The (failure of the) Hasse principle for centres of semisimple groups

J.S. Milne

June 6th, 1987; updated 2017

Throughout, k is a number field and S is a finite set of primes of k. Let G be a semisimple group over k, and let Z be the centre of G (semisimple groups are always assumed to be connected). We shall investigate the kernel $\mathrm{Ker}(G,S)$ of

$$H^1(k,\mathbb{Z}) \to \prod_{v \notin S} H^1(k_v, Z).$$

1 Inner forms of SL_m.

We write ζ_m for a primitive mth root of 1 (it will never matter which one), and η_r for $\zeta_{2^r} + \bar{\zeta}_{2^r}$. The Klein Veiergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ will be denoted by V.

LEMMA 1.1. *Let k be a number field, and let t be an integer ≥ 2. Then $\mathrm{Gal}(k(\zeta_{2^t})/k)$ is not cyclic if and only if there is an integer $s < t$ such that*

(a) *$\eta_s \in k$, and*

(b) *-1, $2+\eta_s$, and $-(2+\eta_s)$ are not squares in k.*

In this case, $\mathrm{Gal}(k(\zeta_{2^{s+1}})/k) \approx V$, and $k(i)$ $(= k(\zeta_{2^s}))$, $k(\eta_{s+1})$, and $k(i\eta_{s+1})$ are the three subfields of $k(\zeta_{2^{s+1}})$ quadratic over k.

PROOF. (Artin and Tate 1961, pp. 93–96). Note that

$$\eta_{r+1}^2 = 2 + \eta_r;$$

hence any field containing η_r also contains $\eta_{r'}$ for all $r' < r$.

Note that

$$\zeta_{2^{r+1}}\eta_{r+1} = \zeta_{2^r} + 1;$$

hence any field containing ζ_{2^r} and η_{r+1}, $r \geq 2$, also contains $\zeta_{2^{r+1}}$. On applying this repeatedly, we find that any field containing i and η_r for $r > 2$ contains ζ_r.

Finally note that $k(\eta_r)$ is cyclic over k.

Suppose $k(\zeta_{2^t})$ is not cyclic over k. Then $\eta_t \notin k$ (else $\zeta_{2^t} \in k(i)$, which is cyclic over k). Hence, there is an $s < t$, $s \geq 2$, such that $\eta_s \in k$ but $\eta_{s+1} \notin k$. Note that $i \notin k(\eta_{s+1})$ (else $i \in k(\eta_t)$

I worked this out in the early 1980s because of its applications to Shimura varieties (see 5.23 of my *Introduction to Shimura varieties*) and the only reference I could find, Raghunathan 1981, contained errors (he overlooks Wang's counterexample to Grunwald's theorem).

and so $\zeta_{2^t} \in k(\eta_t)$). It follows that $k(i)$ and $k(\eta_{s+1})$ are linearly disjoint quadratic extensions of k, and it is clear that (a) and (b) and the remaining statements are fulfilled.

The converse is obvious. □

PROPOSITION 1.2. *Let G be an inner form of* SL_m *over k; then* $\mathrm{Ker}(G,S) \neq 0$ *if and only if there is an s such that*

(a) $2^{s+1}|m$;

(b) $\eta_s \in k$;

(c) -1, $2+\eta_s$, *and* $-(2+\eta_s)$ *are not squares in k;*

(d) *S contains all primes v of k lying over 2 for which* -1, $2+\eta_s$, *and* $-(2+\eta_s)$ *are not squares in k_v.*

In this case, $\mathrm{Ker}(G,S)$ *has order* 2.

PROOF. Since the centre of a group is not changed by an inner twist, $Z = \mu_m$. Therefore,

$$H^1(k,Z) = H^1(k,\mu_m) = k^\times/k^{\times m}$$

and

$$H^1(k_v,Z) = H^1(k_v,\mu_m) = k_v^\times/k_v^{\times m}.$$

Consequently,

$$\mathrm{Ker}(G,S) = \{a \in k^\times \mid a \text{ is a local } m\text{th power for all } v \notin S\}/k^{\times m}.$$

This is precisely the set studied by the Grunwald-Wang theorem, and so the proposition is an immediate consequence of that theorem (Artin and Tate 1961, p. 96). (The Grunwald-Wang theorem is a direct consequence of the above lemma.) □

EXAMPLE 1.3. The simplest example where the Hasse principle fails is the following: $k = \mathbb{Q}$, $G = \mathrm{SL}_8$, and $S = \{2\}$. Then $\mathrm{Ker}(G,S)$ consists of elements of $\mathbb{Q}^\times$ that are 8th powers locally at all primes of k except 2, modulo global 8th powers. It is easily seen that 16 is an 8th power at all such primes, but it is obviously not an 8th power in $\mathbb{Q}$ (ibid., p. 96).

REMARK 1.4. If $\eta_m \in k$, then $\mathrm{Ker}(G,S) = 0$.

2 Outer forms of SL_m

The group of outer automorphisms of SL_m has order 2, and so, modulo inner twists, SL_m has a unique outer form for each quadratic extension F of k. The centre of this outer form is $\mu'_m =_{\mathrm{df}} \mathrm{Ker}(m\colon T' \to T')$, where T' is the torus over k whose k-rational points are the elements of norm 1 in $F^\times$. We analyse the action of $\mathrm{Gal}(\bar{k}/k)$ on μ'_m.

Fix a quadratic extension F of k, and let $T = \mathrm{Res}_{F/k}(\mathbb{G}_m)$. Then

$$T(\bar{k}) = (\bar{k}^\times)^{\mathrm{Hom}(F,k)} \approx \bar{k}^\times \times \bar{k}^\times.$$

An element τ of $\mathrm{Gal}(\bar{k}/k)$ acts according to the rule

$$(\tau\alpha)(\sigma) = \tau\alpha(\tau^{-1}\circ\sigma), \quad \sigma \in (\bar{k}^\times)^{\mathrm{Hom}(F,\bar{k})}.$$

The map $T(k) \hookrightarrow T(\bar{k})$ is $a \mapsto (\sigma a)_\sigma \colon F^\times \to (\bar{k}^\times)^{\mathrm{Hom}(F,\bar{k})}$. The norm map $T \to \mathbb{G}_m$ is $(\alpha_\sigma) \mapsto \prod \alpha_\sigma \colon (\bar{k}^\times)^{\mathrm{Hom}(F,\bar{k})} \to \bar{k}^\times$.

Now write $\mathrm{Gal}(F/k) = \{1, \sigma\}$, and identify $T(\bar{k})$ with $\bar{k}^\times \times \bar{k}^\times$ (the factors correspond to 1 and σ respectively). Then $\tau \in \mathrm{Gal}(\bar{k}/k)$ acts according to the rule:

$$\tau|F = \mathrm{id}; \text{ then } \tau(\alpha, \beta) = (\tau\alpha, \tau\beta);$$
$$\tau|F = \sigma; \text{ then } \tau(\alpha, \beta) = (\tau\beta, \tau\alpha).$$

(Check:

$$(\alpha, \beta) \text{ is fixed by all } \tau \text{ fixing } F \iff (\alpha, \beta) \in F \times F;$$
$$(\alpha, \beta) \text{ is fixed by all } \tau \text{ fixing } k \iff \alpha \in F \text{ and } \beta = \alpha.)$$

The map $T(k) \hookrightarrow T(\bar{k})$ is $a \mapsto (a, \sigma a) \colon F \hookrightarrow \bar{k}^\times \times \bar{k}^\times$. The norm map $T \to \mathbb{G}_m$ is $(\alpha, \beta) \mapsto \alpha\beta$.

Let T' be the kernel of the norm map $T \to \mathbb{G}_m$. Then $T'(\bar{k})$ is the subset (α, α^{-1}) of $\bar{k}^\times \times \bar{k}^\times$. Use the first coordinate to identify $T'(\bar{k})$ with $\bar{k}^\times$. Then $\tau \in \mathrm{Gal}(\bar{k}/k)$ acts according to the rule:

$$\tau|F = \mathrm{id}; \text{ then } \tau * \alpha = \tau\alpha;$$
$$\tau|F = \sigma; \text{ then } \tau * \alpha = \tau\alpha^{-1}.$$

Let μ'_m be the kernel of multiplication by m on T'. Then μ'_m becomes isomorphic to μ_m over F. Let 2^t be the power of 2 dividing m, and let ζ generate $\mu_{2^t}(F) = \mu'_{2^t}(F)$; thus $\zeta = \zeta_{2^s}$ for some $s \leq t$, and $\mu_{2^t}(F) = \langle \zeta \rangle$. Then

$$\sigma * \zeta = \sigma(\bar{\zeta}).$$

Since $\mathrm{Aut}(\mathbb{Z}/2^s\mathbb{Z})$ has only 4 elements of order dividing 2, namely, ± 1, $\pm 2^{s-1}$, when $s \geq 3$, there are 4 possible actions of σ on ζ. They are:

(i) $\sigma\zeta = \bar{\zeta}$; then $\sigma * \zeta = \zeta$;

(ii) $\zeta \in k$, so that $\sigma\zeta = \zeta$; then $\sigma * \zeta = \bar{\zeta}$;

(iii) $\sigma\zeta = -\bar{\zeta}$; then $\sigma * \zeta = -\zeta \quad (s \geq 3)$;

(iv) $\sigma\zeta = -\zeta$; then $\sigma * \zeta = \bar{\zeta} \quad (s \geq 3)$.

PROPOSITION 2.1. *Let G be an outer form of SL_m over k corresponding to a quadratic extension F of k, and let S be a finite set of primes. Then there is an exact sequence*

$$0 \to \mathrm{Ker}(F/k, G, S) \to \mathrm{Ker}(G, S) \to \mathrm{Ker}(G_F, S)$$

where

$$\mathrm{Ker}(F/k, G, S) = \mathrm{Ker}\left(H^1(F/k, Z) \to \prod_{v \notin S} H^1(F_w/k_v, Z) \right).$$

Moreover, $\mathrm{Ker}(F/K, G, S) = 0$ *unless*

(a) *we are in case (ii) (hence $\zeta = \zeta_{2^s} \in k$),*

(b) $2^{s+1}|m$ *(by our notations, $\zeta_{2^{s+1}} \notin F$), and*

(c) *S contains v if v does not split in F and $\zeta_{2^{s+1}} \notin F_v$.*

In this case, $\mathrm{Ker}(F/k, G, S)$ *has order* 2.

PROOF. The exact sequence follows immediately from the diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^1(\mathrm{Gal}(F/k, Z) & \longrightarrow & H^1(k, Z) & \longrightarrow & H^1(F, Z) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \prod H^1(\mathrm{Gal}(F_w/k_v, Z) & \longrightarrow & \cdots & \longrightarrow & \cdots
\end{array}$$

Let $M = Z(F)(2) = \langle \zeta \rangle$. Then

$$H^1(\mathrm{Gal}(F/k), M) =_{\mathrm{df}} \mathrm{Ker}(1+\sigma)/\mathrm{Im}(1-\sigma).$$

In the four cases, a direct computation shows that

(i) $H^1(\mathrm{Gal}(F/k), M) = \{\pm 1\}$;

(ii) $H^1(\mathrm{Gal}(F/k), M) = \langle \zeta \rangle / \langle \zeta^2 \rangle$;

(iii) $H^1(\mathrm{Gal}(F/k), M) = 0$;

(iv) $H^1(\mathrm{Gal}(F/k), M) = 0$;

Thus $\mathrm{Ker}(F/k, G, S) = 0$ in cases (iii) and (iv). Consider case (i) and choose a prime v of k remaining inert in F; then the same calculation shows that $H^1(\mathrm{Gal}(F_v/k_v), M) = \{\pm 1\}$ and the map from the global group to the local group is an isomorphism (note that s may change, but that doesn't matter in this case). Thus, $\mathrm{Ker}(F/k, G, S) = 0$ in case (i) also.

It remains to consider (ii). Let v be a prime of k.

(a) If v splits in F, then the map from the global group to the local group is zero.

(b) Assume v does not split in F, and let w be the prime lying over it. Let ζ' generate $Z(F_w)(2)$; thus $\zeta = \zeta'$ or else it is a power of it. The same calculation as in the global situation shows $\langle \zeta' \rangle / \langle \zeta'^2 \rangle$. Since the map from the global group to the local group is the obvious one, we see that it is bijective if and only if $\zeta' = \zeta$; otherwise, it is zero. We see therefore that $\mathrm{Ker}(F/k, G, S) = 0$ if and only if there is a nonsplit $v \notin S$ such that ζ generates $Z(F_w)(2)$. This proves the proposition. □

EXAMPLE 2.2. The simplest example where $\mathrm{Ker}(F/k, G, S) \neq 0$ is the following. Let $k = \mathbb{Q}$, and let F be any quadratic extension of $\mathbb{Q}$ not containing i. Let G be an outer form of SL_4 corresponding to F. There are only finitely many primes v of $\mathbb{Q}$ such that v does not split in F and $F_w \quad (w|v)$ does not contain i (if v does not split in F and is unramified in both F and $\mathbb{Q}(i)$, then $\mathbb{Q}_v(i) \subset F_w$). Choose S to be any finite set of primes of $\mathbb{Q}$ containing all these primes. Then $\zeta = -1$ (so $s = 1$) , and we are in case (ii), $4|m$, and S contains v if v does not split in F and $i \notin F_w$.

REMARK 2.3. The proposition shows that the order of $\mathrm{Ker}(G, S)$ divides 4. It looks easy to write down examples where it is exactly 4 (although I haven't done this), and it is probably possible to find examples where it is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and where it is $\mathbb{Z}/4\mathbb{Z}$. In particular, I don't believe Raghunathan 1981, Lemma 2.1. (There is an error in his proof on p. 329 where he forgets the special case of the Grunwald-Wang theorem.)

3 Groups with no factors of type A

THEOREM 3.1. *Let G be a simply connected semisimple group over a number field k. The kernel* $\mathrm{Ker}(G,S)$ *is zero if G has no factors of type A_m.*

PROOF. We can write $G=\prod G_i$, where $G_i = \mathrm{Res}_{k_i/k}\, G^i$ with G^i absolutely almost simple (Milne 2017, 24.3). As $Z(G)=\prod Z(G_i)=\prod \mathrm{Res}_{k_i/k}\, Z(G^i)$, and $\mathrm{Ker}(G,S)=\prod \mathrm{Ker}(G^i,S)$ (S also denotes the set of primes of k_i lying over a prime of S) we can assume that G itself is absolutely almost simple (and simply connected). □

PROPOSITION 3.2. *Let G be an absolutely almost-simple group over a number field k, and let S be any finite set of primes of k. Then* $\mathrm{Ker}(G,S)=0$.

PROOF. Apply the next lemma to $M =_{\mathrm{df}} Z(\bar{k})$. □

LEMMA 3.3. *Let M be a* $\mathrm{Gal}(\bar{k}/k)$*-module, and assume that there is a Galois extension L of k such that*

(a) *the action of* $\mathrm{Gal}(\bar{k}/k)$ *factors through* $\mathrm{Gal}(L/k)$*;*

(b) *for all primes ℓ dividing the order of M, the ℓ-Sylow subgroup of* $\mathrm{Gal}(L/k)$ *is cyclic.*

Then, for every set of primes S of k,

$$H^1(k,M)\to\prod_{v\notin S} H^1(k_v,M)$$

is injective.

PROOF. Well-known (and easy). □

Now apply the following table (Milne 2017, pp. 516–517):

Type	Centre	OutAut
B_n	μ_2	1
C_n	μ_2	1
D_4	$\mu_2\times\mu_2$	S_3
D_{2n} $(n>2)$	$\mu_2\times\mu_2$	$\mathbb{Z}/2\mathbb{Z}$
D_{2n+1}	μ_4	$\mathbb{Z}/2\mathbb{Z}$
E_6	μ_3	$\mathbb{Z}/2\mathbb{Z}$
E_7	μ_2	1
E_8, F_4, G_2	1	1

Postscript December 11, 2003

For applications to Shimura varieties, it is interesting to have an example where the Hasse principle fails for $Z(G)$ in the following case:

(a) G is simply connected,

(b) the ground field k is totally real, and

(c) S consists of the infinite primes.

Take $k = \mathbb{Q}[\sqrt{7}]$. Then

$$k^{\times}/k^{\times 8} \to \prod_{v \text{ finite}} k_v^{\times}/k_v^{\times 8}$$

is not injective.[1] Thus, the Hasse principle fails for the centre of an inner form of SL_8 over k, and therefore also for the centre of the simply connected group over $\mathbb{Q}$ obtained from an inner form of SL_8 by restriction of scalars.

References.

Artin, E., and Tate, J., 1961, Class Field Theory, Harvard University, Department of Mathematics.

Raghunathan, M. S., 1981, Isogenies and congruence subgroups. Manifolds and Lie groups (Notre Dame, Ind., 1980), pp. 325–336, Progr. Math., 14, Birkhäuser, Boston, Mass.

Milne, J., 2017, Algebraic groups, The theory of group schemes of finite type over a field, Cambridge University Press, 2017.

[1] Neukirch, Jürgen; Schmidt, Alexander; Wingberg, Kay. Cohomology of number fields. Grundlehren der Mathematischen Wissenschaften, 323. Springer-Verlag, Berlin, 2000, p. 459.