Quadratic Extensions of Local and Global Fields

BY DANIEL BUMP

Class Field Theory is the study of abelian extensions of local and global fields. It also encompasses the theory of central simple algebras over local and global fields. In these notes we will study the special case of quadratic extensions, and quaternion division algebras. Many aspects of the general case are already present.

1 Central Simple Algebras

In this section, an *algebra* over a field F will be a finite-dimensional associative algebra, that is, a ring A containing F in its center such that $\dim_F(A) < \infty$. A *module* over a ring will be always be a left module.

Let R be a ring. An R-module M is called *semisimple* or *completely reducible* if for every R-submodule N there exists an R-submodule P such that $M = N \oplus P$. A submodule P such that $M = N \oplus P$ is called *complementary* to N in M. If N has a complement, we say that N is *complemented*, so the condition of semisimplicity can be expressed by saying that every submodule is complemented.

Proposition 1. *Let M be a completely reducible module over a ring R. Then any submodule or quotient module of M is completely reducible.*

Proof. First, suppose that U is a quotient module of M and V a submodule of U. We may write $U \cong M/K$ for some submodule K of M. Then if N is the preimage of V in M, there exists a submodule P of M such that $M = N \oplus P$. The image W of P in U is a submodule satisfying $U = V \oplus W$, proving that U is semisimple.

If now N is a submodule of N, then $M = N \oplus P$ for some submodule P and $N \cong M/P$. Since we have already proved that quotient modules are semisimple, it follows that N is semisimple. □

If M is an R-module, M is called *simple* or *irreducible* if M is nonzero and has no proper nontrivial submodules. For example if $\mathfrak{m}$ is a maximal left ideal then $R/\mathfrak{m}$ is simple.

Proposition 2. (Schur's Lemma) *Let M be a simple R-module. Then $\mathrm{End}_R(M)$ is a division ring.*

Proof. If $f \in \mathrm{End}_R(M)$ is a nonzero endomorphism, then $\ker(f)$ is a proper submodule, so $\ker(f) = 0$. Similarly the image $\mathrm{im}(f)$ is a nonzero submodule, so $\mathrm{im}(f) = M$. We see that f is bijective, and its inverse map is also in $\mathrm{End}_R(M)$. This proves that every nonzero element of $\mathrm{End}_R(M)$ is invertible, so $\mathrm{End}_R(M)$ is a division ring. □

Lemma 3. *If M is a nonzero semisimple R-module, then M contains a simple submodule.*

Proof. Let $0 \neq x \in M$. Then Rx is a nonzero submodule of M, hence is semisimple. It is sufficient to show that Rx contains a simple submodule. Hence we may assume that $M = Rx$.

Let $\mathrm{Ann}(x) = \{r \in R | rx = 0\}$. Since $x \neq 0$, $\mathrm{Ann}(x)$ is proper, so let $\mathfrak{m}$ be a maximal left ideal containing $\mathrm{Ann}(x)$. Then $\mathfrak{m}/\mathrm{Ann}(x)$ is a submodule of the semisimple module $R/\mathrm{Ann}(x) \cong Rx = M$, so it has a complementary submodule P, which is isomorphic to $R/\mathfrak{m}$ and therefore simple. □

Proposition 4. *Let M be a module over the ring R. The following are equivalent.*
(i) M is a sum of simple modules.
(ii) M is a direct sum of simple modules.
(iii) M is semisimple.

Proof. It is clear that (ii) implies (i).

Let us show that (i) implies (iii). If M is a sum of simple modules and N is a submodule, we claim that N is complemented. If not, let P be a maximal submodule such that the sum $N \cap P = 0$. The existence of P follows from Zorn's Lemma. We claim that $N + P = M$, so that P is a complement of N. If not, then $N + P$ is a proper submodule of M, and since M is generated by simple modules, there is a simple module M_0 such that $M_0 \nsubseteq N + P$. Then $M_0 \cap (N + P)$ is a proper submodule of M_0, hence zero. This means that if $P' = P + M_0$ then P' is strictly larger than P and $P' \cap N = 0$. This contradicts the maximality of P.

Next we claim that (iii) implies (ii). Assuming M is semisimple, let N be a submodule of M which maximal with respect to the property that it is a direct sum of simple modules. The existence of such N is easily proved by Zorn's Lemma. If N is proper, then it is complemented, and its complement is nonzero, hence contains a simple module by Lemma 3. Adding this submodule to N gives a larger module which is a direct sum of simple modules, contradicting the maximality of N. □

Let A be a ring, and M an A-module. Then M is also naturally a module over the ring $\mathrm{End}_A(M)$ of A-module endomorphisms of M, namely if $f \in \mathrm{End}_A(M)$ and $m \in M$ we define $f \cdot m = f(m)$.

Theorem 5. (Jacobson) *Let A be a ring and M a semisimple A-module. Regard M as a module for $B = \mathrm{End}_A(M)$. Then if $\alpha \in \mathrm{End}_B(M)$ and if $m_1, \cdots, m_r \in \mathrm{End}_B(M)$, there exists $\lambda \in A$ such that $\lambda m_i = \alpha m_i$ for $i = 1, \cdots, r$.*

This is the *Jacobson Density Theorem.*

Proof. First we consider the case where $r = 1$. Denoting $m_1 = m$, we must show that if $m \in M$ then $\alpha m \in Am$. Note that Am is an A-submodule, and since M is semisimple it is complemented. Let $M = Am \oplus N$, where N is another submodule, and let $p: M \longrightarrow M$ be the projection map, which is the identity on Am and zero on N. Clearly $p \in \mathrm{End}_A(M) = B$, so α commutes with p. Thus $\alpha m = \alpha p(m) = p\alpha(m) \in \mathrm{Im}(p) = Am$, and the case $r = 1$ is settled.

In general, note that $M^r = M \oplus \cdots \oplus M$ (r copies) is a semisimple module, and we can apply the special case just proved to it with $m = (m_1, \cdots, m_r)$. The statement that $\lambda m = \alpha m$ means that $\lambda m_i = \alpha m_i$, and the result follows. □

A ring R is called *semisimple* if R is itself semisimple as a left R-module.

Proposition 6. *Let R be a semisimple ring. Then any R-module is semisimple.*

Proof. Let M be an R-module. Then if m_i ($i \in I$) are generators (possibly infinitely many) we can represent M as a quotient of $R^I = \bigoplus_{i \in I} R$. Indeed, R^I may be identified with the set of functions $f: I \longrightarrow R$ such that $f(i) = 0$ for all but finitely many I, and we can map $R^I \longrightarrow M$ surjectively by sending $f \longmapsto \sum_i f(i) m_i$. Since R is a direct sum of simple modules, so is R^I, and therefore R^I is semisimple. Because a quotient of a semisimple module is semisimple, so is M. □

Theorem 7. (Wedderburn) *Let R be a semisimple ring. Then R has finitely many isomorphism classes of simple modules. Let V_i ($i = 1, \cdots, n$) be a set of representatives of these classes. Let R_i be the sum of all left ideals of R which are isomorphic to V_i. Then R_i is a two-sided ideal and*

$$R = R_1 \oplus \cdots \oplus R_n.$$

Let us write $1 = e_1 + \ldots + e_n$, where $e_i \in R_i$. Then e_i are central idempotents and $e_i e_j = 0$ if $i \neq j$. The ideal R_i is a ring with unit e_i.

Proof. Let V_i ($i \in I$) be representatives of the distinct isomorphism classes of simple R-modules. We will prove later that there are only finitely many of these but for the time being we accept the possibility that the indexing set I might be infinite.

If L is a simple left ideal then observe that

$$LV_i = \begin{cases} V_i & \text{if } L \cong V_i \text{ as } R\text{-modules;} \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

Indeed, if $LV_i \neq 0$, then $LV_i = V_i$ since V_i is simple and LV_i is a submodule. Let $v \in V_i$ such that $Lv \neq 0$. Then $x \longmapsto xv$ is a nontrivial R-module homorphism $L \longrightarrow V_i$, and since both are simple, it is an isomorphism. This proves (1).

Now let R_i be the sum of left ideals isomorphic to V_i. We claim that R_i is a two-sided ideal. It is clearly a left ideal. On the other hand, if L is a left ideal isomorphic to V_i, and if $a \in R$, then either $La = 0$, or $La \cong L$, since $x \longmapsto La$ is then a nonzero R-module homomorphism $L \longrightarrow La$. Thus R_i is closed under right multiplication by a, and is therefore a two-sided ideal. By (1) we have

$$R_i R_j = \begin{cases} 0 & \text{if } i \neq j; \\ R_i & \text{if } i = j. \end{cases} \tag{2}$$

Since R is semisimple, it is a direct sum of simple left ideals. Since each of these is contained in one of the R_i, we have $R = \sum_{i \in I} R_i$. Write $1 = \sum_{i \in I} e_i$, where $e_i \in R_i$. All but finitely many e_i are zero. On the other hand, $V_j = 1 \cdot V_j = \sum e_i \cdot V_j = 0$ if $e_i = 0$ by (1), which is a contradiction since by definition a simple module is nonzero. Thus the index set I is finite, and we may take $I = \{1, 2, 3, \cdots, n\}$.

Let us show now that if $x \in R_i$ then

$$e_j x = x e_j = \begin{cases} x & \text{if } i = j; \\ 0 & \text{if } i \neq j. \end{cases} \tag{3}$$

By (2), we have $e_j x = x e_j = 0$ if $j \neq i$. On the other hand we have $x = 1 \cdot x = \sum_j e_j \cdot x$, and taking into account the single nonzero term, $e_i x = x$, and similarly $x e_i = x$. The fact that e_i is in the center of R is now clear, since it commutes with the elements of R_j for every J.

By (2) and (3), it is clear that R_i is a ring with unit e_i.

Now let us show that the sum $R = \sum R_i$ is direct. Suppose that $\sum_i r_i = 0$, where $r_i \in R_i$. Multiplying by e_i shows that each $r_i = 0$. □

An ideal N of a ring A is called *nilpotent* if $N^r = 0$. A ring R is called (left-) *Artinian* if any descending chain $I_1 \supset I_2 \supset \cdots$ of left ideals eventually terminates.

(Strictly speaking we should distinguish between left- and right-Artinian rings, but the two concepts coincide for semisimple rings, so this distinction will not be important for us. The coincidence of the left- and right-Artinian properties is not hard to prove though we will not prove it.)

Particularly, an algebra over a field (assumed, as always in this section, finite-dimensional) is clearly Artinian. A *simple* or *irreducible* left R-module is a nonzero left R-module with no proper, nontrivial submodules. If M is a left R-module, its *annihilator* $\mathrm{Ann}(M) = \{x \in R \,|\, xM = 0\}$.

Proposition 8. *Let R be a ring. Let $J(R)$ be the intersection of the maximal left ideals of R. Then $J(R)$ is also the intersection of the annihilators of all simple left R-modules. It is a two-sided ideal. If R is Artinian, then $J(R)$ is the unique maximal nilpotent two-sided ideal of R.*

The ideal $J(R)$ is called the *Jacobson radical.*

Proof. We first note that if I is a maximal left ideal, then R/I is a simple left R-module. Moreover, if M is a simple left R-module, then $M \cong R/I$ for some I, since if we choose $0 \neq m \in M$ then Rm is a nonzero submodule of M, hence $Rm = M$, and the kernel of the homomorphism $x \longmapsto xm$ is an ideal I such that $R/I \cong M$, and I must be maximal since M is simple. Thus

$$\bigcap_{I \text{ maximal}} \mathrm{Ann}(R/I) = \bigcap_{M \text{ simple}} \mathrm{Ann}(M).$$

Evidently if I is any ideal $\mathrm{Ann}(R/I)$ is a two-sided ideal contained in I, so $\bigcap \mathrm{Ann}(M)$ is contained in $J(R)$. To prove the converse, suppose that M is a simple R-module; we show that $J(R)M = 0$. If not, suppose that $m \in M$ such that $J(R)m \neq 0$. Since M is simple, $J(R)m = M$, and so $xm = m$ for some $x \in J(R)$. Now $R(1-x)$ cannot be a proper left ideal since otherwise it is contained in some maximal left ideal I; but $x \in I$ so $1 \in I$, which is a contradiction. Thus $R(1-x) = R$, so $u(1-x) = 1$ for some u. Now $m = u(1-x)m = 0$, which is a contradiction. We have proved that $J(R) = \bigcap \mathrm{Ann}(M)$. It is an intersection of 2-sided ideals, hence a two-sided ideal.

Note that if M is any nonzero R-module, then $J(R)M$ is a proper submodule of M. Indeed, let M_0 be any maximal submodule of M. Clearly M/M_0 is simple, so $J(R)$ annihilates it; thus $J(R)M \subseteq M_0$. It follows that the sequence of ideals $J(R) \supset J(R)^2 \supset J(R)^3 \supset \cdots$ is properly decreasing until (perhaps) it terminates, and if R is Artinian, it *must* terminate, so $J(R)$ is nilpotent. On the other hand, if N is a nilpotent ideal, and M is a simple R-module, then $NM = 0$, since otherwise $M = NM$, hence $M = N^r M$ for all r, which is a contradiction when $N^r = 0$. This shows that $N \subseteq J(R)$. □

Proposition 9. *Let R be an Artinian ring. Then R is semisimple if and only if $J(R) = 0$.*

Proof. If R is semisimple, then it is a direct sum of simple modules. Thus $J(R)R = 0$, so $J(R) = 0$.

Suppose that the intersection $J(R)$ of all maximal left ideals is zero. Since R is Artinian, there is a finite set $I_1, \cdots, I_n$ of maximal left ideals whose intersection is zero. This means that the canonical map

$$R \longrightarrow \bigoplus_{i=1}^{n} (R/I_i)$$

is injective. Thus R is embedded in a direct sum of simple modules, hence is semisimple. □

If R is any ring, let R^{opp} be the algebra obtained from R by reversing the multiplication. Thus, R and R^{opp} are equal as additive groups, but denoting the multiplication in R by $\cdot$ and the multiplication in R^{opp} by $*$ the product in R^{opp}, we have $x * y = y \cdot x$.

Lemma 10. *Let R be a ring. Then $\text{End}_R(R) \cong R^{\text{opp}}$.*

Proof. If $x \in R$ let $\rho_x \colon R \longrightarrow R$ be the map $\rho_x(r) = rx$. Since $\rho_x(tr) = trx = t\,\rho_x(r)$, we have $\rho_x \in \text{End}_R(R)$. Moreover $\rho_x \rho_y = \rho_{yx}$, so $x \longmapsto \rho_x$ is a homomorphism $R^{\text{opp}} \longrightarrow \text{End}_R(R)$. This homomorphism is injective since $x = \rho_x(1)$. To see that it is surjective, let $\varphi \in \text{End}_R(R)$ and let $x = \varphi(1)$. Then $\varphi(r) = \varphi(r \cdot 1) = r\varphi(1) = rx = \rho_x(r)$, so $\varphi = \rho_x$. □

Lemma 11. *Let R be a ring and V a simple R-module. Let $D = \text{End}_R(V)$, and let $V^n = V \oplus \cdots \oplus V$ (n copies). Then $\text{End}_R(V^n) \cong \text{Mat}_n(D)$.*

Proof. Indeed, if $\varphi = (\varphi_{ij}) \in \text{Mat}_n(D)$, then we have an endomorphism V^n mapping

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \longmapsto \begin{pmatrix} \sum \varphi_{1i} v_i \\ \vdots \\ \sum \varphi_{ni} v_i \end{pmatrix}.$$

It is easy to see that every endomorphism is of this type and so $\text{End}_R(V^n) \cong \text{Mat}_n(D)$. □

Proposition 12. *Let R be an Artinian ring. The following are equivalent.*

(i) R is semisimple and has a unique isomorphism class of simple modules.
(ii) R has no proper, nontrivial two-sided ideal.
(iii) $R \cong \mathrm{Mat}_n(D)$ where D is a division algebra over F.

An Artinian ring satisfying these equivalent conditions is called *simple*. (We will only consider simple rings that are Artinian.)

Proof. Let us show that (ii) implies (i). Since $J(R)$ is proper, the assumption that R has no proper, nontrivial two-sided ideal implies that $J(R) = 0$ and since R is Artinian, it is therefore semisimple. That it has a unique isomorphism class of ideals is clear from Wedderburn's Theorem 7, since otherwise the R_i in that theorem would be proper, nontrivial two-sided ideals.

Next we prove that (i) implies (iii). Assume that R is semisimple and has a unique isomorphism class of simple modules. Let $D \cong \mathrm{End}_R(V)$. It is a division algebra by Proposition 2. We will prove that $R \cong \mathrm{Mat}_n(D^{\mathrm{opp}})$, which is (iii) with D replaced by its opposite ring. By Lemma 10, it is enough to show that $\mathrm{End}_R(R) \cong \mathrm{Mat}_n(D)$. Since R is semisimple, we may write $R = \bigoplus_{i \in I} L_i$, where each L_i is a simple left ideal, and on our hypothesis each $L_i \cong V$. Since R is Artinian, the number of L_i in this decomposition is finite, so $R = L_1 \oplus \ldots \oplus L_n \cong V^n$ as an R-module. Now by Lemma 11 we have $\mathrm{End}_R(R) \cong \mathrm{End}_R(V^n) \cong \mathrm{Mat}_n(D)$.

Finally, to prove that (iii) implies (ii), we must show that $R = \mathrm{Mat}_n(D)$ has no proper, two-sided ideals. It is straightforward to show that if $x \in \mathrm{Mat}_n(D)$ is any nonzero matrix, then $RxR = R$, so the ideal generated by x is not proper. □

Theorem 13. (Wedderburn) *A semisimple Artinian ring is a direct sum of matrix rings, each of which is a matrix ring over a division ring.*

Proof. This follows from combining Theorem 7 with Proposition 12. □

Suppose that A and B are algebras over a field F. Then $A \otimes B = A \otimes_F B$ is also an algebra with multiplication satisfying

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'.$$

The ring $A \otimes B$ contains copies of A and B, namely the subrings $A \otimes 1$ and $1 \otimes B$.

An F-algebra A is called *central* if the center of A is F. The importance of centrality in the proofs to come is shown by the following considerations.

Example 14. It is not always true that the tensor product of semisimple algebras is semisimple. If F has characteristic p and E/F is a nontrivial purely inseparable field extension, then $E \otimes E$ will be a commutative ring containing nonzero nilpotent elements. Wedderburn's Theorem shows that a commutative semisimple Artinian ring is a direct sum of fields, and so cannot contain nonzero nilpotents. To give a precise instance, let T be an indeterminate, and let $E = \mathbb{F}_p(T)$ be the field of fractions of the polynomial ring $\mathbb{F}_p[T]$, where p can by any prime. Let $F = \mathbb{F}_p(T^p)$. Then E/F is a purely inseparable extension of degree p. The element $T \otimes 1 - 1 \otimes T$ is nilpotent since raising it to the p-th power gives $T^p \otimes 1 - 1 \otimes T^p$.

Nevertheless, it is still true that if A and B are semisimple then so is $A \otimes B$, provided one of A and B is central.

Proposition 15. *Let A and B be algebras over F. Assume that B is central.*
(i) If A and B are semisimple then $A \otimes B$ is a semisimple algebra.
(ii) If A and B are simple then $A \otimes B$ is a semisimple algebra.

Proof. First note that (ii) implies (i), since an F-algebra is semisimple if and only if it is a direct sum of simple algebras, and since the tensor product is distributive over direct sums.

We must prove (ii). Assume that A and B are simple. Let $I \subseteq A \otimes B$ be a nontrivial ideal, and let

$$0 \neq u = \sum_{k=1}^{N} a_k \otimes b_k \in I$$

with the a_k linearly independent and N minimal. Since B is simple, the two-sided ideal generated by b_N is not proper, that is, $Bb_NB = B$. This means that left and right multiplying by elements of $1 \otimes B$ we may assume that $b_N = 1$. Now if $\beta \in B$ we have

$$\sum_{k=1}^{N-1} a_k \otimes (\beta b_k - b_k \beta) = (1 \otimes \beta)\left[\sum_{k=1}^{N} a_k \otimes b_k\right] - \left[\sum_{k=1}^{N} a_k \otimes b_k\right](1 \otimes \beta) \in I.$$

The minimality of N implies that $\beta b_k - b_k \beta = 0$ for all k, so the $b_k \in F$ and therefore $u \in A \otimes 1$. Now since $A \otimes 1 \cong A$ is simple, the ideal generated by u is all of $A \otimes 1$ and in particular $1 \otimes 1 \in I$. Thus $I = A \otimes B$ proving that $A \otimes B$ is simple. □

Lemma 16. *Let A and B be algebras over F, and assume that B is central. Identify $A = A \otimes 1$ and $B = 1 \otimes B$ with their images in $A \otimes B$. Then $x \in A \otimes B$ commutes with all elements of B if and only if $x \in A$.*

Proof. Let $a_1, \cdots, a_n$ be an F-basis of A. Write

$$x = \sum_k a_k \otimes b_k, \qquad b_k \in B.$$

Then if x commutes with $\beta \in B$ we have

$$0 = (1 \otimes \beta)x - x(1 \otimes \beta) = \sum_k a_k \otimes (\beta b_k - b_k \beta).$$

Since the a_k are linearly independent, this means that all b_k commute with β. Hence if x commutes with all elements of B, the b_k are in F and hence $x \in A$. □

Proposition 17. *Let F be a field, and let A and B be F-algebras. Assumpe that B is central. Suppose that Z is the center of A, so that $F \subseteq Z \subseteq A$. Then the center of $A \otimes B$ is $Z \otimes 1$.*

Proof. Suppose that $z \in A \otimes B$ is in the center. Then by Lemma 16, $z \in A \otimes 1$, and since $Z \otimes 1$ is the center of $A \otimes 1$, it follows that $z \in Z \otimes 1$. □

We will use these results in two different ways.

- If A is an F-algebra and K/F is an extension field, then $K \otimes A$ is naturally a K-algebra. Its dimension over K is the same as the dimension of A over F. We see from Propositions 15 and 17 that if A is a central simple F-algebra then $K \otimes F$ is a central K-algebra. This algebra is said to be obtained from A by *extending the ground field*, or by *extension of scalars*.
- If A and B are central simple F-algebras then by Propositions 15 and 17 so is $A \otimes B$.

As an application of the first idea, let us show that central simple algebras become matrix rings when the ground field is extended sufficiently far. We will denote by $\bar{F}$ the algebraic closure of the field F.

Proposition 18. *Suppose that F is a field and A is central simple algebra. Then $\bar{F} \otimes A \cong \mathrm{Mat}_n(\bar{F})$ as $\bar{F}$-algebras for some n.*

Proof. Indeed, $\bar{F} \otimes A$ is a central simple algebra over $\bar{F}$, hence is isomorphic to a matrix ring $\mathrm{Mat}_n(D)$, where D is a central division algebra over $\bar{F}$. However D must equal $\bar{F}$ since if $x \in D$ then the field $\bar{F}(x)$ generated by x is finite-dimensional over $\bar{F}$, which is algebraically closed, so $\bar{F}(x) = \bar{F}$. The result follows. □

If A is a central simple algebra over F, then Proposition 18 shows that the dimension of A over F is n^2 for some n, and we call n the *reduced degree* of A.

Proposition 19. *Let A be a central simple algebra. Then*

$$A \otimes A^{\mathrm{opp}} \cong \mathrm{End}_F(A) \cong \mathrm{Mat}_{n^2}(F), \qquad n = \dim(A).$$

Proof. Consider the linear map $A \otimes A^{\mathrm{opp}} \longrightarrow \mathrm{End}_F(A)$, in which $a \otimes b$ is mapped to the endomorphism $L_{a \otimes b}\colon A \longrightarrow A$ such that $L_{a \otimes b}(x) = axb$. This is clearly a ring homomorphism, and its kernel is zero, since by Proposition 15 $A \otimes A^{\mathrm{opp}}$ has no proper nontrivial two-sided ideals. Comparing dimensions, it must be an isomorphism of $A \otimes A^{\mathrm{opp}}$ onto $\mathrm{End}_F(A) \cong \mathrm{Mat}_{n^2}(A)$. □

Proposition 20. *Let E be a finite-dimensional F-vector space, and let A be a semisimple F-subalgebra of $\mathrm{End}_F(E)$. Let $R = \mathrm{End}_A(E)$. Then R is semisimple and $A = \mathrm{End}_R(E)$.*

Proof. The fact that $A = \mathrm{End}_R(E)$ is a special case of the Jacobson Density Theorem. Thus our main task is to confirm the semisimplicity of R.

We recall that any module over a semisimple ring is semisimple. Let $V_1, V_2, \cdots$ be representatives of the isomorphism classes of irreducible left A-modules, and let E_i be the V_i-*isotypic* part if E, that is, the sum of all submodules isomorphic to V_i. Thus

$$E = E_1 \oplus \cdots \oplus E_r$$

where each E_i is an R-submodule of E that consists of the direct sum of several copies of the same simple R-module. Since A is a ring of endomorphisms of E, and since each E_i is an A-submodule, we may write $A = A_1 \oplus \cdots \oplus A_r$ where A_i is the image of A in $\mathrm{End}_F(E_i)$. It is also clear that any A-module endomorphism of E maps E_i into itself. Thus

$$R = \bigoplus R_i, \qquad R_i = \mathrm{End}_A(E_i) = \mathrm{End}_{A_i}(E_i).$$

If we know that R_i is semisimple, then the Proposition is proved also for A and E.

Thus we reduce to the case where E is isotypic, that is, $E \cong V^n$ is a direct sum of n copies of a fixed simple A-module V. Let $D = \mathrm{End}_A(V)$. Then D is a division ring by Schur's Lemma. Moreover, by Lemma 11, we have $\mathrm{End}_A(V^n) \cong \mathrm{Mat}_n(D)$. Thus in the isotypic case $\mathrm{End}_A(E)$ is a matrix ring over a division algebra and hence semisimple. □

If R is a ring and A a subring, the *commuting ring* of A in R is its centralizer, that is,

$$\{x \in R \mid xa = ax \text{ for all } a \in A\}.$$

Proposition 21. *Let R be a central simple algebra over the field F. Let A be a semisimple F-subalgebra of R, and let B be the commuting ring of A in R. Regard R as a left A-module. Then $\mathrm{End}_A(R) \cong B \otimes_F R^{\mathrm{opp}}$ as F-algebras. In this isomorphism, $b \otimes r \in B \otimes_F R^{\mathrm{opp}}$ corresponds to the linear transformation $x \longmapsto bxr$ of R.*

Proof. We have a map

$$\Phi\colon R \otimes R^{\mathrm{opp}} \longrightarrow \mathrm{End}_K(R), \qquad \Phi(u \otimes v)x = uxv.$$

By Proposition 19, Φ is a isomorphism of F-algebras. It is clear that $\Phi(B \otimes R^{\mathrm{opp}}) \subseteq \mathrm{End}_A(R)$, and we must show that we have equality.

Both $\Phi(B \otimes R^{\mathrm{opp}})$ and $\mathrm{End}_A(R)$ are semisimple F-subalgebras of $\mathrm{End}_F(R)$. Indeed, $\Phi(B \otimes R^{\mathrm{opp}}) \cong B \otimes R$ is semisimple by Proposition 15, and $\mathrm{End}_A(R)$ is semisimple by Proposition 20. It follows from Proposition 20 that if E is a finite-dimensional F-vector space, and if two semisimple subrings of $\mathrm{End}_F(E)$ have the same commuting ring, then they are equal. Also by Proposition 20, the commuting ring of $\mathrm{End}_A(R)$ is A. Thus it is sufficient to show that the commuting ring of $\Phi(B \otimes R^{\mathrm{opp}})$ in $\mathrm{End}_F(R)$ is A. We make use of the isomorphism Φ to transfer the problem of computing the commuting ring back to $B \otimes R^{\mathrm{opp}}$. Since $\Phi(A \otimes 1) = A$, it is sufficient to show that the commuting ring of $B \otimes R^{\mathrm{opp}}$ in $R \otimes R^{\mathrm{opp}}$ is $A \otimes 1$. By Lemma 16, the commuting ring of $B \otimes R^{\mathrm{opp}}$ is contained in $R \otimes 1$. Since the commuting ring of B in R is A by Proposition 20, it follows that the commuting ring of $B \otimes R^{\mathrm{opp}}$ is $A \otimes 1$, as required. □

Theorem 22. *Let D be a central division algebra of reduced degree d over the field F. Let K be a subfield of D containing F. The following conditions are equivalent.*
(i) The field K is a maximal subfield of D.
(ii) K is its own commuting ring in D.
(iii) The degree $[K\colon F]$ equals d.

(iv) $K \otimes D \cong \mathrm{End}_K(D)$ *as* F*-algebras, where* D *is regarded as a* K*-vector space via right-multiplication. In this isomorphism* $k \otimes u \in K \otimes D$ *corresponds to the linear transformation* $x \longmapsto uxk$ *of* D*.*

Proof. We begin by noting that the equivalence of (i) and (ii) is straightforward. Indeed if K is a maximal subfield and x commutes with K then since D is a division algebra $K[x]$ is a field containing K, so $x \in K$; and conversely, if K is not maximal then any element of a larger subfield is in the commuting ring of K in D.

Take $R = D^{\mathrm{opp}}$ in Proposition 21. If B is the commuting ring of K in D, then, then $B \otimes D \cong \mathrm{End}_K(D^{\mathrm{opp}})$ by Proposition 21. In that proposition, the rings A and B acted on R by left multiplication, but we have replaced R by D^{opp}, so now K and B act on D (which has the same underlying space as D^{opp}) by right multiplication. Thus $B \otimes D \cong \mathrm{End}_K(D)$ as F-algebras where K acts on D by right multiplication. This agrees with $K \otimes D$ if and only if $B = K$. Thus (iv) is also equivalent to (ii).

For the equivalence of (iii), let $n = [K\colon F]$. Since $B \otimes D \cong \mathrm{End}_K(D^{\mathrm{opp}})$, we have $B = K$ if and only if the dimensions of $K \otimes D$ and $\mathrm{End}_K(D^{\mathrm{opp}})$ are equal. We have $\dim(K \otimes D) = nd^2$, while $\dim_F \mathrm{End}_K(D^{\mathrm{opp}}) = (d^2/n)^2$, so these dimensions are the same if and only if $d = n$. □

Proposition 23. *Let* D *be a central division algebra over* F*, and let* $A = \mathrm{Mat}_n(D)$ *acting on* D^n *by matrix multiplication in the usual way. Then* $\mathrm{End}_A(D^n) \cong D^{\mathrm{opp}}$*.*

Proof. We have a homomorphism $\Phi\colon A \otimes D^{\mathrm{opp}} \longrightarrow \mathrm{End}_F(D^n)$ given by $\Phi(a \otimes d)x = axd$. Since $A \otimes D^{\mathrm{opp}}$ is simple, this ring homomorphism is injective, and the dimensions of both rings $A \otimes D^{\mathrm{opp}}$ and $\mathrm{End}_F(D^n)$ are $n^2 d^4$, where d is the reduced degree of D. Thus Φ is an isomorphism.

Now $\mathrm{End}_A(D^n)$ is by definition the commuting ring of A in $\mathrm{End}_F(D^n)$, but we may use the isomorphism Φ to transport the problem of computing this commuting ring back to $A \otimes D^{\mathrm{opp}}$, where the commuting ring of $A \otimes 1$ is $1 \otimes D^{\mathrm{opp}} \cong D^{\mathrm{opp}}$ by Lemma 16. □

Proposition 24. *If* D_1 *and* D_2 *are central division algebras over* F *and if* $\mathrm{Mat}_{n_1}(D_1) \cong \mathrm{Mat}_{n_2}(D_2)$*, then* $n_1 = n_2$ *and* $D_1 \cong D_2$*.*

Proof. Let $A = \mathrm{Mat}_n(D)$ be a central simple algebra. Let E be a representative of the unique isomorphism class of simple A-modules. We claim that $D^{\mathrm{opp}} \cong \mathrm{End}_A(E)$, which implies the result, since it shows that D is intrinsically determined by A and E. Indeed, we may take $E = D^n$ and this now follows from Proposition 23. □

We next define the *Brauer group* $B(F)$ of a field F. We define an equivalence relation on central simple algebras over F by $A \sim A'$ if $A \cong \mathrm{Mat}_n(D)$ and $A' \cong \mathrm{Mat}_m(D)$ with the same division algebra D. Let $[A]$ be the equivalence class of A. By Proposition 24, every equivalence class contains a unique division algebra, and we may identify the set $B(F)$ of equivalence classes with the set of isomorphism classes of central division algebras. The tensor product operation induces a multiplication on $B(F)$. Thus if A_1 and A_2 are central simple algebras, representing classes $[A_1], [A_2] \in B(F)$, then $A_1 \otimes A_2 \cong \mathrm{Mat}_n(D_3)$ for some uniquely determined division algebra D_3, and the class $[D_3]$ is the product of $[A_1]$ and $[A_2]$ in $B(F)$. It is not hard to see that this multiplication is associative, and the inverse in $B(F)$ of $[A]$ is $[A^{\mathrm{opp}}]$.

Proposition 25. *Let F be any field, and let $\tau\colon \mathrm{Mat}_n(F) \longrightarrow \mathrm{Mat}_n(F)$ be any automorphism. Then τ is inner: that is, $\tau(x) = \varphi x \varphi^{-1}$ for some $\varphi \in \mathrm{GL}_n(F)$ and all $x \in \mathrm{Mat}_n(F)$.*

Proof. Let $V = F^n$, and give V a new $\mathrm{Mat}_n(F)$-module structure by defining $x \cdot v = \tau(x)v$ for $x \in \mathrm{Mat}_n(F)$ and $v \in V$. Denote by V_τ the set V with this new $\mathrm{Mat}_n(F)$-module structure. Since $\mathrm{Mat}_n(F)$ is a simple algebra, it has a unique irreducible module, and so V_τ and V are isomorphic. Let $\varphi\colon V \longrightarrow V_\tau$ be a module homomorphism. Then, by definition, $\varphi(xv) = \tau(x)\,\varphi(v)$ which means that $\tau(x) = \varphi x \varphi^{-1}$. □

Let A be a central simple algebra over F. We fix an isomorphism $\theta\colon \bar{F} \otimes A \longrightarrow \mathrm{Mat}_n(\bar{F})$ as $\bar{F}$-algebras. Let $\sigma \in \mathrm{Gal}(\bar{F}/F)$. We will denote by σ_n and $\sigma \otimes 1$ the automorphisms of $\mathrm{Mat}_n(\bar{F})$ and $\bar{F} \otimes D$ induced by σ. Let $c_\sigma\colon \mathrm{Mat}_n(\bar{F}) \longrightarrow \mathrm{Mat}_n(\bar{F})$ be the composition

$$c_\sigma = \theta \circ (\sigma \otimes 1) \circ \theta^{-1} \circ {\sigma_n}^{-1}.$$

Thus we have a commutative diagram

$$\begin{array}{ccc}
\bar{F} \otimes A & \xrightarrow{\ \theta\ } & \mathrm{Mat}_n(\bar{F}) \\
\Big\downarrow{\scriptstyle \sigma\otimes 1} & & \Big\downarrow{\scriptstyle \sigma_n} \\
 & & \mathrm{Mat}_n(\bar{F}) \\
 & & \Big\downarrow{\scriptstyle c_\sigma} \\
\bar{F} \otimes A & \xrightarrow{\ \theta\ } & \mathrm{Mat}_n(\bar{F})
\end{array}$$

Lemma 26. *The map c_σ is an $\bar{F}$-linear automorphism of $\mathrm{Mat}_n(\bar{F})$.*

Proof. The maps $\sigma \otimes 1$ and σ_n are only F-linear, but they are automorphisms of $\bar{F} \otimes D$ and $\mathrm{Mat}_n(\bar{F})$. On the other hand θ is an $\bar{F}$-linear automorphism. To check that c_σ is $\bar{F}$-linear, if $\lambda \in \bar{F}$ and $g \in \mathrm{Mat}_n(\bar{F})$ we have

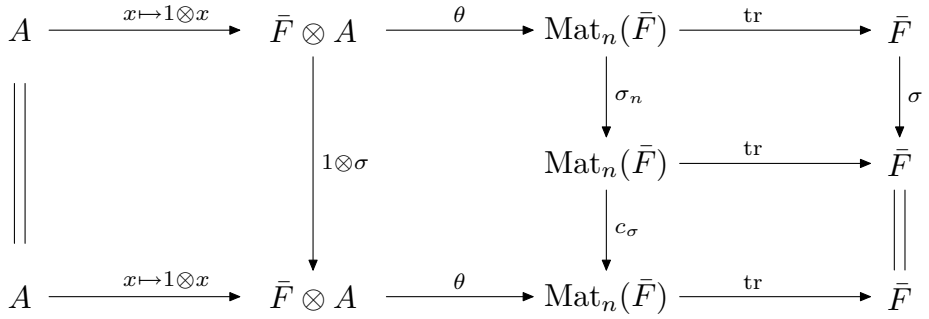
$$\begin{aligned}
&c_\sigma(\lambda g) = \theta \circ (\sigma \otimes 1) \circ \theta^{-1} \circ \sigma_n^{-1}(\lambda g) = \\
&\theta(\sigma \otimes 1)\theta^{-1}\sigma^{-1}(\lambda)\sigma_n(g) = \\
&\theta(\sigma \otimes 1)\sigma(\lambda)^{-1}\theta^{-1}\sigma_n(g) = \\
&\theta\lambda(\sigma \otimes 1)\,\theta^{-1}\sigma_n(g) = \lambda c_\sigma(g).
\end{aligned}$$

□

Theorem 27. *Let A be a central simple algebra over a field F of characteristic zero. Fix an $\bar{F}$-algebra isomorphism $\theta\colon \bar{F} \otimes A \longrightarrow \mathrm{Mat}_n(\bar{F})$. If $a \in A$ then the coefficients of the characteristic polynomial of $\theta(1 \otimes a)$ lie in F; in particular $\mathrm{tr}(\theta(1 \otimes a))$ and $\det(\theta(1 \otimes a))$ lie in F. Their values are independent of the choice of θ.*

For simplicity we will assume that F has characteristic zero. Otherwise, one must replace $\bar{F}$ by the separable closure F^{sep} throughout. Then one needs to know that $F^{\text{sep}} \otimes A$ is a matrix ring over F^{sep}. This is proved in Weil [4], Corollary to Proposition 5 on p. 165. With this fact, one may replace $\bar{F}$ by F^{sep}, and eliminate the assumption that $\text{char}(F) = 0$.

Proof. Let $a \in A$. It is sufficient to show that $\text{tr}(\theta(1 \otimes a))$ and $\det(\theta(1 \otimes a))$ are invariant under $\sigma \in \text{Gal}(\bar{F}/F)$. By Proposition 25 and Lemma 26 there is an element $\varphi \in \text{GL}_n(\bar{F})$ such that for $g \in \text{Mat}_n(\bar{F})$ we have $c_\sigma(g) = \varphi g \varphi^{-1}$. Now consider the following diagram. Each square commutes. In particular, the square in the lower right hand corner commutes since c_σ is conjugation by φ, and the trace is invariant under conjugation. Applying these maps to $a \in A$, we see that $\sigma(\text{tr}(1 \otimes a)) = \text{tr}(\theta(1 \otimes a))$, and so $\text{tr}(\theta(1 \otimes a)) \in F$.



If we change θ to another $\bar{F}$-linear isomorphism θ', we have $\theta' = \tau \circ \theta$, where τ is an automorphism of $\text{Mat}_n(\bar{F})$. The trace is unchanged by Proposition 25. The determinant and other coefficients of the characteristic polynomial of $\theta(1 \otimes a)$ are handled identically. □

We write $\text{tr}(a) = \text{tr}(\theta(1 \otimes a))$ and $\nu(a) = \det(\theta(1 \otimes a))$. They are called the *reduced norm* and *reduced trace*. We want to show that the restrictions of these to a maximal subfield are the ordinary field norm and trace, whose properties we quickly recall in Proposition 28.

Proposition 28. *Let K/F be a finite separable field extension of degree d, and let σ_i: $K \longrightarrow \bar{F}$ be the distinct embeddings, $i = 1, \cdots, d$.*
(i) There exists an isomorphism of $\bar{F}$-algebras

$$\bar{F} \otimes K \cong \bar{F} \oplus \ldots \oplus \bar{F}, \qquad x \otimes u \longmapsto (x\sigma_1(u), \cdots, x\sigma_d(u)).$$

(ii) If $\alpha \in K$, let L_α: $K \longrightarrow K$ be the map $L_\alpha(x) = \alpha x$. Regarding K as an F-vector space and L_α as a linear transformation,

$$\text{tr}(L_\alpha) = \sum_{i=1}^{d} \sigma_i(\alpha), \qquad \det(L_\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha).$$

We define $\mathrm{tr}_{K/L}(\alpha) = \mathrm{tr}(L_\alpha)$ and $N_{K/L}(\alpha) = \det(L_\alpha)$, the familiar norm and trace.

Proof. For each i there is clearly an $\bar{F}$-algebra homomorphism $\bar{F} \otimes K \longrightarrow \bar{F}$ in which $x \otimes u \longmapsto x\sigma_i(u)$. Hence the $\bar{F}$-algebra homorphism above exists, and since both algebras have the same dimension, to show that it is an isomorphism it is sufficient to show that it is injective. Let $u_1, \cdots, u_d$ be an F-basis of K. Injectivity of the homomorphism boils down to the determinant $(\sigma_i(u_j))_{i,j}$ being nonzero, and this is a restatement of Artin's result on the linear independence of characters (Lang [2], Theorem VI.4.1 on p. 283). Now (i) is clear.

For (ii), we can clearly use the isomorphism of (i) to diagonalize of L_α over $\bar{F}$, and we see that its eigenvalues of L_α are the conjugates $\sigma_i(\alpha)$ of α, and now (ii) is clear. □

Proposition 29. *Let D be a central division algebra over F, and let K be a maximal subfield of D. Thus if d is the reduced degree of D, $d = [K\colon F]$. Assume that K/F is a separable extension. Let $N_{K/F}$ and $\mathrm{tr}_{K/F}$ be the norm and trace maps $K \longrightarrow F$, and let $N, \mathrm{tr}\colon D \longrightarrow F$ be the reduced norm and trace. Then the restrictions of N and tr to K are $N_{K/F}$ and $\mathrm{tr}_{K/F}$.*

Proof. For definiteness, we work with the norm; the trace is identical. By Theorem 22, $K \otimes D \cong \mathrm{End}_K(D^{\mathrm{opp}})$ as K-algebras, where D^{opp} is regarded as a K-algebra via left-multiplication. This is equivalent to asserting that $K \otimes D \cong \mathrm{End}_K(D)$, where D is a K-algebra by right multiplication. In this isomorphism of K-algebras, $\Phi\colon K \otimes D \longrightarrow \mathrm{End}_K(D)$ we have

$$\Phi(u \otimes x)\, y = x\, y\, u.$$

The reduced norm of $u \in K$ is then the image of u under the composition

$$K \longrightarrow 1 \otimes K \hookrightarrow K \otimes D \xrightarrow{\Phi} \mathrm{End}_K(D) \xrightarrow{\det} K.$$

Let $\xi_1, \cdots, \xi_d$ be a basis of D as a right vector space over K. We can write

$$u\,\xi_i = \sum_j \xi_j \alpha_{ij}(u), \qquad \alpha_{ij}(u) \in K.$$

Since the reduced norm is the determinant of $\Phi(1 \otimes u)$, it equals $\det(\alpha(u))$, where $\alpha(u)$ is the matrix $\alpha_{ij}(u)$. In particular, by Theorem 27, the coefficients of the characteristic polynomial $p(X) = \det(X \cdot I_d - \alpha(u))$ are in F.

We note that α is a representation of K, and that $\alpha_{ij}(u)$ is the scalar matrix $u I_d$ if $u \in F$. Since K is semisimple, it can be diagonalized over the algebraic closure. This means that there exists $M \in \mathrm{GL}_d(\bar{F})$ such that

$$\alpha(u) = M \begin{pmatrix} \chi_1(u) & & \\ & \ddots & \\ & & \chi_d(u) \end{pmatrix} M^{-1},$$

where $\chi_i\colon K \longrightarrow \bar{F}$ is a homomorphism over F. We claim that there are no repetitions among the χ_i, and the $\chi_i(u)$ are this the d distinct embeddings $K \longrightarrow \bar{F}$ over F. Indeed, since K/F we may choose u to be a primitive element, in which case, since $K = F[u]$ is a separable extension of degree d, the monic irreducible polynomial over F satisfied by of $\alpha(u)$ is of degree d and has no multiple roots. The characteristic polynomial of $\alpha(u)$ is a polynomial of degree d with coefficients in F satisfied by u, so these two polynomials must coincide.

Now it follows that the reduced norm $\nu(u) = \det(\alpha(u)) = \prod\ \chi_i(u)$ is the product of the Galois conjugates of u, hence equals $N_{K/F}(u)$. □

2 The Brauer Group

The results of this section will not be needed right away. Our goal is to prove that the Brauer group equals $H^2(\Gamma, \bar{F}^\times)$, where $\Gamma = \mathrm{Gal}(\bar{F}/F)$. For simplicity we will assume that $\mathrm{char}(F) = 0$. However this assumption may be removed by using Weil [4], Corollary to Proposition 5 on p. 165 to replace $\bar{F}$ by the separable closure F^{sep} throughout.

We begin by defining the cohomology groups. We will only need H^0, H^1 and H^2. First, let Γ be a group and A an abelian group on which Γ acts by automorphisms. (We refer to A as a Γ-*module*.) If $\sigma \in \Gamma$ and $a \in A$, we will denote by ${}^\sigma a$ the image of a under this action by σ.

We will define a group $H^i(\Gamma, A) = H^i(A)$ as follows. The group $H^0(A) = A^\Gamma$ is the group of Γ-invariants. Each higher cohomology group $H^i(A)$ is a quotient group $Z^i(A)/B^i(A)$, where the groups of "cocycles" $Z^i(A)$ and "coboundaries" $B^i(A)$ have yet to be defined. If $\varphi \in Z^i(A)$, we will sometimes denote by $\{\varphi\}$ the cohomology class of φ in $H^i(A)$. Even if the group A is written multiplicatively, we will write the group law in H^i additively, so $\{\varphi\} + \{\psi\} = \{\varphi\psi\}$.

The group $Z^1(A)$ consists of all *crossed homomorphisms* or 1-*cocycles*, which are maps $\varphi\colon \Gamma \longrightarrow A$ which satisfy the *cocycle condition*

$$\varphi(\sigma\tau) = \varphi(\sigma)\,{}^\sigma\varphi(\tau). \tag{4}$$

If $a \in A$ then we may construct a cocycle by defining

$$\varphi(\sigma) = a^{-1} \cdot {}^\sigma a.$$

The cocycles of this form are the *coboundaries* and comprise the group $B^1(A)$.

Similarly, the group $Z^2(A)$ consists of maps $\varphi\colon \Gamma \times \Gamma \longrightarrow A$ which satisfy the *cocycle condition*

$$\varphi(\sigma,\tau)\,\varphi(\sigma\tau,\rho) = \varphi(\sigma,\tau\rho)\,{}^\sigma\varphi(\tau,\rho). \tag{5}$$

If $f\colon \Gamma \longrightarrow A$ is any map, then

$$\varphi(\sigma,\tau) = f(\sigma)\ {}^\sigma f(\tau)\, f(\sigma\tau)^{-1}$$

is a cocycle, since both sides of (5) equal $f(\sigma)^\sigma f(\tau)^{\sigma\tau} f(\rho)\, f(\sigma\tau\rho)^{-1}$. The cocycles of this form are the *coboundaries* and comprise the group $B^2(A)$.

We will not define H^n, Z^n or B^n for $n > 2$, simply because we will not need them.

If Γ is a profinite group (such as a Galois group) we may modify these definitions by requiring that the cocycles all be constant on cosets of some normal open subgroup of Γ (for $Z^1(A)$) or of $\Gamma \times \Gamma$ (for $Z^2(A)$), as must the map f in the definition of $B^2(A)$. This means that the cocycle must factor through a finite quotient of Γ. Thus

$$H^i(\Gamma, A) = \varprojlim H^i(G, A), \tag{6}$$

where G runs through the finite quotients of Γ. For example if $\Gamma = \mathrm{Gal}(\bar{F}/F)$, these are the Galois groups of finite extensions of F.

Lemma 30. *Let Γ be a profinite group, and let G be a finite quotient. Then the natural map $H^i(G, A) \longrightarrow H^i(\Gamma, A)$ is injective.*

This means that we may identify $H^i(G, A)$ with its image in $H^i(\Gamma, A)$, and rewrite (6) this way:

$$H^i(\Gamma, A) = \bigcup_{G \text{ a finite quotient of } \Gamma} H^i(G, A). \tag{7}$$

Proof. It is easy to see that an inverse limit of injections is an injection, so it is sufficient to show that if G is a finite quotient of Γ, and G' is a quotient of G, then the canonical map $H^i(G', A) \longrightarrow H^i(G, A)$ is injective. Let us check this when $i = 2$; the case of other i is similar. Let $p\colon G \longrightarrow G'$ be the canonical map. If $\varphi \in Z^i(G', A)$ is such that $\varphi \circ (p \times p) \in B^i(G, A)$, then we must show that $\varphi \in B^2(G', A)$. Since $\varphi \circ (p \times p)$ is a coboundary we can find $\psi\colon G \longrightarrow A$ such that $\psi(\sigma)\,{}^{\sigma}\psi(\tau)\,\psi(\sigma\tau)^{-1} = \varphi(p(\sigma), p(\tau))$ for all $\sigma, \tau \in G$. Let $s\colon G' \longrightarrow G$ be any map such that $p \circ s = 1_{G'}$, and let $\psi'\colon G' \longrightarrow A$ be the map $\psi \circ s$. Then if $\sigma, \tau \in G$ we have

$$\varphi(p(\sigma), p(\tau)) = \varphi(psp(\sigma), psp(\tau)) = \\ \psi'(p(\sigma))\,{}^{\sigma}\psi'(p(\tau))\,\psi'(p(\sigma\tau))^{-1}.$$

Since $p\colon G \longrightarrow G'$ is surjective, this shows that φ is a coboundary in $B^2(G, A)$. □

The cohomology group $H^i(A)$ is a functor in an obvious way. If $f\colon A \longrightarrow B$ is a homomorphism of Γ-modules, there are induced maps $H^i(f)\colon H^i(A) \longrightarrow H^i(B)$. We will also denote this map as f_*.

Theorem 31. *Suppose that*

$$1 \longrightarrow M \xrightarrow{i} N \xrightarrow{p} Q \longrightarrow 1$$

is a short exact sequence of Γ-modules. Then there exist homomorphisms $\delta_i\colon H^i(Q) \longrightarrow H^{i+1}(M)$ for $i = 0, 1$ such that the following sequence is exact:

$$1 \longrightarrow H^0(M) \xrightarrow{i_*} H^0(N) \xrightarrow{p_*} H^0(Q) \xrightarrow{\delta^0} H^1(M) \xrightarrow{i_*} H^1(N) \xrightarrow{p_*} H^1(Q) \\ \xrightarrow{\delta^1} H^2(M) \xrightarrow{i_*} H^2(N) \xrightarrow{p_*} H^2(Q).$$

This cohomology exact sequence can of course be continued with the higher cohomology groups, though we have not defined them.

Proof. We give the definition of the *connecting homomorphisms* δ^i. It will be convenient to identify M with its image in N, so i becomes an inclusion map. First, suppose that $q \in H^0(Q) = Q^\Gamma$. There exists some $n \in N$ such that $p(n) = q$. We note that $n^{-1} \cdot {}^\sigma n$ is mapped to 1 by p since $q \in Q^\Gamma$. Thus if we define $\varphi(\sigma) = n^{-1} {}^\sigma n$, then $\varphi(\sigma) \in M$, and it is easy to see that $\varphi \in Z^1(M)$. Although φ depends on the choice of n, if we change n we must change it by an element of M which changes φ by a coboundary. Thus taking $\delta^0(q)$ to be the image of φ in $H^1(M)$ gives a well defined map $H^0(Q) \longrightarrow H^1(M)$.

Similarly, given an element of $H^1(Q)$, let $\psi\colon \Gamma \longrightarrow Q$ be a representative cocycle. For each $\sigma \in \Gamma$, let $f(\sigma)$ be an element of N such that $p(f(\sigma)) = \psi(\sigma)$. Define

$$\varphi(\sigma, \tau) = f(\sigma)\, {}^\sigma f(\tau)\, f(\sigma\tau)^{-1}.$$

Applying p gives 1 since $p \circ f$ is a cocycle. Thus $\varphi(\sigma, \tau) \in M$. If we change f to another lift of ψ, we must change it by a function taking values in M, which only changes φ by a coboundary. Finally, if $\psi \in B^1(Q)$ it is easy to check that φ is trivial, so mapping the class $\{\psi\}$ of ψ in $H^1(Q)$ to the class $\{\phi\}$ of φ in $H^2(M)$ gives a well defined map.

We leave it to the reader to check the exactness of the cohomology sequence. □

So far we have assumed the coefficient module A to be abelian. If it is nonabelian, it is still possible to define $H^1(A)$, though it is then just a set. As before, a 1-*cocycle* or *crossed homomorphism* is a map $\varphi\colon \Gamma \longrightarrow A$ satisfying (4), and we consider two cocycles φ and ψ to be *equivalent* or *cohomologous* if there exists some $\alpha \in A$ such that

$$\psi(\sigma) = \alpha^{-1}\, \phi(\sigma)\, {}^\sigma \alpha.$$

The set of equivalence classes of 1-cocycles is then $H^1(A)$. Although $H^1(A)$ is not a group when A is not abelian, it still has a distinguished element that we will denote 1. This is the class of the trivial cocycle which maps every $\sigma \in \Gamma$ to $1 \in A$. (This is admittedly inconsistent since when A is abelian we insisted on writing $H^1(A)$ additively even if A is multiplicative.)

Theorem 32. *Let F be a field, and let $\Gamma = \mathrm{Gal}(K/F)$, where K is a (finite or infinite) Galois extension. Then $H^1(\Gamma, \mathrm{GL}_n(K)) = \{1\}$.*

If K/F is cyclic and $n = 1$, this is Hilbert's Theorem 90, from the *Zahlbericht*. If $n = 1$ and K/F is general, this generalization is due to Emmy Noether. We will abuse the historical record by referring to Theorem 32 as *Hilbert's Theorem 90*.

Proof. Using (6), it is sufficient to show that $H^1(\mathrm{Gal}(E/F), \mathrm{GL}_n(K)) = 1$, where E/F is a finite Galois extension and $E \subseteq K$. Let $\Gamma = \mathrm{Gal}(E/F)$, and let $\varphi\colon \Gamma \longrightarrow \mathrm{GL}_n(K)$ be a 1-cocycle. We will prove that there exists a matrix $J \in \mathrm{GL}_n(K)$ such that

$$\Theta = \sum_{\sigma \in \Gamma} \varphi(\sigma) \cdot {}^\sigma C$$

is nonsingular. Before proving this let us see how it shows that φ is a coboundary. Fixing $\sigma \in \Gamma$, reindexing the summation and making use of the cocycle condition,

$$\Theta = \sum_{\tau \in \Gamma} \varphi(\sigma\tau) \cdot {}^{\sigma\tau}C = \varphi(\sigma) \cdot {}^{\sigma}\left(\sum_{\tau \in \Gamma} \varphi(\tau)\, {}^{\tau}C \right) = \varphi(\sigma)\, {}^{\sigma}\Theta.$$

Thus $\Theta^{-1}\varphi(\sigma)\,{}^{\sigma}\Theta$ is trivial for all σ, showing that φ is cohomologous to the trivial cocycle.

We will construct C to be diagonal, with diagonal entries $c_1, \cdots, c_n$. Writing $\varphi(\sigma) = (\varphi_{ij}(\sigma))$ as a matrix, we construct C inductively so that the minor

$$m_i = \begin{vmatrix} \Sigma\, \varphi_{11}(\sigma)\, {}^{\sigma}c_1 & \Sigma\, \varphi_{12}(\sigma)\, {}^{\sigma}c_2 & \cdots & \Sigma\, \varphi_{1i}(\sigma)\, {}^{\sigma}c_i \\ \Sigma\, \varphi_{21}(\sigma)\, {}^{\sigma}c_1 & \Sigma\, \varphi_{22}(\sigma)\, {}^{\sigma}c_2 & \cdots & \Sigma\, \varphi_{2i}(\sigma)\, {}^{\sigma}c_i \\ \vdots & \vdots & \ddots & \vdots \\ \Sigma\, \varphi_{i1}(\sigma)\, {}^{\sigma}c_1 & \Sigma\, \varphi_{i2}(\sigma)\, {}^{\sigma}c_2 & \cdots & \Sigma\, \varphi_{ii}(\sigma)\, {}^{\sigma}c_i \end{vmatrix}$$

is nonzero. Here each summation is over σ. Assuming that $c_1, \cdots, c_{i-1}$ are constructed so that $m_{i-1} \neq 0$, we show that we can construct c_i so that $m_i \neq 0$. Expanding the determinant in the last column, we have

$$m_i = \sum_{j=1}^{i} M_j \sum_{\sigma} \varphi_{ji}(\sigma)\, {}^{\sigma}c_i = \sum_{\sigma} \left(\sum_{j=1}^{i} M_j \varphi_{ji}(\sigma) \right) {}^{\sigma}c_i,$$

where M_j are the appropriate minors formed with the first $n-1$ columns. Since φ is a crossed homomorphism, $\varphi(1)$ is the identity matrix, so in the last sum, the coefficient of ${}^{1}c_i$ is just $M_i = m_{i-1}$, which is nonzero by inductive hypothesis. By Artin's theorem on linear independence of characters (Lang [2], Theorem VI.4.1 on p. 283), we may choose c_i so that m_i is nonzero. Note that $m_n = \det(\Theta)$, and so we are done. □

As an application, let us consider the following situation. Let F be a field, and K a Galois extension. Let U be a vector space over K. By an *F-structure* on U we mean an F-subspace U_0 such that an F-basis of U_0 is a K-basis of U. For example, F^n is an F-structure in K^n. As another example, if V is any F-vector space, then $U = K \otimes_F V$ is a vector space over K, and we have an injective F-linear map $V \longrightarrow U$ in which $v \longmapsto 1 \otimes v$. It is easy to see that the image U_0 of V in U under this map is an F-structure; indeed, if $\{v_i\}$ is any F-basis of V, then $\{1 \otimes v_i\}$ is an F-basis of U_0 and also an K-basis of U. So $U \cong K \otimes U_0$.

Conversely, suppose that U_0 is an F-structure on U. Then the multiplication map $K \times U_0 \longrightarrow U$ is $\bar{F}$-bilinear and hence induces an F-linear map $K \otimes U_0 \longrightarrow U$, and it is easy to see that this map is an isomorphism.

Proposition 33. *Let K/F be a (finite or infinite) Galois extension, and let $U = K^n$. Let $c\colon \mathrm{Gal}(K/F) \longrightarrow \mathrm{GL}(U)$ be a 1-cocycle, and let*

$$U_0 = \{x \in U \mid c(\sigma)\sigma(x) = x \text{ for all } \sigma \in \mathrm{Gal}(K/F)\}.$$

Then U_0 is an F-structure on U. In particular, $U \cong K \otimes U_0$.

Proof. We will make use of the componentwise action of $\mathrm{Gal}(K/F)$ on K^n whose invariants are just F^n. Every linear transformation of U is given by a matrix, so we may identify $\mathrm{GL}(U) = \mathrm{GL}_n(K)$. By Theorem 32, $c\colon \mathrm{Gal}(K/F) \longrightarrow \mathrm{GL}_n(K)$ is a coboundary, which means that there exists $\Theta \in \mathrm{GL}(V)$ such that $c(\sigma) = L^{-1\sigma}L$ for all σ. As a map $U \longrightarrow U$, we have ${}^{\sigma}L = \sigma L \sigma^{-1}$, so $x \in U_0$ if and only if $L^{-1}\sigma L(x) = x$ or $\sigma L(x) = L(x)$ for all σ. This means that $L(x) \in F^n$, and so $U_0 = L^{-1}F^n$. Thus taking a standard basis of F^n and applying L^{-1} gives an F-basis of U which is contained in U_0, and so U_0 is an F-structure. □

Suppose that

$$1 \longrightarrow M \xrightarrow{i} N \xrightarrow{p} Q \longrightarrow 1 \tag{8}$$

is a short exact sequence. We assume that M is abelian and central in the sense that $i(M) \subset Z(N)$, but we do *not* assume that N and Q are abelian. In this case we call N a *central extension* of Q by M, or informally, we may refer to the short exact sequence as a *central extension.*

Even though Q and N are nonabelian we still have defined a map

$$\delta^1\colon H^1(Q) \longrightarrow H^2(M).$$

To construct it, we proceed as before. Thus, if $\psi\colon \Gamma \longrightarrow Q$ is a 1-cocycle we choose a map $f\colon \Gamma \longrightarrow N$ such that $\psi = p \circ f$ and define

$$\varphi(\sigma, \tau) = i^{-1}(f(\sigma)\,{}^{\sigma}f(\tau)\,f(\sigma\tau)^{-1}).$$

Note that $f(\sigma)f(\sigma\tau)^{-1\sigma}f(\tau)$ is in the image of i because applying p to it gives 1, using the fact that ψ is a 1-cocycle, so this definition makes sense.

Lemma 34. *We have $\varphi \in Z^2(M)$. If we choose a different f' such that $\psi = p \circ f'$ and define $\varphi'(\sigma, \tau) = i^{-1}(f'(\sigma)\,{}^{\sigma}f'(\tau)\,f'(\sigma\tau)^{-1})$. Then $\varphi - \varphi' \in B^2(M)$.*

Proof. We will identify M with its image under i in N. Let us check that φ is a cocycle. We have, after a cancellation

$$\varphi(\sigma, \tau)\,\varphi(\sigma\tau, \rho) = f(\sigma)\,{}^{\sigma}f(\tau)\,{}^{\sigma\tau}f(\rho)\,f(\sigma\tau\rho)^{-1}.$$

This should equal

$$\varphi(\sigma, \tau\rho)\,{}^{\sigma}\varphi(\tau, \rho) = f(\sigma)\,{}^{\sigma}f(\tau\rho)\,f(\sigma\tau\rho)^{-1\sigma}\varphi(\tau, \rho) = f(\sigma)\,{}^{\sigma}\varphi(\tau, \rho)\,{}^{\sigma}f(\tau\rho)\,f(\sigma\tau\rho)^{-1},$$

where we have used the fact that ${}^{\sigma}\varphi(\tau, \rho) \in M$ is central. Expanding this and taking into account another cancellation we see that φ is a cocycle.

The confirmation that $\varphi - \varphi' \in B^2(M)$ is straightforward. □

Thus we obtain a well-defined *connecting homomorphism* $\delta^1\colon H^1(Q) \longrightarrow H^2(M)$ such that $\delta^1(\{\psi\}) = \{\phi\}$.

Proposition 35. *Suppose that (8) is a central extension. If $\psi\colon \Gamma \longrightarrow Q$ is a 1-cocycle then $\delta^1(\{\psi\}) = 0$ in $H^2(M)$ if and only if $\{\psi\}$ is in the image of the natural map $H^1(N) \longrightarrow H^1(Q)$.*

This is a nonabelian substitute for the exactness of the long cohomology exact sequence in Theorem 31.

Proof. We identify M with its image under i. If $\delta^1(\{\psi\}) = 0$, this means that with f and φ as before, φ is a coboundary; in other words

$$f(\sigma)^\sigma f(\tau)\, f(\sigma\tau)^{-1} = \mu(\sigma)^\sigma \mu(\tau)\, \mu(\sigma\tau)^{-1},$$

with $\mu\colon \Gamma \longrightarrow M$. We may replace f by $f' = \mu^{-1} f$, and the resulting $f'\colon \Gamma \longrightarrow N$ is a 1-cocycle. This means that $\{\psi\}$ is the image of $\{f'\} \in H^1(N)$. The converse statement is identical. □

We proceed now to the cohomological interpretation of the Brauer group. Let $\Gamma = \mathrm{Gal}(\bar{F}/F)$. We begin by noting that the $\mathrm{GL}_n(\bar{F})$ is a (nonabelian) Γ-module, since Γ acts componentwise on the matrices.

Also $\mathrm{Aut}(\mathrm{Mat}_n(\bar{F}))$ is a Γ-module. To see this, if $\sigma \in \Gamma$ then as in he previous Section, let $\sigma_n\colon \mathrm{Mat}_n(\bar{F}) \longrightarrow \mathrm{Mat}_n(\bar{F})$ denote the action of $\sigma \in \Gamma$ on matrices. If $\lambda\colon \mathrm{Mat}_n(\bar{F}) \longrightarrow \mathrm{Mat}_n(\bar{F})$ is any $\bar{F}$-linear automorphism and $\sigma \in \Gamma$, then $\sigma_n \circ \lambda \circ \sigma_n^{-1}$ is also $\bar{F}$-linear, even though σ_n is itself not $\bar{F}$-linear. Thus we obtain an action of Γ on $\mathrm{Aut}(\mathrm{Mat}_n(\bar{F}))$.

Now if $m \in \mathrm{GL}_n(\bar{F})$, let $L(m)\colon \mathrm{Mat}_n(\bar{F}) \longrightarrow \mathrm{Mat}_n(\bar{F})$ be conjugation by m, that is, $L(m)x = mxm^{-1}$.

Proposition 36. *The homomorphism $L\colon \mathrm{GL}_n(\bar{F}) \longrightarrow \mathrm{Aut}(\mathrm{Mat}_n(\bar{F}))$ is Γ-equivariant. It is surjective and has as its kernel the subgroup of scalar matrices in $\mathrm{GL}_n(\bar{F})$, isomorphic to $\bar{F}^\times$. Thus we have a central extension*

$$1 \longrightarrow \bar{F}^\times \longrightarrow \mathrm{GL}_n(\bar{F}) \longrightarrow \mathrm{Aut}(\mathrm{Mat}_n(\bar{F})) \longrightarrow 1\,.$$

Proof. It is easy to check that as mappings $\mathrm{Mat}_n(\bar{F}) \longrightarrow \mathrm{Mat}_n(\bar{F})$ we have

$$L({}^\sigma m) = \sigma_n \circ L(m) \circ \sigma_n^{-1}. \tag{9}$$

Hence L is Γ-equivariant. By Proposition 25 it is surjective, and the kernel is clearly the center of $\mathrm{GL}_n(\bar{F})$ consisting of scalar matrices. □

Let A be a central simple algebra over F. If n is the reduced degree of A, we will first show how to associate with A an element of $H^1(\Gamma, \mathrm{Aut}(\mathrm{Mat}_n(\bar{F}))$. As in the previous section, fix an isomorphism $\theta\colon \bar{F} \otimes A \longrightarrow \mathrm{Mat}_n(\bar{F})$ as $\bar{F}$-algebras. Let $\sigma \in \mathrm{Gal}(\bar{F}/F)$. As in the previous section, let $c_\theta(\sigma) \in \mathrm{Aut}(\mathrm{Mat}_n(\bar{F}))$ be the composition

$$c_\theta(\sigma) = \theta \circ (\sigma \otimes 1) \circ \theta^{-1} \circ {\sigma_n}^{-1}.$$

In the last section, we denoted this c_σ, and showed that it was an $\bar{F}$-linear automorphism.

Theorem 37. *The map $c_\theta\colon \Gamma \longrightarrow \mathrm{Aut}(\mathrm{Mat}_n(\bar{F}))$ is a 1-cocycle, and the cohomology class $\{c_\theta\} \in H^1(\mathrm{Aut}(\mathrm{Mat}_n(\bar{F})))$ is independent of the choice of θ and depends only on the isomorphism class of A. The map $A \longmapsto \{c_\theta\}$ gives a bijection from the set of isomorphism classes of central simple algebras of reduced degree n over F to the cohomology set $H^1(\mathrm{Aut}(\mathrm{Mat}_n(\bar{F})))$.*

Proof. The map $\sigma \longmapsto c_\theta(\sigma)$ from $\mathrm{Gal}(\bar{F}/F)$ to $\mathrm{Aut}(\mathrm{Mat}_n(\bar{F}))$ satisfies the cocycle condition

$$c_\theta(\sigma\tau) = c_\theta(\sigma) \cdot {}^\sigma c_\theta(\tau). \tag{10}$$

Indeed, the right-hand side in (10) is the same as $c_\theta(\sigma)\sigma_n c_\theta(\tau)\sigma_n^{-1}$, or

$$\theta(\sigma \otimes 1)\theta^{-1}{\sigma_n}^{-1}\sigma_n\theta(\tau \otimes 1)\theta^{-1}{\tau_n}^{-1}\sigma_n^{-1},$$

and after cancellations we obtain (10). If θ' is another isomorphism then using Proposition 25 we can write $\theta = L(M) \circ \theta'$, where $M \subset \mathrm{GL}_n(\bar{F})$. Using (9), we have

$$L(M)^{-1} c_\theta(\sigma) L({}^\sigma M) = c_{\theta'}(\sigma). \tag{11}$$

In other words $c(\sigma)$ is changed to an equivalent cocycle. The conclusion is that A is associated with a unique cohomology class in $H^1(\mathrm{Aut}(\mathrm{Mat}_n(\bar{F})))$.

Now let us show that if two central simple algebras A and B of the same reduced degree n produce the same cohomology class they are isomorphic. Using (11) we may replace the cocycle associated with A by any equivalent cocycle, so we may assume that A and B are associated with cocycles that are equal. This means that we have isomorphisms $\theta_A \colon \bar{F} \otimes A \longrightarrow \mathrm{Mat}_n(\bar{F})$ and $\theta_B \colon \bar{F} \otimes B \longrightarrow \mathrm{Mat}_n(\bar{F})$ such that

$$\theta_A(\sigma \otimes 1)\theta_A^{-1}{\sigma_n}^{-1} = \theta_B(\sigma \otimes 1)\theta_B^{-1}{\sigma_n}^{-1}$$

for all $\sigma \in \Gamma$. Rewriting this

$$\Theta \circ (\sigma \otimes 1) = (\sigma \otimes 1) \circ \Theta,$$

where $\Theta = \theta_B^{-1}\theta_A \colon \bar{F} \otimes A \longrightarrow \bar{F} \otimes B$, we see that Θ must map the F-subalgebra $F \otimes A \cong A$ of Γ-invariants isomorphically onto $F \otimes B \cong B$, so $A \cong B$.

Finally we must show that every cohomology class $\{c\} \in H^1(\mathrm{Aut}(\mathrm{Mat}_n(\bar{F})))$ is associated to a central simple algebra. Choosing a representative cocyle c, let us construct an algebra as follows. Let

$$A = \{x \in \mathrm{Mat}_n(\bar{F}) \,|\, c_\sigma\sigma(x) = x \text{ for all } \sigma \in \mathrm{Gal}(\bar{F}/F)\}.$$

By Proposition 33, A is an F-structure on $\mathrm{Mat}_n(\bar{F})$ and so $\bar{F} \otimes A \cong \mathrm{Mat}_n(\bar{F})$ as vector spaces. It is obvious that A is an F-algebra, so this is actually an isomorphism of $\bar{F}$-algebras. We show that A is a central simple algebra. Indeed, as a finite-dimensional algebra it is Artinian. If I is any nonzero ideal, it is an F-vector subspace of A, and so $\bar{F}I$ is an ideal in $\mathrm{Mat}_n(\bar{F}) = \bar{F}A \cong \bar{F} \otimes A$; since $\mathrm{Mat}_n(\bar{F})$ is simple, this means that $\bar{F}I = \mathrm{Mat}_n(\bar{F})$. Since A is an F-structure and I a vector subspace, $I = A \cap \bar{F}I = A$, proving that A is simple.

It is easy to check that the cocycle obtained from A agrees with c if we take $\theta \colon \bar{F} \otimes A \longrightarrow \mathrm{Mat}_n(\bar{F})$ to be this isomorphism. □

Now let A be a central simple algebra of reduced degree n. We have associated with A a cohomology class in $H^1(\mathrm{Aut}(\mathrm{Mat}_n(\bar{F})))$ which was denoted $\{c_\theta\}$ in Theorem 37. Since the independence of the class on A was established, let us denote it as $\boldsymbol{c}_A$. Now consider $\delta^1(\boldsymbol{c}_A) \in H^2\big(\bar{F}^\times\big)$, where $\delta^1 \colon H^1(\mathrm{Aut}(\mathrm{Mat}_n(\bar{F}))) \longrightarrow H^2\big(\bar{F}^\times\big)$ is the coboundary map.

Theorem 38. *If A and B are central simple algebras then $\delta^1(\boldsymbol{c}_A) = \delta^1(\boldsymbol{c}_B)$ if and only if $[A] = [B]$ in $B(F)$. Moreover $\delta^1(\boldsymbol{c}_{A\otimes B}) = \delta^1(\boldsymbol{c}_A) + \delta^1(\boldsymbol{c}_B)$. The map $[A] \longmapsto \delta^1(\boldsymbol{c}_A)$ is a well-defined isomorphism of $B(F)$ with $H^2(\bar{F}^\times)$.*

Proof. Let $\theta_A\colon \bar{F}\otimes A \longrightarrow \mathrm{Mat}_n(\bar{F})$ and $\theta_B\colon \bar{F}\otimes B \longrightarrow \mathrm{Mat}_m(\bar{F})$ be given isomorphisms. We recall how $\delta^1(\boldsymbol{c}_A)$ and $\delta^1(\boldsymbol{c}_B)$ are constructed. We choose maps $\gamma_A\colon \Gamma \longrightarrow \mathrm{GL}_n(\bar{F})$ and $\gamma_B\colon \Gamma \longrightarrow \mathrm{GL}_m(\bar{F})$ such that

$$c_{\theta_A}(\sigma)x = \gamma_A(\sigma)\,x\,\gamma_A(\sigma)^{-1}, \qquad c_{\theta_B}(\sigma)\,y = \gamma_B(\sigma)\,y\,\gamma_B(\sigma)^{-1},$$

for $x \in \mathrm{Mat}_n(\bar{F})$ and $y \in \mathrm{Mat}_m(\bar{F})$. Then $\delta^1(\boldsymbol{c}_A)$ and $\delta^1(\boldsymbol{c}_B)$ are represented by cocycles φ_A and φ_B in $Z^2(\Gamma, \bar{F}^\times)$ defined by

$$\varphi_A(\sigma,\tau) = \gamma_A(\sigma)\,{}^\sigma\gamma_A(\sigma)\,\gamma_A(\sigma\tau)^{-1}, \qquad \varphi_B(\sigma,\tau) = \gamma_B(\sigma)\,{}^\sigma\gamma_B(\sigma)\,\gamma_B(\sigma\tau)^{-1}.$$

Identifying $\mathrm{Mat}_n(\bar{F}) \otimes \mathrm{Mat}_m(\bar{F}) = \mathrm{Mat}_{nm}(\bar{F})$, we may take $\theta_{A\otimes B}\colon \bar{F}\otimes A\otimes B \longrightarrow \mathrm{Mat}_{nm}(\bar{F})$ to be the composition

$$\bar{F}\otimes A\otimes B \longrightarrow \bar{F}\otimes A\otimes \bar{F}\otimes B \overset{\theta_A\otimes\theta_B}{\longrightarrow} \mathrm{Mat}_n(\bar{F})\otimes \mathrm{Mat}_m(\bar{F}) \longrightarrow \mathrm{Mat}_{nm}(\bar{F}),$$

where all the maps are isomorphisms. Now we can take $\gamma_{A\otimes B}\colon G \longrightarrow \mathrm{GL}_{nm}(\bar{F})$ to be $\gamma_{A\otimes B}(\sigma) = \gamma_A(\sigma)\otimes\gamma_B(\sigma)$ and we see immediately that

$$\delta^1(\boldsymbol{c}_{A\otimes B}) = \delta^1(\boldsymbol{c}_A) + \delta^1(\boldsymbol{c}_B) \tag{12}$$

and similarly

$$\delta^1(\boldsymbol{c}_{A^{\mathrm{opp}}}) = -\,\delta^1(\boldsymbol{c}_A).$$

(Recall that we write the group law in $H^2(\bar{F}^\times)$ additively even though the group $\bar{F}^\times$ is written multiplicatively.) As a special case, $A \otimes \mathrm{Mat}_k(F) \cong \mathrm{Mat}_k(A)$, while $\delta^1(\boldsymbol{c}_{\mathrm{Mat}_k(F)}) = 0$, so

$$\delta^1(\boldsymbol{c}_{\mathrm{Mat}_k(A)}) = \delta^1(\boldsymbol{c}_A). \tag{13}$$

Now let us show that if A and B are central simple algebras of the same reduced degree d and that $\delta^1(\boldsymbol{c}_A) = \delta^1(\boldsymbol{c}_B)$ then A and B are isomorphic. Indeed, we have

$$\delta^1(\boldsymbol{c}_{A\otimes B^{\mathrm{opp}}}) = \delta^1(\boldsymbol{c}_A) - \delta^1(\boldsymbol{c}_B) = 0,$$

and by Proposition 35 and Theorem 32 it follows that the cohomology class of $\boldsymbol{c}_{A\otimes B^{\mathrm{opp}}}$ in $H^1(\mathrm{Aut}(\mathrm{Mat}_{d^2}(\bar{F}))$ is trivial. By Theorem 37 it follows that $A\otimes B^{\mathrm{opp}} \cong \mathrm{Mat}_{d^2}(\bar{F})$ and since B^{opp} is the inverse of B in the Brauer group, it follows that $A \cong B$.

Next let us show that if A and B are arbitrary central simple algebras such that $\delta^1(\boldsymbol{c}_A) = \delta^1(\boldsymbol{c}_B)$ then $[A]$ and $[B]$ are equal in the Brauer group. We can find integers k and l such that $\mathrm{Mat}_k(A)$ and $\mathrm{Mat}_l(B)$ have the same degree. Then by (13),

$$\delta^1(\boldsymbol{c}_{\mathrm{Mat}_k(A)}) = \delta^1(\boldsymbol{c}_A) = \delta^1(\boldsymbol{c}_B) = \delta^1(\boldsymbol{c}_{\mathrm{Mat}_l(B)})$$

and by the case just discussed, this implies that $\mathrm{Mat}_k(A) \cong \mathrm{Mat}_l(B)$, and therefore $[A] = [B]$ in the Brauer group.

We now see that $[A] \mapsto \delta^1(\boldsymbol{c}_A)$ is a well defined injective map of $B(F)$ into $H^2(\mathrm{Gal}(\bar{F}/F), \bar{F}^\times)$, and by (12), it is a group homomorphism. We must show that it is surjective. Given $\varphi \in Z^2(\mathrm{Gal}(\bar{F}/F), \bar{F}^\times)$, we show how to realize $\{\varphi\} = \delta^1(\{c\})$ for some $c \in H^1(\mathrm{Gal}(\bar{F}/F), \mathrm{Aut}(\mathrm{Mat}_n(\bar{F})))$. This is sufficient, since then by Theorem 37 we have $\{c\} = \boldsymbol{c}_A$ for some central simple algebra A.

Let K/F to be a finite extension such that φ factors through $G \times G$, where $G = \mathrm{Gal}(K/F)$. Enlarging K if necessary, we may assume that the values of φ are in K. Then we may identify φ with a cocycle in $H^2(\mathrm{Gal}(K/F), K^\times)$. Let $n = [K\colon F]$, and let $\gamma\colon G \longrightarrow \mathrm{GL}_n(K)$ be defined as follows. We will construct $\gamma(\sigma)$ as an $n \times n$ matrix indexed by pairs μ, ν of elements of G. Specifically, we define

$$\gamma(\sigma)_{\mu\nu} = \begin{cases} \varphi(\sigma, \nu) & \text{if } \mu = \sigma\nu; \\ 0 & \text{otherwise.} \end{cases} \tag{14}$$

Let us check that

$$\gamma(\sigma)\,{}^\sigma\gamma(\tau) = \varphi(\sigma, \tau)\,\gamma(\sigma\tau). \tag{15}$$

Indeed, the μ, ν entry of the matrix on the left is

$$\sum_\lambda \gamma(\sigma)_{\mu\lambda}\,{}^\sigma\gamma(\tau)_{\lambda\nu}.$$

A typical term is nonzero if and only if $\sigma\lambda = \mu$ and $\tau\nu = \lambda$; this can only happen if $\sigma\tau\nu = \mu$, in which case there is exactly one nonzero term. It equals

$$\varphi(\sigma, \tau\nu)\,{}^\sigma\varphi(\tau, \nu) = \varphi(\sigma, \tau)\,\varphi(\sigma\tau, \nu) = \varphi(\sigma, \tau)\,\gamma(\sigma\tau)_{\mu\nu},$$

as required.

Now if $\sigma \in G$ let $c(\sigma) \in \mathrm{Aut}(\mathrm{Mat}_n(\bar{F}))$ be conjugaction by $\gamma(\sigma)$. Then c is a cocycle since $\gamma(\sigma)\,{}^\sigma\gamma(\tau)$ and $\gamma(\sigma\tau)$ differ by a scalar matrix, hence induce the same automorphism on conjugation. It follows from the definition of δ^1 that $\delta^1(\{c\}) = \{\varphi\}$.

□

Let K/F be a finite extension, and let $G = \mathrm{Gal}(K/F)$. Given a particular cocycle $\varphi\colon G \times G \longrightarrow K^\times$, we may construct a particular F-algebra A_φ as follows. A_φ will be a free left K-vector space with basis $\{x_\sigma\}$ where σ runs through G, subject to the rules

$$x_\sigma k = {}^\sigma k x_\sigma, \qquad k \in K$$

and

$$x_\sigma x_\tau = \varphi(\sigma, \tau) x_{\sigma\tau}.$$

The associative law is easily checked; in particular $(x_\sigma x_\tau)x_\rho = x_\sigma(x_\tau x_\rho)$ boils down to the cocycle condition on φ. It is straightforward to show that K is a maximal subfield and that F is the center.

We may construct an n-dimensional represention of $A = A_\varphi$ as follows. Note that $\{x_\varphi\}$ are a basis of A_φ as either a left- or right-vector space. If $a \in A$, then $x \longmapsto ax$ is K-linear with respect to the right K-vector space structure on A. Let $R(a)$ be the matrix of this linear tranformation with respect to the basis $\{x_\varphi\}$. Concretely, this means that $L(a)$ is the matrix with coefficients $L(a)_{\mu\nu}$ where

$$a x_\nu = \sum_\mu x_\mu L(a)_{\mu\nu}.$$

Proposition 39. *The F-subalgebra $L(A)$ of $\mathrm{Mat}_n(K)$ is an F-structure. We have $K \otimes A \cong \mathrm{Mat}_n(K)$ as F-algebras. The algebra A is central simple.*

Proof. Clearly $R(A)$ is an n^2-dimensional vector subspace of $\mathrm{Mat}_n(K)$, which is an n^2-dimensional K-vector space. To show that it is an F-structure, it is sufficient to show that elements of $R(A)$ which are linearly independent over F remain linearly independent over K. We leave this verification to the reader. It follows from the fact that $R(A)$ is an F-structure that $K \otimes A \cong \mathrm{Mat}_n(K)$, and since A is central, this implies that it is central simple, since if I were any nonzero ideal, the image of $K \otimes I$ in $\mathrm{Mat}_n(K)$ would be an ideal in $\mathrm{Mat}_n(K)$, which would be all of $\mathrm{Mat}_n(K)$, and so $I = A$. □

Proposition 40. *Suppose that K/F is abelian and that $\varphi(\sigma, \tau) \in F^\times$ for all $\sigma, \tau \in G = \mathrm{Gal}(K/F)$, and let $A = A_\varphi$. Then $\delta^1(\boldsymbol{c}_{A^{\mathrm{opp}}}) = \{\varphi\}$.*

Proof. Since we are working with A^{opp}, we consider the representation of A^{opp} defined by *right* translation:

$$x_\nu a = \sum_\mu R_{\mu\nu}(a)\, x_\mu.$$

Let $\gamma(\sigma) = R(x_\sigma) \in \mathrm{GL}_n(F)$. We compute easily that

$$\gamma(\sigma)_{\mu\nu} = \begin{cases} \varphi(\sigma, \nu) & \text{if } \mu = \sigma\nu; \\ 0 & \text{otherwise.} \end{cases}$$

In other words, this γ agrees with the γ we used in (14). Now we will show that the F-structure in $\mathrm{Mat}_n(K)$ determined by this set of γ is just $R(A)$. This means that we must show that $c(\sigma) \circ \sigma$ is trivial on $R(A)$, where $c(\sigma)$ is conjugation by $\gamma(\sigma)$, in other words

$$R(a) = \gamma(\sigma)^\sigma R(a)\, \gamma(\sigma)^{-1}.$$

We check this separately for $a \in K$ and for a

□

3 Quaternion algebras

In this section, let F be a field whose characteristic is not equal to 2.

Proposition 41. *Let F be a field of characteristic not equal to 2, and let $a, b \in F^\times$. The following are equivalent.*
(i) The equation

$$x^2 - a y^2 - b z^2 = 0 \tag{16}$$

is solvable with $(x, y, z) \in F$, not all zero;
(ii) The equation

$$x^2 - a y^2 - b z^2 + a b w^2 = 0; \tag{17}$$

is solvable with $(x, y, z, w) \in F^4$*, not all zero;*
(iii) The element b *is a norm from* $F(\sqrt{a})$*.*
(iv) The element a *is a norm from* $F(\sqrt{b})$*.*

Proof. We will prove the equivalence of (i), (ii) and (iii). Of course the equivalence of (iv) is identical.

If a is a square, say $a = u^2$, then (i) and (ii) are true with $(x, y, z) = (u, 1, 0)$, and $w = 0$ for (ii). Also (iii) is true since $F(\sqrt{a}) = F$ and so the norm map $N: F(\sqrt{a}) \longrightarrow F$ is trivially surjective. Thus we may assume in this proof that a is not a square. In this case the norm map is given by

$$N(x + y\sqrt{a}) = x^2 - ay^2.$$

It is clear that (i) $\Rightarrow$ (ii), since we may take $w = 0$.

We prove (ii) $\Rightarrow$ (iii). Assume (17) with x, y, z, w not all zero. We claim that $z + w\sqrt{a} \neq 0$. For if $z + w\sqrt{a} = 0$, then the norm $z^2 - aw^2 = 0$, and since a is not a square, z and w are both zero. Also $x^2 - ay^2 = b(z^2 - aw^2) = 0$ so similarly x and y are both zero. We have a contradiction since it is assumed that x, y, z, w are not all zero, proving $z + w\sqrt{a} \neq 0$. Now we see that b is the norm of $(x + y\sqrt{a})/(z + w\sqrt{a})$, and (iii) is satisfied.

We prove (iii) $\Rightarrow$ (i). If $b = N(u + v\sqrt{a})$ then $b = u^2 - av^2$ and we may take $(x, y, z) = (u, v, 1)$. □

Definition 42. (Hilbert symbol) *Let* $a, b \in F^\times$*. The* Hilbert symbol $(a, b)_F$ *is defined to be* 1 *if the equivalent conditions of Proposition 41 are satisfied; otherwise, we define* $(a, b)_F = -1$*.*

If F is local, the Hilbert symbol has further important properties that may be found in Theorem 60.

Let $a, b \in F^\times$. Define $Q_F(a, b)$ to be the four-dimensional associative algebra with an F-basis $1, i, j, k$ subject to the relations

$$i^2 = a, \qquad j^2 = b, \qquad ij = -ji = k.$$

These imply

$$k^2 = -ab, \qquad jk = -kj = -bi, \qquad ki = -ik = -aj.$$

For example, $Q_{\mathbb{R}}(-1, -1)$ is the familiar ring of Hamilton quaternions. If F is fixed, we denote $Q(a, b) = Q_F(a, b)$. The algebra $Q(a, b)$ has an involution denoted $\xi \longmapsto \xi^*$ defined by

$$(x + yi + zj + wk)^* = x - yi - zj - wk.$$

We have

$$(\xi\eta)^* = \eta^*\xi^*. \tag{18}$$

Proposition 43. *(i) Let* F *be a field and* $a, b \in F^\times$*. Then* $Q(a, b) = Q_F(a, b)$ *is a central simple algebra. It is a matrix ring if and only if the Hilbert symbol* $(a, b)_F = 1$*. Otherwise it is a division algebra.*
(ii) We have $Q(a, b) \cong Q(b, a)$*.*

(iii) If $a \in F^\times$ *then* $Q(1,a) \cong \mathrm{Mat}_2(F)$.
(iv) If $a \in F^\times$, *then* $Q(a,-a) \cong \mathrm{Mat}_2(F)$.
(v) If $a, 1-a \in F^\times$, *then* $Q(a,1-a) \cong \mathrm{Mat}_2(F)$.
(vi) If $\lambda, \mu, a, b \in F^\times$ *then* $Q(\lambda^2 a, \mu^2 b) \cong Q(a,b)$.
(vii) If $a_1, a_2, b_1, b_2 \in F^\times$, *then*

$$Q(a_1,b_1) \otimes Q(a_2,b_2) \cong Q(a_1, b_1b_2) \otimes Q(b_2, a_1a_2). \tag{19}$$

(vii) If $a, b, b' \in F^\times$, *then* $Q(a,b) \otimes Q(a,b') \cong \mathrm{Mat}_2(A)$ *where* $A = Q(a,bb')$.

Proof. We postpone (i) until after (vi).

For (ii), it is clear that interchanging the roles of i and j turns $Q_F(a, b)$ into $Q_F(b, a)$.

For (iii), $Q_F(1,a) \cong \mathrm{Mat}_2(F)$ under the isomorphism

$$i \longmapsto \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}, \qquad j \longmapsto \begin{pmatrix} & 1 \\ a & \end{pmatrix}, \qquad k \longmapsto \begin{pmatrix} & 1 \\ -a & \end{pmatrix}.$$

We postpone (v) until after (vi) and (i).

For (vi), multiplying i, j and k by λ, μ and $\lambda\mu$, respectively produces a new basis for $Q_F(a,b)$ showing that it is isomorphic to $Q_F(\lambda^2 a, \mu^2 b)$.

Returning to (i), let $A = Q_F(a,b)$. Using (vi) and (iii), $\bar{F} \otimes A = Q_{\bar{F}}(a,b) \cong Q_{\bar{F}}(1,1) \cong \mathrm{Mat}_2(F)$. Thus $Q_F(a,b)$ is a central simple algebra by Proposition 18. Since its reduced degree is 2, either it is a division ring or else it is isomorphic to $\mathrm{Mat}_2(F)$. If $(a,b)_F = 1$, then referring to (ii) of Proposition 41, there exist x, y, z and w in F, not all zero, such that $x^2 - ay^2 - bz^2 + abw^2 = 0$. Then

$$(x + yi + zj + wk)(x + yi + zj + wk)^* = 0,$$

showing that $x + yi + zj + wk$ is a zero divisor and so $Q_F(a, b)$ is not a division ring. Since it is a central simple algebra whose reduced degree 2 is prime, it is either a division ring or a matrix ring by Proposition 12. Thus it is a matrix ring. Conversely if $(a, b) = -1$, then for any nonzero element $x + yi + zj + wk$ of $Q_F(a,b)$ we have $x^2 - ay^2 - bz^2 + abw^2 \neq 0$, in F, so

$$(x^2 - ay^2 - bz^2 + abw^2)^{-1}(x + yi + zj + wk)^*$$

is an inverse of $x + yi + zj + wk$, proving that it is a division ring. This proves (i).

Now (v) follows from (i) since $1 - a = N(1 - \sqrt{a})$ is a norm from $F(\sqrt{a})$, so the Hilbert symbol $(a, 1-a)_F = 1$.

We prove now (vii). By definition, $A = Q(a_1, b_1)$ and $B = Q(a_2, b_2)$ have bases $1, i_1, j_1, k_1$ and $1, i_2, j_2, k_2$ respectively such that

$$\begin{aligned} i_1^2 &= a_1, & j_1^2 &= b_1, & i_1 j_1 &= -j_1 i_1 = k_1, \\ i_2^2 &= a_2, & j_2^2 &= b_2, & i_2 j_2 &= -j_2 i_2 = k_2. \end{aligned}$$

Now it is easy to see that

$$1 \otimes 1, \qquad i_1 \otimes 1, \qquad j_1 \otimes j_2, \qquad k_1 \otimes j_2$$

span a subalgebra C of $A \otimes B$ isomorphic to $Q(a_1, b_1 b_2)$, and that

$$1 \otimes 1, \qquad 1 \otimes j_2, \qquad i_1 \otimes i_2, \qquad -i_1 \otimes k_2$$

span a subalgebra D of $A \otimes B$ isomorphic to $Q(b_2, a_1 a_2)$. By the universal property of the tensor product of F-algebras, there is induced an F-algebra homomorphism $D \otimes C \longrightarrow A \otimes B$ which is easily seen to be bijective, since the 16 vectors spanned by the tensor products of the four basis vectors of C with the four basis vectors of D are easily seen to span $A \otimes B$. This proves (19).

Finally for (viii), we have $Q_F(b', a^2) \cong \mathrm{Mat}_2(F)$ since the Hilbert symbol $(b', a^2)_F = 1$. Since for any algebra A over F it is straightforward to see that

$$A \otimes \mathrm{Mat}_2(F) \cong \mathrm{Mat}_2(A),$$

the statement follows using (vii). □

Proposition 44. *Let A be a central simple algebra of reduced degree 2 over F, and let $u \in A$. Then $\mathrm{tr}(u) = 0$ if and only if $u^2 \in F$ and either $u^2 = 0$ or $u \notin F$.*

Proof. Embed $A \longrightarrow \bar{F} \otimes A \cong \mathrm{Mat}_2(\bar{F})$. The image of u in $\mathrm{Mat}_2(\bar{F})$ will have trace zero if and only if its Jordan canonical form is one of the following three possibilities:

$$\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Since $\mathrm{char}(F) \neq 2$

$$\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}^2 \in F \text{ and } \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} \notin F,$$

while the other two possibilities satisfy $u^2 = 0$. □

Proposition 45. *In $Q(a,b)$, the reduced trace of $x + yi + zj + wk$ is $2x$.*

Proof. By the criterion of Proposition 44, the trace of $yi + zj + wk$ is zero since it is not in F (unless $y = z = w = 0$) but its square is $y^2 a + z^2 b - w^2 ab \in F$. On the other hand $x \in F$ and its reduced trace is clearly $2x$. □

Proposition 46. *Let A be a central simple algebra of reduced degree 2. Then $A \cong Q(a, b)$ for some $a, b \in F$.*

Proof. Choose an element i of $A_0 = \{u \in A \mid \mathrm{tr}(u) = 0\}$ such that $i \notin F$. Now the three linear forms on A defined by $u \longmapsto \mathrm{tr}\,(u)$, $\mathrm{tr}(iu)$ and $\mathrm{tr}(ui)$ vanish on a vector subspace of the four-dimensional vector space A of dimension at least 1, so there exists a nonzero $j \in A$ such that $j, ij, ji \in A_0$. By Proposition 44

$$ij + ji = (i + j)^2 - i^2 - j^2 \in F$$

since $i + j, i, j \in A_0$. On the other hand $\mathrm{tr}(ij + ji) = 0$. Since $F \cap A_0 = \{0\}$ we have $ij = -ji$. Denote $k = ij = -ji$. Let $a = i^2$ and $b = j^2$. We have $k^2 = ijij = -i^2 j^2 = -ab$. We see that A is a homomorphic image of $Q(a,b)$, but $Q(a,b)$ is simple, so $A \cong Q(a,b)$. □

Proposition 47. *Let A be a central simple algebra of reduced degree 2. Then the square of A in the Brauer group is trivial.*

Proof. By Proposition 46, we may assume that $A = Q(a,b)$. By (18), $x \longmapsto x^*$ is an isomorphism $A \cong A^{\mathrm{opp}}$, and the result follows from Proposition 19. □

4 Quadratic Defect and the Norm Index

This section is strongly influenced by O'Meara [3].

Let F be a nonarchimedean local field. We assume that the characteristic $\mathrm{char}(F) \neq 2$. Let $\mathfrak{o}$ be the ring of integers in F, and $\mathfrak{p}$ its prime ideal. We will denote by $\mathrm{ord}\colon F \longrightarrow \mathbb{Z} \cup \{\infty\}$ the (additive) valuation, so $\mathrm{ord}(x) = \infty$ if and only if $x = 0$, and $\mathfrak{o} = \{x \in F | \mathrm{ord}(x) \geqslant 0\}$. If K/F is an extension field, we denote by $\mathfrak{o}_K$ the ring of integers in K, and by $\mathfrak{p}_K$ its prime ideal. We will also denote by $N_{K/F}$ and $\mathrm{tr}_{K/F}$ the norm and trace maps from $K \longrightarrow F$. If the field K is fixed, we may also denote these as simply N and tr.

One of the major results of local class field theory is that if K/F is an abelian extension of local fields, then $F^\times/NK^\times \cong \mathrm{Gal}(K/F)$. An important step is to prove the *norm index equality* $[F^\times\colon NK^\times] = [K\colon F]$. In this section, we will prove that $[F^\times\colon NK^\times] \geqslant 2$ when K/F is quadratic.

If R is any ring, we will denote by $R^\square = R^\times/(R^\times)^2$ the group of *square classes* in R. If $x \in R^\times$, we will denote by $x^\square$ the coset $x(R^\times)^2$, which is the image of x in $R^\square$.

Proposition 48. *The groups $F^\square$ and $\mathfrak{o}^\square$ are finite, and $|F^\square| = 2|\mathfrak{o}^\square|$ There are only a finite number of quadratic extensions of F, equal in number to $|F^\square| - 1$.*

Proof. From the short exact sequence

$$1 \longrightarrow \mathfrak{o}^\times \longrightarrow F^\times \xrightarrow{\mathrm{ord}} \mathbb{Z} \longrightarrow 0$$

we get a short exact sequence

$$1 \longrightarrow \mathfrak{o}^\square \longrightarrow F^\square \longrightarrow (\mathbb{Z}/2\mathbb{Z}) \longrightarrow 0, \tag{20}$$

and so $|F^\square| = 2|\mathfrak{o}^\square|$. The latter is finite since the squares in $\mathfrak{o}^\times$ form an open subgroup of this compact group, by Proposition 50.

Since the characteristic of F is not equal to 2, any quadratic extension of F is of the form $F(\sqrt{d})$, where d is a nonsquare in F, and $F(\sqrt{d}) = F(\sqrt{d'})$ if and only if d and d' are in the same square class. Thus the number of quadratic extensions equals the number of nontrivial square classes. □

If the residue characteristic $\mathrm{char}(\mathfrak{o}/\mathfrak{p})$ is 2 we say that F is *dyadic*. In general everything that we do will be valid for arbitrary local fields but the proofs will be more difficult for dyadic fields.

Proposition 49. (Hensel's Lemma) *Let F be a nonarchimedean local field with local ring $\mathfrak{o}$, and let $f(x) \in \mathfrak{o}[x]$ be a polynomial. If $a_0 \in \mathfrak{o}$ satisfies*

$$|f(a_0)| < |f'(a_0)|^2,$$

then there exists $a \in \mathfrak{o}$ *such that* $|a - a_0| \leqslant |f(a_0)/f'(a_0)^2| < 1$ *and* $f(a) = 0$.

Proof. See Lang, *Algebraic Number Theory*, p.42. □

Hensel's Lemma implies that any element of F sufficiently close to the identity is a square. More precisely:

Proposition 50. *Let* $\varepsilon \in \mathfrak{o}^\times$. *(i) If* $\varepsilon \equiv 1 \bmod 4\mathfrak{p}$, *then* ε *is a square.*
(ii) If F *is not dyadic, and* $\varepsilon \in \mathfrak{o}^\times$, *then* ε *is a square if and only if the image of* ε *in* $\mathfrak{o}/\mathfrak{p}$ *is a square.*

Proof. For (i), apply Hensel's Lemma to $f(x) = x^2 - \varepsilon$ with $a_0 = 1$.

If F is not dyadic, then 4 is the square of a unit, so (i) implies that if ε is a square mod $\mathfrak{p}$, it is a square, which is (ii). □

Proposition 51. *Suppose that* F *is not dyadic.*
(i) We have $[\mathfrak{o}^\times : (\mathfrak{o}^\times)^2] = 2$ *and* $[F^\times : (F^\times)^2] = 4$.
(ii) If $a, b \in \mathfrak{o}^\times$, *then the Hilbert symbol* $(a, b)_F = 1$.
(iii) If $a \in \mathfrak{o}^\times$ *is not a square and* $K = F(\sqrt{a})$, *then*

$$N(K^\times) = \{x \in F^\times \mid \mathrm{ord}(x) \text{ is even}\}.$$

(iv) If a *is a unit and* ϖ *is a generator of* $\mathfrak{p}$, *then*

$$(a, \varpi)_F = \begin{cases} 1 & \text{if } a \text{ is a square;} \\ -1 & \text{otherwise.} \end{cases}$$

Proof. By Proposition 48, part (i) amounts to showing that there are two square classes in $\mathfrak{o}^\times$, and by Proposition 50, it is sufficient to show that there are exactly two square classes in $(\mathfrak{o}/\mathfrak{p})^\times$. This is clear since $(\mathfrak{o}/\mathfrak{p})^\times$ is cyclic.

For part (ii), we may assume that b is not a square since if b is a square then it is certainly a norm from $F(\sqrt{a})$ and so $(a, b)_F = 1$. Then, b is not a square mod $\mathfrak{p}$ by Proposition 50. Denoting $K = F(\sqrt{b})$, the finite field $\mathfrak{o}_K/\mathfrak{p}_K$ is thus the unique quadratic extension of $\mathfrak{o}/\mathfrak{p}$, and is generated by the image of $\sqrt{b}$ mod $\mathfrak{p}$. Since the norm map is surjective for finite fields, we may solve the equation $a = x^2 - by^2 \bmod \mathfrak{p}$. This means that $a + by^2$ is a square mod $\mathfrak{p}$ and so by Proposition 50 it is a square in $\mathfrak{o}$. Therefore we may solve $a = x^2 - by^2$ and $(a, b)_F = 1$.

For (iii), assuming that $a \in \mathfrak{o}^\times$ is not a square, we have seen that $N(K^\times)$ contains all units of $\mathfrak{o}^\times$. It also contains all squares, and so it contains all elements of even valuation. On the other hand, we claim that $N(K^\times)$ cannot contain any element of order 1. Thus if $x, y \in F$, we must show that $\mathrm{ord}(x^2 - ay^2) \neq 1$. There are two cases. If x and y have distinct valuations, then since the valuation is nonarchimedean, $\mathrm{ord}(x^2 - ay^2) = \min(\mathrm{ord}(x^2), \mathrm{ord}(ay^2))$ is the minimum of two even numbers, hence even. On the other hand if x and y have the same valuation, and if $u = x/y$, then a and u are both units and $u^2 - a$ has odd valuation; since $u^2 - a \in \mathfrak{o}$ this means $u^2 - a \in \mathfrak{p}$, which is a contradiction by Proposition 50.

For (iv), we ask under what circumstances there exists a nonzero solution (x, y, z) to

$$x^2 - ay^2 - \varpi z^2 = 0.$$

If a is a square, clearly there is a solution. If a is not a square, we claim there is no solution. Since the order of ϖz^2 is odd, it is enough to show that the order of $x^2 - ay^2$ is even. Both x^2 and ay^2 have even order. If x and y have different orders, then $\mathrm{ord}(x^2 - ay^2) = \min(\mathrm{ord}(x^2), \mathrm{ord}(ay^2))$, which is even. On the other hand, if they have the same order r, write $x = \xi\varpi^r$, $y = \eta\varpi^r$ with $\xi, \eta \in \mathfrak{o}^\times$. Then

$$x^2 - ay^2 = \varpi^{2r}(\xi^2 - a\eta^2).$$

Since a is not a square, it is not a square mod $\mathfrak{p}$, so $\xi^2 - a\eta^2$ is a unit. Thus the order of $x^2 - ay^2$ is $2r$ and is even. □

In contrast with the nondyadic case, dyadic fields have $F^\times/(F^\times)^2$ larger than 4. For example, let $F = \mathbb{Q}_2$. We first note that if $u \in \mathfrak{o}^\times$ is a square mod 8 then it is a square. Indeed, if $x^2 - u = 0$ has a root a_0 mod 8, then $f'(a_0) = 2a_0$, so $|f(a_0)| \leqslant \frac{1}{8} < \frac{1}{4} = |f'(a_0)|$. On the other hand, $1, 3, -3, -1$ represent distinctive square classes mod 8, so they represent the distinct square classes in $\mathfrak{o}^\times/(\mathfrak{o}^\times)^2$. With this information and (20) we may enumerate the square classes and the extension field. We have $|F^\times/(F^\times)^2| = 8$ and the square classes are given by Table 1. We also tabulate the index of the norms from the corresponding quadratic fields, and the *quadratic defect* of the units, a concept we will describe next. If F is a larger dyadic field than $\mathbb{Q}_2$ the number of square classes will be even larger than 8.

square class representative a	representatives of $NF(\sqrt{a})/(F^\times)^2$ (u with $x^2 - ay^2 = u$ solvable)	$\mathfrak{d}(a)$ (when $a \in \mathbb{Z}_2^\times$)
1	all classes	0
3	$1, -3, -2, 6$	$2\mathfrak{o}$
-3	$1, 3, -1, -3$	$4\mathfrak{o}$
-1	$1, 2, -3, -6$	$2\mathfrak{o}$
2	$1, -1, 2, -2$	
6	$1, 3, -2, -6$	
-6	$1, 6, -1, -6$	
-2	$1, 2, 3, 6$	

Table 1. Norms from quadratic extensions of $\mathbb{Q}_2$.

Let F be a dyadic field. Suppose that $\varepsilon \in F$ is a nonsquare. We try to approximate ε by squares. Specifically, we write $\varepsilon = \alpha^2 - u$ with $|u|$ as small as possible. If $u\mathfrak{o}$ is the fractional ideal generated by u, then we call $u\mathfrak{o} = \mathfrak{d}(u)$ the *quadratic defect* of u. If u is a square, we define $\mathfrak{d}(u)$ to be 0.

Proposition 52. *Suppose that F is dyadic and that $\varepsilon \in \mathfrak{o}^\times$ is a nonsquare. Then the quadratic defect $\mathfrak{d}(\varepsilon)$ is an integral ideal dividing $4\mathfrak{o}$. We have $\mathfrak{d}(\varepsilon) = 4\mathfrak{o}$ if and only if $F(\sqrt{\varepsilon})/F$ is an unramified extension. If $\mathfrak{d}(\varepsilon)$ is a proper divisor of 4, it equals $\mathfrak{p}^N$ where N is odd.*

Proof. First we note that the quadratic defect cannot be greater (that is, more highly divisible) than $4\mathfrak{o}$, since if $|\varepsilon - \alpha^2| < 4$ then ε is a square by Proposition 50.

Next we show that $F(\sqrt{\varepsilon})/F$ is unramified if and only if ε has quadratic defect $4\mathfrak{o}$. Suppose that $F(\sqrt{\varepsilon})/F$ is unramified. Let $\alpha \in \mathfrak{o}_K$, where $K = F(\sqrt{\varepsilon})$, be such that the image of α in $\mathfrak{o}_K/\mathfrak{p}_K$ generates the residue class extension. If the irreducible polynomial satisfied by α is $f(x) = x^2 + ax + b = 0$, with $a, b \in \mathfrak{o}$, then K/F is unramified if and only if the discriminant $a^2 - 4b$ of f is not divisible by $\mathfrak{p}$. In that case, it is a unit. Since $\sqrt{a^2 - 4b}$ and $\sqrt{\varepsilon}$ generate the same quadratic extension, we have $a^2 - 4b = \lambda^2\varepsilon$ for some $\lambda \in \mathfrak{o}$. If K/F is unramified, then both ε and $a^2 - 4b$ are units, so λ is also a unit, and ε differs from the square $(\lambda^{-1}a)^2$ by a multiple of 4, so the quadratic defect is at least 4, and since we have already shown that it cannot exceed 4, we have $\mathfrak{d}(\varepsilon) = 4\mathfrak{o}$.

On the other hand, if the quadratic defect of ε is $4\mathfrak{o}$, then ε differs from a square a^2 by a multiple of 4, that is, we can solve $\varepsilon - a^2 = -4b$ for some $a, b \in \mathfrak{o}$. Then if α is a root of the equation $f(x) = x^2 + ax + b = 0$, it is an integer. The extension $F(\alpha) = F(\varepsilon)$ since the discriminant of f is ε. And since ε is a unit, this means that K/F is unramified.

It remains to be shown that if the quadratic defect of ε is less than (that is, a proper divisor of) 4, then it is odd. Suppose $\mathfrak{d}(\varepsilon) = \mathfrak{p}^{2k}$ is even. By the definition of $\mathfrak{d}(\varepsilon)$, we may write $\varepsilon - a^2 = \varpi^{2k}\gamma$, with ϖ a generator of $\mathfrak{p}$ and γ a unit, but we cannot write $\varepsilon - b^2 \in \mathfrak{p}^N$ for any $N > 2k$. Since the residue field has characteristic p, the squaring map is a bijection on $\mathfrak{o}/\mathfrak{p}$, and this means that we can find $\beta \in \mathfrak{o}$ such that $\beta^2 \equiv \gamma \bmod \mathfrak{p}$. Now

$$\varepsilon - (a - \varpi^k\beta)^2 = \varpi^{2k}(\gamma - \beta^2) + 2a\varpi^k\beta.$$

Since ϖ^{2k} is a proper divisor of 4, $\mathfrak{p}^{k+1}$ divides 2, so the last expression is in $\mathfrak{p}^{2k+1}$, which is a contradiction. □

Proposition 53. *Let F be dyadic. Then there exists a unique square class of units with quadratic defect $4\mathfrak{o}$.*

Proof. This follows from Proposition 52, since F has a unique quadratic unramified extension. (See Lang, *Algebraic Number Theory*, Proposition 9 on p. 49.) □

Proposition 54. *Let F be dyadic. If ε, $a \in \mathfrak{o}^\times$ such that ε is not a square, $\varepsilon \equiv a^2$ mod $\mathfrak{p}^N$ but $\varepsilon \not\equiv a^2$ mod $\mathfrak{p}^{N+1}$, and if N is odd, then $\mathfrak{p}^N = \mathfrak{d}(\varepsilon)$.*

Proof. Multiplying ε by a square unit, we may assume that $a = 1$. Clearly $\mathfrak{d}(\varepsilon) | \mathfrak{p}^N$. If $\mathfrak{d}(\varepsilon)$ is a higher power of $\mathfrak{p}$, then we may write $\varepsilon \equiv (1 + \rho)^2$ mod $\mathfrak{p}^{N+1}$ for some ρ. This means that $\rho(\rho + 2) = \varepsilon - 1 \equiv \gamma\varpi^N$ mod $\mathfrak{p}^{N+1}$, where γ is a unit. If $2|\rho$, then $2|\rho + 2$ also, so $4|\varepsilon - 1$ which is impossible since $\mathrm{ord}(\varepsilon - 1)$ is odd, and $4\mathfrak{o}$ is the maximum possible quadratic defect. Thus $2 \nmid \rho$. This means that ρ and $\rho + 2$ have the same order, so their product has even order, which is a contradiction since $\varepsilon - 1$ has odd order. □

The last Proposition is important because with it, the quadratic defect becomes computable. For example, let $i = \sqrt{-1}$ and $F = \mathbb{Q}_2(i)$. There are 16 square classes in F, of which 8 may be represented by units. The quadratic defects are tabulated in Table 2. The maximal ideal $\mathfrak{p}$ is generated by $1+i$, and $\mathfrak{p}^4 = 4\mathfrak{o}$. Without Proposition 54, the correctness of such a table would be difficult to check.

unit ε	$\mathfrak{d}(\varepsilon)$
1	0
$3+2i$	$\mathfrak{p}^3$
$1+4i$	$4\mathfrak{o}$
$3-2i$	$\mathfrak{p}^3$
$2+i$	$\mathfrak{p}$
$2-i$	$\mathfrak{p}$
$4+i$	$\mathfrak{p}$
i	$\mathfrak{p}$

Table 2. Square classes of units in $\mathbb{Q}_2(i)$, and their quadratic defects.

Proposition 55. *Let K/F be unramified. Then $NK^\times$ consists of all elements of F of even order.*

Proof. First, we show that $NK^\times$ contains $\mathfrak{o}^\times$. This is the Corollary on p. 50 of Lang's *Algebraic Number Theory*. We give a direct proof in the present context. We have already proved this in Proposition 51 (iii) if F is not dyadic. We therefore assume F is dyadic. We may write $K = F(\sqrt{\Delta})$, where $\Delta \in \mathfrak{o}^\times$ has quadratic defect $4\mathfrak{o}$, and we may assume that $\Delta \equiv 1 \bmod 4$, so write $\Delta = 1+4\gamma$ with $\gamma \in \mathfrak{o}^\times$. Let $\varepsilon \in \mathfrak{o}^\times$. To show that $\varepsilon \in NK^\times$ it is sufficient to show that $\Delta \in NF(\sqrt{\varepsilon})^\times$ by Proposition 41. Since the squaring map is a bijection of $\mathfrak{o}/\mathfrak{p}$, we may find λ such that $\gamma \equiv -\lambda^2\varepsilon \bmod \mathfrak{p}$. Now $1 - 4\lambda^2\varepsilon \equiv \Delta \bmod 4\mathfrak{p}$ so $\Delta + 4\lambda^2\varepsilon$ is a square by Proposition 50 (i). This means we can write $\Delta = \mu^2 - 4\lambda^2\varepsilon$, so it is a norm from $NF(\sqrt{\varepsilon})$, as required.

Since $NK^\times$ contains $\mathfrak{o}^\times$ and all squares, it contains all elements of even valuation. On the other hand, since K/F is unramified, the group of norms does not contain any elements of odd valuation. □

Lemma 56. *Let $a, b \notin F^\times$ and $d \in F$. Suppose that there exist (x, y) and (u, v) such that*

$$ax^2 + by^2 = 1,$$
$$au^2 + bv^2 = d.$$

Then there exist (z, w) such that

$$z^2 + abw^2 = d.$$

Proof. If $d = 0$ this is trivial. Assume $d \neq 0$. Define a symmetric bilinear form $H: F^2 \times F^2 \longrightarrow F$ by

$$H\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) = {}^t\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\begin{pmatrix} a & \\ & b \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = ax_1y_1 + bx_2y_2.$$

Thus with $\xi = {}^t(x, y)$ we have $H(\xi, \xi) = 1$. Let η be a vector orthogonal to ξ with respect to H. Adjusting η by a suitable constant we may assume that matrix $M = (\xi, \eta)$ with columns ξ and η has determinant 1. Then

$$ {}^tM \cdot \begin{pmatrix} a & \\ & b \end{pmatrix} \cdot M = \begin{pmatrix} {}^t\xi \\ {}^t\eta \end{pmatrix} \begin{pmatrix} a & \\ & b \end{pmatrix} (\xi, \eta) = \begin{pmatrix} H(\xi,\xi) & 0 \\ 0 & H(\eta,\eta) \end{pmatrix}. $$

Since $H(\xi, \xi) = 1$, taking determinants on both sides shows that

$$ {}^tM \cdot \begin{pmatrix} a & \\ & b \end{pmatrix} \cdot M = \begin{pmatrix} 1 & \\ & ab \end{pmatrix}. $$

Now let

$$ (u, v)\,{}^tM^{-1} \begin{pmatrix} 1 & \\ & ab \end{pmatrix} M^{-1} \begin{pmatrix} u \\ v \end{pmatrix} = (u, v) \begin{pmatrix} a & \\ & b \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = d, $$

so $z^2 + abw^2 = d$ with

$$ \begin{pmatrix} z \\ w \end{pmatrix} = M^{-1} \begin{pmatrix} u \\ v \end{pmatrix}. $$ □

Theorem 57. *Let K/F be a quadratic extension. Then $[F^\times\colon NK^\times] \geqslant 2$. We have equality if K/F is unramified, or if $K = F(\sqrt{\varpi})$, where ϖ is a generator of $\mathfrak{p}$.*

Proof. First assume that K/F is not dyadic. Write $K = F(\sqrt{\alpha})$. Since we may change α by a square, we may assume that either α is a unit or a generator of $\mathfrak{p}$. If it is a unit, then by Proposition 51, part (iii), the norms from K are precisely the elements of even valuation in F, and these have index two. On the other hand, suppose that $\alpha = \varpi$ is a generator of $\mathfrak{p}$. Since $-\varpi$ is a norm, $NK^\times$ contains elements of every valuation, and it is sufficient to show that the units which are norms are of index two in $\mathfrak{o}^\times$, and this follows from Proposition 51 (iv).

For the rest of the proof we may assume that F is dyadic. Writing $K = F(\sqrt{\alpha})$, since we may multiply α by any square, we may assume that either $\alpha = \varpi$ is a generator of $\mathfrak{p}$ or that $\alpha = \varepsilon$ is a unit. In any case, let Δ be a unit of quadratic defect $4\mathfrak{o}$. Multiplying Δ by a unit, we may assume that $\Delta \equiv 1 \bmod 4$.

First assume that $K = F(\sqrt{\varpi})$, where ϖ is a generator of $\mathfrak{p}$. Since $N\sqrt{\varpi} = -\varpi$, the group $NK^\times$ contains elements of every valuation, so it is sufficient to show that $N\mathfrak{o}_K^\times$ has index two in $\mathfrak{o}^\times$. We will show that 1 and Δ are coset representatives for $\mathfrak{o}^\times/N\mathfrak{o}^\times$. They are in different cosets, since $\Delta \notin NK^\times$; this follows from Proposition 41 because we have already proved that $\varpi \notin NF(\sqrt{\Delta})$ in Proposition 55. Thus we must show that if $\varepsilon \in \mathfrak{o}^\times$, then either ε or $\varepsilon\Delta$ is a norm from $K^\times$. Assume not; choose a counterexample ε of maximal quadratic defect. Since ε is not a norm, it is not a square, so the quadratic defect is nonzero; denote it $\mathfrak{p}^N$. Since $\varepsilon\Delta$ is not a norm, it is not a square, so ε lies in a different square class than Δ. By Proposition 53, the quadratic defect of ε is not 4. $\mathfrak{p}^N$ is a proper divisor of 4. By Proposition 52, $N = 2k + 1$ is odd. Multiplying ε by a square we may assume that $\varepsilon = 1 + \gamma\varpi^{2k+1}$, where γ is a unit. Since the squaring map of $\mathfrak{o}/\mathfrak{p}$ is a bijection, we may find $\delta \in \mathfrak{o}^\times$ such that $\gamma \equiv \delta^2 \bmod \mathfrak{p}$. Now $\varepsilon(1 - \varpi(\delta\varpi^k)^2) \equiv (1 + \gamma\varpi^{2k+1})(1 - \gamma\varpi^{2k+1}) \equiv 1 \bmod \mathfrak{p}^{2k+2}$, and so

$$ \varepsilon N(1 + \delta\varpi^k\sqrt{\varpi}) \equiv 1 \bmod \mathfrak{p}^{2k+2}. $$

This means that the quadratic defect of $\varepsilon N(1 + \delta\varpi^k\sqrt{\varpi})$ either zero or greater than that of ε, contradicting the assumed maximality of ε.

Next we assume that $K = F(\sqrt{\varepsilon})$ where ε is a unit. In this case, we will only prove the inequality $[K\colon F] \geqslant 2$. If ε has quadratic defect $4\mathfrak{o}$, then by Proposition 55, the index of $NK^\times$ is certainly 2, so we may assume that the quadratic defect of ε is $\mathfrak{p}^{2k+1}$. Multiplying ε by a square, we may assume that $\varepsilon \equiv 1 \bmod \mathfrak{p}^{2k+1}$ and write $\varepsilon = 1 + \gamma\varpi^{2k+1}$, where ϖ is a prime element and $\gamma \in \mathfrak{o}^\times$. First, we show that $NK^\times$ is a proper subgroup of $F^\times$ by showing that $\alpha = \Delta - \varepsilon$ is not a norm. Note that $\operatorname{ord}(\alpha) = 2k + 1$. If α is a norm from K, then $1 = \alpha x^2 + \varepsilon y^2$ for some x and y by Proposition, and $\Delta = \alpha u^2 + \beta v^2$ with $u = v = (1, 1)$. By Lemma 56, it follows that $\Delta = z^2 + \alpha\varepsilon w^2$ is solvable. Thus Δ is a norm from $F(\sqrt{-\alpha\varepsilon})$, so $-\alpha\varepsilon$ is a norm from $F(\sqrt{\Delta})$. This contradicts Proposition 55, since $-\alpha\varepsilon$ has odd order. □

In Theorem 57, we *almost* proved the norm index equality $[F^\times\colon NK^\times] = 2$, but left one case open. Later we will finish the proof, making use of the fact that there is a unique quaternion division algebra over F. Both these facts are generalized in the local class field theory, where it is shown that if K/F is any abelian extension, then $F^\times/NK^\times \cong \operatorname{Gal}(K/F)$. The isomorphism is closely connected with the computation of the Brauer group of F, which turns out to be isomorphic to $\mathbb{Q}/\mathbb{Z}$.

Lemma 58. *Suppose that* $(a, b)_F = (a, b')_F$. *Then* $Q(a, b) \cong Q(a, b')$.

Proof. Proposition 43 (vii), $Q(a, b) \otimes Q(a, b') \cong \operatorname{Mat}_2(Q(a, bb'))$. But $Q(a, bb') \cong \operatorname{Mat}_2(F)$ by Proposition 43 (i) and Proposition 55, so $Q(a, b)$ and $Q(a, b')$ are inverses in the Brauer group. By Proposition 47, $Q(a, b)$ has order two in $B(F)$, so by Proposition 47, $Q(a, b) \cong Q(a, b')$. □

Theorem 59. *There is a unique quaternion division algebra* D *over* F. *We have, for* a, $b \in F^\times$

$$Q(a, b) \cong \begin{cases} \operatorname{Mat}_n(F) & \text{if } (a, b)_F = 1; \\ D & \text{if } (a, b)_F = -1. \end{cases}$$

Proof. Let Δ be a unit such that $F(\sqrt{\Delta})/F$ is unramified, and let ϖ be a prime element. By Proposition 43 (i) and Proposition 55, $D = Q(\Delta, \varpi)$ is a division algebra. By Proposition 43 (i), what we must show is that if $(a, b)_F = -1$ then $Q(a, b) \cong D$. We may change a and b by squares without changing either $(a, b)_F$ or $Q(a, b)$, so we may assume that a and b both have order $\leqslant 1$.

First note that if ϖ' is any other generator of $\mathfrak{p}$, then $Q(\Delta, \varpi') \cong D$. Indeed, $(\Delta, \varpi')_F = -1 = (\Delta, \varpi)_F$ so this follows from Lemma 58.

Next let us show that if ϖ is any prime element and ε is any unit such that $(\varpi, \varepsilon)_F = -1$, then $Q(\varpi, \varepsilon) \cong D$. Since Δ is a norm from $F(\sqrt{\varpi})$ but ε is not, the Hilbert symbol $(\varpi, \varepsilon)_F = -1 = (\varpi, \Delta)_F$ and so $Q(\varpi, \varepsilon) \cong Q(\varpi, \Delta) = D$ by Lemma 58.

Finally, suppose that ε and δ are units such that $(\varepsilon, \delta)_F = -1$. Let ϖ be a prime element. Multiplying ϖ by δ if necessary, we may assume that ϖ is not a norm from $F(\sqrt{\varepsilon})$. Then $(\varepsilon, \varpi)_F = -1$, and so we have proved that $Q(\varepsilon, \varpi) \cong D$. Now $(\varepsilon, \varpi)_F = (\varepsilon, \delta)_F = -1$, so by Lemma 58, $Q(\varepsilon, \delta) \cong D$.

These cases exhaust the possibilities and the Theorem is proved. □

Now we may give another interpretation of the Hilbert symbol. The subgroup of $B(F)$ generated by the unique quaternion algebra D over F is a subgroup μ of order 2. Let $i\colon \mu \longrightarrow \{\pm 1\}$ be the unique isomorphism. The content of Theorem 59 is that

$$(a,b)_F = i[Q(a,b)]. \tag{21}$$

Theorem 60. *The Hilbert symbol has the following properties.*
(i) We have $(a,b)_F \cong (b,a)_F$.
(ii) If $a \in F^\times$, *then* $(a,-a)_F = 1$.
(iii) If $a, 1-a \in F^\times$, *then* $(a,1-a)_F = 1$.
(iv) If $\lambda, \mu, a, b \in F^\times$ *then* $(\lambda^2 a, \mu^2 b)_F = (a,b)_F$.
(v) If $a, b, b' \in F^\times$, *then* $(a,b)_F(a,b')_F = (a,bb')_F$.
(vi) If $a \in F^\times$, *then* $(a,b)_F = 1$ *for all* b *if and only if* a *is a square.*

Parts (v), (vi) and (i) may be expressed by saying that the Hilbert symbol is a non-degenerate symmetric bilinear pairing on the square classes. However since it takes values in ± 1 it is also true that it is *skew-symmetric*, and it is this statement which generalizes to the n-th order Hilbert symbol defined when F contains the n-th roots of unity.

Proof. Properties (i)–(iv) were clear earlier in Section 4. For example, $-a = N(\sqrt{a})$ and $1-a = N(1+\sqrt{a})$, so $(a,-a)_F = (a,1-a)_F = 1$. However (v) is really new here. It can seen from Proposition 43 (vii) using (21). For (vi), if a is not a square, then by Theorem 57, the norm $F(\sqrt{a})^\times \longrightarrow F^\times$ is not surjective, so we may find $b \in F^\times$ which is not in the image. Then $(a,b)_F = -1$. □

We may now finish what we started with Theorem 57.

Theorem 61. *Let* K/F *be a quadratic extension of local fields. Then* $[F^\times : NK^\times] = 2$.

Although we are assuming that F is nonarchimedean, this is also true F is archimedean. In that case, $F = \mathbb{R}$, $K = \mathbb{C}$, and the norms are the positive reals, which have index two in $\mathbb{R}^\times$.

Proof. Assume that F is nonarchimedean. Let $K = F(\sqrt{a})$. Then $x \longmapsto (a,\, x)_F$ is a homomorphism $F^\times \longrightarrow \{\pm 1\}$ whose kernel is precisely $NK^\times$. It is surjective by Theorem 57, and so the index of the kernel is 2. □

5 Fundamental Discriminants

So far we have been concerned mainly with local fields. We begin now to study the global law of quadratic reciprocity.

Proposition 62. *Let* F *be a finite extension of* $\mathbb{Q}$, *and let* $\mathfrak{o} = \mathfrak{o}_F$ *be the ring of integers. Then* $\mathfrak{o}$ *is a free* $\mathbb{Z}$*-module of rank* $n = [F\colon \mathbb{Q}]$. *Let* $\alpha_1, \cdots, \alpha_n$ *be a basis. Let* $\alpha \longrightarrow \alpha^{(i)}$ *denote the* n *distinct embeddings. Then*

$$D = \det(\alpha_i^{(j)})^2 \in \mathbb{Z}$$

and is independent of the choice of basis.

Proof. We assume known the fact that $\mathfrak{o}$ is a free $\mathbb{Z}$-module of rank n. Applying an element $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ just permutes the embeddings $\alpha \longrightarrow \alpha^{(i)}$, that is, multiplies the columns of the matrix $(\alpha_i^{(j)})$. Thus applying σ multiplies $\det(\alpha_i^{(j)})$ by ± 1, hence leaves D unchanged. Therefore $D \in \mathbb{Q}$ and since the $\alpha_i^{(j)}$ are algebraic integers, it is in $\mathbb{Z}$.

The determinant $\det(\alpha_i^{(j)})$ is only changed by sign if α_i is replaced by another $\mathbb{Z}$-basis, since if β_i is another basis then $\beta_j = \sum c_{ij}\alpha_i$ for some $(c_{ij}) \in \mathrm{GL}(n, \mathbb{Z})$, so $\det(\beta_i^{(j)}) = \det(c_{ij})\det(\alpha_i^{(j)}) = \pm \det(\alpha_i^{(j)})$. □

The integer D is called the *discriminant* of F.

Let F be a quadratic extension of $\mathbb{Q}$. We may write $F = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Q}$. Since we may multiply d by α^2 where $\alpha \in \mathbb{Q}^\times$ without changing F, we may assume that d is a squarefree integer. However this choice of d is not the best. It is better to write $F = \mathbb{Q}(\sqrt{D})$ where D is the *discriminant* of F.

Proposition 63. *If d is a squarefree integer and D is the discriminant of $\mathbb{Q}(\sqrt{d})$, then*

$$D = \begin{cases} d & \text{if } d \equiv 1 \bmod 4; \\ 4d & \text{if } d \equiv 2, 3 \bmod 4. \end{cases}$$

If $d \equiv 1 \bmod 4$, then $\mathfrak{o} = \mathbb{Z}[(1+\sqrt{D})/2]$; otherwise $\mathfrak{o} = \mathbb{Z}[\sqrt{D}]$.

Proof. Let us determine under what circumstances $a + b\sqrt{d} \in \mathfrak{o}$, where a and b are in $\mathbb{Q}$. It is necessary and sufficient that the norm and trace are in $\mathbb{Z}$, so

$$a^2 - db^2, \qquad 2a \in \mathbb{Z}.$$

Since d is squarefree, it is easy to see that

$$\alpha \in \mathbb{Q},\ d\alpha^2 \in \mathbb{Z} \Longrightarrow \alpha \in \mathbb{Q}. \tag{22}$$

In particular, $d(2b)^2 = -4(a^2 - db^2) + (2a)^2$. By (22), it follows that $2b \in \mathbb{Z}$. Thus we may write $a = 2A$, $b = 2B$, where $A, B \in \mathbb{Z}$ and $4 | A^2 - dB^2$. Note that since d is squarefree, $d \not\equiv 0 \bmod 4$. If A is odd then $A^2 \equiv 1 \bmod 4$ and if A is even the $A^2 \equiv 0 \bmod 4$. It follows that A and B are both even unless $d \equiv 1 \bmod 4$, in which case either A and B are both even or both odd. From this we deduce that if $d \equiv 1 \bmod 4$, then $\mathfrak{o} = \mathbb{Z}[(1 + \sqrt{D})/2]$; otherwise $\mathfrak{o} = \mathbb{Z}[\sqrt{D}]$. We may now compute the discriminant taking $\alpha_1 = 1$ and $\alpha_2 = (1+\sqrt{D})/2$ or $\alpha_2 = \sqrt{D}$. □

We say $D \in \mathbb{Z}$ is a *fundamental discriminant* if it is the discriminant of a quadratic field. The fundamental discriminants are precisely the numbers that occur in Proposition 63. We call a fundamental discriminant *elementary* if it is one of the following numbers:

$-4, 8$ or -8;
p where $p \equiv 1 \bmod 4$ is prime;
$-p$ where $p \equiv 3 \bmod 4$ is prime.

It is easy to see that every fundamental discriminant may be factored uniquely as a product of coprime elementary fundamental discriminants.

A *Dirichlet character* mod N is by definition a character χ of $(\mathbb{Z}/N\mathbb{Z})^\times$. We say χ is *primitive* if χ does not factor through the natural map

$$(\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/d\mathbb{Z})^\times$$

for any proper divisor d of N. Whether or not χ is primitive, we extend it to a function on all of $\mathbb{Z}/N\mathbb{Z}$ by denoting $\chi(\bar{a}) = 0$ if $a \in \mathbb{Z}$ and $\gcd(a, N) > 1$. A Dirichlet character χ modulo N is called *quadratic* if χ is nontrivial but $\chi^2 = 1$. It is called *primitive* if it does not factor through the canonical homomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/d\mathbb{Z})^\times$ for any proper divisor d of N.

Proposition 64. *Let D be a fundamental discriminant. Then there is a unique primitive quadratic Dirichlet character χ_D modulo D such that D and $\chi_D(-1)$ have the same sign. If D is not divisible by 8, then χ_D is the unique primitive quadratic Dirichlet character modulo D.*

Proof. Factor $D = D_1 \cdots D_r$, where each D_i is an elementary fundamental discriminant, and the D_i are coprime. If χ is a Dirichlet character modulo D, then since

$$(\mathbb{Z}/D\mathbb{Z})^\times \cong \prod_i (\mathbb{Z}/D_i\mathbb{Z})^\times$$

we may factor χ uniquely as $\prod \chi_i$, where χ_i is a Dirichlet character modulo D_i. It is clear that χ is primitive if and only if each χ_i is primitive. It is therefore sufficient to check this statement when D is an elementary fundamental discriminant.

If $D = -4$, 8 or -8, one checks immediately that there is a unique primitive Dirichlet character χ_D modulo D such that $\chi_D(-1)$ has the same sign as D; these χ_D are given by the following table:

n mod 8	$\chi_{-4}(n)$	$\chi_8(n)$	$\chi_{-8}(n)$
1	1	1	1
3	-1	-1	1
5	1	-1	-1
7	-1	1	-1

If p is an prime, then $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$. It has a unique quadratic character χ. If $p \equiv 1 \bmod 4$ then -1 is a square in $(\mathbb{Z}/p\mathbb{Z})^\times$, since as a cyclic group of order $p-1$ it contains an element of order 4 whose square is the unique element -1 of order 1. Thus $\chi(-1) = 1$. On the other hand, if $p \equiv 3 \bmod 4$ then -1 is not a square mod p, and since the kernel of χ consists of the squares, $\chi(-1) = -1$. In either case, if $D = \pm p$ is the corresponding elementary fundamental discriminant, $\chi(-1)$ has the same sign as D. □

We wish to embed quadratic fields in cyclotomic fields. This will be useful since the decomposition of primes in cyclotomic fields can be studied very easily; hence we will get the decomposition of primes in quadratic fields, and the quadratic reciprocity law. To accomplish the embedding, we will use *Gauss sums*, which we recall.

If χ is a primitive character modulo N, let

$$\tau(\chi) = \sum_{a \bmod N} \chi(a) e^{2\pi i a/N}.$$

This is a Gauss sum.

Proposition 65. *Let χ be a primitive Dirichlet character modulo N. Then*

$$|\tau(\chi)| = \sqrt{N}. \tag{23}$$

If n is any integer, we have

$$\sum_{a \bmod N} \chi(a) e^{2\pi i n a/N} = \overline{\chi(n)}\,\tau(\chi). \tag{24}$$

Proof. We first prove (24). If n is relatively prime to N, then $\overline{\chi(n)}$ is the reciprocal of $\chi(n)$, and we may move it to the left-hand side; the identity

$$\sum_{a \bmod N} \chi(na) e^{2\pi i n a/N} = \tau(\chi)$$

follows from simply reordering the residue classes. On the other hand if $d = \gcd(N, n) > 1$, then by definition $\chi(n) = 0$ so we must show that

$$\sum_{a \bmod N} \chi(a) e^{2\pi i n a/N} = 0. \tag{25}$$

Let $M = N/d$, and let $n_0 = n/d$. We parametrize the cosets $a \bmod N$ by writing $a = Mq + r$, where q is chosen modulo d and r is chosen modulo M. The sum equals

$$\sum_{\substack{q \bmod d \\ r \bmod M}} \chi(Mq + r) e^{2\pi i n_0 r/M}.$$

For fixed r we claim that

$$0 = \sum_{q \bmod d} \chi(qd + r) = \sum_{\substack{a \bmod N \\ a \equiv r \bmod M}} \chi(a).$$

The reason is that since χ is primitive it does not factor through the canonical map $(\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/M\mathbb{Z})^\times$, so χ is nontrivial on the kernel of this map. This means that there exists $\lambda \equiv 1 \bmod M$ such that $\chi(\lambda) \neq 1$. Multiplying the sum on the right side by $\chi(\lambda)$ does not change the sum since it permutes the $\chi(a)$; hence this sum is zero. This proves (25) and hence (24).

Now let us prove (23). We have

$$\begin{aligned} \left| \sum_{n \bmod N} \chi(a) e^{2\pi i a n/N} \right|^2 &= \left(\sum_{a \bmod N} \chi(a) e^{2\pi i n a/N} \right) \left(\sum_{m \bmod N} \overline{\chi(b)}\, e^{-2\pi i m b/N} \right) \\ &= \sum_{a,b \bmod N} \chi(a)\overline{\chi(b)}\, e^{2\pi i n(a-b)/N}. \end{aligned}$$

By (24), this is $|\tau(\chi)|^2$ if $(n,N)=1$, and zero otherwise. Summing over n, we have

$$\phi(N)|\tau(\chi)|^2 = \sum_{a,b \bmod N} \chi(a)\overline{\chi(b)} \sum_{n \bmod N} e^{2\pi i n(a-b)/N}$$
$$= N \sum_{\substack{a,b \bmod N \\ a \equiv b \bmod N}} \chi(a)\overline{\chi(b)}.$$

Here ϕ is Euler's function, that is, $\phi(N)$ is the number of residue classes prime to N. Now assuming $a \equiv b$ modulo N,

$$\chi(a)\overline{\chi(b)} = \begin{cases} 1 & \text{if } \gcd(N,a) = \gcd(N,b) = 1; \\ 0 & \text{otherwise.} \end{cases}$$

Thus the right-hand side is $N\phi(N)$, proving (23). □

Proposition 66. *Let D be a fundamental discriminant. Then*

$$\tau(\chi_D)^2 = D.$$

Proof. By (24),

$$\overline{\tau(\chi_D)} = \sum \chi_D(a) e^{-2\pi i n/D} = \chi_D(-1)\tau(\chi_D).$$

Multiplying by $\tau(\chi_D)$ and using (23), we get $\tau(\chi_D)^2 = \chi_D(-1)|D| = D$ since D and $\chi_D(-1)$ have the same sign. □

If N is a nonnegative integer, let $\zeta_N = e^{2\pi i/N}$.

Corollary 67. *Let D be a fundamental discriminant. Then $\mathbb{Q}(\sqrt{D})$ is contained in $\mathbb{Q}(\zeta_D)$.*

Proof. Clear since $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\tau(\chi_D))$ and $\tau(\chi_D) \in \mathbb{Q}(\zeta_D)$. □

Now we come to the fundamental significance of the character χ_D: it describes the decomposition of prime ideals in $\mathbb{Q}(\sqrt{D})$. We recall some basic facts from algebraic number theory in the present setting.

Let p be a prime not dividing D. The *decomposition field* K for p is the subfield of $\mathbb{Q}(\zeta_D)$ that is characterized as follows. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$ acts transitively on the primes of $\mathfrak{o}_{\mathbb{Q}(\zeta_D)} = \mathbb{Z}[\zeta_D]$ above p. If $\mathfrak{P}$ is such a prime, then K is the fixed field of the stabilizer in $\mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$ of $\mathfrak{P}$. It is the smallest field K such that if $\mathfrak{q} = \mathfrak{P} \cap \mathfrak{o}_K$, then $\mathfrak{P}$ is the unique prime ideal of $\mathfrak{o}_{\mathbb{Q}(\zeta)}$ above $\mathfrak{q}$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$ is abelian, it can also be characterized as the largest field in which p splits completely. The residue field $\mathfrak{o}_K/\mathfrak{q} \cong \mathbb{F}_p$. The *decomposition group* $\mathrm{Gal}(\mathbb{Q}(\zeta_D)/K)$ is isomorphic to the Galois group of $\mathbb{Z}[\zeta_D]/\mathfrak{P}$ over $\mathbb{F}_p$. It is generated by the Frobenius element $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$, which is the automorphism such that $\sigma_p(\zeta) = \zeta^p$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q}) \cong (\mathbb{Z}/D\mathbb{Z})^\times$, the order of σ_p in $\mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$ equals the order of p in $(\mathbb{Z}/D\mathbb{Z})^\times$, and if this order is f, it follows that f is the degree of $\mathbb{Z}[\zeta_D]/\mathfrak{P}$ over $\mathbb{F}_p$. Consequently there are exactly r primes of $\mathbb{Z}[\zeta_D]$ above p, where $r = n/f$.

Theorem 68. *Let D be a fundamental discriminant, and let $\mathfrak{o}$ be the ring of integers in $\mathbb{Q}(\sqrt{D})$. Let p be a prime. Then*

$$\chi_D(p) = \begin{cases} 1 & \text{if } p \text{ splits in } \mathfrak{o}; \\ -1 & \text{if } p \text{ remains prime in } \mathfrak{o}; \\ 0 & \text{if } p \text{ ramifies in } \mathfrak{o}. \end{cases}$$

Proof. We assume known the fact that the rational primes which ramify in a field are precisely those that divide the discriminant, so the last case is clear. We may assume that $p \nmid D$ and that p is nonramified in $\mathfrak{o}$.

We note that p splits in $\mathfrak{o}$ if and only if the restriction of $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$ to $\mathbb{Q}(\sqrt{D})$ is trivial. This is because σ_p generates the decomposition group, so its restriction to $\mathbb{Q}(\sqrt{D})$ is trivial if and only if σ_p is contained in its fixed field, which is the decomposition field. By Corollary 67, it is sufficient to compute the effect of σ_p on the Gauss sum $\tau(\chi_D)$. We have

$$\sigma_p(\tau(\chi_D)) = \sum_{a \bmod N} \chi(a) e^{2\pi i p a/N} = \chi_D(p)\,\tau(\chi_D)$$

by (24), and the statement is now clear. □

We may now prove the quadratic reciprocity law, whose statement we recall. Let p be an odd prime, a an integer. We say that a is a *quadratic residue* modulo p if $\gcd(a, p) = 1$ and $x^2 \equiv a$ has a solution modulo p. In this case it the equation has two solutions, x and $-x$, which are distinct because p is odd. We say that a is a *quadratic nonresidue* if $x^2 \equiv a$ has no solutions. We define the *Legendre symbol*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue;} \\ -1 & \text{if } a \text{ is a quadratic nonresidue;} \\ 0 & \text{if } p \mid a. \end{cases}$$

Theorem 69. *The Legendre symbol has the following properties.*

(a) If p is an odd prime, then

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4; \\ -1 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

(b) If p is an odd prime, then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8; \\ -1 & \text{if } p \equiv \pm 3 \bmod 8. \end{cases}$$

(c) If p and q are odd primes then

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \bmod 4 \text{ and } q \equiv 1 \bmod 4; \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \bmod 4. \end{cases}$$

Part (c) is the *quadratic reciprocity law.*

Proof. Since $a \longmapsto \left(\frac{a}{p}\right)$ is the unique quadratic character modulo p, we have

$$\left(\frac{a}{p}\right) = \chi_D(a), \qquad D = \begin{cases} p & \text{if } p \equiv 1 \bmod 4; \\ -p & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

With this in mind, (a) follows from the fact that D and $\chi_D(-1)$ have the same sign, which is asserted in Proposition 64.

For (b), we need to compute $\left(\frac{q}{p}\right)$ where $q = 2$ or q is an odd prime. Noting that $\mathfrak{o}_{\mathbb{Q}(\sqrt{D})}$ is generated by $\theta = \frac{1}{2}(1 + \sqrt{D})$, by Theorem 68 we see that $\left(\frac{q}{p}\right) = 1$ if and only of q splits in $\mathbb{Q}(\sqrt{D})$. A necessary and sufficient condition is that the polynomial

$$f(X) = X^2 - X + \frac{1}{4}(1 - D)$$

satisfied by θ has a root α in $\mathbb{F}_q$, since q splits if and only if there is a prime ideal $\mathfrak{q}$ of $\mathfrak{o}_{\mathbb{Q}(\sqrt{D})}$ such that $\mathfrak{q} \cap \mathbb{Z} = (q)$ and $\mathfrak{o}_{\mathbb{Q}(\sqrt{D})}/\mathfrak{q} \cong \mathbb{F}_q$; and if this is true then the image of θ under this isomorphism will be the required root α.

Now f will have a root in $\mathbb{F}_q$ if and only if the discriminant D of f is a square in $\mathbb{F}_q$. Assume first q is an odd prime. We have proved that

$$\left(\frac{q}{p}\right) = \left(\frac{D}{q}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \bmod 4; \\ \left(\frac{-p}{q}\right) & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

This boils down to the quadratic reciprocity law (c).

On the other hand, suppose that if $q = 2$. Then f has a root in $\mathbb{F}_2$ if and only if $\frac{1}{4}(1 - D)$ is even. This means that either $p \equiv 1 \bmod 4$ and that $\frac{1}{4}(1 - p)$ is even, or that $p \equiv 3 \bmod 4$ and that $\frac{1}{4}(1 + p)$ is even; that is, $p \equiv \pm 1 \bmod 8$. This proves (b). □

6 The Hilbert Reciprocity Law

The Hilbert symbol may be defined by Definition 42 for any local field. We have already discussed the nonarchimedean symbols. For archimedean fields, the symbol is simply described.

Proposition 70. *(i) Let $F = \mathbb{R}$, and let $a, b \in \mathbb{R}^\times$. Then the Hilbert symbol*

$$(a, b)_{\mathbb{R}} = \begin{cases} -1 & \textit{if } a, b \textit{ are both negative;} \\ 1 & \textit{otherwise.} \end{cases}$$

(ii) Let $F = \mathbb{C}$. Then $(a, b)_{\mathbb{C}} = 1$ for all $a, b \in \mathbb{C}^\times$.

Proof. For (i), clearly $x^2 - ay^2 - bz^2 = 0$ will have a solution with nonzero (x, y, z) if and only if a, b are not both negative, and for (ii), there will always be a solution. □

Proposition 71. *Let $F = \mathbb{Q}_2$.*
(i) If p, q are odd integers, then

$$(p, q)_F = \begin{cases} -1 & \text{if } p \equiv q \equiv 3 \text{ mod } 4; \\ 1 & \text{otherwise.} \end{cases}$$

(ii) If p is an odd integer, then

$$(2, p)_F = \begin{cases} 1 & \text{if } p \equiv \pm 1 \text{ mod } 8; \\ -1 & \text{otherwise.} \end{cases}$$

(iii) We have $(2, 2)_F = 1$.

Proof. This can be read off from Table 1. □

Now let F be a global field of characteristic not equal to 2. For each place v of F, there is a Hilbert symbol for F_v, defined as above, which we now denote as $(a, b)_v$. The *Hilbert reciprocity law*, for $a, b \in F^\times$, is the formula

$$\prod_v (a, b)_v = 1. \tag{26}$$

Note that $(a, b)_v = 1$ for almost all v by Proposition 51, since for almost all v, v is nonarchimedean, nondyadic, and a, v are units. Hence the left-hand side in (26) is a finite product.

Let $D = Q_F(a, b)$ be the quaternion algebra. If v is a place of F, then $F_v \otimes Q_F(a, b) \cong Q_{F_v}(a, b)$. We say that D *ramifies* at v if $Q_{F_v}(a, b)$ is a division algebra. In view of Theorem 59, we may express (26) as saying that the number of places where D ramifies is even. This statement is closely related to the quadratic reciprocity law. In this section, we will derive the Hilbert reciprocity law when $F = \mathbb{Q}$ from the ordinary quadratic reciprocity law.

Theorem 72. *Let $F = \mathbb{Q}$, and let $a, b \in \mathbb{Q}^\times$. Then $(a, b)_v = 1$ for all but finitely many places v of F, and*

$$\prod_v (a, b)_v = 1. \tag{27}$$

Proof. Using the bilinearity of the Hilbert symbol, we reduce immediately to the case where both a, b are either a prime or -1. If p and q are odd primes, then

$$(p, q)_v = \begin{cases} \left(\frac{q}{p}\right) & \text{if } v = p; \\ \left(\frac{p}{q}\right) & \text{if } v = q; \\ -1 & \text{if } v = 2 \text{ and } p \equiv q \equiv 3 \bmod 4; \\ 1 & \text{otherwise.} \end{cases}$$

Thus (27) with $a = p$ and $b = q$ amounts to the quadratic reciprocity law.

If p is an odd prime then

$$(2,p)_v = \begin{cases} 1 & \text{if } v=2 \text{ and } p \equiv \pm 1 \bmod 8; \\ -1 & \text{if } v=2 \text{ and } p \equiv \pm 3 \bmod 8; \\ \left(\frac{2}{p}\right) & \text{if } v=p; \\ 1 & \text{otherwise.} \end{cases}$$

In this case, $(2,p)_2$ and $(2,p)_p$ are equal, so (27) with $a=2$ and $b=p$ is satisfied.

We have $(2,2)_v = 1$ for all v, so (27) with $a=2$ and $b=2$ is satisfied.

We have considered enough cases to conclude (27) if a and b are both positive. On the other hand $(a,-a)_v = 1$ for all v, so if $a>0$ and $b<0$ we have

$$\prod_v (a,b)_v = \prod_v (a,-ab)_v, \tag{28}$$

which is 1 since a and $-ab$ are both positive. Finally, if a and b the same identity (28) are both negative, the same identity reduces to the case where only one of a and b are negative and the other positive – the case just proved. □

Bibliography

[1] I. N. Herstein. *Noncommutative rings*. The Carus Mathematical Monographs, No. 15. Published by The Mathematical Association of America, 1968.

[2] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[3] O. T. O'Meara. *Introduction to quadratic forms*. Springer-Verlag, New York, 1971. Second printing, corrected, Die Grundlehren der mathematischen Wissenschaften, Band 117.

[4] André Weil. *Basic number theory*. Springer-Verlag, New York, third edition, 1974. Die Grundlehren der Mathematischen Wissenschaften, Band 144.