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

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

(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

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

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 (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_i) 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

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

and

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

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 λ, $\zeta = \eta_1, 1-\lambda^2 = \eta_2, \ldots, 1-\lambda^p = \eta_p$ 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 $i, j \geqslant 1$.
(b) If $i+j \geq p+1$, then $(a, b)_v = 1$ for all $a \in U_i$ and $b \in U_j$.
(c) $(\eta_i, \lambda)_v = \begin{cases} 1, & \text{for } 1 \leqslant i \leqslant p-1 \\ \zeta, & \text{for } i = p. \end{cases}$
(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

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

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 $\prod\limits_{v \in T} \zeta_{v,i} = 1$, 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 $X/A \approx \operatorname{Hom}(A, \mu_m)$ (note by the way that both groups are isomorphic to $\operatorname{Gal}(K(\sqrt[m]{K_T})/K)$, by class field theory and Kummer theory, respectively), and, vice versa, $A \approx \operatorname{Hom}(X/A, \mu_m)$. 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 $J_K/J_{K,S} \xrightarrow{\approx} I_K$.) 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))

$$\begin{tikzcd}
I_K \arrow[r, "F_{K'/K}"] \arrow[d, "\mathrm{con}"'] & G(K'/K) \arrow[d, "V"] \\
I_{K'} \arrow[r, "F_{K''/K'}"] & G(K''/K'),
\end{tikzcd}$$

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 $V: (G/G^c) \to G^c/(G^c)^c$ 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 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 $Q_1 = Q$, clearly, but this is a poor result in view of Minkowski's theorem, to the effect that Q has no non-trivial extension, *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, $[K:Q] = 2$, 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 $N = N_{K/Q}$. For example, in case $K = Q(\sqrt{2})$ or $Q(\sqrt{5})$ 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 $K = Q(\sqrt{3})$, 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 $K = Q(\sqrt{3})$ 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 $b \in (K^*)^2$.

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

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 $\mathrm{Gal}(L/K)$ 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 $N_1 N_2 N_3 = \{x \in K^* | x^2 \in N\}$. (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 $N_1 N_2 N_3 = K^*$ (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 $N_1 N_2 N_3 = \operatorname{Ker} \varphi$ and is a subgroup of index 2 in K^*. (The inclusion $N_1 N_2 N_3 \subset \operatorname{Ker} \varphi$ is trivial. From Exercise 5.1 above and Chapter VII, § 11.4 one sees that the index of $N_1 N_2 N_3$ 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 $\operatorname{Spl}_S(L/K)$ the set of primes $v \notin S$ such that v splits completely in L (i.e. such that $L \underset{K}{\otimes} K_v \approx K^{[L:K]}$), and by $\operatorname{Spl}'_S(L/K)$ 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 $\operatorname{Spl}_S(L/K) \subset \operatorname{Spl}'_S(L/K)$ always, and equality holds if K is Galois, in which case $\operatorname{Spl}'_S(L/K)$ 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 $\mathrm{Ker}\,\theta = \mathrm{Ker}\,\theta'$, 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):

$$\begin{tikzcd}
\hat{H}^{-2}(H,\mathbb{Z}) \arrow[r, phantom, "\approx"] \arrow[d, "\mathrm{cor}"'] & H^{ab} \arrow[r, "\sim"] \arrow[d, "\theta"'] & C_E/N_{L/E}C_L \arrow[r, phantom, "\approx"] \arrow[d, "N_{E/K}"] & \hat{H}^{0}(H,C_L) \arrow[d, "\mathrm{cor}"] \\
\hat{H}^{-2}(G,\mathbb{Z}) \arrow[r, phantom, "\approx"] & G^{ab} \arrow[r, "\sim"] & C_K/N_{L/K}C_L \arrow[r, phantom, "\approx"] & \hat{H}^{0}(G,C_L).
\end{tikzcd}$$

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

1.1. $F_{L/K}(b)$ has to permute $\sqrt[m]{a}$ to another root of $x^m - a$, so $F_{L/K}(b) = \mu$ for some m^{th} root of 1. Since $\mu_m \subset K$, μ is independent of the choice of a.

1.2. First check $S(a,a')$ contains all the ramified primes. If $\mathfrak{p} \notin S(a,a')$, then $\mathfrak{p} \nmid m$ and $a, a' \in \mathcal{O}_{\mathfrak{p}}^{\times}$. Thus $\mathfrak{p} \nmid a, a'$ as $(a) = (a') = \mathcal{O}_{\mathfrak{p}}$. By Kummer theory $\mathfrak{p}$ is unramified in $K(\sqrt[m]{a})$ and $K(\sqrt[m]{a'})$. Hence $\mathfrak{p}$ is unramified in $K(\sqrt[m]{a}, \sqrt[m]{a'}) = L'$.

Next, by VII.3.2,

$$\begin{tikzcd}
I^{S(a,a')} \arrow[r, "F_{L'/K}"] \arrow[d, "\|"'] & Gal(L'/K) \arrow[d] \\
I^{S(a,a')} \arrow[r, "F_{L/K}"] & Gal(L/K)
\end{tikzcd},
\qquad L = K(\sqrt[m]{a}) \text{ or } K(\sqrt[m]{a'}).$$

Thus, if $b \in S(a,a')$,

$$\begin{aligned}
\left(\frac{aa'}{b}\right) \sqrt[m]{a}\sqrt[m]{a'} &= F_{L'/K}(b)\left(\sqrt[m]{a}\sqrt[m]{a'}\right) \\
&= F_{L'/K}(b)(\sqrt[m]{a}) \cdot F_{L'/K}(b)(\sqrt[m]{a'}) \\
&= F_{L_1/K}(b)(\sqrt[m]{a}) \cdot F_{L_2/K}(b)(\sqrt[m]{a'}) \qquad L_1 = K(\sqrt[m]{a}) \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\; L_2 = K(\sqrt[m]{a'}) \\
&= \left(\frac{a}{b}\right)\sqrt[m]{a} \cdot \left(\frac{a'}{b}\right)\sqrt[m]{a'}.
\end{aligned}$$

1.3. By definition

$$\begin{aligned}\left(\frac{a}{bb'}\right)\sqrt[m]{a} &= F_{L/k}(bb')(\sqrt[m]{a}) \\ &= F_{L/k}(b)\left(F_{L/k}(b')(\sqrt[m]{a})\right) \\ &= \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)\sqrt[m]{a}.\end{aligned}$$

1.4. If $v \notin S(a)$ then $v \nmid m$. Thus $x^m - 1$ is separable in k_v, the residue field of v, and $\mu_m \subset \mathcal{O}_v \twoheadrightarrow k_v$ gives an injection $\mu_m \hookrightarrow k_v^\times$ (otherwise if not x^m-1 has repeated roots over k_v). Thus $m \mid \# k_v^\times = N(v) - 1$.

Now by definition $F_{L/k}(v)(x) \equiv x^{N(v)} \pmod{v}$ for all $x \in \mathcal{O}_v$. Thus

$$\left(\frac{a}{v}\right)\sqrt[m]{a} \equiv \sqrt[m]{a}^{\,N(v)} \Rightarrow \left(\frac{a}{v}\right) \equiv \sqrt[m]{a}^{\,N(v)-1} \equiv a^{\frac{N(v)-1}{m}} \pmod{v}.$$

1.5. ((i)⇒(ii)) If $\left(\frac{a}{v}\right) = 1$ then $a^{\frac{N(v)-1}{m}} = 1$. Let $\alpha \in \overline{k_v}$ be a solution of $x^m - a$. Then $\alpha^{N(v)-1} = (\alpha^m)^{\frac{N(v)-1}{m}} = a^{\frac{N(v)-1}{m}} = 1$, so in fact $\alpha \in k_v$.

Thus $x^m \equiv a \pmod{\mathfrak{p}_v}$ is solvable in k_v.

((ii) ⇒ (i)) In this case $\left(\frac{a}{v}\right) \equiv a^{\frac{N(v)-1}{m}} \equiv x^{N(v)-1} \equiv 1 \pmod{\mathfrak{p}_v}$, so $\left(\frac{a}{v}\right) = 1$ as μ_m injects into $k_v^\times$.

((iii) ⇒ (ii)) By definition $|a|_v = 1$, so $v(a) = 0$. Hence $v(x) = 0$ as well, and $x^m \equiv a \pmod{\mathfrak{p}_v}$ by restriction ((ii) ⇒ (iii)) Since $f(x)=x^m-a$ satisfies $f'(x)=mx^{m-1}\notin \mathfrak{p}_v$ and

$$|f(x)|_v<1 \ , \quad |f'(x)|_v=1 \ ,$$

by Hensel's Lemma one have a solution for $f(x)$ in K_v.

1.6. First suppose $b=\mathfrak{p}$ is prime. Then, by the proof of 1.4

$$\left(\frac{\zeta}{\mathfrak{p}}\right) \equiv \zeta^{\frac{Nv-1}{m}} \pmod{\mathfrak{p}}, \quad \zeta\in\mu_m .$$

But this implies equality as $\mu_m \hookrightarrow k_v^\times$. Now, if $b=\prod \mathfrak{p}^{n_p}$ is prime to m, then by the Chinese Remainder Theorem

$$\left(\frac{\zeta}{b}\right) = \prod \zeta^{\frac{N(v)-1}{m}\cdot n_p} = \zeta^{\frac{N(b)-1}{m}} .$$

1.7. We need to show $\left(\frac{c}{b}\right)=1$ if $c\equiv 1 \pmod{b}$. Writing $b=\prod \mathfrak{p}^{n_p}$, by the Chinese Remainder Theorem it suffices to show

$$\left(\frac{c}{\mathfrak{p}}\right)=1 \quad \text{if} \quad c\equiv 1 \pmod{\mathfrak{p}}, \quad \mathfrak{p}\nmid m .$$

But this is clear as $\left(\frac{c}{\mathfrak{p}}\right)\equiv c^{\frac{Nv-1}{m}} \equiv 1 \pmod{\mathfrak{p}}$, so $\left(\frac{c}{\mathfrak{p}}\right)=1$.

1.8. We need to show that if $c\in K^\times$ such that $c\in (K_v^*)^m$ for all $v\in S(a)$, then

$$\left(\frac{a}{(c)^{S(a)}}\right)=1 \ , \quad (c)^{S(a)}=\sum_{v\notin S(a)} v(c)\cdot v$$

By weak approximation there exists $\alpha\in K^\times$ such that $|\alpha^{-m}c-1|_v<\varepsilon$ for all $v\in S(a)$. Therefore by VII.3.3, $F_{L/K}((\alpha^{-m}c)^{S(a)})=1$. Now

$$F_{L/K}((c)^{S(a)}) = F_{L/K}((\alpha)^{S(a)})^m \, F_{L/K}((\alpha^{-m}c)^{S(a)}) = F_{L/K}((\alpha)^{S(a)})^m = 1 .$$

Hence $\left(\frac{a}{(c)^{S(a)}}\right)=1$, as desired.

1.9. Recall that numbers $\equiv 1 \pmod{8}$ are squares in $\mathbb{Z}_2^\times$. This is because $x^2+x-2b=0$ has a simple root in $\mathbb{Z}/2$, and the equation is equivalent to $(1+2x)^2 = 8b+1$.

Now, note that $PQ^{-1} \equiv 1 \pmod{8a_0}$, and

↳ if $p \in S \setminus \{2\}$ (so $v_p(a) = v_p(a_0) > 0$) then $PQ^{-1} \in (\mathbb{Q}_p^\times)^2$,

↳ if $p = 2$ then $PQ^{-1} \in (\mathbb{Q}_2^\times)^2$.

Hence the conditions of 1.8 are satisfied, and $(\frac{a}{p}) = (\frac{a}{Q})$ if $P \equiv Q \pmod{8a_0}$.

1.10. If $a = -1$ or 2 then quadratic reciprocity amounts to checking a finite number of cases ($P = 3, 5, 7, 17$). For the important case, write

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

The exercise explains why $\langle P, Q \rangle$ depends only on $P, Q \pmod{8}$, so again it suffices to check it on primes $3, 5, 7, 17$.

2.1. Same argument as 1.1.

2.2. $(a,b)_v (a,b')_v = (a,bb')_v$ is because ψ_v is a group homomorphism and $\mathrm{im}(\psi_v)$ fixes the m^{th} roots of 1.

To show $(a,b)_v (a',b)_v = (aa',b)_v$ we use VII.4.3:

$$\begin{tikzcd}
K_v \arrow[r, hook, "i_v"] \arrow[d, "\shortparallel"'] & J_v \arrow[r, "\psi_{L'/K}"] \arrow[d, "\shortparallel"'] & \mathrm{Gal}(L'^v/K_v) \arrow[d, "\vartheta"'] \\
K_v \arrow[r, hook, "i_v"] & J_v \arrow[r, "\psi_{L/K}"] & \mathrm{Gal}(L^v/K_v)
\end{tikzcd}$$

, $L' = K(\sqrt[m]{a}, \sqrt[m]{a'})$

$L = K(\sqrt[m]{a})$ or $K(\sqrt[m]{a'})$.

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

$= \psi_v(b)(\sqrt[m]{a}) \cdot \psi_v(b)(\sqrt[m]{a'}) = (a,b)_v \sqrt[m]{a} \; (a',b)_v \sqrt[m]{a'}$.

2.3. If $a = c^m$ for some $c \in K_v^\times$, then $\psi_v(a) = \psi_v(c)^m = 1$, so $(a,b)_v = 1$.

Similarly if $b \in (K_v^\times)^m$.

The unique extension to $K_v^\times \times K_v^\times$ has to factor through $(K_v^\times)^m \times (K_v^\times)^m$.

Since $K^\times \hookrightarrow K_v^\times$ is dense, one can choose representatives $x_\lambda \in K^\times/(K_v^\times)^m$ with $x_\lambda \in K^\times$ ($(K_v^\times)^m$ is open in $K^\times$). Thus the extension is defined by

$$(x_\lambda (K_v^\times)^m, x_{\lambda'} (K_v^\times)^m)_v = (x_\lambda, x_{\lambda'})_v .$$

2.4. If $b \in N_{K_v(\sqrt[m]{a})/K_v}(K_v(\sqrt[m]{a})^\times)$, then $\psi_v(b) = 1$ by III.6.2, and so $(a,b)_v = 1$.

If $(a,b)_v = 1$ then $\psi_v(b)(\sqrt[m]{a}) = \sqrt[m]{a}$, and so $\psi_v(b) = 1 \in \mathrm{Gal}(K_v(\sqrt[m]{a})/K_v)$.

Therefore $b \in \ker(\psi_v : K_v^\times \longrightarrow \mathrm{Gal}(L/K))$

$= N_{K_v(\sqrt[m]{a})/K_v}(K_v(\sqrt[m]{a})^\times)$ by local class field theory.

2.5. The lemma in the exercise tells us that if $a+b = x^n$ for some $x \in (K_v^\times)^m$, then $b = x^m - a$ is a norm from $K_v(\sqrt[m]{a})$, and so

$$(a,b)_v = 1.$$

2.6. A computation tells us that

$$1 = (ab, -ab)_v = (a,-a)_v (a,b)_v (b,a)_v (b,-b)_v$$
$$= (a,b)_v (b,a)_v .$$

2.7. If $K_v = \mathbb{C}$, or if $K_v = \mathbb{R}$ and m is odd, then $(K^\times)^m = K^\times$, and so $(a,b)_v = 1$ by 2.4. If $K_v = \mathbb{R}$ and $m = 2$, then a and b are both not in $N_{K_v(\sqrt{a})/K_v}(K_v(\sqrt{a})^\times)$ iff $a<0$ and $b<0$. (use 2.4).

2.8. By definition $\psi_v(b) = \psi_{L/K}(i_v(b)) = F_{L/K}(v)^{v(b)}$ $(= (a,b)_v)$

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

Thus $(a,b)_v = \left(\frac{a}{v}\right)^{v(b)}$ if $v \notin S(a)$.

More generally, if $v \notin S$, write $a = \pi^{v(a)} a_0$, $b = \pi^{v(b)} b_0$, with $v(\pi) = 1$.

Then $$(a,b)_v = (\pi^{v(a)}, \pi^{v(b)})_v (\pi^{v(a)}, b_0)_v (a_0, \pi^{v(b)})_v (a_0, b_0)_v$$
$$= (\pi, \pi)^{v(a)v(b)} (\pi, b_0)_v^{v(a)} (a_0, \pi)_v^{v(b)} (a_0, b_0)_v .$$

Notice: $v \notin S(a_0,b_0) \Rightarrow (a_0, b_0)_v = 1.$

$(-\pi, \pi)_v = 1 \Rightarrow 1 = (-\pi, \pi)_v = (-1, \pi)_v (\pi, \pi)_v = \left(\frac{-1}{\pi}\right) (\pi, \pi)_v$

$(a_0, \pi)_v = \left(\frac{a_0}{v}\right)^{v(\pi)} = \left(\frac{a_0}{\pi}\right)$

$(\pi, b_0)_v = (b_0, \pi)_v^{-1} = \left(\frac{b_0}{\pi}\right)^{-1}$.

Therefore

$$(a,b)_v = \left(\frac{-1}{\pi}\right)^{v(a)v(b)} \left(\frac{b_0}{\pi}\right)^{-v(a)} \left(\frac{a_0}{\pi}\right)^{-v(b)}$$

$$= \left(\frac{(-1)^{v(a)v(b)}\, a^{v(b)}\, b^{-v(a)}}{\pi}\right) .$$

2.9. By definition of the Artin map $\psi(K^\times) = 1$. Thus

$$\prod_v \psi_v(b_v) = 1 \quad , \quad b \in K^\times ,$$

and $\prod_v (a,b)_v = 1$.

2.10. Three computations:

↳ $$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{v \notin S(a)} \left(\frac{a}{v}\right)^{v(b)} \prod_{v \notin S(b)} \left(\frac{b}{v}\right)^{-v(a)}$$

$$= \prod_{v \notin S(a)} (a,b)_v \prod_{v \notin S(b)} (b,a)_v^{-1}$$

$$= \prod_{v \notin S(a)} (a,b)_v \prod_{v \notin S(b)} (a,b)_v$$

$$= \prod_v (a,b)_v \prod_{v \in S(a) \cap S(b)} (a,b)_v^{-1}$$

$$= \prod_{v \in S(a) \cap S(b)} (b,a)_v$$

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

↳ If $S(\lambda) = S$, then every $v \notin S$ satisfies $v(\lambda) = 0$. Thus

$$\left(\frac{b}{\lambda}\right) = \prod_{v \notin S(\lambda)} \left(\frac{b}{v}\right)^{v(\lambda)} = 1 ,$$

and so $\left(\frac{\lambda}{b}\right) = \prod_{v \in S} (b,\lambda)_v$.

2.11. Three Computations; apply 1.10 after that.

↳ Notice $(a,P)_\infty = 1$ since $P \in N_{\mathbb{R}(\sqrt{a})/\mathbb{R}}(\mathbb{R}(\sqrt{a}))$. (in both cases where $\mathbb{R}(\sqrt{a}) = \mathbb{R}$ or $\mathbb{C}$). Since $S(-1) = S$, one has

$$\left(\frac{-1}{P}\right) = \prod_{v \in S} (P,-1)_v = (P,-1)_2 \, (P,-1)_\infty = (P,-1)_2 .$$

↳ As $S(2) = S$,

$$\left(\frac{2}{P}\right) = \prod_{v \in S} (P,2)_v = (P,2)_2 \, (P,2)_\infty = (P,2)_2 .$$

↳ If P and Q are distinct odd integers, then $S(P) \cap S(Q) = S$, so

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)^{-1}$$

$$= \prod_{v \in S} (Q,P)_v = (Q,P)_2 \, (Q,P)_\infty = (Q,P)_2 .$$

2.12. Let $v \in S$, so $v \mid p$. Write $\lambda = 1 - \zeta$, where ζ generates μ_p.

$\boxed{\frac{\lambda^{p-1}}{p} \equiv -1 \pmod{\mathfrak{P}_v}}$ One observes that λ is a root of $\frac{(1-x)^p - 1}{(1-x)-1}$, so

$$\frac{(1-\lambda)^p - 1}{(1-\lambda)-1} = \sum_{k=0}^{p-1} \binom{p}{k+1} (-\lambda)^k = 0 .$$

$$\Rightarrow \lambda^{p-1} = -p - \sum_{k=1}^{p-2} \binom{p}{k+1} (-\lambda)^k .$$

This tells us that $\frac{\lambda^{p-1}}{p} \equiv -1 \pmod{\lambda}$. If we can show that $v(\lambda) > 0$ (recall $v \mid p$ means $v(p) > 0$) then we can deduce $\frac{\lambda^{p-1}}{p} \equiv -1 \pmod{\mathfrak{P}_v}$. To see this one simply observes $p = \lambda^{p-1} \prod_{k=1}^{p-1} \frac{1-\zeta^k}{1-\zeta}$, and $\prod_{k=1}^{p-1} \frac{1-\zeta^k}{1-\zeta}$ is a unit.

Thus $v(p) > 0$ implies $v(\lambda) > 0$.

$\boxed{a \equiv 1 \pmod{p\lambda\mathcal{O}_v} \Rightarrow a \text{ is } v\text{-primary}}$ In this case, using the above

$$a = 1 + p\lambda c' = 1 + \lambda^p \frac{p}{\lambda^{p-1}} c' = 1 + \lambda^p c, \qquad c, c' \in \mathcal{O}_v.$$

Write $a = \alpha^p$ with $\alpha \in \overline{K_v}$, and write $\alpha = 1 + \lambda x$. Consider

$$\begin{aligned} f(X) &= \frac{1}{\lambda^p}\left((1+\lambda X)^p - a\right) \\ &= X^p + \sum_{k=2}^{p-1} \frac{1}{\lambda^{p-1}} \binom{p}{k} \lambda^{k-1} X^k + \frac{1}{\lambda^{p-1}} pX - c. \end{aligned}$$

Notice x is a root of $f(X)$, and $f(X) \equiv X^p - X - c \pmod{\mathfrak{p}_v}$ as $v(\lambda) > 0$.

→ If $c \equiv 0 \pmod{\mathfrak{p}_v}$, then $f(X)$ has a solution in K_v by Hensel's Lemma, so $a \in (K_v^\times)^m$ and $K_v(\sqrt[m]{a}) = K_v$ is clearly unramified over K_v.

→ If $c \not\equiv 0 \pmod{\mathfrak{p}_v}$, then we still have $f(X)$ separable mod $\mathfrak{p}_v$. This implies $K_v(x)/K_v$ is unramified, but $K_v(x) = K_v(1+\lambda x) = K_v(\sqrt[m]{a})$. (Here we used the fact that if $K(\alpha)/K$ is Galois with $K(\alpha) = L$ and K number fields, and $\operatorname{minpoly}(\alpha) \in \mathcal{O}_K[x]$ is separable mod $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$, then $\mathfrak{p}$ is unramified in L.)

$\boxed{(a,b)_v = \zeta^{-S(c)v(b)},\ a \text{ as above.}}$ Here $S = \operatorname{Tr}_{k_v/(\mathbb{Z}/p)}$ where $v \mid p$.

If $c \equiv 0 \pmod{\mathfrak{p}_v}$, then $a \in (K_v^\times)^m$ by above, so $(a,b)_v = 1$. Also $\zeta^{-S(c)v(b)} = \zeta^{-S(0)v(b)} = 1$.

Now consider $c \not\equiv 0 \pmod{\mathfrak{p}_v}$. As v is unramified in $K(\sqrt[m]{a})$, $i_v(b) \in J_K^S$.

By definition $\psi_v(b) = F_{L/K}(i_v(b)^S) = F_{L/K}(v)^{v(b)}$

$$F_{L/K}(\underset{\substack{\downarrow \\ (\text{The } x \text{ from } \alpha = 1+\lambda x)}}{x}) \equiv x^{N(v)} \equiv x + S(c) \pmod{\mathfrak{p}_v} \qquad \leftarrow \text{ as } x^p \equiv x + c \pmod{\mathfrak{p}_v}.$$

If $F_{L/K}(v)(\alpha) = \zeta^i \alpha$, our goal is to show that $-S(\bar{c}) \equiv i \pmod{\mathfrak{P}_v}$, which will imply $(a,b)_v = \zeta^{-S(\bar{c})v(b)}$ by above. Let

$$\alpha_j = \zeta^j \alpha = 1 + \lambda x_j, \text{ some } x_j \in K(\sqrt[n]{a}).$$

Then

$$x_{j+1} = \frac{\alpha_{j+1} - 1}{\lambda} = \frac{\zeta \alpha_j - 1}{\lambda} = -1 + \zeta x_j = -1 + (1-\lambda) x_j .$$

Thus, as $v(\lambda) > 0$, $x_{j+1} \equiv x_j - 1 \pmod{\mathfrak{P}_v}$. Also,

$$F_{L/K}(v)(x) = F_{L/K}(v)\left(\frac{\alpha - 1}{v}\right) = \frac{F_{L/K}(v)(\alpha) - 1}{v} = \frac{\zeta^i \alpha - 1}{v} = x_i .$$

Hence $x + S(\bar{c}) \equiv x_i \equiv x - i \pmod{\mathfrak{P}_v}$.

2.13. (a) Notice $\eta_j + \lambda^j \eta_i = \eta_{i+j}$. Using 2.5,

$$1 = \left(\frac{\eta_j}{\eta_{i+j}}, \frac{\lambda^j \eta_i}{\eta_{i+j}} \right)_v$$

$$= (\eta_j, \lambda^j)_v (\eta_j, \eta_i)_v (\eta_j, \eta_{i+j})_v^{-1} (\eta_{i+j}, \lambda^j)_v^{-1} (\eta_{i+j}, \eta_i)_v^{-1} (\eta_{i+j}, \eta_{i+j})_v$$

$$= (\eta_i, \eta_j)_v^{-1} (\eta_{i+j}, \eta_j)_v (\eta_{i+j}, \lambda)_v^{-j} (\eta_i, \eta_{i+j})_v$$

(Here $(\eta_j, \lambda^j)_v = (1 - \lambda^j, \lambda^j)_v = 1$ by 2.5.)

(b) If $i + j \geqslant p+1$, then $\eta_{i+j} \in U_{p+1} \subset (K_v^\times)^p$. Hence $(\eta_i, \eta_j)_v = 1$ by the previous exercise. The result follows since any $a \in U_i$ can be written as

$$a = \eta_i^{d_i} \eta_{i+1}^{d_{i+1}} \cdots \eta_p^{d_p} x_p , \quad x_p \in U_{p+1} ,$$

and similarly for U_j.

(c) If $1 \le i \le p-1$, then $(\eta_i, \lambda)_v^i = (\eta_i, \lambda^i)_v = 1$. But $(\eta_i,\lambda)_v$ is a p^{th} root of 1, so $(\eta_i,\lambda)_v = 1$. If $i=p$, then by 2.12

$$\begin{aligned}(\eta_p, \lambda)_v &= \zeta^{-S(-1)\,v(\lambda)} = \zeta^{-S(-1)} \\ &= \zeta^{-(-1)} = \zeta \quad \text{as } f_{v/p} = 1.\end{aligned}$$

(d) We need to show uniqueness of $(K_v^\times)/(K_v^\times)^p \times (K_v^\times)/(K_v^\times)^p$, and we know $(K_v^\times)/(K_v^\times)^p$ is generated by $\lambda, \zeta, 1-\lambda, \dots, 1-\lambda^p$. But properties (a) and (c) tells us how it must be defined recursively!

2.14. Here we consider $K = \mathbb{Q}(\zeta)$, ζ a primitive third root of 1.

$\boxed{a, b \equiv \pm 1 \pmod{3R}, \text{ relatively prime.}}$ Then $S = \{\lambda, \infty\}$, and 2.7 tells us that $(-,-)_\infty = 1$. Hence by 2.10

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = (b,a)_\lambda .$$

Since $3R = \lambda^2 R$, one observes that $\pm a, \pm b \in U_2$ (for some sign). Thus $(\pm b, \pm a)_\lambda = 1$ by 2.13 (b). Now, $(-1,a)_\lambda^2 = (1,a)_\lambda = 1$, and so $(-1,a)_\lambda = 1$ as we are working over μ_3. In particular this implies

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = 1.$$

$\boxed{a = \pm(1+3(m+n\zeta))}$ Then $N(a) = (1+3m-\frac{3n}{2})^2 + (\frac{3\sqrt{3}n}{2})^2$, and

$$\frac{N(a)-1}{3} = 3(m+n-mn)+2m-n .$$

Now, using 1.6, $\left(\frac{\zeta}{a}\right) = \zeta^{\frac{N(a)-1}{3}} = \zeta^{2m-n} = \zeta^{-m-n}$.

Next observe that, by 2.10, $\left(\frac{\lambda}{a}\right) = (a,\lambda)_\lambda = (1+3(m+n\zeta), \lambda)_\lambda$.

Write $1+3(m+n\zeta) = 1+2(m+n)\lambda^2 - (m+3n)\lambda^3 + n\lambda^4$

$$= (1+2(m+n)\lambda^2)(1-(m+3n)\lambda^3)(1+\lambda^4 x), \quad x \in R.$$

Note that $(1+2(m+n)\lambda^2)(1-\lambda^2)^{2(m+n)} \in U_4$ with $(1-\lambda^2, \lambda)_\lambda = 1$, so by 2.13

$$(1+2(m+n)\lambda^2, \lambda)_\lambda = 1$$

As $1+\lambda^4 x \in U_4$, $(1+\lambda^4 x, \lambda)_\lambda = 1$. Finally, by considering $(1-(m+3n)\lambda^3)(1-\lambda^3)^{-(m+3n)}$, one has $(1-(m+3n)\lambda^3, \lambda)_\lambda = (1-\lambda^3, \lambda)_\lambda^{m+3n} = \zeta^{m+3n} = \zeta^m$. Therefore

$$\left(\frac{\lambda}{a}\right) = \zeta^m.$$

$\boxed{\text{Application}}$ Fix $q \equiv 1 \pmod 3$ prime, so q is totally split in $\mathbb{Q}(\zeta)$.

($\Rightarrow$) Let 2 be a cubic residue mod q. Write $q = \pi\bar{\pi}$ with $\pi \equiv \pm 1 \pmod{3R}$. WLOG $\pi \equiv 1 \pmod{3R}$. Then $\mathbb{Z}/q\mathbb{Z} \cong R/\pi R$, and so

$$\begin{aligned}
2 \text{ cubic residue mod } q &\Leftrightarrow 2 \text{ cubic residue mod } \pi \\
&\Leftrightarrow \left(\frac{2}{\pi}\right) = 1 \\
&\Leftrightarrow \left(\frac{\pi}{2}\right) = 1 \\
&\Leftrightarrow \pi \text{ cubic residue mod } (2) = 2R \\
&\Leftrightarrow \pi \equiv 1 \pmod{2R} \text{ as } 1 \text{ is the only cube mod } 2R \\
&\Leftrightarrow \pi = 1 + 6(\alpha + \beta\zeta), \quad \alpha, \beta \in \mathbb{Z}.
\end{aligned}$$

Therefore $q = (1+6(\alpha+\beta\zeta)) \cdot (1+6(\alpha+\beta\zeta^2))$

$$= (1+6n-3m)^2 + 27m^2.$$

(⇐) Suppose $q = x^2+27y^2$. Letting $\pi = x+3\sqrt{3}iy \in \mathbb{Z}[\zeta]$, one observes that $q = \pi\bar{\pi}$. As before 2 is a cubic residue mod q iff $\left(\frac{\pi}{2}\right) = 1$. By 1.6, $\left(\frac{\pi}{2}\right) \equiv \pi^{\frac{N(2)-1}{3}} \equiv \pi \pmod{(2)}$. Hence we need to show $\pi \equiv 1 \ (\mathrm{mod}\ (2) = 2R)$. But

$$\pi = x+3(1+2\zeta)y = x+3y+6\zeta y \equiv x+y \pmod{(2)},$$

and x and y must have opposite parity as q is odd. Thus $\pi \equiv 1 \pmod{2}$, as desired

2.15. By the notations from before, we are considering

$$K = \mathbb{Q}(\zeta_3), \quad m = 3, \quad a = 2, \quad S = \{v : v \mid 3 \text{ or } v \mid \infty\}.$$

If $p \neq 2,3$, then $p \notin S(2)$. Hence

$$\begin{aligned}\psi_p(p)\sqrt[3]{2} &= (2,p)_p\sqrt[3]{2} \\ &= \left(\frac{2}{p}\right)\sqrt[3]{2} && \text{by } 2.8 \\ &= F_{L/\mathbb{Q}}(p)(\sqrt[3]{2}) \\ &\equiv (\sqrt[3]{2})^p \pmod{p} && \text{by } 1.4.\end{aligned}$$

- If $p \equiv 1 \pmod{3}$ and of the form x^2+27y^2, then $\left(\frac{2}{p}\right) = 1$, so

$$F_{L/\mathbb{Q}}(p)(\sqrt[3]{2}) = \sqrt[3]{2}$$

and $F_{L/\mathbb{Q}}(p) \equiv id$.

→ If $p \equiv 1 \pmod 3$ and not of the form x^2+27y^2, then $\left(\frac{2}{p}\right) \neq 1$,

so $2^{\frac{p-1}{3}} \not\equiv 1 \pmod p$, implying $\left(\frac{2}{p}\right) = \zeta^i$ for $3 \nmid i$. Hence

$$\mathrm{Frob}_{L/\mathbb{Q}}(p)(\sqrt[3]{2}) = \zeta^i\sqrt[3]{2}, \quad \mathrm{Frob}_{L/\mathbb{Q}}(p)(\zeta^i\sqrt[3]{2}) = \zeta^{2i}\sqrt[3]{2} \neq \zeta^i\sqrt[3]{2}, \sqrt[3]{2},$$

Note $\mathrm{Frob}(p)(\zeta) = \zeta^p = \zeta$ as $\zeta \equiv 1 \pmod p$

implying $\mathrm{Frob}_{L/\mathbb{Q}}(p)$ is a 3-cycle.

→ If $p \equiv 2 \pmod 3$, then $\mathrm{Frob}_{L/\mathbb{Q}}(p)(\zeta) = \zeta^2$.

↳ If $\mathrm{Frob}_{L/\mathbb{Q}}(p)(\sqrt[3]{2}) = \zeta^i\sqrt[3]{2}$, $3 \nmid i$, then

$$\mathrm{Frob}_{L/\mathbb{Q}}(p)(\zeta^i\sqrt[3]{2}) = \zeta^{2i}\zeta^i\sqrt[3]{2} = \sqrt[3]{2},$$

$$\mathrm{Frob}_{L/\mathbb{Q}}(p)(\zeta^{2i}\sqrt[3]{2}) = \zeta^{4i}\zeta^i\sqrt[3]{2} = \zeta^{2i}\sqrt[3]{2}.$$

↳ If $\mathrm{Frob}_{L/\mathbb{Q}}(p)(\sqrt[3]{2}) = \sqrt[3]{2}$, then

$$\mathrm{Frob}_{L/\mathbb{Q}}(p)(\zeta\sqrt[3]{2}) = \zeta^2\sqrt[3]{2},$$

$$\mathrm{Frob}_{L/\mathbb{Q}}(p)(\zeta^2\sqrt[3]{2}) = \zeta\sqrt[3]{2}.$$

In either case $\mathrm{Frob}_{L/\mathbb{Q}}(p)$ is a 2-cycle if $p \equiv 2 \pmod 3$.

2.16. $\boxed{\text{Counterexample}}$ Except for the T'-condition, everything else holds in the assumptions of the exercise for this example ($\mathrm{C\ell}(\mathbb{Q}(\sqrt{-14})) = 4 \neq 1$, which may mess up the T'-condition). We want to try to find a T-unit $x \in \mathbb{Q}$ such that

$$(x,-14)_\infty = -1, \quad (x,-14)_2 = -1, \quad (x,-14)_7 = 1.$$

As x is a T-unit, $x = \pm 2^a 7^b$. But $(x,-14)_\infty = -1$, so $x = -2^a 7^b$.

Observe now that $N = N_{\mathbb{Q}_7(\sqrt{-14})^\times/\mathbb{Q}_7^\times}(\mathbb{Q}_7(\sqrt{-14})^\times)$ contains $(\mathbb{Q}_7^\times)^2$, and $14 \in N$, $2 \in (\mathbb{Q}_7^\times)^2$. Hence $7 = \frac{14}{2} \in N$. This implies, by 2.4, that

$(x,-14)_7 = (-1,-14)_7 = \left(\frac{-1}{7}\right)$ as $S=\{2,\infty\}$ and $S(-1)=S$.

$$= -1 \neq 1,$$

a contradiction.

$\boxed{a\in A_0 \text{ lemma}}$ Let $a\in A$ such that $\pi_v(a)\in\pi_v(A_0)$ for all v, where $\pi_v : X=\prod_v K_v^\times/(K_v^\times)^m \to K_v^\times/(K_v^\times)^m$. Pick a representation $\tilde{a}\in K_v^\times$ of a. Then, as $\pi_v(\tilde{a})\in\pi_v(A_0)$, locally $\sqrt[m]{\tilde{a}}\in L_{v'} = K_v(\sqrt[m]{a_1},\dots,\sqrt[m]{a_r})$ for all $v'|v$, $v\in T$.

Now, let $M=L(\sqrt[m]{a})$. We want to show $M=L$. Locally one has:

↳ if $v\in T'$ then $M_w=L_v$ for all $w|v$, so $N_{M_w^\times/L_v^\times}(M_w^\times)=L_v^\times$.

↳ if $v\notin T'$ then v is unramified, so $N_{M_w^\times/L_v^\times}(\mathcal{O}_w^\times)=\mathcal{O}_v^\times$ for $w|v$.

Thus $J_L = L^\times J_{L,T'} \subset L^\times N_{M/L}(J_M)$, and by class field theory

$$\mathrm{Gal}(M/L) \cong J_L/L^\times N_{M/L}(J_M) = 1.$$

Hence $M=L$, and $\sqrt[m]{\tilde{a}}\in L$. This implies $a\in A_0$.

$\boxed{\text{Proving exercise}}$ Define $f: X\to\mu_m$ by $f((\alpha_v)) = \langle (x_v),(\alpha_v)\rangle$.

If we denote $A_1=$ Subgroup generated by $i_v(a_i)$ for all v, the problem is resolved if we can find $x\in A$ such that $\langle x,-\rangle|_{A_1} = f(-)|_{A_1}$.

By above $A\cap A_1 = A_0$, and f is trivial on A_0 by condition (i). Since $A \overset{\langle -,-\rangle}{\cong} \mathrm{Hom}(X/A,\mu_m)$ by the explanation of this exercise, it suffices to show the existence of some $g\in\mathrm{Hom}(X,\mu_m)$ with $g|_A\equiv 1$ and $g|_{A_1}\equiv f|_{A_1}$

As $A \cap A_1 = A_0$, one defines $\tilde{g}$ on the subgroup $AA_1 \subset X$ precisely by $\tilde{g}|_A \equiv 1$ and $\tilde{g}|_{A_1} \equiv f|_{A_1}$. Then $\tilde{g}$ can be extended to g by the following claim.

Claim: If G is a finite abelian m-torsion group,
H a subgroup of G,
then $\mathrm{res} : \mathrm{Hom}(G, \mu_m) \to \mathrm{Hom}(H, \mu_m)$ is a surjection.

Proof. Observe $\mathrm{Hom}(G, \mu_m) = \mathrm{Hom}(G, \mathbb{C}^\times)$, and similarly for H. Thus, given a homomorphism $H \xrightarrow{\varphi} \mathbb{C}^\times = GL_1(\mathbb{C})$, simply consider the induction $\mathrm{Ind}_H^G \varphi : G \to GL_n(\mathbb{C})$, followed by projection to $GL_1(\mathbb{C})$. □

3. v splits completely in L $\Leftrightarrow$ $\overset{\overset{L^v}{\shortparallel}}{L_w} = K_v$, $\quad w | v$

$\Leftrightarrow$ $\mathrm{Gal}(L_w/K_v) = 1$

$\Leftrightarrow$ $\psi_v \equiv 1$ $\quad$ ($\psi_v : K_v^\times \to G^{w/v}$ is surjective)

$\Leftrightarrow$ $i_v(K_v^\times) \subset K^\times N_{L/K} J_L$ by class field theory.

Class field theory tells us that ψ_v maps $U_v = \mathcal{O}_v^\times$ onto the inertia group $I_v = \mathrm{Gal}(L^v/L^{v,ur})$. Hence

v is unramified in L $\Leftrightarrow$ $\psi_v|_{\mathcal{O}_v^\times} \equiv 1$

$\Leftrightarrow$ $i_v(U_v) \subset \ker \psi_{L/K} = K^\times N_{L/K} J_L$.

By VII.5.1, the Hilbert class field (unramified at all nonarchimedean places, and split completely at the archimedean ones) is the class field to $K^\times J_{K,S}$, where $S = \{$archimedean primes$\}$ and $J_{K,S} = \prod_{v \in S} K_v^\times \cdot \prod_{v \notin S} \mathcal{O}_v^\times$. Also, writing K' to be the Hilbert class field, one has

$$\mathrm{Gal}(K'/K) \overset{\xleftarrow{\mathrm{Art}}}{\cong} J_K / K^\times J_{K,S} = J_{K,\text{finite}} \Big/ K^\times \cdot \prod_{v \nmid \infty} \mathcal{O}_v^\times \overset{\sim}{=} Cl(K).$$

$$F_{K'/K}(\mathfrak{a}) =: F_{K'/K}(x_{\mathfrak{a}}) \longleftarrow\!\!\shortmid \ x_{\mathfrak{a}} = (\pi_v^{n_v}) \ \longleftarrow\!\!\shortmid \ \mathfrak{a} = \prod_{v | \mathfrak{a}} v^{n_v}.$$

Thus $[K':K] = \# Cl(K) =: h_K$, and the residue class degree of an arbitrary ideal $\mathfrak{a}$ (necessarily unramified in K') is determined by the order of $F_{K'/K}(\mathfrak{a})$ in $\mathrm{Gal}(K'/K)$. Thus

$\mathfrak{a}$ splits completely $\Leftrightarrow$ $F_{K'/K}(\mathfrak{a}) = 1$ $\Leftrightarrow$ $\mathfrak{a}$ is principal.

Notice that, if K_1 is the class field unramified all all nonarchimedean places (with no condition at infinity), then $Gal(K_1/K) \cong I_K/P_K^+$ by looking at our previous isomorphism. Hence

$$Gal(K'/K_1) \cong P_K/P_K^+ ;$$

and this is an abelian 2-group. Now, observe one has a map

$$\begin{aligned} K_S &\longrightarrow (\mathbb{R}^\times/(\mathbb{R}_{>0})^\times)^{r_1} =: R \\ \alpha &\longmapsto (\sigma_i \alpha) \end{aligned}$$

with kernel K_S^+, and so $K_S/(K_S)^+ \hookrightarrow R$. Also one has, by weak approximation, a surjection

$$P_K \twoheadrightarrow \frac{R}{K_S/K_S^+}$$

with kernel P_K^+. Hence $(P_K : P_K^+) = 2^{r_1}/(K_S : K_S^+)$.

Now let K be a real quadratic field $(r_1 = 2)$. Dirichlet's unit theorem implies

$$\mathcal{O}_K^\times = K_S = \{\pm 1\} \times \langle \varepsilon \rangle ,$$

where ε is a fundamental unit for K. We now have 4 cases.

→ $\varepsilon > 0$ and $\sigma(\varepsilon) < 0$ (so $N(\varepsilon) = -1$). Then $K_S^+ = \langle \varepsilon^2 \rangle$, and $[K_S : K_S^+] = 4$. So $[P : p^+] = [K_1 : K'] = 1$.

→ $\varepsilon < 0$ and $\sigma(\varepsilon) > 0$. Same as above.

→ $\varepsilon > 0$ and $\sigma(\varepsilon) > 0$ (so $N(\varepsilon) = +1$). Then $K_S^+ = \langle \varepsilon \rangle$, so $[K_S : K_S^+] = 2$ and $[K_1 : K'] = 2$.

→ $\varepsilon < 0$ and $\sigma(\varepsilon) < 0$. Same as above.

Explicit Examples Let us compute K' for the first five imaginary quadratic fields $\mathbb{Q}(\sqrt{-15})$, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{-23})$, $\mathbb{Q}(\sqrt{-6})$, $\mathbb{Q}(\sqrt{-31})$. without using CM theory. Observe the infinity places are always unramified.

(a) $K = \mathbb{Q}(\sqrt{-15})$. We claim $K' = K(\sqrt{-3})$. Observe $K' = K(\sqrt{-5})$. Hence by Kummer theory $\Delta_{K'}$ divides both $2^2 3$ and $2^2 5$, implying $\Delta_{K'} | 2^2$. Thus we just need to check $v|2$ is unramified. But $-3 = 1 + 2^2 \cdot (-1) = 1 + \lambda c$, taking $\lambda = 1-(-1) = 2$, hence by 2.12 K'/K is unramified at all $v|2$.

(b) $K = \mathbb{Q}(\sqrt{-5})$. We claim $K' = K(\sqrt{-1})$. Again $\Delta_{K'} | 2^2$. We have

$$\begin{tikzcd}
& K' \arrow[dl, dash] \arrow[dr, dash, "e_v=1 \text{ for } v|2."] & \\
\mathbb{Q}(\sqrt{5}) \arrow[dr, dash, "e_2=2"'] & & \mathbb{Q}(\sqrt{-1}) \arrow[dl, dash, "e_2=2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

To see $e_v = 1$ for $v|2$, observe $K' = \mathbb{Q}(\sqrt{-1})(\sqrt{5})$ and $5 = 1 + 2^2(1)$, so by 2.12 $K'/\mathbb{Q}(\sqrt{-1})$ is unramified at all $v|2$. Therefore $K'/\mathbb{Q}(\sqrt{-5})$ has this property as well.

(c) $K = \mathbb{Q}(\sqrt{-23})$: Consider the roots x_1, x_2, x_3 of $x^3 - x - 1$. Since its discriminant is -23, the Galois group is S_3 (23 is not a square). Thus

$$K' = \mathbb{Q}(\sqrt{-23})(x_1, x_2, x_3) = K(x_i).$$

Since $23 = \prod_{i \neq j} (x_i - x_j)^2$, if a prime p in K satisfies $p \nmid 23$, then $x^3 - x - 1$ is still separable mod p, so p is unramified in K'/K. We now

Consider primes $\mathfrak{p}$ lying over 23. Let $\mathfrak{P}$ lie over $\mathfrak{p}$ in K', and consider $K'/\mathbb{Q}$. The derivative $3x^2-1$ of x^3-x-1 has a root mod 23, since $3x^2 \equiv 1 \pmod{23} \Leftrightarrow x^2 \equiv 8 \pmod{23}$ and 8 is a quadratic residue mod 23. Hence x^3-x-1 has a simple root in $\mathbb{Z}/23$, implying the existence of a root in $\mathbb{Q}_{23}$ by Hensel's Lemma. This root is the image of some x_i in $\mathbb{Q}_{23}$, so

$$K'_{\mathfrak{P}} = \mathbb{Q}_{23}(\sqrt{-23}, x_i) = \mathbb{Q}_{23}(\sqrt{-23}) \text{ has degree 2 over } \mathbb{Q}_{23}.$$

Thus $e_{\mathfrak{P}/23} f_{\mathfrak{P}/23} = 2$. But $e_{\mathfrak{P}/23} \geq 2$ since $23 = \prod_{i \neq j} (x_i - x_j)^2$, so $e_{\mathfrak{P}/23} = 2$. Also $e_{\mathfrak{p}/23} = 2$ since $\mathfrak{p} \mid \Delta_{K/\mathbb{Q}}$. Thus $e_{\mathfrak{P}/\mathfrak{p}} = 1$, and $\mathfrak{P}$ is unramified over $\mathfrak{p}$, implying K'/K is the Hilbert class field of K.

(d) Similar to (a).

(e) Similar to (c).

2

4.1. Clear.

4.2. Clear

4.3. (⇒) Suppose f represents 0. If $b\in(K^\times)^2$ then $K(\sqrt{b})=K$, so $c\in N_{K(\sqrt{b})/K^\times}(K(\sqrt{b})^\times)=K^\times$ is clear. If $b\notin(K^\times)^2$, then by 4.2 $f(X,Y,0)$ does not represent 0, so there must exist x,y,z with $z\neq 0$ such that $x^2-by^2=cz^2 \Rightarrow c=(\frac{x}{z})^2-b(\frac{y}{z})^2$.

(⇐) If $c=\alpha^2-b\beta^2$, then $f(\alpha,\beta,1)=0$ and f represents 0.

4.4. Solution in the exercise

4.5. By 4.3 $f=X^2-bY^2-cZ^2$ represents 0 in K_v iff c is a norm from $K_v(\sqrt{b})$. But by 2.4 this is iff $(b,c)_v=1$.

Hence, as $(b,c)_v=1$ for all $v\notin S(b,c)$ by 2.8, $(b,c)_v=1$ for almost all v. We are considering $m=2$, so $(b,c)_v\in\{\pm1\}$. By the product formula, there must be an even number of v for which $(b,c)_v\neq 1$.

4.6. Let $f=X^2-bY^2-cZ^2+acT^2$.

Suppose f does not represent 0 in K_v.

→ If $a\in(K_v^\times)^2$ then $f(0,0,\sqrt{a},1)=0$, so $a\notin(K_v^\times)^2$

→ If $b\in(K_v^\times)^2$ then $f(\sqrt{b},1,0,0)=0$, so $b\notin(K_v^\times)^2$.

→ By 4.4(ii), $c\notin N(K(\sqrt{b})^\times/K^\times)$ and $c\notin N(K(\sqrt{a})^\times/K^\times)$.

→ We now need to show $K_v(\sqrt{a}) = K_v(\sqrt{b})$ and $ab \in (K_v^\times)^2$. Since $a, b \notin (K_v^\times)^2$, by class field theory $N(K_v(\sqrt{a})^\times/K^\times)$ has index 2 in $K^\times$ since $Gal(K_v(\sqrt{a})/K) = \mathbb{Z}/2$ (and similarly for $K(\sqrt{b})$).

Since $c \notin N(K_v(\sqrt{a})^\times/K^\times)$,

$$K_v^\times = N(K_v(\sqrt{a})^\times/K^\times) \sqcup c \cdot N(K_v(\sqrt{a})^\times/K^\times).$$

Also $N(K_v(\sqrt{b})^\times/K^\times) \cap c N(K_v(\sqrt{a})^\times/K^\times) = \emptyset$ by 4.4 (ii), so $N(K_v(\sqrt{b})^\times/K^\times) \subset N(K_v(\sqrt{a})^\times/K^\times)$, and this is an equality by what is discussed above. By III. 2.6 (Proposition 3), this implies $K_v(\sqrt{a}) = K_v(\sqrt{b})$. This implies $ab \in (K_v^\times)^2$.

Now suppose $a, b \notin (K_v^\times)^2$, $ab \in K_v^\times$, $c \notin N = N(K_v(\sqrt{a})^\times/K) = N(K_v(\sqrt{b})^\times/K^\times)$. Then, write $f = X^2 - bY^2 - c(Z^2 - aT^2)$, one sees that the set of elements represented by f is $(N - cN) \cup N \cup (-cN)$. As $c \notin N$, one has N and cN disjoint, and f does not represent 0 in K_v.

↳ Under these conditions, suppose $A \neq K_v^\times$, where $A = (N - cN) \sqcup N \sqcup (-cN)$. If $-1 \in N$, then $-cN = cN$, so $cN \cup N \subset A$, a contradiction (we already showed that $K_v^\times = N \cup cN$). So $-1 \notin N$

Since $-1 \notin N$, $0 \notin N + N$, so $(N+N) \subset K_v^\times = N \sqcup cN$. If $cn \in N+N$ for some $n \in N$, then $cN \subset N+N$, Also $-cN \not\subset cN$ (else $-1 \in N$), implying $N \cap (-cN) \neq \emptyset$, and $-c \in N \Rightarrow -cN = N$. Hence $N+N = N - cN$, and $cN \subset N + N = N - cN \subset A$, a contradiction (for that will imply $A = K_v^\times$). Thus $cN \cap (N+N) = \phi$, and $N + N \subset N$.

Finally let us show that f represents every element in $K_v^\times$, unless $K_v \cong \mathbb{R}$ and f is positive definite.

$\boxed{K \text{ function field}}$ If $A \neq K_v^\times$, then $N + N \subset N$. Hence, as $1 \in N$, $p-1 \in N$, where $p = \operatorname{char} K_v$. But this means $-1 \in N$, a contradiction.

$\boxed{K \text{ number field}}$ Suppose $K_v/\mathbb{Q}_p$ is nonarchimedean. Then, just like above, $\{-1+p^n\}_{n \geq 1} \subset N$. As N is closed (finite index and open implies closed), and $-1+p^n \to -1$, this implies $-1 \in N$, a contradiction.

If $K_v = \mathbb{C}$, clearly $-1 \in N$ as $f(i,0,0,0) = -1$.

If $K_v = \mathbb{R}$, then f cannot be negative definite as $f(1,0,0,0) > 0$. If f is nondefinite then f represents $\mathbb{R}^\times$, and if f is positive definite then f represents $\mathbb{R}^\times_{>0}$.

4.7. If $K_v = \mathbb{R}$ then f represents 0 iff it is not definite (clear). So now let v be nonreal. It suffices to assume f has 5 variables. Write

$$f = a X_1^2 + g(X_2, X_3, X_4, X_5).$$

Then 4.6 tells us g either represents 0 or $K_v^\times$. In the former case we are done (let $X_1 = 0$). In the latter case, g will represent $-a$, and we are also done (let $X_1 = 1$).

4.8. $\boxed{n=1}$ Trivial

$\boxed{n=2}$ Write $f = x^2 - by^2$, and suppose f represents 0 in each K_v. Let $L = K(\sqrt{b})$. Then, by 4.3, $L^v = K_v$ for all v. By Cebotarev's density theorem, the density of primes v that split completely is $\frac{1}{\#\mathrm{Gal}(L/K)}$. But this equals 1, so $K(\sqrt{b}) = K$ and $b \in (K^\times)^2$. By 4.2, f represent 0 in K.

$\boxed{n=3}$ Write $f = x^2 - by^2 - cz^2$. Let $L = K(\sqrt{b})$, which is cyclic over K. Using 4.3 and the Hasse norm theorem (VIII. 9.6), one has

$$\begin{aligned} f \text{ represents } 0 \text{ in } K &\Leftrightarrow c \in N_{L/K}(L^\times) \\ &\Leftrightarrow c \in N_{L^v/K_v}((L^v)^\times) \text{ for all } v \in \Sigma_K \\ &\Leftrightarrow f \text{ represents } 0 \text{ in } K_v \text{ for all } v \in \Sigma_K. \end{aligned}$$

$\boxed{n=4}$ Write $f = x^2 - by^2 - cz^2 + acT^2$, and write $g = x^2 - by^2 - cz^2$. By 4.4,

$$\begin{aligned} f \text{ represents } 0 \text{ in } K &\Leftrightarrow g \text{ represents } 0 \text{ in } K(\sqrt{ab}) \\ &\Leftrightarrow g \text{ represents } 0 \text{ in } K_v(\sqrt{ab}) \text{ for all } v \text{ (by above)} \\ &\Leftrightarrow f \text{ represents } 0 \text{ in } K_v \text{ for all } v. \end{aligned}$$

$\boxed{n=5}$ Write $f = ax_1^2 + bx_2^2 - g(x_3, \ldots, x_n)$ where g has $n-2 \geq 3$ variables. Suppose f represent 0 in K_v for all v. By 4.5 g represents 0 in K_v for all v outside a finite set S.

↳ Let $v \in S$. As f represents 0 in K_v, there exists $x_{1,v}, \dots, x_{n,v} \in K_v$, not all zero, such that $a x_{1,v}^2 + b x_{2,v}^2 = g(x_{3,v}, \dots, x_{n,v})$. Since $(K_v^\times)^2$ is open in $K_v^\times$, $g(K_v^\times, \dots, K_v^\times)$ is open. By weak approximation, there exists $x_1, x_2 \in K$ such that $a x_1^2 + b x_2^2$ is sufficiently close to $a x_{1,v}^2 + b x_{2,v}^2$ for all $v \in S$. As g does not represent 0 in K_v, $v \in S$, each $a x_{1,v}^2 + b x_{2,v}^2$ is nonzero. Hence we can further assume that $a x_1^2 + b x_2^2 \in g(K_v^\times, \dots, K_v^\times)$ for all $v \in S$. Writing $c = a x_1^2 + b x_2^2$, this means c is represented by g in K_v for all $v \in S$.

↳ For $v \notin S$, g represents 0 in K_v, hence represents c.

By induction, $cY^2 - g(X_3, \dots, X_n)$ represents 0 in K (since it represents 0 in K_v for all v). Thus f represents 0, for

$$cY^2 - g(X_3, \dots, X_n) = a(x_1 Y)^2 + b(x_2 Y)^2 - g(X_3, \dots, X_n)$$

with x_1, x_2 already chosen (and we choose appropriate $Y, X_3, \dots, X_n$, not all zero, to make sure the above quadratic form vanishes).

4.9. By 4.8, f represents 0 in K $\Leftrightarrow$ f represents 0 in K_v for all v.

$\Leftrightarrow$ f is nondefinite at real places v by 4.7.

4.10. By 4.9, $c \in \mathbb{Q}$ is represented by $X^2+Y^2+Z^2$ in $\mathbb{Q}$ iff $f = X^2+Y^2+Z^2-cT^2$ represents 0 in each of $\mathbb{Q}_p$ and $\mathbb{R}$.

$\boxed{\text{At } \mathbb{R}}$ We require f to be nondefinite, forcing $c>0$.

$\boxed{\text{At } \mathbb{Q}_p,\ p\neq 2}$ Here $(-1,-1)_p = 1$ as $p \notin S(-1) = S = \{2,\infty\}$, so by 2.8

$$(-1,-1)_p = \left(\frac{-1}{p}\right)^{v_p(-1)} = 1 .$$

Thus by 4.5, $f(-,-,-,0) = x^2+y^2+z^2$ represents 0.

$\boxed{\text{At } \mathbb{Q}_2}$ Define $H_a^{\varepsilon} = \{x \in \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 : (x,a)_2 = \varepsilon\}$ for $\varepsilon \in \{\pm 1\}$. Then

$\boxed{\text{well-defined by 2.4, since } (\mathbb{Q}_2^\times)^2 \subset N(\mathbb{Q}_2(\sqrt{a})^\times)}$

f represents 0 in $\mathbb{Q}_2$

$\Leftrightarrow \{x \in \mathbb{Q}_2 : x \text{ represented by } x^2+y^2\} \cap \{x \in \mathbb{Q}_2 : x \text{ represented by } -(z^2-cT^2)\} \neq \emptyset$

$\Leftrightarrow \{x \in \mathbb{Q}_2 : x^2+y^2-xW^2 \text{ represents } 0\} \cap \{x \in \mathbb{Q}_2 : z^2-cT^2+xW^2 \text{ represents } 0\} \neq \emptyset$

$\overset{4.5}{\Leftrightarrow} \{x \in \mathbb{Q}_2 : (-1,x)_2 = 1\} \cap \{x \in \mathbb{Q}_2 : (c,-x)_2 = 1\} \neq \emptyset$

$\Leftrightarrow \quad H_{-1}^{1} \cap H_c^{(c,-1)_2} \neq \emptyset .$

We now try to understand H_a^{ε} better.

- → If $a=1$ in $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$, then $\# H_1^1 = 8$ and $\# H_1^{-1} = 0$.
- → Suppose $a \neq 1$ in $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$. Then by local class field theory $N_a = N(\mathbb{Q}_2(\sqrt{a})^\times)$ has index two in $\mathbb{Q}_2^\times$. Thus, by 2.4, $H_a^1 = N_a$ and $H_a^{-1} =$ (the other coset of $\mathbb{Q}_2^\times/N_a$, implying $\# H_a^1 = \# H_a^{-1} = 4$, $H_a^1 \cap H_a^{-1} = \emptyset$.

Observe that if $\overset{\neq 1}{a} \neq \overset{*}{a'}$ then $H_a^{\varepsilon} \cap H_{a'}^{\varepsilon'} \neq \phi$. Thus

$$H_a^{\varepsilon} \cap H_{a'}^{\varepsilon'} = \phi \iff \begin{array}{l} a = a' \text{ and } \varepsilon = -\varepsilon', \\ \text{or } \ a' = 1 \text{ and } \varepsilon' = -1 \qquad (\text{or } a = 1 \text{ and } \varepsilon = -1). \end{array}$$

Note that if $c = 1$ then $(c,-1)_2 = 1 \neq -1$. Therefore, applying this to our case,

$$H_{-1}^{1} \cap H_c^{(c,-1)_2} = \phi \iff c = -1 \text{ and } (c,-1)_2 = -1.$$

But $(-1,-1)_2 = -1$, so one has

$$H_{-1}^{1} \cap H_c^{(c,-1)_2} \neq \phi \iff c \neq -1 \text{ in } \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2.$$

This forces c to be of the form $4^n r$, $r \not\equiv 7 \pmod 8$.

$\boxed{\text{Summary}}$ $c \in \mathbb{Q}$ is a sum of three rational squares iff

$$c = 4^n r, \quad r > 0 \text{ and } r \not\equiv 7 \pmod 8$$

Every rational number is a sum of four squares: we are done if $c = 4^n r$, $r > 0$ and $r \not\equiv 7 \pmod 8$, and if $r \equiv 7 \pmod 8$, consider $4^n(r-1) + 4^n = 4^n(r-1) + (2^n)^2$.

4.11. By the same argument as above the 4-squares claim follows from the 3-squares claim. Following the argument in this exercise, it remains to show that if x has common denominator $d > 0$, then x' has common denominator $|a|^2 d < d$. This is because

$$x' = x - \frac{2(x,a)}{(a,a)}a = x + \frac{|x-a|^2 - |x|^2 - |a|^2}{|a|^2}a = x + \frac{|z|^2 - c - |a|^2}{|a|^2}a$$

$$= \frac{|z|^2 - c}{d|a|^2}da + z \quad \left(\begin{array}{c} da, z \text{ are} \\ \text{both integers} \end{array}\right).$$

4.12. Let $f = X^2 - bY^2 - cZ^2$. By 4.6,

$$\{ d \in K_v^\times : f \text{ does not represent } d \}$$

$$= \{ d \in K_v^\times : X^2 - bY^2 - cZ^2 - dT^2 \text{ does not represent } 0 \}$$

$$= \{ d \in K_v^\times : -\tfrac{d}{c} \notin (K_v^\times)^2,\ b \notin (K_v^\times)^2,\ b(-\tfrac{d}{c}) \in (K_v^\times)^2,\ c \notin N(K_v(\sqrt{b})^\times) \}$$

$$= \{ d \in K_v^\times : -\tfrac{d}{c} \notin (K_v^\times)^2,\ b(-\tfrac{d}{c}) \in (K_v^\times)^2 \} \text{ and } c \notin N(K_v(\sqrt{b})^\times)\} .$$

$$= \{ d \in K_v^\times : -\tfrac{d}{c} \in b(K_v^\times)^2 \} \text{ and } c \notin N(K_v(\sqrt{b})^\times)$$

$$= -bc(K_v^\times)^2, \text{ a coset of } (K_v^\times)^2 \text{ in } K_v^\times.$$

Now let $K = \mathbb{Q}$, and let f be positive definite. Then f does not represent 0 in $\mathbb{Q}_\infty = \mathbb{R}$, and by 4.5 there must exist a prime p such that f does not represent 0 in $\mathbb{Q}_p$. By above, f only represents a coset of $(\mathbb{Q}_p^\times)^2$ in $\mathbb{Q}_p^\times$, so f does not represent all positive integers. (In particular, $(\mathbb{Q}_p^\times)^2$ and $p(\mathbb{Q}_p^\times)^2$ are different cosets, so f does not represent 1 or p in $\mathbb{Q}$.)

5.1. Let $n_1 \in N_1$, so $n_1 = k_1^{1+\sigma} = k_1^{1+\tau}$ for some $k_1 \in K_1^\times$. Hence $n_1^2 = k_1^{2(1+\sigma)} = k_1^{1+\sigma+\rho+\tau} = N_{L/K}(k_1)$; and $n_1 \in N$. By symmetry,

$$N_1 N_2 N_3 \subset \{ x \in K^\times : x^2 \in N \}$$

Conversely let $x \in K^\times$ such that $x^2 = y^{1+\rho+\sigma+\tau}$ for some $y \in L^\times$. Consider $u = x^{-1} y^{1+\rho}$. Then $u^\rho = u$ as x is stable under $1, \sigma, \rho, \tau$, implying $u \in K_1$. Furthermore,

$$N_{K_1/K}(u) = u^{1+\sigma} = x^{-1} y^{1+\rho} x^{-\sigma} y^{\sigma+\tau} = 1,$$

So by Hilbert's Theorem 90 there exists $y_1 \in K_1^\times$ with $\overbrace{y_1^{\sigma-1}}^{=y_1^{\tau-1}} = x^{-1} y^{1+\rho}$. Similarly there exists $y_2 \in K_2^\times$ with $\overbrace{y_2^{\rho-1}}^{=y_2^{\tau-1}} = x^{-1} y^{1+\sigma}$.

Now, letting $y_3 = y_1 y^\rho / y_2$,

$$y_3^\tau = \frac{y_1 x^{-1} y^{1+\rho} y^\sigma}{y_2 x^{-1} y^{1+\sigma}} = \frac{y_1 y^\rho}{y_2} = y_3,$$

So $y_3 \in K_3^\times$. Further, $y_3^{1+\rho} = (y_1 y_2^{-1})^2 x y^{\rho-\tau}$, implying

$$x = (y_1^{-1})^{1+\sigma} y_2^{1+\tau} y_3^{1+\rho} \in N_1 N_2 N_3,$$

and $\{x \in K^\times : x^2 \in N\} \subset N_1 N_2 N_3$.

5.2. If L^w/K_w has degree 4 for some w, then $G^w = Gal(L^w/K_w) = G$. Thus local norms are global norms by VII.11.4. Now, local class field theory says that $Gal(L^v/K_v) \cong K_v^\times / N_{L^v/K_v}(L_v^\times) \subset G$. Thus, if $x \in K^\times \subset K_v^\times$ then $x^2 \in N_{L^v/K_v}(L_v^\times)$ since elements of G has order at most 2. This implies that $x^2 \in N$, so $N_1 N_2 N_3 \overset{5.1}{=} \{x \in K^\times : x^2 \in N\} = K^\times$.

We now assume all local degrees of L/K is either 1 or 2. Write

$$K_i = K(\sqrt{a_i}) \quad , \quad S_i = \{\text{primes of } K \text{ which split in } K_i\}.$$

We can assume $a_3 = a_2 a_1$ (they differ by a square). If $v \in S_1$, then $K_v(\sqrt{a_1}) = K_v$, so $K_v(\sqrt{a_3}) = K_v(\sqrt{a_2})$, implying $\frac{a_2}{a_3} \in (K_v^\times)^2 \subset N_{K_v^\times(\sqrt{x})/K_v^\times}$ for any $x \in K_v^\times$. Hence (by 2.4 and 2.6) $(a_3, x)_v = (a_3, x)_v \left(\frac{a_2}{a_3}, x\right)_v = (a_2, x)_v$ for any $v \in S_1$. Using similar arguments one gets

$$\prod_{v\in S_1} (a_2, x)_v = \prod_{v\in S_1} (a_3, x)_v$$

$$\prod_{v\in S_2} (a_3, x)_v = \prod_{v\in S_2} (a_1, x)_v$$

$$\prod_{v\in S_3} (a_1, x)_v = \prod_{v\in S_3} (a_2, x)_v .$$

Let us now show $\prod_{v\in S_1} (a_3, x)_v = \prod_{v\in S_2} (a_3, x)_v$, so by symmetry all six terms above are equal. But this is because

$$1 = \prod_{v\in \Sigma_K} (a_3, x)_v = \prod_{v \in S_1\cup S_2 \cup S_3} (a_3, x)_v \quad \text{by 6.2 } (G \text{ is abelian}; \#G^v = 1 \text{ or } 2)$$

$$\swarrow v \in S_3$$

$$= \prod_{v\in S_1\cup S_2} (a_3, x)_v \quad \text{as } a_3 = (\sqrt{a_3})^2 \text{ in } K_v = K_v(\sqrt{a_3})$$

$$= \prod_{v\in S_1} (a_3, x)_v \prod_{v\in S_2} (a_3, x)_v \prod_{v\in S_1\cap S_2} (a_3, x)_v$$

$$= \prod_{v\in S_1} (a_3, x)_v \prod_{v\in S_2} (a_3, x)_v \quad \text{as } \underset{\substack{\uparrow \\ K = K_1 K_2 .}}{S_1 \cap S_2 \subset S_3}$$

The above also tells us that $\prod_{v\in S_1} (a_3,x)_v \in \{\pm 1\}$, so one can define

$$\varphi(x) = \prod_{v \in S_1} (a_2,x)_v = \left(\begin{array}{c}\text{the other five}\\ \text{characterizations above}\end{array}\right) \in \{\pm 1\}, \quad x \in K^\times .$$

By 2.4 this implies $N_1 N_2 N_3 \subset \ker \varphi$. Using the notation of VII. 11.4, one has

$$\ker f = \frac{\{a \in K^\times : a \text{ is a local norm everywhere}\}}{\{a \in K^\times : a \text{ is a global norm}\}}, \quad \# \ker f = 2 .$$

Define

$$\begin{aligned} K^\times &\longrightarrow \ker f \\ x &\longmapsto x^2 , \end{aligned}$$

which makes sense as all local degrees are 1 or 2 (so $\# K_v^\times / N_{L^v/K_v}(L^{v\times}) \leq 2$, implying $[x^2] = [x]^2 = N_{L^v/K_v}(L^{v\times})$ for all v). By 5.1 one gets

$$K^\times / N_1 N_2 N_3 \hookrightarrow \ker f ,$$

so $\# K^\times / N_1 N_2 N_3 \leq 2$. Since $N_1 N_2 N_3 \subset \ker \varphi \subset K^\times$, we are reduced to showing that $\ker \varphi \neq K^\times$ (for this will imply $N_1 N_2 N_3 = \ker \varphi$). We use 2.16 : assuming there exists $v \in S_1 \setminus S_2$, $w \in S_3 \setminus (S_2 \cup S_1)$ such that

$$(a_2, -)_v \neq \mathrm{id} , \qquad (a_2, -)_w \neq \mathrm{id} ,$$

then 2.16 (together with 2.9) tells us that $\varphi(x) = \prod_{v \in S_1} (a_2, x)_v = -1$ for some v, giving $\ker \varphi \neq K^\times$. In fact, by symmetry we just need to show

$$\left(\exists \begin{array}{l} v \in S_1 \setminus S_2 \\ w \in S_3 \setminus (S_1 \cup S_2) \end{array}\right) \text{ or } \left(\exists \begin{array}{l} v \in S_2 \setminus S_3 \\ w \in S_1 \setminus (S_2 \cup S_3) \end{array}\right) \text{ or } \left(\exists \begin{array}{l} v \in S_3 \setminus S_1 \\ w \in S_2 \setminus (S_1 \cup S_3) \end{array}\right).$$

If this is not possible, then $\Sigma_{K_i,f} = S_i$ for some i, so by the Chebotarev density theorem $K_i = K$, a contradiction.

5.3. We first show that $L = \mathbb{Q}(\sqrt{13}, \sqrt{17})$ has local degree 1 or 2, by showing that one of 13, 17, $13 \cdot 17$ must be a square in $\mathbb{Q}_p$ for all p.

$\boxed{p \neq 2, 13, 17}$ Then $\left(\frac{13 \cdot 17}{p}\right) = \left(\frac{13}{p}\right)\left(\frac{17}{p}\right)$.

$\boxed{p = 2}$ As $17 \equiv 1$ (mod 2), $\left(\frac{17}{2}\right) = 1$

$\boxed{p = 13, 17}$ One has $\left(\frac{17}{13}\right) = 1$ and $\left(\frac{13}{17}\right) = 1$.

Now let x be a product of primes p with $\left(\frac{p}{13}\right) = -1$. By quadratic reciprocity $\left(\frac{13}{p}\right) = -1$. Since $K_1 = \mathbb{Q}(\sqrt{13})$ has discriminant d, we see that p is inert in K_1 (in particular, it is not split in K_1).

Letting $S = \{2, \infty\}$, by 2.8 if $p \notin S(17) = \{2, 17, \infty\}$,

$$(17, x)_p = \left(\frac{17}{p}\right)^{v_p(x)}.$$

Also as $17 \notin S$, as $17 \nmid x$ (so $v_{17}(x) = 0$),

$$(17, x)_{17} = \left(\frac{x^1}{17}\right) = \left(\frac{x}{17}\right).$$

We can now compute

$$\varphi(x) = \prod_{p \in S_1} (17, x)_p \quad , \quad S_1 = \left\{ p : \left(\frac{p}{13}\right) = 1 \right\} \cup \infty$$

As $17 > 0$, $(17, x)_\infty = 1$. Also, if $p \in S_1 \setminus \{17, \infty\}$, then $v_p(x) = 0$.

Hence $\varphi(x) = \left(\frac{x}{17}\right)$. (For example, $\varphi(5) = -1$, so $5 \notin \ker \varphi = \{x \in \mathbb{Q}^\times : x^2 \in N\}$. Thus 5^2 is not a global norm, but is a local norm as the local degrees of L are 1 or 2.)

5.4. Suppose $\mathrm{Gal}(L/K) = \mathbb{Z}/2 \times \mathbb{Z}/2$ with K having exactly one prime v of local degree 4. Let w be the prime of L above K.

We now show $\hat{H}^{-1}(G, L^\times) = 0$, $\hat{H}^{-1}(G, L_w^\times) = \mathbb{Z}/2\mathbb{Z}$. We will use diagrams from VII.11.2 to VII.11.4 without reference.

The short exact sequence $0 \to L^\times \xrightarrow{f} J_L \xrightarrow{g} C_L \to 0$ induces

$$\hat{H}^{-2}(G, J_L) \xrightarrow{g_2} H^{-2}(G, C_L) \to \hat{H}^{-1}(G, L^\times) \xrightarrow{f_1} \hat{H}^{-1}(G, J_L) \xrightarrow{g_1} \hat{H}^{-1}(G, C_L)$$

To show $\hat{H}^{-1}(G, L^\times) = 0$ it suffices to show that

- g_2 is surjective
- g_1 is injective.

Lemma: There is a commutative diagram

$$\begin{tikzcd}
\hat{H}^r(G, J_L) \cong \bigoplus\limits_{v \in \Sigma_K} H^r(G^v, (L^v)^\times) \arrow[rr, "g"] & & \hat{H}^r(G, C_L) \\
\hat{H}^r(G^w, (L^w)^\times) \arrow[u, hook, "i_w"] & & \hat{H}^{r-2}(G^w, \mathbb{Z}) = \hat{H}^{r-2}(G, \mathbb{Z}). \arrow[u, "\cong"', "u_{L/K}\cdot"] \arrow[ll, "\cong", "u_{L_w/K_w}\cdot"']
\end{tikzcd}$$

Proof. All the isomorphisms are established in VII, so we just need to show commutativity. To do this we use the diagram (from VII.11.2)

$$\begin{tikzcd}
\hat{H}^2(G, J_L) = \bigoplus\limits_{v \in \Sigma_K} H^2(G^v, (L^v)^\times) \arrow[r, "g"] \arrow[dr, "\mathrm{inv}"'] & \hat{H}^2(G, C_L) \arrow[d, "\beta_1"', "\cong"] \arrow[r, phantom, "\ni"] & u_{L/K} \arrow[d, mapsto] \\
 & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \frac{1}{n}
\end{tikzcd}$$

where $n = \# G$, and $\mathrm{inv}(u_{L/K}) = \frac{1}{n}$. Hence any element of $\hat{H}^2(G, J_L)$

that maps to $\frac{1}{n}$ under inv has image $u_{L/K}$ under g. In particular, as L^w/K_w has degree n, one sees that

$$g(1,\dots,1,u_{L^w/K_w},1,\dots) = u_{L/K}.$$

This gives commutativity. □

- Applying Lemma to $r=-2$ shows g_2 is surjective as the rightmost map is an isomorphism.
- Now apply Lemma to $r=-1$. Then, as G^v is cyclic for $v \neq w$, by Hilbert's Theorem 90 $\hat{H}^{-1}(G^v,(L^v)^\times) = \hat{H}^1(G^v,(L^v)^\times) = 0$. Thus i_w is also an isomorphism, implying g_1 is injective.

Next, to show $\hat{H}^{-1}(G, L_w^\times) = \mathbb{Z}/2\mathbb{Z}$ we use the facts that

$$\hat{H}^{-1}(G, L_w^\times) = \hat{H}^{-1}(G^w, L_w^\times) \cong \hat{H}^{-3}(G, \mathbb{Z})$$

and that

$$\hat{H}^{-3}(G,\mathbb{Z}) \times \underbrace{\hat{H}^{3}(G,\mathbb{Z})}_{\mathbb{Z}/2\mathbb{Z}} \longrightarrow \underbrace{\hat{H}^{0}(G,\mathbb{Z})}_{\mathbb{Z}/4\mathbb{Z}}$$

is a perfect pairing, to give us $\hat{H}^{-3}(G,\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

Finally, let $A = \{ x \in L^\times : N_{L/K}(x) = 1 \}$

$A_w = \{ x \in L_w^\times : N_{L_w/K_w}(x) = 1 \}$

$\overline{A} =$ closure of A in L_w.

Then, by definition of $\hat{H}^{-1}(G, A)$,

$$\hat{H}^{-1}(G, A) = \ker\left(A/\langle\sigma-1\rangle_{\sigma\in G}A \xrightarrow{\cdot\sum_{\sigma\in G}\sigma} A^G \right).$$

If $A = L^\times$, then $\hat{H}^{-1}(G, L^\times) = 0$ means that

$$A = (L^\times)^{e-1}(L^\times)^{\sigma-1}(L^\times)^{\tau-1},$$

and if $A = L_w^\times$, then $\hat{H}^{-1}(G, L_w^\times) = \mathbb{Z}/2\mathbb{Z}$ means that

$$\overline{A} = (L_w^\times)^{e-1}(L_w^\times)^{\sigma-1}(L_w^\times)^{\tau-1}$$

is of index 2 in A_w. Thus the elements of norm 1 in L are not dense in the elements of norm 1 in L_w.

One example is $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\zeta_8)$, where ζ_8 is an 8th root of unity. Then L is unramified outside 2, and totally ramified at 2.

6.1. If L and M are Galois over K, then so is LM. Now

$$\begin{aligned} \mathfrak{p} \in \mathrm{Spl}_s(LM/K) &\Leftrightarrow F_{LM/K}(\mathfrak{p}) = 1 \\ &\Leftrightarrow F_{LM/K}|_L(\mathfrak{p}) = 1 \quad \text{and} \quad F_{LM/K}|_M(\mathfrak{p}) = 1 \\ &\Leftrightarrow F_{L/K}(\mathfrak{p}) = 1 \quad \text{and} \quad F_{M/K}(\mathfrak{p}) = 1 \\ &\Leftrightarrow \mathfrak{p} \in \mathrm{Spl}_s(L/K) \cap \mathrm{Spl}_s(M/K). \end{aligned}$$

Therefore

$$\begin{aligned} L \subset M &\Leftrightarrow \mathrm{Spl}_s(M/K) \subset \mathrm{Spl}_s(L/K) \\ &\Leftrightarrow \mathrm{Spl}_s(LM/K) = \mathrm{Spl}_s(M/K) \quad \text{by above} \\ &\Leftrightarrow [LM:K] = [M:K] \quad \text{by Tchebotarev's density theorem} \\ &\Leftrightarrow L \subset M. \end{aligned}$$

Application Let S contain the primes $\mathfrak{p}$ such that

- $\mathfrak{p}$ is archimedean,
- $f \notin \mathcal{O}_{\mathfrak{p}}[x]$,
- f does not split in $\mathcal{O}/\mathfrak{p}$,
- $\mathfrak{p}$ divides $\mathrm{disc}(f)$.

Thus f has integral coefficients and unit discriminant in $\mathcal{O}_{\mathfrak{p}}[x]$ for any $\mathfrak{p} \notin S$, and also f splits in $\mathcal{O}/\mathfrak{p}$. Thus $\mathfrak{p}$ splits completely in the splitting field L of f for all $\mathfrak{p} \notin S$. Hence $\mathrm{Spl}_s(K) = \mathrm{Spl}_s(L)$, implying $K = L$ by above, and f splits into linear factors in $L = K$.

6.2. Let us show v has a split factor in E iff at least one conjugate of G^v is contained in H (the argument for the case v split completely is exactly the same as the one we present).

($\Rightarrow$) Let w_E in E be a split factor of v, so $G_{w_E/v} = 1$. Then all w in L above w_E has $\sigma \in G_{w/v}$ satisfying $\sigma|_E \equiv 1$, implying $G_{w/v} \subset H$.

($\Leftarrow$) Suppose w in L above v has $G_{w/v} \subset H$. Let w_E lie below w and above v. We want to show $G_{w_E/v} = 1$. Let $\sigma_E \in G_{w_E/v}$, and pick $\sigma \in G$ with $\sigma|_E = \sigma_E$. Writing $w' = \sigma(w)$, there exists $\tau \in \overbrace{\mathrm{Gal}(L/E)}^{=H}$ with $\tau(w') = w$, so $\tau\sigma(w) = w$. This implies $\tau\sigma \in G_{w/v}$, and $\sigma \in \tau^{-1} G_{w/v} \subset \tau^{-1} H = H$. Therefore $\sigma|_E \equiv 1$, and $G_{w_E/v} = 1$.

Now, we have (letting S contain the archimedean and ramified primes in L/k)

$$\begin{aligned} \mathrm{Spl}'_S(E/k) &= \{ v \notin S : v \text{ has a split factor in } E \} \quad \text{by definition} \\ &= \{ v \notin S : \rho^{-1} G^v \rho \subset H \text{ for some } \rho \in G \} \\ &= \{ v \notin S : F_{L/k}(v) \subset \bigcup_{\rho \in G} \rho H \rho^{-1} \} \quad \text{as } F_{L/k}(v) \text{ generates } G^v \end{aligned}$$

Thus, by Chebotarev's density theorem, $\mathrm{Spl}'_S(E/k)$ has density

$$\Big| \bigcup_{\rho \in G} \rho H \rho^{-1} \Big| \Big/ |G|. \quad \leftarrow \boxed{\text{OK as } S \text{ is a finite set}}$$

Notice $\bigcup_{\rho\in G} \rho H \rho^{-1} = \bigcup_{\rho\in G/H} \rho H \rho^{-1}$, so

$$\left|\bigcup_{\rho\in G} \rho H \rho^{-1}\right| \le |G/H|\,(|H|-1)+1 = |G|+1-\frac{|G|}{|H|} \le |G|.$$

Hence, if $\mathrm{Spl}'_S(E/k)$ has density 1, then $|H|=|G|$, implying $H=G$ and $E=K$.

Application Let S contain the primes $\mathfrak{p}$ such that

- $\mathfrak{p}$ is archimedean,
- $f \notin \mathcal{O}_{\mathfrak{p}}[x]$,
- $\mathfrak{p}$ divides $\mathrm{disc}(f)$,
- f has no roots mod $\mathfrak{p}$,
- $\mathfrak{p}$ divides the conductor of $E = K[x]/(f(x))$ over K.

Therefore, for all $\mathfrak{p}\notin S$, f has a root mod $\mathfrak{p}$, and $\mathfrak{p}$ decomposes in E based on the factorization of f mod $\mathfrak{p}$. In particular, all $\mathfrak{p}\notin S$ has a split factor in E, implying $\mathrm{Spl}'_S(E/k)$ has density 1. Thus $E=K$, and f has a root in K (in fact f is linear since it is irreducible).

Nonexample Let $a, b, ab \in K$ be nonsquares, so $f=(x^2-a)(x^2-b)(x^2-ab)$ has no roots in K. By quadratic reciprocity, two nonsquares in a finite field is always a square, so f always has solutions mod $\mathfrak{p}$.

6.3 Consider the permutation representations

$$\rho : G \to \mathrm{Aut}(\mathbb{C}[G/H]) \quad ; \quad \rho' : G \to \mathrm{Aut}(\mathbb{C}[G/H']).$$

We know that $\rho \cong \rho'$ iff $\chi_\rho = \chi_{\rho'}$. By definition

$$\chi_\rho(g) = \#\{ g'H \in G/H : gg'H = g'H \}$$

$$= \# \{ g'H \in G/H : g \in g'H(g')^{-1} \}$$

$$= \# \{ g' \in G : (g')^{-1} g g' \in H \} / \# H.$$

Since $\chi_\rho(1) = \frac{\# G}{\# H}$, $\rho \cong \rho'$ implies $\# H = \# H'$. One immediately sees that $\rho \cong \rho'$ iff each conjugacy class of G meets H and H' in the same number of elements. If H is a normal subgroup of G, then $\chi_\rho = \frac{\# G}{\# H} \cdot 1_H$, so necessarily $H = H'$.

6.4. We need to prove the following

Claim: Let $K/\mathbb{Q}$ be a finite extension and let L be a Galois extension containing K. Write $G = \mathrm{Gal}(L/\mathbb{Q})$, $H = \mathrm{Gal}(L/K)$,

$$\begin{tikzcd} L \arrow[d, dash, "H"] \arrow[ddd, dash, bend right=60, "G"'] \\ K \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

and let $\rho : G \to \mathrm{Aut}(\mathbb{C}[G/H])$ be the permutation representation of H, with χ its character. Then, for all primes p of $\mathbb{Q}$ unramified in N, its decomposition type (the residue degrees f_i) is uniquely determined by χ.

To prove this, we make use of the following fact.

Theorem. With setup as above, the following are equivalent.

(i) $\mathfrak{p}$ has decomposition type $(f_1, \ldots, f_r)$ in K.

(ii) If one writes $K = \mathbb{Q}(a)$, then the Frobenius F of any prime of N over $\mathfrak{p}$ has cycle type $(f_1, \ldots, f_r)$ when restricted to acting on the conjugates of a inside N.

Proof. Let $\mathfrak{D}$ be a prime of N above $\mathfrak{p}$, and let $\mathfrak{P}_\sigma = \mathfrak{D}^\sigma \cap K$ for any $\sigma \in G$. Then

$$\begin{aligned}
\mathfrak{P}_\sigma = \mathfrak{P}_{\sigma'} &\Leftrightarrow \mathfrak{D}^\sigma \text{ and } \mathfrak{D}^{\sigma'} \text{ are conjugate in } K \\
&\Leftrightarrow \sigma^{-1}\tau\sigma' \in G_{\mathfrak{D}/\mathfrak{p}} \text{ for some } \tau \in Gal(L/K) \\
&\Leftrightarrow \sigma^{-1}\tau\sigma' = F^m \text{ for some } m \in \mathbb{Z} \\
&\Leftrightarrow \sigma^{-1}(a) = F^m(\sigma')^{-1}(a) \\
&\Leftrightarrow \sigma'(a) \text{ and } (\sigma')^{-1}(a) \text{ is in the same orbit under } F
\end{aligned}$$

Therefore the number of primes in K lying over $\mathfrak{p}$ is equal to the number of cycles in F. It now suffices to show that

$$F^m\sigma(a) = \sigma(a) \Leftrightarrow f_{\mathfrak{P}_\sigma/\mathfrak{p}} \text{ divides } m.$$

But this is because

$$\begin{aligned}
\sigma^{-1}F^m\sigma \in Gal(L/K) &\Leftrightarrow (F^\sigma)^m \in Gal(L/K) \cap G_{\mathfrak{D}^\sigma/\mathfrak{p}} = G_{\mathfrak{D}^\sigma/\mathfrak{P}} \\
&\Leftrightarrow (F^\sigma)^m \in \langle F_{N/K}(\mathfrak{D}^\sigma) \rangle = \langle (F^\sigma)^{f_{\mathfrak{P}_\sigma/\mathfrak{p}}} \rangle \\
&\Leftrightarrow f_{\mathfrak{P}^\sigma/\mathfrak{p}} \text{ divides } m. \quad \square
\end{aligned}$$

With this theorem, it suffices to show the cycle type of F acting on G/H is determined by χ, for G/H can be identified with the conjugates of a in L. But this is now clear, since for a cycle σ of F,

$\chi(g) \cdot \sigma =$ number of points fixed by permutations of elements in σ

7.1. Let $\varphi : I^S \to H$ be admissible. By VII. 4.1. there is a continuous $\gamma : C_K \to H$ such that $\gamma(x) = \varphi((x)^S)$ for all $x \in J_K^S$.

As H is discrete, $\ker(\gamma)$ is open, and of finite index as H is finite.

Thus the existence theorem gives us a finite abelian L/K satisfying

$N_{L/K} C_L = \ker \gamma$ and $\psi_{L/K} : C_K/\ker\gamma \xrightarrow{\cong} \mathrm{Gal}(L/K)$.

Let $v \notin S$. Then, for all $x \in U_v$, $\varphi((x)^S) = 1 = \gamma(x)$. Thus $i_v(U_v)$ lies in $\ker(\gamma) = N_{L/K} C_L$, implying v is unramified (see exercise 3).

Now define $\alpha = \gamma \circ \psi_{L/K}^{-1} : \mathrm{Gal}(L/K) \longrightarrow H$, which is injective.

$$\begin{tikzcd} \mathrm{Gal}(L/K) \arrow[r] \arrow[dr] & H \\ & C_K/\ker\gamma \arrow[u] \end{tikzcd}$$

If $\mathfrak{a} \in I^S$, write $\mathfrak{a} = (x)^S$ for some $x \in J_K^S$. Then

$$\varphi(\mathfrak{a}) = \gamma((x)^S) = \alpha \circ \psi_{L/K}((x)^S)$$

$$= \alpha\left(F_{L/K}((x)^S)\right) = \alpha\left(F_{L/K}(\mathfrak{a})\right).$$

7.2. By injectivity of α, this implies $F_{L/K}(v) \equiv 1$ for all v in the set of density 1. But Chebotarev's Density Theorem tells us such v has density $\frac{1}{\#\mathrm{Gal}(L/K)}$, implying $L = K$, and $\alpha \equiv 1$. Thus $\varphi \equiv 1$.

Thus, two admissible maps $I^S \to H$ that agrees on a set of primes of density one are equal.

7.3. By 7.2 one has $\alpha' \circ F_{L/K} = \varphi = \alpha \circ F_{L/K}$.

Let $M = LL'$. Then, by VII.3.2.,

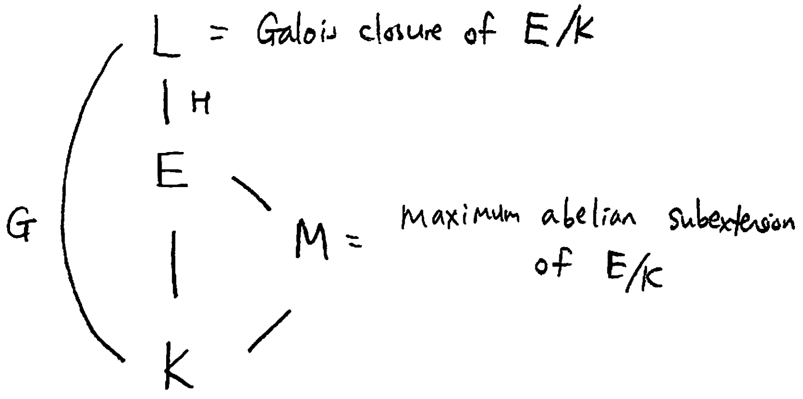
$$\begin{tikzcd} I^S \arrow[r, "F_{M/K}"] \arrow[d, "\parallel"'] & Gal(M/K) \arrow[d, "r_{\mathcal{L}}"] & \\ I^S \arrow[r, "F_{L/K}"] & Gal(\mathcal{L}/K) \arrow[r, "\alpha_{\mathcal{L}}"] & H \end{tikzcd}$$

, $\mathcal{L} = L$ or L', $\alpha_L = \alpha$, $\alpha_{L'} = \alpha'$.

Hence $\alpha_L \circ r_L \circ F_{M/K} = \alpha_{L'} \circ r_{L'} \circ F_{M/K}$. Since $F_{M/K}$ is surjective (by Chebotarev's density theorem) and $\alpha_{\mathcal{L}}$ is injective, this implies $\ker r_L = Gal(M/L)$ and $\ker r_{L'} = Gal(M/L')$ are equal, and so $L = L'$. Thus $r_{\mathcal{L}} \equiv 1$, and $\alpha_L \circ F_{M/K} = \alpha_{L'} \circ F_{M/K}$. By surjectivity of $F_{M/K}$, one gets

$$\begin{matrix} \alpha_L & = & \alpha_{L'} \\ \parallel & & \parallel \\ \alpha & & \alpha' \end{matrix}.$$

8. Our setup is the following:


L = Galois closure of E/K
H
E
G
M = maximum abelian subextension of E/K
K

By the compatibility of the Artin map, one has

$$\begin{tikzcd}
H^{ab} \arrow[r, "\cong"] \arrow[d, "\vartheta"'] & C_E/N_{L/E}C_L \arrow[d, "N_{E/K}"] \\
G^{ab} \arrow[r, "\cong"] & C_K/N_{L/K}C_L
\end{tikzcd}$$

, $C_? = J_?/?^*$

Since $G^{ab}/\vartheta(H^{ab}) = \mathrm{Gal}(M/K) = C_K/N_{M/K}C_M$ and

$$\frac{C_K/N_{L/K}C_L}{N_{E/K}C_E/N_{E/K}N_{L/E}C_L} = C_K/N_{E/K}C_E ,$$

the above diagram tells us

$$C_K/N_{M/K}C_M = C_K/N_{E/K}C_E ,$$

so $N_{M/K}C_M$ and $N_{E/K}C_E$ has the same index in C_K. But $N_{E/K} = N_{M/K}N_{E/M}$, so $N_{E/K}C_E \subset N_{M/K}C_M$, and

$$N_{E/K}C_E = N_{M/K}C_M .$$