

Remark finally that, if in general there is an abelian variety B^g of characteristic zero, whose ring $\mathcal{A}_0(B)$ contains a field R_0 of degree $2g$ with a system $\iota,\sigma_1,\cdots,\sigma_g$, then there is an A defined over an algebraic number field of finite degree, whose ring $\mathcal{A}_0(A)$ contains a field isomorphic to R_0 with the same system $\sigma_1,\cdots,\sigma_g$. Indeed, B can be defined over a finitely generated field $\kappa=Q(y_1,\cdots,y_r)$ with transcendency degree d. Then, denote by V the locus of $(y_1,\cdots,y_r)$ over $\bar{Q}$. Taking $\mathfrak{V}$ as the set of all divisorial valuations of κ, Prop. 1 shows that there is an abelian variety B′, with the same property as B and defined over a field κ' of transcendency degree $d-1$. Repeating this process d times, we arrive at a disired A.

§ 5. Lemmas from analytic theory.

In this §, we consider only the case of universal domain C.

Let K be a totally imaginary quadratic extension of a totally real field K_0 of degree g, and let $\sigma_1,\cdots,\sigma_g$ be a system of isomorphisms of K, inducing all the g isomorphisms of K_0. Then, σ_0 commutes with all automorphisms of the Galois closure of K, hence we see from Lefschetz's criterion (cf. Lefschetz [5]) that there is an abelian variety A, whose ring $\mathcal{A}_0(\mathrm{A})$ contains a subfield R_0 isomorphic to K with an isomorphism ι, and $\sigma_1,\cdots,\sigma_g$ are exactly the system of isomorphisms of K determined by A, R_0, ι.

Now, let A have this property, and let Ω be a period matrix of A. Then we have $\mathrm{S}(\mu)\Omega=\Omega\mathrm{C}(\mu)$ for μ in $\mathcal{A}(\mathrm{A})$, where $\mathrm{C}(\mu)$ is a rational integral matrix of degree $2g$. Transforming $\mathrm{S}(\mu)$ into diagonal form for μ in R, we see that Ω can be isomorphically transformed into the form (ω_{ij}), where $\omega_{ij}=\sigma_i\omega_j$ and $\omega_1,\cdots,\omega_{2g}$ form a basis of an ideal of $\iota(\mathrm{R})$. Therefore, if A, A$'$ have the above property with the same system $\sigma_1,\cdots,\sigma_g$, they must be isogeneous.

Finally, we remark the following facts: Let A be simple and $\mathcal{A}(\mathrm{A})=\mathrm{R}$ the principal order of the field $\mathcal{A}_0(\mathrm{A})$ of degree $2g$. Assume that there is an positive divisor X whose all elementary divisors are 1, i.e. $l(\mathrm{X})=1$ (cf. Weil [11]). Then, for an ideal $\mathfrak{a}$ of R, $\lambda_{\mathfrak{a}}\mathrm{A}$ has also a positive divior Y with $l(\mathrm{Y})=1$ if and only if $\mathfrak{a}\mathfrak{a}'=(\alpha)$ and $\iota\alpha$ is a totally positive number in K_0. The proof is omitted here.

§ 6. Unramified extension k_0.

In the following §§ 6, 7, we assume that A is defined over an algebraic number field k of finite degree, and the condition (A) in § 3 is satisfied. Hence A is simple. We assume furthermore that $\mathrm{R}=\mathcal{A}(\mathrm{A})$ is the principal order of $\mathcal{A}_0(\mathrm{A})$ and that k contains K^*. This implies $k_{\mathrm{R}}=k$. Let finally k' be the Galois closure of k and $\mathfrak{G}$ the Galois group of k' over K^*.

Let A, A$'$ satisfy these conditions with the same $K=\iota\mathrm{R}=\iota'\mathrm{R}'$ and the same system $\sigma_1,\cdots,\sigma_g$ for these ι,ι'. Then they are isogeneous (§ 5), and we can write $\mathrm{A}'=\lambda_{\mathfrak{a}}\mathrm{A}$ with an ideal $\mathfrak{a}$ in R (§ 2). Conversely, for any ideal $\mathfrak{b}$ in R, $\lambda_{\mathfrak{b}}\mathrm{A}$ has the same property as A with the same K and $\sigma_1,\cdots,\sigma_g$. Thus, for a given K and $\sigma_1,\cdots,\sigma_g$, there are just h non-isomorphic $\mathrm{A}_1,\cdots,\mathrm{A}_h$, h being the class number of K.

Let σ be an automorphism of k'. If there is an automorphism τ of K such that $\sum\sigma\sigma_i H=\sum\sigma_i H\tau$, then $\mathrm{S}^{\sigma}(\mu^{\sigma})=\sigma[\mathrm{S}(\mu)]$ has characteristic roots $\{\sigma\sigma_1\iota\mu,\cdots,\sigma\sigma_g\iota\mu\}=\{\sigma_1\tau\iota\mu,\cdots,\sigma_g\tau\iota\mu\}$. Thus, if we define

ι' by $\tau\iota\mu=\iota'\mu^{\sigma}$, $\mathrm{A}, \mathrm{R}, \iota$ and $\mathrm{A}^{\sigma}, \mathrm{R}^{\sigma}, \iota'$ have the same system $\sigma_1,\cdots,\sigma_g$. Hence σ permutes the isomorphism-classes of $\mathrm{A}_1,\cdots,\mathrm{A}_h$ among themselves. The relation $\mathrm{A}^{\sigma}\cong\lambda_{\mathfrak{a}}\mathrm{A}$ ($\cong$denoting the isomorphism of abelian varieties) determines the class of $\mathfrak{a}$ uniquely, so we can write this class as $\langle\sigma\rangle$. Consider now σ in $\mathfrak{G}$, then we have $\sum\sigma\sigma_i H=\sum\sigma_i H$, hence $\langle\sigma\rangle$ can be defined. Moreover, as $\mathrm{S}^{\sigma}(\mu^{\sigma})=\sigma[\mathrm{S}(\mu)]$ has the same characteristic roots as $\mathrm{S}(\mu)$, hence as $\mathrm{S}(\mu^*)$, and as $\mu^{\sigma}\rightarrow\mu^*$ is an automorphism of $\mathrm{R}_0=\mathcal{A}_0(\mathrm{A})$, we see $\mu^*=\mu^{\sigma}$. Let τ be also in $\mathfrak{G}$ and put $\mathrm{A}^{\tau}\cong\lambda_{\mathfrak{b}}\mathrm{A}$. Then we have $(\mathrm{A}^{\tau})^{\sigma}\cong\lambda_{\mathfrak{b}}^{\sigma}\mathrm{A}^{\sigma}\cong\lambda_{\mathfrak{b}^{\sigma}}\lambda_{\mathfrak{a}}\mathrm{A}\cong\lambda_{\mathfrak{ab}}\mathrm{A}$ as $\mathfrak{b}^{\sigma}=\mathfrak{b}^*$. This shows that $\sigma\rightarrow\langle\sigma\rangle$ is a homomorphism of $\mathfrak{G}$ into the ideal class group of K. Denote by k_0 the subfield of k' corresponding to the kernel of this homomorphism. Then, any automorphism σ of $\bar{k}$ over K^* fixes all elements of k_0 if and only if $\mathrm{A}^{\sigma}\cong\mathrm{A}$. Clearly k_0 is contained in k, and is abelian over K^*. If finally there is a positive divisor X on A with $l(\mathrm{X})=1$, then there are just h' abelian varieties among $\mathrm{A}_1,\cdots,\mathrm{A}_h$, having X_i with $l(\mathrm{X}_i)=1$, where h' denotes the number of classes in K, whose norm to K_0 are the principal class in the narrower sence. Remark that $l(\mathrm{X}^{\sigma})=1$ if $l(\mathrm{X})=1$.

Let now $\mathfrak{p}$ be a prime ideal of the first degree in K^* such that a prime divisor $\mathfrak{P}$ of $\mathfrak{p}$ in k is non-exceptional for A and $\mathrm{N}\mathfrak{p}$ is unramifield in k_0. Denote by $\sigma_{\mathfrak{p}}$ the Frobenius automorphism of $\mathfrak{p}$ in k_0/K^*, and put $\mathfrak{c}=\tau_1^{-1}\mathfrak{p}\cdots\tau_s^{-1}\mathfrak{p}$. Considering mod. $\mathfrak{P}$, we have $\tilde{k}(\tilde{x}^{p})\supset\tilde{k}(\lambda_{\tilde{\mathfrak{c}}}\tilde{x})$, as all prime divisors of $(\iota\pi_{\mathfrak{p}})$ in K divide $\mathfrak{c}$. As $\mathrm{N}\mathfrak{c}=p^{g}$, we have moreover $\tilde{k}(\tilde{x}^{p})=\tilde{k}(\lambda_{\tilde{\mathfrak{c}}}\tilde{x})$, that is, $\mathrm{A}^{\sigma_{\mathfrak{p}}}\cong\lambda_{\tilde{\mathfrak{c}}}\tilde{\mathrm{A}}$. Now, $\tilde{\mathrm{A}}$ being simple, we have $\mathcal{A}(\tilde{\mathrm{A}})=\tilde{\mathrm{R}}$. As we have $\mathrm{A}^{\sigma_{\mathfrak{p}}}\cong\lambda_{\mathfrak{a}}\mathrm{A}$ with $\mathfrak{a}\in\langle\sigma_{\mathfrak{p}}\rangle$, this shows that $\mathfrak{c}\in\langle\sigma_{\mathfrak{p}}\rangle$. We have seen therefore that $(\tau_1^{-1}\mathfrak{p}\cdots\tau_s^{-1}\mathfrak{p})^{f}$ is a principal ideal in K if and only if $\sigma_{\mathfrak{p}}^{f}$ is the identity. Summing up, we have,

THEOREM 2. *Let K be a totally imaginary quadratic extension of a totally real field K of degree g, and $\sigma_1,\cdots,\sigma_g$ be a set of isomorphisms of K into $\mathbf{C}$, inducing all the g isomorphisms of K_0. Assume that $\sigma_1,\cdots,\sigma_g$ satisfy the condition in* (A). *Then there are just h non-isomorphic abelian varieties $\mathrm{A}_1,\cdots,\mathrm{A}_h$, defined over an algebraic number field k of finite degree such that $\iota_i\mathcal{A}(\mathrm{A}_i)$ is the principal order of K, and A_i, $\mathcal{A}(\mathrm{A}_i)$, ι_i have the system $\sigma_1,\cdots,\sigma_g$, where ι_i are isomorphisms: $\iota_i\mathcal{A}_0(\mathrm{A}_i)=K$. Then, the field k_0 defined as above for these* A *is the class field of K^* for the ideal group $I=\{\mathfrak{b}|(\tau_1^{-1}\mathfrak{b}\cdots\tau_s^{-1}\mathfrak{b})\sim 1$ in $K\}$, and $\sigma\longleftrightarrow\langle\sigma\rangle$ gives an explicit form of Artin's reciprocity law.*

COROLLARY. *Notations and assumptions being the same as in the theorem 2, if some A_i has a positive devisor X_i with $l(\mathrm{X}_i)=1$, then* *just h'* A_i*'s have* X_i *with* $l(\mathrm{X}_i)=1$. *If moreover each one of h' classes in K, whose norms to K are the principal class in the narrower sense, contains an ideal of the form* $\tau_1^{-1}\mathfrak{b}\cdots\tau_s^{-1}\mathfrak{b}$ *with* $\mathfrak{b}$ *in K^*, then isomorphism-classes of these h'* A_i*'s are conjugate to each other over K^*.*

§ 7. Field of division-points.

Let $\mathfrak{P}$ be a non-exceptional prime ideal in $k=k_{\mathrm{R}}$ for A, and put $\mathrm{N}_{k/K^*}\mathfrak{P}=\mathfrak{p}^f$. By the Cor. 1 of Prop. 3, §3, we have $(\iota\pi_{\mathfrak{P}})=(\tau_1^{-1}\mathfrak{p}\cdots\tau_s^{-1}\mathfrak{p})^f$. Moreover any conjugate of $\iota\pi_{\mathfrak{P}}$ has absolute value $(\mathrm{N}\mathfrak{p})^{1/2}$. Now, take a system of ideal numbers in K^* (cf. Hecke [4]), and denote by $\hat{\alpha}, \hat{\beta}, \hat{\varpi}, \cdots$, the ideal numbers representing ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{p}, \cdots$ in K^*. Then, as in § 3, we see that any conjugate of $\prod_{i=1}^{s}\tau_i^{-1}\hat{\alpha}$ has the absolute value $|\mathrm{N}\hat{\alpha}|^{1/2}=|\mathrm{N}\mathfrak{a}|^{1/2}$. Thus, $\prod_{i-1}^{s}\tau_i^{-1}\hat{\alpha}$ is determined up to a root of unity factor (not necessarily in K) by $\mathfrak{a}$ only. This shows especially:

$$\iota\pi_{\mathfrak{P}}=\eta\prod_{i=1}^{s}\tau_i^{-1}\hat{\varpi}^f,$$

where η is a root of unity.

Denote by E the group of all roots of unity in R. For any point b on A, we denote by Eb the 0-cycle $\sum_{\varepsilon\in\mathrm{E}}(\varepsilon b)$ on A, and by $k(\mathrm{E}b)$ the smallest field containing k, over which the cycle Eb is rational.

$\mathfrak{a}$ being an ideal in R, let b be a proper $\mathfrak{a}$ division-point on A. Assume that $\mathrm{N}\mathfrak{p}$ is prime to $\iota\mathfrak{a}$, and that $k(\mathrm{E}b)$ (mod. $\mathfrak{P}$) is equal to $\tilde{k}(\mathrm{E}\tilde{b})$, which is certainly the case for almost all $\mathfrak{P}$. Let now f_0 be the smallest exponent such that the congruence $\eta[\prod_{i=1}^{s}\tau_i^{-1}\hat{\varpi}]^{f_0}\equiv\iota\varepsilon$ mod. $\iota\mathfrak{a}$ holds, with some roots of unity η, $\iota\varepsilon$, the latter being in K. Denote then $F=l.c.m.[f, f_0]$. As $\pi_{\mathfrak{P}}^e$ leaves Eb invariant if and only if $\pi_{\mathfrak{P}}^e\equiv\varepsilon$ mod. $\mathfrak{a}$, $\varepsilon\in\mathrm{E}$, and as $\tilde{b}$ is a proper $\tilde{\mathfrak{a}}$ division-point on $\tilde{\mathrm{A}}$, the above expression for $\iota\pi_{\mathfrak{P}}$ shows that F is equal to the relative degree of any prime divisor of $\mathfrak{P}$ in $k(\mathrm{E}b)$ over K^*. This implies that $k(\mathrm{E}b)$ is equal to the composite field of k and the class field $k_{\mathfrak{a}}$ over K^* for the ideal group $I_{\mathfrak{a}}=\{(\hat{\beta})\,|\,\eta\prod\tau_i^{-1}\hat{\beta}\equiv\iota\varepsilon$ mod. $\iota\mathfrak{a}$; η a root of unity and $\varepsilon\in\mathrm{E}\}$. Evidently, this class field contains k_0. Hence we have proved

THEOREM 3. *For proper* $\mathfrak{a}$ *division-point b, we have* $k(\mathrm{E}b)=k\smile k_{\mathfrak{a}}$. *If especially* A *is defined over k, then we have* $k(\mathrm{E}b)=k_{\mathfrak{a}}$.

UNIVERSITY OF TOKYO

BIBLIOGRAPHY

[1] M. Deuring, Die Zetafunktionen einer algebraischen Kurven von Geschlecht Eins, Nachr. Akad. Wiss. Göttingen, 1953, 85–94.

[2] E. Hecke, Höhere Modulfunktionen und ihre Anwendung auf die Zahlentheorie, Math. Ann., **71** (1912), 1–37.

[3] E. Hecke, Über die Konstruktion relative Abelscher Zahlkörper durch Modulfunktionen von zwei Variabeln, Math. Ann., **74** (1913), 465–510.

[4] E. Hecke, Eine neue Art von Zetafunktionen und ihre Beziehung zur Verteilung der Primzahlen, II, Math. Z., **6** (1920), 11–51.

[5] S. Lefschetz, On certain numerical invariants of algebraic varieties with application to Abelian varieties, Trans. Amer. Math. Soc., **22** (1921), 327–482.

[6] H. Morikawa, On abelian varieties, Nagoya Math. J., **6** (1953), 151–170.

[7] G. Shimura, Reduction of algebraic varieties with respect to a discrete valuation of the basic field, Amer. J. Math., **77** (1955), 134–176.

[8] A. Weil, Foundations of algebraic gometry, New York, 1946.

[9] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Paris, 1948.

[10] A. Weil, Variétés abéliennes et courbes algébrique, Paris, 1948.

[11] A. Weil, Théorème fondamentaux de la théorie des fonctions thêta, Séminaire Bourbaki, Paris, 1949.

[12] A. Weil, Number of solutions of equations in finite fields, Bull. Amer. Math. Soc., **55** (1949), 497–508.

[13] A. Weil, Arithmetic on algebraic varieties, Ann. of Math. (2), **53** (1951), 412–444.

[14] A. Weil, Jacobi sums as "Grössencharaktere", Trans. Amer. Math. Soc., **73** (1952), 487–495.

On the Zeta-Function of an Elliptic Function Field with Complex Multiplications

Max DEURING

Let us consider an algebraic curve of genus one

$$E \,:\, f(x, y)=0$$

defined over an algebraic number field k. Take any prime divisor $\mathfrak{p}$ of k and consider the curve

$$E/\mathfrak{p} \,:\, \bar{f}(\bar{x}, \bar{y})=0$$

where $\bar{f}(\bar{x}, \bar{y})$ denotes the residue class of $f(x, y)$ modulo $\mathfrak{p}$. I shall call $E/\mathfrak{p}$ the reduction of E modulo $\mathfrak{p}$. If the reduced curve $E/\mathfrak{p}$ is again a curve of genus one defined over the residue field $k/\mathfrak{p}$, I shall say that E is regular for $\mathfrak{p}$. We know that E is regular for almost all prime divisors of k. The zeta-function of the curve E is defined by

$$\zeta(s, E, k)=\prod_{\mathfrak{p}} \zeta(s, E/\mathfrak{p})$$

where $\zeta(s, E/\mathfrak{p})$ denotes the zeta-function of the curve $E/\mathfrak{p}$ and the product is taken over all prime divisors of k for which E is regular. In the case where E has complex multiplications, it can be proved that

$$(1) \qquad \zeta(s, E, k)=\frac{\zeta(s, k)\zeta(s-1, k)}{L(s-\frac{1}{2}, \chi_E)\, L(s-\frac{1}{2}, \bar{\chi}_E)}$$

where $\zeta(s, k)$ is the zeta-function of k, χ_E is a "Grössencharacter" of k and $L(s, \chi_E)$ is the L-function defined by the character χ_E.

Now a question arises, whether it is possible to change the definition of the zeta-function in such a way that we get in the representation (1) the L-function in the strict sense, namely, whose character χ is defined exactly modulo the conductor. In fact, when the character is defined modulo the conductor, the functional equation of L-series has a simple form; otherwise it is not so simple. Furthermore, it is an interesting problem to find out the meaning of prime factors of the conductor of χ for the given elliptic curve E. In order to find this, it is necessary to take into account also the corresponding function field K of rational functions on the curve E and to define the zeta-function which is attached to the field K rather than to the curve E. When we take the curve E modulo $\mathfrak{p}$, this has the following meaning for the field K: to consider a certain extension $\mathfrak{p}^*$ of $\mathfrak{p}$ in K and to take the residue field $K/\mathfrak{p}^*$. If E is regular for $\mathfrak{p}$, $K/\mathfrak{p}^*$ is again elliptic and is the function field of the curve $E/\mathfrak{p}$. When such a curve E exists for the given function field K (that amounts to saying that such an extension $\mathfrak{p}^*$ of $\mathfrak{p}$ exists), I shall say that K is regular for $\mathfrak{p}$. There are infinitely many ways to extend $\mathfrak{p}$ in K; but it can be proved that if K is regular for $\mathfrak{p}$ there is only extension $\mathfrak{p}^*$ of $\mathfrak{p}$ for which $K/\mathfrak{p}^*$ is elliptic.

Now I shall define the zeta-function of K by

$$\zeta(s, K) = \prod_{\mathfrak{p}} \zeta(s, K, \mathfrak{p})$$

where the product is taken over all prime divisors $\mathfrak{p}$ of k, $\zeta(s, K, \mathfrak{p})$ is the zeta-function of $K/\mathfrak{p}$ or the zeta-function of genus 0 over $k/\mathfrak{p}$ according as K is regular or is not regular for $\mathfrak{p}$. Defining $\zeta(s, K)$ in this way we have

$$\zeta(s, K) = \frac{\zeta(s, k)\zeta(s-1, k)}{L(s-\frac{1}{2}, \chi_K)L(s-\frac{1}{2}, \chi_K)}$$

where χ_K is a "Grössencharacter" defined exactly modulo its conductor and $L(s, \chi_K)$ is the L-function defined by the character χ_K. It is clear that $L(s, \chi_K)$ differs from $L(s, \chi_E)$ only in a finite number of factors in the Euler product. Moreover, the prime factors of the conductor $\mathfrak{f}$ of χ_K are those prime divisors of k for which K is not regular. This is the main result.

I shall now go a little into the detail of the proof. To prove that there exists either no or exactly one extension $\mathfrak{p}^*$ of $\mathfrak{p}$ in K for which $K/\mathfrak{p}^*$ is elliptic is rather easy in the case where $\mathfrak{p}$ does not divide 2 or 3. This is done by taking a suitable equation for K in Weierstrass' form: $y^2 = 4x^3 - g_2x - g_3$. We can treat the case $\mathfrak{p} | 3$ similarly by taking an equation of the form $y^2 = x^3 + \alpha x^2 + \beta x + \gamma$. If $\mathfrak{p} | 2$ the matter gets more complicated.

A question arises whether this is true for curves of higher genus, but I shall not formulate any conjecture about this. I should not be surprised if it is not true for curves of higher genus.[1]

For our purpose it is necessary to consider two elliptic function fields which are birationally equivalent in the algebraic closure of k but not in k. Let K and K' be two elliptic function fields defined

[1] Dr. E. Lamprecht informed me, that he found a proof for the corresponding fact in the case of higher genus.

over k which are birationally equivalent over the algebraic closure of k. Then we can represent K and K' as follows:

$$K=k(x, y),\ y^2=4x^3-g_2x-g_3,$$
$$K'=k(x', y'),\ y^2=4x^3-g'_2x-g'_3,$$

where g_2, g_3, g'_2, g'_3 are numbers in k.

K and K' have the same invariant

$$j=2^6\cdot 3^3\frac{g_2^3}{g_2^3-27g_3^2}=2^6\cdot 3^3\frac{g_2'^3}{g_2'^3-27g_3'^2}\ .$$

For simplicity, we shall restrict ourselves to the case $g_2g_3\neq 0$, namely $j\neq 0$, $\neq 2^6\cdot 3^3$. Since K and K' are birationally equivalent, there exists an element c of k such that $g'_2=g_2c^2$, $g'_3=g_3c^3$. K and K' are birationally equivalent over k if and only if c is the square of a number in k.

Now the following two theorems hold.

THEOREM 1. *Suppose that K is regular for $\mathfrak{p}$. Then K' is regular for $\mathfrak{p}$ if and only if $\mathfrak{p}$ is unramified in $k(\sqrt{c})$.*

THEOREM 2. *Suppose that K has complex multiplications. Denoting by χ and by χ' respectively the Grössencharacter of k obtained from K and from K', we have*

$$\chi'(\mathfrak{p})=\left(\frac{c}{\mathfrak{p}}\right)^{-1}\chi(\mathfrak{p})$$

where $\left(\frac{c}{\mathfrak{p}}\right)$ is the quadratic residue symbol in k.

Now supposing that K has complex multiplications, denote by R the ring of endomorphisms of K and by Σ the quotient field of R; we can regard Σ as a subfield of k. To find out the meaning of the prime factors of the conductor of χ, we proceed as follows.

First we prove that we can find a function field K', determined by a certain prime divisor $\mathfrak{q}_0$ of Σ, with the following properties: i) if K is regular for $\mathfrak{p}$ and $\mathfrak{p}\nmid\mathfrak{q}_0$ then K' is also regular for $\mathfrak{p}$; ii) $\chi_{K'}$ is defined modulo an ideal $\mathfrak{m}'=\mathfrak{q}_0\mathfrak{a}'$ where $\mathfrak{a}'$ is an ideal having only those prime divisors for which K is not regular. We can take $\mathfrak{q}_0$ in infinitely many ways; so that we can conclude that the conductor $\mathfrak{f}$ of χ_K is composed of only those prime divisors for which K is not regular.

To prove that $\mathfrak{f}$ must contain every prime divisors for which K is not regular, we need the following theorem.

THEOREM 3. *Let j be a singular invariant and k be an algebraic number field containing j. For any prime divisor $\mathfrak{p}$ of k, there exists* *an elliptic curve E having the invariant j, defined over k, which is regular for $\mathfrak{p}$.*

In the case where $\mathfrak{p}\nmid 2$, $\nmid 3$, we take as E the curve defined by an equation

$$(2) \qquad y^2=4x^3-3j(j-2^6\cdot 3^3)c^2x-j(j-2^6\cdot 3^3)^2c^3.$$

If we can take c such that $\Delta=2^6\cdot 3^3j^2(j-2^6\cdot 3^3)c^6\not\equiv 0$ mod. $\mathfrak{p}$, then the curve defined by (2) is regular for $\mathfrak{p}$. When $\mathfrak{p}\nmid j$ it suffices to put $c=1$. If $\mathfrak{p}\mid j$, the number j is divisible exactly by a power of $\mathfrak{p}$ whose exponent is a multiple of 3 and if $\mathfrak{p}\mid j-2^6\cdot 3^3$, the number $j-2^6\cdot 3^3$ is divisible by a power of $\mathfrak{p}$ whose exponent is a multiple of 2. Hence we can choose a number c in k in such a way that $\Delta\not\equiv 0$ mod $\mathfrak{p}$; this proves the existence of the curve E, defined over k, which is regular for $\mathfrak{p}$, in case $\mathfrak{p}\nmid 2$, $\nmid 3$. In case $\mathfrak{p}\mid 2$ or $\mathfrak{p}\mid 3$, the matters are much more complicated. In these cases one has to investigate the first two or three members in the $\mathfrak{p}$-adic expansion of the number j.

Finally I call your attention to a problem which is closely connected with the above. K, Σ, R being as above, take any integral ideal $\mathfrak{a}$ of R and consider the subfield $K^{\mathfrak{a}}$ of K which is the composite of all fields K^{α} where α runs over all elements of $\mathfrak{a}$. Then it is well-known that the invariant j' of $K^{\mathfrak{a}}$ is a conjugate of the invariant j of K over the rational number field. The problem is whether there exists an isomorphism of K onto $K^{\mathfrak{a}}$ which maps j onto j'. This is in general not true. But we can prove that for any singular invariant j there exists a function field K with the invariant j for which an isomorphism of K onto $K^{\mathfrak{a}}$ exists. Such a function field is determined by taking a suitable c in the equation (2).

A detailed account has been given in three papers: Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins, Part 1, Nachr. d. Akad. d. Wiss. Göttingen, 1953, p. 85, Part 2, ibid., 1955, p. 13, Part 3, ibid., 1956, p. 37.

GÖTTINGEN

Representatives of the Connected Component of the Idèle Class Group

Emil Artin

André Weil has determined the structure of the connected component of the group of idèle classes of a number field, by describing the structure of the dual of this group. In view of the importance of the connected component it is maybe not without interest to give a direct description by exhibiting a system of representing idèles.

We shall use the following notations:

Let k be an algebraic number field which has r_1 real infinite primes and r_2 complex infinite primes. As usual we put $r=r_1+r_2-1$.

Let $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_r$ be a given system of independent totally positive units, not necessarily a system of fundamental units. By (ε) we denote the group of units generated by the ε_i and by d the index of the group (ε) in the group of all units.

An idèle shall be denoted by $\mathfrak{a}$, its components by $\mathfrak{a}_\mathfrak{p}$ and we set: $P(\mathfrak{a})=\prod_\mathfrak{p} |\mathfrak{a}_\mathfrak{p}|_\mathfrak{p}$. Let J be the group of all idèles, C the group of idèle classes and $P(a)=P(\mathfrak{a})$, if the idèle class is represented by the idèle $\mathfrak{a}$.

By J_0 resp C_0 we mean the kernels of the maps P.

Let U be the subgroup of those idèles of J_0 which have local units as components for every finite prime, and have a positive component at every real infinite prime.

$\bar{U}$ is the group of those idèles of U which have component 1 at every infinite prime.

$\tilde{U}$ is the group of all idèles of U which have component 1 at all finite primes. It is the connected component of the group J_0.

If $\mathfrak{a} \in U$, then $\mathfrak{a}=\tilde{\mathfrak{a}}\bar{\mathfrak{a}}$ denotes the unique decomposition: $\tilde{\mathfrak{a}} \in \tilde{U}$, $\bar{\mathfrak{a}} \in \bar{U}$. For the principal idèle ε_i we have therefore $\varepsilon_i=\tilde{\varepsilon}_i\bar{\varepsilon}_i$.

R denotes the additive reals and Z the additive group of ordinary integers, endowed with the topology where the ideals of Z form a fundamental system of neighborhoods of 0.

$\bar{Z}$ is the completion of Z. $\bar{Z}$ is isomorphic to the direct product of all Z_p, where Z_p is the group of all p-adic integers.

Set $V=R\oplus\bar{Z}$ and imbed the integers m by the diagonal map. Thus an element $\lambda\in V$ is a pair $\lambda=(s, x)$ with $s\in R$, $x\in\bar{Z}$ and the integer m is identified with the pair (m, m).

The group $\bar{U}$ has a fundamental system of neighborhoods of 1 consisting of subgroups of finite index. This allows us to extend the exponentiation $\bar{\mathfrak{a}}^m$ of an element $\bar{\mathfrak{a}}\in\bar{U}$ by an integer m to an exponentiation $\bar{\mathfrak{a}}^x$ where $x\in\bar{Z}$.

If s is a real number we mean by $\tilde{\varepsilon}_i^s$ the idèle in $\tilde{U}$ which is obtained from $\tilde{\varepsilon}_i$ by raising each infinite component into the power s (defining it in some fixed way but taking care that we obtain a real number for à real infinite prime).

For any $\lambda=(s, x)\in V$ we define $\varepsilon_i^\lambda=\tilde{\varepsilon}_i^s\bar{\varepsilon}_i^x$ and notice that for an integer this exponentiation has the usual meaning.

Our first contention is the following: If

$$\bar{\varepsilon}_1^{x_1}\bar{\varepsilon}_2^{x_2}\cdots\bar{\varepsilon}_r^{x_r}=1, \qquad x_i\in\bar{Z}$$

then $x_1=x_2=\cdots=x_r=0$. Since $\bar{Z}$ is Hausdorff it suffices to show that the x_i are arbitrarily close to 0 and this means in the topology of $\bar{Z}$ that they are divisible by any given integer m. To prove this let y_i be an integer, approximating x_i with the accuracy $2dm$

$$y_i\equiv x_i \pmod{2dm}.$$

$\eta=\varepsilon_1^{y_1}\varepsilon_2^{y_2}\cdots\varepsilon_r^{y_r}$ is a unit and we have

$$\bar{\eta}=\bar{\varepsilon}_1^{y_1}\bar{\varepsilon}_2^{y_2}\cdots\bar{\varepsilon}_r^{y_r}=\bar{\varepsilon}_1^{y_1-x_1}\cdots\bar{\varepsilon}_r^{y_r-x_r}.$$

This shows that η is a $2dm$-th power of an element of the local field $k_\mathfrak{p}$ for every finite prime $\mathfrak{p}$. It is well known that this guarantees that η is a dm-th power of an element $\alpha\in k$. This α is a local unit at every finite prime, hence of a unit of k. The element α^d lies in the group (ε):

$$\alpha^d=\varepsilon_1^{\nu_1}\varepsilon_2^{\nu_2}\cdots\varepsilon_r^{\lambda_r}$$

and from $\eta=\alpha^{dm}$ we deduce that y_i is divisible by m. Hence $x_i\equiv y_i\equiv 0 \pmod{m}$ and this is what we wanted to prove.

Let $\phi_j(t)$ be the idèle which has component $e^{2\pi it}$ at the j-th complex prime and all other components equal to 1. We contend next that a product

$$(1) \qquad \varepsilon_1^{\lambda_1}\varepsilon_2^{\lambda_2}\cdots\varepsilon_r^{\lambda_r}\phi_1(t_1)\phi_2(t_2)\cdots\phi_{r_2}(t_{r_2})$$

with $\lambda_i\in V$, $t_j\in R$ is a principal idèle α if and only if all λ_i and all t_j are ordinary integers.

Indeed, if $\alpha \in k$ then we find:

$$\bar{\alpha} = \bar{\varepsilon}_1^{x_1} \bar{\varepsilon}_2^{x_2} \cdots \bar{\varepsilon}_r^{x_r}, \qquad x_i \in \bar{Z}, \qquad \lambda_i = (s_i, x_i).$$

α is a unit at all finite primes hence a unit of k. Its d-th power α^d lies in (ε) and we can write

$$\alpha^d = \varepsilon_1^{y_1} \varepsilon_2^{y_2} \cdots \varepsilon_r^{y_r}, \qquad y_i \in Z.$$

We obtain $\bar{\varepsilon}_1^{dx_1 - y_1} \cdots \bar{\varepsilon}_r^{dx_r - y_r} = 1$ and consequently $dx_i = y_i$. This implies that the integer y_i is divisible by d and proves that each x_i is an ordinary integer. Set $\eta = \varepsilon_1^{x_1} \varepsilon_2^{x_2} \cdots \varepsilon_r^{x_r}$, we have $\bar{\alpha} = \bar{\eta}$ so that in each local field α and η are equal; even if we knew this only in one local field we would already deduce $\alpha = \eta$. Substituting this in (1) and cancelling the terms $\bar{\varepsilon}_i^{x_i}$ we get

$$\tilde{\varepsilon}_1^{s_1} \tilde{\varepsilon}_2^{s_2} \cdots \tilde{\varepsilon}_r^{s_r} \phi_1(t_1) \cdots \phi_{r_2}(t_{r_2}) = \tilde{\varepsilon}_1^{x_1} \tilde{\varepsilon}_2^{x_2} \cdots \tilde{\varepsilon}_r^{x_r}.$$

The independence of the absolute values of the ε_i at the infinite primes allows us to conclude that $s_i = x_i$, that each λ_i is an integer. We are left with

$$\phi_1(t_1) \cdots \phi_{r_2}(t_{r_2}) = 1$$

which is only possible if each t_j is an integer.

We take now a direct sum $rV + r_2 Z$ of r terms V and r_2 terms Z and map this group by (1) into J_0. We follow this map by the canonical map $J_0 \to C_0$ and have a continuous map of the group $rV + r_2 Z$ into C_0. We have seen that the kernel of this map is $rZ + r_2 Z$. Factoring out this kernel we obtain a continuous isomorphism into:

$$(2) \qquad r \cdot V/Z + r_2 \cdot R/Z \to C_0.$$

It is well known that the group V/Z is compact, connected and infinitely and uniquely divisible. This group is called the solenoid. Each circle R/Z is compact, connected and infinitely (but not uniquely) divisible. The left side of (2) is compact, our map is bicontinuous. The image D_0 is compact connected and infinitely divisible.

We contend now that every infinitely divisible idèle class a of C_0 belongs to D_0. Since D_0 is closed it will be enough to show that a lies in the closure of D_0. Let h be the class number of k and m any integer. Since a is divisible we may write $a = b^{2hm}$. The class b^h can be represented be an idèle which has unit components at all finite primes, the class b^{2h} therefore by an idèle $\mathfrak{c}$ of U. The class a is represented by $\mathfrak{c}^m = \hat{\mathfrak{c}}^m \cdot \bar{\mathfrak{c}}^m$. By suitable (highly divisible) choice of m we can bring $\bar{\mathfrak{c}}^m$ as close to 1 as we like. If we can prove that the class of $\hat{\mathfrak{c}}^m = \mathfrak{d}$ belongs to D_0 we will have shown the contention.

This amounts to prove that every idèle $\tilde{\mathfrak{d}} \in \tilde{U}$ has the form (1). Since $P(\tilde{\mathfrak{d}})=1$ and since the absolute values of the ε_i at the infinite primes are independent we can find real numbers $s_1, s_2, \cdots, s_r$ such that the idèle

$$\tilde{\varepsilon}_1^{s_1}\tilde{\varepsilon}_2^{s_2}\cdots\tilde{\varepsilon}_r^{s_r}=\varepsilon_1^{\lambda_1}\varepsilon_2^{\lambda_2}\cdots\varepsilon_r^{\lambda_r}, \qquad \lambda_i=(s_i, 0)$$

has at each prime the same absolute value as $\tilde{\mathfrak{d}}$. At a real infinite prime the components are positive, no adjustment is necessary. At a complex prime we can use the idèle $\phi_j(t_j)$ to adjust the argument of the complex number. Thus

$$\tilde{\mathfrak{d}}=\varepsilon_1^{\lambda_1}\varepsilon_2^{\lambda_2}\cdots\varepsilon_r^{\lambda_r}\phi_1(t_1)\phi_2(t_2)\cdots\phi_{r_2}(t_{r_2})$$

and this completes the proof.

We have also seen that the compact set D_0 contains the image of the connected component $\tilde{U}$ of the group J_0. The group D_0 contains therefore the connected component of C_0; since D_0 is connected, it is itself the connected component of C_0. The map (1) gives the desired explicit representation.

The connected component of C differs from D_0 merely by a line. Its topological structure is therefore that of a direct product of r solenoids, r_2 circles and one real line.

PRINCETON UNIVERSITY

Number Theoretical Investigations on Groups of Finite Order

Richard BRAUER

Consider a group G of finite order n. If K is a given field, we can form the group algebra Γ of G with regard to K. This is an associative algebra such that there exists a basis whose elements form a group G_1 isomorphic with G under multiplication. If we identify G_1 with G, then Γ consists of the elements

$$(1) \qquad \gamma=\sum_{g\in G} a_g g, \qquad a_g \in K.$$

If K is an algebraic number field, the elements γ with integral a_g form an 'order' J in Γ. Here, orders are defined by the following properties. (I) J is a subring of Γ, $1 \in J$. (II) If $\mathfrak{o}$ is the ring of integers in K, J is an $\mathfrak{o}$-module which can be generated finitely. (III) The ring J does not belong to any proper subalgebra Γ. We may then study the number theory in J, and in particular its relationship with group theoretical properties of G. If $n>1$, J is not a maximal order in Γ.

The main purpose of this talk is a discussion of a number of conjectures and open problems. I know the great interest Japanese mathematicians have taken as well in the theory of arithmetics of algebras as in group theory, and perhaps I should say that I have come here to ask for help, since I would like very much to know the answers to my questions.

In order to formulate the conjectures, I have to give some definitions and simple remarks. When I speak of an ideal of J, I shall always mean a two-sided ideal which contains elements different from 0 of K. If $\mathfrak{P}$ is a prime ideal of J, then $\mathfrak{P}\frown K=\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$ and $J\supset\mathfrak{P}\supseteq\mathfrak{p}J$. The prime ideals $\mathfrak{P}$ dividing a fixed $\mathfrak{p}$ are in one-to-one correspondence with the prime ideals $\mathfrak{P}^*$ of $J/\mathfrak{p}J$. Now, $J/\mathfrak{p}J$ may be identified with the group algebra Γ^* of G formed over the residue class field $K^*=\mathfrak{o}/\mathfrak{p}$. Again, the prime ideals $\mathfrak{P}^*$ of Γ^* are in one-to-one correspondence with the irreducible representations F of Γ^* in the field K^* such that $\mathfrak{P}^*$ is the kernel of F. Each representation F is obtained from a representation F_0 of G in K^* by linear extension. If $\phi(g)$ is the trace of $F_0(g)$, $g \in G$, and if F_0 is absolutely irreducible, it is seen easily that the prime ideal $\mathfrak{P}$ of J corresponding to $\mathfrak{P}^*$ consists of the elements (1) such that

$$\sum a_g^* \phi(gh) = 0^* \qquad (\text{for all } h \in G).$$

Here, a_g^* is the residue class of $a_g \in \mathfrak{o}$ (mod $\mathfrak{p}$).

We next write $\mathfrak{p}J$ as intersection of ideals $\mathfrak{B}_\tau \neq J$,

$$\mathfrak{p}J = \mathfrak{B}_1 \frown \mathfrak{B}_2 \frown \cdots \frown \mathfrak{B}_t \tag{2}$$

such that $\mathfrak{B}_\sigma$ and $\mathfrak{B}_\tau$ are relatively prime for $\sigma \neq \tau$, i.e., $(\mathfrak{B}_\sigma, \mathfrak{B}_\tau) = J$. If none of the $\mathfrak{B}_\tau$ can be written as the intersection of two relatively prime ideals, we call $\mathfrak{B}_1, \mathfrak{B}_2, \cdots, \mathfrak{B}_t$ the block ideals of $\mathfrak{p}J$. They are uniquely determined. Actually, $\mathfrak{p}J$ is the product of the $\mathfrak{B}_\tau$, and any two of the $\mathfrak{B}_\tau$ commute. Each prime ideal $\mathfrak{P}$ dividing $\mathfrak{p}J$ divides $\mathfrak{B}_1\mathfrak{B}_2\cdots\mathfrak{B}_t$ and hence $\mathfrak{P}$ divides exactly one of the $\mathfrak{B}_\tau$. Let B_τ be the set of the prime ideals $\mathfrak{P}$ dividing $\mathfrak{B}_\tau$. Replace now each prime ideal $\mathfrak{P}$ by the corresponding modular representation F. Thus, the irreducible modular representations F of G are distributed into disjoint sets $B_1, B_2, \cdots, B_t$ which are called the 'blocks' of representations.[1]

We shall assume that the algebraic number field K is a splitting field of the semisimple algebra Γ, i.e., that the irreducible representations $X_1, X_2, \cdots, X_k$ of G in K are absolutely irreducible. This assumption is certainly satisfied, if K contains the n-th roots of unity.

If X_i is an ordinary irreducible representation of G in K, we can always find coordinate systems such that the coefficients of each $X_i(g)$, $g \in G$, are local integers for $\mathfrak{p}$. Then the residue class map carries X_i into a modular representation X_i^* of G in K^*. Here, X_i^* is not uniquely determined by X_i. However, if $F_1, F_2, \cdots, F_l$ are the different modular irreducible representations of G in K^*, then the multiplicity d_{ij} of F_j as irreducible constituent of X_i^* is uniquely determined. These d_{ij} are the decomposition numbers. For each X_i all F_j actually appearing in X_i^* belong to the same block B. We shall count X_i as a member of the block B in this case. Thus, the ordinary irreducible representations $X_1, X_2, \cdots, X_k$ of G in K are also distributed into our blocks $B_1, B_2, \cdots, B_t$.

Set

$$c_{ij} = \sum_{\rho=1}^{k} d_{\rho i}\, d_{\rho j}. \tag{3}$$

[1] For a discussion of blocks, I may refer to the book by G. Azumaya and T. Nakayama, "Daisûgaku II" (Algebra II), Iwanami-Shoten, Tokyo (1954).

If F_i and F_j belong to different blocks, then $c_{ij}=0$. If i and j range over the indices for which F_i and F_j belong to a fixed block B_τ, the numbers c_{ij} represent the Cartan invariants of the algebra $J/\mathfrak{B}_\tau$.

Finally, for each block B we define the 'defect' δ of the block. If p is the rational prime divisible by $\mathfrak{p}$, δ is the largest integer such that p^δ divides $n/Dg\,X_i$ for some $X_i \in B$. Equivalently, we may say that δ is the largest integer such that p^δ divides some n/DgF_j with $F_j \in B$.

I now come to the discussion of the conjectures mentioned above.

(I). Given p and δ, consider all blocks B of defect δ for all finite groups G. The conjecture is that the decomposition numbers d_{ij} corresponding to the block lie below a bound depending only on p and δ. Because of (3), this is equivalent with the corresponding statement concerning the Cartan invariants c_{ij}. Our conjecture means that for given p and given defect δ, representations X_i^* cannot split into too many irreducible modular constituents.

Let me discuss some known results in support of this conjecture. If $\delta=0$, the block consists of one X_i and one F_j and $d_{ij}=1$, $c_{jj}=1$. The conjecture is still true for $\delta=1$. A number of years ago, I studied groups whose order is divisible only by the first power of a prime p.[2] The results obtained for blocks of defect 1 in this case hold in general for blocks of defect 1. We have here $d_{ij}\leqq 1$, $c_{ij}\leqq p$. We may make our conjecture more precise by asking: Is it true that

$$c_{ij}\leqq p^\delta$$

for the Cartan invariants of a block B of defect δ?

In the case $\delta=1$, we can describe exactly which systems (d_{ij}) can occur and can give relations between the types which occur and group theoretical properties of G. It would be highly desirable to have analogous results for higher defects. For $\delta=2$, it is no longer true that $d_{ij}\leqq 1$.

There is a result weaker than the conjecture above which can be proved for arbitrary defect. The Cartan invariants c_{ij} belonging to a block B of defect δ may be taken as the coefficients of a quadratic form H which is positive definite. Then it can be shown that, for given p and δ and all finite groups G, the form H belongs to a finite number of classes. This is proved by showing that if B consists of

[2] R. Brauer, Investigations on group characters, Ann. of Math. **42** (1941), 936–958.

α ordinary representations X_i and β modular representations F_j, we have[3)]

(a)	$\det(c_{ij})=p^{\mu}$	with	$\mu\leqq\delta+(\beta-1)(\delta-1)$.
(b)	$\beta<\alpha$	for	$\delta>0$.
(c)	$\alpha\leqq p^{2\delta-2}$	for	$\delta>1$.

For our present purposes, an inequality weaker than (c) would suffice which I have given a number of years ago. In the form stated here, it was obtained by W. Feit and myself improving the inequality $\alpha\leqq\frac{1}{4}p^{2\delta}$ which we had given recently.[4)]

For $\delta\leqq2$, we have $\alpha\leqq p^{\delta}$. Probably, this is true for all δ. There is one way in which this inequality might be proved. The quadratic form belonging to the matrix $p^{\delta}(c_{ij})^{-1}$ has integral coefficients. If it could be shown that β is the smallest integer $\neq0$ represented by this form, this would yield the inequality $\alpha\leqq p^{\delta}$. This method works for $\delta=2$ and in some special cases; however I feel somewhat doubtful about the general case.

(II). We have the problem of determining the number of blocks of a fixed defect δ for a given group G. Let me mention first that this can be done at once when the characters of G are known. However, this is not what we want, since our aim is to obtain new properties of the group characters.

The situation is here opposite to that in (I), where small defects could be handled while the case of large defects seems difficult. For $\delta>0$, we have a satisfactory treatment of (II) in form of a reduction to groups of smaller order.[5)] However, the problem remains to characterize the number of blocks of defect 0 of a group G by group theoretical properties. If a complete answer to the problem of the exact number of representations in a block could be given, this would answer our question. This process is feasible in the case $g\equiv0\pmod p$, $g\not\equiv0$

[3)] The fact that $\det(c_{ij})$ is a power of p and the inequality in (b) are well known facts in the theory of modular representations of finite groups. The inequality in (a) is a consequence of the fact that δ is the largest elementary divisor of (c_{ij}) and that it appears with multiplicity 1.

Cf. R. Brauer, On the arithmetic in a group ring, Proc. Nat. Acad. Sci. **30** (1944), 109–114; M. Osima, Notes on blocks of group characters, Math. J. of Okayama Univ. **4** (1955), 175–188; R. Brauer, Zur Darstellungstheorie der Gruppen endlicher Ordnung, (to appear in Math. Zeitschr.).

[4)] Cf. R. Brauer, On the structure of groups of finite order, to appear in the Proc. Internat. Congress of Math. Amsterdam 1954.

[5)] Cf. the papers quoted in 3).

(mod p^2). Let P be a Sylow-subgroup of G of order p and let N be its normalizer. Then the number of blocks of defect 0 of G is $k-k'$ where k is the class number of G and k' that of N. In particular, $k \geqq k'$. I don't know a direct proof for this inequality which does not involve representation theory. Actually, it would be of interest to know the necessary and sufficient conditions for k and k' to be equal.

(III). Suppose that p^a is the exact power of p in g. By definition of the defect δ of a block B, the degrees of the ordinary representations in B are all divisible by $p^{a-\delta}$ while some of these degrees are not divisible by $p^{a-\delta+1}$. The problem arises to determine when degrees divisible by $p^{a-\delta+1}$ occur in a block B. Let us call this the case of a raised degree.

In the work mentioned in (II), a subgroup D of G of order p^δ is associated with a block B of defect δ. This is the defect group of the block. Each conjugate group may be taken; apart from this, the defect group D is uniquely determined. The simplest conjecture is that raised degrees occur, if and only if D is abelian. If this conjecture is true, it would furnish a generalization of the known fact that no raised degrees are possible, if $g \not\equiv 0 \pmod{p^2}$. The conjecture is trivially true in the case of p-groups. In order to test the conjecture further, I have studied the case $p=2$, $g \equiv 0 \pmod 8$, $g \not\equiv 0$ (mod 16) in which special methods are available. While the answer is not complete, I like to state the results obtained, since they are helpful in studying special groups. As above, let P denote the Sylow subgroup of G so that here P has order 8. Let B be a block of defect 3; $D=P$. We then have the following cases.

(A) *P the quaternion group of order* 8.

CASE 1. The block consists of four characters of odd degrees z_1, z_2, z_3, z_4 and three characters of even degress. We have an equation

$$\varepsilon_1 z_1 + \varepsilon_2 z_2 + \varepsilon_3 z_3 + \varepsilon_4 z_4 = 0$$

where each ε_i is ± 1 and where

$$\varepsilon_1 z_1 \equiv \varepsilon_2 z_2 \equiv \varepsilon_3 z_3 \equiv \varepsilon_4 z_4 + 4 \pmod 8.$$

The three even degrees are given by

$$z_5 = \pm(\varepsilon_1 z_1 + \varepsilon_2 z_2), \qquad z_6 = \pm(\varepsilon_1 z_1 + \varepsilon_3 z_3), \qquad z_7 = \pm(\varepsilon_1 z_1 + \varepsilon_4 z_4).$$

Actually, these are special cases of relations available for the values of the characters.

As an example, I mention the extended icosahedral group of order 120 which has a block B with the degrees

$$z_1=3,\ z_2=3,\ z_3=5,\ z_4=1,\ z_5=6,\ z_6=2,\ z_7=2.$$

CASE 2. The block consists of four equal odd degrees z and one even degree $2z$.

For instance, this case arises for $G=P$, $z=1$.

(B) *P the dihedral group of order* 8.

The block consists of four characters of odd degrees z_1, z_2, z_3, z_4 and one of an even degree z_5 and we have equations

$$\varepsilon_1 z_1+\varepsilon_2 z_2=\varepsilon_3 z_3+\varepsilon_4 z_4=z_5$$

with $\varepsilon_i=\pm 1$. For instance, for the alternating group A_6, we have $z_1=1$, $z_2=9$,' $z_3=5$, $z_4=5$, $z_5=10$; for A_7: $z_1=1$, $z_2=15$, $z_3=21$, $z_4=35$, $z_5=14$; for the simple group of order 168: $z_1=1$, $z_2=7$, $z_3=3$, $z_4=3$, $z_5=6$.

(C) *P abelian of type* (2, 2, 2).

CASE 1. B consists of eight odd degrees z_i, $1\leqq i\leqq 8$ which satisfy a relation $\sum \varepsilon_i z_i=0$ with $\varepsilon_i=\pm 1$.

Example. The simple group of order 504 where we have the degrees 1, 7, 7, 7, 7, 9, 9, 9 in a block.

CASE 2. B consists of four characters of odd degrees z_1, z_2, z_3, z_4 and one even degree z_5 with an equation

$$2z_5=\varepsilon_1 z_1+\varepsilon_2 z_2+\varepsilon_3 z_3+\varepsilon_4 z_4, \qquad (\varepsilon_i=\pm 1).$$

(D) *and* (E) *P abelian of type* (4, 2) *or of type* (8).

Here, B consists of eight equal odd degrees.

I do not know whether the case 2 in (C) can occur. Apart from this, our conjecture is true for the groups considered here.

In principle, one can obtain a finite number of similar types for each given defect group by combining the known relations for characters. However, in general, the number of cases to be distinguished will be large and it will not be clear which cases can actually occur. Still it might be useful to work out further cases.

Our special results lead to the following question: If the characters of a finite group G are known, how much information about the structure of the Sylow groups P can be obtained from this knowledge of the characters? Even if the conjecture (III) is not true in general, it seems that results in this direction could be obtained.

(IV). In the case of defect $\delta=1$, the structure of the residue class ring $J/\mathfrak{B}$ of J modulo a block ideal $\mathfrak{B}$ can be described rather completely. The question arises whether analogous results exist for higher defects. Still more generally, it may be possible to investigate the rings $J/\mathfrak{B}^r$, $r \geqq 1$. This would lead to a deeper study of the number theory of J. In particular, from our point of view we would be interested in connections with group theorectical properties.

There are some known facts concerning the structure of the indecomposable components of the modular regular representation which might be understood more clearly by such an investigation. Also there would be hope that this work would lead to results in connection with the questions asked above.

(V). I mention some questions concerning modular representations which have remained unanswered. The degrees of the ordinary irreducible representations X_i divide the order n of the group. The corresponding fact is not true for the degrees f_j of the modular irreducible representations F_j. However, it seems possible that at least the power of the fixed prime p dividing f_j always divides n.

If Γ^* now denotes the group algebra of G with respect to an arbitrary field K^* of prime characteristic p, Γ^* is semi-simple, if and only if p does not divide n. If $p \mid n$, the problem arises to determine the radical N of Γ^*. It is not very difficult to give necessary and sufficient conditions that an element

$$\gamma = \sum_{g \in G} c_g g, \qquad c_g \in K^*$$

of Γ^* belongs to N. Let p^r denote the highest power of p for which there exist elements of order p^r in G. If h is an arbitrary element and t a p-regular element of G, let $Z(h, t)$ denote the set of all elements g of G for which the p^r-th powers of hg and of t are conjugate in G. Then necessary and sufficient conditions are given by the equations in K^*

$$\sum_{g \in Z(h,t)} c_g = 0$$

for all $h, t \in G$ and t p-regular.

However, in this form the equations are too complicated to be of much value. For instance, except in the simplest cases, they cannot be used to find the rank of the radical.[6] The question is whether it is possible to obtain simpler conditions which really enable us to study the radical. There would be some interest in having formulas for the ranks of the powers of N and for the exponent of N.

(VI). It must be emphasized that it is much easier to ask questions than to answer them. In this connection, I mention the

[6] Of course, if the irreducible representations of G in K^* have the degrees $f_1, f_2, \cdots$, this rank is given by $n - f_1^2 - f_2^2 - \cdots$.

two well known problems: (1) What are the necessary and sufficient conditions that a square array A of complex numbers represents the table of characters of a finite group G? (2) How much additional information is required in order that G be uniquely determined? The answer to these questions seems to be very difficult. Perhaps, it may be worthwhile to study these questions for special types of groups.

(VII). There are various applications of the results obtained to group theoretical questions. However, these applications are still rather scattered and for this reason, I shall not attempt to give a summary. In many cases, we can get information about the characters of groups G of which only little is known. For instance, if the order n is given and if G is assumed to be simple, it is often possible to show that the known relations lead to contradictions and hence that no simple group of that order n can exist. For other values of n, the results enable us to find the characters and, on the basis of this, determine G. I think that it is possible to determine all simple groups up to some rather high order n in this manner, possibly with the exception of a few values.

In concluding, I would like to mention one particular type of problem. Given a group H of finite order and a set S of elements $h \neq 1$ of H. What are the groups G which contain H as a subgroup such that the centralizers of the elements $h \in S$ in G lie in H? For instance, we may take for S the elements $\neq 1$ of one or several Sylow groups of H and then the theory of blocks gives us at least some results concerning G. There are many ways in which our question can be modified.

Perhaps, I can describe the situation best by taking up a simple example. Let H be the cyclic group of order 3 and let S be the set consisting of a generating element of H. Here, the order n of G must have the form $n = 3f(f+1)m^2$ where f and m are natural integers, $f \equiv 1 \pmod 3$, $m \not\equiv 0 \pmod 3$. There exist infinitely many groups G which satisfy the conditions. Each such G has a unique maximal normal subgroup $G_0 \neq G$ and the group G/G_0 is simple and satisfies the same conditions. Two simple groups G of this type are known, the simple groups of order 60 (with $f=4$ and $m=1$) and of order 168 (with $f=7$ and $m=1$). I don't know whether any further simple groups exist. In general, one can ask whether conditions of this type can ever be satisfied by infinitely many simple groups.

HARVARD UNIVERSITY

Galois Groups Acting on the Multiplicative Groups of Local Fields

Kenkichi IWASAWA

Let k be a finite extension of degree m over Q_p, the field of p-adic numbers, and E a finite tamely ramified Galois extension of k. Let F be the inertia field of E/k and let $[E:F]=e$, $[F:k]=f$. The Galois group $G(E/F)$ is then a normal subgroup of the Galois group $G(E/k)$, and, $G(E/F)$ and $G(E/k)/G(E/F)=G(F/k)$ are both cyclic groups. In the following, we assume that the group $G(E/k)$ contains an element σ of order f which induces the Frobenius automorphism on the unramified extension F/k. $G(E/k)$ is then generated by σ and a generator τ of $G(E/F)$, and the defining relations are given by

$$\sigma^f=1, \qquad \tau^e=1, \qquad \sigma\tau\sigma^{-1}=\tau^q,$$

where q is the number of elements in the residue class field of E. Let p^κ be the highest power of p dividing the order of any root of unity in E and let w be a primitive p^κ-th root of unity in E. We, then, further assume that $\kappa\geqq 1$ and that $[E:k(w)]$ is divisible by p, and even by 4 when $p=2$. Under these assumptions, the action of the Galois group $G(E/k)$ on the multiplicative group U_1, consisting of all units a in E with $a\equiv 1$ mod. π ($\pi=$ a prime element in E), can be explicitly described as follows.

We first notice that for any a in U_1 and for any p-adic integer α, a^α is defined as usual and is again an element of U_1. Therefore, if we denote by O_p the ring of p-adic integers and by R the group ring of $G(E/k)$ over O_p, R can be considered as an operator domain of U_1 in an obvious way, and for our purpose, it is sufficient to determine the structure of the R-group U_1. Then, as an R-group, U_1 contains $m+1$ generators $a_0, a_1, \cdots, a_m$ over R with the following fundamental relations:

$$a_0^{\sigma-g}=a_1^{p^\kappa\lambda}, \qquad a_0^{1-\sigma^f}=a_1^{p^\kappa\mu}, \qquad a_0^{\tau-\zeta}=1.$$

Here, g is a rational integer satisfying $w^\sigma=w^g$, ζ is a root of unity in O_p uniquely determined by $w^\tau=w^\zeta$, and λ and μ are elements in R defined by

$$\lambda=\frac{1}{e}\sum_{j=0}^{e-1}\zeta^{-j}\tau^{j}, \qquad \mu=\left(\sum_{i=0}^{f-1}g^{i}\sigma^{-i-1}\right)\lambda.$$

Now, let Ω be an algebraic closure of k and V the ramification field of the extension Ω/k, i.e. composite of all finite tamely ramified extensions of k in Ω. Furthermore, let A be the maximal abelian extension of V in Ω. As the Galois group $G(A/V)$ is an abelian normal subgroup of the Galois group $G(A/k)$ with the factor group $G(V/k)$, the latter acts on $G(A/V)$ in a natural way. Using the result mentioned above, we can, then, explicitly give the action of $G(V/k)$ on $G(A/V)$ as follows: let $\bar{Q}_p$ denote the factor group of the additive group of Q_p modulo the additive group of O_p and C the set of all continuous functions on the compact group $G(V/k)$ (in its Krull topology) with values in the discrete group $\bar{Q}_p$. C is then an O_p-module in an obvious way. But we can also make C a $G(V/k)$-module by putting

$$(\rho h)(\omega)=h(\rho^{-1}\omega),$$

for any ρ in $G(V/k)$ and any $h=h(\omega)$ in C. Let X be the direct sum of $\bar{Q}_p$ and m copies of the module C. For any ρ in $G(V/k)$ and any $x=(a, h_1, \cdots, h_m)$ in X, where $a \in \bar{Q}_p$, $h_i \in C$, we put

$$\rho x=(b, \rho h_1, \cdots, \rho h_m),$$

with a suitable b in $\bar{Q}_p$ depending on ρ, a and h_i, of which precise definition is, however, omitted here. X is thus also made a $G(V/k)$-module. Now, the compact abelian group $G(A/V)$ is, as a $G(V/k)$-group, isomorphic with the character group of the discrete $G(V/k)$-group X as defined above[1].

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

[1] For the details, c.f. K. IWASAWA, On Galois groups of local fields: Trans. Amer. Math. Soc., **80** (1955), pp. 448–469.

On the Generalized Principal Ideal Theorem

Tadao TANNAKA

In the following lines I am intending to give several remarks concerning principal ideal problem, which I have obtained recently. As is well known principal ideal theorem, which asserts that every ideal $\mathfrak{a}$ in an algebraic field k becomes principal in its absolute class field K, was first formulated by D. Hilbert, and was proved by Ph. Furtwängler, employing Artin's general law of reciprocity. Furtwängler's result was in substance of group-theoretical nature. S. Iyanaga generalized the arithmetical part of the principal ideal theorem to the case of "Strahl" class field, and his theorem runs as follows:

If K is "Strahl" class field over k, and $\mathfrak{f}=\mathfrak{f}(K/k)$, $\mathfrak{F}=\mathfrak{F}(K/k)$ its conductor and modulus of genus respectively, then every ideal $\mathfrak{a}$ of k which is prime to $\mathfrak{f}$ becomes principal in K and moreover it belongs to the "Strahl" $R_K(\mathfrak{F})$ modulo $\mathfrak{F}$.

If K/k is (in general ramified) cyclic field, so the situation is quite simple and we have the following formula by direct computation

$$(1) \qquad a=\frac{h\cdot 2^{\rho}\prod e_{\mathfrak{p}}}{n\cdot(\varepsilon:\mathfrak{N}(\theta))}$$

where

a: ambigous class number,

h: absolute class number of k,

ρ: number of ramifying infinite spots of k,

$e_{\mathfrak{p}}$: exponent of ramification of $\mathfrak{p}$,

n: relative degree of $K/k=(K:k)$,

ε: units in k,

θ: elements of K whose norm $\mathfrak{N}(\theta)$ are units in k.

If we assume further that K is absolute class field, so we have immediately $a=1$ and this is a generalized form of principal ideal theorem. From this fact we are naturally lead to the following conjecture: If K is the absolute class field over k, and $\mathfrak{A}$ is an ambigous ideal in the suitable sense, then $\mathfrak{A}$ is a principal ideal in K, and this is the main object of present investigation. I have introduced a concept of ambigousness in my paper [1]. I called namely an ideal $\mathfrak{A}$ in K ambigous, if it satisfies the following conditions:

$$\mathfrak{A}^{1-\sigma}=(A_\sigma),\qquad \frac{A_\tau\cdot A_\sigma^\tau}{A_{\sigma\tau}}=\varepsilon_{\sigma,\tau}=\varepsilon_{\tau,\sigma}.$$

Our main theorem, which I have obtained recently, is now

MAIN THEOREM 1. *If K is the absolute class field over k, then every ambigous ideal in K is principal.*

Now we shall proceed to the proof of this theorem. Most essential part of our proof is the following lemma, which was first proved by Dr. Terada.

LEMMA. *Let K be the absolute class field over k and Ω/k its cyclic intermediate field, then every (in ordinary sense) ambigous ideal in Ω becomes principal in K.*

This lemma was conjectured by myself and proved to be true for several groups of lower degrees. First complete proof resting on the basis of Furtwängler's method was, as was already mentioned, given by Terada (see Bibliography [2]), after a rather complicated and elaborate computation. Afterwards I was also able to give an alternative proof which depends upon Artin's splitting group, and is much simpler than that of Dr. Terada. We shall give a brief sketch of my own proof of this lemma.

Let K be the (absolute) class field over k, $\bar{K}$ the second class field, and G the Galois group $G(\bar{K}/k)$ of $\bar{K}/k$, then K belongs to the commutator subgroup G' of G, in the sense of Galois theory. If a prime ideal $\mathfrak{P}$ in $\bar{K}$ is a divisor of $\mathfrak{q}$ and $\mathfrak{p}$ in K and k respectively, then we have for the Frobenius automorphism $\sigma=\left[\frac{K/k}{\mathfrak{P}}\right]$ following relations

$$\left(\frac{\bar{K}/K}{\mathfrak{q}}\right)=\sigma^f,\qquad N_{K/k}(\mathfrak{q})=\mathfrak{p}^f$$

where parenthesis $\left(\quad\right)$ means Artin symbol, and

$$\left(\frac{\bar{K}/k}{\mathfrak{p}}\right)=\mathrm{V}_{G\to G'}(\sigma)=\prod_\tau S_\tau S_\sigma S_{\sigma\tau}^{-1}$$

($S_1=1$, S_τ: representatives for the factor group $G/G'=\Gamma$, V: Verlagerung).

Our lemma can then be stated as the following purely group-theoretical theorem:

LEMMA. *Let G be a metabelian group with commutator subgroup G', H be an invariant subgroup of G with the cyclic quotient group G/H, and A an element of H with $ASA^{-1}S^{-1}\in H'$ (S being a genera-*

tor of G/H) *then the "Verlagerung"* $\mathrm{V}(A)=\mathrm{V}_{H\to G'}(A)=\prod_T TATA^{-1}$ *from* H *to* G' *is the uuit element of* G. *Thereby* T *runs over a fixed representative system of* H/G', *and* $\overline{TA}$ *means the representative corresponding to the coset* TAG'.

Now we introduce Artin's splitting group $\overline{\mathfrak{U}}$, which is generated by $\mathfrak{U}=G'$ and the symbols $A_\sigma(\sigma\neq 1)$ $(\sigma\in\Gamma=G/G')$ with Γ as operator domain which acts on $\overline{\mathfrak{U}}$ as

$$\begin{aligned}&U^\sigma=S_\sigma U S_\sigma^{-1} \qquad (U\in G'=\mathfrak{U})\\ &A_\tau^\sigma=A_\sigma^{-1}A_{\sigma\tau}D_{\sigma,\tau}^{-1}\\ &(A_1=1,\ S_\tau S_\sigma S_{\sigma\tau}^{-1}=D_{\sigma,\tau}).\end{aligned}$$

We have then

$$A_{\sigma\tau}\equiv A_\sigma A_\tau^\sigma \qquad \mathrm{mod}\ \mathfrak{U}$$

so that the splitting group $\overline{\mathfrak{U}}$ is symbolically generated by $\mathfrak{U}$ and

$$A_i=A_{\sigma_i} \qquad (i=1, 2, \cdots)$$

where $\sigma_1, \sigma_2, \cdots$ are generators of the group Γ. We have also

$$\begin{aligned}&(U_\sigma S_\sigma)(U_\tau S_\tau)(U_\sigma S_\sigma)^{-1}(U_\tau S_\tau)^{-1}\\ &=U_\sigma^{1-\tau}U_\tau^{\sigma-1}A_\sigma^{\tau-1}A_\tau^{1-\sigma}\\ &=(U_\sigma^{1-\tau}U_\tau^{U_\sigma-1})(U_\sigma^{1-U_\tau}U_\tau^{\sigma-1})(A_\sigma^{\tau-1}A_\tau^{1-\sigma}).\end{aligned}$$

From these facts we have the following results. Using the additive manner of writing every element of G' can be represented in the form

$$\sum_{r,s} A_{r,s}\Delta_r C_s$$

where $A_{r,s}=-A_{s,r}$, $A_{r,r}=0$, $\Delta_r=1-S_r$ (S_r denotes the representative of G/G' which corresponds to a fixed system of generators of $\Gamma=G/G'$ or the elements of G') and C_r the elements which correspond to S_r.

Now we can transform our lemma in the form:

LEMMA. *Let* M *be an additive group (with the group algebra* $Z[G]$ *as operator domain) with the (not necessarily independent) base elements* $C_1, C_2, \cdots, C_n$ *and* C *and*

$$\begin{aligned}&N_iC_i=\sum_{r,s=1}^n A_{r,s}^{(i)}\Delta_r C_s+\sum_{j=1}^n B_j^{(i)}\delta_j \qquad (i=1, 2, \cdots, n),\\ &\quad\delta_i=\Delta C_i-\Delta_i C,\\ &\quad\Delta_i=1-S_i, \qquad \Delta=1-S,\\ &\quad N_i\Delta_i=0,\\ &\quad A_{r,s}^{(i)}=-A_{s,r}^{(i)}, \qquad A_{r,r}^{(i)}=0,\\ &\quad N_i=1+S_i+S_i^2+\cdots+S_i^{e_i-1}\end{aligned}$$

$\left(\begin{array}{l}e_i\text{: } \textit{order of } S_i \text{ modulo } G'\textit{, so that}\\ e_i=1,\ N_i=1 \textit{ if } S_i \textit{ represents the element of } \mathfrak{U}=G'\end{array}\right).$

If then

$$\sum_{i=1}^{n} \Gamma'_i \delta_i = \sum_{r,s} F_{r,s} \Delta_r C_s \qquad (F_{r,s} = -F_{s,r},\ F_{r,r}=0)$$

we have

$$N_1 \cdots N_n \sum_{i=1}^{n} \Gamma_i C_i = 0.$$

Key points of the proof of this lemma is firstly the identity

$$(2) \qquad \left| \sum_r A^{(i)}_{jr} \Delta_r \right|_{i,j} = 0$$

and secondly an identity of the form

$$(3) \qquad N_1 \cdots N_n C_i = A \delta_i \qquad (i=1, 2, \cdots, n).$$

From the last identity we have

$$N_1 \cdots N_n \sum_i \Gamma'_i C_i = A \sum_i \Gamma'_i \delta_i$$
$$= A \sum_{r,s} F_{r,s} \Delta_r C_s$$

so that our lemma is now reduced to

$$(4) \qquad A(\Delta_r C_s - \Delta_s C_r) = 0.$$

Concerning the detail of the proof of the identities (2) (3) and (4), we refer to my notes [3] and [4].

I have also obtained a generalization of this lemma, to the case of "Strahl" class field, which contains Iyanaga's theorem as a special case. I have obtained namely the following theorem:

THEOREM 2. *Let K be the "Strahl" class field* mod. $\mathfrak{f}(K/k)$ *over k, and Ω a cyclic intermediate field of K/k. Let also $\mathfrak{M} = \mathfrak{f}(K, \Omega, k)$ denote the ideal* Max $\{\mathfrak{f}(K/\Omega), \mathfrak{F}(\Omega/k)\}$ *in Ω. If $\mathfrak{a}$ is an ideal of Ω in ambigous class modulo $\mathfrak{M}$, then $\mathfrak{a}$ lies in the "Strahl" modulo $\mathfrak{F}(K/k)$, when considered as an ideal in K. Thereby $\mathfrak{F}(K/k)$ denotes the modulus of genus of K with respect to k.*

After these preliminaries we shall now proceed to the PROOF OF OUR MAIN THEOREM. For the sake of completeness we shall repeat our assertion once more: *Let K be the absolute class field over k, then if $\mathfrak{A}^{1-\sigma} = (A_\sigma)$, $\dfrac{A_\tau \cdot A_\sigma^\tau}{A_{\sigma\tau}} = \varepsilon_{\sigma,\tau} = \varepsilon_{\tau,\sigma}$ we can infer that $\mathfrak{A} \sim 1$ holds.*

To make the situation of our proof clearer we shall prove our theorem in a more general form.

THEOREM 3. *If K is the "Strahl" class field* mod $\mathfrak{f}$ *over k and*

$$\mathfrak{D}^{1-\sigma} = (A_\sigma), \qquad \frac{A_\tau \cdot A_\sigma^\tau}{A_{\sigma\tau}} = \varepsilon_{\sigma,\tau} = \varepsilon_{\tau,\sigma} \equiv 1 \pmod{\mathfrak{f}}$$

then $\mathfrak{D}$ is a principal ideal.

Let σ_i $(i=1, 2, \cdots, n)$ be the basis of the Galois group $G(K/k)$ and put $A_i = A_{\sigma_i}$, theh we have

$$(5) \qquad A_i^{N_i} = \varepsilon_i \equiv 1 \pmod{\mathfrak{f}}, \quad A_i^{\Delta_j} = A_j^{\Delta_i}.$$

From the norm theorem concerning everywhere splitting algebra, we have

$$(6) \qquad \varepsilon_i = \mathrm{N}_{L_i}(A_i')$$

where A_i' is an element of the field L_i belonging to the group

$$\{\sigma_1\} \times \cdots \times \{\sigma_{i-1}\} \times \{\sigma_{i+1}\} \times \cdots \times \{\sigma_n\}.$$

It then follows from the principal genus theorem

$$A_i' \equiv B^{1-\sigma_i} \qquad (\mathrm{mod}\ \mathfrak{f}/\mathfrak{D}(L_i))$$

so that if we write A_i' instead of $A_i'/B^{1-\sigma_i}$ we have

$$(7) \qquad \varepsilon_i = \mathrm{N}_{L_i}(A_i'), \qquad A_i' \equiv 1 \quad (\mathrm{mod}\ \mathfrak{f}/\mathfrak{D}(L_i)).$$

From $\varepsilon_i = \mathrm{N}_{L_i}(A_i') = A_i^{N_i}$ we have by classical norm theorem of Hilbert

$$(8) \qquad A_i = A_i' A_i''^{\Delta_i}, \qquad A_i'' \in K.$$

Now for the principal ideal (A_i') in L_i we have

$$(9) \qquad \mathrm{N}_{L_i}((A_i')) = (1)$$

so that it holds again by Hilbert's norm theorem concerning ideals

$$(10) \qquad (A_i') = \mathfrak{A}_i^{\Delta_i}, \qquad \mathfrak{A}_i \text{ ideal in } L_i$$

and

$$(11) \qquad \mathfrak{A}^{\Delta_i} = \mathfrak{A}_i^{\Delta_i}(A_i''^{\Delta_i}) = \mathfrak{A}^{\Delta_i}(A_i''^{\Delta_i})$$
$$(\mathfrak{A} = \prod_i \mathfrak{A}_i).$$

As we can prove easily $\mathfrak{f}/\mathfrak{D}(L_i) \geqq \mathfrak{f}(K, L_i, k)$, we have by the author's principal ideal theorem $\mathfrak{A}_i \in R_K(\mathfrak{F})$ (="Strahl" mod $\mathfrak{F}$ in K). (Thereby we should notice that every factor of $\mathfrak{A}_i$ can be so chosen that it is unramified in K, though it is not proved here in detail).

We have by further computations

$$\mathfrak{A}_i = (A_i'''), \qquad A_i''' \equiv 1 \pmod{\mathfrak{F}},$$
$$\mathfrak{A} = (A) = \prod (A_i'''), \qquad A = \prod A_i''' \equiv 1 \pmod{\mathfrak{F}},$$
$$(A_i') = \mathfrak{A}_i^{\Delta_i} = \mathfrak{A}^{\Delta_i} = (A)^{\Delta_i},$$
$$\mathfrak{D}^{\Delta_i} = (A)^{\Delta_i}(A_i'''^{\Delta_i}).$$

We can now start from $\mathfrak{D}/(A)$ instead of $\mathfrak{D}$, because $A_i''^{\Delta_i}$ satisfy the conditions

$$A_i''^{\Delta_i} \equiv 1 \pmod{\mathfrak{F}} \qquad (\text{by } A_i = A_i' A_i''^{\Delta_i})$$

and

$$(A_i''^{\Delta_i})^{\Delta_j}=(A_j''^{\Delta_j})^{\Delta_i},$$
$$(A_i''^{\Delta_i})^{N_i}=1.$$

$B_i=B_{\sigma_i}=A_i''^{\Delta_i}$ can then be extended to an one-dimensional Galois cocycle, so that it holds by Speiser-Noether's norm theorem

$$A_i''^{\Delta_i}=B^{\Delta_i},$$

and

$$\left(\frac{\mathfrak{D}}{A}\right)^{\Delta_i}=(B^{\Delta_i}),$$
$$\mathfrak{D}=(AB)\mathfrak{c} \qquad (\mathfrak{c}:\ k\text{-ideal}).$$

By Iyanaga's general principal ideal theorem $\mathfrak{c}$ belongs to the "Strahl" modulo $\mathfrak{F}$, so we have $\mathfrak{D}\sim 1$ as was desired.

Now we shall return once more to the case of absolute class field.

By the correspondence

$$\mathfrak{D}\ (\text{ambigous}) \rightarrow \varepsilon_{\sigma,\tau}$$

we obtain an isomorphism from the group of ambigous classes onto the subgroup $H'^2(G, E)$ of $H^2(G, E)$ (2-dimensional cohomology group of G with units group E as coefficients), which consists of cohomology classes of $H^2(G, E)$ containing cocycles with $\varepsilon_{\sigma,\tau}=\varepsilon_{\tau,\sigma}$. That this isomorphism is "onto" follows from norm theorem concerning everywhere splitting algebra. Thus from our MAIN THEOREM, we can deduce the following theorem, which would be in itself of some interest.

THEOREM 4. *If K is absolute class field over k, then we have*

$$H'^2(G, E)=1.$$

TÔHOKU UNIVERSITY

BIBLIOGRAPHY

[1] T. Tannaka, Über eine Indexrelation, Sci. Rep. Tôhoku Univ. (1), **23** (1934), pp. 343–358.

[2] F. Terada, On a generalization of the principal ideal theorem, Tôhoku Math. Journ. (2), **1** (1949), pp. 229–269.

[3] T. Tannaka, Some remarks concerning principal ideal theorem, Tôhoku Math. Journ. (2), **1** (1949), pp. 270–278.

[4] T. Tannaka, An alternative proof of a generalized principal ideal theorem, Proc. Japan Acad., **25** (1949), pp. 26–31.

A Conjecture on the Cohomology of Algebraic Number Fields and the Proof of its Special Case

Tadasi NAKAYAMA

Let k be an algebraic number field and K be its Galois extension with Galois group G. There exists then a certain canonical (or fundamental) 2-cohomology class α of G in the idèle-class group C_K of K (Weil [10], Nakayama [7], Hochschild-Nakayama [3]), which generates the 2-cohomology group $H^2(G, C_K)$ of G in C_K and whose properties practically cover the class field theory. By means of this canonical 2-cohomology class α Tate's fundamental theorem reduces the problem of determining cohomology groups of G in C_K, in various dimensions, to a purely algebraic problem (Tate [8], Artin-Tate [1], Chevalley [2]); for every $n \gtreqless 0$ the cup multiplication of α gives an isomorphism of $H^{n-2}(G, Z)$ and $H^n(G, C_K)$, where Z is the module of rational integers (operated by G trivially) and where the cup product is with respect to the natural pairing of Z and C_K. Similar phenomena prevail for the idèle group J_K and the group K^* of non-zero elements of K too, instead of the idèle-class group C_K, with Z replaced by some other modules (which are however not purely algebraic) (Tate [9]).

Now, in the present paper, we wish to study the Galois cohomology of algebraic number fields in an a little more general setting. Thus, in view of the fact that (matrix) representations of the Galois group are quite important for the structure of the Galois extension of an algebraic number field, we consider the (representation-) module M of a representation of the Galois group G in the ring Z of rational integers, and construct the tensor product $M \otimes C_K$ of M and C_K, over Z, which may be regarded as a G-module in natural way. So we consider the cohomology of G is $M \otimes C_K$. If we turn to the contravariant representation, our problem is equivalent to to consider the cohomology groups of G in the G-module $\mathrm{Hom}(M, C_K)$ of Z-homomorphisms of a representation-module M of G over Z into C_K. Now, in view of various indications, the author is led to dare to *conjecture*[1] the following: *The cup multiplication of the canonical 2-cohomology*

[1] Cf. the end of the paper.

class α, in the sense of the natural pairing of M and C_K to $M\otimes C_K$, gives an isomorphism

$$(1) \qquad H^n(G, M\otimes C_K) \cong H^{n-2}(G, M)$$

However, the author has been able to *confirm* this only in the special case when M belongs to an "*essentially abelian*" (integral) representation of G. The last is defined as follows: If $G=1$, any representation of G in Z is called essentially abelian. Assume $G\neq 1$ and assume that the notion of essentially abelian representation is defined for its proper subgroups. Then a representation $M(\sigma)$ $(\sigma \in G)$ of G in Z is called essentially abelian, when and only when it is equivalent, in Z, to a direct component of a representation of form

$$\begin{pmatrix} M_1(\sigma) & & 0 \\ & \ddots & \\ * & & M_s(\sigma) \end{pmatrix}$$

where each $M_i(\sigma)$ is either an abelian representation of G or a direct component of a representation of G induced, in the sense of Frobenius, by an essentially abelian representation of a proper subgroup of G. Except perhaps a methodological, the author does not claim any particular importance on this special type of integral representations.

In spite of this restriction on the type of representation, our result gives a quite natural generalization of the result of Artin-Tate. However, since again the canonical 2-class α is the only essentially arithmetic factor in it, else being rather algebraic, it is doubtful that it will give much new for the arithmetic of Galois extensions of algebraic number fields. Nevertheless, it seems true that, besides its own interest, it gives something in the way of applications too; for instance, it gives us some information about the behaviour of systems (vectors, e.g.) of idèle-classes under the operation of Galois group.

In terms of the groups of Tate [9] we (make similar conjectures and) obtain similar results for the cohomology in $M\otimes J_K$ and $M\otimes K^*$.

One difficulty in our problem seems to lie in that little is known about group representations in Z. Thus the author is led to try to make transition to representations in (rational) l-adic integers Z_l, l running over rational primes, in taking advantage of the fact that the connected component of 1 of the idèle-class group C_K has comparatively simpler cohomological properties as is shown in Weil [10]. Now, in order to give a sketch of this process, it is perhaps convenient, and of some interest, to start with the case of (generalized) Galois cohomology of finite fields. Thus let k be, meantime, a *finite* *field* and K be its Galois (cyclic) extension with Galois group G. Here we consider the group K^* of non-zero elements of K, and we contend that

$$H^n(G, M \otimes K^*) = 0 \qquad (n \gtreqless 0) \tag{2}$$

for any representation module M of G over Z, which is naturally a far-going generalization of a theorem of Wedderburn. To prove this, we first replace K^*, as we are allowed, by a finite G-module A satisfying

$$H^n(G, A) = 0 \qquad (n \gtreqless 0). \tag{3}$$

Further, by means of the fundamental exact sequences (for dimensions 0, 1, say) for the cohomology of subgroups and factor groups, Sylow group argument in cohomology, Shapiro's theorem, and a lemma (Osima-Mackey) on the tensor product of induced modules, among others, we may reduce the problem to the case where G is a cyclic group of prime order l, A is of order a power of l, and M belongs to a faithful irreducible representation of G in Z. Now, if we pass from Z to Z_l, there is only one such representation, given by the cyclotomic polynomial of l-th roots of 1;

$$\text{a generator } \sigma \rightarrow \begin{pmatrix} 0 & & -1 \\ 1 & & -1 \\ & \cdots\cdots & \\ 0 & 1 & -1 \end{pmatrix}. \tag{4}$$

The transition from Z to Z_l is indeed allowed because of the l-group property of A; more precisely $M \otimes A = M_l \otimes_l A$, where M_l is obtained from M by coefficient extension from Z to Z_l and $\otimes_l$ means tensor product over Z_l. Now, the representation module M over Z of (4) is the dimension shifter of Chevalley [2] and Tate [8]. So, $H^n(G, M \otimes A) = H^{n+1}(G, A)$ whence $=0$. (This simplified argument, which has replaced the writer's original somewhat complicated computation, is due to a remark by J.-P. Serre).

In this proof we may replace our finite G-module A with a totally disconnected compact G-module A, satisfying (3), since Z_l may be considered as an operator ring of the "l-component" of such a module. Our way of reduction allows us also to replace the cyclic G by any finite group provided that its representation belonging to M is "essentially abelian" as defined above. These observations we want to apply on returning to the case of algebraic number field k, to some factor-module of the Artin splitting module A of the canonical 2-class α for K/k. It is shown by Tate [8] that A satisfies (3). However, since it is not totally disconnected, nor compact, we consider instead the splitting module A^* of the natural image α^* of α in the factor-group C_K/D_K of C_K with respect to its connected component D_K of 1. Suppose first that the degree $[K:k](=[G])$ is *odd*. Then the cohomology of D_K is trivial; indeed, if D'_K denotes the natural image in C_K of the compact part of the connected component of 1 in J_K, then D_K/D'_K is of unique division while D'_K is a regular (G-)module (Weil [10]). It follows that also A^* satisfies (3). Let $\tilde{A}$ be the completion (compactification) of A^*. As $\tilde{A}/A^*$ is seen to be of unique division, $\tilde{A}$ too satisfies (3). To $\tilde{A}$ we can apply the above consideration, to find $H^n(G, M\otimes\tilde{A})=0$ $(n\gtreqless 0)$ provided that M belongs to an essentially abelian representation. Because of the cited properties of $\tilde{A}/A^*$, D_K/D'_K, D'_K, this entails further

$$(5) \qquad H^n(G, M\otimes A)=0 \qquad (n\gtreqless 0).$$

Now that this is secured, we can show by an argument quite similar to that of Tate [8] that (1) is the case (under the same assumption on M) and the isomorphism may indeed be obtained by the cup multiplication of α.

Let us next turn to the general case where $[K:k]=[G]$ is, perhaps, *even*. Then D'_K is no more cohomologically trivial, but is a direct sum of tori which are in correspondence to complex valuations of K (Weil [10]). Here the tori corresponding to complex valuations of K which are prolongation of a real valuation of k are to be studied, and naturally only the 2-components of cohomology groups are to be investigated. Although now $H^n(G, M\otimes\tilde{A})=0$ does not hold, in general, we are able to prove, by virtue of the above concrete structure of D'_K and by means of some rather troublesome arguments on induced modules, cup multiplication and cohomology sequences, that (5) remains valid, which entails again the isomorphism (1) by the cup multiplication of α, all under the same assumption on M. The author regrets that this proof to the case of even $[K:k]$ must be left here, since it is rather lengthy. He regrets also to have to leave the case of $M\otimes J_K$, $M\otimes K^*$, but wants to note that it depends, naturally, on the result of Tate [9] strongly and its proof includes much of the reproduction of his argument, as the author presumes from the brief indication in [9], in a somewhat generalized setting.

The above proof to a special case of our conjecture makes much use of the fact that the connected component D_K of 1 in C_K can be "handled". The argument may be applied to other sort of "class formation", in the sense of Artin, if the situation is similar. Need-less to say that it can be applied to the case when the belonging G-module is a totally disconnected compact group; thus, for instance, to the case of Kummer extension as has been studied in Kawada [5], to the case of class field theory of function fields (of one variable) over a finite field, and, with the help of completion argument, to local class field theory, the case which ought to have been mentioned earlier. Unfortunately it seems to fail to be applied to the case of unramified extensions of classical function fields as in Kawada-Tate [6]; however it is hoped to be able to approach this case since we have here the concrete structure of "connected part".

In spite of the powerlessness of his above method, the author is tempted to dare to conjecture that the theorem is true for any class formation, even without any restriction on M either. This would be confirmed if (5) be true (with any M) for any G-module A satisfying (3). In particular, he is tempted to conjecture that (2) is true for any field K which splits no non-commutative (not necessarily central) division algebra over the invariant field of G (cf. Hochschild-Nakayama [3], Hochschild-Serre [4]). However, instead of going too far in conjecturing, the author has to, as he wishes to, try to reduce his ignorance and powerlessness in representation theory, cohomology and arithmetic, to find his way.

Addendum. By virtue of a remark of J. Tate it has become possible to prove (5) for any G-module A satisfying (3) and for a module M of essentially abelian representation, to remove the connected component consideration in our proof, and thus to extend the result to general class formations (including the case of unramified extensions of classical function fields in Kawada-Tate [6]) (under the same restriction on M however).

Added in proof: The author has recently been able to confirm the conjecture, in its strongest form and indeed for any $[G]$-torsion free G-module M.

THE INSTITUTE FOR ADVANCED STUDY AND
NAGOYA UNIVERSITY

REFERENCES

[1] E. Artin-J. Tate, Algebraic Numbers anc Algebraic Functions, to come.

[2] C. Chevalley, Class Field Theory, Lecture notes, Nagoya Univ. 1953-54.

[3] G. Hochschild-T. Nakayama, Cohomology in class field theory, Ann. Math., **55** (1952), 348-366.

[4] G. Hochschild-J.-P. Serre, Cohomology of group extensions, Trans. Amer. Math. Soc., **74** (1953), 110-134.

[5] Y. Kawada, On class formations, Duke Math. J., **22** (1955), 165–178.

[6] Y. Kawada-J. Tate, On the Galois cohomology of unramified extensions of function fields in one variable, Amer. J. Math., **77** (1954), 197–217.

[7] T. Nakayama, Idèle-class factor sets and class field theory, Ann. Math., **55** (1952), 73–84.

[8] J. Tate, Higher dimensional cohomology groups of class field theory, Ann. Math., **56** (1952), 294–297.

[9] J. Tate, The cohomology groups of algebraic number fields, Proc. Intern. Congress Math. Amsterdam 1954.

[10] A. Weil, Sur la théorie du corps de classes, J. Math. Soc. Japan, **3** Takagi commemoration number (1951), 1–35.

Density in a Family of Abelian Extensions

Tomio KUBOTA

Let Ω be a finitely algebraic number field and $\mathfrak{A}$ be a finite abelian group of order n. Let $\mathfrak{F}$ be a family of abelian extensions over Ω whose Galois groups are all isomorphic to $\mathfrak{A}$. Denote by f_K the conductor of $K \in \mathfrak{F}$ over Ω, and, for an ideal $\mathfrak{a}$ of Ω, denote by $\mathrm{N}\mathfrak{a}$ the absolute norm from Ω of $\mathfrak{a}$. Then the density in $\mathfrak{F}$ of a subfamily $\mathfrak{F}_0$ of $\mathfrak{F}$ is defined by

$$\omega(\mathfrak{F}_0\,;\ \mathfrak{F}) = \lim_{s\to 1,\ s>1} \frac{\displaystyle\sum_{K\in\mathfrak{F}_0} \frac{1}{\mathrm{N}f_K^s}}{\displaystyle\sum_{K\in\mathfrak{F}} \frac{1}{\mathrm{N}f_K^s}}. \tag{1}$$

In §3, §4 and §6, this density will be studied in connection with the arithmetical properties of field extensions.

Denote now by $\mathfrak{K}$ the family of all abelian extensions K over Ω such that the Galois group of K/Ω is isomorphic to $\mathfrak{A}$. Then we see that the series $\sum_{K\in\mathfrak{K}} \frac{1}{\mathrm{N}f_K^s}$ converges and therefore defines an analytic function $\Lambda(s)$ for $s>1$. A property of $\Lambda(s)$ will be derived in §5.

NOTATIONS. Together with defined above, the following notations will hold the same meanings henceforward.

n_0: exponent of $\mathfrak{A}$, i.e., the L.C.M. of the orders of elements of $\mathfrak{A}$.

I: the idèle group of Ω.

G_Ω: the Galois group of the full abelian extension over Ω.

κ: (continuous) homomorphism of G_Ω into (discrete) $\mathfrak{A}$. Under the reciprocity law of class field theory, we can also consider κ to be a mapping of I into $\mathfrak{A}$.

f_κ: conductor of the idèle group determined as the kernel of κ.

$\mathfrak{p}$: prime ideal of Ω.

U: the group of elements of I whose components are all units.

Ω_m: field obtained by adjunction to Ω of a primitive m-th root of unity.

For every number field L, $L^\times$ will stand for the multiplicative group of non zero elements of L or the group of principal idèles of L, and $L^{\times m}$ will stand for the group of all m-th powers of elements of $L^{\times}$.

If a is an integer and p is a prime number, then we shall mean by $p^c \| a$ that we have simultaneously $p^c | a$ and $p^{c+1} \nmid a$. This notation will similarly be applied to ideals, while, in the following, we shall exclusively make use of integral ideals.

§1. Preliminaries.

LEMMA 1. (*Hasse*) *Let $l^\nu (l^\nu > 2)$ be a power of a prime number l and let P_{l^ν} be the field obtained by adjunction, to the rational number field, of a primitive l^ν-th root of unity. Then an element α of $\Omega^{\times}$ with $\alpha \in \Omega_{l^\nu}^{\times l^\nu}$ is in general, already in $\Omega^{\times l^\nu}$. Only in the case where $l=2$ and $\Omega \frown P_{2^\nu}$ is the largest real subfield of $P_{2^\mu} (\mu \leqq \nu)$, the group of all $\alpha \in \Omega^{\times}$ with $\alpha \in \Omega_{2^\nu}^{\times 2^\nu}$ is generated by $\Omega^{\times 2^\nu}$ and an element $\lambda^*_{\mu,\nu}$ of Ω such that*

$$\lambda^*_{\mu,\nu} = \begin{cases} \lambda_{2^\mu}^{2^{\nu-1}} & \textit{for} \quad \lambda < \nu, \\ -\lambda_{2^\nu}^{2^{\nu-1}} & \phantom{\textit{for}} \quad \mu = \nu, \end{cases} \qquad \lambda_{2^\mu} = -(\zeta_{2^\mu} + \zeta_{2^\mu}^{-1}) + 2,$$

where ζ_{2^μ} is determined by $\zeta_{2^0} = 1$ and by $\zeta_{2^{\mu+1}}^2 = \zeta_{2^\mu}$.

PROOF. See Hasse [4], §1.

For every abelian group A, we shall denote by A^m the group of all m-th powers of elements of A. The assertions of following three lemmas are elementary properties of finitie abelian groups.

LEMMA 2. *Let A and C be finite abelian groups, B a subgroup of A and e_0 the exponent of C. Then, in order that a homomorphism φ' of B into C can be extended to a homomorphism φ of A into C, it is necessary and sufficient that we have $\varphi'(A^d \frown B) \subset C^d$ for every $d | c_0$.*

PROOF. Let $a_1, \cdots, a_r$ be a basis of A modulo B and let m_i be the order of a_i modulo B. Assume that the condition is satisfied. Then, we can choose $\sigma_i \in C$ such that $\varphi'(a_i^{m_i}) = \sigma_i^{m_i}$. Set $\varphi(a) = \sigma_1^{x_1} \cdots \sigma_r^{x_r} \varphi'(b)$ for $a = a_1^{x_1} \cdots a_r^{x_r} b \in A$ $(b \in B,\ 0 \leqq x_i < m_i)$. Then φ is well-defined on A and extends φ'. The necessity is obvious.

LEMMA 3. *Let A and C be finite abelian groups, C' be a subgroup of C and c_0, c_0' be exponents of C, C' respectively. For every power $l^r \geqq 1$ of a prime number $l | c_0'$, denote by $\rho(l, r)$ the highest power of l both with $\rho(l, r) | c_0$ and with $C'^{l^r} \subset C^{\rho(l,r)}$. Furthermore, let b be an element of A. Then, in order that the set of images of b by all homomorphisms of A into C contains C', it is necessary and sufficient that we have $b^{l^r} \notin A^{l\rho(l,r)}$ for every l^r with $l\rho(l, r) | c_0$.*

PROOF. Let N, N' be such that $l^N \| c_0$, $l^{N'} \| c_0'$ respectively. Suppose that the condition is satisfied. Then we have $b^{l^r} \notin A^{l^N}$ for every l^r with $r<N'$, which shows that the order of b modulo A^{c_0} is divisible by c_0', whence the order of b itself is divisible by c_0'. Therefore it gives a homomorphism φ' into C of the cyclic group generated by b such that $\varphi'(b)$ is an arbitrary element of C'. Now, consider a power b^m of b. Then, for every $d|c_0$, we see that $\varphi'(b^m)$ belongs to C^d whenever b^m belongs to A^d. In fact, if $l^r \| m$ and $r<N'$, then c_0 is divisible by $l\rho(l, r)$ and therefore we have $b^m \notin A^{l\rho(l,r)}$, while we have $\varphi'(b^m) \in C^{\rho(l,r)}$. If $l^{N'}|m$, then we have obviously $\varphi'(b^m) \in C^{l^N}$. On the other hand, for every prime factor l_0 of c_0 which does not divide c_0', $\varphi(b^m)$ belongs to $C^{l_0^{N_0}}$, where $l_0^{N_0} \| c_0$. Thus, by lemma 2, φ' can be extended to a homomorphism φ of A into C. Conversely, suppose that the condition is not satisfied. Then it gives an l^r such that $l\rho(l, r)|c_0$, $b^{l^r} \in A^{l\rho(l,r)}$. Moreover, we can choose an element c' of C' with $c'^{l^r} \in C^{\rho(l,r)}$, $\notin C^{l\rho(l,r)}$. Therefore it follows from lemma 2 that there is no homomorphism φ of A into C with $\varphi(b)=c'$, which completes the proof.

LEMMA 4. *Let A, C be finite abelian groups and c_0 be the exponent of C. For every prime number $l|c_0$, denote by C_l the group of all elements c of C with $c^l=1$, and, for every $d|c_0$, let there be given a subgroup $A^{(d)}$ of A with following properties: a) $A^{(d)} \supset A^d$. b) if $d'|d$, then $A^{(d')} \supset A^{(d)}$. c) if $(d, d')=1$, then $A^{(d)} \frown A^{(d')} = A^{(dd')}$. d) for every power $l^i|c_0$, $A^{(l^{i-1})}/A^{(l^i)}$ is of the type $(l, l, \cdots)$. Then, N being such that $l^N \| c_0$, the number g of all homomorphisms φ of A into C is $\prod_{l|c_0} \prod_{i=1}^{N} (A^{(l^i)} : A^{l^i})^{u_{i-1}-u_i}$ times the number g_1 of all φ satisfying $\varphi(A^{(d)}) \subset C^d$ for every $d|c_0$, where u_i is the rank of $C^{l^i} \frown C_l (0 \leqq i \leqq N)$.*

PROOF. Under condition c), it is sufficient to prove the case where $c_0=l^N$ is a power of a prime number. Now, we have

$$g=\prod_{i=0}^{N-1}(A^{l^i} : A^{l^{i+1}})^{ui}, \quad g_1=\prod_{i=0}^{N-1}(A^{(l^i)} : A^{(l^{i+1})})^{ui}.$$

Therefore we have

$$\frac{g}{g_1}=\prod_{i=0}^{N-1}\frac{(A^{l^i} : A^{l^{i+1}})^{u_i}}{(A^{(l^i)} : A^{(l^{i+1})})^{u_i}}=\prod_{i=0}^{N-1}\frac{(A : A^{l^{i+1}})^{u_i}(A : A^{(l^i)})^{u_i}}{(A : A^{l^i})^{u_i}(A : A^{(l^{i+1})})^{u_i}}$$

$$=\prod_{i=0}^{N-1}\frac{(A^{(l^{i+1})} : A^{l^{i+1}})^{u_i}}{(A^{(l^i)} : A^{l^i})^{u_i}}=\prod_{i=1}^{N}\frac{(A^{(l^i)} : A^{l^i})^{u_{i-1}}}{(A^{(l^i)} : A^{l^i})^{u_i}},$$

which is to be proved.

Let $\mathfrak{a}$ be an ideal of Ω and m be a natural number. Then we denote by $U_{\mathfrak{a}}$ the group of all $\boldsymbol{u} \in \boldsymbol{U}$ such that the $\mathfrak{p}$-component $u_{\mathfrak{p}}=1$

(mod $\mathfrak{p}^c$) for every $\mathfrak{p}^c \| \mathfrak{a}$ (no condition for every $\mathfrak{p} \nmid \mathfrak{a}$). Furthermore we set $\Omega^{(m)} = \boldsymbol{U}\boldsymbol{I}^m \frown \Omega^\times$, $\Omega_{\mathfrak{a}}^{(m)} = \boldsymbol{U}_{\mathfrak{a}}\boldsymbol{I}^m \frown \Omega^\times$ and $\iota_{\mathfrak{a}}(\Omega^\times \boldsymbol{I}^m \frown \boldsymbol{U}) = V_{\mathfrak{a}}^{(m)}$, where $\iota_{\mathfrak{a}}$ is a natural homomorphism of $\boldsymbol{U}$ into $V_{\mathfrak{a}} = V_{\mathfrak{a}}^{(1)} = \boldsymbol{U}/\boldsymbol{U}_{\mathfrak{a}}$.

Lemma 5. $V_{\mathfrak{a}}^{(m)}/V_{\mathfrak{a}}^m \cong \Omega^{(m)}/\Omega_{\mathfrak{a}}^{(m)}$.

Proof. The isomorphism is given by $\Omega^{(m)} \ni \alpha \leftrightarrow \iota_{\mathfrak{a}}(\boldsymbol{u})$, where $\alpha = \boldsymbol{u}\boldsymbol{a}^m$ with $\boldsymbol{u} \in \boldsymbol{U}$, $\boldsymbol{a} \in \boldsymbol{I}$. For, this correspondence is obviously "onto" and multiplicative. And from $1 = \boldsymbol{u}\boldsymbol{a}^m$ follows $\boldsymbol{u} \in \boldsymbol{U}^m$ and therefore $\iota_{\mathfrak{a}}(\boldsymbol{u}) \in V_{\mathfrak{a}}^m$. Conversely, from $\iota_{\mathfrak{a}}(\boldsymbol{u}) = 1$ follows $\boldsymbol{u} \in \boldsymbol{U}_{\mathfrak{a}}$ and therefore $\alpha \in \boldsymbol{U}_{\mathfrak{a}}\boldsymbol{I}^m \frown \Omega^\times = \Omega_{\mathfrak{a}}^{(m)}$, which proves the lemma.

Lemma 6. *If m, m' are integers, then we have $V_{\mathfrak{a}}^{(m)m'} \subset V_{\mathfrak{a}}^{(mm')}$. If further $(m, m') = 1$ then we have $V_{\mathfrak{a}}^{(m)} \frown V_{\mathfrak{a}}^{(m')} = V_{\mathfrak{a}}^{(mm')}$.*

Proof. The first assertion follows at once from the definition. To prove the second, it is sufficient to show that $V_{\mathfrak{a}}^{(m)} \frown V_{\mathfrak{a}}^{(m')} \subset V_{\mathfrak{a}}^{(mm')}$. Let $v = \iota_{\mathfrak{a}}(\alpha\boldsymbol{a}^m) = \iota_{\mathfrak{a}}(\alpha'\boldsymbol{a}'^{m'})$ be an arbitrary element of $V_{\mathfrak{a}}^{(m)} \frown V_{\mathfrak{a}}^{(m')}$. Choose integers x, y such that $mx + m'y = 1$. Then $(\alpha\boldsymbol{a}^m)^{m'y}(\alpha'\boldsymbol{a}'^{m'})^{mx} = \alpha^{m'y}\alpha'^{m'x}(\boldsymbol{a}^y\boldsymbol{a}'^x)^{mm'}$ is also an element of $\boldsymbol{U}$ and we have $v = \iota_{\mathfrak{a}}(\alpha\boldsymbol{a}^m)^{m'y}\iota_{\mathfrak{a}}(\alpha'\boldsymbol{a}'^{m'})^{mx} = \iota_{\mathfrak{a}}(\alpha^{m'y}\alpha'^{mx}(\boldsymbol{a}^y\boldsymbol{a}'^x)^{mm'}) \in V_{\mathfrak{a}}^{(mm')}$.

Let $c_{\mathfrak{a}}$ be the number of all homomorphisms of $V_{\mathfrak{a}}$ into $\mathfrak{A}$ and let $n_{\mathfrak{a}}$ be the number of all homomorphisms of $\boldsymbol{I}/\Omega^\times\boldsymbol{U}_{\mathfrak{a}}$ into $\mathfrak{A}$. $n_{\mathfrak{a}}$ is then the number of all κ with $f_\kappa | \mathfrak{a}$.

Lemma 7 *There are positive constants γ_1, γ_2 depending only on Ω and on $\mathfrak{A}$ such that $\gamma_1 c_{\mathfrak{a}} < n_{\mathfrak{a}} < \gamma_2 c_{\mathfrak{a}}$.*

Proof. It follows from lemma 2 that a homomorphism κ' of $\boldsymbol{U}/\boldsymbol{U}_{\mathfrak{a}}$ into $\mathfrak{A}$ is extended to a homomorphism κ of $\boldsymbol{L}/\Omega^\times\boldsymbol{U}_{\mathfrak{a}}$ into $\mathfrak{A}$ if and only if $\kappa'(V_{\mathfrak{a}}^{(d)})$ is contained in $\mathfrak{A}^d$ for every $d | n_0$. But, by lemma 5, $V_{\mathfrak{a}}^{(d)}/V_{\mathfrak{a}}^d$ is a factor group of $\Omega^{(d)}/\Omega^{\times d}$. Since the latter group is independent of $\mathfrak{a}$, our lemma is proved.

Now we consider the series $\sum_{\mathfrak{a}} \frac{c_{\mathfrak{a}}}{\mathrm{N}\mathfrak{a}^s}$, where the sum is extended over all ideals $\mathfrak{a}$ of Ω. Since $(\mathfrak{a}, \mathfrak{b}) = 1$ implies $c_{\mathfrak{a}\mathfrak{b}} = c_{\mathfrak{a}}c_{\mathfrak{b}}$ and since $c_{\mathfrak{p}^m}$ is bounded for all powers of prime ideals, we see that $\prod_{\mathfrak{p}}\left(\sum_{m=0}^{\infty} \frac{c_{\mathfrak{p}^m}}{\mathrm{N}\mathfrak{p}^{ms}}\right)$ converges (absolutely) for every $s > 1$ and therefore is equal to $\sum_{\mathfrak{a}} \frac{c_{\mathfrak{a}}}{\mathrm{N}\mathfrak{a}^s}$. It follows from this fact that every infinite series or product observed in the following converges absolutely for $s > 1$.

Let $f_1(s)$, $f_2(s)$ be functions defined for $s > 1$. Then we mean by $f_1(s) \sim f_2(s)$ that $\gamma = \lim_{s \to 1,\, s > 1} \frac{f_1(s)}{f_2(s)}$ exists and is different from 0. If especially $\gamma = 1$, then we write $f_1(s) \approx f_2(s)$. Moreover, we mean $\lim_{s \to 1, s > 1} \frac{f_1(s)}{f_2(s)} = 0$ by $f_1(s) \prec f_2(s)$. For example, if M is a set of prime ideals of Ω, then we have

$$(2) \qquad \prod_{\mathfrak{p}\in M}\Big(\sum_{m=0}^{\infty}\frac{c_{\mathfrak{p}^m}}{\mathrm{N}\mathfrak{p}^{ms}}\Big)\sim\prod_{\mathfrak{p}\in M}\Big(1+\frac{c_{\mathfrak{p}}}{\mathrm{N}\mathfrak{p}^{s}}\Big).$$

If further $m_{\mathfrak{p}}$'s are integers defined and bounded for all $\mathfrak{p}\in M$, then we have

$$(3) \qquad \prod_{\mathfrak{p}\in M}\Big(1+\frac{m_{\mathfrak{p}}}{\mathrm{N}\mathfrak{p}^{s}}\Big)\sim\prod_{\mathfrak{p}\in M}\Big(1+\frac{1}{\mathrm{N}\mathfrak{p}^{s}}\Big)^{m_{\mathfrak{p}}}.$$

§2. Fundamental lemmas.

Two fundamental lemmas will be deduced in this paragraph from the results of §1 and from Tschebotareff's density theorem.

LEMMA 8. *Let* $\mathfrak{m}$ *be an ideal of* Ω *and let* $\boldsymbol{b}$ *be an idèle of* Ω *with* $\mathfrak{p}$*-component* 1 *for every* $\mathfrak{p}\nmid\mathfrak{m}$. *Let* $\mathfrak{h}$ *be an ideal of* Ω *divisible only by powers of prime factors in* Ω *of* 2 *and such that* $(\mathfrak{h},\mathfrak{m})=1$, *and let* $\mathfrak{A}'$ *be the subgroup of* $\mathfrak{A}$ *formed by all* $\kappa(\boldsymbol{b})\in\mathfrak{A}$ *such that* $(f_\kappa,\mathfrak{m})=1$ *and that, for every prime factor* $\mathfrak{l}$ *in* Ω *of* 2, f_κ *is not divisible by any higher power of* $\mathfrak{l}$ *than* $\mathfrak{h}$. *Furthermore,* $\mathfrak{a}$ *being an ideal of* Ω *with* $(\mathfrak{a}, 2\mathfrak{m})=1$, *let* $\mathfrak{M}$ *be the set of all* $\mathfrak{a}$ *such that the set of all* $\kappa(\boldsymbol{b})$ *with* $f_\kappa\,|\,\mathfrak{h}\mathfrak{a}$ *does not coincide with* $\mathfrak{A}'$. *Then we have*

$$\sum_{\mathfrak{a}\in\mathfrak{M}}\frac{c_{\mathfrak{a}}}{\mathrm{N}\mathfrak{a}^{s}}\prec\sum_{\mathfrak{a}}\frac{c_{\mathfrak{a}}}{\mathrm{N}\mathfrak{a}^{s}}\,.$$

PROOF. Let n_0' be the exponent of $\mathfrak{A}'$. Then lemma 3 shows that we have $\mathfrak{a}\in\mathfrak{M}$ if and only if we have

$$(4) \qquad \boldsymbol{b}^{l^r}\in\Omega^{\times}U_{\mathfrak{h}\mathfrak{a}}\boldsymbol{I}^{l\rho(l,r)}$$

for some l^r with $l\rho(l,r)\,|\,n_0$, where $\rho(l,r)$ is defined for $\mathfrak{A}$, $\mathfrak{A}'$ instead of C, C' in lemma 3. Now, (4) is equivalent with

$$(5) \qquad \boldsymbol{b}^{l^r}U_{\mathfrak{h}\mathfrak{a}}\boldsymbol{I}^{l\rho(l,r)}\frown\Omega^{\times}\neq\phi \quad (\phi\text{: the empty set}).$$

If $\boldsymbol{b}^{l^r}U_{\mathfrak{h}}\boldsymbol{I}^{l\rho(l,r)}\frown\Omega^{\times}$ is empty, then there is no $\mathfrak{a}$ with (5). If not, then $\boldsymbol{b}^{l^r}U_{\mathfrak{h}}\boldsymbol{I}^{l\rho(l,r)}\frown\Omega^{\times}$ is a coset of $\Omega^{\times}$ modulo $\Omega_{\mathfrak{h}}^{(l\rho(l,r))}$ and therefore we can choose a system $\{\beta\}_{l,r}$ of representatives of $\boldsymbol{b}^{l^r}U_{\mathfrak{h}}\boldsymbol{I}^{l\rho(l,r)}\frown\Omega^{\times}$, modulo $\Omega^{\times l\rho(l,r)}$, and (5) is equivalent with that

$$(6) \qquad \beta\in\boldsymbol{b}^{l^r}U_{\mathfrak{h}\mathfrak{a}}\boldsymbol{I}^{l\rho(l,r)}$$

is satisfied for some $\beta\in\{\beta\}_{l,r}$. Since β is in $\boldsymbol{b}^{l^r}U_{\mathfrak{h}}\boldsymbol{I}^{l\rho(l,r)}$ and since we have $(\mathfrak{m},\mathfrak{h}\mathfrak{a})=1$, (6) is again equivalent with that

$$(7) \qquad \beta\in U_{\mathfrak{a}}\boldsymbol{I}^{l\rho(l,r)}$$

is satisfied for some $\beta\in\{\beta\}_{l,r}$. Now, it follows from the assumption in the theorem that there is at least one $\mathfrak{a}$ such that the set of all $\kappa(\boldsymbol{b})$ with $f_\kappa \mid \mathfrak{h}\mathfrak{a}$ coincides with $\mathfrak{A}'$. Since (7) is not satisfied for such $\mathfrak{a}$, every β is not an $l\rho(l, r)$-th power in Ω. Therefore, by lemma 1, β is, in general, not an $l\rho(l, r)$-th power in $\Omega_{l\rho(l,r)}$. Only in some special cases of $l\rho(l, r)=2^\nu>2$, β may be one of $\lambda^*_{\mu,\nu}$. Since, however $\lambda^*_{\mu,\nu}(\mu<\nu)$ is a 2^ν-th power residue of every ideal $\mathfrak{a}$ with $(\mathfrak{a}, 2)=1$, β cannot be any $\lambda^*_{\mu,\nu}$ with $\mu<\nu$. Thus in every case we can conclude that, if (7) holds, then $\mathfrak{a}$ cannot be divisible by any prime ideal $\mathfrak{p}$ with following properties: a) $\mathfrak{p}$ is prime to n. b) in the case where $l\rho(l, r)=2^\nu$ and $\beta=\lambda^*_{\nu,\nu}\beta'^{2^\nu}$ with $\beta' \in \Omega^\times$ $\mathfrak{p}$ is not decomposed in $\Omega(\sqrt{\beta})$, while, in any other case, $\mathfrak{p}$ is completely decomposed in $\Omega_{l\rho(l,r)}$ but is not completely decomposed in $\Omega_{l\rho(l,r)}(\sqrt[l\rho(l,r)]{\beta})$. Let $F_{l,r,\beta}$ be the set of all $\mathfrak{p}$ with a) and b), and let $\mathfrak{M}_{l,r,\beta}$ be the set of all $\mathfrak{a}$ such that $\mathfrak{p} \nmid \mathfrak{a}$ for every $\mathfrak{p} \in F_{l,r,\beta}$. Then, by (2), we have following relations:

$$\sum_{\mathfrak{a}\in\mathfrak{M}} \frac{c_\mathfrak{a}}{\mathrm{N}\mathfrak{a}^s} \leqq \sum_{l,r,\beta} \sum_{\mathfrak{a}\in\mathfrak{M}_{l,r,\beta}} \frac{c_\mathfrak{a}}{\mathrm{N}\mathfrak{a}^s},$$

$$\sum_{\mathfrak{a}\in\mathfrak{M}_{l,r,\beta}} \frac{c_\mathfrak{a}}{\mathrm{N}\mathfrak{a}^s} \sim \prod_{\mathfrak{p}\notin F'_{l,r,\beta}} \left(1+\frac{c_\mathfrak{p}}{\mathrm{N}\mathfrak{p}^s}\right),$$

$$\sum_{\mathfrak{a}} \frac{c_\mathfrak{a}}{\mathrm{N}\mathfrak{a}^s} \sim \prod_{\mathfrak{p}} \left(1+\frac{c_\mathfrak{p}}{\mathrm{N}\mathfrak{p}^s}\right).$$

On the other hand, Tschebotareff's theorem implies that we have

$$\prod_{\mathfrak{p}\notin F'_{l,r,\beta}} \left(1+\frac{c_\mathfrak{p}}{\mathrm{N}\mathfrak{p}^s}\right) < \prod_{\mathfrak{p}} \left(1+\frac{c_\mathfrak{p}}{\mathrm{N}\mathfrak{p}^s}\right),$$

which completes the proof.

LEMMA 9. *Let* $\mathfrak{m}$, $\mathfrak{n}$ *be ideals of* Ω *such that* $(\mathfrak{n}, 2\mathfrak{m})=1$ *and let* $\mathfrak{h}$ *be an ideal of* Ω *divisible only by powers of prime factors in* Ω *of* 2 *and such that* $(\mathfrak{h}, \mathfrak{m})=1$. *Then,* $\mathfrak{a}$ *being an ideal of* Ω *such that* $(\mathfrak{a}, 2\mathfrak{m}\mathfrak{n})=1$, *there exists the largest positive constant* λ *with* $n_{\mathfrak{h}\mathfrak{n}\mathfrak{a}} \geqq \lambda c_{\mathfrak{h}\mathfrak{n}\mathfrak{a}}$ *for every* $\mathfrak{a}$. λ *depends only on* Ω, $\mathfrak{A}$ *and* $\mathfrak{h}$, *and, if we denote by* $\mathfrak{M}$ *the set of all* $\mathfrak{a}$ *with* $n_{\mathfrak{h}\mathfrak{n}\mathfrak{a}}>\lambda c_{\mathfrak{h}\mathfrak{n}\mathfrak{a}}$, *then we have*

$$\sum_{\mathfrak{a}\in\mathfrak{M}} \frac{c_\mathfrak{a}}{\mathrm{N}\mathfrak{a}^s} < \sum_{\mathfrak{a}} \frac{c_\mathfrak{a}}{\mathrm{N}\mathfrak{a}^s}.$$

PROOF. Let l be a prime factor of n_0. Set $\mathfrak{c}=\mathfrak{h}\mathfrak{n}\mathfrak{a}$. Then it follows from lemma 4, lemma 6 and from what stated in the proof of lemma 7 that $\frac{n_\mathfrak{c}}{c_\mathfrak{c}}$ is determined by the indices $(V_\mathfrak{c}^{(l^i)} : V_\mathfrak{c}^{l^i})$, where $l^i \mid n$. Since we have $(V_\mathfrak{c}^{(l^i)} : V_\mathfrak{c}^{l^i})=(\Omega^{(l^i)} : \Omega_\mathfrak{c}^{(l^i)})$ by lemma 5, all $(V_\mathfrak{c}^{(l^i)} : V_\mathfrak{c}^{l^i})$ are made largest possible whenever we choose $\mathfrak{c}$ such that all $(\Omega^{(l^i)} : \Omega_\mathfrak{c}^{(l^i)})$ are largest possible. Now, for such $\mathfrak{c}$, $\lambda=\frac{n_\mathfrak{c}}{c_\mathfrak{c}}$ is the required constant. For, since we have $(\mathfrak{n}, 2)=1$, an element β of $\Omega^{(l^i)}$ which does not belong to $\Omega_{\mathfrak{n}}^{(l^i)}$ can only be $\lambda^*_{\nu,\nu}=-\lambda_{2^i}^{2^{i-1}}$ of lemma 1 whenever β is an l^i-th power in Ω_{l^i}. Therefore it gives infinitely many prime ideals $\mathfrak{p}$ of Ω such that we have $\beta\notin\Omega_{\mathfrak{p}}^{(l^i)}$, and, consequently, we can choose an ideal $\mathfrak{b}$ of Ω such that $(\Omega^{(l^i)}:\Omega_{\mathfrak{h}\mathfrak{b}}^{(l^i)})=(\Omega^{(l^i)}:\Omega_{\mathfrak{c}}^{(l^i)})$ and such that $\mathfrak{b}$ is prime to any given ideal of Ω, which shows that λ is independent of $\mathfrak{n}$ and of $\mathfrak{m}$. Next, assume that we have $\dfrac{n_{\mathfrak{c}'}}{c_{\mathfrak{c}'}}>\lambda$ for some $\mathfrak{c}'=\mathfrak{h}\mathfrak{n}\mathfrak{a}'$ with $(\mathfrak{a}', 2\mathfrak{m}\mathfrak{n})=1$. Then we have $(\Omega^{(l^i)}:\Omega_{\mathfrak{c}'}^{(l^i)})<(\Omega^{(l^i)}:\Omega_{\mathfrak{c}}^{(l^i)})$ for some l^i, whence $\Omega_{\mathfrak{c}'}^{(l^i)}\supsetneqq\Omega_{\mathfrak{c}}^{(l^i)}$. This shows that, $\{\beta\}$ being a system of representatives of $\Omega^{(l^i)}/\Omega_{\mathfrak{h}\mathfrak{n}}^{(l^i)}$, we have $\beta\in U_{\mathfrak{a}'}I^{l^i}$, $\notin U_{\mathfrak{a}}I^{l^i}$ for some l, i and $\beta\in\{\beta\}$. Now, the last assertion of the lemma is obtained in a similar way to the last part of the proof of lemma 8.

§3. Density and the reciprocity law.

Let $\mathfrak{m}$, $\boldsymbol{b}$ be as in lemma 8 and let χ be a character of $\mathfrak{A}$. Then we set $\Lambda_{\mathfrak{m}}(s,\chi)=\sum\limits_{\kappa:(f_\kappa,\mathfrak{m})=1}\dfrac{\chi(\kappa(\boldsymbol{b}))}{\mathrm{N}f_\kappa^s}$. If especially $\chi=1$ is a unit character, then we set $\Lambda_{\mathfrak{m}}(s,1)=\Lambda_{\mathfrak{m}}(s)$. Every $\Lambda_{\mathfrak{m}}(s,\chi)$ is defined whenever we have $s>1$.

Let next $\mathfrak{l}$ be a prime factor of 2 in Ω which does not divide $\mathfrak{m}$, then there exists the lowest exponent ω such that an element α of Ω is an n-th power in the $\mathfrak{l}$-adic field of Ω whenever we have $\alpha\equiv1 \pmod{\mathfrak{l}^\omega}$. Let $\mathfrak{h}_1,\cdots,\mathfrak{h}_v$ be all ideals of Ω which divide $\prod\limits_{\mathfrak{l}}\mathfrak{l}^\omega$, where we may assume $\mathfrak{h}_1=1$ and $\mathfrak{h}_v=\prod\limits_{\mathfrak{l}}\mathfrak{l}^\omega$. Then, to each $\mathfrak{h}_i$, there corresponds a subgroup $\mathfrak{A}_i$ of $\mathfrak{A}$ in such a way as $\mathfrak{A}'$ corresponds to $\mathfrak{h}$ in lemma 8.

THEOREM 1. *If there is an element of $a\in\mathfrak{A}_1$ with $\chi(a)\neq1$, then we have $\Lambda_{\mathfrak{m}}(s,\chi)\prec\Lambda_{\mathfrak{m}}(s)$, if $\chi(\mathfrak{A}_1)=1$, then $\Lambda_{\mathfrak{m}}(s,\chi)\sim\Lambda_{\mathfrak{m}}(s)$ and if especially $\chi(\mathfrak{A}_v)=1$, then we have $\Lambda_{\mathfrak{m}}(s,\chi)=\Lambda_{\mathfrak{m}}(s)$.*

PROOF. Set $\zeta_{\mathfrak{m}}(s)=\prod\limits_{\mathfrak{p}\nmid\mathfrak{m}}(1-\mathrm{N}\mathfrak{p}^{-s})^{-1}$, $\zeta_{\mathfrak{m}}(s)\Lambda_{\mathfrak{m}}(s,\chi)=J_{\mathfrak{m}}(s,\chi)$ and $\sum\limits_{\kappa\, f_\kappa\mid\mathfrak{c}}\chi(\kappa(\boldsymbol{b}))=n'_{\mathfrak{c}}$. Then we have $J_{\mathfrak{m}}(s)=\sum\limits_{(\mathfrak{c},\mathfrak{m})=1}\dfrac{\mathfrak{n}_{\mathfrak{c}}}{\mathrm{N}\mathfrak{c}^s}$ and

$$J_{\mathfrak{m}}(s,\chi)=\sum_{(\mathfrak{c},\mathfrak{m})=1}\frac{n'_{\mathfrak{c}}}{\mathrm{N}\mathfrak{c}^s}=\sum_i\sum_{(\mathfrak{c},\mathfrak{h}_v)=\mathfrak{h}_i}\frac{n'_{\mathfrak{c}}}{\mathrm{N}\mathfrak{c}^s}$$

$$=\sum_{i,(\mathfrak{h}_i,\mathfrak{m})=1}\left(\prod_{\mathfrak{l},\mathfrak{l}^\omega\mid\mathfrak{h}_i}(1-\mathrm{N}\mathfrak{l}^{-s})^{-1}\cdot\sum_{(\mathfrak{a},2\mathfrak{m})=1}\frac{n'_{\mathfrak{h}_i\mathfrak{a}}}{\mathrm{N}(\mathfrak{h}_i\mathfrak{a})^s}\right).$$

Moreover, it follows from lemma 7 and lemma 8 that we have

$$\sum_{(\mathfrak{a},2\mathfrak{m})=1}\frac{n'_{\mathfrak{h}_i\mathfrak{a}}}{\mathrm{N}(\mathfrak{h}_i\mathfrak{a})^s}\begin{cases} = \displaystyle\sum_{(\mathfrak{a},2\mathfrak{m})=1}\frac{n_{\mathfrak{h}_i\mathfrak{a}}}{\mathrm{N}(\mathfrak{h}_i\mathfrak{a})^s} & \text{if } \chi(\mathfrak{A}_i)=1,\\ < \displaystyle\sum_{(\mathfrak{a},2\mathfrak{m})=1}\frac{n_{\mathfrak{h}_i\mathfrak{a}}}{\mathrm{N}(\mathfrak{h}_i\mathfrak{a})^s} \leqq J_{\mathfrak{m}}(s) & \text{otherwise,}\end{cases}$$

while lemma 9 implies $\sum_{(\mathfrak{a},2\mathfrak{m})=1}\frac{n_{\mathfrak{h}_i\mathfrak{a}}}{\mathrm{N}(\mathfrak{h}_i\mathfrak{a})^s}\sim J_{\mathfrak{m}}(s)$. This proves the first and the second assertion of the theorem. The third assertion is obvious because from $\chi(\mathfrak{A}_v)=1$ follows $n'_{\mathfrak{c}}=n_{\mathfrak{c}}$.

Let $\bar{\mathfrak{F}}$ be a set of homomorphisms κ and $\bar{\mathfrak{F}}_0$ be a subset of $\bar{\mathfrak{F}}$. Then we set analogously to (1)

$$\omega(\bar{\mathfrak{F}}_0,\bar{\mathfrak{F}})=\lim_{s\to1,s>1}\frac{\displaystyle\sum_{\kappa\in\bar{\mathfrak{F}}_0}\frac{1}{\mathrm{N}f_\kappa^s}}{\displaystyle\sum_{\kappa\in\bar{\mathfrak{F}}}\frac{1}{\mathrm{N}f_\kappa^s}}.$$

LEMMA 10. *Let* $\mathfrak{m}$ *be an ideal of* Ω *and let* $\bar{\mathfrak{K}}$ *be the set of all* κ *with* $(f_\kappa,\mathfrak{m})=1$. *Let* $\bar{\mathfrak{K}}_1$ *be the subset of* $\bar{\mathfrak{K}}$ *which consists of all* $\kappa\in\bar{\mathfrak{K}}$ *such that the set of all* $\kappa(\boldsymbol{a})$ $(\boldsymbol{a}\in\boldsymbol{I})$ *does not coincides with* $\mathfrak{A}$. *Then we have* $\omega(\bar{\mathfrak{K}}_1,\bar{\mathfrak{K}})=0$.

PROOF. Let $\mathfrak{A}'$ be any proper subgroup of order n' of $\mathfrak{A}$. For an ideal $\mathfrak{a}$ of Ω, let $c'_{\mathfrak{a}}$ be the number of all homomorphisms of $V_{\mathfrak{a}}$ into $\mathfrak{A}'$ and let $n'_{\mathfrak{a}}$ be the number of all homomorphisms of $\boldsymbol{I}/\Omega^\times U_{\mathfrak{a}}$ into $\mathfrak{A}'$. Then it follows from (2) and from lemma 7, applied to $c'_{\mathfrak{a}}$, $n'_{\mathfrak{a}}$ instead of $c_{\mathfrak{a}}$, $n_{\mathfrak{a}}$, that we have

$$\sum_{(\mathfrak{a},\mathfrak{m})=1}\frac{n'_{\mathfrak{a}}}{\mathrm{N}\mathfrak{a}^s}<\gamma'\prod_{\mathfrak{p}\nmid\mathfrak{m}}\left(\sum_{m=0}^{\infty}\frac{c'_{\mathfrak{p}^m}}{\mathrm{N}\mathfrak{p}^{ms}}\right)\sim\prod_{\mathfrak{p}\nmid\mathfrak{m}}\left(1+\frac{c'_{\mathfrak{p}}}{\mathrm{N}\mathfrak{p}^s}\right),$$

where γ' is a positive constant. Furthermore, by (2) and by lemma 9, we have $\zeta_m(s)\left(\sum_{\kappa\in\bar{\mathfrak{K}}}\frac{1}{\mathrm{N}f_\kappa^s}\right)=J_m(s)\sim\prod_{\mathfrak{p}\nmid\mathfrak{m}}\left(1+\frac{c_{\mathfrak{p}}}{\mathrm{N}\mathfrak{p}^s}\right)$. Now, let M be the set of all $\mathfrak{p}$ with $(\mathfrak{p},n)=1$ and $\left(\frac{\Omega_{n_0}/\Omega}{\mathfrak{p}}\right)=1$. Then we have $c_{\mathfrak{p}}=n$ and $c'_{\mathfrak{p}}=n'$. Therefore, by (2) any by Tschebotareff's theorem, we have

$$0\leqq\lim_{s\to1,s>1}\frac{\displaystyle\prod_{\mathfrak{p}\nmid\mathfrak{m}}\left(1+\frac{c'_{\mathfrak{p}}}{\mathrm{N}\mathfrak{p}^s}\right)}{\displaystyle\prod_{\mathfrak{p}\nmid\mathfrak{m}}\left(1+\frac{c_{\mathfrak{p}}}{\mathrm{N}\mathfrak{p}^s}\right)}\leqq\lim_{s\to1,s>1}\prod_{\mathfrak{p}\nmid\mathfrak{m},\mathfrak{p}\in M}\frac{1+\dfrac{n'}{\mathrm{N}\mathfrak{p}^s}}{1+\dfrac{n}{\mathrm{N}\mathfrak{p}^s}}$$

$$=\lim_{s\to1,s>1}\prod_{\mathfrak{p}\nmid\mathfrak{m},\mathfrak{p}\in M}\left(1+\frac{1}{\mathrm{N}\mathfrak{p}^s}\right)^{n'-n}=0.$$

On the other hand, we have obviously

$$\zeta_{\mathfrak{m}}(s)\Bigl(\sum_{\kappa\in\mathfrak{K}_1}\frac{1}{\mathrm{N}f_\kappa^s}\Bigr)\leqq\sum_{\mathfrak{A}'}\sum_{(\mathfrak{a},\mathfrak{m})=1}\frac{n'_{\mathfrak{a}}}{\mathrm{N}\mathfrak{a}^s},$$

where $\mathfrak{A}'$ runs over all proper subgroups of $\mathfrak{A}$. Our lemma is thereby proved.

THEOREM 2. *$\mathfrak{m}$, $\mathbf{b}$ being as in lemma 8, let $\overline{\mathfrak{K}}$ be the set of all κ with $(f_\kappa, \mathfrak{m})=1$ and let $\overline{\mathfrak{K}}_0$ be the subset of $\overline{\mathfrak{K}}$ which consists of all $\kappa\in\overline{\mathfrak{K}}$ with $\kappa(\mathbf{b})=1$. Then $\omega(\overline{\mathfrak{K}}_0\,;\,\overline{\mathfrak{K}})$ exists and is not less than $\frac{1}{n}$.*

PROOF. Notations being as in theorem 1, we have

$$\omega(\overline{\mathfrak{K}}_0\,;\,\overline{\mathfrak{K}})=\frac{1}{n}\lim_{s\to1,s>1}\sum_{\chi}\frac{\Lambda_{\mathfrak{m}}(s,\chi)}{\Lambda_{\mathfrak{m}}(s)}.$$

The theorem follows immediately from this and from theorem 1.

COROLLARY. *$\mathfrak{m}$, $\mathbf{b}$ being as in lemma 8, let $\mathfrak{K}$ be the family of all abelian extensions K over Ω with following conditions: a) the Galois group of K over Ω is isomorphic to $\mathfrak{A}$. b) the conductor of K over Ω is prime to $\mathfrak{m}$. Furthermore, let $\mathfrak{K}_0$ be the subfamily of $\mathfrak{K}$ which consists of all $K\in\mathfrak{K}$ with $(\mathbf{b}, K/\Omega)=1$ (symbol of Chevalley* [1]*). Then the density $\omega(\mathfrak{K}_0\,;\,\mathfrak{K})$ exists and is equal to $\omega(\overline{\mathfrak{K}}_0\,;\,\overline{\mathfrak{K}})$ of theorem 2.*

PROOF. Besides notations in lemma 10 and theorem 2, let n^* be the number of automorphisms of A. Then, by lemma 10, we have

$$\omega(\overline{\mathfrak{N}}_0\,;\,\overline{\mathfrak{K}})=\lim_{s\to1,s>1}\frac{\displaystyle\sum_{\kappa\in\mathfrak{K}_0}\frac{1}{\mathrm{N}f_\kappa^s}}{\displaystyle\sum_{\kappa\in\mathfrak{K}}\frac{1}{\mathrm{N}f_\kappa^s}}$$

$$=\lim_{s\to1,s>1}\frac{\displaystyle\sum_{\kappa\in\mathfrak{K}_0,\,\notin\mathfrak{K}_1}\frac{1}{\mathrm{N}f_\kappa^s}}{\displaystyle\sum_{\kappa\in\mathfrak{K},\,\notin\mathfrak{K}_1}\frac{1}{\mathrm{N}f_\kappa^s}}$$

$$=\lim_{s\to1,s>1}\frac{\displaystyle\sum_{K\in\mathfrak{K}_0}\frac{n^*}{\mathrm{N}f_K^s}}{\displaystyle\sum_{K\in\mathfrak{K}}\frac{n^*}{\mathrm{N}f_K^s}}=\omega(\mathfrak{K}_0\,;\,\mathfrak{K}),$$

which proves our assertion.

THEOREM 3. *Notations being as in theorem 2, let especially $\mathbf{b}$ be an idèle of Ω with $\mathfrak{p}$-component 1 for every $\mathfrak{p}\neq\mathfrak{x}$ and with such $\mathfrak{x}$-*

component $\mathfrak{b}_\mathfrak{r}$ *that we have* $\mathfrak{r} \| \mathfrak{b}_\mathfrak{r}$, *where* $\mathfrak{r}$ *is a prime ideal of* Ω *with* $\mathfrak{r} | \mathfrak{m}$ *and* $\mathfrak{r} \nmid 2$. *Then we have* $\omega(\bar{\mathfrak{K}}_0 ; \bar{\mathfrak{K}}) = \dfrac{1}{n}$.

PROOF. Under the assumption of the theorem, we can show that the group $\mathfrak{A}_1$ of theorem 1 coincides with $\mathfrak{A}$. In fact, let β be an element of $\boldsymbol{b}^{l^r} \boldsymbol{U} \boldsymbol{I}^{l^{r+1}} \frown \Omega^\times$, where $l^{r+1} | n_0$. Then, since the ideal (β) generated by β satisfies $(\beta) = \mathfrak{r}^{l^r} \mathfrak{b}^{l^{r+1}}$ for some ideal $\mathfrak{b}$ of Ω, β cannot be equal to $\lambda^*_{\mu,\nu}$ of lemma 1 even if $l=2$. It gives therefore an ideal $\mathfrak{a}$ of Ω such that $(\mathfrak{a}, 2\mathfrak{m})=1$ and that $\beta \notin \boldsymbol{U}_\mathfrak{a} \boldsymbol{I}^{l^{r+1}}$ for all l, r and β, which shows $\mathfrak{A} = \mathfrak{A}_1$ (see the proof of lemma 8). Now, the theorem follows immediately from theorem 1.

This proof does not require that part of theorem 2 which is due to lemma 7.

COROLLARY. *Let* $\mathfrak{r}$ *be an ideal of* Ω *which does not divide 2 and let* $\mathfrak{m}$ *be an ideal of* Ω *which is divisible by* $\mathfrak{r}$. *Furthermore,* $\mathfrak{K}$ *being as in corollary to theorem 2, let* $\mathfrak{K}_0$ *be the subfamily of* $\mathfrak{K}$ *which consists of all* $K \in \mathfrak{K}$ *with* $\left(\dfrac{K/\Omega}{\mathfrak{r}}\right) = 1$. *Then we have* $\omega(\mathfrak{K}_0 ; \mathfrak{K}) = \dfrac{1}{n}$.

PROOF. Similar to the proof of corollary to theorem 2.

§4. Ramifications.

THEOREM 4. *Let* $\mathfrak{m}$, $\mathfrak{n}$, $\mathfrak{h}$ *be as in lemma 9 and let* $\bar{\mathfrak{h}}$ *be the product of all prime factors in* Ω *of* $(2, \mathfrak{m})$. *Then there is a constant* λ' *depending only on* Ω, $\mathfrak{A}$, $\mathfrak{h}$ *and* $\bar{\mathfrak{h}}$ *such that*

$$\sum_{(\mathfrak{b}, \mathfrak{h}\mathfrak{m}\mathfrak{n})=1} \frac{n_\mathfrak{c}}{N\mathfrak{c}^s} \approx \lambda' \sum_{(\mathfrak{b}, \mathfrak{h}\mathfrak{m}\mathfrak{n})=1} \frac{c_\mathfrak{c}}{N\mathfrak{c}^s},$$

where $\mathfrak{c} = \mathfrak{h}\mathfrak{n}\mathfrak{b}$.

PROOF. Let $\mathfrak{h}_i$, $\mathfrak{l}$ and ω be as in the beginning of §3. Then it follows from lemma 9 that there is a constant $\lambda_{\mathfrak{h}\mathfrak{h}_i}$ such that

$$\sum_{(\mathfrak{a}, 2\mathfrak{m}\mathfrak{n})=1} \frac{n_{\mathfrak{h}\mathfrak{h}_i\mathfrak{n}\mathfrak{a}}}{N(\mathfrak{h}\mathfrak{h}_i\mathfrak{n}\mathfrak{a})^s} \approx \lambda_{\mathfrak{h}\mathfrak{h}_i} \sum_{(\mathfrak{a}, 2\mathfrak{m}\mathfrak{n})=1} \frac{c_{\mathfrak{h}\mathfrak{h}_i\mathfrak{n}\mathfrak{a}}}{N(\mathfrak{h}\mathfrak{h}_i\mathfrak{n}\mathfrak{a})^s}.$$

This shows that

$$\sum_{\mathfrak{c}} \frac{n_\mathfrak{c}}{N\mathfrak{c}^s} = \sum_i \sum_{(\mathfrak{b}, \mathfrak{h}_\nu) = \mathfrak{h}_i} \frac{n_\mathfrak{c}}{N\mathfrak{c}^s}$$

$$= \sum_{i, (\mathfrak{h}_i, \mathfrak{h}\mathfrak{h})=1} \left(\prod_{\mathfrak{l}, \mathfrak{l}^\omega | \mathfrak{h}_i} (1 - N\mathfrak{l}^{-s})^{-1} \sum_{(\mathfrak{a}, 2\mathfrak{m}\mathfrak{n})=1} \frac{n_{\mathfrak{h}\mathfrak{h}_i\mathfrak{n}\mathfrak{a}}}{N(\mathfrak{h}\mathfrak{h}_i\mathfrak{n}\mathfrak{a})^s} \right)$$

$$\approx \sum_{i, (\mathfrak{h}_i, \mathfrak{h}\mathfrak{h})=1} \left(\prod_{\mathfrak{l}, \mathfrak{l}^\omega | \mathfrak{h}_i} (1 - N\mathfrak{l}^{-s})^{-1} \cdot \lambda_{\mathfrak{h}\mathfrak{h}_i} \sum_{(\mathfrak{a}, 2\mathfrak{m}\mathfrak{n})=1} \frac{c_{\mathfrak{h}\mathfrak{h}_i\mathfrak{n}\mathfrak{a}}}{(N\mathfrak{h}\mathfrak{h}_i\mathfrak{n}\mathfrak{a})^s} \right)$$

$$= \sum_{i,(\mathfrak{h}_i,\mathfrak{h}\mathfrak{h})=1} \left(\lambda_{\mathfrak{h}\mathfrak{h}_i} \frac{c_{\mathfrak{h}\mathfrak{h}_i\mathfrak{n}}}{N(\mathfrak{h}\mathfrak{h}_i\mathfrak{n})^s} \prod_{\mathfrak{l},\mathfrak{l}^w \mid \mathfrak{h}_i} (1-N\mathfrak{l}^{-s})^{-1} \sum_{(\mathfrak{a},2\mathfrak{m}\mathfrak{n})=1} \frac{c_\mathfrak{a}}{N\mathfrak{a}^s} \right).$$

Set now $\sigma_\mathfrak{p}(s)=\sum_{m=0}^{\infty} \frac{c_{\mathfrak{p}^m}}{N\mathfrak{p}^{ms}}$. Then we have

$$\sum_{(\mathfrak{a},2\mathfrak{m}\mathfrak{n})=1} \frac{c_\mathfrak{a}}{N\mathfrak{a}^s} = \prod_{\mathfrak{p} \nmid 2\mathfrak{m}\mathfrak{n}} \sigma_\mathfrak{p}(s), \qquad \sum_{(\mathfrak{b},\mathfrak{h}\mathfrak{m}\mathfrak{n})=1} \frac{c_\mathfrak{c}}{N\mathfrak{c}^s} = \frac{c_{\mathfrak{h}\mathfrak{n}}}{N(\mathfrak{h}\mathfrak{n})^s} \sum_{\mathfrak{p} \nmid \mathfrak{h}\mathfrak{m}\mathfrak{n}} \sigma_\mathfrak{p}(s)$$

and therefore

$$\frac{\displaystyle\sum_{(\mathfrak{b},\mathfrak{h}\mathfrak{m}\mathfrak{n})=1} \frac{n_\mathfrak{c}}{N\mathfrak{c}^s}}{\displaystyle\sum_{(\mathfrak{b},\mathfrak{h}\mathfrak{m}\mathfrak{n})=1} \frac{c_\mathfrak{c}}{N\mathfrak{c}^s}} \approx \sum_{i,(\mathfrak{h}_i,\mathfrak{h}\mathfrak{h})=1} \left(\frac{\lambda_{\mathfrak{h}\mathfrak{h}_i} c_{\mathfrak{h}_i}}{N\mathfrak{h}_i^s} \prod_{\mathfrak{l},\mathfrak{l}^w \mid \mathfrak{h}_i} (1-N\mathfrak{l}^{-s})^{-1}) \cdot \prod_{\mathfrak{l},\mathfrak{l} \nmid \mathfrak{h}\mathfrak{h}} \sigma_\mathfrak{l}(1)^{-1} \right),$$

which proves the theorem.

THEOREM 5. *Let $\mathfrak{X}$ be a finite set of prime ideals of Ω, and, for each $\mathfrak{x} \in \mathfrak{X}$, let there be given an integer $u_\mathfrak{x} \geqq 0$. Let $\bar{\mathfrak{K}}$ be the set of all κ and let $\bar{\mathfrak{K}}_0$ be the set of all $\kappa \in \bar{\mathfrak{K}}$ with $\mathfrak{x}^{u_\mathfrak{x}} \| f_\kappa$ for every $\mathfrak{x} \in \mathfrak{X}$. Then $\omega(\bar{\mathfrak{K}}_0; \bar{\mathfrak{K}})$ exists.*

PROOF. Set $\prod_{\mathfrak{x}\in\mathfrak{X},\, u_\mathfrak{x}=0} \mathfrak{x}=\mathfrak{m}$, $\prod_{\mathfrak{x}\in\mathfrak{X},\, \mathfrak{x} \nmid 2} \mathfrak{x}^{u_\mathfrak{x}}=\mathfrak{n}$ and $\prod_{\mathfrak{x}\in\mathfrak{X},\, \mathfrak{x} \mid 2} \mathfrak{x}^{u_\mathfrak{x}}=\mathfrak{h}$. Denote by $\tilde{n}_\mathfrak{c}$ the number of all κ with $f_\kappa=\mathfrak{c}$. Then, for any $\mathfrak{d}$ with $\mathfrak{d} \mid \mathfrak{h}\mathfrak{n}$, we have

$$\sum_{\mathfrak{d}' \mid \mathfrak{d}} \left(\zeta_{\mathfrak{h}\mathfrak{m}\mathfrak{n}}(s) \sum_{(\mathfrak{a},\mathfrak{h}\mathfrak{m}\mathfrak{n})=1} \frac{\tilde{n}_{\mathfrak{d}'\mathfrak{a}}}{N(\mathfrak{h}\mathfrak{n}\mathfrak{a})^s} \right) = \sum_{(\mathfrak{a},\mathfrak{h}\mathfrak{m}\mathfrak{n})=1} \frac{n_{\mathfrak{d}\mathfrak{a}}}{N(\mathfrak{h}\mathfrak{n}\mathfrak{a})^s},$$

where $\zeta_{\mathfrak{h}\mathfrak{m}\mathfrak{n}}(s)$ is as in the proof of theorem 1. Therefore, denoting by $\mu(\ )$ the Möbius' function for the ideals of Ω, we have

$$\zeta_{\mathfrak{h}\mathfrak{m}\mathfrak{n}}(s) \sum_{(\mathfrak{a},\mathfrak{h}\mathfrak{m}\mathfrak{n})=1} \frac{\tilde{n}_{\mathfrak{h}\mathfrak{n}\mathfrak{a}}}{N(\mathfrak{h}\mathfrak{n}\mathfrak{a})^s}$$
$$= \sum_{\mathfrak{d} \mid \mathfrak{h}\mathfrak{n}} \left(\mu\left(\frac{\mathfrak{h}\mathfrak{n}}{\mathfrak{d}}\right) \sum_{(\mathfrak{a},\mathfrak{h}\mathfrak{m}\mathfrak{n})=1} \frac{n_{\mathfrak{d}\mathfrak{a}}}{N(\mathfrak{h}\mathfrak{n}\mathfrak{a})^s} \right).$$

Thus, by theorem 4, we have

$$(8) \qquad \sum_{\kappa\in\mathfrak{K}_0} \frac{1}{Nf_\kappa^s} = \sum_{(\mathfrak{a},\mathfrak{h}\mathfrak{m}\mathfrak{n})=1} \frac{\tilde{n}_{\mathfrak{h}\mathfrak{n}\mathfrak{a}}}{N(\mathfrak{h}\mathfrak{n}\mathfrak{a})^s}$$
$$\approx \zeta_{\mathfrak{h}\mathfrak{m}\mathfrak{n}}(s)^{-1} \sum_{\mathfrak{d} \mid \mathfrak{h}\mathfrak{n}} \left(\mu\left(\frac{\mathfrak{h}\mathfrak{n}}{\mathfrak{d}}\right) N\left(\frac{\mathfrak{d}}{\mathfrak{h}\mathfrak{n}}\right)^s \cdot \lambda'_\mathfrak{d} \cdot \sum_{(\mathfrak{a},\mathfrak{h}\mathfrak{m}\mathfrak{n})=1} \frac{c_{\mathfrak{d}\mathfrak{a}}}{N(\mathfrak{d}\mathfrak{a})^s} \right)$$
$$= \zeta_{\mathfrak{h}\mathfrak{m}\mathfrak{n}}(s)^{-1} \sum_{\mathfrak{d} \mid \mathfrak{h}\mathfrak{n}} \left(c_\mathfrak{d} \lambda'_\mathfrak{d} \cdot \mu\left(\frac{\mathfrak{h}\mathfrak{n}}{\mathfrak{d}}\right) N\left(\frac{1}{\mathfrak{h}\mathfrak{n}}\right)^s \sum_{(\mathfrak{a},\mathfrak{h}\mathfrak{m}\mathfrak{n})=1} \frac{c_\mathfrak{a}}{N\mathfrak{a}^s} \right),$$

where $\lambda'_\mathfrak{d}$ is a constant. On the other hand, it follows from theorem 4 that there is a constant λ_Ω such that

$$\sum_{\kappa\in\mathfrak{K}}\frac{1}{\mathrm{N}f_\kappa^s}\approx\lambda_\Omega\cdot\zeta_\Omega(s)^{-1}\sum_{\mathfrak{a}}\frac{c_{\mathfrak{a}}}{\mathrm{N}\mathfrak{a}^s}\,,\tag{9}$$

where $\zeta_\Omega(s)$ is the Dedekind's zeta-function of Ω and $\mathfrak{a}$ runs over all ideals of Ω. Now, our theorem follows immediately from (8) and (9).

COROLLARY. *$\mathfrak{X}$ and $u_{\mathfrak{r}}$ being as in theorem 5, let $\mathfrak{K}$ be the family of all abelian extensions K over Ω such that the Galois group of K over Ω is isomorphic to $\mathfrak{A}$. Let $\mathfrak{K}_0$ be the subfamily of $\mathfrak{K}$ which consists of all $K\in\mathfrak{K}$ with $\mathfrak{r}^{u_{\mathfrak{r}}}\|f_K$. Then the density $\omega(\mathfrak{K}_0;\mathfrak{K})$ exists and is equal to $\omega(\overline{\mathfrak{K}}_0;\overline{\mathfrak{K}})$ of theorem 5.*

PROOF. Similar to the proof of corollary to theorem 2.

EXAMPLE 1. Let $\mathfrak{r}$ be a prime ideal of Ω which does not divide 2. Assume that $\mathfrak{X}$ of theorem 5 consists of only one prime ideal $\mathfrak{r}$ with $u_{\mathfrak{r}}=u>0$. Then we have $\mathfrak{m}=1$, $\mathfrak{n}=\mathfrak{r}^u$ and $\mathfrak{h}=1$. Set $\sigma_{\mathfrak{p}}(s)=\sum\limits_{m=0}^{\infty}\frac{c_{\mathfrak{p}^m}}{\mathrm{N}\mathfrak{p}^{ms}}$. Then, by (8), we have

$$\sum_{\kappa\in\mathfrak{K}}\frac{1}{\mathrm{N}f_\kappa^s}\approx\lambda_\Omega\cdot\zeta_{\mathfrak{r}}(s)^{-1}(c_{\mathfrak{r}^u}-c_{\mathfrak{r}^{u-1}})\mathrm{N}\mathfrak{r}^{-us}\sum_{(\mathfrak{a},\mathfrak{r})=1}\frac{c_{\mathfrak{a}}}{\mathrm{N}\mathfrak{a}^s}\,,$$

whence

$$\begin{aligned}\omega(\overline{\mathfrak{K}}_0;\overline{\mathfrak{K}})&=\lim_{s\to1,s>1}\frac{\zeta_\Omega(s)\prod\limits_{\mathfrak{p}\neq\mathfrak{r}}\sigma_{\mathfrak{p}}(s)}{\zeta_{\mathfrak{r}}(s)\prod\limits_{\mathfrak{p}}\sigma_{\mathfrak{p}}(s)}(c_{\mathfrak{r}^u}-c_{\mathfrak{r}^{u-1}})\mathrm{N}\mathfrak{r}^{-us}\\&=\frac{c_{\mathfrak{r}^u}-c_{\mathfrak{r}^{u-1}}}{\sigma_{\mathfrak{r}}(1)(1-\mathrm{N}\mathfrak{r}^{-1})\mathrm{N}\mathfrak{r}^u}\,.\end{aligned}$$

If the family $\mathfrak{K}_0$ of corollary to theorem 5 consists of all K with $f_K=\mathfrak{r}^u$, then $\omega(\mathfrak{K}_0;\mathfrak{K})$ has also the same value.

EXAMPLE 2. Next, assume $\mathfrak{r}\nmid 2\mathfrak{n}$ and $u_{\mathfrak{r}}=0$. Then we have $\mathfrak{m}=\mathfrak{r}$, $\mathfrak{n}=1$, $\mathfrak{h}=1$, $\sum\limits_{\kappa\in\mathfrak{K}_0}\frac{1}{\mathrm{N}f_\kappa^s}\approx\lambda_\Omega\cdot\zeta_{\mathfrak{r}}(s)^{-1}\sum\limits_{(\mathfrak{a},\mathfrak{r})=1}\frac{c_{\mathfrak{a}}}{\mathrm{N}\mathfrak{a}^s}$ and

$$\sigma_{\mathfrak{r}}(s)=\sum_{m=0}^{\infty}\frac{c_{\mathfrak{r}}}{\mathrm{N}\mathfrak{r}^{ms}}=\left(1+\frac{c_{\mathfrak{r}}-1}{\mathrm{N}\mathfrak{r}^s}\right)(1-\mathrm{N}\mathfrak{r}^{-s})^{-1},$$

whence

$$\begin{aligned}\omega(\overline{\mathfrak{K}}_0;\overline{\mathfrak{K}})&=\lim_{s\to1,s>1}\frac{\zeta_\Omega(s)\prod\limits_{\mathfrak{p}\neq\mathfrak{r}}\sigma_{\mathfrak{p}}(s)}{\zeta_{\mathfrak{r}}(s)\prod\limits_{\mathfrak{p}}\sigma_{\mathfrak{p}}(s)}\\&=(1-\mathrm{N}\mathfrak{r}^{-1})^{-1}\,\sigma_{\mathfrak{r}}(1)^{-1}=\left(1+\frac{c_{\mathfrak{r}}-1}{\mathrm{N}\mathfrak{r}}\right)^{-1}\\&=\frac{\mathrm{N}\mathfrak{r}}{\mathrm{N}\mathfrak{r}+c_{\mathfrak{r}}-1}\,.\end{aligned}$$

We have therefore $\omega(\mathfrak{K}_0;\mathfrak{K})=\dfrac{N\mathfrak{r}}{N\mathfrak{r}+c_{\mathfrak{r}}-1}$ if $\mathfrak{K}_0$ of corollary to theorem 5 consists of all K unramified at $\mathfrak{r}$.

§5. The order of $\Lambda(s)$ at $s=1$.

$\Lambda(s)$ is defined, as in §3, by $\sum\limits_{\kappa}\dfrac{1}{Nf_\kappa^s}$, where the sum is extended over all homomorphisms κ of G_Ω into $\mathfrak{A}$.

LEMMA 11. *Let n_d be the number of elements of $\mathfrak{A}$ with order d and η be the number of irreducible representations of $\mathfrak{A}$ in Ω. Then we have $\eta=\sum\limits_{d\mid n_0}n_d/(\Omega_d:\Omega)$.*

PROOF. There are just n_d characters of order d of $\mathfrak{A}$. χ be one of them. Then, σ^i running over all automorphisms of Ω_d over Ω, the representation

$$\begin{pmatrix}\chi & & & \\ & \chi^\sigma & & \\ & & \chi^{\sigma^2} & \\ & & & \ddots\end{pmatrix}$$

is equivalent with an irreducible representation of $\mathfrak{A}$ in Ω. Conversely, every irreducible representation of $\mathfrak{A}$ in Ω is obtained in such a way, from which follows easily the lemma.

THEOREM 6. $\Lambda(s)\sim(s-1)^{-(\eta-1)}$.

PROOF. Since from (2) and from theorem 4 follows

$$\zeta_\Omega(s)\Lambda(s)\sim\prod_{\mathfrak{p}}\left(1+\frac{c_\mathfrak{p}}{N\mathfrak{p}^s}\right),$$

it suffices to prove

$$\prod_{\mathfrak{p}}\left(1+\frac{c_\mathfrak{p}}{N\mathfrak{p}^s}\right)\sim(s-1)^{-\eta}.$$

Now, for every $d\mid n_0$, denote by M_d the set of all prime ideals $\mathfrak{p}$ of Ω such that $\left(\dfrac{\Omega_d/\Omega}{\mathfrak{p}}\right)=1$. Then, Tschebotareff's theorem shows that

$$\prod_{\mathfrak{p}\in M_d}\left(1+\frac{1}{N\mathfrak{p}^s}\right)\sim(s-1)^{-1/(\Omega_d:\Omega)}.$$

Therefore, making use of (3), we have

$$\prod_{\mathfrak{p}}\left(1+\frac{c_\mathfrak{p}}{N\mathfrak{p}^s}\right)\sim\prod_{\mathfrak{p}}\left(1+\frac{\sum\limits_{d,M_d\ni\mathfrak{p}}n_d}{N\mathfrak{p}^s}\right)$$

$$\sim\prod_{\mathfrak{p}}\prod_{d\ M_d\ni\mathfrak{p}}\left(1+\frac{1}{N\mathfrak{p}^s}\right)^{n_d}=\prod_{d}\prod_{\mathfrak{p}\in M_d}\left(1+\frac{1}{N\mathfrak{p}^s}\right)^{n}$$

$$\sim\prod_{d}(s-1)^{-n_d/(\Omega_d:\Omega)}=(s-1)^{-\sum\limits_{d}n_d/(\Omega_d:\Omega)}.$$

The theorem follows immediately from this and from lemma 11.

§6. Further results.

In this paragraph, we shall denote by $\mathfrak{K}$ the family of all abelian extensions K over Ω such that the Galois group of K/Ω is isomorphic to $\mathfrak{A}$.

THEOREM 7. *Let Ω_0 be an arbitrary subfield of Ω and let $\mathfrak{K}_0$ be the family of all $K\in\mathfrak{K}$ such that there exists a normal extension k of Ω_0 with $K=\Omega k$. Then we have*

$$\sum_{K\in\mathfrak{K}_0}\frac{1}{\mathrm{N}f_K^s}\sim 1 \text{ and } \omega(\mathfrak{K}_0;\,\mathfrak{K})=0.$$

PROOF. Let $\bar{\Omega}$ be a normal extension of Ω_0 which contains Ω. Then we have $f^{\sigma}_{\Omega k/\Omega}=f_{\bar{\Omega}k/\Omega}$ for every automorphism σ of $\bar{\Omega}$ over Ω_0, and $f^{\sigma_0}_{k/k\frown\Omega}=f_{k/k\frown\Omega}$ for every automorphism σ_0 of $k\frown\Omega$ over Ω_0. Therefore we have $f_{\bar{\Omega}k/\bar{\Omega}}=\mathfrak{p}_{0,1}\mathfrak{p}_{0,2}\cdots\mathfrak{p}_{0,t}\bar{\mathfrak{r}}$ and $f_{k/k\frown\Omega}=\mathfrak{p}_{0,1}\mathfrak{p}_{0,2}\cdots\mathfrak{p}_{0,t}\mathfrak{r}_0$, where $\mathfrak{p}_{0,i}$ is a prime ideal of Ω_0 which divides neither n nor the relative discriminant $\mathfrak{d}(\bar{\Omega}/\Omega_0)$, while $\bar{\mathfrak{r}}$, $\mathfrak{r}_0$ are ideals of $\bar{\Omega}$, $k\frown\Omega$ respectively, which are composed of prime factors of n and of $\mathfrak{d}(\bar{\Omega}/\Omega_0)$. This shows that $f_{\Omega k/\Omega}=\mathfrak{p}_{0,1}\mathfrak{p}_{0,2}\cdots\mathfrak{p}_{0,t}\mathfrak{r}$, where $\bar{\mathfrak{r}}\,|\,\mathfrak{r}$ and $\mathfrak{r}\,|\,\mathfrak{r}_0$. Therefore, by lemma 7, there is a constant γ such that

$$\sum_{K\in\mathfrak{K}_0}\frac{1}{\mathrm{N}f_K^s}<\gamma\prod_{\mathfrak{p}_0}\left(1+\frac{c_{\mathfrak{p}_0}}{\mathrm{N}\mathfrak{p}_0^s}\right)\prod_{\mathfrak{w}}\left(\sum_{m=0}^{\infty}\frac{c_{\mathfrak{w}^m}}{\mathrm{N}\mathfrak{w}^{ms}}\right), \tag{10}$$

where the former product is extended over all prime ideals $\mathfrak{p}_0$ of Ω_0 witn $\mathfrak{p}_0\nmid n\mathfrak{d}(\bar{\Omega}/\Omega_0)$, and the latter over all prime ideals $\mathfrak{w}$ of Ω with $\mathfrak{w}\,|\,n\mathfrak{d}(\bar{\Omega}/\Omega_0)$. Moreover, $\mathrm{N}\mathfrak{p}_0$ is at least an $(\Omega:\Omega_0)$-th power of a prime number. Hence the left side of (10) is ~ 1. Since $\mathfrak{K}_0$ is not empty, the first assertion of the theorem is proved. The second assertion follows immediately from the first and from theorem 6.

COROLLARY 1. *Let Ω_0 be a subfield of Ω over which Ω is normal and let $\mathfrak{K}_0$ be the family of all $K\in\mathfrak{K}$ such that K is normal over Ω_0. Then we have $\omega(\mathfrak{K}_0;\,\mathfrak{K})=0$.*

PROOF. This follows immediately from theorem 7.

COROLLARY 2. *Let Ω_0 be an arbitrary subfield of Ω. Then there are infinitely many extensions K over Ω with following properties: a) the Galois group of over Ω is isomorphic to $\mathfrak{A}$. b) there is no normal extension k over Ω_0 such that $K=\Omega k$.*

PROOF. This follows from theorem 6, theorem 7 and lemma 10.

NAGOYA UNIVERSITY

References

[1] C. Chevalley, Généralisation de la théorie du corps de classes pour les extensions infinis, J. Math. Pures Appl. (**9**), **15** (1936), pp. 359–371.

[2] H. Hasse, Invariante Kennzeichnung relativ-abelscher Zahlkörper mit vorgegebner Galoisgruppe über einem Teilkörper des Grundkörpers, Abh. Deutsch. Akad. d. Wiss. zu Berlin, Math.-Naturw. Kl., Jahrg. 1947, Nr. **8**.

[3] H. Hasse, Die Multiplikationsgruppe der abelschen Körper mit fester Galoisgruppe, Abh. Math. Sem. Univ. Hamburg, **16** (1949), pp. 29–40.

[4] H. Hasse, Zum Existenzsatz von Grunwald in der Klassenkörpertheorie, J. Reine Angew. Math., **188** (1950), pp. 40–64.

[5] A. Weil, Sur la théorie du corps de classes, J. Math. Soc. Japan, **3** (1951), pp. 1–35.

Fibre Spaces and Sheaves in Number Theory

Keijiro YAMAZAKI

Part I

0. A. Weil [5] has introduced successfully the concept of the fibre space into algebraic geometry. We have tried in [6] to establish an analogous theory on number fields. We shall sketch the results in [6] in Part I.

1. Let k be any algebraic number field of a finite or an infinite degree and $S(k)$ the set of all finite prime divisors of k. If k is of a finite degree, we introduce the weakest T_1-topology into $S(k)$. If k is of an infinite degree, then the topological space $S(k)$ will be determined as the projective limit of $S(k_\lambda)$ where k_λ runs over all subfields of finite degrees of k. Hereafter we fix an algebraic number field k of a finite degree.

Let W be the group of all roots of unity; we denote by $\overline{W}$ the set of all elements of W and the symbols 0 and ∞. We introduce the weakest T_1-topology into $\overline{W}$, and new operations in $\overline{W}$ as follows: $00=0$, $\infty\infty=\infty$, $0^{-1}=\infty$, $\infty^{-1}=0$, $\zeta 0=0\zeta=0$, $\zeta\infty=\infty\zeta=\infty$ for all $\zeta\in W$. But we do not define 0∞ and $\infty 0$.

LEMMA. Let K be an algebraic number field containing all roots of unity and $K(\mathfrak{p})^*$ the multiplicative group of the residue class field modulo a finite prime divisor $\mathfrak{p}$ of K. Then there exists one and only one isomorphism $\iota_\mathfrak{p}$ of $K(\mathfrak{p})^*$ into W such that for all $c\in K(\mathfrak{p})^*$ the residue class of $\iota_\mathfrak{p}(c)$ modulo $\mathfrak{p}$ is identical with c.

Applying this lemma to $k(W)=K$, we define $f(\mathfrak{p})$ for $f\in k^*$ and $\mathfrak{p}\in S(k(W))$ as follows: ($|\ |_\mathfrak{p}$ means a valuation representing $\mathfrak{p}$, and $\bar{f}$ is the residue class of f mod $\mathfrak{p}$.)

$$f(\mathfrak{p})=\begin{cases} 0 & \text{if } |f|_\mathfrak{p}<1,\\ \infty & \text{if } |f|_\mathfrak{p}>1,\\ \iota_\mathfrak{p}(\bar{f}) & \text{if } |f|_\mathfrak{p}=1.\end{cases}$$

Next we introduce an equivalence relation of $S(k(W))$ as follows: Let $\mathfrak{p}$ be equivalent to $\mathfrak{q}$ if and only if $f(\mathfrak{p})=f(\mathfrak{q})$ for all $f\in k^*$. We denote by $\bar{S}(k)$ the quotient space of $S(k(W))$ with respect to this relation. Then $\bar{S}(k)$ is provided with the weakest T_1-topology and the assignment $\mathfrak{p} \rightarrow f(\mathfrak{p})$ induces a $\bar{W}$-valued function on $\bar{S}(k)$ for each $f \in k^*$. If $\mathfrak{p} \in S(k(W))$ induce $\mathfrak{p}' \in S(k)$, then $\mathfrak{p}'$ depends only upon the equivalence class $\bar{\mathfrak{p}}$ of $\mathfrak{p}$, and $\bar{\mathfrak{p}} \in \bar{S}(k)$ will be said to *lie above* $\mathfrak{p}'$. Moreover $\bar{\mathfrak{p}}$, $\bar{\mathfrak{q}} \in \bar{S}(k)$ will be said to be *conjugate* with each other if and only if they lie above the same $\mathfrak{p}' \in S(k)$.

2. Now we state a general definition.

DEFINITION. *Let S be a topological space and $\mathfrak{R}(S)$ a set of $\bar{W}$-valued functions defined on some non-empty open subsets of S; we denote by $\mathfrak{D}(f)$ the domain of definition of $f \in \mathfrak{R}(S)$. We call the pair $(S, \mathfrak{R}(S))$ a W-variety, if the following conditions are satisfied.*

1) *Any two non-empty open subsets of S always intersect with each other.*

2) *Any $f \in \mathfrak{R}(S)$ does not take identically the value 0 or ∞. If $f \in \mathfrak{R}(f)$ is not a continuous function, then f takes a constant value on some non-empty open subset of S, and $f(x) \neq 0, \infty$ for all $x \in \mathfrak{D}(f)$.*

3) *For any two functions f and g in $\mathfrak{R}(S)$, there exists one and only one function h in $\mathfrak{R}(S)$ such that $f(x)g(x)$ and $h(x)$ are defined and coincide with each other for all x in some non-empty open subset of S. We denote by fg this function h. Whenever $f(x)g(x)$ is defined, $(fg)(x)$ is defined and $f(x)g(x) = (fg)(x)$.*

4) *There exists a function e in $\mathfrak{R}(S)$ such that $\mathfrak{D}(e) = S$ and $e(x) = 1$ for all $x \in S$.*

5) *For any $f \in \mathfrak{R}(S)$, there exists a function f' in $\mathfrak{R}(S)$ such that $\mathfrak{D}(f') \subset \mathfrak{D}(f)$ and $f'(x) = f(x)^{-1}$ for all $x \in \mathfrak{D}(f')$.*

EXAMPLES of W-varieties.

1) $S = W$, $\mathfrak{R}(W) =$ the set of all assignments of ζ^n to $\zeta \in W$ for all integers n.

2) Let $\mathfrak{m}$ be an integral divisor of k which may contain real primes; we denote by $|\mathfrak{m}|$ the set of all points in $\bar{S}(k)$ lying above finite primes contained in $\mathfrak{m}$. $S = \bar{S}(k) - |\mathfrak{m}|$, $\mathfrak{R}(S) =$ the set of all elements $f \in k^*$ such that $f \equiv 1 \bmod \mathfrak{m}$. We regard any element of $\mathfrak{R}(S)$ as a $\bar{W}$-valued function on S as in 1.

Now we can define some general concepts analogously to algebraic geometry, open subvarieties, rational mappings, direct products under a suitable condition, and group W-varieties.

3. We define fibre spaces over a W-variety. Here we define only principal fibre spaces (Cf. [6]).

DEFINITION. *A principal fibre W-space is a collection as follows:*

1) *A W-variety B,*

2) *a W-variety S called the base W-variety,*

3) *a rational mapping of B onto S,*

4) *a group W-variety G called the structural group which operates on B.*

Assume that there exist an open covering $\{U_i\}$ *of* S *and a birational mapping* Φ_i *of* $U_i \times G$ *onto* $\pi^{-1}(U_i)$ *for each* i *such that*

$$\pi(\Phi_i(x, g)) = x \qquad \text{for all } x \in U_i \text{ and } g \in G,$$
$$\Phi_i(x, g)g' = \Phi_i(x, gg') \quad \text{for all } x \in U_i \text{ and } g, g' \in G.$$

In particular we shall consider the case that the base W-variety S is $\bar{S}(k)-|\mathfrak{m}|$ (example 2) in 2.) and the structural group is W (example 1) in 2.). We call a principal fibre W-space B over S *rational*, if and only if the following additional condition is satisfied about $\{U_i\}$ in the above definition: For each i, every conjugate element of any element in U_i is contained in U_i. Now all classes of isomorphic rational principal fibre W-spaces of group W over S form a group $\mathfrak{B}(S)$ similarly as in topology. Then the following fact holds.

The group $\mathfrak{B}(S)$ *defined in the above is isomorphic to the factor group* $A_{\mathfrak{m}}/S_{\mathfrak{m}}$ *where* $A_{\mathfrak{m}}$ *is the group of all ideals in* k *prime to* $\mathfrak{m}$ *and* $S_{\mathfrak{m}}$ *is the group of all principal ideals generated by elements* $f \in k^*$ *such that* $f \equiv 1 \bmod \mathfrak{m}$.

Part II

0. In Part I we have concerned ourselves exclusively with the multiplicative structure of algebraic number fields. In order to take the additive structure of these fields also into account, we shall define "*variety over integers*" (Cf. [4]) analogously to the definition of algebraic varieties by J.-P. Serre [1] and generalize the concept of fibre space.

1. Let ν be a discrete valuation in any field K. We shall denote by $\mathfrak{o}_\nu$, $\mathfrak{p}_\nu$ and κ_ν the valuation ring, its maximal ideal and the residue field $\mathfrak{o}_\nu/\mathfrak{p}_\nu$. Let $F(X)$ be in the polynomial ring $\mathfrak{o}_\nu[X]$ of indeterminates (X) with coefficients in $\mathfrak{o}_\nu$. We shall denote by $\bar{F}^{(\nu)}(X)$ the polynomial in $\kappa_\nu[X]$ which is the class of $F(X)$ modulo $\mathfrak{p}_\nu$.

Let k be a field and N a set of infinitely many non-equivalent discrete valuations in k such that the following conditions are satisfied.

1) $\mathfrak{o} = \bigcap_{\nu \in N} \mathfrak{o}_\nu$ *is a Noetherean ring.*

2) k *is the quotient field of* $\mathfrak{o}$.

3) *Every element of* k *other than zero is* $\mathfrak{p}_\nu$*-unit for almost all* ν *in* N.

Let $\mathbf{K}$ be a universal domain over k (in Weil's sense [3]) and T a maximal subset of independent variables of $\mathbf{K}$ over k. We fix k, N, $\mathbf{K}$ and T once for all.

For any discrete valuation ν in k, there exists one and only one discrete valuation $\hat{\nu}$ in $k(T)$ which is a prolongation of ν such that all elements of T are $\mathfrak{p}_{\hat{\nu}}$-integral and their residue classes modulo $\mathfrak{p}_{\hat{\nu}}$ are also independent variables over the residue field $\mathfrak{o}_\nu+\mathfrak{p}_{\hat{\nu}}/\mathfrak{p}_{\hat{\nu}}$ which may be identified with $\kappa_\nu=\mathfrak{o}_\nu/\mathfrak{p}_\nu$. We denote by $\mathfrak{K}_\nu$ the algebraic closure of the residue field $\kappa_{\hat{\nu}}=\mathfrak{o}_{\hat{\nu}}/\mathfrak{p}_{\hat{\nu}}$ for each $\nu\in N$, then $\mathfrak{K}_\nu$ is a universal domain over κ_ν by the above identification of the subfield $\mathfrak{o}_\nu+\mathfrak{p}_{\hat{\nu}}/\mathfrak{p}_{\hat{\nu}}$ with $\kappa_\nu=\mathfrak{o}_\nu/\mathfrak{p}_\nu$ for every $\nu\in N$. We denote by S^n and $\mathfrak{S}^n_\nu$ the n-space over $\mathbf{K}$ and $\mathfrak{K}_\nu$ respectively.

2. An *N-set* is a set $\{\xi\}$ of elements with an associated function of the elements whose values are discrete valuations in N, the *ground discrete valuation* of ξ, denoted by ξ.

Any subset of an N-set is an N-set with the same ground discrete valuations. The *direct product* of any two N-sets $\mathfrak{U}$ and $\mathfrak{V}$, denoted by $\mathfrak{U}\times\mathfrak{V}$, is the set of all pairs (ξ,η) such that $\xi\in\mathfrak{U}$, $\eta\in\mathfrak{V}$ and $\xi=\eta$; we define the ground discrete valuation of (ξ,η) in $\mathfrak{U}\times\mathfrak{V}$ as follows: $(\xi,\eta)=\xi=\eta$. Then $\mathfrak{U}\times\mathfrak{V}$ is an N-set.

EXAMPLE. We denote by $\mathfrak{S}^n_N$, or simply by $\mathfrak{S}^n$, the set-theoretical direct sum of n-spaces $\mathfrak{S}^n_\nu$ for all $\nu\in N$. We define the ground discrete valuation of an element in $\mathfrak{S}^n_\nu$ to be ν. Then $\mathfrak{S}^n_N$ is an N-set. We may identify $\mathfrak{S}^m\times\mathfrak{S}^n$ with $\mathfrak{S}^{m+n}$ by the indentifications of the $\mathfrak{S}^m_\nu\times\mathfrak{S}^n_\nu$ with the $\mathfrak{S}^{m+n}_\nu$. $\mathfrak{S}^0$ may be identified with N.

Let $\mathfrak{U}$ and $\mathfrak{V}$ be two N-sets. An *N-mapping* of $\mathfrak{U}$ into $\mathfrak{V}$ is a mapping φ of $\mathfrak{U}$ into $\mathfrak{V}$ such that $\varphi(\xi)=\xi$ for all $\xi\in\mathfrak{U}$. By a *function* on an N-set $\mathfrak{U}$ we understand an N-mapping of $\mathfrak{U}$ into $\mathfrak{S}^1$.

We shall define the *sheaf* $\mathbf{F}(\mathfrak{U})$ *of germs of functions* on a non-empty N-set $\mathfrak{U}$ when $\mathfrak{U}$ is provided with a topology. Let $F_{\mathfrak{V}}$ be the ring of all functions on $\mathfrak{V}$ for any open subset $\mathfrak{V}$ of $\mathfrak{U}$ and $\rho_{\mathfrak{V}\mathfrak{V}'}$ the homomorphism of $F_{\mathfrak{V}'}$ into $F_{\mathfrak{V}}$ defined by the restrictions of the domains of definition of functions for each pair of non-empty open subsets $\mathfrak{V}$ and $\mathfrak{V}'$ of $\mathfrak{U}$ such that $\mathfrak{V}$ is contained in $\mathfrak{V}'$. Then the system $\{F_{\mathfrak{V}},\rho_{\mathfrak{V}\mathfrak{V}'}\}$ defines a sheaf $\mathbf{F}(\mathfrak{U})$ of rings $\mathbf{F}(\mathfrak{U})_\xi$ over $\mathfrak{U}$; $\mathbf{F}(\mathfrak{U})_\xi$ is the direct limit of $F_{\mathfrak{V}}$ where $\mathfrak{V}$ runs over all open subsets of $\mathfrak{U}$ containing ξ, for each $\xi\in\mathfrak{U}$.

It is easily seen that the canonical homomorphism of $F_{\mathfrak{V}}$ into the ring $\Gamma(\mathfrak{V},\mathbf{F}(\mathfrak{U}))$ of all sections of $\mathbf{F}(\mathfrak{U})$ on $\mathfrak{V}$ is an onto-isomorphism for every non-empty open subset $\mathfrak{V}$ of $\mathfrak{U}$, therefore we may identify the functions on $\mathfrak{V}$ with the sections of $\mathbf{F}(\mathfrak{U})$ on $\mathfrak{V}$ for every non-empty open subset $\mathfrak{V}$ of $\mathfrak{U}$. Any section f of $\mathbf{F}(\mathfrak{U})$ on a neighborhood of ξ in $\mathfrak{U}$ determines an element of $\mathbf{F}(\mathfrak{U})_\xi$; we denote by f_ξ this element and call f_ξ the *function element* of the function f at ξ. For any non-empty subset $\mathfrak{V}$ of $\mathfrak{U}$ we have the canonical homomorphism $\varepsilon_{\mathfrak{V}}$ of the sheaf, denoted by $\mathbf{F}(\mathfrak{U})\,|\,\mathfrak{V}$, induced by $\mathbf{F}(\mathfrak{U})$ on $\mathfrak{V}$ into $\mathbf{F}(\mathfrak{V})$ by the restrictions of the domains of definition of functions; if $\mathfrak{V}$ is open in $\mathfrak{U}$, then the homomorphism $\varepsilon_{\mathfrak{V}}$ of $\mathbf{F}(\mathfrak{U})\,|\,\mathfrak{V}$ into $\mathbf{F}(\mathfrak{V})$ is an onto-isomorphism.

Now we state a temporary definition. An *N-variety* is a non-empty N-set $\mathfrak{U}$ provided with a topology and a sheaf $\mathbf{O}$ of subrings $\mathbf{O}_\xi$ of $\mathbf{F}(\mathfrak{U})_\xi$ over $\mathfrak{U}$; $\mathbf{O}$ is said to be the *sheaf of germs of regular functions* on $\mathfrak{U}$ and a section of $\mathbf{O}$ on a non-empty open subset $\mathfrak{V}$ of $\mathfrak{U}$ is said to be *regular function* on $\mathfrak{V}$ which is a function on $\mathfrak{V}$ by the above identification.

Let $\mathfrak{U}$ and $\mathfrak{V}$ be two N-varieties. An N-mapping φ of $\mathfrak{U}$ into $\mathfrak{V}$ is said to be *regular* if the following conditions are satisfied.

1) *φ is continuous.*

2) *If ξ is in $\mathfrak{U}$ and f is a regular function on a neighborhood of $\varphi(\xi)$, then the function $f\circ\varphi$ is regular on some neighborhood of ξ.*

Moreover an N-mapping φ of $\mathfrak{U}$ onto $\mathfrak{V}$ is said to be *biregular* if f is one-to-one mapping of $\mathfrak{U}$ onto $\mathfrak{V}$ and the both φ and φ^{-1} are regular. Let $\mathfrak{V}$ be a non-empty subset of an N-variety $\mathfrak{U}$ which is an intersection of an open subset and a closed subset of $\mathfrak{U}$ and $\mathbf{O}_{\mathfrak{V}}$ the image of $\mathbf{O}\,|\,\mathfrak{V}$ by the canonical homomorphism $\varepsilon_{\mathfrak{V}}$ of $\mathbf{F}(\mathfrak{U})\,|\,\mathfrak{V}$ into $\mathbf{F}(\mathfrak{V})$. Then the N-variety $\mathfrak{V}$ with the sheaf $\mathbf{O}_{\mathfrak{V}}$ is said to be a *subvariety*[1] of $\mathfrak{U}$.

3. Let A be any subring of $\mathfrak{o}[T]$. We define a structure of N-variety on $\mathfrak{S}^n$ as follows. If $F(X)$ is a polynomial of n indeterminates (X) with coefficients in $\mathfrak{o}[T]$, we shall denote $\overline{F}^{(\nu)}(X)$ simply by $\overline{F}^{(\nu)}(X)$ and $\overline{F}^{(\nu)}(\xi)$ simply by $\overline{F}(\xi)$ if $(\xi)\in\mathfrak{S}^n$ and $(\xi)=\nu$. First we introduce into $\mathfrak{S}^n$ a topology in which the family of all the $\{(\xi);\,(\xi)\in\mathfrak{S}^n,\ \overline{F}(\xi)=0\}$ such that the $F(X)$ are in $A[X]$ is a base of all closed sets; we denote by ${}_A\mathfrak{S}^n$ the N-set $\mathfrak{S}^n$ provided with this topology.

Next we define a sheaf ${}_A\mathbf{O}^n$ of subrings ${}_A\mathbf{O}^n_\xi$ of $F({}_A\mathfrak{S}^n)_\xi$ over ${}_A\mathfrak{S}^n$ as follows. Let an element u of $\mathbf{F}({}_A\mathfrak{S}^n)_\xi$ be contained in ${}_A\mathbf{O}^n_\xi$ if there exist two polynomials $F(X)$ and $G(X)$ in $A[X]$ such that $\overline{G}(\xi)\neq 0$

[1] For any non-empty subset $\mathfrak{V}$ of an N-variety $\mathfrak{U}$ the structure of N-variety can be defined and the concept of regular mappings of $\mathfrak{V}$ into an N-variety also can be defined similarly.

and the function f; $\eta \to \bar{F}(\eta)/\bar{G}(\eta)$ defined on some neighborhood of ξ determines the function element $f_\xi = u$ at ξ. Thus we have defined an N-variety ${}_A\mathfrak{S}^n$ provided with the sheaf ${}_A\mathbf{O}^n$; we call this N-variety the *affine n-N-space* provided with *A-structure*. If A is the ring $\mathfrak{o}[\boldsymbol{T}]$, then we shall omit the term "$A-$".

A subvariety $\mathfrak{U}$ of $\mathfrak{S}^n$ is said to be an *affine N-variety* and $\mathfrak{S}^n$ to be the *ambient N-space* for $\mathfrak{U}$, if $\mathfrak{U}$ is identical with a subvariety of ${}_A\mathfrak{S}^n$, denoted by ${}_A\mathfrak{U}$, as a point set for some subring A of $\mathfrak{o}[\boldsymbol{T}]$ finitely generated over $\mathfrak{o}$; ${}_A\mathfrak{U}$ is said to be an affine N-variety *provided with A-structure* and $\mathfrak{U}$ to be *defined over A*.

DEFINITION. *A prealgebraic N-variety is an N-variety* $\mathfrak{U}$ *such that the following condition* (I) *is satisfied.*

(I) *There exist a finite open covering* $\{\mathfrak{U}_i\}$ *of* $\mathfrak{U}$ *and a biregular mapping* φ_i *of* $\mathfrak{U}_i$ *onto an affine N-variety* $\mathfrak{V}_i$ *for every i.*

We call a pair of an open subvariety $\mathfrak{U}_0$ of $\mathfrak{U}$ and a biregular mapping φ of $\mathfrak{U}_0$ onto an affine N-variety a *coordinate system*; a coordinate system $(\mathfrak{U}_0, \varphi)$ is said to be *defined over A* if $\varphi(\mathfrak{U}_0)$ is defined over A. If suitable systems $\{(\mathfrak{U}_i, \varphi_i)\}$ defined over A satisfy (I), we say that the prealgebraic N-variety $\mathfrak{U}$ is *defined over A* and A is a *ring of definition for* $\mathfrak{U}$; any prealgebraic N-variety is defined over some subring A of $\mathfrak{o}[\boldsymbol{T}]$ finitely generated over $\mathfrak{o}$. For any prealgebraic N-variety $\mathfrak{U}$ defined over A, there exists one and only one structure of N-variety on $\mathfrak{U}$, denoted by ${}_A\mathfrak{U}$, such that for every coordinate system $(\mathfrak{U}_0, \varphi)$ of $\mathfrak{U}$ defined over A, $\mathfrak{U}_0$ is open in ${}_A\mathfrak{U}$ and φ is a biregular mapping of $\mathfrak{U}_0$ provided with the structure of the open subvariety of ${}_A\mathfrak{U}$ onto the affine N-variety ${}_A\varphi(\mathfrak{U}_0)$ provided with A-structure. We denote by ${}_A\mathbf{O}$ the sheaf of germs of regular functions on ${}_A\mathfrak{U}$ if $\mathbf{O}$ is the sheaf of germs of regular functions on $\mathfrak{U}$; ${}_A\mathbf{O}_\xi$ may be identified with a subring of $\mathbf{O}_\xi$ for every ξ in $\mathfrak{U}$.

Let $\mathfrak{U}$ and $\mathfrak{V}$ two prealgebraic N-varieties defined over A and φ an N-mapping of $\mathfrak{U}$ into $\mathfrak{V}$. If φ is a regular mapping of ${}_A\mathfrak{U}$ into ${}_A\mathfrak{V}$, then φ is a regular mapping of $\mathfrak{U}$ into $\mathfrak{V}$; such a regular mapping $\mathfrak{U}$ into $\mathfrak{V}$ is said to be *defined over A*. Let $\mathfrak{V}$ be a non-empty open subset of a prealgebraic N-variety $\mathfrak{U}$ and f a function on $\mathfrak{V}$. Then f is a regular function on ${}_A\mathfrak{V}$ if and only if f is a regular mapping of ${}_A\mathfrak{V}$ into ${}_A\mathfrak{S}^1$. Any regular function f on $\mathfrak{V}$ is said to be *defined over A* if f is regular on ${}_A\mathfrak{V}$.

Let $\mathfrak{U}$ and $\mathfrak{V}$ be any two prealgebraic N-varieties such that $\mathfrak{U} \times \mathfrak{V}$ is non-empty. Then there exists one and only one structure of prealgebraic N-variety on the direct product $\mathfrak{U} \times \mathfrak{V}$ such that, for every pair of coordinate systems $(\mathfrak{U}_0, \varphi)$ and $(\mathfrak{V}_0, \psi)$ of $\mathfrak{U}$ and $\mathfrak{V}$,

$(\mathfrak{U}_0\times\mathfrak{V}_0,\ \varphi\times\psi)$ is a coordinate system in $\mathfrak{U}\times\mathfrak{V}$. If a prealgebraic N-variety $\mathfrak{U}$ satisfy the following additional condition (II), then we say that $\mathfrak{U}$ is an *algebraic N-variety.*

(II) *The diagonal subset* $\Delta_{\mathfrak{U}}$ *of* $\mathfrak{U}\times\mathfrak{U}$ *is closed in* $\mathfrak{U}\times\mathfrak{U}$.

It is easily seen that the direct product of any two algebraic N-varieties is also an algebraic N-variety or empty and any affine N-variety is an algebraic N-variety.

4. Let $\mathfrak{U}$ be an algebraic N-variety defined over A. If $\mathfrak{U}$ is *irreducible,* that is, any two non-empty open subsets always intersect with each other, then we can define the rational function on $\mathfrak{U}$ as follows: It is easily seen that the ring $\Gamma(\mathbf{O}, \mathfrak{V})$ is an integral domain for every non-empty open subset $\mathfrak{V}$ of $\mathfrak{U}$; we denote by $R_{\mathfrak{V}}$ the quotient field of $\Gamma(\mathbf{O}, \mathfrak{V})$. The natural homomorphism $\rho_{\mathfrak{V}\mathfrak{V}'}$ of $\Gamma(\mathbf{O}, \mathfrak{V}')$ into $\Gamma(\mathbf{O}, \mathfrak{V})$ induces an onto-isomorphism $\bar{\rho}_{\mathfrak{V}\mathfrak{V}'}$ of $R_{\mathfrak{V}'}$ onto $R_{\mathfrak{V}}$ for each pair of non-empty open subsets $\mathfrak{V}$, $\mathfrak{V}'$ such that $\mathfrak{V}\subset\mathfrak{V}'$, and the system $\{R_{\mathfrak{V}}, \bar{\rho}_{\mathfrak{V}\mathfrak{V}'}\}$ defines a simple sheaf $\mathbf{R}(\mathfrak{U})$ over $\mathfrak{U}$; we may identify the field $R(\mathfrak{U})=\Gamma(\mathbf{R}(\mathfrak{U}), \mathfrak{U})$ with the $\mathbf{R}(\mathfrak{U})_\xi$. Moreover we may canonically identify $\mathbf{O}_\xi$ with a subring of $\mathbf{R}(\mathfrak{U})_\xi$ and therefore may identify $\mathbf{O}_\xi$ with a subring of $R(\mathfrak{U})$; we call an element of the field $R(\mathfrak{U})$ a *rational function* on $\mathfrak{U}$. $\mathbf{R}(\mathfrak{U})_\xi$ is the quotient field of $\mathbf{O}_\xi$; we denote by ${}_A\mathbf{R}(\mathfrak{U})_\xi$ the quotient field of ${}_A\mathbf{O}_\xi$ in $\mathbf{R}(\mathfrak{U})_\xi$ and denote by ${}_A\mathbf{R}(\mathfrak{U})$ the sheaf of rings ${}_A\mathbf{R}(\mathfrak{U})_\xi$ over ${}_A\mathfrak{U}$. The field ${}_AR(\mathfrak{U})=\Gamma({}_A\mathbf{R}(\mathfrak{U}), {}_A\mathfrak{U})$ may be identified with a subfield of $R(\mathfrak{U})$; a rational function in ${}_AR(\mathfrak{U})$ is said to be *defined over A.*

EXAMPLE. Let k be the field of all rational numbers and N the set of all non-equivalent non-archimedean valuations denoted by prime rational integers, $p, q, \cdots$. Then we call a N-variety "*Z-variety*" and shall generally use the term "*Z-*" instead of "*N-*". Moreover we denote by Z the ring of all rational integers. Let K be any algebraic number field of a finite degree and $Z[\omega]$ the ring of all integers in K where (ω) is in some S^n. We define an affine Z-variety $\mathfrak{U}_{(\omega)}$ in $\mathfrak{S}^n$ to be $\{(\xi);\ \bar{F}(\xi)=0$ for all $F(X)\in Z[X]$ such that $F(\omega)=0\}$. Then we see that $\mathfrak{U}_{(\omega)}$ is defined over Z and is irreducible and the field ${}_ZR(\mathfrak{U}_{(\omega)})$ of rational functions on $\mathfrak{U}_{(\omega)}$ defined over Z is isomorphic to K. Moreover we see that if we denote by (p) the subvariety of $\mathfrak{S}^n$ defined by the equation $p=0$, then the number of irreducible components of ${}_Z\mathfrak{U}_{(\omega)}\frown(p)$ is equal to the number of discrete valuations in K which are prolongations of p. Furthermore let L be a finite extension of K, $Z[\omega, \eta]$ the ring of all integers in L where (η) is in some S^m and $\mathfrak{U}_{(\omega,\eta)}$ the affine Z-variety in $\mathfrak{S}^n\times\mathfrak{S}^m$ defined by (ω, η) as above; we denote by π the projection of $\mathfrak{S}^n\times\mathfrak{S}^m$ onto $\mathfrak{S}^n$. Then

π maps $\mathfrak{U}_{(\omega,\eta)}$ onto $\mathfrak{U}_{(\omega)}$ and for any irreducible component $\mathfrak{p}$ of ${}_Z\mathfrak{U}_{(\omega)}\frown(p)$, $\pi^{-1}(\mathfrak{p})$ has the irreducible components $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_g$ where g is the number of discrete valuations in L which are prolongations of the discrete valuation in K corresponding to $\mathfrak{p}$.

5. Let $\mathfrak{G}$ be an algebraic N-variety and ν in N. Then we shall denote by $\mathfrak{G}_\nu$ the set of all those elements in $\mathfrak{G}$ whose ground discrete valuation is ν. Now let $\mathfrak{G}_\nu$ be provided with a structure of group or empty for every ν in N, and then we define the mapping of $\mathfrak{G}\times\mathfrak{G}$ onto $\mathfrak{G}$ which coincides with the group operation $(g, g')\to gg'$ on $\mathfrak{G}_\nu\times\mathfrak{G}_\nu$ for every ν in N and the mapping of $\mathfrak{G}$ onto itself which coincides with the inversion mapping on $\mathfrak{G}_\nu$. We denote by 1_ν the identity of G_ν. If the N-mapping $\nu\to 1_\nu$ is regular[1] wherever 1_ν is defined and the above N-mappings $\mathfrak{G}\times\mathfrak{G}\to\mathfrak{G}$ and $\mathfrak{G}\to\mathfrak{G}$ are regular, then we say that $\mathfrak{G}$ is an *algebraic group N-variety*.

DEFINITION. *A principal fibre N-space is a collection as follows:*

1) *an algebraic N-variety* $\mathfrak{B}$,

2) *an algebraic N-variety* $\mathfrak{S}$, *called the base N-variety,*

3) *a regular mapping* π *of* $\mathfrak{B}$ *onto* $\mathfrak{S}$,

4) *an algebraic group N-variety* $\mathfrak{G}$ *which operates on* $\mathfrak{B}$.

Assume that there exist a finite open covering $\{\mathfrak{U}_i\}$ *of* $\mathfrak{S}$ *and a biregular mapping* Φ_i *of* $\mathfrak{U}_i\times\mathfrak{G}$ *onto* $\pi^{-1}(\mathfrak{U}_i)$ *for each i such that*

$$\pi(\Phi_i(\xi, g))=\xi \quad \textit{for all} \quad (\xi, g)\in\mathfrak{U}_i\times\mathfrak{G},$$
$$\Phi_i(\xi, g)g'=\Phi_i(\xi, gg') \quad \textit{for all} \quad (\xi, g, g')\in\mathfrak{U}_i\times\mathfrak{G}\times\mathfrak{G}.$$

We can also define general (non-principal) fibre N-space analogously to the case of W-variety (Cf. [6]).

EXAMPLE. Let $\mathfrak{S}$ be the affine Z-variety $\mathfrak{U}_{(\omega)}$ defined in 4. and $\mathfrak{G}$ the open subvariety of $\mathfrak{S}^1$ defined by the equation $X\neq 0$; $\mathfrak{G}$ is an algebraic group Z-variety. Then *classes of isomorphic principal fibre Z-spaces of the group* $\mathfrak{G}$ *over* $\mathfrak{S}$ *correspond to all ideal classes of* ${}_ZR(\mathfrak{U}_{(\omega)})=K$. In order to prove this fact we define an analogue $\mathfrak{P}^n$ of the projective n-space and treat sections of fibre space of the fibre $\mathfrak{P}^1$ and of the above group Z-variety $\mathfrak{G}$ over $\mathfrak{U}_{(\omega)}$ analogously to the case of W-variety (Cf. [6]).

Moreover we can generalize this result to the case of the group Z-variety $GL(n, \mathfrak{S}^1)$ (an analogue of $GL(n, k)$) so that we have the concept of generalized ideal class analogously to the case of an algebraic curve over the complex number field (Cf. [2]).

In the above example we have not treated any archimedean prime of a number field. In order to supplement this point it seems necessary to clarify the relation between the algebraic varieties over rational numbers and the algebraic Z-varieties, especially in the opposite direction to the process of "reduction modulo $\mathfrak{p}$ for all discrete valuation $\mathfrak{p}$".

UNIVERSITY OF TOKYO

BIBLIOGRAPHY

[1] J.-P. Serre, Faisceaux algébriques cohérents, Ann. of Math., **61** (1955), pp. 197–278.

[2] A. Weil, Généralisation des fonctions abéliennes, Jour. Math. pures et appl., **17** (1938), pp. 47–87.

[3] A. Weil, Foundations of algebraic geometry, (1946).

[4] A. Weil, Number theory and algebraic geometry, Proc. Int. Con. Math. (1950), Vol. 2, pp. 90–100.

[5] A. Weil, Fibre spaces in algebraic geometry, Lecture notes at University of Chicago, (1952).

[6] K. Yamazaki, On fibre spaces in the algebraic number theory, Jour. Math. Soc. Japan, **7** (1955), pp. 182–201.

Units of Fixed Points in Involutorial Algebras

K. G. RAMANATHAN

§ 1. Let A be a simple algebra of finite rank over the field Γ of rational numbers. Let A have an involutorial anti-automorphism $*$ so that

$$(\alpha+\beta)^*=\alpha^*+\beta^*,\ (\alpha\beta)^*=\beta^*\alpha^*,\ (\alpha)^{**}=\alpha. \qquad (1)$$

An element ξ of A is said to be a *fixed point* under the involution if $\xi=\xi^*$. ξ is also then said to be *symmetric*. If $\xi=-\xi^*$ we call ξ *skew symmetric*.

Let $\mathfrak{O}$ be an order in A relative to the ring of rational integers. An element u in $\mathfrak{O}$ is said to be a *unit* if u and u^{-1} belong to $\mathfrak{O}$. u is said to be a unit of the fixed point ξ if $u^*\xi u=\xi$. The units of ξ obviously form a group $\Gamma(\xi)$, called the unit group of ξ. The object of this note is to outline proofs of two theorems, the first one being

THEOREM 1. *Let ξ be symmetric or skew symmetric and let norm of ξ over Γ be not zero. Then $\Gamma(\xi)$ has a finite set of generators.*

In order to prove this one has to develop first the reduction theory of positive forms over a semi-simple algebra over $\bar{\Gamma}$, the field of real numbers.

§ 2. Let Δ be a division algebra of finite rank g over Γ. Let Z be its centre so that $(Z:\Gamma)=h$, $(\Delta:Z)=s^2$ and $g=hs^2$. Let $\bar{\Delta}$ denote the Kronecker product $\Delta\otimes\bar{\Gamma}$. By taking a basis, called normal basis, of $\bar{\Delta}/\bar{\Gamma}$ constituted by the simple components of the semi-simple algebra $\bar{\Delta}$, any element ξ in $\bar{\Delta}$ can be represented by the g rowed matrix

$$\check{\xi}=\begin{pmatrix} x_1 & & & \\ & x_2 & & \\ & & \ddots & \\ & & & \cdot \end{pmatrix} \qquad (2)$$

consisting of blocks of real, complex and quaternion matrices, complex numbers and quaternions being represented respectively by 2 rowed and 4 rowed real matrices. The matrix algebra of regular representation has the involution $\check{\xi}\to\check{\xi}'$, $'$ denoting the transposed of a matrix.

We say ξ in $\bar{\Delta}$ is *positive* and denote $\xi>0$ if 1) $\check{\xi}=\check{\xi}'$ and 2) the characteristic roots of ξ are all positive.

Let $\mathfrak{o}$ be an order in Δ relative to Γ and let $\delta_1,\cdots,\delta_g$ be a minimal base of $\mathfrak{o}$ over Γ. $\delta_1,\cdots,\delta_g$ is also a base of $\bar{\Delta}/\bar{\Gamma}$. For $\xi\in\bar{\Delta}$ let $\hat{\xi}$ denote the matrix representing ξ by means of the regular representation with regard to the basis $\delta_1,\cdots,\delta_g$. Then there exists a g-rowed matrix γ with elements in $\bar{\Gamma}$ such that

$$\hat{\xi}=\gamma^{-1}\check{\xi}\gamma. \qquad (3)$$

If ξ^* is the element in $\bar{\Delta}$ such that $\hat{\xi}^*=\gamma^{-1}\check{\xi}'\gamma$ then $\xi\to\xi^*$ is an involution in' $\bar{\Delta}$. If $\mathrm{A}=\mathfrak{M}_n(\Delta)$ is the algebra of square matrices over Δ the involution $\xi\to\xi^*$ in Δ can be extended to $\bar{A}=A\otimes\bar{\Gamma}$ in a trivial way. An element $S=(a_{kl})$ in $\bar{A}$ is said to be *positive* if $S=S^*$ and all the characteristic roots of S are positive. The set P of positive matrices of S constitutes a symmetric Riemannian space of $(hns+r_1-r_3)\cdot n\cdot s/2$ real dimensions, (with obvious meanings for r_1 and r_3) and with the metric $ds^2=\sigma(S^{-1}\cdot dS\cdot S^{-1}\cdot dS)$.

Let $\mathfrak{O}$ denote the order in A constituted by matrices V with elements in $\mathfrak{o}$. V is a unit of $\mathfrak{O}$ if V and V^{-1} belong to it. The unit group $\Gamma(\mathfrak{O})$ is represented in P as a discontinuous group of mappings $S\to S[V]=V^*SV$. One can, by a combination of the methods of Siegel and Weyl construct a fundamental region R in P for $\Gamma(\mathfrak{O})$.

§ 3. Let now Δ be an involutorial division algebra with an involution $(*)$. On Z, the centre of Δ, $*$ is an automorphism, so either $*$ leaves Z fixed or there is a subfield Z_0 of Z with $(Z:Z_0)=2$ which is left fixed. Accordingly the involution is said to be of the first or the second kind. For the sake of simplicity, we consider only involutions of the first kind. Albert has shown that in this case $\Delta=Z$ or is a quaternion algebra over Z. Since the first case has already been studied by us, let us consider the case where Δ is a quaternion algebra over Z. Let Z_i be a completion of Z by an archimedian valuation of Z and put $\Delta_i=\Delta\otimes Z_i$. The involution $*$ in Δ can be trivially extended to Δ_i. But Δ_i itself has an involution as can be easily seen. If $X\in\Delta_i$ then X and X^* can have the following three forms

$$\left.\begin{array}{ll} X=\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}, & X^*=V^{-1}X'V \\ X=\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}, & X^*=V^{-1}\underline{X}'V \\ X=x, & X^*=x' \end{array}\right\} \qquad (4)$$

where $V=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and the bar below means that the complex conjugate matrix is taken. The three cases occur according as Z_i is the completion of Z at a real infinite prime spot at which $\varDelta$ is unramified, complex infinite prime spot, or real infinite prime spot at which $\varDelta$ is ramified.

Let $S=S^*$ be an element of the matrix algebra $A=\mathfrak{M}_n(\varDelta)$ and let S be non-singular. We associate with S a topological space $\mathfrak{H}$ in the following manner: Consider $\bar{A}_i=A\otimes Z_i$. Then we can write $S=C_i^* C_i$ for every i such that $\varDelta$ is unramified at Z_i. If $\varDelta$ is ramified Z_i, then $S=C_i^*\begin{pmatrix} E_{p_i} & 0 \\ 0 & -E_{q_i} \end{pmatrix} C_i$ where E_r denotes the unit matrix of order r. Let now H_0 denote the positive matrix

$$H_0=\begin{pmatrix} H_1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & \cdot \\ & & & & H_t \end{pmatrix} \qquad (5)$$

where $H_i=C_i'C_i$. Let H denote the matrix in $\bar{A}$ obtained by taking the components in (5) each taken s times $(s^2=(\varDelta:Z))$. Then H is a positive matrix in $\bar{A}$ in the sense of § 2. $\mathfrak{H}$ is now the space constituted by the different H. It can be shown that $\mathfrak{H}$ again is a symmetric Riemannian space with the metric $ds^2=\sigma(H^{-1}dH\cdot H^{-1}dH)$. Let $d\omega$ denote the volume element corresponding to this metric. A simple calculation shows that $\mathfrak{H}$ has the topological dimension,

$$r_1 n(n+1)+2r_2 n^2+4\sum_{i=1}^{r_3} p_i q_i.$$

Let us denote by S itself the matrix corresponding to S by the regular representation of $\bar{A}$ over $\bar{\Gamma}$. The matrices $V\in\bar{A}$ satisfying

$$V^*SV=S$$

constitute the *orthogonal group* $\Omega(S)$ of S. It has a representation $H\rightarrow V'HV$ in the $\mathfrak{H}$ space. The unit group $\Gamma(S)$ of S constituted by matrices V in A with elements in $\mathfrak{o}$ is a discontinuous subgroup of $\Omega(S)$. One can construct by using the ideas in § 2 a fundamental region F for $\Gamma(S)$ in $\mathfrak{H}$. The properties of F show the truth of theorem 1 in the case S is symmetric. If S is skew symmetric we follow again the same method. The computations here are slightly more cumbersome if n is odd than if n is even.

The second theorem concerns the measure of F measured with $d\omega$. The theorem is

THEOREM 2. *If S is non-singular and is either symmetric or skew symmetric*

$$\int_F d\omega$$

is finite except for a trivial case.

The proof of this is rather long and depends on ideas which have been developed recently by Siegel. Detailed proofs of these theorems will appear later.

We remark that in the statement of theorem 1 we had not stipulated any condition on the involution. But in the proof above we had considered a special involution which arises from an involution in the division algebra. By the results of Albert one can show that this is no restriction of generality.

The integers (p_i, q_i) which occur in the definition of H_i in (5) are said to form a *system of signatures* of S.

TATA INSTITUTE OF FUNDAMENTAL RESEARCH,
BOMBAY, INDIA

REFERENCES

[1] A. A. Albert: Structure of Algebras, New York, 1939.

[2] K. G. Ramanathan: Units of quadratic forms, Annals of Math., **56** (1952) pp. 1–10.

[3] C. L. Siegel: Discontinuous groups, Annals of Math., **44** (1943), pp. 674–689.

[4] C. L. Siegel: Indefinite quadratische Formen und Funktionentheorie II, Math. Annalen, **124** (1952), pp. 364–387.

[5] H. Weyl: Fundamental domains for lattice groups in division algebras, Festschrift. A. Speiser, Zürich, 1945.

On Siegel's Modular Functions

Ichiro SATAKE

Introduction.

Let $\mathfrak{H}_n$ be the generalized upper half-plane of degree n, namely the space of all complex symmetric matrices $Z=X+iY$ of degree n with the imaginary parts $Y>0$, and M_n be the modular group of degree n operating on $\mathfrak{H}_n$. Siegel's modular function $F(Z)$ is an analytic function on $\mathfrak{H}_n$ invariant under the modular transformations $\sigma \in M_n$, so that it may be regarded as a function defined on the quotient space $M_n \backslash \mathfrak{H}_n$. But $M_n \backslash \mathfrak{H}_n$ is not compact and it was reasonable that Siegel defined modular function as a quotient of two modular forms which are regular even in the points at infinity in the sense that they possess convergent regular Fourier expansions.

To clarify the behaviors of modular functions in such points at infinity of $M_n \backslash \mathfrak{H}_n$, let us first introduce the notion of complex analytic manifold with ramifications or briefly V-manifold. A V-manifold $\mathfrak{V}$ is, roughly spoken, a topological space such that each point $p \in \mathfrak{V}$ has a system of neighbourhoods U_p homeomorphic to the quotient spaces $G_p \backslash \tilde{U}_p$, $\tilde{U}_p$ being domains in the complex n-space C^n, G_p finite groups of analytic automorphisms of $\tilde{U}_p$, and these systems of $\tilde{U}_p$, G_p and the maps φ_p from $\tilde{U}_p$ onto U_p satisfying some consistency conditions. On such a V-manifold we can define without any difficulties the notions of differential forms, holomorphic or meromorphic functions, divisors, ...etc and translate the usual theories of them in our case. Especially we can prove de Rham's theorem and if the V-manifold is compact Poincaré's duality theorem on Betti groups.

Now the quotient space $\mathfrak{V}_n = M_n \backslash \mathfrak{H}_n$ is of course a V-manifold. It is very plausible that by joining some V-manifolds of lower dimensions $\mathfrak{V}_n$ can be completed to a compact V-manifold $\bar{\mathfrak{V}}_n$. In §§3–5 we shall actually carry out this compactification in the case of $n=2$. For that purpose we shall use some sorts of theta-functions as the uniformizing parameters at the point at infinity.

After these preparations the modular functions of degree n can be defined (at least in the case of $n=2$) simply as meromorphic functions on $\bar{\mathfrak{V}}_n$. Also the modular forms of degree n of weight m can be regarded as sections of faisceau $\mathcal{A}_m$ of germs of automorphic forms of weight m on $\bar{\mathfrak{V}}_n$. This faisceau $\mathcal{A}_m$ being a coherent analytic faisceau, it would be possible to apply the theory recently developed by Serre [3] to $\mathcal{A}_m$, if $\bar{\mathfrak{V}}_n$ were proved to be a projective variety. Then the formula of dimension of the space of modular forms would be obtained, which is of particular importance for the arithmetic theory of quadratic forms. But we could not decide whether it is possible or not.

§1. The definition of V-manifold.

Let $\mathfrak{V}$ be a (Hausdorff) topological space. A *local uniformizing system* (abbreviated in the following as l.u.s.) $\{\tilde{U}, G, \varphi\}$ for an open set U in $\mathfrak{V}$ is by definition a collection of the following objects:

$\tilde{U}$: a domain in the complex n-space C^n,

G: a finite group of analytic automorphisms of $\tilde{U}$,

φ: a continuous map from $\tilde{U}$ onto U such that $\varphi\circ\sigma=\varphi$ for all $\sigma\in G$, so that it induces a map from the quotient space $G\backslash\tilde{U}$ onto U, which we shall assume to be a homeomorphism.

Two l.u.s. $\{\tilde{U}, G, \varphi\}$, $\{\tilde{U}', G', \varphi'\}$ are said to be *equivalent*, if there exists an analytic isomorphism λ from $\tilde{U}$ onto $\tilde{U}'$ such that

$$G'=\lambda\circ G\circ\lambda^{-1}, \qquad \varphi'=\varphi\circ\lambda^{-1}.$$

Then λ is called an *isomorphism* from $\{\tilde{U}, G, \varphi\}$ onto $\{\tilde{U}', G', \varphi'\}$. More generally we shall call an *injection* from $\{\tilde{U}, G, \varphi\}$ into $\{\tilde{U}', G', \varphi'\}$ an analytic isomorphism λ from $\tilde{U}$ onto an open submanifold of $\tilde{U}'$ such that for any $\sigma\in G$ there exists $\sigma'\in G'$ satisfying the relation $\lambda\circ\sigma=\sigma'\circ\lambda$ (then σ' is uniquely determined by σ) and that $\varphi=\varphi'\circ\lambda$. Of course such an injection exists only if $U=\varphi(\tilde{U})$ is contained in $U'=\varphi'(\tilde{U}')$.

LEMMA 1. *Let λ be an injection from $\{\tilde{U}, G, \varphi\}$ into $\{\tilde{U}', G', \varphi'\}$. If $\sigma'(\lambda(\tilde{U}))\frown\lambda(\tilde{U})\neq\phi$ for an element $\sigma'\in G'$, then $\sigma'(\lambda(\tilde{U}))=\lambda(\tilde{U})$. Denoting by G_1' the subgroup of G' consisting of all such $\sigma'\in G'$, G is isomorphic to G_1' by the correspondence $\sigma\to\sigma'$ defined by the relation $\lambda\circ\sigma=\sigma'\circ\lambda$.*

PROOF. Assume that $\sigma'(\lambda(\tilde{U}))\frown\lambda(\tilde{U})\neq\phi$. Then there exist $\tilde{p}, \tilde{q}\in\tilde{U}$ such that $\sigma'\circ\lambda(\tilde{p})=\lambda(\tilde{q})$. Then, since $\varphi(\tilde{p})=\varphi(\tilde{q})$, we have $\tau(\tilde{p})=\tilde{q}$ for some $\tau \in G$. By the definition there exists $\tau' \in G'$ such that $\lambda \circ \tau = \tau' \circ \lambda$. Hence we have $\sigma'(\lambda(\tilde{p})) = \tau'(\lambda(\tilde{p}))$. As the fixed points of G' in $\tilde{U}'$ form a submanifold of $\tilde{U}'$ of complex dimension less than n, we can assume that $\lambda(\tilde{p})$ is not a fixed point of G'. Then we have $\sigma' = \tau'$ and so $\sigma'(\lambda(\tilde{U})) = \lambda(\tau(\tilde{U})) = \lambda(\tilde{U})$. We have proved at the same time that $\sigma' \in G'$ such that $\sigma'(\lambda(\tilde{U})) = \lambda(\tilde{U})$ belongs to the image of the correspondence $\sigma \to \sigma'$, which is clearly an isomorphism of G into G'. The remainder of the lemma is now obvious.

LEMMA 2. *Let λ, μ be two injections from $\{\tilde{U}, G, \varphi\}$ into $\{U', G', \varphi'\}$. Then there exists a uniquely determined $\sigma' \in G'$, such that $\mu = \sigma' \circ \lambda$.*

PPOOF. Let $\tilde{p} \in \tilde{U}$. As we have $\varphi'(\mu(\tilde{p})) = \varphi(\tilde{p}) = \varphi'(\lambda(\tilde{p}))$, there exists $\sigma' \in G'$ such that $\mu(\tilde{p}) = \sigma'(\lambda(\tilde{p}))$. Choosing $\lambda(\tilde{p})$ not to be a fixed point of G', the automorphism $\sigma' \in G'$ is uniquely determined. As the set of non-fixed points of G' in $\lambda(\tilde{U})$ is connected and everywhere dense in $\lambda(\tilde{U})$, the same relation holds for all $\tilde{p} \in \tilde{U}$. Hence $\mu = \sigma' \circ \lambda$ for a uniquely determined $\sigma' \in G'$, q.e.d.

Now let λ be an injection from $\{\tilde{U}, G, \varphi\}$ into $\{\tilde{U}', G', \varphi'\}$ and λ' be one from $\{\tilde{U}', G', \varphi'\}$ into $\{\tilde{U}'', G'', \varphi''\}$. Then we can see easily that $\lambda' \circ \lambda$ is an injection from $\{\tilde{U}, G, \varphi\}$ into $\{\tilde{U}'', G'', \varphi''\}$. In particular, let λ be an injection from $\{\tilde{U}, G, \varphi\}$ into $\{\tilde{U}', G', \varphi'\}$ and λ' one from $\{\tilde{U}', G', \varphi'\}$ into $\{\tilde{U}, G, \varphi\}$. Then, $\lambda' \circ \lambda$ being an injection from $\{\tilde{U}, G, \varphi\}$ into itself, we have by Lem. 1 $\lambda' \circ \lambda = \sigma$ for some $\sigma \in G$ and similarly $\lambda \circ \lambda' = \sigma'$ for some $\sigma' \in G'$. Then it follows that $\lambda \circ \sigma = \sigma' \circ \lambda$, and that $(\sigma^{-1} \circ \lambda') \circ \lambda = 1$, $\lambda \circ (\sigma^{-1} \circ \lambda') = 1$. Thus λ being an isomorphism, $\{U, G, \varphi\}$ and $\{U', G', \varphi'\}$ are equivalent.

That being said, we shall give the definition of V-manifold.

DEFINITION. *A V-manifold is a composite concept formed of a topological space $\mathfrak{V}$ and a family $\mathfrak{F}$ of l.u.s. for open subsets in $\mathfrak{V}$ satisfying the following conditions.*

(1) *If $\{\tilde{U}, G, \varphi\}$, $\{\tilde{U}', G', \varphi'\} \in \mathfrak{F}$ and $U = \varphi(\tilde{U})$ is contained in $U' = \varphi'(\tilde{U}')$, then there exists an injection from $\{\tilde{U}, G, \varphi\}$ into $\{\tilde{U}', G', \varphi'\}$.*

(2) *The uniformized open sets, namely the open sets U for which there exist l.u.s. $\{\tilde{U}, G, \varphi\}$ in $\mathfrak{F}$, form a basis of open sets in $\mathfrak{V}$.*

By what we have mentioned above, two l.u.s. in $\mathfrak{F}$ for one and the same open set in $\mathfrak{V}$ are always equivalent by the condition (1).

Also if $\{\tilde{U}, G, \varphi\}$, $\{\tilde{U}', G', \varphi'\}$, $\{\tilde{U}'', G'', \varphi''\}$ are l.u.s. in $\mathfrak{F}$ such that $\varphi(\tilde{U})\subset\varphi'(\tilde{U}')\subset\varphi''(\tilde{U}'')$, then the injection from $\{\tilde{U}, G, \varphi\}$ into $\{\tilde{U}'', G'', \varphi''\}$ is given by the composition of those from $\{\tilde{U}, G, \varphi\}$ into $\{\tilde{U}', G', \varphi'\}$ and from $\{\tilde{U}', G', \varphi'\}$ into $\{\tilde{U}'', G'', \varphi''\}$.

Two families $\mathfrak{F}$, $\mathfrak{F}'$ of l.u.s. are said to be *equivalent* if $\mathfrak{F}\smile\mathfrak{F}'$ satisfies the condition (1). Equivalent families are regarded to define one and the same V-manifold structure on the space $\mathfrak{V}$. In the following, when we are concerned with a V-manifold $\mathfrak{V}$, we shall consider exclusively l.u.s. in the family $\mathfrak{F}$ defining the V-manifold structure of $\mathfrak{V}$; so we shall call them simply l.u.s. of $\mathfrak{V}$.

Let $\mathfrak{V}$ be a V-manifold and $p\in\mathfrak{V}$. For a l.u.s. $\{\tilde{U}, G, \varphi\}$ for $U\ni p$, take a $\tilde{p}\in\tilde{U}$ such that $\varphi(\tilde{p})=p$. Then for any l.u.s. $\{\tilde{U}_p, G_p, \varphi_p\}$ for U_p such that $p\in U_p\subset U$, there exists an injection λ from $\{\tilde{U}_p, G_p, \varphi_p\}$ into $\{\tilde{U}, G, \varphi\}$ such that $\tilde{p}\in\lambda(\tilde{U}_p)$. It follows from Lemma 1 that for sufficiently small U_p the inverse image $\varphi_p^{-1}(p)$ of p consists of only one point and the group G_p is isomorphic to the isotropy group of $\tilde{p}$ in G. Such a l.u.s. $\{\tilde{U}_p, G_p, \varphi_p\}$ is called a *sufficiently small* l.u.s. around p. For such a l.u.s. $\{\tilde{U}_p, G_p, \varphi_p\}$ the group structure of G_p is uniquely determined by p so that we shall call G_p simply the *isotropy group* of p.

The ordinary complex analytic manifold is nothing other than a V-manifold for which the isotropy group of each point reduces to the unity group. On a V-manifold $\mathfrak{V}$, the set $\mathfrak{X}$ of all ramified points, namely the points where the isotropy groups are not trivial, forms a subvariety of complex dimension less than n.[1] $\mathfrak{V}-\mathfrak{X}$ is an ordinary (connected) complex analytic manifold.

PROPOSITION 1. *Let $\mathfrak{D}$ be a domain in C^n and $\mathfrak{G}$ be a properly discontinuous group of analytic automorphisms of $\mathfrak{D}$. Then the quotient space $\mathfrak{G}\backslash\mathfrak{D}$ possesses a canonical V-manifold structure.*

PROOF. Let Φ be the canonical map from $\mathfrak{D}$ onto $\mathfrak{V}=\mathfrak{G}\backslash\mathfrak{D}$. For $p\in\mathfrak{V}$, take $\tilde{p}\in\mathfrak{D}$ such that $\Phi(\tilde{p})=p$ and let G_p be the isotropy group of p in $\mathfrak{G}$. Let further $\tilde{U}_p$ be a connected open neighbourhood of $\tilde{p}$ such that $\sigma(\tilde{U}_p)=\tilde{U}_p$ for $\sigma\in G_p$ and $\sigma(\tilde{U}_p)\frown\tilde{U}_p=\phi$ for $\sigma\notin G_p$. Then, denoting by φ_p the map induced by Φ on $\tilde{U}_p$, we have a l.u.s. $\{\tilde{U}_p, G_p, \varphi_p\}$ for $U_p=\varphi_p(\tilde{U}_p)$. Since it is clear that the neighbour-

[1] An analytic subvariety $\mathfrak{x}$ of $\mathfrak{v}$ is a (closed) subset of $\mathfrak{v}$ such that for any l.u.s. $\{\tilde{U}, G, \varphi\}$ for U, $\varphi^{-1}(\mathfrak{x}\frown U)$ is a (G-invariant) analytic subvariety of $\tilde{U}$ in the usual sense.

hoods of p which are uniformized in this sense form a complete system of neighbourhoods, the condition (2) is satisfied. If $\{\tilde{U}_p, G_p, \varphi_p\}$, $\{\tilde{U}_{p'}, G_{p'}, \varphi_{p'}\}$ are two l.u.s. defined as above such that $\Phi(\tilde{U}_p)\subset\Phi(\tilde{U}'_p)$, then there exists $\lambda\in\mathfrak{G}$ such that $\lambda(\tilde{U}_p)\subset\tilde{U}'_p$, which defines an injection from $\{\tilde{U}_p, G_p, \varphi_p\}$ into $\{\tilde{U}'_p, G'_p, \varphi'_p\}$. Hence the condition (1) is also satisfied by our family of l.u.s.

§2. The V-manifolds $\mathfrak{V}_n$ and $\mathfrak{W}_{n-1}$.

Let $\mathfrak{H}_n$ be the generalized upper half-plane of degree n, namely the space of all complex symmetric matrices $Z=X+iY$ of degree n with the imaginary part $Y>0$. Siegel's modular group M_n is the group of all symplectic transformations

$$\sigma=\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

of degree $2n$ with rational integral coefficients, acting on $\mathfrak{H}_n$ in the following form

$$\sigma(Z)=(AZ+B)(CZ+D)^{-1}.$$

Then, M_n being a properly discontinuous group of analytic automorphisms of $\mathfrak{H}_n$, the quotient space $\mathfrak{V}_n=M_n\backslash\mathfrak{H}_n$ becomes a V-manifold canonically. As is shown easily $\mathfrak{V}_n$ is not compact, and the purpose of the following considerations is to construct suitable compactification $\overline{\mathfrak{V}}_n$ of $\mathfrak{V}_n$ which is also a V-manifold.

For that purpose, we shall first construct a V-manifold $\mathfrak{W}_{n-1}$ which can be regarded as the set of all classes w.r.t. M_n of the limit points of the sequences $Z^{(k)}=(z^{(k)}_{ij})$ such that $y^{(k)}_n\to\infty$ $(k\to\infty)$, while all the other $z^{(j)}_{ij}$ and $x^{(k)}_n$ remain in some bounded domain, $x^{(k)}_n$, $y^{(k)}_n$ denoting the real and the imaginary parts of $z^{(k)}_n=z^{(k)}_{nn}$ respectively. The subgroup $\mathfrak{G}$ of M_n leaving fixed the totality of such limit points will be as follows:

$$\mathfrak{G}=\left\{\sigma=\begin{pmatrix} A\,B \\ C\,D \end{pmatrix};\ A=\begin{pmatrix} & 0 \\ * & \vdots \\ & 0 \\ & \pm1 \end{pmatrix},\ C=\begin{pmatrix} & 0 \\ * & \vdots \\ & 0 \end{pmatrix}\right\}.$$

PROPOSITION 2. *Put*

$$M'_{n-1}=\left\{\sigma=\begin{pmatrix} A^* & 0 & B^* & 0 \\ 0 & 1 & 0 & 0 \\ C^* & 0 & D^* & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix};\ \sigma^*=\begin{pmatrix} A^* & B^* \\ C^* & D^* \end{pmatrix}\in M_{n-1}\right\},$$

$$\tilde{\mathfrak{N}}=\left\{\sigma=\begin{pmatrix} I^* & 0 & 0 & \pm\mathfrak{s}^* \\ {}^t\mathfrak{g}^* & \pm 1 & {}^t\mathfrak{s}^* & s \\ 0 & 0 & I^* & \mp\mathfrak{g}^* \\ 0 & 0 & 0 & \pm 1 \end{pmatrix};\ \mathfrak{g}^*, \mathfrak{s}^*, s \text{ integral}\right\},$$

I^* denoting the unit matrix of degree $n-1$. Then M'_{n-1} is a subgroup of $\mathfrak{G}$ isomorphic to M_{n-1}, $\tilde{\mathfrak{N}}$ is a normal subgroup of $\mathfrak{G}$ and we have

$$\mathfrak{G}=M'_{n-1}\cdot\tilde{\mathfrak{N}}. \qquad M'_{n-1}\frown\tilde{\mathfrak{N}}=\{I\}.$$

PROOF. Let us write $\sigma\in\mathfrak{G}$ as follows

$$\sigma=\begin{pmatrix} A^* & 0 & B^* & \mathfrak{b}_1 \\ {}^t\mathfrak{a}_2 & \pm 1 & {}^t\mathfrak{b}_2 & b \\ C^* & 0 & D^* & \mathfrak{d}_1 \\ {}^t\mathfrak{c}_2 & 0 & {}^t\mathfrak{d}_2 & d \end{pmatrix}.$$

Then since σ is symplectic

$$\sigma^{-1}=\begin{pmatrix} {}^tD^* & \mathfrak{d}_2 & -{}^tB^* & -\mathfrak{b}_2 \\ {}^t\mathfrak{d}_1 & d & -{}^t\mathfrak{b}_1 & -b \\ -{}^tC^* & -\mathfrak{c}_2 & {}^tA^* & \mathfrak{a}_2 \\ 0 & 0 & 0 & \pm 1 \end{pmatrix}.$$

Hence we have

$$\begin{aligned} &\mathfrak{c}_2=\mathfrak{d}_2=0, \quad d=\pm 1, \\ &{}^tA^*D^*-{}^tC^*B^*=I^*, \\ &{}^tA^*C^*-{}^tC^*A^*=0, \\ &{}^tB^*D^*-{}^tD^*B^*=0, \\ &{}^tA^*\mathfrak{d}_1\pm\mathfrak{a}_2-{}^tC^*\mathfrak{b}_1=0, \\ &{}^tB^*\mathfrak{d}_1\pm\mathfrak{b}_2-{}^tD^*\mathfrak{b}_1=0, \end{aligned}$$

which imply in particular

$$\sigma^*=\begin{pmatrix} A^* & B^* \\ C^* & D^* \end{pmatrix}\in M_{n-1}.$$

It follows easily that the correspondence $\varphi:\sigma\rightarrow\sigma^*$ is a homomorphism from $\mathfrak{G}$ into M_{n-1} and that $\tilde{\mathfrak{N}}$ is the kernel of this homomorphism. On the other hand, the correspondence

$$\psi:\sigma^*=\begin{pmatrix} A^* & B^* \\ C^* & D^* \end{pmatrix}\rightarrow\sigma=\begin{pmatrix} A^* & 0 & B^* & 0 \\ 0 & 1 & 0 & 0 \\ C^* & 0 & D^* & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

is an isomorphism from M_{n-1} into $\mathfrak{G}$ such that $\varphi\circ\psi=1$. Hence φ is a homomorphism onto M_{n-1} and $\mathfrak{G}$ splits into $\mathfrak{N}$ and M'_{n-1} as stated in the Proposition.

Writing $Z \in \mathfrak{H}_n$ in the form

$$Z = \begin{pmatrix} Z^* & \mathfrak{z} \\ {}^t\mathfrak{z} & z \end{pmatrix},$$

we have

$$\sigma(Z) = \begin{pmatrix} \sigma^*(Z^*) & (A^* - \sigma^*(Z^*)C^*)\mathfrak{z} \\ & z - (C^*Z^* + D^*)^{-1}C^*[\mathfrak{z}] \end{pmatrix} \text{ for } \sigma \in M'_{n-1},$$

$$\sigma(Z) = \begin{pmatrix} Z^* & \pm\mathfrak{z} + Z^*\mathfrak{g}^* + \mathfrak{s}^* \\ & z \pm 2{}^t\mathfrak{z}\mathfrak{g}^* + Z^*[\mathfrak{g}^*] + s \end{pmatrix} \text{ for } \sigma \in \widetilde{\mathfrak{N}}.$$

If can be seen easily that

$$\mathfrak{N} = \left\{ \sigma = \begin{pmatrix} I & \begin{matrix} 0 & 0 \\ 0 & s \end{matrix} \\ 0 & I \end{pmatrix};\ s \text{ integral} \right\}$$

is a normal subgroup of $\mathfrak{G}$ contained in $\widetilde{\mathfrak{N}}$ and that $\widetilde{M}_{n-1} = \mathfrak{G}/\mathfrak{N}$ can be regarded as an effective, properly discontinuous group of analytic automorphisms $\mathfrak{H}_{n-1} \times C^{n-1} = \{(Z^*, \mathfrak{z})\}$. Let us put

$$\mathfrak{W}_{n-1} = \widetilde{M}_{n-1} \backslash (\mathfrak{H}_{n-1} \times C^{n-1}).$$

$\mathfrak{W}_{n-1}$ has a structure like a fibre space in the following sense. There exists a natural projection π from $\mathfrak{W}_{n-1}$ onto $\mathfrak{V}_{n-1} = M_{n-1} \backslash \mathfrak{H}_{n-1}$ which projects the class of $(Z^*, \mathfrak{z})$ w.r.t. $\widetilde{M}_{n-1}$ to that of Z^* w.r.t. M_{n-1}. $Z^* \in \mathfrak{H}_{n-1}$ let us denote its class w.r.t. M_{n-1} by $[Z^*]$. Then for any $[Z^*] \in \mathfrak{V}_{n-1}$

$$\pi^{-1}[Z^*] \approx \varDelta[Z^*] \backslash C^{n-1},$$

$\varDelta[Z^*]$ being the group of all translations of the space $C^{n-1} = \{(\mathfrak{z})\}$ of the form

$$\mathfrak{z} \to \pm\mathfrak{z} + Z^*\mathfrak{g}^* + \mathfrak{s}^*,\ \ \mathfrak{g}^*, \mathfrak{s}^* : \text{integral}.$$

Hence, denoting by $\mathfrak{A}[Z^*]$ the abelian variety with the period matrix (I^*, Z^*), $\pi^{-1}[Z^*]$ may be written as $\{\pm I^*\} \backslash \mathfrak{A}[Z^*]$.

§3. Junction of $\mathfrak{V}_n$ and $\mathfrak{W}_{n-1}$.

Let $\mathfrak{V}$, $\mathfrak{W}$ be V-manifolds of dimension n, m and $n > m$. If we can define a V-manifold structure on $\mathfrak{V} \smile \mathfrak{W}$ (supposing $\mathfrak{V} \frown \mathfrak{W} = \phi$) such that $\mathfrak{V}$ becomes an open V-submanifold of $\mathfrak{V} \smile \mathfrak{W}$ and $\mathfrak{W}$ a regularly imbedded V-submanifold of $\mathfrak{V} \smile \mathfrak{W}$, then we shall say that we have joined $\mathfrak{W}$ to $\mathfrak{V}$, or we have defined a *junction* of $\mathfrak{V}$ and $\mathfrak{W}$. Here the meaning of open V-submanifold will be obvious. A *regularly imbedded* V-submanifold $\mathfrak{W}$ of a V-manifold $\mathfrak{V}$ is a subspace of $\mathfrak{V}$ such that for any l.u.s. $\{\tilde{U}_q, G_q, \varphi_q\}$ of $\mathfrak{V}$ around $q \in \mathfrak{W}$ there exist a l.u.s. $\{\tilde{V}_q, H_q, \psi_q\}$ of $\mathfrak{W}$ around q and a *regular injection* ρ from $\{\tilde{V}_q, H_q, \psi_q\}$ into $\{U_q, G_q, \varphi_q\}$, namely an analytic isomorphism from $\tilde{V}_q$ onto a regularly imbedded analytic submanifold of $\tilde{U}_q$ such that for any $\tau \in H_q$ there exists a $\sigma \in G_q$ satisfying the relation $\rho \circ \tau = \sigma \circ \rho$ and that $\psi_q = \varphi_q \circ \rho$. For such regular injections we have the following lemmae which can be proved quite similarly as Lem. 1 and 2.

LEMMA 3. *Let ρ be a regular injection from $\{\tilde{V}_q, H_q, \psi_q]$ into $\{\tilde{U}_q, G_q, \varphi_q\}$. Put*

$$G_1 = \{\sigma\,;\ \sigma \in G_q,\ \sigma(\rho(\tilde{V}_q)) = \rho(\tilde{V}_q)\},$$
$$N_1 = \{\sigma\,;\ \sigma \in G_q,\ \sigma(\rho(\tilde{q}')) = \rho(\tilde{q}') \text{ for all } \tilde{q}' \in \tilde{V}_q\}.$$

Then N_1 is a normal subgroup of G_1. For $\tau \in H_q$, $\sigma \in G_q$ satisfying the relation $\rho \circ \tau = \sigma \circ \rho$ belongs to G_1 and is uniquely determined modulo N_1. The correspondence $\tau \to \sigma N_1$ is an isomorphism from H_q onto G_1/N_1.

LEMMA 4. *Let ρ, κ be two regular injections from $\{\tilde{V}_q, H_q, \psi_q\}$ into $\{\tilde{U}_q, G_q, \varphi_q\}$. Then there exists $\sigma \in G_q$ such that $\kappa = \sigma \circ \rho$. If σ' is an other element of G_q satisfying the same relation, then there exists $\sigma'' \in N_1$ such that $\sigma' = \sigma \circ \sigma''$.*

Now let us consider the junction of $\mathfrak{V}_n$ and $\mathfrak{W}_{n-1}$. Let $q \in \mathfrak{W}_{n-1}$ and $\{\tilde{V}_q, H_q, \psi_q\}$ be a l.u.s. of $\mathfrak{W}_{n-1}$ around q such that $\tilde{V}_q \subset \mathfrak{H}_{n-1} \times C^{n-1}$ and that H_q is the isotropy group of $\psi_q^{-1}(q) = \tilde{q} = (Z^{*0}, \mathfrak{z}^0)$ in $\tilde{M}_{n-1}$. Let $\tilde{U}_q$ be a connected open neighbourhood of $(Z^{*0}, \mathfrak{z}^0, 0)$ in the space $\mathfrak{H}_{n-1} \times C^{n-1} \times C$ such that

$$\tilde{U}_q \frown (\mathfrak{H}_{n-1} \times C^{n-1} \times \{0\}) = \tilde{V}_q \times \{0\},$$
$$\mathrm{pr}_{\mathfrak{H}_{n-1} \times C^{n-1}} \tilde{U}_q = \tilde{V}_q.$$

Let us operate $\tilde{M}_{n-1} = \mathfrak{G}/\mathfrak{N}$ on $\mathfrak{H}_{n-1} \times C^{n-1} \times C$ in the following way:

$$\bar{\sigma}(Z^*, \mathfrak{z}, e^{2\pi i z}) = (Z^{*\prime}, \mathfrak{z}', e^{2\pi i z'}) \text{ if } \sigma\begin{pmatrix} Z^* & \mathfrak{z} \\ & z \end{pmatrix} = \begin{pmatrix} Z^* & \mathfrak{z}' \\ & z' \end{pmatrix},$$

$\bar{\sigma}$ being the class of $\sigma \in \mathfrak{G}$ modulo $\mathfrak{N}$. Then the isotropy group G_q of $(Z^{*0}, \mathfrak{z}^0, 0)$ can be identified with H_q and we can take $\tilde{U}_q$ so as to be invariant under G_q.

Let us put

$$\tilde{\tilde{U}}_q=\left\{Z=\begin{pmatrix} Z^* & \mathfrak{z} \\ & z\end{pmatrix};\ (Z^*, \mathfrak{z}, e^{2\pi i z})\in \tilde{U}_q\right\}.$$

Then taking $\tilde{U}_q$ sufficiently small we can prove the following

PROPOSITION 3. (1) *$\tilde{\tilde{U}}_q$ is an (unramified) covering space of $\tilde{U}_q-\tilde{V}_q\times\{0\}$ w.r.t. the map*

$$Z=\begin{pmatrix} Z^* & \mathfrak{z} \\ & z\end{pmatrix}\to(Z^*, \mathfrak{z}, e^{2\pi i z}).$$

The group of covering transformations is $\mathfrak{N}$.

(2) *If $\sigma(\tilde{\tilde{U}}_q)\frown\tilde{\tilde{U}}_q\not=\phi$ for $\sigma\in M_n$, then $\sigma\in\mathfrak{G}$ and the class of σ modulo $\mathfrak{N}$ belongs to G_q.*

The assertion (1) is evident. To prove (2) we shall use the reduction theory of Siegel.[2]

We shall call $Z=X+iY\in\mathfrak{H}_n$ *reduced in Siegel's sense* if the following conditions are satisfied.

(I) $$\text{abs}\,|CZ+D|\geqq 1,$$

$\{C, D\}$ being any coprime symmetric pair of matrices.

(II) Y is reduced in Minkowski's sense, namely

$$Y[\mathfrak{g}_k]\geqq y_k \quad (1\leqq k\leqq n),$$
$$y_{k,\,k+1}\geqq 0 \quad (1\leqq k\leqq n-1),$$

y_{kl} being the (k, l)-component of Y and $y_k=y_{kk}$, and $\mathfrak{g}_k$ being vectors with integral components $g_1,\cdots,g_n$, of which g_i $(k\leqq i\leqq n)$ are coprime.

(III) $$\text{abs}\,x_{kl}\leqq\frac{1}{2}\quad(1\leqq k, l\leqq n),$$

x_{kl} being the (k, l)-component of X.
It is known that these conditions are not independent, but only a finite number of them are sufficient. Siegel has proved that the set of all reduced matrices in $\mathfrak{H}_n$ forms a fundamental region of M_n.

LEMMA 5. *For any $Z=\begin{pmatrix} Z^* & \mathfrak{z} \\ & z\end{pmatrix}$ there exists $\sigma\in\mathfrak{G}$ such that $\sigma(Z)=Z'=\begin{pmatrix} Z^{*\prime} & \mathfrak{z}' \\ & z'\end{pmatrix}$ satisfies the following conditions.*

(*) *$Z^{*\prime}$ is reduced.*

(II') $$Y^{*\prime}[\mathfrak{g}^*]+2\,{}^t\mathfrak{y}'\mathfrak{g}^*\geqq 0,\quad y'_{n-1,n}\geqq 0,$$

$Y^{*\prime}$, $\mathfrak{y}'$ being the imaginary parts of $Z^{*\prime}$, $\mathfrak{z}'$, respectively, and $\mathfrak{g}^*$ any integral $(n-1)$-vector.

(III') $$\text{abs}\,x'_{kn}\leqq\frac{1}{2}\quad(1\leqq k\leqq n).$$

[2] Cf. Siegel [1].

PROOF. Since $M'_{n-1} \subset \mathfrak{G}$ we can choose $\sigma \in M'_{n-1}$ such that $\sigma^*(Z^*) = Z^{*\prime}$ is reduced. Hence we can assume at first that Z^* is reduced.

Letting $\mathfrak{g}^*$ be arbitrary integral $(n-1)$-vectors, we shall consider the following function

$$Y^*[\mathfrak{g}^*] + 2\,{}^t\mathfrak{y}\mathfrak{g}^* = Y^*[\mathfrak{g}^* + Y^{*^{-1}}\mathfrak{y}] - Y^*[Y^{*^{-1}}\mathfrak{y}].$$

Let $\mathfrak{g}_0^*$ be the (integral) value of $\mathfrak{g}^*$ at which this function attains its minimum. Then, putting $\mathfrak{y}' = \pm(Y^*\mathfrak{g}_0^* + \mathfrak{y})$ we have

$$\begin{aligned} Y^*[\mathfrak{g}^*] + 2\,{}^t\mathfrak{y}'\mathfrak{g}^* &= Y^*[\pm\mathfrak{g}^* + \mathfrak{g}_0^* + Y^{*^{-1}}\mathfrak{y}] - Y^*[\mathfrak{g}_0^* + Y^{*^{-1}}\mathfrak{y}] \\ &\geqq 0 \end{aligned}$$

for all integral $(n-1)$-vectors $\mathfrak{g}^*$. Hence if we put

$$\sigma = \left(\begin{array}{cc|cc} \pm I^* & 0 & & \\ {}^t\mathfrak{g}_0^* & 1 & \multicolumn{2}{c}{0} \\ & & \pm I^* & \mp\mathfrak{g}_0^* \\ \multicolumn{2}{c|}{0} & 0 & 1 \end{array}\right) \in \mathfrak{G}$$

we can see that $Z' = \sigma(Z) = \begin{pmatrix} Z^* & \pm(\mathfrak{g} + Z^*\mathfrak{g}_0^*) \\ & z + 2\,{}^t\mathfrak{z}\mathfrak{g}_0^* + Z^*[\mathfrak{g}_0^*] \end{pmatrix}$ satisfies the conditions $(*)$ and (II′).

Since $\tilde{\mathfrak{N}} \subset \mathfrak{G}$ contains also the translations.

$$\begin{pmatrix} Z^* & \mathfrak{z} \\ & z \end{pmatrix} \to \begin{pmatrix} Z^* & \mathfrak{z} + \mathfrak{s}^* \\ & z + s \end{pmatrix},$$

it is easy to see that we can choose $\sigma \in \mathfrak{G}$ so that $Z' = \sigma(Z)$ satisfies the conditions $(*)$, (II′) and (III′).

Let us remark that if Z^*, $\mathfrak{z}$ and the real part x of z are in some bounded domain then the possibilities of such σ are of only finite numbers.

LEMMA 6. *Let Z^*, $\mathfrak{z}$ be in some bounded domain and the imaginary part y of z be sufficiently large. Then there exists $\sigma \in \mathfrak{G}$ such that $\sigma(Z) = \sigma\begin{pmatrix} Z^* & \mathfrak{z} \\ & z \end{pmatrix}$ is reduced in Siegel's sense.*

PROOF. By the above lemma and remark, it is sufficient to show that if Z^*, $\mathfrak{z}$ and the real part x of z satisfy the conditions $(*)$, (II′) and (III′) and Z^* lies in some bounded domain, then the conditions (I), (II) and (III) are satisfied by Z if we take y sufficiently large.

(I) We can take $\{C, D\}$ of the following form

$$C = \begin{pmatrix} C_0 & 0 \\ 0 & 0 \end{pmatrix} {}^t\!\begin{pmatrix} Q & * \end{pmatrix}, \quad D = \begin{pmatrix} D_0 & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} Q & * \end{pmatrix}^{-1},$$

$\{C_0, D_0\}$ being a coprime symmetric pair of matrices of degree r $(1 \leqq r \leqq n)$, $|C_0| \neq 0$ and Q an (n, r)-matrix such that $(Q\ *)$ is unimodular. Then putting

$$S_0=X[Q]+C_0^{-1}D_0,\quad T_0=Y[Q],$$

we have

$$\begin{aligned}\mathrm{abs}\,|CZ+D|&=\mathrm{abs}\,|C_0Z[Q]+D_0|\\&=\mathrm{abs}\,|C_0|\,\mathrm{abs}\,|S_0+iT_0|.\end{aligned}$$

As $\mathrm{abs}\,|C_0|\geqq 1$, $\mathrm{abs}\,|S_0+iT_0|\geqq|T_0|$, we have

$$\mathrm{abs}\,|CZ+D|\geqq|T_0|=|Y[Q]|.$$

Denoting by $Y^*(i_1,\cdots,i_{r-1};j_1,\cdots,j_{r-1})$ the $(i_1,\cdots,i_{r-1};j_1,\cdots,j_{r-1})$-th minor of degree $r-1$ of Y^*, the coefficient of y in $|Y[Q]|$ is

$$\sum_{\substack{1\leqq i_1<\cdots<i_{r-1}\leqq n-1\\ 1\leqq j_1<\cdots<j_{r-1}\leqq n-1}} Y^*(i_1,\cdots,i_{r-1};\ j_1,\cdots,j_{r-1})\begin{vmatrix}q_{i_11} & \cdots q_{i_1r}\\ \cdots & \cdots\\ q_{i_{r-1}1} & \cdots q_{i_{r-1}r}\\ q_{n1} & \cdots q_{nr}\end{vmatrix}\begin{vmatrix}q_{j_11} & \cdots q_{j_1r}\\ \cdots & \cdots\\ q_{j_{r-1}1} & \cdots q_{j_{r-1}r}\\ q_{n1} & \cdots q_{nr}\end{vmatrix},$$

which is >0 unless $(q_{n1},\cdots,q_{nr})=(0,\cdots,0)$. Hence if $(q_{n1},\cdots,q_{nr})\neq(0,\cdots,0)$ the condition (I) is satisfied by taking y sufficiently large. If $(q_{n1},\cdots,q_{nr})=(0,\cdots,0)$, then $r\leqq n-1$ and we may assume that $\{C, D\}$ is of the form

$$C=\begin{pmatrix}C^* & 0\\ 0 & 0\end{pmatrix},\quad D=\begin{pmatrix}D^* & 0\\ 0 & 1\end{pmatrix},$$

$\{C^*, D^*\}$ being a coprime symmetric pair of matrices of degree $n-1$. Hence the condition (I) is satisfied since Z^* is reduced so that

$$\mathrm{abs}\,|CZ+D|=\mathrm{abs}\,|C^*Z^*+D^*|\geqq 1.$$

(II) Writing $\mathfrak{g}_k=\begin{pmatrix}\mathfrak{g}_k^*\\ g_n\end{pmatrix}$, the first part of the condition (II) can be written as follows:

$$Y[\mathfrak{g}_k]=Y^*[\mathfrak{g}_k^*]+2g_n{}^t\mathfrak{y}\mathfrak{g}_k^*+g_n^2y\geqq y_k.$$

Hence, if $k\leqq n-1$, $g_n\neq 0$, it is satisfied by taking y sufficiently large. If $g_n=0$, then $k\leqq n-1$ and Z satisfies this condition since Z^* is reduced. If $k=n$, then $g_n=\pm 1$ and this condition is nothing other than the first part of (II′).

The second part of (II) is also satisfied since Z^* is reduced and $\mathfrak{z}$ satisfies the second part of (II′).

(III) This condition coincides with the corresponding part of (*) and (III′).

Now the assertion (2) of Prop. 3 follows easily. Assuming $\tilde{U}_q$ to be sufficiently small, let $\sigma(\tilde{\tilde{\tilde{U}}}_q)\frown\tilde{\tilde{\tilde{U}}}_q\neq\phi$ for $\sigma\in M_n$. Then there exist Z, $Z'\in\tilde{\tilde{\tilde{U}}}_q$ such that $\sigma(Z)=Z'$. By Lem. 6 we can take τ, $\tau'\in\mathfrak{G}$ such that $\tau(Z)$, $\tau'(Z')$ are reduced. Then $\tau'\sigma\tau^{-1}(\tau(Z))=\tau'(Z')$. Taking Z such that $\tau(Z)$ lies in the interior of Siegel's fundamental region, it follows that $\tau'\sigma\tau^{-1}=1$. Hence $\sigma=\tau'^{-1}\tau\in\mathfrak{G}$. Then by the definition $\tilde{\tilde{U}}_q$ it follows that σ modulo $\mathfrak{N}$ belongs to G_q.

It follows from Prop. 3 (2) that defining the map φ_q by

$$\varphi_q(Z^*,\mathfrak{z},w)=\begin{cases}\text{the class of } (Z^*,\mathfrak{z}) \text{ w.r.t. } \tilde{M}_{n-1}, \\ \text{if } w=0, \\ \text{the class of } \begin{pmatrix} Z^* & \mathfrak{z} \\ & z \end{pmatrix} \text{ w.r.t. } M_n, \\ \text{if } w=e^{2\pi iz},\end{cases}$$

the system $\{\tilde{U}_q, G_q, \varphi_q\}$ satisfies the condition of l.u.s. Also it can be seen easily from Prop. 3 (1) that these l.u.s. together with the natural,injections satisfy the conditions of l.u.s. defining a junction of $\mathfrak{V}_n$ and $\mathfrak{W}_{n-1}$. Thus we have constructed the V-manifold $\mathfrak{V}_n\smile\mathfrak{W}_{n-1}$ which is a junction of $\mathfrak{V}_n$ and $\mathfrak{W}_{n-1}$.

§4. The compactification of the case of $n=2$.

The V-manifold $\mathfrak{V}_n\smile\mathfrak{W}_{n-1}$ constructed in the preceding section is not yet compact. It is necessary that $\mathfrak{W}_{n-1}$ is completed to a compact V-manifold $\overline{\mathfrak{W}}_{n-1}$ and this $\overline{\mathfrak{W}}_{n-1}$ is joined to $\mathfrak{V}_n$. But in general this procedure is much complicated and we could not decide whether it is possible or not. So in the following we shall limit ourselves only to the case of $n=2$ and show the possibility of the compactification of $\mathfrak{V}_2$.

The structure of $\mathfrak{W}_1$ is known by the classical theory of elliptic functions. Namely the V-manifold structure of $\mathfrak{W}_1=\tilde{M}_1\backslash\mathfrak{H}_1\times C$ is trivial[3] and $\mathfrak{W}_1$ is homeomorphic to $C\times C$ by the analytic mapping

$$\text{the class of } (z_1, z_{12})\rightarrow(j(z_1),\ \wp(z_{12};\ 1, z_1)),$$

$\bar{C}=C\smile\{\infty\}$ being the complex sphere, j the absolute invariant of elliptic curve and $\wp$ the Weierstrass' elliptic function.

The compactification of $\mathfrak{W}_1$ will be as follows:

$$\overline{\mathfrak{W}}_1\approx\bar{C}\times\bar{C}=(C\times\bar{C})\smile(\{\infty\}\times C)\smile(\{\infty\}\times\{\infty\}).$$

We shall show in the following that we can actually join $\mathfrak{W}_{12}\approx\{\infty\}\times C$, $\mathfrak{V}_0\approx\{\infty\}\times\{\infty\}$ to $\mathfrak{V}_2\smile\mathfrak{W}_1$ so that $\overline{\mathfrak{V}}_2=\mathfrak{V}_2\smile\mathfrak{W}_1\smile\mathfrak{W}_{12}\smile\mathfrak{V}_0$ becomes a compact V-manifold.

$\mathfrak{W}_{12}$ can be regarded as the set of all classes w.r.t. M_2 of the limit points of the sequences $Z^{(k)}=\begin{pmatrix} z_1^{(k)} & z_{12}^{(k)} \\ & z_2^{(k)} \end{pmatrix}$ such that $z_{12}^{(k)}$ and the real parts $x_1^{(k)}$, $x_2^{(k)}$ of $z_1^{(k)}$, $z_2^{(k)}$ are bounded and the imaginary parts $y_1^{(k)}$,

[3] A V-manifold structure of $\mathfrak{v}$ is said to be trivial if the corresponding faisceau of germs of holomorphic functions coincides with that of some usual complex analytic structure of $\mathfrak{v}$.

$y_2^{(k)}$ of $z_1^{(k)}$, $z_2^{(k)}$ tend to infinity. The subgroup $\mathfrak{G}'$ of M_2 leaving fixed the set of all such limit points will consist of the transformations of the form

$$(\S)\qquad Z\to Z[U]+S,$$

where

$$U=\begin{pmatrix}\pm1 & 0\\ 0 & \pm1\end{pmatrix},\ \begin{pmatrix}0 & \pm1\\ \pm1 & 0\end{pmatrix},$$

S: symmetric matrix with integral components.

Let $\mathfrak{N}'$ be the normal subgroup of $\mathfrak{G}'$ formed of all transformations of the form (§) with

$$U=\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ \pm\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\ S=\begin{pmatrix}s_1 & 0\\ 0 & s_2\end{pmatrix}.$$

Then $\bar{\mathfrak{G}}'=\mathfrak{G}'/\mathfrak{N}'$ can be considered as an effective group of analytic automorphisms of the space $C=\{(z_{12})\}$ consisting of the transformation

$$z_{12}\to\pm z_{12}+s_{12},\quad s_{12}\ \text{integral}.$$

The V-manifold $\mathfrak{W}_{12}$ is defined as the quotient space $\bar{\mathfrak{G}}'\backslash C$.

Let $q\in\mathfrak{W}_{12}$ be the class of $\tilde{q}=(z_{12}^0)$ w.r.t. $\bar{\mathfrak{G}}'$ and $\{\tilde{V}_q, H_q, \varphi_q\}$ be a l.u.s. of $\mathfrak{W}_{12}$ around q such that $(z_{12}^0)\in\tilde{V}_q\subset C$ and that H_q is the isotropy group of (z_{12}^0) in $\bar{\mathfrak{G}}'$. Let $\tilde{U}_q$ be a connected open neighbourhood of $(0, z_{12}^0, 0)$ in $C\times C\times C$ such that

$$\{0\}\times\tilde{V}_q\times\{0\}\subset\tilde{U}_q\subset C\times\tilde{V}_q\times C.$$

Now let $\mathfrak{N}_0'$ be the normal subgroup of $\mathfrak{G}'$ formed of all transformations of the form (§) with

$$U=\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ S=\begin{pmatrix}s_1 & 0\\ 0 & s_2\end{pmatrix}.$$

Then we can make $\tilde{\mathfrak{G}}'=\mathfrak{G}'/\mathfrak{N}_0'$ operate on the space $C\times C\times C$ as an effective group of analytic automorphisms in the following way:

$$\tilde{\sigma}(e^{2\pi iz_1},\ z_{12},\ e^{2\pi iz_2})=(e^{2\pi iz_1'},\ z_{12}',\ e^{2\pi iz_2'})$$

$$\text{if}\quad\sigma\begin{pmatrix}z_1 & z_{12}\\ & z_2\end{pmatrix}=\begin{pmatrix}z_1' & z_{12}'\\ & z_2'\end{pmatrix},$$

$\tilde{\sigma}$ being the class of $\sigma\in\mathfrak{G}'$ modulo $\mathfrak{N}_0'$. Then the isotropy group G_q of $(0, z_{12}^0, 0)$ in $\tilde{\mathfrak{G}}'$ is the inverse image of $H_q\subset\bar{\mathfrak{G}}'$ by the canonical homomorphism $\tilde{\mathfrak{G}}'=\mathfrak{G}'/\mathfrak{N}_0'\to\bar{\mathfrak{G}}'=\mathfrak{G}'/\mathfrak{N}'$. We can take $\tilde{U}_q$ so as to be invariant under G_q.

In the similar way as in the preceding section we can prove that taking $\tilde{U}_q$ sufficiently small and putting

$$\varphi_q(w_1, z_{12}, w_2)=\begin{cases}\text{the class of } (z_{12}) \text{ w.r.t. } \bar{\mathfrak{G}}',\\ \text{if } w_1=w_2=0,\\ \text{the class of } (z_1, z_{12}) \text{ w.r.t. } \tilde{M}_1,\\ \text{if } w_1=e^{2\pi i z_1},\ w_2=0, \text{ or } w_1=0,\ w_2=e^{2\pi i z_1},\\ \text{the class of } \begin{pmatrix} z_1 & z_{12} \\ & z_2 \end{pmatrix} \text{ w.r.t. } M_2,\\ \text{if } w_1=e^{2\pi i z_1},\ w_2=e^{2\pi i z_2},\end{cases}$$

$\{\tilde{U}_q, G_q, \varphi_q\}$ satisfies the condition of l.u.s. of $\mathfrak{V}_2 \smile \mathfrak{W}_1 \smile \mathfrak{W}_{12}$ around q and these l.u.s. together with the natural injections define a junction of $\mathfrak{V}_2 \smile \mathfrak{W}_1$ and $\mathfrak{W}_{12}$.

Next let us consider $\mathfrak{V}_0 \approx \{\infty \times \infty\}$. This point can be regarded as the limit of the sequences $Z^{(k)}=\begin{pmatrix} z_1^{(k)} & z_{12}^{(k)} \\ & z_2^{(k)} \end{pmatrix}$ such that the real parts of $z_1^{(k)}, z_{12}^{(k)}, z_2^{(k)}$ are bounded and denoting by $y_1^{(k)}, y_{12}^{(k)}, y_2^{(k)}$ the imaginary parts of them respectively $y_1^{(k)}-y_{12}^{(k)}$, $y_2^{(k)}-y_{12}^{(k)}$, $y_{12}^{(k)}$ tend to infinity. The subgroup $\mathfrak{G}''=\mathfrak{N}''$ of M_2 leaving fixed this limit point will consist of the transformations of the form

$$Z \to Z[U]+S,$$

U being an arbitrary unimodular matrix and S an arbitrary integral symmetric matrix.

Let $\mathfrak{N}_0''$ be the normal subgroup of $\mathfrak{G}''$ formed of all transformations of the above form with

$$U \equiv I \pmod 2.$$

Then the factor group $\mathfrak{G}''=\mathfrak{G}''/\mathfrak{N}_0''$ is, as is seen easily, isomorphic to the symmetric group of three letters. This isomorphism will be given an explicit form by the following considerations.

Let us introduce the theta functions (Theta-Nullwert) of the following type:

$$\vartheta_{\mathfrak{m}}^*(Z)=\sum_{\mathfrak{g}=\mathfrak{m}\ (\mathrm{mod}\ 2)}^{*} e^{\pi i Z[\mathfrak{g}]}$$

$\mathfrak{m}$ being the integral vectors which are determined modulo 2 and the star attached to the summation symbol denotes that the summation is taken over all non-associated primitive integral vectors $\mathfrak{g}$ satisfying the relation $\mathfrak{g} \equiv \mathfrak{m} \pmod 2$. Two primitive integral $\mathfrak{g}$, $\mathfrak{g}'$ are said to be associated if $\mathfrak{g}'=\pm\mathfrak{g}$.

We can prove easily the following transformation formulae:

$\vartheta_{\mathfrak{m}}^*(Z[U])=\vartheta_{\bar{U}\mathfrak{m}}^*(Z)$ for any unimodular matrix U,
$\vartheta_{\mathfrak{m}}^*(Z+S)=(-1)^{m_1 s_1+m_2 s_2}\vartheta_{\mathfrak{m}}^*(Z)$ for any integral symmetric matrix

$$S=\begin{pmatrix} s_1 & s_{12} \\ & s_2 \end{pmatrix}.$$

Since we have $U\mathfrak{m}\equiv\mathfrak{m} \pmod 2$ for $U\equiv I \pmod 2$, the functions ϑ^*_{10}, ϑ^*_{11}, ϑ^*_{01} are all invariant or two of them change their signs by the transformations of $\mathfrak{N}''_0$. It follows easily that putting

$$w_1=\frac{\vartheta^*_{10}(Z)\vartheta^*_{11}(Z)}{\vartheta^*_{01}(Z)}\,,\quad w_2=\frac{\vartheta^*_{01}(Z)\vartheta^*_{10}(Z)}{\vartheta^*_{11}(Z)}\,,\quad w_3=\frac{\vartheta^*_{11}(Z)\vartheta^*_{01}(Z)}{\vartheta^*_{10}(Z)}\,,$$

these functions are all invariant under $\mathfrak{N}''_0$ and that $\mathfrak{G}''=\mathfrak{G}''/\mathfrak{N}''_0$ acts on them as the symmetric permutation group.

The behavior of these functions around the point at infinity is described in the following

LEMMA 7. *The functions w_1, w_2, w_3 are expressed by the convergent power series of $u_1=e^{2\pi i(z_1-z_{12})}$, $u_2=e^{2\pi i z_{12}}$, $u_3=e^{2\pi i(z_2-z_{12})}$ of the following from*

$$\begin{aligned}w_1&=u_1+(\text{terms of higher order}),\\ w_2&=u_2+(\text{terms of higher order}),\\ w_3&=u_3+(\text{terms of higher order}).\end{aligned}$$

PROOF. Putting $\mathfrak{g}=\begin{pmatrix}2g'_1+1\\ 2g'_2\end{pmatrix}$, we have

$$\begin{aligned}\vartheta^*_{10}(Z)&=\sum\nolimits^* e^{\pi iZ[\mathfrak{g}]}\\ &=\sum\nolimits^* e^{\pi i\{z_1(2g_1'+1)^2+2z_{12}(2g_1'+1)2g_2'+z_24g_2'^2\}}\\ &=e^{\pi iz_1}\sum\nolimits^* e^{4\pi i\{z_1(g_1'^2+g_1')+z_{12}(2g_1'g_2'+g_2')+z_2g_2'^2\}}\\ &=e^{\pi iz_1}\sum\nolimits^* u_1{}^{2(g_1'^2+g_1')}u_2{}^{2\{(g_1'+g_2')^2+(g_1'+g_2')\}}u_3{}^{2g_2'^2}\\ &=e^{\pi iz_1}\{1+(\text{terms of order }\geqq 1)\}.\end{aligned}$$

Similarly we have

$$\begin{aligned}\vartheta^*_{01}(Z)&=e^{\pi iz_2}\sum\nolimits^* u_1{}^{2g_1'^2}u_2{}^{2\{(g_1'+g_2')^2+(g_1'+g_2')\}}u_3{}^{2(g_2'^2+g_2')}\\ &=e^{\pi iz_2}\{1+(\text{terms of order }\geqq 1)\},\\ \vartheta^*_{11}(Z)&=e^{\pi i(z_1-2z_{12}+z_2)}\sum\nolimits^* u_1{}^{2(g_1'^2+g_1')}u_2{}^{2(g_1'+g_2'+1)^2}u_3{}^{2(g_2'^2+g_2')}\\ &=e^{\pi i(z_1-2z_{12}+z_2)}\{1+\text{terms of order }\geqq 1)\}.\end{aligned}$$

Lemma follows easily from these expressions, q.e.d.

Now let $\tilde{U}_\infty$ be a connected open neighbourhood of $(0, 0, 0)$ in the space $C\times C\times C=\{(w_1, w_2, w_3)\}$ invariant under the permutations of the coordinates and let $\tilde{\tilde{U}}{}^0_\infty$ be the set of all $Z\in\mathfrak{H}_2$ such that y_1-y_{12}, y_2-y_{12}, y_{12} are sufficiently large. Then the above lemma shows that if $\tilde{U}_\infty$ is sufficiently small then we can take $\tilde{\tilde{U}}{}^0_\infty$ such that $\tilde{\tilde{U}}{}^0_\infty$ is mapped onto $\{(w_1, w_2, w_3)\in\tilde{U}_\infty;\ w_1\cdot w_2\cdot w_3\neq 0\}$ by the map $Z\rightarrow(w_1, w_2, w_3)$. $\tilde{U}_\infty$, $\tilde{\tilde{U}}{}^0_\infty$ being so, let $\tilde{\tilde{U}}_\infty$ be the set of all $Z\in\mathfrak{H}_2$ equivalent with $Z'\in\tilde{\tilde{U}}{}^0_\infty$ w.r.t. the group $\mathfrak{G}''$. Then we can prove the following proposition.

PROPOSITION 4. (1) *$\tilde{\tilde{\tilde{U}}}_\infty$ is an (unramified) covering space of $\{(w_1, w_2, w_3) \in \tilde{U}_\infty;\ w_1 \cdot w_2 \cdot w_3 \neq 0\}$ w.r.t. the map*

$$Z \to (w_1, w_2, w_3),$$

$$w_1 = \frac{\vartheta_{10}^*(Z)\vartheta_{11}^*(Z)}{\vartheta_{01}^*(Z)}, \quad w_2 = \frac{\vartheta_{01}^*(Z)\vartheta_{10}^*(Z)}{\vartheta_{11}^*(Z)}, \quad w_3 = \frac{\vartheta_{11}^*(Z)\vartheta_{01}^*(Z)}{\vartheta_{10}^*(Z)}.$$

The group of covering transformations is $\mathfrak{N}_0''$.

(2) *If $\sigma(\tilde{\tilde{\tilde{U}}}_\infty) \frown \tilde{\tilde{\tilde{U}}}_\infty \neq \phi$ for $\sigma \in M_2$ then $\sigma \in \mathfrak{G}''$.*

The proof will be given in the next section.

Next, let Z be in $\tilde{\tilde{\tilde{U}}}{}^0_\infty$ and $y_2 \to \infty$. Then the functions ϑ_{10}^*, $\vartheta_{11}^*/e^{\pi i z_2}$, $\vartheta_{01}^*/e^{\pi i z_2}$ convèrge uniformly as follows:

$$\vartheta_{10}^*(Z) \to e^{\pi i z_1},$$

$$\vartheta_{11}^*(Z)/e^{\pi i z_2} \to e^{\pi i (z_1 - 2z_{12})} \sum_{g'=-\infty}^{\infty} u_1^{2(g'^2+g')} u_2^{2(g'+1)^2}$$

$$= \sum_{g'=-\infty}^{\infty} e^{\pi i \{z_1(2g'+1)^2 + 2z_{12}(2g'+1)\}}$$

$$= \vartheta_2(2z_{12};\ 1,\ 4z_1),$$

$$\vartheta_{01}^*(Z)/e^{\pi i z_2} \to \sum_{g'=-\infty}^{\infty} u_1^{2g'^2} u_2^{2(g'^2+g')}$$

$$= \sum_{g'=-\infty}^{\infty} e^{\pi i (z_1 4g'^2 + 2z_{12} 2g')}$$

$$= \vartheta_3(2z_{12};\ 1,\ 4z_1).$$

Hence we have

$$\frac{\vartheta_{10}^*(Z)\vartheta_{11}^*(Z)}{\vartheta_{01}^*(Z)} \to e^{\pi i z_1} \frac{\vartheta_2(2z_{12};\ 1,\ 4z_1)}{\vartheta_3(2z_{12};\ 1,\ 4z_1)},$$

$$\frac{\vartheta_{01}^*(Z)\vartheta_{10}^*(Z)}{\vartheta_{11}^*(Z)} \to e^{\pi i z_1} \frac{\vartheta_3(2z_{12};\ 1,\ 4z_1)}{\vartheta_2(2z_{12};\ 1,\ 4z_1)},$$

$$\frac{\vartheta_{11}^*(Z)\vartheta_{01}^*(Z)}{\vartheta_{10}^*(Z)} \to 0.$$

Let $\tilde{\tilde{\tilde{V}}}{}^0_\infty$ be the set of all $(z_1, z_{12}) \in \mathfrak{H}_2 \times C$ such that $Z = \begin{pmatrix} z_1 & z_{12} \\ & z_2 \end{pmatrix} \in \tilde{\tilde{\tilde{U}}}{}^0_\infty$ if y_2 is sufficiently large. Let $\tilde{\tilde{\tilde{V}}}_\infty$ be the set of all $(z_1, z_{12}) \in \mathfrak{H}_1 \times C$ equivalent with $(z_1', z_{12}') \in \tilde{\tilde{\tilde{V}}}{}^0_\infty$ w.r.t. the group $\mathfrak{H}''$ formed of all the transformations of the form

$$(z_1, z_{12}) \to (z_1 + s_1,\ \ \pm s_{12} + z_1 g_1 + s_{12}),$$

s_1, g_1, s_{12} being rational integers. Then the following proposition can be proved by the theory of elliptic theta functions. (See the next section.)

PROPOSITION 5. (1) *$\tilde{\tilde{\tilde{V}}}_\infty$ is an (unramified) covering space of $\{(w_1 w_2);\ (w_1, w_2, 0) \in \tilde{U}_\infty,\ w_1 \cdot w_2 \neq 0\}$ w.r.t. the map*

$$(z_1, z_{12}) \to (w_1, w_2),$$
$$w_1 = e^{\pi i z_1} \frac{\vartheta_2(2z_{12};\, 1,\, 4z_1)}{\vartheta_3(2z_{12};\, 1,\, 4z_1)}, \quad w_2 = e^{\pi i z_1} \frac{\vartheta_3(2z_{12};\, 1,\, 4z_1)}{\vartheta_2(2z_{12};\, 1,\, 4z_1)}.$$

The group of covering transformations consists of the transformations of the form

$$(z_1, z_{12}) \to (z_1 + s_1,\ \ \pm z_{12} + z_1 g_1 + s_{12})$$

with $g_1 \equiv 0 \pmod 2$.

(2) *If* $\bar{\sigma}(\widetilde{\widetilde{\widetilde{V}}}_\infty) \frown \widetilde{\widetilde{\widetilde{V}}}_\infty \neq \phi$ *for* $\bar{\sigma} \in \tilde{M}_1$, *then* $\bar{\sigma} \in \mathfrak{H}''$.

Finally, let (z_1, z_{12}) be in $\widetilde{\widetilde{\widetilde{V}}}{}^0_\infty$ and $y_1 \to \infty$. Then the functions $\vartheta_2/e^{\pi i z_1}$, ϑ_3 converge uniformly as follows:

$$\vartheta_2(2z_{12};\, 1,\, 4z_1)/e^{\pi i z_1} \to e^{2\pi i z_{12}} + e^{-2\pi i z_{12}},$$
$$\vartheta_3(2z_{12};\, 1,\, 4z_1) \to 1,$$

so that we have

$$e^{\pi i z_1} \frac{\vartheta_2(2z_{12};\, 1,\, 4z_1)}{\vartheta_3(2z_{12};\, 1,\, 4z_1)} \to 0,$$
$$e^{\pi i z_1} \frac{\vartheta_3(2z_{12};\, 1,\, 4z_1)}{\vartheta_2(2z_{12};\, 1,\, 4z_1)} \to \frac{1}{e^{2\pi i z_{12}} + e^{-2\pi i z_{12}}}.$$

Let $\widetilde{\widetilde{\widetilde{W}}}{}^0_\infty$ be the set of all $z_{12} \in C$ such that $(z_1, z_{12}) \in \widetilde{\widetilde{\widetilde{V}}}{}^0_\infty$ if y_1 is sufficiently large. Then $\widetilde{\widetilde{\widetilde{W}}}{}^0_\infty$ consists of all z_{12} with the imaginary parts y_{12} sufficiently large. Put $\widetilde{\widetilde{\widetilde{W}}}_\infty = \{\pm z_{12};\, z_{12} \in \widetilde{\widetilde{\widetilde{W}}}{}^0_\infty\}$. $\widetilde{\widetilde{\widetilde{W}}}_\infty$ is clearly invariant under the transformations

$$z_{12} \to \pm z_{12} + s_{12}$$

with s_{12} integral, which constitute the group we have formerly denoted by $\mathfrak{G}'$.

Now the following proposition is obvious.

PROPOSITION 6. $\widetilde{\widetilde{\widetilde{W}}}_\infty$ *is an (unramified) covering space of* $\{w_2;\ (0, w_2, 0) \in \tilde{U}_\infty,\ w_2 \neq 0\}$ *w.r.t. the map*

$$z_{12} \to w_2 = \frac{1}{e^{2\pi i z_{12}} + e^{-2\pi i z_{12}}}.$$

The group of covering transformations is $\mathfrak{G}'$.

From these considerations it will be now clear how we should take the l.u.s. $\{\tilde{U}_\infty, G_\infty, \varphi_\infty\}$ around the point at infinity p_∞ in order to define the junction of $\mathfrak{V}_0 = \{p_\infty\}$ to $\mathfrak{V}_2 \smile \mathfrak{W}_1 \smile \mathfrak{W}_{12}$. Namely, let $\tilde{U}_\infty$ be an ε-cube with sufficiently small ε in the space $C^3 = \{(w_1, w_2, w_3)\}$ and G_∞ be the symmetric permutation group of the coordinates in C^3. Let φ_∞ be as follows

$$\varphi_\infty(w_1, w_2, w_3)=\begin{cases} p_\infty, \text{ if } w_1=w_2=w_3=0 \\ \text{the class of } z_{12}\in\tilde{\tilde{W}}_\infty \text{ w.r.t. } \mathfrak{G}', \\ \text{if } w_1=w_3=0 \text{ and } w_2 \text{ is as in Prop. 6,} \\ \text{the class of } (z_1, z_{12})\in\tilde{\tilde{V}}_\infty\text{w.r.t. } \tilde{M}_1, \\ \text{if } w_3=0 \text{ and } w_1,\ w_2 \text{ are as in Prop. 5,} \\ \text{the class of } Z\in\tilde{\tilde{U}}_\infty \text{ w.r.t. } M_2, \\ \text{if } w_1, w_2, w_3 \text{ are as in Prop. 4.} \end{cases}$$

We have to complete this definition of φ_∞ taking care of its G_∞-invariance. Then it can be proved easily by Prop. 4, 5, 6 that the system $\{\tilde{U}_\infty, G_\infty, \varphi_\infty\}$ satisfies the condition of l.u.s. and that there exist natural injections between these l.u.s. and the l.u.s. we have formerly defined. Thus we have established the junction of $\mathfrak{V}_2\smile\mathfrak{W}_1\smile\mathfrak{W}_{12}$ and $\mathfrak{V}_0$.

The compactness of $\overline{\mathfrak{V}}_2=\mathfrak{V}_2\smile\mathfrak{W}_1\smile\mathfrak{W}_{12}\smile\mathfrak{V}_0$ will be proved in the next section.

§ 5. The compactification of the case of $n=2$ (continued).

Let us put

Γ_2=the group of all unimodular matrices of degree 2,

$\Gamma_2(2)=\{U;\ U\in\Gamma_2,\ U\equiv I \pmod 2\}$.

Let $Y=\begin{pmatrix} y_1 & y_{12} \\ & y_2\end{pmatrix}$ be a positive definite symmetric matrix of degree 2. We shall call Y reduced w.r.t. $\Gamma_2(2)$ if the following conditions are satisfied:

$$\text{(i)} \qquad Y[\mathfrak{g}]\geqq y_1,$$

for all primitive integral vectors $g\equiv\begin{pmatrix}1\\0\end{pmatrix}$ (mod 2),

$$\text{(ii)} \qquad Y[\mathfrak{g}]\geqq y_2,$$

for all integral vectors $\mathfrak{g}=\begin{pmatrix}g_1\\g_2\end{pmatrix}\equiv\begin{pmatrix}0\\1\end{pmatrix}$ (mod 2) with $g_2=\pm1$,

$$\text{(iii)} \qquad y_{12}\geqq0.$$

Now $\Gamma_2(2)$ can be regarded as a discontinuous group of transformations of the space of all $Y>0$ in the following way:

$$U: Y\to Y[U].$$

Then we can prove analogously to the reduction theory of Minkowski that the totality of Y reduced w.r.t. $\Gamma_2(2)$ forms a fundamental region of the group of transformations $\Gamma_2(2)$.

We shall first prove the following lemma.

LEMMA 8. *Y is reduced w.r.t. $\Gamma_2(2)$ if and only if*

$$0 \leqq y_{12} \leqq y_1 \text{ and } y_2.$$

REMARK. It is known that Y is reduced in the sense of Minkowski, namely w.r.t. Γ_2 if and only if

$$0 \leqq 2y_{12} \leqq y_1 \leqq y_2.$$

PROOF. Putting $\mathfrak{g} = \begin{pmatrix} 2g_1'+1 \\ 2g_2' \end{pmatrix}$. (i) can be written as follows.

$$y_1(g_1'^2+g_1')+y_{12}(2g_1'g_2'+g_2')+y_2g_2'^2 \geqq 0.$$

We have, in particular, for $g_1'=0$, $g_2'=\pm 1$

$$\pm y_{12}+y_2 \geqq 0.$$

Similarly we have from (ii)

$$y_1 \pm y_{12} \geqq 0.$$

Hence we have $0 \leqq y_{12} \leqq y_1$ and y_2.

Conversely, assume that $0 \leqq y_{12} \leqq y_1$ and y_2. Then (i) is satisfied since

$$\begin{aligned} & y_1(g_1'+g_1')+y_{12}(2g_1'g_2'+g_2')+y_2g_2'^2 \\ \geqq & \, y_{12}(g_1'+g_1')+y_{12}(2g_1'g_2'+g_2')+y_{12}g_2'^2 \\ = & \, y_{12}\{(g_1'+g_2')^2+(g_1'+g_2')\} \geqq 0. \end{aligned}$$

Similary (ii) is also satisfied, q.e.d.

Now we shall proceed to the proofs of the propositions in the preceding section.

PROOF OF PROP. 4. (1) Let $\mathfrak{T}$ be the group of all translations

$$Z \to Z+S$$

with integral S. Then $\mathfrak{T}$ is a normal subgroup of $\mathfrak{G}''$, $\mathfrak{N}_0''$ and $\mathfrak{G}''$, $\mathfrak{N}_0''$ split into $\mathfrak{T}$ and the subgroups isomorphic to Γ_2, $\Gamma_2(2)$, respectively.

Now, since $\tilde{U}_\infty$ is sufficiently, small, it follows from Lem. 7 that the correspondence

$$(u_1, u_2, u_3) \to (w_1, w_2, w_3)$$

is one-to-one. Hence for $Z, Z' \in \tilde{\tilde{\tilde{U}}}{}_\infty^0$, we have $w_i(Z)=w_i(Z')$ $(1 \leqq i \leqq 3)$ if and only if $u_i(Z)=u_i(Z')$ $(1 \leqq i \leqq 3)$, namely

$$Z'=Z+S$$

with integral S. Therefore $\{(w_1, w_2, w_3) \in \tilde{U}_\infty;\ w_1 \cdot w_2 \cdot w_3 \neq 0\}$ is homeomorphic to the quotient space $\mathfrak{T} \backslash \tilde{\tilde{\tilde{U}}}{}_\infty^0$.

On the other hand, $\tilde{\tilde{\tilde{U}}}{}_\infty^0$ is invariant under the transformations

$$Z \to Z[U]$$

with

$$U = \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \pm\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \ \pm\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix},$$
$$\pm\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \pm\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \ \pm\begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix},$$

which form the isotropy group of $Z = \begin{pmatrix} 2z & z \\ z & 2z \end{pmatrix} \in \tilde{\tilde{U}}^0_\infty$. Since these transformations from a complete system of representatives of $\mathfrak{G}''/\mathfrak{N}_0'' \cong \Gamma_2/\Gamma_2(2)$, we have $\tilde{\tilde{U}}_\infty = \mathfrak{G}''\tilde{\tilde{U}}^0_\infty = \mathfrak{N}_0''\tilde{\tilde{U}}^0_\infty$.

It follows easily that for $Z, Z' \in \tilde{\tilde{U}}_\infty$, we have $w_i(Z) = w_i(Z')$ $(1 \leqq i \leqq 3)$ if and only if $Z' = \sigma(Z)$ with $\sigma \in \mathfrak{N}_0''$. Hence $\{(w_1, w_2, w_3) \in \tilde{U}_\infty; w_1 \cdot w_2 \cdot w_3 \neq 0\}$ is homeomorphic to the quotient space $\mathfrak{N}_0'' \backslash \tilde{\tilde{U}}_\infty$. Moreover $\mathfrak{N}_0''$ has no fixed point in $\tilde{\tilde{U}}_\infty$. For if it were not so, $\mathfrak{N}_0''$ would have a fixed point in $\tilde{\tilde{U}}^0_\infty$. Suppose that

$$Z = \sigma(Z) = Z[U] + S$$

for $Z \in \tilde{\tilde{U}}^0_\infty$, $\sigma \in \mathfrak{N}_0''$. Then we have $Y = Y[U]$. But by the definition of $\tilde{\tilde{U}}^0_\infty$, $y_1 - y_{12}$, $y_2 - y_{12}$, y_{12} are sufficiently large. Hence by Lem. 8 Y is in the interior of the fundamental domain of $\Gamma_2(2)$ constructed above. Hence $U = I$ and so $S = 0$. This completes the proof of (1).

(2) For any $Z \in \mathfrak{H}_2$ we can choose $\sigma \in \mathfrak{G}''$ such that $Z' = \sigma(Z)$ satisfies the following conditions:

(II) Y' is reduced in Minkowski's sense. Namely

$$0 \leqq 2y'_{12} \leqq y'_1 \leqq y'_2,$$

(III) $$\operatorname{abs} x'_{kl} \leqq \frac{1}{2} \qquad (1 \leqq k, l \leqq 2).$$

In the similar way as in §3 it is sufficient to show that if Z satisfies (II), (III) and y_{12} is sufficiently large, then Z is reduced in Siegel's sense. Hence we have only to prove the condition (I) stated in §3 under these assumptions.

The notations being the same as in the proof of Lem. 6, we have

$$\operatorname{abs} |CZ + D| \geqq |Y[Q]|.$$

Hence it is sufficient to show that for any Q, $|Y[Q]| \geqq 1$, if $K \leqq 2y_{12} \leqq y_1 \leqq y_2$ with sufficiently large K. If Q is a unimodular matrix, it is evident. Let Q be a primitive integral vector $\begin{pmatrix} q_1 \\ q_2 \end{pmatrix}$. Then

$$\begin{aligned} Y[Q] &= y_1q_1^2+2y_{12}q_1q_2+y_2q_2^2 \\ &= (y_1-y_{12})q_1^2+y_{12}(q_1+q_2)^2+(y_2-y_{12})q_2^2 \\ &\geqq \frac{K}{2}\{q_1^2+(q_1+q_2)^2+q_2^2\} \geqq \frac{K}{2}\,. \end{aligned}$$

This proves our assertion.

PROOF OF PROP. 5. (1) Let $\mathfrak{H}''$ be the group of all transformations of the form

$$(z_1, z_{12}) \to (z_1+s_1,\ \ \pm z_{12}+z_1g_1+s_{12})$$

with integral s_1, g_1, s_{12} and $\mathfrak{H}_0''$ be the subgroup of $\mathfrak{H}''$ formed of all transformations of the above form with $g_1 \equiv 0 \pmod 2$.

It is clear that $w_i(z_1, z_{12})=w_i(z_1', z_{12}')$ $(i=1, 2)$ if $(z_1', z_{12}')=\sigma(z_1, z_{12})$ for $\sigma \in \mathfrak{H}_0''$. The converse can be proved in the similar way as above, but it can be proved also as follows.

By the well-known formula in the theory of elliptic function we have

$$\frac{\vartheta_2^2(2z_{12}\,;\,1,\,4z_1)}{\vartheta_3^2(2z_{12}\,;\,1,\,4z_1)} = \frac{\vartheta_2^2}{\vartheta_3^2} \cdot \frac{\wp(2z_{12}\,;\,1,\,4z_1)-e_1}{\wp(2z_{12}\,;\,1,\,4z_1)-e_2}\,,$$

where

$$e_1=\wp\left(\frac{1}{2}\,;\,1,\,4z_1\right), \qquad e_2=\wp\left(\frac{1}{2}+2z_1;\,1,\,4z_1\right),$$

$$\vartheta_2=\vartheta_2(0;\,1,\,4z_1), \qquad \vartheta_3=\vartheta_3(0;\,1,\,4z_1).$$

The values of e_1, e_2, $\vartheta_2/e^{\pi i z_1}$, ϑ_3 depend only on z_1 modulo $\frac{1}{2}$.

Suppose that $w_i(z_1, z_{12})=w_i(z_1', z_{12}')$ $(i=1, 2)$. Then since

$$w_1(z_1, z_{12})\cdot w_2(z_1, z_{12})=e^{2\pi i z_1}$$

we have $z_1 \equiv z_1' \pmod 1$. Hence the corresponding values of e_1, e_2, ϑ_2^2, ϑ_3^2 coincide. Since

$$\frac{w_1(z_1, z_{12})}{w_2(z_1, z_{12})} = \frac{\vartheta_2^2(2z_{12}\,;\,1,\,4z_1)}{\vartheta_3^2(2z_{12}\,;\,1,\,4z_1)}$$

we have by the above formula

$$\wp(2z_{12}\,;\,1,\,4z_1)=\wp(2z_{12}'\,;\,1,\,4z_1').$$

It follows, as is well-known, that

$$2z_{12}' = \pm 2z_{12}+m_1 4z_1+m_2$$

with integral m_1, m_2. But if so, we have

$$w_1(z_1', z_{12}')=w_1(z_1, z_{12}')=(-1)^{m_2}\,w_1(z_1, z_{12}),$$

whence follows that $m_2 \equiv 0 \pmod 2$. This proves that $(z_1', z_{12}')=\sigma(z_1, z_{12})$ with $\sigma \in \mathfrak{H}_0''$.

Now, $\overset{\approx}{\widetilde{V}}{}^0_\infty$ is invariant under the transformation

$$(z_1, z_{12}) \rightarrow (z_1, -z_{12}+z_1),$$

which leaves invariant the points of the form $(2z, z)$. Since this transformation together with the identity forms a complete system of representatives of $\mathfrak{H}''/\mathfrak{H}_0''$, we have $\overset{\approx}{\widetilde{V}}_\infty = \mathfrak{H}''\overset{\approx}{\widetilde{V}}{}^0_\infty = \mathfrak{H}_0''\overset{\approx}{\widetilde{V}}{}^0_\infty$. Hence it follows from what we have said above that $\{(w_1, w_2);\ (w_1, w_2, 0) \in \widetilde{U}_\infty,\ w_1 \cdot w_2 \neq 0\}$ is homeomorphic to the quotient space $\mathfrak{H}_0''\backslash\overset{\approx}{\widetilde{V}}_\infty$.

Since the fixed points (z_1, z_{12}) of $\mathfrak{H}_0''$ is of the form

$$z_{12} = z_1\frac{g_1}{2} + \frac{s_{12}}{2}$$

with g_1, s_{12} integral and $g_1 \equiv 0 \pmod 2$, we have $y_{12} = y_1\frac{g_1}{2}$ with integral $\frac{g_1}{2}$. But for $(z, z_{12}) \in \overset{\approx}{\widetilde{V}}{}^0_\infty$ we have $y_1 > y_{12} > 0$. Therefore $\overset{\approx}{\widetilde{V}}{}^0_\infty$ has no fixed point of $\mathfrak{H}_0''$, hence so is also $\overset{\approx}{\widetilde{V}}_\infty$. This proves (1).

(2) It can be proved easily that a fundamental region of $\widetilde{M}_1$ is given by the totality of (z_1, z_{12}) satisfying the following conditions:

($*$) z_1 is reduced,

(II′) $$0 \leqq 2y_{12} \leqq y_1,$$

(III′) $$\operatorname{abs} x_{12} \leqq \frac{1}{2}.$$

For any $(z_1, z_{12}) \in \mathfrak{H}_1 \times C$ we can choose $\sigma \in \mathfrak{H}''$ such that $(z_1', z_{12}') = \sigma(z_1, z_{12})$ satisfies (II′) and

(III) $$\operatorname{abs} x_1,\ \operatorname{abs} x_{12} \leqq \frac{1}{2}.$$

Hence (2) follows from the fact that if (z_1, z_{12}) satisfies the conditions (II′) (III) and y_{12} is sufficiently large, then it satisfies also the condition ($*$).

PROOF OF THE COMPACTNESS OF $\mathfrak{B}_2$. Let $\{p_k\}$ be a sequence in $\mathfrak{B}_2$, p_k being the class of $Z^{(k)} \in \mathfrak{H}_2$ w.r.t. M_2. We may assume $Z^{(k)}$ to be reduced in Siegel's sense. Then we have, in particular,

(II) $$0 \leqq 2y_{12}^{(k)} \leqq y_1^{(k)} \leqq y_2^{(k)}.$$

If $y_2^{(k)}$ is bounded, then $Z^{(k)}$ is bounded so that we can choose a subsequence of $\{Z^{(k)}\}$ which is convergent in $\mathfrak{H}_2$. Then the corresponding subsequence of $\{p_k\}$ converges in $\mathfrak{B}_2$.

If $y_1^{(k)}$ is bounded but not $y_2^{(k)}$, then we can choose a subsequence $\{Z'^{(k)}\}$ such that $\{(z_1'^{(k)}, z_2'^{(k)})\}$ converges to $(z_1, z_{12}) \in \mathfrak{H}_1 \times C$ and $y_2'^{(k)} \rightarrow \infty$.

Then the corresponding subsequence $\{p'_k\}$ of $\{p_k\}$ converges to the class of (z_1, z_{12}) in $\mathfrak{W}_1$.

If $y_{12}^{(k)}$ is bounded but not $y_1^{(k)}$, then we can choose a subsequence $\{Z'^{(k)}\}$ such that $\{z'^{(k)}_{12}\}$ converges to $z_{12} \in C$ and $y'^{(k)}_1 \to \infty$, $y'^{(k)}_2 \to \infty$. Then the corresponding subsequence $\{p'_k\}$ of $\{p_k\}$ converges to the class of z_{12} in $\mathfrak{W}_{12}$.

If $y_{12}^{(k)}$ is not bounded, then we can choose a subsequence $\{Z'^{(k)}\}$ of $\{Z^{(k)}\}$ such that $y_{12}^{(k)} \to \infty$. Then by (II) we have also $y'^{(k)}_1 - y'^{(k)}_{12} \to \infty$, $y'^{(k)}_2 - y'^{(k)}_{12} \to \infty$. Hence the corresponding subsequence $\{p'_k\}$ of $\{p_k\}$ converges to $p_\infty \in \mathfrak{V}_0$.

Similarly, we can prove that any sequence from $\mathfrak{W}_1 \smile \mathfrak{W}_{12} \smile \mathfrak{V}_0$, $\mathfrak{W}_{12} \smile \mathfrak{V}_0$ has a convergent subsequence. In fact we have, as was stated at the beginning of §4,

$$\mathfrak{W}_1 \smile \mathfrak{W}_{12} \smile \mathfrak{V}_0 \approx \bar{C} \times \bar{C},$$

$$\mathfrak{W}_{12} \smile \mathfrak{V}_0 \approx \bar{C}.$$

Hence the V-manifold $\bar{\mathfrak{V}}_2 = \mathfrak{V}_2 \smile \mathfrak{W}_1 \smile \mathfrak{W}_{12} \smile \mathfrak{V}_0$ is compact.

We have thus established the following theorem.

THEOREM 1. $\mathfrak{V}_2 = M_2 \backslash \mathfrak{H}_2$ *can be completed to a compact V-manifold* $\bar{\mathfrak{V}}_2$. $\bar{\mathfrak{V}}_2$ *is a junction of* $\mathfrak{V}_2$ *und* $\overline{\mathfrak{W}}_2$ *homeomorphic to* $\bar{C} \times \bar{C}$.

UNIVERSITY OF TOKYO

BIBLIOGRAPHY

[1] C. L. Siegel, Einführung in die Theorie der Modulfunktionen n-ten Grades, Math. Ann., **116** (1939).

[2] C. L. Siegel, Lectures on the analytical theory of quadratic forms, Princeton (1934–35).

[3] H. Cartan, Fonctions automorphes et espaces analytiques, seminaire (1953–54).

Plongement Projectif d'une Variété de Groupe

Claude CHEVALLEY

Soit V une variété définie sur un corps K et qui admet une loi de composition normale définie sur K. Il a été établi par M. Barsotti qu'il y a une variété projective définie sur K, birationnellement équivalente à V, dont une partie ouverte convenable est une variété de groupe (relativement à la loi normale donnée). Nous nous proposons d'indiquer le schéma d'une nouvelle démonstration de ce fait; cette démonstration fait usage de la technique des spécialisations de cycles, à laquelle nous nous proposons de consacrer prochainement une étude. Cette étude n'étant pas encore publiée, nous nous abstiendrons d'entrer ici dans le détail de certaines démonstrations.

Faisant usage des travaux de A. Weil sur la théorie des variétés de groupes, on sait d'une part que V est birationnellement équivalente à une variété de group G définie sur un sur-corps K' de K, d'autre part qu'il y a une partie ouverte V_1 de V, définie sur K, qui est un "morceau de groupe" (group chunk); on peut supposer sans restriction de généralité que $V_1 = V$, que V est une variété affine définie sur K et que V est une partie ouverte de G.

Montrons d'abord qu'on peut supposer que K' est la fermeture algébrique $\bar{K}$ de K (dans le domaine universel). Soit $V_{\bar{K}}$ l'ensemble des points de V algébriques sur K. Alors tout $u \in G$ peut se mettre sous la forme st, avec $s \in V_{\bar{K}}$, $t \in V$; en effect, uV^{-1} est une partie ouverte de G, et $V \frown uV^{-1}$ est une partie ouverte non vide de V, qui contient donc au moins un point de $V_{\bar{K}}$, ce qui démontre notre assertion. De plus, il y a un nombre fini de points s_i $(1 \leqq i \leqq h)$ de $V_{\bar{K}}$ tels que G soit la réunion des s_iV, comme il résulte tout de suite du fait que tout ensemble non vide de parties ouvertes de G admet au moins un élément maximal. Soint $\xi_1, \cdots, \xi_n$ les coordonnées affines sur V. Pour chaque i $(1 \leqq i \leqq h)$, soient $\xi_j^{(i)}$ les fonctions sur s_iV définies per $\xi_j^{(i)}(s_ix) = \xi_j(x)$; ces fonctions définissent sur s_iV une structure de variété affine définie sur $\bar{K}$. Soit x_0 un point générique de V sur K. Pour chaque i, x_0 appartient à s_iV et est un point rationel sur $\bar{K}(x_0)$ de cette variété affine. Soit T_i la fonction sur V à valeurs dans $s_i V$, définie sur $\bar{K}$, telle que $T_i(x_0)=x_0$; c'est une correspondance birationnelle. Si i, i' sont des indices quelconques entre 1 et h, il y a une fonction $T_{ii'}$ sur $s_i V$ à valeurs dans $s_{i'}V$, définie sur $\bar{K}$, telle que $T_{ii'}(x_0)=x_0$. Les correspondances $T_{ii'}$ sont partout birégulières: elles définissent sur $G=\bigcup_{i=1}^{h} s_i V$ une structure de variété de groupe définie sur $\bar{K}$, ce qui démontre notre assertion. Supposons donc à partir de maintenant la variété G définie sur $\bar{K}$.

Ceci dit, le principe de la démonstration consiste à construire un diviseur D de V, rationnel sur K, qui possède la propriété suivante: l'application qui à tout $s \in G$ fait correspondre la trace sur l'ouvert V de G du diviseur translaté sD de D est injective. On associera alors à s le point de Chow dans l'espace projectif P ambiant de V (qui est affine) de la trace de sD sur V (considérée comme définissant un cycle de P).

LEMME 1. *Soit s un élément de G rationnel sur $\bar{K}$ qui possède la propriété suivante: pour tout $x \in V_K$ tel que $sx \in V$, sx est conjugué de x par rapport à K. Alors s est l'élément neutre I.*

On peut évidemment supposer $\dim G>0$. Il existe des fonctions rationnelles $f_1, \cdots, f_n$ en n lettres à coefficients dans $\bar{K}$ (n étant la dimension de l'espace affine ambiant de V) telles que, pour tout point $a=(a_1, \cdots, a_n)$ de V tel que les f_i soient définies en a, sa soit dans V et que l'on ait $\xi_i(sa)=f_i(a_1, \cdots, a_n)$ (les ξ_i étant les fonctions coordonnées sur V). Soit i un indice tel que ξ_i ne soit pas constante. Soit w_0 un point générique de V sur K, et soit F la fonction sur V, à valeurs dans le plan affine, définie sur $\bar{K}$, telle que $F(v_0)=(\xi(v_0), f_i(\xi_1(v_0), \cdots, \xi_n(v_0)))$; soit C le lieu de $F(v_0)$ par rapport à $\bar{K}$. Soit U l'ensemble des points $a \in V$ en lequel toutes les f_i sont définies; il existe une partie ouverte non vide Γ de C telle que tout point $(x, y) \in \Gamma$ qui est rationnel sur $\bar{K}$ soit l'image par F d'un point de $U \frown V_K$; il en résulte que, si $(x, y) \in \Gamma$, y est conjugué de x par rapport à K. Montrons que C est une courbe. Puisque ξ_i n'est pas constante, la première fonction coordonnée n'est pas constante sur C; il suffit donc de montrer que C n'est pas le plan tout entier; or, dans le cas contraire, pour tout point $(x, y) \in \Gamma$ rationnel sur $\bar{K}$, il y aurait une infinité de points $y' \in \bar{K}$ tels que $(x, y') \in F(U)$, ce qui n'est pas.

Soit $P(X, Y)=0$ une équation de C. Il y a une partie finie A de $\bar{K}$ telle que, pour $x \in \bar{K}-A$, tout point de C d'abcisse x appartienne à $F(U)$. Supposons d'abord K infini. Il y a une infinité de points

$x \in K-A$ tels que l'équation $P(x, Y)=0$ ait au moins une solution dans K; cette solution étant conjuguée de x par rapport à K est égale à x; comme $P(x, x)=0$ pour une infinité de valeurs de x, on a $P(X, X)=0$ et C est la diagonale du plan. On a donc $f_i(\xi_1, \cdots, \xi_n)=\xi_i$ pour tout indice i tel que ξ_i ne soit pas constant. La même formule subsiste évidemment si ξ_i est constant. On a donc $sx=x$ pour tout $x \in U$, d'où $s=I$. Supposons maintenant que K soit un corps fini à q éléments. Pour tout $N>0$, soit K_N le corps fini à q^{2N} éléments. Il y a un nombre fixe c tel que, exception faite pour au plus c valeurs de x, la condition $x \in K_N$ entraîne que l'équation $P(x, Y)=0$ ait une racine de la forme $x^{q^\nu}(0 \leqq \nu \leqq 2N-1)$. Nous allons montrer qu'il y a un m tel que l'on ait ou bien $P(X, X^{q^m})=0$ ou bien $P(X^{q^m}, X)=0$. Supposons le contraire. Désignons par e le degré de P. Le nombre de solutions de l'équation $P(x, x^{q^\nu})$ est au plus eq^ν. Supposons $\nu \geqq N$, et évaluons autrement le nombre de solutions de l'équation proposée en éléments de K_N. Soit P' le polynome déduit de P en élevant ses coefficients à la puissance $q^{2N-\nu}$; si $P(x, x^{q^\nu})=0$, $x \in K_N$, on a aussi $P'(x^{q^{2N-\nu}}, x)=0$; cette équation a au plus $eq^{2N-\nu}$ solutions. Le nombre des $x \in K_N$ tels que $P(x, Y)=0$ ait une solution conjuguée de x par rapport à K est donc $\leqq 2e(1+\cdots+q^N)=2e(q^{N+1}-1)(q-1)^{-1}$; la différence entre ce nombre et q^{2N} devient $>c$ pour N assez grand, d'où contradiction. On conclut de là que, si ξ_i n'est pas constante, il y a un automorphisme fixe σ_i de $\bar{K}/K$ tel que, pour tout $v \in V_K \frown U$, on ait $\xi_i(sv)=\sigma_i(\xi_i(v))$. Ceci dit, l'ensemble $V-U$ n'a qu'un nombre fini de composantes irréductibles, et ces composantes sont définies sur $\bar{K}$. On en déduit que l'intersection U' de U et de ses conjugués par rapport à K est une partie ouverte non vide de V; si $v \in V_K \frown U'$, on voit par récurrence sur k que les $s^k v$ sont tous conjugués de v par rapport à K et appartiennent à U'; comme v n'a qu'un nombre fini de conjugués par rapport à K, il en résulte que s est d'ordre fini. On a alors, pour tout $v \in U' \frown V_K$, $\xi_i(v)=\xi_i(s^r v)=(\xi_i(v))^{\sigma_i^r}$, si r est tel que $s^r=I$. Or, si ξ_i n'est pas constante, il y a des points $v \in U' \frown V_K$ tels que $K(\xi_i(v))$ soit une extension de degré arbitrairement grand de K; on en conclut que σ_i^r est l'automorphisme identique de $\bar{K}$. Mais il est bien connu qu'aucun automorphisms distinct de l'identité de $\bar{K}/K$ n'est d'ordre fini; σ_i est donc l'identité, et le lemme est démontré.

Ceci dit, il nous sera commode dans la suite de pouvoir supposer que $r \geqq 2$. Nous allons d'abord traiter séparément le cas où $r=1$. L'adhérence de V dans l'espace projectif P est alors une courbe $\bar{V}$; on en déduit par le processus de normalisation par rapport à K une courbe $\overline{V}_1$ normale sur K, définie sur K. Cette courbe n'est pas nécessairement absolument normale, mais on en déduit une courbe absolument normale $\overline{V}_2$ par le processus de normalisation par rapport à un sur-corps K_2 de K, que l'on peut supposer purement inséparable sur K; la courbe $\overline{V}_2$ n'est définie que sur K_2. Comme $\overline{V}_2$ et G sont des courbes sans singularité, et comme $\overline{V}_2$ est complète, il y a une bijection de G sur une partie ouverte V_2 de $\overline{V}_2$ qui est une correspondance birationnelle partout birégulière; V_2 est donc une variété de groupe. Soit V_1 son image dans $\overline{V}_1$; comme $\overline{V}_1$ est définie sur K, il suffira d'établir que V_1 est une variété de groupe. Or cela résultera de l'assertion suivante, qui nous sera encore utile dans la suite:

PROPOSITION 1. *Soit V une variété définie sur un corps K, normale sur K et munie d'une loi de composition normale définie sur K. Soit V' une variété* (*absolument*) *normale déduite de V par normalisation sur un sur-corps K' de K algébrique et purement inséparable sur K. Si V' est une variété de groupe, il en est de même de V.*

Soient x_0, y_0 des points génériques indépendants de V sur K, et soient x, y des points quelconques de V. Comme V, et par suite aussi $V\times V$, est normale sur K, il suffira, pour montrer que la multiplication dans le groupe est définie au point (x, y), d'établir qu'il y a une extension et une seule de la spécialisation $(x_0, y_0)\rightarrow(x, y)$ en une spécialisation de (x_0, y_0, x_0y_0). Soit T le graphe de la correspondance birationnelle entre V et V'; comme V' se déduit de V par normalisation sur K', T est une variété qui est complète au-dessus de tout point de V; comme K' est purement inséparable sur K, T définit une bijection de V' sur V. Soient s_0, t_0, s, t les points de V' qui correspondent à x_0, y_0, x, y. Comme K' est purement inséparable sur K, $(x_0, y_0)\rightarrow(x, y)$ est une spécialisation sur K'; T étant définie sur K', il résulte tout de suite de ce que nous avons dit que $(x_0, y_0, s_0, t_0)\rightarrow(x, y, s, t)$ est une spécialisation sur K'; il en est donc de même de $(x_0, y_0, s_0, t_0, s_0t_0)\rightarrow(x, y, s, t, st)$; on en déduit que, si z est le point de V tel que $(z, st)\in T$, $(x_0, y_0, x_0y_0)\rightarrow(x, y, z)$ est une spécialisation sur K. Soit réciproquement z_1 tel que $(x_0, y_0, x_0y_0)\rightarrow(x, y, z_1)$ soit une spécialisation sur K, donc aussi sur K'. Utilisant toujours le fait que T est complète au-dessus de tout point de V, on voit que cette spécialisation se prolonge en une spécialisation de $(x_0, y_0, x_0y_0, s_0, t_0)$, donc aussi de $(x_0, y_0, x_0y_0, s_0, t_0, s_0t_0)$, d'où il résulte tout de suite que $(z_1, st)\in T$, *d'où* $z_1=z$. Ceci démontre la prop. 1.

Retournons aux notations utilisées plus haut, et supposons à partir de maintenant que la dimension r de la variété affine V est

$\geqq 2$. Tout cycle Z de V définit un cycle $\bar{Z}$ de la variété projective $\bar{V}$ adhérence de V dans l'espace projectif P. Par ailleurs, Z définit aussi un cycle $\tilde{Z}$ dans la variété G; si $s \in G$, nous désignerons par $F(s, Z)$ la trace sur V du cycle $s\tilde{Z}$ de G.

LEMME 2. *Soit n un entier >0, et soit s un élément $\neq I$ de G rationnel sur $\bar{K}$. Il existe alors un diviseur positif premier rationnel sur K, soit D, de V qui possède les propriétés suivantes: on a $|D| \neq |F(s, D)|$, et les composantes de D sont des variétés de degré $\geqq n$, rationnelles sur $\bar{K}$.*

(Nous désignons par $|Z|$ le support d'un cycle Z; nous appelons degré d'un cycle Z sur V le degré du cycle $\bar{Z}$ de P). Pour tout $m>0$, les diviseurs positifs de degré m de P sont représentés par les points d'un espace projectif Q_m. Soit E_m l'ensemble des points de Q_m qui représentent des diviseurs A de P tels que ou bien $\bar{V} \subset |A|$ ou bien $\bar{V} \cdot A$ ne soit pas une variété irréductible prise avec le coefficient 1; E_m est une partie fermée de Q_m, et, comme $r \geqq 2$, il résulte d'un lemme de Nakai que $\dim Q_m - \dim E_m$ augmente indéfiniment avec m, donc est $\geqq 2$ pour m assez grand. Soit x un point de V_K tel que sx soit dans V mais ne soit pas conjugué de x par rapport à K (lemma 1). Les points représentatifs des diviseurs dont les supports contiennent un point donné de P forment une sous-variété de codimension 1 de Q_m; prenant donc m assez grand, il y a un point $a \in Q_m - E_m$ qui représente un diviseur A tel que $x \in |A|$ mais qu'aucun conjugué de sx par rapport à K n'appartienne à $|A|$; on peut de plus supposer a rationnel sur $\bar{K}$. La trace sur V de $\bar{V} \cdot A$ est de la forme $1 \cdot D_1$, où D_1 est une variété rationnelle sur $\bar{K}$, de degré $\geqq m$; de plus, si σ est un automorphisme de $\bar{K}/K$, $\sigma \cdot D_1$ ne contient pas le point $s \cdot x$; soit D le cycle premier rationnel sur K déterminé par D_1; on a donc $x \in |D|$, $sx \notin |D|$; comme $sx \in |F(s, D)|$, on a $|F(s, D)| \neq |D|$; si on a pris $m \geqq n$, D possède les propriétés requises.

Tenant compte de ce que $G - V$ ne contient qu'un nombre fini de variétés de dimension $r-1$, on voit facilement qu'il y a un $m_0 > 0$ qui possède la propriété suivante: si A est une sous-variété de dimension $r-1$ de V de degré $\geqq m_0$, et si s est élément quelconque de G, $s\tilde{A}$ rencontre V. Si D est un diviseur positif de V dont toutes les composantes sont de degrés $\geqq m_0$, une condition nécessaire et suffisante pour que $F(s, D) = F(s', D)$ est que l'on ait $s\tilde{D} = s'\tilde{D}$, i.e. $s^{-1}s'\tilde{D} = \tilde{D}$.

En effet, si on avait $F(s, D)=F(s', D)$, $s\tilde{D}\neq s'\tilde{D}$, il y aurait au moins une composante A de D telle que l'une au moins des variétés $s\tilde{A}$, $s'\tilde{A}$ soit dans $G-V$, ce qui est impossible.

Si $\varDelta$ est un diviseur positif sur G, rationnel sur $\bar{K}$, l'ensemble des $s\in G$ tels que $s\varDelta=\varDelta$ est évidemment un ensemble fermé rationnel sur $\bar{K}$ (car si A et B sont des sous-variétés de G rationnelles sur $\bar{K}$, l'ensemble des s tels que $sA=B$ est fermé et rationnel sur $\bar{K}$).

LEMME 3. *Il existe un diviseur positif D de V rationnel sur K tel que $s\rightarrow F(s, D)$ soit une application injective de G dans l'ensemble des diviseurs de V.*

Nous construirons par récurrence une suite finie (D_k) de diviseurs positifs rationnels sur K de V dont toutes les composantes sont de degrés $\geqq m_0$ (m_0 ayant la propriété indiquée ci-dessus). Nous partons d'un diviseur premier rationnel sur K_1, soit D_1, dont les composantes sont de degrés $\geqq m_0$. Si D_k est construit, et si $s\rightarrow F(s, D_k)$ est injective, nous arrêtons notre construction. Sinon, l'ensemble E_k des $s\in G$ tels que $s\tilde{D}_k=\tilde{D}_k$, qui est fermé et rationnel sur $\bar{K}$, contient au moins un point $s_k\neq I$ rationnel sur $\bar{K}$, puisque les composantes de D_k sont de degrés $\geqq m_0$. Les degrés des cycles $F(s, D_k)$ pour tous les $s\in G$ sont bornés; soit m_{k+1} un entier strictement supérieur à tous ces degrés. Il existe un diviseur positif A_{k+1} de V, rationnel sur K, dont les composantes sont de degrés $\geqq \max(m_{k+1}, m_0)$ tel que $E(s_k, A_{k+1})\neq A_{k+1}$; soit $D_{k+1}=D_k+A_{k+1}$. On voit alors facilement que, si $s\in G$ est tel $sD_{k+1}=D_{k+1}$, on doit avoir $sD_k=D_k$, d'où $s\in E_k$, et $sA_{k+1}=A_{k+1}$, d'où $s\neq s_k$; l'ensemble E_{k+1} est donc contenu dans E_k mais $\neq E_k$. Comme les E_k sont des ensembles fermés, notre construction s'arrête au bout d'un nombre fini de pas, ce qui démontre le lemme.

Soit D un diviseur qui possède la propriété du lemme 3. Soit v_0 un point générique de V par rapport à K, et soit Z_0 le cycle $F(v_0, D)$ de l'espace projectif P. Nous désignerons par γ_0 le point de Chow de ce cycle.

Le cycle $F(v_0, D)$ est rationnel sur $K(v_0)$; c'est en effet l'image de D par la fonction f sur V à valeurs dans V telle que $f(x)=v_0x$ pour tout $x\in V$ tel que $v_0x\in V$, et f est définie sur $K(v_0)$. Il résulte de là que Z_0 est rationnel sur $K(v_0)$, d'où $K(\gamma_0)\subset K(v_0)$. Par ailleurs, $K(v_0)$ est purement inséparable sur $K(\gamma_0)$. Soit en effet σ un automorphisme du domaine universel qui laisse fixes les points de $K(\gamma_0)$, donc aussi les cycles Z_0 et $F(v_0, D)$; comme σ transforme $F(v_0, D)$ en $F(\sigma\cdot v_0, D)$, il résulte du caractère injectif de l'application $s\rightarrow F(s, D)$

que $\sigma\cdot v_0 = v_0$, ce qui démontre notre assertion.

Soit Γ_0 le lieu de γ_0 par rapport à K. On sait qu'il existe une variété projective Γ_1 définie sur K, un point générique γ_1 de Γ_1 par rapport à K et une application φ de Γ_1 sur Γ_0 qui possèdent les propriétés suivantes: on a $K(\gamma_1) = K(v_0)$, $\varphi(\gamma_1) = \gamma_0$; Γ_1 est normale sur K; φ est définie sur K, est partout définie sur Γ_1 et l'image réciproque par φ de tout point de Γ_0 est un ensemble fini.

Soit Γ_2 une variété projective absolument normale déduite de Γ_1 par normalisation sur une extension algébrique purement inséparable K' de K. Il y a donc une application bijective ψ de Γ_2 sur Γ_1, définie sur K', qui est partout définie, qui est une correspondance birationnelle entre Γ_2 et Γ_1. Soit γ_2 le point de Γ_2 tel que $\psi(\gamma_2) = \gamma_1$; c'est un point générique de Γ_2 sur $\bar{K}$, et $\bar{K}(\gamma_2) = \bar{K}(v_0)$. Il y a donc une fonction g sur G, à valeurs dans Γ_2, définie sur $\bar{K}$, telle que $g(v_0) = \gamma_2$. Nous allons montrer que g est partout définie. Soit $s \in G$; comme Γ_2 est complète, il y a au moins un $\delta_2 \in \Gamma_2$ tel que $(v_0, \gamma_2) \to (s, \delta_2)$ soit une spécialisation sur $\bar{K}$; G étant normale, pour montrer que g est définie en s, il suffit de montrer qu'il n'y qu'un nombre fini de points δ_2 possédant cette propriété. Comme l'image réciproque de tout point de Γ_0 par $\varphi\circ\psi$ est finie, il suffit de montrer qu'il n'y qu'un nombre fini de points γ_0 de Γ_0 tels que $(v_0, \gamma_0) \to (s, \delta_0)$ soit une spécialisation sur $\bar{K}$, donc qu'il n'y qu'un nombre fini de cycles Z de l'espace projectif tels que $(v_0, Z_0) \to (s, Z)$ soit une spécialisation sur $\bar{K}$. Or, soit Z un pareil cycle. La théorie des spécialisations de cycles montre qu'il existe un cycle X sur V tel que $(v_0, Z_0, F(v_0, D)) \to (s, Z, X)$ soit une spécialisation sur $\bar{K}$. Or la spécialisation $v_0 \to s$ se prolonge d'une manière et d'une seule en une spécialisation de $(v_0, v_0\tilde{D})$ qui spécialise $v_0\tilde{D}$ en $s\tilde{D}$; comme $F(v_0, D)$ est la trace de $v_0\tilde{D}$ sur V, on en conclut que X est la trace de $s\tilde{D}$ sur V, d'où $X = F(s, D)$. Par ailleurs, X est aussi la trace sur V du cycle Z de l'espace projectif; Z est donc la somme de $F(s, D)$ et d'un cycle de $\bar{V}$ dont les composantes ne rencontrent pas V. Mais $\bar{V} - V$ ne contient qu'un nombre fini de variétés de dimension $r-1$; comme par ailleurs Z est du même degré que Z_0, on voit qu'il n'y qu'un nombre fini de possibilités pour Z, et notre assertion est établie. De plus, on voit que $(\varphi\circ\psi)(g(s))$ est le point de Chow d'un cycle dont la trace sur V est $F(s, D)$, ce qui montre que g est une application bijective de G sur $g(G)$. Soit h la fonction sur Γ_2 à valeurs dans G, définie sur $\bar{K}$, telle que $h(\gamma_2) = v_0$.

Si $\delta_2=g(s)$, avec un $s \in G$, $(\gamma_2, v_0)\to(\delta_2, s)$ est une spécialisation sur $\overline{K}$; comme g est injective et définie sur $\overline{K}$, s est le seul point de G possédant cette propriété; comme Γ_2 est normale, il en résulte que h est définie en tout point de Γ_2. De plus, h ne peut évidemment être définie en un point de Γ_2 n'appartenant pas à $g(G)$; ce dernier ensemble est donc ouvert dans Γ_2 et est une variété de groupe. Il résulte alors de la proposition 1 que $\psi(g(G))$ est un variété de groupe. Comme Γ_1 est définie sur K, le théorème est démontré.

COLUMBIA UNIVERSITY

Arithmétique et Classes de Diviseurs sur les Variétés Algébriques

André NÉRON

1.—Introduction.

Pour toute variété algébrique V, nous désignons par $G(V)$ le groupe des V-diviseurs, par $G_a(V)$ le groupe des V-diviseurs algébriquement équivalents à zéro, par $G_l(V)$ le groupe de V-diviseurs linéairement équivalents à zéro. Pour tout corps k de définition de V, nous désignons par $G^k(V)$ le groupe de V-diviseurs rationnels sur k et par $G_a^k(V)$ et $G_l^k(V)$ les intersections de ce groupe avec $G_a(V)$ et $G_l(V)$ respectivement. Rappelons les résultats suivants, valables pour toute variété V projective normale.

(A)—Le groupe $G_a(V)/G_l(V)$ est "birationnellement isomorphe" au groupe des points d'une variété abélienne appelée variété de Picard de V (voir [1], [2], [3], [5]).

(B)—Le groupe $G(V)/G_a(V)$ est un groupe de type fini ([9], [4]).

L'une des méthodes les plus fréquement utilisées pour étudier ces deux derniers groupes consiste à "fibrer" V par une famille de courbes paramétrée par une variété algébrique B. Il est commode d'autre part d'introduire un "demi-domaine universel" F (Cf [5]), c'est-à-dire un sous-corps F algébriquement fermé du domaine universel, de degré de transcendance infini sur le corps premier, et tel que le domaine universel soit lui-même de degré de transcendance infini sur F. L'étude des groupes $G(V)$, $G_a(V)$, $G_l(V)$ se ramène, par transport de structure, à celle des groupes $G^F(V)$, $G_a^F(V)$, $G_l^F(V)$. On peut alors considérer un point générique M de B sur F et la courbe C de paramètre M. Pour tout $X \in G^F(V)$, l'intersection $X \cdot C$ est définie. L'application $\theta : X \rightarrow X \cdot C$ est un homomorphisme de $G^F(V)$ sur $G^{F(M)}(C)$. Soit $H^F(V, C)$ le noyau de cet homomorphisme, c'est-à-dire le groupe composé des V-diviseurs rationnels sur F et dont aucune composante ne rencontre C. Posons $H_l^F(V,C) = G_l^F(V) + H^F(V,C)$. On montre sans difficulté que les relations $X \in H_l^F(V,C)$ et $X \cdot C \in G_l^{F(M)}(C)$ sont équivalentes. Donc $H_l^F(V, C) = \theta^{-1}(G_l^{F(M)}(C))$, et on a l'isomorphisme

$$G^F(V)/H_l^F(V, C) \approx G^{F(M)}(C)/G_l^{F(M)}(C).$$

Or il est possible, en raisonnant par récurrence sur la dimension de V, de ramener l'étude de la structure du groupe $G^{F'}(V)/G_l^{F'}(V)$ à celle du groupe $G^{F'}(V)/H_l^{F'}(V, C)$. On voit ainsi apparaître l'analogie entre le problême de la détermination de la structure de $G(V)/G_l(V)$ et le problème arithmétique traité par Weil dans sa thèse [10], à savoir celui de la détermination de la structure du groupe $G^k(C)/G_l^k(C)$, où k un corps de nombres algébriques et C une courbe définie sur k. Compte tenu de l'isomorphisme précédent, le premier problème ne diffère essentiellement du second que par la substitution du corps de fonctions $F(M)$ au corps de nombres k.

En exploitant cette analogie, j'ai obtenu dans ma thèse [4] une démonstration de (B) et, en même temps, de certains résultats de nature partiellement arithmétique. En particulier, le groupe $G^k(C)/G_l^k(C)$ est de type fini pour tout corps k de type fini et toute courbe C définie sur k[1] (Dans le cas particulier où k est un corps de nombres, c'est le théorème de Weil).

Cependant, il est possible de mettre en évidence, plus nettement qu'il n'apparaît dans ces démonstrations, le parallélisme entre le cas des corps de nombres et celui des corps de fonctions. On peut en effet adapter de façon explicite au cas des corps de fonctions l'une des théories qui jouent chez Weil un rôle essentiel, celle nommée par lui théorie des "distributions". Rappelons que celle-ci, initialement introduite et développée par Weil dans le premier chapitre de sa thèse, a été reprise et développée par Northcott ([6], [7]), puis à nouveau par Weil sous une forme plus abstraite dans un mémoire des Annals of Mathematics [12]. En prenant ce dernier mémoire comme point de départ, je me propose déssayer de montrer comment on peut réaliser l'adaptation annoncée et, en même temps, obtenir une simplification de la dernière partie (celle qui concerne la "descente infinie") de la démonstration de (B) que j'ai donnée dans [4].

2.—La théorie des "distributions" pour les points à coordonnées dans un corps de fonctions algébriques.

Dans les deux premiers paragraphes, nous allons retranscrire quelques définitions et résultats du mémoire de Weil [12] auquel nous renvoyons pour des détails plus complets, et en particulier pour les démonstrations.

[1] Il semble possible d'étendre assez facilement ce résultat au cas du groupe $G^k(V)/G_l^k(V)$ attaché à un corps de type fini k et à une variété V *quelconque* définie sur k, en utilisant la variété de Picard de V au lieu de la jacobienne de C.

1. Fonctions de valuation.

Soit K un corps. Notons $\mathbf{V}(K)$ l'ensemble des valuations canoniques non triviales de K. Pour tout sous-anneau de K notons $\mathbf{V}(K/A)$ le sous-ensemble de $\mathbf{V}(K)$ formé des valuations de $\mathbf{V}(K)$ qui sont $\geqq 0$ sur A (donc en particulier nulles sur A si A est un corps). Notons K^* le groupe multiplicatif des éléments non nuls de K et considérons le groupe $\mathbf{F}'(K)=\Pi_{\omega\in \mathbf{V}(K)}\omega(K^*)$ des "fonctions" qui font correspondre à toute valuation de K^* une valeur de cette valuation. A tout $x\in K^*$ correspond un élément de $\mathbf{F}'(K)$ noté $[x]$ et défini par $[x](\omega)=\omega(x)$. Or puisque les $\omega(K^*)$ sont des groupes totalement ordonnés, $\mathbf{F}'(K)$ est un groupe réticulé. Le sous-groupe minimal de $\mathbf{F}'(K)$ contenant les $[x]$ et fermé pour les opérations sup et inf est un groupe réticulé que nous notons $\mathbf{F}(K)$. Ses éléments s'appellent les *fonctions de valuation* attachées à K. D'après les propriétés des opérations sup et inf, tout $X\in \mathbf{F}(K)$ se met sous la forme

$$X=\inf_{\alpha}\sup_{\beta}[x_{\alpha\beta}] \tag{1}$$

où $\{x_{\alpha\beta}\}$ $(1\leqq\alpha\leqq m,\ 1\leqq\beta\leqq n_{\alpha})$ est un sous-ensemble fini de K^*. La restriction de $\mathbf{F}(K)$ à $\mathbf{V}(K/A)$ est notée $\mathbf{F}(K/A)$. La restriction de $[x]$ à $\mathbf{V}(K/A)$ est encore notée $[x]$.

2. Fonctions de valuation et diviseurs.

Soit V une variété algébrique normale de dimension n définie sur un corps k et soit K le corps des fonctions sur V qui sont rationnelles sur k.

Il existe des liens étroits entre les V-diviseurs et les fonctions de valuation attachées à K. Commençons par remarquer que le groupe $G(V)$ (resp. $G^k(V)$) possède une structure de groupe réticulé et est engendré au moyen des opérations sup et inf par les éléments de $G_l(V)$ (resp. $G_l^k(V)$), c'est-à-dire par les diviseurs des fonctions sur V (resp. des fonctions sur V rationnelles sur k). On constate immédiatement l'existence d'un homomorphisme naturel du groupe réticulé $\mathbf{F}(K/k)$ sur le groupe réticulé $G^k(V)$ obtenu en faisant correspondre à $X=\inf_{\alpha}\sup_{\beta}[x_{o\beta}]$ le V-diviseur $\inf_{\alpha}\sup_{\beta}(x_{\alpha\beta}))$ où $(x_{\alpha\beta})$ désigne le diviseur de la fonction $x_{\alpha\beta}$ sur V.

Différents critères permettent de comparer dans certains cas, deux fonctions de valuation données sous la forme (1) en utilisant des propriétés géométriques simples des diviseurs $(x_{\alpha\beta})$ des $x_{\alpha\beta}$ correspondants. Ces critères ([12], Th. 3 et Coroll. 1 et 2) se déduisent facilement du suivant

Pour que $\inf_i[x_i]\prec 0$, *il suffit que les* $(x_i)_0$ *soient sans point* *commun* (D'après l'homomorphisme précédent, il faut que les $(x_i)_0$ soient sans composante commune).

Un autre résultat important du mémoire de Weil fait intervenir le groupe des V-diviseurs "partout localement intersection complète" (ou "partout localement linéairement équivalents à zéro"). Rappelons qu'un V-diviseur est dit partout localement intersection complète si à tout $P \in V$ on peut faire correspondre un $x_P \in K$ tel que P n'appartienne à aucune des composantes de $T-(x_P)$. L'ensemble de ces V-diviseurs est stable pour les opérations du groupe réticulé $G(V)$. C'est donc un sous-groupe réticulé de ce dernier que nous noterons $G_c(V)$. L'ensemble $G^k(V) \frown G_c(V)$, qui est encore un groupe réticulé, sera noté $G_c^k(V)$. Dans le cas particulier où V est projective non singulière on a, comme on sait, $G_c(V)=G(V)$.

Désignons, pour tout point P de V, par A_P l'anneau local de P sur V et associons à P un x_P comme plus haut. Pour toute valuation $\omega \in \mathbf{V}(K/A_P)$ $\omega(x_P)$ ne dépend que de T, P et ω, mais non du choix particulier de x_P. On peut donc noter cette expression ω_P. Le résultat de Weil annoncé plus haut ([12], Th. 13) est le suivant:

Soit T un V-diviseur rationel sur k, partout localement intersection complète. Alors il existe une et une seule fonction de valuation $X_T \in \mathbf{F}(K/k)$ telle que sa restriction à $\mathbf{F}(K/A_P)$ soit, pour tout $P \in V$, définie par $X_T(\omega)=\omega_P$. L'application $T \to X_T$ est un isomorphisme du groupe réticulé $G_c^k(V)$ dans le groupe réticulé $\mathbf{F}(K/k)$.

Weil donne en outre une caractérisation simple de l'image de cet isomorphisme.

3. *Distributions.*

Les notations étant les mêmes que dans le paragraphe précédent, supposons maintenant que k est un corps de fonctions algébriques sur un corps de constantes k_0, c'est-à-dire que k est de degré de transcendance fini sur k_0 et k_0 algébriquement fermé dans k. On désignera par B un modèle projectif normal de l'extension k de k_0 c'est-à-dire une variété projective normale définie sur k_0 et telle que k soit le corps des fonctions sur V définie sur k_0.

A l'ensemble $G(B)$ des diviseurs sur B, nous adjoindrons deux éléments notés (0) et (∞), qui seront considérés respectivement comme les diviseurs des fonctions 0 et ∞. Pour tout B-diviseur D nous conviendrons que $(\infty) \prec D \prec (0)$, que $(0)+D=(0)$ et $(\infty)+D=(\infty)$. L'ensemble obtenu sera noté $\tilde{G}(B)$. C'est encore un ensemble réticulé (ou un treillis). Les éléments (0) et (∞) seront considérés comme rationels sur k_0. Le résultat de leur adjonction à $G^{k_0}(B)$ sera noté $\tilde{G}^{k_0}(B)$.

Soit $X = \inf_\alpha \sup_\beta [x_{\alpha\beta}]$ un élément de $\mathrm{F}(K/k)$ et considérons l'application Δ de l'ensemble des places k-valuées f de K dans $\tilde{G}^{k_0}(B)$ définie par

$$\Delta(f) = \inf_\alpha \sup_\beta ((f(x_{\alpha\beta})))$$

où $(f(x_{\alpha\beta}))$ désigne le diviseur de la fonction $f(x_{\alpha\beta})$ sur B. Une telle application Δ sera appellée une *distribution* attachée à la fonction de valuations X. En réalité, Δ n'est pas exactement définie par la donnée de X, mais dépend du choix particulier des $x_{\alpha\beta}$. Cependant, nous allons montrer que si Δ et Δ' sont deut distributions attachées au même X, on peut trouver deux B-diviseurs D_1 et D_2 tels qu'on ait, quel que soit f,

$$\Delta(f) + D_1 \prec \Delta'(f) \prec \Delta(f) + D_2.$$

La démonstration de cette propriété se ramème facilement à celle du théorème suivant

THÉORÈME 1.—*Soient K, k et B comme ci-dessus et soient (x_i) $(i=1, \cdots, n)$ des éléments de K tels que* $\inf_i [x_i] < 0$ *dans* $\mathrm{F}(K/k)$. *Alors il existe un B-diviseur D_0 tel que*

$$\inf_i (f(x_i)) \prec D_0$$

pour toute place k-valuée f de K.

Ce théorème est en fait une conséquence immédiate du théorème 5 de [12] et d'une des formules intervenant dans la démonstration de ce dernier. Pour plus de commodité, reproduisons cependant cette démonstration dans le cas particulier du théorème 1.

Puisque $\inf_i [x_i] \prec 0$ dans $\mathrm{F}(K/k)$, il existe, d'après ([12], Th. 2, Coroll. 1) un polynome $P \in k[X] = k[X_1 \cdots, X_n]$ tel que $P(x) = 0$ et $P(0) = 1$. Donc on a une relation

$$1 = \sum a_\nu M_\nu(x)$$

où $a_\nu \in k$ pour tout ν et où les M_ν sont des monômes. D'où, puisque les $f(x_i)$ sont des spécialisations compatibles entre elles des x_i sur k

$$(2) \qquad 1 = \sum a_\nu M_\nu(f(x_i)).$$

Soit ω une valuation quelconque de k. On a $\inf_i \omega(x_i) \leqq 0$ ou $\inf_i \omega(x_i) > 0$ pour tout i. Dans ce dernier cas on a $\omega(M_\nu(f(x_i))) \geqq v(f(x_i))$ pour tout i. La relation (2) entraîne donc

$$(3) \qquad \inf_i (\omega(f(x_i))) \leqq \inf (0, \sup_\nu (v(a_\nu^{-1})).$$

A tout B-diviseur D premier sur k associons maintenant la valuation ω_D de K qui, à tout $x \in K^*$, fait correspondre le coefficient de D dans (x) et telle qu'on ait, pour tout D, $\omega_D(0)=\infty$ et $\omega_D(\infty)=-\infty$.

On obtient le théorème (1) en appliquant la relation (3) à chacune des valuations ω_D. On peut prendre $D_0=\inf(0, \sup_\nu a_\nu^{-1})$.

Une conséquence du théorème 1 est le "théorème de décomposition", valable pour toute variété V *projective non singulière*. Dans ce cas, pour tout V-diviseur T rationnel sur k, la fonction de valuation X_T (voir paragraphe 2 ci-dessus ou [12], Chap. V) est définie. On peut exprimer X_T sous la forme $\inf_\alpha \sup_\beta [x_{\alpha\beta}]$, avec, pour tout couple d'indices α, β, $x_{\alpha\beta} \in K$ et $(x_{\alpha\beta})=T+X_\alpha-Y_\beta$ où les X_α et, de même, les Y_β, sont sans point commun. Nous désignerons par Δ_T la distribution $f \to \inf_\alpha \sup_\beta ((f(x_{\alpha\beta})))$ attachée à X_T.

Soit P un point de V rationnel sur k et soit f_P l'une des places k-valuées de K de centre P. Lorsque le symbole $x(P)$ est défini, on a $f_P(x)=x(P)$, et l'expression $f_P(x)$ ne dépend donc que de P et non du choix particulier de f_P. D'autre part, supposons qu'il existe un indice α tel que $x_{\alpha\beta}(P)$ ne soit pas défini pour tout β; on a alors $P \in T+Y_\alpha$ et, comme il existe un β tel que $P \notin Y_\beta$, on a $\sup_\beta((x_{\alpha\beta}))=(0)$. Il résulte de là que, dans tous les cas, $\Delta_T(f_P)$ ne dépend que de P et non du choix particulier de f_P. Nous écrirons $\Delta_T(P)$ au lieu de $\Delta_T(f_P)$. *Le théorème de décomposition* se déduit facilement du théorème 1, de la relation $X_{(x)}=[x]$ et de l'existence de l'isomorphisme $T \to X_T$. Son énoncé est le suivant:

Soit x un élément de K, et soit $(x)=\sum m_i T_i$, où les m_i sont des entiers et les T_i des V-diviseurs premiers rationnels sur k. Alors il existe deux V-diviseurs D_1 et D_2 rationnels sur k tels qu'on ait quel que soit P

$$\sum_i m_i \cdot \Delta_{T_i}(P)+D_1 \prec (x(P)) \prec \sum_i m_i \Delta_{T_i}(P)+D_2.$$

4. *Interprétation géométrique du théorème 1.*

Donnons une interprétation géométrique du théorème 1 dans le cas particulier suivant: supposons V projective non singulière et les x_i tels que $(x_i)=X_i-X$, où les V-diviseurs X, X_i sont positifs, les X_i étant sans point commun. Ce cas particulier contient celui de l'application à la démonstration du théorème (B), dont nous parlerons au chapitre suivant.

Soient P^r et P^s les espaces projectifs contenant respectivement V et B. Soit M un point générique de B sur k_0 tel que $k=k_0(M)$ et soit Q un point générique de V sur k. Considérons la variété $\mathcal{V}$ lieu de $Q \times M$ sur k_0 dans le produit $P^r \times P^s$.

Désignons par p l'application rationnelle de $\mathcal{V}$ sur B définie par la projection $Q\times M\rightarrow M$. Il sera commode d'employer aussi la lettre p pour désigner la projection algébrique sur B d'un $\mathcal{V}$-cycle ou la projection ensembliste sur B d'un ensemble algébrique sur $\mathcal{V}$.

Pour tout i, considérons la fonction y_1 sur $\mathcal{V}$, définie sur k, telle que $y_1(Q\times M)=x_i(Q)$. On a, quel que soit i, $(x_i)=(y_i)\cdot P^r\times M$. Donc, puisque les X_i sont sans point commun, l'ensemble algébrique intersection des supports des (y_i) ne rencontre pas $V\times M$ et est contenu dans l'ensemble algébrique $\mathcal{V}_0=p^{-1}(B_0)$, où B_0 est l'ensemble algébrique fondamental pour p sur B. Désignons d'autre part par $\mathcal{V}_m$ l'ensemble algébrique des points multiples de $\mathcal{V}$. Puisque V est sans point multiple, on a $B_m=p(V_m)\neq B$. Posons $\mathcal{V}^*=\mathcal{V}_m\cup\mathcal{V}_0$ et $B^*=B_m\cup B_0=p(V^*)$.

Soit P un point de V rationnel sur k, et soit $\mathcal{P}$ le lieu de $P\times M$ sur k_0. Soit de plus f_P une place k-valuée de K de centre P. On peut supposer $f_P(x_i)$ défini pour tout i, car sinon on aurait $P\in X$, et comme il existe un i tel que $P\notin X_i$, on aurait $\inf_i((f_P(x_i)))=(\infty)$. On a

$$n_i=f_P(x_i)=x_i(P)=y_i(P\times M).$$

En désignant par z_i la fonction induite par y_i sur $\mathcal{P}$, on a donc

$$(u_i)=p((z_i)).$$

L'interprétation du théorème 1 est la suivante: il existe un B-diviseur D_0 tel que

$$\inf_i((u_i))\prec D_0.$$

Or considérons une composante commune Z aux $(z_i)_0$. Si elle est simple sur $\mathcal{V}$, cette composante appartient aux $(y_i)_0$, donc à l'ensemble algébrique $\mathcal{V}_0$. On a donc dans tous les cas $Z\subset\mathcal{V}^*$, donc $p(Z)\subset B^*$. Il en résulte que les composantes de $\inf_i((u_i))$ sont contenues dans B^*. L'affirmation de l'existence de D_0 équivaut à celle de l'existence d'une borne supérieure pour les coefficients de ces composantes ou, ce qui revient au même, à la suivante:

Le coefficient dans $\inf_i(z_i)_0$ *d'une composante commune* Z *aux* $(z_i)_0$ *se projetant proprement sur* B *admet une borne supérieure qui ne dépend pas de* P *ni de* Z.

Dans le cas particulier où la dimension de B_m est $\leqq\dim(B)-2$, Z est toujours simple sur $\mathcal{V}$ et il suffit de démontrer l'existence d'une borne supérieur pour les multiplicités d'intersection $i[Z,(y_i)_0\cdot\mathcal{P}]$[2].

[2] Pour les multiplicités d'intersection, propres ou excédentaires, nous employons les notations de P. Samuel [8].

Lorsqu'il n'en est pas ainsi, on peut se ramener à la démonstration de l'existence d'une borne supérieure analogue en plongeant $\mathcal{V}$ dans une variété $\mathcal{V}'$ sur laquelle les composantes de $\mathcal{V}_m$ sont simples et telle qu'il existe, pour tout i, une fonction y'_i sur $\mathcal{V}'$ induisant y_i sur $\mathcal{V}$. Dans [4], j'ai obtenu une démonstration directe de l'existence de cette borne supérieure en utilisant un lemme de la théorie des intersections (chap. II, lemme 4 et Coroll.) Ce lemme n'est pas indispensable pour la démonstration de (B) où il peut être remplacé avantageusement, comme nous verrons plus loin, par les propriétés de la notion de hauteur (qui résultent du théorème 1). Cependant, il semble intéressant de signaler que l'utilisation des fonctions de valuation permet d'en donner une démonstration relativement simple, et même d'obtenir le résultat suivant, légèrement plus précis:

THÉORÈME 2. *Soient V une variété, q un entier positif et U_j $(j=1,\cdots,r)$ des V-diviseurs positifs. Soit E l'ensemble algébrique intersection des supports des U_j. Soient Z une sous-variété simple de V, non contenue dans E et Y une sous-variété de V contenant Z, telles que les conditions suivantes soient satisfaites*:

(A)—*Z est simple sur Y.*

(B)—*Z est une composante propre de chacune des intersections $Y\cdot U_j$* sur *V.*

(C)—*Pour toute composante E_h de E, on a $q_h=i[Z;Y\cdot E_h]\leqq q$.*

Alors, si l'on pose $i[Z;Y\cdot U_j]=m_j$, on a $\inf_j m_j\leqq m$, où m est un nombre positif qui ne dépend que des U_j et de q, mais non de Z ni de Y.[3]

On peut, en utilisant un recouvrement de V, se ramener au cas où V est une variété dans un espace affine puis, par projection sur l'un d'un nombre fini de sous-espaces de ce dernier, et compte tenu de l'hypothèse "Z simple sur V", au cas où V est elle-même un espace affine.

Montrons qu'on peut de plus se ramener au cas où l'intersectoin E est réduite à une variété. Soit k un corps de définition algébriquement fermé des U_j et posons $A=k[x]=k[x_1,\cdots,x_n]$ où $x_1,\cdots,x_n$ représentent les coordonnées dans V. Soient J l'idéal de A engendré par les u_j, J' l'idéal des éléments de A qui s'annulent sur E et, pour tout h, J_h l'idéal des éléments de A qui s'annulent sur la composante E_h de E. D'après le théorème des zéros de Hilbert, il existe un

[3] Ce théorème était connu, dans le cas $r=2$, par Enriques, qui l'a utilisé dans la démonstration d'un résultat préliminaire au "lemme d'Enriques-Severi". Cette derniere démonstration a été simplifiée par Zariski par une méthode qui pourrait être rattachée à la théorie des paragraphes 1 à 3 ci-dessus (voir [13]).

entier q tel que

$$J'^q \subset J.$$

De plus

$$\prod_h J_h \subset \bigcap_h J_h = J'.$$

Donc

$$(\prod_h J_h)^q \subset J. \tag{4}$$

Or tout idéal I de A est de type fini, donc détermine une fonction de valuation $X_I \in \mathbf{F}(K/A)$ définie par $X_I(\omega) = \inf_{y \in I} \omega(y)$ (Cf [12], Chap. V); on vérifie aisément les propriétés $X_I \prec X_{I'}$ pour $I \supset I'$ et $X_{I \cdot J} = X_I + X_J$. La relation (4) entraîne donc

$$X_J \prec q \textstyle\sum_h X_{J_h}. \tag{5}$$

Posons $K = k(x)$. Soit f_Y une place de K ayant pour centre Y, à valeurs dans le corps K' des fonctions sur Y définies sur k. Pour tout $x \in K$ telle que la fonction x_Y induite par x sur Y soit définie, on a $x_Y = f_Y(x)$; soit ω_Z la valuation de K' qui, à tout $u' \in K'$, fait correspondre le coefficient de Z dans le Y-diviseur (u').

Par hypothèse $f_Y(x_i)$ est définie pour tout i, et coïncide avec la fonction induite par x_i sur Y. Compte tenu de ([11], Chap. VIII, Th. 4) on a, pour tout $h, i[Z; Y \cdot U_j] = \omega_Z(f_Y(u_j))$. Nous avons donc à démontrer que $X_J(\omega_Z \circ f_Y)$ admet une borne supérieure indépendante de Y et de Z. D'après (5), il suffit de montrer qu'il en est de même de chacun des $X_{J_h}(\omega_Z \circ f_Y)$.

D'où la réduction annoncée: nous pouvons supposer que l'intersection E est réduite à une variété. Par hypothèse on a $q_1 = i[Z; Y \cdot E] \leqq q$. Soient ω_E la valuation de K qui, à tout $y \in K$, fait correspondre la multiplicité de y en E. On peut trouver un élément t de $k(u)$, qu'on peut choisir parmi un ensemble fini qui ne dépend pas de Y ni de Z, tel que l'hypersurface $t = 0$ contienne E et coupe proprement Y en Z avec la multiplicité q_1. Soit z un élément arbitraire de $k(t)$ et posons $z = t^l z_0$, la fonction z_0 étant définie et non nulle pour $t = 0$. On a $(z) = l(t) + (z_0)$. Comme E n'est contenue dans aucune des composantes de (z_0), on a $\omega_E(z) = l$ et $i[Z; (z) \cdot Y] = l \ i[Z; (t) \cdot Y] = lq_1$. Donc $\omega_Z \circ f_Y$ coïncide avec $q_1 \omega_E$ sur $k(t)$. D'autre part, puisque 0 est la seule spécialisation de t compatible avec $x_i \to 0$ sur k, on a la relation $\inf_i [x_i] \prec 0$ dans $\mathbf{F}(K/k(t))$. L'application de ([12], Th. 5) entraîne donc bien l'existence d'une borne supérieure pour $\inf_i (\omega_Z(f_Y(x_i)))$.

5. *Hauteur d'un point.*

Nous reprenons maintenant les notations des paragraphes 2 et 3.

Soit y un point de l'espace projectif P^n, de coordonnées $(y_0, y_1, \cdots, y_n)$ rationnelles sur k. Associons-lui le B-diviseur $D = -\inf((y_i))$. Le degré de ce diviseur n'est pas modifié quand on multiplie tous les y_i par un même élément de k. Donc ce degré ne dépend que de y. On le notera $h(y)$ et on l'appellera *hauteur* du point y.

On a évidemment, puisque $\deg((y_i))=0$, $h(y) \geqq 0$ pour tout y. On peut ajouter que $h(y)=0$ si et si seulement le point y est rationnel sur k_0. En effet, supposons $y_0=1$ et $y_1 \notin k_0$. Soit E un B-diviseur premier sur k_0, positif et $\prec (y_1)_\infty$. Alors on a $\inf_i \omega_D(y_i) \leqq 0$ pour tout B-diviseur D premier sur k, puisque $\omega_D(y_0)=0$ et $\inf_i v_E(y_i)<0$. Donc $h(y) \geqq \deg E > 0$.

Signalons encore l'interprétation suivante du symbole $h(y)$. Soit φ l'application de B sur P^n définie par les y_i et posons $Y=\varphi(V)$; Y est aussi la variété lieu de y sur k_0. Si l'on désigne par Z la section de Y par un hyperplan de P^n coupant proprement P^n, on a $h(y)=\deg(\varphi^{-1}(Z))$. En effet, on peut supposer les y_i tous$\neq 0$. La section Y_i de Y par $y_i=0$ est alors définie pour tout i, et on a d'après ([11], Chap. VIII, Th. 4, Coroll. 2)

$$(z/y_i)=\varphi^{-1}(Z)-\varphi^{-1}(Y_i).$$

On a

$$h(y)=\deg D'$$

avec

$$D'=-\inf_i (y_i/z)=\inf_i (\varphi^{-1}(Y_i)-\varphi^{-1}(Z)).$$

Or, puisque les $\varphi^{-1}(Y_i)$ n'ont pas de composante commune, on a $D'=\varphi^{-1}(Z)$.

REMARQUE.—Le symbole $h(y)$ n'est pas défini de manière intrinsèque, en ce sens que l'application $y \rightarrow h(y)$ ne dépend pas seulement du corps k, mais aussi au modèle projectif B choisi. Cependant, on peut remarquer que si h' est le symbole défini au moyen d'un autre modèle projectif B', on a une relation de la forme $\gamma_1 h(y) \leqq h'(y) \leqq \gamma_2 h(y)$ valable pour tout y, où γ_1 et γ_2 sont des constantes réelles positives. En effet soit $B=t(B')$, où t est une transformation birationnelle. Soient φ et $\varphi'=\varphi\circ t$ les applications rationnelles de B et B' dans P^n définies par les y_i et posons comme ci-dessus $D=\varphi^{-1}(Z)$, $D'=\varphi^{-1}(Z)$. On a $D=t(D')$. Soit H' une section hyperplane générique de B' et posons $H_0=t(H')$; on a $h'(y)=\deg(D \cdot H_0) \leqq \deg D \cdot \deg H_0$. Donc $h'(y) \leqq h(y) \cdot \deg H_0$.

THÉORÈME 3.—*Pour $h(y)$ borné, le degré de la variété Y lieu de y sur k est également borné.*

Soit en effet, comme plus haut, φ l'application de B sur P^n

définie par les y_i. D'après ([11], Chap. VI, Th. 1), on a une relation de la forme

$$\varphi^{-1}(x)=p^f\sum_{\nu=1}^{m}U_\nu$$

où p est la caractéristique, f un entier positif et les U_ν des sous-variétés de B conjuguées entre elles par rapport à $k_0(y)$. On a donc

$$\deg(\varphi^{-1}(y))=p^f\cdot m\cdot e$$

où e est le degré de l'une quelconque des composantes U_ν. Soit $n-t$ la dimension de Y et considérons des section Y_ν $(\nu=1,\cdots,t)$ de Y par des hyperplans génériques indépendants sur k_0 dans P^n. Le degré de Y est le nombre des points communs aux Y_ν. Les Y_ν se coupent proprement dans P^n en des points qui sont tous génériques de Y sur k_0. Donc les $\varphi^{-1}(Y_i)$ se coupent proprement sur B, et on a

$$\varphi^{-1}(Y_1, Y_2,\cdots, Y_t)=\varphi^{-1}(Y_2)\cdot\varphi^{-1}(Y_2)\cdots\varphi^{-1}(Y_t).$$

En comparant les degrés des deux membres, on obtient

$$p^f\cdot m\cdot e\cdot\deg(Y)\leqq(h(y))^t$$

d'où le résultat annoncé.

Une conséquence du théorème 3 est que le lieu Y de y ne peut appartenir, d'après le théorème de Bertini-Chow, qu'à un nombre fini de systèmes algébriques.

6. *Définition du symbole h_T.*

Il sera commode d'introduire la relation d'équivalence suivante: pour tout ensemble **E**, on dira que deux fonctions f et g sur **E** à valeurs réelles, éventuellement infinies, sont équivalentes s'il existe deux constantes a_1 et a_2 telles que pour tout

$$f(x)+a_1\leqq g(x)\leqq f(x)+a_2$$

pour tout $x\in\mathbf{E}$.

La relation d'équivalence ainsi définie sera notée $\asymp$. On écrira parfois $f(x)\asymp g(x)$ au lieu de $f\asymp g$.

Soit maintenant T un V-diviseur rationnel sur k et supposons qu'il appartienne à une série linéaire sans point fixe L sur V. On peut trouver dans L des V-diviseurs T_i rationnels sur k et sans point commun, et il existe des $x_i\in K$ tels que $(x_i)=T_i-T$. Soit φ l'application de V dans P^n définie par les x_i. Alors, d'après le choix des T_i, φ est définie en tout point P de V. Nous désignerons par h_T la fonction sur l'ensemble des points de V rationnels sur k, à valeurs entières positives, définie par

$$h_T(P)=h(\varphi(P)).$$

Cette fonction ne dépend pas seulement de T mais aussi du choix des x_i. Cependant, nous allons montrer que sa classe pour la relation $\asymp$ ne dépend que de T, et même de la classe de T pour la relation d'équivalence linéaire.

Soit en effet T' un V-diviseur rationnel sur k linéairement équivalent à T. Puisque V est normale, il existe une série linéaire sans point fixe L' sur V contenant T' (on peut supposer $L' \supset L$). Considérons des éléments T'_j de L' sans point commun, rationnels sur k, et des $x'_j \in K$ tels que $(x'_j)=T'_j-T'$. Soit φ' l'application rationnelle définie sur k de V dans un espace projectif définie par les x'_j, et posons

$$h'_{T'}(P)=h(\varphi'(P)).$$

Soit de plus t un élément de K tel que $(t)=T-T'$. On a d'après ([12], Th. 3)

$$T=\inf_i [x_i]=\inf_i [tx'_j].$$

On peut trouver d'après ([12], Th. 1) pour tout P rationnel sur k, une place f_P de K à valeurs dans k, qui soit une extension des spécialisations $x_i \rightarrow x_i(P)$ et $x'_j \rightarrow x'_j(P)$ sur k. Le théorème 1 entraîne l'existence de deux B-diviseurs D_1 et D_2 tels que

$$-\inf_i ((f_P(x_i)))+D_1 \prec -\inf_i ((f_P(x'_j))) \prec -\inf_i ((f_P(x_i)))+D_2.$$

D'où, en passant aux degrés, le résultat annoncé: $h'_{T'} \asymp h_T$.

Si Γ désigne une classe d'équivalence linéaire sur V représentable par les éléments d'une série linéaire L sans point fixe, on peut donc poser

$$h_\Gamma(P)=h_T(P)$$

en prenant T arbitraire dans L. Le symbole h_Γ est parfaitement défini à l'équivalence $\asymp$ près par la donnée de Γ.

De plus, si Γ et Γ' sont deux telles classes, il en est de même de $\Gamma+\Gamma'$, et on a

$$h_{\Gamma+\Gamma'} \asymp h_\Gamma+h_{\Gamma'}.$$

En effet, soient (x_i), (x'_j) des sous-ensembles finis de K associés, comme plus haut, à Γ et Γ' respectivement, tels que $(x_i)=T_i-T$ $(x'_j)=T'_j-T'$ avec $T_i \in L$ et $T'_j \in L'$ et tels que les T_i, et de même les T'_j, soient sans point commun; il suffit de remarquer que les $T_i+T'_j$ sont sans point commun et d'utiliser les $x_i\ x'_j$ pour définir le symbole $h_{\Gamma+\Gamma'}$. On peut étendre la définition du symbole h_Γ aux classes $\Gamma_1-\Gamma_2$ obtenues par différence de deux classes $\Gamma_1-\Gamma_2$ du type précédent. Il suffit de poser

$$h_\Gamma(P)=h_{\Gamma_1}(P)-h_{\Gamma_2}(P).$$

Le symbole h_Γ ainsi étendu est encore parfaitement défini à l'équivalence $\asymp$ près par la donnée de Γ.

Remarquons que dans le cas particulier où la variété V est non singulière, le symbole h_Γ est défini quel que soit Γ. Dans ce cas, on peut aussi définir h_Γ par la formule

$$h_\Gamma(P)=\deg(\Delta_T(P))$$

avec $T\in\Gamma$, où Δ_T est le symbole défini au paragraphe 3. Les résultats, qui précèdent sont alors une conséquence immédiate du théorème de décomposition.

Signalons enfin le résultat suivant:

THÉORÈME 4. *Soient V une variété complète non singulière définie sur k, V' une variété normale définie sur k et u une application rationnelle de V' sur V définie sur k. Soit Γ une classe de V-diviseurs pour l'équivalence linéaire. Alors, les V'-diviseurs $T'=u^{-1}(T)$, avec $T\in\Gamma$, appartiennent à une même classe Γ' pour l'équivalence linéaire. Si le symbole h_Γ est défini, il en est de même de $h_{\Gamma'}$ et on a*

$$h_\Gamma(u(P'))\asymp h_{\Gamma'}(P')$$

pour tout $P'\in V'$.

En effet l'application $T\rightarrow T'=u^{-1}(T)$ est un isomorphisme du groupe ordonné $G(V)$ dans le groupe ordonné $G(V')$. De plus tout corps de définition de T contenant k est un corps de définition de T'.

D'autre part, en appelant K le corps des fonctions sur V définies sur k on a, pour tout $x\in K$, et compte tenu des hypothèses sur V et V', d'après ([11], Chap. VIII, Th. 4, Coroll. 2)

$$u^{-1}((x))=(x\circ u).$$

Donc l'isomorphisme précédent envoie $G_l(V)$ dans $G_l(V')$. Donc les T' appartiennent bien à une même classe Γ' pour $T\in\Gamma$ et l'application $\Gamma\rightarrow\Gamma'$ est un isomorphisme de $G(V)/G_l(V)$ dans $G(V')/G_l(V')$.

Supposons que le symbole h_Γ soit défini. On peut se ramener au cas où Γ contient une série linéaire sans point fixe L définie sur k. Alors l'image de L sur V est une série linéaire sans point fixe L' définie sur k. Soient T_i $(i=0,\cdots,n)$ des éléments de L rationnels sur k sans point commun et soit pour tout i, $x_i\in K$ tel que $(x_i)=T_i-T_0$. On a $(x_i\circ u)=T'_i-T'_0$, en posant $T'_i=u^{-1}(T_i)$ pour tout i, et les T'_i sont sans point commun. On peut donc prendre, pour tout $P'\in V'$

$$h_{\Gamma'}(P')=h(\varphi'(P'))=h(\varphi(P))=h_\Gamma(P)$$

où φ et $\varphi'=\varphi\circ u$ désignent les applications rationnelles de V dans un espace projectif définies par les x_i et les x'_i respectivement. D'où le résultat annoncé.

3.—Application à la détermination de la structure de $G(V)/G_a(V)$.

Montrons maintenant comment la théorie qui précède s'applique à la "descente infinie" dans la démonstration de (B). En reprenant les notations de l'introduction, donnons d'abord l'énoncé précis du problème qu'il s'agit de résoudre dans cette partie de la démonstration.

Soient F un demi-domaine universel, k_0 un sous-corps de F algébriquement fermé dans F, B une variété projective normale définie sur k_0, M un point générique de B sur k et C une courbe projective non singulière définie sur $k=k_0(M)$. On suppose que la jacobienne J de C est une variété projective définie sur k, et que la fonction cannonique correspondante φ est également définie sur k. Soit Q un point générique de C sur K et soit V la variété lieu de $Q\times M$ sur F dans le produit des espaces projectifs contenant respectivement B et C.

A tout V-diviseur U rationnel sur F, on associe le C-diviser A défini par $A\times M=U\cdot(A\times M)$ et le point $P=S[\varphi(A)]$, (c'est-à-dire $\sum m_i\varphi(A_i)$ si $A=\sum m_iA_i$) de la jacobienne J. L'application $U\rightarrow P$ de $G^F(V)$ sur J est un homomorphisme ζ dont le noyau est $H_l^F(V,C)$ et dont l'image est le groupe de tous les points de J rationnels sur $F(M)$. Posons $H_a=\zeta(G_a^F(V))$.

Il s'agit de prouver que H/H_a est un groupe de type fini en supposant déjà démontrée la propriété suivante: pour tout entier s positif différent de la caractéristique, le groupe H/sH est un groupe fini.

Pour cela on se fixe arbitrairement un entier $s\neq p$ et >1 et on choisit des représentants $\bar{P}_\alpha(\alpha=1,\cdots,l)$ de chacune des classes de $H(\text{mod}\, sH)$. En partant d'un élément quelconque P_0 de H on peut construire une suite infinie $P_0, P_1,\cdots,P_\nu,\cdots$ d'éléments de H et une suite d'entiers positifs $\alpha_0,\alpha_1,\cdots,\alpha_\nu$, tous $\leqq l$, tels que l'on ait pour tout ν

$$sP_\nu=P_{\nu-1}-\bar{P}_{\alpha_\nu}.$$

Il nous suffit de montrer que, pour ν assez grand, P_ν ne peut représenter qu'un nombre fini de classes de $H(\text{mod}\, H_a)$ indépendantes de la suite $\{P_\nu\}$ choisie.

Faisons correspondre à tout entier α l'application rationnelle u_α de J sur J définie par $u_\alpha(Q)=sQ+\bar{P}_\alpha$ pour tout $Q\in J$. La théorie des variétés abéliennes permet de montrer que pour tout α et pour tout J-diviseur X, on a une équivalence linéaire de la forme

$$X_\alpha=u_\alpha^{-1}(X)\sim(s^2-1)X+X'_\alpha$$

avec $X'_\alpha \succ 0$. Prenons pour X un hyperplan arbitraire dans l'espace projectif contenant J. Le symbole h_Y est défini pour tout Y puisque J est non singulière et on a d'après le théorème 4, pour tout $P \in H$

$$h_{X_\alpha}(P) \asymp h_X(u_\alpha(P)) \asymp (s^2-1)h_X(P) + h_{X'_\alpha}(P).$$

Donc

$$(s^2-1)h_X(P) \leqq h_X(u_\alpha(P)) + a_\alpha$$

où a_α est un entier indépendant de P. Si l'on pose $h_X(P_\nu) = h_\nu$ pour tout ν, et si l'on fait $P = P_\nu$, $\alpha = \alpha_\nu$ dans la formule ci-dessus, on obtient, en posant $a = \sup_\alpha a_\alpha$,

$$(s^2-1)h_\nu \leqq h_{\nu-1} + a.$$

Donc h_ν est, pour ν assez grand, inférieur à un nombre réel b indépendant de la suite P_ν choisie $\left(\text{pour tout } \varepsilon \text{ réel positif, on peut prendre } b = a\dfrac{s^2-1}{s^2-2} + \varepsilon\right)$.

Désignons par P^r et P^s les espaces projectifs contenant J et B respectivement. Soit R un point générique de J sur k et considérons dans le produit $P^r \times P^s$ la variété $\mathcal{J}$ lieu de $R \times M$ sur k_0. Il est commode de considérer en même temps que $\mathcal{J}$, le modèle projectif $\mathcal{J}' = T(J)$, où T est l'application birationnelle partout birégulière de $P^r \times P^s$ dans P^{rs+r+s} qui, au point $(x_0, \cdots, x_r) \times (y_0, \cdots, y_s)$, fait correspondre le point ayant pour coordonnées les $x_i y_j$.

Pour tout ν, désignons par $\mathcal{P}_\nu$ le lieu de $P_\nu \times M$ sur F et posons $\mathcal{P}'_\nu = T(\mathcal{P}_\nu)$. Puisque $h(P_\nu) \leqq b$ pour ν assez grand, et puisque $h(M) = \deg(B)$, on a $h(T(P_\nu \times M)) \leqq b \deg(B) = b'$ pour ν assez grand. Donc d'après le théorème 3, $\mathcal{P}'_\nu$ ne peut appartenir, pour ν assez grand, qu'à un nombre fini de systèmes algébriques sur $\mathcal{J}'$ indépendants du choix de la suite $\{P_\nu\}$, et de même $\mathcal{P}_\nu$ ne peut appartenir qu'à un nombre fini de systèmes algébriques sur $\mathcal{J}$. En d'autres termes, il existe un nombre fini de couples $(\mathcal{W}_\beta, F_\beta)$ composés d'un cycle positif $\mathcal{W}_\beta$ sur $\mathcal{J}$ rationnel sur F et d'un corps de définition F_β de $\mathcal{W}_\beta$ contenant k_0, contenu dans F et algébriquement fermé, tels qu'on ait la propriété suivante: quelle que soit la suite $\{P_\nu\}$ on peut, à tout indice ν assez grand, faire correspondre un entier $\beta_\nu \leqq l$ tel que $\mathcal{P}_\nu$ soit une spécialisation de $\mathcal{W}_{\beta_\nu}$ sur F_{β_ν}. Pour tout β, le cycle $\mathcal{W}_\beta \cdot (J \times M)$ est de la forme $S_\beta \times M$ où S_β est un point de J rationnel sur $F_\beta(M)$. Or on peut trouver un C-diviseur A_β rationnel sur $F_\beta(M)$ et tel que $S[\varphi(A_\beta)] = S_\beta$. Le lieu $\mathcal{A}_\beta$ de $A_\beta \times M$ sur F est un V-diviseur positif rationnel sur F_β et tel que $\zeta(\mathcal{A}_\beta) = S_\beta$. Pour tout ν, on peut étendre la spécialisation $\mathcal{W}_{\beta_\nu} \to \mathcal{P}_\nu$ à une spécialisation $\mathcal{A}_{\beta_\nu} \to \mathcal{U}_\nu$ sur

F_{β_ν}. On a nécessairement $\zeta(\mathcal{U}_\nu)=P_\nu$. Or, pour tout β, l'ensemble des spécialisations de $\mathcal{A}_\beta$ sur F_β est un système algébrique de diviseurs positifs sur V, et les images sur J des éléments de cet ensemble appartiennent à une même classe (mod H_a). Nous venons de montrer que P_ν appartient, pour ν assez grand, à l'une de ces classes, d'où le résultat annoncé.

POITIERS

BIBLIOGRAPHIE

[1] W. L. Chow, Mémoir en préparation.

[2] J. Igusa, On the Picard varieties attached to algebraic varieties, American Journal of Mathematics, **74** (1952), pp. 1–22.

[3] T. Matsusaka, On the algebraic construction of the Picard variety, Proc. Japan Acad., **28** (1952), pp. 5–8.

[4] A. Néron, Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps, Bull. Soc. Math. de France, **80** (1952), pp. 101–166.

[5] A. Néron et P. Samuel, La variété de Picard d'une variété normale, Annales de l'Institut Fourier, **4** (1952), pp. 1–30.

[6] D. G. Northcott, An inequality in the theory of arithmetic on algebraic varieties, Proc. Cambridge Phil. Soc., **45** (1949), pp. 502–509.

[7] D. G. Northcott, A further inequality in the theory of arithmetic on algebraic varieties, ibid., pp. 510–518.

[8] P. Samuel, La notion de multiplicitè en Algèbre et en Géométrie algébrique, Journal de Math. pures et appliquées, **30** (1951), pp. 159–274.

[9] F. Severi, Sui fondamenti della geometria numerativa e sulla teoria delle caratteristiche, Atti del R. Istituto Veneto di Scienze, Lettere ed Arti, **24** (1916).

[10] A. Weil, L'arithmétique sur les courbes algébriques, Acta mathematica, **52** (1929), pp. 281–315.

[11] A. Weil, Foundations of Algebraic Geometry, American Mathematical Society, Colloquium Publications, 29 (1946).

[12] A. Weil, Arithmetic on algebraic varieties, Ann. of Math., **53** (1951), pp. 412–444.

[13] O. Zariski, Complete linear systems on normal varieties and a generalisation of a lemma of Enriques-Severi, Ann. of Math., **55** (1952), pp. 552–592.

Some Results in the Theory of the Differential Forms of the First Kind on Algebraic Varieties

Yoshikazu NAKAI

The theory of the differential forms of the first kind on algebraic varieties are developed systematically in the classical case, by the use of harmonic integrals and we have much results in this subject owing to the continuous efforts of eminent mathematicians. But in the abstract case, i.e. in the algebraic geometry over the universal domain of characteristic $p(\neq 0)$, the situations are quite different and the theory is still hanging in the air. Moreover the recent work of J. Igusa [1][1] shows us that the abstract theory has quite different nature from the classical one, and his example seems to indicate some new role of the theory of the differential forms in abstract algebraic geometry. The author is especially interested in the theory of the differential forms of the first kind on abstract algebraic varieties. The present paper will contain some results which will make some contributions toward this purpose.

§1 contains some auxiliary results which are necessary in the following paragraphs. In §2, we shall give a necessary and sufficient condition for a differential form ω to be of the first kind in terms of its coefficients. We shall also introduce the expression for ω in the language of adjoint forms as is usaully done in the classical case. In §3, we shall proceed as follows: Let V^r be a normal projective variety defined over a field k, $\mathbf{C}$ a generic hyperplane section of V with reference to k and $\bar{\omega}$ an $(r-1)$-fold differential form of the first kind on $\mathbf{C}$. We shall say that $\bar{\omega}$ has the property (P), if there exists an r-fold differential form Ω on V such that $(\Omega)+\mathbf{C}\succ 0$ and $\mathrm{Res}_C\,\Omega=\bar{\omega}$. Then we can characterize $\bar{\omega}$ having the property (P), by a special property of the divisor $(\bar{\omega})$ on $\mathbf{C}$. Meanwhile we can again prove a result of my previous paper in a slightly better form by a quite simple method. Now in the classical case it is known that an $(r-1)$-fold differential form of the first kind ω_C on $\mathbf{C}$, which is the trace on $\mathbf{C}$ of a differential form ω of the first kind on V,

[1] The numbers in the bracket refer to the bibliography at the end of the parer.

has not the property (P). But, at present, no body knows whether the similar results also holds or not in the abstract case. We shall derive in §4 a characteristic property of an $(r-1)$-fold differential form ω which has the property (P) with respect to a generic hyperplane section, then our method enables us to reduce the above problem to the following somewhat interesting conjecture.

CONJECTURE.[2] *Let V^{*r} be a projective variety in a projective space S^{r+1} which is a generic projection of a non-singular variety V with reference to a field of definition k for V, and $F^*(Y_0, Y_1, \cdots, Y_{r+1})$ an irreducible form defining V^*, of degree m. Let A^*_i $(i=0, 1, \cdots, r+1)$ be forms of degree $<m-r$, and suppose that there exists an identity of the form*

$$A^*_0 \partial F^*/\partial Y_0 + A^*_1 \partial F^*/\partial Y_1 + \cdots + A^*_{r+1} \partial F^*/\partial Y_{r+1} = 0.$$

Then the forms A^*'s must be identically zero, provided m is not divisible by the characteristic p of the universal domain.

In the case $r=1$, the above result is true as was shown by Castelnuovo and plays a fundamental role in the theory of the differential forms of the first kind on algebraic surfaces developed by F. Severi [9]. If this conjecture holds true we can answer the above mentioned problem affirmatively and we get also the inequalities $h^{q,0} \leqq h^{0,q}$[3] $(q=1, \cdots, \dim V)$. Moreover we can also prove the preservation of the independency of the differential forms of the first kind on an algebraic variety on its generic hyperplane section by the similar method. The author wishes very much to lift the veil covering this conjecture in the near future.

The author expresses his hearty thanks to Prof. Akizuki for his interest taken in this work and his encouragement throughout the period of investigation.

[2] The conjecture came from the following Lemma: "Let $F(x, y, z)=0$ be an irreducible form defining a plane curve which has only nodal points. Let m be the degree of F and suppose that there exist forms A, B, and C of degree $<m-1$ satisfying the identity $AF'_x + BF'_z + CF'_y = 0$. Then we must have $A=B=C=0$." (Cf. Severi [8]).

In this Lemma the assumption on the singularity of the curve is essential, otherwise we can easily find a counter example $F(x, y, z) = y^2 z - x^3$. But the author does not know whether the assumption that the original variety V is a non-singular variety is necessary or not.

[3] $h^{s,q}$ denotes the dimension of the q-th cohomology group of V with coefficients in the sheaf Ω of germs of s-fold regular differential forms on V, i.e. $h^{s,q} = \dim H^q(V, \Omega^s)$. When $q = r (= \dim V)$, it is known that $h^{r,s} = h^{s,r}$ by the duality theorem of Serre (Cf. Serre [8] and his lecture at the Congress in 1954).

§ 1. Algebraic preliminaries.

Let V^r be a normal variety in a projective space S^n and k_0 the smallest field of definition for V. Let $P=(\xi_0, \xi_1, \cdots, \xi_n)$ be a generic point of V over k_0, and u_{ij} $(i=0, 1, \cdots, r+1 : j=0, 1, \cdots, n)(r+2)(n+1)$ independent variables over $k_0(P)$. Let $\eta_i=\sum_{j=0}^{n} u_{ij}\xi_j$ $(i=0, \cdots, r+1)$, $y_i=\eta_i/\eta_0$. We shall denote by H_i the hyperplane in S^n defined by the equation $\sum_{j=0}^{n} u_{ij}X_j=0$ $(i=0, 1, \cdots, r+1)$ and we shall put $C_i=V\cdot H_i$. Then C's are also normal varieties[4] respectively defind over k_0 $(u_{i0}, \cdots, u_{in})$, and $(y_i)=C_i-C_0$.[5] We shall denote by K the field generated by u_{ij} over k_0. We shall fix these notations throughout the rest of the papers.

PROPOSITION 1. *Let A^{r-1} be a subvariety of V, different from C_0, then for any set of indices $i_1, \cdots, i_s$ chosen from among $1, \cdots, r$, we can find functions $z_1, \cdots, z_{r-s}$ such that the functions $y_{i_1}, \cdots, y_{i_s}$, $z_1, \cdots, z_{r-s}$ are uniformizing parameters*[6] *along A on V if $s<r$.*

PROOF. We shall use the induction on s. When $s=0$ the assertion is trivial. Suppose that the prop. is true for integers $<s$. Moreover we can assume that $i_j=j$ and $\xi_0=\eta_0$, in this case we must, of course replace k_0 by the field $k=k_0$ $(u_{01}, \cdots, u_{0n})$. Let $M=(1, x_1, \cdots, x_n)$ be a generic point of A over $K'(\supset K)$, and $\sum_{j=1}^{n} a_{ij}(X_j-x_j)=0$ $(i=1, \cdots, n-r)$ the defining equation for the tangent linear variety to V at M. Then Prop. 1 is equivalent to say that the rank of the matrix $\begin{pmatrix} u_{ij} \\ a_{kj} \end{pmatrix}$ $(i=1, \cdots, s : k=1, \cdots, n-r : j=1, \cdots, n)$ is equal to $n-r+s$. Suppose that the rank of this matrix is $<n-r+s$, then by the induction assumption we have $\dim_{k(x)}(u_{ij}) \leqq ns-r+s-1$, hence $\dim_k(x, u_{ij}) \leqq \dim_k(x)+\dim_{k(x)}(u_{ij}) \leqq ns+s-1$. On the other hand $\dim_k(x, u_{ij})=\dim_k(u_{ij})+\dim_K(x) \geqq ns+r-1$. It is a contradiction if $r>s$. q.e.d.

PROPOSITION 2. $v_{C_0}(dy_{i_1}\cdots dy_{i_s})=-(s+1)C_0$ *if $s<r$. In particular if $s<r$, then we have $(dy_{i_1}\cdots dy_{i_s})=-(s+1)C_0$.*

[4] For the properties of a generic hyperplane section C of V we shall refer to Seidenberg [7] and Nakai [6].

[5] Stricktly speaking, y_i's are quantities, and not functions following the usage of Weil [11]. But we shall identify y_i's with the functions f_i's on V defined over $k_0(u)$ by $f_i(P)=y_i$ respectively, since it will cause no confusions.

[6] Concerning the definitions and the properties of uniformizing parameters, the readers are expected to refer Weil [11] and Nakai [5]. We shall cite Weil's book by (F).

PROOF. For the sake of simplicity we shall assume that $i_j=j$. Let $y'_1=1/y_1, y'_i=y_i/y_1$ $(i=2,\cdots,r)$, then $dy_1=-y_1^2dy'_1$ and $dy_i=y_1dy'_i-y_1^2y'_idy'_1$, hence we have $dy_1\cdots dy_s=-y_1^{s+1}dy'_1\cdots dy'_s$. Since as we see easily, $y'_1,\cdots,y'_r$ are uniformizing parameters on V along C_0 we immediately have the first half of the proposition. Concerning the second half of the proposition, it is a direct consequence of Prop. 1.
q.e.d.

PROPOSITION 3. *Let A^{r-1} be a subvariety of V different from C_0, and suppose that $y_1,\cdots,y_r$ are not uniformizing parameters on V along A. Then the r functions $y_1,\cdots,y_{i-1},y_{i+1},\cdots,y_r,y_{r+1}$ are uniformizing parameters on V along A, for any choice of index i. $(1\leqq i\leqq r)$.*

PROOF. Suppose that the proposition were false. Then using the same notations as in the proof of Prop. 1, we would immediately get the relation $\dim_{k(x)}(K)\leqq n(r+1)-2$. The rest of the proof is quite similar to that of Prop. 1. q.e.d.

PROPOSITION 4. *Let Y be a divisor defined by $(dy_{i_1}\cdots dy_{i_r})+(r+1)\mathrm{C}_0=\mathrm{Y}$, then Y is a positive divisor on V. Moreover a simple point P' on V, not lying on C_0, is in some component of the divisor Y if and only if the r functions $y_{i_1},\cdots,y_{i_r}$ are not uniformizing parameters on V at P'.*

PROOF. For the sake of simplicity we assume that $i_j=j$ and $\xi_0=\eta_0$. If $y_1,\cdots,y_r$ are uniformizing parameters on V at P' then we easily see that the point P' is not in any component of Y. Suppose that $y_1,\cdots,y_r$ are not uniformizing parameters at P' on V, and let $\sum_{j=1}^{n}a_{ij}(X_j-x'_j)=0$ $(i=1,\cdots,n-r)$ be the set of defining equations for the tangent linear variety to V at $\mathrm{P}'=(1,x'_1,\cdots,x'_n)$. Since P' is simple on V the rank of the matrix (a_{ij}) is $n-r$. We shall assume that $\det|a_{ij}|(j=r+1,\cdots,n:i=1,\cdots,n-r)$ is different from 0. Let $(1,x_1,\cdots,x_n)$ be a generic point of V over K, then the functions x_i $(i=1,\cdots,r)$ are uniformizing parameters on V at P'. We shall put $dy_i=\sum_{j=1}^{n}\alpha_{ij}dx_j$. Then since $y_i=\sum_{j=1}^{n}u_{ij}x_j+u_{i0}$, we see immediately $\alpha_{ij}=u_{ij}+\sum_{t=r+1}^{n}u_{it}\,\partial x_t/\partial x_j$. By our assumptions we have $\det\begin{vmatrix}u_{ij}\\a_{kj}\end{vmatrix}=0$, $(i=1,\cdots,r:k=1,\cdots,n-r:j=1,\cdots,n)$. Now multipying t-th column by $\partial x_t/\partial x_j$ $(t>r)$ and adding them to j-th column $(j\leqq r)$, we see that

$$0=\det\begin{vmatrix}n_{ij}\\a_{kj}\end{vmatrix}=\begin{vmatrix}\alpha_{ij} & *\\0 & a_{kj}\end{vmatrix}.$$

This means that the function det $|\alpha_{ij}|$ is zero at $\mathbf{P}'$. Since $dy_1\cdots dy_r$ $=\det|\alpha_{ij}|\,dx_1\cdots dx_r$, and $\mathbf{P}'$ is a simple point of $\mathbf{V}$ there exists a component of $\mathbf{Y}$ containing $\mathbf{P}$. This completes the proof. q.e.d.

PROPOSITION 5. *Let* $\mathbf{Y}_i$ *be the positive divisor defined by* $(dy_1\cdots\widehat{dy_i}\cdots dy_{r+1})+(r+1)\mathbf{C}_0=\mathbf{Y}_i$, *then* $\mathbf{Y}_i$ *and* $\mathbf{Y}_j$ *have no common component.*

This is an immediate consequence of Prop. 3 and 4.

Let $\mathbf{V}^*$ be a variety in a projective space S^{r+1} whose generic point over K is given, in homogeneous coordinates, by $(\eta_0,\eta_1,\cdots,\eta_{r+1})$. Then as is known $\mathbf{V}$ and $\mathbf{V}^*$ are birationally equivalent over K. This variety will henceforce be called *a generic projection of* $\mathbf{V}$ *with reference to* k_0, *in the projective space* S^{r+1}, or simply, *a generic projection of* $\mathbf{V}$. Let $x_i=\xi_i/\eta_0$, then by F-II, Prop. 22 and 24, $\mathfrak{o}=K[x]$ is integral over $\mathfrak{o}'=K[y]$, moreover by our assumption on $\mathbf{V}$, $\mathfrak{o}$ is integrally closed in its quotient field. Let $\mathfrak{f}$ be the conductor of $\mathfrak{o}'$ in $\mathfrak{o}$. Then we have the

PROPOSITION 6.[7] *Every prime divisor of* $\mathfrak{f}$ (*as an ideal of* $\mathfrak{o}$) *is of rank* 1.

PROOF. First we shall show that every prime divisor of $\mathfrak{f}$ (as an ideal of $\mathfrak{o}'$) is of rank 1. Let α be an element of $\mathfrak{o}$, and $\mathfrak{a}_\alpha$ the ideal of $\mathfrak{o}'$ which consists of elements a in $\mathfrak{o}'$ such that $a\alpha\in\mathfrak{o}'$. First we shall show that the rank of $\mathfrak{a}_\alpha$ is 1. Let $\mathfrak{a}_\alpha=\mathfrak{a}_1\frown\mathfrak{a}_2$ be the reduced expression as an intersection of primary ideals, where every primary in $\mathfrak{a}_1$ is of rank 1 and every primary in $\mathfrak{a}_2$ is of rank >1. Let b be an element of $\mathfrak{a}_1$ not in $\mathfrak{a}_2$ and d/a be the representation of α as a quotient of $a\in\mathfrak{o}'$ and $d\in\mathfrak{o}'$. Then $\alpha b\mathfrak{a}_2\subset\mathfrak{o}'$, i.e. $db\mathfrak{a}_2\subset a\mathfrak{o}'$. But since in $\mathfrak{o}'$ the theorem of unmixedness holds,[8] every prime divisor of $a\mathfrak{o}'$ is of rank 1. On the other had since $\mathfrak{a}_2$ is of rank>1 we see easily that $db\in a\mathfrak{o}'$, i.e. $\alpha b\in\mathfrak{o}'$. This means that $b\in\mathfrak{a}_\alpha$ it is a contradiction. Since $\mathfrak{f}=\bigcap_\alpha\mathfrak{a}_\alpha$, every prime divisor of $\mathfrak{f}$ is also of rank 1.

Let $\mathfrak{f}=\mathfrak{a}_1\frown\mathfrak{a}_2$ be the representation of $\mathfrak{f}$ in $\mathfrak{o}$, where every primary in $\mathfrak{a}_1$ is of rank 1 and that of $\mathfrak{a}_2$ is of rank >1. As before let b be an element of $\mathfrak{a}_1$. Then if $\mathfrak{a}_1\subset\mathfrak{o}'$, $\mathfrak{f}=\mathfrak{f}\frown\mathfrak{o}'=(\mathfrak{a}_1\frown\mathfrak{o}')\frown(\mathfrak{a}_2\frown\mathfrak{o}')=\mathfrak{a}_1\frown(\mathfrak{a}_2\frown\mathfrak{o}')$. Since the rank of every prime divisor of $\mathfrak{f}$ in $\mathfrak{o}'$ is of rank 1 we see that $\mathfrak{a}_1\subset\mathfrak{a}_2\frown\mathfrak{o}'\in\mathfrak{a}_2$,[9] and $\mathfrak{f}=\mathfrak{a}_1$ as asserted. Suppose that $\mathfrak{a}_1\not\subset\mathfrak{o}'$, then we can suppose that b is not in $\mathfrak{o}'$. Then $\mathfrak{a}_b$ is an ideal different from

[7] This proposition is due to M. Nagata.

[8] This is immediate since $\mathfrak{o}'\cong K[Y_1,\cdots,Y_{r+1}]/F(Y)$.

[9] Since $\mathfrak{o}$ and $\mathfrak{o}'$ are integral extensions of a polynomial ring $K[y_1,\cdots,y_r]$, the rank of the ideals are preserved, cf. Nagata [3].

the unit ideal $\mathfrak{o}'$ and of rank 1. Since $b\mathfrak{a}_2\subset\mathfrak{f}$, we have $\mathfrak{a}_2\frown\mathfrak{o}'\subset\mathfrak{a}_b$. It is a contradiction since rank$(\mathfrak{a}_2\frown\mathfrak{o}')>1$ and rank $\mathfrak{a}_b=1$. Thus we have proved the proposition. q.e.d.

Let $F^*(Y_0, Y_1,\cdots, Y_{r+L})$ be an irreducible homogeneous polynomial defining the generic projection V^* in S^{r+1}, and $F(Y_1,\cdots, Y_{r+1})=F^*(1, Y_1,\cdots, Y_{r+1})$. Then since $F(y)=0$ we have $\sum_{i=1}^{r+1}F_i dy_i=0$, where we put $F_i=\partial F/\partial y_i$. From this we get the relation $dy_{r+1}=-\sum_{i=1}^{r}F_i/F_{r+1}dy_i$. Multiplying both sides by $dy_1\cdots dy_{i-1}\cdot dy_{i+1}\cdots dy_r$, we get

$$dy_1\cdots\widehat{dy_i}\cdots dy_{r+1}=(-1)^{r-i}F_i/F_{r+1}dy_1\cdots dy_r.$$

Hence we have

$$(F_i)-(F_{r+1})=\mathbf{Y}_i-\mathbf{Y}_{r+1}.$$

Since $\mathbf{Y}_i$ and $\mathbf{Y}_{r+1}$ have no common component we easily see that $(F_{r+1})_0-\mathbf{Y}_{r+1}=\mathbf{X}\succ 0$. Then we have $(F_i)_0=\mathbf{X}+\mathbf{Y}_i$ for any i. It is easy to see that the divisor $\mathbf{X}$ is rational over the field K. Let $\mathfrak{a}$ be the ideal $(F_1,\cdots, F_{r+1})\mathfrak{o}'$ and $\mathfrak{a}^*=\bigcap_{\mathfrak{p}}(\mathfrak{a}\mathfrak{o}_{\mathfrak{p}}\frown\mathfrak{o})$, where $\mathfrak{p}$ runs over all prime ideals of $\mathfrak{o}$, of rank 1. Then since $\mathfrak{a}\subset\mathfrak{f}$ we have $\mathfrak{a}^*\subset\mathfrak{f}\mathfrak{o}_{\mathfrak{p}}\frown\mathfrak{o}$. On the other hand every prime divisor of $\mathfrak{f}$ is of rank 1 by Prop. 6, we see that $\bigcap_{\mathfrak{p}}\mathfrak{f}\mathfrak{o}_{\mathfrak{p}}\frown\mathfrak{o}=\mathfrak{f}$, hence we have $\mathfrak{a}^*\subset\mathfrak{f}$. Thus we have

PROPOSITION 7. *Let α be an element of $\mathfrak{o}$, such that $(\alpha)_0\succ\mathbf{X}$, Then α is contained in the conductor $\mathfrak{f}$.*

In the following, any element of $K[y]$, which is contained in the conductor of $K[x]$ in $K[y]$, will be called *an adjoint polynomial in y*. It may also be remarked here that the divisor $\mathbf{X}$ defined above does not depend on the choice of hyperplane at infinity, and is determined uniquely when $\mathbf{V}$ and $\mathbf{V}^*$ are given.

PROPOSITION 8. *The generic projection from $\mathbf{V}$ onto $\mathbf{V}^*$ is biregular at any point which is not contained in any component of $\mathbf{X}$.*

PROOF. Without loos of generalities we can assume that $\xi_i=\eta_i$ $(i=0,\cdots, r+1)$. Let $\mathfrak{f}_i$ $(i\leqq r)$ be the conductor of $K[\eta_\lambda/\eta_i]$ in $K[\xi_\lambda/\xi_i]$. Let $\mathbf{P}'$ be a point on $\mathbf{V}$ not contained in any component of $\mathbf{X}$, and assume that $\mathbf{P}'$ is not on $\mathbf{C}_0$. Then we can pass to the affine representatives $\mathbf{V}_0$ where $\xi_0\neq 0$. Let $\mathfrak{q}$ be the ideal in $K[x]$ $(x_\lambda=\xi_\lambda/\xi_0)$ corresponding to $\mathbf{P}'$, we shall show that $\mathfrak{q}\not\supset\mathfrak{f}_0$. Suppose that $\mathfrak{q}\supset\mathfrak{f}_0$, then there exists a prime $\mathfrak{p}$ of $\mathfrak{f}_0$ such that $\mathfrak{q}\supset\mathfrak{p}$. But since rank $\mathfrak{f}_0$ is equal to 1, $\mathfrak{p}$ must be the ideal corresponding to some component prime rational cycle of $\mathbf{X}$. This means that $\mathbf{P}'$ is in some component of $\mathbf{X}$. Thus we have $\mathfrak{q}\not\supset\mathfrak{f}_0$. Hence there exists an element h in $\mathfrak{f}_0$ not in $\mathfrak{q}$, and then $x_\lambda=x_\lambda h/h$, $xh\in K[\eta_\lambda/\eta_0]$. This proves that the projection is biregular at P'. The proof for the remaining case is similar. q.e.d.

As an application of Prop. 8, we have the

PROPOSITION 9. *Let V^r be a normal variety in a projective space. If* $\deg V<r+2$, *then the geometric genus P_g is zero. In the case* $\deg V=r+2$, *we can conclude that the geometric genus is less than or equal to* 1. *Moreover in this case if $P_g=1$, V is contained in a linear subvariety of dimension $r+1$,* i.e. *V is a hypersurface.*

PROOF. Let m be the degree of V. Then we have $(F_1)=X+Y_1-(m-1)\cdot C_0$, i.e. $X\sim(m-1)\cdot C_0-Y_1$. Since $Y_1\sim K+(r+1)\cdot C_0$, where K denotes the canonical divisor of V, we have $X+K\sim(m-r-2)\cdot C_0$. From this relation we easily have the first assertion, since $X\succ 0$. If $m=r+2$, we have $X+K\sim 0$, hence $K\prec 0$ and $l(K)\leqq 1$. Then if $l(K)=1$, we must have $K=0$, and X must also be a zero cycle. Hence by Prop. 8, the generic projection from V onto V^* is everywhere biregular and $K[x]=K[y]$. This proves our assertion.

This is a generalization of a well known result that a non-singular cubic curve of genus 1 is a plane curve.[10]

§ 2. Representation of the differential form of the first kind.

We shall retain, in this paragraph, to the same notations and assumptions as in § 1.

Let

$$\omega=\sum_{i_1<\cdots<i_q} f_{i_1\cdots i_q}\, dy_{i_1}\cdots dy_{i_q} \tag{2.1}$$

be a q-fold differential form of the 1st kind on V, where the coefficients $f_{i_1\cdots i_q}$ are assumed to be skew symmetric with respect to its indices and the sum is extended over all set of indices $i_1<\cdots<i_q$ taken from $1,\cdots,r$. We shall determine a necessary and sufficient conditions for ω to be of the 1st kind.

Let $j_1,\cdots,j_{r-q}$ be the set of indices complementary to $i_1,\cdots,i_q$. Then multiplying ω by $dy_{j_1}\cdots dy_{j_{r-q}}$ we get

$$(dy_{j_1}\cdots dy_{j_{r-q}}\wedge\omega)+(r-q+1)C_0\succ 0.$$

From this we have immediately the relations

$$(f_{i_1\cdots i_q})+Y_{r+1}-qC_0\succ 0. \tag{2.2}$$

The condition (2.2) means that ω is finite along any subvariety A of dimension $r-1$, outside of C_0 and the component of Y_{r+1}.

Next we shall determine the condition that ω is finite along C_0.

[10] E.g., cf. van-der-Waerden [10].

Let $y_1'=1/y_1, y_i=y_i/y_1$ $(i=2,\cdots,r)$. Then as we easily see y_i' $(i=1,\cdots,r)$ are uniformizing parameters on V along $\mathbf{C}_0$,[11] and

$$\begin{aligned}&dy_1dy_{i_2}\cdots dy_{i_q}=-y_1^{q+1}dy_1'dy_{i_2}'\cdots dy_{i_q}',\\ &dy_{i_1}\cdots dy_{i_q} \qquad (i_j>1)\\ &=y_1^q dy_{i_1}'\cdots dy_{i_q}'-y_1^{q+1}\sum_{\alpha=1}^{q}(-1)^{\alpha-1}y_{i_\alpha}'dy_1'dy_{i_1}'\cdots\widehat{dy}_{i_\alpha}'\cdots dy_{i_q}'.\end{aligned}$$

Hence

$$\begin{aligned}\omega &= \sum_{1<i_2<\cdots<i_q}\!\!{}_1\, f_{1i_2\cdots i_q}dy_1dy_{i_2}\cdots dy_{i_q} + \sum_{1<i_1<\cdots<i_q}\!\!{}_2\, f_{i_1\cdots i_q}dy_{i_1}\cdots dy_{i_q}\\ &=-y_1^{q+1}\textstyle\sum_1 f_{1i_2\cdots i_q}dy_1'dy_{i_2}'\cdots dy_{i_q}'+\textstyle\sum_2\{y_1^q f_{i_1\cdots i_q}dx_{i_1}'\cdots dy_{i_q}'\\ &\quad -y_1^{q+1}f_{i_1\cdots i_q}\sum_{\alpha=1}^{q}(-1)^{\alpha-1}y_{i_\alpha}'dy_1'dy_{i_1}'\cdots\widehat{dy}_{i_\alpha}'\cdots dy_{i_q}'\}\\ &=-y_1^{q+1}\textstyle\sum_1\{f_{1i_2\cdots i_q}+\displaystyle\sum_{\alpha\neq 1,i_2,\cdots,i_q}y_\alpha' f_{\alpha i_2\cdots i_q}\}dy_1'dy_{i_2}'\cdots dy_{i_q}'\\ &\quad -y_1^q\textstyle\sum_2 f_{i_1\cdots i_q}dy_{i_1}'\cdots dy_{i_q}',\end{aligned}$$

where $\sum_1$ denotes the sum extended over all sets of indices $i_2<\cdots<i_q$ taken from $2,\cdots,r$, and $\sum_2$ the sum over all sets of indices $i_1<i_2<\cdots<i_q$ taken from $2,\cdots,r$.

Since ω is finite along $\mathbf{C}_0$ we must have

$$v_{C_0}(\sum_{\alpha\neq i_2,\cdots i_q}y_\alpha f_{\alpha i_2\cdots i_q})\geqq q$$

for any set of indices $(1<)i_2<\cdots<i_q$ taken from $2,\cdots,r$. Quite similarly we get the following conditions

$$(\sum_{\alpha\neq i_1,\cdots,i_{q-1}}y_\alpha f_{\alpha i_1\cdots i_{q-1}})+\mathbf{Y}_{r+1}-q\mathbf{C}_0\succ 0. \tag{2.3}$$

Finally we shall determine the condition for ω to be finite along any component of $\mathbf{Y}_{r+1}$. By Prop. 4, $y_1,\cdots,y_r$ are not uniformizing parameters along any component of $\mathbf{Y}_{r+1}$, hence by Prop. 3 it is possible to use the functions, say, $y_2,\cdots,y_r,y_{r+1}$ as uniformizing parameters on V along any component of $\mathbf{Y}_{r+1}$. Using the relation $\sum_{i=1}^{r+1}F_i dy_i=0$, we can represent $dy_1=-(1/F_1)\sum_{i=2}^{r+1}F_i dy_i$. Substituting this in the expression (2.1), we see

$$\begin{aligned}\omega &=-(1/F_1)\sum_{1<i_2<\cdots<i_q}\!\!{}_1\, f_{1i_2\cdots i_q}(\sum_{i=2}^{r+1}F_i dy_i)dy_{i_2}\cdots dy_{i_q}\\ &\quad+\sum_{1<i_1<\cdots<i_q}\!\!{}_2\, f_{i_1\cdots i_q}dy_{i_1}\cdots dy_{i_q}\\ &=-(F_{r+1}/F_1)\textstyle\sum_1 f_{1i_2\cdots i_q}dy_{r+1}dy_{i_2}\cdots dy_{i_q}\\ &\quad-\textstyle\sum_2\{f_{i_1\cdots i_q}-(F_{i_1}/F_1)f_{1i_2\cdots i_q}+(F_{i_2}/F_1)f_{1i_1i_3\cdots i_q}-\cdots\\ &\qquad\qquad\cdots+(-1)^q(F_{i_q}/F_1)f_{1i_1\cdots i_{q-1}}\}dy_{i_1}\cdots dy_{i_q}.\end{aligned}$$

[11] E.g., cf. Th. 1 of Nakai [5].

We shall put

$$g_{i_0 i_1 \cdots i_q} = \sum_{\alpha=0}^{q} (-1)^{\alpha} F_{i_\alpha} f_{i_0 i_1 \cdots \hat{i}_\alpha \cdots i_q}.$$

Then we have

$$(g_{i_0 \cdots i_q}/F_1) + \mathbf{Y}_1 - q\mathbf{C}_0 \succ 0$$

by a reasoning similar to one which was used to deduce the relation (22). Thus we get $(g_{i_0 \cdots i_q}/F_{r+1}) + \mathbf{Y}_{r+1} - q\mathbf{C}_0 \succ 0$. Since $(F_1/F_{r+1}) = \mathbf{Y}_1 - \mathbf{Y}_{r+1}$, this to equivalent to the relation

$$(2.4) \qquad ((1/F_{r+1}) \sum_{\alpha=0}^{q} (-1)^{\alpha} F_{i_\alpha} f_{i_0 i_1 \cdots \hat{i}_\alpha \cdots i_q}) + \mathbf{Y}_{r+1} - q\mathbf{C}_0 \succ 0.$$

The conditions (2.2) (2.3) and (2.4) are sufficient for ω to be of the first kind when V is a non-singular variety. In fact these conditions imply that ω is finite along any subvariety of dimension $r-1$, hence $(\omega) \succ 0$. Since $\mathbf{V}$ is assumed to be non-singular, it implies that ω is of the 1st kind.

REMARK. It should be remarked here that these conditions are necessary but not sufficient if $\mathbf{V}$ admits some singular points. In this case, the condition $(\omega) \succ 0$ does not necessarily imply that ω is of the 1st kind (Kawahara [2]).

For an r-fold differential form $\omega = f dy_1 \cdots dy_r$, the necessary and sufficient conditions for ω to be of the first kind is simply the relation

$$(2.5) \qquad (f) + \mathbf{Y}_{r+1} - (r+1)\mathbf{C}_0 \succ 0.$$

As an application of the above considerations we immediately have

PROPOSITION 10. *Let* $\mathbf{V}^r$ *be a normal hypersurface in* S^{r+1} *and assume that* $\mathbf{V}$ *has a* $q(<r)$*-fold differential form of the first kind on* $\mathbf{V}$, *then* $\deg \mathbf{V} > q+1$.

PROOF. Let $m = \deg \mathbf{V}$, then $\mathbf{Y}_{r+1} \sim (m-1)\mathbf{C}_0$. Hence if there exists a q-fold differential form of the first kind, there must exist the functions satisfying the conditions (2.2) and (2.3). From this we get the desired inequality, $m-q-1>0$.

This limit is the best one in the sense that there exists a normal surface of degree 3 in S^3 which has a differential form of the first kind and of the first degree.

In the following we shall put one more additional condition that $\mathbf{V}$ is arithmetically normal.

Let us put

$$A_{i_1 \cdots i_q} = f_{i_1 \cdots i_q} F_{r+1}.$$

Then

$$\begin{aligned}&(A_{i_1\cdots i_q})-\mathbf{X}+(m-q-1)\mathbf{C}_0\\&=\{(F_{r+1})+\mathbf{X}-\mathbf{Y}_{r+1}+(m-1)\mathbf{C}_0\}+\{(f_{i_1\cdots i_q})+\mathbf{Y}_{r+1}-q\mathbf{C}_0\}\succ 0\end{aligned}$$

by (2.2) and the argument of § 1. Hence if f's are defined over K A's are elements of $K[\xi_i/\eta_0]$. Moreover $(A_{i_1\cdots i_q})_0\succ\mathbf{X}$, hence A's are in $K[y]$, i.e. A's are adjoint polynomials of degree at most equal to $m-q-1$. Then the above considerations yield at once the following

THEOREM 1.[12] *Let V^{*r} be a generic projection of a non-singular arithmetically normal projective variety, and $F(Y_1,\cdots,Y_{r+1})=0$ the defining equation for V^* of degree m. Let ω be a q-fold differential form of the first kind on V, K' a common field of definition for ω and V^*, and $(y_1,\cdots,y_{r+1})$ a generie point of V^* over K'. Then if $q<r$, ω can be written in the form*

$$\omega=\sum_{i_1<\cdots<i_q}A_{i_1\cdots i_q}/F_{r+1}dy_{i_1}\cdots dy_{i_q},\tag{2.1$'$}$$

where the sum is extended over the set of indices $i_1<\cdots<i_q$ taken from $1,\cdots,r$, and A's are adjoint polynomials in $K'[y]$ of degree at most equal to $m-q-1$, skew symmetric with respect to the indices, satisfying the following conditions:

$$\sum_{\alpha\neq i_1,\cdots,i_{q-1}}y_\alpha A_{\alpha i_1\cdots i_{q-1}}=A^*_{i_1\cdots i_{q-1}}\tag{2.2$'$}$$

are the adjoint polynomials of degree not greater than $m-q-1$.
(2.3′) *There exist the adjoint polynomials $A^{**}_{i_0i_1\cdots i_q}$ of degree $\leqq m-q-1$ such that*

$$\sum_{\alpha=0}^{q}(-1)^\alpha F_{i_\alpha}A_{i_0\cdots\hat{i_\alpha}\cdots i_q}=A^{**}_{i_0i_1\cdots i_q}F_{r+1}.$$

Conversely if the coefficients of ω in the expression (2.1′) satisfy the above conditions, then ω is a q-fold differential form of the first kind. For an r-fold differential form of the 1st kind it is simply written as

$$\omega=A/F_{r+1}dy_1\cdots dy_r,$$

where A is an adjoint polynomial in $K'[y]$ of degree at most equal to $m-r-2$.

For the proof it may be necessary to remark here that a function f such that $(f)+\mathbf{Y}_{r+1}-q\mathbf{C}_0\succ 0$ can be written as a linear combination, with constant coefficients, of the similar functions which are defined over K, since $\mathbf{Y}_{r+1}$ and $\mathbf{C}_0$ are rational over K (F-VIII, Th. 10).

[12] After I have completed this work, I heard from Y. Kawahara that he also arrived at the similar results to Th. 1 in his unpublished paper.

§ 3. The differential forms on the generic hyperplane section.

We shall treat mainly in this paragraph the $(r-1)$-fold differential forms of V^r and the trace ω_C of ω on a hyperplane section $\mathbf{C}$ of V. For this purpose we shall make frequent use of the Poincaré residue of an r-fold differential forms of V with respect to $\mathbf{C}$, hence we shall briefly sketch its definition and main properties.

Let V^r be a normal variety defined over k, $\mathbf{C}$ a generic hyperplane section of V with reference to the field k and Ω an r-fold differential form on V such that $v_C(\Omega)\geqq -1$. Let y be a function on V such that $v_C(y)=1$. Then y is chosen as a member of uniformizing parameters on V along $\mathbf{C}$. Expressing Ω in the form

$$\Omega=(h/y)dydy_1\cdots dy_{r-1}$$

we can define the Poincaré residue of Ω with respect to $\mathbf{C}$, denoted by $\mathrm{Res}_C\,\Omega$, by the following formula

$$\mathrm{Res}_C\,\Omega=\bar{h}\,d\bar{y}_1\cdots d\bar{y}_{r-1}$$

where $\bar{\ }$ denotes the trace on $\mathbf{C}$ of the functions on V. It is not difficult to see that this definition does not depend on the choice of uniformizing parameters $y, y_1, \cdots, y_{r-1}$ used to define it, but it is determined uniquely when Ω and $\mathbf{C}$ are given. It is also easy to see that $\mathrm{Res}_C\,\Omega=0$ if and only if Ω is finite on $\mathbf{C}$. When $\mathrm{Res}_C\,\Omega\neq 0$ we have the following relation

$$(3.1)\qquad (\mathrm{Res}_C\,\Omega)=((\Omega)+\mathbf{C})\cdot\mathbf{C}.$$

For the proof we refer to Zariski [12]. We shall fix these V and $\mathbf{C}$ throughout this paragraph.

PROPOSITION 11. *Let ω be an $(r-1)$-fold differential form on V^r such that ω induces on $\mathbf{C}$ a well defined differential form ω_C. Let Ω be the r-fold differential form defined by $\Omega=dy\wedge\omega/y$, then we have* $\mathrm{Res}_C\,\Omega=\omega_C$, *where y is a function on V such that $v_C(y)=1$.*

This is immediate from its definition.

Let ω be an $(r-1)$-fold differential form on V such that the trace ω_C of ω on $\mathbf{C}$ is well defined. Then Prop. 11 and (3.1) yield that $(\omega_C)=\left(\left(\dfrac{dy\wedge\omega}{y}\right)+\mathbf{C}\right)\cdot\mathbf{C}$, where y is a function on V such that $(y)=\mathbf{C}-\mathbf{C}_0$, and $\mathbf{C}_0$ is an irreducible hyperplane section of V. Since $(dy)=-2\mathbf{C}_0$, we see $(dy\wedge\omega)+2\mathbf{C}_0-(\omega)=X$ is a positive divisor,[13] and we have

$$(3.2)\qquad (\omega_C)=((\omega)+X-\mathbf{C}_0)\cdot\mathbf{C}.$$

[13] Cf. Prop. 3 of Nakai [4].

Then if we choose C_0 in such a way that

(1) $(\omega)\cdot C$ does not contain any component of $C\cdot C_0$

(2) ω_C is finite along $C\cdot C_0$,

we must have $(X-C_0)\cdot C\succ 0$. This is surely the case when C_0 is a generic hyperplane section of V with reference to a field of definition for ω. Thus we have

THEOREM 2. *Let ω be an $(r-1)$-fold differential form on V^r such that the trace ω_C of ω on C is well defined and not zero. Then for a suitable choice of the hyperplane section C_0 of V we can write the divisor of ω_C in the form*

$$(\omega_C)=((\omega)+X-C_0)\cdot C$$

where X is a positive divisor such that $(X-C_0)\cdot C\succ 0$.

This gives a slightly more precise form of the C-divisor $\bar{X}$ which appeared in Theorem 2 of Nakai [3].

COROLLARY. *Let ω be an $(r-1)$-fold differential form of the 1st kind on V^r such that $\omega_C\neq 0$, and K the canonical divisor of V. Then there exists a positive divisor Z, linearly equivalent to $K+2C$ such that $(\omega_C)=(Z-C_0)\cdot C$, where C_0 is a suitable member of the linear system $|C|$.*

Let the functions y_i ($i=1,\cdots,r+1$) and the divisors Y_i be as in §1, and $\omega=\sum_{i=1}^{r} f_i dy_1\cdots\widehat{dy_i}\cdots dy_r$ a differential form of the 1st kind on V. Then as is proved, the coefficients f_i must be in the module $\mathfrak{L}(Y_{r+1}-(r-1)C_0)$.[14] Now we have

PROPOSITION 12. *Notations and assumptions are as above, the trace of ω on C_0 is zero if and only if the coefficients f_i's are in the module $\mathfrak{L}(Y_{r+1}-rC_0)$.*

PROOF. Let $y_1'=1/y_1$ and $\Omega=dy_1'\wedge\omega/y_1'$. Then $\Omega=-(f_1/y_1)dy_1\cdots dy_r$. Hence if $\omega_{C_0}=0$, Ω is finite along C_0, i.e. $(f_1)+Y_{r+1}-rC_0\succ 0$. Conversely if f_1 satisfies the above conditions, then $(\Omega)+C_1\succ 0$ and $\omega_{C_0}=\mathrm{Res}_{C_0}\Omega=0$. For the remaining f_i's, the assertion is the direct consequence of the condition (2.3), or of the similar considerations as above. q.e.d.

PROPOSITION 13. *Let V^r, C and K be as above, and $\bar{\omega}$ be an $(r-1)$-fold differential form on C, then there exists a divisor Z linearly equivalent to $K+C$ such that $(\bar{\omega})=Z\cdot C$, or equivalently there exists an r-fold differential form Ω on V such that $v_C(\Omega)=-1$ and $\mathrm{Res}_C\,\Omega=\bar{\omega}$.*

PROOF. Let us denote by W_m the section of V with the

[14] Let X be a V-divisor, then $\mathfrak{L}(X)$ denotes the module of the functions on V such that $(f)+X\succ 0$.

hypersurface of order m. Then there exists an integer n_0 such that $(\bar{\omega})+\mathrm{W}_{n_0}\cdot\mathrm{C}\succ 0$. On the other hand there exists also an integer n_1 such that $\mathrm{Tr}_{\mathrm{C}}|\mathrm{K}+n\mathrm{C}|$[15] is complete on C for $n\geqq n_1$, by the lemma of Castelnuovo. Hence we can see easily that, if we denote by n an integer greater than $\max(n_0, n_1)$, there exists a hypersurface section W_{n-1} and a positive divisor Z' in $|\mathrm{K}+n\mathrm{C}|$ such $(\bar{\omega})+\mathrm{W}_{n-1}\mathrm{C}=\mathrm{Z}'\cdot\mathrm{C}$, i.e. $(\bar{\omega})=\mathrm{C}\cdot(\mathrm{Z}'-\mathrm{W}_{n-1})$ which proves the first half of the proposition. Now $\mathrm{Z}'\sim\mathrm{K}+n\mathrm{C}$, we can find an r-fold differential from Ω' on V such that $(\Omega')=\mathrm{Z}'-\mathrm{C}-\mathrm{W}_{n-1}$. Then $(\mathrm{Res}_{\mathrm{C}}\,\Omega')=(\mathrm{Z}'-\mathrm{W}_{n-1})\cdot\mathrm{C}=(\bar{\omega})$. Since the $(r-1)$-fold differential forms on C form a vector space of dimension 1 over the function field of C, it is easy to see that there exists a constant c such that $\mathrm{Res}_{\mathrm{C}}\,c\Omega'=\bar{\omega}$. Then the differential form $\Omega=c\Omega'$ satisfy all the requirements. q.e.d.

Let $\bar{\omega}$ be an $(r-1)$-fold differential form of the first kind on C. Then it may be natural to ask whether there exists a positive divisor Z linearly equivalent to $\mathrm{K}+\mathrm{C}$ such that $(\bar{\omega})=\mathrm{Z}\cdot\mathrm{C}$.

THEOREM 3. *Let* V^r *be a normal variety defined over* k, C *a generic hyperplane section of* V *with reference to* k *and* $\bar{\omega}$ *an* $(r-1)$-*fold differential form of the first kind on* C. *Then there exists a positive divisor* Z *in* $|\mathrm{K}+\mathrm{C}|$ *such that* $(\bar{\omega})=\mathrm{Z}\cdot\mathrm{C}$ *if ond only if there exists an r-fold differential form* Ω *such that* $(\Omega)+\mathrm{C}\succ 0$ *and* $\mathrm{Res}_{\mathrm{C}}\,\Omega=\bar{\omega}$.

The proof is quite similar to that of Prop. 13 and will be omitted. Henceforth any differential form of the first kind on C having the property stated in the above theorem will be said to have the property (P).

Let ω be an $(r-1)$-fold differential form of the 1st kind. Then if the trace ω_{C} of ω on C has the property (P), we shall say that the *differential form* ω *has the property* (P) *with respect to* C. In the classical case, where the universal domain is the field of all complex numbers, it is known that any $(r-1)$-fold differential form of the 1st kind has not the property (P) with respect to a generic hyperplane section of V. Then the Th. 3 yields at once

THEOREM 4. *Let* V *and* C *be as in Th. 3, and* ω *an* $(r-1)$-*fold differential form of the first kind on* V. *Then, if the characteristic of the universal domain is* 0, *the* C-*divisor* (ω_{C}) *is not contained in the linear system* $\mathrm{Tr}_{\mathrm{C}}|\mathrm{K}+\mathrm{C}|$.

[15] This means the trace of the complete linear system $|\mathrm{K}+\mathrm{C}|$ on C, i.e. the set of positive C-divisors of the form $\mathrm{Z}\cdot\mathrm{C}$, where Z is a member of the linear system $|\mathrm{K}+\mathrm{C}|$ on V.

§ 4. The differential forms of the first kind having the property (P).

In this paragraph we shall retain to the notations defined in § 1.

PROPOSITION 14. *Let* V^r *be a normal variety, and*

$$\omega=\sum_{i=1}^{r}(-1)^{i-1}f_i dy_1\cdots\widehat{dy_i}\cdots dy_r{}^{16)}$$

be a differential form of the 1st kind on V. *Suppose that* ω *has the property* (P) *with respect to some* C_i $(1\leqq i\leqq r)$, *then* f_i*'s must be written in the form*

$$f_i=h_i-y_i h_0\ (i=1,\cdots,r), \tag{4.1}$$

where h*'s are the functions on* V *such that* $(h_i)+\mathrm{Y}_{r+1}-r\mathrm{C}_0\succ 0$.

PROOF. For the sake of simplicity we shall assume that ω has the property (P) with respect to C_1. Let $\Omega=dy_1\wedge\omega/y_1$, then $(\Omega)+\mathrm{C}_1+\mathrm{C}_0\succ 0$ and $\mathrm{Res}_{C_1}\Omega=\omega_{C_1}$. By our assumption on ω there exists an r-fold differential form Φ such that $(\Phi)+\mathrm{C}_1\succ 0$ and $\mathrm{Res}_{C_1}\Phi=\omega_{C_1}$. Expressing Φ in the form

$$\Phi=(h_1/y_1)dy_1\cdots dy_r$$

we have $(h_1)+\mathrm{Y}_{r+1}-r\mathrm{C}_0\succ 0$. Since $\mathrm{Res}_{C_1}(\Omega-\Phi)=0$, the differential form $\Omega-\Phi$ must be finite on C_1, i.e. the function $h_1/y_1-f_1/y_1=h_0$ must be in $\mathfrak{L}(\mathrm{Y}_{r+1}-r\mathrm{C}_0)$. This proves the assertion for $i=1$, i.e. $f_1=h_1-y_1h_0$.

Let $z_i=y_1/y_i$, then $(z_i)=\mathrm{C}_1-\mathrm{C}_i$. Let $\Omega_i=dz_i\wedge\omega/z_i$, then we have $(\Omega_i)+\mathrm{C}_i+\mathrm{C}_1\succ 0$ as before and $\mathrm{Res}_{C_1}\Omega_i=\omega_{C_1}$. The simple calculation shows that

$$\Omega_i=(y_if_1-y_1f_i)/y_1y_i\cdot dy_1\cdots dy_r.$$

We shall recall here that the function $(y_if_1-y_1f_i)$ is in the module $\mathfrak{L}(\mathrm{Y}_{r+1}-(r-1)\mathrm{C}_0)$. By a similar reasoning as above we see that the function $h_1/y_1-(y_if_1-y_1f_i)/y_1y_i$ is in the module $\mathfrak{L}(\mathrm{Y}_{r+1}-(r+1)\mathrm{C}_0+\mathrm{C}_i)$. Hence we can write $h_1/y_1-f_1/y_1+f_i/y_i=h_i/y_i$ with function h_i satisfying $(h_i)+\mathrm{Y}_{r+1}-r\mathrm{C}_0\succ 0$, or equivalently $f_i=h_i-y_ih_0$. This proves the proposition.

PROPOSITION 15. *Let* V *be a normal variety defined over* k_0, C *a generic hyperplane section of* V *with respect to* k_0 *and* ω *an* $(r-1)$*-fold differential form of the first kind on* V. *Assume that* ω *has the property* (P) *with respect to* C, *then* ω *has the property* (P) *with respect to any irreducible section* $\mathrm{C}(m)$ *of* V *with a hypersurface of order* $m(\geqq 1)$.

[16] We attached the signs to simplify the fomulas which will come in the future.

PROOF. Without loss of generality we may assume that $\mathbf{C}$ is one of $\mathbf{C}_i$ $(1 \leqq i \leqq r)$ defined in §1. Then we can express ω in the form

$$\omega = \sum_{i=1}^{r} (-1)^{i-1} f_i dy_1 \cdots dy_i \cdots dy_r$$

with the supplementary conditions

$$(4.2) \qquad f_i = h_i - y_i h_0, \ h_i\text{'s are in } \mathfrak{L}(\mathbf{Y}_{r+1} - r\mathbf{C}_0)$$

by the preceding proposition. Let α be a function on $\mathbf{V}$ such that $(\alpha) = \mathbf{C}(m) - m\mathbf{C}_0$ and $\Omega' = d\alpha \wedge \omega$. Then since ω is of the first kind and $v_{\mathbf{C}_0}(d\alpha) \geqq -m-1$, we have $(\Omega') + (m+1)\mathbf{C}_0 \succ 0$, or equivalently $(\sum_{i=1}^{r} \alpha_i f_i) + \mathbf{Y}_{r+1} + (m-r)\mathbf{C}_0 \succ 0$ where $d\alpha = \sum_{i=1}^{r} \alpha_i dy_i$. Let g be a function on $\mathbf{V}$ defined by $g = \sum_{i=1}^{r} \alpha_i f_i + m\alpha h_0 = \sum_{i=1}^{r} \alpha_i h_i + h_0(m\alpha - y_1\alpha_1 - \cdots - y_r\alpha_r)$ then it will be shown that $(g) = \mathbf{Y}_{r+1} + (m-r-1)\mathbf{C}_0 \succ 0$. Suppose for a moment that this is already proved, then the differential form $\Omega = \left(\dfrac{g}{\alpha}\right) dy_1 \cdots dy_r$ is easily seen to satisfy the condition $(\Omega) + \mathbf{C}(m) \succ 0$. Moreover $\Omega - \Omega'/\alpha$ is finite along $\mathbf{C}(m)$, hence $\mathrm{Res}_{\mathbf{C}(m)}\Omega = \mathrm{Res}_{\mathbf{C}(m)}(\Omega'/\alpha) = \omega_{\mathbf{C}(m)}$, which proves that ω has the property (P) with respect to $\mathbf{C}(m)$. Next we shall show that $(g) + \mathbf{Y}_{r+1} + (m-r-1)\mathbf{C}_0 \succ 0$. For this purpose it will be sufficient to prove the following

PROPOSITION 16. *Notations and assumptions being as before, let* $\mathbf{C}(m)$ *be an irreducible section of* $\mathbf{V}$ *with a hypersurface of order* m, *different from* $\mathbf{C}_0$, *and* α *a function such that* $(\alpha) = \mathbf{C}(m) - m\mathbf{C}_0$. *Let* $d\alpha = \sum_{i=1}^{r} \alpha_i dy_i$, *then* $v_{\mathbf{C}_0}(\alpha_i) \geqq -(m-1)$ *and* $v_{\mathbf{C}_0}(\sum_{i=1}^{r} \alpha_i y_i - m\alpha) \geqq -(m-1)$.

PROOF. Let $\omega^* = y_1^m d(\alpha/y_1^m)$, then $\omega^* = d\alpha - m\alpha dy_1/y_1 = \sum_{i=1}^{r} \alpha_i dy_i - m\alpha dy_1/y_1$. Now using the functions $y_1' = 1/y_1$ and $y_i' = y_i/y_1$ $(i = 2, \cdots, r)$ as uniformizing parameters on $\mathbf{V}$ along $\mathbf{C}_0$, we have

$$\omega^* = -y_1 \left\{ \sum_{i=1}^{r} \alpha_i y_i - m\alpha \right\} dy_1' + y_1 \sum_{i=2}^{r} \alpha_i dy_1'.$$

Since α/y_1^m is finite along $\mathbf{C}_0$, we have $v_{\mathbf{C}_0}(\omega^*) \geqq -m$. Then we easily have $v_{\mathbf{C}_0}(y_1\alpha_i) \geqq -m$ and $v_{\mathbf{C}_0}(y_1(\sum_{i=1}^{r} \alpha_i y_i - m\alpha)) \geqq -m$. From this we have the assertion. q.e.d.

To complete the proof of Prop. 15, we must show that ω has the property (P) with respect to $\mathbf{C}_0$, which was excluded in the above proof. The simple calculation shows us that $\omega_{\mathbf{C}_0} = (-y_1'^{r-1} f_1 dy_2' \cdots dy_r')_{\mathbf{C}_0} = (y_1'^{r} h_0 dy_2' \cdots dy_r')_{\mathbf{C}_0}$. Let $\Omega = -h_0 dy_1 \cdots dy_r$, then $(\Omega) + \mathbf{C}_0 \succ 0$

and $\Omega = y_1'^{r+1} h_0 dy_1' \cdots dy_r'$. Hence $\mathrm{Res}_{C_0}(\Omega) = (y_1' y_1'^{r+1} h_0 dy_2' \cdots dy_r')_{C_0} = (y_1'^{r} h_0 dy_2' \cdot \cdot \cdot dy_r')_{C_0} = \omega_{C_0}$. This completes the proof of Proposition 15. q.e.d.

In the following we shall simply say that *the differential form of the 1st kind has the property* (P), if it has the property (P) with respect to some generic hyperplane section of V. It is reasonable by Prop. 15.

We shall now translate the conditions of Prop. 14 in the language of adjoint forms. Let $\omega = \sum_{i=1}^{r} (-1)^{i-1} f_i dy_1 \cdots \widehat{dy_i} \cdots dy_r$ be a differential form of the 1st kind on V, having the property (P). Then the coefficients f_i's are of the form $f_i = h_i - y_i h_0$, where h_i's are contained in $\mathfrak{L}(\mathbf{Y}_{r+1} - r\mathbf{C}_0)$. Then by (2.4) we have

$$(1/F_{r+1})\left(\sum_{i=1}^{r} F_i h_i - \left(\sum_{i=1}^{r} y_i F_i\right) h_0\right) \in \mathfrak{L}(\mathbf{Y}_{r+1} - (r-1)\mathbf{C}_0)$$

hence

$$(1/F_{r+1})\left(\sum_{i=1}^{r} F_i h_i - \left(\sum_{i=1}^{r+1} y_i F_i\right) h_0\right) \in \mathfrak{L}(\mathbf{Y}_{r+1} - r\mathbf{C}_0).$$

Then if we put the above function $-h_{r+1}$ and $F_0 = -\sum_{i=1}^{r+1} y_i F_i$, we get the relation

$$(4.3) \qquad \sum_{i=0}^{r+1} h_i F_i = 0, \quad \text{with the functions } h_i\text{'s in } \mathfrak{L}(\mathbf{Y}_{r+1} - r\mathbf{C}_0).$$

Now we shall assume that V is arithmetically normal, then multiplying (4.3) by F_{r+1} and putting $A_i = F_{r+1} h_i$, we have

$$(4.4) \qquad \sum_{i=0}^{r+1} A_i F_i = 0,$$

where A_i's are, as is easily seen, the adjoint polynomials of degree $\leqq m-r-1$. Let $A_i^* = \eta_0^{m-r-1} A_i$ and $F_i^* = \eta_0^{m-1} F_i$, then we easily see that $F_i^* = \partial F^* / \partial \eta_i$, where F^* is, an in §1, the defining homogeneous form for the generic projection V*. Then the identity (4.4) is transformed into

$$(4.5) \qquad \sum_{i=0}^{r+1} A_i^* F_i^* = 0$$

with adjoint forms A_i^* of degree $\leqq m-r-1$.

PROPOSITION 17. *Let* V *be a nonsingular arithmetically normal variety and let* V *admit an* $(r-1)$*-fold differential form of the 1st kind, having the property* (P). *Using the notations in* §1, *let* $\omega = \sum_{i=1}^{r} (-1)^{i-1} (A_i'/F_{r+1}) dy_1' \cdots \widehat{dy_i'} \cdots dy_r$ *be such one. Then there exist adjoint polynomials* A_i $(0 \leqq i \leqq r+1)$ *of degrees* $\leqq m-r-1$ *such that*

i) $A_i' = A_i - y_i A_0$,

ii) $\sum_{i=0}^{r+1} A_2^* F_i^* = 0$, *where* $A_i^* = \eta_0^{m-r-1} A_i$ *and* $F_i^* = \partial F^*/\partial \eta_i$.

Conversely, if there exist adjoint forms A_i^* *satisfying the above condition ii), then the differential form*

$$\omega = \sum_{i=1}^{r} (-1)^{i-1}(A_i - y_i A_0)/F_{r+1} dy_1 \cdots \widehat{dy}_i \cdots dy_r$$

is a differential form of the first kind having the property (*P*).

Proof. The first half of the proposition is already proved. To prove the second part, we must verify the conditions (2.2′) and (2.3′), but it will be a simple verification. q.e.d.

Now we are well prepared to discuss the usage of our conjecture which we shall restate in the following

Conjecture. *Let* V^* *be a generic projection in* S^{r+1} *of a non-singular variety* V^r *in a projective space, and* $F^*(Y_0, Y_1, \cdots, Y_{r+1})$ *an irreducible form defining* V^*. *Let* m *be the degree of* F^* *and* A_i^* *the forms of degrees* $< m-r$ *such that*

$$\sum_{i=0}^{r+1} A_i^* F_i^* = 0. \tag{5.1}$$

Then A^**'s must be identically zero, provided* m *is not divisible by the characteristic* p *of the universal domain.*

Proposition 18. *Assume that our conjecture holds true, and let* V *be a non-singular variety whose projective degree is not divisible by the characteristic* p. *Using the same notations as in* § 1 *let* A_i^* $(i=0, 1, \cdots, r+1)$ *be forms in* Y*'s of degree* $< m-r$ *such that*

$$\sum_{i=0}^{r+1} A_i^*(\eta) F_i^*(\eta) = 0. \tag{5.2}$$

Then A_i^* *must be of the form* $\eta_i N^*$, *where* N^* *is a form of degree* $\leqq m-r-2$.

Proof. From the relation (5.2) we have the identity

$$\sum_{i=0}^{r+1} A_i^*(Y) F_i^*(Y) = N^*(Y) F^*(Y) \tag{5.3}$$

with a polynomial N^* of degree $\leqq m-r-2$. On the other hand we have the Euler's identity for homogeneous form

$$\sum_{i=0}^{r+1} Y_i F_i^* = mF^*. \tag{5.4}$$

Combining (5.3) and (5.4) we get an identity

$$\sum_{i=0}^{r+1} (mA_2^* - Y_i N^*) F_i^* = 0.$$

The lemma implies that $A_i^* = Y_i N^*/m$. q.e.d.

Combining the Propositions 16, 17 and 18 we see the following

If our conjecture holds true, then any $(r-1)$-fold differential form $(\neq 0)$ of the first kind on a non-singular projective variety cannot have the property (P), *provided* $\deg \mathrm{V}$ *is not divisible by the characteristic* p *of the universal domain.*

At the end, we shall give one more proposition, from which we can deduce the preservation of the independency of the differential forms of the first kind on its generic hyperplane section.

PROPOSITION 19. *Using the same assumptions and notations as in Prop. 18, let* A_i^* $(i=1,\cdots,q+1)$ *be the forms in* Y*'s of degree* $\leqq m-q-1 (q\leqq r)$, *and assume that there exists a relation of the form*

$$(5.5) \qquad \sum_{i=1}^{r+1} A_i^*(\eta)F_{\lambda_i}^*(\eta)=0.$$

Then $A_i^*=0$.

PROOF. When $q=r$, this is a special case of the preceding proposition. We shall use the induction on the number $r-q$. Suppose that $q<r$, then $q+1\leqq r$, there exists an index j such that F_j does not appear in (5.5). We shall assume that F_0 does not appear in (5.5). Let $\mathrm{V}_0^*=\mathrm{V}^*\cdot S_0^r$, where S_0 is a linear variety in S^{r+1} defined by the equation $Y_0=0$. Then as is easily seen that V_0^* is a generic projection of $\mathrm{V}_0=\mathrm{V}\cdot H_0$ where H_0 is a hyperplane defined in § 1, V_0^* is defined by the form $F^{*0}(Y_1,\cdots,Y_{r+1})=F^*(0,Y_1,\cdots,Y_{r+1})$ and $\partial F^{*0}/\partial Y_i= F_i^*(0,Y_1,\cdots,Y_{r+1})$ if $i\geqq 1$. Applying the induction assumption on V_0^* we see that $A^{*0}=0$, where A^{*0} is the restriction of A^* on V_0^*. Since degrees of A^*'s are less than m these are the identities, and we see that A^*'s must be of the form $A_i^*=\eta_0A_i^{**}$. Thus we have analogous relations $\sum_{i=1}^{q+1} A_i^{**}(\eta)F_{\lambda_i}^*(\eta)=0$. Continuing this process in finite number we arrive at the conclusion. q.e.d.

As a consequence of this proposition we have the following:

Assume that our conjecture holds true. Let V *be a non-singular arithmetically normal projective variety, whose degree is not divisible by the characteristic of the universal domain. Let* C *be a generic hyperplane section of* V *with reference to a field of definition for* V. *Then the restriction map from the vector space of the q-fold differential forms of the first kind on* V *into the vector space of the q-fold differential forms of the first kind on* C *is an isomorphism* $(q<\dim \mathrm{V})$.

PROOF. Let $\omega = \sum_{i_1<\cdots<i_q} A_{i_1\cdots i_q}/F_{r+1}dy_{i_1}\cdots dy_{i_q}$ be a differential form of the 1st kind, and suppose that $\omega_{C_1}=0$. Then $A_{i_1\cdots i_q}$ $(1<i_1<\cdots i_q)$ must be of the form $y_1A'_{i_1\cdots i_q}$ with adjoint A's of the degree $\leqq m-q-2$.

(I) The case $q<r-1$.

Let $i_0, i_1,\cdots, i_q$ be a set of indices taken from $2,\cdots, r$. Then as in §2 we can find adjoint polynomials $A'_{i_0\cdots i_q}$ of degree $\leqq m-q-2$ such that

$$\sum_{j=0}^{q}(-1)^j F_{i_j} A'_{i_0\cdots\hat{i}_j\cdots i_q} = F_{r+1} A'_{i_0\cdots i_q}.$$

Hence by the preceding proposition we have $A_{i_1\cdots i_q}=0$ if $1<i_1\cdots<i_q$. Moreover we see by (2.2′) that $A_{1i_2\cdots i_q}$ are polynomials of degree $\leqq m-q-2$. Then again using the similar argument to the above we see that there exist adjoint polynomials $A'_{i_1\cdots i_q}$ such that

$$\sum_{j=1}^{q}(-1)^j F_{i_1} A_{1i_1\cdots\hat{i}_j\cdots i_q} = F_{r+1} A'_{1i_1\cdots i_q}.$$

From this we have also $A_{1i_2\cdots i_q}=0$. Hence $\omega=0$.

(II) The case $q=r-1$.

In this case we shall assume that $\omega_{C_0}=0$, without losing any generality, where ω is as above. Then A's are adjoint polynomials of degree $\leqq m-r-1$ by Prop. 12, and we have the relation $\sum_{i=1}^{r} A_i F_i = A' F_{r+1}$ by (2.3′). This implies that $A_i=0$. Hence $\omega=0$. q.e.d.

UNIVERSITY OF KYOTO

BIBLIOGRAPHY

[1] Igusa, J., On some problems in abstract algebraic geometry. Proc. Nat. Acad. Sci. U.S.A., **41** (1955), pp. 964–967.

[2] Kawahara, Y., A note on the differential forms on everywhere normal varieties. Nagoya Math. Jour., **2** (1951), pp. 93–94.

[3] Nagata, M., Basic theorems on general commutative rings. Mem. Coll. Sci. Kyoto Univ., **29** (1955), pp. 59–77.

[4] Nakai, Y., On the divisors of differential forms on algebraic varieties. Jour. Math. Soc. of Japan, **5** (1953), pp. 184–199.

[5] Nakai, Y., On the independency of differential forms on algebraic varieties. Mem. Coll. Sci. Kyoto Univ., **28** (1953), pp. 67–80.

[6] Nakai, Y., Note on the intersection of an algebraic variety with the generic hyperplane. ibid., **26** (1951), pp. 185–187.

[7] Seidenberg, A., The hyperplane sections of normal varieties. Trans. of Amer. Math. Soc., **69** (1950), pp. 357–386.

[8] Serre, J.-P., Faisceaux algébriques cohérents. Ann. of Math., **61** (1955), pp. 197–278.

[9] Severi, F., Sugl'integrali algebrici semplici et doppi. Rend. r. Acad. Lincei, **7** (1928), pp. 1–14.

[10] Waerden, B. L. van-der., Finführung in die algebraische Geometrie. Julius Springer, Berlin (1939).

[11] Weil, A., Foundations of algebraic geometry. Amer. Math. Colloq. Pub., **29** (1946).

[12] Zariski, O., Complete linear system on normal varieties and a generalizations of a lemma of Enriques-Severi. Ann. of Math., **55** (1952), pp. 552–592.

Sur la dimension homologique des anneaux et des modules noethériens

Jean-Pierre SERRE

Dans sa conférence au Colloque de Topologie de Bruxelles [7], J.-L. Koszul a montré quel avantage il y a à exposer la théorie des syzygies de Hilbert en utilisant le langage homologique. Ce point de vue a été repris et systématisé par H. Cartan et S. Eilenberg (cf. [3], Chap. VIII), qui ont notamment étendu les résultats de Koszul à d'autres anneaux que l'anneau des polynômes, par exemple à l'anneau des séries formelles, ou convergentes. En fait, ces résultats sont valables dans tout anneau local régulier: c'est ce que viennent de montrer M. Auslander et D. Buchsbaum, dans un article récent [2], où ils étudient également les relations existant entre la notion de "dimension homologique", introduite dans [3], et la notion classique de dimension, due à Krull; ces relations généralisent celles qui étaient connues dans le cas classique (cf. [5] par exemple).

Dans ce qui suit, je me propose d'exposer certains des résultats de [2], en les complétant sur plusieurs points, et notamment en montrant que la validité du théorème des syzygies caractérise les anneaux locaux réguliers (cf. th. 3). La conséquence sans doute la plus intéressante de cette caractérisation est le fait que tout anneau de fractions d'un anneau local régulier est régulier (cf. th. 5).

1. Conventions et terminologie.

a) Tous les anneaux considérés par la suite seront supposés *commutatifs*, *noethériens*, et *à élément unité*; tous les modules sur ces anneaux seront supposés *unitaires*, et *de type fini*, donc *noethériens*.

b) Si E est un module sur un anneau A, nous appellerons *dimension homologique* de E, et nous noterons $\mathrm{dh}_A(E)$ l'entier (fini ou égal à $+\infty$) appelé dimension "projective" de E, et noté $\dim_A E$, dans [3]: ce changement de terminologie parait nécessaire, si l'on veut appliquer cette notion à la géométrie "projective". Rappelons que $\mathrm{dh}_A(E) \leqq n$ signifie qu'il existe une suite exacte:

$$0 \to P_n \to \cdots \to P_1 \to P_0 \to E \to 0,$$

où les P_i sont des A-modules projectifs (facteurs directs de modules libres).

De même, nous noterons gl.dh(A) la borne supérieure, finie ou infinie, des dh$_A(E)$, pour E parcourant tous les A-modules (se borner aux modules de type fini ne change pas gl.dh(A), d'après un résultat de M. Auslander [1]).

Pour toutes les autres définitions et notations d'algèbre homologique, nous renvoyons à [3].

c) Si A est un anneau, nous noterons dim(A) sa *dimension* au sens de Krull (cf. [8], [13], [14] par exemple), c'est-à-dire la borne supérieure des entiers n tels qu'il existe $n+1$ idéaux premiers emboîtés distincts dans A:

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n.$$

Si $\mathfrak{a}$ est un idéal de A, nous noterons dim$(\mathfrak{a})$ la dimension de l'anneau quotient $A/\mathfrak{a}$. Si A est un anneau local, on sait que dim(A) et les dim$(\mathfrak{a})$ sont finis.

d) Si A est un anneau, et si $\mathfrak{p}$ est in idéal premier de A, nous noterons $A_{\mathfrak{p}}$ l'anneau de fractions de A relativement au complémentaire de $\mathfrak{p}$ (cf. [13], Chap. 2 ainsi que [14], Chap. I, no. 4); rappelons que c'est l'ensemble des fractions a/s, $a \in A$, $s \notin \mathfrak{p}$, deux fractions a/s et a'/s' étant identifiées si et seulement si il existe $s'' \notin \mathfrak{p}$ tel que $s''(s'a-sa')=0$; l'anneau $A_{\mathfrak{p}}$ est un anneau local d'idéal maximal $\mathfrak{p}A_{\mathfrak{p}}$ et de corps des restes le corps des fractions de $A/\mathfrak{p}$; la dimension de $A_{\mathfrak{p}}$ est appelée le *rang* de $\mathfrak{p}$, et notée rg$(\mathfrak{p})$.

e) Soit E un A-module. Si $\mathfrak{a}$ est un idéal de A, et si F est un sous-module de E, nous noterons $\mathfrak{a}F$ (ou $\mathfrak{a}\cdot F$) le sous-module de E engendré par les produits $a\circ f$ où a parcourt $\mathfrak{a}$ et f parcourt F. L'idéal $\mathfrak{a}$ sera dit *diviseur de zéro* dans E/F s'il existe $x \in E$, $x \notin F$, tel que $\mathfrak{a}x \subset F$ (c'est-à-dire $ax \in F$ pour tout $a \in \mathfrak{a}$). Soit $F=\bigcap Q_i$ une *décomposition primaire réduite* ([6], §6–[15], Chap. IV) de F dans E, les Q_i correspondant aux idéaux premiers $\mathfrak{p}_i$; nous dirons que les $\mathfrak{p}_i$ sont *les idéaux premiers de F dans E*; on sait ([6], cor. au th. 13–[15], Chap. IV, th. 7) qu'un idéal $\mathfrak{a}$ est diviseur de zéro dans E/F si et seulement si il est contenu dans l'un des $\mathfrak{p}_i$ (ou dans la réunion des $\mathfrak{p}_i$, cela revient au même d'après la prop. 6 du Chap. I de [13]); en particulier, l'ensemble des $a \in A$ qui sont diviseurs de zéro dans E/F est égal à la réunion des $\mathfrak{p}_i$.

f) Conformément à l'usage de N. Bourbaki, nous dirons qu'une application f: $E \to E'$ est *injective* si $f(e_1)=f(e_2)$ entraîne $e_1=e_2$, *surjective* si $f(E)=E'$, *bijective* si elle est à la fois injective et surjective. Une application injective (resp. surjective, bijective) est appelée une *injection* (resp. une *surjection,* une *bijection*).

2. La notion de E-suite.

Soit A un anneau local d'idéal maximal $\mathfrak{m}$, et soit E un A-module.

DÉFINITION 1. *Une suite* $(a_1, \cdots, a_q)$ *d'éléments de* $\mathfrak{m}$ *est appelée une* E*-suite si, pour tout* $i \leqq q$, *l'élément* a_i *n'est pas diviseur de zéro dans* $E/(a_1, \cdots, a_{i-1})E$. *L'entier* q *est appelé la longueur de la* E*-suite.* (Cf. [2], §3.)

Une E-suite $(a_1, \cdots, a_q)$ est dite *maximale* s'il n'existe aucun élément $a_{q+1} \in \mathfrak{m}$ tel que $(a_1, \cdots, a_q, a_{q+1})$ soit une E-suite; cela signifie que tout élément de $\mathfrak{m}$ est diviseur de zéro dans $E/(a_1, \cdots, a_q)E$; si $\mathfrak{p}_1, \cdots, \mathfrak{p}_k$ désignent les idéaux premiers de $(a_1, \cdots, a_q)E$ dans E, la condition précédente équivaut à dire que $\mathfrak{m}$ est contenu dans la réunion des $\mathfrak{p}_i$, donc est égal à l'un des $\mathfrak{p}_i$ (cf. no. 1).

Nous montrerons plus loin que, si E n'est pas réduit à 0, toute E-suite peut être prolongée en une E-suite maximale (cor. à la prop. 2), et que deux E-suites maximales ont même longueur (th. 2).

PROPOSITION 1. *Soit* E *un* A*-module, et soit* $\hat{E}$ *son complété, considéré comme module sur le complété* $\hat{A}$ *de* A. *Si une suite* $(a_1, \cdots, a_q)$ *est une* E*-suite* (*resp. une* E*-suite maximale*), *c'est aussi une* $\hat{E}$*-suite* (*resp. une* $\hat{E}$*-suite maximale*).

Puisque A est un anneau local, c'est un anneau de Zariski, et le foncteur $\hat{E}$ est un foncteur *exact* ([15], Chap. V, §2); en particulier, supposons que F soit un A-module et que $a \in \mathfrak{m}$ soit non diviseur de zéro dans F; on a une suite exacte:

$$0 \to F \xrightarrow{a} F \to F/aF \to 0,$$

d'où, par complétion, la suite exacte $0 \to \hat{F} \xrightarrow{a} \hat{F} \to \hat{F}/a\hat{F} \to 0$, qui montre que a est non diviseur de zéro dans $\hat{F}$. Par récurrence sur q, on en déduit que, si $(a_1, \cdots, a_q)$ est une E-suite, c'est aussi une $\hat{E}$-suite. Supposons maintenant que $(a_1, \cdots, a_q)$ soit une E-suite maximale i.e. que $\mathfrak{m}$ soit un idéal premier de $F = (a_1, \cdots, a_q)E$ dans E; il existe alors (cf. no. 1) un élément $x \in E$, $x \notin F$, tel que $\mathfrak{m} \cdot x \subset F$; on aura donc $\hat{\mathfrak{m}} \cdot x = \hat{A} \cdot \mathfrak{m} \cdot x \subset \hat{A} \cdot F = \hat{F}$, et $x \notin \hat{F}$ puisque $\hat{F} \cap E = F$ (cf. [15], loc. cit.); donc $\hat{\mathfrak{m}}$ est diviseur de zéro dans $\hat{E}/\hat{F} = \hat{E}/(a_1, \cdots, a_q)\hat{E}$, ce qui montre bien que la $\hat{E}$-suite $(a_1, \cdots, a_q)$ est maximale.

PROPOSITION 2. *Soit* E *un* A*-module, et soient* $\mathfrak{p}_i$ *les idéaux* *premiers de* 0 *dans* E. *Si* $(a_1, \cdots, a_q)$ *est une* E*-suite, on a* $q \leqq \dim(\mathfrak{p}_i)$ *pour tout* i.

Nous utiliserons le lemme suivant:

LEMME 1. *Soit* E *un* A*-module et soit* a *un élément de* $\mathfrak{m}$ *qui ne soit pas diviseur de zéro dans* E. *Si* $\mathfrak{p}$ *est un idéal premier de* 0 *dans* E, *il existe un idéal premier* $\mathfrak{p}'$ *de* aE *dans* E *qui contient l'idéal* $\mathfrak{p}+(a)$.

(Cf. [5], §135, no. 8).

S'il n'existait pas d'idéal $\mathfrak{p}'$ vérifiant les conditions de l'énoncé, l'idéal $\mathfrak{p}+(a)$ ne serait pas diviseur de zéro dans E/aE (no. 1), autrement dit, la relation $(\mathfrak{p}+(a))\cdot x \subset aE$ entraînerait $x \in aE$; comme on a évidemment $ax \in aE$, ceci signifie que la relation $\mathfrak{p}\cdot x \subset aE$ entraînerait $x \in aE$. 'Considérons alors le sous-module N de E formé des x tels que $\mathfrak{p}\cdot x=0$; puisque $\mathfrak{p}$ est un idéal premier de 0 dans E, on a $N \neq 0$ (cf. no. 1); mais, si $x \in N$, on a $\mathfrak{p}\cdot x=0 \subset aE$, d'où $x \in aE$, d'après ce que nous venons de voir, et l'on peut écrire $x=ay$, avec $y \in E$. La relation $\mathfrak{p}\cdot x=0$ s'écrit alors $\mathfrak{p}\cdot ay=0$, et, comme a n'est pas diviseur de zéro dans E, ceci entraîne $\mathfrak{p}\cdot y=0$, i.e. $y \in N$. On voit donc que $N=aN$, et, comme a appartient à $\mathfrak{m}$, ceci entraîne $N=0$ (cf. [3], Chap. VIII, Prop. 5.1'), d'où la contradiction cherchée.

Démontrons maintenant la prop. 2 par récurrence sur q, le cas $q=0$ étant trivial. Soit $\mathfrak{p}$ l'un des idéaux $\mathfrak{p}_i$, et soit $\mathfrak{p}'$ un idéal premier vérifiant les conditions du lemme 1 (avec $a=a_1$). Puisque le module E/a_1E possède la E/a_1E-suite $(a_2, \cdots, a_q)$, l'hypothèse de récurrence montre que $q-1 \leqq \dim(\mathfrak{p}')$. Mais $\mathfrak{p}' \subset \mathfrak{p}$, $\mathfrak{p}' \neq \mathfrak{p}$ (car sinon on aurait $a_1 \in \mathfrak{p}$, et a_1 serait diviseur de zéro dans E); d'où $\dim(\mathfrak{p}') \leqq \dim(\mathfrak{p})-1$, et $q \leqq \dim(\mathfrak{p})$, cqfd.

COROLLAIRE. *Si* E *est un* A*-module* $\neq 0$, *toute* E*-suite peut être prolongée en une* E*-suite maximale.*

En effet, la condition $E \neq 0$ signifie que l'ensemble des idéaux premiers de 0 dans E est non vide, et la prop.^{2}1 montre alors que la longueur de toute E-suite est bornée par la dimension de l'un quelconque de ces idéaux.

3. Relations entre les notions de E-suite et de dimension homologique.

Les notations étant les mêmes que précédement, nous désignerons par k le corps des restes de l'anneau local A; puisque k est un anneau quotient de A, on peut le considérer comme un A-module, et les $\mathrm{Tor}_p^A(E, k)$ sont donc définis pour tout entier $p \geqq 0$ et tout A-module E. D'après [3], Chap. VIII, les relations:

$$\text{“}\mathrm{Tor}_p^A(E, k)=0\text{”} \quad \text{et} \quad \text{“}\mathrm{dh}_A(E)<p\text{”}$$

sont équivalentes. En particulier, gl.dh(A) est égal à $\mathrm{dh}_A(k)$, lui-même égal au plus petit entier q tel que $\mathrm{Tor}_{q+1}^A(k, k)=0$.

PROPOSITION 3. *Soit E un A-module $\neq 0$, et soit $(a_1, \cdots, a_q)$ une E-suite. Si $Q=E/(a_1, \cdots, a_q)E$, on a* $\mathrm{dh}_A(Q)=\mathrm{dh}_A(E)+q$.

(Ce résultat est bien connu dans la théorie classique des syzygies, cf. [5], §152, no. 6; dans le cas des anneaux locaux, voir [2], §3 ainsi que [16], no. 76, lemme 2.)

Par récurrence sur q, on voit que l'on peut supposer $q=1$. Désignons par u l'homothétie de rapport a_1 dans E. On a une suite exacte:

$$(*) \qquad 0 \to E \overset{u}{\to} E \to Q \to 0.$$

Pour tout entier $p \geqq 0$, u définit un homomorphisme

$$u_p : \mathrm{Tor}_p^A(E, k) \to \mathrm{Tor}_p^A(E, k).$$

Il résulte des propriétés générales des Tor que l'on obtient le même homomorphisme u_p en considérant l'homothétie de rapport a_1 dans k, et non plus dans E. Comme a_1 appartient à $\mathfrak{m}$, cette homothétie est identiquement nulle, et l'on a $u_p=0$ pour tout p. La suite exacte:

$$\cdots \to \mathrm{Tor}_p^A(E, k) \to \mathrm{Tor}_p^A(E, k) \to \mathrm{Tor}_p^A(Q, k) \to \mathrm{Tor}_{p-1}^A(E, k) \to \cdots$$

associée à la suite exacte $(*)$ se décompose donc en suites exactes partielles:

$$0 \to \mathrm{Tor}_p^A(E, k) \to \mathrm{Tor}_p^A(Q, k) \to \mathrm{Tor}_{p-1}^A(E, k) \to 0.$$

Si l'on pose $s=\mathrm{dh}_A(E)$, les suites exactes précédentes montrent que $\mathrm{Tor}_p^A(Q, k) \neq 0$ pour $p \leqq s+1$ et $\mathrm{Tor}_p^A(Q, k)=0$ pour $p > s+1$, ce qui montre bien que $\mathrm{dh}_A(Q)=s+1$, cqfd.

PROPOSITION 4. *Supposons que* gl.dh(A) *soit finie,et égale à s. Alors, si E est un A-module $\neq 0$, la longueur de toute E-suite maximale est égale à $s-\mathrm{dh}_A(E)$.*

Soit $(a_1, \cdots, a_q)$ une E-suite maximale, et soit $Q=E/(a_1, \cdots, a_p)E$. D'après la proposition précédente, on a $\mathrm{dh}_A(E)=\mathrm{dh}_A(Q)-q$, et il nous suffira donc de prouver que $\mathrm{dh}_A(Q)=s$. D'après ce que nous avons vu au no. 2, l'idéal $\mathfrak{m}$ de A est diviseur de zéro dans Q; on peut donc trouver un élément $x \in Q$, $x \neq 0$, tel que $\mathfrak{m} \cdot x=0$; l'élément x engendre donc un sous-module de Q isomorphe à k, et l'on a ainsi obtenu une suite exacte:

$$0 \to k \to Q \to Q/k \to 0.$$

On en déduit la suite exacte:

$$\mathrm{Tor}_{s+1}^A(Q/k, k) \to \mathrm{Tor}_s^A(k, k) \to \mathrm{Tor}_s^A(Q, k).$$

Puisque $s=$gl.dh(A), on a $\mathrm{Tor}_{s+1}^A(Q/k, k)=0$, et $\mathrm{Tor}_s^A(k, k) \neq 0$; d'où $\mathrm{Tor}_s^A(Q, k) \neq 0$, ce qui montre que $\mathrm{dh}_A(Q) \geqq s$; comme il est trivial que $\mathrm{dh}_A(Q) \leqq s$, la proposition est démontrée.

COROLLAIRE 1. *Pour que* $\mathrm{dh}_A(E)$ *soit égal à* s, *il faut et il suffit que* $\mathfrak{m}$ *soit un idéal premier de* 0 *dans* E.

En effet, les deux conditions équivalent à dire que toute E-suite est vide.

COROLLAIRE 2. *Si* $\mathrm{gl.dh}(A)$ *est finie, on a* $\mathrm{gl.dh}(A) \leqq \dim(A)$.

(En fait, on a $\mathrm{gl.dh}(A) = \dim(A)$, cf. [2], lemme 4.2, ainsi que les ths. 1 et 3 ci-après.)

En appliquant la prop. 4 à $E = A$, on voit que s est égal à la longueur de toute A-suite maximale; la prop. 2 montre alors que $s \leqq \dim(\mathfrak{p})$, pour tout idéal premier $\mathfrak{p}$ de 0 dans A, d'où *a fortiori* $s \leqq \dim(A)$.

THÉORÈME 1. *Si* A *est un anneau local régulier* (cf. [14], p. 29) *de dimension* n, *on a* $\mathrm{gl.dh}(A) = n$.

(Cf. [2], §4, ainsi que [3], Chap. VIII.)

Par définition, l'idéal $\mathfrak{m}$ de A peut être engendré par n éléments $(x_1, \cdots, x_n)$; de plus on sait ([14], loc. cit.) que, pour tout $i \leqq n$, l'anneau $A/(x_1, \cdots, x_{i-1})$ est un anneau local régulier, donc intègre, et x_i n'est pas diviseur de zéro dans $A/(x_1, \cdots, x_{i-1})$. Il s'ensuit que $(x_1, \cdots, x_n)$ est une A-suite; en appliquant la prop. 3 avec $E = A$, et en remarquant que $E/(a_1, \cdots, a_n)E = A/\mathfrak{m} = k$, on obtient:

$$\mathrm{dh}_A(k) = \mathrm{dh}_A(A) + n = n \text{ (puisque } A \text{ est } A\text{-libre),}$$

ce qui démontre le théorème, car $\mathrm{dh}_A(k) = \mathrm{gl.dh}(A)$.

Puisque $\mathrm{gl.dh}(A) = n < +\infty$, on peut appliquer la prop. 4. D'où:

COROLLAIRE 1. *Si* E *est un* A*-module* $\neq 0$, *la longueur de toute suite maximale est égale à* $n - \mathrm{dh}_A(E)$

Et, en appliquant la prop. 2:

COROLLAIRE 2. *Si* $\mathfrak{p}_i$ *désignent les idéaux premiers de* 0 *dans* E, *on a* $\mathrm{dh}_A(E) \geqq n - \dim(\mathfrak{p}_i)$ *pour tout* i.

Remarques.

1) On peut avoir $\mathrm{dh}_A(E) > n - \dim(\mathfrak{p}_i)$ pour tout i, comme le montrent de nombreux exemples. Cf. [5], §155, no. 8.

2) Le corollaire 1 ci-dessus fournit un procédé commode pour calculer $\mathrm{dh}_A(E)$. A titre d'exemple, montrons que tout anneau local régulier A de dimension 2 est factoriel, résultat dû à Krull ([9], Satz 9) et Samuel ([14], p. 61): puisque l'on sait que A est intégralement clos, il nous suffit de montrer que tout idéal premier minimal $\mathfrak{p}$ de A est principal; or il existe évidemment un élément $a \in \mathfrak{m}$ non contenu dans $\mathfrak{p}$, et cet élément n'est pas diviseur de zéro dans $A/\mathfrak{p}$; en appliquant le cor. 1 au module $A/\mathfrak{p}$, on en déduit

$\mathrm{dh}_A(A/\mathfrak{p}) \leq 1$, d'où $\mathrm{dh}_A(\mathfrak{p}) \leq 0$, ce qui signifie que $\mathfrak{p}$ est un A-module libre, donc est un idéal principal, cqfd.

4. Codimension homologique d'un module sur un anneau local.

THÉORÈME 2. *Soit A un anneau local. Si E est un A-module $\neq 0$, toutes les E-suites maximales ont même longueur.*

(Cf. [2], §3.)

Soient $(a_1, \cdots, a_p)$ et $(a'_1, \cdots, a'_q)$ deux E-suites maximales; d'après la prop. 1, ce sont aussi des $\hat{E}$-suites maximales. En vertu d'un théorème de Cohen ([4], cor. 2 au th. 15 - voir aussi [14], Chap. IV), l'anneau local complet $\hat{A}$ est isomorphe au quotient d'un anneau local régulier B; ainsi, $\hat{E}$ se trouve muni d'une structure de B-module. Si $(b_1, \cdots, b'_q)$ désignent de représentants dans B de $(a_1, \cdots, a'_q)$, il est clair que $(b_1, \cdots, b_p)$ et $(b'_1, \cdots, b'_q)$ sont des $\hat{E}$-suites maximales, et le cor. 1 au th. 1 montre alors que $p = q = \dim(B) - \mathrm{dh}_B(\hat{E})$, cqfd.

DÉFINITION 2. *Si E est un A-module $\neq 0$, on appelle codimension homologique de E, et on note* $\mathrm{codh}_A(E)$, *la longueur de toute E-suite maximale.*

Remarques.

1) La notation $\mathrm{codh}_A(E)$ est justifiée par le cor. 1 au th. 1: si A est un anneau local régulier de dimension n, on a:

$$\mathrm{dh}_A(E) + \mathrm{codh}_A(E) = n.$$

2) A la différence de la notion de dimension homologique, celle de codimension est indépendante de l'anneau A considéré, et ne dépend que du module E. De façon plus précise, si E est un A-module, et si l'anneau A est un quotient d'un anneau local B, on a:

$$\mathrm{codh}_A(E) = \mathrm{codh}_B(E).$$

On peut donc écrire $\mathrm{codh}(E)$ au lieu de $\mathrm{codh}_A(E)$ sans risque d'ambiguïté.

3) Il serait intéressant de trouver une démonstration directe du th. 2, n'utilisant ni les théorèmes de structure de Cohen, ni la notion de dimension homologique.

Exemples.

1) Prenons pour module E l'anneau local A lui-même. D'après la prop. 2, on a $\mathrm{codh}(A) \leq \dim(\mathfrak{p})$ pour tout idéal premier $\mathfrak{p}$ de 0 dans A, et, en particulier, $\mathrm{codh}(A) \leq \dim(A)$. Les anneaux locaux A vérifiant l'égalité $\mathrm{codh}(A) = \dim(A)$ sont ceux qui possèdent un "système distinct de paramètres", au sens de Nagata ([11], §7); on trouvera diverses caractérisations de ces anneaux dans le mémoire

précité de Nagata, et notamment celle-ci: ce sont les anneaux locaux dans lesquels le théorème d'équidimensionnalité de Cohen-Macaulay est valable. Ces anneaux ont pour analogues, dans la théorie classique des syzygies, les quotients d'un anneau de polynômes par un idéal "parfait" (cf. [5], §153).

2) Soit A un anneau local intègre, intégralement clos, et de dimension $\geqq 2$, et soit $\mathfrak{a}$ un idéal fractionnaire de A; supposons que $\mathfrak{a}$ soit un idéal "divisoriel" (cf. [15], p. 82). Je dis que l'on a alors $\operatorname{codh}(\mathfrak{a}) \geqq 2$ (lorsque $\mathfrak{a}=A$, on retrouve le résultat démontré dans [16], no. 76). En effet, on peut tout d'abord supposer (par multiplication par un élément convenable de A) que l'idéal $\mathfrak{a}$ est contenu dans A; si x est un élément non nul de $\mathfrak{m}$, l'idéal $x\cdot\mathfrak{a}$ est un idéal divisoriel, donc est intersection de puissances symboliques d'idéaux premiers minimaux $\mathfrak{p}_\alpha$ (cf. [15], Chap. IV, §4); comme $\dim(A) \geqq 2$, aucun des $\mathfrak{p}_\alpha$ n'est égal à $\mathfrak{m}$, et l'on peut donc choisir un $y \in \mathfrak{m}$ qui n'appartient à aucun des $\mathfrak{p}_\alpha$. Montrons maintenant que (x, y) est une $\mathfrak{a}$-suite, ce qui établira notre assertion; puisque A est intègre et $x \neq 0$, x est non diviseur de zéro dans A, donc *a fortiori* dans $\mathfrak{a} \subset A$; de même, y n'étant contenu dans aucun des $\mathfrak{p}_\alpha$ n'est pas diviseur de zéro dans $A/x\cdot\mathfrak{a}$, donc *a fortiori* dans $\mathfrak{a}/x\cdot\mathfrak{a} \subset A/x\cdot\mathfrak{a}$, cqfd.

3) La notion de codimension homologique permet d'énoncer de façon un peu plus simple certains résultats relatifs aux faisceaux algébriques cohérents. Ainsi, le th. 2 du no. 74 de [16] s'énonce de la façon suivante:

Soit V une variété algébrique projective, soit $\mathscr{F}$ un faisceau algébrique cohérent sur V, et soit p un entier $\geqq 0$. Les deux conditions suivantes sont équivalentes:

(a) $H^q(V, \mathscr{F}(-n))=0$ *pour n assez grand et* $0 \leqq q < p$.

(b) *Pour tout $x \in V$, on a* $\operatorname{codh}(\mathscr{F}_x) \geqq p$.

(On observera que la condition (b) ne fait pas intervenir le plongement de V dans un espace projectif, alors qu'il n'en est pas de même, *a priori*, pour la condition (a)).

Supposons V irréductible, de dimension r, et appliquons la théorème avec $\mathscr{F}=\mathcal{O}$, et $p=r$; nous voyons ainsi que la condition "$H^q(V, \mathcal{O}(-n))=0$ pour n assez grand et $0 \leqq q < r$" est vérifiée si et seulement si tous les anneaux locaux $\mathcal{O}_x$, $x \in V$, vérifient les conditions de l'exemple 1 ci-dessus; ce résultat contient évidemment comme cas particulier celui du no. 75 de [16].

5. Caractérisation homologique des anneaux locaux réguliers.

THÉORÈME 3. *Soit A un anneau local. Pour que* gl.dh(A) *soit* *finie, il faut et il suffit que A soit un anneau local régulier.*

Si A est régulier, nous savons déjà (cf. th. 1) que $\mathrm{gl.dh}(A) = \dim(A) < +\infty$. Pour démontrer la réciproque, nous aurons besoin du théorème suivant:

Théorème 4. *Soit A un anneau local, d'idéal maximal $\mathfrak{m}$, de corps des restes $k = A/\mathfrak{m}$, et soit n la dimension du k-espace vectoriel $\mathfrak{m}/\mathfrak{m}^2$. Pour tout entier $p \geqq 0$, le A-module $\mathrm{Tor}_p^A(k, k)$ est un k-espace vectoriel de dimension $\geqq \binom{n}{p}$.*

Admettons provisoirement le th. 4, et montrons comment il entraîne le th. 3: du fait que $\mathrm{Tor}_n^A(k, k)$ est dimension $\geqq 1$ sur k, on a $n \leqq \mathrm{gl.dh}(A)$; d'autre part, le cor. 2 à la prop. 4 montre que $\mathrm{gl.dh}(A) \leqq \dim(A)$, d'où $n \leqq \dim(A)$, ce qui entraîne que A est un anneau local régulier (cf. [14], p. 29).

Le reste de ce n° va être consacré à la démonstration du théorème 4.

Soit $\xi_1, \cdots, \xi_n$ une base du k-espace vectoriel $V = \mathfrak{m}/\mathfrak{m}^2$, et soient $x_1, \cdots, x_n$ des représentants dans $\mathfrak{m}$ des $\xi_1, \cdots, \xi_n$; on sait (cf. [3], Chap. VIII, Prop. 5-1' par exemple) que les x_i engendrent l'idéal $\mathfrak{m}$. Au moyen des x_i on peut, par un procédé bien connu (cf. [7], §2, ou [3], Chap. VIII), définir un complexe $L = \sum_{p=0}^{p=n} L_p$; rappelons-en brièvement la définition:

Un élément de L_p est une application $(i_1, \cdots, i_p) \to a(i_1, \cdots, i_p)$ qui fait correspondre à toute suite $(i_1, \cdots, i_p)$ d'entiers $\leqq n$ un élément de l'anneau A dépendant de façon alternée de $i_1, \cdots, i_p$; on munit L_p d'une structure évidente de A-module, qui en fait un A-module libre de rang $\binom{n}{p}$; l'opérateur bord d: $L_p \to L_{p-1}$ est donné par la formule:

$$(da)(i_1, \cdots, i_{p-1}) = \sum_{i=1}^{i=n} x_i \cdot a(i, i_1, \cdots, i_{p-1}).$$

On a en particulier $L_1 = A^n$, $L_0 = A$, et l'opérateur d: $L_1 \to L_0$ fait correspondre à tout système $a(i) \in A^n$ l'élément $\sum x_i \cdot a(i) \in A$; on a donc $d(L_1) = \mathfrak{m}$.

Lemme 2. *Pour tout entier $p \geqq 1$, l'opérateur d définit, par passage au quotient, une application injective d' de $L_p/\mathfrak{m}L_p$ dans $\mathfrak{m}L_{p-1}/\mathfrak{m}^2L_{p-1}$.*

Posons $L'_p = L_p/\mathfrak{m}L_p$; un élément de L'_p peut s'identifier à une application $(i_1, \cdots, i_p) \to \alpha(i_1, \cdots, i_p)$, où $\alpha(i_1, \cdots, i_p)$ est un élément de k dépendant de façon alternée de $i_1, \cdots, i_p$. On peut également identifier $\mathfrak{m}L_{p-1}/\mathfrak{m}^2L_{p-1}$ à $\mathfrak{m}/\mathfrak{m}^2 \otimes L_{p-1}/\mathfrak{m}L_{p-1} = V \otimes L'_{p-1}$, et l'opérateur d' défini par d, est donné par la formule:

$$(d'\alpha)(i_1,\cdots,i_{p-1})=\sum_{i=1}^{i=n}\xi_i\otimes\alpha(i,i_1,\cdots,i_{p-1}).$$

Mais, par hypothèse, les ξ_i forment une base de V; donc $d'\alpha=0$ entraîne que, pour tout i, $\alpha(i,i_1,\cdots,i_{p-1})=0$, c'est-à-dire $\alpha=0$, cqfd.

On notera que le complexe L défini ci-dessus n'est en général pas acyclique; autrement dit, la suite:

$$0\to L_n\to L_{n-1}\to\cdots\to L_1\to L_0\to k\to 0,$$

n'est pas nécessairement exacte. Le lemme suivant montre que l'on peut toutefois la "compléter" en une suite exacte:

LEMME 3. *Il existe une suite exacte de A-modules:*

$$\cdots\to M_p\xrightarrow{d}M_{p-1}\to\cdots\to M_0\to k\to 0$$

qui vérifie les conditions suivantes:

a) *Si Q_p désigne le noyau de $d:M_p\to M_{p-1}$, l'homomorphisme d définit, par passage au quotient, une bijection de $M_p/\mathfrak{m}M_p$ sur $Q_{p-1}/\mathfrak{m}Q_{p-1}$.*

b) *Le module M_p est somme directe du module L_p et d'un module libre N_p; la restriction de d à L_p applique L_p dans L_{p-1} et coïncide avec l'homomorphisme d défini ci-dessus.*

Nous allons construire les M_p et $d:M_p\to M_{p-1}$ par récurrence sur l'entier p. Pour $p=0$, on pose $M_0=L_0=A$; pour $p=1$, on pose $M_1=L_1$; du fait que $d(L_1)=\mathfrak{m}$, la suite $M_1\to M_0\to k\to 0$ est exacte, et d applique biunivoquement $M_1/\mathfrak{m}M_1$ sur $\mathfrak{m}/\mathfrak{m}^2$.

Supposons donc que la suite exacte $M_{p-1}\to M_{p-2}\to\cdots\to M_0\to k\to 0$ ait été définie, et qu'elle vérifie les conditions a) et b).

Du fait que le composé $L_p\xrightarrow{d}L_{p-1}\xrightarrow{d}L_{p-2}$ est nul, on a $d(L_p)\subset Q_{p-1}$, d'où un homomorphisme $d'':L_p/\mathfrak{m}L_p\to Q_{p-1}/\mathfrak{m}Q_{p-1}$. Je dis que d'' est injectif. Tout d'abord, puisque $M_{p-1}/\mathfrak{m}M_{p-1}\to Q_{p-2}/\mathfrak{m}Q_{p-2}$ est bijectif (d'après la condition a), le noyau Q_{p-1} de $d:M_{p-1}\to Q_{p-2}$ est contenu dans $\mathfrak{m}M_{p-1}$; il nous suffit donc de prouver que l'homomorphisme composé:

$$L_p/\mathfrak{m}L_p\xrightarrow{d''}Q_{p-1}/\mathfrak{m}Q_{p-1}\to\mathfrak{m}M_{p-1}/\mathfrak{m}^2M_{p-1}$$

est injectif; mais la condition b) entraîne que $\mathfrak{m}M_{p-1}/\mathfrak{m}^2M_{p-1}$ est isomorphe à la somme directe de $\mathfrak{m}L_{p-1}/\mathfrak{m}^2L_{p-1}$ et de $\mathfrak{m}N_{p-1}/\mathfrak{m}^2N_{p-1}$, et notre assertion résulte donc du lemme 2.

Soient alors $y_1,\cdots,y_k$ des éléments de Q_{p-1} dont les classes mod $\mathfrak{m}Q_{p-1}$ forment une base d'un supplémentaire de $d''(L_p/\mathfrak{m}L_p)$ dans le k-espace vectoriel $Q_{p-1}/\mathfrak{m}Q_{p-1}$. Posons $N_p=A^k$, et définissons $d:N_p\to Q_{p-1}$ par la condition que d applique la base canonique de N_p sur $y_1,\cdots,y_k$; prenons pour M_p la somme directe de L_p et de N_p, et définissons d sur M_p par linéarité. Par construction, d applique M_p

dans Q_{p-1}, et définit un isomorphisme de $M_p/\mathfrak{m}M_p$ sur $Q_{p-1}/\mathfrak{m}Q_{p-1}$; il s'ensuit (cf. [3], Chap. VIII, Prop. 5.1′) que $d(M_p)=Q_{p-1}$, et il est clair que les conditions a) et b) sont satisfaites, cqfd.

Montrons maintenant comment le lemme 3 entraîne le théorème 4. Par définition, les $\mathrm{Tor}_p^A(k, k)$ sont les modules d'homologie du complexe formé par les $M_p \otimes_A k = M_p/\mathfrak{m}M_p$. Mais, d'après la condition a), $d(M_p)=Q_{p-1}$ est contenu dans $\mathfrak{m}M_{p-1}$, ce qui montre que l'opérateur bord du complexe précédent est identiquement nul; donc $\mathrm{Tor}_p^A(k, k)$ est isomorphe à $M_p/\mathfrak{m}M_p$. Mais, d'après la condition b), $M_p/\mathfrak{m}M_p$ est isomorphe à la somme directe de $L_p/\mathfrak{m}L_p$ et de $N_p/\mathfrak{m}N_p$, et, comme $L_p/\mathfrak{m}L_p$ est un espace vectoriel de dimension $\binom{n}{p}$ sur k, le théorème 4 est démontré, et, avec lui, le théorème 3.

6. Applications.

Nous montrerons d'abord comment les résultats qui précèdent permettent de démontrer, de façon simple, le théorème de Cohen-Macaulay ([4], th. 21- cf. aussi [14], p. 53 et [11], §7):

PROPOSITION 5. *Soit A un anneau local régulier de dimension n et d'idéal maximal $\mathfrak{m}$, et soient $a_1, \cdots, a_p$ des éléments de $\mathfrak{m}$ tels que* $\dim(A/(a_1, \cdots, a_p))=n-p$. *Alors tous les idéaux premiers de l'idéal $(a_1, \cdots, a_p)$ sont de rang p et de dimension $n-p$.*

Si $a_1, \cdots, a_p$ sont des éléments quelconques de $\mathfrak{m}$, on a évidemment $\dim(A/(a_1, \cdots, a_p)) \geqq n-p$; si l'égalité est vérifiée, nous dirons que le système $a_1, \cdots, a_p$ est *pur*; cela équivaut à dire que les $a_1, \cdots, a_p$ font partie d'un système de paramètres de A, cf. [14], Chap. II, no. 4.

Ceci posé, raisonnons par récurrence sur p, le cas $p=0$ étant trivial. Puisque le système $a_1, \cdots, a_p$ est pur, il en est même du système $a_1, \cdots, a_{p-1}$, et l'hypothèse de récurrence montre que les idéaux premiers $\mathfrak{p}_i$ de cet idéal sont tous de dimension $n-p+1$. L'élément a_p n'appartient à aucun des $\mathfrak{p}_i$, car, si l'on avait par exemple $a_p \in \mathfrak{p}_1$, on aurait $(a_1, \cdots, a_p) \subset \mathfrak{p}_1$, d'où:

$$\dim(A/(a_1, \cdots, a_p)) \geqq \dim(A/\mathfrak{p}_1)=n-p+1,$$

contrairement à l'hypothèse.

Il s'ensuit (cf. no. 1) que a_p n'est pas diviseur de zéro dans $A/(a_1, \cdots, a_{p-1})$, et de même a_i n'est pas diviseur de zéro dans $A/(a_1, \cdots, a_{i-1})$; la suite $(a_1, \cdots, a_p)$ est donc une A-suite, au sens de la définition 1. La prop. 3 montre alors que $\mathrm{dh}_A(A/(a_1, \cdots, a_p))=\mathrm{dh}_A(A)+p=p$. Si maintenant $\mathfrak{p}$ désigne un idéal premier de $(a_1, \cdots, a_p)$, le cor. au th. 1 montre que $p \geqq n-\dim(\mathfrak{p})$; d'autre part, l'hypothèse entraîne $\dim(\mathfrak{p}) \leqq n-p$, d'où $\dim(\mathfrak{p})=n-p$. En outre, $\mathfrak{p}$ contient l'un des $\mathfrak{p}_i$, soit $\mathfrak{p}_1$ par exemple, et l'hypothèse de récurrence entraîne que $\mathrm{rg}(\mathfrak{p}_1)=p-1$; comme $\mathfrak{p}$ contient x_p, qui n'est pas contenu dans $\mathfrak{p}_1$, on a $\mathfrak{p} \neq \mathfrak{p}_1$, d'où $\mathrm{rg}(\mathfrak{p}) \geqq \mathrm{rg}(\mathfrak{p}_1)+1=p$; en sens inverse, on a l'inégalité évidente $\mathrm{rg}(\mathfrak{p})+\dim(\mathfrak{p}) \leqq n$, c'est-à-dire $\mathrm{rg}(\mathfrak{p}) \leqq p$, d'où $\mathrm{rg}(\mathfrak{p})=p$, cqfd.

COROLLAIRE. *Si A est un anneau local régulier, et si $\mathfrak{p}$ est un idéal premier de A, on a* $\mathrm{rg}(\mathfrak{p})+\dim(\mathfrak{p})=\dim(A)$.

(Ce résultat est dû à Krull, cf. [8], Satz 11.)

Les notations étant les mêmes que ci-dessus, soit $a_1, \cdots, a_p$ un système pur d'éléments de $\mathfrak{p}$, ayant le plus grand nombre possible d'éléments. Puisque $\mathfrak{p}$ contient l'idéal $(a_1, \cdots, a_p)$, il contient au moins l'un des idéaux premiers $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ de cet idéal, soit $\mathfrak{p}_1$ par exemple. Montrons que l'on a $\mathfrak{p}=\mathfrak{p}_1$, ce qui démontrera le corollaire, en vertu de la proposition précédente. Si l'on avait $\mathfrak{p} \neq \mathfrak{p}_1$, l'idéal $\mathfrak{p}$ ne serait contenu dans aucun des $\mathfrak{p}_i$ (aucun des $\mathfrak{p}_i$ ne peut contenir $\mathfrak{p}_1$ puisque $\dim(\mathfrak{p}_i)=\dim(\mathfrak{p}_1)$ d'après la proposition précédente); d'après la prop. 6 du Chap. I de [13], il existerait alors un élément $a_{p+1} \in \mathfrak{p}$ tel que $a_{p+1} \notin \mathfrak{p}_i$ pour tout i; cette dernière propriété entraîne que $A/(a_1, \cdots, a_{p+1})$ est un anneau de dimension $\dim(A)-p-1$ (cf. [14], p. 28); le système $a_1, \cdots, a_{p+1}$ serait donc pur, contrairement au caractère maximal de l'entier p, cqfd.

Le corollaire précédent signifie que la dimension de l'anneau de fractions $A_{\mathfrak{p}}$ est égale à $\dim(A)-\dim(\mathfrak{p})$; le résultat suivant précise la structure de $A_{\mathfrak{p}}$:

THÉORÈME 5. *Si A est un anneau local régulier, et si $\mathfrak{p}$ est un idéal premier de A, l'anneau $A_{\mathfrak{p}}$ est aussi un anneau local régulier.*

En effet, d'après le th. 3, il suffit de démontrer que $\mathrm{gl.dh}(A_{\mathfrak{p}})<+\infty$; comme nous savons que $\mathrm{gl.dh}(A)<+\infty$, notre assertion résulte donc de l'inégalité

$$(*) \qquad \mathrm{gl.dh}(A_{\mathfrak{p}}) \leqq \mathrm{gl.dh}(A),$$

démontrée dans [2], §4.

(Pour être complets, rappelons brièvement la démonstration de l'inégalité (*): si $n=\mathrm{gl.dh}(A)$, on peut trouver une suite exacte de A-modules:

$$0 \rightarrow L_n \rightarrow \cdots \rightarrow L_1 \rightarrow L_0 \rightarrow A/\mathfrak{p} \rightarrow 0,$$

où les L_i sont libres; par produit tensoriel avec $A_{\mathfrak{p}}$, on en déduit que le $A_{\mathfrak{p}}$-module $A/\mathfrak{p} \otimes_A A_{\mathfrak{p}}=A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ est de dimension homologique $\leqq n$, d'où l'inégalité cherchée.)

Remarques.

1) Le théorème précédent était connu dans divers cas particuliers: il avait été démontré, pour les anneaux locaux géométriques, par Zariski ([17], §5.3), pour les anneaux locaux complets non ramifiés, par Cohen ([4], th. 20), et, sans faire d'hypothèse sur A, mais en supposant $\mathfrak{p}$ "analytiquement non ramifié", par Nagata ([11], §13).

2) Lorsque A est non ramifié, il en est de même de $A_{\mathfrak{p}}$, d'après un résultat de Nagata ([10], cf. aussi [11], Lemme 1.19); en fait, ce résultat peut se déduire très simplement du théorème 5 lui-même: il suffit de montrer que, si x est un élément de $\mathfrak{p}$ tel que l'anneau A/xA soit régulier, il en est même de l'anneau $A_{\mathfrak{p}}/xA_{\mathfrak{p}}$, ce qui résulte du th. 5, appliqué à l'anneau A/xA, et à l'idéal premier $\mathfrak{p}/xA$ de cet anneau.

Le théorème 5 peut être appliqué au problème des "chaînes d'idéaux premiers":

PROPOSITION 6. *Soit A un anneau local, isomorphe au quotient d'un anneau local régulier. Si $\mathfrak{p}' \subset \mathfrak{p}$ sont deux idéaux premiers de A, toutes les chaînes saturées d'idéaux premiers joignant $\mathfrak{p}'$ à $\mathfrak{p}$ ont même longueur, à savoir* $\dim(\mathfrak{p}') - \dim(\mathfrak{p})$.

On peut se borner au cas où A est régulier, et, dans ce cas, il suffit de montrer que, si $\mathfrak{p}' \subset \mathfrak{p}$ sont deux idéaux premiers consécutifs, on a $\dim(\mathfrak{p}') = \dim(\mathfrak{p}) + 1$.

Dire que $\mathfrak{p}'$ et $\mathfrak{p}$ sont consécutifs signifie que l'idéal $\mathfrak{p}'A_{\mathfrak{p}}$ est de dimension 1. Puisque $A_{\mathfrak{p}}$ est régulier (th. 5), on peut lui appliquer le cor. à la prop. 5, et l'on voit ainsi que $\mathrm{rg}(\mathfrak{p}'A_{\mathfrak{p}}) = \dim(A_{\mathfrak{p}}) - 1$, c'est-à-dire $\mathrm{rg}(\mathfrak{p}') = \mathrm{rg}(\mathfrak{p}) - 1$; appliquant le cor. à la prop. 5 à l'anneau A lui-même, on en déduit bien que $\dim(\mathfrak{p}') = \dim(\mathfrak{p}) + 1$, cqfd.

Remarque.

La prop. 6 ne s'étend pas à un anneau local quelconque: un contre-exemple a été récemment construit par Nagata; cf. [12], où l'on trouvera également des résultats plus généraux que notre prop. 6.

Ce qui fait toutefois l'intérêt de cette proposition, c'est le fait que la condition "A est isomorphe au quotient d'un anneau local régulier" est une condition très large; en effet, elle est vérifiée par les anneaux locaux *complets* (d'après les théorèmes de Cohen, cf. [4], cor. 2 au th. 15), par les anneaux locaux de *fonctions analytiques* (puisque l'anneau des séries convergentes est régulier), et par les anneaux locaux *de la géométrie algébrique* (éventuellement sur un anneau de Dedekind - cf. [10], ainsi que l'exemple ci-après).

Dans tout ce qui précède, nous ne nous sommes intéressés qu'aux anneaux locaux; cela tient au fait que la notion de dimension homologique a un caractère *local* (cf. [3], Chap. VII, Exer. 11): on pourra donc traduire les résultats obtenus en des résultats valables pour tout anneau. En particulier:

THÉORÈME 6. *Soit A un anneau, et soit n un entier. Les deux conditions suivantes sont alors équivalentes*:

a) $\mathrm{gl.dh}(A) \leqq n$.

b) *Pour tout idéal maximal $\mathfrak{m}$ de A, l'anneau local $A_{\mathfrak{m}}$ est un anneau local régulier de dimension $\leqq n$.*

Cela résulte immédiatement du th. 3, et du fait que $\mathrm{gl.dh}(A)$ est égale à la borne supérieure des $\mathrm{gl.dh}(A_{\mathfrak{m}})$, d'après [3], loc. cit.

COROLLAIRE 1. $\mathrm{gl.dh}(A)$ *est égal, soit à* $+\infty$, *soit à* $\dim(A)$.

COROLLAIRE 2. *Si* $\mathrm{gl.dh}(A) < +\infty$, *pour tout idéal premier $\mathfrak{p}$ de A l'anneau local $A_{\mathfrak{p}}$ est régulier.*

En effet, si $\mathfrak{m}$ est un idéal maximal contenant $\mathfrak{p}$, l'anneau $A_{\mathfrak{m}}$ est un anneau local régulier d'après le th. 6, et, comme $A_{\mathfrak{p}}$ est un anneau de fractions de $A_{\mathfrak{m}}$, c'est un anneau local régulier, d'après le th. 5.

Exemple.

Soit K un anneau de Dedekind, et soit $A = K[X_1, \cdots, X_n]$ un anneau de polynômes sur K; d'après un résultat (encore inédit) de S. Eilenberg, on a $\mathrm{gl.dh}(A) = n + \mathrm{gl.dh}(K) \leqq n+1$; le cor. 2 ci-dessus redonne alors un théorème de Nagata [10].

BIBLIOGRAPHIE

[1] M. Auslander, On the dimension of modules and algebras. III. Global dimension. Nagoya Math. J., **9** (1956), pp. 67–77.

[2] M. Auslander and D. A. Buchsbaum, Homological dimension in noetherian rings. Proc. Nat. Acad. Sci. USA, **42** (1956), pp. 36–38.

[3] H. Cartan and S. Eilenberg, Homological Algebra. Princeton Math. Ser., No. 19, (1956).

[4] I. S. Cohen, On the structure and ideal theory of complete local rings. Trans. Amer. Math. Soc., **59** (1946), pp. 54–106.

[5] W. Gröbner, Moderne algebraische Geometrie. Springer (1949).

[6] P. M. Grundy, A generalization of additive ideal theory. Proc. Camb. Phil. Soc., **38** (1942), pp. 241–279.

[7] J.-L. Koszul, Sur un type d'algèbres différentielles en rapport avec la transgression. Colloque de Topologie, Bruxelles (1950), pp. 73–81.

[8] W. Krull, Dimensionstheorie in Stellenringen. Journ. Crelle, **179** (1938), pp. 204–226.

[9] W. Krull, Zur Theorie der kommutativen Integritätsbereiche. Journ. Crelle, **192** (1954), pp. 230–252.

[10] M. Nagata, A general theory of algebraic geometry over Dedekind domains. Amer. J. of Math., **78** (1956), pp. 78–116.

[11] M. Nagata, The theory of multiplicity in general local rings. Ce Symposium, pp. 191–226.

[12] M. Nagata, On the chain problem of prime ideals. Nagoya Math. J., **10** (1956), pp. 51–64.

[13] D. G. Northcott, Ideal theory. Cambridge Univ. Press (1953).

[14] P. Samuel, Algèbre locale. Mém. Sci. Math., no. 123, Paris (1953).

[15] P. Samuel, Commutative algebra (Notes by D. Herzig), Cornell Univ. (1953).

[16] J.-P. Serre, Faisceaux algébriques cohérents. Ann. of Math., **61** (1955), pp. 197–278.

[17] O. Zariski, The concept of a simple point of an abstract algebraic variety. Trans. Amer. Math. Soc., **62** (1947), pp. 1–52.

The Theory of Multiplicity in General Local Rings

Masayoshi NAGATA

The notion of multiplicity in local rings was introduced by Chevalley ([1] and [2]). Though his definition was restricted only to ideals generated by systems of parameters of local rings which contain fields, Samuel ([15]) generalized the definition to primary ideals belonging to the maximal ideal of a local ring containing a field under a nice idea to make use of the Hilbert characteristic function and Samuel ([16]) defined the multiplicity also in local rings which contain no field by the same way as in [15].

The purpose of the present paper is to reconstruct the theory of multiplicity in local rings[1] and to prove some further important results as follows:

THE EXTENSION FORMULA.[2] Let $\mathfrak{o}$ be a local ring and let $\mathfrak{o}'$ be a semi-local ring which is a finite $\mathfrak{o}$-module. Assume that there exists a system of linearly independent elements $a_1=1, a_2, \cdots, a_r$ of $\mathfrak{o}'$ over $\mathfrak{o}$ such that $c\mathfrak{o}'$ is contained in the module $\sum a_i\mathfrak{o}$ with an element c of $\mathfrak{o}$ which is not a zero-divisor in $\mathfrak{o}'$. Then for any primary ideal $\mathfrak{q}$ of $\mathfrak{o}$ belonging to the maximal ideal, the relative multiplicity of $\mathfrak{q}\mathfrak{o}'$ with respect to $\mathfrak{o}$ is equal to $e(\mathfrak{q})\cdot r$ (where $e(\mathfrak{q})$ denotes the multiplicity of $\mathfrak{q}$).

THE THEOREM OF ADDITIVITY. Let $\mathfrak{o}$ be a local ring and let $\mathfrak{q}$ be a primary ideal belonging to the maximal ideal of $\mathfrak{o}$. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be all of prime divisors of zero whose co-rank are equal to rank $\mathfrak{o}$ and let $\mathfrak{q}_1, \cdots, \mathfrak{q}_n$ be primary components of zero belonging to $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ respectively. Then $e(\mathfrak{q})=\sum_i e((\mathfrak{q}+\mathfrak{q}_i)/\mathfrak{q}_i)$.

THE REDUCTION THEOREM. Let $\mathfrak{o}$ be a local ring and assume that zero ideal is primary. Let $\mathfrak{p}$ be the prime divisor of the zero ideal. Then for any primary ideal $\mathfrak{q}$ of $\mathfrak{o}$ belonging to the maximal

[1] Many of results in Samuel [15] and [16] can be generalized and can be proved in simpler way. On the other hand, the treatment in Samuel [15] and [16] contains some errors. The serious one is in the proof of our Theorem 1 (in § 5). Though it was corrected in Nagata [9], the proofs were sketchy and we want to prove it again in detail.

[2] This is a slight generalization of an assertion in Samuel [16].

ideal, the multiplicity $e(\mathfrak{q})$ of $\mathfrak{q}$ is equal to $e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})\cdot\text{length } \mathfrak{o}_{\mathfrak{p}}$.

A CHARACTERIZATION OF REGULAR LOCAL RINGS.[3] A local ring is regular if and only if it is of multiplicity one and unmixed.[4]

THE EXISTENCE THEOREM OF DISTINCT SYSTEM OF PARAMETERS. A local ring $\mathfrak{o}$ has a distinct system of parameters if and only if the unmixedness theorem holds in $\mathfrak{o}$ (and in this case, any system of parameters of $\mathfrak{o}$ is distinct.[4])

THE MULTIPLICITY OF RINGS OF QUOTIENTS. Let $\mathfrak{p}$ be a prime ideal of a local ring $\mathfrak{o}$. If $\text{rank } \mathfrak{p}+\text{co-rank } \mathfrak{p}=\text{rank } \mathfrak{o}$ and if $\mathfrak{p}$ is analytically unramified, then the multiplicity of $\mathfrak{o}_{\mathfrak{p}}$ is not greater than that of $\mathfrak{o}$.

Though our treatment will include the case of local rings which contain no field, many of our treatment are simpler than the already known treatment. In particular, the proof of the *theorem of transition* (originally proved by Chevalley ([2]) and generalized a little by Samuel ([15]) (only for geometric local rings in the sense of Chevalley [2]) and ours is a generalization for arbitrary local rings) is essentially simpler than those given by Chevalley ([2]) and Samuel ([15]) (or [16]).[5] Though the proof of the *associativity formula* (originally proved by Chevalley ([2]) for geometric local rings and ours is a generalization for arbitrary local rings) is simpler than that was given by Chevalley ([2]) (or Samuel ([16]) if we restrict only to geometric local rings (in a generalized sense due to Nagata ([9])), the general case is not so simple and the essential difficulty lies in absence of subfields.

Since we need to make use of some basic results on general (Noetherian) local rings, we shall list them in § 1. We shall observe the Hilbert characteristic function in § 2 and define the notion of form rings in § 3. Then we shall define the notion of multiplicity in § 4 and observe some elementary properties of the notion in § 5. In § 6, we shall prove the extension formula and the theorem of additivity. In § 7, we shall prove the existence theorem of distinct system of parameters, which generalizes not only the original unmixedness theorem (in polynominal rings) due to Lasker-Macaulay but also its generalization to regular local rings due to Cohen ([3]). In § 8, we shall prove the characterization of regular local rings (stated above). We shall prove in § 9 the theorem of transition. In

[3] The case when $\mathfrak{o}$ contains a field, the proof is easy and it well known (see Samuel [15]).

[4] For the definitions, see § 7.

[5] Our simplification was given in essential by Nagata [9].

§ 10, we shall prove the associativity formula only for complete local integrity domains and applying it to complete unramified regular local rings, we shall prove the reduction theorem in § 11. Then using the redution theorem, we shall prove the general case of the associativity formula in § 12. In § 13, we shall prove the assertion on the multiplicity of rings of quotients. In § 14, we shall concern the complete tensor products of local rings. In appendix, we shall give a proof of the well known result that a polynomial $f(x)$ in one indeterminate x with coefficients in the field of rational numbers is a linear combination of binomial coefficients with integer coefficients if there exists one integer N such that for any integer n greater than N, $f(n)$ is an integer and this results shows that the multiplicity and the relative multiplicity are natural numbers.

The writer wants to express here his hearty thanks to Mr. H. Matsumura for a critical reading of the manuscript of the present paper.

TERMINOLOGY: We will mean under a ring a commutative ring with identity, under a local ring a Noetherian local ring and under a semi-local ring a Noetherian semi-local ring. Further, we say that a local ring $\mathfrak{o}$ dominates another local ring $\mathfrak{o}'$ if 1) $\mathfrak{o}$ contains $\mathfrak{o}'$ and 2) the maximal ideal of $\mathfrak{o}$ lies over that of $\mathfrak{o}'$ (see Nagata [11, I]). The terminology used in Nagata [10] (normal rings, derived normal rings, rank (of ideals or of rings), co-rank (of ideals), integral extensions, almost finite integral extensions, the J-radical, the rings of quotients and so on) will be used in the same sense. Basic terminology on local rings (completions, system of parameters, regular system of parameters, regular local rings, analytical unramifiedness and so on) will be used in the usual sense. But, according to the definition in Nagata [10], the dimension of a local ring in the usual sense will be called the rank and the dimension of an ideal in the usual sense will be called the co-rank. (The equi-dimensional local ring in the sense of Chevalley [2] will be called an unmixed local ring.)

NOTATIONS: When $\mathfrak{o}$ is a ring and when $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$ or a multiplicatively closed subset of $\mathfrak{o}$ which does not contain zero, the symbol $\mathfrak{o}_{\mathfrak{p}}$ will denote the ring of quotients of $\mathfrak{o}$ with respect to $\mathfrak{p}$ (see [10]). When $\mathfrak{o}$ is a ring and when x is a transcendental element over $\mathfrak{o}$, we will denote by $\mathfrak{o}(x)$ the ring $\mathfrak{o}[x]_S$, where S is the intersection of complementary sets of ideals of $\mathfrak{o}[x]$ generated by maximal ideals of $\mathfrak{o}$ (if $\mathfrak{o}$ is a local ring with maximal ideal $\mathfrak{m}$, then $\mathfrak{o}(x)=\mathfrak{o}[x]_{\mathfrak{m}\mathfrak{o}[x]}$) (see [11, I]). The symbol $\binom{n}{r}$ will denote the usual binomial cofficients.

When $\mathfrak{o}$ is a subring of another ring $\mathfrak{o}'$, the symbol $[\mathfrak{o}' : \mathfrak{o}]$ will denote the number of maximally linearly independent elements of $\mathfrak{o}'$ over $\mathfrak{o}$ (when it is well defined).

RESULTS ASSUMED TO BE KNOWN:

(1) On the theory of general rings; the results stated in Nagata [10] will be used freely.

(2) Basic notions and results on polynomial rings, especially on homogeneous ideals, will be used freely.

(3) On the general theory of local rings; many of well known results will be used freely and they will be listed in § 1.

§ 1. Well known results on the general theory of local rings.

LEMMA 1.1. *If $\mathfrak{o}$ is a local ring with maximal ideal $\mathfrak{m}$, then the completion $\mathfrak{o}^*$ of $\mathfrak{o}$ is a local ring with maximal ideal $\mathfrak{m}\mathfrak{o}^*$. Further,* rank $\mathfrak{o}$=rank $\mathfrak{o}^*$. *If $\mathfrak{a}$ is an ideal of $\mathfrak{o}$, then $\mathfrak{a}\mathfrak{o}^* \cap \mathfrak{o} = \mathfrak{a}$ and $\mathfrak{o}^*/\mathfrak{a}\mathfrak{o}^*$ is the completion of $\mathfrak{o}/\mathfrak{a}$.* (Krull [5])

For the proof, see Chevalley [1] or Cohen [3] or Krull [5] or Nagata [9] or Samuel [16]. (The equality that rank $\mathfrak{o}$=rank $\mathfrak{o}^*$ follows from our treatment in § 3.)

LEMMA 1.2. *Let $\mathfrak{a}$ be an ideal of a semi-local ring $\mathfrak{o}$ and let $\mathfrak{o}^*$ be the completion of $\mathfrak{o}$. If b is an element of $\mathfrak{o}$, then $\mathfrak{a}\mathfrak{o}^* : b\mathfrak{o}^* = (\mathfrak{a} : b\mathfrak{o})\mathfrak{o}^*$.* (Zariski [17])

For the proof, see Nagata [7] or [9] or Samuel [16] or Zariski [17].

COROLLARY. *If an element a of $\mathfrak{o}$ is not a zero-divisor in $\mathfrak{o}$, then a is not a zero-divisor in $\mathfrak{o}^*$.* (Chevalley [1])

LEMMA 1.3. *Let $\mathfrak{o}$ be a complete semi-local ring with J-radical $\mathfrak{m}$. If $\mathfrak{a}_i$'s are ideals of $\mathfrak{o}$ such that $\mathfrak{a}_{i+1} \subseteqq \mathfrak{a}_i$ for any i and that $\bigcap_i \mathfrak{a}_i = 0$, then there exists an integer $n(k)$ for any given integer k (>0) such that $\mathfrak{a}_{n(k)} \subseteqq \mathfrak{m}^k$.* (Chevalley [1])

For the poof, see Chevalley [1] or Cohen [3] or Nagata [9] or Samuel [16].

COROLLARY. *Let $\mathfrak{o}$ be a semi-local ring with J-radical $\mathfrak{m}$ and let c be an element of $\mathfrak{o}$ which is not a zero-divisor. Then there exists an integer $n(k)$ for any given integer k such that $\mathfrak{m}^{n(k)} : c\mathfrak{o} \subseteqq \mathfrak{m}^k$.* (Chevalley [1])

LEMMA 1.4. *Let $\mathfrak{o}^*$ be the completion of a semi-local ring $\mathfrak{o}$ and let $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ be ideals of $\mathfrak{o}$. Then $(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n)\mathfrak{o}^* = \mathfrak{a}_1\mathfrak{o}^* \cap \cdots \cap \mathfrak{a}_n\mathfrak{o}^*$.* (Nagata [8])

For the proof, see Nagata [8] or [9].

LEMMA 1.5. *Let $\mathfrak{o}$ be a complete local ring with maximal ideal*

$\mathfrak{m}$ *and let* $\mathfrak{o}'$ *be a local ring which dominates* $\mathfrak{o}$. *If* $\mathfrak{o}'/\mathfrak{m}\mathfrak{o}'$ *is a finite* $\mathfrak{o}/\mathfrak{m}$*-module, then* $\mathfrak{o}'$ *is a finite* $\mathfrak{o}$*-module,* $\mathfrak{o}'$ *is a complete local ring and* $\mathfrak{o}$ *is a subspace of* $\mathfrak{o}'$. (Chevalley [1])

For the proof, see Chevalley [1] or Choen [3] or Nagata [9] or Samuel [16].

LEMMA 1.6. *If* $\mathfrak{o}'$ *is a finite integral extension of a semi-local integrity domain* $\mathfrak{o}$, *then* $\mathfrak{o}$ *is a subspace of* $\mathfrak{o}'$. (Chevalley [1])

For the proof, see Chevalley [1] or Nagata [9] or Samuel [16].

LEMMA 1.7. *A complete local ring* $\mathfrak{o}$ *has a coefficient ring* I (*that is,* I *is dominated by* $\mathfrak{o}$ *and is a homomorphic image of a discrete valuation ring whose maximal ideal is generated by the characteristic of the residue class field of* $\mathfrak{o}$ *and, furthermore, the residue class field of* $\mathfrak{o}$ *coincides with that of* I). (Cohen [3])

For the proof, see Cohen [3] or Samuel [16].[6)]

LEMMA 1.8. *If* $\mathfrak{o}$ *is a complete local integrity domain, then any integral extension of* $\mathfrak{o}$ *has only one maximal ideal.* (Cohen [3])

For the proof, see Cohen [3] or Nagata [7].

LEMMA 1.9. *If* $\mathfrak{o}$ *is a complete local integrity domain, then any almost finite integral extension of* $\mathfrak{o}$ *is a finite* $\mathfrak{o}$*-module* (*hence it is a complete local integrity domain*). (Nagata [8, II])

For the proof, see Nagata [8, II] or [11, II].

LEMMA 1.10. *If* $\mathfrak{o}$ *is a regular local ring then the completion of* $\mathfrak{o}$ *is also regular and conversely.* (Krull [5])

For the proof, see Cohen [3] or Krull [5] or Nagata [9].

LEMMA 1.11. *Let* $\mathfrak{o}$ *be a local ring and let* x *be a transcendental element over* $\mathfrak{o}$. *Then* $\mathfrak{o}$ *is regular if and only if* $\mathfrak{o}(x)$ *is regular.* (Nagata [11, II]) (cf. Cohen [3])

The proof is easy.

LEMMA 1.12. *Let* $\mathfrak{o}$ *be a regular local ring and let* $\mathfrak{a}$ *be an ideal of* $\mathfrak{o}$. *Then* $\mathfrak{o}/\mathfrak{a}$ *is regular if and only if* $\mathfrak{a}$ *is generated by a subset of a regular system of parameters of* $\mathfrak{o}$. (Chevalley [1] and Cohen [3])

For the proof, see Chevalley [1] or Cohen [3] or Nagata [9].

LEMMA 1.13. *A regular local ring is a normal ring.* (Krull [5])

For the proof, see Krull [5] or Nagata [9] or Samuel [16].

LEMMA 1.14. *An unramified regular local ring is a unique factorization ring, that is, any element is expressible uniquely as the product of irreducible elements* (*prime elements*) *up to units.* (Y. Mori)

[6)] It was communicated to the writer that Mr. Narita gave a much simpler proof of the assertion and that his proof will appear in the journal "Sûgaku". On the other hand, the proof of this assertion in Nagata [7] is a little simpler than Cohen's only for the case when the residue class field is perfect or the case when $\mathfrak{o}$ contains a field and is not correct in the general case.

For the proof, see Krull [6] or Nagata [9] or [11, II]. We shall make use of only the assertion in the complete case and the proof of the case was given by Cohen [3]; see Cohen [3] or Samuel [16].

LEMMA 1.15. *Let $\mathfrak{o}$ be a local ring and let $\mathfrak{a}$ be an ideal of $\mathfrak{o}$ generated by r elements and whose rank is r. If $\mathfrak{o}/\mathfrak{a}$ is a regular local ring, then $\mathfrak{o}$ is a regular local ring.*

The proof is immediate from the definition of regular local rings.

LEMMA 1.16. *If $\mathfrak{o}$ is a complete local integrity domain and if $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$ of rank 1, then* co-rank $\mathfrak{p}=$ rank $\mathfrak{o}-1$. (Cohen [3])

For the proof, see Cohen [3] or Nagata [9].

COROLLARY. *If $\mathfrak{o}$ is a complete local integrity domain, then the length of any maximal chain of prime ideals of $\mathfrak{o}$ is equal to* rank $\mathfrak{o}$. (Cohen [3])

LEMMA 1.17. *Let $\mathfrak{o}^*$ be the completion of a normal local ring $\mathfrak{o}$ and let a ($a\neq 0$, $a\mathfrak{o}\neq\mathfrak{o}$) be an element of $\mathfrak{o}$. If any prime divisor of $a\mathfrak{o}$ is analytically unramified, then $\mathfrak{o}^*$ contains no nilpotent element other than zero,* i.e., *$\mathfrak{o}$ is analytically unramified. Further, in this case, any prime divisor of zero of $\mathfrak{o}^*$ is contained properly in a prime divisor of $\mathfrak{p}\mathfrak{o}^*$ with a suitable prime divisor $\mathfrak{p}$ of $a\mathfrak{o}$.* (Zariski [17])

For the proof, see Nagata [8] or [9] or [11, I] or Zariski [17].

LEMMA 1.18. *If $\mathfrak{o}$ is a complete regular local ring and if $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$, then $\mathfrak{o}_{\mathfrak{p}}$ is a regular local ring.* (Nagata [11, II])

For the proof, see Nagata [11, II]. We shall make use of only the case when $\mathfrak{o}$ is unramified and the case was proved by Cohen [3].

LEMMA 1.19. *Let $\mathfrak{p}$ be a prime ideal of a regular local ring $\mathfrak{o}$ with maximal ideal $\mathfrak{m}$. If an element f of $\mathfrak{o}$ is not in $\mathfrak{m}^n$, then f is not in $\mathfrak{p}^n\mathfrak{o}_{\mathfrak{p}}$.* (Nagata [11, II])

For the proof, see Nagata [11, II].

LEMMA 1.20. *If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of rank r and s respectively in an unramified regular local ring, then $\mathfrak{a}+\mathfrak{b}$ is at most of rank $r+s$.* (Nagata [11, V])

For the proof, see Nagata [11, V]; when the ring contains a field, then considering the completion, the assertion is reduced to the complete case and the case was proved by Chevalley [2] and the other case can be proved similarly.

§ 2. The Hilbert characteristic function.

A ring $\mathfrak{o}$ is called a *primary ring* if it is a local ring whose non-units are nilpotent. Then a (Noetherian) ring satisfies the minimum condition for ideals if and only if it is the direct sum of a finite number of primary rings. On the other hand, let M be a module over a ring $\mathfrak{o}$. Assume that M has a composition series (as an $\mathfrak{o}$-module). Then the length of the composition series is called the *length* of M (over $\mathfrak{o}$) and will be denoted by $l(M; \mathfrak{o})$ or merely by $l(M)$; observe that the length is well defined independently on the choice of composition series by virtue of the Jordan-Hoelder-Schreier theorem. Observe further that if M is a finite module over a ring $\mathfrak{o}$ which satisfies the minimum condition for ideals, then $l(M)$ is defined.

LEMMA 2.1. *Assume that a primary ring A dominates another primary ring A' and that the residue class field K of A is a finite algebraic extension of the residue class field K' of A'. Then for any finite module M over A, we have $l(M; A') = [\mathrm{K} : K'] \cdot l(M; A)$.*

PROOF. Let $M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$ be a composition series of M as an A-module ($n = l(M; A)$). Then each M_{i-1}/M_i ($i = 1, 2, \cdots, n$) is an irreducible K-module and therefore $l(M_{i-1}/M_i; K') = [K : K']$. Thus we see that M has a composition series of length $n \cdot [K : K']$ as an A'-module and the assertion is proved.

LEMMA 2.2. *If a ring A is the direct sum of primary rings $A_1, \cdots, A_r$, then $l(A)$ is the sum of all $l(A_i)$.*

The proof is easy and we omit it.

REMARK 1. Similar assertion as above for direct sums of modules holds good obviously.

We shall denote hereafter by A a primary ring, by F the ring of polynomials over A in indeterminates $X_1, \cdots, X_s$, by $\mathfrak{a}$ a homogeneous ideal of F, by $F(n)$ the A-module of homogeneous forms of degree n in F, by $\mathfrak{a}(n)$ the module $\mathfrak{a} \frown F(n)$ and by $\chi(\mathfrak{a}; n)$ the length of the A-module $F(n)/\mathfrak{a}(n)$. This $\chi(\mathfrak{a}; n)$ is called the *Hilbert characteristic function* of $\mathfrak{a}$. We will remark here that $l(F(n)) = \binom{n+s-1}{s-1} \cdot l(A)$, because the number of monomial of degree n is equal to $\binom{n+s-1}{s-1}$.

LEMMA 2.3. *If $\mathfrak{a}$ and $\mathfrak{b}$ are homogeneous ideals of F, then*

$$\chi(\mathfrak{a} + \mathfrak{b}; n) = \chi(\mathfrak{a}; n) + \chi(\mathfrak{b}; n) - \chi(\mathfrak{a} \frown \mathfrak{b}; n).$$

PROOF. We have obviously $(\mathfrak{a}(n) + \mathfrak{b}(n))/\mathfrak{a}(n) = \mathfrak{b}(n)/(\mathfrak{a}(n) \frown \mathfrak{b}(n))$ and $\chi(\mathfrak{a}; n) - \chi(\mathfrak{a} + \mathfrak{b}; n) = \chi(\mathfrak{a} \frown \mathfrak{b}; n) - \chi(\mathfrak{b}; n)$, which proves our assertion.

LEMMA 2.4. *If f is a homogeneous form of degree d such that $\mathfrak{a} : fF = \mathfrak{a}$, then $\chi(\mathfrak{a} + fF; n) = \chi(\mathfrak{a}; n) - \chi(\mathfrak{a}; n-d)$ for any $n \geqq d$.*

PROOF. If g is an element of $F(n-d)$ such that $fg \in \mathfrak{a}(n)$, then $g \in \mathfrak{a}$ because $\mathfrak{a} : fF = \mathfrak{a}$, hence $g \in \mathfrak{a}(n-d)$, which shows that $\mathfrak{a}(n) \frown$

$f \cdot F(n-d) = f \cdot \mathfrak{a}(n-d)$. Obviously $\mathfrak{a}(n) + f \cdot F(n-d) = (\mathfrak{a} + fF)(n)$ and $(\mathfrak{a} + fF)(n)/\mathfrak{a}(n) = f \cdot F(n-d)/(f \cdot F(n-d) \frown \mathfrak{a}(n)) = f \cdot F(n-d)/f \cdot \mathfrak{a}(n-d)$. Since f is not a zero-divisor in F,[7] the mapping ϕ from $F(n-d)$ into $F(n)$ such that $\phi(h) = fh$ is an isomorphism and we have $l((\mathfrak{a}+fF)(n)/\mathfrak{a}(n)) = l(f \cdot F(n-d)/f \cdot \mathfrak{a}(n-d)) = l(F(n-d)/\mathfrak{a}(n-d))$. Thus we have $\chi(\mathfrak{a}; n) - \chi(\mathfrak{a}+fF; n) = \chi(\mathfrak{a}; n-d)$, which proves our assertion.

We say that $\mathfrak{a}$ is *irrelevant* if co-rank $\mathfrak{a} = 0$.

PROPOSITION 1. *$\chi(\mathfrak{a}; n)$ is a polynomial in n for sufficiently large n.* (Hilbert [4] and Samuel [15])

PROOF. When $\mathfrak{a}$ is irrelevant, $\mathfrak{a}$ contains $F(n)$ for sufficiently large n and $\chi(\mathfrak{a}; n) = 0$ for such n. This shows the validity of the assertion for irrelevant ideals, in particular for the irrelevant prime ideal. Therefore we will prove the assertion by induction on the largeness of $\mathfrak{a}$. If there exist homogeneous ideals $\mathfrak{b}$ and $\mathfrak{c}$ which contain properly $\mathfrak{a}$ such that $\mathfrak{a} = \mathfrak{b} \frown \mathfrak{c}$, then we see the assertion by our induction assumption and by Lemma 2.3. If there exists no such ideal, then $\mathfrak{a}$ is a primary ideal. By the above observation, we may assume that co-rank $\mathfrak{a} \geqq 1$. Then there exists a homogeneous form f of degree 1 such that $\mathfrak{a} : fF = \mathfrak{a}$. By Lemma 2.4, $\chi(\mathfrak{a}; n) = \sum_1^n \chi(\mathfrak{a}+fF; i) + \chi(\mathfrak{a}; 0)$ and we see the assertion also in this case.

REMARK 2. As we have known, if $\mathfrak{a}$ is of co-rank zero, then $\chi(\mathfrak{a}; n) = 0$ for sufficiently large n. If $\mathfrak{a}$ is of co-rank r $(r > 0)$, then we shall see that $\chi(\mathfrak{a}; n)$ is a polynomial of degree $r-1$ (for sufficiently large n). A proof will be given in § 3.

LEMMA 2.5. *Let $\mathfrak{b}$ be a homogeneous ideal which coincides with $\mathfrak{a}$ up to irrelevant primary components. Then $\chi(\mathfrak{a}; n) = \chi(\mathfrak{b}; n)$ for sufficiently large n.* (Samuel [15])

PROOF. By our assumption, there are irrelevant ideals $\mathfrak{q}$ and $\mathfrak{q}'$ such that $\mathfrak{q} \frown \mathfrak{a} = \mathfrak{q}' \frown \mathfrak{b}$. Let N be an integer such that $F(N)$ is contained in $\mathfrak{q} \frown \mathfrak{q}'$. Then for any n which is not less than N, we have $\mathfrak{a}(n) = \mathfrak{b}(n)$ and the assertion is proved.

A homogeneous element f of degree 1 is called a *superficial* element with respect to $\mathfrak{a}$ if $\chi(\mathfrak{a}; n) = \chi(\mathfrak{a} : fF; n)$ for sufficiently large n.

LEMMA 2.6. *Assume that the residue class field K of A contains infinitely many elements and that* co-rank $\mathfrak{a}$ *is different from zero. Then there exists a superficial element f with respect to $\mathfrak{a}$. In this case, if a finite number of proper submodules $M_1, \cdots, M_t$ of $F(1)$*

[7] Let $\mathfrak{p}$ be the maximal ideal of A. Then any element of F which is not in $\mathfrak{p}F$ is not a zero-divisor. From the assumption that $\mathfrak{a}{:}fF = \mathfrak{a}$, we see that f is not in any prime divisor of $\mathfrak{a}$. Since $\mathfrak{p}F$ is nilpotent, $\mathfrak{p}F$ is contained in every prime divisor of $\mathfrak{a}$, hence f is not in $\mathfrak{p}F$ and f is not a zero-divisor.

are given, then we can choose f outside of any of M_i's. (Samuel [15])

PROOF. Let $\mathfrak{p}_1,\cdots,\mathfrak{p}_u$ be all the prime divisors of $\mathfrak{a}$ different from the irrelevant prime ideal and set $M_{t+i}=\mathfrak{p}_i(1)$ for each i. Let $\mathfrak{m}$ be the maximal ideal of A. Then $M_i+\mathfrak{m}F(1)\neq F(1)$ for any $i=1,\cdots,t+u$ because $\mathfrak{m}$ is the J-radical of A (see [10, §6]). Set $V_i=(M_i+\mathfrak{m}F(1))/\mathfrak{m}F(1)$ for each i. Then $V_i\neq F(1)/\mathfrak{m}F(1)$. Since K contains infinitely many elements and since V_i's are proper subspace of $F(1)/\mathfrak{m}F(1)$, there exists an element f' of $F(1)/\mathfrak{m}F(1)$ which is not in any of V_i's. Let f be an element of $F(1)$ whose residue class modulo $\mathfrak{m}F(1)$ is f'. Then f is not in any of M_i's; in particular f is not in any of $\mathfrak{p}_j$'s. Therefore $\mathfrak{a}$ and $\mathfrak{a}:fF$ coincide with each other up to irrelevant primary components. Thus f is a superficial element by Lemma 2.5.

REMARK 3. If $\mathfrak{a}$ is a primary ideal, then it is superfluous to assume that K contains infinitely many elements only for the existence of superficial element. But, in the general case, the assumption is essential as is easily seen.

§ 3. Form rings of a local ring.

Let $\mathfrak{o}$ be a local ring with maximal ideal $\mathfrak{m}$ and let $\mathfrak{q}$ be a primary ideal belonging to $\mathfrak{m}$. Then $A=\mathfrak{o}/\mathfrak{q}$ is a primary ring. The module $\mathfrak{q}^n/\mathfrak{q}^{n+1}(\mathfrak{q}^0=\mathfrak{o})$ can be regarded as an A-module and is called the $\mathfrak{q}$-*form* of $\mathfrak{o}$ of degree n; this will be denoted by $F(\mathfrak{q};n)$. The direct sum $F(\mathfrak{q})$ of all $F(\mathfrak{q};n)$ is called the *form ring* of $\mathfrak{o}$ with respect to $\mathfrak{q}$. Let $x_1,\cdots,x_s$ be a base of $\mathfrak{q}$ and let $x'_1,\cdots,x'_s$ be the classes of them in $F(\mathfrak{q};1)$. For any elements $a'\in F(\mathfrak{q};i)$ and $b'\in F(\mathfrak{q};j)$, take representatives a and b of them in $\mathfrak{o}$ and define $a'b'$ to be the class of ab in $F(\mathfrak{q};i+j)$. By this definition of multiplication, $F(\mathfrak{q})$ becomes a ring and is generated by $x'_1,\cdots,x'_s$ over A. Therefore there exists a uniquely determined homomorphism ϕ from the ring $F=A[X_1,\cdots,X_s]$ onto $F(\mathfrak{q})$ which maps X_i to x_i. As is easily seen, the kernel $\mathfrak{a}$ of ϕ is a homogeneous ideal of F. Therefore the Hilbert characteristic function $\chi(\mathfrak{a};n)$ is defined. Then $\chi(\mathfrak{a};n)=l(F(\mathfrak{q};n))$. Since $l(\mathfrak{o}/\mathfrak{q}^n)=\sum_0^{n-1}l(F(\mathfrak{q};i))$, we see immediately from Proposition 1 the following

PROPOSITION 2. *$l(\mathfrak{o}/\mathfrak{q}^n)$ is a polynomial in n for sufficiently large n.* (Samuel [15])

This polynomial will be denoted by $\sigma(\mathfrak{q};n)$.

REMARK 1. Let $\mathfrak{o}^*$ be the completion of $\mathfrak{o}$ and set $\mathfrak{q}^*=\mathfrak{q}\mathfrak{o}^*$. Then $\mathfrak{o}^*/\mathfrak{q}^{*n}=\mathfrak{o}/\mathfrak{q}^n$ for any n. Therefore the form ring of $\mathfrak{o}$ with respect to $\mathfrak{q}$ is also that of $\mathfrak{o}^*$ with respect to $\mathfrak{q}^*$. By the same reason, we see that $\sigma(\mathfrak{q};n)=\sigma(\mathfrak{q}^*;n)$.

REMARK 2. As will be shown in appendix and as is well known, $\sigma(\mathfrak{q}; n)$ is a linear combination of binomial coefficients with integer coefficients.

Let a be an element of $\mathfrak{o}$. Then there corresponds a unique element a' of the form ring $F(\mathfrak{q})$ as follows: 1) if $a=0$, then $a'=0$ and 2) if $a\neq 0$, then a' is the class of a in $F(\mathfrak{q}; n)$, where n is the integer such that $a \in \mathfrak{q}^n$ and $a \notin \mathfrak{q}^{n+1}$. This a' is called the $\mathfrak{q}$-*form* of a and n is called the *degree* of a with respect to $\mathfrak{q}$ (when $a=0$, we regard that the degree is infinite). Observe that a' may be regarded as a homogeneous form of degree n in $x'_1, \cdots, x'_s$. Therefore there exists a homogeneous form f in F whose residue class modulo $\mathfrak{a}$ is a'. Such f is called a *form* in F which corresponds to a.

On the other hand, an element a of $\mathfrak{q}$ is called a *superficial* element of $\mathfrak{q}$ if there exists an integer c such that $(\mathfrak{q}^n : a\mathfrak{o})\frown\mathfrak{q}^c = \mathfrak{q}^{n-1}$ for any n greater than c. Then we have

PROPOSITION 3. *An element a of $\mathfrak{q}$ is a superficial element of $\mathfrak{q}$ if and only if a corresponds to a superficial element in F with respect to the homogeneous ideal $\mathfrak{a}$.*

PROOF. Assume that a corresponds to a superficial element f with respect to $\mathfrak{a}$ and let c be an integer such that $\chi(\mathfrak{a}; n)=\chi(\mathfrak{a} : fF; n)$ for any $n \geqq c$. Obviously $(\mathfrak{q}^n : a\mathfrak{o})\frown\mathfrak{q}^c$ $(n>c)$ contains $\mathfrak{q}^{n-1}$ because a is in $\mathfrak{q}$. Let b be any element of $(\mathfrak{q}^n : a\mathfrak{o})\frown\mathfrak{q}^c$. Then $ab \in \mathfrak{q}^n$. Let g be a form in F which corresponds to b. If g is of degree not less than $n-1$, we have b is in $\mathfrak{q}^{n-1}$. We will assume the contrary. Then $\deg (fg) \leqq n-1$ and therefore fg is in $\mathfrak{a}$ (because ab is in $\mathfrak{q}^n$), hence g is in $\mathfrak{a} : fF$. Since $\chi(\mathfrak{a}; m)=\chi(\mathfrak{a} : fF; m)$ for any $m \geqq c$ and since the degree of g is not less than c, we have g is in $\mathfrak{a}$, which is a contradiction to the definition of corresponding forms. Thus b is in $\mathfrak{q}^{n-1}$ and we have $(\mathfrak{q}^n : a\mathfrak{o})\frown\mathfrak{q}^c=\mathfrak{q}^{n-1}$ $(n>c)$, which shows that a is a superficial element of $\mathfrak{q}$. Conversely assume that a is a superficial element of $\mathfrak{q}$, that is, there exists an integer c such that $(\mathfrak{q}^n : a\mathfrak{o})\frown\mathfrak{q}^c=\mathfrak{q}^{n-1}$ for any $n>c$. Let f be a form in F which corresponds to a. We have only to show that $\mathfrak{a}(n)=(\mathfrak{a} : fF)(n)$ for any $n>c$. Let g be an element of $(\mathfrak{a} : fF)(n)$ and assume that $g \notin \mathfrak{a}$. Then there exists an element b of $\mathfrak{o}$ such that g is a form which corresponds to b. Then ab is in $\mathfrak{q}^{n+2}$ because fg is of degree $n+1$ and is in $\mathfrak{a}$. This shows that $(\mathfrak{q}^{n+2} : a\mathfrak{o})\frown\mathfrak{q}^c$ contains b which is not in $\mathfrak{q}^{n+1}$, which is a contradiction. Thus we have $g \in \mathfrak{a}$ (hence $g \in \mathfrak{a}(n)$), i.e., $(\mathfrak{a} : fF)(n)$ is contained in $\mathfrak{a}(n)$. Since the converse inclusion is obvious, we have the required result.

COROLLARY. *If the residue class field K of $\mathfrak{o}$ contains infinitely* *many elements and if* $b_1, \cdots, b_t$ *are ideals of* $\mathfrak{o}$ *which do not contain* $\mathfrak{q}$, *then there exists a superficial element* a *of* $\mathfrak{q}$ *which is not in any of* $\mathfrak{b}_i$*'s.* (Samuel [15])

PROOF. Let M_i be the module $F(\mathfrak{q}; 1)\frown((\mathfrak{q}^2+\mathfrak{b}_i)/\mathfrak{q}^2)$. If $M_i=F(\mathfrak{q}; 1)$, then $\mathfrak{q}^2+\mathfrak{b}_i \supseteqq \mathfrak{q}$, hence $\mathfrak{q}^2 \subseteqq \mathfrak{q}^3+\mathfrak{b}_i$. Therefore $\mathfrak{q} \subseteqq \mathfrak{q}^3+\mathfrak{b}_i$. Similarly we have $\mathfrak{q} \subseteqq \mathfrak{q}^n+\mathfrak{b}_i$ for any n. Thus we have $\mathfrak{q} \subseteqq \bigcap_n(\mathfrak{q}^n+\mathfrak{b}_i)=\mathfrak{b}_i$ and is a contradiction. Therefore we have $M_i \neq F(\mathfrak{q}; 1)$ and we can apply Lemma 2.6. Thus the assertion is proved.

LEMMA 3.1. *If* a *is a superficial element of* $\mathfrak{q}$ *and if* a *is not a zero-divisor, then* $\mathfrak{q}^n : a\mathfrak{o}=\mathfrak{q}^{n-1}$ *for sufficiently large* n. (Samuel [15])

PROOF. There exists an integer n such that $\mathfrak{q}^n : a\mathfrak{o} \subseteqq \mathfrak{q}^c$ for any given integer c (see § 1) and our assertion is proved.

PROPOSITION 4. *Let* x *be an element of* $\mathfrak{o}$. *Then we have*

$$l(\mathfrak{o}/(\mathfrak{q}^n+x\mathfrak{o}))=l(\mathfrak{o}/\mathfrak{q}^n)-l(\mathfrak{o}/(\mathfrak{q}^n : x\mathfrak{o})). \quad \text{(Samuel [15])}$$

PROOF. Obviously $l(\mathfrak{o}/\mathfrak{q}^n)=l(\mathfrak{o}/(\mathfrak{q}^n+x\mathfrak{o}))+l((\mathfrak{q}^n+x\mathfrak{o})/\mathfrak{q}^n)$ and $(\mathfrak{q}^n+x\mathfrak{o})/\mathfrak{q}^n =x\mathfrak{o}/(\mathfrak{q}^n \frown x\mathfrak{o})$. Let ϕ be the homomorphism from $\mathfrak{o}$ onto $x\mathfrak{o}$ such that $\phi(a)=xa$. Then $\mathfrak{o}=\phi^{-1}(x\mathfrak{o})$ and $\mathfrak{q}^n : x\mathfrak{o}=\phi^{-1}(\mathfrak{q}^n \frown x\mathfrak{o})$. Therefore we have $l(\mathfrak{o}/(\mathfrak{q}^n : x\mathfrak{o}))=l(x\mathfrak{o}/(\mathfrak{q}^n \frown x\mathfrak{o}))=l((\mathfrak{q}^n+x\mathfrak{o})/\mathfrak{q}^n)$. Thus the proof is completed.

COROLLARY 1. *Set* $\mathfrak{q}'=(\mathfrak{q}+x\mathfrak{o})/x\mathfrak{o}$. *Then we have* $\sigma(\mathfrak{q}'; n)=\sigma(\mathfrak{q}; n) -l(\mathfrak{o}/(\mathfrak{q}^n : x\mathfrak{o}))$ *for sufficiently large* n.

COROLLARY 2. *If* x *is a superficial element of* $\mathfrak{q}$, *then there exists an integer* C *such that* $\sigma(\mathfrak{q}; n)-\sigma(\mathfrak{q}; n-1) \leqq \sigma(\mathfrak{q}', n) \leqq \sigma(\mathfrak{q}; n)-\sigma(\mathfrak{q}; n-1)+C$. (Samuel [15])

PROOF. Let c be an integer such that $(\mathfrak{q}^n : x\mathfrak{o})\frown\mathfrak{q}^c=\mathfrak{q}^{n-1}$ for any $n>c$. Then setting $C=l(\mathfrak{o}/\mathfrak{q}^c)$, we have the inequality.

COROLLARY 3. *If furthermore* x *is not a zero-divisor, then we have* $\sigma(\mathfrak{q}; n)-\sigma(\mathfrak{q}; n-1)=\sigma(\mathfrak{q}'; n)$.

PROOF. This follows from Lemma 3.1 and Proposition 4.

REMARK 3. The degree of $\sigma(\mathfrak{q}; n)$ coincides with the rank of $\mathfrak{o}$. (Samuel [16])

PROOF. We first prove the assertion under the assumption that the residue class field K contains infinitely many elements. When rank $\mathfrak{o}=0$, the assertion is obvious and we will prove the assertion by induction on the rank of $\mathfrak{o}$. Let x be a superficial element of $\mathfrak{q}$; we can choose x so that x is not in any prime ideal whose co-rank is equal to rank $\mathfrak{o}$. Then rank $\mathfrak{o}/x\mathfrak{o}=$ rank $\mathfrak{o}-1$. By the above Corollary 2, $\sigma(\mathfrak{q}/x\mathfrak{o}; n)$ coincides with $\sigma(\mathfrak{q}; n)-\sigma(\mathfrak{q}; n-1)$ up to constant terms and therefore $\deg(\sigma(\mathfrak{q}/x\mathfrak{o}; n))=\deg(\sigma(\mathfrak{q}; n))-1$. By our induction assumption, $\deg(\sigma(\mathfrak{q}/x\mathfrak{o}; n))=$ rank $\mathfrak{o}/x\mathfrak{o}=$ rank $\mathfrak{o}-1$, which shows that $\deg(\sigma(\mathfrak{q}; n))=$ rank $\mathfrak{o}$. Now the general case follows from

LEMMA 3.2. *If* x *is a transcendental element over* $\mathfrak{o}$, *then* $(\mathfrak{o}/\mathfrak{q}^n)(x)$

$=\mathfrak{o}(x)/\mathfrak{q}^n\mathfrak{o}(x)$ *and therefore* $\sigma(\mathfrak{q};n)=\sigma(\mathfrak{q}\mathfrak{o}(x);n)$.

The proof is easy and we omit it.

COROLLARY. *If* x *is a superficial element of* $\mathfrak{q}$, *then* rank $\mathfrak{o}/x\mathfrak{o}$ $=$ rank $\mathfrak{o}-1$.

Next we will give the proof of Remark 2 in §2. Let $\mathfrak{m}$ be the irrelevant prime ideal and consider the local ring $F_{\mathfrak{m}}/\mathfrak{a}F_{\mathfrak{m}}$. Let $\mathfrak{q}$ be the ideal of the local ring generated by the classes of $X_1,\cdots,X_s$. Then $\chi(\mathfrak{a};n)=l(\mathfrak{q}^n/\mathfrak{q}^{n+1})=\sigma(\mathfrak{q};n)-\sigma(\mathfrak{q};n-1)$ for sufficiently large n. Therefore we see the assertion by Remark 3 above.

From this result and from Remark 3, we have the following

REMARK 4. With the same notations as before in this §, co-rank $\mathfrak{a}$ $=$ rank $\mathfrak{o}$. (Krull [5] and Samuel [16])

LEMMA 3.3. *Assume that there exists an ideal* $\mathfrak{n}$ *of* $\mathfrak{o}$ *such that* $\mathfrak{n}\frown\mathfrak{q}^c=0$ *for an integer* c. *Then* 1) *the length of* $\mathfrak{n}$ *is finite and* 2) *for any superficial element* x *of* $\mathfrak{q}$, *the residue class* x' *of* x modulo $\mathfrak{n}$ *is a superficial element of* $(\mathfrak{q}+\mathfrak{n})/\mathfrak{n}$ (*in the local ring* $\mathfrak{o}/\mathfrak{n}$). (Nagata [9])

PROOF. We have $(\mathfrak{q}^c+\mathfrak{n})/\mathfrak{q}^c=\mathfrak{n}$, which shows the finiteness of the length of $\mathfrak{n}$. Since x is a superficial element of $\mathfrak{q}$, there exists an integer c' such that $(\mathfrak{q}^n:x\mathfrak{o})\frown\mathfrak{q}^{c'}=\mathfrak{q}^{n-1}$ for any $n>c'$. We may assume without loss of generality that $c=c'$. We denote by $\mathfrak{q}'$ the ideal $(\mathfrak{q}+\mathfrak{n})/\mathfrak{n}$ and by $\mathfrak{o}'$ the local ring $\mathfrak{o}/\mathfrak{n}$. Let b' be any element of $(\mathfrak{q}'^n:x'\mathfrak{o}')\frown\mathfrak{q}'^c$ $(n>c)$ and let b be a representative of b' in $\mathfrak{o}$. Since $b'\in\mathfrak{q}'^c$, we may choose b from $\mathfrak{q}^c$. Since $b'x'\in\mathfrak{q}'^n$, we have $bx\in\mathfrak{q}^n+\mathfrak{n}$. We express bx in the form $q+y$ with $q\in\mathfrak{q}^n$ and $y\in\mathfrak{n}$. We may regard the expression $bx=q+y$ as an expression of bx in $\mathfrak{q}^c+\mathfrak{n}$. Since $\mathfrak{q}^c\frown\mathfrak{n}=0$, we see that such an expression is uniquely determined. Since $bx\in\mathfrak{q}^c$, we have $bx=q$ (and $y=0$). Since $\mathfrak{q}\in\mathfrak{q}^n$, we have $bx\in\mathfrak{q}^n$ and $b\in(\mathfrak{q}^n:x\mathfrak{o})\frown\mathfrak{q}^c=\mathfrak{q}^{n-1}$. Therefore we have $b'\in\mathfrak{q}'^{n-1}$ and x' is a superficial element of $\mathfrak{q}'$. Thus the proof is completed.

§4. The definition of multiplicity.

Let again $\mathfrak{o}$ be a local ring with maximal ideal $\mathfrak{m}$ and let $\mathfrak{q}$ be a primary ideal belonging to $\mathfrak{m}$. Then $l(\mathfrak{o}/\mathfrak{q}^n)$ is the polynomial $\sigma(\mathfrak{q};n)$ for sufficiently large n and the degree d of $\sigma(\mathfrak{q};n)$ coincides with rank $\mathfrak{o}$, as we have proved in §3. Let a be the coefficient of n^d in $\sigma(\mathfrak{q};n)$. Then $(d!)a$ is called the *multiplicity* of $\mathfrak{q}$ and will be denoted by $e(\mathfrak{q})$. $e(\mathfrak{m})$ is called the multiplicity of $\mathfrak{o}$ and will be denoted by $m(\mathfrak{o})$.

Next, we will generalize the above definition to semi-local rings. Let $\mathfrak{o}$ be a semi-local ring and let $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ be some of maximal ideals of $\mathfrak{o}$. Further let $\mathfrak{q}_1,\cdots,\mathfrak{q}_r$ be primary ideals belonging to $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$

respectively and set $\mathfrak{m}=\mathfrak{q}_1\frown\cdots\frown\mathfrak{q}_r$. Then $\mathfrak{o}/\mathfrak{m}^n$ is isomorphic to the direct sum of rings $\mathfrak{o}/\mathfrak{q}_1^n$ $(=\mathfrak{o}_{\mathfrak{p}_1}/\mathfrak{q}_1^n\mathfrak{o}_{\mathfrak{p}_1}), \cdots, \mathfrak{o}/\mathfrak{q}_r^n$ $(=\mathfrak{o}_{\mathfrak{p}_r}/\mathfrak{q}_r^n\mathfrak{o}_{\mathfrak{p}_r})$. Therefore $l(\mathfrak{o}/\mathfrak{m}^n)=\sum\sigma(\mathfrak{q}_i\mathfrak{o}_{\mathfrak{p}_i};n)$ for sufficiently large n; this polynomial will be denoted by $\sigma(\mathfrak{m};n)$. The degree d of $\sigma(\mathfrak{m};n)$ is the maximum of rank $\mathfrak{p}_1,\cdots,$ rank $\mathfrak{p}_r$. Let a be the coefficient of n^d in $\sigma(\mathfrak{m};n)$. Then $(d\,!)a$ is called the multiplicity of $\mathfrak{m}$ and is denoted by $e(\mathfrak{m})$. When $\mathfrak{m}$ is the J-radical of $\mathfrak{o}$, $e(\mathfrak{m})$ is called the multiplicity of $\mathfrak{o}$ and is denoted by $m(\mathfrak{o})$.

From this definition, *we have, assuming that* rank $\mathfrak{p}_i=d$ *if and only if* $i\leqq s$, *the equality* $e(\mathfrak{m})=\sum_1^s e(\mathfrak{q}_i)$. On the other hand, $e(\mathfrak{q}_i)=e(\mathfrak{q}_i\mathfrak{o}_{\mathfrak{p}_i})$ for any i. In particular, the multiplicity of $\mathfrak{o}$ is the sum of multiplicity of local rings which are rings of quotients of $\mathfrak{o}$ and whose rank is equal to rank $\mathfrak{o}$.

With the same $\mathfrak{o}, \mathfrak{p}_1,\cdots,\mathfrak{p}_r, \mathfrak{q}_1,\cdots,\mathfrak{q}_r$ and $\mathfrak{m}$ as above, we assume further that there exists a local ring $\mathfrak{o}'$ which is a subring of $\mathfrak{o}$ such that 1) each $\mathfrak{p}_1$ lies over the maximal ideal $\mathfrak{m}'$ of $\mathfrak{o}'$ and 2) each $\mathfrak{o}/\mathfrak{p}_i$, is a finite module over $\mathfrak{o}'/\mathfrak{m}'$. Then $\mathfrak{o}/\mathfrak{m}^n$ can be regarded as an $\mathfrak{o}'$-module and $l(\mathfrak{o}/\mathfrak{m}^n;\mathfrak{o}')$ is defined. Then $l(\mathfrak{o}/\mathfrak{m}^n;\mathfrak{o}')=\sum l(\mathfrak{o}/\mathfrak{q}_i^n;\mathfrak{o}')=\sum[\mathfrak{o}/\mathfrak{p}_i:\mathfrak{o}'/\mathfrak{m}']\cdot l(\mathfrak{o}/\mathfrak{q}_i^n)$ (by Lemma 2.1), hence this is a polynomial in n for sufficiently large n; this polynomial will be denoted by $\sigma(\mathfrak{m};\mathfrak{o}';n)$. Observe that the degree d of $\sigma(\mathfrak{m};\mathfrak{o}';n)$ is equal to that of $\sigma(\mathfrak{m};n)$. Let a be the coefficient of n^d in $\sigma(\mathfrak{m};\mathfrak{o}';n)$. Then $(d\,!)a$ is called *the relative multiplicity* of $\mathfrak{m}$ with respect to $\mathfrak{o}'$ and is denoted by $rm(\mathfrak{m};\mathfrak{o}')$. From this definition, we have $rm(\mathfrak{m};\mathfrak{o}')=\sum_1^s e(\mathfrak{q}_i)\cdot[\mathfrak{o}/\mathfrak{p}_i:\mathfrak{o}'/\mathfrak{m}']$.

As will be shown in appendix, multiplicity and relative multiplicity are natural numbers.

We will add here the following remark:

Let $\mathfrak{o}$ be a local ring with maximal ideal $\mathfrak{m}$ and let $\mathfrak{q}$ be a primary ideal belonging to $\mathfrak{m}$. Let $\mathfrak{M}$ be the maximal ideal of the form ring $F(\mathfrak{q})$ which corresponds to the irrelevant prime ideal. Further let $\mathfrak{Q}$ be the ideal of $F(\mathfrak{q})$ generated by the forms of elements of $\mathfrak{q}$. Then $\sigma(\mathfrak{q};n)=\sigma(\mathfrak{Q}F(\mathfrak{q})_{\mathfrak{M}};n)$ and the multiplicity $e(\mathfrak{q})$ is equal to $e(\mathfrak{Q}F(\mathfrak{q})_{\mathfrak{M}})$.

For the proof, see § 3.

§ 5. Elementary properties of multiplicity.

LEMMA 5.1. *Let* $\mathfrak{q}$ *be a primary ideal belonging to the maximal ideal* $\mathfrak{m}$ *of a local ring* $\mathfrak{o}$ *and let* $\mathfrak{o}^*$ *be the completion of* $\mathfrak{o}$. *Then* $e(\mathfrak{q})=e(\mathfrak{q}\mathfrak{o}^*)$. *Similar fact holds for semi-local rings.*

PROOF. As was shown in § 3, $\sigma(\mathfrak{q};n)=\sigma(\mathfrak{q}\mathfrak{o}^*;n)$ and $e(\mathfrak{q})=e(\mathfrak{q}\mathfrak{o}^*)$.

On the other hand, we have obviously

LEMMA 5.2. *If a local ring* $\mathfrak{o}$ *is of rank* 0, *then for any primary ideal* $\mathfrak{q}$ *of* $\mathfrak{o}$, $e(\mathfrak{q})=l(\mathfrak{o})$. (Samuel [15])

Next we will consider the case of rank 1.

LEMMA 5.3. *Let $\mathfrak{o}$ be a local ring of rank* 1, *let $\mathfrak{q}$ be a primary ideal of $\mathfrak{o}$ belonging to the maximal ideal $\mathfrak{m}$ and assume that x is a superficial element of $\mathfrak{q}$. Then* 1) *if x is not a zero-divisor, then $e(\mathfrak{q})=e(x\mathfrak{o})=l(\mathfrak{o}/x\mathfrak{o})$ and* 2) *if x is a zero-divisor, then $e(\mathfrak{q})=e(x\mathfrak{o})<l(\mathfrak{o}/x\mathfrak{o})$.* (Nagata [9])

PROOF OF 1). By Corollary 3 to Proposition 4, $\sigma(\mathfrak{q}/x\mathfrak{o};n)=\sigma(\mathfrak{q};n)-\sigma(\mathfrak{q};n-1)=e(\mathfrak{q})$ (because the degree of $\sigma(\mathfrak{q};n)$ is equal to 1). By Lemma 5.2, $\sigma(\mathfrak{q}/x\mathfrak{o};n)=l(\mathfrak{o}/x\mathfrak{o})$. Thus we have $e(\mathfrak{q})=l(\mathfrak{o}/x\mathfrak{o})$. Since x is not a zero-divisor, x is a superficial element of the primary ideal $x\mathfrak{o}$. Therefore the same can be applied and we have $e(x\mathfrak{o})=l(\mathfrak{o}/x\mathfrak{o})$. Thus 1) is proved.

PROOE OF 2). We will first show that $e(x\mathfrak{o})<$length $\mathfrak{o}/x\mathfrak{o}$. Let y be a non-zero element of $\mathfrak{o}$ such that $xy=0$. Then there exists an integer m such that $y\notin x^m\mathfrak{o}$. Let n be a sufficiently large integer. Then $l(\mathfrak{o}/x\mathfrak{o})=\sigma(x\mathfrak{o}/x\mathfrak{o};n)=\sigma(x\mathfrak{o};n)-l(\mathfrak{o}/(x^n\mathfrak{o}:x\mathfrak{o}))$ by Proposition 4. Since $x^n\mathfrak{o}:x\mathfrak{o}$ contains y which is not in $x^{n-1}\mathfrak{o}$, $x^n\mathfrak{o}:x\mathfrak{o}$ contains $x^{n-1}\mathfrak{o}$ properly. Theorefore $\sigma(x\mathfrak{o};n-1)$ is greater than $l(\mathfrak{o}/(x^n\mathfrak{o}:x\mathfrak{o}))$ and $l(\mathfrak{o}/x\mathfrak{o})$ is greater than $\sigma(x\mathfrak{o};n)-\sigma(x\mathfrak{o};n-1)=e(x\mathfrak{o})$. Next we will show that $e(\mathfrak{q})=e(x\mathfrak{o})$. Set $\mathfrak{n}=0:x\mathfrak{o}$. Since x is superficial element of $\mathfrak{q}$, there exists an integer c such that $(\mathfrak{q}^n:x\mathfrak{o})\frown\mathfrak{q}^c=\mathfrak{q}^{n-1}$ for $n>c$. Since $\mathfrak{n}$ is contained in any of $\mathfrak{q}^n:x\mathfrak{o}$, we have $\mathfrak{n}\frown\mathfrak{q}^c=0$. Therefore by Lemma 3.3, $l(\mathfrak{n})$ is finite and therefore $e(\mathfrak{q})=e(\mathfrak{q}+\mathfrak{n})/\mathfrak{n}$ and $e(x\mathfrak{o})=e((x\mathfrak{o}+\mathfrak{n})/\mathfrak{n})$. Further by Lemma 3.3, (x modulo $\mathfrak{n}$) is a superficial element of $(\mathfrak{q}+\mathfrak{n})/\mathfrak{n}$. Therefore we may replace $\mathfrak{o}$ by $\mathfrak{o}/\mathfrak{n}$, $\mathfrak{q}$ by $(\mathfrak{q}+\mathfrak{n})/\mathfrak{n}$ and x by (x modulo n). Repeating the same procedure, we reach to the case when x is not a zero-divisor and we have $e(\mathfrak{q})=e(x\mathfrak{o})$ by 1). Thus the proof is completed.

Thirdly, we will consider local rings of rank greater than 1.

LEMMA 5.4. *Let $\mathfrak{o}$ be a local ring of rank greater than* 1, *let $\mathfrak{q}$ be a primary ideal of $\mathfrak{o}$ belonging to the maximal ideal $\mathfrak{m}$ and assume that x is a superficial element of $\mathfrak{q}$. Then we have $e(\mathfrak{q})=e(\mathfrak{q}/x\mathfrak{o})$.* (Samuel [15])

PROOF. By Corollary 2 to Proposition 4, $\sigma(\mathfrak{q}/x\mathfrak{o};n)$ and $\sigma(\mathfrak{q};n)-\sigma(\mathfrak{q};n-1)$ coincide up to constant terms. Let d be the degree of $\sigma(\mathfrak{q};n)$, which coincides with rank $\mathfrak{o}$ and $d>1$. Therefore the coefficient of n^{d-1} in $\sigma(\mathfrak{q}/x\mathfrak{o};n)$ coincides with that of $\sigma(\mathfrak{q};n)-\sigma(\mathfrak{q};n-1)$ and is obviously $e(\mathfrak{q})/((d-1)!)$. Thus we see the assertion.

On the other hand, we see immediately from Proposition 4 the following

LEMMA 5.5. *If $\mathfrak{q}$ is a primary ideal of a local ring $\mathfrak{o}$ belonging* *to the maximal ideal and if x is an element of $\mathfrak{q}$ such that rank* $\mathfrak{o}/x\mathfrak{o}=\text{rank}\,\mathfrak{o}-1$,[8] *then $e(\mathfrak{q})$ is not greater than $e(\mathfrak{q}/x\mathfrak{o})$.*

(For, $\mathfrak{q}^n:x\mathfrak{o}$ contains $\mathfrak{q}^{n-1}$ and $\sigma(\mathfrak{q}/x\mathfrak{o};n)$ is not less than $\sigma(\mathfrak{q};n)-\sigma(\mathfrak{q};n-1)$.)

COROLLARY 1. *If $x_1,\cdots,x_r$ are elements of $\mathfrak{q}$ such that* 1) rank $(\sum_1^r x_i\mathfrak{o})=r$ *and* 2) $e(\mathfrak{q})=e(\mathfrak{q}/(\sum_1^r x_i\mathfrak{o}))$, *then for any ideal $\mathfrak{a}$ generated by a subset of $x_1,\cdots,x_r$ we have $e(\mathfrak{q})=e(\mathfrak{q}/\mathfrak{a})$.*

COROLLARY 2. *If $\mathfrak{q}$ is the ideal of a local ring $\mathfrak{o}$ generated by a system of parameters of $\mathfrak{o}$, then $e(\mathfrak{q})$ is not greater than $l(\mathfrak{o}/\mathfrak{q})$.*

Now we have

THEOREM 1. *Let $\mathfrak{o}$ be a local ring with maximal ideal $\mathfrak{m}$ and let $\mathfrak{q}$ be a primary ideal belonging to $\mathfrak{m}$. If $\mathfrak{o}/\mathfrak{m}$ contains infinitely many elements, then there exists an ideal $\mathfrak{q}'$ which is generated by a system of parameters of $\mathfrak{o}$ and contained in $\mathfrak{q}$ such that $e(\mathfrak{q}')$.* (Nagata [9])

PROOF. When rank $\mathfrak{o}\leqq 1$, we have proved in Lemmas 5.2–5.3.[9] We will prove the other case by induction on the rank d of $\mathfrak{o}$. Let x be a superficial element of $\mathfrak{q}$. Then by Lemma 5.4, we have $e(\mathfrak{q})=e(\mathfrak{q}/x\mathfrak{o})$. Since rank $\mathfrak{o}/x\mathfrak{o}=\text{rank}\,\mathfrak{o}-1$, there exists a system of parameters $x_2',\cdots,x_d'$ of $\mathfrak{o}/x\mathfrak{o}$ such that $e(\mathfrak{q}/x\mathfrak{o})=e\,(\sum_2^d x_i'(\mathfrak{o}/x\mathfrak{o}))$ and that $x_i'\in\mathfrak{q}/x\mathfrak{o}$. Let x_i be a representative of x_i' in $\mathfrak{o}$ for each i and let $\mathfrak{q}'$ be the ideal generated by $x,x_2,\cdots,x_d$. Since $\mathfrak{q}'\subseteqq\mathfrak{q}$, we have $e(\mathfrak{q})\leqq e(\mathfrak{q}')$. On the other hand, we see by Lemma 5.5 that $e(\mathfrak{q}')\leqq e(\mathfrak{q}'/x\mathfrak{o})=e(\mathfrak{q}/x\mathfrak{o})=e(\mathfrak{q})$. Thus we see that $e(\mathfrak{q})=e(\mathfrak{q}')$ and the proof is completed.

REMARK 1. Lemmas 5.3–5.4 and the above proof shows that one $\mathfrak{q}'$ can be constructed as follows: Let x_1 be a superficial element of $\mathfrak{q}$, let x_2 be a representative of a superficial element of $\mathfrak{q}/x_1\mathfrak{o}$ and so on (in general, let x_i be a representative of a superficial element of $\mathfrak{q}/(\sum_1^{i-1}x_j\mathfrak{o})$). Then the ideal $\mathfrak{q}'$ generated by $x_1,\cdots,x_d$ ($d=\text{rank}\,\mathfrak{o}$) is the required ideal.

On the other hand, in order to reduce the case when the residue class field contains only a finite number of elements to the contrary case, it will be convenient to formulate Lemma 3.2 as following

PROPOSITION 5. *Let x be a transcendental element over a local ring $\mathfrak{o}$ and let $\mathfrak{q}$ be a primary ideal of $\mathfrak{o}$ belonging to the maximal ideal $\mathfrak{m}$. Then we have $l(\mathfrak{o}/\mathfrak{q})=l(\mathfrak{o}(x)/\mathfrak{q}\mathfrak{o}(x))$ and $e(\mathfrak{q})=e(\mathfrak{q}\mathfrak{o}(x))$.*

We will add here some remarks on the notion of *superficial system*

[8] For this condition rank $\mathfrak{o}/x\mathfrak{o}=\text{rank}\,\mathfrak{o}-1$, it is sufficient to be rank $x\mathfrak{o}=1$ (and this last condition is not necessary).

[9] We regard that the ideal generated by the empty set is the zero ideal and that the system of parameters of a local ring of rank zero is the empty set.

of parameters introduced by Samuel [15]. We say that a system of parameters $x_1,\cdots,x_d$ of a local ring $\mathfrak{o}$ is a superficial system of parameters of $\mathfrak{o}$ if x_i modulo $\sum_1^{i-1} x_j\mathfrak{o}$ is a superficial element of $(\sum_1^d x_j\mathfrak{o})/(\sum_1^{i-1} x_j\mathfrak{o})$ for each $i=1,\cdots,d$. Then

REMARK 2. If $\mathfrak{q}$ is the ideal of a local ring $\mathfrak{o}$ generated by a system of parameters of $\mathfrak{o}$ and if the residue class field of $\mathfrak{o}$ contains infinitely many elements, then $\mathfrak{q}$ is generated by a superficial system of parameters of $\mathfrak{o}$. (Samuel [15])

PROOF. Let $x_1,\cdots,x_d$ be a system of parameters of $\mathfrak{o}$ which generates $\mathfrak{q}$. Then a superficial element y of $\mathfrak{q}$ is linear combination of x_i's with coefficients in $\mathfrak{o}$ such that some coefficients are unit in $\mathfrak{o}$. If the coefficient of x_1 is unit, then $\mathfrak{q}$ is generated by $y, x_2,\cdots,x_d$. The same can be applied to $\mathfrak{o}/y\mathfrak{o}$ and $\mathfrak{q}/y\mathfrak{o}$ (which is generated by the residue classes of $x_2,\cdots,x_d$). Thus, repeating the same (or by induction on d), we see the assertion.

REMARK 3. If $\mathfrak{q}$ is the ideal generated by a superficial system of parameters $x_1\cdots,x_d$ of a local ring $\mathfrak{o}$, then $e(\mathfrak{q})=e(\mathfrak{q}/(\sum_1^{d-1} x_i\mathfrak{o}))$. On the other hand, $e(\mathfrak{q})=l(\mathfrak{o}/\mathfrak{q})$ if and only if x_d is not a zero-divisor modulo $\sum_1^{d-1} x_i\mathfrak{o}$. (Samuel [15])

This follows from Lemmas 5.3–5.4.

§ 6. The extension formula and the theorem of additivity.

THEOREM 2 (EXTENSION FORMULA). *Let $\mathfrak{o}$ be a local ring with maximal ideal $\mathfrak{m}$ and let $\mathfrak{q}$ be a primary ideal belonging to $\mathfrak{m}$. Assume that an over-ring $\mathfrak{o}'$ of $\mathfrak{o}$ satisfies the following condition: There exist a system $a_1=1, a_2,\cdots,a_r$ of linearly independent elements of $\mathfrak{o}'$ over $\mathfrak{o}$ and an element c of $\mathfrak{o}$ which is not a zero-divisor in $\mathfrak{o}'$ such that $c\mathfrak{o}'$ is contained in the module $M=\sum a_i\mathfrak{o}$. Then we have*

$$e(\mathfrak{q})\cdot r=rm(\mathfrak{q}\mathfrak{o}';\mathfrak{o}).$$

PROOF. Since $\mathfrak{q}^n M$ contains $\mathfrak{q}^n c\mathfrak{o}'$, $(c\mathfrak{o}'+\mathfrak{q}^n M)/\mathfrak{q}^n M$ may be regarded as a homomorphic image of $c\mathfrak{o}'/\mathfrak{q}^n c\mathfrak{o}'$ (with kernel $(\mathfrak{q}^n M\cap c\mathfrak{o}')/\mathfrak{q}^n c\mathfrak{o}'$). Hence we have

$$(1)\quad l(c\mathfrak{o}'/\mathfrak{q}^n c\mathfrak{o}';\mathfrak{o})\geqq l((c\mathfrak{o}'+\mathfrak{q}^n M)/\mathfrak{q}^n M)=l(M/\mathfrak{q}^n M)-l(M/(c\mathfrak{o}'+\mathfrak{q}^n M)).$$

Since mapping ϕ from $\mathfrak{o}'$ onto $c\mathfrak{o}'$ such that $\phi(a)=ca$ is an isomorphism, we have $l(\mathfrak{o}'/\mathfrak{q}^n\mathfrak{o}';\mathfrak{o})=l(c\mathfrak{o}'/\mathfrak{q}^n c\mathfrak{o}';\mathfrak{o})$. On the other hand, obviously $l(M/\mathfrak{q}^n M)=r\cdot l(\mathfrak{o}/\mathfrak{q}^n)$ and $l(M/(c\mathfrak{o}'+\mathfrak{q}^n M))\leqq l(M/(cM+\mathfrak{q}^n M))=r\cdot l(\mathfrak{o}/(c\mathfrak{o}+\mathfrak{q}^n))$; this last is of less degree than rank $\mathfrak{o}$ because c is not a zero-divisor. Therefore the above inequality (1) shows that the relative multiplicity of $\mathfrak{q}\mathfrak{o}'$ is not less than $r\cdot e(\mathfrak{q})$.

Conversely; since $\mathfrak{q}^n\mathfrak{o}'$ contains $\mathfrak{q}^n M$, $(M+\mathfrak{q}^n\mathfrak{o}')/\mathfrak{q}^n\mathfrak{o}'$ may be regarded as a homomorphic image of $M/\mathfrak{q}^nM$. Hence we have

$$l(M/\mathfrak{q}^nM) \geqq l((M+\mathfrak{q}^n\mathfrak{o}')/\mathfrak{q}^n\mathfrak{o}') \geqq l((c\mathfrak{o}'+\mathfrak{q}^n\mathfrak{o}')/\mathfrak{q}^n\mathfrak{o}';\mathfrak{o}) = l(\mathfrak{o}'/\mathfrak{q}^n\mathfrak{o}';\mathfrak{o}) - l(\mathfrak{o}'/(c\mathfrak{o}'+\mathfrak{q}^n\mathfrak{o}');\mathfrak{o}). \tag{2}$$

Since $l(\mathfrak{o}'/(c\mathfrak{o}'+\mathfrak{q}^n\mathfrak{o}');\mathfrak{o})$ is of less degree than rank $\mathfrak{o}$, the above inequality (2) shows that the relative multiplicity of $\mathfrak{q}\mathfrak{o}'$ is not greater than $r\cdot e(\mathfrak{q})$. Thus we have the equality $r\cdot e(\mathfrak{q}) = rm(\mathfrak{q}\mathfrak{o}';\mathfrak{o})$.

COROLLARY 1. *Let $\mathfrak{o}$ be a local ring and let $\mathfrak{o}'$ be a subring of the total quotient ring of $\mathfrak{o}$ such that $\mathfrak{o}'$ is a finite $\mathfrak{o}$-module. Then for any primary ideal $\mathfrak{q}$ of $\mathfrak{o}$ belonging to the maximal ideal $\mathfrak{m}$ of $\mathfrak{o}$, it holds the equality* $e(\mathfrak{q}) = rm(\mathfrak{q}\mathfrak{o}';\mathfrak{o})$. In particular, for any maximal ideal $\mathfrak{p}'$ of $\mathfrak{o}'$ such that rank $\mathfrak{p}'$ = rank $\mathfrak{o}$, $e(\mathfrak{q}\mathfrak{o}'_{\mathfrak{p}'})$ is not greater than $e(\mathfrak{q})$; they coincide if and only if 1) $\mathfrak{o}/\mathfrak{m} = \mathfrak{o}'/\mathfrak{p}'$ and 2) any other maximal ideal of $\mathfrak{o}'$ is of rank less than that of $\mathfrak{p}'$. In general, $m(\mathfrak{o}') \leqq m(\mathfrak{o})$.

COROLLARY 2. *If $\mathfrak{o}'$ is a finite integral extension of a local integrity domain $\mathfrak{o}$, then for any primary ideal $\mathfrak{q}$ or $\mathfrak{o}$ belonging to the maximal ideal $\mathfrak{m}$ of $\mathfrak{o}$, it holds that* $rm(\mathfrak{q}\mathfrak{o}';\mathfrak{o}) = [\mathfrak{o}':\mathfrak{o}]\cdot e(\mathfrak{q})$.

REMARK. If we apply the extension formula to unmixed local rings (equi-dimensional local rings in the sense of Chevalley [2])[10] which are complete and which contain fields, we see the coincidence of our definition to that of Chevalley [2] as follows:

Let $\mathfrak{o}$ be an unmixed and complete local ring which contains a field k. Then $\mathfrak{o}$ contains a field K which forms a complete set of representatives of the residue class field of $\mathfrak{o}$. Let $x_1, \cdots, x_d$ be a system of parameters of $\mathfrak{o}$. Let $\mathfrak{r}$ be the set of elements of $\mathfrak{o}$ which are expressible as power series in $x_1, \cdots, x_d$ with coefficients in K. Then $\mathfrak{r}$ is a regular local ring. Since $\mathfrak{o}$ is unmixed, any non-zero element of $\mathfrak{r}$ is not a zero-divisor in $\mathfrak{o}$. On the other hand, since x_i's generate an ideal $\mathfrak{q}$ which is primary belonging to the maximal ideal $\mathfrak{m}$ of $\mathfrak{o}$ and since $K = \mathfrak{o}/\mathfrak{m}$, $\mathfrak{o}$ is a finite $\mathfrak{r}$-module. Hence $rm(\mathfrak{q};\mathfrak{r}) = [\mathfrak{o}:\mathfrak{r}]\cdot e(\sum x_i\mathfrak{r})$. Since $K = \mathfrak{o}/\mathfrak{m}$, $rm(\mathfrak{q};\mathfrak{r}) = e(\mathfrak{q})$. Since x_i's form a regular system of parameters of $\mathfrak{r}$, $e(\sum x_i\mathfrak{r}) = 1$. Hence we have $e(\mathfrak{q}) = [\mathfrak{o}:\mathfrak{r}]$.

THEOREM 3 (THE THEOREM OF ADDITIVITY).[11] *Let $\mathfrak{o}$ be a local ring and let $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ be all of prime divisors of zero; we renumber them so that* co-rank $\mathfrak{p}_i$ = rank $\mathfrak{o}$ *if and only if $i \leqq r$. Let $\mathfrak{q}_1, \cdots, \mathfrak{q}_r$ be primary components of zero belonging to $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ respectively. Then it holds the equality* $e(\mathfrak{q}) = \sum_1^r e((\mathfrak{q}+\mathfrak{q}_i)/\mathfrak{q}_i)$.

[10] The definition will be stated in § 7.

[11] This theorem was proved by Northcott-Rees [14] under a certain condition. On the other hand, the last part of this theorem was given by Samuel [16].

In particular, if $\mathfrak{a}$ *and* $\mathfrak{b}$ *are ideals of* $\mathfrak{o}$ *such that* co-rank $\mathfrak{a}$ $>$co-rank $\mathfrak{b}$, *then*

$$e((\mathfrak{q}+\mathfrak{a})/\mathfrak{a})=e((\mathfrak{q}+(\mathfrak{a}\frown\mathfrak{b}))/(\mathfrak{a}\frown\mathfrak{b})).$$

PROOF. We will prove the last assertion at first. Let $x_1,\cdots,x_t$ be a base of $\mathfrak{q}$. Then the form ring $F((\mathfrak{q}+\mathfrak{a})/\mathfrak{a})$, $F((\mathfrak{q}+\mathfrak{b})/\mathfrak{b})$ and $F((\mathfrak{q}+(\mathfrak{a}\frown\mathfrak{b}))/(\mathfrak{a}\frown\mathfrak{b}))$ may be regarded as homomorphic images of the polynomial ring $F=(\mathfrak{o}/\mathfrak{q})[X_1,\cdots,X_t]$ (X_i's being indeterminates) by the natural way. Let $\mathfrak{n}(\mathfrak{a})$, $\mathfrak{n}(\mathfrak{b})$ and $\mathfrak{n}(\mathfrak{a}\frown\mathfrak{b})$ be the kernel of these homomorphisms. Then co-rank $\mathfrak{n}(\mathfrak{a})=$co-rank $\mathfrak{a}$, co-rank $\mathfrak{n}(\mathfrak{b})=$co-rank $\mathfrak{b}$ and co-rank $\mathfrak{n}(\mathfrak{a}\frown\mathfrak{b})=$co-rank $(\mathfrak{a}\frown\mathfrak{b})$ (see §3, Remark 4). Obviously $\mathfrak{n}(\mathfrak{a})\frown\mathfrak{n}(\mathfrak{b})$ contains $\mathfrak{n}(\mathfrak{a}\frown\mathfrak{b})$ and $\mathfrak{n}(\mathfrak{a}\frown\mathfrak{b})$ contains $\mathfrak{n}(\mathfrak{a})\cdot\mathfrak{n}(\mathfrak{b})$. Therefore we see that $\mathfrak{n}(\mathfrak{a})$ and $\mathfrak{n}(\mathfrak{a}\frown\mathfrak{b})$ coincide up to primary components of less co-rank than co-rank $\mathfrak{a}$. Therefore there exist homogeneous ideals $\mathfrak{a}'$, $\mathfrak{b}'$ and $\mathfrak{c}'$ such that 1) co-rank $\mathfrak{a}'=$co-rank $\mathfrak{a}$, co-rank $\mathfrak{b}'<$co-rank $\mathfrak{a}$, co-rank $\mathfrak{c}'<$co-rank $\mathfrak{a}$ and 2) $\mathfrak{n}(\mathfrak{a})=\mathfrak{a}'\frown\mathfrak{c}'$, $\mathfrak{n}(\mathfrak{a}\frown\mathfrak{b})=\mathfrak{a}'\frown\mathfrak{b}'$. By Lemma 2.3, $\chi(\mathfrak{a}'+\mathfrak{c}';n)=\chi(\mathfrak{a}';n)+\chi(\mathfrak{c}';n)-\chi(\mathfrak{a}'\frown\mathfrak{c}';n)$. Since $\chi(\mathfrak{a}'+\mathfrak{c}';\mathfrak{n})$ and $\chi(\mathfrak{c}';n)$ are of less degree than $\chi(\mathfrak{a}';\mathfrak{n})$, we see that $\chi(\mathfrak{a}';n)$ and $\chi(\mathfrak{a}'\frown\mathfrak{c}';n)$ have the same term of the largest degree. Similarly, $\chi(\mathfrak{a}';n)$ and $\chi(\mathfrak{a}'\frown\mathfrak{b}';n)$ have the same term of the largest degree. Thus we see that $\chi(\mathfrak{n}(\mathfrak{a});n)$ and $\chi(\mathfrak{n}(\mathfrak{a}\frown\mathfrak{b});n)$ have the same term of the largest degree and $e((\mathfrak{q}+\mathfrak{a})/\mathfrak{a})=e((\mathfrak{q}+(\mathfrak{a}\frown\mathfrak{b}))/(\mathfrak{a}\frown\mathfrak{b}))$. Now we will prove the first assertion. By the above observation, $e(\mathfrak{q})=e((\mathfrak{q}+(\bigcap_i\mathfrak{q}_i))/(\bigcap_i\mathfrak{q}_i))$. Therefore we may assume that $\bigcap_i\mathfrak{q}_i=0$, that is, all $\mathfrak{p}_i$'s are of the same co-rank ($=$rank $\mathfrak{o}$). Then in the total quotient ring of $\mathfrak{o}$, there exist primitive idempotents $e_1,\cdots,e_r$ such that $\mathfrak{o}e_i$ is isomorphic to $\mathfrak{o}/\mathfrak{q}_i$ for each i. Set $\mathfrak{o}'=\sum e_i\mathfrak{o}$. Then by Corollary 1 to the extension formula, we have $rm(\mathfrak{q}\mathfrak{o}';\mathfrak{o})=e(\mathfrak{q})$. Since any residue class field of $\mathfrak{o}'$ is represented by elements of $\mathfrak{o}$, we have $rm(\mathfrak{q}\mathfrak{o}';\mathfrak{o})$ is the sum of all $e(\mathfrak{q}\mathfrak{o}e_i)=e((\mathfrak{q}+\mathfrak{q}_i)/\mathfrak{q}_i)$ and the assertion is proved.

§7. The existence of distinct system of parameters.

Let $\mathfrak{o}$ be a local ring and let $x_1,\cdots,x_d$ be a system of parameters of $\mathfrak{o}$. Let $\mathfrak{q}$ be the ideal generated by x_i's. Then as was shown in §5, $e(\mathfrak{q})\leqq l(\mathfrak{o}/\mathfrak{q})$. We say that $x_1,\cdots,x_d$ is a *distinct system of parameters* of $\mathfrak{o}$ if $e(\mathfrak{q})=l(\mathfrak{o}/\mathfrak{q})$. As was remarked there, if $x_1,\cdots,x_d$ is a superficial system of parameters, then they form a distinct system of parameters if and only if x_d is not a zero-divisor modulo $\sum_1^{d-1}x_i\mathfrak{o}$.

PROPOSITION 6. *A system of parameters* $x_1,\cdots,x_d$ *of a local ring* $\mathfrak{o}$ *is distinct if and only if the form ring* $F(\mathfrak{q})$, $\mathfrak{q}$ *being the ideal generated by* x_i*'s, is isomorphic to the polynomial ring* F *in* d *in-*

determinates X_i's over $\mathfrak{o}/\mathfrak{q}$. Therefore in this case, $l(\mathfrak{o}/\mathfrak{q}^n)=\binom{n+d}{d}\cdot l(\mathfrak{o}/\mathfrak{q})$ for any n and $x_1,\cdots,x_d$ is a superficial system of parameters.[12]

PROOF. Let $\mathfrak{a}$ be the homogeneous ideal of F which is the kernel of the homomorphism from F onto $F(\mathfrak{q})$ which maps X_i to the form of x_i in $F(\mathfrak{q})$. Set $m=l(\mathfrak{o}/\mathfrak{q})$. Then $l(F(n))=m\cdot\binom{n+d-1}{d-1}$ and $l(F(n)/\mathfrak{a}(n))=l(\mathfrak{q}^n/\mathfrak{q}^{n+1})=\sigma(\mathfrak{q};n+1)-\sigma(\mathfrak{q};n)$ for sufficiently large n. Assume that $\mathfrak{a}\neq 0$ and let f be a non-zero homogeneous form in $\mathfrak{a}$; let c be the degree of f. Then $\mathfrak{a}(n)$ contains all the forms $fX_1^{n_1}\cdots X_d^{n_d}$ $(\sum n_i=n-c)$ and the length of the module of such forms is equal to $\binom{n-c+d-1}{d-1}=(n^{d-1}/((d-1)!))+$(terms of lower degree). Hence the coefficient of n^{d-1} in $\sigma(\mathfrak{q};n+1)-\sigma(\mathfrak{q};n)$ is not greater than $(m-1)/((d-1)!)$, which shows that $e(\mathfrak{q})$ is less than m. Hence, if $x_1,\cdots,x_d$ is a distinct system of parameters, then $\mathfrak{a}=0$. Conversely, if $\mathfrak{a}=0$, then obviously $l(\mathfrak{o}/\mathfrak{q}^n)=m\cdot\binom{n+d}{d}$ and $e(\mathfrak{q})=m$. Further we see that x_1 is a superficial element of $\mathfrak{q}$, and then by induction on i we see that the residue class of x_i modulo $\sum_1^{i-1}x_j\mathfrak{o}$ is a superficial element of $\mathfrak{q}/(\sum_1^{i-1}x_j\mathfrak{o})$. Thus we see that $x_1,\cdots,x_d$ is a superficial system of parameters.

We say that a local ring $\mathfrak{o}$ is unmixed if the co-rank of any prime divisor of zero of the completion $\mathfrak{o}^*$ of $\mathfrak{o}$ is equal to the rank of $\mathfrak{o}$. Then we have

LEMMA 7.1. *If a local ring $\mathfrak{o}$ has a distinct system of parameters, then $\mathfrak{o}$ is unmixed. More generally, if there exists a primary ideal $\mathfrak{q}$ of $\mathfrak{o}$ belonging to the maximal ideal of $\mathfrak{o}$ such that any prime divisor of zero of the form ring $F(\mathfrak{q})$ is of co-rank equal to* rank $\mathfrak{o}$, *then $\mathfrak{o}$ is unmixed.*

PROOF. By virtue of Proposition 6, we may prove only the last assertion. We may assume that $\mathfrak{o}$ is complete. Assume that there exists a prime divisor $\mathfrak{p}$ of zero of $\mathfrak{o}$ which is of co-rank less than rank $\mathfrak{o}$. Let $\mathfrak{p}'$ be the ideal of $F(\mathfrak{q})$ which is generated by all forms which correspond to elements of $\mathfrak{p}$ ($\mathfrak{p}'$ is the kernel of the natural homomorphism from $F(\mathfrak{q})$ onto $F((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})$). Since $\mathfrak{p}$ is a prime divisor of zero, $\mathfrak{p}'$ is contained in a prime divisor of zero of $F(\mathfrak{q})$ (for, there exists an element $a\neq 0$ of $\mathfrak{o}$ such that $a\mathfrak{p}=0$). Since co-rank $\mathfrak{p}<$rank $\mathfrak{o}$, we have co-rank $\mathfrak{p}'<$rank $\mathfrak{o}$, which shows that there exists a prime divisor of $F(\mathfrak{q})$ of co-rank less than rank $\mathfrak{o}$. Thus the assertion is proved.

[12] This result shows that our notion of distinct system of parameters coincides with the notion of "systèm distingué de paramètres" in the sense of Samuel [15].

PROPOSITION 7. *If $x_1, \cdots, x_d$ is a system of parameters of a local ring $\mathfrak{o}$ such that each x_i is not a zero-divisor modulo $\sum_1^{i-1} x_j\mathfrak{o}$, then $x_1, \cdots, x_d$ is a distinct system of parameters of $\mathfrak{o}$ (and conversely).*

PROOF. By the case $i=1$, we see that x_i is not a zero-divisor. Therefore, if $d=1$, our assertion follows from Lemma 5.3 (see the proof to it).[13] Therefore we will prove the assertion by induction on d. Then, by our induction assumption, $x_2, \cdots, x_d$ modulo $x_1\mathfrak{o}$ form a distinct system of parameters of $\mathfrak{o}/x_1\mathfrak{o}$. Let $\mathfrak{q}$ be the ideal generated by x_i's and let $\mathfrak{a}$ be the kernel of the homomorphism from the polynomial ring $F=(\mathfrak{o}/\mathfrak{q})[X_1, \cdots, X_d]$ onto the form ring $F(\mathfrak{q})$ which maps X_i to the form of x_i. We have only to prove that $\mathfrak{a}=0$. Assume the contrary.. Since $\mathfrak{q}/x_1\mathfrak{o}$ is generated by a distinct system of parameters of $\mathfrak{o}/x_1\mathfrak{o}$, the form ring $F(\mathfrak{q}/x_1\mathfrak{o})$ is isomorphic to F/X_1F by the natural way, which shows that $\mathfrak{a}$ is contained in X_1F. Let n be such that $\mathfrak{a}(n+1)\neq 0$. Then there exists an element $f \in F(n)$ which is not in $F(n+1)$ such that $X_1 f \in \mathfrak{a}$. This shows that there exists an element $b \in \mathfrak{q}^n$ which is not in $\mathfrak{q}^{n+1}$ such that $x_1 b \in \mathfrak{q}^{n+2}$, i.e., $x_1 b = \sum c_{i_1 \cdots i_d} x_1^{i_1} \cdots x_d^{i_d}$ with $\sum i_j =$ degree of $x_1 b$ with respect to $\mathfrak{q} \geqq n+2$ and $c_{i_1 \cdots i_d} \in \mathfrak{o}$. Consider a corresponding form f' to the element $x_1 b$ in F. Since $x_1 b$ is in $x_1\mathfrak{o}$ and since $F(\mathfrak{q}/x_1\mathfrak{o}) = F/X_1F$, we see that $f' \in X_1F$, that is, there exists an element b_1 of $\mathfrak{o}$ such that 1) $b_1 \in \mathfrak{q}^{\Sigma i_j - 1}$ and 2) $x_1 b - x_1 b_1 \in \mathfrak{q}^{\Sigma i_j + 1}$. Set $b' = b - b_1$. Then $b' \notin \mathfrak{q}^{n+1}$ and the degree of $x_1 b'$ with respect to $\mathfrak{q}$ is greater than that of $x_1 b$. The same can be applied to $x_1 b'$ and so on and we see that there exists a convergent sequence $b^{(i)}$ in $\mathfrak{o}$ ($b^{(i)} \notin \mathfrak{q}^{n+1}$) such that $x_1 b^{(i)}$ converges to zero. Since x_1 is not a zero-divisor in $\mathfrak{o}$, x_1 is not a zero-divisor in the completion of $\mathfrak{o}$, which shows that $b^{(i)}$ converges to zero and it is a contradiction to that $b^{(i)} \notin \mathfrak{q}^{n+1}$. Thus we have $\mathfrak{a}=0$ and the proof is completed.

THEOREM 4. *If a local ring $\mathfrak{o}$ has a distinct system of parameters, then any system of parameters of $\mathfrak{o}$ is distinct.*

PROOF. When $\mathfrak{o}$ is of rank 1, our assertion is immediate from Lemma 5.3 (cf. foot-note 13)) and we will prove the assertion by induction on the rank of $\mathfrak{o}$. Let $x_1, \cdots, x_d$ be a distinct system of parameters of $\mathfrak{o}$ and let $y_1, \cdots, y_d$ be any system of parameters of $\mathfrak{o}$. We may assume that $x_1\mathfrak{o} + y_1\mathfrak{o}$ is of rank 2, because x_i's and y_j's may be changed to another system of parameters which generate respectively the same ideals. By Proposition 6 (or 7), we see that the residue classes of $x, \cdots, x_d$ modulo $x_1\mathfrak{o}$ form a distinct system of

[13] Another proof can be given as follows: Since x_1 is not a zero-divisor, $l(\mathfrak{o}/x_1\mathfrak{o}) = l(x_1^n\mathfrak{o}/x_1^{n+1}\mathfrak{o})$ for any n, hence $l(\mathfrak{o}/x_1^n\mathfrak{o}) = l(\mathfrak{o}/x_1\mathfrak{o}) \cdot n$ for any n.

parameters of $\mathfrak{o}/x_1\mathfrak{o}$. Hence, by our induction assumption, we see that any system of parameters of $\mathfrak{o}/x_1\mathfrak{o}$ is a distinct system of parameters of $\mathfrak{o}$, which shows by virtue of Proposition 7 that any system of parameters of $\mathfrak{o}$ which contains x_1 as a member is a distinct system of parameters of $\mathfrak{o}$. In particular, any system of parameters of $\mathfrak{o}$ which contains x_1 and y_1 as members is a distinct system of parameters. Then the same can be applied to such a system of parameters (taking y_1 instead of x_1 in the above observation) and we see that any system of parameters of $\mathfrak{o}$ which contains y_1 as a member is also a distinct system of parameters and the assertion is proved.

COROLLARY 1. *Any system of parameters of a regular local ring is a distinct system of parameters.* (Nagata [9])

PROOF. Obviously any regular system of parameters is a distinct system of parameters and the assertion is proved.

COROLLARY 2. *If a local ring $\mathfrak{o}$ has a distinct system of parameters and if $\mathfrak{a}$ is an ideal of $\mathfrak{o}$ generated by r elements and of rank r, then $\mathfrak{o}/\mathfrak{a}$ has distinct system of parameters, hence any system of parameters of $\mathfrak{o}/\mathfrak{a}$ is distinct and $\mathfrak{o}/\mathfrak{a}$ is unmixed.*

PROOF. A base of $\mathfrak{a}$ of r elements is a subset of a system of parameters of $\mathfrak{o}$, which is distinct by our theorem. Therefore $\mathfrak{o}/\mathfrak{a}$ has distinct system of parameters.

COROLLARY 3. *Assume that a local ring $\mathfrak{o}$ is a finite module over a Noetherian subring $\mathfrak{r}$ and that $\mathfrak{o}$ has a linearly independent module base over $\mathfrak{r}$. If $\mathfrak{r}$ has a distinct system of parameters, then $\mathfrak{o}$ has also a distinct system of parameters and therefore any system of parameters of $\mathfrak{o}$ is distinct.*

PROOF. Let $\mathfrak{q}$ be the ideal of $\mathfrak{r}$ generated by a (distinct) system of parameters of $\mathfrak{r}$. Then $rm(\mathfrak{q}\mathfrak{o}; \mathfrak{r})=[\mathfrak{o}:\mathfrak{r}]\cdot e(\mathfrak{q})=[\mathfrak{o}:\mathfrak{r}]\cdot l(\mathfrak{r}/\mathfrak{q})=l(\mathfrak{o}/\mathfrak{q}\mathfrak{o}; \mathfrak{r})$, which show that $e(\mathfrak{q}\mathfrak{o})=l(\mathfrak{o}/\mathfrak{q}\mathfrak{o}; \mathfrak{o})$ and that the system of parameters which generates $\mathfrak{q}$ is a distinct system of parameters of $\mathfrak{o}$.

Though we have seen by Propositions 6 and 7 important characterization of distinct systems of parameters, we will now give another characterizations of the notion at the point of view of theory of ideals. In order to do it, we will introduce the notion of unmixedness theorem.

We say that the *unmixedness theorem* holds in a ring $\mathfrak{o}$ if the following condition is satisfied: If an ideal $\mathfrak{a}$ of $\mathfrak{o}$ is generated by r elements and if $\mathfrak{a}$ is of rank r (r may be zero; see foot-note 9)), then any prime divisor of $\mathfrak{a}$ is of rank r.

REMARK 1. By the above definition, we see that if the unmixedness theorem holds in a ring $\mathfrak{o}$, then 1) the prime divisor of zero is of rank zero, that is, the zero ideal has no imbedded prime divisor and

2) if $\mathfrak{a}$ is the ideal of $\mathfrak{o}$ generated by r elements and if rank $\mathfrak{a}=r$, then the unmixedness theorem holds also in $\mathfrak{o}/\mathfrak{a}$.

REMARK 2. In any ring of rank zero, the unmixedness theorem holds good. In a ring of rank 1, the theorem holds if and only if the zero ideal has no imbedded prime divisor. (Hence, in a local ring of rank 1, the theorem holds if and only if the maximal ideal is not a prime divisor of zero.)

THEOREM 5. *The unmixedness theorem holds in a local ring* $\mathfrak{o}$ *if and only if* $\mathfrak{o}$ *has a distinct system of parameters.*

PROOF. Assume that $\mathfrak{o}$ has a distinct system of parameters and let $\mathfrak{a}$ be the ideal generated by r elements and of rank r. Then $\mathfrak{o}/\mathfrak{a}$ is unmixed by Corollary 2 to Theorem 4, which show that any prime divisor $\mathfrak{p}$ of $\mathfrak{a}$ is of co-rank equal to rank $\mathfrak{o}-r$. Therefore rank $\mathfrak{p}$ is not greater than r. Since $\mathfrak{a}$ is of rank r, it follows that rank $\mathfrak{p}=r$.[14] Thus the unmixedness theorem holds in $\mathfrak{o}$. Conversely, assume that the unmixedness theorem holds in $\mathfrak{o}$. When $\mathfrak{o}$ is of rank zero, then the empty set is the distinct system of parameters. In the other case, we can construct a distinct system of parameters $x_1,\cdots,x_d$ in the following way: We can choose x_1 so that it is not a zero-divisor because prime divisors of zero are of rank zero. Since rank $x_1\mathfrak{o}=1$, the unmixedness theorem holds in $\mathfrak{o}/x_1\mathfrak{o}$ and we can choose x_2 so that x_2 is not a zero-divisor modulo $x_1\mathfrak{o}$. Repeating the same (or by induction argument), we can choose a system of parameters $x_1,\cdots,x_d$ so that each x_i is not a zero-divisor modulo $\sum_1^{i-1}x_j\mathfrak{o}$. Then $x_1,\cdots,x_d$ form a distinct system of parameters of $\mathfrak{o}$ by Proposition 7 and the proof is completed.

Combining Theorem 4, Theorem 5 and Proposition 7, we can derive many interesting results on the theory of ideals. We want to state here some of them in below.

We will first state a corollary to Theorem 5:

COROLLARY. *The unmixedness theorem holds in a local ring* $\mathfrak{o}$ *if and only if the theorem holds in the completion* $\mathfrak{o}^*$ *of* $\mathfrak{o}$.

PROOF. If $x_1,\cdots,x_d$ is a distict system of parameters of $\mathfrak{o}$, then it is a distinct system of parameters of $\mathfrak{o}^*$. Conversely, assume that $x_1^*,\cdots,x_d^*$ be a distinct system of parameters of $\mathfrak{o}^*$. Let $x_1,\cdots,x_d$ be elements of $\mathfrak{o}$ such that each $x_i-x_i^*$ is in $\mathfrak{m}\mathfrak{q}^*$, where $\mathfrak{m}$ is the maximal ideal of $\mathfrak{o}$ and $\mathfrak{q}^*$ is the ideal of $\mathfrak{o}^*$ generated by x_i^*'s. Let $\mathfrak{q}$ be the ideal of $\mathfrak{o}$ generated by x_i's. Then $\mathfrak{q}\mathfrak{o}^*+\mathfrak{m}\mathfrak{q}^*=\mathfrak{q}^*$ and we

[14] Observe that we have proved in the same time that for any prime ideal $\mathfrak{p}$ of $\mathfrak{o}$ rank $\mathfrak{p}$+co-rank $\mathfrak{p}$=rank $\mathfrak{o}$. We can prove easily further that any maximal chain of prime ideals in an unmixed local ring $\mathfrak{o}$ has length equal to rank $\mathfrak{o}$ (see Nagata [12]).

have $\mathfrak{q}\mathfrak{o}^*=\mathfrak{q}^*$. Hence $x_1,\cdots,x_d$ is a distinct system of parameters of both $\mathfrak{o}^*$ and $\mathfrak{o}$. Thus we see our assertion by virtue of Theorem 5.

PROPOSITION 8. *The unmixedness theorem holds in a Noetherian ring* $\mathfrak{o}$ *if and only if it holds in the ring* $\mathfrak{o}_{\mathfrak{m}}$ *of quotients of with respect to any maximal ideal* $\mathfrak{m}$ *of* $\mathfrak{o}$.

PROOF. The if part is immediate from the definition and we will prove the only if part. Assume that the unmixedness theorem holds in $\mathfrak{o}$ and let $\mathfrak{m}$ be a maximal ideal of $\mathfrak{o}$ and let r be the rank of $\mathfrak{m}$. Then there exist elements $x_1,\cdots,x_r$ of $\mathfrak{m}$ such that $\sum_1^s x_i\mathfrak{o}$ is of rank s for any $s=1,\cdots,r$. Then $x_1,\cdots,x_r$ is a system of parameters of $\mathfrak{o}_{\mathfrak{m}}$ which satisfies the condition in Proposition 7 and we see the validity of the unmixedness theorem in $\mathfrak{o}_{\mathfrak{m}}$.

COROLLARY. *If the unmixedness theorem holds in a Noetherian ring* $\mathfrak{o}$, *then it holds in any ring of quotients of* $\mathfrak{o}$.

PROOF. By Proposition 8, we have only to treat the case of the ring of quotients of $\mathfrak{o}$ with respect to a prime ideal. Then the proof of such a case is the same as in Proposition 8.

PROPOSITION 9. *If the unmixedness theorem holds in a Noetherian ring* $\mathfrak{o}$, *then it holds in the polynomial ring over* $\mathfrak{o}$ *in a finite number of indeterminates.*

PROOF. Making use of induction argument on the number of indeterminates, we have only to prove the case of one indeterminate X. On the other hand, by Proposition 8, we have only to prove that if $\mathfrak{p}$ is a prime ideal $\mathfrak{o}[X]$, then the theorem holds in $\mathfrak{o}[X]_{\mathfrak{p}}$. Therefore, setting $\mathfrak{p}'=\mathfrak{p}\frown\mathfrak{o}$, we may assume that $\mathfrak{o}=\mathfrak{o}_{\mathfrak{p}'}$ by the corollary to Proposition 8. Let $\mathfrak{q}$ be the primary ideal of $\mathfrak{o}$ generated by a distinct system of parameters of $\mathfrak{o}$. If $\mathfrak{q}\mathfrak{o}[X]_{\mathfrak{p}}$ is a primary ideal belonging to the maximal ideal, then $\mathfrak{o}[X]_{\mathfrak{p}}=\mathfrak{o}(x)$ and we see the existence of distinct system of parameters of $\mathfrak{o}[X]_{\mathfrak{p}}$ in this case. In the other case, we have $\mathfrak{p}\mathfrak{o}[X]_{\mathfrak{p}}/\mathfrak{q}\mathfrak{o}[X]_{\mathfrak{p}}$ is of rank 1 and $\mathfrak{p}\mathfrak{o}[X]_{\mathfrak{p}}$ is not a prime divisor of $\mathfrak{q}\mathfrak{o}[X]_{\mathfrak{p}}$. Let x be an element of $\mathfrak{p}\mathfrak{o}[X]_{\mathfrak{p}}$ which is not a zero-divisor modulo $\mathfrak{q}\mathfrak{o}[X]_{\mathfrak{p}}$. Further let $x_1,\cdots,x_d$ be a distinct system of parameters which generates $\mathfrak{q}$. Then the system of parameters $x_1,\cdots,x_d$, x of $\mathfrak{o}[X]_{\mathfrak{p}}$ satisfies the condition in Proposition 7 and we see the existence of distinct system of parameters of $\mathfrak{o}[X]_{\mathfrak{p}}$. Thus the proof is completed.

REMARK 3. Though we stated the unmixedness theorem taking the notion of rank to be standard, we can state an equivalent condition as follows:

(i) In a local ring or more generally in a Noetherian ring whose any maximal ideal is of the same rank with the ring: Let d be the rank of the ring. If an ideal $\mathfrak{a}$ of the ring is generated by r elements and is of co-rank $d-r$, then any prime divisor of $\mathfrak{a}$ is of co-rank $d-r$.

(Indeed, in the case of local rings, we can see easily by the similar way as in the proof of Theorem 5 that the above condition is equivalent to the existence of distinct system of parameters.)

(ii) In the general Noetherian rings: If an ideal $\mathfrak{a}$ of a ring $\mathfrak{o}$ is generated by r elements, if $\mathfrak{m}$ is a maximal ideal containing $\mathfrak{a}$ and if rank $\mathfrak{m}/\mathfrak{a}$ is rank $\mathfrak{m}-r$, then for any prime divisor $\mathfrak{p}$ of $\mathfrak{a}$ contained in $\mathfrak{m}$, rank $\mathfrak{m}/\mathfrak{p}=$ rank $\mathfrak{m}-r$.

§8. A characterization of regular local rings.

LEMMA 8.1. *Let $\mathfrak{o}$ be a complete local integrity domain and let x be a transcendental element over $\mathfrak{o}$. Then $\mathfrak{o}(x)$ is unmixed and analytically unramified.*[15]

PROOF. Let $\mathfrak{o}'$ be the derived normal ring of $\mathfrak{o}$. Since $\mathfrak{o}$ is complete, $\mathfrak{o}'$ is a finite $\mathfrak{o}$-module (see § 1) and is a local ring (see § 1). Therefore $\mathfrak{o}'(x)$ is the derived normal ring of $\mathfrak{o}(x)$ and $\mathfrak{o}'(x)$ is a finite $\mathfrak{o}(x)$-module. Hence $\mathfrak{o}(x)$ is a subspace of $\mathfrak{o}'(x)$ (see § 1). Therefore we have only to prove the assertion for $\mathfrak{o}'(x)$. Thus we way assume that $\mathfrak{o}$ is normal. Now we will prove the assertion by induction on the rank of $\mathfrak{o}$ (because when rank $\mathfrak{o}=0$, our assertion is obvious). Let a be an element of $\mathfrak{o}$ ($a\neq 0$, $a\mathfrak{o}\neq\mathfrak{o}$) and let $\mathfrak{p}_1,\cdots,\mathfrak{p}_n$ be all the prime divisors of $a\mathfrak{o}$. Then rank $\mathfrak{p}_i=1$ for any i because $\mathfrak{o}$ is normal. Since $\mathfrak{o}$ is complete, we have co-rank $\mathfrak{p}=$ rank $\mathfrak{o}-1$ (see § 1). Further by our induction assumption, each $\mathfrak{p}_i\mathfrak{o}(x)$ is analytically unramified and $\mathfrak{o}(x)/\mathfrak{p}_i\mathfrak{o}(x)$ is unmixed. From the analytical unramifiedness of $\mathfrak{p}_i\mathfrak{o}(x)$, we have the analytical unramifiedness of $\mathfrak{o}(x)$ and that any prime divisor $\mathfrak{P}^*$ of zero of the completion $\mathfrak{o}^*$ of $\mathfrak{o}(x)$ is contained in some divisor of some $\mathfrak{p}_i\mathfrak{o}^*$ (see § 1). By the unmixedness of $\mathfrak{o}(x)/\mathfrak{p}_i\mathfrak{o}(x)$, any prime divisor of $\mathfrak{p}_i\mathfrak{o}^*$ is of co-rank equal to rank $\mathfrak{o}-1$. Hence co-rank $\mathfrak{P}^*$ is not less than rank $\mathfrak{o}$, hence co-rank $\mathfrak{P}^*=$ rank $\mathfrak{o}$. Thus the proof is completed.

LEMMA 8.2. *Let $\mathfrak{o}^*$ be the completion of a semi-local ring $\mathfrak{o}$. If $\mathfrak{q}$ is a primary ideal belonging to a prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, then any prime divisor of $\mathfrak{q}\mathfrak{o}^*$ is contained in some prime divisor of $\mathfrak{p}\mathfrak{o}^*$.*

PROOF. We will prove the assertion by induction on $l(\mathfrak{p}\mathfrak{o}_{\mathfrak{p}}/\mathfrak{q}\mathfrak{p}_{\mathfrak{p}})$

[15] We can prove further that the completion of $\mathfrak{o}(x)$ is an integrity domain. But we need not prove it in the present paper and we shall not prove the fact. On the other hand, we can prove more generally the following: If a local ring $\mathfrak{o}$ is unmixed and if x is a transcendental element over $\mathfrak{o}$, then $\mathfrak{o}(x)$ is also unmixed. See Nagata [12].

(because it is one if and only if $\mathfrak{p}=\mathfrak{q}$ and in this case the assertion is obvious). On the other hand, we may assume that $\mathfrak{q}=0$ because $\mathfrak{o}^*/\mathfrak{q}\mathfrak{o}^*$ is the completion of $\mathfrak{o}/\mathfrak{q}$. Let $\mathfrak{q}'$ be a primary ideal which is minimal among non-zero primary ideal belonging to $\mathfrak{p}$. Then by our induction assumption, any prime divisor of $\mathfrak{q}'\mathfrak{o}^*$ is contained in some prime divisor of $\mathfrak{p}\mathfrak{o}^*$. Let a be a non-zero element of $\mathfrak{q}'$ and let S be the complementary set of $\mathfrak{p}$ with respect to $\mathfrak{o}$. Further let $\mathfrak{p}_1^*, \cdots, \mathfrak{p}_n^*$ be all the prime divisors of $\mathfrak{p}\mathfrak{o}^*$ and let b^* be any element of $\mathfrak{o}^*$ which is not in any of $\mathfrak{p}_i^*$. Assume that $\mathfrak{a}^*\mathfrak{b}^*=0$ $(\mathfrak{a}^* \in \mathfrak{o}^*)$ (and we have only to prove that $a^*=0$). Since every prime divisor of $\mathfrak{q}'\mathfrak{o}^*$ is contained in some of $\mathfrak{p}_i^*$'s, we have $a^* \in \mathfrak{q}'\mathfrak{o}^*$. Since $\mathfrak{q}'\mathfrak{o}_S=\mathfrak{q}'\mathfrak{o}_{\mathfrak{p}}=a\mathfrak{o}_{\mathfrak{p}}$, we have $\mathfrak{q}'\mathfrak{o}_S^*=a\mathfrak{o}_S^*$. Therefore there exists an element s of S such that $a^*s=aa^{**}$ $(a^{**} \in \mathfrak{o}^*)$. Since any element of S is not a zero-divisor in $\mathfrak{o}^*$ (by our assumption that $\mathfrak{q}=0$; see § 1), we have only to prove that $aa^{**}=0$. Since $0:a\mathfrak{o}^*=(0:a\mathfrak{o})\mathfrak{o}^*$ (see § 1), we have $0:a\mathfrak{o}^*=\mathfrak{p}\mathfrak{o}^*$ and $a^{**}b^* \in \mathfrak{p}\mathfrak{o}^*$. Since b^* is not in any prime divisor of $\mathfrak{p}\mathfrak{o}^*$, we have $a^{**} \in \mathfrak{p}\mathfrak{o}^*$ and $aa^{**}=0$. Thus the assertion is proved.

COROLLARY. *If $\mathfrak{o}$ is a complete local ring whose zero ideal is primary and if x is a trascendental element over $\mathfrak{o}$, then $\mathfrak{o}(x)$ is unmixed.*

THEOREM 6. *A local ring $\mathfrak{o}$ is regular if and only if it is of multiplicity one and unmixed.*[16]

PROOF. The only if part is obvious and we will prove the if part. When rank $\mathfrak{o}=0$, our assertion is obvious and we will prove the assertion by induction on the rank of $\mathfrak{o}$. Since we have only to prove that the completion of $\mathfrak{o}$ is regular (see § 1), we may assume that $\mathfrak{o}$ is complete (also by the definition of unmixedness). Let $\mathfrak{m}$ be the maximal ideal of $\mathfrak{o}$.

(1) If the zero ideal of $\mathfrak{o}$ has more than one prime divisors, then $m(\mathfrak{o})$ is greater than 1 by the theorem of additivity. Therefore the zero ideal is a primary ideal.[17]

(2) We will prove the case where $\mathfrak{o}/\mathfrak{m}$ contains infinitely many elements. Let x be a superficial element of $\mathfrak{m}$, (i) If $\mathfrak{o}$ is of rank 1, $e(x\mathfrak{o})=l(\mathfrak{o}/x\mathfrak{o})$, because x is not a zero-divisor (by Lemma 5.3), hence $x\mathfrak{o}=\mathfrak{m}$. Since in a Noetherian ring any principal ideal generated by an element of its J-radical cannot contain properly any prime ideal

[16] There are local integrity domains of multiplicity one which are not regular (see Nagata [12]).

[17] If we make use of the reduction theorem which will be proved in § 11 (in order to prove the theorem, we do not make use of the present Theorem 6), then we see immediately that $\mathfrak{o}$ is an integrity domain.

other than zero, we see that $\mathfrak{o}$ is an integrity domain and $\mathfrak{o}$ is a discrete valuation ring, namely, $\mathfrak{o}$ is a regular local ring. (ii) Now we assume that $\mathfrak{o}$ is of rank greater than 1. By Lemma 5.4, we have $m(\mathfrak{o}/x\mathfrak{o})=1$. Since any minimal prime divisor $x\mathfrak{o}$ is of rank 1, it is of co-rank equal to rank $\mathfrak{o}-1$ (because $\mathfrak{o}$ is complete). Let $\mathfrak{p}$ be the intersection of the primary components of $x\mathfrak{o}$ belonging to minimal prime divisors of $x\mathfrak{o}$. Then by the theorem of additivity we have $m(\mathfrak{o}/\mathfrak{p})=1$. Since $\mathfrak{o}/\mathfrak{p}$ is unmixed, $\mathfrak{o}/\mathfrak{p}$ is a regular local ring by our induction assumption and $\mathfrak{p}$ is a prime ideal. By the primeness of $\mathfrak{p}$, we see that $x\mathfrak{o}=\mathfrak{p}\mathfrak{o}_{\mathfrak{p}}$. By the same reason stated above, we see that $\mathfrak{o}_{\mathfrak{p}}$ is a discrete valuation ring. Let $\mathfrak{P}$ be the prime divisor of zero of $\mathfrak{o}$. Then we have $\mathfrak{P}\mathfrak{o}_{\mathfrak{p}}=0$. Since the zero-ideal of $\mathfrak{o}$ is primary, that $\mathfrak{P}\mathfrak{o}_{\mathfrak{p}}=0$ shows that $\mathfrak{P}=0$ and we see that $\mathfrak{o}$ is an integrity domain. Let $\mathfrak{o}'$ be the derived normal ring of $\mathfrak{o}$. Then by Corollary 1 to the extension formula, we have $rm(\mathfrak{m}\mathfrak{o}';\mathfrak{o})=1$, which shows that $\mathfrak{o}'$ is of multiplicity one, $e(\mathfrak{m}\mathfrak{o}')=1$ and, denoting by $\mathfrak{m}'$ the maximal ideal of $\mathfrak{q}'$, $\mathfrak{o}'/\mathfrak{m}'=\mathfrak{o}/\mathfrak{m}$. Let y be a superficial element of $\mathfrak{m}'$. Then, since $y\mathfrak{o}'$ has no imbedded prime divisor, applying the above observation on $\mathfrak{o}$ to $\mathfrak{o}'$, we see that $y\mathfrak{o}'$ is a prime ideal and $\mathfrak{o}'/y\mathfrak{o}'$ is regular, which shows that $\mathfrak{o}'$ is regular. Let $\mathfrak{q}$ be the ideal of $\mathfrak{o}$ generated by a system of parameters such that $e(\mathfrak{q})=1$. Then we have $e(\mathfrak{q}\mathfrak{o}')=1$. Since $\mathfrak{o}'$ is regular, $e(\mathfrak{q}\mathfrak{o}')=l(\mathfrak{o}'/\mathfrak{q}\mathfrak{o}')$ (because $\mathfrak{q}$ is generated by a distinct system of parameters of $\mathfrak{o}'$ by Corollary 1 to Theorem 4). Therefore we have $\mathfrak{q}\mathfrak{o}'=\mathfrak{m}'$ and in particular $\mathfrak{m}\mathfrak{o}'=\mathfrak{m}'$. Since $\mathfrak{o}/\mathfrak{m}=\mathfrak{o}'/\mathfrak{m}'$, we have $\mathfrak{o}=\mathfrak{o}'$. Thus $\mathfrak{o}$ is a regular local ring.

(3) Now we treat the case where $\mathfrak{o}/\mathfrak{m}$ contains only a finite number of elements. Let x be a transcendental element over $\mathfrak{o}$. We have only to show that $\mathfrak{o}(x)$ is regular (see § 1). By Proposition 5, we have $m(\mathfrak{o}(x))=1$. By the corollary to Lemma 8.2, we see that $\mathfrak{o}(x)$ is unmixed. Therefore by (2) we see that $\mathfrak{o}(x)$ is regular and the proof is completed.

§ 9. The theorem of transition.

THEOREM 7 (THE THEOREM OF TRANSITION). *Let $\mathfrak{o}^*$ be the completion of a local ring $\mathfrak{o}$, let $\mathfrak{q}$ be a primary ideal of $\mathfrak{o}$ with prime divisor $\mathfrak{p}$ and let $\mathfrak{p}^*$ be a minimal prime divisor of $\mathfrak{p}\mathfrak{o}^*$. Set $m(\mathfrak{p}^*)=l(\mathfrak{o}^*_{\mathfrak{p}^*}/\mathfrak{p}\mathfrak{o}^*_{\mathfrak{p}^*})$. Then we have $l(\mathfrak{o}^*_{\mathfrak{p}^*}/\mathfrak{q}\mathfrak{o}^*_{\mathfrak{p}^*})=m(\mathfrak{p}^*)\cdot l(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{q}\mathfrak{o}_{\mathfrak{p}})$, $\sigma(\mathfrak{q}\mathfrak{o}^*_{\mathfrak{p}^*};n)=m(\mathfrak{p}^*)\cdot\sigma(\mathfrak{q}\mathfrak{o}_{\mathfrak{p}};n)$ and $e(\mathfrak{q}\mathfrak{o}^*_{\mathfrak{p}^*})=m(\mathfrak{p}^*)\cdot e(\mathfrak{q}\mathfrak{o}_{\mathfrak{p}})$.*

PROOF. The second equality follows from the first one because it is also true of $\mathfrak{q}^n\mathfrak{o}_{\mathfrak{p}}\frown\mathfrak{o}$ for any n and the third equality follows from the second immediately. We will prove the first equality by induction on $l(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{q}\mathfrak{o}_{\mathfrak{p}})$. We may assume without loss of generality that $\mathfrak{q}=0$ because $\mathfrak{o}^*/\mathfrak{q}\mathfrak{o}^*$ is the completion of $\mathfrak{o}/\mathfrak{q}$. Let $\mathfrak{q}'$ be a primary ideal which is minimal among those belonging to $\mathfrak{p}$ and different from zero. Let a be a non-zero element of $\mathfrak{q}'$. Then $0:a\mathfrak{o}=\mathfrak{p}$ and $\mathfrak{q}'\mathfrak{o}_{\mathfrak{p}}=a\mathfrak{o}_{\mathfrak{p}}$. Therefore we have $0:a\mathfrak{o}^*=\mathfrak{p}\mathfrak{o}^*$ (see § 1) and $\mathfrak{q}'\mathfrak{o}^*_{\mathfrak{p}^*}=a\mathfrak{o}^*_{\mathfrak{p}^*}$. Therefore we see that $a\mathfrak{o}^*_{\mathfrak{p}^*}$ is a faithful $(\mathfrak{o}^*_{\mathfrak{p}^*}/\mathfrak{p}\mathfrak{o}^*_{\mathfrak{p}^*})$-module generated by one element, which shows that $l(a\mathfrak{o}^*_{\mathfrak{p}^*})=m(\mathfrak{p}^*)$. Since by our induction-assumption $l(\mathfrak{o}^*_{\mathfrak{p}^*}/\mathfrak{q}'\mathfrak{o}^*_{\mathfrak{p}^*})=m(\mathfrak{p}^*)\cdot l(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{q}'\mathfrak{o}_{\mathfrak{p}})$ and since $l(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{q}'\mathfrak{o}_{\mathfrak{p}})=l(\mathfrak{o}_{\mathfrak{p}})-1$, we see the assertion.

COROLLARY 1. *If* $\mathfrak{p}$ *is analytically unramified, then* $l(\mathfrak{o}^*_{\mathfrak{p}^*}/\mathfrak{q}'\mathfrak{o}^*_{\mathfrak{p}^*})=l(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{q}\mathfrak{o}_{\mathfrak{p}})$ *and* $e(\mathfrak{q}\mathfrak{o}_{\mathfrak{p}})=e(\mathfrak{q}\mathfrak{o}^*_{\mathfrak{p}^*})$.

COROLLARY 2. *Let* $\mathfrak{p}$ *be a prime ideal of a local ring* $\mathfrak{o}$ *and let* $\mathfrak{o}^*$ *be the completion of* $\mathfrak{o}$. *If* $\mathfrak{p}^*$ *is a minimal prime divisor of* $\mathfrak{p}\mathfrak{o}^*$, *then* $\operatorname{rank}\mathfrak{p}=\operatorname{rank}\mathfrak{p}^*$.

COROLLARY 3. *If a local ring* $\mathfrak{o}$ *is unmixed, then for any prime ideal* $\mathfrak{p}$ *of* $\mathfrak{o}$, $\operatorname{rank}\mathfrak{p}+\text{co-rank}\,\mathfrak{p}=\operatorname{rank}\mathfrak{o}$. (Nishi [13])

PROOF. Let $\mathfrak{o}^*$ be the completion of $\mathfrak{o}$. Then there exists a prime divisor $\mathfrak{p}^*$ of $\mathfrak{p}\mathfrak{o}^*$ such that $\text{co-rank}\,\mathfrak{p}=\text{co-rank}\,\mathfrak{p}^*$ because $\mathfrak{o}^*/\mathfrak{p}\mathfrak{o}^*$ is the completion of $\mathfrak{o}/\mathfrak{p}$. By Corollary 2, $\operatorname{rank}\mathfrak{p}=\operatorname{rank}\mathfrak{p}^*$. Since any prime divisor of zero of $\mathfrak{o}^*$ is of co-rank equal to rank $\mathfrak{o}$, $\operatorname{rank}\mathfrak{p}^*+\text{co-rank}\,\mathfrak{p}^*=\operatorname{rank}\mathfrak{o}$ and the assertion is proved.

REMARK. Since $\operatorname{rank}\mathfrak{p}^*+\text{co-rank}\,\mathfrak{p}^*=\operatorname{rank}\mathfrak{o}$ and $\operatorname{rank}\mathfrak{p}^*=\operatorname{rank}\mathfrak{p}$ for any minimal prime divisor $\mathfrak{p}^*$ of $\mathfrak{p}\mathfrak{o}^*$, we see immediately that $\text{co-rank}\,\mathfrak{p}^*=\text{co-rank}\,\mathfrak{p}$ for any minimal prime divisor of $\mathfrak{p}\mathfrak{o}^*$.

§ 10. The associativity formula.

THEOREM 8 (THE ASSOCIATIVITY FORMULA). *Let* $x_1,\cdots,x_d$ *be a system of parameters of a local ring* $\mathfrak{o}$ *and set* $\mathfrak{q}=\sum_1^d x_i\mathfrak{o}$, $\mathfrak{a}=\sum_1^s x_i\mathfrak{o}$. *Then we have*

$$e(\mathfrak{q})=\sum_{\mathfrak{p}} e(\mathfrak{a}\mathfrak{o}_{\mathfrak{p}})\cdot e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p}),$$

where $\mathfrak{p}$ *runs over all (minimal) prime divisors of* $\mathfrak{a}$ *such that* $\text{co-rank}\,\mathfrak{p}=d-s$ *and* $\operatorname{rank}\mathfrak{p}=s$.

In the present paragraph, we will prove only the case where $\mathfrak{o}$ is a complete local integrity domain. The general case will be proved in § 12.

(1) When $\mathfrak{o}$ contains a field: $\mathfrak{o}$ contains a coefficient field $\mathfrak{k}$ (see § 1). Let $\mathfrak{r}$ be the set of elements of $\mathfrak{o}$ which are expressible as power series in $x_1,\cdots,x_d$ with coefficients in $\mathfrak{k}$. Then $\mathfrak{r}$ is a regular local ring and $\mathfrak{o}$ is a finite $\mathfrak{r}$-module. Since $\mathfrak{o}$ and $\mathfrak{r}$ have the same residue class field $\mathfrak{k}$, we have by the extension formula that $e(\mathfrak{q})=[\mathfrak{o}:\mathfrak{r}]$.

Set $\mathfrak{p}'=\sum_1^s x_i\mathfrak{r}$. Then $\mathfrak{p}'$ is a prime ideal of $\mathfrak{r}$. Let S be the complementary set of $\mathfrak{p}'$ with respect to $\mathfrak{r}$. Then we have $e(\mathfrak{q})=[\mathfrak{o}_S:\mathfrak{r}_{\mathfrak{p}'}]$ $=rm(\mathfrak{p}'\mathfrak{o}_S;\ \mathfrak{r}_{\mathfrak{p}'})/e(\mathfrak{p}'\mathfrak{r}_{\mathfrak{p}'})=rm(\mathfrak{p}'\mathfrak{o}_S;\ \mathfrak{r}_{\mathfrak{p}'})=\sum_{\mathfrak{p}} e(\mathfrak{p}'\mathfrak{o}_{\mathfrak{p}})\cdot[\mathfrak{o}/\mathfrak{p}:\mathfrak{r}/\mathfrak{p}']$. Further $[\mathfrak{o}/\mathfrak{p}:\mathfrak{r}/\mathfrak{p}']=e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})$, because $\mathfrak{o}/\mathfrak{p}$ and $\mathfrak{r}/\mathfrak{p}'$ are in the same situation as $\mathfrak{o}$ and $\mathfrak{r}$ above. Thus the assertion is proved in this case.

(2) In order to treat the case where $\mathfrak{o}$ contains no field, we will begin from a special case where $\mathfrak{o}$ is an unramified regular local ring, $s=1$ and there exists an element u of $\mathfrak{o}$ such that $u, x_2, \cdots, x_d$ is a regular system of parameters of $\mathfrak{o}$.

Since x_i's form a distinct system of parameters by Corollary 1 to Theorem 4, we have $e(\mathfrak{q})=l(\mathfrak{o}/\mathfrak{q})$. Therefore $e(\mathfrak{q})$ is characterized by $u^{e(\mathfrak{q})}\in\mathfrak{q}$ and $u^{e(\mathfrak{q})-1}\notin\mathfrak{q}$, namely, if we express x_1 as a power series in $u, x_2, \cdots, x_d$ with coefficients in $\mathfrak{o}$ outside of $\mathfrak{m}$, then $e(\mathfrak{q})$ is the least degree of the term of the form (unit)$\cdot u^n$. Let $f_1^{j_1}\cdots f_t^{j_t}$ be the factorization of x_1 to the product of irreducible elements f_i (see § 1). Then the $\mathfrak{p}$'s in our theorem are the $f_i\mathfrak{o}$'s and $e(x_1\mathfrak{o}_{f_i\mathfrak{o}})=j_i$. On the other hand, $e((\mathfrak{q}+f_i\mathfrak{o})/f_i\mathfrak{o})$ is the least degree of the term of f_i of the form (unit)$\cdot u^n$. Therefore $e(\mathfrak{q})$ is the sum of $e(x_1\mathfrak{o}_{f_i\mathfrak{o}})\cdot e((\mathfrak{q}+f_i\mathfrak{o})/f_i\mathfrak{o})$ and the assertion is proved in this case.

(3) Now we consider the case where $\mathfrak{o}$ is a complete local integrity domain which does not contain any field. Let I be the coefficient ring of $\mathfrak{o}$ (see § 1) and let $\mathfrak{r}$ be the set of all elements of $\mathfrak{o}$ which are expressible as power series in x_i's with coefficients in I. Obviously $\mathfrak{r}$ is complete and $\mathfrak{o}$ is a finite $\mathfrak{r}$-module (see § 1). We first treat the case where $\mathfrak{r}=\mathfrak{o}$. Let $X_1, \cdots, X_d$ be indeterminates and consider the formal power series ring $\mathfrak{R}=I\{X_1, \cdots, X_d\}$. Then there exists an element f of $\mathfrak{R}$ such that $\mathfrak{R}/f\mathfrak{R}=\mathfrak{r}$ (x_i is the residue class of X_i). Set $\mathfrak{Q}=f\mathfrak{R}+\sum_1^d X_i\mathfrak{R}$, $\mathfrak{A}=f\mathfrak{R}+\sum_1^s X_i\mathfrak{R}$ and $\mathfrak{N}=\sum_1^s X_i\mathfrak{R}$. Since $f, X_1, \cdots, X_d$ form a distinct system of parameters of $\mathfrak{R}$, we have $e(\mathfrak{q})=e(\mathfrak{Q})=e(\mathfrak{Q}/\mathfrak{N})$ $(=l(\mathfrak{o}/\mathfrak{q}))$. Let $\mathfrak{P}_1, \cdots, \mathfrak{P}_t$ be all of prime divisors of $\mathfrak{A}$ ($\mathfrak{P}_i/f\mathfrak{R}$'s are all of $\mathfrak{p}$'s). Since $\mathfrak{R}_{\mathfrak{P}_i}$ is regular (see § 1), $f, X_1, \cdots, X_s$ form a distinct system of parameters of $\mathfrak{R}_{\mathfrak{P}_i}$. Therefore we have $e(\mathfrak{a}\mathfrak{r}_{\mathfrak{p}_i})=e(\mathfrak{A}\mathfrak{R}_{\mathfrak{P}_i})=$ $e(\mathfrak{A}\mathfrak{R}_{\mathfrak{P}_i}/\mathfrak{N}\mathfrak{R}_{\mathfrak{P}_i})$, where $\mathfrak{p}_i=\mathfrak{P}_i/f\mathfrak{R}$. If we apply the result in (2) to $\mathfrak{R}/\mathfrak{N}$, we have $e(\mathfrak{Q}/\mathfrak{N})=\sum_i e(\mathfrak{A}\mathfrak{R}_{\mathfrak{P}_i}/\mathfrak{N}\mathfrak{R}_{\mathfrak{P}_i})\cdot e((\mathfrak{Q}+\mathfrak{P}_i)/\mathfrak{P}_i)$. Since $e(\mathfrak{q})=e(\mathfrak{Q}/\mathfrak{N})$ and since $e(\mathfrak{a}\mathfrak{r}_{\mathfrak{p}_i})=e(\mathfrak{A}\mathfrak{R}_{\mathfrak{P}_i}/\mathfrak{N}\mathfrak{R}_{\mathfrak{P}_i})$, we have the assertion in the case where $\mathfrak{r}=\mathfrak{o}$. Next we consider the case where $\mathfrak{r}\neq\mathfrak{o}$. Set $\mathfrak{a}'=\sum_1^s x_i\mathfrak{r}$ and $\mathfrak{q}'=\sum_1^d x_i\mathfrak{r}$ and let $\mathfrak{p}_1', \cdots, \mathfrak{p}_t'$ be all of (minimal) prime divisors of $\mathfrak{a}'$. Then the above observation shows that $e(\mathfrak{q}')=\sum_i e(\mathfrak{a}'\mathfrak{r}_{\mathfrak{p}'_i})\cdot e((\mathfrak{q}'+\mathfrak{p}_i')/\mathfrak{p}_i')$. Let $\mathfrak{m}'$ be the maximal ideal of $\mathfrak{r}$ and let S_i be the complementary set of $\mathfrak{p}_i'$ with respect to $\mathfrak{r}$. Since $\mathfrak{o}/\mathfrak{m}=\mathfrak{r}/\mathfrak{m}'$, $rm(\mathfrak{q};\mathfrak{r})=e(\mathfrak{q})$ and therefore $e(\mathfrak{q})=[\mathfrak{o}:\mathfrak{r}]\cdot e(\mathfrak{q}')=[\mathfrak{o}:\mathfrak{r}]\cdot(\sum_i e(\mathfrak{a}'\mathfrak{r}_{\mathfrak{p}'_i})\cdot e((\mathfrak{q}'+\mathfrak{p}_i')/\mathfrak{p}_i'))$. Further $e(\mathfrak{a}'\mathfrak{r}_{\mathfrak{p}_i})\cdot$

$[\mathfrak{o}:\mathfrak{r}]=rm(\mathfrak{a}\mathfrak{o}_{S_i};\mathfrak{r}_{\mathfrak{p}'_i})=\sum_{\mathfrak{p}\supset\mathfrak{p}'_i}[\mathfrak{o}/\mathfrak{p}:\mathfrak{r}/\mathfrak{p}'_i]\cdot e(\mathfrak{a}\mathfrak{o}_{\mathfrak{p}})$ and, considering $\mathfrak{o}/\mathfrak{p}$ and $\mathfrak{r}/\mathfrak{p}'_i$ for each pair $(\mathfrak{p}, \mathfrak{p}'_i)$ such that $\mathfrak{p}\supseteqq\mathfrak{p}'_i$ $(\mathfrak{p}\frown\mathfrak{r}=\mathfrak{p}'_i)$, we have $[\mathfrak{o}/\mathfrak{p}:\mathfrak{r}/\mathfrak{p}'_i]\cdot e((\mathfrak{q}'+\mathfrak{p}'_i)/\mathfrak{p}'_i)=rm((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})=e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})$ (because $\mathfrak{r}/\mathfrak{m}'=\mathfrak{o}/\mathfrak{m}$). Therefore we have the assertion also in this case. Thus the proof of the case where $\mathfrak{o}$ is a complete local integrity domain is completed.

§ 11. The reduction theorem.

LEMMA 11.1. *Let $\mathfrak{o}$ be a local ring and assume that the zero ideal is primary. Let $\mathfrak{m}$ be the maximal ideal of $\mathfrak{o}$ and let $\mathfrak{p}$ be the prime divisor of zero. If $\mathfrak{q}$ is a primary ideal belonging to $\mathfrak{m}$ and if $\mathfrak{n}$ is a primary ideal belonging to $\mathfrak{p}$ such that $l(\mathfrak{n}\mathfrak{o}_{\mathfrak{p}})=1$, then $e(\mathfrak{q})-e((\mathfrak{q}+\mathfrak{p})/\mathfrak{n})$ is not greater than $e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})$.*

PROOF. Let a be a non-zero element of $\mathfrak{n}$. Then $\mathfrak{n}\mathfrak{o}_{\mathfrak{p}}=a\mathfrak{o}_{\mathfrak{p}}$. Therefore by the theorem of additivity we have $e((\mathfrak{q}+\mathfrak{n})/\mathfrak{n})=e((a\mathfrak{o}+\mathfrak{q})/a\mathfrak{o})$. Set $\mathfrak{q}'=(\mathfrak{q}+a\mathfrak{o})/a\mathfrak{o}$. Then $\sigma(\mathfrak{q};n)-\sigma(\mathfrak{q}';n)=l(\mathfrak{o}/(\mathfrak{q}^n:a\mathfrak{o}))$ for sufficiently large n by Proposition 4. Obviously $\mathfrak{q}^n:a\mathfrak{o}$ contains $\mathfrak{p}+\mathfrak{q}^n$ and therefore we have $l(\mathfrak{o}/(\mathfrak{q}^n:a\mathfrak{o}))\leqq\sigma((\mathfrak{q}+\mathfrak{p})/\mathfrak{p};n)$ for sufficiently large n. Thus we have $\sigma(\mathfrak{q};n)-\sigma(\mathfrak{q}';n)\leqq\sigma((\mathfrak{q}+\mathfrak{p})/\mathfrak{p};n)$, which shows the required result.

From this result, we see easily, applying the same to $\mathfrak{o}/\mathfrak{n}$ and so on, the following fact:

$e(\mathfrak{q})$ is not greater than $l(\mathfrak{o}_{\mathfrak{p}})\cdot e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})$. If $e(\mathfrak{q})=l(\mathfrak{o}_{\mathfrak{p}})\cdot e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})$, then for any primary ideal $\mathfrak{n}'$ belonging to $\mathfrak{p}$, $e((\mathfrak{q}+\mathfrak{n}')/\mathfrak{n}')=l(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{n}'\mathfrak{o}_{\mathfrak{p}})\cdot e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})$.

Using this result, we prove the following

THEOREM 9 (THE REDUCTION THEOREM). *Let $\mathfrak{o}$ be a local ring with maximal ideal $\mathfrak{m}$ and assume that the zero ideal of $\mathfrak{o}$ is primary. Let $\mathfrak{p}$ be the prime divisor of zero. Then for any primary ideal $\mathfrak{q}$ belonging to $\mathfrak{m}$, $e(\mathfrak{q})=e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})\cdot l(\mathfrak{o}_{\mathfrak{p}})$.*

PROOF. (1) When $\mathfrak{o}/\mathfrak{m}$ contains only a finite number of elements, we consider $\mathfrak{o}(X)$ (X being a transcendental element over $\mathfrak{o}$). Then by Proposition 5, $e(\mathfrak{q})=e(\mathfrak{q}\mathfrak{o}(X))$, $e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})=e((\mathfrak{q}+\mathfrak{p})\mathfrak{o}(X)/\mathfrak{p}\mathfrak{o}(X))$ and $l(\mathfrak{o}_{\mathfrak{p}})=l(\mathfrak{o}(X)_{\mathfrak{p}\mathfrak{o}(X)})$. Therefore we may assume that $\mathfrak{o}/\mathfrak{m}$ contains infinitely many elements.

(2) When $\mathfrak{o}$ is complete: There exists an unramified complete regular local ring $\mathfrak{r}$ which has an ideal $\mathfrak{a}$ such that $\mathfrak{o}=\mathfrak{r}/\mathfrak{a}$. Let ϕ be the homomorphism from $\mathfrak{r}$ onto $\mathfrak{o}$ and set $\mathfrak{q}^*=\phi^{-1}(\mathfrak{q})$. Let $y_1,\cdots,y_s$ ($s=\text{rank }\mathfrak{o}$) be elements of $\mathfrak{q}^*$ such that the ideal $\mathfrak{q}'$ of $\mathfrak{o}$ generated by $\phi(y_i)$'s is a primary ideal belonging to $\mathfrak{m}$ and $e(\mathfrak{q})=e(\mathfrak{q}')$ (by Theorem 1). Then there exists elements $x_1,\cdots,x_r$ ($r=\text{rank }\mathfrak{a}=\text{rank }\mathfrak{r}-s$) of $\mathfrak{a}$ such that $x_1,\cdots,x_r,y_1,\cdots,y_s$ is a system of parameters of $\mathfrak{r}$. Then the ideal $\mathfrak{b}$, generated by $x_1,\cdots,x_r$, is contained in $\mathfrak{a}$ and of rank r. Since

$\mathfrak{r}$ is regular, $x_1, \cdots, x_r, y_1, \cdots, y_s$ is a distinct system of parameters by Corollary 1 to Theorem 4. We denote by $\mathfrak{q}''$ the ideal generated by y's. Now we apply the associativity formula to $\mathfrak{r}$. Then we have

$$e(\mathfrak{b}+\mathfrak{q}'')=\sum_{\mathfrak{P}} e(\mathfrak{b}\mathfrak{r}_{\mathfrak{P}})\cdot e((\mathfrak{q}''+\mathfrak{P})/\mathfrak{P}),$$

where $\mathfrak{P}$ runs over all prime divisors of $\mathfrak{b}$ (they are of co-rank s and of rank r by Theorem 5). Since $x_1, \cdots, x_r, y_1, \cdots, y_s$ is a distinct system of parameters, we have $e(\mathfrak{b}+\mathfrak{q}'')=e((\mathfrak{q}''+\mathfrak{b})/\mathfrak{b})$. Since $x_1, \cdots, x_r$ is a distinct system of parameters of $\mathfrak{r}_{\mathfrak{P}}$ (by the corollary to Proposition 8 or by the fact that $\mathfrak{r}_{\mathfrak{P}}$ is regular), $e(\mathfrak{b}\mathfrak{r}_{\mathfrak{P}})=l(\mathfrak{r}_{\mathfrak{P}}/\mathfrak{b}\mathfrak{r}_{\mathfrak{P}})$. Thus we have $e((\mathfrak{q}''+\mathfrak{b})/\mathfrak{b})=\sum_{\mathfrak{P}} l(\mathfrak{r}_{\mathfrak{P}}/\mathfrak{b}\mathfrak{r}_{\mathfrak{P}})\cdot e((\mathfrak{q}''+\mathfrak{P})/\mathfrak{P})$. Let $\mathfrak{Q}$ be the primary component of $\mathfrak{b}$ belonging to $\mathfrak{P}$. Then by the theorem of additivity, we have $e((\mathfrak{q}''+\mathfrak{b})/\mathfrak{b}) = \sum_{\mathfrak{Q}} e((\mathfrak{q}''+\mathfrak{Q})/\mathfrak{Q})$. Thus we have $\sum_{\mathfrak{Q}} e((\mathfrak{q}''+\mathfrak{Q})/\mathfrak{Q}) = \sum_{\mathfrak{P}} e((\mathfrak{q}''+\mathfrak{P})/\mathfrak{P})\cdot l(\mathfrak{r}_{\mathfrak{P}}/\mathfrak{Q}\mathfrak{r}_{\mathfrak{P}})$ (because $\mathfrak{Q}\mathfrak{r}_{\mathfrak{P}}=\mathfrak{b}\mathfrak{r}_{\mathfrak{P}}$ by the definition of $\mathfrak{Q}$). Then the observation after Lemma 11.1 can be applied to each $\mathfrak{r}/\mathfrak{Q}$ and we have, for any $\mathfrak{Q}$, that $e((\mathfrak{q}''+\mathfrak{Q})/\mathfrak{Q})=l(\mathfrak{r}_{\mathfrak{P}}/\mathfrak{Q}\mathfrak{r}_{\mathfrak{P}})e((\mathfrak{q}''+\mathfrak{P})/\mathfrak{P})$. Then this shows, applying the same to $\mathfrak{r}/\mathfrak{Q}$ ($\mathfrak{Q}$ being taken to be a primary ideal belonging to the same prime ideal with $\mathfrak{a}$), that $e((\mathfrak{q}''+\mathfrak{a})/\mathfrak{a}) = l(\mathfrak{r}_{\mathfrak{P}}/\mathfrak{a}\mathfrak{r}_{\mathfrak{P}})\cdot e((\mathfrak{q}''+\mathfrak{P})/\mathfrak{P}) = l(\mathfrak{o}_{\mathfrak{p}})\cdot e((\mathfrak{q}'+\mathfrak{p})/\mathfrak{p})$ and $e(\mathfrak{q}) = e(\mathfrak{q}') = l(\mathfrak{o}_{\mathfrak{p}})\cdot e((\mathfrak{q}'+\mathfrak{p})/\mathfrak{p})$. Since $e(\mathfrak{q}) \leqq l(\mathfrak{o}_{\mathfrak{P}})\cdot e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})$, we have $e((\mathfrak{q}'+\mathfrak{p})/\mathfrak{p}) \leqq e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})$. Since $\mathfrak{q}' \subseteqq \mathfrak{q}$, we have $e((\mathfrak{q}'+\mathfrak{p})/\mathfrak{p}) = e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})$ and the assertion is proved in this case.

(3) We will prove the general case. Let $\mathfrak{o}^*$ be the completion of $\mathfrak{o}$ and let $\mathfrak{p}_1^*, \cdots, \mathfrak{p}_t^*$ be all of prime divisors of zero of $\mathfrak{o}^*$ such that their co-rank are equal to rank $\mathfrak{o}$ and let $\mathfrak{q}_1^*, \cdots, \mathfrak{q}_t^*$ be the primary component of zero belonging to $\mathfrak{p}_1^*, \cdots, \mathfrak{p}_t^*$ respectively. Then by the theorem of additivity, we have $e(\mathfrak{q})=e(\mathfrak{q}\mathfrak{o}^*)=\sum_i e((\mathfrak{q}\mathfrak{o}^*+\mathfrak{q}_i^*)/\mathfrak{q}_i^*)$. Then applying the result in (2), we have $e(\mathfrak{q})=\sum_i e((\mathfrak{q}\mathfrak{o}^*+\mathfrak{p}_i^*)/\mathfrak{p}_i^*)\cdot l(\mathfrak{o}^*_{\mathfrak{p}^*_i})$. By the theorem of transition, we have $l(\mathfrak{o}^*_{\mathfrak{p}^*_i})=l(\mathfrak{o}^*_{\mathfrak{p}^*_i}/\mathfrak{p}\mathfrak{o}^*_{\mathfrak{p}^*_i})\cdot l(\mathfrak{o}_{\mathfrak{p}})$. Therefore $e((\mathfrak{q}\mathfrak{o}^*+\mathfrak{p}_i^*)/\mathfrak{p}_i^*)\cdot l(\mathfrak{o}^*_{\mathfrak{p}^*_i})=e((\mathfrak{q}\mathfrak{o}^*+\mathfrak{p}_i^*)/\mathfrak{p}_i^*)\cdot l(\mathfrak{o}^*_{\mathfrak{p}^*_i}/\mathfrak{p}\mathfrak{o}^*_{\mathfrak{p}^*_i})\cdot l(\mathfrak{o}_{\mathfrak{p}})$. On the other hand, applying the above result to the case where $\mathfrak{p}=0$, we have $e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p}) = \sum_i e((\mathfrak{q}\mathfrak{o}^*+\mathfrak{p}_i^*)/\mathfrak{p}_i^*)\cdot l(\mathfrak{o}^*_{\mathfrak{p}^*_i}/\mathfrak{p}\mathfrak{o}^*_{\mathfrak{p}^*_i})$. Therefore we have $e(\mathfrak{q})=e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})\cdot l(\mathfrak{o}_{\mathfrak{p}})$ and the assertion is proved completely.

COROLLARY 1. *Let $\mathfrak{o}$ be a local ring and let $\mathfrak{q}$ be a primary ideal belonging to the maximal ideal $\mathfrak{m}$ of $\mathfrak{o}$. Then we have*

$$e(\mathfrak{q})=\sum_{\mathfrak{p}} e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})\cdot l(\mathfrak{o}_{\mathfrak{p}}),$$

where $\mathfrak{p}$ runs over all prime ideal of $\mathfrak{o}$ such that co-rank $\mathfrak{p}=$ rank $\mathfrak{o}$.

The proof is immediate from the theorem of additivity and our reduction theorem.

COROLLARY 2. *Let $\mathfrak{o}$ and $\mathfrak{q}$ be the same as above Corollary 1 and let $\mathfrak{n}$ be the radical of $\mathfrak{o}$. Then $e(\mathfrak{q})=e(\mathfrak{q}+\mathfrak{n})$.*

For, in the formula in Corollary 1, the right side does not change under the replacement of $\mathfrak{q}$ by $\mathfrak{q}+\mathfrak{n}$.

§ 12. Continuation of the proof of the associativity formula.

Now we will prove the general case of the associativity formula.

(1) When $\mathfrak{o}$ is complete: Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_h$ be all of prime divisors of zero of $\mathfrak{o}$ such that their co-rank are equal to rank $\mathfrak{o}$. Then by the reduction theorem, we have $e(\mathfrak{q})=\sum_i e((\mathfrak{q}+\mathfrak{p}_i)/\mathfrak{p}_i)\cdot l(\mathfrak{o}_{\mathfrak{p}_i})$, $e(\mathfrak{a}\mathfrak{o}_{\mathfrak{p}})=\sum_{\mathfrak{p}_i\subset\mathfrak{p}} e((\mathfrak{a}+\mathfrak{p}_i)\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}_i\mathfrak{o}_{\mathfrak{p}})\cdot l(\mathfrak{o}_{\mathfrak{p}_i})$. Since $e((\mathfrak{q}+\mathfrak{p}_i)/\mathfrak{p}_i)=\sum_{\mathfrak{p}\supset\mathfrak{p}_i} e((\mathfrak{a}+\mathfrak{p}_i)\mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}_i\mathfrak{o}_{\mathfrak{p}})\cdot e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})$ for each i, by the observation in § 10, we have the required result easily.

(2) The non-complete case: Let $\mathfrak{o}^*$ be the completion of $\mathfrak{o}$. Then by (1) we have $e(\mathfrak{q})=e(\mathfrak{q}\mathfrak{o}^*)=\sum_{\mathfrak{p}^*} e(\mathfrak{a}\mathfrak{o}^*_{\mathfrak{p}^*})\cdot e((\mathfrak{q}\mathfrak{o}^*+\mathfrak{p}^*)/\mathfrak{p}^*)$, where $\mathfrak{p}^*$ runs over prime divisors of $\mathfrak{a}\mathfrak{o}^*$ such that their co-rank are equal to $d-s$ and they contain some prime divisors of zero of co-rank d (such $\mathfrak{p}^*$ must be of rank s because $\mathfrak{o}^*$ is complete). By the theorem of transition $e(\mathfrak{a}\mathfrak{o}^*_{\mathfrak{p}^*})=e(\mathfrak{a}\mathfrak{o}_{\mathfrak{p}})\cdot l(\mathfrak{o}^*_{\mathfrak{p}^*}/\mathfrak{p}\mathfrak{o}^*_{\mathfrak{p}^*})$ for any minimal prime divisor $\mathfrak{p}^*$ of $\mathfrak{p}\mathfrak{o}^*$; observe that our $\mathfrak{p}^*$'s in the former summation are minimal prime divisors $\mathfrak{p}\mathfrak{o}^*$'s. Since rank $\mathfrak{p}=$ rank $\mathfrak{p}^*$ for any minimal prime divisor $\mathfrak{p}^*$ of $\mathfrak{p}\mathfrak{o}^*$ by Corollary 2 to the theorem of transition, we see that a minimal prime divisor $\mathfrak{p}^*$ of $\mathfrak{p}\mathfrak{o}^*$ appears in the above summation if and only if it is of co-rank $d-s$. Hence $e((\mathfrak{q}+\mathfrak{p})/\mathfrak{p})=e((\mathfrak{q}+\mathfrak{p})\mathfrak{o}^*/\mathfrak{p}\mathfrak{o}^*)$ $=\sum_{\mathfrak{p}^*} e((\mathfrak{q}\mathfrak{o}^*+\mathfrak{p}^*)/\mathfrak{p}^*)\cdot l(\mathfrak{o}^*_{\mathfrak{p}^*}/\mathfrak{p}\mathfrak{o}^*_{\mathfrak{p}^*})$, where $\mathfrak{p}^*$ runs over all minimal prime divisors of $\mathfrak{p}\mathfrak{o}^*$ which appears in the former summation. Therefore we have the required equality and the proof of the associativity formula is completed.

§ 13. Multiplicity of rings of quotients.

THEOREM 10. *Let $\mathfrak{p}$ be a prime ideal of a local ring $\mathfrak{o}$. If* rank $\mathfrak{p}+$co-rank $\mathfrak{p}=$ rank $\mathfrak{o}$ *and if $\mathfrak{p}$ is analytically unramified, then the multiplicity of $\mathfrak{o}_{\mathfrak{p}}$ is not greater than that of $\mathfrak{o}$.*

PROOF. Let $\mathfrak{m}$ be the maximal ideal of $\mathfrak{o}$. If $\mathfrak{o}/\mathfrak{m}$ contains only a finite number of elements, then let x be a transcendental element over $\mathfrak{o}$ and consider $\mathfrak{o}(x)$. By Proposition 5, $m(\mathfrak{o})=m(\mathfrak{o}(x))$ and, observing that $\mathfrak{o}(x)_{\mathfrak{p}\mathfrak{o}(x)}=\mathfrak{o}_{\mathfrak{p}}(x)$, $m(\mathfrak{o}_{\mathfrak{p}})=m(\mathfrak{o}(x)_{\mathfrak{p}\mathfrak{o}(x)})$. Therefore we may assume that $\mathfrak{o}/\mathfrak{m}$ contains infinitely many elements.

(1) When $\mathfrak{o}$ is a complete local integrity domain: Let $x_1, \cdots, x_d$ be a system of parameters of $\mathfrak{o}$ such that $m(\mathfrak{o})=e(\mathfrak{q})$ with the ideal $\mathfrak{q}$ generated by x_i's and let I be the coefficient ring of $\mathfrak{o}$. Let $\mathfrak{r}$ be the set of elements of $\mathfrak{o}$ which are expressible as power series in $x_1, \cdots, x_d$ with coefficients in I. $\mathfrak{r}$ is a complete local integrity domain

and $\mathfrak{o}$ is a finite $\mathfrak{r}$-module. Set $\mathfrak{p}'=\mathfrak{p}\frown\mathfrak{r}$ and $\mathfrak{m}'=\mathfrak{m}\frown\mathfrak{r}$. Further let S be the complementary set of $\mathfrak{p}'$ with respect to $\mathfrak{r}$.

(i) When I is a field: In this case, $\mathfrak{r}$ is a regular local ring. Since $e(\mathfrak{m}')=1$, $\mathfrak{o}/\mathfrak{m}=\mathfrak{r}/\mathfrak{m}'$ and $\mathfrak{m}'\mathfrak{o}=\mathfrak{q}$, we have $e(\mathfrak{q})=rm(\mathfrak{q};\mathfrak{r})=[\mathfrak{o}:\mathfrak{r}]=[\mathfrak{o}_S:\mathfrak{r}_{\mathfrak{p}'}]=rm(\mathfrak{p}'\mathfrak{o}_S;\mathfrak{r}_{\mathfrak{p}'})/e(\mathfrak{p}'\mathfrak{r}_{\mathfrak{p}'})=rm(\mathfrak{p}'\mathfrak{o}_S;\mathfrak{r}_{\mathfrak{p}'})$ (because $\mathfrak{r}_{\mathfrak{p}'}$ is regular (see §1)). Since $rm(\mathfrak{p}'\mathfrak{o}_S;\mathfrak{r}_{\mathfrak{p}'})$ is not less than $e(\mathfrak{p}'\mathfrak{o}_{\mathfrak{p}})\geqq e(\mathfrak{p}\mathfrak{o}_{\mathfrak{p}})$, we have the assertion in this case.

(ii) When I is not a field: Let $X_1,\cdots,X_d$ be indeterminates and consider the formal power series ring $\mathfrak{R}=I\{X_1,\cdots,X_d\}$. Then there exists an element f of $\mathfrak{R}$ such that $\mathfrak{r}=\mathfrak{R}/f\mathfrak{R}$ (where x_i is the residue class of X_i). Let ϕ be the homomorphism from $\mathfrak{R}$ onto $\mathfrak{r}$ and set $\mathfrak{P}'=\phi^{-1}(\mathfrak{p}')$. Since $\mathfrak{R}$ is a regular local ring $\mathfrak{R}_{\mathfrak{P}'}$ is a regular local ring (see §1). Further the degree of f with respect to the maximal ideal of $\mathfrak{R}$ is not less than the degree of f with respect to $\mathfrak{P}'\mathfrak{R}_{\mathfrak{P}'}$ (see §1). Since $f, X_1,\cdots,X_d$ is a distinct system of parameters of $\mathfrak{R}$ by Corollary 1 to Theorem 4, we have $e(f\mathfrak{R}+\sum_1^d X_i\mathfrak{R})=e(\sum x_i\mathfrak{r})=l(\mathfrak{r}/\sum x_i\mathfrak{r})\geqq$(degree of f with respect to the maximal ideal of $\mathfrak{R}$). On the other hand, since $\mathfrak{R}_{\mathfrak{P}'}$ is regular, $e(\mathfrak{p}'\mathfrak{r}_{\mathfrak{p}'})=e(\mathfrak{P}'\mathfrak{R}_{\mathfrak{P}'}/f\mathfrak{R}_{\mathfrak{P}'})$ is equal to the degree of f with respect to $\mathfrak{P}'\mathfrak{R}_{\mathfrak{P}'}$ as is easily seen. Thus we see that $m(\mathfrak{r}_{\mathfrak{p}'})$ is not greater than $e(\sum x_i\mathfrak{r})$. Now, $e(\mathfrak{m})=e(\mathfrak{q})=rm(\mathfrak{q};\mathfrak{r})=[\mathfrak{o}:\mathfrak{r}]\cdot e(\sum x_i\mathfrak{r})\geqq[\mathfrak{o}_S:\mathfrak{r}_{\mathfrak{p}'}]\cdot e(\mathfrak{p}'\mathfrak{r}_{\mathfrak{p}'})=rm(\mathfrak{p}'\mathfrak{o}_S;\mathfrak{r}_{\mathfrak{p}'})\geqq e(\mathfrak{p}'\mathfrak{o}_S)\geqq e(\mathfrak{p}\mathfrak{o}_{\mathfrak{p}})$. Thus the proof of this case is completed.

(2) When $\mathfrak{o}$ is complete: Let $\mathfrak{P}_1,\cdots,\mathfrak{P}_r$ be all of prime divisors of zero such that their co-rank are equal to rank $\mathfrak{o}$; we renumber them so that $\mathfrak{P}_i\subseteqq\mathfrak{p}$ if and only if $i\leqq s$. Then by Corollary 1 to the reduction theorem, we have $m(\mathfrak{o})=\sum_1^r m(\mathfrak{o}/\mathfrak{p}_i)\cdot l(\mathfrak{o}_{\mathfrak{P}_i})$ and $m(\mathfrak{o}_{\mathfrak{p}})=\sum_1^s m(\mathfrak{o}_{\mathfrak{p}}/\mathfrak{P}_i\mathfrak{o}_{\mathfrak{p}})\cdot l(\mathfrak{o}_{\mathfrak{P}_i})$. Then we have the assertion by (1) (applying the result to $\mathfrak{o}/\mathfrak{P}_i$).

(3) Now we will prove the general case. Let $\mathfrak{o}^*$ be the completion of $\mathfrak{o}$ and let $\mathfrak{p}^*$ be a minimal prime divisor of $\mathfrak{p}\mathfrak{o}^*$ such that co-rank $\mathfrak{p}=$co-rank $\mathfrak{p}^*$. By Corollary 2 to the theorem of transition, rank $\mathfrak{p}=$rank $\mathfrak{p}^*$. Hence rank $\mathfrak{p}^*+$co-rank $\mathfrak{p}^*=$ rank $\mathfrak{o}^*$ and we have $m(\mathfrak{o}^*)\geqq m(\mathfrak{o}^*_{\mathfrak{p}^*})$. Obviously $m(\mathfrak{o})=m(\mathfrak{o}^*)$. On the other hand, since $\mathfrak{p}$ is analytically unramified, we have $m(\mathfrak{o}_{\mathfrak{p}})=m(\mathfrak{o}^*_{\mathfrak{p}^*})$ by Corollary 1 to the theorem of transition. Thus we see the assertion.

COROLLARY. *If* $\mathfrak{o}$ *is a regular local ring and if a prime ideal* $\mathfrak{p}$ *of* $\mathfrak{o}$ *is analytically unramified, then* $\mathfrak{o}_{\mathfrak{p}}$ *is also a regular local ring. If furthermore* $\mathfrak{o}$ *is unramified, then* $\mathfrak{o}_{\mathfrak{p}}$ *is also unramified.*

PROOF. Since $m(\mathfrak{o})=1$, we have $m(\mathfrak{o}_{\mathfrak{p}})=1$. Since $\mathfrak{o}$ and therefore also $\mathfrak{o}_{\mathfrak{p}}$ have distinct system of parameters, $\mathfrak{o}_{\mathfrak{p}}$ is unmixed (see §7). Therefore $\mathfrak{o}_{\mathfrak{p}}$ is regular by Theorem 6. For the last assertion, see §1.

§ 14. Complete tensor products.

A subring B of a semi-local ring $\mathfrak{o}$ is called a *basic ring* of $\mathfrak{o}$ if 1) B is a homomorphic image of a discrete valuation ring and 2) any maximal ideal $\mathfrak{p}$ of $\mathfrak{o}$ lies over the maximal ideal $\mathfrak{n}$ of B and $\mathfrak{o}/\mathfrak{p}$ is a finite algebraic extension of $B/\mathfrak{n}$. Let $\mathfrak{o}$ and $\mathfrak{o}'$ be semi-local rings which have the same basic ring B. Let $\mathfrak{o}''$ be the tensor product of $\mathfrak{o}$ and $\mathfrak{o}'$ over B and let $\mathfrak{M}(n)$ be the ideal of $\mathfrak{o}''$ generated by $\mathfrak{m}^n$ and $\mathfrak{m}'^n$, where $\mathfrak{m}$ and $\mathfrak{m}'$ denote the J-radicals of $\mathfrak{o}$ and $\mathfrak{o}'$ respectively. Then the limit space of the inverse system $\{\mathfrak{o}''/\mathfrak{M}(n); n=1, 2, \cdots\}$ is called the *complete tensor product* of $\mathfrak{o}$ and $\mathfrak{o}'$ over B. As was shown in [11, II], this notion corresponds to the notion of Kronecker product of $\mathfrak{o}$ and $\mathfrak{o}'$ over B in the sense of Chevalley [2], namely, when $\mathfrak{o}$ and $\mathfrak{o}'$ are complete local rings and if B is a field, then $\mathfrak{o}^*$ is the Kronecker product in his sense.

PROPOSITION 11. *Assume that $\mathfrak{o}$ and $\mathfrak{o}'$ are local rings and that B is a field. Then for any primary ideals $\mathfrak{q}$ and $\mathfrak{q}'$ belonging to $\mathfrak{m}$ and $\mathfrak{m}'$ respectively, we have*

$$rm(\mathfrak{q}\mathfrak{o}^*+\mathfrak{q}'\mathfrak{o}^*; B)=rm(\mathfrak{q}; B)\cdot rm(\mathfrak{q}'; B).$$

PROOF.[18] We shall use the notation $l(\ \ )$ in the sense of $l(\ \ ; B)$. Set $f(i)=l(\mathfrak{q}^i/\mathfrak{q}^{i+1})$ and $g(i)=l(\mathfrak{q}'^i/\mathfrak{q}'^{i+1})$ and denote by $\mathfrak{m}^*$ the ideal of $\mathfrak{o}^*$ generated by $\mathfrak{q}$ and $\mathfrak{q}'$. To calculate the length of $\mathfrak{o}^*/\mathfrak{m}^{*n}$, we remark that $\mathfrak{o}^*/\mathfrak{m}^{*n}$ is the homomorphic image of the $(\mathfrak{o}/\mathfrak{q}^n)\otimes_B(\mathfrak{o}'/\mathfrak{q}'^n)$ with the kernel $\sum_{i+j=n}(\mathfrak{q}^i/\mathfrak{q}^n)\otimes(\mathfrak{q}'^j/\mathfrak{q}'^n)$. Considering $\mathfrak{o}/\mathfrak{q}^n$ and $\mathfrak{o}'/\mathfrak{q}'^n$ as B-modules, we see that $\mathfrak{o}/\mathfrak{q}^n$ and $\mathfrak{o}'/\mathfrak{q}'^n$ are isomorphic to $\sum_{i<n}(\mathfrak{q}^i/\mathfrak{q}^{i+1})$ and $\sum_{i<n}(\mathfrak{q}'^i/\mathfrak{q}'^{i+1})$ respectively; $\sum(\mathfrak{q}^i/\mathfrak{q}^n)=\sum_{i\leq j<n}(\mathfrak{q}^j/\mathfrak{q}^{j+1})$, $(\mathfrak{q}'^i/\mathfrak{q}'^{in})=\sum_{i\leq j<n}(\mathfrak{q}'/\mathfrak{q}'^{j+1})$. Therefore $\mathfrak{o}^*/\mathfrak{m}^{*n}=\sum_{i+j<n}(\mathfrak{q}^i/\mathfrak{q}^{i+1})\otimes(\mathfrak{q}'^j/\mathfrak{q}'^{j+1})$, which shows that $l(\mathfrak{o}^*/\mathfrak{m}^{*n})=\sum_{i+j<n}f(i)g(j)$. Set $e=rm(\mathfrak{q}; B)$, $e'=rm(\mathfrak{q}'; B)$, $d=\text{rank}\,\mathfrak{o}$ and $d'=\text{rank}\,\mathfrak{o}'$. Since the case $dd'=0$ is easy by the above equality, we shall treat only the case where $dd'>0$. Since $l(\mathfrak{o}/\mathfrak{q}^n)=(e/(d!))n^d+(\text{terms of lower degree})$ (for sufficiently large n), we have $f(n)=(e/(d-1)!)n^{d-1}+(\text{terms of lower degree})$. Similarly we have $g(n)=(e'/(d'-1)!)n^{d'-1}+(\text{terms of lower degree})$. Since $\int_0^n\int_0^{n-x}x^{d-1}y^{d'-1}dxdy=((d-1)!(d'-1)!/(d+d')!)n^{d+d'}+(\text{terms of lower degree})$, we have $\sum_{i+j<n}i^{d-1}j^{d'-1}=((d-1)!(d'-1)!/(d+d')!)n^{d+d'}+(\text{terms of lower degree})$ and $l(\mathfrak{o}^*/\mathfrak{m}^{*n})=\sum_{i+j<n}f(i)g(j)=(ee'/(d-d')!)n^{d+d'}+(\text{terms of lower degree})$, which prove our result.

REMARK. We have proved in the same time that $\text{rank}\,\mathfrak{o}^*=\text{rank}\,\mathfrak{o}+\text{rank}\,\mathfrak{o}'$.

[18] The present proof was given by Samuel [15].

COROLLARY 1. *Assume further that* $\mathfrak{o}/\mathfrak{m}\otimes_B\mathfrak{o}'/\mathfrak{m}'$ *is a field, then* $e(\mathfrak{q})\cdot e(\mathfrak{q}')=e(\mathfrak{q}\mathfrak{o}^*+\mathfrak{q}'\mathfrak{o}^*)$ *and in particular* $\mathfrak{m}(\mathfrak{o}^*)=\mathfrak{m}(\mathfrak{o})\cdot\mathfrak{m}(\mathfrak{o}')$. (Samuel [15])

COROLLARY 2. *Let* $\mathfrak{o}$ *and* $\mathfrak{o}'$ *be semi-local rings with the same basic field* B *and let* $\mathfrak{o}^*$ *be the complete tensor product of* $\mathfrak{o}$ *and* $\mathfrak{o}'$ *over* B. *Then for any ideals* $\mathfrak{q}$ *and* $\mathfrak{q}'$ *of* $\mathfrak{o}$ *and* $\mathfrak{o}'$ *which are intersections of primary ideals belonging to maximal ideals, we have* $rm(\mathfrak{q}; B)\cdot rm(\mathfrak{q}'; B)=rm(\mathfrak{q}\mathfrak{o}^*+\mathfrak{q}'\mathfrak{o}^*; B)$.

Appendix. Numerical polynomials.

Let $f(x)$ be a polynomial in one indeterminate x with coefficients in the field of rational numbers. We say that $f(x)$ is numerical if there exists an integer N such that $f(n)$ is an integer for any integer n greater than N.

PROPOSITION A. *If* $f(x)$ *is a numerical polynomial of degree* d, *then there exist integers* $c_0,\cdots,c_d$ *such that* $f(x)=d_0\binom{x+d}{d}+c_1\binom{x+d-1}{d-1}+\cdots+c_{d-1}\binom{x+1}{1}+c_d$.

PROOF. When $d=0$ our assertion is obvious and we will prove the assertion by induction on d. Let c be the coefficient of x^d in $f(x)$. Then $f(x)-f(x-1)=cdx^{d-1}+$(terms of lower degree). Since $f(x)-f(x-1)$ is also numerical, we see by our induction assumption that $c\cdot(d!)=c_0$ is an integer. Then $c_0\binom{x+d}{d}$ is numerical and $f(x)-c_0\binom{x+d}{d}$ is a numerical polynomial of degree less than d. Therefore we see the assertion by our induction assumption.

From this proposition we see immediately the following

PROPOSITION B. *If* $f(x)$ *is a numerical polynomial, then* $f(n)$ *is an integer for any integer* n.

On the other hand, we see immediately that the multiplicity and relative multiplicity are natural numbers by virtue of Proposition A.

UNIVERSITY OF KYOTO

BIBLIOGRAPHY

[1] C. Chevalley, On the theory of local rings, Ann. of Math., **44** (1943), pp. 690–708.

[2] C. Chevalley, Intersections of algebraic and algebroid varieties, Trans. Amer. Math. Soc., **57** (1945), pp. 1–85.

[3] I. S. Cohen, On the structure and ideal theory of complete local rings, Trans. Amer. Math. Soc., **59** (1946), pp. 54–106.

[4] D. Hilbert, Über die Theorie der algebraischen Formen, Math. Ann., **36** (1898), pp. 473–534.

[5] W. Krull, Dimensionstheorie in Stellenringen, Crelle's Journ., **179** (1938), pp. 204–226.

[6] W. Krull, Zur Theorie der Kommutativen Integritätsbereiche, Crelle's Journ., **192** (1953), pp. 230–252.

[7] M. Nagata, On the structure of complete local rings, Nagoya Math. Journ., **1** (1950), pp. 63–70; Corrections, Nagoya Math. Journ., **5** (1953), pp. 145–147.

[8] M. Nagata, Some remarks on local rings, Nagoya Math. Journ., **6** (1953), pp. 53–58.

[8, II] M. Nagata, Some remarks on local rings, II, Memoirs Kyoto Univ., **28** (1953), pp. 109–120.

[9] M. Nagata, Local rings, Sûgaku, **5** (1953–54), pp. 104–114 and pp. 229–238 (in Japanese).

[10] M. Nagata, Basic theorems on general commutative rings, Memoirs Kyoto Univ., **29** (1955), pp. 59–77.

[11] M. Nagata, A general theory of algebraic geometry over Dedekind domains, I, II, III and V (forthcoming).

[12] M. Nagata, On the chain problem of prime ideals (forthcoming).

[13] M. Nishi, On the dimension of local rings, Memoirs Kyoto Univ., **29** (1955), pp. 7–9.

[14] D. Northcott and D. Rees, A note on reductions of ideals with an application to the generalized Hilbert function, Proc. Cambridge Phil. Soc., **50** (1954), pp. 353–359.

[15] P. Samuel, La notion de multiplicité en algèbre et en géométrie algébrique, Journ. Math. Pures Appl., **30** (1951), pp. 159–274.

[16] P. Samuel, Algèbre locale, Mémorial Scien. Math., No. **123** (1953).

[17] O. Zariski, Analytical irreducibility of normal varieties, Ann. of Math., **49** (1948), pp. 352–361.

Addenda. It was communicated to the writer by Professor J.-P. Serre that (1) he proved that if $\mathfrak{p}$ is a prime ideal of a regular local ring $\mathfrak{o}$, then $\mathfrak{o}_{\mathfrak{p}}$ is also regular, in his paper "Sur la dimension homologique des anneaux et des modules noethériens" (these proceedings, pp. 175–189) and (2) he treated also the theory of multiplicity in his forthcoming paper "Multiplicités d'intersection et caractéristiques d'Euler-Poincaré"; there are some substancially common results with our treatment and furthermore he proved our associativity formula by a simpler way than ours. He defined the notion of multiplicity in a finite module: Let E be a finite module over a local ring $\mathfrak{o}$ and let $\mathfrak{q}$ be a primary ideal belonging to the maximal ideal of $\mathfrak{o}$. Then he denoted the multiplicity of $\mathfrak{q}$ in E by $e_E(\mathfrak{q})$. The notion plays a similar rôle as our notion of relative multiplicity. On the other hand, if we want to calculate $e_E(\mathfrak{q})$ from our standing point, then it becomes as follows: We consider the module $\mathfrak{o}+E$ as a ring by defining to be $E^2=0$; which becomes a local ring. Then $e_E(\mathfrak{q})=e(\mathfrak{q}(\mathfrak{o}+E))-e(\mathfrak{q})$.

Added in proof: [11, I] and [12] appeared in Amer. J. of Math., 78 (1956), pp. 78–116 and Nagoya Math. J., 10 (1956), pp. 51–64 respectively.

Cohomology of Function Fields and Other Algebras

Daniel ZELINSKY

In this lecture I would like to present a homological characterization of finitely separably generated algebraic function fields due to A. Rosenberg and myself [5]. The characterization is in terms of the cohomology groups of algebras first introduced by Hochschild [4] and later recast by Cartan and Eilenberg [2; Chapter IX]. Specifically, if A is an algebra with unit over a field k and M is a two-sided A-module (thus M is a left A^e-module where $A^e = A \otimes_k A^*$) we denote by $H^n(A, M)$ the nth cohomology group of A with coefficients in M, or, in Cartan-Eilenberg's terminology, $\mathrm{Ext}^n_{A^e}(A, M)$. And by $\dim A$ (or k-$\dim A$ when it is necessary to specify the base field explicitly) we denote the supremum of all n such that $H^n(A, M) \neq 0$ for some M. Thus $\dim A = \mathrm{l.}\dim_{A^e} A$, the left dimension of the A^e-module A. Our characterization is as follows: *A field extension A of k is a finitely separably generated algebraic function field if and only if the transcendence degree of A over k is finite and equal to* $\dim A$. The proof actually exhibits a few more properties of the dimension of field extensions, as stated in the theorems below.

THEOREM 1 (Subadditivity of dimension). *Let A be an algebra over a field K and let k be a subfield of K. Then* k-$\dim A \leqq k$-$\dim K + K$-$\dim A$. *Also* k-$\dim A \geqq k$-$\dim K$.

The proof is based on (1) a similar subadditivity theorem for modules: If $R \to S$ is a homomorphism of a ring R into a ring S and if A is any left S-module then $\mathrm{l.}\dim_R A \leqq \mathrm{l.}\dim_R S + \mathrm{l.}\dim_S A$ [2; Chapter XVI, Exercise 5, or 3; Proposition 3] (in our application $R = A^e = A \otimes_k A^*$ and $S = A \otimes_K A^*$); (2) the identity $A \otimes_K A^* \cong A^e \otimes_{K^e} K$ which is easily verified (the isomorphism is induced by $a \otimes_K a^* \to a \otimes_k a^* \otimes_{K^e} 1$); and (3) the change of rings formula: If $R \to S$ is a ring-homomorphism, if S is projective as right R-module and if B is any left R-module, then $\mathrm{l.}\dim_R B \geqq \mathrm{l.}\dim_S S \otimes_R B$ [2; VI, 4.1.3] (in our application $B = K$, $R = K^e$ and $S = A^e$, the mapping being an inclusion mapping). The first inequality then follows immediately: k-$\dim A = \mathrm{l.}\dim_{A^e} A \leqq \mathrm{l.}\dim_{A^e} A \otimes_K A^* + \mathrm{l.}\dim_{A \otimes_K A^*} A = \mathrm{l.}\dim_{A^e} A^e \otimes_{K^e} K + K$-$\dim A \leqq \mathrm{l.}\dim_{K^e} K + K$-$\dim A = k$-$\dim K + K$-$\dim A$.

As for the second inequality, A is a direct sum of copies of K even as a K^e-module, hence k-dim $K = \text{l.}\dim_{K^e} K = \text{l.}\dim_{K^e} A \leqq \text{l.}\dim_{A^e} A$ by a second change of rings formula [2; VI, 4.1.4].

THEOREM 2. *If A is a finitely separably generated algebraic function field of finite transcendence degree over k then* dim A = *transcendence degree of A over k.*

First k-dim $k(x) \leqq 1$ if x is an indeterminate over k, because $k(x)^e = k(x) \otimes_k k(x)$ is a principal ideal ring so that every $k(x)^e$-module (in particular $k(x)$) has left dimension at most 1. Next if $K = k(x_1, \cdots, x_n)$ with $x_1, \cdots, x_n$ independent indeterminates over k, then k-dim $K \leqq n$ by repeated use of the subadditivity in Theorem 1. We prove k-dim $K = n$ by exhibiting a noncobounding n-cocycle of K into K: $f(u_1, \cdots, u_n) = \prod_i \partial u_i / \partial x_i$. The fact that f does not cobound results from an identity that coboundaries satisfy: If f is the coboundary of an $(n-1)$-cochain g, then

$$Af(u_1, \cdots, u_n) = \sum_i (u_i y_i - y_i u_i) \text{ with } y_i = Ag(u_1, \cdots, \hat{u}_i, \cdots, u_n)$$

where the operator A on a function h is defined as the alternating sum of the values of h, summed over all permutations of the variables. Finally, if A is a finite separable algebraic extension of K, then K-dim $A = 0$ [4; Theorem 4.1] and so by both inequalities in Theorem 1, $n = k$-dim $K \leqq k$-dim $A \leqq k$-dim K.

COROLLARY. *For any field extension A of k,* dim $A \geqq$ *transcendence degree of A over k.*

For if K is a subfield generated by a transcendence basis, dim $A \geqq$ dim K by Theorem 1 and dim K = transcendence degree of A by Theorem 2.

THEOREM 3. *If A is a finitely generated extension field of k with no separable generation over k then* dim $A = \infty$.

Let $A = k(t_1, \cdots, t_r)$ and let s be the maximum integer such that $k(t_1, \cdots, t_s)$ can be separably generated over k. Let K be a rational function field over which $k(t_1, \cdots, t_s)$ is algebraic and separable. Then $k(t_1, \cdots, t_s, t_{s+1})$ is separable over $K(t_{s+1})$ so that $K(t_{s+1})$ has no separable generation over K (else $k(t_1, \cdots, t_{s+1})$ would also have a separable generation, contrary to the choice of s). Write $y = t_{s+1}$ and consider the subfield $K(y)$ of A. (Note that y is algebraic over K by the maximality of s). By Theorem 1 it suffices to prove dim $K(y) = \infty$. We shall actually prove that a certain scalar extension $G \otimes_k K(y)$ is a commutative ring with minimum condition and nonzero radical, which implies that dim $G \otimes_k K(y) = \infty$ [1; Propositions 14 and 15]; since dim is invariant under scalar extension [2; IX, 7.2] this will complete the proof.

Let $\{x_1, \cdots, x_n\}$ be a transcendence basis of K and let f be an irreducible polynomial in $n+1$ variables such that

$$(*) \qquad f(x_1, \cdots, x_n, y)=0.$$

Since $(*)$ is the minimum equation of y over K and $K(y)$ is inseparable over K, the exponent of y in each nonzero term is a multiple of the characteristic p. If x_i actually occurs in $(*)$ then $\{x_1, \cdots, \hat{x}_i, \cdots, x_n, y\}$ is another transcendence basis of $K(y)$ and, since $K(y)$ has no separable generation, x_i is also inseparable over $k(x_i, \cdots, \hat{x}_i, \cdots, x_n, y)$. The same argument then shows that the exponents of x_i in $(*)$ are also multiples of p. Hence, if G is the field obtained by adjoining to k the pth roots of all the coefficients of f, then $f=g^p$ for some polynomial g with coefficients in G. If $z=g(x_1, \cdots, x_n, y) \in G \otimes_k K(y)$, then $z^p=0$ so that $G \otimes_k K(y)$ is commutative, satisfies the minimum condition because $[G:k]$ is finite, and contains a nilpotent element, hence a nonzero radical.

THEOREM 4. *If A is a field extension of k with no finite generation then* $\dim A \geqq 1+$*transcendence degree of A over k.*

The Corollary of Theorem 2 disposes of the case of infinite transcendence degree. In case the transcendence degree of A is $n<\infty$, let K be a subfield generated by a transcendence basis. Then A has no finite generation over K and so $[A:K]$ is infinite. It will suffice to prove $\dim A' \geqq 1+n$ for some subfield A' of A since by Theorem 1 $\dim A \geqq \dim A'$. So we may reduce to the case where $[A:K]=\aleph_0$. In these circumstances we can show that a special first cohomology group of A over K is not zero, namely $H^1(A, A \otimes_K A)$—that is, there is a non-inner derivation δ of A into $A \otimes_K A$ over K. This is a computation based on representing A as the union of a denumerable tower of subfields A_i, each of finite degree over K, thus inducing a topology on $A \otimes_K A$ (neighborhoods of zero are $U_i=\{x \in A \otimes_K A \mid ax=xa$ for all a in $A_i\}$) under which $A \otimes_K A$ is not complete. The required derivation is $a \rightarrow ax-xa$ where x is a suitably chosen element of the completion. (For computations we refer to [5].) If we now extend the derivations $\delta_i=\partial/\partial x_i$ $(i=1, \cdots, n)$ of K into K to derivations of A into the ring of all K-linear transformations on A and if we consider K-linear transformations on A as $(1 \otimes_K A)$-linear transformations on $A \otimes_K A$ then we can construct an $(n+1)$-cocycle

$$f(u_1, \cdots, u_{n+1})=[\delta_1(u_1) \cdots \delta_n(u_n)]\delta(u_{n+1})$$

of A into $A \otimes_K A$ which may be proved to be not a coboundary by the same identity used in Theorem 2. This proves Theorem 4.

Theorems 2, 3, and 4 complete the proof of the characterization asserted at the beginning of the lecture.

We may make several remarks about these theorems. Theorem 1 remains true even when K is not a field if we assume that A is projective as a K-module. In many cases we expect the first inequality in this theorem to be an equality. That this is not always the case is easy to demonstrate by examples. One such example may be produced from a more precise version of Theorem 4:

THEOREM 4′. *If A is a denumerably and separably generated field extension of k then* $\dim A = 1 +$ *transcendence degree of* A. (We refer again to [5] for the proof; in the case of zero transcendence degree, Theorem 4′ implies that A is absolutely segregated—i.e., $\dim A \leqq 1$—which is a result due to Kuročkin).

If we choose an algebraic extension field A of k which has a subfield K such that $[A:k] = [K:k] = \aleph_0$, then Theorem 4′ asserts that k-dim $A = K$-dim $A = k$-dim $K = 1$, so that equality in the subadditivity theorem does not hold.

Eilenberg has recently used a spectral sequence argument to show the first inequality in Theorem 1 is an equality when all dimensions are finite and when K is special—in particular when K is a rational function field.

Theorem 4 and the Corollary of Theorem 2 assert that no field extension has dimension zero unless it is finite and separable. As a matter of fact, this can be proved of arbitrary algebras.

Theorems 2, 3, and 4′ give the exact dimension of all field extensions except those which have finite transcendence degree and are separably but not denumerably generated: In the case of finite transcendence degree and separable generation, if K is a rational function field over which A is separable and algebraic and if $[A:K] < \aleph_0$ then $\dim A = \dim K =$ transcendence degree; if $[A:K] = \aleph_0$ then $\dim A = 1 + \dim K = 1 +$ transcendence degree; but it is difficult to believe that $[A:K] = \aleph_1$ should imply $\dim A = 2 + \dim K$, etc.; presumably $[A:K] > \aleph_0$ implies $\dim A = \infty$, but so far our attempts to settle this question have been unsuccessful, even in the case of zero transcendence degree.

NORTHWESTERN UNIVERSITY

REFERENCES

1. M. Auslander, On the dimension of modules and algebras, III. Global dimension, Nagoya Math. J., **9** (1955), pp. 67–77.
2. H. Cartan and S. Eilenberg, Homological Algebra, Princeton, 1956.

3. S. Eilenberg, M. Ikeda, and T. Nakayama, On the dimension of modules and algebras, I, Nagoya Math. J., **8** (1955) pp. 49–57.
4. G. Hochschild, On the cohomology groups of an associative algebra, Annals of Math., **46** (1945), pp. 58–67.
5. A. Rosenberg and D. Zelinsky, Cohomology of infinite algebras, Trans. Amer. Math. Soc., **82** (1956), pp. 85–98.

Short Notes

An Existence Theorem of Algebras

Goro AZUMAYA

It is a well-known arithmetical theorem that if K is a discrete valuated complete field and if L is a finite extension field of K such that the residue class field of L is separable over that of K then there exists a unique subfield (that is, the inertial field) T such that T is unramified over K and every residue class of L is represented by an element of T. The theorem has been extended by Nakayama to the case where L is a division algebra, so that T is an up to inner automorphisms uniquely determined inertial division algebra. On the other hand, there is an important algebraic theorem, called Wedderburn-Malcev's, which asserts that if R is an algebra over a field K such that the semi-simple residue class algebra R/N of R modulo its radical N is separable over K then there exists one and—up to inner automorphisms—only one semi-simple subalgebra S such that every residue class of R modulo N is represented by an element of S. Now in the present lecture, we aim to prove a fundamental theorem which includes above two theorems as particular cases. In the proof of this theorem, which seems to be considerably difficult, a particular type of algebras, called maximally central, play however a quite essential role, and so we shall study such algebras as a main subject.

Let K be a commutative ring with unit element. Let R be a ring with coefficient ring K. We shall R an *algebra* over K if R has a finite (not necessarily linearly independent) module-basis over K. Let now R be an algebra over K with unit element and possessing a linearly independent basis. Then R can be looked upon in a natural way as a right-module of the direct product $R \times R'$, where R' is inverse-isomorphic to R. Let us call R a *maximally central algebra* over K if $R \times R'$ coincides with the K-endomorphism ring of R, or what comes to the same, if for a basis $a_1, a_2, \cdots, a_m$ of R the $m \times m$ matrix $(a_j a_i)$ is a regular matrix. The notion of maximally central algebras is a natural expansion of that of central simple algebras. In fact, we can show, among others, following theorems: 1) Every full matrix ring over K is maximally central, 2) If R and S are both maximally central over K then so is the direct product $R \times S$ too, 3) If R is maximally central over K then K coincides with the center of R, and two-sided ideals of R and ideals of K correspond one-to-one and lattice-isomorphically; from this it follows in particular that in case K is a field R is maximally central if and only if it is central simple, 4) If R is maximally central over K and if Q is an over-algebra of R having a unit element in common with R, then Q is a direct product of R and the commuter algebra S of R in Q, and between subalgebras of $Q=R\times S$ containing R and subalgebras of S there is a one-to-one and lattice-isomorphic correspondence, 5) Furthermore, we can introduce the concept of *algebra class group* over K for maximally central algebras in just a similar way as in the case of central simple algebras.

From now on, we restrict ourselves to the case where K is a *complete local ring* in the sense that K has a unique maximal ideal P, for which $\bigcap_{\nu=1}^{\infty} P^{\nu}=0$ holds, and K is complete with respect to the topology which is defined by taking all the powers P^{ν} as a system of neighbourhoods of 0. (Naturally, every field as well as the valuation ring of every discrete valuated complete field is a *complete local ring.*) Let R be an algebra over K and N its radical (in the sense of Jacobson). Then the two-sided ideal PR is contained in N, and so the residue class algebra $\bar{R}=R/N$ is regarded as a semi-simple algebra over the residue class field $\bar{K}=K/P$. Furthermore, we can verify that for any given system of matrix units $\{\bar{e}_{ij}\}$ in $\bar{R}$ there exists actually a system of matrix units $\{e_{ij}\}$ in R such that each e_{ij} is a representative of $\bar{e}_{ij}$. Let us call R *unramified* over K if $PR=N$. Now R is maximally central over K if and only if R is unramified and $\bar{R}$ is central simple over $\bar{K}$. These show that if we associate with every algebra class $\{R\}$, where R is maximally central over K, the algebra class $\{\bar{R}\}$ we have an isomorphism of the algebra class group over K into that over $\bar{K}$. As a matter of fact, this isomorphism is moreover an onto-mapping. To prove this, it is indispensable to introduce the notions of Galois extensions of K and their crossed products. Namely, a complete local ring L containing K and possessing a linearly independent basis over K is called a *Galois extension* of K if L is (as algebra) unramified over K and the residue class field $\bar{L}$ of L is a separable Galois extension of $\bar{K}$. In this case, the automorphism group G of L over K—the Galois group of L/K—is mapped isomorphically, in the natural manner, onto the Galois group $\bar{G}$ of $\bar{L}/\bar{K}$. Further, for any given (finite, separable) Galois extension field $\bar{L}$ of $\bar{K}$ there exists an up to K-isomorphisms unique Galois extension L of K whose residue class field coincides with $\bar{L}$. Now, for a Galois extension L of K we can construct a *crossed product* $(L/K, a_{\sigma,\tau})$ by means of a factor set $\{a_{\sigma,\tau}\}$ of L/K in just the same way as in the case of a Galois extension fields. $(L/K, a_{\sigma,\tau})$ is then a maximally central algebra over K and in fact the (central simple) residue class algebra modulo its radical is the crossed product $(\bar{L}/\bar{K}, \bar{a}_{\sigma,\tau})$ of $\bar{L}/\bar{K}$. By making use of these facts, we may find that the above mentioned isomorphism $\{R\}\rightarrow\{\bar{R}\}$ is an onto-mapping, and from this we can deduce further that for any given central simple algebra

$\overline{R}$ over $\overline{K}$ there exists an up to K-isomorphisms unique maximally central algebra R over K whose residue class algebra modulo radical coincides with $\overline{R}$. Now, on the basis of these results, we have finally the following main theorem:

THEOREM. *Let R be an algebra over a complete local ring K such that the semi-simple residue class algebra R/N of R modulo its radical N is separable over the residue class field K/P of K. Then there exists one and —up to inner automorphisms—only one unramified subalgebra S such that every residue class of R modulo N is represented by an element of S.*

HOKKAIDO UNIVERSITY

Cohomology Theory for Algebras

Masatoshi IKEDA, Hiroshi NAGAO and Tadasi NAKAYAMA

Cohomology theory for algebras has been introduced and developed by G. Hochschild [6], [7], [8], and the 1-, 2- and 3- dimensional cohomology groups have been interpreted with reference to classical notions of structure of algebras. E.g. algebras with vanishing 1-dimensional cohomology groups are separable semi-simple algebras ([6], Theorem 4. 1). Here we summarize our results on cohomological dimensions of algebras. Our main result is the characterization of algebras with vanishing n-cohomology groups, i.e. the characterization of algebras with dimension $\leqq n-1$ $(n\geqq 2)$ ([9], Main theorem).

Let A be an (associative) algebra (of finite rank) possessing a unit element 1, *and N be its radical.*

(I) *If* $\dim A\leqq n-1$ $(n\geqq 2)$, *then*

α) *A/N is separable semi-simple, and*

β) $l.\dim_A \mathfrak{l}\leqq n-1$ *for every left ideal $\mathfrak{l}$ of A.*

Conversely

(II) *if α) is the case and if*

β_1) $l.\dim_A N\leqq n-2$

then $\dim A\leqq n-1$.

We shall sketch the proofs of (I) and (II).

PROOF OF (I). Let $\mathfrak{l}$ be a left ideal of A and $\mathfrak{m}$ be an A-A-module satisfying $\mathfrak{m}\mathfrak{l}=0$. Let $C^n(A, \mathfrak{m})$ be the n-dimensional cochain group, $C^n_{\mathfrak{l}}(A, \mathfrak{m})$ be its subgroup consisting of cochains which map $A\times\cdots\times A\times\mathfrak{l}$ into zero and $C^n_{[\mathfrak{l}]}(A, \mathfrak{m})=L(Q^n_{\mathfrak{l}}, \mathfrak{m})$ be the group of linear mapping of $Q^n_{\mathfrak{l}}=A\times\cdots\times A\times\mathfrak{l}$ (with $n-1$ A's) into $\mathfrak{m}$. Here $Q^n_{\mathfrak{l}}$ is an A-module under the operation

$$a*(a_1\times\cdots\times a_{n-1}\times m)=aa_1\times\cdots\times a_{n-1}\times m-a\times a_1a_2$$
$$\times\cdots\times a_{n-1}\times m+\cdots\pm a\times a_1\times\cdots\times a_{n-2}\times a_{n-1}m.$$

We define the coboundary operators as usual, and we have the cochain complexes $C(A, \mathfrak{m})$, $C_{\mathfrak{l}}(A, \mathfrak{m})$ and $C_{[\mathfrak{l}]}(A, \mathfrak{m})$. Since $C(A, \mathfrak{m})/C_{\mathfrak{l}}(A, \mathfrak{m})\simeq C_{[\mathfrak{l}]}(A, \mathfrak{m})$, we have the following exact sequence;

$$\to H^n_{\mathfrak{l}}(A, \mathfrak{m})\to H^n(A, \mathfrak{m})\to H^n_{[\mathfrak{l}]}(A, \mathfrak{m})\to H^{n+1}_{\mathfrak{l}}(A, \mathfrak{m})\to\cdots$$

On the other hand we have the so-called reduction theorems; $H^{n+r}_{\mathfrak{l}}(A, \mathfrak{m}) \simeq H^r_{\mathfrak{l}}(A, C^n(A, \mathfrak{m})) \simeq H^r(A, C^n_{\mathfrak{l}}(A, \mathfrak{m}))$ and $H^{n+r}_{[\mathfrak{l}]}(A, \mathfrak{m}) \simeq H^r(A, C^n_{[\mathfrak{l}]}(A, \mathfrak{m}))\simeq H^r_{[\mathfrak{l}]}(A, C^n(A, \mathfrak{m}))$. By the second relation, $H^n_{[\mathfrak{l}]}(A, \mathfrak{m})\simeq H^1(A, L(Q^{n-1}_{\mathfrak{l}}, \mathfrak{m}))\simeq \mathrm{Ext}\ (Q^{n-1}_{\mathfrak{l}}, \mathfrak{m})$ and consequently $H^n_{[\mathfrak{l}]}(A, \mathfrak{m})=0$ if and only if $Q^{n-1}_{\mathfrak{l}}$ is projective, i.e. $l.\ \dim_A\leqq n-2$.

We assume now that $\dim A\leqq n-1$. Then in the above exact sequence $H^n(A,\mathfrak{m})=H^{n+1}(A,\mathfrak{m})=0$, therefore $H^n_{[\mathfrak{l}]}(A,\mathfrak{m})\simeq H^{n+1}_{\mathfrak{l}}(A,\mathfrak{m})\simeq H^n(A,C^1_{\mathfrak{l}}(A,\mathfrak{m}))=0$ and, as was shown above, $l.\ \dim_A\mathfrak{l}\leqq n-2$.

Next we show α). Since $\dim A\leqq n-1$ if and only if $\dim A_\Omega\leqq n-1$ for the algebraic closure Ω of the ground field, we assume that the ground field is algebraically closed. Let $Ae_1,\cdots, Ae_k$ be the totality of non-isomorphic indecomposable components of A. Then an A-left module $\mathfrak{m}$ of finite rank over Ω is projective if and only if $1\mathfrak{m}\simeq\sum_\kappa t_\kappa Ae_\kappa$. We denote A/N by A, then an A-$\bar{A}$-module $\mathfrak{m}$ satisfying $\mathfrak{m}\bar{A}=\mathfrak{m}$ is an A-$\bar{A}$-projective module if and only if $\mathfrak{m}$ is an A-projective module. Now if $\dim A\leqq n-1$, then Q^{n-1}_N is A-projective and hence A-$\bar{A}$-projective. Let $1*Q^{n-1}_N$ be isomorphic to $\sum_{\kappa,\lambda}t_{\kappa\lambda}(Ae_\kappa\times e_\lambda\Omega)$, then $e_\mu*Q^{n-1}_Ne_\nu\simeq\sum_\kappa t_{\kappa\nu}(Ae_\kappa\times e_\nu\Omega)$ as $e_\mu Ae_\mu$-$e_\nu\Omega$-module. Thus we have

$$(e_\mu*Q^{n-1}_Ne_\nu: \Omega)=\sum_\kappa t_{\kappa\nu}(e_\mu Ae_\kappa: \Omega)=\sum_\kappa t_{\kappa\nu}c_{\mu\kappa}.$$

The mapping $x_1\times\cdots\times x_n\to x_1*(x_2\times\cdots\times x_n)$ defines an A-A-homomorphism of Q^{n-1}_N under the ordinary operation, onto $1*Q^{n-2}_N$ and its kernel is $1*Q^{n-1}_N$. Therefore we have

$$(e_\mu*Q^{n-1}_Ne_\nu: \Omega)=(A: \Omega)^{n-3}(e_\mu A: \Omega)((Ae_\nu: \Omega)-(\bar{A}\bar{e}_\nu: \Omega))-(e\ *Q^{n-2}_Ne_\nu: \Omega),$$
$$(e_\mu*Q^{n-2}_Ne_\nu: \Omega)=(A: \Omega)^{n-4}(e_\mu A: \Omega)((Ae_\nu: \Omega)-(\bar{A}\bar{e}_\nu: \Omega))-(e_\mu*Q^{n-3}_Ne_\nu: \Omega),$$
$$\vdots$$

and $(e_\mu*Ne_\nu: \Omega)=(e_\mu Ne_\nu: \Omega)=c_{\mu\nu}-\delta_{\mu\nu}$.

Consequently

$$\begin{aligned}&(e_\mu*Q^{n-1}_Ne_\nu : \Omega)\\&=(\sum_{i=0}^{n-3}\pm(A : \Omega)^i)((Ae_\nu: \Omega)-(\bar{A}\bar{e}_\nu: \Omega))(e_\mu A : \Omega)+(-1)^n(c_{\mu\nu}-\delta_{\mu\nu})\\&=(\sum_{i=0}^{n-1}\pm(A : \Omega)^i((Ae_\nu: \Omega)-(\bar{A}\bar{e}_\nu: \Omega))(\sum_\lambda c_{\mu\lambda}(\bar{e}_\lambda\bar{A} : \Omega))+(-1)^n(c_{\mu\nu}-\delta_{\mu\nu})\\&=\sum_\kappa t_{\kappa\nu}c_{\mu\kappa}.\end{aligned}$$

This shows that $|c_{\mu\nu}|=\pm1$. Thus we have that if $\dim A\leqq n-1$ then Cartan matrix of A_Ω is uni-modular. On the other hand if A/N is inseparable then the determinant of Cartan matrix of A_Ω is divisible by the characteristic of the ground field. Therefore if $\dim A \leqq n-1$ then A/N is separable.

PROOF OF (II). By (α), there is a subalgebra $\bar{A}$ such that $A=\bar{A}+N$. Let $\mathfrak{m}$ be an A-A-module such that $N\mathfrak{m}=\mathfrak{m}N=0$. If $\delta f(a_1, \cdots, a_n, \bar{a}_{n+1})=0$ wherever $\bar{a}_{n+1} \in \bar{A}$ for an $f \in C^n(A, \mathfrak{m})$, then there is a $g \in C^{n-1}(A, \mathfrak{m})$ such that $(f-\delta g)(a_1, \cdots, a_{n-1}, \bar{a}_n)=0$ whenever $\bar{a}_n \in \bar{A}$. Therefore each class of $H^n(A, \mathfrak{m})$ contains an f such that $f(a_1, \cdots, a_{n-1}, \bar{a}_n)=0$ whenever $\bar{a}_n \in \bar{A}$. Let $\bar{R}(Q_N^{n-1}, \mathfrak{m})$ be the group of $\bar{A}$-homomorphism from Q_N^{n-1} into $\mathfrak{m}$ as $\bar{A}$-right modules. By $(aF)(u)=aF(u)$ and $(Fa)(u)=F(a*u)$ $(a \in A,\ u \in Q_N^{n-1},$ $F \in \bar{R}(Q_N^{n-1}, \mathfrak{m}))$, $\bar{R}(Q_N^{n-1}, \mathfrak{m})$ becomes an A-A-module. The mapping φ defined by $\varphi f(a_1)(a_2, \cdots, m_n)=f(a_1, \cdots, m_n)(a_i \in A,\ m_n \in N)$ for the cochain f satisfying $f(a_1, \cdots, a_{n-1}, \bar{a}_n)=0$, gives an isomorphism from $H^n(A, \mathfrak{m})$ onto $H^1(A, \bar{R}(Q_N^{n-1}, \mathfrak{m}))$. Now if Q_N^{n-1} is projective as A-left module, then Q_N^{n-1} is projective as A-$\bar{A}$-module and we have $H^1(A, \bar{R}(Q_N^{n-1}, \mathfrak{m}))=0$. Thus under the assuption α) and β_1), we have $H^n(A, \mathfrak{m})=0$. If $\mathfrak{m}$ is an arbitrary A-A-module, considering the composition factor groups of $\mathfrak{m}$, we have $H^n(A, \mathfrak{m})=0$.

We shall note some other results without proof.

(III) *If A is a non semi-simple quasi-Frobenius algebra, then* $\dim A=\infty$. ([9])

(IV) $\dim A \leqq \dim A/\mathfrak{a}+l.\ \dim_A (A/\mathfrak{a})$ *for two-sided ide l* $\mathfrak{a} \subseteq N$. ([4])

(V) *If* $\dim A=1$, *then* $\dim A/\mathfrak{a}<\infty$ *for any two-sided ideal* $\mathfrak{a}$ *of* A. *On the other hand for each* $n>1$, *there exist an algebra A and its ideal* $\mathfrak{a}$ *such that* $\dim A=n$ *and* $\dim A/\mathfrak{a}=\infty$. ([5])

OSAKA UNIVERSITY
OSAKA CITY UNIVERSITY
NAGOYA UNIVERSITY

BIBLIOGRAPHY

[1] M. Auslander, On the dimension of modules and algebras, III, Nagoya Math. J., **9** (1955), 67–77.

[2] H. Cartan and S. Eilenberg, Homological Algebras, Princeton Univ. Press, 1955.

[3] S. Eilenberg, Algebras of cohomologically finite dimension, Comment. Math. Helv., **28** (1954), 310–319.

[4] S. Eilenberg, M. Ikeda and T. Nakayama, On the dimension of modules and algebras, I, Nagoya Math. J., **8** (1955), 49–57.

[5] S. Eilenberg, H. Nagao and T. Nakayama, On the dimension of modules and algebras, IV, Nagoya Math. J., **10** (1956), 87–95.

[6] G. Hochschild, On the cohomology groups of an associative algebra, Ann. Math., **46** (1945), 58–67.

[7] G. Hochschild, On the cohomology theory for associative algebras, Ann. Math., **47** (1946), 568–579.

[8] G. Hochschild, Cohomology and representations of associative algebras, Duke Math. J., **14** (1947), 921–948.

[9] M. Ikeda, H. Nagao and T. Nakayama, Algebras with vanishing n-cohomology groups, Nagoya Math. J., **7** (1954), 115-131.

[10] I. H. Rose, On the cohomology theory for associative algebras, Amer. J. Math., **74** (1952), 531-546.

[11] K. S. Shih, Dissertation, Univ. of Illinois, 1953.

On Cohomology Groups in a Field, which is Complete with Respect to a Discrete Valuation

Eizi INABA

Let K be a field, which is complete with respect to a discrete valuation, and $\mathfrak{K}$ be its residue class field. In the case, $\mathfrak{K}$ is perfect, Witt considered central division algebras over K and obtained a theorem on the structure of Brauer group over K. If we consider from the viewpoint of cohomology theory, Witt's theorem can be replaced by a theorem on two-dimensional cohomology in a Galois extension of K. We aim to extend this theorem to the one on higher dimensional cohomology groups, under the assumption that $\mathfrak{K}$ is perfect. For this purpose it seems more natural to consider cohomology groups in a maximal separable algebraic extension L of K rather than to consider those in a finite Galois extension of K. Let G be the Galois group of L over K, and we assign to G the usual topology. We denote with L^* the multiplicative group of all non-zero elements in L, and assign to L^* the discrete topology. Then a continuous cochain in L^* is nothing other than the lifting to L of a cochain, which is defined on the Galois group of some finite Galois extension of K. In the following we consider only continuous cochains. Let Σ be the maximal unramified subfield of L over K. Then the residue class field $\mathfrak{L}$ of L can be identified with the residue class field of Σ and is algebraically closed over $\mathfrak{K}$. We denote with $\mathfrak{G}$ the Galois group of $\mathfrak{L}$ over $\mathfrak{K}$, and we have the following

THEOREM 1. *The n-dimensional cohomology group $H^n(G, L^*)$ is canonically isomorphic to the direct product of $H^n(\mathfrak{G}, Z)$ and $H^n(\mathfrak{K}, \mathfrak{L}^*)$, where Z is the additive group of rational integers, on which $\mathfrak{G}$ operates trivially.*

Next we shall consider the case, where generalized local class field theory, due to Moriya, holds. In this case we have the following

THEOREM 2. *If the dimension n is one or larger than two, $H^n(G, L^*)$ is trivial. $H^2(G, L^*)$ is isomorphically mapped onto the additive group of all rational numbers* mod Z.

OCHANOMIZU UNIVERSITY

BIBLIOGRAPHY

[1] E. Witt, Schiefkörper über diskret bewerteten Körpern, Crelles Journ., **176** (1936), 153–156.

[2] G. Hochschild and T. Nakayama, Cohomology in class field theory, Ann. of Math., **55** (1952), 348–366.

[3] G. Hochschild and J.-P. Serre, Cohomology of group extensions, Trans. of Amer. Math. Soc., **74** (1953), 110–134.

[4] M. Moriya, Eine notwendige Bedingung für die Gültigkeit der Klassenkörpertheorie im Kleinen, Math. Journ. of Okayama Univ., **2** (1952), 13–20.

Some Remarks on Class Formations

Yukiyosi KAWADA

1. E. Artin has established the abstract class field theory in his lecture at Princeton University [1]. There he has given the notion of a class formation which is defined by several axioms, and on the basis of this notion he has proved the main theorems both in local and in global class field theory simultaneously. After his idea I compared in [2], this cohomology-theoretical class formation theory with other known theories of abelian extensions; in particular, J. Tate and I considered the case of algebraic function fields in [3]. Here we shall add some more results concerning class formation theory; namely, on class formation theory in characteristic p ([4]) and the system of Weil-groups in a class formation.

2. We shall repeat here the definition of a class formation. Let k_0 be a given ground field and Ω be a fixed infinite separable normal algebraic extension of k_0. We consider the set $\mathfrak{K}$ of all finite extensions of k_0 contained in Ω. Let us assume that an abelian group $A(k)$ is attached to each $k \in \mathfrak{K}$ with the following properties: (i) for k, $K \in \mathfrak{K}$ and $k \subset K$ there exists an isomorphism $\varphi_{k/K}$ of $A(k)$ into $A(K)$, (ii) for a normal K/k the Galois group $G = G(K/k)$ operates on $A(K)$ and $\varphi_{k/K}A(k) = A(K)^G$ (and some more additional conditions on $A(k)$ such that we can apply the usual Galois theory for the limit group $A(\Omega/k_0)$ of $\{A(K); K \in \mathfrak{K}\}$), (iii) for normal K/k the cohomology groups of G over the coefficient group $A(K)$ satisfy: $H^1(G, A(K)) = 0$, $H^2(G, A(K)) \cong Z/nZ$ $(n = [K:k])$. Then we call $\{A(k); k \in \mathfrak{K}\}$ *a class formation*. By class field theory we know that for a $\mathfrak{p}$-adic number field k_0 (or for an algebraic number field k_0) and for its algebraic closure Ω we can take as $A(k)$ the multiplicative group k^* (or the idèle class group C_k). Once these axioms are satisfied, we can prove the isomorphism theorem to the effect that $A(k)/A(K/k) \cong G(K/k)$ $(A(K/k) = \varphi_{k/K}^{-1}(\mathrm{N}_G A(K)))$ holds for abelian K/k $(k, K \in \mathfrak{K})$, the general theory of norm residue symbols, etc. To prove the existence theorem of a class field over k for given subgroup H of $A(k)$ we have to determine the set $\mathfrak{A}(k)=\{A(K/k)$; for all abelian K/k in $\mathfrak{K}\}$ explicitly. This cannot be done in the abstract theory.

For any given Ω/k_0 we can choose $A(k)$ suitably (at least theoretically) so that $\{A(k)\}$ makes a class formation. In some cases we can determine $A(k)$ explicitly. (I) Soppose that (i) $\chi(k)=0$, (ii) k contains all the roots of unity, (iii) $k=\mathrm{N}_{K/k}K$ holds for any normal K/k. Then we can take $A(k)=(k^*\otimes(Q/Z))^{\wedge}$ (in general $A^{\wedge}$ means the character group of A). We have a simple interpretation of the usual Kummer theory by class formation theory (see [2]). (II) Let k_0 be an algebraic function field of one variable over the complex number field C and let Ω be the maximal unramified extension field of k_0. Then we can take as $A(k)$ the locally compact character group of the divisor class group of k with the natural locally compact topology. The relation between the classical function theory and the class formation theory can be established (see [3]).

3. Now we shall consider the case of characteristic p. Let k_0 be an arbitrary field of characteristic p. Let Ω be the maximal separable p-extension of k_0. Then we can take $A(k)=((V_k/\wp V_k)\otimes(Q^*/Z))^{\wedge}$ where V_k means the module of all Witt's vectors in k of infinite length, $\otimes$ means the tensor product over Z and $Q^*=\{a/p^n;\ a\in Z,\ n=1,2,\cdots\}$. $\mathfrak{A}(k)$ is the set of all open subgroups of $A(k)$ of finite indices p^n $(n=1,2,\cdots)$. We can prove also that $A(k)$ is topologically isomorphic to the Galois group of the maximal abelian p-extension of k. In particular, let k_0 be formal power series field of t over a finite constant field $\mathrm{GF}(p^f)$. Let $a(\neq 0)\in k$ and $b=x(\mathrm{mod}\ \wp V_k)\otimes(1/p^n)$ $(x=(x_0, x_1,\cdots)\in V_k)$, then we can define a continuous pairing of the multiplicative group k^* and $(V_k/\wp V_k)\otimes(Q^*/Z)$ into R/Z by $(a, b)=\eta\cdot\mathrm{Tr}\cdot\mathrm{Res}_n((x_0, x_1,\cdots, x_{n-1})da/a)$, where Tr means the trace from $\mathrm{GF}(p^f)$ to $\mathrm{GF}(p)$ and η means the injection of the module of Witt's vectors of length n with components in $\mathrm{GF}(p)$ into R/Z. By this pairing $k^*/\mathrm{GF}(p^f)$ is isomorphically mapped to a dense submodule of $((V_k/\wp V_k)\otimes(Q^*/Z))^{\wedge}$. Using this fact we can prove that $\{A(k)=k^*;\ k\in\mathfrak{K}\}$ makes another class formation and we can prove all the theorems in class field theory including the existence theorem over k and the explicit formula of the norm residue symbol as far as the p-extensions are concerned. In a similar way we can derive the classical results over an algebraic function field of one variable with a finite constant field from our general results on class formation theory in characteristic p (as far as the p-extensions are concerned).

Next, let k_0 be an algebraic function field of one variable over an algebraically closed constant field of characteristic p, and let Ω be the maximal unramified separable p-extension of k_0. In this case we can take $A(k)=((V_k^*/\wp V_k^*)\otimes(Q^*/Z))^{\wedge}$ where V_k^* means the module of all Witt's vectors in k which split locally for all prime divisors of k. Moreover, $A(k)$ is topologically isomorphic to the Galois group of the maximal unramified p-extension of k_0 over k_0.

4. A. Weil [6] has considered a system of groups $G_{K,k}$ $(k\subset K)$ with the properties A, B, C, D for an algebraic number field k. This theory can be established also on the basis of the axioms of a class formation $\{A(k)\}$. Moreover, we can consider the universal group $G_{\Omega,k}$ in some cases. In case (I) in 2, and in cases in 3 we can take simply as $G_{\Omega,k}$ the Galois group $G(\Omega/k)$. In case (II) in 2 we can take as (an equivalence of) $G_{\Omega,k}$ the group extension of the fundamental group $F(k)$ of the Riemann surface of k by Z with the canonical 2-cohomology class of $F(k)$ over Z. We have a simple topological interpretation of $G_{\Omega,k}$ ([7], [8]).

UNIVERSITY OF TOKYO

BIBLIOGRAPHY

[1] E. Artin and J. Tate, Algebraic Numbers and Algebraic Functions, II Mimeographed Notes (forthcoming).

[2] Y. Kawada, Class formations, Duke Math. J., **22** (1955), 165–178.

[3] Y. Kawada and J. Tate, On the Galois cohomology of unramified extensions of function fields in one variable, Amer. J. Math., **77** (1955), 197–217.

[4] K. Kawada and I. Satake, Class formations II, J. Fac. Sci. Univ. Tokyo, **7** (1956), 353–389.

[5] E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n, J. Reine Angew. Math., **176** (1937), 126–140.

[6] A. Weil, Sur la théorie du corps de classes, J. Math. Soc. Japan, **3** (1951), 1–35.

[7] Y. Kawada, On the relation between class field theory and other theories of abelian extensions (in Japanese), Sûgaku, **6** (1954), 129–150.

[8] Y. Kawada, Class formations III, J. Math. Soc. Japan, **7** (1955), 453–490.

Certain Subfields of Rational Function Fields

Hideo KUNIYOSHI

Let $K=k(x_1,\cdots,x_n)$ be a purely transcendental extension of any field k, and G be a group of linear transformations in $x_1,\cdots,x_n$. G induces an automorphism group $\bar{G}$ of K. We denote by L the subfield of K consisting of elements fixed by the automorphisms of $\bar{G}$, and investigate the problem whether L is purely transcendental over k or not. It has been already solved affirmatively when k is the field of all complex numbers and G is abelian. It is also true for any k of characteristic $p>0$ when G is the regular representation of cyclic group of order p^n. In the present note we shall generalize it for p-groups satisfying certain condition (C). These conditions are satisfied when G is the regular representation of any p-group.

In the following, k means any field of characteristic $p>0$, $K=k(x_1,\cdots,x_n)$ a purely transcendental extension over k, and G a group of order p^n consisting of linear transformations in $x_1,\cdots,x_n$. As a group of linear transformations, G is equivalent to a group G' with matrices of the form

$$\text{(1)} \qquad \begin{pmatrix} 1 & & & * \\ 0 & 1 & & \\ \vdots & \ddots & \vdots & \ddots \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

The matrices of type (i,i) consisting of the first i rows and the first i columns of such matrices form a group G_i which is homomorphic to G. So that, we get a series of homomorphisms

$$\text{(2)} \qquad (e)=G_1\leftarrow\cdots\leftarrow G_i\leftarrow\cdots\leftarrow G_n=G,$$

the kernel H_i of the homomorphism $G_i\rightarrow G_{i+1}$ being abelian group of type $(p,\cdots,p)$ with order at most p^{i-1}. We assume further that G satisfies the following conditions:

(C) *the order of H_i is at most p.*

Then, H_i is included in the center of G_i.

When we take an equivalent representation G', the system of generators $x_1,\cdots,x_n$ of field K are changed into another system of generators $y_1,\cdots,y_n$ of K by a linear transformation. Then the assertion to be proved is:

Let $K_n=k(y_1,\cdots,y_n)$ be purely transcendental over k and G_n be a linear transformation group in $y_1,\cdots,y_n$ of matrices of the form (1). *If G_n satisfies the condition* (C), *then the field L_n consisting of elements fixed by the automorphism group G_n of K_n induced by G_n is purely transcendental over k.*

G_n induces in the subfield $K_i=k(y_1,\cdots,y_i)$ an automorphism group G_i which is also induced by G_i. Since K_i and G_i satisfy the same assumption of the above-mentioned assertion, we may prove it by induction on the number n of generators $y_1,\cdots,y_n$.

Assume that the assertion has been proved for $n=i-1$. We prove it for $n=i$, $G_{i-1}\neq(e)$, and $H_1\neq(e)$. Let us denote by

$s,t,\cdots$	elements in $\bar{G}_i/\bar{H}_i$,
$\sigma_s,\sigma_t,\cdots$	their representatives in $\bar{G}_i$,
$\varepsilon_{s,t}$	their factor set in $\bar{H}_i$,
ε	a generating element of $\bar{H}_i$.

From (1), we have

$$\varepsilon y_i=y_i+a_{i-1},\quad a_{i-1}\in K_{i-1},$$

where $\sigma a_{i-1}=a_{i-1}$. We put $\theta=y_i/a_{i-1}$, then

$$\varepsilon\theta=\theta+1,\quad \sigma_s\theta=\theta+b_{i-1},\quad b_{i-1}\in K_{i-1},$$

and $\wp\theta=\theta^p-\theta$ is invariant under $\bar{H}_i$. We may write $(s-1)\wp\theta$ instead of $(\sigma_s-1)\wp\theta$. Since they form a l-cocycle of $\bar{G}_{i-1}$ in K_{i-1}, there exists c_{i-1} in K_{i-1} such that

$$(s-1)\wp\theta=(s-1)c_{i-1},$$

which shows $\wp\theta-c_{i-1}\in L_i$. We take it as the i-th element u_i in L_i. Then

$$\begin{aligned}(\bar{G}_i:1)=(K_i:L_i)&\leqq(K_i:L_{i-1}(u_i))\\ &=(K_i:K_{i-1}(u_i))(K_{i-1}(u_i):L_{i-1}(u_i))\\ &\leqq p\cdot(\bar{G}_{i-1}:1)=(\bar{G}_i:1).\end{aligned}$$

Hence $L_i=L_{i-1}(u_i)=k(u_1,\cdots,u_i)$. It is obvious that u_i are free generators of L_i over k, because the degree of transcendency of L_i is i.

Tôhoku University

Bibliography

[1] H. Kuniyoshi, On purely transcendency of a certain field, Tôhoku Math. Journ., **6** (1955), pp. 101–108.

[2] K. Masuda, On a problem of Chevalley, Nagoya Math. Journ., **8** (1955), pp. 59-63.

[3] E. Witt, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f, Journ. für Math., **174** (1935), pp. 237–245.

On the Arithmetic on a Galois Structure

Katsuhiko Masuda

1. Let k be a topological field, G be a topological group. Denote by M the topological k-module consisting of all continuous mappings of G into k, and define the left operation of G on M by

$$(\alpha f)^g(h)=\alpha f(hg) \qquad f\in M, \quad g, h\in G, \ \alpha\in k.$$

We define a continuous distributive multiplication in M to make it a topological algebra, not necessarily associative, over k. If the operation of G gives (continuous) automorphism of the thus obtained algebra, we call it a topological Galois algebra over k with Galois group G. We call a topological algebra K over k with G as a left operator group also a topological Galois algebra over k with Galois group G, if and only if there exists a k-G-permissible ring-isomorphic homeomorphism onto K from one of topological Galois algebras obtained by M. The concept of topological Galois algebra is useful to combine the investigation of Galois extension fields and that of representations of topological groups, [1] [3] [5][1]. A separable normal extension field over k with Galois group G_1 is a topological Galois algebra over k as discrete topological field with Galois group G_1 as compact group with usual topology originally due to Krull.

2. Let K be a topological Galois algebra over k with Galois group G. Suppose from now on that there exists a linearly dense set $\varDelta$ of continuous representations of G with regular matrices in k. For each pair of two representations D_λ, D_μ in $\varDelta$ there exists a matrix $C_{\lambda,\mu}$ in k, uniquely determined, such that

$$D_\lambda \times D_\mu = D_{\lambda\mu} C_{\lambda,\mu},$$

where we denote by × the Kronecker product of matrices in K. We call the pair of $\varDelta$,and the set $\{C_{\lambda,\mu};\ D_\lambda, D_\mu \in \varDelta\}$ of matrices in k as the Galois structure corresponding to a Galois algebra K. As $\varDelta$ is linearly dense in M and the multiplication in K is continuous, the multiplication in K is uniquely determined by its Galois structure. Conditions for K to be associative or commutative or associative and commutative can be formulated by certain explicit conditions for a Galois structure corresponding to it, [1] [5] [7]. Here we remark that the most general associative and commutative Galois structure of a finite Galois group generates over k the invariant field in the purely transcendental extension field obtained by adjunction of all elements in G as algebraically independent variables.

3. Let H be a closed subgroup in G. If a Galois algebra K over k with Galois group G is the direct sum of Galois algebra over k with Galois group H and its conjugates for G/H, we call that K is directly decomposable with reference to H. The condition for K to be directly decomposable with reference to H can be formulated as a certain direct reduction of the Galois structure corresponding to K into the Galois structure of H and this reduction keeps the condition on Galois structures for commutativity, associativity and semi-simplicity, [2] [3]. Thus the construction problem of Galois fields with given Galois group over k is formulated as an existence problem of certain matrices. This may be a generalization of the algebraic part of the classical problem on the division of periods, [6]. The direct decomposition of a Galois structure is of arithmetical character. It suggests us to generalize the concept of n-th power residues mod $\mathfrak{p}$. We can prove that if k has a discrete valuation $\mathfrak{p}$ with finite residue class field, a direct decomposition in $k_{\mathfrak{p}}$ of a suitable Galois structure in k corresponds to a direct decomposition in the residue class field $\tilde{k}_{\mathfrak{p}}$ of k.

YAMAGATA UNIVERSITY

[1] (added in proof) This fact is useful in the cohomology theory. This will be discussed by the author in another chance.

BIBLIOGRAPHY

[1] H. Hasse, Invariante Kennzeichnung galoisscher Körper mit vorgegebener Galoisgruppe, J. riene angew. Math., **187** (1950), 14–43.

[2] K. Masuda, Direct decomposition of Galois algebras, Tôhoku Math. J., Ser. II, **4** (1952), 122–130.

[3] K. Masuda, One-valued mappings of groups into fields, Nagoya Math. J., **6** (1953), 41–52.

[4] K. Masuda, Hasse factor systems reduced mod $\mathfrak{p}$, J. reine angew. Math., **193** (1954), 161–165.

[5] T. Nakayama, On construction and characterization of Galois algebras with given Galois groups, J. reine angew. Math., **189** (1951), 100–117.

[6] A. Weil, Généralization des fonctions abéliennes, J. math. pure appliquées, **17** (1938), 47–87.

[7] P. Wolf, Grundlagen der Theorie der invarianten Kennzeichnung galoisscher Körper mit vorgegebener Galoisgruppe, Math. Nachr., **9** (1953), 201–216.

Cycles on Algebraic Varieties

Hisasi MORIKAWA

Applying the theory of harmonic integrals, we shall prove some relations between cycles and multiple integrals on an algebraic variety and give a new birational invariant.

Notations:

V : a compact non-singular algebraic variety of dimension n imbedded in a projective space,

$V_1(V_2)$: the first (second) component of $V\times V$,

$\delta(V)$: the diagonal subvariety of $V\times V$,

W_r : a generic hyperplane section of dimension r of V,

$H_r(V, Q)$: the r-th homology group of V over Q,

$H_{p,q}(V, Q)$: the subgroup of classes of type (p, q),

$\mathfrak{H}_r(V, Q)$: the subgroup of $H_{2r}(V, Q)$ containing algebraic cycles,

$\{\Gamma_r^1, \cdots, \Gamma_r^{B_r}\}$: a base of $H_r(V_1, Q)$,

$\{\varDelta_r^1, \cdots, \varDelta_r^{B_r}\}$: the base of $H_r(V_2, Q)$ corresponding to $\{\Gamma_r^1, \cdots, \Gamma_r^{B_r}\}$,

$\{\Gamma_r^{1*}, \cdots, \Gamma_r^{B_r*}\}$: the base of $H_{2n-r}(V_2, Q)$ such that $I(\Gamma_r^i\Gamma_r^{j*})=\delta_{ij}$,

$\{\varDelta_r^{1*}, \cdots, \varDelta_r^{B_r*}\}$: the base of $H_{2n-r}(V_2, Q)$ corresponding to $\{\Gamma_r^{1*}, \cdots, \Gamma_r^{B_r*}\}$,

$\Omega^{(p,q)}$: the period matrix of harmonic forms of type (p, q) with period cycles $\Gamma_r^1, \cdots, \Gamma_r^{B_r}$, where $p+q=r\leqq n$,

$\Omega^{(n-p,n-p)}$: the period matrix of harmonic forms of type $(n-q, n-p)$ with period cycle $\Gamma_r^{1*}, \cdots, \Gamma_r^{B_r*}$ where $p+q=r\leqq n$,

$\delta(X)$: the cycle on $\delta(V)$ corresponding to a cycle X on V.

By virture of the intersection theory we have

LEMMA 1. *Let C be a cycle of dimension $2r$. Then*

$$ {}^t(I(C\times\Delta_r^{i*}\delta(\Gamma_r^{j*}))=(I(C\Gamma_r^{i*}\Gamma_r^{j*})). $$

Applying Lemma 1 we get

PROPOSITION 1. *Let C be a cycle of type $(r\mp s,\ r\pm s)$ with complex coefficients. Then*

$$ \Lambda(C)\Omega^{(n-q\mp s,\,n-p\pm s)}=\Omega^{(p,q)}(I(\Gamma_r^{i*}\Gamma_r^{j*})). $$

By the theory of harmonic integrals we get

LEMMA 2. *$(I(W_r\Gamma_r^{i*}\Gamma_r^{j}))$ is non-singular.*

THEOREM 1. *Let C be a cycle of type (r,r). Then*

$$ \Omega^{[r]}(I(C\Gamma_r^{i*}\Gamma_r^{j*}))(I(W_r\Gamma_r^{i*}\Gamma_r^{j*}))^{-1}=\begin{pmatrix}\Lambda_0(C) & & & \\ & \Lambda_1(C) & & \\ & & \ddots & \\ & & & \Lambda_{[r/2]}(C)\end{pmatrix}\cdot\Omega^{[r]} $$

where

$$ \Omega^{[r]}=\begin{pmatrix}\Omega^{(r,0)}\\ \Omega^{(r-2,2)}\\ \vdots\\ \Omega^{(1,r-1)}\end{pmatrix}\ \text{for odd } r,\quad =\begin{pmatrix}\Omega^{(r,0)}\\ \Omega^{(r,1)}\\ \vdots\\ \Omega^{(r/2,\ r/2)}\end{pmatrix}\ \text{for even } r. $$

THEOREM 2. *Let $\{S_1,\cdots,S_l\}$ be a base of the module of rational matrices $S=(s_{ij})$ such that*

$$ \sum_{i,j}s_{ij}\Gamma_r^{i*}\Gamma_r^{j*}\approx 0. $$

Let $K_{2r}(V,Q)$ be the submodule of $H_{2r}(V,Q)$ consisting of classes Z such that

$$ I(Z\Gamma_r^{i*}\Gamma_r^{j*})=0,\quad i,j=1,2,\cdots,B_r. $$

Then there exists an isomorphism of

$$ H_{r,r}(V,Q)/H_{r,r}(V,Q)\frown K_{2r}(V,Q) $$

onto the module of rational matrices M satisfying

(i) $\Omega^{[r]}M=\Lambda\Omega^{[r]}$

with a matrix Λ,

(ii) $\mathrm{Sp}\,S_\nu M(I(W_r\Gamma_r^{i*}\Gamma_r^{j*}))=0,\quad \nu=1,2,\cdots,l.$

THEOREM 3. *Let $\{S_1,\cdots,S_l\}$ be a base of the module of rational matrices $S=(s_{ij})$ such that*

$$ \sum_{i\,j}s_{ij}\Gamma_1^{i*}\Gamma_1^{j*}\approx 0. $$

Let $K'_{2n-2}(V,Q)$ be the submodule of $H_{2n-2}(V,Q)$ consisting of classes Z such that

$$ I(W_2Z\Gamma_1^{i*}\Gamma_1^{j*})=0,\quad i,j=1,2,\cdots,B_1. $$

Then there exists an isomorphism of

$$ \mathfrak{H}_{n-1}(V,Q)/\mathfrak{H}_{n-1}(V,Q)\frown K'_{2n-2}(V,Q) $$

onto the module of rational matrices M satisfyiug

(i) $\Omega^{(1,0)}M=\Lambda\Omega^{(1\ 0)}$ *with a matrix* Λ,

(ii) $\mathrm{Sp}\, S\ M(I(W_1\Gamma_1^{i*}\Gamma_1^{j*}))=0,\quad \nu=1,2,\cdots,l.$

THEOREM 4. *The degree of* $\mathfrak{H}_{n-1}(V,Q)/\mathfrak{H}_{n-1}(V,Q)\frown K'_{2n-2}(V,Q)$ *is a birational invariant.*

NAGOYA UNIVERSITY

Zusammenhang zwischen 2-Kohomologiegruppe und Differente

Mikao MORIYA

1. Es sei $\mathfrak{o}$ ein Z.P.I.-Ring und k der Quotientenkörper von $\mathfrak{o}$; ferner sei K eine endlich-separable Erweiterung über k mit $\mathfrak{O}$ als Hauptordnung. Bekanntlich ist dann $\mathfrak{O}$ auch ein Z.P.I.-Ring. Für ein beliebiges nicht-triviales Primideal $\mathfrak{P}$ aus $\mathfrak{O}$ bezeichnet $K_{\mathfrak{P}}$ bzw. $\mathfrak{O}_{\mathfrak{P}}$ die $\mathfrak{P}$-adische Hülle von K bzw. $\mathfrak{O}$. Ist nun $\mathfrak{p}$ das durch $\mathfrak{P}$ teilbare Primideal aus $\mathfrak{o}$, so kann man wie üblich annehmen, daß die $\mathfrak{p}$-adischen Hüllen $k_{\mathfrak{p}}$ und $\mathfrak{o}_{\mathfrak{p}}$ bzw. in $K_{\mathfrak{P}}$ und $\mathfrak{O}_{\mathfrak{P}}$ enthalten sind. Wir bezeichnen mit $\mathfrak{D}_{\mathfrak{P}}(K/k)$ den $\mathfrak{P}$-Beitrag der Differente von K/k. Da bekanntlich das Erweiterungsideal von $\mathfrak{D}_{\mathfrak{P}}(K/k)$ in $\mathfrak{O}_{\mathfrak{P}}$ mit der Differente von $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ übereinstimmt, so können wir ohne Mißverständnis mit $\mathfrak{D}_{\mathfrak{P}}(K/k)$ auch die Differente von $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ bezeichnen. Der Exponent von $\mathfrak{D}_{\mathfrak{P}}(K/k)$ in bezug auf $\mathfrak{P}$ heiße der $\mathfrak{P}$-*Exponent* der Differente K/k.

Nun versteht man unter einem *normalen* 2-Kozyklus f von $\mathfrak{O}/\mathfrak{o}$ über $\mathfrak{O}_{\mathfrak{p}}$ eine bilineare Abbildung des Ringes $\mathfrak{O}$ in $\mathfrak{O}_{\mathfrak{P}}$ mit folgenden Eigenschaften:

1) Für beliebige Elemente X, Y aus $\mathfrak{O}$ gilt:

$$f(X,Y)=f(Y,X).$$

2) Für beliebige Elemente X_i, Y_i $(i=1,2)$ aus $\mathfrak{O}$ gilt:

$$f(X_1+X_2, Y_1+Y_2)=\textstyle\sum_{i,j=1}^{2} f(X_i, Y_j).$$

3) Für beliebige Elemente X, Y, Z aus $\mathfrak{O}$ gilt:

$$Xf(X,Z)+f(X,YZ)=f(XY,Z)+Zf(X,Y).$$

4) Für ein beliebiges Element x bzw. X aus $\mathfrak{o}$ bzw. $\mathfrak{O}$ gilt:

$$f(x,X)=0.$$

Ferner versteht man unter einer *normalen* 1-Kokette g von $\mathfrak{O}/\mathfrak{o}$ über $\mathfrak{O}_{\mathfrak{P}}$ eine lineare Abbildung von $\mathfrak{O}$ in $\mathfrak{O}_{\mathfrak{P}}$, welche für ein beliebiges Element x aus $\mathfrak{o}$ bzw. X aus $\mathfrak{O}$ stets den Gleichungen

$$g(x)=0 \quad \text{und} \quad g(xX)=xg(X)$$

genügen. Setzt man dann für beliebige Elemente X, Y aus $\mathfrak{O}$

$$\delta g(X, Y)=Yg(X)+Xg(Y)-g(XY),$$

so ist δg offenbar ein normaler 2-Kozyklus von $\mathfrak{O}/\mathfrak{o}$ über $\mathfrak{O}_{\mathfrak{P}}$; δg heißt der 2-Korand von g. Definiert man nun die Summe von zwei Kozyklen in üblicher Weise, so bildet die Gesamtheit $Z^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})$ aller normalen 2-Kozyklen von $\mathfrak{O}/\mathfrak{o}$ über $\mathfrak{O}_{\mathfrak{P}}$ einen Modul mit $\mathfrak{O}_{\mathfrak{P}}$ als Multiplikatorenbereich; ebenso bildet die Gesamtheit $B^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})$ der 2-Koränder aller normalen 1-Koketten einen $\mathfrak{O}_{\mathfrak{P}}$-Untermodul von $Z^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})$. Der Faktormodul $H^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})$ nach $B^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})$ heißt die *normale 2-Kohomologiegruppe* von $\mathfrak{O}/\mathfrak{o}$ über $\mathfrak{O}_{\mathfrak{P}}$. Jedes Element aus $H^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})$ nennt man eine normale 2-Kohomologieklasse und insbesondere ist $B^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})$ die Nullklasse genannt.

Es sei $H^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})=U_0 \supsetneqq U_1 \supsetneqq \cdots \supsetneqq U_i \supsetneqq \cdots$ eine absteigende Folge von den $\mathfrak{O}_{\mathfrak{P}}$-Untermoduln aus $H^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})$ von der Art, daß sie im endlichen abbricht (d.h. das letzte Glied der Folge ist die Nullklasse) und jeder Faktormodul U_i/U_{i+1} $(i \geqq 0)$ ein einfacher $\mathfrak{O}_{\mathfrak{P}}$-Modul ist. Dann heißt diese Folge eine $\mathfrak{O}_{\mathfrak{P}}$-Kompositionsreihe von $H^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})$; dabei ist die Länge einer $\mathfrak{O}_{\mathfrak{P}}$-Kompositionsreihe eine Invariante von $H^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})$ und sie heiße die *$\mathfrak{O}_{\mathfrak{P}}$-Länge* von $H^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})$.

2. Die Struktur der normalen 2-Kohomologiegruppe $H^{(2)}(\mathfrak{O}_{\mathfrak{P}}/\mathfrak{o}_{\mathfrak{p}}; \mathfrak{O}_{\mathfrak{P}})$ von $\mathfrak{O}_{\mathfrak{P}}/\mathfrak{o}_{\mathfrak{p}}$ über $\mathfrak{O}_{\mathfrak{P}}$ habe ich bereits bestimmt ([1]), und zwar gilt folgender

Hauptsatz. *Die normale 2-Kohomologiegruppe $H^{(2)}(\mathfrak{O}_{\mathfrak{P}}/\mathfrak{o}_{\mathfrak{p}}; \mathfrak{O}_{\mathfrak{P}})$ besitzt eine endliche $\mathfrak{O}_{\mathfrak{P}}$-Basis; das annullierende Ideal aus $\mathfrak{O}_{\mathfrak{P}}$ einer beliebigen normalen 2-Kohomologieklasse von $\mathfrak{O}_{\mathfrak{P}}/\mathfrak{o}_{\mathfrak{p}}$ über $\mathfrak{O}_{\mathfrak{P}}$ ist stets ein Teiler von $\mathfrak{D}_{\mathfrak{P}}(K/k)$. Ferner ist die $\mathfrak{O}_{\mathfrak{P}}$-Länge von $H^{(2)}(\mathfrak{O}_{\mathfrak{P}}/\mathfrak{o}_{\mathfrak{p}}; \mathfrak{O}_{\mathfrak{P}})$ gleich dem $\mathfrak{P}$-Exponenten von $\mathfrak{O}_{\mathfrak{P}}(K/k)$.*

Man kann auch beweisen, daß $H^{(2)}(\mathfrak{O}_{\mathfrak{P}}/\mathfrak{o}_{\mathfrak{p}}; \mathfrak{O}_{\mathfrak{P}})$ ein zyklischer $\mathfrak{O}_{\mathfrak{p}}$-Modul ist, wenn $\mathfrak{O}_{\mathfrak{P}}$ über $\mathfrak{o}_{\mathfrak{p}}$ *einfach normal* ist (d.h. $\mathfrak{O}_{\mathfrak{P}}$ entsteht aus $\mathfrak{o}_{\mathfrak{p}}$ durch Ringadjunktion eines einzigen Elementes). Da die Differente von $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ dann und nur dann der größte gemeinsame Teiler der Differenten aller Elementen aus $\mathfrak{O}_{\mathfrak{P}}$ ist, wenn $\mathfrak{O}_{\mathfrak{P}}$ über $\mathfrak{o}_{\mathfrak{p}}$ einfach normal ist, so schließt man ohne weiteres:

Satz 1. *Die Differente von $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ ist ein gemeinsamer, aber kein größter gemeinsamer Teiler der Differenten aller Elemente aus $\mathfrak{O}_{\mathfrak{P}}$, wenn $H^{(2)}(\mathfrak{O}_{\mathfrak{P}}/\mathfrak{o}_{\mathfrak{p}}; \mathfrak{O}_{\mathfrak{P}})$ kein zyklischer $\mathfrak{O}_{\mathfrak{P}}$-Modul ist.*

Ferner kann man beweisen, daß jeder normale 2-Kozyklus von $\mathfrak{O}/\mathfrak{o}$ über $\mathfrak{O}_{\mathfrak{P}}$ stets als die Einschränkung eines normalen 2-Kozyklus von $\mathfrak{O}_{\mathfrak{P}}/\mathfrak{o}_{\mathfrak{p}}$ über $\mathfrak{O}_{\mathfrak{P}}$ auf $\mathfrak{O}/\mathfrak{o}$ betrachtet werden kann, und daß $H^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})$ zu $H^{(2)}(\mathfrak{D}_{\mathfrak{P}}/\mathfrak{o}_{\mathfrak{p}}; \mathfrak{O}_{\mathfrak{P}})$ $\mathfrak{O}_{\mathfrak{P}}$-isomorph ist.

Satz 2. *Die normale 2-Kohomologiegruppe $H^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})$ ist $\mathfrak{O}_{\mathfrak{P}}$-isomorph zu $H^{(2)}(\mathfrak{O}_{\mathfrak{P}}/\mathfrak{o}_{\mathfrak{p}}; \mathfrak{O}_{\mathfrak{P}})$. Also ist der $\mathfrak{P}$-Exponent der Differente von K/k gleich der $\mathfrak{O}_{\mathfrak{P}}$-Länge von $H^{(2)}(\mathfrak{O}/\mathfrak{o}; \mathfrak{O}_{\mathfrak{P}})$.*

Okayama Universität

Bibliographie

[1] M. Moriya, Theorie der 2-Cohomologiegruppen in diskret bewerteten perfekten Körpern, Proc. of the Japan Acad., **30** (1954), 787–790.

[2] M. Moriya, Theorie der 2-Kohomologiegruppen in diskret bewerteten perfekten Körpern, Math. Journ., Okayama Univ., **5** (1955), No. 1, 43–77.

Idealtheorie in Unendlichen Algebraischen Zahlkörpern

Noboru Nakano

Unter einem unendlichen algebraischen Zahlkörper verstehen wir, wie gewöhnlich, den Körper, welcher als der Vereinigungskörper von abzählbar unendlich vielen algebraischen Zahlkörpern $\mathfrak{K}_1 \subset \mathfrak{K}_2 \subset \cdots \subset \mathfrak{K}_\nu \subset \mathfrak{K}_{\nu+1} \subset \cdots$ definiert wird, wobei jedes $\mathfrak{K}_\nu$ von endlichem Grade in Bezug auf den Rationalkörper $\mathfrak{K}_0$ ist. Ferner bezeichnen wir mit $\mathfrak{O}$, $\mathfrak{O}_\nu$ resp. die Menge aller ganzen algebraischen Zahlen aus $\mathfrak{K}$, $\mathfrak{K}_\nu$.

In $\mathfrak{O}$ ist dann der Teilerkettensatz nicht immer gültig. Danach kann ein von Einheits- und Null-ideal verschiedenes Ideal $\mathfrak{a}$ in $\mathfrak{O}$ idempotent sein und $\mathfrak{a}$ kann nicht immer endlich viele Primidealteiler besitzen (Stiemke [1]). Unter diesen Umständen haben wir oft $\mathfrak{a}=\mathfrak{b}\mathfrak{a}$ und $\mathfrak{a}:\mathfrak{b}=\mathfrak{a}$, obwohl $\mathfrak{a}$ ein von Nullideal verschiedenes Ideal und $\mathfrak{b}$ ein von $\mathfrak{O}$ verschiedener Teiler von $\mathfrak{a}$ ist. Im ersten Paragraphen wollen wir somit die notwendige und hinreichende Bedingung dafür suchen, dass $\mathfrak{a}=\mathfrak{b}\mathfrak{a}$ oder $\mathfrak{a}:\mathfrak{b}=\mathfrak{a}$ ist.

In seiner Arbeit hat Herr W. Krull die bewertungstheoretische Behandlung der Idealtheorie in $\mathfrak{O}$ entwickelt und in der Methode von der Topologisierung des Bewertungsringraumes eine notwendige und hinreichende Bedingung dafür untersucht, dass für zwei gegebene Ideale $\mathfrak{a}$ und $\mathfrak{b}$ ein Ideal $\mathfrak{c}$ existiert, so dass es der Gleichung $\mathfrak{a}=\mathfrak{b}\mathfrak{c}$ genügt. Seine Untersuchung beschäftigt sich mit dem Fall, dass $\mathfrak{a}$ und $\mathfrak{b}$ die genannten „*überall endlichen Ideale*“ sind (Krull [3]). Im zweiten Paragraphen wollen wir dann in der idealtheoretischen Methode dieses Problem untersuchen.

In (3), (4) im §1 und im §2 wollen wir darum eine *Annahme* über die zugrund gelegten Ideale machen; Es sei $\mathfrak{q}$ die zu einem beliebigen Primideal $\mathfrak{p}$ gehörige isolierte Primärkomponente (kurz mit I.P.K.) von einem Ideal $\mathfrak{a}$ und sei N ein hinreichend grosser Index, so muss $\mathfrak{q} \frown \mathfrak{O}_\nu$ die zu $\mathfrak{p} \frown \mathfrak{O}_\nu$ gehörige I.P.K. von $\mathfrak{a} \frown \mathfrak{O}_\nu$ für alle ν $(\nu \geqq N)$ sein und N muss für alle $\mathfrak{p}$ beschränkt sein (Nakano [9], s. 274, Hilfssatz 1).

§1. Produkte und Quotienten von Idealen.

(1) Ein Ideal ist dann und nur dann idempotent, wenn seine sämtli-

chen Primärkomponenten gleich idempotente Primideale sind (Nakano [5]). Ist $\mathfrak{a}$ ein nicht idempotentes Ideal, so ist $\bigcap_{n=1}^{\infty}\mathfrak{a}^n=(o)$.

(2) Zu zwei gegebenen Idealen $\mathfrak{a}$ $(\neq(o))$ und $\mathfrak{b}$ $(\neq\mathfrak{O})$ erhalten wir dann und nur dann $\mathfrak{a}=\mathfrak{a}\mathfrak{b}$, wenn $\mathfrak{b}=\mathfrak{b}^2$ und $\mathfrak{q}=\mathfrak{q}\mathfrak{p}$ für alle zu $\mathfrak{p}$ $(\geqq\mathfrak{b}\supset\mathfrak{a})$ gehörigen I.P.K. $\mathfrak{q}$ von $\mathfrak{a}$ sind. Aus $\mathfrak{a}=\mathfrak{a}\mathfrak{b}$ folgt $\mathfrak{b}=\mathfrak{b}^2$, aber nicht umgekehrt.

(3) Es sei $\mathfrak{a}=\mathfrak{q}\frown(\bigcap_{\tau}\mathfrak{q}_{(\tau)})$, wobei $\mathfrak{q}$, $\mathfrak{q}_{(\tau)}$, $\tau\in\mathfrak{J}$ alle zu Primidealen $\mathfrak{p}$, $\mathfrak{p}_{(\tau)}$ gehörigen I.P.K. von $\mathfrak{a}$ sind. Dann erhalten wir mit Hilfe obiger *Annahme*

(i) $\mathfrak{q}\supset\bigcap_{\tau}\mathfrak{q}_{(\tau)}$ $\rightleftarrows$ (ii) $\mathfrak{p}\supset\bigcap_{\tau}\mathfrak{q}_{(\tau)}$ $\rightleftarrows$ (iii) $\mathfrak{p}\supset\bigcap_{\tau}\mathfrak{p}_{(\tau)}$.

(4) Es sei $\mathfrak{a}=\mathfrak{q}\frown(\bigcap_{\tau}\mathfrak{q}_{(\tau)})$, so ist dann und nur dann $\mathfrak{a}:\mathfrak{p}=\mathfrak{a}$, wenn $\mathfrak{q}:\mathfrak{p}=\mathfrak{q}$ oder $\mathfrak{p}\supset\bigcap_{\tau}\mathfrak{p}_{(\tau)}$ ist (mit Hilfe von (3)). Aus $\mathfrak{a}:\mathfrak{p}=\mathfrak{a}$ folgt $\mathfrak{p}=\mathfrak{p}^2$ oder $\mathfrak{p}\supset\bigcap_{\tau}\mathfrak{p}_{(\tau)}$, aber nicht umgekehrt.

(5) Es sei $\mathfrak{b}$ $(\neq\mathfrak{O})$ ein Teiler von $\mathfrak{a}$ $(\neq(o))$, so erhalten wir $\mathfrak{a}:\mathfrak{b}=\mathfrak{a}$, wenn $\mathfrak{b}=\mathfrak{b}^2$ und $\mathfrak{q}:\mathfrak{p}=\mathfrak{q}$ für alle zu $\mathfrak{p}$ $(\geqq\mathfrak{b}\supset\mathfrak{a})$ gehörigen I.P.K. $\mathfrak{q}$ von $\mathfrak{a}$ sind.

(6) Wenn $\mathfrak{a}:\mathfrak{b}=\mathfrak{a}$, $\mathfrak{a}\subset\mathfrak{b}$ und $\mathfrak{b}\neq\mathfrak{b}^2$ sind, dann existieren mindestens endlich viele nicht-idempotente I.P.K. $\mathfrak{q}_{(t)}^{(b)}$ $(t=1,2,\cdots,n)$ von $\mathfrak{b}$. Ist $\mathfrak{q}_{(t)}^{(a)}$ eine zu $\mathfrak{p}_{(t)}$ $(\geqq\mathfrak{q}_{(t)}^{(b)})$ gehörige I.P.K. von $\mathfrak{a}$, und stellen wir $\mathfrak{a}$ in der Form von $\mathfrak{a}=\mathfrak{a}'\frown\mathfrak{a}''$ dar, wobei $\bigcap_{t=1}^{n}\mathfrak{q}_{(t)}^{(a)}=\mathfrak{a}'$, $\bigcap_{\xi}\mathfrak{q}_{(\xi)}=\mathfrak{a}''$, so wird $\mathfrak{a}'\supset\mathfrak{a}''$. Daraus ergibt sich: Wenn $\mathfrak{a}:\mathfrak{b}=\mathfrak{a}$, $\mathfrak{a}\subset\mathfrak{b}$ ist, dann erhalten wir entweder $\mathfrak{b}=\mathfrak{b}^2$ oder $\mathfrak{a}'\supset\mathfrak{a}''$.

§2. Multiplikativeigenschaft der Ideale.

In $\mathfrak{O}$ können wir die zum Primideal $\mathfrak{p}$ gehörigen Primäridealen $\mathfrak{q}$ in folgende vier Arten einteilen (Nakano [6]);

$$\begin{array}{lll}
\text{A.}\ \ \mathfrak{p}\neq\mathfrak{p}^2; & \text{(i)} & \mathfrak{q}\ \text{heisst erste Art, wenn}\ \mathfrak{q}\mathfrak{p}\neq\mathfrak{q},\ \mathfrak{q}:\mathfrak{p}\neq\mathfrak{q}\ \text{sind,} \\
\text{B.}\ \ \mathfrak{p}=\mathfrak{p}^2; & \left\{\begin{array}{l}\text{(ii)} \\ \text{(iii)} \\ \text{(iv)}\end{array}\right. & \begin{array}{l}\mathfrak{q}\ \text{heisst zweite Art, wenn}\ \mathfrak{q}\mathfrak{p}\neq\mathfrak{q},\ \mathfrak{q}:\mathfrak{p}=\mathfrak{q}\ \text{sind,} \\ \mathfrak{q}\ \text{heisst dritte Art, wenn}\ \mathfrak{q}\mathfrak{p}=\mathfrak{q},\ \mathfrak{q}:\mathfrak{p}\neq\mathfrak{q}\ \text{sind,} \\ \mathfrak{q}\ \text{heisst vierte Art, wenn}\ \mathfrak{q}\mathfrak{p}=\mathfrak{q},\ \mathfrak{q}:\mathfrak{p}=\mathfrak{q}\ \text{sind.}\end{array}
\end{array}$$

(1) Ein Ideal, dessen jede isolierte Primärkomponente von erster oder zweiter Art ist, soll nach Herrn W. Krull „*überall endlich*“ heissen. Unter Hinzufügung unserer *Annahme* gilt dabei folgender Satz; Sind $\mathfrak{a}$ und $\mathfrak{b}$ überall endliche Ideale und ist $\mathfrak{a}\subset\mathfrak{b}$, so gibt es dann und nur dann $\mathfrak{c}$ von der Art, dass $\mathfrak{a}=\mathfrak{b}\mathfrak{c}$ ist, wenn

$$\cdots\subseteqq\mathfrak{a}_\nu:\mathfrak{b}_\nu\subseteqq\mathfrak{a}_{\nu+1}:\mathfrak{b}_{\nu+1}\subseteqq\cdots\subseteqq\mathfrak{a}_\lambda:\mathfrak{b}_\lambda\subseteqq\cdots$$

ist, wobei $\mathfrak{a}_\nu=\mathfrak{a}\frown\mathfrak{O}_\nu$, $\mathfrak{b}_\nu=\mathfrak{b}\frown\mathfrak{O}_\nu$, $\nu\geqq N$ ist.

(2) Um diesen Satz zu erweitern, wollen wir folgende zwei Hilfssätze vorausschicken.

(i) Ist $\mathfrak{q}^{(a)}\subset\mathfrak{q}^{(b)}$ und setzen wir $\mathfrak{q}^{(a)}\frown\mathfrak{O}_\nu=\mathfrak{p}_\nu^{e_\nu}$, $\mathfrak{q}^{(b)}\frown\mathfrak{O}_\nu=\mathfrak{p}_\nu^{f_\nu}$ $\nu\geqq N$, so ist $\mathfrak{q}^{(a)}:\mathfrak{q}^{(b)}=\bar{\mathfrak{q}}$ oder $\mathfrak{q}$, wobei

$$\bar{\mathfrak{q}}=\{\cdots,\ \mathfrak{p}_{\nu}^{e_{\nu}}:\mathfrak{p}_{\nu}^{f_{\nu}},\ \mathfrak{p}_{\nu+1}^{e_{\nu+1}}:\mathfrak{p}_{\nu+1}^{f_{\nu+1}},\cdots,\ \mathfrak{p}_{\lambda}^{e_{\lambda}}:\mathfrak{p}_{\lambda}^{f_{\lambda}},\cdots\}$$

und
$$\mathfrak{q}=\{\cdots,\ \mathfrak{p}_{\nu}^{e_{\nu}+1}:\mathfrak{p}_{\nu}^{f_{\nu}},\ \mathfrak{p}_{\nu+1}^{e_{\nu+1}+1}:\mathfrak{p}_{\nu+1}^{f_{\nu+1}},\cdots,\ \mathfrak{p}_{\lambda}^{e_{\lambda}+1}:\mathfrak{p}_{\lambda}^{f_{\lambda}}\cdots\}$$

sind (Nakano [8]).

(ii) Es sei $\mathfrak{a}\subset\mathfrak{b}\subset\mathfrak{p}$ und $\mathfrak{q}^{(a)}$ bzw. $\mathfrak{q}^{(b)}$ die zu $\mathfrak{p}$ gehörige I.P.K. von $\mathfrak{a}$ bzw. $\mathfrak{b}$, und es sei $\mathfrak{h}$ der Durchschnitt von sämtlichen Primidealen $\mathfrak{p}$ derart, dass $\mathfrak{q}^{(a)}:\mathfrak{q}^{(b)}=\mathfrak{q}$ ist, und ferner sei

$$\cdots\subsetneqq\mathfrak{h}_{\nu}\mathfrak{a}_{\nu}:\mathfrak{b}_{\nu}\subsetneqq\mathfrak{h}_{\nu+1}\mathfrak{a}_{\nu+1}:\mathfrak{b}_{\nu+1}\subsetneqq\cdots\subsetneqq\mathfrak{h}_{\lambda}\mathfrak{a}_{\lambda}:\mathfrak{b}_{\lambda}\subsetneqq\cdots,$$

wobei $\mathfrak{h}_{\nu}=\mathfrak{h}\frown\mathfrak{O}_{\nu}$ ist. Dann ist $\mathfrak{q}$ die zu $\mathfrak{p}$ gehörige I.P.K. von $\mathfrak{a}:\mathfrak{b}$, so ist $\mathfrak{q}=\bar{\mathfrak{q}}$, wenn $\mathfrak{p}\not\supset\mathfrak{h}$ ist, und ist $\mathfrak{q}\supset\mathfrak{q}$, wenn $\mathfrak{p}\supset\mathfrak{h}$ ist.

Unter Hinzufügung unserer *Annahme* erhalten wir nach (i) und (ii) folgenden Hauptsatz; Sind $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale und ist $\mathfrak{a}\subset\mathfrak{b}$, so gibt es dann und nur dann $\mathfrak{c}$, derart, dass $\mathfrak{a}=\mathfrak{b}\mathfrak{c}$ ist, wenn für jede zwei entsprechende $\mathfrak{q}^{(a)}$, $\mathfrak{q}^{(b)}$ ein drittes $\mathfrak{q}$ existiert, derart dass $\mathfrak{q}^{(a)}=\mathfrak{q}^{(b)}\mathfrak{q}$ ist, und ferner

$$\cdots\subsetneqq\mathfrak{h}_{\nu}\mathfrak{a}_{\nu}:\mathfrak{b}_{\nu}\subsetneqq\mathfrak{h}_{\nu+1}\mathfrak{a}_{\nu+i}:\mathfrak{b}_{\nu+1}\subsetneqq\cdots\subsetneqq\mathfrak{h}_{\lambda}\mathfrak{a}_{\lambda}:\mathfrak{b}_{\lambda}\subsetneqq\cdots$$

ist, wobei $\mathfrak{h}_{\nu}$ in gleicher Weise wie oben (ii) definiert wird.

HIROSHIMA UNIVERSITÄT

BIBLIOGRAPHIE

[1] E. Stiemke, Über unendliche algebraische Zahlkörper (kurz U.A.Z.), Math. Zeit., **25** (1926), 9–39.

[2] W. Krull, Idealtheorie in U.A.Z., Math. Zeit., **29** (1929), 42–54.

[3] W. Krull, Idealtheorie in U.A.Z. (II), l.c., **31** (1930), 527–557.

[4] N. Nakano, Über den Fundamentalsatz der Idealtheorie in U.A.Z., Jour. Sci. of Hiroshima Univ., **15** (1952), 171–175.

[5] N. Nakano, Über idempotente Ideale in U.A.Z., l.c., **17** (1953), 11–20.

[6] N. Nakano, Über die Einteilung von Primäridealen in U.A.Z., l.c., **17** (1954), 321–343.

[7] N. Nakano, Über das Produkt von Primäridealen in U.A.Z., l.c., **18** (1954), 129–136.

[8] N. Nakano, Über den Primäridealquotienten in U.A.Z., l.c., **18** (1955), 257–269.

[9] N. Nakano, Idealtheorie im Stiemkeschen Körper, l.c., **18** (1955), 271–287.

On the Structure of Complete Local Rings[1]

Masao NARITA

I. S. Cohen proved a structure-theorem of complete local rings in his paper, "On the structure and ideal theory of complete local rings" (1946). We can extend this theorem to a more general one. In the following, the word "local ring" will be used to indicate a ring satisfying the following three conditions. (i) The local ring $\mathfrak{O}$ is a commuatative ring with unity 1. (ii) Every non-unit of $\mathfrak{O}$ belongs to the maximal ideal $\mathfrak{m}$ of $\mathfrak{O}$. (iii) $\bigcap_{i=1}^{\infty}\mathfrak{m}^i=(0)$. In the following, the symbols $\mathfrak{O}$, $\mathfrak{m}$, F and φ will be always used to express a local ring, its maximal ideal, its residue field $\mathfrak{O}/\mathfrak{m}$ and the canonical mapping of $\mathfrak{O}$ onto F, respectively.

LEMMA 1. *Let $\mathfrak{O}$ be a local ring with characteristic p. If there exists a positive integer n such that $\mathfrak{m}^{p^n}=(0)$, then $\mathfrak{O}$ contains a subfield K' which is isomorphic to F^{p^n}, such that $\varphi(K')=F^{p^n}$.*

Let ψ be the correspondence of F^{p^n} into $\mathfrak{O}$ such that $\psi(\alpha^{p^n})=a^{p^n}$, $\alpha\in F$, $a\in\varphi^{-1}(\alpha)$. It is to be noticed that a^{p^n} is uniquely determined by α^{p^n}. Then $\psi(F^{p^n})$ is a required subfield of $\mathfrak{O}$.

LEMMA 2. *Let $\mathfrak{O}$ be a local ring satisfying the same conditions as Lemma 1. Then $\mathfrak{O}$ contains a subfield K which is isomorphic to F such that $\varphi(K)=F$.*

Let $\{\gamma_\tau\}_{\tau\in\Gamma}$ be a p-basis of F. Let us choose arbitrarily an element c_τ once for all from $\varphi^{-1}(\gamma_\tau)$, $\tau\in\Gamma$. The subfield of $\mathfrak{O}$ which is generated by K' and $\{c_\tau\}_{\tau\in\Gamma}$ is a required subfield of $\mathfrak{O}$.

THEOREM 1. *Let $\mathfrak{O}$ be a complete local ring with the same characteristic as the residue field F, then $\mathfrak{O}$ contains a subfield K which is isomorphic to F, such that $\varphi(K)=F$.*[2]

In case where the characteristic of $\mathfrak{O}$ and F are both zero, this theorem may be easily proved by using Hensel's lemma.[3] So we shall assume that F has a characteristic p. By Lemma 2, the ring $\mathfrak{O}/\mathfrak{m}^i$, $i=1,2,3,\cdots$ contains a subfield K_i which is isomorphic to F. Moreover we can assume that K_{i+1} is mapped on K_i by the canonical mapping $\mathfrak{O}/\mathfrak{m}^{i+1}\rightarrow\mathfrak{O}/\mathfrak{m}^i$. Let α_i be an element of K_i which corresponds to $\alpha\in F$ under the correspondence $\mathfrak{O}/\mathfrak{m}\rightarrow F$, and a_i be an element of $\mathfrak{O}$ such that a_i is mapped on α_i under the mapping $\mathfrak{O}\rightarrow\mathfrak{O}/\mathfrak{m}^i$. Then the sequence $a_1, a_2, a_3,\cdots$ is a Cauchy sequence, so has a limit in $\mathfrak{O}$. This limit is independent of the choice of a_i, and is uniquely determined by the sequence $\alpha_1, \alpha_2,\cdots$. The subset of $\mathfrak{O}$ which consists of such limits is a required subfield of $\mathfrak{O}$.

LEMMA 3. *Let $\mathfrak{O}$ be a local ring having a characteristic different from the characteristic of F. If there exists a positive integer n such that $\mathfrak{m}^n=(0)$, then $\mathfrak{O}$ contains a subring $\mathfrak{O}_0$ with a maximal ideal (p) such that $\varphi(\mathfrak{O}_0)=F$.*

Let ψ be the mapping of F^{p^n} into $\mathfrak{O}$ such that $\psi(\alpha^{p^n})=a^{p^n}$, $\alpha\in F$, $a\in\varphi^{-1}(\alpha)$. We write $A_{pn}, A_{pn+1},\cdots, A_{p2n}$ for $\psi(F^{p^n}), \psi(F^{p^{n+1}}),\cdots,\psi(F^{p^{2n}})$ respectively. Put now $A=A_{p2n}+pA_{p2n-1}+p^2A_{p2n-2}+\cdots+p^{n-1}A_{pn+1}$, then A is a subring of $\mathfrak{O}$. Let R be a ring generated by A and $\{c_\tau\}_{\tau\in\Gamma}$, $c_\tau\in\varphi^{-1}(\gamma_\tau)$. Then R is a required subring of $\mathfrak{O}$.

THEOREM 2. *A complete local ring $\mathfrak{O}$ having a characteristic different from the characteristic of F contains a complete subring $\mathfrak{O}_0$ with a maximal ideal (p) such that $\varphi(\mathfrak{O}_0)=F$.*

It is easy to prove this theorem by using Lemma 3 in the same way as we proved Theorem 1 by using Lemma 2.

The following theorem is evident by the proof of Theorem 2.

THEOREM 3. *Let $\mathfrak{O}$ be a complete local ring having a characteristic different from the characteristic of F, then every complete subring of $\mathfrak{O}$ with a maximal ideal (p), which is mapped on F by φ, is mutually isomorphic to each other.*

INTERNATIONAL CHRISTIAN UNIVERSITY

NOTES

1) Details of the proofs were published on Journal of Mathematical Society of Japan, Vol. 7, Supplement, 1955.

2) A. Geddes also proved this theorem by an analogous method as ours. See J. Lond. Math. Soc., **29** (1954), pp. 334–341. He treated only the equi-characteristic case, and did not prove Theorem 2 of this paper.

3) See M. Nagata's paper, "On the structure of complete local rings," Nagoya Math. J., **1** (1950), pp. 63–70.

On Orthogonal Groups over Number Fields

Takashi ONO

It is well known as the "Hasse principle" that the representability of a quadratic form (with coefficients in an algebraic number field) by another form follows from the local representabilities everywhere. If we wish to consider arithmetic properties of the algebraic groups over number fields, the first thing to do would be to get some results of this type for the orthogonal groups, since they can be treated in close relation with the corresponding quadratic forms by the method of Dieudonné [1] and, at the same time, these groups play roles for the algebraic groups as in the classical theory of Lie groups.

For this reason, we have tried in [3] and [4] to consider the imbedding (in a certain sense) of an orthogonal group $O(W, g)$ in another orthogonal group $O(V, f)$, where f, g are quadratic forms on the spaces V and W respectively. (For two forms f, g on the same V, the imbedding of groups turns out to be the conjugateness of $O(V, f)$ and $O(V, g)$ in $GL(V)$).

Let K be a field of characteristic $\neq 2$, and let V and W be finite dimensional vector spaces over K. Suppose that there is a semi-linear mapping Θ of W into V. Let f be a symmetric bilinear form on V. We denote by Θf a form on W which is defined by $\Theta f(x, y) = (f(\Theta x, \Theta y))^{\theta^{-1}}$ for $x, y \in W$, where θ is the automorphism of K associated with Θ. Now suppose that two nondegenerate forms f and g are given on the spaces V and W respectively. We say that f semi-similarly represents $g: f \overset{\propto}{\to} g$, if $g = \lambda \cdot \Theta f$ for some semi-linear injection Θ of W into V and for some $\lambda \in K^*$. If the injection Θ is linear, we say that f similarly represents $g: f \overset{\infty}{\to} g$, and furthermore, if the scalar $\lambda = 1$, then we say simply that f represents $g: f \overset{\sim}{\to} g$. Particularly if V and W have the same dimensionalities, we take away the arrows in the above notations and say that f and g are semi-similar: $f \propto g$, similar: $f \infty g$ and congruent: $f \sim g$ respectively.

Proposition 1. *If $f \overset{\infty}{\to} g$, then we have $0 \leqq \nu(f) - \nu(g) \leqq \dim V - \dim W$, where $\nu(f)$ is the index of f on V.*

Now, for a form f on a space V, we denote by $O(V, f)$ the orthogonal of f, by $O^+(V, f)$ the rotation group of f and by $\Omega(V, f)$ the commutator subgroup of $O(V, f)$. Furthermore, we denote by $\Gamma(V, f)$ any one of these three types of groups. Let W_0 be another vector space and let Θ be a semi-linear isomorphism between W_0 and V. Let σ be $\in GL(V)$. We define $\Theta\sigma \in GL(W)$ by putting $\Theta\sigma(w) = \Theta^{-1}\sigma\Theta(w)$, $w \in W$. It implies that σ leaves f invariant if and only if $\Theta\sigma$ leaves Θf invariant. We have that $\Theta(\Gamma(V, f)) = \Gamma(W, \Theta f)$, where the groups Γ's on both sides belong to the same type of those three groups. (We always use two Γ's in this sense.) Assume that there are forms f, g on the spaces V, W respectively. We say that the group $\Gamma(W, g)$ is semi-linearly imbedded in $\Gamma(V, f)$, if $\Theta(\Gamma(\Theta(W), f_1)) = \Gamma(W, g)$ for some semi-linear injection Θ of W into V, where f_1 is the restriction of f to $\Theta(W)$. Particularly, if $\Gamma(W, g)$ is semi-linearly imbedded in $\Gamma(V, f)$ with a linear injection Θ, we say simple that $\Gamma(W, g)$ is linearly imbedded in $\Gamma(V, f)$. Using these terminologies, we get the following

Theorem 1. *$\Gamma(W, g)$ is (semi)-linearly imbedded in $\Gamma(V, f)$ if and only if f (semi)-similarly represents $g: f \overset{\propto}{\to} g (f \overset{\infty}{\to} g)$.*

For a form f on V, let e_i $(i = 1, \cdots, n)$ be some orthogonal basis. Put $a_i = f(e_i, e_i)$ and $d_i = a_1 \cdots a_i$. We define the Clifford algebra $C(f)$ of f as a tensor product over $K: C(f) = (a_1, d_1) \otimes (a_2, d_2) \otimes \cdots \otimes (a_n, d_n)$, where (a, b) is the quaternion algebra defined by a, b. (This algebra is different from the habitual one. That is the one introduced by Witt as $S(f)$ in [5]). As for the discriminant $d(f)$ of a form f, we set $\Delta(f) = (-1)^{n(n-1)/2} \cdot d(f)$, where $n = \dim V$. We put $A(f, g) = C(f) \otimes C(g) \otimes (d(g), d(f)d(g))$, $B(f, g) = A(f, g) \otimes (-1, d(f)d(g))$.

Since the possibility of the imbedding of groups may be characterized by the similar representability of forms: $f \overset{\infty}{\to} g$ (Theorem 1), our problems are reduced to the propositions of Hasse type for the representability of forms which may be regarded as a complement of a series of theorems due to Hasse [2].

Now, assume that K is a locally compactly valued field of characteristic $\neq 2$.

Proposition 2. *Let K be non-archimedean. Let $n = \dim V$, $m = \dim W$. Then,*

i) *if $n - m = 1$, n: odd, $f \overset{\propto}{\to} g$ if and only if $B(f, g) \sim 1$ in $K(\sqrt{\Delta(g)})$,*

ii) *if* $n-m=1$, n: *even*, $f \overset{\infty}{\to} g$ *if and only if* $B(f, g) \sim 1$ *in* $K(\sqrt{\varDelta(f)})$,

iii) *if* $n-m=2$, n: *odd*, $f \overset{\infty}{\to} g$ *always*,

iv) *if* $n-m=2$, n: *even*, $f \overset{\infty}{\to} g$ *if and only if* $B(f, g) \sim 1$ *in* $K(\sqrt{\varDelta(f)}, \sqrt{\varDelta(g)})$,

v) *if* $n-m \geqq 3$, $f \overset{\infty}{\to} g$ *always*.

In the local considerations, we meet the question, "how do the p-adic numbers resemble the real numbers?". In fact, as in the following theorem, we can generalize several statements on the real numbers which are proved by the methods peculier to these numbers to the case of completely valued fields.

THEOREM 2. *Let K be locally compatly vnlued. Assume that* $\dim V \geqq \dim W$. *Then, the following three conditions are equivalent.*

i) *f simil rly represents* $g : f \overset{\infty}{\to} g$,

ii) $0 \leqq \nu(f) - \nu(g) \leqq \dim V - \dim W$, (*For the case where* $\dim V = \dim W$ *is even and K is non-archimedean, we add the condition* $d(f) \sim d(g)$.

iii) *$\Gamma(W, g)$ is linearly imbedded in $\Gamma(V, f)$.*

It is remarkable that although the discriminants and Clifford algebras of forms are used to characterize the usual representability forms over local fields, the similar representability may be characterized by the indices of forms which are a much simpler notion than the Clifford algebras.

Now, let K be either a field of algebraic numbers or a field of algebraic functions of one variable over a finite field of characteristic $\neq 2$. By using the arithmetic theory of simple algebras and our considerations above, we get the following theorems of Hasse type.

THEOREM 3. *$f \overset{\infty}{\to} g$ in K if and only if $f \overset{\infty}{\to} g$ in $K_{\mathfrak{p}}$ for every $\mathfrak{p}$.*

THEOREM 4. *$f \overset{\infty}{\to} g$ in K if and only if* $0 \leqq \nu_{\mathfrak{p}}(f) - \nu_{\mathfrak{p}}(g) \leqq \dim V - \dim W$ *for every $\mathfrak{p}$.*

THEOREM 5. *$\Gamma(W, g)$ is linearly imbedded in $\Gamma(V, f)$ if and only if $\Gamma(W_{\mathfrak{p}}, g)$ is linearly imbedded in $\Gamma(V_{\mathfrak{p}}, f)$ for every $\mathfrak{p}$.*

From Theorem 4, we observe some examples showing that a global property comes from weaker local properties everywhere. E.g. "If $f \overset{\infty}{\to} g$ in $K_{\mathfrak{p}}$ for every $\mathfrak{p}$, then $f \overset{\infty}{\to} g$ in K". "If $O(W_{\mathfrak{p}}, g)$ is topologically imbedded in $O(V_{\mathfrak{p}}, f)$ for everg $\mathfrak{p}$, then $O(W, g)$ is linearly imbedded in $O(V, f)$". We may further weaken the local assumptions under certain conditions on W.

NAGOYA UNIVERSITY

BIBLIOGRAPHY

[1] J. Dieudonné, Sur les groupes classiques, Actual. Scient. et Ind., no. 1040, Paris, 1948.

[2] H. Hasse, Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen, Crelles J., **152** (1923), pp. 129-148. etc.

[3] T. Ono, Arithmetic of Orthogonal Groups, J. Math. Soc. Japan, **7** (1955). pp. 79-91.

[4] T. Ono, Arithmetic of Orthogonal Groups, II, Nagoya Math. J., **9** (1955), pp. 129–146

[5] E. Witt, Theorie der quadratischen Formen in beliebigen Körpern, Crelles J., **176** (1937), pp. 31–44.

On Fermat Function Fields

Shuichi TAKAHASHI

1. Definition of Fermat function fields. Let Q be the field of rational numbers, a, b non-zero elements of Q, then the solution of the equation

$$ax^l+by^l+1=0 \qquad (l\text{: odd prime}) \tag{1}$$

generates a function field $K=Q(x, y)$ which after Hasse is called a Fermat function field. Hasse's original investigation [1] is devoted to the determination of its genus

$$g=(l-1)(l-2)/2$$

and g linearly independent holomorphic differentials and some remarks on Weierstrass points.

2. Purpose of this investigation. Equation

$$ax^l+by^l+z^l=0 \tag{2}$$

determines an absolutely irreducible non-singular curve Γ in the projective plane (x, y, z), and geometrically equation (2) and Fermat's equation

$$x^l+y^l+z^l=0 \tag{3}$$

determine the same curve over a field of definition $\overline{Q}$ (the algebraic closure of Q).

Many investigators on Fermat's problem concern the non-trivial rational integral points on Γ. From this respect Hasse's investigation is isolated, and he does not even enter into the integral properties of the coefficient field. The main purpose of this note is to fill up this gap.

3. Characteristic preserving specializations. Let us consider the function field K or its coefficient extension $K\cdot k_0$. An important case is $k_0=Q(\zeta)$, where ζ is a primitive l-th root of unity. Then our first method is to specialize K (or $K\cdot k_0$) over Q (or over k_0) to an algebraic extension k of Q (or k_0) by a prime divisor of K (or of $K\cdot k_0$). This method used by Weil [2] and Siegel [3] gives upper bound of the number of rational solutions of (1). Here Weil's notion of the distribution [4] plays an important role.

4. Characteristic increasing specializations. Our next method is to specialize the function field $K \cdot k_0$ over k_0 by a divisor of $K \cdot k_0$ induced by a prime divisor P of k_0. Then the function field becomes $K \cdot k_0/(P)$ by this specialization. For $p = l$ this method was used by Legendre, Wendt, Dickson and others and fruitful results are found by the principle used by Vinogradoff on Goldbach's problem [5] and on Waring's problem [6] and by Siegel on quadratic forms [7]. In this direction Hasse-Weil's zeta-function plays an important role.

TÔHOKU UNIVERSITY

BIBLIOGRAPHY

[1] H. Hasse, Über den algebraischen Funktionenkörper der Fermatschen Gleichung, Acta de Szeged, **13** (1949–50), 195–207.

[2] A. Weil, L'arithmétique sur les courbes algébriques, Acta Math., **52** (1929), 281–315.

[3] C. L. Siegel, Über einige Anwendungen Diophantischer Approximationen, Abh. Preuss. Akad., 1929, 70 pp.

[4] A. Weil, Arithmetic on algebraic varieties, Ann. of Math., **53** (1951), 412–444.

[5] I. M. Vinogradoff, Some theorems concerning the theory of primes, Rec. Math., **2** (1937), 179–195.

[6] I. M. Vinogradoff, On Waring's problem, Ann. of Math., **36** (1935), 395–405.

[7] C. L. Siegel, Über die analytische Theorie der quadratischen Formen, Ann. of Math., **36** (1935), 527–606.

[8] A. Weil, Numbers of solutions of equations in finite fields, Bull. A.M.S., **55** (1949), 497–508.

[9] A. Weil, Jacobi sums as "Grössencharaktere", Trans. A.M.S., **73** (1952), 487–495.

Über die Struktur der Metabelschen Gruppen

Kiyosi TAKETA

$\mathfrak{G}$ sei maximale metabelsche Gruppe, die eine gegebene Abelsche Gruppe $\mathfrak{A}$ als einen maximalen Abelschen Normalteiler enthält.

Wir wollen hier die Invarianten der Faktorgruppe $\mathfrak{G}/\mathfrak{A}$ bestimmen.

Seien $\sigma_1, \sigma_2, \cdots, \sigma_g$ erzeugende Elemente von $\mathfrak{G}/\mathfrak{A}$ also $\mathfrak{G} = \{\sigma_1, \sigma_2, \cdots, \sigma_g, \mathfrak{A}\}$, dann stellen die Automorphismen $\mathfrak{a}^\sigma \rightarrow \mathfrak{a}$ die Faktorgruppe $\mathfrak{G}/\mathfrak{A}$ treu dar.

Unsre Frage führt sich also zu der die Invarianten von solchen Automorphismengruppe Γ zu bestimmen.

Man nimmt o.B.d.A. an, daß $\mathfrak{A}$ eine p-Gruppe sei, und a_i; $i = 1, 2, \cdots, n$, ihre Basiselemente mit der Ordnung p^{α_i} der Art, daß

$$\alpha_1 \leqq \alpha_2 \leqq \cdots \leqq \alpha_n.$$

Dann wird

$$a_i^{\sigma} = a_1^{a_{i1}} a_2^{a_{i2}} \cdots a_n^{a_{in}},$$

wobei

$$p^{\alpha_k - \alpha_i} \mid a_{ik}, \qquad i<k,$$

ist.

Γ wird eine Kongruenzgruppe mit den Matrizen der Gestalt

$$(1) \qquad A = \begin{pmatrix} a_{11} & a_{12} \cdots a_{1n} \\ a_{21} & a_{22} \cdots a_{2n} \\ \cdots & \cdots \\ \cdots & \cdots \\ a_{n1} & a_{n2} \cdots a_{nn} \end{pmatrix}$$

nach dem Modul

$$\begin{pmatrix} p^{\alpha_1} & p^{\alpha_2} \cdots p^{\alpha_n} \\ p^{\alpha_1} & p^{\alpha_2} \cdots p^{\alpha_n} \\ \vdots & \vdots \qquad \vdots \\ p^{\alpha_1} & p^{\alpha_2} \cdots p^{\alpha_n} \end{pmatrix}.$$

Alle Elemente Γ lassen sich in der Art setzen, daß

$$(2) \qquad A = \sum_{i=0}^{\alpha_n - 1} p^i A_i,$$

wobei

$$A_0 + pA_1 + \cdots + p^j A_j, \qquad j \leqq \alpha_n - 1,$$

nach dem mod p^{α_n} voneinander vertauschbar werden.

Dann wird Γ 1∼isomorph zu einer Kongruenzgruppe Γ_* mod p, deren Elemente die Gestalt

$$\begin{pmatrix} A_0 & & & & \\ A_1 & \cdot & & & \\ \cdot & \cdot & \cdot & & \\ & \cdot & \cdot & \cdot & \\ & & \cdot & \cdot & \cdot \\ A_{\alpha_n - 1} & \cdot & & A_1 & A_0 \end{pmatrix} \qquad \text{mod}\, p$$

annehmen.

Γ_* ist also vom Grade $\alpha_n n$, und die Frage führt sich zum Falle, wo $\mathfrak{A}$ bloß vom Typus $(1,1,\cdots,1)$ ist.

Fügt man alsdann o.B.d.A. noch die Annahme hizu, daß Γ irreduzibel sei, so wird Γ 1∼isomorph zu einer Gruppe $\mathfrak{P} \times \mathfrak{H}$, wobei $\mathfrak{H}$ eine zyklische Gruppe der Ordnung $p^u - 1$, und $\mathfrak{P}$ eine p-Gruppe ist.

Bei Γ wird $\mathfrak{H}$ durch die Matrizen der Gestalt

$$\begin{pmatrix} H & & & \\ & H & & \\ & & \ddots & \\ & & & H \end{pmatrix}$$

dargestellt, wobei die Hauptdiagonalkästchen H vom Grade u ist, und gesamt ein Galois-feld $\mathrm{GF}_{(p^u)}$ erzeugen, also wird $u \mid n$, und setzt man $n = um$, dann kann Γ als eine maximale Abelsche Substitutionsgruppe Grades m in $GF_{(p^u)}$ betrachtet werden. Da $\mathfrak{H}$ aber als eine zyklische Gruppe der Ordnung p^u-1 klar geworden ist, so genügt es nur den Typus von $\mathfrak{P}$ zu bestimmen.

Nun sei $\Gamma_{\mathfrak{P}}$ eine Darstellung von $\mathfrak{P}$, dann für jede Matrix $A=(a_{ij})$ von $\Gamma_{\mathfrak{P}}$ kann man so annehmen, daß

$$a_{ij}\in GF_{(p^u)},\quad a_{ii}=1,\quad a_{kl}=0,\quad l>k.$$

Braucht man statt A die Matrix $\bar{A}=A-E$, so sind solche Matrizen wie $\bar{A}$ voneinander vertauschbar. Wir bilden für $\mathfrak{P}$ eine Art Gruppenmatrix

$$\mathbf{P}=\bar{A}_1x_1+\bar{A}_2x_2+\cdots+\bar{A}_{p^k}x_{p^k},$$

wobei p^k die Ordnung von $\mathfrak{P}$ bedeutet, und wir nennen sie abgeleitete Gruppenmatrix von $\mathfrak{P}$ und $\bar{A}$ ihr Element.

Ich habe mich lange beschäftigt um $\mathbf{P}$ in bequeme Form zu transformieren, so daß man die verlangte Invarianten von $\mathfrak{G}/\mathfrak{A}$ durch Abzählung der Elemente von $\mathbf{P}$, die erst nach dem p^x-ten Potenzieren verschwinden, geometrisch bestimmen kann.

Neulich gelang es mir alle möglichen Gestalten von $\mathbf{P}$ in drei Formen zusammenzufassen, und jede von solchen Formen genug klar zu machen, um die Abzählung der obigen Elemente auszurichten.

Musasi Technische Hochschule

On Some Extensions of Epstein's Z-series

Tsuneo TAMAGAWA

In the following lines, we shall define a certain kind of Z-series obtained as a natural extension of Epstein's Z-series.

To avoid complication, we shall treat only a simple case. Let k be a totally real algebraic number field with a finite degree n, $k^{(1)},\cdots,k^{(n)}$ the conjugates of k, and k^m the vector space of all m-dimensional column vectors whose coefficients are in k. We shall consider k^m as a mn-dimensional vector space over the rational field Q. If an additive subgroup Λ of k^m is a free abelian group generated by some basis of k^m over Q, we call Λ a m-dimensional lattice over k. For every basis $\mathfrak{a}_1,\cdots\mathfrak{a}_{mn}$ of Λ, there exist uniquely determined mn vectors $\mathfrak{a}_1^*,\cdots,\mathfrak{a}_{mn}^*$ such that

$$\mathrm{Sp}_{k/Q}({}^t\mathfrak{a}_i\mathfrak{a}_j^*)=\begin{cases}1 & i=j,\\ 0 & i\neq j.\end{cases}$$

These mn vectors are also linearly independent over Q and generate a lattice Λ^*. Clearly this lattice Λ^* depends only upon Λ. We shall call Λ^* the complementary lattice of Λ.

The transformation matrix $\mathfrak{D}$ defined by

$$(\mathfrak{a}_1 \cdots \mathfrak{a}_{mn}) = (\mathfrak{a}_1^* \cdots \mathfrak{a}_{mn}^*)\mathfrak{D}$$

is non singular and we denote the absolute value of the determinant of this matrix with $D(\Lambda)$. $D(\Lambda)$ is a rational number and also depends only upon Λ.

Let $\mathfrak{o}$ be the set of all $\alpha \in k$ such that $\alpha \in \Lambda \subset \Lambda$, then $\mathfrak{o}$ is an order of k. If $\mathfrak{x}_2 \in \Lambda$ is equal to $\varepsilon \mathfrak{x}_1$ where ε is a unit of $\mathfrak{o}$, we say $\mathfrak{x}_2$ is equivalent to $\mathfrak{x}_1$. We can divide the set of all non zero vectors of Λ in equivalence classes.

Let $\mathfrak{S} = (\mathfrak{S}_1 \cdots \mathfrak{S}_n)$ be a set of n positive definite symmetric matrices with degree m, and S the product of the determinants of $\mathfrak{S}_1, \cdots, \mathfrak{S}_n$. Put

$$\mathfrak{S}[\mathfrak{x}] = \prod_{j=1}^{n} {}'\mathfrak{x}^{(j)} \mathfrak{S}_j \mathfrak{x}^{(j)}$$

where $\mathfrak{x}^{(j)}$ is the conjugate of $\mathfrak{x}$ in $k^{(j)}$. If $\mathfrak{x}_2$ is equivalent to $\mathfrak{x}_1$ we have $\mathfrak{S}[\mathfrak{x}_1] = \mathfrak{S}[\mathfrak{x}_2]$. Put

$$\zeta(S ; \mathfrak{S}, \Lambda) = \sum_{\mathfrak{x}}{}' \frac{1}{\mathfrak{S}[\mathfrak{x}]^s}$$

where s is a complex variable and the summation ranges over all representatives of equivalence classes in above sense.

This series converges if the real part of s is greater than $\frac{m}{2}$, and defines a holomorphic function in that region. Besides above defined series, we have to define a θ-series corresponding to that series. Put

$$\theta(\tau_1, \cdots, \tau_n ; \mathfrak{S}, \Lambda) = \sum_{\mathfrak{x} \in \Lambda}{}' \exp\left(-\pi S^{-\frac{1}{mn}} D(\Lambda)^{-\frac{1}{mn}} \sum_{j=1}^{n}{}' \tau_j {}'\mathfrak{x}^{(j)} \mathfrak{S} \mathfrak{x}^{(j)}\right)$$

where $\tau_1, \cdots, \tau_n$ are positive variables.

Using the linear transformation formula of θ function, we have a functional equation of this θ series as follows:

$$\theta(\tau_1, \cdots, \tau_n ; \mathfrak{S}, \Lambda) = (\tau_1 \cdots \tau_n)^{-\frac{m}{2}} \theta(\tau_1^{-1}, \cdots, \tau_n^{-1} ; \mathfrak{S}^{-1}, \Lambda^*)$$

where Λ^* is the complementary lattice of Λ and $\mathfrak{S}^{-1}$ is the set $(\mathfrak{S}_1^{-1}, \cdots, \mathfrak{S}_n^{-1})$.

Using this functional equation, we can prove that $\zeta(s, \mathfrak{S}, \Lambda)$ is meromorphic in the whole S-plane, has only one pole of order 1 at $s = \frac{m}{2}$, and satisfies the following functional equation

$$\xi(s, \mathfrak{S}, \Lambda) = \xi\left(\frac{m}{2} - s, \mathfrak{S}^{-1}, \Lambda^*\right)$$

where

$$\xi(s, \mathfrak{S}, \Lambda) = (SD(\Lambda))^{\frac{s}{m}} \pi^{-ns} \Gamma(s)^n \zeta(s, \mathfrak{S}, \Lambda).$$

If Δ is an arbitrary division algebra over k, we can also define the same type of Z-series and prove the functional equations of these functions.

The definition and proof are quite same as above, so we omit the detail.

The most interesting generalization is the following one. Let k be a number field defined as above, and $\mathfrak{S}$ an arbitrary non singular symmetric matrix with degree m whose coefficients are in k. Following Siegel's results, we can define the representation mass $M(\mathfrak{S}, \mathfrak{x})$ for every $\mathfrak{x}\in\Lambda$ such that $\mathfrak{S}[\mathfrak{x}]={}'\mathfrak{x}\mathfrak{S}\mathfrak{x}$ is totally positive. If $\mathfrak{x}_2$ is equal to $\mathfrak{U}\mathfrak{x}_1\varepsilon$ where $\mathfrak{U}$ is a unit of $\mathfrak{S}$ whose coefficients are in $\mathfrak{o}$ and ε a unit of $\mathfrak{o}$, we say $\mathfrak{x}_2$ is equivalent to $\mathfrak{x}_1$ with respect to $\mathfrak{S}$. Put

$$\zeta(s, \mathfrak{S}, \Lambda)=\sum_{\mathfrak{x}}{}'\frac{M(\mathfrak{S}, \mathfrak{x})}{\mathrm{N}_{k/Q}(\mathfrak{S}[\mathfrak{x}])^{s}}$$

where $\sum'$ ranges over all representatives of equivalence classes with respect to $\mathfrak{S}$. We presume that this function has probably similar functional properties as above defined Z-functions, but the reduction theory of indefinite quadratic forms in algebraic number fields being very complicated, we have not yet obtained any results.

UNIVERSITY OF TOKYO

Additive Prime Number Theory in the Totally Real Algebraic Number Field

Tikao TATUZAWA

Thanks to the remarkable work of Vinogradov, we know that every sufficiently large odd integer can be expressed as a sum of three primes. Less attention has been paid to the problem of representing numbers in an algebraic number field as the sum of primes. Rademacher carried over the Hardy-Littlewood formula in the rational case to a real quadratic number field on a certain hypothesis concerning the distribution of the zeros of Hecke's $\zeta(s, \lambda)$ functions.

Let K be a totally real algebraic number field of degree n with exactly n real conjugates $K=K^{(1)}, K^{(2)},\cdots, K^{(n)}$. A number ν in K is called totally positive, $0\prec\nu$, whenever the n conjugates $\nu^{(1)}, \nu^{(2)},\cdots, \nu^{(n)}$ are all positive; $\nu\prec\mu$ means $0\prec\mu-\nu$. An algebraic integer is said to be prime if the principal ideal which it generates is a prime ideal. We denote by J the modul consists of all expressions $\pm\lambda_1\pm\lambda_2\pm\cdots$, with totally positive primes $\lambda_1, \lambda_2,\cdots$ in K. We use the letter c to denote a positive constant depending only on K not necessarily the same each time it occurs.

Employing the Brun-Schnirelman method, we will prove without any hypothesis that all integers in J are at most c sums of $\pm\lambda$, where λ are totally positive primes. For this purpose we will develop some lemmas.

Let $P(\mathfrak{a}, \zeta)$ denote the number of integers ξ in K such that

$$\xi \equiv \beta\,(\mathrm{mod.}\,\mathfrak{a}), \quad 0 \prec \xi \prec \zeta,$$

where β, ζ are integers in K with $\zeta^{(i)} \leqq c\mathrm{N}(\zeta)^{1/n}$ and $\mathfrak{a}$ is an integral ideal in K. We can choose a basis $(\alpha_1, \alpha_2, \cdots, \alpha_n)$ of $\mathfrak{a}$ such that

$$|\alpha_j^{(i)}| \leqq c\mathrm{N}\mathfrak{a}^{1/n}, \quad 1 \leqq i, j \leqq n.$$

Thus $P(\mathfrak{a}, \zeta)$ is the number of lattice points for which the inequalities

$$0 < x_1\alpha_1^{(1)} + \cdots + x_n\alpha_n^{(1)} + \beta^{(1)} < \zeta^{(1)}$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$0 < x_1\alpha_1^{(n)} + \cdots + x_n\alpha_n^{(n)} + \beta^{(n)} < \zeta^{(n)}$$

hold, whence follows

$$P(\mathfrak{a}, \zeta) = \frac{\mathrm{N}(\zeta)}{\sqrt{d}\,\mathrm{N}\mathfrak{a}} + O\left(\left(\frac{\mathrm{N}(\zeta)}{\mathrm{N}(\mathfrak{a})}\right)^{1-1/n} + 1\right),$$

where d is the discriminant of K.

Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_k$ be prime ideals in K. We denote by $P(\mathfrak{a}, \zeta; \mathfrak{p}_1, \cdots, \mathfrak{p}_k)$ the number of integers ξ in K satisfying

$$\xi \equiv \beta\,(\mathrm{mod.}\,\mathfrak{a}), \quad 0 \prec \xi \prec \zeta,$$

$$\xi \notin \mathfrak{p}_i, \ \zeta - \xi \notin \mathfrak{p}_i, \quad 1 \leqq i \leqq k.$$

Clearly we have

$$P(\mathfrak{a}, \zeta; \mathfrak{p}_1, \cdots, \mathfrak{p}_k) = P(\mathfrak{a}, \zeta, \mathfrak{p}_1, \cdots, \mathfrak{p}_{k-1}) - v_k P(\mathfrak{a}\mathfrak{p}_k, \zeta; \mathfrak{p}_1, \cdots, \mathfrak{p}_{k-1}),$$

where

$$v_k = 2 \quad \text{if} \quad \zeta \notin \mathfrak{p}_k \quad \text{and} \quad v_k = 1 \quad \text{if} \quad \zeta \in \mathfrak{p}_k.$$

By iteration we obtain

$$\begin{aligned} &P(\mathfrak{a}, \zeta; \mathfrak{p}_1, \cdots, \mathfrak{p}_k) \\ &\quad = P(\mathfrak{a}, \zeta) - \sum_{1 \leqq r_1 \leqq k} v_{r_1} P(\mathfrak{a}\mathfrak{p}_{r_1}, \zeta; \mathfrak{p}_1, \cdots, \mathfrak{p}_{r_1-1}) \\ &\quad = P(\mathfrak{a}, \zeta) - \sum_{1 \leqq r_1 \leqq k} v_{r_1} P(\mathfrak{a}\mathfrak{p}_{r_1}, \zeta) + \sum_{1 \leqq r_2 < r_1 \leqq k} v_{r_1} v_{r_2} P(\mathfrak{a}\mathfrak{p}_{r_1}\mathfrak{p}_{r_2}, \zeta; \mathfrak{p}_1, \cdots, \mathfrak{p}_{r_2-1}) \\ &\quad = \cdots\cdots\cdots\cdots . \end{aligned}$$

Consequently, making use of Brun's method, we get

$$P(\mathfrak{o}, \zeta; \mathfrak{p}_1, \cdots, \mathfrak{p}_k) \leqq P(\mathfrak{o}, \zeta) + \sum_{i=1}^{2t} (-1)^i \sum_{r_1, \cdots, r_i} v_{r_1} \cdots v_{r_i} P(\mathfrak{p}_{r_1} \cdots \mathfrak{p}_{r_i}, \zeta)$$

where $\mathfrak{o}$ is the maximal order of K and

$$k = k_0 > k_1 > \cdots > k_t \geqq 0, \quad r_1 > r_2 > \cdots > r_{2t} > 0,$$

$$k_{\lfloor j-1/2 \rfloor} \geqq r_j, \quad 1 \leqq j \leqq 2t.$$

Hence we have

$$P(\mathfrak{o}, \zeta; \mathfrak{p}_1, \cdots, \mathfrak{p}_k) \leqq \mathrm{N}(\zeta)\tau + O\left(\mathrm{N}(\zeta)^{1-1/n} \prod_{m=0}^{t-1} (2k_m)^2\right),$$

where

$$\tau=\frac{1}{\sqrt{d}}\left(1+\sum_{i=1}^{2t}(-1)^{i}\sum_{r_1,\cdots,r_i}\frac{v_{r_1}\cdots v_{r_i}}{\mathrm{N}(\mathfrak{p}_{r_1})\cdots\mathrm{N}(\mathfrak{p}_{r_i})}\right).$$

Let ζ be a totally positive integer with $\zeta^{(i)}\leqq c\mathrm{N}(\zeta)^{1/n}$ and $\mathfrak{p}_1,\cdots,\mathfrak{p}_k$ be all prime ideals satisfying

$$11\leqq \mathrm{N}\mathfrak{p}_i\leqq \mathrm{N}(\zeta)^{c}.$$

There exists c such that

$$P(\mathfrak{o},\zeta;\mathfrak{p}_1,\cdots,\mathfrak{p}_k)=O\left(\frac{\mathrm{N}(\zeta)}{\log^2\mathrm{N}(\zeta)}\sum_{\zeta\in\mathfrak{a}}\frac{1}{\mathrm{N}\mathfrak{a}}\right).$$

This is obtained by the same method with the rational case. Thus, if we denote by $P(\zeta)$ the number of solutions of

$$\zeta=\lambda+\lambda',\quad 0\prec\lambda,\lambda'\prec\zeta,$$

where λ,λ' are primes with $\lambda^{(i)}\leqq c\mathrm{N}(\lambda)^{1/n}$ and $\lambda'^{(i)}\leqq c\mathrm{N}(\lambda')^{1/n}$, then

$$P(\zeta)=O\left(\frac{\mathrm{N}(\zeta)}{\log^2\mathrm{N}(\zeta)}\sum_{\zeta\in\mathfrak{a}}\frac{1}{\mathrm{N}\mathfrak{a}}\right).$$

Combined this with the prime ideal theorem obtained by Hecke-Landau, we have the following result. If we write

$A(x)=$the number of $\{\zeta;0\prec\zeta\prec x\}$,

$E(x)=$the number of $\{\zeta;0\prec\zeta\prec x,\ \zeta=\lambda+\lambda',\ 0\prec\lambda,\lambda'\prec\zeta,\ \lambda,\lambda'$ are primes$\}$,

then

$$E(x)>cA(x)$$

for sufficiently large positive integer x. Finally, carried over the density theorem enunciated by Schnirelmann-Landau-Mann to the algebraic number field, we get the desired result.

Gakushuin University

Bibliography

[1] E. Artin and P. Scherk, On the sum of two sets of integers, Annals of Math., **44** (1943), 138–142.

[2] E. Landau, Über Ideale und Primideale in Idealklassen, Math. Zeitschr., **2** (1918), 52–154.

[3] E. Landau, Über einige neuere Fortschritte der additiven Zahlentheorie, Cambridge Tract, 1937.

[4] H. Rademacher, Zur additiven Primzahltheorie algebraischer Zahlkörper, Teile I, II, Abh. Math. Sem. Hamburg, **3** (1924), 109–163, 331–378; Teile III, Math. Zeitschr., **27** (1927), 321–426.

[5] H. Rademacher, Über die Anwendung der Viggo Brunschen Methode auf die Theorie der algebraischen Zahlkörper, Berliner Akademie der Wissenschaften, Sitzungsberichte, 1923, 211–218.

[6] I. Vinogradov, Some theorems concerning the theory of primes, Recueil Math., N.S. **2** (1937), 175–195.

A Generalization of the Principal Ideal Theorem

Fumiyuki TERADA

The object of this note is to give a cohomological description of a generalized principal ideal theorem.

1. Let G be a finite group and S be its automorphism. H be the invariant subgroup of G generated by all the elements of the form $\sigma\cdot S(\sigma^{-1})$ and $\sigma\tau\sigma^{-1}\tau^{-1}$. Then H is S-invariant and G/H is abelian. Let $\sigma_1,\cdots,\sigma_m$ be representatives of generators of the abelian group G/H, where we may assume that these elements generate the group G. This is accomplished by adding them certain elements of H. Let $e_1,\cdots,e_m$ be the order of $\sigma_1,\cdots,\sigma_m$ mod H.

Let us consider the group rings $Z[G]$, $Z[H]$, and $Z[G']$ of G, H and G' respectively, where G' is the commutator subgroup of G and Z is the rational integral domain. For these groups, it is known that

$$\begin{aligned} G/G' &\cong H^{-2}(G,Z)\cong I_G/(1-\sigma)I_G, \\ H/H' &\cong H^{-2}(H,Z)\cong I_H/(1-h)I_H, \\ G'/G'' &\cong H^{-2}(G',Z)\cong I_{G'}/(1-g')I_{G'}, \end{aligned}\tag{1}$$

where I_G is an ideal of $Z[G]$ generated by all the elements of the form $(1-\sigma)Z[G]$. Similarly $I_H=(1-h)Z[H]$, $h\in H$ and $I_{G'}=(1-g')Z[G']$, $g'\in G'$.

Next we shall consider the abelian groups $\mathfrak{g}=G/G'$ and $\mathfrak{h}=H/G'$, and a mapping S which maps an element $\bar{\sigma}$ of $\mathfrak{g}$ to the element $s(\sigma)\cdot\sigma^{-1}\ (\mathrm{mod}\ G')$ of $\mathfrak{h}$. And denote the restriction mapping $H^{-2}(G,Z)\rightarrow H^{-2}(H,Z)$ by R. Then we have the following theorem.

THEOREM 1. *If an element a of $H^{-2}(G,Z)$ satisfies $Sa=0$, then $Ra=0$.*

PROOF. Let M be the direct sum $\sum_{i=0}^{n-1} Z(G)\bar{S}^i$, where $\bar{S}$ is a symbol such that $\bar{S}^n=1$ and n is the order of the automorphism S. If we define $\bar{S}(\sigma\bar{S}^i)$ by $S(\sigma)\bar{S}^{i+1}$, then M will have a structure of ring. Let I_M be the ideal of M generated by all elements $\xi-1$, $\xi\in M$. To avoid confusion, we shall use the following notations.

$$a_i=\sigma_i-1\ \ (i=1,\cdots,m),\quad a_0=\bar{S}-1,$$
$$f_i=1+\sigma_i+\cdots+\sigma_i^{e_i-1}\ \ (i=1,\cdots,m).$$

Now by the isomorphism (1) and the definition of S^*, it is sufficient to prove the following:

If an element $a\in I_G$ satisfies $S^*a\in I_{G'}$, then

$$Ra\equiv 0 \quad \mathrm{mod}\ (1-h)I_H.$$

And this is described as a problem in the module I_M as follows:

If

$$\sum_{i=1}^{m} \gamma_i'\{(\sigma_i-1)a_0-(\bar{S}-1)a_i\}$$
$$\equiv \sum_{i,j=1}^{m} f_{ij}\{(\sigma_i-1)a_j-(\sigma_j-1)a_i\} \qquad \mathrm{mod}\ (h-1)I_H,$$

then we have $\sum \gamma_i' f_1\cdots f_m a_i \equiv 0 \quad \mathrm{mod}\ (h-1)I_H$.

Now, we shall find an element $D \in M$ such that

$$D\{(\sigma_i-1)a_j-(\sigma_j-1)a_i\}\equiv 0 \quad \mathrm{mod}\ (h-1)I_H \ (i, j=1,\cdots, m),$$
$$D\{(\sigma_i-1)a_0-(\bar{S}-1)a_j\}\equiv f_1\cdots f_m a_i \quad \mathrm{mod}\ (h-1)I_H \ (i=1,\cdots, m).$$

We do not concern in the detail of the existence of D. The theorem follows from these relations immediately. q.e.d.

2. Let $\bar{\Omega}/\Omega$ be a normal extension with Galois group G. S be an automorphism of G. Then S induces an automorphism of the factor group $C_\Omega/\mathrm{N}_{\bar{\Omega}/\Omega}C_{\bar{\Omega}}$ of the idèle class group C_Ω of Ω. Let C be the image of the endomorphism $S-1$ of $C_\Omega/\mathrm{N}_{\bar{\Omega}/\Omega}C_{\bar{\Omega}}$. Then there exists an abelian extension K_S of Ω such that $\mathrm{N}_{K/\Omega}C_K=C$ (the existence theorem of class field theory). The Galois group of $\bar{\Omega}/K$ is exactly the group H which was treated in § 1. By the isomorphism theorem of class field theory (i.e. $H^{-2}(G, Z)\rightarrow H^0(G, C_{\bar{\Omega}})$) and Theorem 1, we have the following theorem.

THEOREM 2. *The kernel of the endomorphism* $S-1$ *of the group* $C_\Omega/\mathrm{N}_{\bar{\Omega}/\Omega}C_{\bar{\Omega}}$ *is contained in* $\mathrm{N}_{\bar{\Omega}/K}C_{\bar{\Omega}}$, *when it is considered in* K, *where* K *is the abelian extension corresponding to the idèle class group* $C_\Omega^{S-1}\mathrm{N}_{\bar{\Omega}/\Omega}C_{\bar{\Omega}}$.

By the usual correspondence which exists between idèles and ideals, we have an analogous result concerning ideals. Using a result concerning the conductor and the module of genus which is obtained by Prof. Tannaka, we can describe this as a norm theorem of a normal extension $\bar{\Omega}/\Omega$. Especially, if S generates the Galois group of a cyclic extension Ω/k and $K(\supset\Omega)$ is the absolute (in generally ray) class field of k, we have a generalized principal ideal theorem. Describing it in the case of unramified extensions, we have the following theorem.

THEOREM 3. *Let* k *be an algebraic number field,* K *the absolute class field of* k, *and* Ω *a cyclic intermediate field of* K/k. *Let* S *be a generator of the Galois group of the cyclic extension* Ω/k. *Then all the ambigous ideals in* Ω (i.e. $\mathfrak{A}^{1-S}$=*principal*) *become principal in* K.

TÔHOKU UNIVERSITY

BIBLIOGRAPHY

[1] F. Terada, On a generalized principal ideal theorem, Tôhoku Math. Journ., **6** (1954).

[2] T. Tannaka, Some Remarks concerning principal ideal theorem, Tôhoku Math. Journ., **1** (1951).

[3] F. Terada, A generalization of the principal ideal theorem, Journ. Math. Soc. Japan, **7** (1955).

Theory of Arithmetic Linear Transformations and its Application to an Elementary Proof of Dirichlet's Theorem About the Primes in an Arithmetic Progression

Koichi YAMAMOTO

1. A. Selberg proved the Dirichlet's theorem about the primes in an arithmetic progression elementarily. His proof is based on the so-called Selberg's inequality, and it seems that the connection to the classical proof is not clear enough.

We present here a unified interpretation of these two methods by a new principle, which we shall call, theory of arithmetic linear transformations. This principle was, in essence, perceived by Dirichlet, Möbius, Glaisher, Landau, Hardy, Selberg and others, but seems not fully recognized. Our principle is elementary in its character, and it reveals (Theorem 1) that the classical (Dirichlet-Mertens-Landau) method and Selberg's new method revolve around the same crucial point. It also reveals that Selberg's inequality is not the simplest formula for the purpose, and is only next-to-the-best. However, Selberg's inequality becomes essential if we try to prove the prime number theorem by our method.

2. Let $\alpha=(\alpha_1, \alpha_2, \cdots)$ be a sequence to numbers and $f(x)$ be a function defined on $[1, \infty)$. We define an arithmetic linear transformation S_α by

$$(S_\alpha f)(x)=\sum_{n\leq x}\alpha_n f\left(\frac{x}{n}\right).$$

S_α is considered as a linear transformation on the totality of functions defined on $[1, \infty)$. Addition and multiplication are defined as usual. We find that $S_\alpha+S_\beta=S_{\alpha+\beta}$, and $S_\alpha S_\beta=S_\gamma$, with $\gamma_n=\sum_{m|n}\alpha_m\beta_{\frac{n}{m}}$, or γ is the "convolution" of α and β; in notation $\gamma=\alpha*\beta$. Convolution is commutative, associative, and distributive w.r.t. addition. A sequence α is called regular if $\alpha_1\neq 0$. Regular sequences form an abelian group w.r.t. convolution-multiplication. A sequence is called multiplicative (or factorizable resp.) if $\alpha_m\alpha_n=\alpha_{mn}$ for $(m, n)=1$ (or unconditionally, resp.). E.g. character mod k are regular and factorizable at the same time. If α is factorizable, then term-by-term multiplication $\alpha\beta$ by α is distributive w.r.t. convolution.

We denote by ι the sequence $(1,1,1,\cdots)$; by μ the sequence $(\mu(1), \mu(2),\cdots)$, with $\mu(n)$ Möbius' function; by log the sequence $(\log 1, \log 2,\cdots)$; by Λ the sequence $(\Lambda(1), \Lambda(2),\cdots)$, with $\Lambda(n)$ Mangoldt's function. Now let k be a positive integer>1, and denote characters mod k by $\chi,\cdots$. We also denote by χ the sequence $(\chi(1), \chi(2),\cdots)$. Let a be prime to k and

$1 \leqq a \leqq k-1$. Denote the sequence $(\iota_a(1), \iota_a(2), \cdots)$ by ι_a, with $\iota_a(n)=1$ or 0, according as $n \equiv a \pmod{k}$ or not. Denote by ε the sequence $(1, 0, 0, \cdots)$. This is the neutral element of the group of the regular sequences. We find:

$$\iota * \mu = \mu * \iota = \varepsilon;\ \chi * \chi\mu = \chi\mu * \chi = \varepsilon;$$
$$\iota * \Lambda = \log,\ \mu * \log = \Lambda;\ \chi * \chi\Lambda = \chi \log,\ \chi\mu * \chi \log = \chi\Lambda;$$
$$\chi = \sum \chi(a)\iota_a,\ \iota_a = (1/\varphi(k)) \sum \overline{\chi}(a)\chi,$$

where the first sum is extended over $\varphi(k)$ a's such that $(a, k)=1$ and that $1 \leqq a \leqq k-1$, and the second sum is over the $\varphi(k)$ characters mod k.

3. Let us denote by 1 the function defined on $[1, \infty)$ and with constant value 1. $\psi(x) = S_\Lambda 1$ then is Tschebyscheff's function. χ_1 stands for the principal character. Then we find:

LEMMA 1. $S_\mu(x) = O(x)$.

LEMMA 2. $S_\iota(\log x) = x + O(\log x)$.

LEMMA 3. $\psi(x) = O(x)$.

LEMMA 4. $S_\Lambda(x) = x \log x + O(x)$.

LEMMA 5. $S_\Lambda(\log x) = O(x)$.

But these are well-known results. Now let $\chi \neq \chi_1$ and define $\beta_\chi = \sum_{n=1}^{\infty} \chi(n)/n$. (This is $= L(1, \chi)$ if we use Dirichlet's L-functions.)

LEMMA 6. *If $\beta_\chi \neq 0$, then $S_{\chi\Lambda}(x) = O(x)$.*

LEMMA 7. *If $\beta_\chi = 0$, then $S_{\chi\Lambda}(x) = -x \log x + O(x)$.*

LEMMA 8. *There is at most one non-principal character with $\beta_\chi = 0$. Such a character, if it exists, must be a real character.*

THEOREM 1. *There are only two possibilities. (1) Either Dirichlet's theorem is true for every k. (2) Or there is a unique real character with $\beta_\chi = 0$, and then we would have $\sum' \log p/p = O(1)$, the sum extending over primes $p \leqq x$ such that $\chi(p) = 1$ for this exceptional character χ.*

4. Mertens and Landau proved $\beta_\chi \neq 0$ for non-principal real characters χ. The method does not make use of L-functions or continuity of functions at all.

On the other hand Selberg proved (Ann. of Math., vol. 50 (1949), 297–304) that $\sum'_{p \leqq x, \chi(p)=1} \log p/p > c \log x$ with some positive constant, and his proof is very elegant. We need not continuity of functions here, too. For our purpose to prove $\sum'_{\chi(p)=1} \log p/p = \infty$ we can simplify his proof to some extent.

THEOREM 2. *If k is a positive integer >1 and a is prime to k, then there exist infinitely many prime numbers in the arithmetic progression $a, a+k, a+2k, \cdots$.*

KYUSHU UNIVERSITY