Exercises†

Exercise 1: The power residue symbol
Exercise 2: The norm residue symbol
Exercise 3: The Hilbert class field
Exercise 4: Numbers represented by quadratic forms
Exercise 5: Local norms not global norms
Exercise 6: On decomposition of primes
Exercise 7: A lemma on admissible maps
Exercise 8: Norms from non-abelian extensions

Exercises 1: The Power Residue Symbol (Legendre, Gauss, et al.)

This exercise is based on Chapter VII, § 3, plus Kummer theory (Chapter III,
§ 2). Let m be a fixed natural number and K a fixed global field containing
the group \( \mu_m \) of mth roots of unity. Let \( S \) denote the set of primes of K
consisting of the archimedean ones and those dividing m. If \( a_1, \ldots, a_s \) are
elements of \( K^* \), we let \( S(a_1, \ldots, a_s) \) denote the set of primes in \( S \), together
with the primes \( p \) such that \( |a_i|_p \neq 1 \) for some \( i \). For \( a \in K^* \) and \( b \in f^{S(a)} \)
the symbol \( \left( \frac{a}{b} \right) \) is defined by the equation
\[
\left( \frac{a}{b} \right)^{f_{L/K}} = \left( \frac{a}{b} \right)^{\sqrt{a}},
\]
where \( L \) is the field \( K(\sqrt{a}) \).

Exercise 1.1. Show \( \left( \frac{a}{b} \right) \) is an mth root of 1, independent of the choice
of \( \sqrt{a} \).

Exercise 1.2. Working in the field \( L' = K(\sqrt{a}, \sqrt{a'}) \) and using Chapter
VII, § 3.2 with \( K' = K \) and \( L = K(\sqrt{a}) \), show
\[
\left( \frac{a'a}{b} \right) = \left( \frac{a}{b} \right) \left( \frac{a'}{b} \right)
\]
if \( b \in f^{S(a,a')} \).

Exercise 1.3. Show
\[
\left( \frac{a}{bb'} \right) = \left( \frac{a}{b} \right) \left( \frac{a}{b'} \right)
\]
if \( b \in f^{S(a)} \).

† These "exercises" refer primarily to Chapter VII, "Global class field theory", and were
prepared after the Conference by Tate with the connivance of Serre. They adumbrate
was not enough time in the Conference itself,

Hence,
\[
\left( \frac{a}{b} \right) = \prod_{v \in S(a)} \left( \frac{a}{v} \right)^{n_v} \quad \text{if } b = \sum n_v v.
\]

Exercise 1.4. (Generalized Euler criterion.) If \( v \not\in S(a) \) then \( m(N_v - 1) \),
where \( N_v = [K(v) : K] \), and \( \left( \frac{a}{v} \right) \) is the unique mth root of 1 such that
\[
\left( \frac{a}{v} \right) \equiv a^{rac{N_v - 1}{m}} \pmod{p_v}.
\]

Exercise 1.5. (Explanation of the name "power residue symbol"). For
\( v \not\in S(a) \) the following statements are equivalent:
(i) \( \left( \frac{a}{v} \right) = 1 \).
(ii) The congruence \( x^m \equiv a \pmod{p_v} \) is solvable with \( x \in a_v \).
(iii) The equation \( x^m = a \) is solvable with \( x \in K_v \).

(Use the fact that \( K(v)^* \) is cyclic of order \( (N_v - 1) \), and Hensel’s lemma,
Chapter II, App. C.)

Exercise 1.6. If \( b \) is an integral ideal prime to \( m \), then
\[
\left( \frac{\zeta}{b} \right) = \zeta^{\frac{N_b b - 1}{m}} \quad \text{for } \zeta \in \mu_m.
\]

(Do this first, using Exercise 1.4, in case \( b = v \) is prime. Then for general
\( b = \sum n_v v \), note that, putting \( N_b = 1 + m r \), we have
\[
N_b = \prod (1 + m r) \equiv 1 + m \sum n_v r \pmod{m^2}.
\]

Exercise 1.7. If \( a \) and \( b \in f^{S(a)} \) are integral, and if \( a' = a \pmod{b} \),
then \( \left( \frac{a'}{b} \right) = \left( \frac{a}{b} \right) \).

Exercise 1.8. Show that Artin’s reciprocity law (Chapter VII, § 3.3) for a
simple Kummer extension \( L = K(\sqrt{a}) \) implies the following statement: If \( b \) and \( b' \in f^{S(a)} \), and \( \left( \frac{a}{b'} \right) = (c) \) is the principal ideal of an element \( c \in K^* \)
such that \( c \in (K_v^*)^m \) for all \( v \in S(a) \), then \( \left( \frac{a}{b'} \right) = \left( \frac{a}{b} \right) \). Note that for \( v \not\in S \),
the condition \( c \in (K_v^*)^m \) will certainly be satisfied if \( c \equiv 1 \pmod{p_v} \).

Exercise 1.9. Specialize now to the case \( K = Q, m = 2 \). Let \( a, b, \ldots \)
denote arbitrary non-zero rational integers, and let \( P, Q, \ldots \) denote positive,
odd rational integers. For \( (a, P) = 1 \), the symbol \( \left( \frac{a}{P} \right) = \left( \frac{a}{(P)} \right) = \pm 1 \) is
defined, is multiplicative in each argument separately, and satisfies

\[
\left( \frac{a}{P} \right) = \left( \frac{b}{P} \right) \quad \text{if } a \equiv b \pmod{P}.
\]

Artin's reciprocity law for \( \mathbb{Q}(\sqrt{a})/\mathbb{Q} \) implies

(*)

\[
\left( \frac{a}{P} \right) = \left( \frac{a}{Q} \right) \quad \text{if } P \equiv Q \pmod{8a_0},
\]

where \( a_0 \) denotes the "odd part of \( a \)," i.e. \( a = \text{odd} \cdot a_0 \), with \( a_0 \) odd. (Use the fact that numbers \( \equiv 1 \pmod{8} \) are 2-adic squares.)

Exercise 1.10. From Exercise 1.9 it is easy to derive the classical law of quadratic reciprocity, namely

\[
\left( \frac{-1}{P} \right) = (-1)^{\frac{p-1}{2}}, \quad \left( \frac{2}{P} \right) = (-1)^{\frac{p-1}{2}}, \quad \text{and} \quad \left( \frac{P}{Q} \right) = \left( \frac{Q}{P} \right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}.
\]

Indeed the formula (*) above allows one to calculate \( \left( \frac{a}{P} \right) \) as function of \( P \) for any fixed \( a \) in a finite number of steps, and taking \( a = -1 \) and 2 one proves the first two assertions easily. For the last, define

\[
\langle P, Q \rangle = \left( \frac{P}{Q} \right) \left( \frac{Q}{P} \right), \quad \text{for } (P, Q) = 1.
\]

Then check first that if \( P \equiv Q \pmod{8} \) we have

\[
\langle P, Q \rangle = \left( \frac{-1}{Q} \right)
\]

and the given formula is correct. (Writing \( Q = P + 8a \) one finds using Exercise 1.9 that, indeed,

\[
\left( \frac{Q}{P} \right) = \left( \frac{8a}{P} \right) = \left( \frac{8a}{Q} \right) = \left( \frac{-P}{Q} \right).
\]

Now, given arbitrary relatively prime \( P \) and \( Q \), one can find \( R \) such that \( RP \equiv Q \pmod{8} \) and \( (R, Q) = 1 \) (even \( R \equiv 1 \pmod{Q} \)), and then, by what we have seen,

\[
\langle P, Q \rangle \langle R, Q \rangle = \langle PR, Q \rangle = \left( \frac{-1}{Q} \right).
\]

Fixing \( R \) and varying \( P \), keeping \( (P, Q) = 1 \), we see that \( \langle P, Q \rangle \) depends only on \( P \pmod{8} \). By symmetry (and the fact that the odd residue classes \( \pmod{8} \) can be represented by numbers prime to any given number), we see that \( \langle P, Q \rangle \) depends only on \( Q \pmod{8} \). We are therefore reduced to a small finite number of cases, which we leave to the reader to check. The next exercise gives a general procedure by which these last manoeuvres can be replaced.
system of representatives of the cosets of \( \mu_n \) in \( \mu_m \), we have for each \( x \in F \):
\[
x^m - a = \prod_{\alpha \in \mu_m} (x - \zeta \alpha) = N_{F(\alpha)/F} \left( \prod_{i=1}^{m/\ell} (x - \zeta_i \alpha) \right),
\]
Q.E.D.

**Exercise 2.6.** Show that \( (a, b)_e (b, a)_e = 1 \). (Just use bilinearity on \( 1 = (ab, -ab)_e \).)

**Exercise 2.7.** If \( v \) is archimedean, we have \( (a, b)_e = 1 \) unless \( K_v \) is real, both \( a < 0 \) and \( b < 0 \) in \( K_v \), and \( m = 2 \). (In the latter case we do in fact have \( (a, b)_e = -1 \); see the remark in Exercise 2.4. Note that \( m > 2 \) implies that \( K_v \) is complex for every archimedean \( v \).)

**Exercise 2.8.** (Relation between norm-residue and power-residue symbols.)

If \( v \notin S(a) \), then \( (a, b)_e = \frac{(c)}{b} \); in particular, \( (a, b)_e = 1 \) for \( v \notin S(a, b) \).

(See the first lines of Exercise 1 for the definition of \( S \) and \( S(a) \), etc. The result follows from the description of the local Artin map in terms of the Frobenius automorphism in the unramified case. More generally,
\[
v \notin S \Rightarrow (a, b)_e = \left( \frac{c}{b} \right), \text{ where } c = (-1)^{v(a)(b)} a^{v(b)} b^{-v(a)}
\]
is a unit in \( K_v \) which depends bilinearly on \( a \) and \( b \). To prove this, just write \( a = \pi^{v(a)} a_0 \) and \( b = \pi^{v(b)} b_0 \) where \( v(\pi) = 1 \), and work out \( (a, b)_e \) by the previous rules; for the geometric analog discussed in remark 3.6 of Chapter VII, see Serre, loc. cit., Ch. III, Section 4.)

**Exercise 2.9.** (Product Formula.) For \( a, b \in K^* \) we have \( \prod (a, b)_e = 1 \), the product being taken over all primes \( v \) of \( K \).

**Exercise 2.10.** (The general power-reciprocity law.) For arbitrary \( a \) and \( b \) in \( K^* \) we define
\[
\left( \frac{a}{b} \right) = \prod_{v \in S(a)} \left( \frac{a}{b} \right)_e = \left( \frac{a}{(b)^{S(a)}} \right).
\]
where \((b)^e\) is defined in Chapter VII, § 3.2.

**Warning:** With \( \frac{a}{b} \) defined in this generality the rule \( \left( \frac{ab}{b} \right) = \left( \frac{a}{b} \right) \left( \frac{b}{b} \right) \) does not always hold, but it does hold if \( S(b) \cap S(a, a') = S \), and especially if \( b \) is relatively prime to \( a \) and \( a' \). The other rule, \( \left( \frac{a}{bb'} \right) = \left( \frac{a}{b} \right) \left( \frac{a}{b'} \right) \) holds in general.

Using Exercises 2.6, 2.8, and 2.9, prove that
\[
\left( \frac{a}{b} \right) \left( \frac{b}{a} \right)^{-1} = \prod_{v \in S(a) \cap S(b)} (b, a)_e.
\]

**Exercise 2.11.** If \( K = Q \) and \( m = 2 \), then \( S = \{ 2, \infty \} \), and for \( P > 0 \) are equivalent with
\[
(-1, P)_2 = (-1)^{P-1} 2^\frac{P-1}{2}, \quad (2, P)_2 = (-1)^{P-1} 2^\frac{P-1}{2} \quad \text{and} \quad (P, Q)_2 = (-1)^P 2^\frac{P-1}{2}.
\]

In particular
\[
\left( \frac{a}{b} \right) \left( \frac{b}{a} \right)^{-1} = \prod_{v \in S} \left( \frac{b}{a} \right)_v \quad \text{if } S(a) \cap S(b) = S,
\]
and
\[
\left( \frac{b}{a} \right) = \prod_{v \in S} \left( \frac{b}{a} \right)_v \quad \text{if } S(b) \subseteq S.
\]

**Exercise 2.12.** An element \( a \in K \) is called \( v \)-primary (for \( m \)) if \( K(\zeta^m)/K \) is unramified at \( v \). For \( v \notin S \), there is no problem: an element \( a \) is \( v \)-primary if and only if \( v(a) = 0 \mod m \). Suppose now \( v \) divides \( m \) and \( m = p \) is a prime number.

Let \( \zeta \) be a generator of \( \mu_p \), and put \( \lambda = 1 - \zeta \). (Check that \( \lambda^{p-1}/p \) is a unit at \( v \), and more precisely, that \( \lambda^{p-1} \equiv -p \mod \lambda p \), so that \( \lambda^{p-1}/p \equiv -1 \mod \lambda p \).) Let \( a \) be such that \( a \equiv 1 \mod \lambda p \), so that we have \( a = 1 + \lambda^p c \), with \( c \in o_v \). Prove that \( a \) is \( v \)-primary, and that for all \( b \),
\[
(a, b)_e = \left( \frac{-\lambda^{p-1}/p}{b} \right)_e,
\]
where \( S \) denotes the trace from \( k(v) \) to the prime field and \( \lambda \) is the residue of \( c \). Also, if \( a \equiv 1 \mod (p \lambda p) \), then \( a \) is \( v \)-hyperprimary, i.e. \( a \in (K_v)^* \).

(1) Let \( a^* = a \), and write \( a = 1 + \lambda x \). Check that \( x \) is the root of a polynomial \( f(X) \in o_v[X] \) such that \( f(X) \equiv X^p - X - c \mod p \). Thus \( f(x) \equiv x - 1 \equiv 0 \mod p \), so \( K_v(\zeta^m)/K_v \) is indeed unramified. And if \( c \equiv 0 \mod p \), then \( f(X) \) splits by Hensel's lemma, so \( K_v(\zeta^m/a) = K_v \). Now \( x^p \equiv x + c \mod p \), so if \( Nv = p^f \), then
\[
x^p = x^{\nu} \equiv x + c + c^p + \ldots + c^{p^{f-1}} \equiv x + S(c) \mod p \]
on the other hand, if \( x' = \zeta x = 1 + \lambda x' \), then \( x' \equiv x - 1 \mod p \). Combining these facts gives the formula for \( (a, b)_e \).

**Exercise 2.13.** Let \( p \) be an odd prime, \( \zeta \) a primitive \( p \)th root of unity, \( K = Q(\zeta) \), and \( m = p \). Then \( p \) is totally ramified in \( K \), and \( \lambda = 1 - \zeta \) generates the prime ideal corresponding to the unique prime \( v \) of \( K \) lying over \( p \). Let \( U_i \) denote the group of units \( 1 \mod \lambda^i \) in \( K^*_v \), for \( i = 1, 2, \ldots \).

Then the image of \( \eta_i = 1 - \lambda^i \) generates \( U_i/\lambda U_i \), which is cyclic of order \( p \), and the image of \( \lambda \) generates \( K^*_v/(K^*_v)^p U_1 \). By the preceding exercise,
Hence, by Tchebotarow's theorem, the densities of these sets of primes are
\(1/6, 1/3\) and \(1/2\), respectively.

**Exercise 2.16.** Consider again an arbitrary \(K\) and \(m\). Let \(a_1, \ldots, a_r\) be the \(m\)th roots of those elements. Let \(T\) be a finite set of primes of \(K\)
\[ J_L = L^*J_{L,T}, \]
where \(T\) is the set of primes of \(L\) lying over \(T\). Suppose we are given elements \(\zeta_{v,i} \in \mu_m\) for \(v \in T\) and \(1 \leq i \leq r\), such that

(i) For each \(i\), we have \(\prod_{v \in T} \zeta_{v,i} = 1\), and

(ii) For each \(v \in T\), there exists an \(x_v \in K_v^*\) such that \((x_v, a_v) = \zeta_{v,i}\) for all \(i\).

Show then that there exists a \(T\)-unit \(x \in K_T\) such that \((x, a) = \zeta_{v,i}\) for all \(v \in T\) and \(1 \leq i \leq r\).

The additional condition on \(T\), involving \(T_1\), is necessary, as is shown by the example \(K = \mathbb{Q}, m = 2, T = \{\infty, 2, 7\}, r = 1, a_1 = -14, \zeta_{7,1} = -1, \zeta_{2,1} = 1\). To prove the statement, consider the group \(X = \prod_{v \in T} (K_v^*/(K_v^*)^m)\), the subgroup \(A\) generated by the image of \(K_v^*_1\), and the smaller subgroup \(A_0\) generated by the images of the elements \(a_v, 1 \leq i \leq r\). The form \(\langle x, y \rangle = \prod_{v \in T} (x_v, y_v)\) gives a non-degenerate pairing of \(X\) with itself to \(\mu_m\) under which \(A\) is self orthogonal, and indeed exactly so, because \([X] = m^2\) and \([A] = m^t\), where \(t = [T]\). (See step 4 in the proof of the second inequality in Chapter VII, § 9, the notations \(S, \sigma, \gamma\) and \(t\) being replaced by \(T, m\), and \(t\) here.) Thus \(X/A \approx \text{Hom}(A, \mu_m)\) (note by the way that both groups are isomorphic to \(\text{Gal}(K(\sqrt{m}/K))K\), by class field theory and Kummer theory, respectively), and vice versa, \(A \approx \text{Hom}(X/A, \mu_m)\). So far, we have not used the condition that \(J_L = L^*J_{L,T}\). Use it to show that if \(a \in A\) and \(\pi_a(a) \in \pi(A_0)\) for all \(v\), where \(\pi_a\) is the projection of \(X\) onto \(K_v^*/(K_v^*)^m\), then \(a \in A_0\), i.e. \(\sqrt{m}a \in L\). Now show that, in view of the dualities and orthogonalities discussed above, this last fact is equivalent to the statement to be proved.

**Exercise 3:** The Hilbert Class Field

Let \(L/K\) be a global abelian extension, \(v\) a prime of \(K\), and \(i_v: K_v^* \to J_K\) the canonical injection. Show that \(v\) splits completely in \(L\) if and only if \(i_v(K_v^*) \subset K^*N_{L/K}J_L\), and, for non-archimedean \(v\), that \(v\) is unramified in \(L\) if and only if \(i_v(U_v) \subset K^*N_{L/K}J_L\), where \(U_v\) is the group of units in \(K_v\).

(See Chapter VII, § 5.1, § 6.3.) Hence, the maximal abelian extension of \(K\) which is unramified at all non-archimedean primes and is split compl.

S now denotes the set of archimedean primes. (Use the Main Theorem...
This extension (Chapter VII, § 5.1) and the fact that \( K^*N_{L/K} J_L \) is closed.) This extension is called the Hilbert class field of \( K \); we will denote it by \( K' \). Show that the Frobenius homomorphism \( F_{K/K} \) induces an isomorphism of the ideal classes of \( K' \) onto the Galois group \( \mathbb{G}(K'/K) \). (Use the Main Theorem and the isomorphism \( J_{K/K} \approx I_K \).) Thus the degree \( [K': K] = \mathbb{G}(K'/K) \) is the number of real primes of \( K \).

We have \( Q_1 = Q \), clearly, but this is a poor result in view of Minkowski's theorem, to the effect that \( Q \) has no non-trivial extension which is unramified at all non-archimedean primes (Minkowski, "Geometrie der Zahlen", p. 130, or "Diophantische Approximationen" p. 127). Consider \( [K_1 : K'] = 1 \) or \( 2 \), according to whether \( N_{E} = -1 \) or \( N_{E} = 1 \), where \( E \) is a fundamental unit in \( K_1 \), and \( N = N_{K_1/K} \). For example, in case \( K = \mathbb{Q}(\sqrt{2}) \) or \( \mathbb{Q}(\sqrt{5}) \) we have \( K' = K_1 \), because the class number is 1, and consequently also the other hand, if \( K = \mathbb{Q}(\sqrt{3}) \), then again \( K' = K_1 \) or \( K = K_1 \), because the units \( \epsilon = 1+\sqrt{2} \) and \( 1 = 1+\sqrt{3} \) have norm -1. On the other hand, if \( K = \mathbb{Q}(\sqrt{3}) \), then again \( K' = K_1 \) or \( K = K_1 \), because the units \( \epsilon = 1+\sqrt{2} \) and \( 1 = 1+\sqrt{3} \) have norm -1. Show that \( K_1 = K(\sqrt{-1}) \) for any local law everywhere (as in the case \( K = \mathbb{Q}(\sqrt{3}) \) just considered), then \( N_{E} = 1 \), and \( K_1 \neq K' \). However, when \( N_{E} = 1 \) is a local norm everywhere, and is therefore the norm of a number in \( K \), there is still no general rule for predicting whether or not it is the norm of a unit.

Exercise 4. Numbers Represented by Quadratic Forms

Let \( K \) be a field of characteristic different from 2, and

\[ f(X) = \sum a_{ij} X_i X_j \]

a non-degenerate quadratic form in \( n \) variables with coefficients in \( K \). We say that \( f \) represents an element \( \epsilon \) in \( K \) if the equation \( f(X) = \epsilon \) has a solution \( X = x \in K^n \) such that not all \( x_i \) are zero. If \( f \) represents 0 in \( K \), then \( f \) represents all elements in \( K \). Indeed, we have

\[ t(X+Y) = t^2 f(X) + t B(X,Y) + f(Y). \]

If \( f(x) = 0 \) but \( x \neq (0,0,\ldots,0) \), then by the non-degeneracy there is a \( y \in K^n \) such that \( B(x,y) \neq 0 \), so that \( f(tx+y) \) is a non-constant linear function of \( t \) and takes all values in \( K \) as \( t \) runs through \( K \).

A linear change of coordinates does not affect questions of representability, and by such a change we can always bring \( f \) to diagonal form: \( f = \sum a_i x_i^2 \) with all \( a_i \neq 0 \). If \( f = c x_1^2 - g(x_2, \ldots, x_n) \) then \( f \) represents 0 if and only if \( g \) represents \( c \), because if \( g \) represents 0 then it represents \( c \). Hence, the question of representability of non-zero \( c \)'s by forms \( g \) in \( n-1 \) variables is equivalent to that of the representability of \( 0 \) by forms \( f \) in \( n \) variables. The latter question is not affected by multiplication of \( f \) by a non-zero constant; hence we can suppose \( f \) in diagonal form with \( a_1 = 1 \) in treating it:

Exercise 4.1. The form \( f = x^2 \) does not represent 0.

Exercise 4.2. The form \( f = x^2 - b Y^2 \) represents 0 if and only if \( b \in (K^*)^2 \).
EXERCISE 4.3. The form \( f = X^2 - bY^2 - cZ^2 \) represents 0 if and only if \( c \) is a norm from the extension field \( K(\sqrt{b}) \).

EXERCISE 4.4. The following statements are equivalent:

(i) The form \( f = X^2 - bY^2 - cZ^2 + aT^2 \) represents 0 in \( K \).

(ii) \( a \) is a product of \( a \) from \( K(\sqrt{b}) \) and a norm from \( K(\sqrt{ab}) \).

(iii) \( a \) is a product of \( a \) from \( K(\sqrt{ab}) \), a norm from \( K(\sqrt{a}) \), and a norm from \( K(\sqrt{b}) \).

(iv) The form \( g = X^2 - bY^2 - cZ^2 \) represents 0 in the field \( K(\sqrt{ab}) \).

EXERCISE 4.5. The form \( f \) of Exercise 4.3 represents 0 in a local field \( K \), if and only if the quadratic norm residue symbol \((b, c)_K = 1\). Hence \( f \) represents 0 in \( K \) for any but a finite number of \( v \) and the number of \( v \) for which it does not represent 0. Moreover, these last two statements are invariant under multiplication of \( f \) by a scalar and consequently hold for an arbitrary non-degenerate form in three variables over \( K \).

EXERCISE 4.6. Let \( f \) be as in Exercise 4.4. Show that if \( f \) does not represent 0 in a local field \( K \), then \( a \not\in (K^*)^2 \) and \( b \not\in (K^*)^2 \), but \( ab \in (K^*)^2 \), and \( c \) is not a norm from the quadratic extension \( K(\sqrt{a}) = K(\sqrt{b}) \). (Just use the fact that the norm groups from the different quadratic extensions of \( K \) are subgroups of index 2 in \( K^* \), no two of which coincide.) Now suppose conversely that those conditions are satisfied. Show that the set of elements in \( K \) which are represented by \( f \) is \( N = cN \) where \( N \) is the group of non-zero norms from \( K(\sqrt{a}) \), and in particular, that \( f \) does not represent 0 in \( K \).

Show, furthermore, that if \( N = cN \neq K^* \), then \( -1 \not\in N \), and \( N + N \subset N \). Hence \( f \) represents every non-zero element of \( K \) unless \( K \approx \mathbb{R} \) and \( f \) is positive definite.

EXERCISE 4.7. A form \( f \) in \( n \geq 5 \) variables over a local field \( K \) represents 0 unless \( K \) is real and \( f \) definite.
EXERCISES

360

For further developments and related work see O. T. O’Meara: “Intro-
duction to Quadratic Forms” (Springer, 1963) or Z. I. Borevič and I. R.
Z. I. Borevič and I. R. Shafarevič, “Number Theory”, Academic Press,
New York; German translation, S. I. Borevič and I. R. Shafarevič,
“Zahlentheorie”, Birkhäuser Verlag, Basel.]

Exercise 5: Local Norms Not Global Norms, etc.

Let $L/K$ be Galois with group $G = (1, \rho, r, s) \cong (Z/2Z)^2$, and let $K_1$, $K_2$, and $K_3$ be the three quadratic intermediate fields left fixed by $\rho, r, s$, respectively. Let $N_i = \text{N}_{K_i/K}$ for $i = 1, 2, 3$, and let $N = N_{L/K}(*)$.

Exercise 5.1. Show that $N_1N_2N_3 = \{ x \in K^* | x^2 \in N \}$. (This is pure algebra, not arithmetic; one inclusion is trivial, the other can be proved by the methods used in Exercise 4.3.)

Exercise 5.2. Now assume $K$ is a global field. Show that if the local degree of $L$ over $K$ is 4 for some prime, then $N_1N_2N_3 = K^*$ (cf. Chapter VII, § 11.4). Suppose now that all local degrees are 1 or 2. For simplicity, suppose $K$ of characteristic $\neq 2$, and let $K_i = K(\sqrt{a_i})$ for $i = 1, 2, 3$. For each $i$, let $S_i$ be the (finite) set of primes of $K$ which split in $K_i$, and for $x \in K^*$ put

$$\varphi(x) = \prod_{v \in S_1} (a_2, x)_v \prod_{v \in S_2} (a_3, x)_v \prod_{v \in S_3} (a_1, x)_v = \prod_{v \in S_1} (a_2, x)_v \prod_{v \in S_2} (a_3, x)_v \prod_{v \in S_3} (a_1, x)_v = \pm 1,$$

where $(x, y)_v$ is the quadratic norm residue symbol. Show that $N_1N_2N_3 = \text{Ker} \varphi$ is a subgroup of index 2 in $K^*$. (The inclusion $N_1N_2N_3 \subseteq \text{Ker} \varphi$ is trivial. From Exercise 5.1 above and Chapter VII, § 11.4 one sees that the index of $N_1N_2N_3$ in $K^*$ is at most 2. But there exists an $x$ with $\varphi(x) = 1$ by Exercise 2.16.)

Exercise 5.3. Let $K = Q$ and $L = Q(\sqrt{13}, \sqrt{17})$. Show that if $x$ is a product of primes $p$ such that $p = 2, 3, 5, 7, 11, \ldots$, then

$$\varphi(x) = \left( x \right)_{17}.$$  Hence $5^2, 7^2, 11^2, 13^2, \ldots$ are some examples of numbers which are local norms everywhere from $Q(\sqrt{13}, \sqrt{17})$ but are not global norms. Of course, not every such number is a square; for example, $-14^2$ is the global norm of $(7+2/13+\sqrt{17})$, and comparing with the above we see that $-1$ is a local norm everywhere but not a global norm.

Exercise 5.4. Suppose now that our global 4-group extension $L/K$ has the property that there is exactly one prime $v$ of $K$ where the local degree is 4: Let $w$ be the prime of $L$ above $v$ and prove that $A^{-1}(G, L^*) = 0$, but

$A^{-1}(G, L^*) \cong \mathbb{Z}/2Z$. (Use the exact sequence near the beginning of local degrees is the global degree. And the map $g: A^{-1}(G, L^*) \rightarrow \hat{A}(G, C_1)$ only one prime.)

Let $A$,resp. $A_{\omega}$, be the group of elements in $L^*$, resp $L^*$, whose norm the above that

$$A = (L^*)^{\omega-1}(L^*)^{-1}(L^*)^{-1},$$

and that

$$\hat{A} = (L^*)^{\omega-1}(L^*)^{-1}(L^*)^{-1},$$

which is of index 2 in $A_{\omega}$. Now, as is well known, there is an algebraic group $T$ defined over $K$ (the twisted torus of dimension 3 defined by the equation which show that the group of rational points on a torus $T$ is not necessarily dense in the group of $v$-adic points (see last paragraph below). However, $L/K$, then $T(K)$ is dense in $T(K_0)$ for every prime $v$ of $K$ such that there exists a prime $v' \neq v$ with the same decomposition group as $v'$ in particular, whenever the decomposition group of $v$ is cyclic, and more particularly, whenever $v$ is archimedean.

As a concrete illustration, take $K = Q$ and $L = Q(\sqrt{-1}, \sqrt{2}) = Q(i)$, where $i^2 = -1$. Then $L$ is unramified except at 2, but totally ramified at 2, and consequently there is just one prime, 2, with local degree 4. Let $M = Q(i)$ where $i^2 = -1$, and let $L_\omega$ and $M_\omega$ denote the completions at the primes above 2. It is easy to give an ad-hoc proof without cohomology that the elements of $L$ with norm 1 are not dense in those of $L_\omega^*$: just check that the element $z = (2+i)/(2-i) \in M_\omega$ is a norm from $L_\omega$ to $L_\omega$, but that $\sigma(z(M_\omega^*))$ contains no element $y \in M$ such that $y$ is a global norm from $L$ to $M$ and such that $\sigma(z(M_\omega^*)) = 1$.

Exercise 6: On Decomposition of Primes

Let $L/K$ be a finite global extension and let $S$ be a finite set of primes of $K$. We will denote by $\text{Spl}_i(L/K)$ the set of primes $v \notin S$ such that $v$ splits completely in $L$ (i.e. such that $L \otimes K_v \cong K_{1,v}$), and by $\text{Spl}_s(L/K)$ the set of primes $v \notin S$ which have a split factor in $L$ (i.e. such that there exists a $K$-isomorphism $L \cong K_v$). Thus $\text{Spl}_i(L/K) \subseteq \text{Spl}_s(L/K)$ always, and equality holds if $K$ is Galois, in which case $\text{Spl}_s(L/K)$ has density $[L : K]^{-1}$ by the Chebotarow density theorem. (Enunciated near end of Chapter VIII, § 3.)
EXERCISES

Exercise 6.1. Show that if $L$ and $M$ are Galois over $K$, then
$L \subset M$ implies $\text{Spl}_J(M) \subset \text{Spl}_J(L)$,

(Indeed, we have $\text{Spl}_J(L/K) = \text{Spl}_J(L/K) \cap \text{Spl}_J(M/K)$.

so $L \subset M$ implies $\text{Spl}_J(M) \subset \text{Spl}_J(L) \subset \text{Spl}_J(L/K) = \text{Spl}_J(M/K)$.

\[
\Rightarrow [LM : K] = [M : K] \Rightarrow L \subset M;
\]

where was Galoisness used? Hence
$L = M$ implies $\text{Spl}_J(L) = \text{Spl}_J(M)$.

Application: If a separable polynomial $f(X) \in K[X]$ splits into linear factors modulo $p$ for all but a finite number of prime ideals $\mathfrak{p}$ of $K$, then $f$ splits into linear factors in $K$. (Take $L = \text{splitting field of } f(X)$, and $M = K$, and $S$ large enough so that $f$ has integral coefficients and unit discriminant outside $S$.) Finally, note that everything in this exercise goes through if we replace “all primes $p \notin S$” and “all but a finite number of primes $p$” by “all $p$ in a set of density $0$”.

Exercise 6.2. Let $L/K$ be Galois with group $G$, let $H$ be a subgroup of $G$, and let $E$ be the fixed field of $H$. For each prime $\mathfrak{p}$ of $K$, let $G_{\mathfrak{p}}^\mathfrak{p}$ denote a decomposition group of $\mathfrak{p}$. Show that $G$ splits completely in $E$ if and only if all of the conjugates of $G_{\mathfrak{p}}^\mathfrak{p}$ are contained in $H$, whereas $G_{\mathfrak{p}}^\mathfrak{p}$ has a split factor in $E$ if and only if at least one conjugate of $G_{\mathfrak{p}}^\mathfrak{p}$ is contained in $H$. Hence, show that the set of primes $\text{Spl}_J(E/K)$ has density $\left(\bigcup_{p \in \mathcal{P}_G} H_{p^{-1}}\right) \cap [G]$. Now prove the lemma on finite groups which states that the union of the conjugates of a proper subgroup is not the whole group (because they overlap a bit at the identity!) and conclude that if $\text{Spl}_J(E/K)$ has density 1, then $E = K$. Application: If an irreducible polynomial $f(X) \in K[X]$ has a root modulo $p$ for all but a finite number of primes $p$, or even for a set of primes of density 1, then it has a root in $K$. This statement is false for reducible polynomials; consider for example $f(X) = (X^2 - a)(X^2 - b)(X^2 - ab)$, where $a$, $b$, and $ab$ are non-squares in $K$. Also, the set $\text{Spl}_J(E/K)$ does not in general determine $E$ up to an isomorphism over $K$; cf. Exercise 6.4 below.

Exercise 6.3. Let $H$ and $H'$ be subgroups of a finite group $G$. Show that the permutation representations of $G$ corresponding to $H$ and $H'$ are isomorphic, as linear representations, if and only if each conjugacy class of $G$ meets $H$ and $H'$ in the same number of elements. Note that if $H$ is a normal subgroup then this cannot happen unless $H' = H$. However, there are examples of subgroups $H$ and $H'$ satisfying the above condition which are not conjugate; check the following one, due to F. Gassmann (Math. Zeit., 25, 1926): Take for $G$ the symmetric group on 6 letters $(x_1)$ and put

\[ H = \{1, (X_1 X_2)(X_3 X_4), (X_1 X_3)(X_2 X_4), (X_1 X_4)(X_2 X_3) \} \]

\[ H' = \{1, (X_1 X_2)(X_3 X_4), (X_1 X_3)(X_2 X_4), (X_1 X_4)(X_2 X_3) \} \]

($H'$ leaves $X_1$ and $X_4$ fixed, where $H'$ leaves nothing fixed; but all elements $\neq 1$ of $H$ and $H'$ are conjugate in $G$.) Note that there exist Galois extensions of $Q$ with the symmetric group on 6 letters as Galois group.

Exercise 6.4. Let $L$ be a finite Galois extension of $Q$, let $G = G(L/K)$, and let $E$ and $E'$ be subfields of $L$ corresponding to the subgroups $H$ and $H'$ of $G$, respectively. Show that the following conditions are equivalent:

(a) $H$ and $H'$ satisfy the equivalent conditions of Exercise 6.3.
(b) The same primes $p$ are ramified in $E$ as in $E'$, and for the non-ramified $p$ the decomposition of $p$ in $E$ and $E'$ is the same, in the sense that the collection of degrees of the factors of $p$ in $E$ is identical with the collection of degrees of the factors of $p$ in $E'$, or equivalently, in the sense that $A[pA] = A'[pA']$, where $A$ and $A'$ denote the rings of integers in $E$ and $E'$, respectively.

(c) The zeta-function of $E$ and $E'$ are the same (including the factors at the ramified primes and at $\infty$).

Moreover, if these conditions hold, then $E$ and $E'$ have the same discriminant. If $H$ and $H'$ are not conjugate in $G$, then $E$ and $E'$ are not isomorphic. Hence, by Exercise 6.3, there exist non-isomorphic extensions of $Q$ with the same decomposition laws and same zeta functions. However, such examples do not exist if one of the fields is Galois over $Q$.

Exercise 7: A Lemma on Admissible Maps

Let $K$ be a global field, $S$ a finite set of primes of $K$ including the archimedean ones, $H$ a finite abelian group, and $\varphi : \mathcal{P} \to H$ a homomorphism which is admissible in the sense of paragraph 3.7 of the Notes. We will consider “pairs” $(L, \sigma)$ consisting of a finite abelian extension $L$ of $K$ and an injective homomorphism $\sigma : G(L/K) \to H$.

Exercise 7.1. Show that there exists a pair $(L, \sigma)$ such that $L/K$ is unramified outside $S$ and $\varphi(\sigma) = \alpha(F_{L/K}(\sigma))$ for all $\sigma \in \mathcal{P}$, where $F_{L/K}$ is as in Section 3 of the Notes. (Use Proposition 4.1 and Theorem 5.1.)

Exercise 7.2. Show that if $\varphi(\sigma) = 1$ for all primes $\sigma$ in a set of density 1 (e.g. for all but a finite number of the primes of degree 1 over $Q$), then $\varphi$ is identically 1. (Use the Tchebotaroff density theorem and Exercise 7.1.) Consequently, if two admissible maps of ideal groups into the same finite group coincide on a set of primes of density 1, they coincide wherever they are both defined.

Exercise 7.3. Suppose we are given a pair $(L', \sigma')$ such that $\alpha'(F_{L'/K}(\sigma)) = \varphi(\sigma)$ for all $\sigma'$ in a set of density 1. Show that $(L', \sigma')$ has
the same properties as the pair \((L, \alpha)\) constructed in Exercise 7.1; in fact,
the extension M/K finite abelian. Let \(L'\), resp. \(\theta'\),
and \(\alpha' = \alpha\). (Clearly we may suppose \(M/K\) and \(L' = L\).
show that if \(L'\) and \(L\) are contained in a common extension \(M\),
then \(L' = L\). By the quotient projection of \(G(M/K)\) onto
\(G(L'/K)\), resp. \(G(L/K)\). By
Exercise 7.2 and Chapter VII, \(\alpha \circ \theta \circ F_{M/K} = \alpha' \circ \theta' \circ F_{M/K}.
Since \(\alpha\) and \(\alpha'\) are injective, and \(F_{M/K}\) surjective, we conclude Ker \(\theta = \text{Ker } \theta'\),
and finally \(\alpha = \alpha'\).

Exercise 8: Norms from Non-abelian Extensions

Let \(E/K\) be a global extension, not necessarily Galois, and let \(M\) be
the maximal abelian subextension. Prove that \(N_{E/K} C_E = N_{M/K} C_M\),
and note
that this result simplifies a bit the proof of the existence theorem, as remarked
during the proof of the lemma in Chapter VII, \(\S\) 12. [Let \(L\) be a Galois
extension of \(K\) containing \(E\), with group \(G\), let \(H\) be the subgroup corresponding
to \(E\), and consider the following commutative diagram (cf.
Chapter VII, \(\S\) 11.3):
\[
\begin{array}{c}
\hat{A} = A(\mathbb{Z}, \mathbb{Z}) \cong H^\mathbb{Z} \cong C_E / N_{E/K} C_L \cong \hat{A}(H, C_L) \\
\text{cor} \downarrow \quad \ast \downarrow \quad \ast \downarrow \\
\hat{A} = A(\mathbb{Z}, \mathbb{Z}) \cong G^\mathbb{Z} \cong C_L / N_{L/K} C_L \cong \hat{A}(G, C_L).
\end{array}
\]

Since \(G^\mathbb{Z} / \theta(H^\mathbb{Z}) \approx G(M/K)\) this gives the result.]