CASSELS-FRÖLICH SOLUTIONS AND CONTEXT

COLIN NI

Abstract. The Cassels and Frölich book on class field theory offers eight wonderful exercises in the back of the book. Here are my solutions to some of them, as well as some exposition on the context and importance of them.

Exercise 1: The Power Residue Symbol

Quadratic reciprocity exhibits an algorithm for computing whether a number is a square mod p. It was a main source of inspiration for a vast amount of number theory, and there are hundreds of published proofs of quadratic reciprocity. Serre proves it in his class *A Course in Arithmetic* using not much more than the basic properties of fields. Class field theory can be seen as a vast generalization of this reciprocity law and others, and this exercise shows how it specializes to quadratic reciprocity.

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 $a_1, \dots, a_r$ are elements of K^*, we let $S(a_1, \dots, a_r)$ 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 $L = K(\sqrt[m]{a})$.

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

Solution. Recall $F_{L/K}$ is a map into $\mathrm{Gal}(L/K) = \mu_m$ given by

$$(r + s\sqrt[m]{a})^{F_{L/K}(\mathfrak{b})} = r + sF_{L/K}(\mathfrak{b})\sqrt[m]{a},$$

so

$$\left(\frac{a}{\mathfrak{b}}\right) = \frac{(\sqrt[m]{a})^{F_{L/K}(\mathfrak{b})}}{\sqrt[m]{a}} = F_{L/K}(\mathfrak{b}) = \text{an } m\text{th root of 1.}$$

Moreover it is independent of the choice of $\sqrt[m]{a}$ since

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

for any $\xi \in \mu_m$. □

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

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

Solution. To use VII, §3.2, we first need to show that $S(a,a')$ contains those primes ramified in L'. Let $\mathfrak{p} \notin S(a,a')$ so that $\mathfrak{p} \nmid a, a', m$. By Lemma 5 in II, §3, the prime $\mathfrak{p}$ is unramified in $L = K(\sqrt[m]{a})$. Moreover if $\mathfrak{P} \mid \mathfrak{p}$, then since $\mathfrak{P} \cap K = \mathfrak{p}$ we have that $\mathfrak{P} \nmid a', m$. Then by the same Lemma $\mathfrak{P}$ is unramified in $L' = K(\sqrt[m]{a}, \sqrt[m]{a'})$. The same holds for $L = K(\sqrt[m]{aa'})$ and $L = K(\sqrt[m]{a'})$. Thus VII, §3.2 gives the following diagram

$$\begin{array}{ccc} I^{S(a,a')} & \xrightarrow{F_{L'/K}} & \mathrm{Gal}(L'/K) \\ {\scriptstyle N_{K/K}=\mathrm{id}}\downarrow & & \downarrow{\scriptstyle \text{restriction}} \\ I^{S(a,a')} & \xrightarrow{F_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

which holds for the three instances of L.

Thus if $\mathfrak{b} \in I^{S(a,a')}$, then applying the diagram three times gives

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

□

Exercise 1.3. Show

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

Hence

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

Solution. At once

$$\begin{aligned} \left(\frac{a}{\mathfrak{b}\mathfrak{b}'}\right) \sqrt[m]{a} &= \left(\sqrt[m]{a}\right)^{F_{L/K}(\mathfrak{b}\mathfrak{b}')} \\ &= \left(\sqrt[m]{a}\right)^{F_{L/K}(\mathfrak{b})F_{L/K}(\mathfrak{b}')} \\ &= \left(\left(\frac{a}{\mathfrak{b}}\right) \sqrt[m]{a}\right)^{F_{L/K}(\mathfrak{b}')} \\ &= \left(\frac{a}{\mathfrak{b}}\right) \left(\sqrt[m]{a}\right)^{F_{L/K}(\mathfrak{b}')} \qquad \left(\left(\tfrac{a}{\mathfrak{b}}\right) \in \mu_m \subset K \text{ by Exercise 1.1}\right) \\ &= \left(\frac{a}{\mathfrak{b}}\right)\left(\frac{a}{\mathfrak{b}'}\right) \sqrt[m]{a}. \end{aligned}$$

The formula for $\left(\frac{a}{\mathfrak{b}}\right)$ follows immediately. □

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

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

Solution. Since $v \notin S(a)$, we have $\mathfrak{p}_v \nmid m$, so $x^m - 1$ is separable in $k(v) = \mathfrak{o}_v/\mathfrak{p}_v$. The multiple roots of this polynomial are those of

$$\gcd(x^m - 1, mx^{m-1}) = 1,$$

so there are none. Thus the mth roots of unity μ_m are all distinct in $k(v)^*$, which implies

$$m = |\mu_m| \mid |k(v)^*| = Nv - 1.$$

By definition of the Frobenius element

$$x^{F_{L/K}(v)} \equiv x^{Nv} \pmod{\mathfrak{p}_v} \quad \text{for } x \in \mathfrak{o}_v.$$

Therefore

$$\left(\frac{a}{v}\right) = \frac{(\sqrt[m]{a})^{F_{L/K}(v)}}{\sqrt[m]{a}} \equiv \frac{\sqrt[m]{a}^{Nv}}{\sqrt[m]{a}} = a^{\frac{Nv-1}{m}} \pmod{\mathfrak{p}_v} \qquad \square.$$

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 $x \in K_v$.

Solution. For (*i*) $\Leftrightarrow$ (*ii*), we first use the fact that $k(v)^*$ is cyclic of order $Nv - 1$ to write

$$k(v)^* = \{x, x^2, \ldots, x^{Nv-1}\}.$$

Since $m \mid (Nv - 1)$ by Exercise 1.4, we have the exact sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & k(v)^{*m} & \longrightarrow & k(v)^* & \longrightarrow & \mu_m & \longrightarrow & 1 \\ & & & & z & \longmapsto & z^{\frac{Nv-1}{m}} & & \end{array}.$$

Thus using the identity

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

from Exercise 1.4, we have $\left(\frac{a}{v}\right) = 1$ in $k(v)$ if and only if $x^m \equiv a \pmod{\mathfrak{p}_v}$ is solvable. It remains to remark that

$$\left(\frac{a}{v}\right) \in \mu_m \subset K$$

ensures $\left(\frac{a}{v}\right) = 1$ in K and that we can always lift x to $\mathfrak{o}_v$.

For (*ii*) $\Leftrightarrow$ (*iii*), first assume we have a solution $x \in K_v$ for $x^m = a$. Then

$$v(x) = \frac{1}{m} v(a) = 0$$

since $v(a) = 0$, so $x \in \mathfrak{O}_v$. Now v is non-archimedean since S contains the archimedean primes, so

$$k(v) = \mathfrak{o}_v/\mathfrak{p}_v \cong \mathfrak{O}_v/\mathfrak{P}_v$$

gives a solution in $\mathfrak{o}_v$. For the converse, we use Hensel's lemma. Put

$$f(z) = z^m - a$$

so that $f'(z) = mz^{m-1}$. We have $f(x) = 0 \pmod{\mathfrak{p}_v}$ and so $|f(x)|_v < 1$, and we have

$$|f'(x)|_v = |mx^{m-1}|_v = |x|_v^{m-1} = 1$$

since $v(x) = 0$. Thus

$$|f(x)|_v < 1 = |f'(x)|_v^2,$$

so by Hensel's lemma $x \in \mathfrak{o}_v$ lifts to a solution in the completion K_v. □

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

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

Solution. The case $\mathfrak{b}$ prime is covered by Exercise 1.4 since $\mu_m \hookrightarrow k(v)$. For general

$$\mathfrak{b} = \sum n_v v,$$

define r_v via $Nv = 1 + mr_v$ using that $m \mid (Nv - 1)$ as in Exercise 1.4. One easily checks that

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

so

$$\frac{N\mathfrak{b} - 1}{m} \equiv \sum n_v \frac{Nv - 1}{m} \pmod{m^2}.$$

Thus

$$\left(\frac{\zeta}{\mathfrak{b}}\right) = \prod_v \left(\frac{\zeta}{v}\right)^{n_v} = \prod_v \zeta^{\frac{Nv-1}{m} \cdot n_v} = \zeta^{\sum_v \frac{Nv-1}{m} n_v} = \zeta^{\frac{N\mathfrak{b}-1}{m}}$$

since $\zeta \in \mu_m$ and so the powers work mod m. □

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

Solution. By Exercise 1.3 it suffices to work with $\mathfrak{b} = v$ prime. Now note $\mathfrak{b} \subset \mathfrak{p}_v$ since $\mathfrak{b}$ is integral, and Exercise 1.4 guarantees $\left(\frac{a}{v}\right)$ is well defined mod $\mathfrak{p}_v$. Again $\mu_m \hookrightarrow k(v)$, so this ensures it is well defined in K. □

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 $c \equiv 1 \pmod{\mathfrak{p}_v}$.

Solution. By Exercise 1.3 it suffices to show that

$$\left(\frac{a}{(c)^{S(a)}}\right) = 1$$

for such c, but the crude form of the reciprocity law [cf VII, §3.3, esp second half] immediately ensures

$$F_{L/K}((c)^{S(a)}) = 1.$$

□

Exercise 1.9. Specialize now to the case $K = \mathbb{Q}$ and $m = 2$. 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 satisfied

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

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

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

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

Solution. Exercise 1.1 gives the definition, 1.2 and 1.3 multiplicativity, and 1.7 the first identity.

For the second identity, it suffices by Exercise 1.8 to show that PQ^{-1} is a square mod p for every prime p dividing a and $p = 2$. Recall the following facts about squares in p-adic fields. A number is a square in $\mathbb{Q}_2^*$ if and only if it is of the form $2^{2n}u$ where $u \equiv 1 \pmod 8$ [cf Arithmetic II, Thm 4]. For p odd, a number is a square in $\mathbb{Q}_p^*$ if and only if it is of the form $p^{2n}u$ where the map $\mathbb{Z}_p^* \to \mathbb{F}_p^*$ takes u to a square. Therefore if

$$P \equiv Q \pmod{8a_0},$$

then PQ^{-1} is a square in $\mathbb{Q}_2^*$ since $PQ^{-1} \equiv 1 \pmod 8$ and in $\mathbb{Q}_p^*$ for p dividing a since $PQ^{-1} \equiv 1 = \text{a square} \pmod p$. □

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

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

Indeed the formula $(*)$ above allows one to calculate $\left(\frac{a}{P}\right)$ as a 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. Now given arbitrary relatively prime P and Q, one can find R such that $RP \equiv Q \pmod 8$ and $(R, Q) = 1$, 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 the P argument in $\langle P, Q\rangle$ depends only the mod 8 residue class. 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 the Q argument in $\langle P, Q\rangle$ depends only on the mod 8 residue class. We are therefore reduced to a small finite number of cases, which we leave to the reader to check.

Solution. It suffices to reduce this problem to a finite number of computations because these are easily checked.

By Exercise 1.9 $\left(\frac{-1}{P}\right)$ and $\left(\frac{2}{P}\right)$ depend only on $P \pmod 8$, so there are four residue classes to check for each case, a finite number in total.

Suppose $P \equiv Q \pmod 8$. Writing $Q = P + 8a$ for some a, we find using Exercise 1.9 that

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

Thus

$$\langle P, Q\rangle = \left(\frac{P}{Q}\right)\left(\frac{-P}{Q}\right) = \left(\frac{P^2}{Q}\right)\left(\frac{-1}{Q}\right) = \left(\frac{-1}{Q}\right).$$

Since $\langle P, Q\rangle$ depends only on the mod 8 residue class in each variable, there are 16 cases to check, a finite number. □

Exercise 3: The Hilbert Class Field

Let L/K be a global abelian extension, v a prime of K, and $i_v\colon K_v^* \to J_K$ 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 that 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.

Solution. Put $n = [L : K] = \mathrm{Gal}(L/K)$. Recall that the injection $G_v \hookrightarrow \mathrm{Gal}(L_v/K_v)$ of the decomposition group of v is an isomorphism, so

$$n_v = n/g_v = e_v f_v g_v / g_v = e_v f_v.$$

Now v splits completely in L if and only if $e_v f_v = 1$, and by what we have seen this is equivalent to $n_v = |G_v| = 1$. Since the local Artin map $\psi_v\colon K_v^* \twoheadrightarrow G_v$ is surjective and since $\psi_{L/K} i_v = \psi_v$, by VII, §6.3, this is equivalent to $\psi_{L/K} i_v = 1$. This just means

$$i_v(K_v^*) \subset \ker \psi_{L/K} = K^* N_{L/K} J_L$$

by class field theory.

Similarly v is unramified in L if and only if $L_v \subset L_{v,\mathrm{nr}}$ if and only if $\mathrm{Gal}(L_v/L_{v,\mathrm{nr}}) = 1$ if and only if

$$\psi_{L/K} i_v = \psi_v\colon U_v \twoheadrightarrow \mathrm{Gal}(L_v/L_{v,\mathrm{nr}})$$

is trivial if and only if

$$i_v(U_v) \subset \ker \psi_{L/K} = K^* N_{L/K} J_L. \qquad \square$$

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. 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 $\mathrm{Gal}(K'/K)$. Thus the degree $[K' : K]$ is equal to the class number $h_K = |H_K|$ of K.

Solution. The surjection

$$\begin{aligned} J_K &\longrightarrow I_K \\ x &\longmapsto \textstyle\prod_{v \notin S} \mathfrak{p}_v^{v(x)} \end{aligned}$$

has kernel J_K^S, so we have $J_K/J_K^S \cong I_K$. Moreover since K^* maps to the principal ideals, this induces a surjection

$$C_K = J_K/K^* \twoheadrightarrow I_K/P_K = H_K$$

with kernel $K^* J_{K,S}$.

Thus the existence theorem [cf VII, §5.1] produces the desired class field to the group $K^*J_{K,S}$: the above shows $K^*J_{K,S}$ has finite index in C_K because the class number h_K is always finite, and it is certainly open. Moreover then by construction the Artin map $\psi_{K'/K}\colon C_K \to \mathrm{Gal}(K'/K)$ induces

$$H_K \cong \frac{C_K}{K^*J_{K,S}} \cong \mathrm{Gal}(K'/K). \qquad \square$$

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 $F_{K'/K}(\mathfrak{a}) = 1$.

Solution. All primes $\mathfrak{p}_v$ are unramified in K' and so $e_v = 1$, and the Frobenius element of such a prime $\mathfrak{p}_v$ has order f_v and so splits completely into $g_v = n_v/f_v$ factors. In particular an arbitrary ideal $\mathfrak{a}$ of K is principal if and only if $\mathfrak{a} = 1 \in P_K$ if and only if

$$F_{K'/K}(\mathfrak{a}) = 1 \in \mathrm{Gal}(K'/K)$$

if and only if $f_v = 1$ if and only if it splits completely. $\square$

The first five (sorted by discriminant) imaginary quadratic fields with class numbers $\neq 1$ 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.

Solution. The five imaginary quadratic fields are $K = \mathbb{Q}(\sqrt{-15}), \mathbb{Q}(\sqrt{-5}), \mathbb{Q}(\sqrt{-23}), \mathbb{Q}(\sqrt{-6}), \mathbb{Q}(\sqrt{-31})$. Since there is only one archimedean prime which is already complex hence split completely, all there is to do is to check that every prime in K is unramified in K'. Let us describe two ways of doing this: one way using discriminants and the other using some basic algebraic number theory.

The first way is to show that the relative discriminant $\mathfrak{d}(K'/K)$ is ± 1 [cf Cor 1 to Thm 1 in I, §5]. To compute this relative discriminant, we use the tower formula [cf Prop 7 in I, §4]:

$$\mathfrak{d}(K') = \mathfrak{d}(K)^{[K':K]} N_K \mathfrak{d}(K'/K).$$

For the discriminant -15, -20, and -24 cases we can do this by hand. For example for the -15 case the claim is that

$$K' := \mathbb{Q}(\sqrt{-15}, \sqrt{-3})$$

is its Hilbert class field. It is easy to check that $[K' : K] = 2$, and it is easy to compute the norm

$$N_K(a + b\sqrt{-15}) = a^2 + 15b^2.$$

Since clearly only ± 1 can have norm 1, it is enough to show that

$$\frac{\mathfrak{d}(K')}{\mathfrak{d}(K)^2} = \pm 1.$$

For this case we can use the following fact: if K_1K_2 is a number field composed up number fields K_1 and K_2 which have relatively prime discriminants and are such that

$$[K_1K_2 : \mathbb{Q}] = [K_1 : \mathbb{Q}][K_2 : \mathbb{Q}],$$

then

$$\mathfrak{d}(K_1K_2) = \mathfrak{d}(K_1)^{[K_2:\mathbb{Q}]} \mathfrak{d}(K_2)^{[K_1:\mathbb{Q}]}.$$

Here

$$K' = \mathbb{Q}(\sqrt{-15}, \sqrt{-3}) = \mathbb{Q}(\sqrt{5})\mathbb{Q}(\sqrt{-3})$$

is composed of two fields $K_1 = \mathbb{Q}(\sqrt{5})$ and $K_2 = \mathbb{Q}(\sqrt{-3})$ which have

$$(\mathfrak{d}(K_1), \mathfrak{d}(K_2)) = (5, -3) = 1$$

and are such that

$$[K' : \mathbb{Q}] = 4 = [K_1 : \mathbb{Q}][K_2 : \mathbb{Q}].$$

Thus

$$\mathfrak{d}(K') = 5^2 \cdot (-3)^2 = 225,$$

and we are done. Similarly for the discriminant -20 case we have

$$K' = \mathbb{Q}(\sqrt{-5}, \sqrt{-1}) = \mathbb{Q}(\sqrt{5})\mathbb{Q}(\sqrt{-1})$$

which have relatively prime discriminants 5 and -4, so

$$\mathfrak{d}(K') = 5^2 \cdot (-4)^2.$$

And again similarly for the discriminant -24 case we have

$$K' = \mathbb{Q}(\sqrt{-6}, \sqrt{-3}) = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{-3})$$

which have relatively prime discriminants 8 and -3, so

$$\mathfrak{d}(K') = 8^2 \cdot (-3)^2.$$

For the remaining two cases we can use Sage. For the discriminant -23 case we can use

```
K.<a> = NumberField(x**2 + 23)
L.<b> = K.extension(x**3 - x - 1)
print(L.absolute_discriminant())
print(K.absolute_discriminant())
```

which prints -12167 and -23 where now $[K' : K] = 3$, and in fact we can check that

```
print(L.relative_discriminant())
```

prints `Fractional ideal (1)`. Similarly for the discriminant -31 case.

Alternatively, we can use some basic algebraic number theory, which we now recall. Consider a Galois extension L/K and a prime $\mathfrak{P}$ lying over another $\mathfrak{p}$ with

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^e \cdots \mathfrak{P}_g^e$$

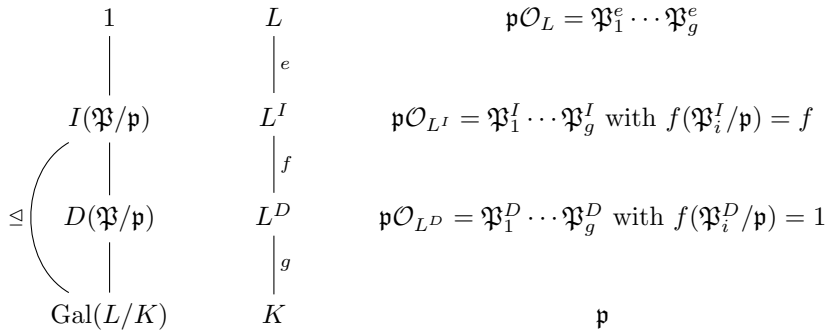
and with residue degree f. We have the decomposition subgroup

$$D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

and the inertia subgroup

$$I(\mathfrak{P}/\mathfrak{p}) = \ker(D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))).$$

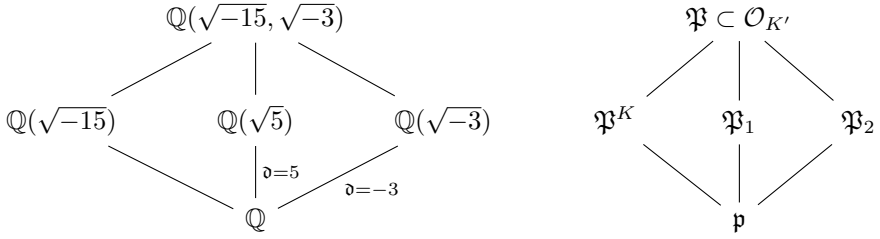
These separate out the splitting behavior of $\mathfrak{p}$ into factors of $\mathfrak{P}$ in the following sense:



In fact, we have the following uniqueness. For $L/F/K$ an intermediate field, denote $\mathfrak{P}^F = \mathfrak{P} \cap F$. Then

- L^D is the largest intermediate field such that $e(\mathfrak{P}^F/\mathfrak{p}) = f(\mathfrak{P}^F/\mathfrak{p}) = 1$
- L^D is the smallest intermediate field such that $\mathfrak{P}$ is the only prime lying over $\mathfrak{P}^F$
- L^I is the largest intermediate field such that $e(\mathfrak{P}^F/\mathfrak{p}) = 1$
- L^I is the smallest intermediate field such that $\mathfrak{P}$ is totally ramified over $\mathfrak{p}$

Let us use this separation behavior of the inertia subgroup to attack the discriminant -15, -20, and -24 cases. For the -15 case, we have the following subfields:



Suppose $\mathfrak{P}^K$ ramifies in K' so that

$$e(\mathfrak{P}/\mathfrak{P}^K) = 2$$

for some $\mathfrak{P}$. Let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be the primes lying below $\mathfrak{P}$ in the other two subfields. Note $e(\mathfrak{P})$ cannot be 4 since then $\mathfrak{p}$ would need to ramify in both $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-3})$, which is impossible due to the shown discriminants which are relatively prime. Thus

$$e(\mathfrak{P}^K) = 1,$$

and so K is the field corresponding to the inertia subgroup $I(\mathfrak{P}/\mathfrak{p})$. It follows from the separation behavior that

$$e(\mathfrak{P}/\mathfrak{P}_1) = e(\mathfrak{P}/\mathfrak{P}_2) = 1$$

and

$$e(\mathfrak{P}_1) = e(\mathfrak{P}_2) = 2,$$

but this is impossible again because of the discriminants.

The same argument works for the other two cases, but we need to check that the discriminants are still relatively prime. For the discriminant -20 case we have $K = \mathbb{Q}(\sqrt{-5})$ and

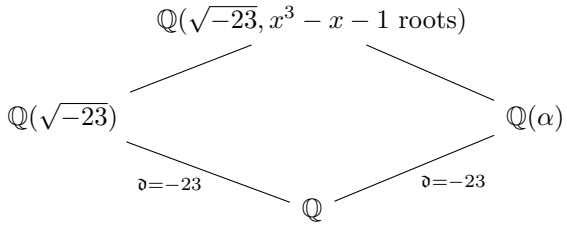
$$K' = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$$

with the other two intermediate fields being $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-1})$ which have relatively prime discriminants 5 and -4. Similarly for the discriminant -24 case we have $K = \mathbb{Q}(\sqrt{-6})$ and

$$K' = \mathbb{Q}(\sqrt{-6}, \sqrt{-3})$$

with the other two intermediate fields being $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-3})$ which have relatively prime discriminants 8 and -3.

For the remaining discriminant -23 and -31 cases we can check for ramification by hand. For the -23 case we have the following subfields:



where α is a root of $x^3 - x - 1$. Here the discriminant of $\mathbb{Q}(\alpha)/\mathbb{Q}$ is -23 because that is the discriminant $-4 \cdot (-1)^3 - 27 \cdot (-1)^2$ of the polynomial $x^3 - x - 1$. Let $\mathfrak{P}^K$ be a prime in $\mathbb{Q}(\sqrt{-23})$ that ramifies in K'. Since

$$\{1, \alpha, \alpha^2\}$$

is a K-basis of K' with discriminant -23, we must have

$$\mathfrak{P}^K \mid -23.$$

Thus $\mathfrak{P}^K = (\sqrt{-23})$. It suffices to find three primes in K' that contain $\sqrt{-23}$ since then $\mathfrak{P}^K$ cannot ramify. Computing the factorization of (23) in $\mathbb{Q}(\alpha)$, we obtain

$$(23) = (23, \alpha - 2)(23, \alpha - 10)^2 \mathcal{O}_{\mathbb{Q}(\alpha)}$$

since

$$x^3 - x - 1 \equiv (x - 2)(x - 10)^2 \pmod{23}.$$

One prime in K' lies above $(23, \alpha - 2)$, so it remains to find two primes in K' that lie above $(23, \alpha - 10)$. But we have

$$(23) = (-23) = (\alpha^3 - \alpha - 24) = (\alpha - 3)\left(\frac{-3 \pm \sqrt{-23}}{2}\right) \subset \mathcal{O}_{K'},$$

so

$$(23, \alpha - 10) \subset \left(\frac{-3 \pm \sqrt{-23}}{2}, \alpha - 10\right) \subset \mathcal{O}_{K'},$$

as desired. The same argument works for the discriminant -31. We check that the discriminant of $x^3 + x - 1$ is $-4 \cdot 1^3 - 27 \cdot (-1)^2 = -31$, compute

$$(31) = (31, \alpha - 17)^2 (31, \alpha - 28) \subset \mathcal{O}_{\mathbb{Q}(\alpha)},$$

and then find two primes above $(31, \alpha - 17)$ by computing

$$(31) = (\alpha^3 + \alpha + 30) = (\alpha + 3)\left(\alpha - \frac{3 \pm \sqrt{-31}}{2}\right) \subset \mathcal{O}_{K'}. \qquad \square$$

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 ideles 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 from (a), where a is a totally positive element of K. Show that $F_{K_1/K}$ gives an isomorphism:

$$I_K/P_K^+ \cong \mathrm{Gal}(K_1/K).$$

Thus, $\mathrm{Gal}(K_1/K')$ 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.

Exercise 4: Numbers Represented by Quadratic Forms

The Hasse-Minkowski theorem patches together solutions in $\mathbb{Q}_p$ and $\mathbb{R}$ of a quadratic form to ensure a solution in $\mathbb{Q}$. For this reason it is called the local-global principal. Serre proves this theorem in his classic *A Course in Arithmetic* using mostly elementary means, except for one use of Dirichlet's deep theorem on arithmetic progressions. This exercises proves the local-global principal using class field theory.

Let K be a field of characteristic different from 2.

Exercise 4.1. The form $f = X^2$ does not represent 0.

Solution. This is because fields are integral domains. □

Exercise 4.2. The form $f = X^2 - bY^2$ represents 0 if and only if $b \in (K^*)^2$.

Solution. By definition $f = X^2 - bY^2$ represents 0 if and only if there exist $x, y \in K$ not both zero such that $x^2 = by^2$. Of course then $x, y \in K^*$, so

$$b = (x/y)^2 \in (K^*)^2.$$

Conversely we can set $(x, y) = (\sqrt{b}, 1)$. □

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 $K(\sqrt{b})$.

Solution. The norm of $K(\sqrt{b})$ is

$$N(s + t\sqrt{b}) = \prod_{\sigma \in \mathrm{Gal}(K(\sqrt{b})/K)} \sigma(s + t\sqrt{b}) = (s + t\sqrt{b})(s - t\sqrt{b}) = s^2 - t^2 b.$$

Thus if f represents 0, then there exists $x, y, z \in K$ not all zero such that $cz^2 = x^2 - by^2$, whence

$$c = (x/z)^2 - b(y/z)^2 = N(x/z + (y/z)\sqrt{b}).$$

Conversely if $c = s^2 - t\sqrt{b}$, then there is the solution $(x, y, z) = (s, t, 1)$. □

Theorem (Hilbert Theorem 90)**.** *If $G = G(E/F)$ is finite cyclic with generator g and $a \in E^*$ is such that $N_{E/F} = 1$, then there exists $b \in E^*$ such that $a = b/g(b)$.*

Proof. V, §2.7. □

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 an 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 $K(\sqrt{ab})$.

Solution. Following the hint, we may obviously assume neither a nor b is a square in K.

For $(i) \Leftrightarrow (ii)$, note (i) if and only if there

$$c(z^2 - at^2) = x^2 - by^2$$

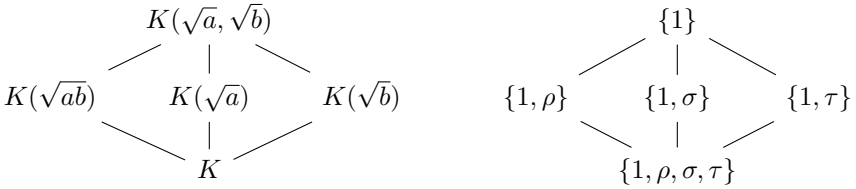
for some x, y, z, t. But inverses of norms are norms, so

$$c = (x^2 - by^2)/(z^2 - at^2)$$

expresses c in the form described in (ii). The converse is just like as before.

For $(iii) \Leftrightarrow (iv)$, we apply Exercise 4.3 with the base field $K(\sqrt{ab})$. Spelling it out, we have that $X^2 - bY^2 - cZ^2$ represents 0 in the field $K(\sqrt{ab})$ if and only if c, as an element of $K(\sqrt{ab})$, is a norm from the extension field $K(\sqrt{ab})(\sqrt{b}) = K(\sqrt{a}, \sqrt{b})$.

For the remainder of this solution, we will show $(ii) \Leftrightarrow (iii)$. We use the following Galois correspondence of $K(\sqrt{a}, \sqrt{b})$ where for instance $\sqrt{ab}$ is fixed by ρ by definition:



We first rewrite (ii) and (iii). Note (ii) is equivalent to

(ii'): there exists $x, y \in L$ such that $x^\sigma = x, y^\tau = y,$ and $x^{1+\rho} y^{1+\rho} = c$.

Indeed by the diagram $x^\sigma = x$ means $x \in K(\sqrt{a})$, $y^\tau = y$ means $y \in K(\sqrt{b})$, and

$$x^{1+\rho} = N_{K(\sqrt{a})/K} x$$

and

$$y^{1+\rho} = N_{K(\sqrt{b})/K} y.$$

Similarly note (iii) is equivalent to

(iii'): there exists $z \in L$ such that $z^{1+\rho} = c$.

Indeed by the diagram

$$N_{K(\sqrt{a},\sqrt{b})/K(\sqrt{ab})} z = z^{1+\rho}.$$

Observe that $(ii') \Rightarrow (iii')$ trivially. Now assume (iii'), and put $u = z^{\sigma+1}/c$. Note

$$u^\sigma = z^{(\sigma+1)\sigma}/c^\sigma = z^{\sigma+1}/c = u$$

shows $u \in K(\sqrt{a})$, and moreover

$$u^{\rho+1} = \frac{z^{(\sigma+1)(\rho+1)}}{c^{\rho+1}} = \frac{z^{(1+\rho)\sigma} z^{1+\rho}}{c^2} = 1.$$

Thus by Hilbert's Theorem 90 for the cyclic extension $K(\sqrt{a})/K$ there exists $x \neq 0$ such that $x^\sigma = x$ and $x^{\rho-1} = u$.

Now putting $y = z^\rho/x$, we can check that (ii') is satisfied. Indeed

$$y^\tau = \frac{z^{\rho\tau}}{x^\tau} = \frac{z^\sigma}{x^\rho} \cdot \frac{z}{z} = \frac{uc}{x^\rho z} = \frac{c}{zx} = \frac{z^\rho}{x} = y$$

and

$$x^{1+\rho} y^{1+\rho} = x^{1+\rho} \cdot \frac{z^{\rho(1+\rho)}}{x^{1+\rho}} = z^{1+\rho} = c. \qquad \square$$

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 nondegenerate form in three variables over K.

Solution. This is just Exercise 4.3 together with Exercise 2.4, noting that certainly K contains the second roots of unity ± 1. Thus by Exercise 2.8, remembering that $S(a, b)$ is finite, f represents 0 in K_v for all but a finite number of v, and by Exercise 2.9 this number must be even. $\square$

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 $K_v(\sqrt{a}) = K_v(\sqrt{b})$. 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 nonzero element of K_v unless $K_v = \mathbb{R}$ and f is positive definite.

Solution. Assume

$$f = X^2 - bY^2 - cZ^2 + acT^2$$

does not represent 0. Then $a \notin (K_v^*)^2$ since otherwise $f(0, 0, \sqrt{a}, 1) = 0$, and similarly $b \notin (K_v^*)^2$ since otherwise $f(\sqrt{b}, 1, 0, 0) = 0$. To show $ab \in (K_v^*)^2$, it suffices to show

$$K_v(\sqrt{a}) = K_v(\sqrt{b})$$

since then a and b differ by a square. It would also follow that c is not a norm from $K_v(\sqrt{a}) = K_v(\sqrt{b})$ since this would contradict condition (ii) of Exercise 4.4, noting that 1 is always a norm.

Still assuming f does not represent zero, let us show that

$$K_v(\sqrt{a}) = K_v(\sqrt{b}).$$

From class field theory $L \mapsto NL^*$ is a bijection of the abelian extensions of K_v with the set of norm subgroups of K_v^* such that

$$[K_v^* : NL^*] = [L : K_v]$$

[cf Prop 3 and Cor to Prop 4 in VI, §2.6]. Thus $NK_v(\sqrt{a})^*$ and $NK_v(\sqrt{b})^*$ are distinct index two subgroups of K_v^*. Therefore

$$NK_v(\sqrt{a})^* NK_v(\sqrt{b})^* = K_v^*,$$

but then we can write $c \in K(\sqrt{ab})$ as a product of a norm from $K(\sqrt{a})$ and a norm from $K(\sqrt{b})$, contradicting condition (iii) in Exercise 4.4.

Now suppose conversely that those conditions are satisfied. Noting that

$$N = NK_v(\sqrt{a}) = NK_v(\sqrt{b}),$$

certainly the elements represented by f are

$$((K_v^*)^2 - b(K_v^*)^2) - c((K_v^*)^2 + a(K_v^*)^2) = N - cN.$$

Since by above c is not a norm from $K_v(\sqrt{a}) = K_v(\sqrt{b})$ and inverses of norms are norms, we have that $0 \notin N - cN$.

Furthermore $-1 \in N$, then $cN = -cN$, but since N and cN are of index two in K_v^* and $c \notin N$, we would have $N - cN = K_v^*$ since $N - cN$ is a subgroup. □

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.

Solution. Any form in 4 variables can easily be put into the form of Exercise 4.6. Moreover, quoting the beginning of exercise [cf page 357], the question of representability of non-zero elements by forms $n-1$ variables is equivalent to that of the representability of 0 by forms in n variables. □

Theorem (Hasse Norm)**.** *If $a \in K^*$ and L/K is cyclic, then $a \in N_{L/K}L^*$ if and only if $a \in N_{L^v/K_v}L^{v*}$ for all primes v.*

Proof. VII, §9.6. □

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.

Solution. For $n. = 1$ this is meaningless by Exercise 4.1.

For $n = 2$ we can assume that f is in the form $X^2 - bY^2$ since otherwise the hypothesis cannot hold. Since f represents 0 in every K_v, by Exercise 4.2 $b \in (K_v^*)^2$ or in other words

$$K_v(\sqrt{b}) = K_v.$$

This means that every v splits completely. But Chebotarev's density theorem asserts the density of such primes must be

$$1/|\mathrm{Gal}(K(\sqrt{b})/K)|,$$

so

$$|\mathrm{Gal}(K(\sqrt{b})/K)| = 1$$

and so $X^2 - bY^2$ represents 0 in K.

For $n = 3$ we specialize the Hasse Norm theorem to the case where G has order two. In this case $L = K(\sqrt{b})$, and the theorem asserts $a = X^2 - bY^2$ has a solution if and only if it has a solution at all places. Thus any form in three variables has a nontrivial zero if and only if it has one at every place.

For $n = 4$ let us assume for simplicity that

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

Then using Exercise 4.4 twice and the $n = 3$ case gives that f represents 0 in every K_v if and only if

$$g = X^2 - bY^2 - cZ^2$$

represents 0 in every $K_v(\sqrt{ab})$ if and only if g represents 0 in $K(\sqrt{ab})$ if and only if f represents 0 in K.

For $n \geq 5$, which will take the remainder of this solution, we proceed by induction. Let

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

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.

Consider a place $v \in S$. Since f represents 0 in K_v, we have

$$c_v \stackrel{\text{def}}{=} ax_{1,v}^2 + bx_{2,v}^2 = g(x_{3,v}, \ldots, x_{n,v})$$

for some $x_{1,v}, x_{2,v}$ not both zero and $x_{3,v}, \ldots, x_{n,v} \in K_v$ not all zero. Now note $(K_v^*)^2$ is open in K_v^*, so there is $\epsilon > 0$ such that an ϵ-ball in the v-norm around 1 is contained in $(K_v^*)^2$ for all $v \in S$, of which we recall there are a finite number. By the weak approximation theorem [cf II, §6] and continuity there is x_1, x_2 such that

$$c = ax_1^2 + bx_2^2$$

is within ϵ of c_v in each v-norm so that

$$\frac{c_v}{c} \in (K_v^*)^2.$$

Now in all places outside S the form $cY^2 - g$ represents 0 since g represents 0, and in all places in S it represents 0 since

$$c \cdot \sqrt{\frac{c_v}{c}}^2 - g(x_{3,v}, \ldots, x_{n,v}) = 0.$$

Thus by induction $cY^2 - g$ represents 0 in K, so of course g represents c in K and f represents 0 in K. □

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.

Solution. This is just Exercise 4.7 together with Exercise 4.8. □

Exercise 6: On Decomposition of Primes

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

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

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

Solution. Indeed, we have

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

by the following argument. Let E be a Galois closure, and let $\mathfrak{P}$ a prime in E over a prime $\mathfrak{p}$ in K. Then $\mathfrak{p}$ splits in both L and M if and only if

$$e(\mathfrak{P}^L/\mathfrak{p}) = f(\mathfrak{P}^L/\mathfrak{p}) = 1$$

and

$$e(\mathfrak{P}^M/\mathfrak{p}) = f(\mathfrak{P}^M/\mathfrak{p}) = 1$$

if and only if

$$L, M \subset E^{D(\mathfrak{P}/\mathfrak{p})}$$

if and only if

$$LM \subset E^{D(\mathfrak{P}/\mathfrak{p})}$$

(here we use Galoisness of L and M) if and only if $\mathfrak{p}$ splits in LM.

So

$$\begin{aligned} L \subset M &\Rightarrow \mathrm{Spl}_S(M) \subset \mathrm{Spl}_S(L) \\ &\Rightarrow \mathrm{Spl}_S(LM/K) = \mathrm{Spl}_S(M/K) \\ &\Rightarrow [LM : K] = [M : K] \qquad \text{(Tchebotarov density theorem)} \\ &\Rightarrow L \subset M, \end{aligned}$$

as desired. □

Application: If a separable polynomial $f(X) \in K[X]$ splits into linear factors mod $\mathfrak{p}$ for all but a finite number of primes ideals $\mathfrak{p}$ of K, then f splits into linear factors in K.

Solution. This is in fact an easy application of the Tchebotarov density theorem. If L is the splitting field of f, then the density of $\mathfrak{p}$ in K such that $(\mathfrak{p}, L/K) = 1$ is $1/[L : K]$. But $(\mathfrak{p}, L/K) = 1$ is equivalent to f splitting mod $\mathfrak{p}$, so the density is 1, hence $L = K$. □

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.

Solution. Let us instead denote by $G(w/v)$ a decomposition group of v, where w is a prime over v. Note v has a split factor in E if and only if

$$e(w^E/v) = f(w^E/v) = 1$$

if and only if

$$L^{D(w/v)} \supset E$$

if and only if $D(w/v) \subset H$. Thus since the decomposition subgroups $D(w/v)$ for varying w are all conjugate, v is split completely in E if and only if the conjugates of $D(w/v)$ are all contained in H. □

Hence, show that the set of primes $\mathrm{Spl}'_S(E/K)$ has density $|\bigcup_{\rho\in G}\rho H\rho^{-1}|/|G|$.

Solution. Recall that

$$D(w/v)\cong \mathrm{Gal}(K(w)/K(v))$$

is cyclic and that the Frobenius element $F_{L/K}(v)$ is the generator. Thus $v\notin S$ has a split factor in E if and only if

$$\rho D(w/v)\rho^{-1}\subset H$$

for some $\rho\in\mathrm{Gal}(L/K)$ if and only if

$$F_{L/K}(v)\subset \rho^{-1}H\rho$$

for some $\rho\in\mathrm{Gal}(L/K)$. For fixed $\rho\in\mathrm{Gal}(L/K)$ the Tchebotarov density theorem asserts the density of such v such that $F_{L/K}(v)\subset\rho^{-1}H\rho$ is $1/|G|$ times the size of the conjugacy class of $\rho H\rho^{-1}$. Thus since any element conjugate to an element in $\rho H\rho^{-1}$ is in some $\rho' H\rho'^{-1}$, the density of $\mathrm{Spl}'_S(E/K)$ is as indicated. □

Now prove the lemma on finite groups which states that the union of the conjugates of a proper subgroup is not the whole group and conclude that if $\mathrm{Spl}'_S(E/K)$ has density 1, then $E=K$.

Solution. Let $H\leq G$ be a proper subgroup of a finite group. Note $\rho H\rho^{-1}$ is independent of the H-coset of ρ since

$$(\rho h)H(\rho h)^{-1}=\rho(hHh^{-1})\rho^{-1}=\rho H\rho^{-1}.$$

Thus

$$\left|\bigcup_{\rho\in G}\rho H\rho^{-1}\right|=\left|\bigcup_{\rho\in G/H}\rho H\rho^{-1}\right|\leq\frac{|G|}{|H|}\cdot|H|-\left|\bigcap_{\rho\in G/H}\rho H\rho^{-1}\right|\leq|G|-1/.$$

Here in the first inequality we use that H is proper so that $|G/H|>1$ and that $|\rho H\rho^{-1}|=|H|$, and in the second we use that that $1\in\rho H\rho^{-1}$. Thus the union of the conjugates of H cannot be all of G.

Since $\mathrm{Spl}'_S(E/K)$ has density

$$\left|\bigcup_{\rho\in G}\rho H\rho^{-1}\right|/|G|,$$

we conclude that if the density is 1, then H must be all of G and so $E=L^H=K$. □

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.

Solution. In fact we can show that f has degree 1, which certainly shows f has a root in K.

Suppose f has degree ≥ 2. Let E be the splitting field of f so that $\mathrm{Gal}(E/K)$ acts transitively on the roots. Note if $f_{\mathfrak{p}}$ has no roots, then by considering its cycle decomposition $F_{E/K}(\mathfrak{p})$ does not have any fixed points, and conversely.

Now the fixed point free actions G_0 in a group form a conjugacy class: if $ghg^{-1}x=x$, then

$$hg^{-1}=g^{-1}x$$

shows h has a fixed point. Moreover this conjugacy class is nonempty because $\mathrm{Gal}(E/K)$ is transitive: by the orbit-stabilizer formula, all transitive group actions on a finite non-singleton set have a fixed point free element. Thus by Tchebotarev the density of such $\mathfrak{p}$ is $|G_0|/|G|$. This has a lower bound of $1/n$ by the 1992 result by Cohen. Therefore there are infinitely many $\mathfrak{p}$ such that $f_\mathfrak{p}$ has no roots. □

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.

Solution. Note no matter what K is, f does not have a root in K. Now let $K = \mathbb{Q}_p$ so that $\mathcal{O}_K = \mathbb{Z}_p$ and

$$K(p) = \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p.$$

Consider the only prime p of $\mathbb{Z}_p$. In $\mathbb{F}_p$ the non-zero squares form an index 2 subgroup and represent $1 \in \mathbb{Z}/2\mathbb{Z}$ in the order 2 quotient group, so the product of two non-squares is a square. Thus f_p has a root $\sqrt{ab}$. □

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 G and H' in the same number of elements. Note that if H is a normal subgroup, then this cannot happen unless $H' = H$.

Solution. Recall that G acts on the cosets of H and hence induces the permutation representation $G \to \mathrm{GL}(\mathbb{C}[G/H])$ defined by

$$g x_{g'H} = x_{gg'H},$$

where $\mathbb{C}[G/H]$ has basis $x_{g'H}$. Recall further that representations $\rho\colon G \to \mathrm{GL}(V)$ of finite groups are determined by their character $\chi_\rho\colon G \to \mathbb{C}$ defined by

$$\chi_\rho(g) = \mathrm{tr}(\rho(g))$$

and that this character is constant on each conjugacy class. Let $\mathrm{conj}\, g$ denote the conjugacy class of g.

Let ρ and ρ' denote the permutation representations of G corresponding to H and H' respectively, and let $g \in G$. Compute

$$\begin{aligned}
\chi_\rho(g) &= \mathrm{tr}(\rho(g)) \\
&= |\{g'H \mid g x_{g'H} = x_{gg'H} = x_{g'H}\}| \\
&= |\{g'H \mid g'^{-1} g g' \in H\}| \\
&= \frac{|H \cap \mathrm{conj}\, g|}{|H|},
\end{aligned}$$

where in the third equality we use that if $g'^{-1} g g' \in H$, then

$$(g'h)^{-1} g (g'h) \in H$$

for all $h \in H$.

Thus if ρ and ρ' are isomorphic as linear representations, then by above

$$|H \cap \mathrm{conj}\, g|/|H| = |H' \cap \mathrm{conj}\, g|/|H'|$$

for all $g \in G$, but taking $g = 1$ shows $|H| = |H'|$, hence each conjugacy class of G meets H and H' in the same number of elements. Conversely if

$$|H \cap \operatorname{conj} g| = |H' \cap \operatorname{conj} g|$$

for all $g \in G$, then similarly taking $g = 1$ shows $|H| = |H'|$, hence ρ and ρ' are isomorphic by above.

Finally, a normal subgroup is its own conjugacy class, so if H is a normal subgroup, then indeed 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

$$H = \{1,\ (X_1\ X_2)(X_3\ X_4),\ (X_1\ X_3)(X_2\ X_4),\ (X_1\ X_4)(X_2\ X_3)\}$$
$$H' = \{1,\ (X_1\ X_2)(X_3\ X_4),\ (X_1\ X_2)(X_5\ X_6),\ (X_3\ X_4)(X_5\ X_6)\}.$$

Solution. Recall that a conjugacy class of a symmetric group is a set of elements of a certain cycle type, for example the conjugacy class of

$$(X_1\ X_2)(X_3\ X_4)$$

in G has 6 elements. Besides the identity, H and H' contain only elements of this cycle type and hence intersect this conjugacy class in 3 elements. Moreover they intersect the conjugacy class of the identity in 1 elements and miss every other conjugacy class. Thus H and H' satisfy the above condition.

However, conjugate subgroups have the same number of fixed points:

$$g\{\text{fixed points of } H\} = \{\text{fixed points of } gHg^{-1}\}.$$

Thus since H fixes X_5 and X_6 whereas H' fixes nothing, H and H' cannot be conjugate. □

Note that there exist Galois extensions of $\mathbb{Q}$ with the symmetric group on 6 letters as Galois group.

Solution. It fact it is standard Galois theory that there are Galois extensions with S_n as Galois group for any positive integer n. □

Exercise 6.4. Let L be a finite Galois extension of $\mathbb{Q}$, let $G = \operatorname{Gal}(L/\mathbb{Q})$, 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 $A/pA \cong A'/pA'$, where A and A' denote the rings of integers in E and E' respectively.
- (c) The zeta-functions 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.

Solution. This is Theorem 1 in Perlis's 1975 paper *On the equation* $\zeta_K(s) = \zeta_{K'}(s)$. Let us outline the argument, which uses the following extra condition:

- (b') Same as (b), but only for all but finite many non-ramified p.

Obviously $(b) \Rightarrow (b')$.

For $(a) \Leftrightarrow (b')$, note that from group theory (a) is equivalent to the coset types of G mod (H, C) and the coset types mod (H', C) being the same for all cyclic subgroups $C \leq G$. When C is a (cyclic) decomposition group of a prime $\mathfrak{p}$, this coset type is the same as its splitting type. By the Frobenius density theorem every C is a decomposition subgroup for infinitely many primes, hence $(a) \Leftrightarrow (b')$.

Now for $(c) \Rightarrow (b)$, recall that

$$\zeta_E(s) = \sum_n \frac{A(n)}{n^s}$$

where $A(n)$ is the number of integral ideals of norm n in E, and similarly for

$$\zeta_{E'}(s) = \sum_n A'(n)/n^s.$$

Letting $s \to \infty$ shows $A'(1) = A(1)$, hence

$$A'(n) = A(n)$$

for all n. Now the number $B(p^f)$ of prime ideals of E of norm p^f is the number of integral ideals minus the number of nonprime ideals:

$$B(p^f) = A(p^f) - \sum A(p^{a_1}) \cdots A(p^{a_t})$$

where $a_1 + \cdots + a_t = n$ for $t \geq 2$. This number $B(p^f)$ determines the splitting type of p in E and similarly B' determines the type in E', so since they depend only on their respective A and A', we have $(c) \Rightarrow (b)$.

Finally for $(a) \Rightarrow (c)$ recall the functional equation

$$Z_E(s) = |\mathfrak{d}(E)|^{(1/2)-s} Z_E(1-s)$$

where

$$Z_E(s) = G_1(s)^{n_1(E)} G_2(s)^{n_2(E)} \zeta_K(s)$$

and

$$G_1(s) = n^{-s/2}\Gamma(s/2)$$

and

$$G_2(s) = (2\pi)^{1-s}\Gamma(s).$$

Since n_1 and n_2 conincide for E and E', the quotient $Z_E/Z_{E'}$ gives

$$\frac{\zeta_E(s)}{\zeta_{E'}(s)} = \left|\frac{\mathfrak{d}(E)}{\mathfrak{d}(E')}\right|^{\frac{1}{2}-s} \frac{Z_E(1-s)}{Z_{E'}(1-s)}.$$

The zeta functions can be written as Euler products, but since have already established $(a) \Leftrightarrow (b')$, they are finite:

$$\frac{\zeta_E(s)}{\zeta_{E'}(s)} = \frac{\prod_{j=1}^m (1-d_j^s)^{-1}}{\prod_{j=1}^n (1-c_j^{-s})^{-1}}.$$

Thus

$$f(s) = |\mathfrak{d}(E)/\mathfrak{d}(E')|^{(1/2)-s}$$

and the ζ function agree by a complex analysis argument [Lemma 2]. This moreover shows the discriminants agree. $\square$

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