J.S. Milne

Trường và Lý thuyết Galois

James S. Milne

LÝ THUYẾT TRƯỜNG VÀ LÝ THUYẾT GALOIS

Phiên bản 4.53, Ngày 27 Tháng 5, 2017

Người dịch: Nguyễn Đức Khánh, Lê Minh Hà
Tham gia hiệu đính: Đoàn An Khương, Mạc Đăng Trường, Phạm Minh Hoàng, Trần Minh Tâm, Nguyễn Thụy Trung, Lê Quốc Tuấn.

Giáo trình này trình bày một cách cô đọng lý thuyết trường, trong đó có lý thuyết Galois của mở rộng hữu hạn, vô hạn và lý thuyết mở rộng siêu việt. Sáu chương đầu bao gồm các nội dung chính của một khóa học chính quy và ba chương cuối cùng ở mức độ nâng cao hơn.

Trích dẫn BibTeX

```
@misc{milneFT,
author={Milne, James S., Người dịch: Nguyễn Đ. Khánh và Lê M. Hà}
title={Lý thuyết trường và lý thuyết Galois (v.4.53)}
year={2017},
note={Xem \url{www.milne.org/math/}}
pages={178}
}
```

Ký hiệu

Ta sử dụng các ký hiệu thông thường của Bourbaki.

$\mathbb{N}$	$= \{0, 1, 2, \ldots\}$,
$\mathbb{Z}$	vành các số nguyên
$\mathbb{R}$	trường số thực
$\mathbb{F}_{\mathrm{p}} = \mathbb{Z}/p\mathbb{Z}$	trường có p phần tử, p là một số nguyên tố.
$X \subset Y$	X là một tập con của Y
$X \stackrel{def}{=} Y$	X được định nghĩa là Y, hoặc bằng Y theo định nghĩa
$X \approx Y$	X đẳng cấu với Y
$X \simeq Y$	X và Y đẳng cấu chính tắc

(hoặc có một đẳng cấu đã cho, hoặc có duy nhất một đẳng cấu).

Khi có một quan hệ tương đương, $[*]$ ký hiệu lớp tương đương chứa $*$. Lực lượng của một tập hợp S được ký hiệu là $|S|$ (do đó $|S|$ là số các phần tử của S, nếu đó là một tập hữu hạn.) Giả sử I và A là các tập hợp. Một họ các phần tử của A được gắn nhãn bởi I, ký hiệu là $(a_i)_{i \in I}$, là một hàm $i \mapsto a_i \colon I \to A$. Trong giáo trình này, p là một số nguyên tố.

Mục lục

CHƯƠNG 1

Các khái niệm và kết quả cơ bản

1.1. Vành

Một **vành** là một tập hợp R được trang bị hai phép toán hai ngôi $+$ và $\cdot$ thỏa mãn:

- $(R, +)$ là một nhóm giao hoán;
- $\cdot$ có tính kết hợp, và tồn tại [1] một phần tử 1_R thỏa mãn $a \cdot 1_R = a = 1_R \cdot a$ với mọi $a \in R$;
- Luật phân phối: với mọi $a, b, c \in R$,

$$(a + b) \cdot c = a \cdot c + b \cdot c$$
$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Ta thường bỏ đi " $\cdot$ " và viết 1 thay cho 1_R khi không có sự lẫn lộn. Nếu $1_R = 0$ thì $R = \{0\}$.

Một **vành con** S của vành R là một tập con chứa 1_R và đóng dưới phép cộng và phép nhân. Nó thừa hưởng cấu trúc vành của R.

Một **đồng cấu vành** $\alpha : R \to R'$ là một ánh xạ thỏa mãn:

$$\alpha(a + b) = \alpha(a) + \alpha(b), \quad \alpha(ab) = \alpha(a)\alpha(b), \quad \alpha(1_R) = 1_{R'}$$

với mọi $a, b \in R$. Vành R được gọi là **giao hoán** nếu phép nhân có tính chất giao hoán:

$$ab = ba \text{ với mọi } a, b \in R.$$

[1] Chúng ta sẽ theo quy ước của Bourbaki, yêu cầu một vành phải có 1, vì thế các đồng cấu cũng cần bảo toàn phần tử 1.

Một vành giao hoán được gọi là một **miền nguyên** nếu $1_R \neq 0$ và phép nhân tuân theo luật giản ước:

$$ab = ac, a \neq 0, \text{ suy ra } b = c.$$

Một **iđêan** I của một vành giao hoán R là một nhóm con của $(R, +)$ có tính chất đóng đối với phép nhân bởi các phần tử của R:

$$r \in R, a \in I, \text{ suy ra } ra \in I.$$

Iđêan sinh bởi các phần tử $a_1, \ldots, a_n$ được ký hiệu bởi $(a_1, \ldots, a_n)$. Ví dụ, (a) là iđêan chính aR.

Chúng ta sẽ coi như độc giả đã làm quen với lý thuyết cơ bản về vành. Ví dụ, trong $\mathbb{Z}$ (hay nói chung, trong bất kỳ một miền Euclid nào) một iđêan I sẽ được sinh bởi một phần tử khác không "nhỏ nhất" của I.

1.2. Trường

Định nghĩa 1.1. Một **trường** là một tập hợp F được trang bị hai luật hợp thành $+$ và $\cdot$ thỏa mãn:

(a) $(F, +)$ là một nhóm giao hoán;

(b) $(F^\times, \cdot)$, với $F^\times = F \setminus \{0\}$, là một nhóm giao hoán;

(c) Có luật phân phối.

Như vậy, một trường là một vành giao hoán khác không mà mọi phần tử khác 0 đều có nghịch đảo. Nói riêng, nó là một miền nguyên. Một trường phải chứa ít nhất hai phần tử khác nhau, 0 và 1. Trường bé nhất, nhưng là một trong những trường quan trọng nhất là $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$.

Một **trường con** S của trường F là một vành con đóng đối với phép lấy nghịch đảo. Nó thừa hưởng cấu trúc của một trường từ F.

Bổ đề 1.2. *Một vành giao hoán khác không R là một trường nếu và chỉ nếu nó không chứa một iđêan nào khác ngoài* (0) *và R.*

Chứng minh. Giả sử R là một trường, và I là một iđêan khác (0) trong R. Nếu a là một phần tử khác 0 của I, thì $1 = a^{-1}a \in I$, và do vậy $I = R$. Ngược lại, giả sử R là một vành giao hoán không có iđêan con thực sự nào khác (0). Nếu $a \neq 0$, thì $(a) = R$, và phải tồn tại một phần tử b trong R thỏa mãn $ab = 1$. □

Ví dụ 1.3. *Các tập hợp sau đây là các trường:* $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ *(p là số nguyên tố).*

Một **đồng cấu trường** $\alpha\colon F \to F'$ đơn thuần là một đồng cấu vành. Đồng cấu đó là một đơn ánh vì $\ker\alpha$ là một iđêan thực sự (nó không chứa 1), và vì thế phải bằng (0).

1.3. Đặc số của Trường

Dễ thấy rằng ánh xạ

$$\mathbb{Z} \to F, \quad n \mapsto 1_F + \cdots + 1_F \quad (n \text{ lần}),$$

là một đồng cấu vành. Ví dụ,

$$(\underbrace{1_F + \cdots + 1_F}_{m}) + (\underbrace{1_F + \cdots + 1_F}_{n}) = \underbrace{1_F + \cdots + 1_F}_{m+n}$$

nhờ tính chất kết hợp của phép cộng. Bởi vậy, hạt nhân của nó là một iđêan trong $\mathbb{Z}$.

Trường hợp 1: Nếu hạt nhân của ánh xạ là (0), khi đó

$$n.1_F = 0 \Rightarrow n = 0 \quad (\text{trong } \mathbb{Z}).$$

Các số nguyên khác 0 được ánh xạ thành các phần tử khả nghịch của F bởi $n \mapsto n \cdot 1_F\colon \mathbb{Z} \to F$, và do vậy ánh xạ này mở rộng được thành một đồng cấu

$$\frac{m}{n} \mapsto (m \cdot 1_F)(n \cdot 1_F)^{-1}\colon \mathbb{Q} \hookrightarrow F.$$

Trong trường hợp này, F chứa một bản sao của $\mathbb{Q}$, và ta nói rằng nó có **đặc số** 0.

Trường hợp 2: Nếu hạt nhân của ánh xạ khác (0), thì $n \cdot 1_F = 0$ với $n \neq 0$ nào đó. Số nguyên dương n nhỏ nhất như thế sẽ phải là một số nguyên tố p (nếu không sẽ tồn tại hai phần tử khác 0 trong F mà tích của chúng bằng 0), và p sinh ra iđêan hạt nhân. Do đó, ánh xạ $n \mapsto n \cdot 1_F\colon \mathbb{Z} \to F$ xác định một đẳng cấu từ $\mathbb{Z}/p\mathbb{Z}$ lên vành con

$$\{m \cdot 1_F \mid m \in \mathbb{Z}\}$$

của F. Trong trường hợp này, F chứa một bản sao của $\mathbb{F}_p$, và ta nói rằng nó có **đặc số** p.

Các trường $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \ldots, \mathbb{Q}$ được gọi là các **trường nguyên tố**. Mọi trường đều chứa đúng một bản sao của đúng một trong các trường nguyên tố đó.

Nhận xét 1.4. *Định lý nhị thức*

$$(a+b)^m = a^m + \binom{m}{1} a^{m-1}b + \binom{m}{2} a^{m-2}b^2 + \cdots + b^m$$

vẫn đúng trong mọi vành giao hoán. Nếu p là số nguyên tố, thì p chia hết $\binom{p^n}{r}$ với mọi r mà $1 \leq r \leq p^n - 1$. Do đó, nếu F có đặc số p, thì

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \text{ với mọi } n \geq 1.$$

*Do vậy, ánh xạ $a \mapsto a^p \colon F \to F$ là một đồng cấu. Nó được gọi là **tự đồng cấu Frobenius** của F. Nếu F có hữu hạn phần tử, tự đồng cấu Frobenius là một tự đẳng cấu.*

1.4. Nhắc lại về vành đa thức

Cho F là một trường.

1.5. *Vành $F[X]$ các đa thức theo ký hiệu (hoặc "biến") X với hệ số trong F là một F-không gian véc tơ có cơ sở $1, X, \ldots, X^n, \ldots$ và phép nhân được xác định bởi*

$$\left(\sum_i a_i X^i\right)\left(\sum_j b_j X^j\right) = \sum_k \left(\sum_{i+j=k} a_i b_j\right) X^k.$$

Với mọi vành R chứa F như là một vành con và phần tử $r \in R$, tồn tại duy nhất một đồng cấu $\alpha \colon F[X] \to R$ thỏa mãn $\alpha(X) = r$ và $\alpha(a) = a$ với mọi $a \in F$.

1.6. ***Thuật toán chia:*** *cho $f(X)$ và $g(X) \in F[X]$ với $g \neq 0$, tồn tại $q(X), r(X) \in F[X]$, ở đó $r = 0$ hoặc $deg(r) < deg(g)$ sao cho*

$$f = gq + r;$$

hơn nữa, $q(X)$ và $r(X)$ được xác định duy nhất. Do đó, $F[X]$ là một miền Euclid có ánh xạ chuẩn là bậc, và do vậy nó là một miền nhân tử hóa.

1.7. *Cho $f \in F[X]$ và $a \in F$. Khi đó*

$$f = (X - a)q + c$$

với $q \in F[X]$ và $c \in F$. Nếu a là một nghiệm của f (tức là $f(a) = 0$), thì $X - a$ chia hết f. Do tính phân tích duy nhất, f có nhiều nhất $\deg(f)$ nghiệm (xem Bài tập 1-3).

1.8. ***Thuật toán Euclid:*** *Cho f và $g \in F[X]$ có ước chung lớn nhất là $d(X)$. Thuật toán Euclid xây dựng các đa thức $a(X)$ và $b(X)$ thỏa mãn*

$$a(X) \cdot f(X) + b(X) \cdot g(X) = d(X), \quad deg(a) < deg(g), \quad deg(b) < deg(f).$$

Thật vậy, không mất tính tổng quát, có thể giả sử rằng $\deg(f) \geq \deg(g)$. Sử dụng thuật toán chia, ta xây dựng một dãy các thương và phần dư như sau

$$\begin{aligned} f &= q_0 g + r_0 \\ g &= q_1 g r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\cdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

ở đó r_n là phần dư cuối cùng khác 0. Vậy thì, r_n chia hết r_{n-1}, do đó chia hết r_{n-2}, ..., g và cuối cùng là f. Hơn nữa,

$$r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) = \cdots = af + bg$$

và do vậy mọi ước chung của f và g chia hết r_n: ta vừa chứng minh rằng $r_n = gcd(f, g)$.

Giả sử $af + bg = d$. Nếu $\deg(a) \geq \deg(g)$, viết $a = gq + r$ với $\deg(r) < \deg(g)$; khi đó

$$rf + (b + qf)g = d,$$

và $b + qf$ hiển nhiên có bậc nhỏ hơn $deg(f)$.

PARI có thể thực hiện thuật chia Euclid: gõ `divrem(13,5)` *trong PARI sẽ trả về $[2, 3]$, tức là $13 = 2 \times 5 + 4$, và $\gcd(m, n)$ trả về ước chung lớn nhất của m và n.*

1.9. *Giả sử I là một iđêan khác (0) trong $F[X]$, và f là một đa thức khác 0 có bậc nhỏ nhất trong I; khi đó $I = (f)$ (vì $F[X]$ là một miền Euclid). Nếu chọn f là một đa thức đơn khởi*[2]*, tức là có hệ số đầu bằng 1 , thì nó sẽ được xác định duy nhất bởi I. Do đó, có một tương ứng $1-1$ giữa các iđêan khác (0) của $F[X]$ với các đa thức đơn khởi trong $F[X]$. Các iđêan nguyên tố tương ứng với các đa thức đơn khởi bất khả quy.*

1.10. *Vì $F[X]$ là một miền nguyên chính, ta có thể xây dựng trường các thương $F(X)$. Các phần tử của nó là các thương f/g với f và g là các đa thức, $g \neq 0$.*

1.5. Phân tích đa thức

Các kết quả sau đây giúp ta xác định xem một đa thức có khả quy hay không, và nếu có thì tìm các nhân tử của nó.

Mệnh đề 1.11. *Giả sử $r \in \mathbb{Q}$ là một nghiệm của đa thức*

$$a_m X^m + a_{m-1}X^{m-1} + \cdots + a_0, \quad a_i \in \mathbb{Z},$$

và $r = c/d$ với $c, d \in \mathbb{Z}, \gcd(c,d) = 1$. Khi đó $c|a_0$ và $d|a_m$.

Chứng minh. Từ phương trình

$$a_m c^m + a_{m-1}c^{m-1}d + \cdots + a_0 d^m = 0$$

ta có ngay $d|a_m c^m$, và do đó $d|a_m$. Tương tự, $c|a_0$. □

Ví dụ 1.12. *Đa thức $f(X) = X^3 - 3X - 1$ bất khả quy trong $\mathbb{Q}[X]$ bởi nghiệm có thể có của nó là ± 1, nhưng $f(1) \neq 0 \neq f(-1)$.*

Mệnh đề 1.13 (Bổ đề Gauss)**.** *Cho $f(X) \in \mathbb{Z}[X]$. Nếu $f(X)$ phân tích không tầm thường trong $\mathbb{Q}[X]$, thì nó phân tích không tầm thường trong $\mathbb{Z}[X]$.*

Chứng minh. Giả sử $f = gh$ trong $\mathbb{Q}[X]$ với $g, h \notin \mathbb{Q}$. Với các số nguyên m, n thích hợp, $g_1 \overset{def}{=} mg$ và $h_1 \overset{def}{=} nh$ có hệ số trong $\mathbb{Z}$, và ta có phân tích

$$mnf = g_1 \cdot h_1 \text{ trong } \mathbb{Z}[X].$$

[2] monic = đơn khởi

Nếu p một số nguyên tố chia hết mn, lấy modulo p, ta có

$$0 = \overline{g}_1 \cdot \overline{h}_1 \text{ trong } \mathbb{F}_p[X].$$

Vì $\mathbb{F}_p[X]$ là một miền nguyên nên p chia hết tất cả các hệ số của ít nhất một trong hai đa thức g_1, h_1, giả sử đó là g_1, thì $g_1 = pg_2$ với $g_2 \in \mathbb{Z}[X]$ nào đó. Khi đó ta có phân tích

$$(mn/p)f = g_2.h_1 \text{ trong } \mathbb{Z}[X].$$

Cứ tiếp tục làm như vậy, cuối cùng ta sẽ lược bỏ được hết tất cả các ước nguyên tố của mn, và thu được một phân tích không tầm thường của f trong $\mathbb{Z}[X]$. □

Mệnh đề 1.14. *Nếu $f \in \mathbb{Z}[X]$ đơn khởi, thì mọi nhân tử đơn khởi của f trong $\mathbb{Q}[X]$ đều nằm trong $\mathbb{Z}[X]$.*

Chứng minh. Giả sử g là một nhân tử đơn khởi của f trong $\mathbb{Q}[X]$, khi đó $f = gh$ với $h \in \mathbb{Q}[X]$ cũng là một đa thức đơn khởi. Chọn m, n là hai số nguyên dương có ít ước nguyên tố nhất sao cho $mg, nh \in \mathbb{Z}[X]$. Như trong chứng minh Bổ đề Gauss, nếu một số nguyên tố p chia hết mn, thì nó chia hết tất cả hệ số của ít nhất một trong các đa thức mg, nh, giả sử là mg, thì khi đó nó chia hết m vì g đơn khởi. Bây giờ $\frac{m}{p}g \in \mathbb{Z}[X]$, điều này mâu thuẫn với định nghĩa của m. □

Ghi chú 1.15. *Ta phác thảo một chứng minh khác của Mệnh đề 1.14. Một số phức α được gọi là một **số nguyên đại số** nếu nó là nghiệm của một đa thức đơn khởi trong $\mathbb{Z}[X]$. Mệnh đề 1.11 chỉ ra rằng mọi số nguyên đại số trong $\mathbb{Q}$ đều nằm trong $\mathbb{Z}$. Các số nguyên đại số lập thành một vành con của $\mathbb{C}$ - Xem Định lý 6.5 trong giáo trình của tôi về Đại số giao hoán. Bây giờ giả sử $\alpha_1, \ldots, \alpha_m$ là các nghiệm phức của f. Theo định nghĩa, chúng là các số nguyên đại số, và các hệ số của các nhân tử đơn khởi của f là các đa thức theo các α_i nào đó, và do vậy chúng cũng là các số nguyên đại số. Nếu chúng nằm trong $\mathbb{Q}$, thì chúng nằm trong $\mathbb{Z}$.*

Mệnh đề 1.16 (Tiêu chuẩn Eisenstein)**.** *Cho*

$$f = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0, \quad a_i \in \mathbb{Z};$$

giả sử có một số nguyên tố p thỏa mãn:

- *p không chia hết a_m;*
- *p chia hết $a_{m-1}, \ldots, a_0$;*
- *p^2 không chia hết a_0;*

thì f bất khả quy trong $\mathbb{Q}[X]$.

Chứng minh. Nếu $f(X)$ phân tích được trong $\mathbb{Q}[X]$, thì nó phân tích được trong $\mathbb{Z}[X]$,

$$a_m X^m + a_{m-1} X^{m-1} + \cdots + a + 0 = (b_r X^r + \cdots + b_0)(c_s X^s + \cdots + c_0)$$

với $b_i, c_i \in \mathbb{Z}$ và $r, s < m$. Vì p chia hết $a_0 = b_0 c_0$ còn p^2 thì không nên p phải chia hết đúng một trong hai số b_0, c_0, giả sử là b_0. Từ đẳng thức

$$a_1 = b_0 c_1 + b_1 c_0$$

ta thấy rằng $p | b_1$, và từ đẳng thức

$$a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0,$$

ta thấy rằng $p | b_2$. Tiếp tục lập luận như vậy, suy ra p chia hết $b_0, b_1, \ldots, b_r$, điều này mâu thuẫn với việc p không chia hết a_m. □

Ba mệnh đề dưới đây vẫn đúng khi thay $\mathbb{Z}$ bởi một miền nhân tử hóa bất kỳ.

Nhận xét 1.17. *Tồn tại một thuật toán phân tích một đa thức trong $\mathbb{Q}[X]$. Xét một đa thức $f \in \mathbb{Q}[X]$. Nhân $f(X)$ với một số hữu tỷ để được một đa thức đơn khởi và sau đó thay nó bởi $D^{deg(f)} f(\frac{X}{D})$, ở đó D là mẫu số chung của tất cả các hệ số của f để thu được một đa thức đơn khởi với hệ số nguyên. Do vậy, ta chỉ cần làm việc với các đa thức có dạng*

$$f(X) = X^m + a_1 X^{m-1} + \cdots + a_m, \quad a_i \in \mathbb{Z}.$$

Từ định lý cơ bản của đại số (xem 5.6 phía dưới), ta biết rằng f phân tích hoàn toàn trong $\mathbb{C}[X]$ thành:

$$f(X) = \prod_{i=1}^{m} (X - \alpha_i), \quad \alpha_i \in \mathbb{C}.$$

Từ phương trình

$$0 = f(\alpha_i) = \alpha_i^m + a_1\alpha_i^{m-1} + \cdots + a_m,$$

suy ra $|\alpha_i|$ *nhỏ hơn một chặn trên, phụ thuộc duy nhất vào bậc và các hệ số của* f*; cụ thể là,*

$$|\alpha_i| \leq max\{1, mB\}, \quad B = max|a_i|.$$

Bây giờ, nếu $g(X)$ *là một nhân tử đơn khởi của* $f(X)$*, thì nghiệm phức của nó là các giá trị* α_i*, và hệ số của nó là các đa thức đối xứng của các nghiệm của nó (xem trang ???). Do vậy, giá trị tuyệt đối của các hệ số của* $g(X)$ *bị chặn bởi một giá trị phụ thuộc vào bậc và các hệ số của* f*. Vì chúng là các số nguyên (bởi 1.14), ta thấy rằng có một số hữu hạn các giá trị có thể có của* $g(X)$*. Như vậy, để tìm các nhân tử của* $f(X)$*, ta (tốt hơn là dùng PARI) chỉ cần thực hiện một số hữu hạn các phép kiểm tra* [3]*.*

Như vậy, ta không cần bận tâm tới bài toán phân tích đa thức trong các vành $\mathbb{Q}[X]$ hay $\mathbb{F}_p[X]$ vì PARI làm được tính toán này. Ví dụ, gõ `content(6*X^2 +18*X-24)` trong PARI trả về 6, và `factor(6*X^2 +18*X-24)` trả về $X-1$ và $X+4$, do đó

$$6X^2 + 18X - 24 = 6(X-1)(X+4)$$

trong $\mathbb{Q}[X]$. Gõ `factormod(X^2+3*X+3,7)` trả về $X+4$ và $X+6$, chỉ ra rằng

$$X^2 + 3X + 3 = (X+4)(X+6)$$

trong $\mathbb{F}_7[X]$.

Nhận xét 1.18. *Có một quan sát khác khá hữu dụng như sau. Cho* $f \in \mathbb{Z}[X]$*, nếu hệ số đầu của* f *không chia hết cho một số nguyên tố* p*, thì một phân tích không tầm thường* $f = gh$ *trong* $\mathbb{Z}[X]$ *sẽ cho một phân tích không tầm thường* $\overline{f} = \overline{g} \cdot \overline{h}$ *trong* $\mathbb{F}_p[X]$*. Do đó, nếu* $f(X)$ *bất khả quy trong* $\mathbb{F}_p[X]$*, ở đó* p *là một số nguyên tố nào đó không chia hết hệ số đầu, thì nó bất khả quy trong* $\mathbb{Z}[X]$*. Tiêu chuẩn này khá hữu ích, nhưng không phải lúc nào cũng hiệu quả. Ví dụ,* $X^4 - 10X^2 + 1$ *bất khả quy trong* $\mathbb{Z}[X]$ *nhưng nó khả quy* [4] *modulo mọi* p *nguyên tố.*

[3] Tất nhiên, có các phương pháp nhanh hơn cách này. Thuật toán Berlekamp - Zassenhaus phân tích đa thức trên một trường hữu hạn phù hợp $\mathbb{F}_p$, nâng các nhân tử này lên các vành $\mathbb{Z}/p^m\mathbb{Z}$ với m nào đó, và sau đó tìm kiếm các nhân tử trong $\mathbb{Z}[X]$ với dạng đúng modulo p^m.

[4] Sau đây là một chứng minh chỉ sử dụng nhận xét tích của hai phần tử không là bình phương

1.6. Mở rộng trường

Một trường E chứa một trường F được gọi là một **mở rộng trường** của F (hoặc đơn giản là một **mở rộng** của F, và ta nói mở rộng E/F). Số chiều của E, xem như là một F-không gian véctơ, và ta viết $[E : F]$ cho số chiều của E, có thể vô hạn, xem như là một $F-$không gian véctơ được gọi là **bậc** của E trên F và được ký hiệu là $[E\colon F]$. Ta nói E hữu hạn trên F nếu nó có bậc hữu hạn trên F.

Nếu E và E' là các mở rộng trường của F, một F-**đồng cấu** $E \to E'$ là một đồng cấu $\phi : E \to E'$ thỏa mãn $\phi(c) = c$ với mọi $c \in F$.

Ví dụ 1.19.

- *Trường số phức* $\mathbb{C}$ *có bậc* 2 *trên* $\mathbb{R}$ *(cơ sở* $\{1, i\}$*).*
- *Trường số thực* $\mathbb{R}$ *có bậc vô hạn trên* $\mathbb{Q}$*: trường* $\mathbb{Q}$ *đếm được và do vậy mọi* $\mathbb{Q}$*-không gian véctơ hữu hạn chiều cũng đếm được. Tuy nhiên, một lập luận nổi tiếng của Cantor chỉ ra rằng* $\mathbb{R}$ *không đếm được.*
- *Trường các* ***số hữu tỉ Gauss***

  $$\mathbb{Q}(i) \stackrel{def}{=} \{a + bi \mid a, b \in \mathbb{Q}\}$$

  có bậc 2 *trên* $\mathbb{Q}$ *(cơ sở* $\{1, i\}$*).*
- *Trường* $F(X)$ *có bậc vô hạn trên* F*; thực ra, ngay cả không gian con* $F[X]$ *của nó cũng có bậc vô hạn trên* F *(cơ sở* $1, X, X^2, \dots$*).*

---

trong $\mathbb{F}_p^\times$ là một bình phương, điều này suy ra từ sự kiện $\mathbb{F}_p^\times$ là nhóm xyclic (xem Bài tập 1-3). Nếu 2 là một bình phương trong $\mathbb{F}_p^\times$, thì

$$X^4 - 10X^2 + 1 = (X^2 - 2\sqrt{2}X - 1)(X^2 + 2\sqrt{2}X - 1).$$

Nếu 3 là một bình phương trong $\mathbb{F}_p$, thì

$$X^4 - 10X^2 + 1 = (X^2 - 2\sqrt{3}X + 1)(X^2 + 2\sqrt{3}X + 1).$$

Nếu cả 2 và 3 đều không là bình phương trong, 6 sẽ là một bình phương trong $\mathbb{F}_p$, và

$$X^4 - 10X^2 + 1 = (X^2 - (5 + 2\sqrt{6}))(X^2 - (5 - 2\sqrt{6})).$$

Nghiên cứu về các đa thức như vậy sử dụng các phương pháp không sơ cấp. Xem chẳng hạn bài báo Brandl, R., Amer. Math. Monthly, 93 (1986), pp 286 – 288, ở đó chứng minh rằng mọi số nguyên không nguyên tố $n \geq 1$ xuất hiện như là bậc của một đa thức trong $\mathbb{Z}[X]$ mà nó bất khả quy trên $\mathbb{Z}$ nhưng khả quy trong mọi modulo nguyên tố.

Mệnh đề 1.20 (TÍNH CHẤT NHÂN CỦA BẬC)**.** *Xét các trường $L \supset E \supset F$. L/F có bậc hữu hạn nếu và chỉ nếu L/E và E/F đều có bậc hữu hạn, và khi đó*

$$[L : F] = [L : E][E : F].$$

Chứng minh. Nếu L có bậc hữu hạn trên F, thì nó chắc chắn có bậc hữu hạn trên E. Hơn nữa, E, là một không gian con của một F-không gian véctơ, cũng có bậc hữu hạn.

Do vậy, giả sử rằng L/E và E/F có bậc hữu hạn, và đặt $(e_i)_{1\leq i\leq m}$ là một cơ sở của E như là một F-không gian vec tơ và đặt $(l_j)_{1\leq j\leq n}$ là một cơ sở của L như là một E-không gian vec tơ. Để hoàn tất chứng minh, ta cần chỉ ra rằng $(e_i l_j)_{1\leq i\leq m, 1\leq j\leq n}$ là một cơ sở của L trên F, bởi vì sau đó L sẽ hữu hạn trên F với bậc $[L : E][E : F]$.

Trước hết, $(e_i l_j)_{i,j}$ sinh ra L. Cho $\gamma \in L$. Khi đó, do $(l_j)_j$ sinh ra L như là một E-không gian vec tơ,

$$\gamma = \sum_j \alpha_j l_j \text{ với } \alpha_j \in E,$$

và bởi vì $(e_i)_i$ sinh ra E như là một F-không gian vec tơ,

$$\alpha_j = \sum_j a_{ij} e_i \text{ với } a_{ij} \in F.$$

Từ hai đẳng thức trên ta có

$$\gamma = \sum_{i,j} a_{ij} e_i l_j.$$

Thứ hai, $(e_i l_j)_{i,j}$ độc lập tuyến tính. Quan hệ tuyến tính $\sum a_{ij} e_i l_j = 0, a_{ij} \in F$ có thể được viết lại $\sum_j (\sum_i a_{ij} e_i) l_j = 0$. Tính độc lập tuyến tính của $(l_j)_j$ chỉ ra rằng $\sum_i a_{ij} e_i = 0$ với mỗi j, và tính độc lập tuyến tính của $(e_i)_i$ chỉ ra rằng $a_{ij} = 0$. □

1.7. Vành con sinh bởi một tập con

Giao của các vành con của một vành lại là một vành. Cho F là một trường con của trường E và S là một tập con của E. Giao của tất cả các vành con của E chứa F và S rõ ràng là vành con nhỏ nhất của E chứa F

và S. Ta gọi nó là vành con của E **sinh bởi** F **và** S **(hay là sinh bởi** F **trên** S**)**, ký hiệu là $F[S]$. Nếu $S = \{\alpha_1, \ldots, \alpha_n\}$, ta viết $F[\alpha_1, \ldots, \alpha_n]$ thay cho $F[S]$. Ví dụ, $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$.

Bổ đề 1.21. *Vành $F[S]$ bao gồm tất cả các phần tử của E có thể biểu diễn được dưới dạng tổng hữu hạn*

$$\sum a_{i_1 \ldots i_n} \alpha_1^{i_1} \ldots \alpha_n^{i_n}, \quad a_{i_1 \ldots i_n} \in F, \quad \alpha_i \in S. \quad (*)$$

Chứng minh. Cho R là một tập tất cả các phần tử như vậy. Hiển nhiên, R là một vành con chứa F và S và nó chứa trong mọi vành con khác cũng chứa F và S. Do vậy R chính là $F[S]$. □

Ví dụ 1.22. *Vành $\mathbb{Q}[\pi], \pi = 3.14159\ldots$, gồm tất cả các số thực có thể viết được dưới dạng tổng hữu hạn*

$$a_0 + a_1\pi + a_2\pi^2 + \cdots + a_n\pi^n, \quad a_i \in \mathbb{Q}.$$

Vành $\mathbb{Q}[i]$ bao gồm tất cả các số phức có dạng $a + bi$ với $a, b \in \mathbb{Q}$.

Chú ý rằng cách viết của một phần tử dưới dạng $(*)$ nói chung không duy nhất. Điều này đúng ngay cả với $\mathbb{R}[i]$.

Bổ đề 1.23. *Cho R là một miền nguyên chứa một trường con F (như là một vành con). Nếu R có hữu hạn chiều, xem như là một F-không gian véctơ, thì nó là một trường.*

Chứng minh. Cho α là một phần tử khác 0 của R - ta phải chứng tỏ rằng α có một nghịch đảo trong R. Ánh xạ $x \mapsto \alpha x : R \to R$ là đơn cấu của F-không gian vec tơ hữu hạn chiều, và do vậy nó là toàn cấu. Nói riêng, tồn tại một phần tử $\beta \in R$ mà $\alpha\beta = 1$. □

Chú ý rằng bổ đề áp dụng cho các vành con (chứa F) của một mở rộng trường E của F với bậc hữu hạn.

1.8. Trường con sinh bởi một tập con

Giao của các trường con của một trường lại là một trường. Cho F là một trường con của trường E, và S là một tập con của E. Giao của tất cả các trường con của E chứa F và S là trường con nhỏ nhất của E chứa F và S. Ta gọi nó là trường con của E **sinh bởi** F **và** S **(sinh bởi** F

trên S), và ký hiệu là $F(S)$. Đó là trường các thương của $F[S]$ trên E, vì là một trường con của E chứa F và S và nằm trong mọi trường khác như vậy. Nếu $S = \{\alpha_1, \ldots, \alpha_n\}$, ta viết $F(\alpha_1, \ldots, \alpha_n)$ thay cho $F(S)$. Như vậy, $F[\alpha_1, \ldots, \alpha_n]$ chứa tất cả các phần tử của E sao cho chúng có thể biểu diễn dưới dạng đa thức của α_i với hệ số trong F, và $F(\alpha_1, \ldots, \alpha_n)$ chứa tất cả các phần tử của E mà chúng có thể biểu diễn dưới dạng thương của hai đa thức như vậy.

Bổ đề 1.23 chỉ ra rằng $F[S]$ là một trường nếu nó hữu hạn chiều trên F, trong trường hợp đó $F(S) = F[S]$.

Ví dụ 1.24. *Trường $\mathbb{Q}(\pi), \pi = 3.14\ldots$, chứa tất cả các số phức mà chúng biểu diễn dưới dạng thương*

$$g(\pi)/h(\pi), \quad g(X), h(X) \in \mathbb{Q}[X], \quad h(X) \neq 0.$$

Vành $\mathbb{Q}[i]$ hiển nhiên là một trường.

Một mở rộng E của F được gọi là **đơn** nếu $E = F(\alpha)$ với $\alpha \in E$ nào đó. Ví dụ, $\mathbb{Q}(\pi)$ và $\mathbb{Q}[i]$ là các mở rộng đơn của $\mathbb{Q}$.

Cho F và F' là các trường con của trường E. Giao của các trường con của E chứa F và F' là trường con bé nhất của E chứa cả F và F'. Ta gọi nó là **hợp** của F và F' trong E, và ký hiệu là $F \cdot F'$. Nó cũng có thể được miêu tả như là trường con của E sinh bởi F' trên F, hay trường con trên F sinh bởi F':

$$F(F') = F \cdot F' = F'(F).$$

1.9. Xây dựng một số mở rộng trường

Cho $f(X) \in F[X]$ là một đa thức đơn khởi bậc m, và (f) là iđêan sinh bởi f. Xét vành thương $F[X]/(f)$, gọi x là ảnh của X trong $F[X]/(f)$, tức là, x là lớp kề $X + (f)$. Khi đó:

(a) Ánh xạ
$$P(X) \mapsto P(x) : F[X] \to F[x]$$
là một toàn cấu trong đó ảnh của $f(X)$ là 0. Do vậy, $f(x) = 0$.

(b) Từ thuật toán chia, ta biết rằng mỗi phần tử g của $F[X]/(f)$ được biểu diễn một cách duy nhất bởi một đa thức r có bậc $< m$. Do đó mỗi phần tử của $F[X]$ có thể biểu diễn duy nhất dưới dạng tổng
$$a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}, \quad a_i \in F. \quad (*)$$

(c) Để cộng hai phần tử biểu diễn dưới dạng $(*)$, chỉ cần cộng các hệ số tương ứng.

(d) Để nhân hai phần tử biểu diễn dưới dạng $(*)$, ta nhân theo cách thông thường, và dùng quan hệ $f(x) = 0$ để biểu thị các đơn thức có bậc $\geq m$ theo x dưới dạng các đơn thức với bậc nhỏ hơn.

(e) Bây giờ giả sử rằng $f(X)$ là bất khả quy. Khi đó mọi phần tử α khác 0 trong $F[X]$đều có nghịch đảo, có thể tìm được như sau: Dùng (b) để viết $\alpha = g(x)$ với $g(X)$ là một đa thức có bậc $\leq m-1$, và dùng thuật toán Euclid trong $F[X]$ để tìm được các đa thức $a(X)$ và $b(X)$ thỏa mãn

$$a(X)f(X) + b(X)g(X) = d(X)$$

ở đó $d(X)$ là ước chung lớn nhất của f và g. Trong trường hợp đang xét, $d(X)$ là 1 vì $f(X)$ bất khả quy và $\deg g(X) < \deg f(X)$. Khi thay X bởi x, đẳng thức trở thành

$$b(x)g(x) = 1.$$

Do vậy $b(x)$ là nghịch đảo của $g(x)$.

Từ các quan sát trên ta đi đến kết luận:

1.25. *Với mỗi đa thức đơn khởi bất khả quy $f(X)$ bậc m trong $F[X]$,*

$$F[x] \overset{đn}{=} F[X]/(f)$$

là một trường bậc m trên F. Hơn nữa, các tính toán trong $F[x]$ được quy về các tính toán trong F.

Ví dụ 1.26. *Cho $f(X) = X^2 + 1 \in \mathbb{R}[X]$. Khi đó $\mathbb{R}[X]$ có:*

- *Các phần tử: $a + bx$, $a, b \in \mathbb{R}$;*
- *Phép cộng: $(a + bx) + (a' + b'x) = (a + a') + (b + b')x$;*
- *Phép nhân: $(a + bx)(a' + b'x) = (aa' - bb') + (ab' + a'b)x$.*

Ta thường viết i thay cho x và $\mathbb{C}$ thay cho $\mathbb{R}[x]$.

Ví dụ 1.27. *Cho* $f(X) = X^3 - 3X - 1 \in \mathbb{Q}[X]$. *Ta đã biết trong Ví dụ 1.12 đa thức này bất khả quy trên* $\mathbb{Q}$, *và do vậy* $\mathbb{Q}[x]$ *là một trường. Nó có cơ sở* $\{1, x, x^2\}$ *như là một* $\mathbb{Q}$*-không gian vec tơ. Cho*

$$\beta = x^4 + 2x^3 + 3 \in \mathbb{Q}[x].$$

Sau đó sử dụng $x^3 - 3x - 1 = 0$, *ta có* $\beta = 3x^2 + 7x + 5$. *Bởi vì* $X^3 - 3X - 1$ *bất khả quy,*

$$gcd(X^3 - 3X - 1, 3X^2 + 7X + 5) = 1.$$

Thực tế, thuật toán Euclid cho ta

$$(X^3 - 3X - 1)(\frac{-7}{37}X + \frac{29}{111}) + (3X^2 + 7X + 5)(\frac{7}{111}X^2 - \frac{26}{111}X + \frac{28}{111}) = 1$$

Do đó

$$(3x^2 + 7x + 5)(\frac{7}{111}x^2 - \frac{26}{111}x + \frac{28}{111}) = 1$$

và ta vừa tìm được phần nghịch đảo của β.

Cũng có thể làm điều này bằng việc sử dụng PARI `beta=Mod(X^4+2*X^3+3, X^3-3*X-1)` sẽ cho $\beta = 3x^2 + 7x + 5$ trong $\mathbb{Q}[X]$, và `beta^(-1)` sẽ cho $\beta^{-1} = \frac{7}{111}x^2 - \frac{26}{111}x + \frac{28}{111}$.

1.10. Trường mầm

Cho f là một đa thức đơn khởi bất khả quy trong $F[X]$. Một cặp (E, α) bao gồm một mở rộng E của F và một phần tử $\alpha \in E$ được gọi là **trường mầm** [5] của f nếu $E = F[\alpha]$ và $f(\alpha) = 0$. Ví dụ, cặp (E, α) với $E = F[X]/(f) = F[x]$ và $\alpha = x$ là một trường mầm[6] của f. Cho (E, α) là một trường mầm, xét toàn cấu của các F-đại số

$$g(X) \mapsto g(\alpha) \colon F[X] \to E.$$

Hạt nhân của nó được sinh bởi một đa thức đơn khởi khác 0, chia hết f, và do vậy phải bằng f. Do đó, đồng cấu này xác định một F-đẳng cấu

$$x \mapsto \alpha \colon F[x] \to E, \quad F[X] \overset{\text{đn}}{=} F[X]/(f).$$

[5] Theo A. Albert, Modern Higher Algebra, 1937, người gọi trường phân rã của một đa thức là trường các nghiệm của nó.

[6] stem field= trường mầm

Nói cách khác, trường mầm (E, α) của f là F-đẳng cấu với trường mầm chính tắc $(F[X]/(f), x)$. Nói riêng, mỗi phần tử của trường mầm (E, α) của f có một biểu diễn duy nhất

$$a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}, \quad a_i \in F, \quad m = deg(f),$$

i.e., $1, \alpha, \ldots, \alpha^{m-1}$ là một F-cơ sở cho $F[\alpha]$, và tính toán trong $F[\alpha]$ có thể thực hiện bằng cùng các quy tắc như trong $F[x]$. Nếu (E, α') là một trường mầm thứ hai của f, thì có duy nhất một F-đẳng cấu $E \to E'$ ánh xạ α thành α'. Chúng ta đôi khi viết "trường mầm $F[\alpha]$" thay cho "trường mầm $(F[\alpha], \alpha)$".

1.11. Phần tử đại số và phần tử siêu việt

Đối với mỗi trường F và một phần tử α của một mở rông trường E, ta có một đồng cấu

$$f(X) \mapsto f(\alpha) \colon F[X] \to E.$$

Có hai khả năng.

Trường hợp 1: Hạt nhân của ánh xạ là (0), do đó với $f \in F[X]$,

$$f(\alpha) = 0 \Rightarrow f = 0(\text{trong } F[X]).$$

Trong trường hợp này, ta nói rằng α **siêu việt trên** F. Đồng cấu $X \mapsto \alpha \colon F[X] \to F[\alpha]$ là một đẳng cấu, và nó mở rộng thành một đẳng cấu $F[X] \to F(\alpha)$.

Trường hợp 2: Hạt nhân của ánh xạ $\neq (0)$, nghĩa là $g(\alpha) = 0$ với $g \neq 0$ nào đó thuộc $F[X]$. Trong trường hợp này, ta nói rằng α **đại số trên** F. Các đa thức g thỏa mãn $g(\alpha) = 0$ lập thành một iđêan khác (0) trong $F[X]$, iđêan đó được sinh ra bởi một đa thức đơn khởi f có bậc thấp nhất thỏa mãn $f(\alpha) = 0$. Ta gọi f là **đa thức tối tiểu** của α trên F. Nó là bất khả qui, bởi nếu không sẽ có hai phần tử khác 0 của E mà tích của chúng bằng 0. Đa thức tối tiểu được xác định trong $F[X]$ bởi một trong các điều kiện sau:

- f đơn khởi; $f(\alpha) = 0$ và chia hết cho mọi đa thức g khác trong $F[X]$ thỏa mãn $g(\alpha) = 0$.
- f là đa thức đơn khởi với bậc nhỏ nhất thỏa mãn $f(\alpha) = 0$;

- f đơn khởi, bất khả quy và $f(\alpha) = 0$.

Chú ý rằng $g(X) \mapsto g(\alpha)$ xác định một đẳng cấu $F[X]/(f) \to F[\alpha]$. Vì $F[X]/(f)$ là một trường, ta cũng có

$$F(\alpha) = F[\alpha].$$

Vì vậy, $F[\alpha]$ là một trường mầm của f.

Ví dụ 1.28. *Cho $\alpha \in \mathbb{C}$ thỏa mãn $\alpha^3 - 3\alpha - 1 = 0$. Khi đó $X^3 - 3X - 1$ đơn khởi, bất khả quy, và có α là một nghiệm, và do vậy nó là đa thức tối tiểu của α trên $\mathbb{Q}$. Tập hợp $\{1, \alpha, \alpha^2\}$ là một cơ sở của $\mathbb{Q}[\alpha]$ trên $\mathbb{Q}$. Các tính toán trong Ví dụ 1.27 chỉ ra rằng nếu β là $\alpha^4 + 2\alpha^3 + 3$ trong $\mathbb{Q}[\alpha]$, thì $\beta = 3\alpha^2 + 7\alpha + 5$, và*

$$\beta^{-1} = \frac{7}{111}\alpha^2 - \frac{26}{111}\alpha + \frac{28}{111}.$$

Nhận xét 1.29. *PARI biết cách tính trong $\mathbb{Q}[\alpha]$. Ví dụ* `factor(X^4+4)` *trả về phân tích*

$$X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$$

trong $\mathbb{Q}[X]$. Bây giờ gõ `nf=nfinit(a^2+2*a+2)` *để xác định một trường số "nf" sinh trên $\mathbb{Q}$ bởi các nghiệm a của $X^2 + 2X + 2$. Thì* `nffactor(nf,x^4+4)` *trả về phân tích*

$$X^4 + 4 = (X - a - 2)(X - a)(X + a)(X + a + 2)$$

trong $\mathbb{Q}[a]$.

Một mở rộng trường E/F được gọi là một mở rộng **đại số**, và E được gọi là **đại số trên** F, nếu tất cả các phần tử của E đều đại số trên F; nếu không nó được gọi là **siêu việt** (hay E được gọi là **siêu việt trên** F). Như vậy, E/F là một mở rộng siêu việt nếu ít nhất một phần tử của E siêu việt trên F.

Mệnh đề 1.30. *Mở rộng trường E/F là một mở rộng hữu hạn nếu và chỉ nếu E là đại số và hữu hạn sinh (như là một trường) trên F.*

Chứng minh.

$\Rightarrow$: Sự kiện α siêu việt trên F thực chất có nghĩa là hệ $1, \alpha, \alpha^2, \ldots$ độc lập tuyến tính trên F. Bởi vậy, nếu E hữu hạn trên F, thì nó đại số trên F. Ta chỉ còn phải chứng minh E hữu hạn sinh trên F. Nếu $E = F$, thì nó sinh bởi tập rỗng. Nếu không, tồn tại một phần tử α_1 thuộc $E \setminus F$. Nếu $E \neq F[\alpha_1]$, tồn tại một phần tử $\alpha_2 \in E \setminus F[\alpha_1]$, ... Vì

$$[F[\alpha_1] : F] < [F[\alpha_1, \alpha_2] : F] < \cdots < [E : F]$$

nên quá trình phải ngừng sau một số hữu hạn bước.

$\Leftarrow$: Đặt $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ với $\alpha_1, \ldots, \alpha_n$ đại số trên F. Mở rộng $F(\alpha_1)/F$ là hữu hạn bởi vì α_1 đại số trên F và do đó trên $F(\alpha_1)$. Theo 1.20, $F(\alpha_1, \alpha_2)$ hữu hạn trên F. Lập luận trên lại có thể lặp lại.

□

Hệ quả 1.31.

(a) Nếu E đại số trên F thì mọi vành con R của E chứa F là một trường.

(b) Nếu trong một chuỗi mở rộng trường $L \supset E \supset F$, L đại số trên E và E đại số trên F, thì L đại số trên F.

Chứng minh.

(a) Ta đã thấy ở trên rằng nếu α đại số trên F, thì $F[\alpha]$ là một trường. Nếu $\alpha \in R$, thì $F[\alpha] \subset R$, và do vậy α có nghịch đảo trong R.

(b) Mọi $\alpha \in L$ là nghiệm của một đa thức đơn khởi $f = X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in E[X]$. Mỗi mở rộng trong chuỗi $F[a_0, \ldots, a_{m-1}, \alpha] \supset F[a_0, \ldots, a_{m-1}] \supset F$ là hữu hạn (1.20), do đó $F[a_0, \ldots, a_{m-1}, \alpha]$ hữu hạn (nên đại số) trên F.

□

1.12. Số siêu việt

Một số phức được gọi là **đại số** hay **siêu việt** dựa trên tính đại số hoặc siêu việt của nó trên $\mathbb{Q}$. Trước hết ta nhắc lại một số mốc lịch sử:

1844: Liouville chứng tỏ rằng các số, sau này được gọi là các số Liouville, là siêu việt.

1873: Hermite chứng minh rằng e là số siêu việt.

1874: Cantor chứng minh rằng tập hợp các số đại số là đếm được, nhưng $\mathbb{R}$ không đếm được. Do vậy, hầu hết các số là siêu việt (nhưng rất khó để chứng tỏ rằng một số cụ thể là số siêu việt) [7].

1882: Lindemann chứng minh rằng π là số siêu việt.

1934: Gelfond và Schneider, một cách độc lập, cùng chứng minh được rằng α^β là các số siêu việt nếu α và β đại số, $\alpha \neq 0, 1$, và $\beta \notin \mathbb{Q}$. (Đó là bài toán nổi tiếng thứ bảy của Hilbert.)

2013: Hằng số Euler

$$\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} 1/k - logn \right)$$

vẫn chưa được chứng minh là số siêu việt hay thậm chí là số vô tỉ (xem Lagarias, Jeffrey C., Euler's constant: Euler's work and modern developments. Bull. Amer. Math. Soc. 50 (2013), no. 4, 527–628; arXiv:1303:1856))

2013: Các số $e + \pi$ và $e - \pi$ chắc chắn là các số siêu việt, nhưng chúng thậm chí chưa được chứng minh là số vô tỉ!

Mệnh đề 1.32. *Tập hợp các số đại số là đếm được.*

Chứng minh. Định nghĩa độ cao $h(r)$ của số hữu tỉ $r = m/n$ viết dưới dạng tối giản là $\max(|m|, |n|)$. Chỉ có một số hữu hạn các số hữu tỉ với độ cao nhỏ hơn một số N cố định. Ký hiệu $A(N)$ là tập hợp các số đại số mà đa thức tối tiểu trên $\mathbb{Q}$ có bậc $\leq N$ và có độ cao của các hệ số đều $< N$. Khi đó $A(N)$ hữu hạn với mỗi N. Chọn một song ánh từ vài đoạn $[0, n(1)]$ của $\mathbb{N}$ lên $A(10)$; mở rộng nó thành một song ánh từ $[0, n(2)]$ lên $A(100)$, và cứ thế. □

[7] Năm 1873 Cantor chứng minh các số hữu tỷ đếm được ... Ông cũng chứng minh rằng các số đại số cũng đếm được. Tuy nhiên những cố gắng của ông trong việc xác định xem các số thực là đếm được hay không vấp phải khó khăn nhiều hơn. Ông đã chứng minh rằng các số thức không đếm được vào khoảng Tháng 12 năm 1873 và công bố khẳng định này trong một bài báo năm 1874 (MacTutor).

Một số Liouville điển hình là $\sum_{n=0}^{\infty} \frac{1}{10^{n!}}$. Trong khai triển thập phân của nó có một dãy tăng dần các chuỗi gồm toàn các số 0. Vì khai triển thập phân của nó không có chu kỳ nên số đó không phải là số hữu tỉ. Ta sẽ chứng minh số tương tự của số đó trong hệ nhị phân là một số siêu việt.

Định lý 1.33. *Số $\alpha = \sum \frac{1}{2^{n!}}$ là một số siêu việt.*

Chứng minh. Giả sử[8] điều này không đúng, và đặt

$$f(X) = X^d + a_1 X^{d-1} + \cdots + a_d, \quad a_i \in \mathbb{Q},$$

là đa thức tối tiểu của α trên $\mathbb{Q}$. Khi đó $[\mathbb{Q}[\alpha] \colon \mathbb{Q}] = d$. Chọn một số nguyên D khác 0 mà $D \cdot f(X) \in \mathbb{Z}[X]$.

Đặt $\sum_N = \sum_{n=0}^{N} \frac{1}{2^{n!}}$, sao cho $\sum_N \to \alpha$ khi $N \to \infty$, và đặt $x_N = f(\sum_N)$. Do α không phải số hữu tỉ, $f(X)$ bất khả quy với bậc > 1, sẽ không có có nghiệm hữu tỉ. Vì $\sum_N \neq \alpha$ nên không thể là nghiệm của $f(X)$, và do đó $x_N \neq 0$. Hiển nhiên là $x_N \notin \mathbb{Q}$; thực ra $(2^{N!})^d D x_N \in \mathbb{Z}$, và do vậy

$$|(2^{N!})^d D x_N| \geq 1. \quad (*)$$

Từ định lý cơ bản của đại số (xem 5.6 bên dưới), ta biết rằng f chẻ ra trong $\mathbb{C}[X]$,

$$f(X) = \prod_{i=1}^{d} (X - \alpha_i), \quad \alpha_i \in \mathbb{C}, \quad \alpha_1 = \alpha,$$

và do vậy

$$|x_N| = \prod_{i=1}^{d} |\sum_N - \alpha_i| \leq |\sum_N - \alpha_1| (\sum_N + M)^{d-1}, \text{ với } M = max_{i \neq 1}\{1, |\alpha_i|\}.$$

Nhưng

$$|\sum_N - \alpha_1| = \sum_{i=N+1}^{\infty} \frac{1}{2^{n!}} \leq \frac{1}{2^{(N+1)!}} \left(\sum_{n=0}^{\infty} \frac{1}{2^n} \right) = \frac{2}{2^{(N+1)!}}.$$

Do vậy

$$|x_N| \leq \frac{2}{2^{(N+1)!}} \cdot (\sum_N + M)^{d-1}$$

[8] Chứng minh này, tôi học từ David Masser, cũng hiệu quả với $\sum \frac{1}{a^{n!}}$ với mọi số nguyên $a \geq 2$.

và

$$|(2^{N!})^d Dx_N| \leq 2.\frac{2^{d.N!}D}{2^{(N+1)!}}(\sum_N + M)^{d-1}$$

nó tiến tới 0 khi $N \to \infty$ bởi vì $\frac{2^{d.N!}D}{2^{(N+1)!}} = \left((\frac{2^d}{2^{N+1}}\right)^{N!} \to 0$. Điều này mâu thuẫn với $(*)$. □

1.13. Dựng hình bằng thước kẻ và compa

Người Hy Lạp đã hiểu được các số nguyên và các số hữu tỉ. Họ đã rất ngạc nhiên khi phát hiện ra rằng độ dài đường chéo của một hình vuông cạnh 1, $\sqrt{2}$, không phải là số hữu tỉ. Họ nhận ra rằng cần phải mở rộng hệ thống số của họ. Sau đó họ mong muốn rằng các số "xây dựng được" là đủ. Giả sử ta được cho một độ dài, gọi là l, một thước kẻ, và một compa (thiết bị để vẽ một hình tròn). Một số thực (hay chính xác hơn là một độ dài) **có thể xây dựng được** nếu nó có thể xây dựng bằng cách thực hiện tuần tự các giao điểm của

- Các đường thẳng vẽ qua hai điểm đã được xây dựng, và
- Các đường tròn có tâm là các điểm đã được xây dựng và bán kính là một độ dài đã được xây dựng.

Những quan sát này dẫn tới ba bài toán nổi tiếng mà họ đã không thể giải quyết được: có thể gấp đôi một lập phương, chia ba một góc, hay cầu phương đường tròn bởi các phép xây dựng chỉ dùng thước kẻ và compa hay không? Chúng ta sẽ thấy rằng câu trả lời cho cả ba câu hỏi là phủ định.

Giả sử F là một trường con của $\mathbb{R}$. Với mỗi số dương $a \in F$, $\sqrt{a}$ ký hiệu căn bậc hai dương của a trong $\mathbb{R}$. Định nghĩa **F-mặt** là $F \times F \subset \mathbb{R} \times \mathbb{R}$. Ta có các định nghĩa sau:

- Một **F-đường thẳng** là một đường thẳng trong $\mathbb{R} \times \mathbb{R}$ đi qua hai điểm trong F-mặt. Chúng là các đường cho bởi phương trình

$$ax + by + c = 0, \quad a, b, c \in F.$$

- Một **F-đường tròn** là một đường tròn trong $\mathbb{R} \times \mathbb{R}$ có tâm là một F-điểm và bán kính là một phần tử của F. Chúng là các đường tròn

được cho bởi phương trình

$$(x-a)^2+(y-b)^2=c^2, \quad a,b,c\in F.$$

Bổ đề 1.34. *Cho $L\neq L'$ là các F-**đường thẳng**, và $C\neq C'$ là các F-**đường tròn**.*

(a) $L\cap L'=\emptyset$ hoặc gồm duy nhất một F-điểm.

(b) $L\cap C=\emptyset$ hoặc gồm một hoặc hai điểm trong $F[\sqrt{e}]$-mặt, với $e\in F$, $e>0$.

(c) $C\cap C'=\emptyset$ hoặc gồm một hoặc hai điểm trong $F[\sqrt{e}]$-mặt, với $e\in F$, $e>0$.

Chứng minh. Các giao điểm được tìm bằng cách giải các phương trình xảy ra đồng thời, và do vậy dẫn tới việc giải các phương trình bậc hai với hệ số trong F. □

Bổ đề 1.35.

(a) Nếu c và d có thể xây dựng được, thì $c+d, -c, cd$ và $\frac{c}{d}\,(d\neq 0)$ cũng vậy.

(b) Nếu $c>0$ xây dựng được, thì $\sqrt{c}$ cũng xây dựng được.

Chứng minh.

(a) Trước hết chứng minh rằng có thể xây dựng một đường vuông góc với một đường thẳng cho trước qua một điểm, và một đường thẳng qua một điểm cho trước song song với một đường thẳng. Do vậy có thể xây dựng một tam giác đồng dạng với một tam giác cho trước. Với lựa chọn phù hợp ta có thể xây dựng cd và c^{-1}.

(b) Vẽ một đường tròn bán kính $\frac{c+1}{2}$ và tâm là $(\frac{c+1}{2},0)$, và vẽ một đường thẳng đứng qua điểm $A=(1,0)$ gặp đường tròn tại P. Độ dài AP là $\sqrt{c}$. (Có thể xem chi tiết tại Artin, M., 1991, Algebra, Prentice Hall, Chapter 13, Section 4.)

□

Định lý 1.36.

(a) Tập hợp tất cả các số xây dựng được lập thành một trường.

(b) Một số α xây dựng được nếu và chỉ nếu nó nằm trong một trường con của $\mathbb{R}$ có dạng

$$\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_r}], \quad a_i \in \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}], \quad a_i > 0.$$

Chứng minh.

(a) Đây là hệ quả trực tiếp từ Bổ đề 1.35.

(b) Từ Bổ đề 1.34 ta suy ra mọi số xây dựng được chứa trong một trường dạng $\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_r}]$. Ngược lại, nếu tất cả các phần tử của $\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}]$ đều xây dựng được, thì $\sqrt{a_i}$ xây dựng được (do 1.35b), và do vậy tất cả các phần tử của $\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_i}]$ xây dựng được. Dùng lập luận này cho $i = 0, 1, \ldots$ ta kết luận rằng tất cả phần tử của $\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_r}]$ xây dựng được.

□

Hệ quả 1.37. *Nếu α xây dựng được, thì α là đại số trên $\mathbb{Q}$, và $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ là một lũy thừa của 2.*

Chứng minh. Theo Mệnh đề 1.20, $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ chia hết

$$[\mathbb{Q}[\sqrt{a_1}] \ldots [\sqrt{a_r}] : \mathbb{Q}]$$

và $[\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_r}] : \mathbb{Q}]$ là một lũy thừa của 2. □

Hệ quả 1.38. *Không thể gấp đôi một lập phương bằng phép dựng hình từ thước thẳng và compa.*

Chứng minh. Bài toán chính là việc xây dựng một hình lập phương với thể tích 2. Việc này yêu cầu xây dựng nghiệm thực của phương trình $X^3 - 2 = 0$. Nhưng đa thức này là bất khả quy (theo tiêu chuẩn Eisenstein 1.16) và do đó $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$. □

Hệ quả 1.39. *Nói chung, không thể chia ba một góc cho trước bằng thước kẻ và compa.*

Chứng minh. Biết một góc có nghĩa là biết cos của góc đó. Do vậy, để chia ba 3α, ta phải xây dựng một lời giải cho

$$\cos 3\alpha = 4\cos^3 \alpha - 3\cos \alpha.$$

Ví dụ, chọn $3\alpha = 60^0$. Từ $\cos 60^0 = \frac{1}{2}$, để xây dựng α, ta phải giải phương trình $8x^3 - 6x - 1 = 0$, một đa thức là bất khả quy (sử dụng 1.11). □

Hệ quả 1.40. *Không thể cầu phương hình tròn bằng thước kẻ và compa.*

Chứng minh. Một hình vuông có cùng diện tích với một đường tròn bán kính r có cạnh $\sqrt{\pi}r$. Do π là số siêu việt [9] nên $\sqrt{\pi}$ cũng vậy. □

Ta tiếp tục xét một bài toán khác từ thời Hy Lạp cổ đại: Liệt kê các số n mà các n-giác đều có thể xây dựng được. Ở đây ta nghiên cứu câu hỏi đối với các số nguyên tố p (xem 5.15 cho trường hợp tổng quát). Chú ý rằng $X^p - 1$ không bất khả quy; cụ thể là

$$X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \cdots + 1).$$

Bổ đề 1.41. *Nếu p là một số nguyên tố, thì $X^{p-1} + \cdots + 1$ bất khả quy; do vậy $\mathbb{Q}[e^{2\pi i/p}]$ có bậc $p-1$ trên $\mathbb{Q}$.*

Chứng minh. Cho $f(X) = (X^p - 1)/(X - 1) = X^{p-1} + \cdots + 1$; thì

$$f(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \cdots + a_2X^2 + a_1X + p.$$

với $a_i = \binom{i+1}{p}$. Bây giờ $p|a_i$ với $i = 1, \ldots, p-2$, và do vậy $f(X+1)$ bất khả quy theo tiêu chuẩn Eisenstein 1.16. Do đó, $f(X)$ là bất khả quy. □

Để xây dựng một p-giác đều, p là một số nguyên tố, ta cần xây dựng

$$\cos\frac{2\pi}{p} = (e^{\frac{2\pi}{p}} + (e^{\frac{2\pi}{p}})^{-1})/2$$

Nhưng

$$\mathbb{Q}[e^{\frac{2\pi i}{p}}] \supset \mathbb{Q}[\cos\frac{2\pi}{p}] \supset \mathbb{Q},$$

và bậc của $\mathbb{Q}[e^{\frac{2\pi i}{p}}]$ trên $\mathbb{Q}[\cos\frac{2\pi}{p}]$ là 2 - phương trình

$$\alpha^2 - 2\cos\frac{2\pi}{p}\alpha + 1 = 0, \quad \alpha = e^{\frac{2\pi i}{p}},$$

chứng tỏ rằng nó ≤ 2, và nó không thể là 1 bởi vì $\mathbb{Q}[e^{\frac{2\pi i}{p}}]$ không chứa trong $\mathbb{R}$. Do vậy

$$\mathbb{Q}[\cos\frac{2\pi}{p} : \mathbb{Q}] = \frac{p-1}{2}.$$

[9] Chứng minh cho điều này có thể được tìm thấy trong nhiều sách lý thuyết số, ví dụ, trong 11.14 của Hardy, G. H., and Wright, E. M., An Introduction to the Theory of Numbers, Fourth Edition, Oxford, 1960.

Vậy nên, nếu p-đa giác đều xây dựng được, thì $(p-1)/2 = 2^k$ với k nào đó (sau này, xem 5.12, ta sẽ thấy chiều ngược lại), nó chỉ ra rằng $p = 2^{k+1}+1$. Nhưng 2^r+1 là một số nguyên tố nếu r là một lũy thừa của 2, bởi vì nếu không r có nhân tử lẻ t và với t lẻ,

$$Y^t + 1 = (Y+1)(Y^{t-1} - Y^{t-2} + \cdots + 1);$$

Từ đó

$$2^{st} + 1 = (2^s+1)((2^s)^{t-1} - (2^s)^{t-2} + \cdots + 1).$$

Như vậy các số nguyên tố p mà p-đa giác đều có thể xây dựng được chính xác là các số nguyên tố có dạng $2^{2^k}+1$ với k nào đó. Những só nguyên tố như vậy được gọi là **số nguyên tố Fermat** (bởi vì ông phỏng đoán tất cả các số có dạng $2^{2^k}+1$ là các số nguyên tố). Với $k = 0, 1, 2, 3, 4$, ta có $2^{2^k}+1 = 3, 5, 17, 257, 65537$, chúng hiển nhiên là các số nguyên tố, nhưng Euler chỉ ra rằng $2^{32}+1 = 641.6700417$, và chúng ta sẽ không biết liệu rằng có còn các số nguyên tố Fermat khác. Vì vậy, chúng ta không biết danh sách tất cả các số nguyên tố p mà p-đa giác đều có thể xây dựng được.

Gauss chứng tỏ rằng [10] $\cos\frac{2\pi}{17}$ bằng

$$\frac{-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}}{16} + \frac{\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}}{8}$$

khi ông ấy 18 tuổi. Thành công đó là một động lực khiến ông trở thành một nhà toán học.

1.14. Trường đóng đại số

Ta nói rằng một đa thức **chẻ ra** trong $F[X]$ (hay trong F) nếu nó là tích của các đa thức bậc 1 trong $F[X]$.

Mệnh đề 1.42. *Đối với một trường Ω, các phát biểu sau là tương đương:*

(a) Mọi đa thức khác hằng số trong $\Omega[X]$ chẻ ra trong $\Omega[X]$.

[10] Hoặc cũng có thể

$$\cos\frac{2\pi}{7} = \frac{-1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34-2\sqrt{17}} + \frac{1}{8}\sqrt{17+3\sqrt{17}-2\sqrt{34-2\sqrt{17}}-\sqrt{170-26\sqrt{17}}}$$

-cả hai biểu cách viết đều đúng.

(b) Mọi đa thức khác hằng số trong $\Omega[X]$ *có ít nhất một nghiệm trong* $\Omega[X]$

(c) Các đa thức bất khả quy trong $\Omega[X]$ *có bậc* 1.

(d) Mọi trường bậc hữu hạn trên Ω *chính bằng* Ω.

Chứng minh. Các phép suy $(a) \to (b) \to (c) \to (a)$ là hiển nhiên.

$(c) \to (d)$. Cho E là một mở rộng hữu hạn của Ω, và cho $\alpha \in E$. Đa thức tối tiểu của α có bậc 1, và do vậy $\alpha \in \Omega$.

$(d) \to (c)$. Cho f là một đa thức bất khả quy trong $\Omega[X]$. Khi đó $\Omega[X]/(f)$ là một mở rộng trường của Ω với bậc $deg(f)$ (xem 1.30), và do vậy $deg(f) = 1$. □

Định nghĩa 1.43.

(a) Một trường được gọi là **đóng đại số** nếu nó thỏa mãn các điều kiện tương đương của Mệnh đề 1.42.

(b) Một trường Ω được gọi là **bao đóng đại số** của một trường con F nếu nó là trường đóng đại số và đại số trên F.

Ví dụ, định lý cơ bản của đại số (xem 5.6 dưới đây) phát biểu rằng trường số phức $\mathbb{C}$ đóng đại số. Nó là một bao đóng đại số của $\mathbb{R}$.

Mệnh đề 1.44. *Nếu* Ω *đại số trên* F *và mọi đa thức* $f \in F[X]$ *chẻ ra trong* $\Omega[X]$*, thì* Ω *đóng đại số (và do đó là một bao đóng đại số của* F*).*

Chứng minh. Giả sử f là một đa thức khác hằng số trong $\Omega[X]$, ta phải chứng tỏ rằng f có một nghiệm trong Ω. Ta biết rằng f có một nghiệm α trong một mở rộng trường hữu hạn Ω' nào đó của Ω. Đặt

$$f = a_n X^n + \cdots + a_0, \quad a_i \in \Omega,$$

và xét các trường

$$F \subset F[a_0, \ldots, a_n] \subset F[a_0, \ldots, a_n, \alpha].$$

Mỗi mở rộng đều là đại số và hữu hạn sinh nên hữu hạn (do 1.30). Vì vậy α thuộc một mở rộng hữu hạn của F, và do đó nó đại số trên F - nó là một nghiệm của một đa thức g với hệ số trong F. Theo giả thiết, g chẻ ra trong $\Omega[X]$ nên tất cả các nghiệm của g trong Ω' đều nằm trong Ω. Nói riêng, $\alpha \in \Omega$. □

Mệnh đề 1.45. *Cho $L \subset F$; thì*

$$\{\alpha \in \Omega \mid \alpha \text{ đại số trên } F\}$$

là một trường.

Chứng minh. Nếu α và β đại số trên F, thì $F[\alpha, \beta]$ là một trường (do 1.31) có bậc hữu hạn trên F (do 1.30) . Do vậy, mọi phần tử của $F[\alpha, \beta]$ đại số trên F, bao gồm $\alpha \pm \beta, \alpha/\beta, \alpha\beta$. □

Trường được xây dựng trong Mệnh đề trên được gọi là **bao đóng đại số của f trong Ω**.

Hệ quả 1.46. *Cho Ω là một trường đóng đại số. Với mỗi trường con F của Ω, bao đóng đại số của F trên Ω là một bao đóng đại số của F.*

Chứng minh. Từ định nghĩa của nó, ta thấy rằng nó đại số trên F và mọi đa thức trong $F[X]$ đều chẻ ra trong nó. Mệnh đề 1.44 chỉ ra rằng nó là một bao đóng đại số của F. □

Vì vậy, khi chúng ta thừa nhận định lý cơ bản của đại số (5.6), mọi trường con của $\mathbb{C}$ có một bao đóng đại số (trong thực tế, một bao đóng đại số chính tắc). Sau này (Chương 6) chúng ta sẽ chứng minh (sử dụng tiên đề chọn) rằng mỗi trường đều có một bao đóng đại số.

Ghi chú 1.47. *Mặc dù có nhiều lớp các trường khác nhau, ví dụ, các trường số và các trường hàm đã được nghiên cứu trước đây, một nghiên cứu có hệ thống về lý thuyết các trường trừu tượng được đưa ra bởi Steinitz vào năm 1910 (Algebraische Theorie der Korper, J. Reine Angew. Math., 137:167–309). Ở đây, ông giới thiệu khái niệm về trường nguyên tố, phân biệt giữa mở rộng tách được và mở rộng không tách được, và chứng tỏ rằng mỗi trường có thể thu được như một mở rộng đại số của một mở rộng thuần túy siêu việt. Ông cũng chứng minh rằng mọi trường có một bao đóng đại số, sai khác nhau một đẳng cấu. Công trình của ông đã có ảnh hưởng tới các nhà đại số học sau này (Noether, van der Waerden, Artin,...) và các bài báo của ông đã được mô tả bởi Bourbaki như là "... Công trình cơ bản, có thể được coi như là nguồn gốc của các khái niệm trong đại số ngày nay". Xem: Roquette, Peter, In memoriam Ernst Steinitz (1871–1928). J. Reine Angew. Math. 648 (2010), 1–11.*

Bài tập

1-1 Cho $E = \mathbb{Q}[\alpha]$, với $\alpha^3 - \alpha^2 + \alpha + 2 = 0$. Biểu diễn $(\alpha^2 + \alpha + 1)(\alpha^2 - \alpha)$ và $(\alpha - 1)^{-1}$ dưới dạng $a\alpha^2 + b\alpha + c$ với $a, b, c \in \mathbb{Q}$.

1-2 Xác định $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$.

1-3 Cho F là một trường và $f(X) \in F[X]$.

(a) Với mọi $a \in F$, chứng minh rằng tồn tại một đa thức $q(X) \in F[X]$ mà
$$f(X) = q(X)(X - a) + f(a).$$

(b) Suy ra rằng $f(a) = 0$ nếu và chỉ nếu $(X - a)|f(X)$.

(c) Suy ra rằng $f(X)$ có thể có nhiều nhất $deg\, g$ nghiệm.

(d) Cho G là một nhóm abel hữu hạn. Nếu G có nhiều nhất m phần tử bậc chia hết m với mỗi ước m của $(G : 1)$, chứng tỏ rằng G là nhóm xyclic.

(e) Suy ra rằng một nhóm con hữu hạn của $F^\times$, F là một trường, là cylic.

1-4 Chứng minh rằng với thước kẻ, compa, và một dụng cụ chia ba góc, ta không thể xây dựng một đa giác đều 7 cạnh.

1-5 Cho $f(X)$ là một đa thức bất khả quy trên F có bậc n, và cho E là một mở rộng trường của F với $[E : F] = m$. Nếu $\gcd(m, n) = 1$, chứng tỏ rằng f bất khả qui trên E.

1-6 Chứng minh rằng không tồn tại một đa thức $f(X) \in \mathbb{Z}[X]$ bậc > 1 mà bất khả quy modulo p với mọi số nguyên tố p.

CHƯƠNG 2

Trường phân rã, nghiệm bội

2.1. Ánh xạ từ mở rộng đơn

Cho E và E' là các trường chứa F. Nhắc lại rằng một F-đồng cấu là một đồng cấu

$$\varphi\colon E \to E'$$

sao cho $\varphi(a) = a$ với mọi $a \in F$. Nói riêng, một F-đồng cấu φ ánh xạ một đa thức

$$\sum a_{i_1\dots i_m}\alpha_1^{i_1}\dots\alpha_m^{i_m}, \quad a_{i_1\dots i_m} \in F,$$

thành

$$\sum a_{i_1\dots i_m}\varphi(\alpha_1)^{i_1}\dots\varphi(\alpha_m)^{i_m}.$$

Một F-đẳng cấu là một F-đồng cấu đồng thời là một song ánh.

Một F-đồng cấu $E \to E'$ giữa các trường, nói riêng, là một F-đơn cấu tuyến tính của các F-không gian véctơ, vì thế nếu E và E' có cùng bậc và hữu hạn trên F, thì mọi F-đồng cấu là một F-đẳng cấu.

Mệnh đề 2.1. *Cho $F(\alpha)$ là một mở rộng đơn của trường F, và Ω là một trường chứa F.*

(a) Giả sử α là một phần tử siêu việt trên F. Với mỗi F-đồng cấu $\varphi\colon F(\alpha) \to \Omega$, $\varphi(\alpha)$ cũng siêu việt trên F, và ánh xạ $\varphi \mapsto \varphi(\alpha)$ xác định một tương ứng một-một

$$\{F\text{-đồng cấu } \varphi : F(\alpha) \to \Omega\} \leftrightarrow \{\text{các phần tử siêu việt của } \Omega \text{ trên } F\}.$$

(b) Giả sử α là một phần tử đại số trên F với đa thức tối tiểu $f(X)$. Với mỗi F-đồng cấu $\varphi\colon F[\alpha] \to \Omega$, $\varphi(\alpha)$ là một nghiệm của $f(X)$ trong

Ω, và ánh xạ $\varphi \mapsto \varphi(\alpha)$ xác định một tương ứng một-một

$$\{F\text{-đồng cấu } \varphi : F[\alpha] \to \Omega\} \leftrightarrow \{\text{nghiệm của } f \text{ trong } \Omega\}.$$

Nói riêng, số các ánh xạ như vậy đúng bằng số các nghiệm phân biệt của f trong Ω.

Chứng minh.

(a) α siêu việt trên F có nghĩa là $F[\alpha]$ đẳng cấu với vành đa thức trong ký hiệu α với hệ số trong F. Với mỗi $\gamma \in \Omega$, tồn tại duy nhất một F-đồng cấu $\varphi\colon F[\alpha] \to \Omega$ ánh xạ α thành γ (xem 1.5). Nó mở rộng được thành một ánh xạ từ trường các thương $F(\alpha)$ của $F[\alpha]$ nếu và chỉ nếu tất cả các phần tử khác 0 của $F[\alpha]$ được ánh xạ thành các phần tử khác 0 của Ω, điều này chỉ xảy ra khi và chỉ khi γ là phần tử siêu việt.

(b) Đặt $f(X) = \sum a_i X^i$, và xét một F-đồng cấu $\varphi\colon F[\alpha] \to \Omega$. Tác động φ lên phương trình $\sum a_i \alpha^i = 0$, ta thu được $\sum a_i \varphi(\alpha)^i = 0$, và điều này chứng tỏ rằng $\varphi(\alpha)$ là một nghiệm của $f(X)$ trong Ω. Ngược lại, nếu $\gamma \in \Omega$ là một nghiệm của $f(X)$, thì ánh xạ $F[X] \to \Omega, g(X) \mapsto g(\gamma)$, được phân tích qua $F[X]/(f(X))$. Khi lấy hợp thành với ánh xạ ngược của đẳng cấu $X + f(X) \mapsto \alpha\colon F[X]/(f(X)) \to F[\alpha]$, ta thu được một đồng cấu $F[\alpha] \to \Omega$ ánh xạ α thành γ.

□

Có thể tổng quát hóa hơn một chút các kết quả trên.

Mệnh đề 2.2. *Cho $F(\alpha)$ là một mở rộng đơn của một trường F, và $\varphi_0\colon F \to \Omega$ là một đồng cấu từ F vào một trường thứ hai Ω.*

(a) Nếu α siêu việt trên F, thì ánh xạ $\varphi \mapsto \varphi(\alpha)$ xác định một tương ứng một-một

$$\{\text{các mở rộng } \varphi\colon F(\alpha) \to \Omega \text{ của } \varphi_0\} \leftrightarrow \{\text{các phần tử của } \Omega \text{ siêu việt trên } \varphi_0(F).\}$$

(b) Nếu α đại số trên F với đa thức tối tiểu $f(X)$, thì ánh xạ $\varphi \mapsto \varphi(\alpha)$ xác định một tương ứng một-một

$$\{\text{các mở rộng } \varphi\colon F[\alpha] \to \Omega \text{ của } \varphi_0\} \leftrightarrow \{\text{các nghiệm của } \varphi_0 f \text{ trong } \Omega\}.$$

Nói riêng, số các ánh xạ như vậy bằng số các nghiệm phân biệt của $\varphi_0 f$ trong Ω.

Ở đây, $\varphi_0 f$ là đa thức thu được bằng cách tác động φ_0 lên các hệ số của f: nếu $f = \sum a_i X^i$ thì $\varphi_0 f = \sum \varphi(a_i) X^i$. Một mở rộng của φ_0 lên $F(\alpha)$ có nghĩa là một đồng cấu $\varphi\colon F(\alpha) \to \Omega$ mà $\varphi|F = \varphi_0$.

Chứng minh của mệnh đề này giống như cách chứng minh của mệnh đề trước.

2.2. Trường phân rã

Cho f là một đa thức đơn khởi với hệ số trong F. Một trường E chứa F gọi là **chẻ** f nếu f chẻ ra trong $E[X]$: $f(X) = \prod_{i=1}^{m}(X - \alpha_i)$ với $\alpha_i \in E$. Nếu thêm vào đó E sinh bởi nghiệm của f,

$$E = F[\alpha_1, \ldots, \alpha_m],$$

thì nó được gọi là một **trường phân rã** hay **trường nghiệm** của f. Chú ý rằng $\prod f_i(X)^{m_i}, (m_i \leq 1)$ và $\prod f_i(X)$ có cùng trường phân rã. Và nếu f có $\deg(f) - 1$ nghiệm trong E, thì nó chẻ ra trong $E[X]$ (vì tổng của các nghiệm có thể biểu diễn được từ các hệ số của f, và nằm trong F).

Ví dụ 2.3.

(a) Cho $f(X) = aX^2 + bX + c \in \mathbb{Q}[X]$, và $\alpha = \sqrt{b^2 - 4ac}$. Trường con $\mathbb{Q}[\alpha]$ của $\mathbb{C}$ là một trường phân rã của f.

(b) Cho $f(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$ bất khả qui và $\alpha_1, \alpha_2, \alpha_3$ là các nghiệm của nó trong $\mathbb{C}$. Vì các nghiệm không thực của f xuất hiện thành cặp liên hợp phức nên hoặc 1 hoặc cả 3 số α_i là các số thực. Khi đó $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] = \mathbb{Q}[\alpha_1, \alpha_2]$ là trường phân rã của $f(X)$. Chú ý rằng $[\mathbb{Q}[\alpha_1] : \mathbb{Q}] = 3$ và $[\mathbb{Q}[\alpha_1, \alpha_2] : \mathbb{Q}[\alpha_1]] = 1$ hoặc 2, do vậy $[\mathbb{Q}[\alpha_1, \alpha_2] : \mathbb{Q}] = 3$ hoặc 6. Về sau (4.2), ta sẽ thấy rằng bậc bằng 3 nếu và chỉ nếu biệt thức của $f(X)$ là bình phương của một số hữu tỷ. Ví dụ, biệt thức của $X^3 + bX + c$ là $-4b^3 - 27c^2$, và do vậy trường phân rã của $X^3 + 10X + 1$ có bậc 6 trên $\mathbb{Q}$.

Mệnh đề 2.4. *Mọi đa thức $f \in F[X]$ có một trường phân rã E_f, và*

$$[E_f : F] \leq (\deg f)! \text{ (deg } f \text{ giai thừa).}$$

Chứng minh. Đặt $F_1 = F[\alpha]$ là một trường mầm của một ước đơn khởi bất khả quy nào đó của f trong $F[X]$. Khi đó $f(\alpha_1) = 0$, và ta chọn

$F_2 = F_1[\alpha_2]$ là trường mầm cho một ước đơn khởi bất khả quy của $f(X)/(X-\alpha_1)$ trong $F_1[X]$. Tiếp tục theo cách đó, ta thu được trường phân rã E_f. Đặt $n = \deg f$. Thì $[F_1 : F] = \deg g_1 \leq n, [F_2 : F_1] \leq n-1, \ldots,$ và do vậy $[E_f : E] \leq n!$. □

Nhận xét 2.5. *Giả sử F là một trường. Với một số tự nhiên n cho trước, có thể tồn tại hoặc không các đa thức bậc n trong $F[X]$ mà trường phân rã của chúng có bậc $n!$ - điều này tùy thuộc vào F. Ví dụ, không tồn tại đa thức như vậy với $n > 1$ nếu $F = \mathbb{C}$ (xem 5.6), và cũng không đúng khi $n > 2$ nếu $F = \mathbb{F}_p$ (xem 4.21) hoặc $F = \mathbb{R}$. Tuy nhiên, sau này (4.31) ta sẽ có thể xây dựng một số vô hạn các đa thức bậc n trong $\mathbb{Q}[X]$ mà trường phân rã của chúng có bậc $n!$.*

Ví dụ 2.6.

(a) Cho $f(X) = (X^p - 1)/(X-1) \in \mathbb{Q}[X]$, p nguyên tố. Nếu ξ là một nghiệm của f, thì các nghiệm còn lại là $\xi^2, \xi^3, \ldots, \xi^{p-1}$, và do vậy trường phân rã của f là $\mathbb{Q}[\xi]$.

(b) Giả sử F có đặc số p, và $f = X^p - X - a \in F[X]$. Nếu α là một nghiệm của f, thì các nghiệm còn lại là $\alpha + 1, \ldots, \alpha + p - 1$, và do vậy trường sinh bởi α trên F là một trường phân rã của f (và $F[\alpha] \simeq F[X]/(f)$ nếu f bất khả quy).

(c) Nếu α là một nghiệm của $X^n - a$, thì các nghiệm còn lại có dạng ξa, với $\xi^n = 1$. Do vậy, nếu F chứa tất cả căn bậc n của 1 (tức là $X^n - 1$ chẻ ra trong $F[X]$), thì $F[\alpha]$ là một trường phân rã của $X^n - a$. Chú ý rằng nếu p là đặc số của F, thì $X^p - 1 = (X-1)^p$, và do vậy, F tự động chứa tất cả căn bậc p của 1.

Mệnh đề 2.7. *Cho $f \in F[X]$, E là một trường sinh bởi các nghiệm của f trên F, và Ω là một trường chứa F mà trong đó f chẻ ra.*

(a) Tồn tại một F-đồng cấu $\varphi : E \to \Omega$; số các đồng cấu như vậy nhiều nhất là $[E : F]$, và bằng $[E : F]$ nếu f có nghiệm phân biệt trong Ω.

(b) Nếu E và Ω đều là các trường phân rã của f thì mỗi F-đồng cấu $E \to \Omega$ là một đẳng cấu. Nói riêng, trường phân rã của f là duy nhất sai khác một F-đẳng cấu với nhau.

Nói rằng f chẻ ra trong Ω nghĩa là $f(X) = \prod_{i=1}^{deg(f)}(X - \alpha_i)$ với $\alpha_1, \alpha_2, \ldots \in \Omega$, và ta nói f có các nghiệm phân biệt trong Ω nếu $\alpha_i \neq \alpha_j$ nếu $i \neq j$.

Chứng minh. Ta bắt đầu với quan sát rằng: cho F, f, và Ω như là trong phát biểu của mệnh đề, L là một trường con của Ω chứa F, và g là một nhân tử của f trong $L[X]$ thì g chia hết f trong $\Omega[X]$, và do vậy (bởi tính phân tích duy nhất trong $\Omega[X]$), g là tích của một số nhân tử $X - \alpha_i$ của f trong $\Omega[X]$; nói riêng, ta thấy rằng g chẻ ra trong Ω, và các nghiệm của nó cũng sẽ phân biệt nếu các nghiệm của f phân biệt.

(a) Theo giả thiết, $E = F[\alpha_1, \ldots, \alpha_m]$ với α_i là các nghiệm của $f(X)$. Đa thức tối tiểu của α_1 là một đa thức bất khả quy f_1 chia hết f, và $\deg(f_1) = [F[\alpha_1]\colon F]$. Từ nhận xét ban đầu với $L = F$, ta thấy rằng f_1 chẻ ra trong Ω, và các nghiệm của nó khác nhau nếu các nghiệm của f khác nhau. Theo Mệnh đề 2.1, tồn tại một F-đồng cấu $\varphi_1\colon F[\alpha_1] \to \Omega$, và số các đồng cấu như vậy nhiều nhất là $[F[\alpha_1]\colon F]$, dấu bằng xảy ra khi f có các nghiệm phân biệt trong Ω.

Đa thức tối tiểu của α_2 trên $F[\alpha_1]$ là nhân tử bất khả quy f_2 của f trong $F[\alpha_1][X]$. Áp dụng nhận xét trên với $L = \varphi_1 F[\alpha_1]$ và $g = \varphi_1 f_2$, ta thấy rằng $\varphi_1 f_2$ chẻ ra trong Ω, và các nghiệm của nó là phân biệt nếu nghiệm của f là phân biệt. Theo Mệnh đề 2.2, mỗi φ_1 mở rộng thành một đồng cấu $\varphi_2\colon F[\alpha_1, \alpha_2] \to \Omega$, và số lượng các mở rộng nhiều nhất là $[F[\alpha_1, \alpha_2]\colon F[\alpha_1]]$, dấu bằng xảy ra khi f có các nghiệm phân biệt trong Ω.

Kết hợp các khẳng định trên ta kết luận rằng tồn tại một F-đồng cấu

$$\varphi\colon F[\alpha_1, \alpha_2] \to \Omega,$$

và số các đồng cấu như vậy nhiều nhất là $[F[\alpha_1, \alpha_2] : F]$, dấu bằng xảy ra khi f có các nghiệm phân biệt trong Ω.

Sau khi áp dụng lập luận m lần, ta thu được (a).

(b) Mọi F-đồng cấu $E \to \Omega$ là đơn ánh, và do vậy, nếu tồn tại các đồng cấu như vậy, thì $[E\colon F] \leq [\Omega\colon F]$. Nếu E và Ω đều là các trường phân rã của f, thì theo (a) tồn tại các đồng cấu $F \leftrightarrows E$, và do vậy $[E\colon F] = [\Omega\colon F]$. Do vậy, mọi F-đồng cấu $E \to \Omega$ là một đẳng cấu.

□

Hệ quả 2.8. *Cho E và L là các mở rộng trường của F, với E hữu hạn trên F.*

(a) Số các F-đồng cấu $E \to L$ nhiều nhất là $[E : F]$.

(b) Tồn tại một mở rộng hữu hạn Ω/L và một F-đồng cấu $E \to \Omega$.

Chứng minh. Viết $E = F[\alpha_1, \ldots, \alpha_m]$ và f là tích các đa thức tối tiểu của α_i. Cho Ω là một trường phân rã của f xem như là một phần tử của $L[X]$. Mệnh đề chứng tỏ rằng tồn tại một F-đồng cấu $E \to \Omega$, và số lượng các đồng cấu như vậy $\leq [E : F]$. Điều đó chứng tỏ (b) đúng, và từ một F-đồng cấu $E \to L$ có thể được xem như là F-đồng cấu $E \to \Omega$. Do đó, (a) được chứng minh. □

Nhận xét 2.9.

(a) Cho $E_1, E_2, \ldots, E_m$ là các mở rộng hữu hạn của F và L là một mở rộng của F. Hệ quả trên chỉ ra rằng tồn tại một mở rộng hữu hạn L_1/L chứa một ảnh đẳng cấu của E_1; sau đó tồn tại một mở rộng hữu hạn L_2/L_1 chứa một ảnh đẳng cấu của E_2. Tiếp tục như vậy, ta sẽ thu được một mở rộng hữu hạn Ω/L chứa một ảnh đẳng cấu của mọi E_i.

(b) Cho $f \in F[X]$. Nếu E và E' đều là các trường phân rã của f, thì ta biết rằng tồn tại một F-đẳng cấu $E \to E'$, nhưng nói chung không có một đẳng cấu nào được ưu tiên hơn. Sai lầm có thể phát sinh nếu chúng ta đơn thuần đồng nhất các trường đẳng cấu với nhau. Tương tự, không phát biểu "trường $F[\alpha]$ sinh bởi một nghiệm của f" sẽ không có nghĩa gì trừ khi f bất khả quy (các trường sinh bởi các nghiệm của hai ước khác nhau không có liên quan gì với nhau). Ngay cả khi f bất khả qui thì phát biểu "trường $F[\alpha, \beta]$ sinh bởi hai nghiệm α, β của f" cũng không có nghĩa vì các mở rộng của $F[\alpha]$ sinh bởi các nghiệm của hai nhân tử khác nhau của f trong $F[\alpha][X]$ có thể rất khác nhau.

2.3. Nghiệm bội

Cho $f, g \in F[X]$. Ngay cả khi f và g không có nhân tử chung trong $F[X]$, ta vẫn hi vọng rằng chúng có thể có nhân tử chung trong $\Omega[X]$ với

trường $\Omega \subset F$ nào đó. Thực tế thì điều đó không xảy ra - Ước chung lớn nhất không thay đổi khi một trường được mở rộng.

Mệnh đề 2.10. *Cho f và g là các đa thức trong $F[X]$, và cho Ω là một mở rộng trường của F. Nếu $r(X)$ là ước chung lớn nhất của f và g trong $F[X]$, thì nó cũng là ước chung lớn nhất của f và g trong $\Omega[X]$. Nói riêng, các đa thức bất khả quy đơn khởi và phân biệt trong $F[X]$ không có nghiệm chung trong bất kỳ mở rộng trường nào của F.*

Chứng minh. Ký hiệu $r_F(X)$ và $r_\Omega(X)$ lần lượt là ước chung lớn nhất của f và g trong $F[X]$ và $\Omega[X]$. Hiển nhiên $r_F(X)|r_\Omega(X)$, nhưng thuật toán Euclid (1.8) chứng tỏ rằng có các đa thức a và b trong $F[X]$ mà

$$a(X)f(X) + b(X)g(X) = r_F(X),$$

và do vậy $r_\Omega(X)$ chia hết $r_F(X)$ trong $\Omega[X]$.

Với khẳng định thứ hai, chú ý rằng giả thuyết dẫn tới $gcd(f, g) = 1$ (trong $F[X]$), và do vậy f và g không có nhân tử chung trong bất kỳ mở rộng trường nào. □

Mệnh đề trên cho phép chúng ta nói về ước chung lớn nhất của f và g mà không cần phải chỉ rõ trường đang xét.

Cho $f \in F[X]$. Khi đó f chẻ ra thành các nhân tử tuyến tính

$$f(X) = a\prod_{i=1}^{r}(X-\alpha_i)^{m_i}, \alpha_i \text{ phân biệt}, m_i \geq 1, \sum_{i=1}^{r} m_i = deg(f), \quad (*)$$

trong $\Omega[X]$ ở đó Ω là một mở rộng nào đó của F (xem 2.4). Ta nói rằng α_i là một nghiệm của f với **bội** m_i trong Ω. Nếu $m_i > 1$, α_i được gọi là **nghiệm bội** của f, nếu không nó được gọi là **nghiệm đơn**.

Dãy các số nguyên không sắp thứ tự $m_1, m_2, \ldots, m_r$ trong (*) độc lập với mở rộng trường Ω được chọn để chẻ f. Thật vậy, f không thay đổi khi Ω bị thay thế bởi trường con $F[\alpha_1, \ldots, \alpha_m]$, nhưng $F[\alpha_1, \ldots, \alpha_m]$ là trường phân rã của f, và bất kỳ hai trường phân rã nào đều F-đẳng cấu với nhau (2.7b). Ta nói rằng f **có một nghiệm bội** khi có ít nhất một $m_i > 1$, và ta nói rằng f **chỉ có các nghiệm đơn** khi tất cả $m_i = 1$.

Ta muốn xác định xem khi nào một đa thức có ít nhất một nghiệm bội. Nếu f có một nhân tử bội trong $F[X]$, tức là $f(X) = \prod f_i(X)^{m_i}$ với $m_i > 1$ nào đó, thì hiển nhiên nó sẽ có một nghiệm bội. Nếu $f = \prod f_i$

với f_i là các đa thức đơn khởi, bất khả quy, phân biệt, thì Mệnh đề 2.10 chỉ ra rằng f có một nghiệm bội nếu và chỉ nếu ít nhất một trong các f_i có nghiệm bội. Vì vậy, vấn đề được quy về việc xác định khi nào một đa thức bất khả quy có một nghiệm bội.

Ví dụ 2.11. *Cho F có đặc số $p \neq 0$, và giả sử F chứa một phần tử a không là một lũy thừa p, ví dụ $a = T$ trong trường $\mathbb{F}_p(T)$. Khi đó $X^p - a$ bất khả quy trong $F[X]$, nhưng $X^p - a = (X - \alpha)^p$ trong trường phân rã của nó. Do vậy một đa thức bất khả quy có thể có nghiệm bội.*

Định nghĩa đạo hàm (hình thức) $f'(X)$ của một đa thức $f(X) = \sum a_i X^i$ là $\sum i a_i X^{i-1}$. Nếu f có hệ số trong $\mathbb{R}$, thì đây à khái niệm đạo hàm quen thuộc trong giải tích. Các quy tắc thông thường cho đạo hàm của tổng và của tích vẫn đúng, nhưng chú ý rằng trong đặc số p, đạo hàm của X^p là 0.

Mệnh đề 2.12. *Đối với mỗi đa thức bất khả quy khác hằng số f trong $F[X]$, các khẳng định sau là tương đương:*

(a) f có nghiệm bội;

(b) $\gcd(f, f') \neq 1$*;*

(c) F có đặc số $p \neq 0$ và f là một đa thức trong X^p;

(d) tất cả các nghiệm của f có bội.

Chứng minh.

$(a) \Rightarrow (b)$ Cho α là một nghiệm bội của f, và viết $f = (X - \alpha)^m g(X), m > 1$ trong một trường phân rã nào đó. Thế thì

$$f'(X) = m(X - \alpha)^{m-1} g(X) + (X - \alpha)^m g'(X). \quad (1)$$

Do vậy $f'(\alpha) = 0$, kéo theo $gcd(f, f') =\neq 1$.

$(b) \Rightarrow (c)$ Vì f bất khả quy và $deg(f') < deg(f)$ nên,

$$gcd(f, f') \neq 1 \Rightarrow f' = 0.$$

Nhưng, vì f không là hằng số nên f' bằng 0 chỉ nếu đặc số là $p \neq 0$ và f là một đa thức trong X^p.

$(c) \Rightarrow (d)$ Giả sử $f(X) = g(X^p)$, và cho $g(X) = \prod_i (X - a_i)^{m_i}$ trong một trường phân rã nào đó của f. Ta có

$$f(X) = g(X^p) = \prod_i (X^p - a_i)^{m_i} = \prod_i (X - a_i)^{pm_i}$$

với $\alpha_i^p = a_i$. Do vậy mọi nghiệm của $f(X)$ có bội ít nhất p.

$(d) \Rightarrow (a)$ Hiển nhiên.

□

Mệnh đề 2.13. *Với mỗi đa thức f khác hằng trong $F[X]$, các khẳng định sau là tương đương:*

(a) $gcd(f, f') = 1$;

(b) f chỉ có các nghiệm đơn (trong bất kỳ trường phân rã nào của f).

Chứng minh. Cho Ω là một mở rộng trường của F mà f chẻ ra trong $\Omega[X]$. Một nghiệm α của f trong Ω là bội nếu và chỉ nếu nó cũng là nghiệm của f'.

Nếu $gcd(f, f') = 1$, thì f và f' không có nhân tử chung $X - \alpha$ trong $\Omega[x]$ (xem 2.10), và do vậy chúng không có nghiệm chung. Do đó f chỉ có các nghiệm đơn.

Nếu f chỉ có các nghiệm đơn, thì $d \stackrel{def}{=} \gcd(f, f')$ phải là một đa thức hằng, bởi nếu không nó sẽ có nghiệm trong Ω, nó sẽ là nghiệm chung của $f(X)$ và $f'(X)$. □

Định nghĩa 2.14. Một đa thức $f \in F[X]$ được gọi là **tách được** nếu nó khác 0 và thỏa mãn các điều kiện tương đương của Mệnh đề 2.13 [1].

Theo như khái niệm này, một đa thức có các nhân tử bội thì không tách được. Những thảo luận trước chỉ ra rằng $f \in F[X]$ không chứa các nhân tử bội sẽ tách được trừ khi

(a) Đặc số của F là $p \neq 0$, và

[1] Đây là khái niệm của Bourbaki. Thường thì (ví dụ trong các sách của Jacobson và các phiên bản trước đó của giáo trình này) một đa thức được gọi là tách được nếu không có nhân tử bất khả quy nào của nó có nghiệm bội.

(b) Ít nhất một trong các nhân tử bất khả quy của f là một đa thức trong X^p.

Chú ý rằng, nếu $f \in F[X]$ tách được, thì nó tách được trên mọi trường Ω chứa F (điều kiện (a) của 2.13 vẫn đúng - xem 2.10)

Định nghĩa 2.15. Một trường F được gọi là **hoàn hảo** nếu mọi đa thức bất khả quy trong $F[X]$ đều tách được.

Mệnh đề 2.16. *Mọi trường đặc số 0 là hoàn hảo. Một trường F có đặc số $p \neq 0$ là hoàn hảo nếu và chỉ nếu mọi phần tử của F là một lũy thừa p.*

Chứng minh. Một trường có đặc số 0 hiển nhiên là hoàn hảo, và do vậy ta có thể giả sử F có đặc số $p \neq 0$. Nếu F chứa một phần tử a mà nó không là một lũy thừa p, thì đa thức $X^p - a \in F[X]$ không tách được (xem 2.11). Ngược lại, nếu mọi phần tử của F là một lũy thừa p, thì mọi đa thức trong X^p với hệ số trong F là một lũy thừa p trong $F[X]$,

$$\sum a_i X^p = (\sum b_i X)^p \text{ nếu } a_i = b_i^p,$$

và do đó nó không bất khả quy. □

Ví dụ 2.17.

(a) Một trường hữu hạn F là hoàn hảo, bởi vì tự đồng cấu Frobenius $a \mapsto a^p : F \mapsto F$ là đơn ánh và do vậy toàn ánh.

(b) Một trường có thể viết như là hợp của các trường hoàn hảo là trường hoàn hảo. Do vậy, mọi trường đại số trên $\mathbb{F}_p$ là hoàn hảo.

(c) Mọi trường đóng đai số là trường hoàn hảo.

(d) Nếu F_0 có đặc số $p \neq 0$, thì $F = F_0(X)$ không hoàn hảo, bởi vì X không là một lũy thừa p.

2.4. Bài tập

2-1 Cho F là một trường đặc số $\neq 2$.

(a) Cho E là một mở rộng cấp hai của F (i.e., $[E : F] = 2$); chứng tỏ rằng

$$S(E) = \{a \in F^\times \mid a \text{ là một bình phương trong } E\}$$

là một nhóm con của $F^\times$ chứa $F^{\times 2}$.

(b) Cho E và E' là các mở rộng bậc hai của F; chứng tỏ rằng có một F-đẳng cấu $\varphi : E \to E'$ nếu và chỉ nếu $S(E) = S(E')$.

(c) Chỉ ra rằng có một dãy vô hạn các trường $E_1, E_2, \ldots$, với E_i là mở rộng cấp hai của $\mathbb{Q}$ mà E_i không đẳng cấu với E_j với $i \neq j$.

(d) Cho p là một số nguyên tố lẻ. Chỉ ra rằng, sai khác đẳng cấu, có duy nhất một trường p^2 phần tử.

2-2

(a) Cho F là một trường đặc số p. Chứng tỏ rằng $X^p - X - a$ bất khả quy trên $F[X]$, do đó nó chẻ ra thành hai nhân tử phân biệt trong $F[X]$.

(b) Với mọi số nguyên tố p, chứng tỏ rằng $X^p - X - 1$ bất khả quy trên $\mathbb{Q}[X]$.

2-3 Xây dựng một trường phân rã cho $X^5 - 2$ trên $\mathbb{Q}$. Bậc của nó trên $\mathbb{Q}$ là bao nhiêu?

2-4 Tìm một trường phân rã cho $X^{p^m} - 1 \in \mathbb{F}_p[X]$. Bậc của nó trên $\mathbb{F}_p$ là bao nhiêu ?

2-5 Cho $f \in F[X]$, với F là một trường đặc số 0. Cho $d = gcd(f, f')$. Chứng tỏ rằng $g(X) = f(X)d(X)^{-1}$ có cùng nghiệm với $f(X)$, và tất cả các nghiệm đó là các nghiệm đơn của $g(X)$.

2-6 Cho $f(X)$ là một đa thức bất khả quy trong $F[X]$, với F có đặc số p. Chứng tỏ $f(X)$ có thể viết $f(X) = g(X^p)$ với $g(X)$ bất khả quy và tách được. Suy ra rằng mọi nghiệm của $f(X)$ có cùng bội p^e trong mọi trường phân rã.

CHƯƠNG 3

Định lý cơ bản của lý thuyết Galois

Trong chương này, chúng ta chứng minh Định lý cơ bản của Lý thuyết Galois về tương ứng một-một giữa các trường con của trường phân rã của một đa thức tách được và các nhóm con của nhóm Galois của f.

3.1. Nhóm các tự đẳng cấu của trường

Xét các trường $E \supset F$. Một F-đẳng cấu $E \to E$ được gọi là một **F-tự đẳng cấu** của E. Các F-tự đẳng cấu của E lập thành một nhóm, ký hiệu là $\mathrm{Aut}(E/F)$.

Ví dụ 3.1. *(a) $\mathbb{C}$ có hai tự đẳng cấu hiển nhiên là ánh xạ đồng nhất và ánh xạ liên hợp phức. Sau này, ta sẽ thấy ở 9.18 rằng khi sử dụng Tiên đề Chọn, có thể xây dựng được một số không đếm được các tự đẳng cấu.*

(b) Cho $E = \mathbb{C}(X)$. Một tự đẳng cấu của E ánh xạ X thành một phần tử sinh khác của E trên $\mathbb{C}$. Theo 9.24 dưới đây, chúng chính là các phần tử $\frac{aX+b}{cX+d}$, $ad - bc \neq 0$. Do đó $\mathrm{Aut}(E/\mathbb{C})$ bao gồm các ánh xạ $f(X) \mapsto f\left(\frac{aX+b}{cX+d}\right)$, $ad - bc \neq 0$, và do đó

$$\mathrm{Aut}(E/\mathbb{C}) \simeq PGL_2(\mathbb{C}),$$

nhóm các ma trận khả nghịch 2×2 với hệ số phức chia thương cho tâm của nó. Những người làm giải tích sẽ thấy rằng đó chính là nhóm các tự đẳng cấu của mặt cầu Riemann. Đây không phải là một sự trùng hợp: trường các hàm phân hình trên mặt cầu Riemann $\mathbb{P}^1_{\mathbb{C}}$ là $\mathbb{C}(z) \simeq \mathbb{C}(X)$, và do vậy tồn tại một ánh xạ $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{C}}) \to \mathrm{Aut}(\mathbb{C}(z)/\mathbb{C})$ mà có thể chứng tỏ rằng đó là một đẳng cấu.

(c) Nhóm $\mathrm{Aut}(\mathbb{C}(X_1, X_2)/\mathbb{C})$ *khá phức tạp - tồn tại một ánh xạ*

$$PGL_3(\mathbb{C}) = \mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}}) \hookrightarrow \mathrm{Aut}(\mathbb{C}(X_1, X_2)/\mathbb{C}),$$

nhưng không phải là một toàn cấu. Khi có nhiều X *hơn, nhóm này vẫn chưa được xác định. Nhóm* $\mathrm{Aut}(\mathbb{C}(X_1, \ldots, X_n)/\mathbb{C})$ *là nhóm các các tự đẳng cấu song hữu tỷ của* $\mathbb{P}^n_{\mathbb{C}}$*, và được gọi là* ***nhóm Cremona****. Việc nghiên cứu nó là một phần của hình học đại số. Xem Wikipedia.*

Trong chương này, ta sẽ tìm hiểu nhóm $\mathrm{Aut}(E/F)$ khi E là một mở rộng hữu hạn của F.

Mệnh đề 3.2. *Nếu* E *là một trường phân rã của một đa thức tách được* $f \in F[X]$*, thì* $\mathrm{Aut}(E/F)$ *có bậc* $[E\colon F]$*.*

Chứng minh. Vì f tách được, nó có $\deg f$ nghiệm phân biệt trong trường phân rã E. Mệnh đề 2.7 chỉ ra rằng có tất cả $[E\colon F]$ các F-đồng cấu phân biệt $E \to E$. VÌ E có bậc hữu hạn trên F nên các đồng cấu này là các đẳng cấu. □

Ví dụ 3.3.

(a) Xét mở rộng đơn $E = F[\alpha]$ *và giả sử* f *là đa thức với hệ số trong* F*, nhận* α *là một nghiệm. Nếu* f *không có nghiệm nào khác trong* E*, thì* $\mathrm{Aut}(E/F) = 1$*. Ví dụ, nếu* $\sqrt[3]{2}$ *ký hiệu căn bậc ba thực của* 2*, thì* $\mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}) = 1$*. Do vậy, trong mệnh đề này, điều kiện* E *là một trường phân rã thực sự cần thiết.*

(b) Cho F *là một trường đặc số* $p \neq 0$*,* a *là một phần tử của* F *không là một lũy thừa* p*. Khi đó* $f = X^p - a$ *có duy nhất một nghiệm trong trường phân rã* E*, và do vậy* $\mathrm{Aut}(E/F) = 1$*. Vì vậy, trong mệnh đề trên, điều kiện* E *là một trường phân rã của một đa thức* tách được *thực sự cần thiết.*

Giả sử G là một nhóm các tự đẳng cấu của một trường E, đặt

$$E^G = Inv(G) = \{\alpha \in E \mid \sigma\alpha = \alpha, \text{với mọi } \sigma \in G\}.$$

Đó là một trường con của E, gọi là trường con các G-**bất biến** của E hay **trường bất biến** của G.

Trong chương này, ta sẽ chứng tỏ rằng nếu E là một trường phân rã của một đa thức tách được trong $F[X]$ và $G = \mathrm{Aut}(E/F)$, thì các ánh xạ

$$M \mapsto \mathrm{Aut}(E/M), \quad H \mapsto Inv(H)$$

lập thành một tương ứng một-một giữa tập hợp các trường trung gian M, $F \subset M \subset E$, và tập hợp các nhóm con H của G.

Định lý 3.4 (E. Artin)**.** *Nếu G là một nhóm hữu hạn các tự đẳng cấu của một trường E và $F = E^G$ thì $[E\colon F] \leq (G : 1)$.*

Chứng minh. Đặt $G = \{\sigma_1 = 1, \ldots, \sigma_m\}$, cần chứng minh rằng mọi hệ $\alpha_1, \ldots, \alpha_n$, gồm $n > m$ phần tử của E đều phụ thuộc tuyến tính trên F. Xét hệ phương trình tuyến tính với các hệ số trong E:

$$\begin{aligned} \sigma_1(\alpha_1)X_1 + \cdots + \sigma_1(\alpha_n)X_n &= 0 \\ \vdots &= \vdots \\ \sigma_m(\alpha_1)X_1 + \cdots + \sigma_m(\alpha_n)X_n &= 0. \end{aligned}$$

Có m phương trình và $n > m$ ẩn nên hệ có nghiệm không tầm thường trong E. Chọn một nghiệm $(c_1, \ldots, c_n)$ sao cho nó có ít phần tử khác 0 nhất. Sau khi đánh số lại các α_i, có thể giả sử rằng $c_1 \neq 0$, và (sau khi nhân bởi một vô hướng) có thể giả sử tiếp $c_1 \in F$. Với các chuẩn hóa đó, ta sẽ chứng minh rằng tất cả c_i đều thuộc F và khi đó phương trình đầu tiên

$$\alpha_1 c_1 + \cdots + \alpha_n c_n = 0,$$

(nhắc lại rằng $\sigma_1 = 1$) là một ràng buộc tuyến tính giữa các α_i.

Thật vậy, nếu không phải tất cả α_i nằm trong F, thì $\sigma_k(c_i) \neq c_i$ với k và i nào đó, $k \neq 1$ và $i \neq 1$. Áp dụng σ_k vào các phương trình

$$\begin{aligned} \sigma_1(\alpha_1)c_1 + \cdots + \sigma_1(\alpha_n)c_n &= 0 \\ \ldots &= \ldots \qquad (*) \\ \sigma_m(\alpha_1)c_1 + \cdots + \sigma_m(\alpha_n)c_n &= 0 \end{aligned}$$

và lưu ý rằng $\{\sigma_k\sigma_1, \ldots, \sigma_k\sigma_m\}$ là một hoán vị của $\{\sigma_1, \ldots, \sigma_m\}$, ta suy ra

$$(c_1, \sigma_k(c_2), \ldots, \sigma_k(c_i), \ldots)$$

cũng là một nghiệm của hệ phương trình $(*)$. Trừ đi phương trình đầu tiên, ta thu được một nghiệm mới $(0, \dots, c_i - \sigma_k(c_i), \dots)$ khác 0 (hãy nhìn vào tọa độ thứ i), nhưng lại có nhiều 0 hơn so với nghiệm chọn ban đầu (xem tọa độ đầu tiên) - đó là một mâu thuẫn. □

Hệ quả 3.5. *Với mọi nhóm hữu hạn G các tự đồng cấu của một trường F thì*

$$G = \mathrm{Aut}(E/E^G).$$

Chứng minh. Từ $G \subset \mathrm{Aut}(E/E^G)$, ta có các bất đẳng thức

$$[E : E^G] \overset{3.4}{\leq} (G : 1) \leq (\mathrm{Aut}(E : E^G) : 1) \overset{2.8a}{\leq} [E : E^G].$$

Do vậy tất cả đều là đẳng thức, và vì thế $G = \mathrm{Aut}(E/E^G)$. □

3.2. Mở rộng tách được, mở rộng chuẩn tắc và mở rộng Galois

Định nghĩa 3.6. Một mở rộng đại số E/F được gọi là **tách được** nếu đa thức tối tiểu của mọi phần tử của E đều tách được; nếu không, nó là mở rộng **không tách được**.

Như vậy, một mở rộng đại số E/F là tách được nếu mọi đa thức bất khả quy trong $F[X]$ có nghiệm trong E đều tách được, và nó không tách được nếu

- F không hoàn hảo, và nói riêng có đặc số $p \neq 0$, và
- tồn tại một phần tử α của E mà đa thức tối tiểu của nó có dạng $g(X^p), g \in F[X]$.

Ví dụ, $E = \mathbb{F}_p(T)$ là một mở rộng không tách được của $\mathbb{F}_p(T^p)$.

Định nghĩa 3.7. Một mở rộng đại số E/F được gọi là **chuẩn tắc** nếu đa thức tối tiểu của mọi phần tử của E đều chẻ ra trong $E[X]$.

Nói cách khác, một mở rộng đại số E/F là chuẩn tắc nếu mọi đa thức bất khả quy $f \in F[X]$ có ít nhất một nghiệm trong E đều chẻ ra trong $E[X]$.

Cho f là một đa thức bất khả quy bậc m trong $F[X]$. Nếu f có một nghiệm trong E, thì

- E/F tách được: suy ra các nghiệm của f phân biệt.
- E/F chuẩn hóa: suy ra f chẻ ra trong E.
- E/F tách được và chuẩn hóa: suy ra f có m nghiệm phân biệt trong E.

Do đó, E/F là chuẩn tắc và tách được nếu và chỉ nếu với mỗi $\alpha \in E$, đa thức tối tiểu của α có $[F[\alpha]\colon F]$ nghiệm phân biệt trong E.

Ví dụ 3.8.

(a) Đa thức $X^3 - 2$ có một nghiệm thực và hai nghiệm không thực . Do đó trường $\mathbb{Q}[\sqrt[3]{2}]$ tách được nhưng không chuẩn tắc trên $\mathbb{Q}$.

(b) Trường $\mathbb{F}_p(T)$ chuẩn tắc nhưng không tách được trên $\mathbb{F}_p(T^p)$ vì đa thức tối tiểu của T là đa thức không tách được $X^p - T^p$.

Định nghĩa 3.9. Cho F là một trường. Một mở rộng hữu hạn E của F được gọi là một mở rộng **Galois** nếu F là trường bất biến của nhóm các F-tự đẳng cấu của E. Khi đó, nhóm này được gọi là **nhóm Galois** của E trên F, và được ký hiệu là $\mathrm{Gal}(E/F)$.

Định lý 3.10. *Đối với một mở rộng E/F, các khẳng định sau đây là tương đương:*

(a) E là trường phân rã của một đa thức tách được $f \in F[X]$;

(b) E là Galois trên F;

(c) $F = E^G$, ở đó $G \subset \mathrm{Aut}(E)$ là một nhóm hữu hạn;

(d) E là chuẩn tắc, tách được, và có bậc hữu hạn trên F;

Chứng minh.

$(a) \implies (b)$. Đặt $G = \mathrm{Aut}(E/F)$ và $F' = E^G \supset F$. Ta phải chứng minh rằng $F' = F$. Lưu ý rằng E cũng là trường phân rã của f xem như là đa thức với hệ số trong F', và f vẫn tách được khi được xem như vậy. Theo Mệnh đề 3.2

$$|\mathrm{Aut}(E/F')| = [E\colon F'] \leq [E\colon F] = |\mathrm{Aut}(E/F)|.$$

Theo Hệ quả 3.5 thì $\mathrm{Aut}(E/F') = G = \mathrm{Aut}(E/F)$, dẫn đến $[E\colon F'] = [E\colon F]$ và $F = F'$.

$(b) \Longrightarrow (c)$. Đặt $G = \mathrm{Gal}(E/F)$. Khi đó $F = E^G$, và G hữu hạn vì E hữu hạn trên F theo 2.8a.

$(c) \Longrightarrow (d)$. Theo Mệnh đề 3.4, ta biết rằng $[E : F] \leq (G : 1)$; nói riêng, nó là một nhóm hữu hạn. Giả sử $\alpha \in E$ và f là đa thức tối tiểu của α; ta phải chứng minh rằng f chẻ ra thành các nhân tử phân biệt trong $E[X]$. Giả sử $\{\alpha_1 = \alpha, \ldots, \alpha_m\}$ là quĩ đạo của α dưới tác động của G lên E, và đặt

$$g(X) = \prod(X - \alpha_i) = X^m + a_1 X^{m-1} + \cdots + a_m.$$

Do a_i là các đa thức đối xứng của α_i, và mỗi $\sigma \in G$ chỉ đơn thuần hoán vị các α_i nên $\sigma a_i = a_i$ với mọi i, và do đó $g(X) \in F[X]$. Đó là một đa thức có hệ số đầu bằng 1 và $g(\alpha) = 0$, nên $f(X)|g(X)$ (xem định nghĩa của đa thức tối tiểu). Nếu $\alpha_i = \sigma\alpha$, thì áp dụng σ lên các phương trình $f(\alpha) = 0$ cho ta $f(\alpha_i) = 0$ nên mỗi nghiệm của g cũng là một nghiệm của f, vì thế ta cũng có $g(X)|f(X)$. Ta kết luận rằng $f(X) = g(X)$, và do vậy $f(X)$ chẻ ra thành các nhân tử phân biệt trong E.

$(d) \Longrightarrow (a)$ Vì E có bậc hữu hạn trên F, nó sinh trên F bởi một số hữu hạn các phần tử $E = F[\alpha_1, \ldots, \alpha_m]$, $\alpha_i \in E$, α_i đại số trên F. Giả sử f_i là đa thức tối tiểu của α_i trên F và f là tích của các f_i. Vì E chuẩn tắc trên F, mỗi f_i chẻ ra trong E và E là trường phân rã của f. Do E tách được trên F, mỗi f_i tách được nên f tách được.

□

Nhận xét 3.11.

*(a) Giả sử E là một mở rộng Galois trên F có nhóm Galois G và $\alpha \in E$. Các phần tử $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ trong quĩ đạo của α dưới tác động của G được gọi là các **liên hợp** của α. Trong chứng minh $(c) \Longrightarrow (d)$ của định lý trên, ta đã chỉ ra rằng đa thức tối tiểu của α là $\prod(X - \alpha_i)$.*

(b) Giả sử G là một nhóm hữu hạn các tự đẳng cấu của trường E. Khi đó E/E^G thỏa mãn các điều kiện của Định lý 3.10. Hệ quả 3.5 chỉ ra rằng $G = \mathrm{Gal}(E/E^G)$ và Mệnh đề 3.2 cho thấy $[E : E^G] = |\mathrm{Gal}(E/E^G)|$.

Hệ quả 3.12. *Mọi mở rộng hữu hạn tách được E của F đều được chứa trong một mở rộng Galois hữu hạn.*

Chứng minh. Giả sử $E = F[\alpha_1, \ldots, \alpha_m]$. Chọn f_i là đa thức tối tiểu của α_i trên F. Tích của các f_i phân biệt là một đa thức tách được trong $F[X]$ và trường phân rã của nó là một mở rộng Galois của F chứa E. □

Hệ quả 3.13. *Cho $E \supset M \supset F$; nếu E là một mở rộng Galois trên F, thì nó là một mở rộng Galois trên M.*

Chứng minh. Ta biết rằng E là trường phân rã của một đa thức tách được $f \in F[X]$; nó cũng là trường phân rã của f được xem như là một phần tử của $M[X]$. □

Nhận xét 3.14. *Khi bỏ giả thiết E tách được trên F, ta vẫn thu được một số kết quả. Một phần tử α của một mở rộng đại số của F được gọi là* ***tách được*** *trên F nếu đa thức tối tiểu của nó trên F là tách được. Chứng minh của Hệ quả 3.12 cho thấy mọi mở rộng hữu hạn sinh bởi các phần tử tách được là mở rộng tách được. Do đó, các phần tử của một mở rộng hữu hạn E của F mà tách được trên F tạo thành một trường con E_{sep} của E, và tách được trên F; đặt $[E : F]_{sep} = [E_{sep} : F]$ (**bậc tách được** của E trên F). Nếu Ω là một trường đóng đại số chứa F, thì mọi F-đồng cấu $E_{sep} \to \Omega$ thác triển được một cách duy nhất lên E, và do đó số các F-đồng cấu $E_{sep} \to \Omega$ bằng $[E : F]_{sep}$. Khi $E \supset M \supset F$ (mở rộng hữu hạn), thì*

$$[E : F]_{sep} = [E : M]_{sep}[M : F]_{sep}.$$

Nói riêng,

$$E \text{ tách được trên } F \Leftrightarrow E \text{ tách được trên } M \text{ và } M \text{ tách được trên } F.$$

Xem Jacobson 1964, I 10, để biết thêm chi tiết.

Định nghĩa 3.15. Một mở rộng hữu hạn $E \supset F$ được gọi là một mở rộng **cyclic, abel, . . . , giải được** nếu nó là một mở rộng Galois có nhóm Galois là một nhóm cyclic, abelian,..., giải được.

3.3. Định lý cơ bản của lý thuyết Galois

Định lý 3.16 (Định lý cơ bản của Lý thuyết Galois). *Cho E là một mở rộng Galois của F, và $G = \mathrm{Gal}(E/F)$. Các ánh xạ $H \mapsto E^H$ và $M \mapsto \mathrm{Gal}(E/M)$ là các song ánh nghịch đảo của nhau giữa tập hợp các nhóm con của G và tập hợp các trường trung gian nằm giữa E và F:*

$$\{\text{Các nhóm con của } G\} \longleftrightarrow \{\text{các trường trung gian } F \subset M \subset E\}.$$

Hơn nữa,

(a) tương ứng trên làm đảo ngược bao hàm thức: $H_1 \supset H_2 \Leftrightarrow E^{H_1} \subset E^{H_2}$;

(b) Các chỉ số bằng các bậc: $(H_1 : H_2) = [E^{H_1} : E^{H_2}]$;

(c) $\sigma H \sigma^{-1} \leftrightarrow \sigma M$, *tức là* $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$; $\mathrm{Gal}(E/\sigma M) = \sigma \,\mathrm{Gal}(E/M)\sigma^{-1}$.

(d) H *làm nhóm con chuẩn tắc trong* $G \Leftrightarrow E^H$ *là mở rộng chuẩn tắc (và do đó Galois) trên* F, *trong trường hợp này*

$$\mathrm{Gal}(E^H/F) \simeq G/H.$$

Chứng minh. Đối với khẳng định đầu tiên, ta phải chứng minh rằng $H \mapsto E^H$ và $M \mapsto Gal(E/M)$ là các ánh xạ ngược của nhau.

Giả sử H là một nhóm con của G. Khi đó, như ta đã thấy trong (3.5), $\mathrm{Gal}(E/E^H) = H$.

Giả sử M là một trường trung gian. Khi đó theo 3.13, E là mở rộng Galois trên M, điều đó có nghĩa là $E^{\mathrm{Gal}(E/M)} = M$.

(a) Ta có các khẳng định hiển nhiên:

$$H_1 \supset H_2 \Rightarrow E^{H_1} \subset E^{H_2} \Rightarrow \mathrm{Gal}(E/E^{H_1} \supset \mathrm{Gal}(E/E^{H_2}).$$

Nhưng $\mathrm{Gal}(E/E^{H_i}) = H_i$.

(b) Như đã thấy trong (3.11b), với mọi nhóm con H của G thì $[E : E^H] = (Gal(E/E^H) : 1)$. Điều này chứng minh (b) trong trường hợp $H_2 = 1$, và trường hợp tổng quát được suy ra từ

$$(H_1 : 1) = (H_1 : H_2)(H_2 : 1) \text{ và } [E : E^{H_1}] = [E : E^{H_2}][E^{H_2} : E^{H_1}].$$

(c) Nếu $\tau \in G$ và $\alpha \in E$ thì $\tau\alpha = \alpha \Leftrightarrow \sigma\tau\sigma^{-1}(\sigma\alpha) = \sigma\alpha$. Do vậy, $\mathrm{Gal}(E/\sigma M) = \sigma \,\mathrm{Gal}(E/M)\sigma^{-1}$ và $\sigma \,\mathrm{Gal}(E/M)\sigma^{-1} \leftarrow \sigma M$.

(d) Cho H là một nhóm con chuẩn tắc của G. Vì $\sigma H \sigma^{-1} = H$ với mọi $\sigma \in G$ nên ta phải có $\sigma E^H = E^H$ với mọi $\sigma \in G$, tức là tác động của G trên E bảo toàn E^H. Ta thu được một đồng cấu

$$\sigma \mapsto \sigma|E^H : G \to \mathrm{Aut}(E^H/F)$$

có hạt nhân là H. Do $(E^H)^{G/H} = F$ nên E^H là một mở rộng Galois trên F (Định lý 3.10) và $G/H \simeq Gal(E^H/F)$ (theo 3.11b).

Ngược lại, giả sử rằng M là một mở rộng chuẩn tắc trên F và đặt $M = F[\alpha_1, \ldots, \alpha_m]$. Với mọi $\sigma \in G$, $\sigma\alpha_i$ là một nghiệm của đa thức tối tiểu của α_i trên F, và do đó cũng nằm trong M. Do vậy $\sigma M = M$, suy ra $\sigma H \sigma^{-1} = H$ (theo (c)).

□

Nhận xét 3.17. *Định lý trên chỉ ra rằng có một song ánh đảo thứ tự giữa các trường trung gian của E/F và các nhóm con của G. Sử dụng điều này ta có thể thu được nhiều kết quả khác như dưới đây.*

(a) Giả sử $M_1, M_2, \ldots, M_r$ là các trường trung gian, và H_i là các nhóm con tương ứng với M_i (tức là $H_i = \mathrm{Gal}(E/M_i)$). Theo định nghĩa, $M_1 M_2 \ldots M_r$ là trường bé nhất chứa tất cả các M_i; do đó nó phải tương ứng với nhóm con lớn nhất chứa trong tất cả H_i, chính là nhóm $\cap H_i$. Vì thế

$$\mathrm{Gal}(E/M_1 \ldots M_r) = H_1 \cap \cdots \cap H_r.$$

*(b) Cho H là một nhóm con của G và $M = E^H$. Nhóm con chuẩn tắc lớn nhất chứa trong H là $N = \cap_{\sigma \in G} \sigma G \sigma^{-1}$ (xem [2, 4.10]), và do vậy E^N, trường hợp thành của các trường σM, là mở rộng chuẩn tắc bé nhất của F chứa M. Nó được gọi là bao đóng **chuẩn tắc**, hay bao đóng **Galois** của M trong E.*

Mệnh đề 3.18. *Cho E và L là các mở rộng trường của F cùng nằm trong một trường nào đó. Nếu E/F là một mở rộng Galois, thì EL/L và $E/E \cap L$ cũng vậy; hơn nữa ánh xạ*

$$\sigma \mapsto \sigma|E\colon\ \mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/E \cap L)$$

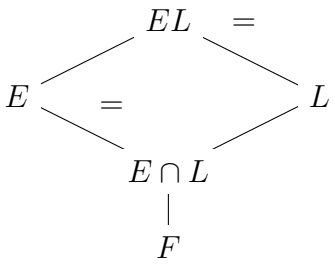
là một đẳng cấu.

Chứng minh. Vì E là một mở rộng Galois trên F nên nó là trường phân rã của một đa thức tối tiểu $f \in F[X]$. Khi đó EL là trường phân rã của f trên L, và E là trường phân rã của f trên $E \cap L$. Do đó EL/L và $E \cap L$ cũng là các mở rộng Galois. Mọi tự đẳng cấu σ của EL giữ cố định các

phần tử của L sẽ ánh xạ các nghiệm của f thành các nghiệm của f, và do đó $\sigma E = E$. Vì thế tồn tại một đồng cấu

$$\sigma \mapsto \sigma|E\colon \operatorname{Gal}(EL/L) \to \operatorname{Gal}(E/E \cap L).$$

Nếu $\sigma \in \operatorname{Gal}(EL/L)$ giữ cố định các phần tử của E, thì nó giữ cố định các phần tử của EL, và do vậy là 1. Như vậy, $\sigma \mapsto \sigma|E$ là một đơn ánh. Nếu $\alpha \in E$ bất biến bởi tất cả các phần tử $\sigma \in \operatorname{Gal}(EL/L)$, thì $\alpha \in L \cap E$. Từ Định lý cơ bản, điều này dẫn tới kết luận rằng ảnh của $\sigma \mapsto \sigma|E$ là $\operatorname{Gal}(E/E \cap L)$.



□

Hệ quả 3.19. *Giả sử trong mệnh đề 3.18, L hữu hạn trên F thì*

$$[EL\colon F] = \frac{[E\colon F][L\colon F]}{[E \cap L\colon F]}.$$

Chứng minh. Theo Mệnh đề 1.20,

$$[EF : L] = [EL : L][L : F],$$

nhưng

$$[EL : L] \overset{3.18}{=} [E : E \cap L] \overset{1.20}{=} \frac{[E : F]}{[E \cap L : F]}.$$

□

Mệnh đề 3.20. *Cho E_1 và E_2 là các mở rộng trường của F nằm trong cùng một trường nào đó. Nếu E_1 và E_2 là các mở rộng Galois trên F, thì E_1E_2 và $E_1 \cap E_2$ cũng là các mở rộng Galois trên F, và*

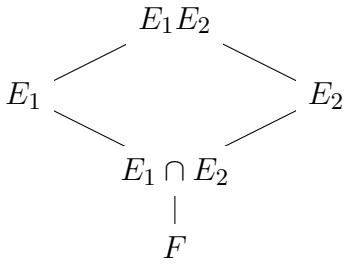
$$\sigma \mapsto (\sigma|E_1, \sigma|E_2)\colon \operatorname{Gal}(E_1E_2/F) \to \operatorname{Gal}(E_1/F) \times \operatorname{Gal}(E_2/F)$$

là một đẳng cấu từ $\mathrm{Gal}(E_1E_2/F)$ *lên các nhóm con*

$$H = \{(\sigma_1, \sigma_2) \mid \sigma_1|E_1 \cap E_2 = \sigma_2|E_1 \cap E_2\}$$

của $\mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$.

Chứng minh. Giả sử $a \in E_1 \cap E_2$ và f là đa thức tối tiểu của nó trên F. Khi đó f có $\deg f$ nghiệm phân biệt trong E_1 và $\deg f$ nghiệm phân biệt trong E_2. Vì f có nhiều nhất $\deg f$ nghiệm trong E_1E_2 nên nó có $\deg f$ nghiệm phân biệt trong $E_1 \cap E_2$. Điều này chứng tỏ rằng $E_1 \cap E_2$ là mở rộng chuẩn tắc và tách được trên F, và do đó là một mở rộng Galois (3.10). Vì E_1 và E_2 là mở rộng Galois trên F, chúng là các trường phân rã của các đa thức tách được $f_1, f_2 \in F[X]$. Bây giờ E_1E_2 là một trường phân rã của f_1f_2, và vì thế nó cũng là một mở rộng Galois trên F. Ánh xạ $\sigma \mapsto (\sigma|E_1, \sigma|E_2)$ rõ ràng là một đơn cấu, và ảnh của nó chứa trong H. Ta sẽ chứng tỏ rằng ảnh của nó là toàn bộ H bằng cách đếm số phần tử.



Từ Định lý cơ bản,

$$\mathrm{Gal}(E_2/F)/\mathrm{Gal}(E_2/E_1 \cap E_2) \simeq \mathrm{Gal}(E_1 \cap E_2/F),$$

do vậy với mỗi $\sigma_1 \in \mathrm{Gal}(E_1/F)$, $\sigma_1|E_1 \cap E_2$ có đúng $[E_2 : E_1 \cap E_2]$ mở rộng thành một phần tử của $\mathrm{Gal}(E_2|F)$. Vì thế,

$$(H : 1) = [E_1 : F][E_2 : E_1 \cap E_2] = \frac{[E_1 : F][E_2 : F]}{[E_1 \cap E_2 : F]},$$

nó bằng $[E_1E_2 : F]$ theo (3.19).

□

3.4. Một số ví dụ

Ví dụ 3.21. *Ta sẽ tìm hiểu mở rộng $\mathbb{Q}[\zeta]/\mathbb{Q}$, ở đó ζ là một căn bặc 7 nguyên thủy của 1, $\zeta = e^{2\pi i/7}$.*

Chú ý rằng $\mathbb{Q}[\zeta]$ là trường phân rã của đa thức $X^7 - 1$ và ζ có đa thức tối tiểu là

$$X^6 + X^5 + X^4 + X^3 + X^2 + X + 1.$$

(xem 1.41). Do vậy, $\mathbb{Q}[\zeta]$ là một mở rộng Galois bậc 6 trên $\mathbb{Q}$. Với mỗi $\sigma \in \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ thì $\sigma\zeta = \zeta^i$, với $1 \le i \le 6$ nào đó, và ánh xạ $\sigma \mapsto i$ xác định một đẳng cấu $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \to (\mathbb{Z}/7\mathbb{Z})^\times$. Ta lấy σ là một phần tử của $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ thỏa mãn $\sigma\zeta = \zeta^3$. σ sinh ra $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ vì lớp của 3 trong $(\mathbb{Z}/7\mathbb{Z})^\times$ sinh ra nhóm này (các lũy thừa của 3 mod 7 là $3, 2, 6, 4, 5, 1$). Ta xét các trường con của $\mathbb{Q}[\zeta]$ tương ứng với các nhóm con $\langle\sigma^3\rangle$ và $\langle\sigma^2\rangle$.

Chú ý rằng $\sigma^3\zeta = \zeta^6 = \overline{\zeta}$ (liên hợp phức của ζ), và vì thế $\zeta + \overline{\zeta} = 2\cos(2\pi/7)$ được giữ cố định bởi σ^3. Bây giờ ta có $\mathbb{Q}[\zeta] \supset \mathbb{Q}[\zeta]^{\langle\sigma^3\rangle} \supset \mathbb{Q}[\zeta + \overline{\zeta}] \neq \mathbb{Q}$. Do đó $\mathbb{Q}[\zeta]^{\langle\sigma^3\rangle} \supset \mathbb{Q}[\zeta + \overline{\zeta}]$ (nhìn vào bậc!). Vì $\langle\sigma^3\rangle$ là một nhóm con chuẩn tắc của $\langle\sigma\rangle$ nên $\mathbb{Q}[\zeta + \overline{\zeta}]$ là mở rộng Galois trên $\mathbb{Q}$, có nhóm Galois $\langle\sigma\rangle/\langle\sigma^3\rangle$. Các liên hợp của $\alpha_1 \overset{def}{=} \zeta + \overline{\zeta}$ là $\alpha_3 = \zeta^3 + \zeta^{-3}$, $\alpha_2 = \zeta^2 + \zeta^{-2}$. Tính trực tiếp, ta có

$$\begin{aligned}
\alpha_1 + \alpha_2 + \alpha_3 &= \sum_{i=1}^{6} \zeta^i = -1 \\
\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 &= -2 \\
\alpha_1\alpha_2\alpha_3 &= (\zeta + \zeta^6)(\zeta^2 + \zeta^5)(\zeta^3 + \zeta^4) \\
&= (\zeta + \zeta^3 + \zeta^4 + \zeta^6)(\zeta^3 + \zeta^4) \\
&= (\zeta^4 + \zeta^6 + 1 + \zeta^2 + \zeta^5 + 1 + \zeta + \zeta^3) \\
&= 1.
\end{aligned}$$

Vì thế đa thức tối tiểu [1] của $\zeta + \overline{\zeta}$ là

$$g(X) = X^3 + X^2 - 2X - 1.$$

[1] Có thể lập luận trực tiếp hơn: đặt $X = \zeta + \overline{\zeta}$ trong

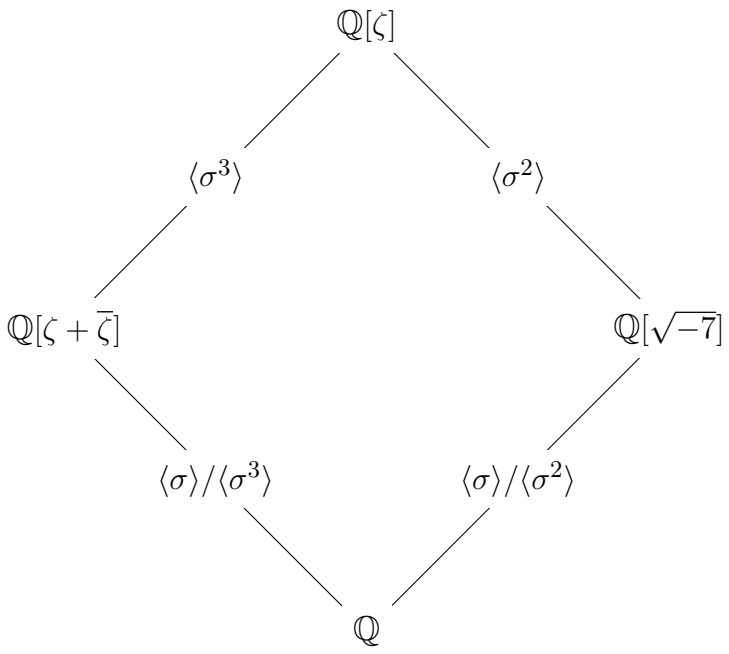
$$(X^3 - 3X) + (X^2 - 2) + X + 1$$

ta thu được $1 + \zeta + \zeta^2 + \cdots + \zeta^6 = 0$.

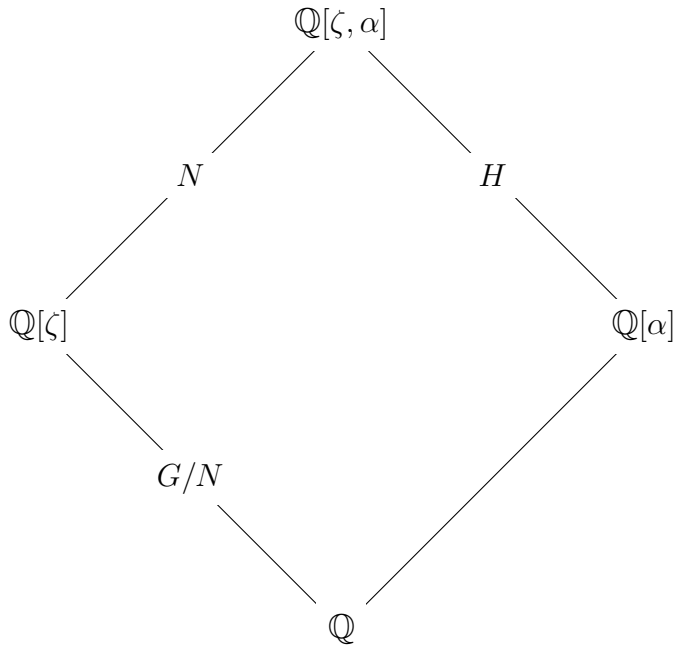
Đa thức tối tiểu của $\cos\frac{2\pi}{7} = \frac{\alpha_1}{2}$ *bằng*

$$\frac{g(2X)}{8} = X^3 + X^2/2 - X/2 - 1/8.$$

Trường con của $\mathbb{Q}[\zeta]$ *tương ứng với* $\langle\sigma^2\rangle$ *được sinh bởi* $\beta = \zeta + \zeta^2 + \zeta^4$. *Đặt* $\beta' = \alpha\beta$. *Khi đó* $(\beta - \beta')^2 = -7$. *Do vậy trường bất biến bởi* $\langle\sigma^2\rangle$ *là* $\mathbb{Q}[\sqrt{-7}]$.



Ví dụ 3.22. *Ta tính nhóm Galois của trường phân rã* E *của* $X^5 - 2 \in \mathbb{Q}[X]$. *Nhắc lại từ bài tập 2-3 rằng* $E = \mathbb{Q}[\zeta, \alpha]$ *với* ζ *là căn bậc* 5 *nguyên thủy của* 1, *và* α *là một nghiệm của* $X^5 - 2$. *Ví dụ, có thể chọn* E *là trường phân rã của* $X^5 - 2$ *trong* $\mathbb{C}$, *với* $\zeta = e^{2\pi i/5}$ *và* α *là căn bặc* 5 *thực của* 2. *Ta có sơ đồ dưới đây*



và

$$[\mathbb{Q}[\zeta]:\mathbb{Q}]=4,\quad [\mathbb{Q}[\alpha]:\mathbb{Q}]=5.$$

Vì 4 *và* 5 *nguyên tố cùng nhau nên*

$$[\mathbb{Q}[\zeta,\alpha]:\mathbb{Q}]=20.$$

Do đó $G=\mathrm{Gal}(\mathbb{Q}[\zeta,\alpha]/\mathbb{Q})$ *có bậc* 20*, và các nhóm con* N *và* H *giữ cố định* $\mathbb{Q}[\zeta]$ *và* $\mathbb{Q}[\alpha]$ *có bậc tương ứng bằng* 5 *và* 4*. Vì* $\mathbb{Q}[\zeta]$ *là mở rộng chuẩn tắc trên* $\mathbb{Q}$ *(nó là trường phân rã của* X^5-1*) nên* N *là nhóm con chuẩn tắc trong* G*. Vì* $\mathbb{Q}[\zeta].\mathbb{Q}[\alpha]=\mathbb{Q}[\zeta,\alpha]$*, ta có* $H\cap N=1$*, và do vậy* $G=N\rtimes_\theta H$*. Hơn nữa,* $H\simeq G/N\simeq(\mathbb{Z}/5\mathbb{Z})^\times$*, là một nhóm cyclic, sinh bởi lớp* 2*. Ký hiệu* τ *là phần tử sinh của* H *tương ứng với* 2 *qua đẳng cấu này, và chọn* σ *là một phần tử sinh của* N*. Khi đó* $\sigma(\alpha)$ *là một nghiệm khác của* X^5-2*, ta có thể chọn là* $\zeta\alpha$ *(sau khi thay* σ *bởi một lũy thừa của nó). Vì vậy*

$$\begin{cases}\tau\zeta=\zeta^2\\ \tau\alpha=\alpha\end{cases}\qquad\begin{cases}\sigma\zeta=\zeta\\ \sigma\alpha=\zeta\alpha.\end{cases}$$

Chú ý rằng $\tau\sigma\tau^{-1}(\alpha)=\tau\sigma\alpha=\tau(\zeta\alpha)=\zeta^2\alpha$ *và nó cố định* ζ*; vì thế* $\tau\sigma\tau^{-1}=\sigma^2$*. Nên* G *có các phần tử sinh* σ *và* τ *và có các quan hệ*

$$\sigma^5=1,\quad \tau^4=1,\quad \tau\sigma\tau^{-1}=\sigma^2.$$

Nhóm con H có năm liên hợp, chúng tương ứng với năm trường $\mathbb{Q}[\zeta^i\alpha]$,

$$\sigma^i H\sigma^{-1} \leftrightarrow \sigma^i\mathbb{Q}[\alpha] = \mathbb{Q}[\zeta^i\alpha], \quad 1 \le i \le 5.$$

3.5. Trở về với các số xây dựng được

Trước đây, ta đã chứng minh (1.36) rằng một số thực α là xây dựng được nếu và chỉ nếu nó chứa trong một trường con của $\mathbb{R}$ có dạng $\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_r}]$ ở đó mỗi a_i là một số dương thuộc $\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}]$. Nói riêng

$$\alpha \text{ xây dựng được} \Rightarrow [\mathbb{Q}[\alpha] : \mathbb{Q}] = 2^s \text{ với } s \text{ nào đó} \quad (2).$$

Bây giờ ta có thể chứng minh một phần của chiều ngược lại như sau.

Định lý 3.23. *Nếu α nằm trong một trường con của $\mathbb{R}$ và là một mở rộng Galois bậc 2^r trên $\mathbb{Q}$, thì nó xây dựng được.*

Chứng minh. Giả sử $\alpha \in E \subset \mathbb{R}$ ở đó E là mở rộng Galois bậc 2^r trên $\mathbb{Q}$, và đặt $G = \mathrm{Gal}(E/\mathbb{Q})$. Vì các p-nhóm hữu hạn giải được ([2, 6.7]) nên tồn tại một dãy các nhóm

$$\{1\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_r = G$$

sao cho G_i/G_{i-1} cócấp 2. Tương ứng với dãy đó là một dãy các trường,

$$E = E_0 \supset E_1 \supset E_2 \supset \cdots \supset E_r = \mathbb{Q}$$

với E_{i-1} có bậc 2 trên E_i. Bổ đề sau đây chứng minh rằng $E_i = E_{i-1}[\sqrt{a_i}]$ với a_i nào đó thuộc E_{i-1}, và $a_i > 0$ bởi vì nếu không thì E_i không thực. Định lý đã được chứng minh. □

Bổ đề 3.24. *Cho E/F là một mở rộng bậc hai của các trường đặc số khác 2. Khi đó $E = F[\sqrt{d}]$ với $d \in F$ nào đó.*

Chứng minh. Cho $\alpha \in E, \alpha \notin F$, và cho $X^2 + bX + c$ là đa thức tối tiểu của α. Thế thì $\alpha = \frac{-b \pm \sqrt{b^2-4ac}}{2}$, và do vậy $E = F[\sqrt{b^2 - 4c}]$. □

Hệ quả 3.25. *Nếu p là một số nguyên tố có dạng $2^k + 1$, thì $\cos\frac{2\pi}{p}$ xây dựng được.*

Chứng minh. Trường $\mathbb{Q}[e^{2\pi i/p}]$ là một mở rộng Galois trên $\mathbb{Q}$ với nhóm Galois $G \simeq (\mathbb{Z}/p\mathbb{Z})^\times$, có bậc $p-1 = 2^k$. Trường $\mathbb{Q}[\cos\frac{2\pi}{p}]$ được chứa trong $\mathbb{Q}[e^{2\pi i/p}]$, và do vậy là mở rộng Galois với bậc chia hết 2^k (định lý cơ bản 3.16 và 1.20). Do $\mathbb{Q}[\cos\frac{2\pi}{p}]$ là một trường con của $\mathbb{R}$, ta có thể áp dụng định lý trên. □

Như vậy một p-đa giác đều, p nguyên tố là xây dựng được nếu và chỉ nếu p là một số nguyên tố Fermat, tức là có dạng $2^{2^r}+1$. Ví dụ, ta đã chứng minh rằng đa giác đều 65537 cạnh xây dựng được mặc dù không có công thức tường minh cho $\cos\frac{2\pi}{65537}$.

Nhận xét 3.26. *Chiều ngược lại của* (2) *không đúng. Đa thức* $f(X) = X^4 - 4X + 2 \in \mathbb{Q}[X]$ *bất khả quy, và ta sẽ chứng tỏ trong (4.9)rằng nhóm Galois của trường phân rã* E *trên* $\mathbb{Q}$ *của đa thức là* S_4*. Mỗi nghiệm của* $f(X)$ *nằm trong một mở rộng bậc* 2^2 *của* $\mathbb{Q}$*. Nếu bốn nghiệm của* $f(X)$ *xây dựng được, thì tất cả các phần tử của* E *sẽ xây dựng được (1.36a). Cho* H *là một nhóm con Sylow của nhóm* S_4*.* E^H *có bậc lẻ trên* $\mathbb{Q}$*, và do vậy các phần tử của* $E^H \setminus \mathbb{Q}$ *không thể xây dựng được* [2]*.*

3.6. Nhóm Galois của một đa thức

Nếu đa thức $f \in F[X]$ tách được, thì trường phân rã F_f của nó là một mở rộng Galois trên F, và ta gọi $\mathrm{Gal}(F_f/F)$ là **nhóm Galois** G_f của f.

Giả sử $f = \prod_{i=1}^{n}(X-\alpha_i)$ trong trường phân rã F_f. Ta biết rằng các phần tử của $\mathrm{Gal}(F_f/F)$ ánh xạ các nghiệm của f thành các nghiệm của f, tức là chúng ánh xạ tập hợp $\{\alpha_1,\ldots,\alpha_n\}$ lên chính nó. Là các tự đẳng cấu, chúng phải là các hoán vị của $\{\alpha_1,\ldots,\alpha_n\}$, và vì các α_i sinh ra F_f nên một phần tử của $\mathrm{Gal}(F_f/F)$ được xác định duy nhất bởi các hoán vị chúng xác định. Vì vậy G_f có thể được đồng nhất với một nhóm con của $Sym(\{\alpha_1,\ldots,\alpha_n\}) \approx S_n$ (nhóm đối xứng trên n phần tử.) Thực ra, G_f chính là tập hợp các hoán vị σ của $\{\alpha_1,\ldots,\alpha_n\}$ sao cho nếu

[2] Như Shuichi Otsuka đã chỉ ra cho tôi, có thể chứng minh điều này mà không cần tới định lý Sylow. Nếu một nghiệm α của $f(X)$ xây dựng được thì sẽ có một tháp các mở rộng bậc hai $\mathbb{Q}[\alpha] \supset M \supset \mathbb{Q}$. Theo lý thuyết Galois, các nhóm $\mathrm{Gal}(E/M) \supset \mathrm{Gal}(E/\mathbb{Q}[\alpha])$ có bậc tương ứng là 12 và 6. Từ $\mathrm{Gal}(E/\mathbb{Q}) = S_4$, $\mathrm{Gal}(E/M)$ phải là nhóm A_4. Nhưng A_4 không có nhóm con cấp 6, nghịch lý. Do vậy không có nghiệm nào của $f(X)$ xây dựng được. (Thực ra $\mathrm{Gal}(E/\mathbb{Q}[\alpha]) = S_3$ nhưng ta không cần đến kết quả đó ở đây.)

$P \in F[X_1, \ldots, X_n]$,

$$P(\alpha_1, \ldots, \alpha_n) = 0 \Rightarrow P(\sigma\alpha_1, \ldots, \sigma\alpha_n) = 0. \tag{3.1}$$

Điều này cho ta một mô tả của G_f không liên quan tới các trường hay các nhóm trừu tượng (không định nghĩa nào đã xuất hiện trong thời Galois)[3]

Chú ý rằng điều này lại một lần chứng tỏ rằng $(G_f : 1)$, và do vậy $[F_f : F]$, chia hết $deg(f)$!.

3.7. Tính giải được của đa thức

Với một đa thức $f \in F[X]$, ta nói rằng phương trình $f(X) = 0$ **giải được bằng căn thức** nếu các nghiệm của nó có thể thu được bằng các phép toán đại số: phép cộng, trừ, nhân, chia và phép khai căn bậc m, hay, chính xác hơn, nếu có một tháp các trường

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m$$

mà

(a) $F_i = F_{i-1}[\alpha_i], \alpha_i^m \in F_{i-1}$;

(b) F_m chứa một trường phân rã của f.

Định lý 3.27 (Galois, 1832)**.** *Cho F là một trường đặc số 0. Phương trình $f = 0$ giải được bằng căn thức nếu và chỉ nếu nhóm Galois của f giải được.*

Ta sẽ chứng minh định lý này sau (5.34). Đồng thời ta cũng sẽ chỉ ra các đa thức $f(X) \in \mathbb{Q}[X]$ có nhóm Galois là S_n, các đa thức này do đó không giải được khi $n \geq 5$ theo [2, 4.37].

Nhận xét 3.28. *Nếu F có đặc số p, thì Định lý không đúng bởi hai lý do:*

[3] Hạt nhân của ánh xạ

$$F[X_1, \ldots, X_n] \to F_f, \quad X_i \mapsto \alpha_i,$$

gồm các đa thức $P(X_1, \ldots, X_n)$ mà $P(\alpha_1, \ldots, \alpha_n) = 0$. Nếu σ là một hoán vị của các α_i thỏa mãn (3.1) thì ánh xạ

$$F[X_1, \ldots, X_n] \to F_f, \quad X_i \mapsto \sigma\alpha_i,$$

được phân tích qua ánh xạ ban đầu, và xác định một F-đẳng cấu $F_f \to F_f$, tức là một phần tử của nhóm Galois. Điều này chỉ ra rằng mọi phép thế thỏa mãn điều kiện (3.1) mở rộng một cách duy nhất thành một phần tử của $G_f$và rõ ràng là mọi phần tử của G_f đều xuất hiện theo cách này.

(a) f có thể không tách được, và do vậy không có nhóm Galois;

(b) $X^p - X - a = 0$ không giải được bằng căn thức mặc dù nó tách được và có nhóm Galois giao hoán (Bài tập 2-2)

Nếu định nghĩa của tính giải được sửa đổi để cho phép có các mở rộng dạng (b) trong chuỗi, và f được yêu cầu phải tách được, thì Định lý đúng trong trường đặc số p.

Chú thích: Phần lớn những gì đã được viết về Galois đều không đáng tin cậy - xem Tony Rothman, "Genius and Biographers: The Fictionalization of Evariste Galois," Amer. Math. Mon. 89, 84 (1982). Phiên bản có chỉnh sửa sẵn trực tuyến tại địa điểm khác nhau [4].

Một nghiên cứu nghiêm cẩn về công trình của Galois "Premier Mémoire" là Edwards, Harold M., Galois for 21st-century readers. Notices AMS 59 (2012), no. 7, 912–923.

3.8. Bài tập

3-1 Cho F là một trường đặc số 0. Chứng minh rằng $F(X^2) \cap F(X^2 - X) = F$ (giao trong trong $F(X)$). [Gợi ý: Tìm các tự đồng cấu σ và τ của $F(X)$, cả hai đều cấp 2, lần lượt giữ cố định $F(X^2)$ và $F(X^2 - X)$, và chứng minh rằng $\sigma\tau$ có bậc hữu hạn.]

3-2 [5] Cho p là một số nguyên tố lẻ, ζ là một căn bậc p nguyên thủy của 1 trong $\mathbb{C}$. Đặt $E = \mathbb{Q}[\zeta]$ và $G = \mathrm{Gal}(E/\mathbb{Q})$; do đó $G = (\mathbb{Z}/(p))^\times$. Cho H là nhóm con chỉ số 2 trong G. Đặt $\alpha = \sum_{i \in H} \zeta^i$ và $\beta = \sum_{i \in G \setminus H} \zeta^i$. Chứng tỏ rằng:

(a) α và β được giữ cố định bởi H;

(b) nếu $\sigma \in G \setminus H$, thì $\sigma\alpha = \beta, \sigma\beta = \alpha$.

Như vậy α và β là các nghiệm của đa thức $X^2 + X + \alpha\beta \in \mathbb{Q}[X]$. Hãy tính $\alpha\beta$ và chứng tỏ rằng trường cố định của H là $\mathbb{Q}[\sqrt{p}]$ khi $p = 1 \pmod 4$ và $\mathbb{Q}[\sqrt{-p}]$ khi $p = 3 \pmod 4$.

[4] http://docs.wixstatic.com/ugd/0427b2_488a653874d44ef8a3dc96e98122907f.pdf

[5] Bài tập này chỉ ra rằng mọi mở rộng bậc hai của $\mathbb{Q}$ đều chứa trong một mở rộng chia đường tròn của $\mathbb{Q}$. Định lý Kronecker-Weber nói rằng mọi mở rộng abel của $\mathbb{Q}$ đều chứa trong một mở rộng chia đường tròn.

3-3 Đặt $M = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ và $E = M[\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}]$ (các trường con của $\mathbb{R}$).

(a) Chứng tỏ rằng M là một mở rộng Galois trên $\mathbb{Q}$ với nhóm Galois là 4-nhóm $C_2 \times C_2$.

(b) Chứng tỏ rằng E là một mở rộng Galois trên $\mathbb{Q}$ với nhóm Galois là nhóm Quaternion.

3-4 Cho E là một mở rộng Galois của F với nhóm Galois G và L là trường bất biến của một nhóm con H của G. Chứng minh rằng nhóm tự đồng cấu của L/F là N/H ở đó N là nhóm chuẩn tắc hóa của H trong G.

3-5 Cho E là một mở rộng hữu hạn của F. Chứng minh rằng cấp của $\mathrm{Aut}(E/F)$ chia hết bậc $[E\colon F]$.

CHƯƠNG 4

Tính nhóm Galois

Trong chương này, ta nghiên cứu các phương pháp chung để tính các nhóm Galois.

4.1. Khi nào $G_f \subset A_n$?

Cho σ là một hoán vị của tập hợp $\{1, 2, \ldots, n\}$. Các cặp (i, j) với $i < j$ nhưng $\sigma(i) > \sigma(j)$ được gọi là các **nghịch thế** của σ, và σ được gọi là **chẵn** hay **lẻ** tùy thuộc vào số các nghịch thế là chẵn hay lẻ. **Dấu** của σ, $\text{sign}(\sigma)$, là $+1$ hay -1 nếu σ chẵn hay lẻ. Ta có thể định nghĩa dấu của một hoán vị σ của một tập hợp S bất kỳ gồm n phần tử bằng cách đánh số tập hợp đó và đồng nhất σ với một hoán vị của $\{1, \ldots, n\}$. Khi đó sign là đồng cấu duy nhất $\text{Sym}(S) \to \{\pm 1\}$ mà $\text{sign}(\sigma) = -1$ đối với mỗi phép thế sơ cấp. Nói riêng, nó độc lập với cách đánh số. Xem GT, 4.25.

Bây giờ xét một đa thức đơn khởi

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n$$

và giả sử $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$ trong một trường phân rã nào đó. Đặt

$$\Delta(f) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j), \quad D(f) = \Delta(f)^2 = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

Định nghĩa **Biệt thức** của f là $D(f)$. Chú ý rằng $D(f)$ khác 0 nếu và chỉ nếu f chỉ có các nghiệm đơn, tức là khi f tách được và không có ước bội. Ký hiệu G_f là nhóm Galois của f, và đồng nhất nó với một nhóm con của $\text{Sym}\{\alpha_1, \ldots, \alpha_n\}$.

Mệnh đề 4.1. *Cho $f \in F[X]$ là đa thức tách được, và $\sigma \in G_f$. Khi đó*

(a) $\sigma\Delta(f) = \text{sign}(\sigma)\Delta(f)$,

(b) $\sigma D(f) = D(f)$.

Chứng minh. Mỗi nghịch thế của σ dẫn tới một dấu âm cho $\sigma\Delta(f)$, và do vậy (a) suy ra từ định nghĩa của $\text{sign}(\sigma)$. Phương trình trong (b) đạt được bằng cách bình phương (a). □

Trong khi $\Delta(f)$ phụ thuộc vào cách đánh số các nghiệm của f thì $D(f)$ không phụ thuộc.

Hệ quả 4.2. *Cho $f(X) \in F[X]$ bậc n và chỉ có các nghiệm đơn, F_f là trường phân rã của f. Khi đó $G_f = \text{Gal}(F_f/F)$. Ta có các khẳng định sau:*

(a) Biệt thức $D(f) \in F$.

(b) Trường con của F_f tương ứng với $A_n \cap G_f$ là $F[\Delta(f)]$. Do vậy

$$G_f \subset A_n \iff \Delta(f) \in F \iff D(f) \text{ là một bình phương trong } F.$$

Chứng minh.

(a) Biệt thức của f là một phần tử của F_f cố định bởi $G_f \stackrel{def}{=} \text{Gal}(F_f/F)$, và do vậy nằm trong F (theo Định lý cơ bản của Lý thuyết Galois).

(b) Bởi vì f có các nghiệm đơn, $\Delta(f) \neq 0$, và do vậy công thức $\sigma\Delta(f) = \text{sign}(\sigma)\Delta(f)$ chứng tỏ rằng một phần tử của G_f cố định $\Delta(f)$ nếu và chỉ nếu nó nằm trong A_n. Vậy nên, dưới tương ứng Galois,

$$G_f \cap A_n \leftrightarrow F[\Delta(f)].$$

Vì thế $G_f \cap A_n = G_f \iff F[\Delta(f)] = F$.

□

Các nghiệm của $X^2 + bX + c$ là $\frac{-b \pm \sqrt{b^2-4c}}{2}$ và do vậy

$$\Delta(X^2 + bX + c) = \sqrt{b^2 - 4c} \quad (\text{hay } -\sqrt{b^2 - 4c}),$$
$$D(X^2 + bX + c) = b^2 - 4c.$$

Mặc dù không có công thức cụ thể cho các nghiệm của f trên các hệ số khi bậc của f lớn hơn 4, ta vẫn có công thức cho biệt thức. Ví dụ,

$$D(X^3 + bX + c) = -4b^3 - 27c^2.$$

Với n càng lớn công thức cho biệt thức càng trở lên phức tạp, ví dụ, với $X^5 + aX^4 + bX^3 + cX^2 + dX + e$ có 59 số hạng. May mắn là, PARI biết chúng. Ví dụ, gõ `poldisc(X^3+a*X^2+b*X+c,X)` trả về biệt thức của $X^3 + aX^2 + bX + c$, như sau

$$-4ca^3 + b^2a^2 + 18cba + (-4b^3 - 27c^2).$$

Nhận xét 4.3. *Giả sử $F \subset \mathbb{R}$. Khi đó $D(f)$ sẽ không là một bình phương nếu nó nhận giá trị âm. Ta biết rằng dấu của $D(f)$ là $(-1)^s$, ở đó $2s$ là số các nghiệm không thực của f trong $\mathbb{C}$ (xem ANT 2.40). Do đó nếu s lẻ thì G_f không nằm trong A_n. Khẳng định này có thể được chứng minh trực tiếp nhờ nhận xét rằng liên hợp phức tác động lên các nghiệm như là một tích của s phép thế sơ cấp rời nhau. Tất nhiên là điều ngược lại không đúng: khi s chẵn, G_f không nhất thiết nằm trong A_n.*

4.2. Khi nào G_f có tính chất truyền dẫn?

Mệnh đề 4.4. *Cho $f(X) \in F[X]$ chỉ có các nghiệm đơn. Khi đó $f(X)$ bất khả quy nếu và chỉ nếu G_f tác động truyền dẫn trên các nghiệm của f.*

Chứng minh.

$\Rightarrow$: Nếu α và β là hai nghiệm của $f(X)$ trong một trường phân rã F_f của f, thì chúng đều nhận $f(X)$ là đa thức tối tiểu, và do vậy $F[\alpha]$ và $F[\beta]$ đều là các trường mầm của f. Vì vậy, có một F-đẳng cấu

$$F[\alpha] \simeq F[\beta], \quad \alpha \leftrightarrow \beta.$$

Viết $F_f = F[\alpha_1, \alpha_2, \dots]$ với $\alpha_1 = \alpha$ và $\alpha_2, \alpha_3, \dots$ là các nghiệm khác của $f(X)$. Khi đó F-đồng cấu $\alpha \mapsto \beta : F[\alpha] \to F_f$ mở rộng (từng bước một) thành một F-đồng cấu $F_f \to F_f$ (dùng 2.2b), đó là một F-đồng cấu biến α thành β.

$\Leftarrow$: Giả sử $g(X) \in F[X]$ là một nhân tử bất khả quy của f, và α là một trong các nghiệm của nó. Nếu β là một nghiệm thứ hai của f, thì

(theo giả thiết) $\beta = \sigma\alpha$ với $\sigma \in G_f$ nào đó.Vì g có hệ số trong F nên,

$$g(\sigma\alpha) = \sigma g(\alpha) = 0,$$

suy ra β cũng là một nghiệm của g. Do vậy, mọi nghiệm của f cũng là một nghiệm của g và do đó $f(X) = g(X)$.

Chú ý rằng khi $f(X)$ bất khả quy bậc n thì $n|(G_f\colon 1)$ vì $[F[\alpha]\colon F] = n$ và $[F[\alpha]\colon F]$ chia hết $[F_f\colon F] = (G_f\colon 1)$. Do đó G_f là một nhóm con truyền dẫn của S_n có bậc chia hết cho n. □

4.3. Đa thức bậc không quá ba

Ví dụ 4.5. *Cho $f(X) \in F[X]$ là một đa thức bậc 2. Khi đó f không tách được nếu và chỉ nếu F có đặc số 2 và $f(X) = X^2 - a$ với $a \in F \setminus F^2$. Nếu f tách được thì $G_f = 1(= A_2)$ hay S_2 tùy thuộc vào $D(f)$ là một bình phương trong F hay không.*

Ví dụ 4.6. *Cho $f(X) \in F[X]$ là một đa thức bậc 3. Có thể giả sử f bất khả quy vì nếu không thì ta quay trở lại trường hợp trước. Khi đó f không tách được nếu và chỉ nếu F có đặc số 3 và $f(X) = X^3 - a$ với $a \in F \setminus F^3$ nào đó. Nếu f tách được, thì G_f là một nhóm con truyền dẫn của S_3 có bậc chia hết cho 3. Chỉ có thể có hai khả năng: $G_f = A_3$ hoặc S_3 tùy thuộc vào $D(f)$ là một bình phương trong F hay không. Chú ý rằng A_3 sinh bởi xích* (123).

Ví dụ $X^3 - 3X + 1 \in \mathbb{Q}[X]$ bất khả quy (xem 1.22), biệt thức của nó là $-4(-3)^3 - 27 = 81 = 9^2$, và do vậy nhóm Galois của nó là A_3.

Mặt khác, $X^3 + 3X + 1 \in \mathbb{Q}[X]$ cũng bất khả quy (dùng 1.11), nhưng biệt thức của nó là -135 không phải là một bình phương trong $\mathbb{Q}$, và do đó nhóm Galois của nó là S_3.

4.4. Phương trình bậc bốn

Cho $f(X)$ là một đa thức bậc bốn không có nghiệm bội. Để tính G_f ta sử dụng tính chất: S_4 có nhóm con chuẩn tắc

$$V = \{1, (12)(34), (13)(24), (14)(23)\}$$

, nó chuẩn tắc vì V chứa tất cả các phần tử có kiểu xích dạng $2 + 2$ (GT 4.29). Giả sử E là một trường phân rã của f, và ta có phân tích

$f(X) = \prod(X - \alpha_i)$ trong E. Đồng nhất nhóm Galois G_f của f với một nhóm con của nhóm đối xứng $\mathrm{Sym}(\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\})$. Xét các phần tử

$$\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4$$
$$\beta = \alpha_1\alpha_3 + \alpha_2\alpha_4$$
$$\gamma = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

chúng đôi một khác nhau vì các α_i phân biệt; ví dụ,

$$\alpha - \beta = \alpha_1(\alpha_2 - \alpha_3) + \alpha_4(\alpha_3 - \alpha_2) = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3).$$

Nhóm $\mathrm{Sym}(\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\})$ tác động truyền dẫn trên $\{\alpha, \beta, \gamma\}$. Nhóm ổn định của mỗi phần tử trong α, β, γ phải là một nhóm con có chỉ số 3 của nhóm S_4, và do vậy có bậc 8. Ví dụ, nhóm ổn định của β là $\langle(1234), (13)\rangle$. Các nhóm cấp 8 trong S_4 là các 2-nhóm con Sylow. Cả ba đều đẳng cấu với D_4. Theo định lý Sylow, V nằm trong một 2-nhóm con Sylow nào đó nhưng vì các 2-nhóm con Sylow liên hợp với nhau và V chuẩn tắc nên nó nằm trong cả ba nhóm con Sylow. Ta suy ra rằng V là giao của ba 2-nhóm con Sylow. Mỗi 2-nhóm con Sylow cố định duy nhất một trong α, β, γ, và do vậy giao của chúng, V, là nhóm con của $\mathrm{Sym}(\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\})$ giữ cố định α, β, γ.

Bổ đề 4.7. *Trường bất biến của $G_f \cap V$ là $F[\alpha, \beta, \gamma]$. Vì thế $F[\alpha, \beta, \gamma]$ là một mở rộng Galois trên F với nhóm Galois $G_f/G_f \cap V$.*

Chứng minh. Phân tích ở trên chỉ ra rằng nhóm con của G_f gồm các phần tử cố định $F[\alpha, \beta, \gamma]$ là $G_f \cap V$, do đó $E^{G_f \cap V} = F[\alpha, \beta, \gamma]$ theo định lý cơ bản của Lý thuyết Galois. Các phát biểu còn lại được suy ra từ định lý cơ bản bằng việc sử dụng tính chất V là chuẩn tắc.

$$\begin{array}{c} E \\ \Big| \; G_f \cap V \\ F[\alpha, \beta, \gamma] \\ \Big| \; G_f/G_f \cap V \\ F \end{array}$$

□

Đặt $M = F[\alpha, \beta, \gamma]$, và $g(X) = (X-\alpha)(X-\beta)(X-\gamma) \in M[X]$- nó được gọi là **giải thức bậc ba**[1] của f. Mọi hoán vị của các α_i (tức là mọi phần tử của G_f) chỉ đơn thuần hoán vị α, β, γ, và do vậy giữ cố định $g(X)$. Như vậy (theo định lý cơ bản) thì $g(X)$ có các hệ số trong F. Cụ thể, ta có bổ đề sau:

Bổ đề 4.8. *Giải thức bậc ba của* $f = X^4 + bX^3 + cX^2 + dX + e$ *là*

$$g = X^3 - cX^2 + (bd - 4e)X = b^2e + 4ce - d^2.$$

Biệt thức của f *và* g *bằng nhau.*

Phác thảo chứng minh. Khai triển $f = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4)$ để biểu diễn b, c, d, e qua $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Khai triển $g = (X-\alpha)(X-\beta)(X-\gamma)$ để biểu diễn các hệ số của g qua $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, và thay vào để biểu diễn chúng qua b, c, d, e. □

Bây giờ xét f là một đa thức bậc bốn bất khả quy và tách được. Khi đó $G = G_f$ là một nhóm con truyền dẫn của S_4 có bậc chia hết cho 4. Ta có các khả năng sau đây:

G	$(G \cap V : 1)$	$(G : V \cap G)$
S_4	4	6
A_4	4	3
V	4	1
D_4	4	2
C_4	2	2

$$(G \cap V : 1) = [E : M]$$
$$(G : V \cap G) = [M : F]$$

Các nhóm dạng D_4 là các 2-nhóm Sylow được thảo luận ở trên, và các nhóm dạng C_4 là các nhóm sinh bởi các xích độ dài 4.

Có thể tính $(G : V \cap G)$ từ giải thức bậc ba g bởi vì $G/V \cap G = \mathrm{Gal}(M/F)$ và M là trường phân rã của g. Một khi biết $(G : V \cap G)$, ta có thể suy ra G trừ trường hợp giá trị đó bằng 2. Nếu $[M : F] = 2$, thì $G \cap V = V$ hoặc C_2. Chỉ có duy nhất nhóm đầu tiên tác động truyền dẫn lên các nghiệm của f, và do vậy (từ 4.4) ta thấy rằng trong trường hợp này $G = D_4$ hoặc C_4 dựa theo f bất khả quy hay không trong $M[X]$.

[1] resolvent cubic

Ví dụ 4.9. *Xét $f(X) = X^4 - 4X + 2 \in \mathbb{Q}[X]$. Nó là đa thức bất khả quy theo tiêu chuẩn Eisenstein (1.16), và giải thức bậc ba của nó là $g(X) = X^3 - 8X + 16$, bất khả quy bởi vì nó không có nghiệm trong $\mathbb{F}_5$. Biệt thức của $g(X)$ là -4864 không phải là một bình phương, và do vậy nhóm Galois của $g(X)$ là S_3. Từ bảng, ta thấy rằng nhóm Galois của $f(X)$ là S_4.*

Ví dụ 4.10. *Xét $f(X) = X^4 + 4X + 2 \in \mathbb{Q}[X]$. Nó là bất khả quy theo tiêu chuẩn Eisenstein (1.16), và giải thức bậc ba của nó là $(X - 4)(X^2 - 8)$; do vậy $M = \mathbb{Q}[\sqrt{2}]$. Từ bảng đã lập ta thấy rằng G_f có dạng D_4 hoặc C_4, nhưng f tách ra trên M (thậm chí như một đa thức của X^2), và do vậy G_f có dạng C_4.*

Ví dụ 4.11. *Xét $f(X) = X^4 - 10X^2 + 4 \in \mathbb{Q}[X]$. Đa thức này bất khả quy trong $\mathbb{Q}[X]$ bởi vì nó bất khả quy trong $\mathbb{Z}[X]$. Giải thức bậc ba của nó là $(X + 10)(X - 4)(X + 4)$, và do vậy G_f có dạng V.*

Ví dụ 4.12. *Xét $f(X) = X^4 - 2 \in \mathbb{Q}[X]$. Nó bất khả quy theo tiêu chuẩn Eisenstein (1.16), và giải thức bậc ba của nó là $g(X) = X^3 + 8X$. Do vậy, $M = \mathbb{Q}[i\sqrt{2}]$. Ta có thể kiểm tra rằng f bất khả quy trên M, và G_f có dạng D_4.*

Như ta đã giải thích trong 1.29, PARI biết làm thế nào để phân tích đa thức trong $\mathbb{Q}[X]$.

Ví dụ 4.13. *(Từ trang web: sci.math.research, tìm kiếm "final analysis") Xét $f(X) = X^4 - 2cX^2 - dX^2 + 2cdX - dc^2 \in \mathbb{Z}[X]$ với $a > 0, b > 0, c > 0, a > b$ và $d = a^2 - b^2$. Cho $r = d/c^2$ và cho ω là số thực dương duy nhất mà $r = \omega^3/(\omega^2 + 4)$. Cho m là số các nghiệm của $f(X)$ trong $\mathbb{Z}$ (tính cả bội). Nhóm Galois của f tính như sau:*

- *Nếu $m = 0$ và ω không hữu tỷ, thì G là nhóm S_4.*
- *Nếu $m = 1$ và ω không hữu tỷ, thì G là nhóm S_3.*
- *Nếu ω hữu tỷ và $\omega^2 + 4$ không là một bình phương thì $G = D_4$.*
- *Nếu ω hữu tỷ và $\omega^2 + 4$ là một bình phương thì $G = V = C_2 \times C_2$.*

Đây là tất cả các trường hợp cần xét. Phần khó là chứng minh rằng trường hợp $m = 2$ không bao giờ xảy ra.

4.5. Ví dụ về các đa thức có nhóm Galois trên $\mathbb{Q}$ là S_p

Bổ đề sau đây cho ta một tiêu chuẩn mà một nhóm con của S_p là toàn bộ nhóm S_p.

Bổ đề 4.14. *Với mỗi số nguyên tố p, nhóm đối xứng S_p được sinh bởi một p-xích và một phép thế sơ cấp.*

Chứng minh. Sau khi đánh số lại nếu cần, có thể giả sử phép thế sơ cấp là $\tau = (12)$, và có thể viết p-xích σ sao cho 1 xuất hiện tại vị trí đầu tiên, $\sigma = (1i_2 \dots i_p)$. Một lũy thừa nào đó của σ sẽ ánh xạ 1 thành 2 và nó vẫn sẽ là một p-xích (ở đây ta đã sử dụng việc p là một số nguyên tố). Sau khi thay σ bởi lũy thừa đó, ta có $\sigma = (12j_3 \dots j_p)$ và sau khi đánh số lại một lần nữa, ta có $\sigma = (123 \dots p)$. Bây giờ

$$(i\, i+1) = \sigma^i (1\, 2) \sigma^{-1}$$

(xem GT 4.29) và do vậy phép thế này nằm trong nhóm con sinh bởi σ và τ. Những phép thế sơ cấp này sinh ra S_p. □

Mệnh đề 4.15. *Cho f là một đa thức bất khả quy bậc p nguyên tố trong $\mathbb{Q}[X]$. Nếu f chẻ ra trong $\mathbb{C}$ và có đúng hai nghiệm không thực thì $G_f = S_p$.*

Chứng minh. Gọi E là trường phân rã của f trong $\mathbb{C}$, $\alpha \in E$ là một nghiệm của f. Do f bất khả quy, $[\mathbb{Q}[\alpha] : \mathbb{Q}] = \deg f = p$ nên $p | [E : Q] = (G_f : 1)$. Suy ra G_f chứa một phần tử cấp p (Định lý Cauchy, GT 4.13), nhưng các phần tử cấp p trong S_p phải là các p-xích (ở đây ta lại dùng p là một số nguyên tố lần nữa).

Xét σ là một liên hợp phức trên $\mathbb{C}$. Khi đó σ hoán đổi hai nghiệm không thực của $f(X)$ và cố định mọi phần tử còn lại. Do đó $G_f \subset S_p$ và chứa một chuyển vị và một p-xích. Nói cách khác $G_f = S_p$. □

Phần còn lại là xây dựng các đa thức thỏa mãn các điều kiện của mệnh đề trên.

Ví dụ 4.16. *Cho $p \geq 5$ là một số nguyên tố. Chọn một số nguyên chẵn m và các số chẵn*

$$n_1 < n_2 < \dots < n_{p-2},$$

đặt

$$g(X) = (X^2 + m)(X - n_1) \cdots (X - n_{p-2}).$$

Đồ thị của g cắt trục Ox tại các các điểm $n_1, \ldots, n_{p-2}$, và nó không có cực đại, cực tiểu địa phương tại bất kỳ điểm nào trong những điểm này (vì n_i là các nghiệm đơn). Do vậy $e = \min_{g'(x)=0} |g(x)| > 0$, và ta có thể chọn một số nguyên lẻ n thỏa mãn $\frac{2}{n} < e$.

Xét

$$f(X) = g(X) - \frac{2}{n}.$$

Vì $\frac{2}{n} < e$, đồ thị của f cũng cắt trục Ox tại đúng $p-2$ điểm, và do vậy f có đúng hai nghiệm không thực. Mặt khác, khi ta viết

$$nf(X) = nX^p + a_1 X^{p-1} + \cdots + a_p,$$

thì a_i là các số chẵn và a_p không chia hết cho 4. Theo tiêu chuẩn Eisenstein, ta kết luận f bất khả quy. Trên $\mathbb{R}$, f có $p-2$ nhân tử tuyến tính và một nhân tử bậc hai, và nó chẻ ra trên $\mathbb{C}$. Vậy nên, mệnh đề trên áp dụng được cho f. [2]

Ví dụ 4.17. *Không nên nghĩ rằng để có nhóm Galois S_p, một đa thức phải có đúng hai nghiệm không thực. Ví dụ, đa thức $X^5 - 5X^3 + 4X - 1$ có nhóm Galois S_5 nhưng tất cả các nghiệm của nó đều thực.*

4.6. Trường hữu hạn

Ký hiệu $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ là trường có p phần tử. Như chú ý trong tiết 1, mọi trường E đặc số p chứa một bản sao của $\mathbb{F}_p$, $\{m.1_E \mid m \in \mathbb{Z}\}$. Không có trở ngại gì khi ta đồng nhất $\mathbb{F}_p$ với một nhóm con của E.

Giả sử E là một trường bậc n trên $\mathbb{F}_p$. Khi đó E có $q = p^n$ phần tử, và do vậy $E^\times$ là một nhóm có cấp $q-1$. Vì vậy các phần tử khác 0 của E là các nghiệm của $X^{q-1} - 1$, và tất cả các phần tử của E (bao gồm 0) là các nghiệm của $X^q - X$. Vì thế E là một trường phân rã của $X^q - X$, và bất kỳ hai trường với q phần tử đều đẳng cấu với nhau.

Mệnh đề 4.18. *Mọi mở rộng của một trường hữu hạn là mở rộng đơn.*

[2] Nếu m đủ lớn, thì $g(X) - 2$ sẽ có đúng hai nghiệm không thực, nghĩa là ta có thể lấy $n = 1$, nhưng chứng minh khá dài (xem Jacobson 1964, p 107) Các suy luận ngắn hơn trong giáo trình được gợi ý cho tôi bởi Martin Ward.

Chứng minh. Xét $E \supset F$. Nhóm $E^\times$ là một nhóm hữu hạn các nhóm nhân của một trường, và do vậy là nhóm xyclic (xem Bài tập 1-3). Nếu ζ sinh ra $E^\times$ như là một nhóm nhân, thì rõ ràng $E = F[\zeta]$. □

Bây giờ, cho E là trường phân rã của $f(X) = X^q - X, q = p^n$. Đạo hàm $f'(X) = -1$, nguyên tố cùng nhau với $f(X)$ (thực tế là với mọi đa thức), và do vậy $f(X)$ có q nghiệm phân biệt trong E. Goị S là tập các nghiệm của nó, S hiển nhiên đóng dưới phép nhân và phép lấy nghịch đảo, nhưng nó cũng đóng dưới phép trừ: nếu $a^q = a$ và $b^q = b$, thì

$$(a - b)^q = a^q - b^q = a - b.$$

Vì thế S là một trường, và do vậy $S = E$. Nói riêng, E có p^n phần tử.

Mệnh đề 4.19. *Với mỗi lũy thừa $q = p^n$, tồn tại một trường $\mathbb{F}_q$ với q phần tử. Đó là trường phân rã của $X^q - X$, và hai trường bất kỳ như thế như đẳng cấu với nhau. Hơn nữa, $\mathbb{F}_q$ là một mở rộng Galois trên $\mathbb{F}_p$ với nhóm Galois xyclic sinh bởi tự đẳng cấu Frobenius $\sigma(a) = a^p$.*

Chứng minh. Chỉ có khẳng định cuối cần chứng minh. Trường $\mathbb{F}_q$ Galois trên $\mathbb{F}_p$ bởi vì nó là trường phân rã của một đa thức tách được. Ta chú ý trong 1.4 rằng $x \overset{\sigma}{\mapsto} x^p$ là một tự đẳng cấu của $\mathbb{F}_q$. Một phần tử a của $\mathbb{F}_q$ cố định bởi σ nếu và chỉ nếu $a^p = a$, nhưng $\mathbb{F}_p$ gồm chính xác hai phần tử như vậy, và do vậy trường cố định của $\langle\sigma\rangle$ là $\mathbb{F}_p$. Điều này chứng minh rằng $\mathbb{F}_p$ Galois trên $\mathbb{F}_p$ và $\langle\sigma\rangle = Gal(\mathbb{F}_q/\mathbb{F}_p)$. □

Hệ quả 4.20. *Cho E là một trường p^n phần tử. Với mỗi ước dương m của n, E chứa đúng một trường con có p^m phần tử.*

Chứng minh. Ta biết rằng E Galois trên $\mathbb{F}_p$ và $\mathrm{Gal}(E/\mathbb{F}_p)$ là nhóm xyclic bậc n sinh bởi σ. Nhóm $\langle\sigma\rangle$ có một nhóm con bậc n/m với mỗi m chia hết n, cụ thể là $\langle\sigma^m\rangle$, và do đó E có đúng một trường con bậc m trên $\mathbb{F}_\mathrm{p}$ với mỗi ước m của n, cụ thể là trường $E^{\langle\sigma^m\rangle}$. Vì có bậc m trên $\mathbb{F}_p$, nên $E^{\langle\sigma^m\rangle}$ có p^m phần tử. □

Hệ quả 4.21. *Mỗi đa thức đơn khởi bất khả quy f bậc $d|n$ trong $\mathbb{F}_p[X]$ xuất hiện đúng một lần như là một nhân tử của $X^{p^n} - X$; do vậy, bậc của trường phân rã của f nhỏ hơn hoặc bằng d.*

Chứng minh. Trước hết, các nhân tử của $X^{p^n} - X$ khác nhau vì nó không có nhân tử chung với đạo hàm của nó. Nếu $f(X)$ bất khả quy bậc d, thì

$f(X)$ có một nghiệm trong một trường bậc d trên $\mathbb{F}_p$. Nhưng trường phân rã của $X^{p^n} - X$ chứa một bản sao của mỗi trường bậc d trên $\mathbb{F}_p$ khi $d|n$. Vì vậy một nghiệm nào đó của $X^{p^n} - X$ cũng là nghiệm của $f(X)$, và vì thế $f(X)|X^{p^n} - X$. Nói riêng, f chia hết $X^{p^d} - X$, và do vậy nó chẻ ra trong trường phân rã bậc d của nó trên $\mathbb{F}_p$. □

Mệnh đề 4.22. *Cho $\mathbb{F}$ là một bao đóng đại số của $\mathbb{F}_p$. Khi đó $\mathbb{F}$ chứa đúng một trường $\mathbb{F}_{p^n}$ với mỗi số nguyên $n \geq 1$, và $\mathbb{F}_{p^n}$ chứa các nghiệm của $X^{p^n} - X$. Hơn nữa,*

$$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m|n.$$

Tập sắp thứ tự cục bộ các trường con hữu hạn của $\mathbb{F}$ đẳng cấu với tập các số nguyên $n \geq 1$, được sắp thứ tự cục bộ bởi tính chia hết.

Chứng minh. Hiển nhiên từ hệ quả trên. □

Mệnh đề 4.23. *Trường $\mathbb{F}_p$ có một bao đóng đại số trên $\mathbb{F}$.*

Chứng minh. Chọn một dãy các số nguyên $1 = n_1 < n_2 < n_3 < \dots$ thỏa mãn $n_i|n_{i+1}$ với mọi i, và mọi số nguyên n chia hết một trong các số n_i. Ví dụ, cho $n_i = i!$. Xây dựng các trường $\mathbb{F}_{p^{n_i-1}}$ bằng quy nạp như sau: $\mathbb{F}_{p^{n_1}} = \mathbb{F}_{\mathrm{p}}$; $\mathbb{F}_{p^{n_i}}$ là trường phân rã của $X^{p^{n_i}} - X$ trên $\mathbb{F}_{p^{n_i-1}}$. Khi đó $\mathbb{F}_{p^{n_1}} \subset \mathbb{F}_{p^{n_2}} \subset \dots$, và ta định nghĩa $\mathbb{F} = \cup \mathbb{F}_{p^{n_i}}$, là hợp của một chuỗi các trường đại số trên $\mathbb{F}_p$, vì vậy nó lại là một trường đại số trên $\mathbb{F}_p$. Hơn nữa, mọi đa thức trong $\mathbb{F}_p[X]$ chẻ ra trong $\mathbb{F}$, và vì thế nó lại là một bao đóng đại số của $\mathbb{F}$(theo 1.44). □

Nhận xét 4.24. *Do các tập $\mathbb{F}_{p^n}$ không phải là các tập con của một tập cố định nên ta cần giải thích việc lấy hợp của chúng một cách hợp lý. Xác định S là hợp rời của $\mathbb{F}_{p^n}$. Với $a, b \in S$, thiết lập $a \sim b$ nếu $a = b$ trong một trong các $\mathbb{F}_{p^n}$. Thế thì $\sim$ là một quan hệ tương đương, và ta cho $\mathbb{F} = S/\sim$.*

PARI phân tích các đa thức modulo p rất nhanh. Nhắc lại rằng câu lệnh là `factormod(f(X),p)`. Ví dụ, để đạt được danh sách tất cả các đa thức monic bậc $1, 2$, hay 4 trên $\mathbb{F}_5$, hỏi PARI để phân tích $X^{625} - X$ modulo 5 (chú ý rằng $625 = 5^4$).

aside Trong một trong những bài báo hiếm hoi được xuất bản khi còn sống, Galois đã đưa ra định nghĩa các trường hữu hạn có bậc là lũy thừa

một số nguyên tố bất kỳ và thiết lập các tính chất cơ bản của chúng, ví dụ, sự tồn tại của phần tử nguyên thủy (Notices AMS, Feb. 2003, p. 198). Vì lý do đó nên các trường hữu hạn thường được gọi là **trường Galois** và các trường có q phần tử thường được ký hiệu là $GF(q)$. aside

4.7. Tính nhóm Galois trên trường $\mathbb{Q}$

Trong phần còn lại của chương này, tôi sẽ phác thảo một phương pháp thực tiễn để tính các nhóm Galois trên $\mathbb{Q}$ và các trường tương tự. Nhắc lại rằng đối với một đa thức tách được $f \in F[X]$, F_f ký hiệu một trường phân rã của f, và $G_f = \mathrm{Gal}(F_f/F)$ là nhóm Galois của f. Hơn nữa, G_f hoán vị các nghiệm $\alpha_1, \alpha_2, \dots$ của f trong F_f:

$$G \subset \mathrm{Sym}\{\alpha_1, \alpha_2, \dots\}.$$

Kết quả đầu tiên dưới đây tổng quát Mệnh đề 4.4.

Mệnh đề 4.25. *Cho $f(X)$ là một đa thức trong $F[X]$ chỉ có các nghiệm đơn. Giả sử các quỹ đạo của G_f tác động lên các nghiệm của f có tương ứng $m_1, \dots, m_r$ phần tử. Khi đó f có phân tích: $f = f_1 \cdots f_r$ ở đó f_i bất khả quy bậc m_i.*

Chứng minh. Có thể giả thiết rằng f đơn khởi. Ký hiệu $\alpha_1, \dots, \alpha_m$, $m = \deg(f)$, là các nghiệm của $f(X)$ trong F_f. Các nhân tử đơn khởi của $f(X)$ trong $F[X]$ tương ứng với các tập con S của $\{\alpha_1, \dots, \alpha_m\}$,

$$S \leftrightarrow f_S = \prod_{\alpha \in S} (X - \alpha),$$

và f_S được giữ cố định dưới tác động của nhóm G_f (và do vậy có hệ số trong F) nếu và chỉ nếu S ổn định dưới tác động của G_f. Do đó các nhân tử bất khả quy của f trong $F[X]$ là các đa thức f_S tương ứng với các tập con bé nhất S của $\{\alpha_1, \dots, \alpha_m\}$ ổn định dưới tác động của G_f, nhưng dễ thấy các tập con này chính là các quỹ đạo của G_f trong $\{\alpha_1, \dots, \alpha_m\}$. □

Nhận xét 4.26. *Chứng minh trên chỉ ra rằng nếu $\{\alpha_1, \dots, \alpha_m\} = \bigcup O_i$ là phân tích của $\{\alpha_1, \dots, \alpha_m\}$ thành hợp rời các quỹ đạo của nhóm G_f; thì*

$$f = \prod f_i, \quad f_i = \prod_{\alpha_i \in O_i} (X - \alpha_i)$$

là phân tích của f thành tích các đa thức bất khả quy trong $F[X]$.

Bây giờ, giả sử F hữu hạn, có p^n phần tử. Thế thì G_f là nhóm xyclic sinh bởi các đồng cấu Frobenius $\sigma\colon x \mapsto x^{p^n}$. Khi xem σ như là một phép thế hoán vị các nghiệm của f thì các quỹ đạo phân biệt của σ tương ứng với các nhân tử trong khai triển dạng xích của nó (GT 4.26). Vì vậy, nếu bậc của các nhân tử bất khả quy phân biệt của f là $m_1, \dots, m_r$, thì σ có kiểu xích

$$m_1 + \cdots + m_r = \deg f.$$

Bổ đề 4.27. *Cho R là vành nhân tử hóa với trường các thương F, và f là một đa thức đơn khởi trong $F[X]$. Cho P là một ideal nguyên tố của R, và $\overline{f}$ là ảnh của f trong $(R/P)[X]$. Giả sử rằng f và $\overline{f}$ đều không có nghiệm bội. Khi đó các nghiệm $\alpha_1, \dots, \alpha_m$ của f nằm trong một mở rộng hữu hạn R' của R, và các rút gọn $\overline{\alpha_i}$ modulo PR' là các nghiệm của $\overline{f}$. Hơn nữa $G_{\bar{f}} \subset G_f$ khi cả hai được đồng nhất với các nhóm con của* $\mathrm{Sym}\{\alpha_1, \dots, \alpha_m\} = \mathrm{Sym}\{\overline{\alpha_1}, \dots, \overline{\alpha_m}\}$.

Chứng minh. Bỏ qua - xem van der Waerden, Modern Algebra, I, 61 (second edition). Chứng minh có sử dụng một số kiến thức đại số giao hoán, xem math.stackexchange.com, question 111850. □

Kết hợp các kết quả này, ta thu được được định lý sau.

Định lý 4.28 (Dedekind)**.** *Cho $f(X) \in \mathbb{Z}[X]$ là đa thức đơn khởi bậc m, và p là một số nguyên tố thỏa mãn $f \mod p$ có các nghiệm đơn (tương đương với $D(f)$ không chia hết cho p). Giả sử $\overline{f} = \prod f_i$ với f_i bất khả quy bậc m_i trong $\mathbb{F}_p[X]$. Khi đó G_f chứa một phần tử có kiểu xích dạng*

$$m = m_1 + \cdots + m_r.$$

Ví dụ 4.29. *Xét $X^5 - X - 1$. Modulo 2, nó phân tích thành*

$$(X^2 + X + 1)(X^3 + X^2 + 1),$$

và modulo 3 nó bất khả quy. Vì vậy G_f chứa $(ik)(lmn)$ và (12345), và do vậy $((ik)(lmn))^3 = (ik)$. Nên $G_f = S_5$ bởi 4.14.

Bổ đề 4.30. *Nếu $H \subset S_n$ là một nhóm con truyền dẫn chứa một phép thế sơ cấp và một $(n-1)$-xích thì $H = S_n$.*

Chứng minh. Sau khi đánh số lại, có thể giả sử rằng $(n-1)$-xích đó là $(123\dots n-1)$. Do tính truyền dẫn, phép thế sơ cấp có thể được biến đổi

thành (in), với $1 \leq i \leq n-1$. Liên hợp (in) bởi $(123\ldots n-1)$ và các lũy thừa của nó sẽ thu được $(1n), (2n), \ldots, (n-1\,n)$ và các phần tử này hiển nhiên sinh ra S_n. □

Ví dụ 4.31. *Chọn các đa thức đơn khởi, tách được bậc* n, f_1, f_2, f_3 *với hệ số trong* $\mathbb{Z}$ *sao cho:*

(a) f_1 *bất khả quy modulo* 2.

(b) $f_2 =$ *(bậc* 1*)(bất khả quy bậc* $n-1$*) modulo* 3.

(c) $f_3 =$ *(bất khả quy bậc* 2*)(tích của* 1 *hoặc* 2 *các đa thức bất khả quy bậc lẻ) modulo* 5.

Đặt

$$f = -15f_1 + 10f_2 + 6f_3,$$

thì ta có

(i) G_f *truyền dẫn (nó chứa một* n*-xích bởi vì* $f \equiv f_1 \bmod 2$*)*

(ii) G_f *chứa một xích độ dài* $n-1$ *(bởi vì* $f \equiv f_2 \bmod 3$*.)*

(iii) G_f *chứa một phép thế sơ cấp (bởi vì* $f \equiv f_2 \bmod 5$*, và do vậy nó chứa tích của một phép thế sơ cấp với một phần tử bậc lẻ giao hoán với nó; sau khi nâng lên lũy thừa lẻ thích hợp, chỉ còn lại một phép thế sơ cấp. Do đó* G_f *là* S_n*.*

Kết quả trên cho ta một phương cách để tính nhóm Galois của một đa thức bất khả quy $f \in \mathbb{Q}[X]$ như sau. Phân tích f modulo một dãy các số nguyên tố p không chia hết $D(f)$ để xác định kiểu xích của các phần tử trong G_f - một định lý khó trong lý thuyết số, là tính hiệu quả của định lý phân bố Chebotarev, nói rằng nếu một kiểu xích xuất hiện trong G_f, thì nó sẽ được tìm thấy bằng cách lấy modulo một tập các số nguyên tố có mật độ dương, và nó sẽ xuất hiện đối với một số nguyên tố nhỏ hơn một chặn nào đó. Bây giờ nhìn vào bảng các nhóm con truyền dẫn của S_n có bậc chia hết cho n và các kiểu xích của chúng. Nếu điều này không đủ để xác định nhóm, thì phải tìm hiểu tác động của nó lên tập các tập con của r nghiệm với r nào đó.

Xem Butler và McKay, *The transitive groups of degree up to eleven*, Comm. Algebra 11 (1983), 863–911. Trong đó có liệt kê tất cả các nhóm

con truyền dẫn của S_n, $n \leq 11$, và đưa ra các kiểu xích của các phần tử của chúng và độ dài quỹ đạo của các nhóm con tác động lên các r-tập các nghiệm. Trừ một số ít ngoại lệ, các bất biến này đủ để xác định nhóm con sai khác đẳng cấu.

PARI có thể tính các nhóm Galois của các đa thức bậc ≤ 11 trên $\mathbb{Q}$. Cú pháp là `polgalois(f)` với f là một đa thức bất khả quy bậc ≤ 11 (hay ≤ 7 phụ thuộc vào thiết lập của bạn), và đầu ra là $(n, s, k,$ tên) với n là bậc của nhóm, s là tên nhóm. Ví dụ, `polgalois(X^5-5X^3+4*X-1)` (xem 4.17) trả về nhóm đối xứng S_5, có bậc 120, `polgalois(X^11-5*X^3+4*X-1)` trả về nhóm đối xứng S_11, bậc 39916800, và `polgalois(X^12-5*X^3+4*X-1)` trả về lỗi. Bạn đọc có thể dùng PARI để kiểm tra ví dụ 4.9-4.12.

Xem thêm Soicher and McKay, *Computing Galois groups over the rationals*, J. Number Theory, 20 (1985) 273–281.

4.8. Bài tập

4-1 Tìm trường phân rã của $X^m - 1 \in \mathbb{F}_p[X]$.

4-2 Tìm trường phân rã của $X^4 - 2X^3 - 8X - 3$ trên $\mathbb{Q}$.

4-3 Tìm bậc của trường phân rã của $X^8 - 2$ trên $\mathbb{Q}$.

4-4 Cho một ví dụ một mở rộng trường E/F bậc 4 sao cho không có trường M với $F \subset M \subset E, [M : F] = 2$.

4-5 Liệt kê tất cả các đa thức bất khả quy bậc 3 trên $\mathbb{F}_7$ trong 10 giây hoặc ít hơn (có tất cả 112).

4-6 Một câu hỏi hại não mà ít học viên cao học biết làm thế nào để tiếp cận vấn đề là xác định các nhóm Galois của

$$X^6 + 2X^5 + 3X^4 + 5X^2 + 6X + 7$$

" [trên $\mathbb{Q}$].

(a) Bạn có thể tìm được nó ?

(b) Bạn có thể tìm nó mà không sử dụng lệnh "polgalois" trong PARI ?

4-7 Cho $f(X) = X^5 + aX + b, a, b \in \mathbb{Q}$. Chứng minh rằng $G_f \approx D_5$ (nhóm nhị diện) nếu và chỉ nếu

(a) $f(X)$ bất khả quy trên $\mathbb{Q}[X]$, và

(b) Biệt thức $D(f) = 4^4a^5 + 5^5b^4$ của $f(X)$ là một bình phương, và

(c) Phương trình $f(X) = 0$ giải được bằng căn thức.

4-8 Chứng minh rằng một đa thức f bậc $n = \prod_{i=1}^{k} p_i^{r_i}$ bất khả quy trên $\mathbb{F}_p$ nếu và chỉ nếu $\gcd(f(x), x^{q^{n/p_i}} - x) = 1$ với mọi i.

4-9 Cho $f(X)$ là một đa thức bất khả quy trong $\mathbb{Q}[X]$ có cả nghiệm thực và nghiệm ảo. Chứng minh rằng nhóm Galois của nó không abel. Có thể bỏ đi điều kiện f bất khả quy không ?

4-10 Cho F là mở rộng Galois của $\mathbb{Q}$, và cho α là một phần tử của F sao cho $\alpha F^{\times 2}$ không cố định bởi tác động của $\mathrm{Gal}(F/\mathbb{Q})$ trên $F^{\times}/F^{\times 2}$. Cho $\alpha = \alpha_1, \ldots, \alpha_n$ là quỹ đạo của α dưới tác động của $\mathrm{Gal}(F/\mathbb{Q})$. Chứng minh:

(a) $F[\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_n}]/F$ Galois với nhóm Galois giao hoán chứa trong $(\mathbb{Z}/2\mathbb{Z})^n$.

(b) $F[\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_n}]/\mathbb{Q}$ Galois với nhóm Galois không giao hoán chứa trong $(\mathbb{Z}/2\mathbb{Z})^n \rtimes \mathrm{Gal}(F/\mathbb{Q})$. (Cf. mol 13794.)

CHƯƠNG 5

Ứng dụng của Lý thuyết Galois

Trong chương này, ta áp dụng định lý cơ bản của Lý thuyết Galois để đạt được các kết quả khác về đa thức và các mở rộng trường.

5.1. Định lý phần tử nguyên thủy

Nhắc lại rằng một mở rộng hữu hạn của trường E/F là đơn nếu $E = F[\alpha]$ với một số phần tử α nào đó trong E. Phần tử α như vậy được gọi là **phần tử nguyên thủy** của E. Ta sẽ chứng minh rằng (ít nhất) mọi các mở rộng tách được có các phần tử nguyên thủy.

Xét ví dụ $\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}$. Ta biết rằng (xem Bài tập 3-3) nhóm Galois của nó trên $\mathbb{Q}$ là một 4-nhóm $\langle \sigma, \tau \rangle$, với

$$\begin{cases} \sigma\sqrt{2} &= -\sqrt{2} \\ \sigma\sqrt{3} &= \sqrt{3} \end{cases}, \quad \begin{cases} \tau\sqrt{2} &= \sqrt{2} \\ \tau\sqrt{3} &= -\sqrt{3} \end{cases}.$$

Chú ý rằng

$$\begin{aligned} \sigma(\sqrt{2} + \sqrt{3}) &= -\sqrt{2} + \sqrt{3}, \\ \tau(\sqrt{2} + \sqrt{3}) &= \sqrt{2} - \sqrt{3}, \\ (\sigma\tau)(\sqrt{2} + \sqrt{3}) &= -\sqrt{2} - \sqrt{3}. \end{aligned}$$

Tất cả chúng đều khác $\sqrt{2} + \sqrt{3}$, và do vậy chỉ có duy nhất phần tử đồng nhất của $\mathrm{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q})$ cố định các phần tử của $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Theo định lý cơ bản, suy ra $\sqrt{2} + \sqrt{3}$ là một phần tử nguyên thủy:

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}].$$

Rõ ràng lập luận này có thể sử dụng trong trường hợp tổng quát hơn.

Nhắc lại rằng một phần tử α đại số trên một trường F là tách được trên F nếu đa thức tối tiểu của nó trên F không có nghiệm bội.

Định lý 5.1. *Cho $E = F[\alpha_1, \ldots, \alpha_r]$ là một mở rộng hữu hạn của F, và giả sử rằng $\alpha_2, \ldots, \alpha_r$ tách được trên F (nhưng α_1 không nhất thiết tách được). Khi đó tồn tại một phần tử $\gamma \in E$ thỏa mãn $E = F[\gamma]$.*

Chứng minh. Đối với các trường hữu hạn, ta đã chứng minh khẳng định này trong 4.18. Vì thế có thể giả sử rằng trường F vô hạn. Chỉ cần chứng minh khẳng định đúng cho $r = 2$, vì từ đó suy ra

$$F[\alpha_1, \alpha_2, \ldots, \alpha_r] = F[\alpha_1', \alpha_3, \ldots, \alpha_r] = F[\alpha_1'', \alpha_4, \ldots, \alpha_r] = \ldots$$

Do đó xét $E = F[\alpha, \beta]$ với β tách được trên F. Ký hiệu f và g là các đa thức tối tiểu của α và β trên F, L là một trường phân rã của fg chứa E. Ký hiệu $\alpha_1 = \alpha, \ldots, \alpha_s$ là các nghiệm của f trong L và $\beta_1 = \beta, \beta_2, \ldots, \beta_t$ là các nghiệm của g. Với mỗi $j \neq 1, \beta_j \neq \beta$, phương trình

$$\alpha_i + X\beta_j = \alpha + X\beta,$$

có nghiệm duy nhất $X = \frac{\alpha_i - \alpha}{\beta - \beta_j}$. Nếu chọn một phần tử $c \in F$ khác các nghiệm này (vì F vô hạn), thì

$$\alpha_i + c\beta_j \neq \alpha + c\beta \text{ trừ khi} i = 1 = j.$$

Đặt $\gamma = \alpha + c\beta$. Ta chứng sẽ chứng minh

$$F[\alpha, \beta] = F[\gamma].$$

Các đa thức $g(X)$ và $f(\gamma - cX)$ có các hệ số trong $F[\gamma]$, và nhận β là một nghiệm:

$$g(\beta) = 0, \quad f(\gamma - c\beta) = f(\alpha) = 0.$$

Thực ra β là nghiệm chung duy nhất của chúng vì ta đã chọn c sao cho $\gamma - c\beta_j \neq \alpha_i$ ngoại trừ trường hợp $i = 1 = j$. Vì thế

$$\gcd(g(X), f(\gamma - cX)) = X - \beta.$$

Ở đây ta tính gcd trong $L[X]$, nhưng nó cũng bằng gcd tính trong $F[\gamma][X]$ (Mệnh đề 2.10). Vì vậy $\beta \in F[\gamma]$, và từ đó suy ra $\alpha = \gamma - c\beta$ cũng nằm trong $F[\gamma]$.Ta có điều phải chứng minh. □

Nhận xét 5.2. *Khi F vô hạn thì chứng minh trên chỉ ra rằng có thể chọn γ có dạng*

$$\gamma = \alpha_1 + c_2\alpha_2 + \cdots + c_r\alpha_r, \quad c_i \in F.$$

Nếu $F[\alpha_1, \ldots, \alpha_r]$ Galois trên F, thì một phần tử như vậy sẽ là một phần tử nguyên thủy với điều kiện nó được di chuyển bởi mọi phần tử không tầm thường của nhóm Galois. Nhận xét này giúp ta có thể dễ dàng mô tả các phần tử nguyên thủy.

Giả thiết của chúng ta khá ít ỏi: nếu *hai* trong các α_i không tách được, thì mở rộng không nhất thiết là đơn. Trước khi đưa ra ví dụ minh họa, ta cần đến một kết quả khác.

Mệnh đề 5.3. *Cho $E = F[\gamma]$ là một mở rộng đại số đơn của F. Khi đó chỉ có một số hữu hạn các trường trung gian M,*

$$F \subset M \subset E.$$

Chứng minh. Giả sử M là một trường trung gian và $g(X)$ là đa thức tối tiểu của γ trên M. Ký hiệu M' là trường con của E sinh bởi các hệ số của $g(X)$ trên F. Rõ ràng $M' \subset M$ và $g(X)$ vẫn là đa thức tối tiểu của γ trên M' nên

$$[E : M'] = \deg g = [E : M],$$

và do vậy $M = M'$; ta vừa chứng tỏ rằng M sinh bởi các hệ số của $g(X)$.

Giả sử $f(X)$ là đa thức tối tiểu của γ trên F. Khi đó $g(X)$ chia hết $f(X)$ trong $M[X]$, và do vậy cũng chia hết $f(X)$ trong $E[X]$. Từ đó, chỉ có hữu hạn các đa thức $g(X)$, nên có hữu hạn các trường trung gian M. □

Nhận xét 5.4.

(a) Chứng minh trên cho ta một mô tả về tất cả các trường trung gian: mỗi trường như vậy được sinh trên F bởi các hệ số của nhân tử $g(X)$ của $f(X)$ trong $E[X]$. Các hệ số của $g(X)$ là các đa thức đối xứng của một số các nghiệm của $f(X)$ (bởi một số nghiệm cố định, không nhất thiết toàn bộ, của các hoán vị của các nghiệm).

(b) Mệnh đề có phát biểu nghịch đảo: nếu E là một mở rộng hữu hạn của F và chỉ có hữu hạn các trường trung gian M, $F \subset M \subset E$, thì

E là một mở rộng đơn của F. Kết quả này cho ta một chứng minh khác của Định lý 5.1 trong trường hợp E tách được trên F, bởi vì Lý thuyết Galois chỉ ra rằng có hữu hạn các trường trung gian trong trường hợp này (ngay cả bao đóng Galois của E trên F chỉ có hữu hạn các trường trung gian).

Ví dụ 5.5. *Mở rộng đai số không đơn đơn giản nhất là* $k(X,Y) \supset k(X^p,Y^p)$*, ở đó k là một trường đóng đại số đặc số p. Đặt* $F = k(X^p,Y^p)$*. Với mọi* $c \in k$*, ta có*

$$k(X,Y) = F[X,Y] \supset F[X+cY] \supset F$$

với bậc của mỗi mở rộng bằng p. Nếu

$$F[X+cY] = F[X+c'Y], \quad c \neq c',$$

thì $F[X+cY]$ *sẽ chứa cả X và Y, điều này không thể xảy ra vì* $[k(X,Y) : F] = p^2$*. Do đó có vô hạn các trường trung gian phân biệt.*[1]

Cũng có thể nhận xét rằng bậc của $k(X,Y)$ *trên* $k(X^p,Y^p)$ *là* p^2*, nhưng nếu* $\alpha \in k(X,Y)$*, thì* $\alpha^p \in k(X^p,Y^p)$*, và do vậy* α *sinh ra một trường bậc không quá p trên* $k(X^p,Y^p)$*.*

5.2. Định lý cơ bản của Đại Số

Trong chương này chúng ta chứng minh định lý cơ bản của đại số.[2]

Định lý 5.6. *Trường số phức* $\mathbb{C}$ *là trường đóng đại số.*

Chứng minh. Ta xác định $\mathbb{C}$ là trường phân rã của X^2+1 trên $\mathbb{R}$, và ký hiệu i là một nghiệm của $X^2+1=0$ trong $\mathbb{C}$. Do vậy $\mathbb{C} = \mathbb{R}[i]$. Ta phải chứng minh rằng (xem 1.44) mọi $f(X) \in \mathbb{R}[X]$ có một nghiệm trong $\mathbb{C}$.

Ta thừa nhận hai kết quả về $\mathbb{R}$:

[1] Zariski chứng minh rằng có cả một trường trung gian M không đẳng cấu với $F(X,Y)$, và Piotr Blass chứng minh trong luận án của ông (University of Michigan 1977), sử dụng kỹ thuật hình học đại số, chứng minh rằng có một dãy vô hạn các trường trung gian đôi một không đẳng cấu.

[2] Vì nó không hẳn chỉ là một định lý trong đại số: Nó là một phát biểu về $\mathbb{R}$ các xây dựng của nó là một phần của giải tích (hoặc có thể tô pô). Thực tế, tôi thích chứng minh dựa trên Định lý của Liouville trong giải tích phức hơn chứng minh đại số đưa ra trong bản thảo này: nếu $f(z)$ là một đa thức không có nghiệm trong $\mathbb{C}$, thì $f(z)^{-1}$ sẽ bị chặn và chỉnh hình trên toàn bộ mặt phẳng phức, và do vậy (bởi Liouville) nó là hằng số. Định lý cơ bản từng là một định lý khá khó chứng minh. Gauss đưa ra một chứng minh trong luận án Tiến sĩ của mình năm 1816. Những lập luận tao nhã được đưa ra ở đây là một sự đơn giản hóa các chứng minh trước đó bởi Emil Artin (xem Artin, E., Algebraische Konstruction reeller Korper, Hamb. Abh., Bd. 5 (1926), 85-90; translation available in Artin, Emil. Exposition by Emil Artin: a selection. AMS; LMS 2007).

◊ Các số thực dương có căn bậc hai.

◊ Mọi đa thức bậc lẻ với hệ số thực có một nghiệm thực.

Cả hai đều là hệ quả trực tiếp của Định lý giá trị trung bình, phát biểu rằng một hàm liên tục trên một khoảng đóng sẽ nhận mọi giá trị giữa giá trị lớn nhất và nhỏ nhất (kể cả hai giá trị này). (Về trực giác, điều này nói rằng, không giống như các số hữu tỷ, trục số thực không có các "lỗ thủng".)

Trước hết ta chỉ ra rằng mọi phần tử của $\mathbb{C}$ có một căn bậc hai. Viết $\alpha = a + bi$, với $a, b \in \mathbb{R}$, và chọn c, d là các số thực mà

$$c^2 = \frac{(a + \sqrt{a^2 + b^2})}{2}, \quad d^2 = \frac{(-a + \sqrt{a^2 + b^2})}{2}.$$

Khi đó $c^2 - d^2 = a$ và $(2cd)^2 = b^2$. Nếu chọn dấu của c và d sao cho cd có cùng dấu với dấu của b, thì $(c + di)^2 = \alpha$ và $c + di$ là một căn bậc hai của α.

Giả sử $f(X) \in \mathbb{R}[X]$, và E là một trường phân rã của $f(X)(X^2 + 1)$. Ta phải chứng minh rằng $E = \mathbb{C}$. Vì $\mathbb{R}$ có đặc số 0 nên đa thức trên tách được, và E Galois trên $\mathbb{R}$. Ký hiệu G là nhóm Galois của mở rộng đó, và H là một 2-nhóm con Sylow của G.

Đặt $M = E^H$. Thế thì M có bậc $(G\colon H)$ trên $\mathbb{R}$, và đó là một số lẻ. Do đó đa thức tối tiểu trên $\mathbb{R}$ của mọi $\alpha \in M$ đều có bậc lẻ (từ tính chất nhân của bậc 1.20), và nó có một nghiệm thực. Bởi vậy đa thức tối tiểu có bậc 1, và $\alpha \in \mathbb{R}$. Như vậy $M = \mathbb{R}$ và $G = H$.

Ta biết rằng $\mathrm{Gal}(E/\mathbb{C})$ là một 2-nhóm. Nếu nó $\neq 1$, thì phải có một nhóm con N chỉ số 2 (GT 4.17). Trường E^N có bậc 2 trên $\mathbb{C}$ (xem 3.24), và do đó nó sinh bởi các căn bậc hai của các phần tử trong $\mathbb{C}$, nhưng ta vừa thấy rằng các căn bậc hai đó nằm trong $\mathbb{C}$. Vì thế $E^N = \mathbb{C}$, mâu thuẫn. Do vậy $\mathrm{Gal}(E/\mathbb{C}) = 1$ và $E = \mathbb{C}$. □

Hệ quả 5.7.

(a) Trường $\mathbb{C}$ là bao đóng đại số của $\mathbb{R}$.

(b) Tập hợp tất cả các số đại số là một bao đóng đại số của $\mathbb{Q}$.

Chứng minh. Phần (a) là hiển nhiên từ định nghĩa của "bao đóng đại số" (1.43), và (b) suy ra rừ Mệnh đề 1.46. □

5.3. Mở rộng cyclotomic

Một **căn bậc** n **nguyên thủy** của 1 trong F là một phần tử cấp n trong $F^\times$. Một phần tử như vậy chỉ có thể tồn tại khi F có đặc số 0 hoặc đặc số p không chia hết n.

Mệnh đề 5.8. *Cho F là một trường đặc số 0 hoặc đặc số p không chia hết n. Gọi E là trường phân rã của $X^n - 1$.*

(a) Tồn tại một căn bậc n nguyên thủy của 1 trong E.

(b) Nếu ζ là một căn bậc n nguyên thủy của 1 trong E, thì $E = F[\zeta]$.

(c) Trường E Galois trên F; với mỗi $\sigma \in \mathrm{Gal}(E/F)$, có một $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ mà $\sigma\zeta = \zeta^i$ với mọi ζ với $\zeta^n = 1$; ánh xạ $\sigma \mapsto [i]$ là một đơn cấu

$$\mathrm{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^\times.$$

Chứng minh.

(a) Các nghiệm của $X^n - 1$ đều phân biệt vì đạo hàm của nó là nX^{n-1} chỉ có nghiệm 0 (ở đây ta dùng điều kiện về đặc số), và do vậy E có n căn bậc n khác nhau của 1. Các căn bậc n của 1 tạo thành một nhóm con hữu hạn $E^\times$, và do vậy (xem Bài tập 1-3) chúng tạo thành một nhóm xyclic. Mọi phần tử sinh đều có bậc n, nên nó là căn bậc n nguyên thủy của 1.

(b) Các nghiệm của $X^n - 1$ là các lũy thừa của ζ nên chúng đều thuộc $F[\zeta]$.

(c) Mở rộng E/F Galois vì E là trường phân rã của một đa thức tách được. Nếu ζ_0 là một căn bậc n nguyên thủy của 1, thì các căn bậc n nguyên thủy còn lại của 1 là ζ_0^i với i nguyên tố cùng nhau với n. Với mọi tự đẳng cấu σ của E, $\sigma\zeta_0$ lại là một căn bậc n nguyên thủy của 1, nó bằng ζ_0^i với i nào đó nguyên tố cùng nhau với n, và ánh xạ $\sigma \mapsto i \bmod n$ là đơn ánh bởi vì ζ_0 sinh ra E trên F. Nó hiển nhiên là một đồng cấu. Hơn nữa, với các căn bậc n khác của 1, $\zeta = \zeta_0^m$,

$$\sigma\zeta = (\sigma\zeta_0)^m = \zeta_0^{im} = \zeta^i.$$

□

Ánh xạ $\sigma \mapsto [i]\colon \mathrm{Gal}(F[\zeta]/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ không nhất thiết phải là một toàn ánh. Ví dụ, nếu $F = \mathbb{C}$, thì ảnh là $\{1\}$, và nếu $F = \mathbb{R}$, thì hoặc là $\{[1]\}$ hoặc là $\{[-1], [1]\}$. Mặt khác, khi $n = p$ là một số nguyên tố, ta đã thấy trong 1.41 rằng $[\mathbb{Q}[\zeta] : \mathbb{Q}] = p - 1$, và do vậy ánh xạ là toàn ánh. Bây giờ ta chứng minh rằng ánh xạ là toàn ánh với mọi n khi $F = \mathbb{Q}$.

Đa thức $X^n - 1$ tất nhiên có một số nhân tử trong $\mathbb{Q}[X]$, cụ thể là các đa thức có dạng $X^d - 1$ với mỗi $d|n$. Thương của $X^n - 1$ cho tất cả các nhân tử đó khi $d < n$ được gọi là **đa thức chia đường tròn thứ** n[3] và kí hiệu là Φ_n. Như vậy

$$\Phi_n = \prod (X - \zeta) \quad \text{(tích trên tất cả các căn bậc } n \text{ nguyên thủy của 1).}$$

Nó có bậc $\varphi(n)$, cấp của $(\mathbb{Z}/n\mathbb{Z})^\times$. Vì mọi căn bậc n của 1 phải là một căn bậc d nguyên thủy của 1 với một d duy nhất nào đó chia hết n, ta thấy rằng

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Ví dụ, $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, và

$$\Phi_6(X) = \frac{X^6 - 1}{(X-1)(X+1)(X^2+X+1)} = X^2 - X + 1.$$

Điều này cho ta một phương pháp truy hồi để tính dễ dàng các đa thức chia đường tròn. Một cách khác là sử dụng lệnh polcyclo(n,X) trong PARI.

Do $X^n - 1$ có hệ số trong $\mathbb{Z}$ và là một đa thức đơn khởi nên mọi nhân tử đơn khởi của nó trong $\mathbb{Q}[X]$ đều có hệ số trong $\mathbb{Z}$ (xem 1.41). Nói riêng, các đa thức chia đường tròn nằm trong $\mathbb{Z}[X]$.

Bổ đề 5.9. *Cho F là một trường đặc số 0 hoặc p không chia hết n, ζ là một căn bậc n nguyên thủy của 1 trong một mở rộng trường nào đó. Các phát biểu sau đây tương đương:*

(a) đa thức Φ_n bất khả quy;

(b) bậc $[F[\zeta]\colon F] = \varphi(n)$;

[3] cyclotomic = chia đường tròn

(c) đồng cấu

$$\mathrm{Gal}(F[\zeta]/F) \to (\mathbb{Z}/n\mathbb{Z})^\times,$$

là một đẳng cấu.

Chứng minh. Do ζ là một nghiệm của Φ_n nên đa thức tối tiểu của ζ chia hết Φ_n. Đa thức đó bằng Φ_n nếu và chỉ nếu $[F[\zeta]\colon F] = \varphi(n)$, điều này đúng khi và chỉ khi phép nhúng $\mathrm{Gal}(F[\zeta]/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ là ánh xạ lên. Nói cách khác nó là một đẳng cấu. □

Định lý 5.10. *Đa thức Φ_n bất khả quy trong $\mathbb{Q}[X]$.*

Chứng minh. Cho $f(X)$ là một nhân tử đơn khởi, bất khả quy của Φ_n trong $\mathbb{Q}[X]$. Các nghiệm của nó sẽ là các căn bậc n nguyên thủy của 1, và ta phải chứng minh rằng chúng bao gồm tất cả các căn bậc n nguyên thủy của 1. Để có điều này ta cần chứng minh rằng

> ζ là một nghiệm của $f(X) \Rightarrow \zeta^i$ là một nghiệm của $f(X)$ với mọi i thỏa mãn $\gcd(i, n) = 1$.

Các số i như vậy là tích các số nguyên tố không chia hết n, và do vậy ta cần chứng tỏ

> ζ là một nghiệm của $f(X) \Rightarrow \zeta^p$ là một nghiệm của $f(X)$, với mọi số nguyên tố p không chia hết n.

Viết

$$\Phi_n(X) = f(X)g(X).$$

Mệnh đề 1.41 chỉ ra rằng $f(X)$ và $g(X)$ nằm trong $\mathbb{Z}[X]$. Giả sử ζ là một nghiệm của f, nhưng với với một số nguyên tố p nào đó không chia hết n, ζ^p không là một nghiệm của f. Thế thì ζ^p là một nghiệm của $g(X)$, $g(\zeta^p) = 0$, và do vậy ζ là một nghiệm của $g(X^p)$. Do $f(X)$ và $g(X^p)$ có một nghiệm chung, chúng phải có nhân tử chung không tầm thường trong $\mathbb{Q}[X]$ (2.10), nó tự khắc nằm trong $\mathbb{Z}[X]$ (1.14).

Ký hiệu $h(X) \mapsto \overline{h}(X)$ cho ánh xạ thương $\mathbb{Z}[X] \to \mathbb{F}_p[X]$, và chú ý rằng, vì $f(X)$ và $g(X^p)$ có một nhân tử chung bậc ≥ 1 trong $\mathbb{Z}[X]$, nên $\overline{f}(X)$ và $\overline{g}(X^p)$ trong $\mathbb{F}_p[X]$ cũng vậy. Định lý nhị thức mod p nói rằng

$$\overline{g}(X)^p = \overline{g}(X^p)$$

(nhắc lại rằng $a^p = a$ với mọi $a \in \mathbb{F}_p$), và do vậy $\overline{f}(X)$ và $\overline{g}(X)$ có một nhân tử chung bậc ≥ 1 trong $\mathbb{F}_p[X]$. Nên $X^p - 1$, khi được xem như là một phần tử của $\mathbb{F}_p[X]$, có nghiệm bội, nhưng ta đã thấy trong chứng minh của Mệnh đề 5.8 rằng điều đó không xảy ra. Mâu thuẫn. □

Nhận xét 5.11. *Lời giải này khá cổ - theo nghĩa nó có từ thời Dedekind năm 1857 - nhưng ý tưởng chính của nó gần đây trở nên phổ biến: từ một khẳng định trong đặc số 0, rút gọn mod p (tại đó khẳng định không đúng hoàn toàn), và khai thắc sự tồn tại của tự đẳng cấu Frobenius $a \mapsto a^p$ để đạt được một chứng minh của khẳng định ban đầu. Ví dụ, đại số giao hoán dùng phương pháp này để chứng minh các kết quả về vành giao hoán, và có các định lý về đa tạp phức được chứng minh đầu tiên bằng cách giảm các đối tượng về đặc số p.*

Tồn tại một mối liên hệ đẹp và bí hiểm giữa những gì xảy ra trong đặc số 0 và đặc số p. Ví dụ, cho $f(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$. Ta có thể

(a) xét các nghiệm của $f = 0$ trong $\mathbb{C}$, và nhận được một không gian tôpô;

(b) lấy rút gọn modulo p, và xét các nghiệm của $\overline{f} = 0$ trong $\mathbb{F}_{p^n}$.

Giả thuyết Weil (Weil 1949; chứng minh một phần bởi Grothendieck năm 1960's và hoàn toàn bởi Deligne năm 1973) khẳng định rằng các số Betti của không gian trong (a) điều khiển lực lượng của các tập hợp trong (b).

Định lý 5.12. *Một n-giác đều xây dựng được nếu và chỉ nếu $n = 2^k p_1 \ldots p_s$ với p_i là các số nguyên tố Fermat phân biệt.*

Chứng minh. n-giác đều có thể xây dựng được nếu và chỉ nếu $\cos \frac{2\pi}{n}$ (hay $\zeta = e^{2\pi i/n}$) xây dựng được. Ta biết rằng $\mathbb{Q}[\zeta]$ Galois trên $\mathbb{Q}$, và do vậy (theo 1.37 và 3.23) ζ xây dựng được nếu và chỉ nếu $[\mathbb{Q}[\zeta] : \mathbb{Q}]$ là một lũy thừa của 2. Nhưng (xem GT 3.5)

$$\varphi(n) = \prod_{p|n} (p-1)p^{n(p)-1}, \quad n = \prod p^{n(p)},$$

và nó là một lũy thừa của 2 nếu và chỉ nếu n có dạng như trong định lý. □

Nhận xét 5.13.

(a) Như ta đã giới thiệu trước đây, các số nguyên tố Fermat là số nguyên tố có dạng $2^{2^k}+1$. Các số dạng này nguyên tố khi $k = 0, 1, 2, 3, 4$, nhưng người ta không biết liệu rằng còn hay không các số nguyên tố Fermat. Do vậy bài toán liệt kê tất cả các số n sao cho n-giác đều xây dựng được vẫn chưa được giải quyết. Xem Wikipedia (Fermat number).

(b) Phần cuối của Gauss, Disquisitiones Arithmeticae (1801), có tiêu đề "Equations defining sections of a Circle". Trong đó, Gauss chứng minh rằng các căn bậc n của 1 tạo thành một nhóm xyclic, $X^n - 1$ là giải được (điều này có từ trước lý thuyết các nhóm abel được phát triển, và trước Galois), và các n-giác đều xây dựng được khi n có dạng trong định lý trên. Ông cũng khẳng định đã chứng minh được chiều ngược lại của phát biểu. Điều này khiến một số người cho rằng ông đã đưa ra chứng minh trên về tính bất khả quy của Φ_n, nhưng vì thiếu các bằng chứng nên tôi vẫn cho rằng đó là của với Dedekind.

5.4. Định lý Dedekind về tính độc lập của các đặc trưng

Định lý 5.14 (Dedekind)**.** *Cho F là một trường, và cho G là một nhóm. Khi đó mọi tập hữu hạn $\{\chi_1, \ldots, \chi_m\}$ các đồng cấu $G \to F^\times$ đều độc lập tuyến tính trên F:*

$$\sum a_i\chi_i = 0 \text{ (như là một hàm } G \to F) \Longrightarrow a_1 = 0, \ldots, a_m = 0.$$

Chứng minh. Ta sẽ chứng minh quy nạp theo m. Với $m = 1$, khẳng định hiển nhiên đúng. Giả sử khẳng định đứng với $m-1$, và giả sử đối với tập hợp $\{\chi_1, \ldots, \chi_m\}$ các đồng cấu $G \to F^\times$ và các $a_i \in F$, thì

$$a_1\chi_1(x) + a_2\chi_2(x) + \ldots a_m\chi_m(x) = 0 \text{ với mọi } x \in G.$$

Ta phải chứng minh rằng $a_i = 0$ với mọi i. Do χ_1 và χ_2 phân biệt, nên $\chi_1(g) \neq \chi_2(g)$ với $g \in G$ nào đó. Thay x bằng gx trong phương trình, ta thấy rằng

$$a_1\chi_1(g)\chi_1(x) + \cdots + a_m\chi_m(g)\chi_m(x) = 0 \text{ với mọi } x \in G.$$

Nhân phương trình thứ nhất với $\chi_1(g)$ và trừ nó cho phương trình thứ hai, ta đạt được phương trình

$$a_2'\chi_2 + \cdots + a_m'\chi_m = 0, \quad a_i' = a_i(\chi_i(g) - \chi_1(g)).$$

Theo giả thiết quy nạp ta có $a_i' = 0$ với $i = 2, 3, \ldots$. Từ $\chi_2(g) - \chi_1(g) \neq 0$, nó suy rằng $a_2 = 0$, và do vậy

$$a_1\chi_1 + \cdots + a_m\chi_m = 0.$$

Giả thuyết quy nạp bây giờ chỉ ra rằng các a_i còn lại cũng bằng 0. □

Hệ quả 5.15. *Cho F và E là các trường, và $\sigma_1, \ldots, \sigma_m$ là các đồng cấu phân biệt $F \to E$. Khi đó $\sigma_1, \ldots, \sigma_m$ độc lập tuyến tính trên E.*

Chứng minh. Áp dụng định lý cho $\chi_i = \sigma_i|F^\times$. □

Hệ quả 5.16. *Cho E là một mở rộng bậc m tách được của F. Gọi $\alpha_1, \ldots, \alpha_m$ là một cơ sở của E trên F, và $\sigma_1, \ldots, \sigma_m$ là các F-đồng cấu phân biệt từ E tới một trường Ω. Khi đó ma trận có phần tử tại tọa độ (i, j) là $\sigma_i\sigma_j$ là một ma trận khả nghịch.*

Chứng minh. Phản chứng: nếu không khả nghịch thì tồn tại $c_i \in \Omega$ mà $\sum_{i=1}^{n} c_i\sigma_i(\alpha_i) = 0$ với mọi j. Nhưng ánh xạ $\sum_{i=1}^{m} c_i\sigma_i : E \to \Omega$ là F-tuyến tính, và do vậy nó dẫn tới $\sum_{i=1}^{n} c_i\sigma_i(\alpha) = 0$ với mọi $\alpha \in E$, mâu thuẫn với Hệ quả 5.15. □

5.5. Định lý cơ sở chuẩn tắc

Định nghĩa 5.17. Cho E là một mở rộng Galois hữu hạn của F với nhóm Galois G. Một cơ sở của E, xem như một F-không gian véctơ được gọi là một **cơ sở chuẩn tắc** nếu nó gồm các liên hợp của một phần tử của E.

Nói cách khác, một cơ sở chuẩn tắc là một cơ sở có dạng

$$\{\sigma\alpha \mid \sigma \in G\}$$

với α nào đó trong E.

Định lý 5.18 (Định lý cơ sở chuẩn tắc[4])**.** *Mọi mở rộng Galois đều có một cơ sở chuẩn tắc.*

[4] normal basis theorem

Đại số nhóm FG của G là một F-không gian véctơ với cơ sở là các phần tử của G và với phép nhân được thác triển từ phép nhân trong G. Như vậy một phần tử của FG là một tổng $\sum_{\sigma\in G} a_\sigma\sigma$, $a_\sigma \in F$, và

$$(\sum_\sigma a_\sigma\sigma)(\sum_\sigma b_\sigma\sigma) = \sum_\sigma(\sum_{\sigma_1\sigma_2} a_{\sigma_1}b_{\sigma_2})\sigma.$$

Mọi tác động F-tuyến tính của G lên một F-không gian véctơ V đều thác triển được một cách duy nhất thành một tác động của FG lên V.

Giả sử E/F là một mở rộng Galois với nhóm Galois G. Khi đó E là một FG-môđun, và Định lý 5.18 nói rằng tồn tại một phần tử $\alpha \in E$ mà

$$\sum_\sigma a_\sigma\sigma \mapsto \sum_\sigma a_\sigma\sigma\alpha : FG \to E$$

là một đẳng cấu của các FG-môđun. Nói cách khác E là một FG-môđun tự do hạng 1.

Ta đưa ra ba chứng minh của Định lý 5.18. Chứng minh đầu tiên giả thiết rằng F vô hạn và chứng minh thứ hai giả sử rằng G là nhóm xyclic. Vì mọi mở rộng Galois của một trường hữu hạn đều là mở rộng xyclic (4.19) nên hai chứng minh này phủ hết tất cả các trường hợp. Chứng minh thứ ba áp dụng cho cả trường hữu hạn và vô hạn, nhưng lại dùng đến định lý Krull-Schmidt.

Chứng minh cho trường vô hạn

Bổ đề 5.19. *Cho $f \in F[X_1, \cdots X_m]$, và S là một tập con vô hạn của F. Nếu $f(a_1, \ldots, a_m) = 0$ với mọi $a_1, \ldots, a_m \in S$, thì f là đa thức 0 (hay $f = 0$ trong $F[X_1, \ldots, X_m]$).*

Chứng minh. Ta chứng minh bằng quy nạp theo m. Với $m = 1$, bổ đề phát biểu rằng một đa thức một biến khác 0 chỉ có hữu hạn nghiệm (xem 1.7). Với $m > 1$, viết f như là một đa thức theo X_m với các hệ số trong $F[X_1, \ldots, X_{m-1}]$,

$$f = \sum c_i(X_1, \ldots, X_{m-1})X_m^i.$$

Với mọi bộ $m-1$ phần tử $a_1, \ldots, a_{m-1}$ của S,

$$f(a_1, \ldots, a_{m-1}, X_m)$$

là một đa thức theo X_m nhận mọi phần tử của S làm nghiệm. Do đó, mỗi hệ số của nó bằng 0: $c_i(a_1, \dots, a_{m-1}) = 0$ với mọi i. Vì điều này đúng cho mọi $(a_1, \dots, a_{m-1})$ nên giả thuyết qui nạp chỉ ra rằng $c_i(X_1, \dots, X_{m-1})$ là đa thức 0. □

Bây giờ ta chứng minh 5.18 trong trường hợp F vô hạn. Đánh số các phần tử của G là $\sigma_1, \dots, \sigma_m$ (với $\sigma_1 = 1$).

Giả sử $f \in F[X_1, \dots, X_m]$ thỏa mãn

$$f(\sigma_1\alpha, \dots, \sigma_m\alpha) = 0$$

với mọi $\alpha \in E$. Đối với mỗi cơ cở $\alpha_1, \dots, \alpha_m$ của E trên F, đặt

$$g(Y_1, \dots, Y_m) = f(\sum_{i=1}^{m} Y_i\sigma_1\alpha_i, \sum_{i=1}^{m} Y_i\sigma_2\alpha_i, \dots) \in E[Y_1, \dots, Y_m].$$

Từ giả thiết đối với f, suy ra $g(a_1, \dots, a_m) = 0$ với mọi $a_i \in F$, và do vậy $g = 0$ (bởi vì F vô hạn). Nhưng do ma trận $(\sigma_i\alpha_j)$ khả nghịch (5.16). g có thể nhận được từ f sau một phép đổi biến tuyến tính khả nghịch, thì f có thể thu được từ g sau một phép đổi biến tuyến tính khả nghịch. Do đó nó cũng bằng 0.

Viết $X_i = X(\sigma_i)$, và cho $A = (X(\sigma_i\sigma_j))$, tức là, A là ma trận $m \times m$ có X_k tại tọa độ (i, j) nếu $\sigma_i\sigma_j = \sigma_k$. Khi đó $det(A)$ là một đa thức theo $X_1, \dots, X_n$, nói cách khác, $det(A) = h(X_1, \dots, X_n)$. Rõ ràng $h(1, 0, \dots, 0)$ là định thức của một ma trận có đúng một số 1 trong mỗi hàng và mỗi cột và các vị trí còn lại đều bằng 0. Do đó các hàng của ma trận là các hoán vị của các hàng của ma trận đơn vị, nên định thức của nó bằng ± 1. Nói riêng, h không đồng nhất bằng 0, và vì thế có một $\alpha \in E^\times$ mà $h(\sigma_1\alpha, \dots, \sigma_m\alpha)(= det(\sigma_i\sigma_j\alpha))$ khác 0. Ta sẽ chứng minh rằng $\{\sigma_i\alpha\}$ là một cơ sở chuẩn tắc. Để làm được điều này, ta chỉ cần chứng tỏ rằng $\sigma_i\alpha$ độc lập tuyến tính trên F. Giả sử

$$\sum_{j=1}^{m} a_j\sigma_j\alpha = 0$$

với $a_j \in F$ nào đó. Áp dụng $\sigma_1, \dots, \sigma_m$ liên tiếp, ta thu được một hệ m-phương trình

$$\sum a_j\sigma_i\sigma_j\alpha = 0$$

theo m ẩn a_j. Vì hệ phương trình này không suy biến, nên a_j bằng 0. Chứng minh của định lý trong trường hợp F vô hạn đã hoàn thành.

Chứng minh khi G là nhóm xyclic

Giả sử G sinh bởi một phần tử σ_0 bậc n. Thế thì $[E\colon F] = n$. Đa thức tối tiểu của σ_0 xem như một tự đồng cấu của F-không gian véctơ F là một đa thức đơn khởi trong $F[X]$ có bậc nhỏ nhất thỏa mãn $P(\sigma_0) = 0$ (xem như một tự đồng cấu của E). Nó chia hết mọi đa thức $Q(X) \in F[X]$ mà $Q(\sigma_0) = 0$. Vì $\sigma_0^n = 1$ nên $P(X)$ chia hết $X^n - 1$. Mặt khác, định lý Dedekind về tính độc lập các đặc trưng (5.14) chỉ ra rằng $1, \sigma_0, \ldots, \sigma_0^{n-1}$ độc lập tuyến tính trên F, nên $deg\, P(X) > n - 1$. Ta kết luận rằng $P(X) = X^n - 1$. Do đó, xem như một $F[X]$-môđun với X tác động như σ_0, E đẳng cấu với $F[X]/(X^n - 1)$. Với bất kỳ phần tử sinh α của E xem như là một $F[X]$-module thì $\alpha, \sigma_0\alpha, \ldots, \sigma_0\alpha^{n-1}$ là một F-cơ sở của E.

Chứng minh chung cho cả hai trường hợp

Định lý Krull-Schmidt phát biểu rằng một môđun M có độ dài hữu hạn trên một vành có thể viết được thành tổng trực tiếp của các môđun bất khả quy và các môđun bất khả quy xuất hiện trong phân tích là duy nhất sai khác thứ tự và đẳng cấu. Do đó $M = \oplus_i m_i M_i$ với M_i bất khả quy và $m_i M_i$ ký hiệu là tổng trực tiếp của m_i bản sao của M_i; tập các lớp đẳng cấu của M_i được xác định duy nhất, và khi ta chọn M_i đôi một không đẳng cấu thì mỗi m_i cũng được xác định duy nhất. Từ điều này, ta suy ra rằng hai môdun M và M' độ dài hữu hạn trên một vành đẳng cấu với nhau nếu $mM = mM'$ với $m \geq 1$ nào đó.

Xét F-không gian véctơ $E \otimes_F E$. Ta cho E tác động lên thành phần tenxơ đầu tiên và cho G tác động lên thành phần thứ hai (nên $a(x \otimes y) = ax \otimes y, a \in E$, và $\sigma(x \otimes y) = x \otimes \sigma y, \sigma \in G$). Ta sẽ chứng minh Định lý 5.18 bằng cách chỉ ra rằng

$$\underbrace{FG \oplus \cdots \oplus FG}_{n} \approx E \otimes_F E \approx \underbrace{E \oplus \cdots \oplus E}_{n}$$

như là các FG-môdun ($n = [E\colon F]$).

Với $\sigma \in G$, ký hiệu $\lambda_\sigma\colon E \otimes_F E \to E$ là ánh xạ $x \otimes y \mapsto x \cdot \sigma y$. Khi đó λ_σ hiển nhiên E-tuyến tính, và $\lambda_\sigma(\tau z) = \lambda_{\sigma\tau}(z)$ với mọi $\tau \in G$ và $z \in E \otimes_F E$. Ta sẽ chứng minh rằng $\{\lambda_\sigma \mid \sigma \in G\}$ là một E-cơ sở của

$\mathrm{Hom}_{E\text{-tuyến tính}}(E \otimes_F E, E)$. Không gian này có số chiều n, ta chỉ cần chứng tỏ tập hợp này độc lập tuyến tính. Nếu $\sum_\sigma c_\sigma \lambda_\sigma = 0, c_\sigma \in E$, thì

$$0 = \sum_\sigma c_\sigma(\lambda_\sigma(1 \otimes y)) = \sum_\sigma c_\sigma \cdot \sigma y$$

với mọi $y \in E$, điều này dẫn tới tất cả $c_\sigma = 0$ bởi định lý Dedekind 5.14.

Xét ánh xạ

$$\phi\colon E \otimes_F E \to EG, \quad z \mapsto \sum_\sigma \lambda_\sigma(z) \cdot \sigma^{-1}.$$

Khi đó ϕ là E-tuyến tính. Nếu $\phi(z) = 0$, thì $\lambda_\sigma(z) = 0$ với mọi $\sigma \in G$, và vì thế $z = 0$ trong $E \otimes_F E$ (bởi vì các λ_σ sinh ra không gian đối ngẫu). Cho nên ϕ là đơn ánh, và từ $E \otimes_F E$ và EG đều có số chiều n trên E, nó là một đẳng cấu. Với $\tau \in G$,

$$\begin{aligned}\phi(\tau z) &= \sum_\sigma \lambda_\sigma(\tau z).\sigma^{-1} \\ &= \sum_\sigma \lambda_{\sigma\tau}(z).\tau(\sigma\tau)^{-1} \\ &= \tau\phi(z),\end{aligned}$$

và do vậy ϕ là một đẳng cấu của các EG-môđun. Nên

$$E \otimes_K E \simeq EG \approx FG \oplus \cdots \oplus FG$$

như là một FG-môdun. Mặt khác, với bất kỳ cơ sở $\{e_1, \ldots, e_n\}$ của E khi coi E là một F-không gian véctơ thì,

$$E \otimes_F E = (e_1 \otimes E) \oplus \cdots \oplus (e_n \otimes E) \simeq E \oplus \cdots \oplus E$$

như các FG-môđun. Chứng minh kết thúc.

Nhận xét 5.20. *Định lý cơ sở chuẩn tắc được phát biểu cho trường hữu hạn bởi Eisenstein vào năm 1850, và được chứng minh cho trường hữu hạn bởi Hensel vào năm 1888. Dedekind sử dụng cơ sở chuẩn tắc trong các trường số trong nghiên cứu của ông về biệt thức vào năm 1880, nhưng ông không có chứng minh tổng quát. Noether đưa ra một chứng minh cho một số trường vô hạn (1932) và Deuring đưa ra một chứng*

minh cho tất cả các trường hợp (cũng vào năm 1932). Chứng minh trên đơn giản hóa ý tưởng của Deuring - xem Blessenohl, Dieter. On the normal basis theorem. Note Mat. 27 (2007), 5-10. Theo Wikipedia, các cơ sở chuẩn tắc được dùng thường xuyên trong các ứng dụng mật mã dựa trên bài toán lôgarit rời rạc như hệ mật đường cong elliptic.

5.6. Định lý thứ 90 của Hilbert

Cho G là một nhóm. Một **G-môđun** là một nhóm abel M cùng với một tác động của G, nghĩa là một ánh xạ $G \times M \to M$ sao cho

(a) $\sigma(m + m') = \sigma m + \sigma m'$ với mọi $\sigma \in G, m, m' \in M$;

(b) $(\sigma\tau)(m) = \sigma(\tau m)$ với mọi $\sigma, \tau \in G$, $m \in M$;

(c) $1m = m$ với mọi $m \in M$.

Do vậy, đưa ra một tác động của G lên M cũng giống như là đưa ra một đồng cấu $G \to \mathrm{Aut}(M)$ (tự đẳng cấu của nhóm abel M).

Ví dụ 5.21. *Cho E là một mở rộng Galois của F với nhóm Galois G. Khi đó $(E, +)$ và $(E^\times, \cdot)$ là các G-môdun.*

Cho M là một G-môđun. Một **đồng cấu chéo**[5] là một ánh xạ $f\colon G \to M$ mà

$$f(\sigma\tau) = f(\sigma) + f(\tau) \text{ với mọi } \sigma, \tau \in G.$$

Chú ý rằng điều kiện này suy ra rằng $f(1) = f(1 \cdot 1) = f(1) + f(1)$, và vì thế $f(1) = 0$.

Ví dụ 5.22.

(a) Cho $f : G \to M$ là một đồng cấu chéo. Với mọi $\sigma \in G$,

$$\begin{aligned} f(\sigma^2) &= f(\sigma) + \sigma f(\sigma), \\ f(\sigma^3) &= f(\sigma.\sigma^2) = f(\sigma) + \sigma f(\sigma) + \sigma^2 f(\sigma) \\ &\cdots \\ f(\sigma^n) &= f(\sigma) + \sigma f(\sigma) + \cdots + \sigma^{n-1} f(\sigma). \end{aligned}$$

[5] cross homomorphism

Do đó nếu G là một nhóm xyclic cấp n sinh bởi σ, thì một đồng cấu chéo $f\colon G \to M$ được xác định bởi giá trị của nó, ký hiệu là x, tại σ, và x thỏa mãn phương trình

$$x + \sigma x + \cdots + \sigma^{n-1}x = 0, \qquad (*)$$

Hơn nữa, nếu $x \in M$ thỏa mãn $(*)$, thì công thức $f(\sigma^i) = x + \sigma x + \cdots + \sigma^{i-1}x$ xác định một đồng cấu chéo $f\colon G \to M$. Do vậy, đối với một nhóm hữu hạn $G = \langle\sigma\rangle$, tồn tại một tương ứng $1-1$

$$\{\textit{các đồng cấu chéo } f\colon G \to M\ \} \overset{f \leftrightarrow f(\sigma)}{\to} \{x \in M \textit{ thỏa mãn (*)}\}.$$

(b) Với mọi $x \in M$, ta xây dựng được một đồng cấu chéo bằng cách đặt

$$f(\sigma) = \sigma x - x \textit{ với mọi } \sigma \in G.$$

Một đồng cấu chéo có dạng này được gọi là một ***đồng cấu chéo chính****.*

(c) Nếu G tác động tầm thường lên M: $\sigma m = m$ với mọi $\sigma \in G$ và $m \in M$, thì một đồng cấu chéo đơn giản là một đồng cấu, và không có các đồng cấu chéo chính khác 0.

Tổng và hiệu của hai đồng cấu chéo lại là một đồng cấu chéo, và tổng và hiệu của hai đồng cấu chéo chính lại là một đồng cấu chéo chính. Vì thế ta có thể xác định

$$H^1(G, M) = \frac{\{\text{các đồng cấu chéo}\}}{\{\text{các đồng cấu chéo chính}\}}$$

(nhóm thương của các nhóm abel). Các nhóm đối đồng điều $H^n(G, M)$ được định nghĩa với mọi $n \in \mathbb{N}$, nhưng vì chúng không được thực hiện cho tới thế kỷ thứ hai mươi nen sẽ không được thảo luận ở đây. Một dãy khớp các G-môđun

$$0 \to M' \to M \to M'' \to 0$$

cho ta một dãy khớp

$$0 \to M'^G \to M^G \to M''^G \xrightarrow{d} H^1(G, M') \to H^1(G, M) \to H^1(G, M'').$$

Cho $m'' \in M''^G$, và cho $m \in M$ biến thành m''. Với mọi $\sigma \in G$, $\sigma m - m$ nằm trong môđun con M' của M, và đồng cấu chéo $\sigma \mapsto \sigma m - m : G \to M'$ biểu thị $d(m'')$. Độc giả có thể tự kiểm tra tính khớp.

Ví dụ 5.23. *Cho $\pi\colon \widetilde{X} \to X$ là một không gian phủ phổ dụng của một không gian tôpô X và Γ là nhóm các phép biến đổi phủ. Dưới một vài giả thuyết khá tổng quát, một Γ-môđun M sẽ xác định một bó $\mathcal{M}$ trên X, và $H^1(X, \mathcal{M}) \simeq H^1(\Gamma, M)$. Ví dụ, khi $M = \mathbb{Z}$ với tác động tầm thường của Γ, nó trở thành đẳng cấu $H^1(X, \mathbb{Z}) \simeq H^1(\Gamma, \mathbb{Z}) = \mathrm{Hom}(\Gamma, \mathbb{Z})$.*

Định lý 5.24. *Cho E là một mở rộng Galois của F với nhóm G; thế thì $H^1(G, E^\times) = 0$. Nói cách khác mọi đồng cấu chéo $G \to E^\times$ đều chính.*

Chứng minh. Giả sử f là một đồng cấu chéo $G \to E^\times$. Trong ký hiệu nhân, điều này có nghĩa là

$$f(\sigma\tau) = f(\sigma)cdot\sigma(f(\tau)), \quad \sigma, \tau \in G,$$

và ta phải tìm một $\gamma \in E^\times$ mà $f(\sigma) = \frac{\sigma\gamma}{\gamma}$ với mọi $\sigma \in G$. Bởi vì $f(\tau)$ khác 0, Hệ quả 5.15 suy ra rằng

$$\sum_{\tau \in G} f(\tau)\tau\colon E \to E$$

không phải là ánh xạ 0, nghĩa là tồn tại $\alpha \in E$ sao cho

$$\beta \overset{def}{=} \sum_{\sigma \in G} f(\tau)\tau\alpha \neq 0.$$

Nhưng khi đó, với $\sigma \in G$,

$$\begin{aligned}\sigma\beta &= \sum_{\tau \in G} \sigma(f(\tau)).\sigma\tau(\alpha) \\ &= \sum_{\tau \in G} f(\sigma)^{-1} f(\sigma\tau).\sigma\tau(\alpha) \\ &= f(\sigma)^{-1} \sum_{\tau \in G} f(\sigma\tau)\sigma\tau(\alpha),\end{aligned}$$

nó bằng $f(\sigma)^{-1}\beta$ bởi vì, khi τ chạy trên G, $\sigma\tau$ cũng vậy. Do đó, $f(\sigma) = \frac{\beta}{\sigma(\beta)}$ và ta có thể chọn $\beta = \gamma^{-1}$. □

Giả sử E là một mở rộng Galois của F với nhóm Galois G. Ta định nghĩa **chuẩn** của một phần tử $\alpha \in E$ là

$$\mathrm{Nm}\,\alpha = \prod_{\sigma \in G} \sigma\alpha.$$

Với mỗi $\sigma \in G$,

$$\tau(\mathrm{Nm}\,\alpha) = \prod_{\sigma\in G} \tau\sigma\alpha = Nm(\alpha),$$

và do đó $Nm(\alpha) \in F$. Ánh xạ

$$\alpha \mapsto \mathrm{Nm}\,\alpha \colon E^\times \to F^\times$$

hiển nhiên là một đồng cấu.

Ví dụ 5.25. *Ánh xạ chuẩn* $\mathbb{C}^\times \to \mathbb{R}^\times$ *là* $\alpha \mapsto |\alpha|^2$ *và ánh xạ chuẩn* $\mathbb{Q}[\sqrt{d}]^\times \to \mathbb{Q}^\times$ *là* $a + b\sqrt{d} \mapsto a^2 - db^2$.

Chúng ta quan tâm tới việc xác định hạt nhân của ánh xạ chuẩn. Rõ ràng một phần tử có dạng $\frac{\beta}{\tau\beta}$ có chuẩn 1, và kết quả sau đây chỉ ra rằng, với các mở rộng xyclic, tất cả các phần tử có chuẩn bằng 1 có dạng này.

Hệ quả 5.26 (Định lý Hilbert 90)**.** [6] *Cho* E *là một mở rộng xyclic hữu hạn của* F *với nhóm Galois* $\langle\sigma\rangle$*; nếu* $\mathrm{Nm}_{E/F}\,\alpha = 1$*, thì* $\alpha = \beta/\sigma\beta$ *với* $\beta \in E$.

Chứng minh. Đặt $m = [E\colon F]$. Điều kiện trên α là $\alpha \cdot \sigma\alpha \cdot \cdots \cdot \sigma^{m-1}\alpha = 1$, và do vậy (xem 5.22a) có một đồng cấu chéo $f\colon \langle\sigma\rangle \to E^\times$ với $f(\sigma) = \alpha$. Định lý 5.24 chỉ ra rằng f là chính, có nghĩa là tồn tại một β với $f(\sigma) = \beta/\sigma\beta$. □

5.7. Mở rộng xyclic

Cho F là một trường chứa một căn bậc n nguyên thủy của 1, $n \geq 2$, và ký hiệu μ_n là nhóm các căn bậc n của 1 trong F. Khi đó μ_n là một nhóm con xyclic của $F^\times$ cấp n với phần tử sinh ζ. Trong phần này, chúng ta sẽ phân loại các mở rộng xyclic cấp n của F.

Xét một trường $E = F[\alpha]$ sinh bởi một phần tử α mà lũy thừa n (nhưng không có lũy thừa nhỏ hơn nào) nằm trong F. Thế thì α là một nghiệm của $X^n - a$, và các nghiệm còn lại là $\zeta^i\alpha$, $1 \leq i \leq n-1$. Vì tất

[6] Đây là Satz 90 trong sách của Hilbert, Theorie der Algebraischen Zahlkorper, 1897. Định lý được phát hiện bởi Kummer trong trường hợp đặc biệt $\mathbb{Q}[\zeta_p]/\mathbb{Q}$, và được phát biểu tổng quát thành Định lý 5.24 bởi E.Noether. Định lý 5.24 , cũng như các tổng quát của nó, cũng được xem như là Định lý Hilbert 90. Để biết thêm về các thảo luận quanh cuốn sách của Hilbert, xem bản giới thiệu trong bản dịch Tiếng Anh (Springer 1998) viết bởi F. Lemmermeyer và N. Schappacher

cả các nghiêm này đều nằm trong E nên E là một mở rộng Galois của F, với nhóm Galois ký hiệu là G. Với mọi $\sigma \in G$, $\sigma\alpha$ cũng là một nghiệm của $X^n - a$, và do vậy $\sigma\alpha = \zeta^i\alpha$ với i nào đó. Do đó $\sigma\alpha/\alpha \in \mu_n$. Ánh xạ

$$\sigma \mapsto \sigma\alpha/\alpha \colon G \to \mu_n$$

không đổi khi thay α bởi một liên hợp, và từ đó suy ra ánh xạ này là một đồng cấu: $\frac{\sigma\tau\alpha}{\alpha} = \frac{\sigma(\tau\alpha)}{\tau\alpha}.\frac{\tau\alpha}{\alpha}$. Vì α sinh ra E trên F nên ánh xạ đó là một đơn ánh. Nếu nó không phải là một toàn ánh thì G có ảnh là một nhóm con μ_d của μ_n, với $d|n, d < n$. Trong trường hợp này, $(\sigma\alpha/\alpha)^d = 1$, tức là $\sigma\alpha^d = \alpha^d$, với mọi $\sigma \in G$ và do vậy $\alpha^d \in F$. Vậy ánh xạ này cũng là một toàn ánh. Ta vừa chứng minh phần đầu tiên của phát biểu sau.

Mệnh đề 5.27. *Cho F là một trường chứa một căn bậc n nguyên thủy của 1, $E = F[\alpha]$ với $\alpha^n \in F$ và không có lũy thừa nhỏ hơn của α nằm trong F. Khi đó E là một mở rộng Galois của F với nhóm Galois xyclic cấp n. Ngược lại, nếu E là một mở rộng xyclic của F bậc n, thì $E = F[\alpha]$ với α nào đó mà $\alpha^n \in F$.*

Chứng minh. Ta chỉ cần chứng minh phát biểu cuối. Giả sử σ sinh ra G và ζ sinh ra μ_n. Ta chỉ cần tìm một phần tử $\alpha \in E^\times$ sao cho $\sigma\alpha = \zeta^{-1}\alpha$, để sau đó $\alpha^n \in F$, và α^n là lũy thừa bé nhất của α nằm trong F. Vì $1, \sigma, \ldots, \sigma^{n-1}$ là các đồng cấu phân biệt $F^\times \to F^\times$, Định lý Dedekind 5.14 chỉ ra rằng $\sum_{i=0}^{n-1} \zeta^i\sigma^i$ khác 0, và do đó có một γ mà $\alpha \stackrel{def}{=} \zeta^i\sigma^i\gamma \neq 0$. Dễ thấy $\sigma\alpha = \zeta^{-1}\alpha$. □

Nhận xét 5.28. *(a) Không khó để chứng minh rằng đa thức $X^n - a$ bất khả quy trong $F[X]$ nếu a không là lũy thừa p đối với mọi số nguyên tố p chia hết n. Khi bỏ điều kiện F chứa một căn bậc n nguyên thủy của 1 thì điều này vẫn đúng ngoại trừ khi nếu $4|n$ thì ta cần thêm điều kiện $a \notin -4F^4$. Xem Lang, Algebra, Springer, 2002, VI, 9, Theorem 9.1, p.297.*

(b) Nếu F có đặc số p (vì thế không có căn bặc p của 1 nào khác 1), thì $X^p - X - a$ bất khả qui trong $F[X]$ ngoại trừ khi $a = b^p - b$ với $b \in F$ nào đó, và khi nó bất khả quy, nhóm Galois của nó là một nhóm xyclic cấp p (sinh bởi $\alpha \mapsto \alpha + 1$ với α là một nghiệm). Hơn nữa, mọi mở rộng của F xyclic bậc p đều là trường phân rã của một đa thức như vậy.

Mệnh đề 5.29. *Cho F là một trường chứa một căn bậc n nguyên thủy của 1. Hai mở rộng xyclic $F[a^{\frac{1}{n}}]$ và $F[b^{\frac{1}{n}}]$ của F bậc n bằng nhau nếu và chỉ nếu $a = b^r c^n$ với $r \in \mathbb{Z}$, nguyên tố cùng nhau với n và $c \in F^\times$, tức là , nếu và chỉ nếu a và b sinh ra cùng một nhóm con của $F^\times/F^{\times n}$.*

Chứng minh. Chỉ có vế "chỉ nếu" cần chứng minh. Ta đã có $F[\alpha] = F[\beta]$ với $\alpha^n = a$ và $\beta^n = b$. Giả sử σ là phần tử sinh của nhóm Galois với $\sigma\alpha\zeta\alpha$, và đặt $\sigma\beta = \zeta^i\beta$, $(i, n) = 1$. Ta có thể viết

$$\beta = \sum_{j=0}^{n-1} c_j\alpha^j, \quad c_j \in F,$$

và do đó

$$\sigma\beta = \sum_{j=0}^{n-1} c_j\zeta^j\alpha^j.$$

So sánh điều này với $\sigma\beta = \zeta^i\beta$, ta thấy rằng $\zeta^i c_j = \zeta^j c_j$ với mọi j. Vì thế $c_j = 0$ với $j \neq i$, hay $\beta = c_i\alpha^i$.

□

5.8. Lý thuyết Kummer

Trong phần này, ta làm việc với trường F chứa một căn bậc n nguyên thủy của 1. Nói riêng, F hoặc có đặc số 0 hoặc có đặc số p không chia hết n.

Hai mệnh đề ở trên đưa ra một phân loại đầy đủ các mở rộng xyclic của F bậc n. Bây giờ ta sẽ mở rộng kết quả này để phân loại các mở rộng abel có số mũ n.(Nhắc lại rằng một nhóm G có **số mũ** n nếu $\sigma^n = 1$ với mọi $\sigma \in G$ và n là số nguyên dương bé nhất có tính chất đó. Một nhóm abel hữu hạn với số mũ n đẳng cấu với một nhóm con của $(\mathbb{Z}/n\mathbb{Z})^r$ với r nào đó.)

Giả sử E/F là một mở rộng Galois hữu hạn với nhóm Galois G. Từ dãy khớp

$$1 \to \mu_n \to E^\times \xrightarrow{x\mapsto x^n} E^{\times n} \to 1$$

ta thu được một dãy đối đồng điều

$$1 \to \mu_n \to F^\times \xrightarrow{x\mapsto x^n} F^\times \cap E^{\times n} \to H^1(G, \mu_n) \to 1.$$

1 ở vế phải là bởi Định lý Hilbert 90. Từ đó ta thu được một đẳng cấu

$$F^\times \cap E^{\times n}/F^{\times n} \to \mathrm{Hom}(G, \mu_n).$$

Ánh xạ này có thể được mô tả như sau: giả sử a là một phần tử của $F^\times$ mà là một lũy thừa n trong E, $a = \alpha^n$; khi đó a sẽ ánh xạ thành đồng cấu $\sigma \mapsto \frac{\sigma\alpha}{\alpha}$. Nếu G là nhóm abel có số mũ n, thì

$$|\mathrm{Hom}(G, \mu_n)| = (G\colon 1).$$

Định lý 5.30. *Ánh xạ*

$$E \mapsto F^\times \cap E^{\times n}$$

xác định một tương ứng $1-1$ *giữa các mở rộng abel hữu hạn của* F *với số mũ* n *nằm trong một bao đóng đại số cố định* Ω *của* F *và các nhóm con* B *của* $F^\times$ *chứa* $F^{\times n}$ *như là một nhóm con có chỉ số hữu hạn. Mở rộng tương ứng với* B *là* $F[B^{\frac{1}{n}}]$*, trường con nhỏ nhất của* Ω *chứa* F *và một căn bậc* n *của mỗi phần tử của* B*. Nếu* $E \leftrightarrow B$*, thì* $[E : F] = (B : F^{\times n})$*.*

Chứng minh. Với mỗi mở rộng Galois hữu hạn E của F, đặt $B(E) = F^\times \cap E^{\times n}$. Khi đó $E \supset F[B(E)^{\frac{1}{n}}]$, và với mỗi nhóm B chứa $F^{\times n}$ như là một nhóm con chỉ số hữu hạn, $B(F[B^{\frac{1}{n}}]) \supset B$. Do đó,

$$[E : F] \geq [F[B(E)^{\frac{1}{n}}] : F] \geq (B(F([B(E)^{\frac{1}{n}}])) : F^{\times n}) \geq (B(E) : F^{\times n}).$$

Nếu E/F là nhóm abel có số mũ n, thì $[E : F] = (B(E) : F^{\times n})$, và dấu bằng xảy ra từ đầu tới cuối: $E = F[B(E)^{\frac{1}{n}}]$.

Tiếp theo ta xét một nhóm B chứa $F^{\times n}$ như là một nhóm con chỉ số hữu hạn, và đặt $E = F[B^{\frac{1}{n}}]$. E là một hợp thành của các mở rộng $F[a^{\frac{1}{n}}]$ với a chạy trên tập hợp các phần tử sinh của $B/F^{\times n}$, và do đó nó là một mở rộng abel hữu hạn số mũ n. Vì vậy,

$$a \mapsto \left(\sigma \mapsto \frac{\sigma a^{\frac{1}{n}}}{a^{\frac{1}{n}}}\right) : B(E)/F^{\times n} \to \mathrm{Hom}(G, \mu_n), \quad G = \mathrm{Gal}(E/F),$$

là một đẳng cấu. Ánh xạ này biến $B/F^{\times n}$ đẳng cấu với một nhóm con của $Hom(G/H, \mu_n)$ của $Hom(G, \mu_n)$ với H chứa $\sigma \in G$ mà $\sigma a^{\frac{1}{n}}/a^{\frac{1}{n}} = 1$ với mọi $a \in B$. Nhưng σ cố định tất cả $a^{\frac{1}{n}}$ với $a \in B$, và do vậy nó là tự đẳng cấu đồng nhất trên $E = F[B^{\frac{1}{n}}]$. Điều này chỉ ra rằng $B(E) = B$, và vì thế $E \mapsto B(E)$ và $B \mapsto F[B^{\frac{1}{n}}]$ là các song ánh ngược. □

Ví dụ 5.31.

(a) Các mở rộng bậc hai của $\mathbb{R}$ *rõ ràng tương ứng* $1-1$ *với các nhóm con của* $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \{\pm 1\}$.

(b) Các mở rộng abel hữu hạn của $\mathbb{Q}$ *với số mũ* 2 *tương ứng* $1-1$ *với các nhóm con hữu hạn của* $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, *là tổng trực tiếp của các nhóm xyclic cấp* 2 *được đánh số bởi các số nguyên tố và* ∞ *(modulo bình phương, mọi số hữu tỷ khác* 0 *có duy nhất một biểu diễn dạng* $\pm p_1 \dots p_r$ *với* p_i *là các số nguyên tố).*

Nhận xét 5.32. *Giả sử* E *là một mở rộng abel hữu hạn của* F *số mũ* n, *và đặt*

$$B(E) = \{a \in F^\times |\ a \text{ trở thành một lũy thừa } n \text{ trong } E\}.$$

Khi đó tồn tại một ghép cặp hoàn hảo

$$(a, \sigma) \mapsto \frac{\sigma a^{\frac{1}{n}}}{a^{\frac{1}{n}}} : \frac{B(E)}{F^{\times n}} \times Gal(E/F) \to \mu_n.$$

Xem Bài tập 2-1 cho trường hợp $n = 2$.

5.9. Chứng minh định lý về tính giải được của Galois

Bổ đề 5.33. *Cho* $f \in F[X]$ *tách được, và* F' *là một mở rộng trường của* F. *Khi đó nhóm Galois của* f *khi coi như một phần tử của* $F'[X]$ *là một nhóm con của nhóm Galois của* f *khi coi như là một phần tử của* $F[X]$.

Chứng minh. Ký hiệu E' là trường phân rã của f trên F', và $\alpha_1, \dots, \alpha_m$ là các nghiệm của $f(X)$ trong E'. Thế thì $E = F[\alpha_1, \dots, \alpha_m]$ là một trường phân rã của f trên F. Mọi phần tử của $\mathrm{Gal}(E'/F')$ hoán vị các α_i và do vậy ánh xạ E thành chính nó. Ánh xạ $\sigma \mapsto \sigma|E$ là một đơn ánh $\mathrm{Gal}(E'/F') \to \mathrm{Gal}(E/F)$. □

Định lý 5.34. *Cho* F *là một trường đặc số* 0. *Một đa thức trong* $F[X]$ *là giải được nếu và chỉ nếu nhóm Galois của nó giải được.*

Chứng minh.

$\Leftarrow$: Giả sử $f \in F[X]$ có nhóm Galois giải được G_f. Đặt $F' = F[\zeta]$ với ζ là một căn bậc n nguyên thủy của 1, n đủ lớn - ví dụ, $n = (\deg f)!$. Bổ đề trên chỉ ra rằng nhóm Galois G của f như là một phần tử của $F'[X]$ là một nhóm con của G_f, và vì thế nó là nhóm giải được (GT 6.6a). Điều này có nghĩa là tồn tại một dãy các nhóm con

$$G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = \{1\}$$

mà mỗi G_i chuẩn tắc trong G_{i-1} và G_{i-1}/G_i là một nhóm xyclic. Gọi E là một trường phân rã của $f(X)$ trên F', và đặt $F_i = E^{G_i}$. Ta có một chuỗi các mở rộng trường

$$F \subset F[\zeta] = F' = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m = E$$

với F_i là mở rộng xyclic trên F_{i-1}. Định lý 5.27 chỉ ra rằng $F_i = F_{i-1}[\alpha_i]$ với $\alpha_i^{[F_i:\, F_{i-1}]} \in F_{i-1}$, với mỗi i, và điều đó chứng tỏ rằng f giải được.

$\Rightarrow$: Ta chỉ cần chứng minh rằng G_f là một nhóm thương của một nhóm giải được (GT 6.6a). Vì thế chỉ cần tìm một mở rộng giải được $\widetilde{E}$ của F mà $f(X)$ chẻ ra trong $\widetilde{E}[X]$.

Ta đã biết rằng tồn tại một tháp các trường

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m$$

thỏa mãn

(a) $F_i = F_{i-1}[\alpha_i], \alpha_i^{r_i} \in F_{i-1}$; và

(b) F_m chứa một trường phân rã của f.

Đặt $n = r_1 \cdots r_m$, và lấy Ω là một trường Galois trên F và chứa (một bản sao của) F_m và một căn bậc n nguyên thủy ζ của 1. Ví dụ, chọn một căn bậc n nguyên thủy γ cho F_m trên F (xem 5.1), và chọn Ω là một trường phân rã của $g(X)(X^n - 1)$ với $g(X)$ là đa thức tối tiểu của γ trên F.

Ký hiệu G là nhóm Galois của Ω/F, và $\widetilde{E}$ là bao đóng Galois của $F_m[\zeta]$ trong Ω. Theo 3.17a, $\widetilde{E}$ là hợp thành của các trường $\sigma F_m[\zeta]$, $\sigma \in G$, và do vậy sinh trên F bởi các phần tử

$$\zeta, \alpha_1, \alpha_2, \ldots, \alpha_m, \sigma\alpha_1, \ldots, \sigma\alpha_m, \sigma'\alpha_1, \ldots$$

Ta thêm các phần tử này vào F để thu được một dãy các trường

$$F \subset F[\zeta] \subset F[\zeta, \alpha_1] \subset \cdots \subset F' \subset F'' \subset \cdots \subset \widetilde{E}$$

trong đó mỗi trường F'' nhận được từ trường đứng trước F' bằng cách thêm một căn bậc r của một phần tử của F' ($r = r_1, \ldots, r_m$, hay n). Theo (5.8) và (5.27) , mỗi mở rộng là abel (và thậm chí là xyclic sau mở rộng thứ nhất), và do vậy $\widetilde{E}/F$ là một mở rộng giải được.

□

Ghi chú 5.35. *Một trong những đóng góp lớn của Galois là chỉ ra rằng một đa thức bất khả quy bậc nguyên tố trong $\mathbb{Q}[X]$ giải được bằng căn thức nếu và chỉ nếu trường phân rã của nó được sinh bởi hai nghiệm bất kỳ của nó* [7]*. Định lý này của Galois đã trả lời một câu hỏi trên mathoverflow năm 2000(mo24081). Với lý thuyết Galois tổng quát, xem mo110727.*

5.10. Đa thức đối xứng

Cho R là một vành giao hoán (có 1). Một đa thức $P(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$ được gọi là **đối xứng** nếu nó không đổi khi các biến của nó được hoán đổi vị trí, tức là nếu

$$P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1, \ldots, X_n) \text{ với mọi } \sigma \in S_n.$$

[7] Pour qu'une équation de degré premier soit résoluble par radicaux, il faut et il suffit que deux quelconques de ces racines étant connues, les autres s'en déduisent rationnellement (Évariste Galois, Bulletin de M. Férussac, XIII (avril 1830), p. 271)

Ví dụ

$$p_1 = \sum_i X_i \qquad = X_1 + \cdots + X_n,$$

$$p_2 = \sum_{i<j} X_i X_j \qquad = X_1X_2 + \ldots X_1X_n + X_2X_3 + \cdots + X_{n-1}X_n,$$

$$p_3 = \sum_{i<j<k} X_iX_jX_k \qquad = X_1X_2X_3 + \ldots$$

$$\ldots$$

$$p_r = \sum_{i_1<\cdots<i_r} X_{i_1} \ldots X_{i_r}$$

$$\ldots$$

$$p_n = X_1X_2 \ldots X_n$$

là các đa thức đối xứng vì p_r là tổng của *tất cả* các đơn thức bậc r tạo ra từ các X_i khác nhau. Các đa thức này được gọi là **đa thức đối xứng sơ cấp.**

Định lý 5.36 (Định lý các đa thức đối xứng)**.** *Mọi đa thức đối xứng $P(X_1, \ldots, X_n)$ trong $R[X_1, \ldots, X_n]$ đều là một đa thức theo các đa thức đối xứng cơ bản với hệ số trong R, tức là , $P \in R[p_1, \ldots, p_n]$.*

Chứng minh. Định nghĩa một thứ tự trên các đơn thức trong X_i như sau

$$X_1^{i_1}X_2^{i_2} \ldots X_n^{i_n} > X_1^{j_1}X_2^{j_2} \ldots X_n^{j_n}$$

nếu hoặc

$$i_1 + i_2 + \cdots + i_n > j_1 + j_2 + \cdots + j_n$$

hoặc dấu bằng xảy ra và đối với một giá trị s nào đó thì

$$i_1 = j_1, \ldots, i_s = j_s, \quad i_{s+1} > j_{s+1}.$$

Ví dụ,

$$X_1X_2X_3^3 > X_1X_2^2X_3 > X_1X_2X_3^2.$$

Giả sử $P(X_1, \ldots, X_n)$ là một đa thức đối xứng, và $X_1^{i_1} \ldots X_n^{i_n}$ là đơn thức cao nhất xuất hiện trong P với hệ số khác 0, do đó

$$P = cX_1^{i_1} \ldots X_n^{i_n} + \text{ đơn thức bậc nhỏ hơn }, c \neq 0.$$

Vì P đối xứng nên nó chứa tất cả các đơn thức thu được từ $X_1^{i_1} \dots X_n^{i_n}$ bằng cách hoán đổi các X_i, Vì vậy $i_1 \geq i_2 \geq \cdots \geq i_n$.

Đơn thức cao nhất trong p_i là $X_1 \dots X_i$, và đơn thức cao nhất trong $p_1^{d_1} \dots p_n^{d_n}$ là

$$X_1^{d_1+\cdots+d_n} X_2^{d_2+\cdots+d_n} \dots X_n^{d_n}. \tag{5.1}$$

Do đó đơn thức cao nhất của

$$P(X_1, \dots, X_n) - c p_1^{i_1-i_2} p_2^{i_2-i_3} \dots p_n^{i_n} \tag{5.2}$$

sẽ nhỏ hơn hẳn đơn thức cao nhất trong $P(X_1, \dots, X_n)$. Ta có thể lặp lại lập luận này với đa thức trong (5.2), và sau một số hữu hạn các bước sẽ thu được biểu diễn của P như là một đa thức trong $p_1, \dots, p_n$. □

Nhận xét 5.37.

(a) Chứng minh của định lý có tính chất thuật toán. Xét ví dụ [8]

$$\begin{aligned} P(X_1, X_2) &= (X_1 + 7X_1X_2 + X_2)^2 \\ &= X_1^2 + 2X_1X_2 + 14X_1^2X_2 + X_2^2 + 14X_1X_2^2 + 49X_1^2X_2^2. \end{aligned}$$

Đơn thức cao nhất là $49X_1^2X_2^2$, và do vậy ta trừ $49p_2^2$, nhận được

$$P - 49p_2^2 = X_1^2 + 2X_1X_2 + 14X_1^2X_2 + X_2^2 + 14X_1X_2^2.$$

Tiếp tục, ta nhận được

$$P - 49p_2^2 - 14p_1p_2 = X_1^2 + 2X_1X_2 + X_2^2$$

và cuối cùng,

$$P - 49p_2^2 - 14p_1p_2 - p_1^2 = 0.$$

(b) Cách viết P như là một đa thức của p_i trong (5.36) là duy nhất. Nếu không, bằng các phép trừ, ta có thể nhận được một đa thức không tầm thường $Q(p_1, \dots, p_n)$ trong p_i, bằng 0 khi được viết như là một đa thức trong X_i. Nhưng các đơn thức cao nhất (5.1) trong các đa thức $p_1^{d_1} \dots p_n^{d_n}$ là phân biệt (ánh xạ $(d_1, \dots, d_n) \mapsto (d_1 + \cdots + d_n, \dots, d_n)$ là đơn ánh), và do vậy chúng không thể loại trừ lẫn nhau.

[8] Từ Wikipedia

Cho

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in R[X],$$

và giả sử rằng f chẻ ra trong một vành S nào đó chứa R:

$$f(X) = \prod_{i=1}^{n}(X - \alpha_i), \quad \alpha_i \in S.$$

Thế thì

$$a_1 = -p_1(\alpha_1, \ldots, \alpha_n), a_2 = p_2(\alpha_1, \ldots, \alpha_n), \ldots, a_n = (-1)^n p_n(\alpha_1, \ldots, \alpha_n)$$

Vì thế các đa thức đối xứng sơ cấp là các nghiệm của $f(X)$ nằm trong R, và do vậy định lý chỉ ra rằng mọi đa thức đối xứng theo các nghiệm của $f(X)$ đều nằm trong R. Ví dụ, biệt thức

$$D(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$$

của f nằm trong R.

Định lý 5.38 (Định lý các hàm đối xứng)**.** *Cho F là một trường. Khi S_n tác động lên $F(X_1, \ldots, X_n)$ bằng cách hoán vị các X_i, trường bất biến là $F(p_1, \ldots, p_n)$.*

Chứng minh. Giả sử $f \in F(X_1, \ldots, X_n)$ đối xứng (cố định bởi S_n). Viết $f = g/h$, $g, h \in F[X_1, \ldots, X_n]$. Các đa thức $H = \prod_{\sigma \in S_n} \sigma h$ và Hf đều đối xứng, và do vậy nằm trong $F[p_1, \ldots, p_n]$ theo 5.36 Suy ra thương $f = Hf/H$ cũng nằm trong $F(p_1, \ldots, p_n)$. □

Hệ quả 5.39. *Trường $F(X_1, \ldots, X_n)$ Galois trên $F(p_1, \ldots, p_n)$ với nhóm Galois S_n (tác động bởi các hoán vị X_i).*

Chứng minh. Ta vừa chứng minh rằng $F(p_1, \ldots, p_n) = F(X_1, \ldots, X_n)^{S_n}$, và do vậy điều phải chứng minh suy ra từ (5.10). □

Trường $F(X_1, \ldots, X_n)$ là trường phân rã trên $F(p_1, \ldots, p_n)$ của

$$g(T) = (T - X_1) \cdots (T - X_n) = X^n - p_1X^{n-1} + \cdots + (-1)^n p_n.$$

Vì thế, nhóm Galois của $g(T) \in F(p_1, \ldots, p_n)$ là S_n.

Ghi chú 5.40. *Các đa thức đối xứng đóng một vai trò quan trọng trong công trình của Galois. Trong Mémoire sur les conditions de résolubilité des équations par radicaux, ông chứng minh mệnh đề sau:*

> *Cho f là một đa thức với các hệ số $\sigma_1, \ldots, \sigma_n$. Cho $x_1, \ldots, x_n$ là các nghiệm của nó, và cho $U, V, \ldots$ là các số nào đó mà là các hàm hữu tỷ theo x_i. Khi đó tồn tại một nhóm G các hoán vị của x_i sao cho các hàm hữu tỷ theo các x_i được giữ cố định dưới tất cả các hoán vị của G chính là các hàm có thể biểu diễn hữu tỷ được thông qua $\sigma_1, \ldots, \sigma_n$ và $U, V, \ldots$*

Khi ta lấy $U, V, \ldots$ là các phần tử của một trường trung gian E nằm giữa các trường hệ số của f và trường phân rã của f, thì phát biểu này nói rằng tồn tại một nhóm G các hoán vị của x_i mà trường bất biến (khi G tác động trên trường phân rã) chính là E.

5.11. Đa thức tổng quát bậc n

Khi ta nói rằng các nghiệm của

$$aX^2 + bX + c$$

là

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

là ta đang nghĩ về a, b, c như là các kí hiệu: với mọi giá trị cụ thể của tồn tại công thức tương tự cho các nghiệm của "đa thức tổng quát" với bậc ≥ 5.

Ta định nghĩa **đa thức bậc n tổng quát** là

$$f(X) = X^n - t_1 X^{n-1} + \cdots + (-1)^{t_n} \in F[t_1, \ldots, t_n][X]$$

ở đó t_i là các ký hiệu. Ta sẽ chứng minh rằng, khi coi f như là một đa thức theo biến X với hệ số trong trường $F(t_1, \ldots, t_n)$, nhóm Galois của nó là S_n. Khi đó Định lý 5.34 chứng minh nhận xét trên (ít nhất trong đặc số 0).

Định lý 5.41. *Nhóm Galois của đa thức bậc n tổng quát là S_n.*

Chứng minh. Cho $f(X)$ là đa thức bậc n tổng quát,

$$f(X) = X^n - t_1X^{n-1} + \cdots + (-1)^n t_n \in F[t_1, \ldots, t_n][X],$$

Nếu ta có thể chứng minh rằng ánh xạ

$$t_i \mapsto p_i : F[t_1, \ldots, t_n] \to F[p_1, \ldots, p_n]$$

là đơn ánh (nghĩa là p_i phụ thuộc đại số trên F) thì nó sẽ mở rộng thành một đẳng cấu

$$F(t_1, \ldots, t_n) \to F(p_1, \ldots, p_n)$$

biến $f(X)$ thành

$$g(X) = X^n - p_1X^{n-1} + \cdots + (-1)^n p_n \in F(p_1, \ldots, p_n)[X].$$

Vì thế phát biểu sẽ suy ra từ Hệ quả 5.39. □

Bây giờ ta sẽ chứng tỏ rằng các p_i độc lập đại số [9]. Giả sử ngược lại, tồn tại một đa thức $P(t_1, \ldots, t_n)$ mà $P(p_1, \ldots, p_n) = 0$. Phương trình (5.1) chỉ ra rằng nếu $m_1(t_1, \ldots, t_n)$ và $m_2(t_1, \ldots, t_n)$ là các đơn thức phân biệt, thì $m_1(p_1, \ldots, p_n)$ và $m_2(p_1, \ldots, p_n)$ có các đơn thức cao nhất khác nhau. Do đó, không thể có khả năng khử lẫn nhau, và $P(t_1, \ldots, t_n)$ phải là đa thức 0.

Nhận xét 5.42. *Do S_n là một nhóm Galois trên $\mathbb{Q}$ và mọi nhóm hữu hạn có thể coi là một nhóm con của S_n nào đó, ta suy ra mọi nhóm hữu hạn đều là một nhóm Galois trên một mở rộng hữu hạn nào đó của $\mathbb{Q}$, nhưng phải chăng mọi nhóm Galois hữu hạn đều xuất hiện như là nhóm Galois trên $\mathbb{Q}$? Câu hỏi này được gọi là bài toán Galois ngược.*

Chương trình Hilbert-Noether để chứng minh khẳng định này là như sau. Hilbert chứng minh rằng nếu G xuất hiện như là nhóm Galois của một mở rộng $E \supset \mathbb{Q}(t_1, \ldots, t_n)$ (t_i là các ký hiệu), thì nó xuất hiện nhiều vô hạn lần như là một nhóm Galois trên $\mathbb{Q}$. Để chứng minh, xem E như là một trường phân rã của một đa thức $f(X) \in k[t_1, \ldots, t_n][X]$ và chứng minh rằng với vô hạn các giá trị của t_i, đa thức thu được trong $\mathbb{Q}[X]$ có nhóm Galois G. (Đây là một định lý khó - xem Serre, J.-P., Lectures on the Mordell-Weil Theorem, 1989, Chapter 9) Noether dự đoán các kết quả sau: Cho $G \subset S_n$ tác động lên $F(X_1, \ldots, X_n)$ bằng cách hoán vị X_i; vậy

[9] Điều này có thể được chứng minh nhờ nhận xét rằng vì $F(X_1, \ldots, X_n)$ đại số trên $F(p_1, \ldots, p_n)$ nên nó phải có bậc siêu việt n (xem Chương 8)

thì $F(X_1, \ldots, X_n)^G \approx F(t_1, \ldots, t_n)$ *(với các ký hiệu* t_i*). Tuy nhiên, Swan đã chứng minh vào năm 1969 rằng phỏng đoán này không đúng với* G *là nhóm xích cấp* 47*. Vì thế hướng tiếp cận này không thể dẫn tới chứng minh rằng mọi nhóm hữu hạn đều xuất hiện như là một nhóm Galois trên* $\mathbb{Q}$*, nhưng nó không loại trừ các cách tiếp cận khác. Để biết thêm thông tin về bài toán này, xem Serre, ibid., Chapter 10; Serre, J.-P., Topics in Galois Theory, 1992; và Wikipedia (Inverse Galois problem)*

Nhận xét 5.43. *Lấy* $F = \mathbb{C}$*, và xét tập con của* $\mathbb{C}^{n+1}$ *xác định bởi phương trình*

$$X^n - T_1 X^{n-1} + \cdots + (-1)^n T_n = 0.$$

Đó là một đa tạp phức S n *chiều. Xét phép chiếu*

$$\pi \colon S \to \mathbb{C}^n, \quad (x, t_1, \ldots, t_n) \mapsto (t_1, \ldots, t_n).$$

Thớ của nó tại một điểm $(a_1, \ldots, a_n)$ *là tập các nghiệm của đa thức*

$$X^n - a_a X^{n-1} + \cdots + (-1)^n a_n.$$

Biệt thức $D(f)$ *của* $f(X) = X^n - T_1 X^{n-1} + \cdots + (-1)^n T_n$ *là một đa thức theo* $\mathbb{C}[T_1, \ldots, T_n]$*. Gọi* Δ *là tập các không điểm của* $D(f)$ *trong* $\mathbb{C}^n$*. Thế thì trên mỗi điểm của* $\mathbb{C} \setminus \Delta$*, có đúng* n *điểm của* S*, và* $S \setminus \pi^{-1}(\Delta)$ *là một không gian phủ trên* $\mathbb{C}^n \setminus \Delta$*.*

VÀI NÉT LỊCH SỬ: Trở lại những 1500 năm trước Công nguyên, người Babylon (ít nhất là) đã biết một công thức chung cho các nghiệm của một đa thức bậc hai. Cardan (khoảng năm 1515 AD) tìm thấy một công thức chung cho các nghiệm của một đa thức bậc ba. Ferrari (khoảng năm 1545 AD) tìm thấy một công thức chung cho những nghiệm của một đa thức bậc bốn (ông giới thiệu giải bậc ba, và sử dụng kết quả của Cardan). Hơn 275 năm tiếp theo đó đã có nhiều nỗ lực không kết quả để tìm công thức tương tự cho các đa thức bằng cấp cao hơn, cho đến khi, vào khoảng năm 1820, Ruffini và Abel đã chứng minh rằng không có công thức chung như vậy.

5.12. Chuẩn và Vết

Nhắc lại rằng, đối với một ma trận $A = (a_{ij})$ cỡ $n \times n$,

$$\begin{aligned}
\mathrm{Tr}(A) &= \sum_i a_{ii} && \text{(vết của } A\text{)} \\
\det(A) &= \sum_{\sigma\in S_n} \mathrm{sign}(\sigma) a_{1\sigma(1)}\dots a_{n\sigma(n)} && \text{(định thức của } A\text{)} \\
c_A(X) &= \det(XI_n - A) && \text{(đa thức đặc trưng của } A\text{)}
\end{aligned}$$

Hơn nữa,

$$c_A(X) = X^n - \mathrm{Tr}(A)X^{n-1} + \dots + (-1)^n \det(A).$$

Giá trị của các đại lượng trên không thay đổi khi A được thay bằng liên hợp UAU^{-1} bởi một ma trận khả nghịch U. Vì thế, với mọi tự đồng cấu α của một không gian véctơ hữu hạn chiều V, ta có thể định nghĩa [10]

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}(A), \det(\alpha) = \det(A), c_\alpha(X) = c_A(X)$$

ở đó A là ma trận của α trong một cơ sở nào đó của V. Nếu β là một tự đồng cấu thứ hai của V,

$$\begin{aligned}
\mathrm{Tr}(\alpha+\beta) &= \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta); \\
\det(\alpha\beta) &= \det(\alpha)\det(\beta).
\end{aligned}$$

Bây giờ, cho E là một mở rộng hữu hạn của F bậc n. Một phần tử α của E xác định một ánh xạ F-tuyến tính

$$\alpha_L \colon E \to E, \quad x \mapsto \alpha x,$$

và ta định nghĩa

$$\begin{aligned}
\mathrm{Tr}_{E/F}(\alpha) &= \mathrm{Tr}(\alpha_L) && \text{(vết của } \alpha\text{)} \\
\mathrm{Nm}_{E/F}(\alpha) &= \det(\alpha_L) && \text{(chuẩn của } \alpha\text{)} \\
c_{\alpha,e/F}(X) &= c_{\alpha L}(X) && \text{(đa thức đặc trưng của } \alpha\text{).}
\end{aligned}$$

Như vậy $\mathrm{Tr}_{E/F}$ là một đồng cấu $(E,+) \to (F,+)$, và $\mathrm{Nm}_{E/F}$ là một đồng cấu $(E^\times,\cdot) \to (F^\times,\cdot)$.

[10] Các hệ số của đa thức đặc trưng

$$c_\alpha(X) = X^n + c_1 X^{n-1} + \dots + c_n$$

của α có các mô tả như sau

$$c_i = (-1)^i \,\mathrm{Tr}(\alpha \mid \wedge^i V)$$

xem Bourbaki, N., Algebra, Chapter 3, 8.11.

Ví dụ 5.44.

(a) Xét mở rộng trường $\mathbb{C} \supset \mathbb{R}$. *Với* $\alpha = a + bi$, *đa thức* α_L *ứng với cơ sở* $\{1, i\}$ *là* $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, *và do vậy*

$$\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(\alpha) = 2\Re(\alpha), \quad \mathrm{Nm}_{\mathbb{C}/\mathbb{R}}(\alpha) = |\alpha|^2.$$

(b) Với $a \in L$, a_L *là một phép nhân bởi một vô hướng. Vì thế*

$$\mathrm{Tr}_{E/F}(a) = na, \quad \mathrm{Nm}_{E/F}(a) = a^n, \quad c_{a,E/F}(X) = (X - a)^n$$

ở đó $n = [E : F]$.

Giả sử $E = \mathbb{Q}[\alpha, i]$ là trường phân rã của $X^8 - 2$. Khi đó E có bậc 16 trên $\mathbb{Q}$, và do vậy để tính vết và chuẩn một phần tử trong E, định nghĩa yêu cầu ta tính vết và chuẩn của một ma trân 16×16. Mệnh đề sau đây cho ta một phương pháp tính nhanh hơn.

Mệnh đề 5.45. *Cho* E/F *là một mở rộng trường hữu hạn, và* $f(X)$ *là đa thức tối tiểu của* $\alpha \in E$. *Khi đó*

$$c_{\alpha,E/F}(X) = f(X)^{[E:\, F[\alpha]]}.$$

Chứng minh. Giả sử $E = F[\alpha]$. Trong trường hợp này, ta phải chứng minh rằng $c_\alpha(X) = f(X)$. Chú ý rằng $\alpha \mapsto \alpha_L$ là một đơn ánh từ E vào vành các tự đồng cấu của F-không gian véctơ E. Định lý Cayley-Hamilton chỉ ra rằng $c_\alpha(\alpha_L) = 0$, và vì thế $c_\alpha(\alpha) = 0$. Do vậy, $f | c_\alpha$, nhưng chúng đều là các đa thức đơn khởi cùng bậc nên phải bằng nhau.

Tổng quát hơn, giả sử $\beta_1, \ldots, \beta_n$ là một cơ sở cho $F[\alpha]$ trên F, và $\gamma_1, \ldots, \gamma_m$ là một cơ sở cho E trên $F[\alpha]$. Như đã thấy trong chứng minh của (1.20), $\{\beta_i \gamma_k\}$ là một cơ sở của E trên F. Viết $\alpha\beta_i = \sum a_{ji}\beta_j$. Khi đó, theo trường hợp đầu đã chứng minh, $A = (a_{ij})$ có đa thức đặc trưng $f(X)$. Nhưng $\alpha\beta_i\gamma_k = \sum a_{ij}\beta_j\gamma_k$, và do vậy ma trận của α_L trương ứng với $\{\beta_i\gamma_k\}$ phân chia thành các khối $n \times n$ với A nằm trên đường chéo và các ma trận 0 nằm ở các vị trí còn lại, từ đó ta suy ra rằng $c_{\alpha L}(X) = c_A(X)^m = f(X)^m$. □

Hệ quả 5.46. *Giả sử các nghiệm của đa thức tối tiểu của α là $\alpha_1, \ldots, \alpha_n$ (trong một trường phân rã chứa E), và $[E\colon F[\alpha]] = m$. Thế thì*

$$\mathrm{Tr}(\alpha) = m\sum_{i=1}^{n}\alpha_i, \quad \mathrm{Nm}_{E/F}\,\alpha = \left(\prod_{i=1}^{n}\alpha_i\right)^m.$$

Chứng minh. Viết đa thức tối tiểu của α là

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_n = \prod(X - \alpha_i),$$

thì

$$a_1 = -\sum \alpha_i, \quad a_n = (-1)^n \prod \alpha_i.$$

Khi đó

$$c_\alpha(X) = (f(X))^m = X^{mn} + ma_1X^{mn-1} + \cdots + a_n^m,$$

với

$$\mathrm{Tr}_{E/F}(\alpha) = -ma_1 = m\sum \alpha_i, \quad \mathrm{Nm}_{E/F}(\alpha) = (-1)^{mn}a_n^m = \left(\prod \alpha_i\right)^m.$$

□

Ví dụ 5.47.

(a) Xét mở rộng $\mathbb{C} \supset \mathbb{R}$. Nếu $\alpha \in \mathbb{C} \setminus \mathbb{R}$, thì

$$c_\alpha(X) = f(X) = X62 - 2\Re(\alpha)X + |\alpha|^2.$$

Nếu $\alpha \in \mathbb{R}$, thì $c_\alpha(X) = (X - a)^2$.

(b) Cho E là trường phân rã của $X^8 - 2$. Khi đó E có bậc 16 trên $\mathbb{Q}$ và nó sinh bởi $\alpha = \sqrt[8]{2}$ và $i = \sqrt{-1}$ (xem Bài tập 16). Đa thức tối tiểu của α là $X^8 - 2$, và do vậy

$$\begin{aligned} c_{\alpha,\mathbb{Q}[\alpha]/\mathbb{Q}}(X) &= X^8 - 2, \\ c_{\alpha,E/\mathbb{Q}}(X) &= (X^2 - 2)^2 \\ \mathrm{Tr}_{\mathbb{Q}[\alpha]/\mathbb{Q}}\,\alpha &= 0, \\ \mathrm{Tr}_{E/\mathbb{Q}}\,\alpha &= 0, \\ \mathrm{Nm}_{\mathbb{Q}[\alpha]/\mathbb{Q}} &= -2, \\ \mathrm{Nm}_{E/\mathbb{Q}}\,\alpha &= 4. \end{aligned}$$

Nhận xét 5.48. *Cho E là một mở rộng tách được của F, và Σ là tập hợp các F-đồng cấu từ E vào một bao đóng đại số Ω của F. Khi đó*

$$\operatorname{Tr}_{E/F}\alpha = \sum_{\sigma\in\Sigma}\sigma\alpha$$
$$\operatorname{Nm}_{E/F}\alpha = \prod_{\sigma\in\Sigma}\sigma\alpha.$$

Khi $E = F[\alpha]$, khẳng định này được suy ra từ 5.46 và quan sát (2.1b) rằng $\sigma\alpha$ là các nghiệm của đa thức tối tiểu $f(X)$ của α trên F. Trong trường hợp tổng quát, $\sigma\alpha$ vẫn là các nghiệm của $f(X)$ trong Ω, nhưng mỗi nghiệm của $f(X)$ xuất hiện $[E\colon F[\alpha]]$ lần (bởi vì mỗi F-đồng cấu $F[\alpha]\to\Omega$ có $[E\colon F[\alpha]]$ mở rộng thành E). Ví dụ, nếu E Galois trên F với nhóm Galois G, thì

$$\operatorname{Tr}_{E/F}\alpha = \sum_{\sigma\in G}\sigma\alpha,$$
$$\operatorname{Nm}_{E/F}\alpha = \prod_{\sigma\in G}\sigma\alpha.$$

Mệnh đề 5.49. *Đối với các mở rộng hữu hạn $E\supset M\supset F$, ta có*

$$\operatorname{Tr}_{M/F}\circ\operatorname{Tr}_{E/M} = \operatorname{Tr}_{E/F},$$
$$\operatorname{Nm}_{M/F}\circ\operatorname{Nm}_{E/M} = \operatorname{Nm}_{E/F}.$$

Chứng minh. Nếu E tách được trên F, thì điều này có thể chứng minh khá dễ dàng bằng việc sử dụng các mô tả trong chú ý trên. Ta bỏ qua chứng minh trong trường hợp tổng quát. □

Mệnh đề 5.50. *Cho $f(X)$ là đa thức đơn khởi bất khả quy với hệ số trong F, và α là một nghiệm của f trong một trường phân rã nào đó của f. Thế thì*

$$\operatorname{disc} f(X) = (-1)^{m(m-1)/2}\operatorname{Nm}_{F[\alpha]/F} f'(\alpha)$$

ở đó f' là đạo hàm hình thức $\frac{df}{dX}$ của f.

Chứng minh. Cho $f(X) = \prod_{i=1}^{m}(X-\alpha_i)$ là một phân tích của f trong

một trường phân rã cho trước của f. Ta có

$$\begin{aligned}\operatorname{disc} f(X) &\overset{def}{=} \prod_{i<j}(\alpha_i-\alpha_j)^2\\ &= (-1)^{m(m-1)/2}.\prod_i\left(\prod_{j\neq i}(\alpha_i-\alpha_j)\right)\\ &= (-1)^{m(m-1)/2}.\prod_i f'(\alpha_i)\\ &= (-1)^{m(m-1)/2}.\operatorname{Nm}_{F[\alpha]/F}(f'(\alpha)) \quad (\text{bởi } 5.48)\end{aligned}$$

□

Ví dụ 5.51. *Ta tính biệt thức của*

$$f(X)=X^n+aX+b, \quad a,b\in F.$$

giả sử rằng nó tách được và bất khả quy, bằng việc tính chuẩn

$$\gamma \overset{def}{=} f'(\alpha)=n\alpha^{n-1}+a, \quad f(\alpha)=0.$$

Nhân phương trình

$$\alpha^n+a\alpha+b=0$$

với $n\alpha^{-1}$ và sắp xếp lại, ta được phương trình

$$n\alpha^{-1}=-na-nb\alpha^{-1}.$$

Vì thế

$$\gamma=n\alpha^{n-1}+a=-(n-1)a-nb\alpha^{-1}.$$

Giải α cho ta

$$\alpha=\frac{-nb}{\gamma+(n-1)a}.$$

Từ hai phương trình cuối, rõ ràng là $F[\alpha]=F[\gamma]$, và do vậy đa thức tối tiểu của γ trên F cũng có bậc n. Nếu ta viết

$$\begin{aligned}f\left(\frac{-nb}{X+(n-1)a}\right)&=\frac{P(X)}{Q(X)}\\ P(X)&=(X+(n-1)a)^n-na(X+(n-1)a)^{n-1}+(-1)^n n^n b^{n-1}\\ Q(X)&=(X+(n-1)a)^n/b,\end{aligned}$$

vậy thì

$$P(\gamma) = f(\alpha).Q(\gamma) = 0.$$

Từ

$$Q(\gamma) = \frac{(\gamma + (n-1)a)^n}{b} = \frac{(-nb)^n}{\alpha^n b} \neq 0$$

và $P(X)$ đơn bậc n, nó phải là đa thức tối tiểu của γ. Vì thế $\mathrm{Nm}\,\gamma$ là $(-1)^n$ lần hằng số của $P(X)$,

$$\mathrm{Nm}\,\gamma = n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n.$$

Vì thế

$$disc(X^n + aX + b) = (-1)^{n(n-1)/2}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n),$$

PARI không làm được tính toán này (bởi vì nó không hiểu các ký hiệu như là các số mũ). Ví dụ,

$$disc(X^5 + aX + b) = 5^5 a^4 + 4^4 a^5.$$

5.13. Bài tập

5-1 Với $a \in \mathbb{Q}$, cho G_a là nhóm Galois của $X^4 + X^3 + X^2 + X + a$. Tìm các số nguyên a_2, a_2, a_3, a_4 sao cho $i \neq j \Longrightarrow G_{a_i}$ không đẳng cấu với G_{a_j}.

5-2 Chứng minh rằng các nghiệm hữu tỷ $a, b \in \mathbb{Q}$ của phương trình Py-ta-go $a^2 + b^2 = 1$ có dạng

$$a = \frac{s^2 - t^2}{s^2 + t^2}, \quad b = \frac{2st}{s^2 + t^2}, \quad s, t \in \mathbb{Q},$$

và dẫn tới rằng mọi tam giác vuông với độ dài các cạnh là các số nguyên có độ dài

$$d(m^2 - n^2, 2mn, m^2 + n^2)$$

với các số nguyên d, m, n (Gợi ý: Sử dụng Định lý Hilbert 90 với mở rộng $\mathbb{Q}[i]/\mathbb{Q}$.)

5-3 Chứng minh rằng một mở rộng hữu hạn của $\mathbb{Q}$ có thể chỉ chứa hữu hạn các căn của 1.

CHƯƠNG 6

Bao đóng đại số

Trong chương này, chúng ta sử dụng bổ đề Zorn để chứng minh rằng mỗi trường F đều có một bao đóng đại số Ω. Nhắc lại rằng nếu F là một trường con của $\mathbb{C}$ thì bao đóng đại số của F trong $\mathbb{C}$ là một bao đóng đại số của F (1.46). Nếu F đếm được thì sự tồn tại của Ω có thể được chứng minh giống như chứng minh đối với trường hữu hạn (4.23), cụ thể là, tập hợp các đa thức đơn khởi bất khả quy trong $F[X]$ là đếm được và có thể liệt kê chúng $f_1, f_2, \ldots$; định nghĩa E_i theo quy nạp bởi $E_0 = F$, E_i là một trường phân rã của f_i trên E_{i-1}; khi đó $\Omega = \cup E_i$ là một bao đóng đại số của F.

Khó khăn trong việc chỉ cho sự tồn tại của một bao đóng đại số của một trường F tùy ý nằm ở lý thuyết tập hợp. Ý tưởng chung ở đây là ta muốn lấy hợp của một họ các trường phân rã tương ứng với các đa thức bất khả quy đơn khởi trong $F[X]$, nhưng cần phải tìm một cách thức thực hiện điều này mà các tiên đề của lý thuyết tập hợp cho phép. Sau khi nhắc lại phát biểu của Bổ đề Zorn, chúng ta sẽ phác thảo ba lời giải [1] cho vấn đề này.

6.1. Bổ đề Zorn

Định nghĩa 6.1.

(a) Một quan hệ $\leq$ trên một tập S là một **thứ tự cục bộ** nếu nó có tính chất phản xạ, bắc cầu, và phản đối xứng ($a \leq b$ và $b \leq a \Rightarrow a = b$).

[1] Tồn tại một cách tự nhiên một số không đếm được các trường không chứa trong $\mathbb{C}$. Ví dụ, trường các chuỗi Laurent hình thức $F((T))$ trên một trường F không đếm được ngay cả khi F hữu hạn.

(b) Một thứ tự cục bộ là một **thứ tự toàn phần** nếu với mọi $s, t \in T$, hoặc $s \leq t$ hoặc $t \leq s$.

(c) Một **chặn trên** của một tập con T của một tập hợp có thứ tự cục bộ $(S, \leq)$ là một phần tử $s \in S$ mà $t \leq s$ với mọi $t \in T$.

(d) Một **phần tử cực đại** của một tập hợp có thứ tự cục bộ S là một phần tử s mà $s \leq s' \Rightarrow s = s'$.

Một tập hợp có thứ tự cục bộ không nhất thiết phải có phần tử lớn nhất, ví dụ, tập hợp các tập con hữu hạn của một tập vô hạn được trang bị thứ tự bởi phép nhúng, nhưng nó không có phần tử lớn nhất.

Bổ đề 6.2 (Zorn)**.** *Cho $(S, \leq)$ là một tập hợp có thứ tự cục bộ khác rỗng mà mọi tập con có thứ tự toàn phần của nó đều có một chặn trên trong S. Khi đó S có một phần tử lớn nhất.*

Bổ đề Zorn [2] tương đương với Tiên đề Chọn, và do vậy độc lập với các tiên đề khác của lý thuyết tập hợp.

Nhận xét 6.3. *Tập hợp S các tập con hữu hạn của một tập vô hạn không mâu thuẫn với Bổ đề Zorn, vì nó chứa các tập con được sắp thứ tự toàn phần nhưng không có chặn trên trong S.*

Mệnh đề sau đây là một ứng dụng điển hình của bổ đề Zorn - chúng ta sẽ sử dụng ký hiệu $*$ để báo hiệu rằng kết quả phụ thuộc vào bổ đề Zorn (hoặc tương đương, phụ thuộc vào Tiên đề Chọn).

Mệnh đề 6.4 (*)**.** *Mọi vành giao hoán A khác 0 có một iđêan cực đại (nghĩa là, cực đại trong số các iđêan **con thực sự**).*

Chứng minh. Gọi S là tập hợp tất cả các iđêan thực sự của A, được sắp thứ tự cục bộ bởi phép nhúng. Nếu T là một tập hợp các iđêan được sắp thứ tự toàn phần thì $J = \cup_{I \in T} I$ lại là một iđêan, và nó là iđêan thực sự vì nếu $I \in J$ thì $1 \in I$ với $I \in T$ nào đó, và I không thể là iđêan thực sự.

[2] Các bình luận sau đây được trích từ A.J. Berrick and M.E. Keating, **An Introduction to Rings and Modules**, 2000: Tên của phát biểu, mặc dù được sử dụng rộng rãi (đầu tiên bởi Lefschetz), nhưng vẫn lôi cuốn sự quan tâm của nhiều nhà sử học (Cambell 1978). Như là một "nguyên lý cực đại" nó được phổ biến và được sử dụng cho các kết quả đại số bởi Zorn năm 1935, và có vẻ như ông không biết đến các sử dụng trước đó trong tôpô, đáng chú ý nhất Kuratowski năm 1922. Zorn cho rằng Artin là người đã nhận ra "bổ đề" thực ra tương đương với Tiên đề Chọn (xem Jech 1973). Đóng góp của Zorn là quan sát thấy bổ đề phù hợp hơn cho các ứng dụng đại số như của ta.

Do vậy J là một chặn trên của T. Từ Bổ đề Zorn, ta suy ra S có một phần tử cực đại, nó là một iđêan cực đại trong A. □

6.2. Chứng minh thứ nhất về sự tồn tại của bao đóng đại số

(Bourbaki, Algèbre, Chap. V, §4.) Một **F-đại số** là một vành chứa F như là một vành con. Giả sử $(A_i)_{i\in I}$ là một họ các F-đại số giao hoán, định nghĩa $\otimes_F A_i$ là thương của F-không gian vectơ với cơ sở $\prod_{i\in I} A_i$ cho các không gian con sinh bởi các phần tử có dạng:

$(x_i)+(y_i)-(z_i)$, ở đó $x_j+y_j=z_j$ với $j\in I$ nào đó và $x_i+y_i\neq z_i$ với mọi $i\neq j$.

$(x_i)=a(y_i)$ ở đó $x_j=ay_j$ với j nào đó trong I và $x_i=y_i$ với mọi $i\neq j$.

(ibid. Chap. II, 3.9) Nó có thể được trang bị một cấu trúc F-đại số giao hoán theo cách tự nhiên nhất, và tồn tại các đồng cấu chính tắc $A_i\to\otimes_F A_i$ của các F-đại số.

Với mỗi đa thức $f\in F[X]$, chọn một trường phân rã E_f, và đặt $\Omega=(\otimes_F E_f)/M$ ở đó M là một iđêan cực đại trong $\otimes_F E_f$ (mà sự tồn tại của M được đảm bảo bởi bổ đề Zorn). Chú ý rằng $F\subset\otimes_F E_f$ và $M\cap F=0$. Do Ω không có iđêan nào khác ngoài (0) và Ω nên nó là một trường (xem 1.2). Hợp thành của các F-đồng cấu $E_f\to\otimes_F E_f\to\Omega$ là một đồng cấu trường nên là một đơn ánh. Vì f chẻ ra trong E_f nên nó phải chẻ ra trong trường lớn hơn Ω. Bao đóng đại số của F trong Ω do vậy là một bao đóng đại số của F (theo 1.44).

Ghi chú 6.5. *Thực ra, có thể chỉ cần lấy $\Omega=(\otimes_F E_f)/M$ ở đó f chạy trên tất cả các đa thức bất khả quy, monic trong $F[X]$ và E_f là trường mầm $F[X]/(f)$ của f (áp dụng phát biểu của 6.7 dưới đây).*

6.3. Chứng minh thứ hai về sự tồn tại của bao đóng đại số

(Jacobson 1964, p 144). Theo 4.23, có thể giả sử F là vô hạn. Điều này cho thấy các trường đại số trên F có cùng lực lương với F (ibid. p143). Chọn một tập không đếm được Ξ gồm các lực lượng lớn hơn lực lượng của F, và đồng nhất F với một tập hợp con của Ξ. Gọi S là tập hợp các bộ ba $(E,+,\cdot)$ ở đó $E\subset\Xi$ và $(+,\cdot)$ là một cấu trúc trường trên

E sao cho $(E, +, \cdot)$ chứa F như là một trường con và đại số trên nó. Ta viết $(E, +, \cdot) \leq (E', +', \cdot')$ nếu vế trái là trường con của vế phải. Theo bổ đề Zorn, S có phần tử cực đại, và sau đó chứng tỏ rằng một phần tử cực đại là đóng đại số. (Xem chi tiết tại ibid. p144)

6.4. Chứng minh thứ ba về sự tồn tại của bao đóng đại số

(Emil Artin.) Xét vành đa thức $F[\ldots, x_f, \ldots]$ theo một họ các ký hiệu x_f, được gắn nhãn bởi các đa thức monic khác hằng $f \in F[X]$. Nếu 1 nằm trong một iđêan I của $F[\ldots, x_f, \ldots]$ sinh bởi các đa thức $f(x_f)$ thì

$$g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n}) = 1 \quad (\text{trong } F[\ldots, x_f, \ldots])$$

với $g_i \in F[\ldots, x_f, \ldots]$ và các đa thức monic khác hằng $f_i \in F[X]$ nào đó. Gọi E là một mở rộng của F mà mỗi $f_i, i = 1, \ldots, n$ có một nghiệm α_i trong E. Dưới F-đồng cấu $F[\ldots, x_f, \ldots] \to E$ ánh xạ

$$\begin{cases} x_{f_1} \mapsto \alpha_i \\ x_f \mapsto 0, \qquad f \notin \{f_1, \ldots, f_n\} \end{cases}$$

quan hệ trên trở thành $0 = 1$. Từ mâu thuẫn này, ta suy ra 1 không thuộc I, và do vậy Mệnh đề 6.4 có thể được áp dụng cho $F[\ldots, x_f, \ldots]/I$ để suy ra rằng I được chứa trong một iđêan cực đại M của $F[\ldots, x_f, \ldots]$. Đặt $\Omega = F[\ldots, x_f, \ldots]/M$. Khi đó Ω là một trường chứa (một bản sao của) F mà mọi đa thức khác hằng trong $F[X]$ có ít nhất một nghiệm. Lặp lại quá trình trên, nhưng bắt đầu với E_1 thay cho F để thu được trường E_2. Tiếp tục theo cách đó để thu được một dãy các trường

$$F = E_0 \subset E_1 \subset E_2 \subset \ldots,$$

và đặt $E = \cup_i E_i$. Khi đó E là đóng đại số bởi vì hệ số của mỗi đa thức khác hằng g trong $E[X]$ nằm trong E_i với một i nào đó, và do vậy g có một nghiệm nằm trong E_{i+1}. Như vậy, bao đóng đại số của F trong E là một bao đóng đại số của F (1.46).

Ghi chú 6.6. *Trường E đại số trên F. Thật vậy, chú ý rằng E_1 được sinh bởi các phần tử đại số trên F, và do vậy nó đại số trên F (áp dụng 1.45). Tương tự, E_2 đại số trên E_1, và do vậy trên F (áp dụng 1.31b). Tiếp tục như vậy, ta thấy rằng mọi phần tử của mỗi E_i đại số trên F.*

Ghi chú 6.7. *Thực ra, E_1 đã là một trường đóng đại số (do vậy là bao đóng đại số trên F). Điều này được suy ra từ khẳng định:*

> *Cho Ω là một trường. Nếu Ω đại số trên một trường con F và mọi đa thức khác hằng số trong $F[X]$ có một nghiệm trong Ω, thì Ω là đóng đại số.*

Để chứng minh điều này, ta cần chỉ ra rằng mọi đa thức bất khả quy f trong $F[X]$ chẻ ra trong $\Omega[X]$ (xem 1.44). Đầu tiên, giả sử rằng f tách được, và E là trường phân rã của f. Theo Định lý 5.1, $E = F[\gamma]$ với γ thuộc E nào đó. Gọi $g(X)$ là đa thức tối tiểu của γ trên F. Khi đó $g(X)$ có các hệ số trong F, và nó có một nghiệm β trong Ω. Cả $F[\gamma]$ và $F[\beta]$ đều là các trường mầm của g, và do vậy có một F-đẳng cấu $F[\gamma] \to F[\beta] \subset \Omega$. Vì f chẻ ra trên $F[\gamma]$ nên nó phải chẻ ra trên Ω.

Lập luận trên là chứng minh đầy đủ nếu F hoàn hảo. Nếu không thì F có đặc số $p \neq 0$, và ta đặt F' là tập hợp tất cả các phần tử x của Ω mà $x^{p^m} \in F$ với m nào đó. Dễ thấy rằng F' là một trường, và ta sẽ hoàn tất chứng minh bằng bổ đề sau khi chứng tỏ được rằng: (a) F' là hoàn hảo, và (b) Mọi đa thức trong $F'[X]$ có nghiệm trong Ω.

Chứng minh (a). *Giả sử $a \in F'$ và $b \overset{def}{=} a^{p^m} \in F$ với m nào đó. Đa thức $X^{p^{m+1}} - b$ có hệ số trong F, và do vậy có nghiệm $\alpha \in \Omega$, tự động nằm trong F'. Bây giờ $\alpha^{p^{m+1}} = a^{p^m}$, dẫn tới $\alpha^p = a$, bởi vì ánh xạ lũy thừa p là đơn ánh trong các trường đặc số p.*

Trước khi tiếp tục, ta chú ý rằng, vì Ω đại số trên một trường hoàn hảo F' nên bản thân nó là hoàn hảo: cho $a \in \Omega$ và g là đa thức tối tiểu của a trên F'; nếu $X^p - a$ bất khả qui trong $\Omega[X]$, thì $g(X^p)$ bất khả qui trong $F'[X]$, nhưng nó không tách được, và đó là một nghịch lý. ***Chứng minh (b).*** *Giả sử $f(X) \in F'[X]$, đặt $f(X) = \sum_i a_i X^i, a_i \in F'$. Với m nào đó, đa thức $\sum_i a_i^{p^m} X^i$ có hệ số trong F, và do vậy có nghiệm $\alpha \in \Omega$. Vì Ω hoàn hảo, ta có thể viết $\alpha = \beta^{p^m}$ với $\beta \in \Omega$. Khi đó*

$$(f(\beta))^{p^m} = (\sum_i a_i \beta^i)^{p^m} = \sum_i a_i^{p^m} \alpha^i = 0,$$

và do vậy β là một nghiệm của f.

6.5. Tính (không) duy nhất của các bao đóng đại số

Định lý 6.8 (*). *Cho Ω là một bao đóng đại số của F và E là một mở rộng đại số của F. Khi đso tồn tại một F-đồng cấu $E \to \Omega$, và, nếu E cũng là một bao đóng đại số của F, thì mọi đồng cấu đó là đẳng cấu.*

Chứng minh. Đầu tiên, giả sử E là sinh đếm được trên F; tức là $E = F\{\alpha_1, \dots, \alpha_n, \dots\}$. Ta có thể thác triển bằng qui nạp ánh xạ nhúng $F \to \Omega$ lên $F[\alpha_1]$ (ánh xạ α_1 tới một nghiệm bất kỳ của đa thức tối tiểu của nó trong Ω), sau đó thác triển tới $F[\alpha_1, \alpha_2]$, và cứ như vậy (xem 2.2).

Trong trường hợp không đếm được, ta dùng bổ đề Zorn. Ký hiệu S là tập hợp các cặp (M, φ_M) với M là một trường $F \subset M \subset E$ và φ_M là một F-đồng cấu $N \to \Omega$. Viết $(M, \varphi_M) \leq (N, \varphi_N)$ nếu $M \subset N$ và $\varphi_N | M = \varphi_M$. Như vậy S trở thành một tập hợp được sắp thứ tự cục bộ. Nếu T là một tập con được sắp thứ tự hoàn toàn của S thì $M' = \cup_{M \in T} M$ là một trường con của E và ta có thể xác định một đồng cấu $\varphi' : M' \to \Omega$ bằng cách đặt $\varphi'(x) = \varphi_M(x)$ nếu $x \in M$. Cặp (M', φ') là một chặn trên của T trong S. Vì vậy, bổ đề Zorn cung cấp cho ta một phần tử cực đại (M, φ) trong S. Giả sử rằng $M \neq E$. khi đó tồn tại một phần tử $\alpha \in E, \alpha \notin M$. Vì α đại số trên M, ta có thể áp dụng 2.2 để mở rộng φ lên $M[\alpha]$, điều này mâu thuẫn với tính cức đại của M. Do vậy $M = E$, và ta hoàn tất chứng minh cho phát biểu thứ nhất.

Nếu E đóng đại số, thì mọi đa thức $f \in F[X]$ chẻ ra trong $E[X]$ và do vậy trong $\varphi(E)[X]$. Cho $\alpha \in \Omega$ và gọi $f(X)$ là đa thức tối tiểu của α. Khi đó $X - \alpha$ là một nhân tử của $f(X)$ trong $\Omega[X]$, nhưng, như ta đã thấy, $f(X)$ chẻ ra trong $\varphi(E)[X]$. Bởi tính phân tích duy nhất, ta suy ra rằng $\alpha \in \varphi(E)$. □

Chứng minh trên là một ứng dụng điển hình của bổ đề Zorn: một khi chúng ta biết làm thế nào để thực hiện một cái gì đó trong một tình huống hữu hạn (hoặc đếm được), bổ đề Zorn cho phép chúng ta làm điều đó trong trường hợp tổng quát.

Nhận xét 6.9. *Ngay cả đối với một trường F hữu hạn, sẽ tồn tại nhiều không đếm được các đẳng cấu từ một bao đóng đại số đến bao đóng đại số khác, không đẳng cấu nào trong số đó là được ưu tiên hơn đẳng cấu khác. Như vậy, sẽ là rất tùy tiện (một cách không đếm được) nếu nói rằng bao đóng đại số của F là duy nhất. Tất cả những gì ta có thể nói*

là: đối với hai bao đóng đại số bất kỳ Ω, Ω' của F thì theo Bổ đề Zorn, tồn tại một F-đẳng cấu $\Omega \to \Omega'$.

6.6. Bao đóng tách được

Cho Ω là một trường chứa F, và $\mathcal{E}$ là một tập hợp các trường trung gian $F \subset E \subset \Omega$ có tính chất sau

(*) với mọi $E_1, E_2 \in \varepsilon$, tồn tại $E \in \varepsilon$ sao cho $E_1, E_2 \subset E$.

Khi đó $E(\mathcal{E}) = \cup_{E \in \varepsilon} E$ là một trường con của Ω (và ta gọi $\cup_{E \in \varepsilon} E$ là một **hợp có hướng**), bởi vì (*) cho thấy mọi tập hữu hạn các phần tử của $E(\mathcal{E})$ đều chứa trong một $E \in \mathcal{E}$, và do đó tích của chúng, tổng, ..., cũng nằm trong $E(\mathcal{E})$.

Ta áp dụng nhận xét này cho tập hợp các trường con E hữu hạn và tách được trên F của Ω. Do hợp của bất kỳ hai trường con đó lại hữu hạn và tách được trên F (so sánh với 3.14), ta thấy rằng hợp L của tất cả các trường con E như vậy là một trường con của Ω. Ta gọi L là **bao đóng tách được** của F trong Ω. Rõ ràng, nó tách được trên F và mọi phần tử của Ω tách được trên F đều nằm trong L. Hơn nữa, vì một mở rộng tách được của một mở rộng tách được cũng là tách được nên Ω thuần không tách được trên L.

Định nghĩa 6.10.

(a) Một trường Ω được gọi là **đóng tách được**[3] nếu mọi đa thức tách được khác hằng trong $\Omega[X]$ đều chẻ ra trong Ω.

(b) Một trường Ω được gọi là **bao đóng tách được**[4] của một trường con F nếu nó tách được và đại số trên F và nó đóng tách được.

Định lý 6.11. *(*)*

(a) Mọi trường đều có một bao đóng tách được.

(b) Cho E là một mở rộng đại số tách được của F, và Ω là một bao đóng đại số tách được của F. Khi đó tồn tại một F-đồng cấu $E \to \Omega$, và nếu E cũng là một bao đóng tách được của F thì mọi đồng cấu như vậy là một đẳng cấu.

[3] separably closed
[4] separable closure

Chứng minh. Thay "đa thức" với "đa thức tách được" trong chứng minh của định lý tương ứng cho bao đóng đại số. Cũng có thể đặt Ω là bao đóng tách được của F trong một bao đóng đại số, và áp dụng các định lý trước. □

Ghi chú 6.12. *Không cần thiết phải dùng toàn bộ Tiên đề Chọn để chứng minh sự tồn tại của các bao đóng đại số và tính duy nhất của chúng sai khác đẳng cấu, mà chỉ cần một tiên đề yếu hơn. Xem Banaschewski, Bernhard. Algebraic closure without choice. Z. Math. Logik Grundlag. Math. 38 (1992), no. 4, 383–385.*

CHƯƠNG 7

Mở rộng Galois vô hạn

Trong chương này, ta sẽ sử dụng Tiền đề chọn. [1]

7.1. Nhóm Tôpô

Định nghĩa 7.1. Một tập hợp G được trang bị một cấu trúc nhóm và một tôpô được gọi là ***nhóm tôpô*** nếu

$$(g,h) \mapsto gh : G \times G \to G,$$
$$g \mapsto g^{-1} : G \to G$$

đều là các ánh xạ liên tục.

Giả sử a là một phần tử của một nhóm tôpô G. Khi đó $a_L\colon\ G \xrightarrow{g\mapsto ag} G$ liên tục bởi vì nó là hợp thành của

$$G \xrightarrow{g\mapsto(a,g)} G \times G \xrightarrow{(g,h)\mapsto gh} G$$

Hơn nữa, nó là một đồng phôi với nghịch đảo là $(a^{-1})_L$. Tương tự, $a_R\colon g \mapsto ga$ và $g \mapsto g^{-1}$ cũng đều là các đồng phôi. Nói riêng, với mọi nhóm con H cuả G, lớp kề aH của H mở hoặc đóng nếu H mở hoặc đóng. Vì phần bù của H trong G là một hợp của những lớp kề như vậy nên điều này chỉ ra rằng H đóng nếu nó mở, và nó mở nếu nó đóng và có chỉ số hữu hạn.

[1] Ta cần giả sử rằng tiền đề chọn để có cảm giác lý thuyết Galois của mở rộng vô hạn. Ví dụ, nó phù hợp lý thuyết tập hợp Zermelo-Fraenkel rằng có một bao đóng đại số L của $\mathbb{Q}$ không có tự đẳng cấu tầm thường. Xem: See: Hodges, Wilfrid, Lauchli's algebraic closure of Q. Math. Proc. Cambridge Philos. Soc. 79 (1976), no. 2, 289–297.

Nhắc lại rằng một ***cơ sở lân cận*** của một điểm x trong một không gian tôpô X là một tập hợp các cân cận $\mathcal{N}$ mà mọi tập con mở U của X chứa x sẽ chứa một phần tử N nào đó của $\mathcal{N}$.

Mệnh đề 7.2. *Cho G là một nhóm tôpô, và $\mathcal{N}$ là một cơ sở lân cận của phần tử trung hòa e của G. Khi đó* [2]

(a) với mọi $N_1, N_2 \in \mathcal{N}$, tồn tại $N' \in \mathcal{N}$ sao cho $e \in N' \subset N_1 \cap N_2$;

(b) với mọi $N \in \mathcal{N}$, tồn tại $N' \in \mathcal{N}$ sao cho $N'N' \subset N$;

(c) với mọi $N \in \mathcal{N}$, tồn tại $N' \in \mathcal{N}$ sao cho $N' \subset N^{-1}$;

(d) với mọi $N \in \mathcal{N}$ và $g \in G$, tồn tại $N' \in \mathcal{N}$, sao cho $N' \subset gNg^{-1}$;

(e) với mọi $g \in G$, $\{gN \mid N \in \mathcal{N}\}$ là một cơ sở lân cận của g.

Ngược lại, nếu G là một nhóm và $\mathcal{N}$ là một tập hợp khác rỗng các tập con của G thỏa mãn (a, b, c, d), thì tồn tại (duy nhất) một tôpô trên G thỏa mãn (e).

Chứng minh. Nếu $\mathcal{N}$ là một cơ sở lân cận tại e trong một nhóm tôpô G, thì (b), (c), và (d) lần lượt là các hệ quả của tính liên tục của $(g, h) \mapsto gh, g \mapsto g^{-1}$, và $h \mapsto ghg^{-1}$, tương ứng. Hơn nữa, (a) là hệ quả của định nghĩa và (e) đúng do g_L là một đồng phôi.

Ngược lại, xét N là một tập hợp khác rỗng các tập con của một nhóm G thỏa mãn các điều kiện (a)-(d). Chú ý rằng từ (a) ta suy ra e nằm trong mọi N thuộc $\mathcal{N}$. Gọi $\mathcal{U}$ là một tập hợp các tập con U của G mà với mọi $g \in U$, tồn tại $N \in \mathcal{N}$ với $gN \subset U$. Tập hợp rỗng và bản thân G nằm trong $\mathcal{U}$, và các hợp của các tập trong $\mathcal{U}$ nằm trong $\mathcal{U}$. Xét $U_1, U_2 \in \mathcal{U}$, và $g \in U_1 \cap U_2$; từ định nghĩa, tồn tại $N_1, N_2 \in \mathcal{N}$ với $gN_1, gN_2 \subset U$. Áp dụng (a) ta thấy có một tập $N' \in \mathcal{N}$ mà $gN' \subset U_1 \cap U_2$, điều này chỉ ra rằng $U_1 \cap U_2 \in \mathcal{U}$. Kết quả là các phần tử của $\mathcal{U}$ là các tập mở của một tôpô trên G. Có thể dễ dàng thấy rằng nó là tôpô duy nhất mà (e) được thỏa mãn.

Tiếp theo ta sử dụng (b) và (d) để chứng tỏ rằng $(g, g') \mapsto gg'$ liên tục. Chú ý rằng các tập $g_1N_1 \times g_2N_2$ tạo thành một cơ sở lân cận cho (g_1, g_2) trong $G \times G$. Do vậy, nếu cho một tập mở $U \subset G$ và một cặp (g_1, g_2) mà $g_1g_2 \in U$, ta phải tìm $N_1, N_2 \in \mathcal{N}$ mà $g_1N_1g_2N_2 \subset U$. Do U

[2] Với các tập con S và S' của G, ta đặt $SS' = \{ss' \mid s \in S, s' \in S'\}$ và $S^{-1} = \{s^{-1} \mid s \in S\}$.

là mở nên tồn tại một tập $N \in \mathcal{N}$ sao cho $g_1 g_2 N \subset U$. Áp dụng (b), ta có một tập N' sao cho $N'N' \subset N$; khi đó $g_1 g_2 N' N' \subset U$. Nhưng do $g_1 g_2 N' N' = g_1 (g_2 N' g_2^{-1}) g_2 N'$, nên ta chỉ cần áp dụng (d) để đạt được một $N_1 \in \mathcal{N}$ sao cho $N_1 \subset g_2 N' g_2^{-1}$.

Cuối cùng, ta sử dụng (c) và (d) để chứng tỏ rằng $g \mapsto g^{-1}$ liên tục. Cho một tập mở $U \subset G$ và một $g \in G$ mà $g^{-1} \in U$, ta phải tìm một tập $N \in \mathcal{N}$ sao cho $gN \subset U^{-1}$. Theo định nghĩa, có một tập $N \in \mathcal{N}$ sao cho $g^{-1}N \subset U$. Từ đó suy ra $N^{-1}g \subset U^{-1}$. Theo (c) ta thấy tồn tại một tập $N' \in \mathcal{N}$ sao cho $N'g \subset U^{-1}$, và theo (d) ta thấy có một tập $N'' \in \mathcal{N}$ sao cho $gN'' \subset g(g^{-1}N'g) \subset U^{-1}$. □

7.2. Tô pô Krull trên nhóm Galois

Nhắc lại (3.9) rằng một mở rộng hữu hạn Ω của F là một mở rộng Galois trên F nếu nó chuẩn tắc và tách được, nghĩa là nếu mọi đa thức bất khả quy $f \in F[X]$ có một nghiệm trong Ω thì có $\deg f$ nghiệm phân biệt trong Ω. Tương tự, ta định nghĩa một mở rộng đại số Ω của F là **Galois** trên F nếu nó chuẩn tắc và tách được. Ví dụ, F^{sep} là một mở rộng Galois của F. Rõ ràng là Ω Galois trên F nếu và chỉ nếu nó là một hợp của các mở rộng Galois hữu hạn.

Mệnh đề 7.3. *Nếu Ω Galois trên F, thì nó là mở rộng Galois trên mọi trường trung gian M.*

Chứng minh. Xét $f(X)$ là một đa thức bất khả quy trong $M[X]$ có một nghiệm a trong Ω. Đa thức tối tiểu f chia hết g (trong $M[X]$), nó cũng phải chẻ ra thành các nhân tử bậc 1 trong $\Omega[X]$. □

Mệnh đề 7.4. *Cho Ω là một mở rộng Galois của F và E là một trường con của Ω chứa F. Khi đó mọi F-đồng cấu $E \to \Omega$ đều thác triển được thành một F-đẳng cấu $\Omega \to \Omega$.*

Chứng minh. Lập luận giống như bổ đề Zorn như trong chứng minh của Định lý 6.8 cho ta thấy mọi F-đồng cấu $E \to \Omega$ mở rộng thành một F-đồng cấu $\alpha : \Omega \to \Omega$. Xét $a \in \Omega$, và f là đa thức tối tiểu của nó trên F. Khi đó Ω chứa chính xác $\deg(f)$ nghiệm của f nên $\alpha(\Omega)$ cũng vậy. Vì thế $a \in \alpha(\Omega)$, suy ra α là toàn ánh. □

Hệ quả 7.5. *Cho $\Omega \supset E \supset F$ như trong Mệnh đề trên. Nếu E ổn định dưới tác động của nhóm* $\mathrm{Aut}(\Omega/F)$*, thì E Galois trên F.*

Chứng minh. Xét $f(X)$ là một đa thức bất khả quy trong $F[X]$, có một nghiệm $a \in E$. Do Ω Galois trên F nên $f(X)$ có $n = \deg(f)$ nghiệm phân biệt $a_1, \ldots, a_n$ trong Ω. Có một F-đẳng cấu $F[a] \to F[a_i] \subset \Omega$ biến a thành a_i (chúng đều là các trường mầm của f), nó mở rộng thành một F-đẳng cấu $\Omega \to \Omega$. Do E ổn định dưới tác động của nhóm $\mathrm{Aut}(\Omega/F)$ nên $a_i \in E$. □

Giả sử Ω là một mở rộng Galois của F và $G = \mathrm{Aut}(\Omega/F)$. Với mỗi tập con S của Ω, ta định nghĩa tập hợp

$$G(S) = \{\sigma \in G \mid \sigma s = s \text{ với mọi } s \in S\}.$$

Mệnh đề 7.6. *Có duy nhất một cấu trúc nhóm tôpô trên G sao cho các tập $G(S)$ tạo thành một cơ sở lân cận của 1. Đối với tôpô này, các tập $G(S)$ với S là G-ổn định tạo thành một cơ sở lân cận của 1 chứa các nhóm con chuẩn tắc mở.*

Chứng minh. Ta sẽ chứng minh rằng tập hợp các tập $G(S)$ thỏa mãn (a,b,c,d) trong 7.2. Nó thỏa mãn (a) vì $G(S_1) \cap G(S_2) = G(S_1 \cup S_2)$. Nó thỏa mãn (b) và (c) vì mỗi tập $G(S)$ là một nhóm. Cho S là một tập con hữu hạn của Ω. Khi đó $F(S)$ là một mở rộng hữu hạn của F, và do vậy chỉ có hữu hạn các F-đồng cấu $F(S) \to \Omega$. Ta thấy $\sigma S = \tau S$ nếu $\sigma|F(S) = \tau|F(S)$, điều này cho thấy $\overline{S} = \bigcup_{\sigma \in G} \sigma S$ là hữu hạn. Bây giờ $\sigma\overline{S} = \overline{S}$ với mọi $\sigma \in G$, và nó dẫn đến $G(\overline{S})$ chuẩn tắc trong G. Do vậy, $\sigma G(\overline{S})\sigma^{-1} = G(\overline{S}) \subset G(S)$, điều này chứng minh (d). Nó cũng chứng minh khẳng định thứ hai. □

Tôpô trên $\mathrm{Aut}(\Omega/F)$ được xây dựng trong mệnh đề được gọi là ***tôpô Krull***. Ta viết $\mathrm{Gal}(\Omega/F)$ cho $\mathrm{Aut}(\Omega/F)$ với tôpô Krull, và nó được gọi là ***nhóm Galois*** của Ω/F. Nhóm Galois của F^{sep} trên F được gọi là ***nhóm Galois tuyệt đối***[3] của F.

[3] Lưu ý rằng nhóm Galois tuyệt đối của F chỉ xác định duy nhất sai khác một tự đẳng cấu trong: nếu F' là một bao đóng đại số khác của F; một đẳng cấu $F' \to F^{\mathrm{sep}}$ sẽ xác định một đẳng cấu $\mathrm{Gal}(F'/F) \to \mathrm{Gal}(F^{\mathrm{sep}}/F)$; một đẳng cấu thứ hai $F' \to F^{\mathrm{sep}}$ sẽ khác với đẳng cấu thứ nhất bởi một phần tử σ của $\mathrm{Gal}(F^{\mathrm{sep}}/F)$, và đẳng cấu $\mathrm{Gal}(F'/F) \to \mathrm{Gal}(F^{\mathrm{sep}}/F)$ mà nó xác định sẽ khác với đẳng cấu ban đầu bởi $\mathrm{inn}(\sigma)$.

Nếu S là một tập hữu hạn ổn định dưới G, thì $F(S)$ là một mở rộng hữu hạn của F ổn định dưới G và do vậy Galois trên F (7.5). Vì thế,

$$\{\mathrm{Gal}(\Omega/E) | E \text{ hữu hạn và Galois trên } F\}$$

là một cơ sở lân cận của 1 bao gồm các nhóm con chuẩn tắc mở.

Mệnh đề 7.7. *Cho Ω Galois trên F. Với mọi trường trung gian E hữu hạn và Galois trên F, ánh xạ*

$$\sigma \mapsto \sigma|E : \mathrm{Gal}(\Omega/F) \to \mathrm{Gal}(E/F)$$

là một toàn ánh liên tục (với tôpô rời rạc trên $\mathrm{Gal}(E/F)$*).*

Chứng minh. Xét $\sigma \in \mathrm{Gal}(E/F)$, và xem nó như một F-đồng cấu $E \to \Omega$. Khi đó σ thác triển được thành một F-đẳng cấu $\Omega \to \Omega$ (xem 7.4), điều đó chỉ ra rằng ánh xạ trên là một toàn ánh. Với mọi tập hữu hạn S các phần tử sinh của E trên F, $\mathrm{Gal}(\Omega/F) = G(S)$, chứng tỏ nghịch ảnh của $1_{\mathrm{Gal}(E/F)}$ là mở trong G. Bởi tính thuần nhất, điều tương tự cũng đúng cho mọi phần tử của $\mathrm{Gal}(E/F)$. □

Mệnh đề 7.8. *Nhóm Galois G của mở rộng Galois Ω/F là compact và hoàn toàn không liên thông.* [4].

Chứng minh. Trước tiên ta chứng minh rằng G là Hausdorff. Nếu $\sigma \neq \tau$, thì $\sigma^{-1}\tau \neq 1_G$, và do vậy nó di chuyển một vài phần tử của Ω tức là có một $a \in \Omega$ mà $\sigma(a) \neq \tau(a)$. Với mỗi S chứa a bất kỳ, $\sigma G(S)$ và $\tau G(S)$ khác nhau bởi vì các phần tử của chúng tác động khác nhau lên a. Như vậy chúng là các tập con mở phân biệt của G, tương ứng chứa σ và τ.

Tiếp theo, ta chứng minh G compact. Như ta đã chú ý ở trên, nếu S là một tập hữu hạn ổn định dưới G, thì $G(S)$ là một nhóm con chuẩn tắc của G, và nó có chỉ số hữu hạn bởi vì nó là hạt nhân của

$$G \to \mathrm{Sym}(S).$$

Do mọi tập hữu hạn chứa trong một tập hữu hạn ổn định [5] nên lập luận ở trên chứng tỏ rằng ánh xạ

$$G \to \prod_{S \text{ hữu hạn, ổn định dưới } G} G/G(S)$$

[4] Theo Bourbaki, ta yêu cầu các không gian compact là Hausdorff. Một không gian tôpô là ***hoàn toàn không liên thông*** (totally disconnected) nếu các thành phần liên thông của nó là các tập hợp gồm đúng một điểm.

[5] Mỗi phần tử của Ω đại số trên F, và quỹ đạo của nó là tập hợp các liên hợp của nó (các nghiệm của đa thức tối tiểu của nó trên F)

là một đơn cấu. Khi ta cho $\prod G/G(S)$ cấu trúc tôpô tích, tôpô cảm sinh trên G là tôpô có tính chất $G(S)$ tạo thành một cơ sở lân cận của e và do đó là tôpô Krull. Theo định lý Tychonoff, $\prod G/G(S)$ là compact, và do vậy ta chỉ cần chứng tỏ G đóng trong tích. Với mỗi $S_1 \subset S_2$, có hai ánh xạ liên tục $\prod G/G(S) \to G/G(S_i)$ là các phép chiếu lên $G/G(S_1)$ và phép chiếu lên $G/G(S_2)$ theo sau bởi ánh xạ $G/G(S_2) \to G/G(S_1)$. Ký hiệu $E(S_1, S_2)$ là tập con đóng của $\prod G/G(S)$ mà trên đó hai ánh xạ trùng nhau. Khi đó $\bigcap_{S_1 \subset S_2} E(S_1, S_2)$ đóng và bằng ảnh của G.

Cuối cùng, với mỗi tập S hữu hạn, ổn định dưới G, $G(S)$ là một nhóm con mở và do vậy đóng. Do $\bigcap G(S) = \{1_G\}$ nên ta kết luận rằng thành phần liên thông của G chứa 1_G chỉ là $\{1_G\}$. Bởi tính thuần nhất, một phát biểu tương tự đúng cho mọi phần tử của G. □

Mệnh đề 7.9. *Với mọi mở rộng Galois Ω/F ta có $\Omega^{\mathrm{Gal}(\Omega/F)} = F$.*

Chứng minh. Mọi phần tử của Ω/F nằm trong một mở rộng Galois hữu hạn của F, và do vậy điều này suy ra từ tính toàn ánh trong Mệnh đề 7.7. □

Ghi chú 7.10. *Có mệnh đề đảo của Mệnh đề 7.8: mọi nhóm compact hoàn toàn không liên thông đều xuất hiện như là một nhóm Galois của một mở rộng Galois nào đó của các trường đặc số 0 (Douady, A., Cohomologie des groupes compact totalement discontinus (d'après J. Tate), Séminaire Bourbaki 1959/60, no. 189). Tuy nhiên, không phải mọi nhóm như vậy sinh ra như một nhóm Galois tuyệt đối của một trường đặc số 0. Ví dụ, nhóm Galois tuyệt đối của một trường đặc số 0, nếu hữu hạn, phải có cấp bằng 1 hoặc 2* [6].

7.3. Định lý cơ bản của Lý thuyết Galois vô hạn

Mệnh đề 7.11. *Cho Ω Galois trên F, với nhóm Galois G.*

(a) Cho M là một trường con của Ω chứa F. Khi đó Ω Galois trên M, nhóm Galois $\mathrm{Gal}(\Omega/M)$ đóng trong Ω, và $\Omega^{\mathrm{Gal}(\Omega/M)} = M$.

(b) Với mọi nhóm con H của G, $\mathrm{Gal}(\Omega/\Omega^H)$ là bao đóng của H.

[6] Định lý (Artin-Schreier, 1927): Cho E là một trường đóng đại số và F là một trường con thực sự của E với $[E\colon F] < \infty$. Thế thì F đóng thực (real-closed) và $E = F[\sqrt{-1}]$. Xem, ví dụ, Jacobson 1964, Chapter VI.

Chứng minh.

(a) Khẳng định thứ nhất được chứng minh trong (7.3). Với mỗi tập con hữu hạn $S \subset M$, $G(S)$ là một nhóm con mở của G, và vì thế nó đóng. Nhưng $\mathrm{Gal}(\Omega/M) = \bigcap_{S\subset M} G(S)$, và do đó nó cũng đóng. Phát biểu cuối bây giờ được suy ra từ (7.9).

(b) Vì $\mathrm{Gal}(\Omega/\Omega^H)$ chứa H và đóng, nó phải chứa bao đóng $\overline{H}$ của H. Mặt khác, cho $\sigma \in H \setminus \overline{H}$; ta phải chứng minh rằng σ di chuyển một vài phần tử của Ω^H. Bởi vì σ không nằm trong bao đóng của H,

$$\sigma\,\mathrm{Gal}(\Omega/E) \cap H = \varnothing$$

với một mở rộng Galois E nào đó của F trong Ω (bởi vì các tập hợp $\mathrm{Gal}(\Omega/E)$ tạo thành một cơ sở lân cận của 1; xem ở trên). Ký hiệu ϕ là toàn ánh $\mathrm{Gal}(\Omega/F) \to \mathrm{Gal}(E/F)$. Khi đó $\sigma|E \notin \phi H$, và do vậy σ di chuyển một số phần tử của $E^{\phi H} \subset \Omega^H$ (áp dụng 3.11b).

□

Định lý 7.12. *Cho Ω Galois trên F với nhóm Galois G. Các ánh xạ*

$$H \mapsto \Omega^H, \quad M \mapsto \mathrm{Gal}(\Omega/M)$$

là các song ánh nghịch đảo của nhau giữa tập hợp các nhóm con đóng của G và tập hợp các trường trung gian giữa Ω và F:

$$\{\textit{các nhóm con đóng của } G\} \leftrightarrow \{\textit{các trường trung gian } F \subset M \subset \Omega\}.$$

Hơn nữa,

(a) tương ứng làm đảo quan hệ bao hàm: $H_1 \supset H_2 \iff \Omega^{H_1} \subset \Omega^{H_2}$;

(b) một nhóm con đóng H của G là mở nếu và chỉ nếu Ω^H có bậc hữu hạn trên F, trong trường hợp đó $(G : H) = [\Omega^H : F]$;

(c) $\sigma H \sigma^{-1} \leftrightarrow \sigma H$, nghĩa là $\Omega^{\sigma H \sigma^{-1}} = \sigma(\Omega^H)$; $\mathrm{Gal}(\Omega/\sigma M) = \sigma\,\mathrm{Gal}(\Omega/M)\sigma^{-1}$;

(d) một nhóm con đóng H của G là chuẩn tắc nếu và chỉ nếu Ω^H Galois trên F, trong trương hợp đó $\mathrm{Gal}(\Omega^H/F) \simeq G/H$.

Chứng minh. Đối với phát biểu đầu tiên, ta phải chứng minh rằng $H \mapsto \Omega^H$ và $M \mapsto \mathrm{Gal}(\Omega/M)$ là các ánh xạ nghịch đảo.

Xét H là một nhóm con đóng của G. Khi đó Ω Galois trên Ω^H và $\mathrm{Gal}(\Omega/\Omega^H) = H$ (xem 7.11).

Xét M là một trường trung gian. Khi đó $\mathrm{Gal}(\Omega/M)$ là một nhóm con đóng của G và $\Omega^{\mathrm{Gal}(\Omega/M)} = M$ (xem 7.11).

(a) Hiển nhiên ta có:

$$H_1 \supset H_2 \Longrightarrow \Omega^{H_1} \subset \Omega^{H_2} \Longrightarrow \mathrm{Gal}(\Omega/\Omega^{H_1}) \supset \mathrm{Gal}(\Omega/\Omega^{H_2}).$$

Nhưng $\mathrm{Gal}(\Omega/\Omega^{H_i}) = H_i$ (xem 7.11).

(b) Như ta đã nhận xét trước đây, một nhóm con đóng chỉ số hữu hạn trong một nhóm tôpô luôn luôn mở. Do G compact nên ngược lại, một nhóm con mở của G luôn có chỉ số hữu hạn. Xét H là một nhóm con như vậy. Ánh xạ $\sigma \mapsto \sigma|\Omega^H$ xác định một song ánh

$$G/H \to \mathrm{Hom}_F(\Omega^H, \Omega)$$

(áp dụng 7.4) từ đó suy ra điều phải chứng minh.

(c) Với $\tau \in G$ và $\alpha \in \Omega$, $\tau\alpha = \alpha \iff \sigma\tau\sigma^{-1}(\sigma\alpha) = \sigma\alpha$. Do vậy, $\mathrm{Gal}(\Omega/\sigma M) = \sigma\,\mathrm{Gal}(\Omega/M)\sigma^{-1}$, nên $\sigma\,\mathrm{Gal}(\Omega/M)\sigma^{-1} \leftrightarrow \sigma M$.

(d) Giả sử $H \leftrightarrow M$. Từ (c) ta suy ra rằng H chuẩn tắc nếu và chỉ nếu M ổn định dưới tác động của G. Nhưng M ổn định dưới tác động của G nếu và chỉ nếu nó là hợp của các mở rộng hữu hạn của F ổn định dưới G nghĩa là hợp của các mở rộng Galois hữu hạn của G. Ta vừa quan sát rằng một mở rộng là Galois nếu và chỉ nếu nó là hợp của các mở rộng Galois hữu hạn.

□

Nhận xét 7.13. *Giống như trong trường hợp hữu hạn (3.17), ta có thể suy ra các phát biểu sau.*

(a) Cho $(M_i)_{i\in I}$ là một họ (có thể vô hạn) các trường trung gian, và giả sử $H_i \leftrightarrow M_i$. Ký hiệu $\prod M_i$ là trường nhỏ nhất chứa tất cả các M_i; khi đó vì $\bigcap_{i\in I} H_i$ là nhóm con (đóng) lớn nhất chứa trong tất cả H_i nên,

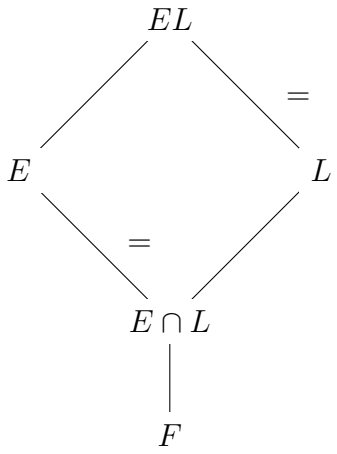
$$\mathrm{Gal}(\Omega/\prod M_i) = \bigcap_{i\in I} H_i.$$

(b) Giả sử $M \leftrightarrow H$. Khi đó nhóm con chuẩn tắc (đóng) lớn nhất chứa trong H là $N = \bigcap_\sigma \sigma H \sigma^{-1}$ (cf. GT 4.10), và do đó Ω^N, là hợp thành của các trường σM, là mở rộng chuẩn tắc nhỏ nhất chứa M.

Mệnh đề 7.14. *Cho E và L là các mở rộng trường của F chứa trong cùng một trường nào đó. Nếu E/F Galois, thì EL/L và $E/E\cap L$ Galois, và ánh xạ*

$$\sigma \mapsto \sigma|E : \mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/E\cap L)$$

là một đẳng cấu của các nhóm tôpô.



Chứng minh. Trước hết ta chứng minh ánh xạ là liên tục. Đặt $G_1 = \mathrm{Gal}(EL/L)$ và $G_2 = \mathrm{Gal}(E/E\cap L)$. Với mỗi tập hữu hạn S các phần tử của E, nghịch ảnh của $G_2(S)$ trong G_1 là $G_1(S)$.

Ta tiếp tục chứng minh rằng ánh xạ là một đẳng cấu nhóm (bỏ qua cấu trúc tôpô). Như trong trường hợp hữu hạn, nó là một đơn cấu (3.18). Gọi H là ảnh của ánh xạ. Khi đó trường bất động của H là $E\cap L$, điều đó suy ra rằng H trù mật trong $\mathrm{Gal}(E/E\cap L)$. Nhưng H đóng bởi vì nó là ảnh liên tục của một không gian compact trong một không gian Hausdorff, và vì thế $H = \mathrm{Gal}(E/E\cap L)$.

Cuối cùng, ta chứng minh rằng nó là mở. Một nhóm con mở của $\mathrm{Gal}(EL/L)$ là đóng (nên compact) có chỉ số hữu hạn; vì thế ảnh của nó trong $\mathrm{Gal}(E/E\cap L)$ compact (và do đó đóng), có chỉ số hữu hạn, và do vậy mở.

□

Hệ quả 7.15. *Cho Ω là một trường đóng đại số chứa F, và cho E và L như trong Mệnh đề. Nếu $\rho\colon E \to \Omega$ và $\sigma\colon L \to \Omega$ là các F-đồng cấu mà $\rho|E \cap L = \sigma|E \cap L$, thì tồn tại một F-đồng cấu $\tau\colon EL \to \Omega$ sao cho $\tau|E = \rho$ và $\tau|L = \sigma$.*

Chứng minh. Theo (7.4), σ thác triển được thành một F-đồng cấu $s : EL \to \Omega$. Có $s|E\cap L = \rho|E\cap L$, ta có thể viết $s|E = \rho\circ\varepsilon$ với $\varepsilon \in \mathrm{Gal}(E/E\cap L)$ nào đó. Theo Mệnh đề,tồn tại duy nhất một $e \in \mathrm{Gal}(EL/L)$ sao cho $e|E = \varepsilon$. Xác định $\tau = s \circ e^{-1}$. □

Ví dụ 7.16. *Cho Ω là một bao đóng đại số của trường hữu hạn $\mathbb{F}_p$. Khi đó $G = \mathrm{Gal}(\Omega/\mathbb{F}_p)$ chứa một phần tử Frobenius chính tắc, $\sigma = (a \mapsto a^p)$, và nó được sinh bởi phần tử này như là một nhóm tôpô tức là G là bao đóng của $\langle\sigma\rangle$. Bây giờ ta sẽ xác định cấu trúc của G.*

Trang bị cho $\mathbb{Z}$ một tôpô sao cho các nhóm $n\mathbb{Z}$, $n \geq 1$ tạo thành một hệ cơ sở các lân cận của 0. Như thế thì hai số nguyên là gần nhau nếu hiệu của chúng chia hết cho một số nguyên lớn.

Giống như với một nhóm tôpô bất kỳ, ta có thể làm đầy[7] *$\mathbb{Z}$ trong tôpô này. Một dãy Cauchy trong $\mathbb{Z}$ là một dãy $(a_i)_{i\geq 1}$, $a_i \in \mathbb{Z}$, thỏa mãn các điều kiện sau đây: với $n \geq 1$, tồn tại một số nguyên N sao cho $a_i \equiv a_j \mod n$ với mọi $i, j > N$. Ta nói một dãy Cauchy trong $\mathbb{Z}$ là tầm thường nếu $a_i \to 0$ khi $i \to \infty$ tức là nếu với mọi $n \geq 1$, tồn tại một số N mà $a_i \equiv 0 \mod n$ với mọi $i > N$. Các dãy Cauchy lập thành một nhóm giao hoán, và các dãy Cauchy tầm thường tạo thành một nhóm con. Ta định nghĩa $\widehat{\mathbb{Z}}$ là thương của nhóm thứ nhất cho nhóm thứ hai. Nó có một cấu trúc vành, và ánh xạ biến $m \in \mathbb{Z}$ thành dãy hằng $m, m, m, \ldots$ đồng nhất $\mathbb{Z}$ với một nhóm con của $\widehat{\mathbb{Z}}$.*

Cho $\alpha \in \widehat{\mathbb{Z}}$ được biểu diễn bởi dãy Cauchy (a_i). Hạn chế của phần tử Frobenius σ lên $\mathbb{F}_{p^n}$ có cấp n. Vì thế $(\sigma|\mathbb{F}_{p^n})^{a_i}$ độc lập với i nếu nó đủ lớn, và ta có thể định nghĩa $\sigma^\alpha \in \mathrm{Gal}(\Omega/\mathbb{F}_p)$ sao cho với mỗi n, $\sigma^\alpha|\mathbb{F}_{p^n} = (\sigma|\mathbb{F}_{p^n})^{a_i}$ với mọi i đủ lớn (phụ thuộc vào n). Ánh xạ $\alpha \mapsto \sigma^\alpha\colon \widehat{\mathbb{Z}} \to \mathrm{Gal}(\Omega/\mathbb{F}_p)$ là một đẳng cấu.

Nhóm $\widehat{\mathbb{Z}}$ không đếm được. Với phần lớn các nhà giải tích thì nó khá khó hiểu - các thành phần liên thông của nó là các tập một điểm. Với các nhà lý thuyết số thì điều này khá tự nhiên - định lý số dư Trung hoa

[7] complete

chỉ ra rằng nó đẳng cấu với $\prod_{p \text{ nguyên tố}} \mathbb{Z}_p$ *ở đó* $\mathbb{Z}_p$ *là vành các số nguyên p-adic.*

Ví dụ 7.17. *Gọi* $\mathbb{Q}^{al}$ *là bao đóng đại số của* $\mathbb{Q}$ *trong* $\mathbb{C}$. $\mathrm{Gal}(\mathbb{Q}^{al}/\mathbb{Q})$ *là một trong những đối tượng cơ bản, và không thể tiếp cận được của toán học.Người ta tin rằng mọi nhóm hữu hạn đều có thể xem là một nhóm thương của nó. Điều này đã được biết, ví dụ, với* S_n *và mọi nhóm đơn sporadic ngoại trừ* M_{23}. *Xem (5.42) và mo80359.*

Mặt khác, ta hiểu được $\mathrm{Gal}(F^{ab}/F)$ *ở đó* $F \subset \mathbb{Q}^{al}$ *là một mở rộng hữu hạn của* $\mathbb{Q}$ *và* F^{ab} *là hợp của tất cả các mở rộng abel hữu hạn của F chứa trong* $\mathbb{Q}^{al}$. *Ví dụ,* $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \simeq \widehat{\mathbb{Z}}^{\times}$. *Đây chính là lý thuyết trường lớp abel - xem giáo trình của tôi về Class Field Theory.*

Ghi chú 7.18. *Một* ***tương ứng Galois đơn*** *là một hệ bao gồm hai tập hợp được sắp thứ tự cục bộ P và Q và các ánh xạ ngược chiều* $f\colon P \to Q$ *và* $g\colon Q \to P$ *sao cho* $gf(p) \geq p$ *với mọi* $p \in P$ *và* $fg(q) \geq q$ *với mọi* $q \in Q$. *Thế thì* $fgf = f$, *bởi vì* $fg(fp) \geq fp$ *và* $gf(p) \geq p$ *suy ra rằng* $f(gfp) \leq f(p)$ *với mọi* $p \in P$. *Tương tự,* $gfg = g$, *và từ đó suy ra f và g xác định một tương ứng* $1-1$ *giữa các tập hợp* $g(Q)$ *và* $f(P)$.

Đối với mỗi mở rộng Galois Ω *của F, ta thu được một tương ứng Galois bằng cách lấy P là tậ hợp các nhóm con của* $\mathrm{Gal}(\Omega/F)$ *và Q là tập hợp các tập con của* Ω, *và đặt* $f(H) = \Omega^H$ *và* $g(S) = G(S)$. *Do vậy, để chứng minh tương ứng* $1-1$ *trong định lý cơ bản, ta chỉ cần xác định các nhóm con đóng chính là các ảnh qua g và các trường trung gian chính là các ảnh qua f. Điều này đã được làm trong (7.11).*

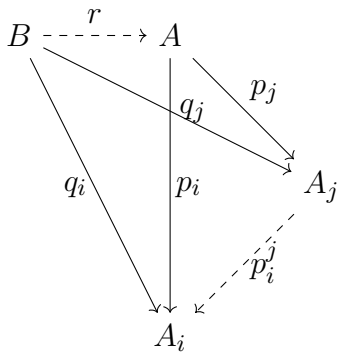
7.4. Nhóm Galois xem như giới hạn ngược

Định nghĩa 7.19. Một thứ tự cục bộ $\leq$ trên một tập hợp I được gọi là ***được định hướng***, và cặp $(I, \leq)$ được gọi là một ***tập hợp được định hướng***, nếu với mọi $i, j \in I$ tồn tại một $k \in I$ sao cho $i, j \leq k$.

Định nghĩa 7.20. Cho $(I, \leq)$ là một tập được định hướng, và C là một phạm trù (ví dụ, phạm trù các nhóm và các đồng cấu, hay phạm trù các nhóm tôpô và các đồng cấu liên tục).

(a) Một ***hệ ngược*** trong C được đánh số bởi $(I, \leq)$ là một họ $(A_i)_{i \in I}$ các vật của C và một họ $(p_i^j\colon A_j \to A_i)_{i \leq j}$ các cấu xạ thỏa mãn $p_i^i = \mathrm{id}_{A_i}$ và $p_i^j \circ p_j^k = p_i^k$ với mọi $i \leq j \leq k$.

(b) Một vật A của C cùng với một họ $(p_j\colon A \to A_j)_{j\in I}$ các cấu xạ thỏa mãn $p_i^j \circ p_j = p_i$ với mọi $i \leq j$ được gọi là một ***giới hạn ngược*** của hệ trong (a) nếu nó có tính chất phổ dụng sau đây: với mọi vật B và họ $(q_j\colon B \to A_j)$ các cấu xạ sao cho $p_i^j \circ q_j = q_i$ với mọi $i \leq j$, tồn tại duy nhất một cấu xạ $r\colon B \to A$ mà $p_j \circ r = q_j$ với j,



Rõ ràng, giới hạn ngược (nếu tồn tại), được xác định duy nhất bởi điều kiện trên, sai khác duy nhất một đẳng cấu. Ta ký hiệu là $\varprojlim(A_i, p_i^j)$, hay chỉ đơn giản là $\varprojlim A_i$.

Ví dụ 7.21. *Cho $(G_i, p_i^j\colon G_j \to G_i)$ là một hệ ngược các nhóm. Đặt*

$$G = \{(g_i) \in \prod G_i \mid p_i^j(g_j) = g_i \text{ với mọi } i \leq j\},$$

và $p_i\colon G \to G_i$ là ánh xạ chiếu. Khi đó $p_i^j \circ p_j = p_i$ chỉ đơn thuần là phương trình $p_i^j(g_j) = g_i$. Nếu (H, q_i) là một họ thứ hai sao cho $p_i^j \circ q_j = q_i$. Ảnh của đồng cấu

$$h \mapsto (q_i(h))\colon H \to \prod G_i$$

nằm trong G, và đó là đồng cấu duy nhất $H \to G$ ánh xạ q_i tới p_i. Vì thế $(G, p_i) = \varprojlim(G_i, p_i^j)$.

Ví dụ 7.22. *Cho $(G_i, p_i^j\colon G_j \to G_i)$ là một hệ ngược các nhóm tôpô và các đồng cấu liên tục. Khi được trang bị tôpô tích, $\prod G_i$ trở thành một nhóm tôpô*

$$G = \{(g_i) \in \prod G_i \mid p_i^j(g_j) = g_i \text{ với mọi } i \leq j\},$$

và G trở thành một nhóm con tôpô với cấu trúc không gian tôpô con. Ánh xạ chiếu p_i liên tục. Nếu H là (H, q_i) là một họ thứ hai sao cho $p_i^j \circ q_j = q_i$. Đồng cấu

$$h \mapsto (q_i(h)) \colon H \to \prod G_i$$

liên tục vì các hợp của nó với các ánh xạ chiếu là liên tục (do tính phổ dụng của tích). Do vậy $H \to G$ liên tục, và điều này chứng tỏ rằng $(G, p_i) = \varprojlim(G_i, p_i^j)$.

Ví dụ 7.23. *Cho $(G_i, p_i^j \colon G_j \to G_i)$ là một hệ ngược các nhóm hữu hạn, và xem nó như một hệ ngược các nhóm tôpô bằng cách cho mỗi G_i một tôpô rời rạc. Một nhóm tôpô G xuất hiện từ một giới hạn ngược của một hệ như thế được gọi là* ***hầu hữu hạn***[8]*.*

Nếu $(x_i) \notin G$, giả sử $p_{i_0}^{j_0}(x_{j_0}) \neq x_{i_0}$, thì

$$G \cap \{(g_j) \mid g_{j_0} = x_{j_0}, g_{i_0} = x_{i_0}\} = \varnothing.$$

Do tập hợp thứ hai là một lân cận mở của (x_i), điều này chỉ ra rằng G đóng trong $\prod G_i$. Theo định lý Tychonoff, $\prod G_i$ là compact, và do vậy G cũng compact. Ánh xạ $p_i \colon G \to G_i$ liên tục, và hạt nhân của nó U_i là một nhóm con mở chỉ số hữu hạn trong G (và do đó là đóng). Vì $\bigcap U_i = \{e\}$, thành phần liên thông của G chứa e chỉ có $\{e\}$. Bởi tính thuần nhất, điều tương tự cũng đúng cho mọi điểm của G: các thành phần liên thông của G là các tập một điểm, G hoàn toàn không liên thông.

Ta vừa chứng minh rằng một nhóm hầu hữu hạn là compact và hoàn toàn không liên thông. Việc chứng minh chiều ngược lại dành cho bạn đọc như một bài tập [9]*.*

Ví dụ 7.24. *Cho Ω là một mở rộng Galois của F. Hợp thành của hai mở rộng Galois hữu hạn trong Ω lại là một mở rộng Galois hữu hạn, và do vậy các mở rộng con Galois hữu hạn của Ω lập thành một tập được định hướng I. Với mỗi E trong I ta có một nhóm hữu hạn $\mathrm{Gal}(E/F)$, và với mỗi $E \subset E'$ ta có một đồng cấu hạn chế $p_E^{E'} \colon \mathrm{Gal}(E/F) \to \mathrm{Gal}(E/F)$. Như vậy, ta thu được một hệ ngược các nhóm hữu hạn $(\mathrm{Gal}(E/F), p_E^{E'})$ đánh số bởi I.*

[8] Một giới hạn ngược cũng được gọi là một giới hạn xạ ảnh (projective limit). Do vậy một nhóm hầu hữu hạn là một giới hạn xạ ảnh của các nhóm hữu hạn.

[9] Cụ thể hơn, nó là Bài tập 3 tiết 7 của Chương 3 trong General Topology của Bourbaki

Với mỗi E, có một đồng cấu hạn chế p_E: $\mathrm{Gal}(\Omega/F) \to \mathrm{Gal}(E/F)$ và, bởi tính phổ dụng của giới hạn ngược, các ánh xạ này xác định một đồng cấu

$$\mathrm{Gal}(\Omega/F) \to \varprojlim \mathrm{Gal}(E/F).$$

Ánh xạ này là một đẳng cấu của các nhóm tôpô. Đây là một phát biểu lại của những gì ta đã trình bày trong chứng minh của (7.8).

7.5. Các nhóm con không mở chỉ số hữu hạn

Ta áp dụng bổ đề Zorn [10] để xây dựng một nhóm con không mở chỉ số hữu hạn trong $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ [11].

Bổ đề 7.25. *Cho V là một không gian véctơ vô hạn chiều. Với mọi $n \geq 1$, tồn tại một không gian con V_n của V sao cho V/V_n có số chiều n.*

Chứng minh. Bổ đề Zorn chỉ ra rằng V chứa các tập con độc lập tuyến tính cực đại, và vì thế sử dụng các lập luận thông thường, một tập con như vậy sinh ra V, nói cách khác nó là một cơ sở. Chọn một cơ sở, và lấy V_n là không gian con sinh bởi tập hợp thu được sau khi bỏ đi n phần tử từ cơ sở. □

Mệnh đề 7.26. *Với mỗi $n \geq 1$, nhóm $\mathrm{Gal}(\mathbb{Q}^{al}/\mathbb{Q})$ có các nhóm con chuẩn tắc không mở chỉ số 2^n.*

Chứng minh. Gọi E là trường con $\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \ldots, \sqrt{p}, \ldots]$, p nguyên tố, của $\mathbb{C}$. Với mỗi p,

$$\mathrm{Gal}(\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \ldots, \sqrt{p}]/\mathbb{Q})$$

là một tích các bản sao của $\mathbb{Z}/2\mathbb{Z}$ đánh số bởi tập hợp {các số nguyên tố $\leq p$} $\cup$ $\{\infty\}$ (áp dụng 5.32; cũng xem thêm 5.51b). Do

$$\mathrm{Gal}(E/\mathbb{Q}) = \varprojlim \mathrm{Gal}(\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \ldots, \sqrt{p}]/\mathbb{Q}),$$

[10] Điều này thực sự cần thiết - xem mo106216.

[11] Điều này trái ngược với: " ... không được biết, thâm chí khi $G = \mathrm{Gal}(\overline{\mathbb{Q}}.\mathbb{Q})$, liệu mọi nhóm con chỉ số hữu hạn trong G là mở; đây là một số vấn đề liên quan tới những bài toán chưa giải được, tất cả đều dường như rất khó". Swinnerton-Dyer, H. P. F., A brief guide to algebraic number theory. Cambridge, 2001, p133

nên nó là tích trực tiếp của các bản sao của $\mathbb{Z}/2\mathbb{Z}$ đánh số bởi các số nguyên tố l của $\mathbb{Q}$ (gồm $l = \infty$) với cấu trúc tôpô tích. Đặt $G = \mathrm{Gal}(E/\mathbb{Q})$, và

$$H = \{(a_l) \in G \mid a_l = 0 \text{ với mọi nhưng hữu hạn } l\}.$$

Đây là một nhóm con của G (Cụ thể hơn, nó là một tổng trực tiếp của các bản sao của $\mathbb{Z}/2\mathbb{Z}$ đánh số bởi các số nguyên tố của $\mathbb{Q}$), và nó trù mật trong G bởi vì [12] rõ ràng là mọi tập con mở của G đều chứa một phần tử của H. Ta có thể xem G/H như một không gian véctơ trên $\mathbb{F}_2$ và áp dụng bổ đề đề để thu được được các nhóm con G_n có chỉ số 2^n trong G chứa H. Nếu G_n mở trong G, thì nó đóng, mâu thuẫn với việc H trù mật. Do đó, G_n không mở, và nghịch ảnh trong $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ là nhóm con [13] thỏa mãn yêu cầu. □

Ghi chú 7.27. *Cho $G = \mathrm{Gal}(\mathbb{Q}^{al}/\mathbb{Q})$. Ta đã chỉ ra trong chứng minh trên rằng có một nhóm con chuẩn tắc đóng $N = \mathrm{Gal}(\mathbb{Q}^{al}/E)$ của G mà G/N là một không gian véctơ trên $\mathbb{F}_2$ không đếm được. Ký hiệu $(G/N)^\vee$ là không gian đối ngẫu của không gian này (cũng không đếm được). Mọi phần tử khác không $f \in (G/N)^\vee$ xác định một toàn ánh $G \to \mathbb{F}_2$ mà hạt nhân của nó là một nhóm con chỉ số 2 của G. Các nhóm con này là phân biệt, và do vậy G có một số không đếm được các nhóm con chỉ số 2. Chỉ có một số đếm được các nhóm con trong chúng mở bởi vì $\mathbb{Q}$ chỉ có một số đếm được các mở rộng bậc hai trong một bao đóng đại số cố định.*

Ghi chú 7.28. *Cho G là một nhóm hầu hữu hạn và hữu hạn sinh như một nhóm tôpô. Một định lý khó mới được chứng minh gần đây phát biểu rằng mọi nhóm con chỉ số hữu hạn trong G là mở (Nikolov, Nikolay; Segal, Dan. On finitely generated profinite groups. I. Strong completeness and uniform bounds. Ann. of Math. (2) 165 (2007), no. 1, 171–238.)*

---

[12] Cho $(a_i) \in G$; thì dãy

$$(a_\infty, 0, 0, 0, \dots), (a_\infty, a_2, 0, 0, \dots), (a_\infty, a_2, a_3, \dots), \dots$$

trong H hội tụ về (a_l).

[13] Nghịch ảnh không mở bởi vì mọi đồng cấu liên tục từ một nhóm compact tới một nhóm tách được là mở. Hoặc có thể lập luận như sau: nếu nghịch ảnh là mở, thì trường bất biến của nó sẽ là một mở rộng không tầm thường E của $\mathbb{Q}$ trong $\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \dots, \sqrt{p}, \dots]$, nhưng khi đó E sẽ bị giữ cố định bởi G_n, trù mật

CHƯƠNG 8

Lý thuyết Galois của đại số étale

Đối với Grothendieck thì việc phân loại các mở rộng trường bằng các nhóm Galois, và việc phân loại các không gian phủ bởi các nhóm cơ bản là hai khía cạnh của cùng một lý thuyết. Trong chương này, ta sẽ diễn đạt lại lý thuyết Galois cổ điển theo quan điểm của Grothendieck. Tôi mặc định rằng bạn đọc đã quen thuộc với ngôn ngữ của lý thuyết phạm trù (Wikipedia: Category theory; Equivalence of categories).

Trong suốt chương này, F là một trường, tất cả các vành và các F-đại số đều giao hoán, và mặc định các tích tenxơ được lấy trên F. Một F-đại số A là hữu hạn nếu nó là hữu hạn sinh khi xem như một F-module.

8.1. Nhắc lại một số kết quả trong đại số giao hoán

Ta sẽ cần tới kết quả cơ bản sau đây trong đại số giao hoán.

Hai iđêan I và J trong một vành A được gọi là **nguyên tố cùng nhau** nếu $I + J = A$. Ví dụ, hai iđêan cực đại phân biệt bất kỳ đều nguyên tố cùng nhau.

Định lý 8.1. *[Định lý phần dư Trung Hoa] Cho $I_1, \dots, I_n$ là các iđêan của một vành A. Nếu I_i nguyên tố cùng nhau với I_j với mọi $i \neq j$, thì ánh xạ*

$$a \mapsto (\dots, a + I_i, \dots) : A \to A/I_1 \times \cdots \times A/I_n \tag{8.1}$$

là một toàn ánh với hạt nhân $\prod I_i$ (do vậy $\prod I_i = \cap I_i$).

Chứng minh. CA 2.12. □

Định lý 8.2. *[Nullstellensatz mạnh] Cho I là một iđêan trong vành đa thức $F[X_1, \dots, X_n]$ và $Z(I)$ ký hiệu là tập các không điểm của I trong*

$(F^{al})^n$. Nếu một đa thức $h \in F[X_1, \ldots, X_n]$ triệt tiêu trên $Z(I)$, thì một lũy thừa nào đó của nó nằm trong I.

Chứng minh. CA 12.8. □

Căn[1] của một iđêan I trong một vành A là tập hợp các phần tử $f \in A$ mà $f^n \in I$ với $n \in \mathbb{N}$ nào đó. Nó lại là một iđêan, và là căn của chính nó.

Căn lũy linh[2] N của A là căn của iđêan (0). Nó bao gồm các phần tử lũy linh trong A. Nếu $N = 0$, thì A được gọi là **rút gọn** [3].

Mệnh đề 8.3. *Cho A là một F-đại số hữu hạn sinh, và I là một iđêan trong A. Căn của I là giao của các iđêan cực đại chứa nó:*

$$rad(I) = \cap\{M \mid M \subset I, M \text{ cực đại}\}.$$

Nói riêng, A là rút gọn nếu và chỉ nếu $\cap\{M \mid M \text{ cực đại}\} = 0$.

Chứng minh. Bởi sự tương ứng giữa các iđêan trong một vành và trong một thương của vành, ta chỉ cần chứng minh điều này cho $A = F[X_1, \ldots, A_n]$.

Bao hàm $rad(I) \subset \cap\{M \mid M \supset I, M$ cực đại$\}$ đúng trong một vành bất kỳ (bởi vì các iđêan cực đại là radical và $rad(I)$ là iđêan radical bé nhất chứa I).

Với chiều ngược lại, cho h nằm trong tất cả các iđêan cực đại chứa I, và cho $(a_1, \ldots, a_n) \in Z(I)$. Ảnh của các ánh xạ

$$f \mapsto f(a_1, \ldots, a_n) : F[X_1, \ldots, X_n] \to F^{al}$$

là một vành con của F^{al} đại số trên F, và do vậy là một trường (xem 1.31a). Do vậy, hạt nhân của ánh xạ là một iđêan cực đại, chứa I, và vì thế chứa h. Điều này chỉ ra rằng $h(a_1, \ldots, a_n) = 0$. Sử dụng định lý mạnh Nullstellensatz ta được $h \in rad(I)$. □

8.2. Đại số étale trên một trường

Định nghĩa 8.4. Một F-đại số A **chéo hóa được** nếu nó đẳng cấu với đại số tích F^n với n nào đó, và nó được goi là **étale**[4] nếu $L \otimes A$ chéo hóa

[1] radical
[2] nilradical
[3] reduced
[4] Đây là một thuật ngữ của Bourbaki. Trong tiếng Pháp, étale nghĩa là dừng, đứng, như triều dừng.

được đối với một trường L nào đó chứa F. Bậc $[A : F]$ của môt F-đại số hữu hạn là số chiều của nó xem như một F-không gian véctơ.

Cho A là một F-đại số hữu hạn. Với mọi tập hữu hạn S các iđêan cực đại trong A, định lý phần dư Trung Hoa (8.1) chỉ ra rằng ánh xạ $A \to \prod_{M\in S} A/M$ là một toàn ánh với hạch $\cap_{M\in S} M$. Nói riêng, $|S| \leq [A\colon F]$, và do vậy A chỉ có hữu hạn các iđêan cực đại. Nếu S là tập hợp tất cả các iđêan cực đại, thì $\cap_{M\in S} M$ là căn lũy linh N của A (8.3), và vì thế A/N là một tích hữu hạn của các trường.

Mệnh đề 8.5. *Các điều kiện sau đây trên một F-đại số hữu hạn A là tương đương:*

(a) A étale;

(b) $L \otimes A$ là rút gọn với mọi trường L chứa F;

(c) A là một tích các mở rộng trường tách được của F.

Chứng minh.

$(a) \Rightarrow (b)$. Giả sử L là một trường chứa F. Theo giả thiết có một trường L' chứa F mà $L' \otimes A$ chéo hóa được. Lấy L" là một trường chứa (các bản sao của) cả L và L' (chẳng hạn, lấy L" là thương của $L \otimes L'$ bởi một iđêan cực đại). Thế thì $L" \otimes A = L" \otimes_{L'} L' \otimes A$ chéo hóa được, và ánh xạ $L \otimes A \to L" \otimes A$ xác định bởi phép nhúng $L \to$ là đơn ánh, và do vậy $L \otimes A$ reduced.

$(b) \Rightarrow (c)$. Ánh xạ $a \mapsto 1 \otimes a\colon A \to L \otimes A$ là đơn ánh nên nếu $L \otimes A$ rút gọn, thì A cũng vậy. Thảo luận phía trên chỉ ra rằng nó là một tích hữu hạn các trường. Giả sử F' là một trong các nhân tử của A. Nếu F' không tách được, thì F có đặc số $p \neq 0$ và vì thế có một phần tử u của F mà đa thức tối tiểu của nó có dạng $f(X^p)$ với $f \in F[X]$ (xem 3.6). Chọn L là trường chứa F sao cho tất cả các hệ số của f là các lũy thừa p của L. Thế thì

$$L \otimes F[u] \simeq L \otimes (F[X]/(f(X^p))) \simeq L[X]/(f(X^p)),$$

không rút gọn bởi vì $f(X^p)$ là một lũy thừa p trong $F[X]$. Vì thế $L \otimes A$ không rút gọn.

$(c) \Rightarrow (a)$. Ta có thể giả sử rằng A là một mở rộng trường tách được của F. Theo Định lý phần tử nguyên thủy (5.1), ta biết rằng $A = F[u]$ với u nào đó. Bởi vì $F[u]$ tách được trên F nên đa thức tối tiểu $f(X)$ của u tách được, có nghĩa là

$$f(X) = \prod (X - u_i), \quad u_i \neq u_j \text{ với } i \neq j,$$

trong một trường phân rã L của f. Bây giờ,

$$L \otimes A \simeq L \otimes F[X]/(f) \simeq L[X]/(f),$$

và theo Định lý phần dư Trung Hoa (8.1),

$$L[X]/(f) \simeq \prod_i L[X]/(X - u_i) \simeq L \times \cdots \times L.$$

□

Hệ quả 8.6. *Một F-đại số A étale nếu và chỉ nếu $F^{sep} \otimes A$ chéo hóa được.*

Chứng minh. Chứng minh (c) suy ra (a) trong (8.5) chỉ ra rằng $L \otimes A$ chéo hóa được nếu một số đa thức tách được chẻ ra trong L. Theo định nghĩa, tất cả các đa thức tách được chẻ ra trong F^{sep}. □

Ví dụ 8.7. *Cho $f \in F[X]$, và $A = F[X]/(f)$ $f = \prod f_i^{m_i}$ ở đó f_i bất khả qui và phân biệt. Theo định lý phần dư Trung Hoa (CA 2.12)*

$$A \simeq \prod_i F[X]/(f_i^{m_i}).$$

F-đại số $F[X]/(f_i^{m_i})$ là một trường nếu và chỉ nếu $m_i = 1$, trong trường hợp này nó là một mở rộng tách được của F nếu và chỉ nếu f_i tách được. Vì thế A là một F-đại số étale nếu và chỉ nếu f là một đa thức tách được.

Mệnh đề 8.8. *Các tích hữu hạn, tích tenxơ, và các thương của các F-đại số chéo hóa được (étale) là chéo hóa được (tương ứng, étale).*

Chứng minh. Đây là điều hiển nhiên với các đại số chéo hóa được, và nó được suy ra từ các đại số étale. □

Hệ quả 8.9. *Hợp thành của một tập hữu hạn các đại số con étale của một F-đại số là étale.*

Chứng minh. Cho A_i là các đại số con étale của B. Thế thì $A_1 \dots A_n$ là ảnh của các ánh xạ

$$a_1 \otimes \cdots \otimes a_n \mapsto a_1 \dots a_n : A_1 \otimes \cdots \otimes A_n \to B,$$

và do vậy là một thương của $A_1 \otimes \cdots \otimes A_n$. □

Mệnh đề 8.10. *Cho A étale trên F, và F' là một trường chứa F. Khi đó $F' \otimes A$ étale trên F'.*

Chứng minh. Cho L thỏa mãn $L \otimes A \simeq L^m$, và cho L' là một trường chứa (các bản sao của) cả L và F'. Thế thì

$$L' \otimes_{F'} (F' \otimes A) \simeq L' \otimes A \simeq L' \otimes_L (L \otimes A) \approx L' \otimes_L L^m \approx (L')^m.$$

□

Nhận xét 8.11. *Cho A là một đại số étale trên F, và viết A như là một tích các trường, $A = \prod_i A_i$. Một phần tử sinh α của A như là một F-đại số là một bộ (α_i) với mỗi α_i là một phần tử sinh của A_i như một F-đại số. Bởi vì mỗi A_i tách được trên F, nên α như vậy tồn tại (5.1). Chọn một α như thế, và lấy $f = \prod_i f_i$ là tích các đa thức tối tiểu của α_i. Thế thì f là một đa thức đơn khởi mà các nhân tử bất khả quy của nó tách được.*

Ngược lại, cho f là một đa thức đơn khởi mà các nhân tử bất khả quy của nó $(f_i)_i$ tách được. Thế thì $A \stackrel{def}{=} \prod_i F[X]/(f_i)$ là một đại số étale trên F với một phần tử sinh chính tắc.

Bằng cách này, ta thu được tương ứng $1-1$ giữa tập các lớp đẳng cấu của các cặp (A, α) bao gồm một F-đại số étale và một phần tử sinh và tập các đa thức đơn khởi mà các nhân tử bất khả quy của nó tách được.

8.3. Phân loại các đại số étale trên một trường

Cố định một bao đóng tách được Ω của F, và cho G là nhóm Galois của Ω trên F. Nhắc lại rằng (Chương 7) đây là một nhóm các F-tự đẳng cấu của Ω, được trang bị tôpô Krull. Cho E là một trường con của Ω,

hữu hạn và Galois trên F. Một lập luận sử dụng bổ đề Zorn chỉ ra rằng ánh xạ

$$\sigma \mapsto \sigma|E \colon G \to Gal(E/F)$$

là toàn ánh. Các nhóm con chuẩn tắc mở của G chính là các hạch của các đồng cấu như vậy, và $G = \lim_{\leftarrow} Gal(E/F)$.

Cho X là một tập hữu hạn với một tác động của G,

$$G \times X \to X.$$

Ta nói rằng tác động là liên tục nếu ánh xạ đó liên tục với tôpô rời rạc trên X và tôpô Krull trên G. Vì X hữu hạn, điều này tương đương với việc nói rằng tác động này phân tích qua $G \to Gal(E/F)$ đối với một trường con nào đó E của Ω hữu hạn và Galois trên F.

Cho A là một F-đại số étale, ký hiệu $\mathcal{F}(A)$ là tập các đồng cấu F-đại số $A \to \Omega$. Khi đó G tác động lên $\mathcal{F}(A)$ thông qua tác động của nó trên G:

$$(\sigma f)(a) = \sigma(f(a)), \quad \sigma \in G, f \in \mathcal{F}(A), a \in A,$$

tức là, $\sigma f = \sigma \circ f$. Tồn tại một mở rộng Galois hữu hạn E của F chứa ảnh của mọi đồng cấu $A \to \Omega$, và tác động của G lên $\mathcal{F}(A)$ phân tích qua $Gal(E/F)$; vì thế nó là liên tục.

Như vậy, $A \rightsquigarrow \mathcal{F}(A)$ là một hàm tử phản biến từ phạm trù các F-đại số étale tới phạm trù các G-tập hợp liên tục hữu hạn.

Ví dụ 8.12. *Cho $A = F[X]/(f)$ với f là một đa thức tách được trong $F[X]$. Thế thì*

$$\mathcal{F}(A) \simeq \{ \text{ nghiệm của } f(X) \text{ trong } \Omega\}.$$

Giả sử rằng A là tích của các F-đại số étale, $A = A_1 \times \cdots \times A_n$. Vì Ω không có ước của không khác không nên mọi đồng cấu $f \colon A \to \Omega$ là bằng 0 trên toàn bộ ngoại trừ một A_i nào đó, và do đó, đưa ra một đồng cấu $A \to \Omega$ thực chất là đưa ra một đồng cấu $A_i \to \Omega$ với i nào đó. Nói cách khác,

$$\mathcal{F}(\prod_i A_i) \simeq \sqcup_i \mathcal{F}(A_i).$$

Nói riêng, với một F-đại số étale $A \simeq \prod_i F_i$,

$$\mathcal{F}(A) \simeq \sqcup_i Hom_{F-\text{đại số}}(F_i, \Omega).$$

Từ Mệnh đề 2.7, ta suy ra rằng $\mathcal{F}(A)$ hữu hạn với bậc $[A : F]$.

Định lý 8.13. *Hàm tử $A \rightsquigarrow \mathcal{F}(A)$ là một tương đương phản biến từ phạm trù các F-đại số étale tới phạm trù các G-tập liên tục hữu hạn.*

Chứng minh thứ nhất. Ta phải chứng minh hai phát biểu sau:

(a) Hàm tử $\mathcal{F}$ hoàn toàn trung thành[5], tức là, với tất cả F-đại số étale A và B, ánh xạ

$$Hom_{F-\text{đại số}}(A, B) \to Hom_{G-\text{tập}}(\mathcal{F}(B), \mathcal{F}(A))$$

là song ánh.

(b) Hàm tử $\mathcal{F}$ gần như là toàn ánh, tức là, mọi G-tập liên tục, hữu hạn đều đẳng cấu với $\mathcal{F}(A)$ với một số F-đại số étale A nào đó.

Cho V là một không gian véctơ trên F, và đặt $V_\Omega = \Omega \otimes_F V$. Khi đó G tác động lên V_Ω thông qua tác động của nó trên Ω, và

$$V \simeq (V_\Omega)^G \stackrel{def}{=} \{v \in V_\Omega \mid \sigma v = v \text{ với mọi } \sigma \in G\}.$$

Để thấy điều này, chọn một F-cơ sở $e = \{e_1, \ldots, e_n\}$ cho V. Khi đó e là một Ω-cơ sở cho V_Ω, và

$$\sigma(a_1 e_1 + \cdots + a_n e_n) = (\sigma a_1)e_1 + \cdots + (\sigma a_n)e_n, \quad a_i \in \Omega.$$

Do đó $a_1 e_1 + \cdots + a_n e_n$ được giữ cố định bởi tất cả $\sigma \in G$ nếu và chỉ nếu $a_1, \ldots, a_n \in F$.

Tương tự, nếu W là một không gian véctơ thứ hai trên F, thì G tác động lên $Hom_{\Omega-\text{tuyến tính}}(V_\Omega, W_\Omega)$ bởi $\sigma\alpha = \sigma \circ \alpha \circ \sigma^{-1}$, và

$$Hom_{F-\text{tuyến tính}}(V, W) \simeq Hom_{\Omega-\text{tuyến tính}}(V_\Omega, W_\Omega)^G. \quad (6)$$

Thật vậy, một lựa chọn của các cơ sở cho V và W xác định một đẳng cấu $Hom_{F-\text{tuyến tính}}(V, W) \simeq M_{m,n}(F)$ (các ma trận $m \times n$ trên F) và $Hom_{\Omega-\text{tuyến tính}}(V_\Omega, W_\Omega) \simeq M_{m,n}(\Omega)$, và G tác động lên $M_{m,n}(\Omega)$. Bây giờ (6) suy ra từ phát biểu hiển nhiên sau đây: $M_{m,n}(F) = M_{m,n}(\Omega)^G$.

Cho A và B là các F-đại số étale. Dưới đẳng cấu

$$Hom_{F\text{tuyến tính}}(A, B) \simeq Hom_{\Omega-\text{tuyến tính}}(A_\Omega, B_\Omega)^G,$$

[5] fully faithful

các đồng cấu F-đại số tương ứng với các đồng cấu Ω-đại số, và do vậy

$$Hom_{F\text{tuyến tính}}(A, B) \simeq Hom_{\Omega-\text{tuyến tính}}(A_\Omega, B_\Omega)^G.$$

Từ (8.6), ta biết rằng A_Ω (resp. B_Ω) là một tích các bản sao của Ω đánh chỉ số bởi các phần tử của $\mathcal{F}(A)$ tương ứng. $\mathcal{F}(B)$). Lấy t là ánh xạ giữa các tập hợp $\mathcal{F}(B) \to \mathcal{F}(A)$. Khi đó

$$(a_i)_{i\in\mathcal{F}(A)} \mapsto (b_j)_{j\in\mathcal{F}(B)}, \quad b_j = a_{t(j)},$$

là một đồng cấu của các Ω-đại số $A_\Omega \to B_\Omega$, và mọi đồng cấu của các Ω-đại số $A_\Omega \to B_\Omega$ có dạng này với duy nhất một t. Nên

$$Hom_{\Omega-\text{đại số}}(A_\Omega, B_\Omega) \simeq Hom_{G-\text{tập}}(\mathcal{F}(B), \mathcal{F}(A)).$$

Đẳng cấu này tương thích với các tác động của G, và do đó

$$Hom_{\Omega-\text{đại số}}(A_\Omega, B_\Omega)^G \simeq Hom_{\text{tập}}(\mathcal{F}(B), \mathcal{F}(A))^G.$$

Nói cách khác,

$$Hom_{F-\text{đại số}}(A, B) \simeq Hom_{G\text{tập}}(\mathcal{F}(B), \mathcal{F}(A)).$$

Điều này chứng minh (a). Với (b), cho S là một G-tập hữu hạn, và cho $S = \sqcup_{i\in I} S_i$ là một phân tích S thành các G-quỹ đạo. Với mỗi i, chọn một $s_i \in S_i$, và cho F_i là trường con của Ω cố định bởi các ổn định hóa của s_i. Khi đó

$$\mathcal{F}(\sqcap_{i\in I} F_i) \simeq S.$$

□

CHỨNG MINH THỨ HAI CỦA ĐỊNH LÝ 8.13

Ta phác thảo chứng minh thứ hai cho định lý. Với một tập hữu hạn S với một tác động liên tục trên G, ta cho

$$\Omega^S = Hom(S, \Omega).$$

Nói cách khác, Ω^S là một tích các bản sao của Ω đánh chỉ số bởi các phần tử của S. Cho G tác động lên Ω^S thông qua tác động của nó lên cả Ω và S:

$$(\gamma f)(\sigma) = \gamma(f(\gamma^{-1}\sigma)), \quad \gamma \in G, \quad f : S \to \Omega, \quad \sigma \in S,$$

Với mọi F-đại số étale A, có một đẳng cấu chính tắc

$$a \otimes c \mapsto (\sigma a.c)_{\sigma \in \mathcal{F}(A)} : \Omega \otimes A \to \Omega^{\mathcal{F}(A)}. \quad (7)$$

Khi ta cho G tác động lên $\Omega \otimes A$ thông qua tác động của nó trên Ω, ánh xạ (7) trở thành đẳng biến. Bây giờ:

(a) với mọi F-đại số étale A,

$$A \simeq (\Omega \otimes A)^G;$$

(b) với mọi tập hữu hạn S với tác động liên tục của G, $(\Omega^S)^G$ là một F-đại số con étale của Ω^S, và

$$\mathcal{F}((\Omega^S)^G) \simeq S.$$

Vì thế, $A \rightsquigarrow \mathcal{F}(A)$ là một tương đương của các phạm trù với tựa nghịch đảo $S \rightsquigarrow (\Omega^S)^G$.

CẢI TIẾN ĐỊNH LÝ 8.13

Cố định một mở rộng Galois Ω của F (hữu hạn hoặc vô hạn), và đặt $G = \mathrm{Gal}(\Omega/F)$. Một F-đại số étale A **chẻ ra** bởi Ω nếu $\Omega \otimes A$ đẳng cấu với một tích các bản sao của Ω. Với một F-đại số như vậy, cho $\mathcal{F}(A) = Hom_{k-\text{đại số}}(A, \Omega)$.

Định lý 8.14. *Hàm tử $A \rightsquigarrow \mathcal{F}(A)$ là một tương đương phản biến từ phạm trù các F-đại số étale chẻ ra bởi Ω tới phạm trù các G-tập hữu hạn.*

Chứng minh. Chứng minh tương tự như chứng minh của Định lý 8.13. Khi Ω là một mở rộng hữu hạn của F, tính "liên tục" có thể bỏ qua. □

PHÁT BIỂU HÌNH HỌC CỦA ĐỊNH LÝ 8.13

Trong mục này, ta giả sử rằng bạn đọc đã quen với khái niệm đa tạp đại số trên một trường F (lược đồ tách hình học rút gọn[6] kiểu hữu hạn trên F). Hàm tử $A \rightsquigarrow Spec(A)$ là một tương đương phản biến từ phạm trù các đại số étale trên F tới phạm trù các đa tạp đại số 0 chiều trên

[6] geometrically-reduced separated scheme

F. Nói riêng, tất cả các đa tạp đại số 0 chiều là affine. Nếu $V = Spec(A)$, thì

$$Hom_{F\text{đại số}}(A, \Omega) \simeq Hom_{Spec(F)}(Spec(\Omega), V) \stackrel{def}{=} V(\Omega)$$

(tập các điểm của V với tọa độ trong Ω).

Định lý 8.15. *Hàm tử $V \rightsquigarrow V(\Omega)$ là một tương đương từ phạm trù các đa tạp đại số 0 chiều trên F tới phạm trù các G-tập hợp liên tục hữu hạn. Qua tương đương này, các đa tạp liên thông tương ứng với các tập hợp tác động truyền dẫn.*

Chứng minh. Kết hợp Định lý 8.13 với tính tương đương $A \rightsquigarrow Spec(A)$. □

8.4. So sánh với lý thuyết không gian phủ

Bạn đọc nên chú ý rằng sự tương tự của (8.13) và (8.15) với phát biểu sau đây:

> Cho F là một không gian tôpô liên thông và đơn liên địa phương, và $\pi\colon \Omega \to F$ là một không gian phủ phổ dụng của F. Ký hiệu G là nhóm các phép biến đổi phủ của Ω/F (sự lựa chọn của $e \in \Omega$ xác định một đẳng cấu của G với nhóm cơ bản $\pi_1(F, \pi e)$). Đối với một không gian phủ E của F, ký hiệu $\mathcal{F}(E)$ là tập hợp các ánh xạ phủ $\Omega \to E$. Thế thì $E \rightsquigarrow \mathcal{F}(E)$ là một tương đương từ phạm trù các không gian phủ của F tới phạm trù các G-tập (với tác động phải).

Để biết thêm thông tin, xem phần về nhóm cơ bản étale trong "Bài giảng về đối đồng điều Étale" của tôi, Szamuely và Tamás, trong Các nhóm Galois và các nhóm cơ bản. CUP, 2009.

CHƯƠNG 9

Mở rộng siêu việt

Trong chương này ta xét các trường $\Omega \supset F$ với Ω lớn hơn F rất nhiều. Chẳng hạn, ta có $\mathbb{C} \supset \mathbb{Q}$.

9.1. Độc lập đại số

Các phần tử $\alpha_1, \ldots, \alpha_n$ của Ω tạo ra một F-đồng cấu

$$f \mapsto f(\alpha_1, \ldots, \alpha_n) : F[X_1, \ldots, X_n] \to \Omega.$$

Nếu hạt nhân của đồng cấu này bằng 0, thì các α_i được gọi là ***độc lập đại số*** trên F, nếu không thì chúng được gọi là ***phụ thuộc đại số*** trên F. Như vậy, các α_i là phụ thuộc đại số trên F nếu tồn tại một đa thức khác không $f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ thỏa mãn $f(\alpha_1, \ldots, \alpha_n) = 0$, và chúng là độc lập đại số nếu

$$a_{i_1,\ldots,i_n} \in F, \quad \sum a_{i_1,\ldots,i_n} \alpha_1^{i_1} \ldots \alpha_n^{i_n} = 0 \Longrightarrow a_{i_1,\ldots,i_n} = 0 \text{ với mọi } i_1, \ldots, i_n.$$

Hãy chú ý sự giống nhau với khái niệm độc lập tuyến tính. Nếu f thuần nhất bậc 1, thì định nghĩa trên trở thành định nghĩa về sự độc lập tuyến tính.

Ví dụ 9.1.

(a) Một phần tử α là độc lập đại số trên F nếu và chỉ nếu nó là phần tử siêu việt trên F.

(b) Các số phức π và e gần như chắc chắn là độc lập đại số trên $\mathbb{Q}$, nhưng điều này vẫn chưa được chứng minh.

*Một tập hợp vô hạn A là **độc lập đại số** trên F nếu mọi tập con hữu hạn của A là độc lập đại số; nếu không, nó là **phụ thuộc đại số** trên F.*

Nhận xét 9.2. *Nếu $\alpha_1, \dots, \alpha_n$ là độc lập đại số trên F, thì ánh xạ*

$$f(X_1, \dots, X_n) \mapsto f(\alpha_1, \dots, \alpha_n) \colon F[X_1, \dots, X_n] \to F[\alpha_1, \dots, \alpha_n]$$

là một đơn ánh, và do vậy là một đẳng cấu. Đẳng cấu này sau đó có thểthác triển tới trường các thương,

$$X_i \mapsto \alpha_i \colon F(X_1, \dots, X_n) \to F(\alpha_1, \dots, \alpha_n).$$

*Trong trường hợp này, $F(\alpha_1, \dots, \alpha_n)$ được gọi là **mở rộng siêu việt thuần**[1] của F. Đa thức*

$$f(X) = X^n - \alpha_1 X^{n-1} + \cdots + (-1)^n \alpha_n$$

có nhóm Galois S_n trên $F(\alpha_1, \dots, \alpha_n)$ (xem 5.41).

Bổ đề 9.3. *Cho $\gamma \in \Omega$ và $a \subset \Omega$. Các điều kiện sau đây là tương đương:*

(a) γ đại số trên $F(A)$;

(b) tồn tại $\beta_1, \dots, \beta_n \in F(A)$ sao cho $\gamma^n + \beta_1 \gamma^{n-1} + \cdots + \beta_n = 0$;

(c) tồn tại $\beta_0, \beta_1, \dots, \beta_n \in F[A]$, không đồng thời bằng 0, sao cho $\beta_0 \gamma^n + \beta_1 \gamma^{n-1} + \cdots + \beta_n = 0$;

(d) tồn tại một đa thức $f(X_1, \dots, X_m, Y) \in F[X_1, \dots, X_m, Y]$ và $\alpha_1, \dots, \alpha_m \in A$ sao cho $f(\alpha_1, \dots, \alpha_m, Y) \neq 0$ nhưng $f(\alpha_1, \dots, \alpha_m, \gamma) = 0$.

Chứng minh. $(a) \Longrightarrow (b) \Longrightarrow (c) \Longrightarrow (a)$ là hiển nhiên.

$(d) \Longrightarrow (c)$. Viết $f(X_1, \dots, X_m, Y)$ như một đa thức theo biến Y với các hệ số trong vành $F[X_1, \dots, X_m]$,

$$f(X_1, \dots, X_m, Y) = \sum f_i(X_1, \dots, X_m) Y^{n-i}.$$

Khi đó (c) đúng với $\beta_i = f_i(\alpha_1, \dots, \alpha_m)$.

$(c) \Longrightarrow (d)$. Các β_i trong (c) có thể viết như là các đa thức theo một số hữu hạn các phần tử $\alpha_1, \dots, \alpha_m$ của A, giả sử $\beta_i = f_i(\alpha_1, \dots, \alpha_m)$ với $f_i \in F[X_1, \dots, X_m]$. Khi đó (d) đúng với $f = \sum f_i(X_1, \dots, X_m) Y^{n-i}$. □

[1] pure transcendental extension

Định nghĩa 9.4. Khi γ thỏa mãn các điều kiện tương đương trong Bổ đề 9.3, nó được gọi là ***phụ thuộc đại số*** trên A (trên F). Một tập hợp B là ***phụ thuộc đại số*** trên A nếu mỗi phần tử của B là phụ thuộc đại số trên A.

Lý thuyết trong phần còn lại của chương này rất quen thuộc với đại số tuyến tính. Những tương ứng sau đây rất hữu ích cho việc nghiên cứu lý thuyết đó:

Đại số tuyến tính	Siêu việt
độc lập tuyến tính	độc lập đại số
$A \subset \mathrm{Span}(B)$	A phụ thuộc đại số trên B
cơ sở	cơ sở siêu việt
chiều	bậc siêu việt

9.2. Cơ sở siêu việt

Định lý 9.5 (Kết quả cơ bản)**.** *Cho $A = \{\alpha_1, \ldots, \alpha_n\}$ và $B = \{\beta_1, \ldots, \beta_n\}$ là hai tập con của Ω. Giả sử*

(a) A độc lập đại số (trên F);

(b) A phụ thuộc đại số trên B (trên F).

Khi đó $m \leq n$.

Ta trước hết chứng minh hai bổ đề sau.

Bổ đề 9.6 (Tính chất trao đổi)**.** *Cho $\{\alpha_1, \ldots, \alpha_n\}$ là một tập con của Ω; nếu B phụ thuộc đại số trên $\{\alpha_1, \ldots, \alpha_m\}$ nhưng không phụ thuộc đại số trên $\{\alpha_1, \ldots, \alpha_{m-1}\}$, thì α_m phụ thuộc đại số trên $\{\alpha_1, \ldots, \alpha_{m-1}, \beta\}$.*

Chứng minh. Vì β phụ thuộc đại số trên $\{\alpha_1, \ldots, \alpha_m\}$ nên tồn tại một đa thức $f(X_1, \ldots, X_m, Y)$ với các hệ số trong F mà

$$f(\alpha_1, \ldots, \alpha_m, Y) \neq 0, \quad f(\alpha_1, \ldots, \alpha_m, \beta) = 0.$$

Viết f như là một đa thức theo biến X_m,

$$f(X_1, \ldots, X_m, Y) = \sum_i a_i(X_1, \ldots, X_{m-1}, Y) X_m^{n-i}.$$

Để ý rằng do $f(\alpha_1, \ldots, \alpha_m, Y) \neq 0$ nên ít nhất một trong các đa thức

$$a_i(\alpha_1, \ldots, \alpha_{m-1}, Y),$$

không là đa thức 0, giả sử $a_{i_0} \neq 0$. Bởi vì β không phụ thuộc đại số trên

$$\{\alpha_1, \ldots, \alpha_{m-1}\},$$

$a_{i_0}(\alpha_1, \ldots, \alpha_{m-1}, \beta) \neq 0$. Vì thế, $f(\alpha_1, \ldots, \alpha_{m-1}, X_m, \beta) \neq 0$. Lại có $f(\alpha_1, \ldots, \alpha_m, \beta) = 0$ nên α_m phụ thuộc đại số trên $\{\alpha_1, \ldots, \alpha_{m-1}, \beta\}$. □

Bổ đề 9.7 (Tính bắc cầu của sự phụ thuộc đại số)**.** *Nếu C phụ thuộc đại số trên B, và B phụ thuộc đại số trên A, thì C phụ thuộc đại số trên A.*

Chứng minh. Lập luận trong chứng minh của Mệnh đề 1.44 chỉ ra rằng nếu γ đại số trên một trường E mà E đại số trên một trường F, thì γ đại số trên F (nếu $a_1, \ldots, a_n$ là các hệ số của đa thức tối tiểu của γ trên E, thì trường $F[a_1, \ldots, a_n, \gamma]$ có bậc hữu hạn trên F). Áp dụng điều này với $E = F(A \cup B)$ và $F = F(A)$. □

Chứng minh. (Định lý 9.5) Giả sử k là số các phần tử chung của A và B. Nếu $k = m$, thì $A \subset B$, và rõ ràng $m \leq n$. Giả sử $k < m$, và viết $B = \{\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_n\}$. Do α_{k+1} phụ thuộc đại số trên $\{\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_n\}$ nhưng không trên $\{\alpha_1, \ldots, \alpha_k\}$ nên tồn tại β_j, $k+1 \leq j \leq n$, mà α_{k+1} phụ thuộc đại số trên $\{\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_n\}$ nhưng không phụ thuộc đại số trên

$$\{\alpha_1, \ldots, \alpha_k, \beta_{k+1}, \ldots, \beta_{j-1}\}.$$

Bổ đề trao đổi khi đó chỉ ra rằng β_j phụ thuộc đại số trên

$$B_1 \stackrel{def}{=} B \cup \{\alpha_{k+1}\} \setminus \{\beta_j\}.$$

Do vậy B phụ thuộc đại số trên B_1, và do vậy A phụ thuộc đai số trên B_1 (bởi 9.7). Nếu $k+1 < m$, lặp lại lập luận với A và B_1. Cuối cùng ta sẽ đạt được $k = m$, và $m \leq n$. □

Định nghĩa 9.8. Một ***cơ sở siêu việt*** cho Ω trên F là một tập độc lập đại số A sao cho Ω đại số trên $F(A)$.

Bổ đề 9.9. *Nếu Ω đại số trên $F(A)$, và A là nhỏ nhất trong số các tập con của Ω với tính chất đó, thì nó là một cơ sở siêu việt cho Ω trên F.*

Chứng minh. Nếu A không độc lập đại số, thì có một $\alpha \in A$ phụ thuộc đại số trên $A \setminus \{\alpha\}$. Ta suy ra từ Bổ đề 9.7 rằng Ω đại số trên $F(A \setminus \{\alpha\})$. □

Định lý 9.10. *Nếu tồn tại một tập con hữu hạn $A \subset \Omega$ mà Ω đại số $F(A)$, thì Ω có một cơ sở siêu việt hữu hạn trên F. Hơn nữa, mọi cơ sở siêu việt là hữu hạn và có cùng số các phần tử.*

Chứng minh. Thực tế, mọi tập con nhỏ nhất A' của A mà Ω đại số trên Ω trên $F(A')$ sẽ là một cơ sở đại số. Phát biểu thứ hai suy ra từ Định lý 9.5. □

Bổ đề 9.11. *Giả sử A độc lập đại số, nhưng $A \cup \{\beta\}$ phụ thuộc đại số. Khi đó β đại số trên $F(A)$.*

Chứng minh. Từ giả thiết suy ra có một đa thức khác 0

$$f(X_1, \ldots, X_n, Y) \in F[X_1, \ldots, X_n, Y]$$

sao cho $f(\alpha_1, \ldots, \alpha_n, \beta) = 0$ với $\alpha_1, \ldots, \alpha_m \in A$ phân biệt. Do A độc lập đại số nên Y xuất hiện trong f như một biến. Do vậy

$$f = g_0 Y^m + g_1 Y^{m-1} + \cdots + g_m, \quad g_i \in F[X - 1, \ldots, X_n], g_0 \neq 0, m \geq 1.$$

Vì $g_0 \neq 0$ và α_i độc lập đại số, $g_0(\alpha_1, \ldots, \alpha_n) \neq 0$. Bởi vì β là một nghiệm của

$$f = g_0(\alpha_1, \ldots, \alpha_n)X^m + g_1(\alpha_1, \ldots, \alpha_n)X^{m-1} + \cdots + g_m(\alpha_1, \ldots, \alpha_n),$$

nên nó đại số trên $F(\alpha_1, \ldots, \alpha_n) \subset F(A)$. □

Mệnh đề 9.12. *Mọi tập con độc lập đại số cực đại của Ω là một cơ sở siêu việt cho Ω trên F.*

Chứng minh. Ta phải chứng minh rằng Ω đại số trên $F(A)$ nếu A lớn nhất trong số các tập con độc lập đại số. Nhưng tính cực đại suy ra rằng, với mọi $\beta \in \Omega \setminus A, A \cup \{\beta\}$ là phụ thuộc đại số, và do vậy bổ đề chỉ ra rằng β đại số trên $F(A)$. □

Nhắc lại rằng (ngoại trừ trong Chương 7), ta sử dụng một dấu sao để đánh dấu một kết quả phụ thuộc vào bổ đề Zorn.

Định lý 9.13 (*). *Mọi tập con độc lập đại số của Ω chứa trong một cơ sở siêu việt của Ω trên F; nói riêng, cơ sở siêu việt tồn tại.*

Chứng minh. Cho S là tập các tập con độc lập đại số của Ω chứa một tập cho trước. Ta có thể sắp thứ tự riêng cho chúng bởi phép bao hàm. Cho T là một tập con được sắp thứ tự của S, và cho $B = \bigcup\{A \mid A \in T\}$. Ta khẳng định $B \in S$ hay nói cách khác B độc lập đại số. Nếu không, có một tập con hữu hạn B' của B mà nó không độc lập đại số. Nhưng tập con như vậy sẽ chứa trong một trong các tập trong T, mâu thuẫn. Bây giờ bổ đề Zorn chỉ ra rằng có một tập độc lập đại số cực đại chứa S. Mệnh đề 9.12 chỉ ra rằng tập đó là một cơ sở siêu việt của Ω trên F. □

Có thể chứng minh rằng hai cở sở siêu việt bất kỳ của Ω (có thể vô hạn) trên F có cùng lực lượng. Lực lượng của một cơ sở siêu việt của Ω trên F được gọi là ***bậc siêu việt*** của Ω trên F. Ví dụ, mở rộng siêu việt thuần $F(X_1, \ldots, X_n)$ có bậc siêu việt n trên F.

Ví dụ 9.14. *Cho $p_1, \ldots, p_n$ là các đa thức đối xứng cơ bản trong $X_1, \ldots, X_n$. Trường $F(X_1, \ldots, X_n)$ đại số trên $F(p_1, \ldots, p_n)$, và do vậy $\{p_1, \ldots, p_n\}$ chứa một cơ sở siêu việt của $F(X_1, \ldots, X_n)$. Bởi vì $F(X_1, \ldots, X_n)$ có bậc siêu việt n, nên $p_1, \ldots, p_n$ phải là một cơ sở siêu việt.*

Ví dụ 9.15. *Cho Ω là trường các hàm phân hình trên một đa tạp phức compact M.*

(a) Hàm phân hình duy nhất trên mặt cầu Riemann là các hàm hữu tỉ theo biến z. Vì thế, trong trường hợp này, Ω là một mở rộng siêu việt thuần của $\mathbb{C}$ với bậc siêu việt 1.

(b) Nếu M là một diện Riemann, thì bậc siêu việt của Ω trên $\mathbb{C}$ là 1, và Ω là một mở rộng siêu việt thuần của $\mathbb{C} \iff M$ đẳng cấu với hình cầu Riemann.

(c) Nếu M có chiều phức n, thì bậc siêu việt $\leq n$, với dấu bằng xảy ra nếu M có thể nhúng trong một không gian xạ ảnh nào đó.

Mệnh đề 9.16. *Hai trường đóng đại số có cùng bậc siêu việt trên F thì F-đẳng cấu với nhau.*

Chứng minh. Chọn một cở sở siêu việt A và A' cho hai trường. Theo giả thiết, có một song ánh $A \to A'$, nó mở rộng duy nhất thành một F-đẳng cấu $F[A] \to F[A']$, và do vậy thành một F-đẳng cấu của các trường các thương $F(A) \to F(A')$. Sử dụng đẳng cấu này để đồng nhất $F(A)$ với $F(A')$. Khi đó hai trường đang xét là các bao đóng đại số của cùng một trường, và do vậy đẳng cấu với nhau (Định lý 6.8). □

Nhận xét 9.17. *Hai trường đóng đại số có cùng lực lượng không đếm được và có cùng đặc số thì đẳng cấu với nhau. Ý tưởng của chứng minh như sau. Gọi F và F' là các trường nguyên tố của Ω và Ω'; ta có thể đồng nhất F với F'. Sau đó chứng minh rằng khi Ω không đếm được, lực lượng của Ω bằng lực lượng của một có sở siêu việt trên F. Cuối cùng, áp dụng mệnh đề.*

Nhận xét 9.18. *Các tự đẳng cấu của $\mathbb{C}$ là gì? Chỉ có hai tự đồng cấu liên tục (cf Bài tập A-8 và lời giải). Nếu ta thừa nhận bổ đề Zorn, thì dễ dàng xây dựng thêm được nhiều nữa: chọn một cơ sở siêu việt A cho $\mathbb{C}$ trên $\mathbb{Q}$, và chọn một hoán vị α của A; α xác định một đẳng cấu $\mathbb{Q}(A) \to \mathbb{Q}(A)$ có thể mở rộng thành một tự đẳng cấu của $\mathbb{C}$. Không có bổ đề Zorn thì chỉ có hai , bởi vì các tự đẳng cấu không liên tục không đo được*[2] [3]*, và ta biết rằng bổ đề Zorn cần thiết cho việc xây dựng các hàm* [4] *không đo được.*

9.3. Định lý Lüroth

Định lý 9.19. *[Lüroth]Cho $L = F(X)$ với X siêu việt trên F. Khi đó mọi trường con E của L chứa thực sự F đều có dạng $E = F(u)$ với $u \in L$ nào đó siêu việt trên F.*

Đầu tiên ta sẽ phác thảo một chứng minh hình học của Định lý Lüroth. Phép nhúng của E vào trong L tương ứng với một ánh xạ từ đường thẳng xạ ảnh $\mathbb{P}^1$ lên một đường cong chính qui hoàn toàn C. Bây giờ công thức Riemann-Hurwitz chỉ ra rằng C có giống 0. Vì việc nó có

[2] nonmeasurable

[3] Một lý thuyết khá cơ bản của G. Mackey nói rằng các đồng cấu đo được của các nhóm Lie là liên tục (xem Theorem B.3, p. 198 của Zimmer, Robert J., Ergodic theory and semisimple groups. Birkhauser, 1984)

[4] "Ta chứng minh rằng sự tồn tại của các tập đo được non-Lebesgue không thể được chứng minh trong lý thuyết tập hợp Zermelo-Frankel nếu không được dùng tiền đề chọn ..." R. Solovay, Ann. of Math., 92 (1970), 1–56.

một điểm F-hữu tỷ (ảnh của bất kỳ điểm F-hữu tỷ của $\mathbb{P}^1$) nên nó đẳng cấu với $\mathbb{P}^1$. Vì thế $E = F(u)$ với một $u \in L$ siêu việt trên F.

Trước khi đưa ra một chứng minh sơ cấp, ta nhắc lại bổ đề Gauss và các hệ quả của nó.

BỔ ĐỀ GAUSS

Cho R là một miền nhân tử hóa, và Q là trường các thương, ví dụ $R = F[X]$ và $Q = F(X)$. Một đa thức $f(T) = \sum a_i T^i$ trong $R[T]$ được gọi là **nguyên thủy** nếu các hệ số a_i không có ước chung nào khác ngoài đơn vị. Mọi đa thức f trong $Q[X]$ có thể viết dưới dang $f = c(f) \cdot f_1$ với $c(f) \in Q$ và f_1 nguyên thủy (viết $f = af/a$ với a là mẫu chung của các hệ số của f), và sau đó viết $f = (b/a)f_1$ với b là ước chung lớn nhất của các hệ số của af). Phần tử $c(f)$ được xác định duy nhất sai khác đơn vị, và $f \in R[X]$ nếu và chỉ nếu $c(f) \in R$.

Bổ đề 9.20. *Nếu $f, g \in R[T]$ là nguyên thủy, thì fg cũng vậy.*

Giả sử $f = \sum a_i T^i$ và $g = \sum b_i T^i$, và p là một phần tử nguyên tố của R. Vì f nguyên thủy, có một hệ số a_i không chia hết cho p - giả sử a_{i_1} là hệ số đầu tiên như vậy. Tương tự, lấy b_{i_2} là hệ số đầu tiên của g không chia hết cho p. Thế thì hệ số của $T^{i_1+i_2}$ trong fg không chia hết cho p. Điều này chứng minh rằng fg nguyên thủy.

Bổ đề 9.21. *Với bất kỳ $f, g \in R[T]$, $c(fg) = c(f)c(g)$ và $(fg)_1 = f_1 g_1$.*

Cho $f = c(f)f_1$ và $g = c(g)g_1$ với f_1 và g_1 nguyên thủy. Thế thì $fg = c(f)c(g)f_1 g_1$ với $f_1 g_1$ nguyên thủy, và do vậy $c(fg) = c(f)c(g)$ và $(fg)_1 = f_1 g_1$.

Bổ đề 9.22. *Cho f là một đa thức trong $R[T]$. Nếu f phân tích thành tích của hai đa thức khác hằng trong $Q[T]$, thì nó phân tích thành tích của hai đa thức khác hằng trong $R[T]$.*

Giả sử $f = gh$ trong $Q[T]$. Khi đó $f_1 = g_1 h_1$ trong $R[T]$, và do vậy $f = c(f).f_1 = (c(f)g_1).h_1$ với $c(f).g_1$ và h_1 trong $R[T]$.

Bổ đề 9.23. *Cho $f, g \in R[T]$. Nếu f chia hết g trong $Q[T]$ và f nguyên thủy, thì nó chia hết g trong $R[T]$.*

Giả sử $fq = g$ với $q \in Q[T]$. Thế thì $c(q) = c(g) \in R$, và do vậy $q \in R[T]$.

CHỨNG MINH ĐỊNH LÝ LÜROTH

Ta định nghĩa bậc $deg(u)$ của một phần tử u của $F(X)$ là số lớn hơn trong số các bậc của tử số và mẫu số của u khi nó viết dưới dạng tối giản.

Bổ đề 9.24. *Cho $u \in F(X) \setminus F$. Thế thì u siêu việt trên F, X đại số trên $F(u)$, và $[F(X)\colon F(u)] = deg(u)$.*

Chứng minh. Viết $u(X) = a(X)/b(X)$ với $a(X)$ và $b(X)$ là các đa thức nguyên tố cùng nhau. $a(T) - b(T)u \in F(u)[T]$, và nó nhận X như là một nghiệm, và do vậy X đại số trên $F(u)$. Từ đó suy u siêu việt trên F (nếu không thì X đại số trên F; 1.31b).

Đa thức $a(T) - b(T)Z \in F[Z,T]$ rõ ràng là bất khả qui. Vì u siêu việt trên F nên

$$F[Z,T] \simeq F[u,T], \quad Z \leftrightarrow u, \quad T \leftrightarrow T,$$

và do vậy $a(T) - b(T)u$ bất khả qui trong $F[u,T]$. Từ đó, nó cũng bất khả quy trong $F(u)[T]$ bởi bổ đề Gauss (9.22). Nó nhận X như là một nghiệm, và do vậy, sai khác một hằng số, nó là đa thức tối tiểu của X trên $F(u)$, và bậc là $deg(u)$. □

Ví dụ 9.25. *Ta có $F(X) = F(u)$ nếu và chỉ nếu*

$$u = \frac{aX + b}{cX + d}$$

($ac \neq 0$) với $aX + b$ và $cX + d$ đều không là một hằng số nhân với cái còn lại. Các điều kiện này tương đương với $ad - bc \neq 0$.

Bây giờ ta chứng minh Định lý 9.19. Chọn u là một phần tử của E không nằm trong F. Thế thì

$$[F(X) : E] \leq [F(X) : F(u)] = deg(u),$$

và do vậy X đại số trên F. Gọi

$$f(T) = T^n + a_1T^{n-1} + \cdots + a_n, \quad a_i \in E,$$

là đa thức tối tiểu của nó. Vì X siêu việt trên F nên $a_j \notin F$, với j nào đó. Ta sẽ chứng minh rằng, với bất kỳ a_j như vậy thì $E = F(a_j)$.

Cho $d(X) \in F[X]$ là đa thức với bậc thấp nhất mà $d(X)a_i(X) \in F[X]$ với mọi i, và cho

$$f_1(X,T) = df(T) = dT^n + da_1T^{n-1} + \cdots + da_n \in F[X,T].$$

Khi đó f_1 nguyên thủy như một đa thức theo biến T, tức là, $\gcd(d, da_1, \ldots, da_n) = 1$ trong $F[X]$. Bậc m của f_1 trong X là bậc lớn nhất của một trong các đa thức $da_1, \ldots,$ giả sử đó là $m = \deg(da_i)$. Viết $a_i = b/c$ với b, c là các đa thức nguyên tố cùng nhau trong $F[X]$. Bây giờ $b(T) - c(T)a_i(X)$ là một đa thức trong $E[T]$ có X như là một nghiệm, và do vậy nó chia hết cho f,

$$f(T) \cdot q(T) = b(T) - c(T) \cdot a_i(T), \quad q(T) \in E[T].$$

Nhân cả hai vế với $c(X)$, ta có

$$c(X) \cdot f(T) \cdot q(T) = c(X) \cdot b(T) - c(T) \cdot b(X).$$

Bởi vì f_1 sai khác f một phần tử khác 0 nên f_1 chia hết $c(X) \cdot b(T) - c(T) \cdot b(X)$ trong $F(X)[T]$. Nhưng vì f_1 nguyên thủy nên nó chia hết $c(X) \cdot b(T) - c(T) \cdot b(X)$ trong $F[X,T]$ (bởi 9.23), tức là, tồn tại một đa thức $h(X,T) \in F[X,T]$ mà

$$f_1(X,T) \cdot h(X,T) = c(X) \cdot b(T) - c(T) \cdot b(X).$$

Đa thức $c(X) \cdot b(T) - c(T) \cdot b(X)$ có bậc lớn nhất m trong X, và m là bậc của $f_1(X,T)$ trong X. Do đó, $c(X) \cdot b(T) - c(T) \cdot b(X)$ có bậc đúng bằng m trong X, và $h(X,T)$ có bậc 0. Do vậy, $h(X,T)$ không chia hết cho một đa thức khác hằng trong $F[X]$.

Do tính đối xứng, $c(X) \cdot b(T) - c(T) \cdot b(X)$ có bậc m trong T, và $h(X,T)$ không chia hết cho một đa thức khác hằng trong $F[T]$. Nên $h(X,T) \in F^\times$, và do đó $f_1(X,T)$ là một hằng số nhân với $c(X) \cdot b(T) - c(T) \cdot b(X)$. Bằng việc so sánh bậc của T, ta thấy rằng $n = m$. Vì thế

$$[F(X) : F(a_i)] = \deg(da_i) = m = n = [F(X) : E] \leq [F(X) : F(a_i)],$$

và do đó $E = F[a_i]$. Cuối cùng, nếu $a_i \notin F$, thì

$$[F(X) : E] \leq [F(X) : F(a_i)] = \deg(a_j) \leq \deg(da_j) \leq \deg(da_i) = m = [F(X) : E],$$

và do vậy $E = F(a_j)$ như yêu cầu.

Nhận xét 9.26. *Định lý Lüroth không đúng khi có nhiều hơn một biến - xem ví dụ của Zariski và Swan. Tuy nhiên, khẳng định sau đây là đúng: nếu $[F(X,Y):E]<\infty$ và F đóng đại số đặc số 0, thì E là một mở rộng siêu việt thuần của F (Định lý của Zariski, 1958).*

Lüroth chứng minh định lý trên $\mathbb{C}$ vào năm 1876. Các trường tổng quát hơn được chứng minh bởi Steinitz vào năm 1910, bằng lập luận trên.

9.4. Cơ sở siêu việt tách

Cho $E \supset F$ là các trường với E hữu hạn sinh trên F. Một tập con $\{x_1,\dots,x_d\}$ của E là **cơ sở siêu việt tách**[5] cho E/F nếu nó độc lập đại số trên F và E là một mở rộng hữu hạn tách được của $F(x_1,\dots,x_d)$.

Định lý 9.27. *Nếu F hoàn hảo, thì mọi mở rộng hữu hạn sinh E của F đều có một cơ sở siêu việt tách trên F.*

Chứng minh. Nếu F có đặc số 0, thì mọi cơ sở siêu việt là tách, và vì thế phát biểu trở thành (9.10). Do vậy ta có thể giả sử rằng F có đặc số $p\neq 0$. Vì F hoàn hảo, mọi đa thức theo $X_1^p,\dots,X_n^p$ với hệ số trong F là một lũy thừa p trong $F[X_1,\dots,X_n]$:

$$\sum a_{i_1\dots i_n}X_1^{i_1p}\dots X_n^{i_np}=(\sum a_{i_1\dots i_n}^{\frac{1}{p}}X_1^{i_1}\dots X_n^{i_n})^p.$$

Cho $E=F(x_1,\dots,x_n)$, và giả sử rằng $n>d+1$ với d là bậc siêu việt của E trên F. Sau khi đánh số lại, có thể giả sử rằng $x_1,\dots,x_d$ là độc lập đại số (9.9). Khi đó $f(x_1,\dots,x_{d+1})=0$ đối với một đa thức bất khả qui $f(X_1,\dots,X_{d+1})$ nào đó với hệ số trong F. Không phải tất cả $\partial f/\partial X_i$ bằng 0, nếu không f sẽ là một đa thức theo $X_1^p,\dots,X_{d+1}^p$, suy ra nó là một lũy thừa p. Sau khi đánh số lại, ta có thể giả sử rằng $\partial f/\partial X_{d+1}\neq 0$. Khi đó, x_{d+1} là đại số tách được trên $F(x_1,\dots,x_d)$ và $F(x_1,\dots,x_{d+1},x_{d+2})$ đại số trên $F(x_1,\dots,x_d,x_{d+1})$. Vì thế nó cũng đại số trên $F(x_1,\dots,x_d)$, và vì thế, bởi Định lý phần tử nguyên thủy (5.1), tồn tại một phần tử y mà $F(x_1,\dots,x_{d+2})=F(x_1,\dots,x_d,y)$. Do đó E sinh bởi $n-1$ phần tử (như là một trường chứa F). Sau khi lặp lại quá trình, có thể một vài lần, ta sẽ có $E=F(z_1,\dots,z_{d+1})$ với z_{d+1} tách được trên $F(z_1,\dots,z_d)$. □

Ghi chú 9.28. *Thực tế, ta đã chứng minh rằng E có một cở sở siêu việt tách với $d+1$ phần tử, ở đó d là bậc siêu việt. Điều này có một diễn đạt*

[5] separating transcendence basis

hình học như sau: mọi đa tạp đại số bất khả quy chiều d trên một trường hoàn hảo F tương đương song hữu tỷ với một siêu mặt H trong $\mathbb{A}^{d+1}$ với phép chiếu $(a_1, \ldots, a_{d+1}) \mapsto (a_1, \ldots, a_d)$ nhận $F(H)$ như là một mở rộng tách được hữu hạn của $F(\mathbb{A}^d)$ (xem bài giảng Hình Học Đại Số của tác giả).

9.5. Lý thuyết Galois siêu việt

Định lý 9.29. *Cho Ω là một trường đóng đại số và F là một trường con hoàn hảo của Ω. Nếu $\alpha \in \Omega$ được giữ cố định bởi tất cả F-tự đồng cấu của Ω, thì $\alpha \in F$, tức là, $\Omega^{Aut(\Omega/F)} = F$.*

Chứng minh. Lấy $\alpha \in \Omega \setminus F$. Nếu α đại số trên F, thì có một F-đồng cấu $F[\alpha] \to \Omega$ ánh xạ α thành một liên hợp của α trong Ω khác α. Đồng cấu này mở rộng thành một đồng cấu từ bao đóng đại số F^{al} của F trong Ω tới Ω (bởi 6.8). Bây giờ chọn một cơ sở siêu việt A cho Ω trên F^{al}. Ta có thể mở rộng đồng cấu của ta thành một đồng cấu $F(A) \to \Omega$ bằng cách ánh xạ mỗi phần tử của A thành chính nó. Cuối cùng, ta có thể mở rộng đồng cấu này thành một đồng cấu từ bao đóng đại số Ω của $F(A)$ tới Ω. F-đồng cấu $\Omega \to \Omega$ thu được tự khắc là đẳng cấu (cf. 6.8).

Nếu α siêu việt trên F, thì nó là phần của của một cơ sở siêu việt A cho Ω trên F (xem 9.13). Nếu A có ít nhất hai phần tử, thì có một tự đẳng cấu σ của A mà $\sigma(\alpha) \neq \alpha$. Bây giờ σ xác định một F-đồng cấu $F(A) \to \Omega$, mở rộng thành một đẳng cấu $\Omega \to \Omega$ như trước đó. Nếu $A = \{\alpha\}$, thì ta cho $F(\alpha) \to \Omega$ là F-đồng cấu biến α thành $\alpha + 1$. Lại một lần nữa, nó mở rộng thành một đẳng cấu $\Omega \to \Omega$. □

Nhận xét 9.30. *Định lý 9.29 đúng với Ω chỉ đóng tách được. Để nhìn thấy điều này, cho Ω^{al} là một bao đóng đại số của Ω. Thế thì mọi tự đẳng cấu σ của Ω/F mở rộng duy nhất thành một tự đẳng cấu $\overline{\sigma}$ của Ω^{al}/F: cho $\alpha \in \Omega^{al}$ và cho $\alpha^{p^n} \in \Omega$; thì $\overline{\sigma}(\alpha)$ là nghiệm duy nhất của $X^{p^n} - \sigma(\alpha^{p^n})$ trong Ω^{al}. Do đó, nếu $\alpha \in \Omega$ cố định bởi tất cả các F-tự đẳng cấu của Ω, thì nó cố định bởi tất cả F-tự đẳng cấu của Ω^{al}, và vì thế nó nằm trong F.*

Cho $\Omega \supset F$ là các trường và $G = Aut(\Omega/F)$. Với mỗi tập con hữu hạn S của Ω, đặt

$$G(S) = \{\sigma \in G \mid \sigma s = s \text{ với mọi } s \in S\}.$$

Như trong Chương 7, các nhóm con $G(S)$ của G có dạng một cơ sở lân cận với duy nhất tôpô trên G, cái mà chúng ta gọi là tô pô Krull. Các lập luận tương tự như trong Chương 7 chỉ ra rằng tôpô này là Hausdorff (nhưng nó không nhất thiết compact).

Định lý 9.31. *Cho $\Omega \supset F$ là các trường mà $\Omega^G = F, G = Aut(\Omega/F)$.*

(a) Với mọi mở rộng hữu hạn E của F trong Ω, $\Omega^{Aut(\Omega/E)} = E$.

(b) Các ánh xạ

$$H \mapsto \Omega^H, \quad M \mapsto Aut(\Omega/M) \tag{9.1}$$

là các song ánh nghịch đảo của nhau giữa tập hợp các nhóm con compact của G và tập hợp các trường trung gian trên đó Ω Galois (có thể vô hạn):

$$\{ \text{ các nhóm con compact của } G\} \leftrightarrow \{\text{các trường } M \text{ mà } F \subset M \overset{Galois}{\subset} \Omega\}$$

(c) Nếu tồn tại một M hữu hạn sinh trên F mà Ω Galois trên M, thì G compact địa phương, và dưới (9.1):

$$\{\text{các nhóm con compact mở của } G \ \}$$

tương ứng $1:1$ với

$$\{ \text{ các trường } M \text{ mà } F \overset{\text{hữu hạn sinh}}{\subset} M \overset{Galois}{\subset} \Omega\}$$

(d) Cho H là một nhóm con của G, và $M = \Omega^H$. Thế thì bao đóng đại số M_1 của M Galois trên M. Hơn nữa, nếu $H = Aut(\Omega/M)$, thì $Aut(\Omega/M_1)$ là một nhóm con chuẩn tắc của H, và $\sigma \mapsto \sigma|M_1$ ánh xạ $H/Aut(\Omega/M_1)$ một cách đẳng cấu vào một nhóm con trù mật của $Aut(M_1/M)$.

Chứng minh. Xem 6.3 of Shimura, Goro., Introduction to the arithmetic theory of automorphic functions. Princeton, 1971 □

9.6. Bài tập

9-1. Tìm tâm của liên hợp phức trong $Aut(\mathbb{C}, \mathbb{Q})$.

Một số bài tập bổ sung

A-1 Cho p là một số nguyên tố và m, n là các số nguyên dương.

(a) Tìm điều kiện cần và đủ đối với m và n để $\mathbb{F}_{p^n}$ có một trường con đẳng cấu với $\mathbb{F}_{p^m}$. Chứng minh khẳng định của bạn.

(b) Nếu tồn tại một trường con như vậy, có bao nhiêu trường con đẳng cấu với $\mathbb{F}_{p^m}$ như thế, và vì sao?

A-2 Chứng minh rằng nhóm Galois của trường phân rã F của $X^3 - 7$ trên $\mathbb{Q}$ đẳng cấu với S_3, và hãy mô tả các trường trung gian giữa $\mathbb{Q}$ và F. Những trường trung gian nào chuẩn tắc trên $\mathbb{Q}$?

A-3 Chứng minh rằng hai trường $Q[\sqrt{7}]$ và $\mathbb{Q}[\sqrt{11}]$ không đẳng cấu với nhau.

A-4 (a) Chứng minh rằng nhóm nhân tất cả các phần tử khác không trong một trường hữu hạn là xyclic.

(b) Xây dựng tường minh một trường có 9 phần tử, và chỉ rõ một phần tử sinh của nhóm nhân của nó.

A-5 Cho X siêu viêt trên một trường F, E là một trường con của $F(X)$ chứa F thực sự. Chứng minh rằng X đại số trên E.

A-6 Chứng minh, càng trực tiếp càng tốt, rằng nếu ζ là một căn nguyên thủy bậc p của 1, p nguyên tố, thì nhóm Galois $\mathbb{Q}[\zeta]$ trên $\mathbb{Q}$ là xyclic cấp $p - 1$.

A-7 Cho G là nhóm Galois của đa thức $X^5 - 2$ trên $\mathbb{Q}$.

(a) Tìm cấp của nhóm G.

(b) Hãy xác định xem G có phải là một nhóm abel hay không?

(c) Hãy xác định xem G có giải được hay không?

A-8 (a) Chứng minh rằng mọi đồng cấu trường từ $\mathbb{R}$ vào $\mathbb{R}$ là song ánh.

(b) Chứng minh rằng $\mathbb{C}$ đẳng cấu với một số nhiều vô hạn trường con của chính nó.

A-9 Cho F là một trường có 16 phần tử. Hỏi các đa thức sau đây có bao nhiêu nghiệm trong F: $X^3 - 1$, $X^4 - 1$, $X^{15} - 1$, $X^{17} - 1$.

A-10 Tìm bậc của một trường phân rã của đa thức $(X^3 - 5)(X^3 - 7)$ trên $\mathbb{Q}$.

A-11 Tìm nhóm Galois của đa thức $X^6 - 5$ trên $\mathbb{Q}$ và trên $\mathbb{R}$.

A-12 Các hệ số của một đa thức $f(X)$ đại số trên một trường F. Chứng minh rằng $f(X)$ là một ước của một đa thức khác không $g(X)$ nào đó với hệ số trong F.

A-13 Cho $f(X)$ là một đa thức bậc n trong $F(X)$, và E là trường phân rã của f. Chứng minh rằng $[E : F]$ là ước của $n!$.

A-14 Tìm một phần tử nguyên thuỷ cho trường $\mathbb{Q}[\sqrt{3}, \sqrt{7}]$, cụ thể là một phần tử sao cho $\mathbb{Q}[\sqrt{3}, \sqrt{7}] = \mathbb{Q}[\alpha]$.

A-15 Cho G là nhóm Galois của $(X^4 - 2)(X^3 - 5)$ trên $\mathbb{Q}$.

(a) Tìm một tập các phần tử sinh cho G và các quan hệ giữa các phần tử đó.

(b) Cấu trúc của nhóm G là gì?

A-16 Cho F là một trường hữu hạn với đặc số khác 2. Chứng minh rằng $X^2 + 1 = 0$ có một nghiệm trong F nếu và chỉ nếu $|F| \equiv 1 \mod 4$.

A-17 Cho E là trường phân rã trên $\mathbb{Q}$ của $(X^2 - 2)(X^2 - 5)(X^2 - 7)$. Tìm một phần tử α trong E sao cho $E = \mathbb{Q}[\alpha]$.

A-18 Cho E là một mở rộng Galoi của F với nhóm Galois S_n, $n > 1$ (n không nguyên tố) Gọi H_1 là nhóm con của S_n gồm các phần tử cố định 1 và H_2 là nhóm con sinh bởi nhóm cyclic $(123 \ldots n)$. Gọi $E_i = E^{H_i}$, $i = 1, 2$. Tìm bậc của E_1, E_2, $E_1 \cap E_2$ và $E_1 E_2$ trên F. Chỉ ra rằng tồn tại một trường M sao cho $F \subset M \subset E_2$, $M \neq F$, $M \neq E_2$ nhưng không tồn tại trường nào thoả mãn với E_1.

A-19 Cho ζ là một căn nguyên thuỷ bậc 12 của 1 trên $\mathbb{Q}$. có bao nhiêu trường con thực sự giữa $\mathbb{Q}[\zeta^3]$ và $\mathbb{Q}[\zeta]$?.

A-20 Cho đa thức $X^3 - 3$, hãy tìm tường minh trường phân rã của nó trên $\mathbb{Q}$ và các phần tử sinh ra nhóm Galois của đa thức đó.

A-21 Cho $E = \mathbb{Q}[\zeta]$, $\zeta^5 = 1$, $\zeta \neq 1$. Chứng minh rằng $i \notin E$ và nếu $L = E[i]$ thì -1 là một chuẩn từ L vào E (Ở đây $i = \sqrt{-1}$).

A-22 Cho E là một mở rộng trường của F. Gọi Ω là bao đóng đại số của E và $\sigma_1, \ldots, \sigma_n$ là các F đẳng cấu phân biệt từ $E \to \Omega$.

(a) Chỉ ra rằng $\sigma_1, \ldots, \sigma_n$ độc lập tuyến tính trên Ω.

(b) Chứng minh rằng $[E : F] \geq m$.

(c) Cho F có đặc số $p > 0$ và L là một trường con của Ω chứa E sao cho $a^p \in E$ với mọi $a \in L$. Chứng minh rằng mỗi σ_i có một mở rộng duy nhất tới một đồng cấu $\sigma_i' : L \to \Omega$.

A-23 Xác định nhóm Galois của trường phân rã F của $X^4 - 3$ trên $\mathbb{Q}$. Xác định số các trường con bậc 2.

A-24 Cho F là một trường con của một trường hữu hạn F. Chứng minh rằng ánh xạ vết $T = \mathrm{Tr}_{E/F}$ và ánh xạ chuẩn $N = \mathrm{Nm}_{E/F}$ của E trên F đều là toàn ánh từ E vào F.

A-25 Chứng minh hoặc đưa ra phản ví dụ cho những khẳng định sau.

(a) Nếu L/F là một mở rộng bậc 2, thì có một tự đẳng cấu σ của L sao cho F là trường cố định của σ.

(b) Cùng khẳng định trên với L là trường hữu hạn.

A-26 Một mở rộng Galois hữu hạn L của một trường K có bậc 8100. Chứng minh rằng có một trường F với $K \subset F \subset L$ sao cho $[F : K] = 100$.

A-27 Một mở rộng đại số L của một trường K với đặc số 0 được sinh bởi một phần tử θ với θ là nghiệm của cả hai đa thức $X^3 - 1$ và $X^4 + X^2 + 1$. Cho $L \neq 0$, tìm đa thức tối tiểu của θ.

A-28 Cho $F/\mathbb{Q}$ là một mở rộng Galois bậc 3^n, $n \geq 1$. Chứng minh rằng có một chuỗi các trường

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n = F$$

sao cho với mọi i, $1 \leq i \leq n-1$, $[F_{i+1} : F_i] = 3$.

A-29 Cho L là trường phân rã trên $\mathbb{Q}$ của một phương trình bậc 5 với nghiệm các phân biệt. Giả sử L có một tự đẳng cấu cố định ba trong các nghiệm đó và tráo đổi hai nghiệm còn lại, và hơn nữa $\sigma \neq 1$ có cấp 5.

(a) Chứng minh rằng nhóm các tự đẳng cấu của L là nhóm đối xứng trên 5 phần tử.

(b) Có bao nhiêu trường con thực sự của L là các mở rộng chuẩn tắc của $\mathbb{Q}$? Với mỗi trường như vậy, tìm $[F : \mathbb{Q}]$.

A-30 Cho L/K là một mở rộng đại số tách được, bậc d. Chứng minh rằng số các trường trung gian giữa K và L không vượt quá $2^{d!}$.

A-31 Cho K là trường phân rã trên $\mathbb{Q}$ của X^5-1. Hãy mô tả nhóm Galois $\mathrm{Gal}(K/\mathbb{Q})$ và chứng minh rằng K có đúng một trường con có bậc 2 trên $\mathbb{Q}$, ký hiệu là $\mathbb{Q}[\zeta+\zeta^4]$, với $\zeta \neq 1$ là nghiệm của X^5-1. Tìm đa thức tối tiểu của $\zeta+\zeta^4$ trên $\mathbb{Q}$. Tìm nhóm $\mathrm{Gal}(L/K)$ với L là trường phân rã trên $\mathbb{Q}$ của

(a) $(X^2-5)(X^5-1)$;

(b) $(X^2+3)(X^5-1)$.

A-32 Cho Ω_1, Ω_2 là các trường đóng đại số có bậc siêu việt trên $\mathbb{Q}$ bằng 5, $\alpha\colon \Omega_1 \to \Omega_2$ là một đồng cấu. Chứng minh rằng α là một song ánh.

A-33 Tìm nhóm các $\mathbb{Q}$- tự đồng cấu của trường $k = \mathbb{Q}[\sqrt{-3}, \sqrt{-2}]$.

A-34 Chứng minh rằng đa thức $f(X) = X^3 - 5$ bất khả quy trên $\mathbb{Q}[\sqrt{7}]$. Gọi L là trường phân rã của $f(X)$ trên $\mathbb{Q}[\sqrt{7}]$, chứng minh rằng $\mathrm{Gal}(L/\mathbb{Q}[\sqrt{7}]) \cong S_3$. Chứng minh rằng tồn tại một trường con K của L sao cho $\mathrm{Gal}(L/K)$ là một nhóm xyclic cấp 3.

A-35 Xác định nhóm Galois G của $f(X) = X^5 - 6X^4 + 3$ trên F, với

(a) $F = \mathbb{Q}$;

(b) $F = \mathbb{F}_2$.

Trong mỗi trường hợp, nếu gọi E là trường phân rã của $f(X)$ trên F, hãy xác định số trường K thỏa mãn $F \subset K \subset E$ và $[K : F] = 2$.

A-36 Cho K là một trường có đặc số p, với p^n phần tử và θ là một tự đồng cấu của K biến mọi phần tử thành lũy thừa bậc p của chúng. Chứng minh rằng tồn tại một tự đồng cấu α của K thỏa mãn $\theta\alpha^2 = 1$ khi và chỉ khi n lẻ.

A-37 Mô tả trường phân rã và nhóm Galois trên $\mathbb{Q}$ của đa thức $X^5 - 9$.

A-38 Cho E là một mở rộng Galois của F thỏa mãn $[E : F] = 5^3 \cdot 43^2$. Chứng minh rằng tồn tại hai trường trung gian thực sự K_1, K_2 thỏa mãn các tính chất sau:

(i) Mỗi trường K_i là một mở rộng Galois của F;

(ii) $K_1 \cap K_2 = F$;

(iii) $K_1K_2 = E$.

A-39 Cho p là một số nguyên tố, $F = \mathbb{F}_{\mathrm{p}}$, m là một số nguyên dương không chia hết cho p. Gọi K là trường phân rã của $X^m - 1$. Tìm $[K : F]$.

A-40 Cho F là một trường có 81 phần tử. Hãy tính số nghiệm nằm trong F của mỗi đa thức sau: $X^{80} - 1, \quad X^{81} - 1, \quad X^{88} - 1$.

A-41 Mô tả nhóm Galois trên $\mathbb{Q}$ của đa thức $X^6 - 7$.

A-42 Cho K là một trường có đặc số $p > 0$, và $F = K(u, v)$ là một mở rộng trường bậc p^2 thỏa mãn $u^p \in K$ và $v^p \in K$. Chứng minh rằng K không hữu hạn, nghĩa là F không phải là một mở rộng đơn của K, và tồn tại vô hạn trường trung gian giữa K và F.

A-43 Xác định trường phân rã và nhóm Galois của $X^3 - 5$ trên $\mathbb{Q}[\sqrt{2}]$.

A-44 Cho p là một số nguyên tố, hãy tìm nhóm Galois trên $\mathbb{Q}$ của đa thức $X^5 - 5p^4X + p$.

A-45 Phân tích đa thức $X^4 + 1$ trên các trường sau: $\mathbb{F}_5, \mathbb{F}_{25}$ và $\mathbb{F}_{125}$. Xác định trường phân rã trong mỗi trường hợp.

A-46 Cho $\mathbb{Q}[\alpha]$ là một mở rộng hữu hạn của $\mathbb{Q}$. Giả sử tồn tại $q \in \mathbb{Q}, q \neq 0$ sao cho $|\rho(\alpha)| = q$ với mọi đồng cấu $\rho : \mathbb{Q}[\alpha] \to \mathbb{C}$. Chứng minh rằng tập hợp các nghiệm của đa thức tối tiểu của α trùng với tập hợp các nghiệm của đa thức tối tiểu của q^2/α. Từ đó suy ra rằng tồn tại một tự đồng cấu σ của $\mathbb{Q}[\alpha]$ thỏa mãn:

(i) $\sigma^2 = 1$ và

(ii) $\rho(\sigma\gamma) = \overline{\rho(\gamma)}$ với mọi $\gamma \in \mathbb{Q}[\alpha]$ và $\rho : \mathbb{Q}[\alpha] \to \mathbb{C}$.

A-47 Cho F là một trường có đặc số bằng 0, p là một số nguyên tố. Biết rằng mọi đa thức bất khả quy $f(X) \in F[X]$ đều có bậc là một lũy thừa của p. Chứng minh rằng mọi phương trình $g(X) = 0, g \in F[X]$ đều giải được bằng căn thức.

A-48 Cho $K = \mathbb{Q}[\sqrt{5}, \sqrt{-7}]$ và L là trường phân rã của $f(X) = X^3 - 10$ trên $\mathbb{Q}$.

(a) Xác định nhóm Galois của K và L trên $\mathbb{Q}$.

(b) K có chứa nghiệm nào của f không?

(c) Tính bậc mở rộng của $K \cap L$ trên $\mathbb{Q}$.

A-49 Xác định trường phân rã (trên $\mathbb{F}_\mathrm{p}$) của $X^{p^r} - X \in \mathbb{F}_\mathrm{p}[X]$, từ đó suy ra rằng $X^{p^r} - X$ có một nhân tử bất khả quy $f \in \mathbb{F}_\mathrm{p}[X]$ bậc r. Gọi $g(X) \in \mathbb{Z}[X]$ là một đa thức đơn có ảnh là f khi lấy modulo p các hệ số. Chứng minh rằng $g(X)$ bất khả quy trên $Q[X]$.

A-50 Gọi E là trường phân rã của $X^3 - 51$ trên $\mathbb{Q}$. Liệt kê tất cả các trường con của E và tìm một phần tử $\gamma \in E$ sao cho $E = \mathbb{Q}[\gamma]$.

A-51 Cho $k = \mathbb{F}_{1024}$ và K là một mở rộng bậc 2 của k. Chứng minh rằng tồn tại duy nhất một k-tự đồng cấu bậc 2 σ của K và tính số phần tử $x \in K^\times$ sao cho $\sigma(x) = x^{-1}$.

A-52 Cho E và F là hai trường hữu hạn có cùng đặc số. Kiểm tra các mệnh đề sau:

(a) Tồn tại một đồng cấu vành từ F vào E khi và chỉ khi $|E|$ là lũy thừa của $|F|$.

(b) Tồn tại một đơn cấu nhóm từ nhóm nhân của F vào nhóm nhân của E khi và chỉ khi $|E|$ là lũy thừa của $|F|$.

A-53 Cho L/K là một mở rộng đại số. Chứng minh rằng L đóng đại số khi và chỉ khi mọi đa thức $f \in K[X]$ có phân tích hoàn toàn trong L.

A-54 Cho K là một trường và $M = K(X)$, X là một biến. L là một trường trung gian khác K. Chứng minh rằng M hữu hạn chiều trên L.

A-55 Cho $\theta_1, \theta_2, \theta_3$ là các nghiệm của $f(X) = X^3 + X^2 - 9X + 1$.

(a) Chứng minh rằng $\theta_i \in \mathbb{R} \setminus \mathbb{Q}$ và phân biệt.

(b) Giải thích tại sao nhóm Galois (trên $\mathbb{Q}$) G của f thuộc $\{A_3, S_3\}$. Cho một mô tả ngắn gọn cách xác định G (mà không tính toàn cụ thể).

(c) Chứng minh rằng các véc tơ hàng của ma trận

$$\begin{pmatrix} 3 & 9 & 9 & 9 \\ 3 & \theta_1 & \theta_2 & \theta_3 \\ 3 & \theta_2 & \theta_3 & \theta_1 \\ 3 & \theta_3 & \theta_1 & \theta_2 \end{pmatrix}$$

đôi một trực giao với nhau. Tính độ dài của chúng và định thức của ma trận trên.

A-56 Cho E/K là một mở rộng Galois với bậc p^2q, trong đó $p > q$ là các số nguyên tố, $q \not| p^2 - 1$. Chứng minh rằng:

(a) tồn tại các trường trung gian L, M sao cho $[L : K] = p^2$ và $[M : K] = q$;

(b) L, M là Galois trên K;

(c) $\mathrm{Gal}(E/K)$ là một nhóm abel.

A-57 Cho $\zeta \in \mathbb{C}$ là một căn bậc 7 của 1.

(a) Chứng minh rằng $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ là đa thức tối tiểu của ζ trên $\mathbb{Q}$.

(b) Tìm đa thức tối tiểu của $\zeta + \zeta^{-1}$ trên $\mathbb{Q}$.

A-58 Cho K là bao đóng Galois trên $\mathbb{Q}$ của $\mathbb{Q}[\sqrt[4]{2}]$. Tính $[K : \mathbb{Q}]$ và xác định lớp các đẳng cấu của $\mathrm{Gal}(K/\mathbb{Q})$.

A-59 Cho p, q là hai số nguyên tố phân biệt, $K = \mathbb{Q}[\sqrt{p}, \sqrt{q}]$.

(a) Chứng minh rằng $\mathrm{Gal}(K/\mathbb{Q}) \cong C_2 \times C_2$.

(b) Chứng minh rằng mọi trường trung gian bậc 2 của K trên $\mathbb{Q}$ đều có dạng $\mathbb{Q}[\sqrt{m}]$ với $m \in \{p, q, pq\}$.

(c) Chứng minh rằng tồn tại $\gamma \in K$ sao cho $K = \mathbb{Q}[\gamma]$.

Bài kiểm tra mẫu

1. (a) Cho σ là một tự đẳng cấu của trường E. Giả sử $\sigma^4 = 1$ và

$$\sigma(\alpha) + \sigma^3(\alpha) = \alpha + \sigma^2(\alpha) \quad \text{với mọi } \alpha \in E,$$

chứng minh rằng $\sigma^2 = 1$.

(b) Cho p là một số nguyên tố, a, b là các số hữu tỉ thỏa mãn $a^2 + pb^2 = 1$. Chứng minh rằng tồn tại các số hữu tỉ c, d sao cho $a = \frac{c^2-pd^2}{c^2+pd^2}$ và $b = \frac{2cd}{c^2+pd^2}$.

2. Cho $f(x)$ là một đa thức bất khả qui bậc 4 trong $\mathbb{Q}[x]$ và $g(x)$ là đa thức giải[6] bậc 3 của f. Tìm quan hệ giữa nhóm Galois của f và của g. Tìm nhóm Galois của f nếu

(a) $g(x) = x^3 - 3x + 1$,

(b) $g(x) = x^3 + 3x + 1$.

3. (a) Có bao nhiêu ước bất khả qui với hệ số đầu bằng 1 của $x^{255} - 1 \in \mathbb{F}_2[x]$? Bậc của chúng bằng bao nhiêu?

(b) Có bao nhiêu ước bất khả qui với hệ số đầu bằng 1 của $x^{255} - 1 \in \mathbb{Q}[x]$? Bậc của chúng bằng bao nhiêu?

4. Cho E là trường phân rã của $(x^5 - 3)(x^5 - 7) \in \mathbb{Q}[x]$. Tìm bậc của E trên $\mathbb{Q}$. Có bao nhiêu trường con thực sự của E không chứa trong các trường phân rã của cả $x^5 - 3$ lẫn $x^5 - 7$? (Bạn có thể giả thiết rằng 7 không phải là một căn bậc 5 trong trường phân rã của $x^5 - 3$.)

5. Xét mở rộng trường $\Omega \supset F$. Một phần tử $a \in \Omega$ được gọi là F-*xây dựng được* nếu nó nằm trong một trường có dạng

$$F[\sqrt{a_1}, \ldots, \sqrt{a_n}], \quad a_i \in F[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}].$$

[6] resolvent

Giả sử Ω là một mở rộng Galois hữu hạn của F và xây dựng một trường $E, F \subset E \subset \Omega$ sao cho mọi $a \in \Omega$ là E-xây dựng được và E là trường nhỏ nhất có tính chất trên.

6. Giả sử Ω là một mở rộng trường của trường F. Chứng minh rằng mọi F-đồng cấu $\Omega \to \Omega$ đều là một đẳng cấu, nếu như

   (a) Ω là trường đóng đại số, và

   (b) Ω có bậc siêu việt hữu hạn trên F.

   Liệu có thể bỏ bớt điều kiện nào trong hai điều kiện trên hay không (Hoặc chứng minh, hoặc đưa ra một phản ví dụ.)

Tài liệu tham khảo

[1] N. Jacobson, *Lectures in Abstract Algebra, Volume III — Theory of Fields and Galois Theory*, van Nostrand, 1964.

[2] J.S.Milne, ***GT*** *Group Theory, v3.14, 2017*, www.jmilne.org/math/, 2017.

[3] J.S.Milne, ***ANT*** *Algebraic Number Theory, v3.06*, www.jmilne.org/math/, 2014.

[4] J.S.Milne, ***CA*** *A Primer of Commutative Algebra, v4.02*, www.jmilne.org/math/, 2017.

[5] http://mathoverflow.net/questions/nnnn/

PARI là một hệ đại số máy tính mã nguồn mở miễn phí.

Chỉ mục