Exercises†

Exercise 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 μ_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 $a_1, \ldots, a_r$ are elements of K^*, we let $S(a_1, \ldots, a_r)$ denote the set of primes in S, together with the primes v such that $|a_i|_v \neq 1$ for some i. For $a \in K^*$ and $\mathfrak{b} \in I^{S(a)}$ the symbol $\left(\frac{a}{\mathfrak{b}}\right)$ is defined by the equation

$$(\sqrt[m]{a})^{F_{L/K}(\mathfrak{b})} = \left(\frac{a}{\mathfrak{b}}\right)\sqrt[m]{a},$$

where L is the field $K(\sqrt[m]{a})$.

EXERCISE 1.1. Show $\left(\frac{a}{\mathfrak{b}}\right)$ is an mth root of 1, independent of the choice of $\sqrt[m]{a}$.

EXERCISE 1.2. Working in the field $L' = K(\sqrt[m]{a}, \sqrt[m]{a'})$ and using Chapter VII, § 3.2 with $K' = K$ and $L = K(\sqrt[m]{a})$, show

$$\left(\frac{aa'}{\mathfrak{b}}\right) = \left(\frac{a}{\mathfrak{b}}\right)\left(\frac{a'}{\mathfrak{b}}\right) \qquad \text{if } \mathfrak{b} \in I^{S(a,a')}.$$

EXERCISE 1.3. Show

$$\left(\frac{a}{\mathfrak{b}\mathfrak{b}'}\right) = \left(\frac{a}{\mathfrak{b}}\right)\left(\frac{a}{\mathfrak{b}'}\right) \qquad \text{if } \mathfrak{b} \in I^{S(a)}.$$

† 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 some of the important results and interesting applications for which unfortunately there was not enough time in the Conference itself.

Hence,

$$\left(\frac{a}{\mathfrak{b}}\right) = \prod_{v \notin S(a)} \left(\frac{a}{v}\right)^{n_v} \qquad \text{if } \mathfrak{b} = \sum n_v v.$$

EXERCISE 1.4. (*Generalized Euler criterion.*) If $v \notin S(a)$ then $m|(Nv-1)$, where $Nv = [k(v)]$, and $\left(\frac{a}{v}\right)$ is the unique mth root of 1 such that

$$\left(\frac{a}{v}\right) \equiv a^{\frac{Nv-1}{m}} \pmod{\mathfrak{p}_v}.$$

EXERCISE 1.5. (*Explanation of the name "power residue symbol".*) For $v \notin S(a)$ the following statements are equivalent:

(i) $\left(\frac{a}{v}\right) = 1$.

(ii) The congruence $x^m \equiv a \pmod{\mathfrak{p}_v}$ is solvable with $x \in \mathfrak{o}_v$.

(iii) The equation $x^m = a$ is solvable with $x \in K_v$.

(Use the fact that $k(v)^*$ is cyclic of order $(Nv-1)$, and Hensel's lemma, Chapter II, App. C.)

EXERCISE 1.6. If $\mathfrak{b}$ is an integral ideal prime to m, then

$$\left(\frac{\zeta}{\mathfrak{b}}\right) = \zeta^{\frac{N\mathfrak{b}-1}{m}} \qquad \text{for } \zeta \in \mu_m.$$

(Do this first, using Exercise 1.4, in case $\mathfrak{b} = v$ is prime. Then for general $\mathfrak{b} = \sum n_v v$, note that, putting $Nv = 1 + mr_v$, we have

$$N\mathfrak{b} = \prod (1+mr_v)^{n_v} \equiv 1 + m\sum n_v r_v \pmod{m^2}.)$$

EXERCISE 1.7. If a and $\mathfrak{b} \in I^{S(a)}$ are integral, and if $a' \equiv a \pmod{\mathfrak{b}}$, then $\left(\frac{a'}{\mathfrak{b}}\right) = \left(\frac{a}{\mathfrak{b}}\right)$.

EXERCISE 1.8. Show that Artin's reciprocity law (Chapter VII, § 3.3) for a simple Kummer extension $L = K(\sqrt[m]{a})$ implies the following statement: *If* $\mathfrak{b}$ *and* $\mathfrak{b}' \in I^{S(a)}$, *and* $\mathfrak{b}'\mathfrak{b}^{-1} = (c)$ *is the principal ideal of an element* $c \in K^*$ *such that* $c \in (K_v^*)^m$ *for all* $v \in S(a)$, *then* $\left(\frac{a}{\mathfrak{b}'}\right) = \left(\frac{a}{\mathfrak{b}}\right)$. Note that for $v \notin S$, the condition $c \in (K_v^*)^m$ will certainly be satisfied if $c \equiv 1 \pmod{\mathfrak{p}_v}$.

EXERCISE 1.9. Specialize now to the case $K = \mathbf{Q}$, $m = 2$. 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 $\mathbf{Q}(\sqrt{a})/\mathbf{Q}$ implies

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

where a_0 denotes the "odd part of a", i.e. $a = 2^v a_0$, 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

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}, \quad \left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}, \quad \text{and} \quad \left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

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

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

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 (mod 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.

Exercise 2: The Norm Residue Symbol (Hilbert, Hasse)

We assume the reciprocity law for Kummer extensions, and use Chapter VII, § 6. The symbols m, K, S, and $S(a_1, \ldots, a_r)$ have the same significance as in Exercise 1. For a and $b \in K^*$ and an arbitrary prime v of K we define $(a, b)_v$ by the equation

$$(\sqrt[m]{a})^{\psi_v(b)} = (a, b)_v \sqrt[m]{a},$$

where $\psi_v : K_v^* \to G^v$ is the local Artin map associated with the Kummer extension $K(\sqrt[m]{a})/K$.

EXERCISE 2.1. Show that $(a, b)_v$ is an mth root of 1 which is independent of the choice of $\sqrt[m]{a}$.

EXERCISE 2.2. Show $(a, b)_v(a, b')_v = (a, bb')_v$ and $(a, b)_v(a', b)_v = (aa', b)_v$. Thus, for each prime v of K, we have a bilinear map of $K^* \times K^*$ into the group μ_m of mth roots of unity.

EXERCISE 2.3. Show that $(a, b)_v = 1$ if either a or $b \in (K_v^*)^m$, and hence that there is a unique bilinear extension of $(a, b)_v$ to $K_v^* \times K_v^*$.

This extension is continuous in the v-adic topology, and can be described by a finite table of values, because $K_v^*/(K_v^*)^m$ is a finite group (of order $m^2/|m|_v$, where $|m|_v$ is the normed absolute value of m at v). Moreover, the extended function on $K_v^* \times K_v^*$ can be described purely locally, i.e. is independent of the field K of which K_v is the completion (because the same is true of ψ_v), and induces a *non-degenerate* pairing of $K_v^*/(K_v^*)^m$ with itself into μ_m; however we will not use these local class field theoretic facts in most of this exercise. For a general discussion of $(a, b)_v$, and also for some explicit formulas for it in special cases, see Hasse's "Bericht", Part II, pp. 53–123, Serre's "Corps Locaux", pp. 212–221, and the Artin–Tate notes, Ch. 12. The symbol $(a, b)_v$ defined here coincides with that of Hasse and Serre, but is the opposite of that defined in Artin–Tate. While we are on the subject, our local Artin maps ψ_v coincide with those in Serre and in Artin–Tate, but are the opposite of Hasse's.

EXERCISE 2.4. Show that $(a, b)_v = 1$ if b is a norm for the extension $K_v(\sqrt[m]{a})/K_v$. (See Chapter VII, § 6.2; the converse is true also, by local class field theory, but this does not follow directly from the global reciprocity law.)

EXERCISE 2.5. We have $(a, b)_v = 1$ if $a + b \in (K_v^*)^m$; in particular, $(a, -a)_v = 1 = (a, 1-a)_v$. (This follows from the purely algebraic lemma: *Let F be a field containing the group μ_m of mth roots of unity, and let $a \in F^*$. Then for every $x \in F$ the element $x^m - a$ is a norm from $F(\sqrt[m]{a})$.* Indeed, let $\alpha^m = a$. The map $\sigma \mapsto \alpha^\sigma/\alpha$ is an isomorphism of the Galois group onto a subgroup μ_d of μ_m and is independent of the choice of α. Hence if (ζ_l) is a

system of representatives of the cosets of μ_d in μ_m, we have for each $x \in F$

$$x^m - a = \prod_{\zeta \in \mu_m} (x - \zeta\alpha) = N_{F(\alpha)/F}\left(\prod_{i=1}^{m/d}(x - \zeta_i\alpha)\right),$$

Q.E.D.)

EXERCISE 2.6. Show that $(a, b)_v(b, a)_v = 1$. (Just use bilinearity on $1 = (ab, -ab)_v$.)

EXERCISE 2.7. If v is archimedean, we have $(a, b)_v = 1$ 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 $(a, b)_v = -1$; 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 $(a, b)_v = \left(\frac{a}{v}\right)^{v(b)}$; in particular, $(a, b)_v = 1$ 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,

$$v \notin S \Rightarrow (a, b)_v = \left(\frac{c}{v}\right), \quad \text{where } c = (-1)^{v(a)v(b)}a^{v(b)}b^{-v(a)}$$

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 $(a, b)_v$ 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 $\prod (a, b)_v = 1$, 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

$$\left(\frac{a}{b}\right) = \prod_{v \notin S(a)} \left(\frac{a}{v}\right)^{v(b)} = \left(\frac{a}{(b)^{S(a)}}\right),$$

where $(b)^s$ is defined in Chapter VII, § 3.2.

Warning: With $\left(\frac{a}{b}\right)$ defined in this generality the rule $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$ 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

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{v \in S(a) \cap S(b)} (b, a)_v.$$

In particular

(*) $$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{v \in S} (b, a)_v, \quad \text{if } S(a) \cap S(b) = S,$$

and

(**) $$\left(\frac{\lambda}{b}\right) = \prod_{v \in S} (\lambda, b)_v, \quad \text{if } S(\lambda) = S.$$

EXERCISE 2.11. If $K = \mathbf{Q}$ and $m = 2$, then $S = \{2, \infty\}$, and for $P > 0$ as in Exercise 1.10, we have $(x, P)_\infty = 1$. Hence the results of Exercise 1.10 are equivalent with

$$(-1, P)_2 = (-1)^{\frac{P-1}{2}}, \quad (2, P)_2 = (-1)^{\frac{P^2-1}{8}}, \quad \text{and} \quad (P, Q)_2 = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}},$$

for odd P and Q. On the other hand, these formulas are easily established working locally in $\mathbf{Q}_2$. In particular, the fact that $(1+4c, b)_2 = (-1)^{v_2(b)c}$, from which the value of $(a, b)_2$ is easily derived for all a, b using Exercises 2.2, 2.5 and 2.6, is a special case of the next exercise.

EXERCISE 2.12. An element $a \in K$ is called *v-primary* (for m) if $K(\sqrt[m]{a})/K$ is unramified at v. For $v \notin S$, there is no problem: an element a is v-primary if and only if $v(a) \equiv 0 \pmod m$. Suppose now v divides m and $m = p$ is a prime number. Let ζ be a generator of μ_p, and put $\lambda = 1 - \zeta$. Check that λ^{p-1}/p is a unit at v, and more precisely, that $\lambda^{p-1} \equiv -p \pmod{p\lambda}$, so that $\lambda^{p-1}/p \equiv -1 \pmod{\mathfrak{p}_v}$. Let a be such that $a \equiv 1 \pmod{p\lambda\mathfrak{o}_v}$, so that we have $a = 1 + \lambda^p c$, with $c \in \mathfrak{o}_v$. Prove that a is v-primary, and that for all b,

$$(a, b)_v = \zeta^{-S(\bar{c})v(b)},$$

where S denotes the trace from $k(v)$ to the prime field and $\bar{c}$ is the v-residue of c. Also, if $a \equiv 1 \pmod{p\lambda\mathfrak{p}_v}$, then a is *v-hyperprimary*, i.e. $a \in (K_v^*)^m$.

(Let $\alpha^p = a$, and write $\alpha = 1 + \lambda x$. Check that x is a root of a polynomial $f(X) \in \mathfrak{o}_v[X]$ such that $f(X) \equiv X^p - X - c \pmod{\mathfrak{p}_v}$. Thus $f'(x) \equiv -1 \not\equiv 0 \pmod{\mathfrak{p}_v}$, so $K_v(x) = K_v(\sqrt[m]{a})$ is indeed unramified. And if $c \equiv 0 \pmod{\mathfrak{p}_v}$ then $f(X)$ splits by Hensel's lemma, so $K_v(\sqrt[m]{a}) = K_v$. Now $x^p \equiv x + c \pmod{\mathfrak{p}_v}$, so if $Nv = p^f$, then

$$x^F = x^{Nv} \equiv x + c + c^p + \ldots + c^{p^{f-1}} \equiv x + S(\bar{c}) \pmod{\mathfrak{p}_v}.$$

On the other hand, if $\alpha' = \zeta\alpha = 1 + \lambda x'$, then $x' \equiv x - 1 \pmod{\mathfrak{p}_v}$. Combining these facts gives the formula for $(a, b)_v$.)

EXERCISE 2.13. Let p be an odd prime, ζ a primitive pth root of unity, $K = \mathbf{Q}(\zeta)$, 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 $\equiv 1 \pmod{\lambda^i}$ in K_v^*, for $i = 1, 2, \ldots$. Then the image of $\eta_i = 1 - \lambda^i$ generates U_i/U_{i+1}, which is cyclic of order p, and the image of λ generates $K_v^*/(K_v^*)^p U_1$. By the preceding exercise,

$U_{p+1} \subset (K_v^*)^p$. Hence the elements $\lambda, \zeta = \eta_1, 1-\lambda^2 = \eta_2, \ldots, 1-\lambda^p = \eta_p$ generate $(K_v^*)/(K_v^*)^p$. But that group is of order $p^2/|p|_v = p^{1+p}$, so these generators are independent mod pth powers. Show that

(a) $(\eta_i, \eta_j)_v = (\eta_i, \eta_{i+j})_v(\eta_{i+j}, \eta_j)_v(\eta_{i+j}, \lambda)_v^{-j}$, for all $i, j \geq 1$.

(b) If $i+j \geq p+1$, then $(a, b)_v = 1$ for all $a \in U_i$ and $b \in U_j$.

(c) $(\eta_i, \lambda)_v = \begin{cases} 1, & \text{for } 1 \leq i \leq p-1 \\ \zeta, & \text{for } i = p. \end{cases}$

(d) $(a, b)_v$ is the unique skew-symmetric pairing $K_v^* \times K_v^* \to \mu_p$ satisfying (a) and (c).

(For (a), note $\eta_j + \lambda^j \eta_i = \eta_{i+j}$, divide through by η_{i+j}, and use Exercise 2.5 and bilinearity; the oddness of p, which implies $(a, b) = (a, -b)$ in general and $(a, a) = 1$ in particular, is used here. The rest all follows easily, except for (c) which is a consequence of the preceding exercise; but note that the first $(p-1)$ cases of (c) are trivialities, because

$$(\eta_i, \lambda)_v^i = (1-\lambda^i, \lambda^i)_v = 1 \Rightarrow (\eta_i, \lambda)_v = 1 \quad \text{for } 1 \leq i \leq p-1.)$$

EXERCISE 2.14. (*Cubic reciprocity law.*) Specialize to $p = 3$ in the preceding exercise. The ring of integers $R = \mathbf{Z} + \mathbf{Z}\zeta$ is a principal ideal domain, whose non-zero elements can be written in the form $\lambda^\nu \zeta^\mu a$, with $a \equiv \pm 1 \pmod{3R}$. Prove

$$(*) \qquad \left(\frac{a}{b}\right) = \left(\frac{b}{a}\right), \quad \text{for relatively prime } a \text{ and } b, \text{ each} \equiv \pm 1 \pmod{3R},$$

and also

$$(**) \qquad \left\{\begin{array}{l} \left(\frac{\zeta}{a}\right) = \zeta^{-m-n} \\ \left(\frac{\lambda}{a}\right) = \zeta^m \end{array}\right\}, \quad \text{for } a = \pm(1+3(m+n\zeta)).$$

As an application, prove: If q is a rational prime $\equiv 1 \pmod 3$, then 2 is a cubic residue (mod q) if and only if q is of the form x^2+27y^2 with $x, y \in \mathbf{Z}$. (Write $q = \pi\bar{\pi}$ with $\pi \equiv \pm 1 \pmod{3R}$. Then $\mathbf{Z}/q\mathbf{Z} \xrightarrow{\sim} R/\pi R$, so 2 is a cubic residue (mod q) if and only if $\left(\frac{2}{\pi}\right) = 1$. Now use (*), and translate $\left(\frac{\pi}{2}\right) = 1$ into a statement about q.)

EXERCISE 2.15. Let L be the splitting field over $\mathbf{Q}$ of the polynomial X^3-2. The Galois group of $L/\mathbf{Q}$ is the symmetric group on three letters. Using the preceding exercise, show that for $p \neq 2, 3$ the Frobenius automorphism is given by the rules:

$F_{L/\mathbf{Q}}(p) = (1)$, if $p \equiv 1 \pmod 3$ and p of the form x^2+27y^2,
$F_{L/\mathbf{Q}}(p) =$ 3-cycle, if $p \equiv 1 \pmod 3$ and p not of the form x^2+27y^2,
$F_{L/\mathbf{Q}}(p) =$ 2-cycle, if $p \equiv -1 \pmod 3$.

Hence, by Tchebotarov'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 a finite family of elements of K^*, and let L be the Kummer extension generated by the mth roots of those elements. Let T be a finite set of primes of K containing $S(a_1, \ldots, a_r)$, and big enough so that both $J_K = K^* J_{K,T}$, and $J_L = L^* J_{L,T'}$, 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 $(x_v, a_i)_v = \zeta_{v,i}$ for all i.

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

The additional condition on T, involving T', is necessary, as is shown by the example $K = \mathbf{Q}$, $m = 2$, $T = \{\infty, 2, 7\}$, $r = 1$, $a_1 = -14$, $\zeta_{\infty,1} = -1$, $\zeta_{2,1} = -1$, $\zeta_{7,1} = 1$. 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_T, and the smaller subgroup A_0 generated by the images of the elements a_i, $1 \leq i \leq r$. The form $\langle x, y \rangle = \prod_{v \in T}(x_v, y_v)_v$ gives a non-degenerate pairing of X with itself to μ_m, under which A is self orthogonal, and indeed exactly so, because $[X] = m^{2t}$ and $[A] = m^t$, where $t = [T]$. (See step 4 in the proof of the second inequality in Chapter VII, § 9, the notations S, n, and s there being replaced by T, m, and t here.) Thus $X/A \approx \mathrm{Hom}(A, \mu_m)$ (note by the way that both groups are isomorphic to $\mathrm{Gal}(K(\sqrt[m]{K_T})/K)$, by class field theory and Kummer theory, respectively), and, vice versa, $A \approx \mathrm{Hom}(X/A, \mu_m)$. 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 $\pi_v(a) \in \pi_v(A_0)$ for all v, where π_v 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 completely at all archimedean ones is the class field to the group $K^* J_{K,S}$, where S now denotes the set of archimedean primes. (Use the Main Theorem

(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 class group $H_K = I_K/P_K$ of K onto the Galois group $G(K'/K)$. (Use the Main Theorem and the isomorphism $J_K/J_{K,S} \xrightarrow{\sim} I_K$.) Thus the degree $[K' : K]$ is equal to the class number $h_K = [H_K]$ of K. The prime ideals in K decompose in K' according to their ideal class, and, in particular, the ones which split completely are exactly the principal prime ideals. An arbitrary ideal $\mathfrak{a}$ of K is principal if and only if $F_{K'/K}(\mathfrak{a}) = 1$.

The "class field tower", $K \subset K' \subset K'' = (K')' \subset \ldots$ can be infinite (see Chapter IX). Using the first two steps of it, and the commutative diagram (see (11.3), diagram (13))

$$\begin{array}{ccc} I_K & \xrightarrow{F_{K'/K}} & G(K'/K) \\ {\scriptstyle \mathrm{con}}\downarrow & & \downarrow{\scriptstyle V} \\ I_{K'} & \xrightarrow{F_{K''/K'}} & G(K''/K'), \end{array}$$

Artin realized that Hilbert's conjecture, to the effect that every ideal in K becomes principal in K', was equivalent to the statement that the Verlagerung† V was the zero map in this situation. Now $G(K''/K')$ is the commutator subgroup of $G(K''/K)$ (Why?), and so Artin conjectured the "Principal ideal theorem" of group theory: *If G is a finite group and G^c its commutator subgroup, then the map $V\colon (G/G^c) \to G^c/(G^c)^c$ is the zero map.* This theorem, and therewith Hilbert's conjecture, was then proved by Furtwängler. For a simple proof, see Witt, *Proc. Intern. Conf. Math., Amsterdam*, 1954, Vol. 2, pp. 71–73.

The first five imaginary quadratic fields with class number $\neq 1$ are those with discriminants -15, -20, -23, -24, and -31, which have class numbers 2, 2, 3, 2, 3, respectively. Show that their Hilbert class fields are obtained by adjoining the roots of the equations X^2+3, X^2+1, X^3-X-1, X^2+3, and X^3+X-1, respectively. In general, if K is an imaginary quadratic field, its Hilbert class field K' is generated over K by the j-invariants of the elliptic curves which have the ring of integers of K as ring of endomorphisms; see Chapter XIII.

Let J_S^+ denote the group of idèles which are positive at the real primes of K and are units at the non-archimedean primes. The class field over K with norm group $K^*J_{K,S}^+$ is the maximal abelian extension which is unramified at all non-archimedean primes, but with no condition at the archimedean primes; let us denote it by K_1. Let P_K^+ denote the group of principal ideals of the form (a), where a is a totally positive element of K. Show that $F_{K_1/K}$ gives an isomorphism: $I_K/P_K^+ \approx G(K_1/K)$. Thus, $G(K_1/K')$ is an elementary

† Called the *transfer* in Chapter IV, § 6, *Note* after Prop. 7.

abelian 2-group, isomorphic to P_K/P_K^+. Show that $(P_K : P_K^+)(K_S : K_S^+) = 2^{r_1}$, where $K_S^+ = K^* \cap J_{K,S}^+$ is the group of totally positive units in K, and r_1 is the number of real primes of K.

We have $\mathbf{Q}_1 = \mathbf{Q}$, clearly, but this is a poor result in view of Minkowski's theorem, to the effect that $\mathbf{Q}$ has no non-trivial extension, *abelian or not*, which is unramified at all non-archimedean primes (Minkowski, "Geometrie der Zahlen", p. 130, or "Diophantische Approximationen" p. 127). Consider now the case in which K is real quadratic, $[K\colon \mathbf{Q}] = 2$, and $r_1 = 2$. Show that $[K_1 : K'] = 1$ or 2, according to whether $N\varepsilon = -1$ or $N\varepsilon = 1$, where ε is a fundamental unit in K, and $N = N_{K/\mathbf{Q}}$. For example, in case $K = \mathbf{Q}(\sqrt{2})$ or $\mathbf{Q}(\sqrt{5})$ we have $K' = K$, because the class number is 1, and consequently also $K_1 = K$, because the units $\varepsilon = 1+\sqrt{2}$ and $\varepsilon = \frac{1}{2}(1+\sqrt{5})$ have norm -1. On the other hand, if $K = \mathbf{Q}(\sqrt{3})$, then again $K' = K$, but $K_1 \neq K$, because $\varepsilon = 2+\sqrt{3}$ has norm 1; show that $K_1 = K(\sqrt{-1})$. In general, when -1 is not a local norm everywhere (as in the case $K = \mathbf{Q}(\sqrt{3})$ just considered), then $N\varepsilon = 1$, and $K_1 \neq K'$. However, when -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

$$f(X) = \sum a_{ij}X_iX_j$$

a non-degenerate quadratic form in n variables with coefficients in K. We say that *f represents an element c in K* if the equation $f(X) = c$ 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

$$(tX+Y) = t^2f(X)+tB(X,Y)+f(Y).$$

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: $f = \sum a_iX_i^2$ with all $a_i \neq 0$. If $f = cX_1^2 - g(X_2, \ldots, X_n)$ 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 $f = X^2 - bY^2$ 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 $f = X^2 - bY^2 - cZ^2 + acT^2$ represents 0 in K.

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

(iii) c, as element of $K(\sqrt{ab})$, is a norm from the field $L = K(\sqrt{a}, \sqrt{b})$.

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

(We may obviously assume neither a nor b is a square in K. Then the equivalence of (i) and (ii) is clear because the reciprocal of a norm is a norm, and the equivalence of (iii) and (iv) follows from Exercise 4.3 with K replaced therein by $K(\sqrt{ab})$. It remains to prove (ii) $\Leftrightarrow$ (iii), and we can assume $ab \notin (K^*)^2$, for otherwise the equivalence is obvious. Then Gal (L/K) is a four-group, consisting of elements $1, \rho, \sigma, \tau$ such that ρ, σ, and τ leave fixed, respectively, $\sqrt{ab}$, $\sqrt{a}$, and $\sqrt{b}$, say. Now (ii) $\Leftrightarrow$ (ii'): $\exists\, x, y \in L$ such that $x^\sigma = x$, $y^\tau = y$, and $x^{1+\rho} y^{1+\rho} = c$; and (iii) $\Leftrightarrow$ (iii') $\exists\, z \in L$ such that $z^{1+\rho} = c$. Hence (ii) $\Rightarrow$ (iii) trivially. Therefore assume (iii'), put $u = c^{-1} z^{\sigma+1}$, and check that $u^\sigma = u$, i.e. $u \in K(\sqrt{a})$, and $u^{\rho+1} = 1$. Hence by Hilbert's theorem 90 (Chapter V, § 2.7) for the extension $K(\sqrt{a})/K$, there exists $x \neq 0$ such that $x^\sigma = x$ and $x^{\rho-1} = u$. Now put $y = z^\rho / x$, and check that (ii') is satisfied.)

So far, we have done algebra, not arithmetic. From now on, we suppose K is a *global field* of characteristic $\neq 2$.

EXERCISE 4.5. The form f of Exercise 4.3 represents 0 in a local field K_v if and only if the quadratic norm residue symbol $(b, c)_v = 1$. Hence f represents 0 in K_v for all but a finite number of v, and the number of v's for which it does not is even. 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_v, then $a \notin (K_v^*)^2$, and $b \notin (K_v^*)^2$, but $ab \in (K_v^*)^2$, and c is *not* a norm from the quadratic extension $K_v(\sqrt{a}) = K_v(\sqrt{b})$. (Just use the fact that the norm groups from the different quadratic extensions of K_v are subgroups of index 2 in K_v^*, no two of which coincide.) Now suppose conversely that those conditions are satisfied. Show that the set of elements in K_v which are represented by f is $N - cN$, where N is the group of non-zero norms from $K_v(\sqrt{a})$, and in particular, that f does not represent 0 in K_v. Show, furthermore, that if $N - cN \neq K_v^*$, then $-1 \notin N$, and $N + N \subset N$. Hence f represents every non-zero element of K_v *unless* $K_v \approx \mathbf{R}$ and f is positive definite.

EXERCISE 4.7. A form f in $n \geq 5$ variables over a local field K_v represents 0 unless K_v is real and f definite.

EXERCISE 4.8. *Theorem: Let K be a global field and f a non-degenerate quadratic form in n variables over K which represents 0 in K_v for each prime v of K. Then f represents 0 in K.* (For $n = 1$, trivial; $n = 2$, cf. Chapter VII, § 8.8; $n = 3$, cf. Chapter VII, § 9.6 and Exercise 4.3; $n = 4$, use Exercise 4.4 to reduce to the case $n = 3$; finally, for $n \geq 5$, proceed by induction: Let

$$f(X) = aX_1^2 + bX_2^2 - g(X_3, \ldots, X_n),$$

where g has $n - 2 \geq 3$ variables. From Exercise 4.5 we know that g represents 0 and hence every number in K_v for all v outside a finite set S. Now $(K_v^*)^2$ is open in K_v^*. Hence, by the approximation theorem there exist elements x_1 and x_2 in K, such that the element $c = ax_1^2 + bx_2^2 \neq 0$ is represented by g in K_v for all v in S, and hence for all v. By induction, the form $cY^2 - g(X_3, \ldots, X_n)$ in $n-1$ variables represents 0 in K. Hence f does.)

EXERCISE 4.9. *Corollary:* If $n \geq 5$, then f represents 0 in K unless there is a real prime v at which f is definite.

EXERCISE 4.10. A rational number c is the sum of three rational squares if and only if $c = 4^n r$ where r is a rational number > 0 and $\not\equiv 7 \pmod 8$; every rational number is the sum of four rational squares.

EXERCISE 4.11. The statements in the preceding exercise are true if we replace "rational" by "rational integral" throughout. (The 4 squares one is an immediate consequence of the 3 squares one, so we will discuss only the latter, although there are more elementary proofs of the four square statement not involving the "deeper" three square one. Let c be a positive integer as in 4.10, so that the sphere $|X|^2 = X_1^2 + X_2^2 + X_3^2 = c$ has a point $x = (x_1, x_2, x_3)$ with rational coordinates. We must show it has a point with *integral* coordinates. Assuming x itself not integral, let z be an integral point in 3-space which is as close as possible to x, so that $x = z + a$, with $0 < |a|^2 \leq 3/4 < 1$. The line l joining x to z is not tangent to the sphere; if it were then we would have $|a|^2 = |z|^2 - |x|^2 = |z|^2 - c$, an integer, contradiction. Hence the line l meets the sphere in a rational point $x' \neq x$. Now show that if the coordinate of x can be written with the common denominator $d > 0$, then those of x' can be written with the common denominator $d' = |a|^2 d < d$, so that the sequence $x, x', (x')', \ldots$ must lead eventually to an integral point. Note that d' is in fact an integer, because

$$d' = |a|^2 d = |x - z|^2 d = (|x|^2 - 2(x, z) + |z|^2) d = cd - 2(dx, z) + |z|^2 d.)$$

EXERCISE 4.12. Let f be a form in three variables over K. Show that if f does not represent 0 locally in K_v, then the other numbers in K_v not represented by f constitute one coset of $(K_v^*)^2$ in K_v^*. (Clearly one can assume $f = X^2 - bY^2 - cZ^2$; now use Exercise 4.6.) Using this, show that if $K = \mathbf{Q}$ and f is positive definite, then f does not represent all positive integers. (Note the last sentence in Exercise 4.5.)

For further developments and related work see O. T. O'Meara: "Introduction to Quadratic Forms" (Springer, 1963) or Z. I. Borevič and I. R. Šafarevič, "Teorija Čisel" ("Nauka", Moskva, 1964). [English translation, Z. I. Borevich and I. R. Shafarevich, "Number Theory", Academic Press, New York: German translation, S. I. Borevicz and I. R. Šafarevič, "Zahlentheorie", Birkhäuser Verlag, Basel.]

Exercise 5: Local Norms Not Global Norms, etc.

Let L/K be Galois with group $G = (1, \rho, \sigma, \tau) \approx (\mathbf{Z}/2\mathbf{Z})^2$, and let K_1, K_2, and K_3 be the three quadratic intermediate fields left fixed by ρ, σ, and τ, respectively. Let $N_i = N_{K_i/K}(K_i^*)$ for $i = 1, 2, 3$, and let $N = N_{L/K}(L^*)$.

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, and 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 (infinite) set of primes of K which split in K_i, and for $x \in K^*$ put

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

where $(x, y)_v$ is the quadratic norm residue symbol. Show that $N_1N_2N_3 = \operatorname{Ker} \varphi$ and is a subgroup of index 2 in K^*. (The inclusion $N_1N_2N_3 \subset \operatorname{Ker} \varphi$ 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 $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt{13}, \sqrt{17})$. Show that if x is a product of primes p such that $\left(\frac{p}{13}\right) = -1$ (e.g. $p = 2, 5, 7, 11, \ldots$), then $\varphi(x) = \left(\frac{x}{17}\right)$. Hence $5^2, 7^2, 10^2, 11^2, 14^2, \ldots$ are some examples of numbers which are local norms everywhere from $\mathbf{Q}(\sqrt{13}, \sqrt{17})$ but are not global norms. Of course, not every such number is a square; for example, -14^2 is the global norm of $\frac{1}{2}(7+2\sqrt{13}+\sqrt{17})$, 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 $\hat{H}^{-1}(G, L^*) = 0$, but

$\hat{H}^{-1}(G, L_w^*) \approx \mathbf{Z}/2\mathbf{Z}$. (Use the exact sequence near the beginning of paragraph 11.4. The map g is surjective, as always when the l.c.m. of the local degrees is the global degree. And the map $g: \hat{H}^{-1}(G, J_L) \to \hat{H}(G, C_L)$ is also injective, because of our assumption that the local degree is 4 for only one prime.)

Let A, resp. A_w, be the group of elements in L^*, resp L_w^*, whose norm to K (resp. to K_v) is 1, and let $\bar{A}$ be the closure of A in L_w^*. It follows from the above that

$$A = (L^*)^{\rho-1}(L^*)^{\sigma-1}(L^*)^{\tau-1},$$

and that

$$\bar{A} = (L_w^*)^{\rho-1}(L_w^*)^{\sigma-1}(L_w^*)^{\tau-1}$$

is of index 2 in A_w. Now, as is well known, there is an algebraic group T defined over K (the twisted torus of dimension 3 defined by the equation $N_{L/K}(X) = 1$) such that $T(K) = A$ and $T(K_v) = A_w$. Hence we get examples 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, it is not hard to show that if T is a torus over K split by a Galois extension L/K, then $T(K)$ is dense in $T(K_v)$ 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 $K = \mathbf{Q}$ and $L = \mathbf{Q}(\sqrt{-1}, \sqrt{2}) = \mathbf{Q}(\zeta)$, where $\zeta^4 = -1$. 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 $M = \mathbf{Q}(i)$ where $i = \zeta^2 = \sqrt{-1}$, and let L_w and M_v 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_w^*: just check that the element $z = (2+i)/(2-i) \in M_v$ is a norm from L_w to L_v, but that $z(M_v^*)^2$ contains no element $y \in M$ such that y is a global norm from L to M *and* such that $N_{M/\mathbf{Q}}(y) = 1$.

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 $\mathrm{Spl}_S(L/K)$ the set of primes $v \notin S$ such that v splits completely in L (i.e. such that $L \otimes_K K_v \approx K^{[L:K]}$), and by $\mathrm{Spl}'_S(L/K)$ the set of primes $v \notin S$ which have a split factor in L (i.e. such that there exists a K-isomorphism $L \to K_v$). Thus $\mathrm{Spl}_S(L/K) \subset \mathrm{Spl}'_S(L/K)$ always, and equality holds if K is Galois, in which case $\mathrm{Spl}'_S(L/K)$ has density $[L:K]^{-1}$ by the Tchebotarov density theorem. (Enunciated near end of Chapter VIII, § 3.)

EXERCISE 6.1. Show that if L and M are Galois over K, then

$$L \subset M \Leftrightarrow \mathrm{Spl}_S(M) \subset \mathrm{Spl}_S(L),$$

(Indeed, we have

$$\mathrm{Spl}_S(LM/K) = \mathrm{Spl}_S(L/K) \cap \mathrm{Spl}_S(M/K),$$

so

$$L \subset M \Rightarrow \mathrm{Spl}_S(M) \subset \mathrm{Spl}_S(L) \Rightarrow \mathrm{Spl}_S(LM/K) = \mathrm{Spl}_S(M/K)$$
$$\Rightarrow [LM:K] = [M:K] \Rightarrow L \subset M;$$

where was Galoisness used?) Hence

$$L = M \Leftrightarrow \mathrm{Spl}_S(L) = \mathrm{Spl}_S(M).$$

Application: *If a separable polynomial $f(X) \in K[X]$ splits into linear factors* mod $\mathfrak{p}$ *for all but a finite number of prime ideals* $\mathfrak{p}$ *of K, then f splits into linear factors in K.* (Take L = 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 $v \notin S$" and "all but a finite number of primes v" by "all v in a set of density 1".

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 v of K, let G^v denote a decomposition group of v. Show that v splits completely in E if and only if all of the conjugates of G^v are contained in H, whereas v has a split factor in E if and only if at least one conjugate of G^v is contained in H. Hence, show that the set of primes $\mathrm{Spl}'_S(E/K)$ has density $[\bigcup_{\rho \in G} \rho H \rho^{-1}]/[G]$. 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 $\mathrm{Spl}'_S(E/K)$ has density 1, then $E = K$. Application: *If an* irreducible *polynomial $f(X) \in K[X]$ has a root* (mod $\mathfrak{p}$) *for all but a finite number of primes* $\mathfrak{p}$, *or even for a set of primes* $\mathfrak{p}$ *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 $\mathrm{Spl}'(E/K)$ 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_i) and put

$$H = \{1,\ (X_1X_2)(X_3X_4),\ (X_1X_3)(X_2X_4),\ (X_1X_4)(X_2X_3)\}$$
$$H' = \{1,\ (X_1X_2)(X_3X_4),\ (X_1X_2)(X_5X_6),\ (X_3X_4)(X_5X_6)\}$$

(H leaves X_5 and X_6 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 $\mathbf{Q}$ with the symmetric group on 6 letters as Galois group.

EXERCISE 6.4. Let L be a finite Galois extension of $\mathbf{Q}$, let $G = G(L/\mathbf{Q})$, 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 $A/pA \approx A'/pA'$, 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 ∞.)

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 $\mathbf{Q}$ with the same decomposition laws and same zeta functions. However, such examples do not exist if one of the fields is Galois over $\mathbf{Q}$.

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 $\varphi: I^S \to H$ a homomorphism which is *admissible* in the sense of paragraph 3.7 of the Notes. We will consider "pairs" (L, α) consisting of a finite abelian extension L of K and an *injective* homomorphism $\alpha: G(L/K) \to H$.

EXERCISE 7.1. Show that there exists a pair (L, α) such that L/K is unramified outside S and $\varphi(\mathfrak{a}) = \alpha(F_{L/K}(\mathfrak{a}))$ for all $\mathfrak{a} \in I^S$, 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 $\varphi(v) = 1$ for all primes v in a set of density 1 (e.g. for all but a finite number of the primes of degree 1 over $\mathbf{Q}$), then φ is identically 1. (Use the Tschebotarov 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', α') such that $\alpha'(F_{L'/K}(v)) = \varphi(v)$ for all v in a set of density 1. Show that (L', α') has

the same properties as the pair (L, α) constructed in Exercise 7.1; in fact, show that if L' and L are contained in a common extension M, then $L' = L$ and $\alpha' = \alpha$. (Clearly we may suppose M/K finite abelian. Let θ, resp. θ', be the canonical projection of $G(M/K)$ onto $G(L/K)$, resp. $G(L'/K)$. By Exercise 7.2 and Chapter VII, § 3.2 we have $\alpha \circ \theta \circ F_{M/K} = \alpha' \circ \theta' \circ F_{M/K}$. Since α and α' are injective, and $F_{M/K}$ surjective, we conclude $\operatorname{Ker}\theta = \operatorname{Ker}\theta'$, hence $L = L'$, 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, § 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, § 11.3):

$$\begin{array}{ccccc} \hat{H}^{-2}(H,\mathbf{Z}) \approx H^{ab} & \xrightarrow{\sim} & C_E/N_{L/E}C_L & \approx & \hat{H}^0(H,C_L) \\ \text{cor}\downarrow & \theta\downarrow & \downarrow N_{E/K} & & \downarrow \text{cor} \\ \hat{H}^{-2}(G,\mathbf{Z}) \approx G^{ab} & \xrightarrow{\sim} & C_K/N_{L/K}C_L & \approx & \hat{H}^0(G,C_L). \end{array}$$

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

Author Index

Numbers in *italics* indicate the pages on which the references are listed.