Solutions to the Cassels-Fröhlich exercises

Dorian Ni

May 2018

First of all, many thanks to Kevin Buzzard for his kind help, and for his willingness to answer even the stupidest questions that I had in mind.

Second of all, I tried to be as complete as possible while solving this exercises, however it is maybe worth mentioning that when the exercises were giving statements about global fields, I always had in mind the number field case. Therefore, there may be special cases for function fields that I haven't treated.

Exercise 1: The Power Residue Symbol

Exercise 1.1.
$\sqrt[m]{a}$ is a root of $X^m - a$ whose roots are the $\xi \sqrt[m]{a}$ with $\xi \in \mu_m$, in $K(\sqrt[m]{a})$ because $\mu_m \subset K$.
And $F_{L/K}(\mathfrak{b}) \in Gal(L/K)$, so $F_{L/K}(\mathfrak{b})(\sqrt[m]{a}) = \xi \sqrt[m]{a}$ for a $\xi \in \mu_m$.
Therefore $\left(\frac{a}{\mathfrak{b}}\right) = \xi$ is a mth root of 1.

Moreover, if $\xi_0 \in \mu_m$,

$$\begin{aligned} F_{L/K}(\mathfrak{b})(\xi_0 \sqrt[m]{a}) &= \xi_0 F_{L/K}(\mathfrak{b})(\sqrt[m]{a}) \\ &= \xi_0 \left(\frac{a}{\mathfrak{b}}\right) \sqrt[m]{a} \end{aligned}$$

Therefore, $\left(\frac{a}{\mathfrak{b}}\right)$ is independent of the choice of $\sqrt[m]{a}$.

Exercise 1.2.
In order to use Chapter VII, §3.2, let's check that $S(a, a')$ contains the primes ramified in $L' = K(\sqrt[m]{a}, \sqrt[m]{a'})$.
Let $\mathfrak{p} \notin S(a, a')$. $\mathfrak{p}$ does not divide m (i.e. $m \notin \mathfrak{p}$), $a, a' \in \mathfrak{o}_\mathfrak{p}^*$.
Therefore, by Chapter III §2 Lemma 5, $m, a \notin \mathfrak{p}$ implies that $\mathfrak{p}$ is unramified in $L = K(\sqrt[m]{a})$. Let $\mathfrak{P}|\mathfrak{p}$ in this extension. $m, a' \notin \mathfrak{P}$ because $\mathfrak{P} \cap K = \mathfrak{p}$. Therefore, we can apply again this lemma 5, and $\mathfrak{P}$ is unramified in $L' = K(\sqrt[m]{a}, \sqrt[m]{a'})$.
Hence $\mathfrak{p}$ is unramified in L'.

Therefore, Chapter VII §3.2 applies and we have the following commutative diagram.

$$\begin{array}{ccc} I^{S(a,a')} & \xrightarrow{F_{L'/K}} & Gal(L'/K) \\ \Big\downarrow{\scriptstyle N_{K/K}=Id} & & \Big\downarrow{\scriptstyle Res} \\ I^{S(a,a')} & \xrightarrow{F_{L/K}} & Gal(L/K) \end{array}$$

And by symmetry, this diagram is valid for $L = K(\sqrt[m]{a})$ and for $L = K(\sqrt[m]{a'})$.
Finally, if $\mathfrak{b} \in I^{S(a,a')}$,

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

Hence,

$$\left(\frac{aa'}{\mathfrak{b}}\right) = \left(\frac{a}{\mathfrak{b}}\right)\left(\frac{a'}{\mathfrak{b}}\right)$$

Exercise 1.3.
Let $a \in K^*$, $\mathfrak{b}, \mathfrak{b}' \in I^{S(a)}$, we have

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

because $\left(\frac{a}{\mathfrak{b}'}\right) \in \mu_m \subset K$.

Therefore,

$$\left(\frac{a}{\mathfrak{b}\mathfrak{b}'}\right) = \left(\frac{a}{\mathfrak{b}}\right)\left(\frac{a}{\mathfrak{b}'}\right)$$

Exercise 1.4.
We have $v \notin S(a)$, so $v \notin S$ and $\mathfrak{p}_v$ does not divide m.

Therefore $X^m - 1$ is separable in $k(v)$. $(gcd(X^m - 1, mX^{m-1}) = 1)$. So the surjection $o_v \twoheadrightarrow k(v)$ induces an injective morphism of μ_m in $k(v)^*$. Thus,

$$m | Nv - 1$$

$F_{L/K}(v)$ is defined by the following property:
$\forall x \in \mathfrak{o}_v$,

$$F_{L/K}(v)(x) = x^{Nv} \pmod{\mathfrak{p}_v}$$

Therefore,

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

And finally,

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

Exercise 1.5.
Suppose (i), we have $a^{\frac{Nv-1}{m}} = 1$ in $k(v)$. Let's show (ii).
Let x be a solution of $X^m - a$ in a algebraic closure of $k(v)$. We have

$$x^{Nv-1} = (x^m)^{\frac{Nv-1}{m}} = a^{\frac{Nv-1}{m}} = 1$$

Therefore $x \in k(v)$, and $x^m = a$ is solvable in $k(v)$.

Suppose (ii), let's show (i).
Let $x \in k(v)$ such that $x^m = a$. Then $a^{\frac{Nv-1}{m}} = 1$ in $k(v)$.
Thus $\left(\frac{a}{v}\right) = 1$ in $k(v)$.
We already seen that $\mu_m \to k(v)$ is injective. Therefore

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

Suppose (iii), let's show (ii).
Let $x \in K_v$ such that $x^m = a$. We have $v(a) = 0$. Therefore $x \in \mathfrak{o}_v$.
Thus, projecting mod $\mathfrak{p}_v$, we have $x^m = a$ in $\mathfrak{o}_v/\mathfrak{p}_v \cong k(v)$. And $x^m = a$ is solvable in $k(v)$.

Suppose (ii), let's show (iii).
Let $f(X) = X^m - a$.
We have a $x \in \mathfrak{o}_v$ such that $f(x) \in \mathfrak{p}_v$. And $f'(x) = mx^{m-1} \notin \mathfrak{p}_v$ because $a \notin \mathfrak{p}_v$.
Hence, $|f(x)|_v < 1$ and $|f'(x)|_v = 1$. Therefore, we can apply Hensel's lemma in K_v (Chapter II, App. C), and we have then a solution $x \in K_v$ to $x^m = a$.

Exercise 1.6.
By exercise 1.4, if v is prime to m, we have

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

Again, $\mu_m \to k(v)$ is injective, therefore

$$\left(\frac{\xi}{v}\right) = \xi^{\frac{Nv-1}{m}}$$

If $\mathfrak{b} = \sum n_v v$ prime to m. Then by the remark in the statement of the exercise.

$$\frac{N\mathfrak{b}-1}{m} = \sum n_v \frac{Nv-1}{m} \pmod{m}$$

Therefore,

$$\begin{aligned}\left(\frac{\xi}{\mathfrak{b}}\right) &= \prod \left(\frac{\xi}{v}\right)^{n_v} \\ &= \prod \xi^{n_v \frac{Nv-1}{m}} \\ &= \xi^{\frac{N\mathfrak{b}-1}{m}}\end{aligned}$$

Exercise 1.7.
By exercise 1.6., $\left(\frac{1}{\mathfrak{b}}\right) = 1$. So by exercise 1.2., it suffices to show $\left(\frac{c}{\mathfrak{b}}\right) = 1$ if $c = 1 \pmod{\mathfrak{b}}$.
And as $\left(\frac{\xi}{\mathfrak{b}}\right) = \prod \left(\frac{\xi}{v}\right)^{n_v}$, if suffices to show $\left(\frac{c}{v}\right) = 1$ if $c = 1 \pmod{\mathfrak{p}_v}$. (because we have $\mathfrak{b} \subset \mathfrak{p}_v$ as $\mathfrak{b}$ is integral, therefore $c = 1 \pmod{\mathfrak{b}}$ implies $c = 1 \pmod{\mathfrak{p}_v}$).
And $\left(\frac{c}{v}\right) = c^{\frac{Nv-1}{m}} = 1 \pmod{\mathfrak{p}_v}$.
Again, μ_m is one-to-one to $k(v)$, thus

$$\left(\frac{c}{v}\right) = 1$$

and this concludes.

Exercise 1.8.
By exercise 1.3., it suffices to show that the Artin's reciprocity law implies that if $c \in K^*$ is such that $c \in (K_v^*)^m$ for all $v \in S(a)$, then $\left(\frac{a}{(c)^{S(a)}}\right) = 1$.
As in Chapter VII, §3.3, by the weak approximation theorem, there is $c' \in K^*$ such that

$$\forall v \in S(a),\ |c'^{-m}c - 1|_v < \epsilon$$

(The ϵ is the one from the reciprocity law, §3.3). Therefore we can apply the reciprocity law and $F_{L/K}((c'^{-m}c)^{S(a)}) = 1$.
And finally,

$$F_{L/K}(c^{S(a)}) = F_{L/K}(c'^{S(a)})^m F_{L/K}((c'^{-m}c)^{S(a)}) = F_{L/K}(c'^{S(a)})^m = 1$$

($Gal(L/K)$ is of order dividing m).
By definition of $\left(\frac{a}{(c)^{S(a)}}\right)$, we have

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

Exercise 1.9.
If p is an odd prime, then the squares in $\mathbb{Q}_p$ are the $p^{2N}u$, with $u \in \mathbb{Z}_p^*$ such that the image of u in $\mathbb{F}_p^*$ is a square.
If $p = 2$, then the squares in $\mathbb{Q}_2$ are the $2^{2N}u$, with $u \in \mathbb{Z}_2^*$ such that u verifies $u = 1 \pmod 8$. (See [Ser94], Chapter 2).
Let P,Q be positive odd primes such that $(a, P) = (a, Q) = 1$ and $P = Q \pmod{8a_0}$ ($a = 2^v a_0$ with a_0 odd). Then, PQ^{-1} is a square in $\mathbb{Q}_v$ for $v(a) \neq 0$, and in $\mathbb{Q}_2$ (m=2). Hence, by exercise 1.8., we have

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

Exercise 1.10.
By exercise 1.4., we have $\left(\frac{-1}{P}\right) = (-1)^{(P-1)/2} \pmod P$. Thus,

$$\left(\frac{-1}{P}\right) = (-1)^{(P-1)/2}$$

By exercise 1.9., $\left(\frac{2}{P}\right)$ depends only on $P \pmod 8$. Thus we can compute $\left(\frac{2}{P}\right)$ for $17, 3, 5, 7$, using exercise 1.5.

$$\left(\tfrac{2}{17}\right) = \left(\tfrac{36}{17}\right) = 1 = (-1)^{\frac{17^2-1}{8}}, \qquad \left(\tfrac{2}{3}\right) = -1 = (-1)^{\frac{3^2-1}{8}},$$
$$\left(\tfrac{2}{5}\right) = -1 = (-1)^{\frac{5^2-1}{8}}, \qquad \left(\tfrac{2}{7}\right) = \left(\tfrac{9}{7}\right) = 1 = (-1)^{\frac{7^2-1}{8}}$$

Thus, because $(-1)^{\frac{P^2-1}{8}}$ also depends only on $P \pmod 8$

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$$

By the explications in exercise 1.10., if $P = Q \pmod 8$, then

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

And if $P \neq Q \pmod 8$, $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)$ only depend on $P \pmod 8$ and on $Q \pmod 8$.

$$\left(\tfrac{3}{5}\right)\left(\tfrac{5}{3}\right) = 1 = (-1)^{\frac{3-1}{2}\frac{5-1}{2}}, \qquad \left(\tfrac{3}{7}\right)\left(\tfrac{7}{3}\right) = -1 = (-1)^{\frac{3-1}{2}\frac{7-1}{2}}, \qquad \left(\tfrac{3}{17}\right)\left(\tfrac{17}{3}\right) = 1 = (-1)^{\frac{17-1}{2}\frac{3-1}{2}},$$
$$\left(\tfrac{5}{7}\right)\left(\tfrac{7}{5}\right) = 1 = (-1)^{\frac{5-1}{2}\frac{7-1}{2}}, \qquad \left(\tfrac{5}{17}\right)\left(\tfrac{17}{5}\right) = 1 = (-1)^{\frac{17-1}{2}\frac{5-1}{2}}, \qquad \left(\tfrac{7}{17}\right)\left(\tfrac{17}{7}\right) = 1 = (-1)^{\frac{17-1}{2}\frac{7-1}{2}}$$

Thus, because $(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$ also depends only on $P \pmod 8$ and $Q \pmod 8$

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

Exercise 2: The Norm Residue Symbol

Exercise 2.1.
As in exercise 1.1.
$\sqrt[m]{a}$ is a root of $X^m - a$ whose roots are the $\xi \sqrt[m]{a}$ with $\xi \in \mu_m$, in $K_v(\sqrt[m]{a})$ because $\mu_m \subset K_v$.

And $\Psi_v(b) \in Gal(L^v/K_v)$, so $\Psi_v(b)(\sqrt[m]{a}) = \xi \sqrt[m]{a}$ for a $\xi \in \mu_m$.
Therefore $(a,b)_v = \xi$ is a mth root of 1.

Moreover, if $\xi_0 \in \mu_m$,

$$\begin{aligned}\Psi_v(b)(\xi_0 \sqrt[m]{a}) &= \xi_0 \Psi_v(b)(\sqrt[m]{a}) \\ &= \xi_0 (a,b)_v \sqrt[m]{a}\end{aligned}$$

Therefore, $(a,b)_v$ is independent of the choice of $\sqrt[m]{a}$.

Exercise 2.2.
As in exercise 1.3., the fact that $(a,bb')_v = (a,b)_v(a,b')_v$ comes from the fact that $\Psi_v : K_v^* \to G^v$ is a group homomorphism and that μ_m is fixed by G^v.
And as in exercise 1.2., $(aa',b)_v = (a,b)_v(a',b)_v$ comes from the fact that we have the following commutative diagram for $K \subset L \subset L'$:

$$\begin{array}{ccccc} K_v & \xrightarrow{i_v} & J_K & \xrightarrow{\Psi_{L'/K}} & Gal(L'^v/K_v) \\ \downarrow{\scriptstyle Id} & & \downarrow{\scriptstyle N_{K/K}=Id} & & \downarrow{\scriptstyle Res} \\ K_v & \xrightarrow{i_v} & J_K & \xrightarrow{\Psi_{L/K}} & Gal(L^v/K_v) \end{array}$$

And recall that $\Psi_v = \Psi_{L/K} \circ i_v$.

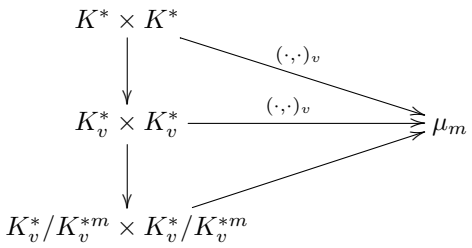
Exercise 2.3.
If there is a $c \in K_v^*$ such as $b = c^m$ then $\Psi_v(b) = \Psi_v(c)^m = Id$ because the order of G^v divide m.
Thus, in this case

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

If there is a $c \in K_v^*$ such as $a = c^m$ then $\sqrt[m]{a}$ is in K_v^*, and $\Psi_v(b)$ is trivial on K_v^*.
Thus, in this case

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

Let's now define the unique extension of $(\cdot,\cdot)_v$ to $K_v^* \times K_v^*$.
As μ_m is of order m, $(\cdot,\cdot)_v$ has to be trivial on $K_v^{*m} \times K_v^{*m}$. Thus we need to have to following commutative diagram.



Furthermore K_v^{*m} is open in K_v^* and K^* is dense in K_v^*. Thus we can choose a set of representatives $(x_\lambda)_{\lambda\in\Lambda}$ for K_v^*/K_v^{*m} in K^*. And then, we need to have

$$(x_{\lambda_1}K_v^{*m}, x_{\lambda_2}K_v^{*m})_v = (x_{\lambda_1}, x_{\lambda_2})_v$$

Thus this show the uniqueness and define the extension to $K_v^* \times K_v^*$. And this definition does not depend on the choice of the representatives (by the beginning of this exercise and by bilinearity).

Exercise 2.4.
Let first remark that $K_v(\sqrt[m]{a})$ is finite extension of K_v. Thus, there is a unique valuation extending v on $K_v(\sqrt[m]{a})$, which is, by restriction, a valuation on $K(\sqrt[m]{a})$ extending v. Furthermore, $K(\sqrt[m]{a})$ is dense in $K_v(\sqrt[m]{a})$, so $K_v(\sqrt[m]{a})$ is a completion for this given valuation.
Thus by chapter VII §6.2, $\Psi_v(N_{K_v(\sqrt[m]{a})/K_v}(K_v(\sqrt[m]{a})^*)) = 1$.
So if $b \in N(K_v(\sqrt[m]{a})^*)$, $\Psi_v(b)(\sqrt[m]{a}) = \sqrt[m]{a}$. And thus,

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

Conversely, if $(a, b)_v = 1$, then $\Psi_v(b)(\sqrt[m]{a}) = \sqrt[m]{a}$, i.e. $\Psi_v(b) = Id$ (because it is in $Gal(K_v(\sqrt[m]{a})/K_v)$). And thus, $b \in \ker(\Psi_v) = N_{K_v(\sqrt[m]{a})/K_v}(K_v(\sqrt[m]{a})^*)$.

Exercise 2.5.
As mentioned in the exercise, if $a + b = x^m$ with $x \in K_v$ then $b = x^m - a$ is a norm for the extension $K_v(\sqrt[m]{a})/K_v$. Therefore, by exercise 2.4,

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

Exercise 2.6.
By bilinearity and the fact that $(c, -c)_v = 1$, we have

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

Exercise 2.7.
We have

$$\mathbb{Q} \subset K \subset \mathbb{C}$$

Therefore, if v is archimedean, we have

$$\mathbb{R} \subset K_v \subset \mathbb{C}$$

Thus, $K_v = \mathbb{R}$ or $K_v = \mathbb{C}$.
If $K_v = \mathbb{C}$ then $K_v = K_v^m$. Thus, by exercise 2.5, $(\cdot,\cdot)_v = 1$.
If $K_v = \mathbb{R}$ then $m = 2$. Thus, in this case,
$(a,b)_v = 1$ if and only if $a > 0$ or $b > 0$, (i.e. a or b is a norm for $K_v(\sqrt{a}) = \mathbb{R}$ or $\mathbb{C}$)).

Exercise 2.8.
If $v \notin S(a)$, then v in unramified in $K(\sqrt[m]{a})/K$. Thus, if $b \in K_v*$ then $i_v(b) \in J_K^{S(a)}$. Thus,

$$\begin{aligned}\Psi_v(b) &= \Psi_{L/K}(i_v(b)) \\ &= F_{L/K}(i_v(b)^{S(a)}) \\ &= F_{L/K}(v(b)v) \\ &= F_{L/K}(v)^{v(b)}\end{aligned}$$

And then,

$$\begin{aligned}\Psi_v(b)(\sqrt[m]{a}) &= F_{L/K}(v)^{v(b)}(\sqrt[m]{a}) \\ &= \left(\frac{a}{v}\right)^{v(b)} \sqrt[m]{a} \\ &= (a,b)_v \sqrt[m]{a}\end{aligned}$$

Hence,

$$\left(\frac{a}{v}\right)^{v(b)} = (a,b)_v$$

In the general case, if $v \notin S$,

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

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

Exercise 2.9.

We know that $\Psi_{L/K}$ is trivial on K^*. Therefore if $b \in K^*$, we have

$$\Psi_{L/K}(b) = \prod_v \Psi_v(b) = 1$$

Thus

$$\prod_v \Psi_v(b)(\sqrt[m]{a}) = \prod_v (a,b)_v \sqrt[m]{a} = \sqrt[m]{a}$$

And

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

Exercise 2.10.
We have

$$\begin{aligned}
\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} &= \prod_{v\notin S(a)} \left(\frac{a}{v}\right)^{v(b)} \prod_{v\notin S(b)} \left(\frac{b}{v}\right)^{-v(a)} \\
&= \prod_{v\notin S(a)} (a,b)_v \prod_{v\notin S(b)} (b,a)_v^{-1} \\
&= \prod_{v\notin S(a)} (a,b)_v \prod_{v\notin S(b)} (a,b)_v \\
&= \prod_v (a,b)_v \prod_{v\notin S(a)\cap S(b)} (a,b)_v^{-1} \\
&= \prod_{v\notin S(a)\cap S(b)} (a,b)_v^{-1}
\end{aligned}$$

Thus

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

Applications: If $S(a) \cap S(b) = S$, then

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

If $S(\lambda) = S$, then for all $v \notin S$, $v(\lambda) = 0$, thus $\left(\frac{b}{\lambda}\right) = 1$ and then

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

Exercise 2.11.
Firstly, let's remark that the symbol $\left(\frac{a}{p}\right)$ define in exercise 2.10 and exercise 1.8 coincide in this case, because the only $v \notin S(a)$ such that $v(p) \neq 0$ is v_p.
Secondly, we have $(x, P)_\infty = 1$ because P is a norm in $\mathbb{R}(\sqrt{a})/\mathbb{R}$ (if either case where $\mathbb{R}(\sqrt{a}) = \mathbb{R}$ or $\mathbb{R}(\sqrt{a}) = \mathbb{C}$).

Then, as $S(-1) = S$, we have

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

And, as $S(2) = S$, we have

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

And, as $S(Q) \cap S(P) = S$, we have

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

Therefore, the result in exercise 1.10 are indeed equivalent to

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

Using the fact given in the exercise, if $P = 1 \pmod 4$, we have

$$(P, -1)_2 = 1 = (-1)^{\frac{P-1}{2}},\ (P, 2)_2 = (-1)^{\frac{P-1}{4}} = (-1)^{\frac{P^2-1}{8}}$$

If either $P = 1 \pmod 4$ or $Q = 1 \pmod 4$,

$$(P, Q)_2 = 1 = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$$

If $P = 3 \pmod 4$ and $Q = 3 \pmod 4$, it is standard fact that

$$(P, -1)_2 = \left(\frac{-1}{P}\right) = -1 = (-1)^{\frac{P-1}{2}}$$

We have $-P = 1 \pmod 4$, thus

$$(-P, 2)_2 = (-1)^{\frac{P+1}{4}} = (-1)^{\frac{P^2-1}{8}} = (-1, 2)_2 (P, 2)_2 = (P, 2)_2$$

(because $(-1, R)_2 = \left(\frac{-1}{R}\right)$ by the preceding exercise) and

$$(-P, Q)_v = 1 = (-1, Q)_v (P, Q)_v = -(P, Q)_v$$

Thus

$$(P, Q)_v = -1 = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$$

And this concludes for quadratic reciprocity.

Exercise 2.12.
ξ is a root of $\frac{X^p-1}{X-1}$.
Thus, λ is a root of

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

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

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

Therefore,

$$\lambda^{p-1} = -p \pmod{p\lambda}$$
$$\lambda^{p-1}/p = -1 \pmod{\lambda}$$

And, by chapter 3, §1, $p = \lambda^{p-1}\prod_{k=1}^{p-1} \frac{1-\xi^k}{1-\xi}$ and $\frac{1-\xi^k}{1-\xi}$ is a unit for $0 \leq k \leq p-1$.
Thus $v(p) \neq 0$ implies $v(\lambda) \neq 0$.
Therefore,

$$\lambda^{p-1}/p = -1 \pmod{\mathfrak{p}_v}$$

Now, if $a = 1 \pmod{p\lambda\mathfrak{o}_v}$ then

$$a = 1 + p\lambda c', \text{ with } c' \in \mathfrak{o}_v$$
$$a = 1 + \lambda^p \tfrac{p}{\lambda^{p-1}} c'$$
$$a = 1 + \lambda^p c$$

And $c = \frac{p}{\lambda^{p-1}}c'$ is in $\mathfrak{o}_v$.

If $f(X) \in \mathfrak{o}_v[X]$ is such that $f(X) = X^p - X - c \pmod{\mathfrak{p}_v}$. Then $f'(X) = -1 \pmod{\mathfrak{p}_v}$. Therefore, if x is a root of $f(X)$, then x is a integral element and $f(x) = 0 \pmod{\mathfrak{p}_v}$, $f'(x) = -1 \pmod{\mathfrak{p}_v}$.
This polynomial is the following: if $\alpha^p = a$ and $\alpha = 1 + \lambda x$, let

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

x is a root of $f(X)$.

If $c = 0 \pmod{\mathfrak{p}_v}$, then by Hensel's lemma, f has a root in K_v (i.e. $a \in (K_v^*)^p$), $K_v(x) = K_v(\sqrt[p]{a}) = K_v$, then a is indeed v-primary. We also have

$$(a, b)_v = 1 = \xi^{-S(0)v(b)}$$

As $f(X)$ is irreducible (because $X^p - a$ is irreducible), $f(X)$ is the minimal polynomial of x. Furthermore, the image of $f(X)$ in the residue field is separable ($f'(X) = -1 \neq 0 \pmod{\mathfrak{p}_\mathfrak{v}}$). Thus $K_v(\sqrt[p]{a}) = K_v(x)$ is unramified over K_v (see lemma in appendix) and x is v-primary.
v is unramified in $K(\sqrt[p]{a})$, thus $i_v(b)$ is in J_K^S.
If $c \neq 0 \pmod{\mathfrak{p}_v}$.
Thus,

$$\begin{aligned}\Psi_v(b) &= \Psi_{L/K}(i_v(b)) \\ &= F_{L/K}(i_v(b)^S) \\ &= F_{L/K}(v(b)v) \\ &= F_{L/K}(v)^{v(b)}\end{aligned}$$

By definition,

$$F_{L/K}(x) = x^{Nv} = x + S(\bar{c}) \pmod{\mathfrak{p}_v}$$

Let $\alpha_i = \xi^i \alpha = 1 + \lambda x_i$. We have

$$\begin{aligned}x_{i+1} &= (\alpha_{i+1} - 1)/\lambda \\ &= (\xi\alpha_i - 1)/\lambda \\ &= -1 + \xi x_i \\ &= -1 + (1 - \lambda)x_i\end{aligned}$$

Thus,

$$x_{i+1} = x_i - 1 \pmod{\mathfrak{p}_v}$$

Finally, if $F_{L/K}(v)(\alpha) = \xi^i \alpha$, then $F_{L/K}(v)(x) = (F_{L/K}(v)(\alpha) - 1)/\lambda = (\alpha_i - 1)/\lambda = x_i$.
And thus

$$\begin{aligned}x + S(\bar{c}) &= x_i \pmod{\mathfrak{p}_v} \\ &= x - i \pmod{\mathfrak{p}_v}\end{aligned}$$

And this allow us to conclude

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

Exercise 2.13.

(a) As $\eta_j + \lambda^j \eta_i = \eta_{i+j}$, we have

$$\begin{aligned} 1 &= (\eta_j/\eta_{i+j}, \lambda^j \eta_i/\eta_{i+j})_v \\ &= (\eta_j, \lambda^j)_v (\eta_j, \eta_i)_v (\eta_j, \eta_{i+j})_v^{-1} (\eta_{i+j}, \lambda^j)_v^{-1} (\eta_{i+j}, \eta_i)_v^{-1} (\eta_{i+j}, \eta_{i+j})_v \\ &= (\eta_i, \eta_j)_v^{-1} (\eta_{j+i}, \eta_j)_v (\eta_{i+j}, \lambda)_v^{-j} (\eta_i, \eta_{i+j})_v \end{aligned}$$

Thus

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

(b) If $i + j \geq p + 1$, we have $\eta_{j+i} \in U_{p+1} \subset K_v^{*p}$. Therefore by (a), we have $(\eta_i, \eta_j)_v = 1$.

If $a \in U_i$ and $b \in U_j$, then $a = \eta_i^{\alpha_i} \eta_{i+1}^{\alpha_{i+1}} ... \eta_p^{\alpha_p} x_a$ with $x_a \in U_{p+1}$ and $b = \eta_j^{\beta_j} \eta_{j+1}^{\beta_{j+1}} ... \eta_p^{\beta_p} x_b$ with $x_b \in U_{p+1}$. Therefore the bilinearity property concludes.

(c) By the preceding exercise,

$$\begin{aligned} (\eta_p, \lambda)_v &= (1 - \lambda^p, \lambda)_v \\ &= \xi^{-S(-1)v(\lambda)} \\ &= \xi^{-S(-1)} \\ &= \xi^{-(-1)} && \text{(because f=1)} \\ &= \xi \end{aligned}$$

(d) By bilinearity, it suffices to show the uniqueness on $(K_v^*)/(K_v^{*p}) \times (K_v^*)/(K_v^{*p})$, and thus, on $\lambda, \eta_1, ..., \eta_p$. And this is done easily with a descending recursion (for i from p to 1, for j from p to 1).

Exercise 2.14.
Let $a, b \in R$ such that $a = \pm 1 \pmod{3R}$ and $b = \pm 1 \pmod{3R}$.
We have $S = \{\infty, \lambda\}$ (with $\lambda = 1 - \xi$). Exercise 2.7 tells us that $(\cdot, \cdot)_\infty = 1$. Therefore,

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

And $3R = \lambda^2 R$, thus $a = \pm 1 \pmod{3R}$ and $b = \pm 1 \pmod{3R}$ est equivalent to $\pm a \in U_2$ and $\pm b \in U_2$.
By exercise 2.13 (b), we have

$$(\pm a, \pm b)_{v_\lambda} = 1$$

But $(-1, x)_{v_\lambda} = 1$ because $(-1, x)_{v_\lambda}^2 = 1$ and $(-1, x)_{v_\lambda} \in \mu_3$.
Therefore,

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$$

If $a = \pm(1 + 3(m + n\xi))$. We have

$$\begin{aligned}\left(\frac{\xi}{a}\right) &= \left(\frac{\xi}{(a)^S}\right) \\ &= \left(\frac{\xi}{(a)}\right) && \text{(because } v_\lambda(a) = 0\text{)} \\ &= \xi^{\frac{Na-1}{3}} && \text{(Exercise 1.6)}\end{aligned}$$

We have $N(a) = (1 + 3m - 3n/2)^2 + (3\sqrt{3}n/2)^2$, and

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

Therefore,

$$\left(\frac{\xi}{a}\right) = \xi^{-m-n}$$

By exercise 2.10, we have $\left(\frac{\lambda}{a}\right) = (a, \lambda)_{v_\lambda}$.
And as, $(-1, x)_{v_\lambda} = 1$, we will work with $a = 1 + 3(m + n\xi)$.

Firstly, if $x = 1 + k\lambda^2$, then we have

$$x(1 - \lambda^2)^k \in U_4$$

And because $(1 - \lambda^2, \lambda)_{v_\lambda} = 1$, therefore $(x, \lambda)_{v_\lambda} = 1$.
If $x = 1 + k\lambda^3$, then we have

$$x(1 - \lambda^3)^k \in U_4$$

And because $(1 - \lambda^3, \lambda)_{v_\lambda} = \xi$, therefore $(x, \lambda)_{v_\lambda} = \xi^{-k}$.

Then,

$$\begin{aligned}1 + 3(m + n\xi) &= 1 + 2(m + n)\lambda^2 - (m + 3n)\lambda^3 + n\lambda^4 \\ &= (1 + 2(m + n)\lambda^2)(1 - ((m + 3n)\lambda^3 + n\lambda^4)x_1) && \text{with } x_1 = (1 + 2(m + n)\lambda^2)^{-1} \in U_2 \\ &= (1 + 2(m + n)\lambda^2)(1 - (m + 3n)\lambda^3 + \lambda^4 x_2) && \text{with } x_2 \in R \\ &= (1 + 2(m + n)\lambda^2)(1 - (m + 3n)\lambda^3)(1 + \lambda^4 x_3) && \text{with } x_3 \in R\end{aligned}$$

Thus,

$$(1 + 3(m + n\xi), \lambda)_{v_\lambda} = \xi^{m+3n} = \xi^m$$

And this concludes.

By quadratic reciprocity, a theorem from Lagrange and h(-3) = 1, we have

$$\begin{aligned}q = 1 \pmod 3 &\iff -3 \text{ is a square mod } 4q \\ &\iff \text{there is a form of discriminant } -3 \text{ representing } q \\ &\iff \text{there are } x, y \in \mathbb{Z} \text{ such that } q = x^2 - xy + y^2 \\ &\iff \text{there is } \pi \in \mathbb{Z}[\xi], \text{ such that } q = \pi\bar{\pi}\end{aligned}$$

Furthermore, by explicit calculation mod 3 on $q = x^2 - xy + y^2$, we have either $\pm x = 1$ or $\pm y = 1$, so we can choose $\pi = 1 \pmod{3R}$.

Thus, by $\mathbb{Z}/q\mathbb{Z} \cong R/\pi R$ (because $g = 2$ so $f = 1$),

$$\begin{aligned}
2 \text{ is a cubic residue } (\text{mod } q) &\iff 2 \text{ is a cubic residue } (\text{mod } \pi) \\
&\iff \left(\frac{2}{\pi}\right) = 1 \\
&\iff \left(\frac{\pi}{2}\right) = 1 \\
&\iff \pi \text{ is a cubic residue } (\text{mod } 2R) \\
&\iff \pi = 1 \pmod{2R} \qquad (1 \text{ is the only cube } (\text{mod } 2R)) \\
&\iff \pi = 1 + 6(n' + m'\xi)
\end{aligned}$$

Thus, if 2 is a cubic residue (mod q) implies $q = (1+6(n'+m'\xi))(1+6(n'+m'\xi^2)) = (1+6n'-3m')^2+27m'^2$. Reciprocally, if $q = x^2 + 27y^2$, then $x^2 = 1 \pmod 3$ and we can choose $x = 1 \pmod 3$. Then

$$\begin{aligned}
q &= (1 + 3x')^2 + 27y^2 \\
&= (1 + 3(x' + y) - 3y)^2 + 27y^2 \\
&= \pi\bar{\pi}
\end{aligned}$$

with $\pi = 1 + 3(x' + y + 2y\xi)$. We have

$$\begin{aligned}
q &= (1 + 3x')^2 + 27y^2 \pmod 2 \\
&= 1 + 3x' + 27y \pmod 2 \\
&= 1 + x' + y \pmod 2
\end{aligned}$$

And $q = 1 \pmod 2$. Thus $x' + y$ is even, and $\pi = 1 + 6(n' + m'\xi)$. This concludes our discussion.

Exercise 2.15.
Firslty, if $p = 1 \pmod 3$. We have

$$\begin{aligned}
F_{L/\mathbb{Q}}(p)(\xi) &= \xi^p \pmod p \\
&= \xi \pmod p
\end{aligned}$$

Thus,

$$F_{L/\mathbb{Q}}(p)(\xi) = \xi$$

(because, as $p \neq 3$, $X^3 - 1$ is separable mod p).

And, similarly, if $p = 2 \pmod 3$. We have

$$F_{L/\mathbb{Q}}(p)(\xi) = \xi^2$$

Now,

$$p = 1 \pmod 3, p = x^2 + 27y^2 \Longrightarrow 2 \text{ cubic residue } (\text{mod } p)$$
$$\Longrightarrow F_{L/\mathbb{Q}}(p)(\sqrt[3]{2}) = \sqrt[3]{2}$$

(True locally, and as $p \neq 2$, 3, $X^3 - 2$ is separable mod p)
Thus,

$$F_{L/\mathbb{Q}}(p) = Id$$

And,

$$p = 1 \pmod 3, p \text{ not of the form } x^2 + 27y^2 \Longrightarrow 2 \text{ not a cubic residue } (\text{mod } p)$$
$$\Longrightarrow 2^{\frac{p-1}{3}} \neq 1 \pmod p$$
$$\Longrightarrow F_{L/\mathbb{Q}}(p)(\sqrt[3]{2}) = \sqrt[3]{2}^p = \xi^i \sqrt[3]{2} \pmod p$$

with $i = 1$ or 2. Thus, $F_{L/\mathbb{Q}}(p)$ is a 3-cycle.

Finally, if $p = -1 \pmod p$. There are two cases.
If $F_{L/\mathbb{Q}}(p)(\sqrt[3]{2}) = \xi^i \sqrt[3]{2}$ with $i \neq 0$

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

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

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

Thus, in either case, $F_{L/\mathbb{Q}}(p)$ is a 2-cycle.

Exercise 2.16.
Let's first work out the exemple. It is clear that, apart from $J_L = L^* J_{L,T'}$, the data verifies the condition of the theorem.
We are now looking for a T-unit x such that

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

As $x \in \mathbb{Q}_T$, x is of the form $\pm 2^n 7^m$.
The condition $(x, -14)_\infty = -1$ imposes x to be of the form $-2^n 7^m$.
By chapter VI, the norm subgroup $N\mathbb{Q}_7(\sqrt{-14})^*$ of $\mathbb{Q}_7^*$ is of order 2 (the order of the Galois group) and contains $\mathbb{Q}_7^{*2}$.
We have $\mathbb{Q}_7^*/\mathbb{Q}_7^{*2} =< -1, 7 >$ (for a description of the squares in $\mathbb{Q}_p$ see [Ser94], Chapter 2), and as 2 is a square in $\mathbb{Q}_7^*$ and 14 is a norm, thus 7 is norm. Thus

$$(x, -14)_7 = (-1, -14)_7 = -1 \neq 1$$

Therefore, we can't find such an x.

Suppose $J_L = L^* J_{L,T'}$, and let $a \in A$ such that $\pi_v(a) \in \pi_v(A_0)$ for all $v \in T$.
First, let's lift a to an element $\tilde{a}$ of K_T.
The hypothesis tells us that $\forall v' \in T'$, $\sqrt[m]{\tilde{a}} \in K_v(\sqrt[m]{a_i}) = L_{v'}$.

Now, let $M = L(\sqrt[m]{\tilde{a}})$ then for all w dividing $v' \in T'$, we have $M_w = L_{v'}$.
Therefore, $N_{M_w/L_{v'}}(M_w^*) = L_{v'}^*$ for $v' \in T'$.
On the other hand, if $v' \notin T'$, then v' is unramified ($\tilde{a} \in K_T$) and $N_{M_w/L_{v'}}(U_w) = U_{v'}$ (Chapter VI, §1.2, proposition 1, $q = 0$).

Therefore, $J_{L,T'} = \prod_{v' \in T'} L_{v'} \prod_{v' \notin T'} U_{v'} \subset N_{M/L}(J_M)$.
And thus, the hypothesis $J_L = L^* J_{L,T'}$ tells us that $Gal(M/L) \cong J_L / L^* N_{M/L}(J_M) \cong 1$.
Thus, $M = L$ and $\sqrt[m]{\tilde{a}} \in L$.

Now as in the proof of lemma 3 in Chapter III §2. If $\sqrt[m]{\tilde{a}} \in K'(\sqrt[m]{a_1})$, let's take σ generating the Galois group, i.e. $\sigma(\sqrt[m]{a_1}) = \xi \sqrt[m]{a_1}$. $\sigma(\sqrt[m]{\tilde{a}}) = \xi^j \sqrt[m]{\tilde{a}}$. Thus by decomposing $\sqrt[m]{\tilde{a}}$ on the basis given by the powers of $\sqrt[m]{a_1}$, and by looking at the effect of σ. We obtain $\sqrt[m]{\tilde{a}} = c_j \sqrt[m]{a_1}^j$, with $c_j \in K'$.
By induction, we obtain $\sqrt[m]{\tilde{a}} = c \sqrt[m]{a_1}^{j_1} ... \sqrt[m]{a_r}^{j_r}$, and thus

$$\tilde{a} = c^m a_1^{j_1} ... a_r^{j_r}$$

And, therefore, in X, we have $a \in A_0$.

Let's prove the theorem now.
Let define $f : X \to \mu_m$ by $f((y_v)) = \prod_{v \in T} (x_v, y_v)_v =< (x_v), (y_v) >$.
Firstly remark that f is trivial on A_0. In fact,

$$f(a_i) = \prod_{v \in T} \zeta_{v,i} = 1$$

Now, define B_0 the subgroup of X generated by the $i_v(a_i)$.
We can now reformulate the problem, we are looking for an $x \in A$ such that $< x, \cdot >_{|B_0} = f_{|B_0}$.
Indeed, in that case, by evaluating on $i_v(a_i)$, we would have $< x, a_i >=< x_v, a_i >$, and this for all $v \in T$ and $i \in \{1, ..., r\}$.

By the duality $A \approx \hom(X/A, \mu_m)$, it suffices to find $g \in \hom(X, \mu_m)$ such that $g_{|A} = 1$ and $g_{|B_0} = f_{|B_0}$.

Now, by the preceding discussion, we have $A \cap B_0 = A_0$. As $f_{|A_0} = 1$, we can define $\tilde{g}$ on $A \times B_0 \subset X$ by $\tilde{g}_{|A} = 1$ and $\tilde{g}_{|B_0} = f_{|B_0}$.

If we can extend this $\tilde{g}$ to X, that concludes the exercise.
Let's make this a lemma:

Lemma: Let G be a finite group of m-torsion, H a subgroup of G. Then $Res : \hom(G, \mu_m) \to \hom(H, \mu_m)$

is surjective.

PROOF: First let prove that $Res : \hom(G, \mathbb{C}^*) \to \hom(H, \mathbb{C}^*)$ is surjective. Let $\varphi \in \hom(H, \mathbb{C}^*)$, $x \notin H$. x is of order n in G/H. Let's now define $\varphi' :< H, x > \to \mathbb{C}^*$ by sending $h \in H$ to $\varphi(h)$ and x to any nth-root of $\varphi(x^n)$.
(For one to convince himself that it is well-defined, one can use the isomorphism
$< H, x > \cong (H \oplus < x >)/ < (x^n, x^{-n}) >$).
Thus, we can extend φ to G.
Now, suppose that $\varphi \in \hom(H, \mu_m)$. Then, we can extend φ to $\varphi' : G \to \mathbb{C}^*$, but as G is of m-torsion, we have $\varphi'(G) \subset \mu_m$.

That concludes.

Exercise 3: The Hilbert Class Field

Firstly,

$$\begin{aligned}
v \text{ split completely in } L &\iff L^v = K_v && \text{(because } [L^v : K_v] = \#G^v = ef\text{)} \\
&\iff Gal(L^v/K_v) = 1 \\
&\iff G^v = 1 \\
&\iff \psi_v = 1 && \text{(equivalent because } \psi_v : K_v \to G^v \text{ is surjective)} \\
&\iff \psi_{L/K} \circ i_v = 1 \\
&\iff i_v(K_v^*) \subset \ker(\psi_{L/K}) = K^* N_{L/K}(J_L)
\end{aligned}$$

Secondly, by chapter 4, §2.7, $\psi_v : U_v \to Gal(L^v/L^v_{nr})$ is surjective. Therefore

$$\begin{aligned}
v \text{ is unramified in } L &\iff L^v = L^v_{nr} \\
&\iff Gal(L^v/L^v_{nr}) = 1 \\
&\iff \psi_v(U_v) = 1 \\
&\iff \psi_{L/K}(i_v(U_v)) = 1 \\
&\iff i_v(U_v) \subset \ker(\psi_{L/K}) = K^* N_{L/K}(J_L)
\end{aligned}$$

We have $J_K/K^*J_{K,S} \cong I_K/P_K \cong H_K$ which is finite. Thus $K^*J_{K,S}$ is of finite index in J_K. And $J_{K,S}$ is open in J_K, therefore $K^*J_{K,S}$ is open J_K.
Hence, we can use the existence theorem, and the previous remark and the unicity in the existence theorem tells us that we then have the maximal abelian extension K' of K which is unramified at all non-archimedean places and split completely at all archimedean places.
And the isomorphism $J_K/K^*J_{K,S} \cong H_K$ gives us that $F_{K'/K}$ induces indeed an isomorphism beetween H_K and $Gal(K'/K)$.

The residue class degree of a non-archimedean prime ideal in K' (which is therefore unramified) is determined by the order of its image in $Gal(K'/K) \cong H_K$.
In particular,

$$\begin{aligned}
\mathfrak{a} \text{ split completely in } L &\iff \text{its residue class degree is 1} \\
&\iff \text{its image in } Gal(K'/K) \text{ is 1} \\
&\iff F_{K'/K}(\mathfrak{a}) = 1 \\
&\iff \mathfrak{a} = 1 \text{ in } H_K \\
&\iff \mathfrak{a} \text{ is principal}
\end{aligned}$$

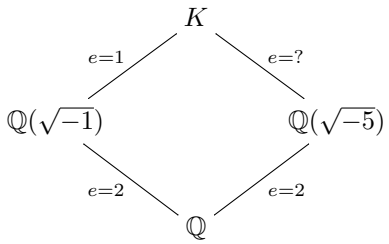
Let's work out the first three examples.

To show that an extension which is of degree the class number (the Hilbert class field degree) is the Hilbert

class field, it suffices, by unicity, to show that all archimedean primes split completely and that all non-archimedean primes are unramified.
In the cases we are interested in, the only archimedean prime is already complex and therefore split completely in any extension. Therefore, we only have to show that all non-archimedean primes are unramified.

1- Let's prove that the Hilbert class field K of $\mathbb{Q}(\sqrt{-15})$ is obtained by adding the roots of X^2+3.
We have $K=\mathbb{Q}(\sqrt{-15})(\sqrt{-3})=\mathbb{Q}(\sqrt{-15})(\sqrt{5})$, thus the discriminant of K divides $2^2 3$ and $2^2 5$ (chapter 3,) and thus divides 2^2.
Hence, if a prime v of K does not divide 2, then v is unramified.
Now, if v divides 2. As $a=-3=1+2^2(-1)=1+\lambda^2 c$, we can apply exercise 2.12, and K is unramified at v.
Conclusion: K is unramified at all non-archidean places, and thus is the Hilbert class field.

2- Let's prove that the Hilbert class field K of $\mathbb{Q}(\sqrt{-5})$ is obtained by adding the roots of X^2+1. We have $K=\mathbb{Q}(\sqrt{-5})(\sqrt{-1})$,thus the discriminant of K divides -2^2.
Hence, if v prime of K does not divide 2, then v is unramified.
Now, if v divides 2. We have the following extensions:



The index are the ramification indexes of $2\mathbb{Z}$. Let's justify them.
Top left: $K=\mathbb{Q}(\sqrt{-1})(\sqrt{5})$. So if v divides 2. As $a=5=1+2^2=1+\lambda^2 c$, we can apply exercise 2.12, and K is unramified at v.
Bottom left: $2=-i(1+i)^2$. Bottom right: As $O_{\mathbb{Q}(\sqrt{-5})}=\mathbb{Z}[\sqrt{-5}]$ ($-5=3 \bmod 4$), we can apply Kummer's theorem (see chapter III, Appendix), and we have $2O_{\mathbb{Q}(\sqrt{-5})}=(2O_{\mathbb{Q}(\sqrt{-5})}+(\sqrt{-5}+1)O_{\mathbb{Q}(\sqrt{-5})})^2$.

Finally, by multicativity of the ramification index. If v is a prime dividing 2 in $\mathbb{Q}(\sqrt{-5})$, then v in unramified in K.
Hence, K is indeed the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$.

3- Let's prove that the Hilbert class field K of $\mathbb{Q}(\sqrt{-23})$ is obtained by adding the roots of X^3-X-1 (namely x_1,x_2,x_3).
Firstly, as -23 is the discriminant of X^3-X-1, we have $K=\mathbb{Q}(\sqrt{-23})(x_1,x_2,x_3)=\mathbb{Q}(x_1,x_2,x_3)=\mathbb{Q}(\sqrt{-23})(x_i)$, for any x_i (see [Con]).
Furthermore, a calculus shows that X^3-X-1 is separable mod $\mathfrak{p}$ if and only if $\mathfrak{p}$ does not divide 23. In the case $\mathfrak{p}|23$, $\gcd(X^3-X-1,3X^2-1)=X-2/3=X-16 \bmod 23$. Thus, if $\mathfrak{p}$ does not divide 23, $\mathfrak{p}$ is unramified in K (see the lemma in appendix).
Let work out the case $\mathfrak{p}$ divides 23, i.e. $\mathfrak{p}=(\sqrt{-23})$. Let $\mathfrak{P}$ be a prime in K dividing $\mathfrak{p}$.
We have $23=(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2$. Therefore $e(\mathfrak{P}|23)\geq 2$. We have seen that X^3-X-1 is reducible and have 16 as a double root (by the above calculation of the gcd). Therefore X^3-X-1 also have

a single root in $\mathbb{Z}/23\mathbb{Z}$. By the existence of this single root and by Hensel's lemma, there is a root in $\mathbb{Q}_{23}$. It is the image a x_i in $\mathbb{Q}_{23}$.
Therefore, we have $K^{23} = \mathbb{Q}_{23}(\sqrt{-23}, x_i) = \mathbb{Q}_{23}(\sqrt{-23})$. And $K^{23}/\mathbb{Q}_{23}$ is of degree $2 = e(\mathfrak{P}|23)f((\mathfrak{P}|23))$. Hence $e(\mathfrak{P}|23) = 2$.
Thus, $e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|23)/e(\mathfrak{p}|23) = 1$. And $\mathfrak{p}$ is unramified in K.
And finally, K is indeed the Hilbert class field of $\mathbb{Q}(\sqrt{-23})$.

Let's prove that $J_K/(K^* J^+_{K,S}) \cong I_K/P^+_K$.
First $J_K/(K^* J^+_{K,S}) \cong (I_K \times \{\pm 1\}^{r_1})/Im(K^*)$, where r_1 is the number of real places.
Then, by the weak approximation theorem : the map $K^* \to I_K \times \{\pm 1\}^{r_1} \to \{\pm 1\}^{r_1}$ is surjective of kernel K^{*+}. (the last map is the projection onto $\{\pm 1\}^{r_1}$).
Thus,

$$(I_K \times \{\pm 1\}^{r_1})/Im(K^*) \cong I_K/Im(K^{*+})$$

And finally,

$$J_K/(K^* J^+_{K,S}) \cong I_K/P^+_K$$

K is real quadratic so the global units are $K_S = \{\pm 1\} \times < \epsilon >$ where ϵ is a fundamental unit.
Let $\sigma \in Gal(K/\mathbb{Q})$ be the non trivial element.
If $N\epsilon = 1$.

Either $\epsilon > 0, \sigma(\epsilon) > 0$ then $K^+_S =< \epsilon >$
Or $\epsilon < 0, \sigma(\epsilon) < 0$ then $K^+_S =< -\epsilon >$
In both case $(K_S : K^+_S) = 2$, thus $(P_K : P^+_K) = 2$ and $[K_1 : K'] = 2$.

If $N\epsilon = -1$.

Either $\epsilon > 0, \sigma(\epsilon) < 0$ then $K^+_S =< \epsilon^2 >$
Or $\epsilon < 0, \sigma(\epsilon) > 0$ then $K^+_S =< \epsilon^2 >$
In both case $(K_S : K^+_S) = 4$, thus $(P_K : P^+_K) = 1$ and $[K_1 : K'] = 1$.

Exercise 4: Numbers Represented by Quadratic Forms

Exercise 4.1.
For all $x \in K^*$, $f(x) = x^2 \neq 0$ so f does not represent 0.

Exercise 4.2.
Let $f = X^2 - bY^2$.
f represents 0 implies that there is $(x, y) \in K^2 - \{0\}$ such that $f(x, y) = x^2 - by^2 = 0$. $y = 0 \Rightarrow x = 0$, therefore $y \neq 0$.
Hence, f represents 0 implies that there is $(x, y) \in K^2 - \{0\}$ such that $b = (x/y)^2$, and thus b is in $(K^*)^2$.
Reciprocally, if b is a square $b = z^2$, then $f(z, 1) = 0$, i.e. f represents 0.

Exercise 4.3.
Let $f = X^2 - bY^2 - cZ^2$.
There are two cases depending on whether b is a square or not.
If b is a square : f represents 0 and c is a norm from $K(\sqrt{b}) = K$.
If b is not a square: $f(X, Y, 0)$ does not represent 0, so if $f(x, y, z) = 0$ then $z \neq 0$ and $c = (x/z)^2 - b(y/z)^2$ is a norm from $K(\sqrt{b})$.
Reciprocally, if $c = x^2 - by^2$ is a norm from $K(\sqrt{b})$ then $f(x, y, 1) = 0$ and f represents 0.
Hence,

$$f \text{ represents 0 if and only if } c \text{ is a norm from } K(\sqrt{b}).$$

Exercise 4.4.
To whole solution is detailed in the statement of the exercise in the book.

Exercise 4.5.
Let $f = X^2 - bY^2 - cZ^2$.

$$\begin{aligned} f \text{ represent 0 in } K_v \text{ if and only if } & \text{ c is norm from } K_v(\sqrt{b}) && \text{(Exercise 4.3)} \\ \text{if and only if } & \ (b, c)_v = 1 && \text{(Exercise 2.4)} \end{aligned}$$

By exercise 2.8, for $v \notin S(b, c)$, we have $(b, c)_v = 1$.
Thus, $(b, c)_v = 1$ for almost all v.
As $(b, c)_v \in \{\pm 1\}$, and by exercise 2.9, as

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

the number of v such that f does not represent 0 in K_v (i.e. such that $(a, b)_v = -1$) is even.

Exercise 4.6.
Let $f = X^2 - bY^2 - cZ^2 + acT^2$. And suppose that f does not represent 0 in K_v.
If $a \in (K_v)^2$, then $f(0, 0, \sqrt{a}, 1) = 0$. Thus, $a \notin (K_v)^2$.
If $b \in (K_v)^2$, then $f(\sqrt{b}, 1, 0, 0) = 0$. Thus, $b \notin (K_v)^2$.
As f does not represent 0, we have $c \notin NK_v(\sqrt{a})^*$ and $c \notin NK_v(\sqrt{b})^*$. And

$$NK_v(\sqrt{b})^* \cap cNK_v(\sqrt{a})^* = \emptyset$$

As $a, b \notin (K_v)^2$, the norm subgroups $NK_v(\sqrt{a})^*$ and $NK_v(\sqrt{b})^*$ of K_v^* are of index 2 (the order of the Galois groups $Gal(K_v(\sqrt{a})/K_v)$ and $Gal(K_v(\sqrt{b})/K_v)$). Thus as

$$K_v^* = NK_v(\sqrt{a})^* \sqcup cNK_v(\sqrt{a})^*$$

we have $NK_v(\sqrt{b})^* \subset NK_v(\sqrt{a})^*$. And thus

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

By chapter VI, §2.6, that implies that

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

which is equivalent to

$$ab \in (K_v^*)^2$$

Conversely, as $f = (X^2 - bY^2) - c(Z^2 - aT^2)$ then

$$f(K_v^4) = NK_v(\sqrt{b}) - cNK_v(\sqrt{a})$$

The set of elements A represented by f is $A = (N - cN) \cup (-cN) \cup N$ where $N = NK_v(\sqrt{a})^*$.
And as $c \notin N$, we have $N \cap cN = \emptyset$, and f does not represent 0.

Furthermore, let's suppose that $A \neq K_v^*$.
If $-1 \in N$ then $cN \cup N \subset A$ and we would have $A = K_v^*$ (N of index 2 in K_v^*), so $-1 \notin N$.
If $c \in N + N = N - cN$ (because $-1, c \notin N$), then $cN \subset N + N \subset A$, impossible. Therefore $cN \cap N + N = \emptyset$, and $N + N \subset N$.

Let's distinguish two cases:
Function Field Case: As $N + N \subset N$ and $1 \in N$, thus $p - 1 \in N$ where p is the characteristic of the field. Thus $-1 \in N$.
And therefore, we cannot have $A \neq K_v^*$.

Number Field Case: If K_v is an extension of $\mathbb{Q}_p$, then as $(p^n - 1)_{n \in N}$ is a sequence of elements of N ($N + N \subset N$ and $1 \in N$), and as N is closed in K_v^* (see chapter VI, §2.7). Then, $-1 \in N$.
And therefore, we cannot have $A \neq K_v^*$.

If $K_v = \mathbb{C}$, it is clear that $-1 \in N$.
If $K_v = \mathbb{R}$, if f is not definite, f represents $\mathbb{R}^*$, and if f is definite positive, then f represents $\mathbb{R}_+^*$.

Hence, the only case where f does not represent all K_v^* is $K_v = \mathbb{R}$ and f definite positive.

Exercise 4.7.
Firstly, if $K_v = \mathbb{R}$, then it is trivial that

$$f \text{ represents } 0 \text{ if and only if } f \text{ is not definite.}$$

Suppose now that K_v is not real. It suffices to show that any form f in 5 variables represents 0.
The preceding exercise tells us that any form in 4 variables either represents 0 or every element of K_v^* (by multiplication by a scalar we can obtained any form in 4 variables, and the properties "represents 0" and "represents K_v^*" are stable by multiplication by a scalar).
Let $f = aX_1^2 + g(X_2, X_3, X_4, X_5)$. Then if g represents 0 we are done. And if g does not represent 0, g represent $-a$ and we are also done.

Exercise 4.8.
Case $n = 1$: trivial

Case $n = 2$: Let $f = X^2 - bY^2$, and suppose that f represents 0 in K_v, for all v.
Let $L = K(\sqrt{b})$. By Tchebotarev density theorem, the density of primes that split completely in L is $1/\#Gal(L/K)$. (The image of v by $F_{L/K}$ must of order $ef = 1$, must be $Id_{K/L}$).
But, for all v, we have $K_v(\sqrt{b}) = K_v$.
Thus $\#Gal(L/K) = 1$, and $L = K$, i.e. b is a square in K, i.e. f represents 0.

Case $n = 3$: Without loss of generality, we can take $f = X^2 - bY^2 - cZ^2$. Let $L = K(\sqrt{b})$, L is cyclic, therefore the Hasse norm theorem applies (Chapter VII, §9.6), and

$$\begin{aligned} f \text{ represents 0 in K} &\text{ if and only if } c \in N_{L/K}(L^*) \\ &\text{if and only if } c \in N_{L^v/K_v}(L^{v*}), \text{ for all } v \\ &\text{if and only if } f \text{ represents 0 in } K_v, \text{ for all } v. \end{aligned}$$

Case n=4: Without loss of generality, we can take $f = X^2 - bY^2 - cZ^2 + acT^2$. Let $g = X^2 - bY^2 - cZ^2$. By exercise 4.4 and case $n = 3$, we have

$$\begin{aligned} f \text{ represents 0 in K} &\text{ if and only if } g \text{ represents 0 in } K(\sqrt{ab}) \\ &\text{if and only if } g \text{ represents 0 in } K_v(\sqrt{ab}), \text{ for all } v \\ &\text{if and only if } f \text{ represents 0 in } K_v, \text{ for all } v. \end{aligned}$$

Case $n \geq 5$: Let $f = aX_1^2 + bX_2^2 - g(X_3, ..., X_n)$, and suppose that f represents 0 in K_v for all v.
By exercise 4.5, and because g is a form in $n - 2 \geq 3$ variables, g represents 0 in K_v for all v outside a finite set S.
For $v \in S$, there is $(x_{1,v}, ..., x_{n,v}) \in (K_v^*)^n$ such that $g(x_{3,v}, ..., x_{n,v}) = ax_{1,v}^2 + bx_{2,v}^2$.
As $(K_v^*)^2$ is open in K_v^*, $g(K_v^*, ..., K_v^*)$ is open. Therefore by the weak approximation theorem, there is $(x_1, x_2) \in (K^*)^2$ such that $ax_1^2 + bx_2^2$ is sufficiently close to $ax_{1,v}^2 + bx_{2,v}^2$ for all $v \in S$, i.e. such that $ax_1^2 + bx_2^2 \in g(K_v^*, ..., K_v^*)$ for all $v \in S$.
Therefore if $c = ax_1^2 + bx_2^2$, c is represented by g in K_v, for all $v \in S$. For $v \notin S$, g represents 0 and therefore represents c.
By induction, the form $cY^2 - g(X_3, ..., X_n)$ in $n - 1$ variables represents 0 in K. Hence f does.

Exercise 4.9.
Let f be a form in $n \geq 5$ variables.
By exercise 4.7 and 4.8, we have

$$\begin{aligned} f \text{ represents 0 in K} &\text{ if and only if } f \text{ represents 0 in } K_v, \text{ for all } v \\ &\text{if and only if for all } v, \text{ such that } K_v = \mathbb{R}, f \text{ is not definite} \end{aligned}$$

Exercise 4.10.
Let $c \in \mathbb{Q}$.
c is represented by $X^2+Y^2+Z^2$ is equivalent to $f = X^2+Y^2+Z^2-cT^2$ represents 0 in $\mathbb{Q}$ which is equivalent to $f = X^2+Y^2+Z^2-cT^2$ represents 0 in $\mathbb{Q}_p$ for all p and in $\mathbb{R}$.

Condition for $\mathbb{R}$: f represents 0 in $\mathbb{R}$ if and only if f is not definite if and only if $c > 0$.

Condition for $\mathbb{Q}_p$, $p \neq 2$: As $(-1,-1)_p = 1$ (exercise 2.8 because $p \notin S(-1) = S = \{\infty, 2\}$ and $v_p(-1) = 0$), thus $X^2+Y^2+Z^2$ represents 0 in $\mathbb{Q}_p$ (exercise 4.5). And therefore, f always represents 0 in $\mathbb{Q}_p$, it does not depends on c.

Condition for $\mathbb{Q}_2$: For this case, let's specialize a demonstration from [Ser94].
Firstly, let's consider $H_a^\epsilon = \{x \in \mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 | (x,a)_2 = \epsilon\}$.
Let suppose that $a \neq 1$ in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$. Then, $NK_v^*(\sqrt{a})$ is of index two in K_v^* ($\#Gal(K_v(\sqrt{a})/K_v) = 2$). Thus the homomorphism from $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ to $\{\pm 1\}$ which send x to $(x,a)_2$ is surjective. Thus $\#H_a^\epsilon = \#(\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2)/2 = 4$.
If $a = 1$ in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$, then $\#H_1^1 = 8$ and $\#H_1^{-1} = 0$.
Thus

$$H_a^\epsilon \cap H_{a'}^{\epsilon'} = \emptyset \iff a = a' \text{ and } \epsilon = -\epsilon'$$

Now, $X_1^2+X_2^2+X_3^2-cX_4^2$ represents 0 is equivalent to

$$\{x \in \mathbb{Q}_2 | x \text{ is represented by } X_1^2+X_2^2\} \cap \{x \in \mathbb{Q}_2 | x \text{ is represented by } -X_3^2+cX_4^2\} \neq \emptyset$$

$$\{x \in \mathbb{Q}_2 | X_1^2+X_2^2-xY^2 \text{represents 0 }\} \cap \{x \in \mathbb{Q}_2 | X_3^2-cX_4^2+xY^2 \text{represents 0 }\} \neq \emptyset$$

$$\{x \in \mathbb{Q}_2 | (-1,x)_2 = 1\} \cap \{x \in \mathbb{Q}_2 | (c,-x)_2 = 1\} \neq \emptyset$$

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

And by the preceding argument $H_{-1}^1 \cap H_c^{(c,-1)_2} = \emptyset$ if and only if $c = -1$ in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ and $(c,-1)_2 = -1$ if and only if $c = -1$ in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ (because $(-1,-1)_2 = -1$).

Conclusion: $c \in \mathbb{Q}$ is a sum of three rational squares if and only if $c > 0$ and $-c \notin (\mathbb{Q}_2^*)^2$ (i.e. $v_2(c)$ is not even or $-c \neq 1 \pmod 8$, which, if we write $c = 4^n r$ where 4 does not divide r, is equivalent to $r \neq 7 \pmod 8$).

Let $c \in \mathbb{Q}$ and $c > 0$. Write $c = 4^n r$ where 4 does not divide r.
Two cases: Firstly, if $r \neq 7 \pmod 8$, then c is a sum of 3 rational squares, so indeed of 4 rational squares.
Secondly, if $r = 7 \pmod 8$, then $4^n(r-1)$ is a sum of 3 rational squares, so c is the sum of this three squares plus $(2^n)^2$.

Exercise 4.11.
We just have to verify that x' can be written with the common denominator $|a|^2 d$.
This point is the following:

$$\begin{aligned}
x' &= -\frac{2(a,x)}{|a|^2}a + x \\
&= \frac{|x-a|^2 - |x|^2 - |a|^2}{|a|^2}a + x \\
&= (\frac{|z|^2 - c}{|a|^2} - 1)a + x \\
&= \frac{|z|^2 - c}{|a|^2}a + z \\
&= \frac{|z|^2 - c}{d|a|^2}da + z
\end{aligned}$$

And that concludes, as da and z are points with integer coordinates.

Exercise 4.12.
The properties "represents 0" and "being a coset of $(K_v^*)^2$ in K_v^*" are stable by multiplication by an element of K.
Thus, without loss of generality, let assume that $f = X^2 - bY^2 - cZ^2$, and that f does not represent 0 in K_v.
Now, by exercise 4.6,

$$\begin{aligned}
\{d \in K_v^* |\text{ f represents d}\} &= \{d \in K_v^* | X^2 - bY^2 - cZ^2 - dT^2 \text{ does not represent } 0\} \\
&= \{d \in K_v^* | (-d/c) \notin (K_v^*)^2, b \notin (K_v^*)^2, b(-d/c) \in (K_v^*)^2, c \notin NK_v(\sqrt{b})\} \\
&= \{d \in K_v^* | (-d/c) \notin (K_v^*)^2, b(-d/c) \in (K_v^*)^2\} \\
&= \{d \in K_v^* | (-d/c) \notin (K_v^*)^2, (-d/c) \in b(K_v^*)^2\} \\
&= \{d \in K_v^* | (-d/c) \in b(K_v^*)^2\} \\
&= -bc(K_v^*)^2
\end{aligned}$$

Let have f positive definite and $K = \mathbb{Q}$.
f does not represent 0 in $\mathbb{R}$, and by exercise 4.5, the number of places where f does not represent 0 is even. Therefore, there is a prime p such that f does not represent 0 in $\mathbb{Q}_p$. Therefore f only represent a coset of $(Q_p^*)^2$ in Q_p^*. In particular, $(Q_p^*)^2$ and $p(Q_p^*)^2$ are two different cosets. Hence f does not represent 1 or p in $\mathbb{Q}_p$, and thus, in $\mathbb{Q}$ either.

Exercise 5: Local Norms Not Global Norms, ect.

Exercise 5.1.
Let $x \in N_1$, we have $z \in K_1^*$, then

$$x^2 = N_1(z)^2 = z^{2+2\sigma} = z^{1+\rho+\sigma+\tau} = N(z)$$

as $z^\rho = z$ and $z^\sigma = z^\tau$.
Therefore $N_1 \subset \{x \in K^* | x^2 \in N\}$, and by symmetry, $N_i \subset \{x \in K^* | x^2 \in N\}$. And as $\{x \in K^* | x^2 \in N\}$ is stable by multiplication, we have

$$N_1 N_2 N_3 \subset \{x \in K^* | x^2 \in N\}$$

Reciprocally, let $x \in K^*$ such that $x^2 \in N$, i.e. $x^2 = y^{1+\rho+\sigma+\tau}$, for a $y \in L$.
We are gonna use Hilbert's theorem 90.
Let $u = x^{-1}y^{1+\rho}$, we have $u^\rho = u$, with $u \in K_1$, which is a finite extension of K with Galois group $Gal(K_1/K) = \{1, \sigma\} = \{1, \tau\}$.
Thus by Hilbert's theorem 90, there is $y_1 \in K_1^*$ ($y_1^\rho = y_1$) such that $y_1^{\sigma-1} = y_1^{\tau-1} = x^{-1}y^{1+\rho}$.
Same for K_2, there is $y_2 \in K_2^*$ ($y_2^\sigma = y_2$) such that $y_2^{\rho-1} = y_2^{\tau-1} = x^{-1}y^{1+\sigma}$.

Now, let $y_3 = y_1 y^\rho / y_2$. We have

$$\begin{aligned} y_3^\tau &= y_1^\tau (y^\rho)^\tau / y_2^\tau \\ &= y_1 x^{-1} y^{1+\rho} y^\sigma / (y_2 x^{-1} y^{1+\sigma}) \\ &= y_1 y^\rho / y_2 \\ &= y_3 \end{aligned}$$

Therefore $y_3 \in K_3^*$. Furthermore

$$y_3^{1+\rho} = (y_1 y_2^{-1})^2 x y^{\rho-\sigma}$$

Hence,

$$x = (y_1^{-1})^{1+\sigma} y_2^{1+\tau} y_3^{1+\rho}$$

And that concludes:

$$N_1 N_2 N_3 \subset \{x \in K^* | x^2 \in N\}$$

Exercise 5.2.
Let's suppose that the local degree of L over K is 4 for some prime, then the elements which are local norms everywhere are global norms.
We have $N_1 N_2 N_3 \subset \{x \in K^* | x^2 \in N\}$, let's show that if $x \in K^*$ then x^2 is in N. We can equivalently show that x^2 is a local norm at every prime. In fact $K_v^*/NL^{v*} \cong Gal(L^v/K_v) \subset G$, so the elements of K_v^*/NL^{v*} are of order 1 or 2. Therefore $x^2 \in NL^{v*}$ for all v, and thus $x^2 \in N$.
Hence,

$$N_1 N_2 N_3 = K^*$$

Suppose now that all the local degrees are 1 or 2.
Remember that $(a,b)_v = 1$ if and only if b is a norm from $K_v(\sqrt{a})/K_v$.
Now let $v \in S_1$, we have $K_v(\sqrt{a_1}) = K_v$, thus as $a_3 = a_2 a_1$, we have $K_v(\sqrt{a_2}) = K_v(\sqrt{a_3})$, i.e. $a_2/a_3 \in (K_v^*)^2$.
And thus, $(a_2, x)_v = (a_3, x)_v$.
Thus,

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

Let's prove now that $\prod_{v\in S_1} (a_3,x)_v = \prod_{v\in S_2} (a_3,x)_v$. For that purpose, we will need the following facts:

Fact 1: If $v \in S_3$, then $(a_3, x)_v = 1$.

Fact 2: $\prod_{v\in \mathfrak{M}_K} (a_3,x)_v = 1$. (Exercise 2.9).

Fact 3: $S_1 \cap S_2 \subset S_3$. (Because $\sqrt{a_1}, \sqrt{a_2} \in K_v$, implies that $\sqrt{a_1 a_2} \in K_v$).

Fact 4: $S_1 \cup S_2 \cup S_3 = \mathfrak{M}_K$ (Because if $v \in \mathfrak{M}_K$, as G is abelian, all its conjugates are in G^v, therefore v split completely in $Fix(H) = K_i$ or L, if G^v is of order, respectively, two or one. See exercise 6.2).

We have then:

$$\begin{aligned} 1 = \prod_{v\in S_1\cup S_2\cup S_3} (a_3,x)_v &= \prod_{v\in S_1\cup S_2} (a_3,x)_v \\ &= \prod_{v\in S_1} (a_3,x)_v \prod_{v\in S_2} (a_3,x)_v \prod_{v\in S_2\cap S_1} (a_3,x)_v^{-1} \\ &= \prod_{v\in S_1} (a_3,x)_v \prod_{v\in S_2} (a_3,x)_v \end{aligned}$$

Thus,

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

Hence, we have indeed:

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

By this definition-proposition, it is now trivial that $N_1N_2N_3 \subset Ker\varphi$.
With the notation of chapter VII, §11.4, have $f : \hat{H}^0(G, L^*) \to \hat{H}^0(G, J_L)$.

$$Kerf = \left(\frac{a \in K^* | a \text{ is a local norm everywhere}}{a \in K^* | a \text{ is a global norm}} \right)$$

And $Kerf = \text{Coker } g$, Coker g is dual to $Ker(res : H^3(G, \mathbb{Z}) \to \prod_v H^3(G^v, \mathbb{Z}))$.
For all v, $H^3(G^v, \mathbb{Z})) = 0$, and $H^3(G, \mathbb{Z}) = \mathbb{Z}/2$.
Therefore $\#Kerf = 2$.

Now, consider $\begin{array}{ccc} K^* & \longrightarrow & Kerf \\ x & \longmapsto & x^2 \end{array}$.
This application is well defined, because the locals degrees are 1 or 2 (and therefore $K_v^*/NL^{v*} \leq 2$). And by exercise 5.1, it factorises by $N_1N_2N_3$.
Thus, $K^*/(N_1N_2N_3)$ is of order less than 2.
As $N_1N_2N_3 \subset Ker\varphi \subset K^*$, we have

$$Ker\varphi = N_1N_2N_3 \text{ or } Ker\varphi = K^*$$

Now, as long as one of the $(a_2, .)_v$ with $v \in S_1$, and a $(a_2, .)_v$ with $v \notin S_1$ are non trivial homomorphisms, we can use exercise 2.16 to prove the existence of an x such that $\varphi(x) = -1$, which would implies that $Ker\varphi \neq K^*$, i.e. $Ker\varphi = N_1N_2N_3$.
This condition is equivalent to $S_1 \not\subset S_2$ and $S_3 \not\subset S_2$.
In fact by the different form of φ, it suffices to show that ($S_1 \not\subset S_2$ and $S_3 \not\subset S_2$) or ($S_2 \not\subset S_1$ and $S_3 \not\subset S_1$) or ($S_1 \not\subset S_3$ and $S_2 \not\subset S_3$). And this is easy, because if it was not true, we would have $S_i = \mathfrak{M}_K$ for a certain i, but by Tchebotarev density theorem, this is possible only if $K_i = K$.

Exercise 5.3.
Firstly, let's verify that all the local degrees are 1 or 2.
For the infinite places, it is always the case.
For p prime, it suffices to show that either 13, 17 or $13 \cdot 17$ are squares in $\mathbb{Q}_p$.

First case: $p \notin \{2, 13, 17\}$. We have

$$\begin{aligned} 13 \text{ square in } \mathbb{Q}_p &\iff \left(\frac{13}{p}\right) = 1 \\ 17 \text{ square in } \mathbb{Q}_p &\iff \left(\frac{17}{p}\right) = 1 \\ 13 \cdot 17 \text{ square in } \mathbb{Q}_p &\iff \left(\frac{13 \cdot 17}{p}\right) = 1 \end{aligned}$$

And by multiplicativity of the Legendre symbol, we are done.

Second case: $p = 13$ or $p = 17$. As $\left(\frac{17}{13}\right) = 1$ and $\left(\frac{13}{17}\right) = 1$ (it is nice to prove it with the quadratic reciprocity proven exercise 1 and 2), 13 is a square in $\mathbb{Q}_{17}$ and 17 is a square in $\mathbb{Q}_{13}$.

Third case: $p = 2$, $17 \cong 1 \pmod 8$, and therefore 17 is a square in $\mathbb{Q}_2$.

Hence, we are in the setup of exercise 5.2.
Then, recall that for $\mathbb{Q}(\sqrt{13})$, if p is prime,

$$\left(\frac{p}{13}\right) = 1 \iff p \text{ splits in } \mathbb{Q}(\sqrt{13})$$

Therefore $S_1 = \{p | \left(\frac{p}{13}\right)\} \cup \infty$.
By exercise 2.8, we have if $p \notin \{2, 13, 17, \infty\}$,

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

$$(17, x)_{17} = \left(\frac{c}{17}\right)$$

where $c = (-1)^{v_{17}(x)} 17^{-v_{17}(x)} x$.

Thus, if x is a product of primes p such that $\left(\frac{p}{13}\right) = -1$. We have

$$\varphi(x) = \prod_{v \in S_1} (17, x)_v$$

If $v = \infty$, $(17, x)_v = 1$ as $17 > 0$.
If $v = v_p$ with $p = 17$, ($17 \in S_1$ as $\left(\frac{17}{13}\right) = 1$) $(17, x)_v = \left(\frac{c}{17}\right) = \left(\frac{x}{17}\right)$.
If $v = v_p$ with $\left(\frac{p}{13}\right) = 1$ and $p \neq 17$, then as $v_p(x) = 0$, we have $(17, x)_p = \left(\frac{17}{p}\right)^{v_p(x)} = 1$.

Thus,

$$\varphi(x) = \left(\frac{x}{17}\right)$$

For example, $\varphi(5) = -1$, thus $5 \notin Ker\varphi = N_1 N_2 N_3 = \{x \in \mathbb{Q}^* | x^2 \in N\}$. And thus 5^2 is not a global norm, but 5^2 is a local norm everywhere (as it is a square, and the local degrees are 1 or 2).

Exercise 5.4.
Let's consider the short exact sequence:

$$0 \longrightarrow L^* \xrightarrow{f} J_L \xrightarrow{g} C_L \longrightarrow 0$$

And the associated long exact sequence of cohomology :

$$\hat{H}^{-2}(G, J_L) \xrightarrow{g} \hat{H}^{-2}(G, C_L) \longrightarrow \hat{H}^{-1}(G, L^*) \xrightarrow{f} \hat{H}^{-1}(G, J_L) \xrightarrow{g} \hat{H}^{-1}(G, C_L)$$

Given this long exact sequence, to show that $\hat{H}^{-1}(G, L^*) = 0$, it suffices to show that:

1) That $g : \hat{H}^{-2}(G, J_L) \to \hat{H}^{-2}(G, C_L)$ is surjective.
2) That $g : \hat{H}^{-1}(G, J_L) \to \hat{H}^{-1}(G, C_L)$ is injective.

Remark: In the following, we will, as in chapter VII, identify $\hat{H}^r(G, J_L)$ with $\bigoplus_{v\in\mathfrak{M}_K} \hat{H}^r(G^v, (L^v)^*)$.

Let's prove the following lemma:
Lemma: Let w be a prime such that the local degree at w is the global degree of the extension.
Then the following diagram is commutative:

$$\begin{array}{ccc} \bigoplus_{v\in\mathfrak{M}_K} \hat{H}^r(G^v, (L^v)^*) & \xrightarrow{\quad g \quad} & \hat{H}^r(G, C_L) \\ \uparrow{\scriptstyle i_w} & & \uparrow{\scriptstyle u_{L/K}\cdot} \\ \hat{H}^r(G^w, L_w^*) & \xleftarrow[u_{L_w/K_w}\cdot]{} & \hat{H}^{r-2}(G, \mathbb{Z}) \end{array}$$

Where i_w is the inclusion, $u_{L^w/K_w}\cdot$ is the cup product with u_{L^w/K_w} the canonical generator of $\hat{H}^2(G, L^{w*})$, and $u_{L/K}\cdot$ is the cup product with $u_{L/K}$ the canonical generator of $\hat{H}^2(G, C_L)$.

Proof of the lemma Firstly, let's remark that this diagram is well defined as $\hat{H}^{r-2}(G^w, \mathbb{Z}) = \hat{H}^{r-2}(G, \mathbb{Z})$ (because $G^w = G$).
Then, the key is in the construction of $u_{L/K}$.
Chapter VII, §11.2 gives us the following commutative diagram:

$$\begin{array}{ccc} \bigoplus_{v\in\mathfrak{M}_K} \hat{H}^2(G^v, (L^v)^*) & \xrightarrow{\quad g \quad} & \hat{H}^2(G, C_L) \\ & \searrow^{inv_1} & \downarrow{\scriptstyle inv} \\ & & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \end{array}$$

with $inv_1 = \sum_v inv_v$, and $n = \#G$.
Thus, as $u_{L/K}$ is the element of $\hat{H}^2(G, C_L)$ such as $inv(u_{L/K}) = \frac{1}{n}$. Thus any element x of $\bigoplus_{v\in\mathfrak{M}_K} \hat{H}^2(G^v, (L^v)^*)$ with $inv_1(x) = \frac{1}{n}$ maps to $u_{L/K}$ through g. And, in particular, as the local degree of w is n, $i_w(u_{L^w/K_w}) = (1, 1, ..., u_{L^w/K_w}, ...)$ maps to $u_{L/K}$ through g.
And that (with the fact that g is a homomorphism) suffices to conclude the commutativity of the diagram.

Let's now apply this lemma to $r = -2$. As the cup product with $u_{L/K}$ is an isomorphism (and surjective in particular), the lemma proves 1).
Let's apply the lemma to $r = -1$. In that case, if $v \neq w$, G^v is cyclic, thus $\hat{H}^{-1}(G^v, (L^v)^*) = \hat{H}^1(G^v, (L^v)^*) = 0$ by Hilbert's theorem 90.
Thus, $i_0 : \hat{H}^{-1}(G^w, L_w^*) \to \bigoplus_{v\in\mathfrak{M}_K} \hat{H}^{-1}(G^v, (L^v)^*)$ is an isomorphism. As all the arrow in the diagram are isomorphisms, g is an isomorphism from $\bigoplus_{v\in\mathfrak{M}_K} \hat{H}^{-1}(G^v, (L^v)^*)$ to $\hat{H}^{-1}(G, C_L)$. In particular, we have proven 2).

And that concludes that

$$\hat{H}^{-1}(G, L^*) = 1$$

As $\hat{H}^{-1}(G, L_w^*) \cong \hat{H}^{-3}(G, \mathbb{Z})$.
And by the perfect duality, we have $\hat{H}^{-3}(G, \mathbb{Z}) \times \hat{H}^3(G, \mathbb{Z}) \cong \hat{H}^0(G, \mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$. And as $\hat{H}^3(G, \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. Thus,

$$\hat{H}^{-1}(G, L_w^*) = \mathbb{Z}/2\mathbb{Z}$$

Concrete illustration: $K = \mathbb{Q}$, $L = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\xi)$ with $\xi^4 = -1$.

If $p \neq 2$, by multiplicativity of the Legendre symbol $\mathbb{Q}_p(\sqrt{-1}, \sqrt{2})$ is of degree 1 or 2 over $\mathbb{Q}_p$.
If $p = 2$, $(p) = ((\xi + 1)^4)$, because $(\xi + 1)^4 = 2i(1 + \sqrt{2})^2$. Therefore, 2 is totally ramified and $\mathbb{Q}_2(\xi)/\mathbb{Q}_2$ is of degree 4.

Let $M = \mathbb{Q}(i)$, L_W, M_v the completions at the primes above 2 ($M_v = \mathbb{Q}_2(i)$ and $L_w = \mathbb{Q}_2(i, \sqrt{2})$).
We have the following commutative diagram:

$$\begin{array}{ccc} N_{L/\mathbb{Q}}^{-1}(\{1\}) & \hookrightarrow & N_{L_w/\mathbb{Q}}^{-1}(\{1\}) \\ \downarrow{\scriptstyle N_{L_w/M_v}} & & \downarrow{\scriptstyle N_{L/M}} \\ N_{L/M}(L^*) \cap N_{M/\mathbb{Q}}^{-1}(\{1\}) & \hookrightarrow & N_{L_w/M_v}(L_w^*) \cap N_{M_v/\mathbb{Q}}^{-1}(\{1\}) \end{array}$$

Remark: we have $(N_{L_w/M_v})_{|L} = N_{L/M}$. Thus by continuity of N_{L_w/M_v}, if $N_{L/\mathbb{Q}}^{-1}(\{1\})$ is dense in $N_{L_w/\mathbb{Q}}^{-1}(\{1\})$, then $N_{L/M}(L^*) \cap N_{M/\mathbb{Q}}^{-1}(\{1\})$ is dense in $N_{L_w/M_v}(L_w^*) \cap N_{M_v/\mathbb{Q}}^{-1}(\{1\})$.

Now let $z = \frac{2+i}{2-i}$.
It is clear that $N_{M_v/\mathbb{Q}}(z) = 1$. Let's prove that $z \in N_{L_w/M_v}(L_w^*)$. We have

$$z = \frac{2+i}{2-i} = \frac{(2+i)^2}{5}$$

As $(2+i)^2 = N_{L_w/M_v}(2+i)$, it suffices to prove that 5 is norm from L_w.
Let $x \in \mathbb{Q}_2$ such that $x^2 = -7$. We have

$$N_{L_w/M_v}(ix + \sqrt{2}i) = (ix)^2 - 2i^2 = 5$$

Thus, $z \in N_{L_w/M_v}(L_w^*) \cap N_{M_v/\mathbb{Q}}^{-1}(\{1\})$.

$z(M_v^*)^2$ induces an open subset in $N_{L_w/M_v}(L_w^*) \cap N_{M_v/\mathbb{Q}}^{-1}(\{1\})$ containing z.
Let's show that $X = z(M_v^*)^2 \cap (N_{L/M}(L^*) \cap N_{M/\mathbb{Q}}^{-1}(\{1\})) = \emptyset$.

Remark: from now on, we will make an extensive use of the fact that $\mathbb{Z}[i]$ the ring of integers of $\mathbb{Q}(i)$ is factorial. The primes in $\mathbb{Z}[i]$ are the following :

- if $p = 3 \pmod 4$, p is prime in $\mathbb{Z}[i]$.
- if $p = 1 \pmod 4$, there are two primes dividing p, π and $\bar{\pi}$.

- if $p = 2$, there is one prime dividing p. Explicitly, $2 = -i(1+i)^2$.

Firstly, let $x \in \mathbb{Q}(i)^*$ such that $N_{M/\mathbb{Q}}(x) = 1$. By writing x as $\frac{y_1}{y_2}$ with y_1, y_2 coprime in $\mathbb{Z}[i]$, by decomposing y_1 and y_2 into their prime factors, and by taking the norm, we see that we must have $x = u\frac{y}{\bar{y}}$, with u a unit, i.e. $u \in \{\pm 1, \pm i\}$.
As $\frac{1+i}{1-i} = i$, we can assume that $u \in \pm 1$.
Let's say $y = v + iu$ and $m = u^2 + v^2$, such that $x = \pm 1\frac{y^2}{m} = \frac{t^2}{m}$.

Now, $x = \frac{t^2}{m} \in z(M_v^*)^2 = z(\mathbb{Q}_2(i)^*)^2 = 5(\mathbb{Q}_2(i)^*)^2$ is equivalent to $5m \in (\mathbb{Q}_2(i)^*)^2$.
As $5m$ is real, it implies that $\pm 5m \in \mathbb{Q}_2^2$.
Write $m = 2^{v_2(m)}m_0$, it implies that $v_2(m)$ is even and $\pm 5m_0 = 1 \pmod 8$ (i.e. $m = \pm 5 \pmod 8$).

Let's prove that all the positive integers represented by $X^2 + Y^2$ are of the form

$$m = 2^{\alpha_2} \prod_{p=1 \pmod 4} p^{\alpha_p} \prod_{p=3 \pmod 4} p^{2\beta_p}$$

by making it a direct application of exercise 4.

$$\begin{aligned}
m \text{ is represented by } X^2+Y^2 \text{ in } \mathbb{Z} &\iff m \text{ is represented by } X^2+Y^2 \text{ in } \mathbb{Q} && \text{(exercise 4.9)}\\
&\iff m \text{ is represented by } X^2+Y^2 \text{ in } \mathbb{Q}_v, \forall v && \text{(exercise 4.8)}\\
&\iff X^2+Y^2-mZ^2 \text{ respresents 0 in } \mathbb{Q}_v, \forall v\\
&\iff (-1,n)_v = 1, \text{ for all } v && \text{(exercise 4.5)}\\
&\iff (-1,n)_p = 1, \text{ for all odd primes } p \qquad && ((-1,n)_\infty = 1 \text{ and } \prod (-1,n)_v = 1)
\end{aligned}$$

And, as, for $p = 1 \pmod 4$, $(-1,n)_p = \left(\frac{-1}{p}\right)^{v_p(n)} = 1$, and for $p = 3 \pmod 4$, $(-1,n)_p = \left(\frac{-1}{p}\right)^{v_p(n)} = (-1)^{v_p(n)}$, then

$$m \text{ is represented by } X^2+Y^2 \text{ in } \mathbb{Z} \iff \text{ for all prime } p = 3 \pmod 4, v_p(n) \text{ is even.}$$

Let's come bake to our m. The preceding fact tells us that $m_0 = \prod_{p=1 \pmod 4} p^{\alpha_p} \prod_{p=3 \pmod 4} p^{2\beta_p}$, which implies that $m_0 = 1 \pmod 4$. And as we had $m_0 = \pm 5 \pmod 8$, we finally have

$$m_0 = 5 \pmod 8$$

As $m_0 = 5 \pmod 8$, there is a prime $p_0 = 5 \pmod 8$ such that α_{p_0} is an odd positive integer.

Suppose now that $x = \frac{t^2}{m}$ is in $N_{L/M}(L^*)$, which is equivalent to $m \in N_{L/M}(L^*)$, i.e. $m = u^2 - 2v^2$ with $u, v \in \mathbb{Q}(i)$. Let multiply by d^2 where d is the common denominator d of u, v and divide by d'^2 where d' is $\gcd(du, dv)$.
Therefore, we have $m' = u'^2 - 2v'^2$, with $u', v', m' \in \mathbb{Z}[i]$, u', v' are coprime and $p_0 | m'$, as we have divided by

a square and α_0 was odd.

Now, we have

$$0 = \bar{u'}^2 - 2\bar{v'}^2 \pmod{p_0\mathbb{Z}[i]}$$

But as $p_0 = 5 \pmod 8$, 2 is not a square in $\mathbb{Z}/p_0\mathbb{Z}$, and $\mathbb{Z}/p_0\mathbb{Z} = \mathbb{Z}[i]/p_0\mathbb{Z}[i]$, as -1 is square in $\mathbb{Z}/p_0\mathbb{Z}$ ($p_0 = 1 \pmod 4$). (See exercise 1.10 for the criterion of being a square).
Therefore, it follows that $\bar{v'} = 0 \pmod{p_0\mathbb{Z}[i]}$ and $\bar{u'} = 0 \pmod{p_0\mathbb{Z}[i]}$, i.e. $p_0|u'$ and $p_0|v'$. Contradiction with the fact that u' and v' are coprime.

Hence, as announced,

$$z(M_v^*)^2 \cap (N_{L/M}(L^*) \cap N_{M/\mathbb{Q}}^{-1}(\{1\})) = \emptyset$$

Exercise 6: On Decomposition of Primes

Exercise 6.1.
Let ML/K be the compositum of M and L. And let S contains the archimedean primes and the primes ramified in ML.
Then,

$$\begin{aligned}
\mathfrak{p} \in Spl_S(LM/K) &\iff F_{ML/K}(\mathfrak{p}) = (1) && \text{(as a conjuguacy class of } Gal(ML/K)) \\
&\iff F_{ML/K}(\mathfrak{p})_{|M} = (1) \text{ and } F_{ML/K}(\mathfrak{p})_{|L} = (1) \\
&\iff F_{L/K}(\mathfrak{p}) = (1) \text{ and } F_{M/K}(\mathfrak{p}) = (1) && \text{(by the demonstration of §3.2, chapter VII)} \\
&\iff \mathfrak{p} \in Spl_S(L/K) \text{ and } \mathfrak{p} \in Spl_S(M/K)
\end{aligned}$$

Thus,

$$Spl_S(LM/K) = Spl_S(L/K) \cap Spl_S(M/K)$$

Then,

$$\begin{aligned}
L \subset M &\Rightarrow Spl_S(M/K) \subset Spl_S(L/K) && (\text{as } F_{M/K}(\mathfrak{p})_{|L} = F_{L/K}(\mathfrak{p})) \\
&\Rightarrow Spl_S(LM/K) = Spl_S(M/K) \\
&\Rightarrow [LM : K] = [M : K] && \text{(By Tchebotarev density theorem)} \\
&\Rightarrow L \subset M
\end{aligned}$$

Thus

$$L = M \iff Spl_S(M/K) = Spl_S(L/K)$$

Application:
Firstly, we can take f unitary.
Secondly, choice of S: S will contain the following primes

- the archimedean primes
- the primes $\mathfrak{p}$ such that $f \notin \mathcal{O}_{\mathfrak{p}}[X]$
- the primes $\mathfrak{p}$ such that f does not split mod $\mathfrak{p}$
- the primes $\mathfrak{p}$ dividing the discriminant of f

Assertion: For all prime $\mathfrak{p}$ outside S, $\mathfrak{p}$ splits completely in the splitting field of f.

Thirdly, let's consider $K(\alpha)/K$ with α separable and let $f = \pi_{\alpha,K}$ the minimal polynomial of α. Have $\mathfrak{p}$ outside S.
f is separable. And if $\overline{f}$ is the image of f mod $\mathfrak{p}$, then $\overline{f}$ is separable because if α_i, α_j are different roots of f in an algebraic closure, then $\mathfrak{p} \not| \alpha_i - \alpha_j$, as $\mathfrak{p}$ does not divide the discriminant of f.
Thus, if $\overline{f}$ splits mod $\mathfrak{p}$, we can Hensel's lemma, and f split in $K_{\mathfrak{p}}$. Therefore,

$$K(\alpha) \otimes_K K_{\mathfrak{p}} = K_{\mathfrak{p}}^{deg(f)}$$

i.e. $\mathfrak{p}$ splits completely in $K(\alpha)$.

Now, the general case of the assertion is obtained by induction and by the following facts:

- If $g|f$ and f is separable and splits mod $\mathfrak{p}$, then g does too.
- If $K \subset M \subset L$, if $\mathfrak{p}$ splits completely, into the product of $\mathfrak{p}_1, ..., \mathfrak{p}_n$, primes in M, and if each primes $\mathfrak{p}_i$ splits completely in L, then $\mathfrak{p}$ splits completely in L.

Therefore, the assertion is true.

Now, as the splitting field of f is Galois over K, and as $Spl_S(K) = \mathfrak{M}_K - S \subset Spl_S(L)$, then $L \subset K$. And thus,

$$L = K, \text{ i.e. } f \text{ splits into linear factors in } K.$$

Exercise 6.2.
Suppose that v splits completely in E (i.e. $G^v = \{Id\}$). Let $\sigma \in G_w$ with w a prime in L above v, and let w_E the corresponding prime in E.
We have $\sigma_{|E} \in G_{w_E}$. But $G_{w_E} = \{Id\}$. Therefore $\sigma_{|E} = Id$ and $\sigma \in Gal(L/E)$. Thus $G_w \subset Gal(L/E)$, and this is true for all w above v (i.e. for all conjugates of G^v).

Reciprocally, suppose that for all w prime in L above v, $G_w \subset H$.
Let w_E be a prime in L above v.
Let $\sigma_E \in G_{w_E}$ and $\sigma \in Gal(L/K)$ such that $\sigma_{|E} = \sigma_E$.
Then, let w prime in L above w_E, and $w' = \sigma(w)$.
There is $\tau \in Gal(L/E)$ such that $\tau(w') = w$.
Therefore

$$(\tau \circ \sigma)w = w$$

i.e. $\tau \circ \sigma \in G_w \subset H$, and $\sigma \in \tau^{-1}H = H$. Therefore $\sigma_E = \sigma_{|E} = Id$. And $G_{w_E} = \{Id\}$, and this is true for all w_E, therefore v splits completely in E.
Finally,

$$v \text{ splits completely in } E \text{ if and only if all the conjugates of } G^v \text{ are contained in } H$$

Now, suppose that v has a split factor in E.
There is w_E above v such that $G_{w_E} = \{Id\}$. Then, for all w prime in L above w_E, if $\sigma \in G_w$, $\sigma_{|E} \in G_{w_E}$ (i.e. $\sigma_{|E} = Id$). Thus $G_w \subset H$.

Reciprocally, suppose that $G_w \subset H$, with w prime in L. w is above w_E prime in E.
And, let $\sigma_E \in G_{w_E}$, $\sigma \in Gal(L/K)$ such that $\sigma_{|E} = \sigma_E$. Then, $w' = \sigma(w)$ and there is $\tau \in Gal(L/E)$ such that $\tau(w') = w$.
Therefore

$$(\tau \circ \sigma)w = w$$

i.e. $\tau \circ \sigma \in G_w \subset H$, and $\sigma \in \tau^{-1}H = H$. Therefore $\sigma_E = \sigma_{|E} = Id$. And $G_{w_E} = \{Id\}$, therefore v has a split factor in E.

Let S contains the archimedean primes, and the primes that ramify in L. We have

$$\begin{aligned} Spl'_S(E/K) &= \{v \notin S, v \text{ has a split factor in } E\} \\ &= \{v \notin S, \exists \rho \in G, \rho G^v \rho^{-1} \subset H\} \\ &= \{v \notin S, \exists \rho \in G, F_{L/K}(v) \text{ is the conjugacy class of an element in } \rho^{-1} H \rho\} \\ &= \{v \notin S, F_{L/K}(v) \text{ is the conjugacy class of an element in } H\} \\ &= \bigsqcup_{<\sigma>, \sigma \in H} \{v \notin S, F_{L/K}(v) =< \sigma >\} \end{aligned}$$

Thus by Tchebotarev density theorem (and S finite),

$$Spl'_S(E/K) \text{ has density } |\bigcup_{\rho \in G} \rho H \rho^{-1}|/|G|.$$

We have $\bigcup_{\rho \in G} \rho H \rho^{-1} = \bigcup_{\rho \in G/H} \rho H \rho^{-1} = \left(\bigcup_{\rho \in G} \rho (H-1) \rho^{-1} \right) \bigcup \{1\}$.
Thus

$$\begin{aligned} |\bigcup_{\rho \in G} \rho H \rho^{-1}| &\leq |G/H|(|H|-1)+1 \\ &\leq |G| - |G/H| + 1 \end{aligned}$$

Therefore, if H is a proper subgroup, then $|\bigcup_{\rho \in G} \rho H \rho^{-1}| < |G|$.

If $Spl'_S(E/K)$ has density 1, then $H = G$ and $E = K$.

Application: Let f be an irreducible separable polynomial. Let L be the splitting field of f. And $E = K(\alpha)$, with α a root of f.
Let S contains the following primes:

- the archimedean primes
- the primes $\mathfrak{p}$ such that f has no root mod $\mathfrak{p}$,
- the primes $\mathfrak{p}$ such that $f \notin \mathcal{O}_{\mathfrak{p}}[X]$
- the primes $\mathfrak{p}$ dividing the discriminant of f

The same reasoning as in exercise 6.1 applies, and, therefore by Hensel's lemma, f has a root in $K_{\mathfrak{p}}$ for all $\mathfrak{p} \notin S$.
Thus, for all $\mathfrak{p} \notin S$, $\mathfrak{p}$ has a spit factor in E.
Therefore $Spl'_S(E/K)$ has density 1. And $E = K$.
And therefore f has a root in K (i.e. $f = X - \alpha$).

Example of what can happen for f reducible: Let $f = (X-a)(X-b)(X-ab)$ with a, b, ab non squares in $\mathbb{Q}_p$. (This is always possible in $\mathbb{Q}_p$, see [Ser94], Chapter 2).
In a finite field, the product of two non squares is a square. Therefore, f has a root mod p for all p. But f

has no root in $\mathbb{Q}_p$.

Exercise 6.3.
Let $\rho : G \to Aut(\mathbb{C}[G/H])$ and $\rho' : G \to Aut(\mathbb{C}[G/H'])$ the permutation representations of G corresponding, respectively, to H and H'.

$$\rho \sim \rho' \iff \chi_\rho = \chi_{\rho'}$$

Fact:
$$\chi_\rho(g) = tr(\rho(g)) = \#\{g'H \in G/H, gg'H = g'H\} = \#\{g'H \in G/H, g'^{-1}gg' \in H\}$$

Thus, $g = 1$ gives us $\#G/H = \#G/H'$, i.e. $\#H = \#H'$.
And thus $\chi_\rho(g) = \#\{g' \in G, g'^{-1}gg' \in H\}/\#H = \#(< g > \cap H)\#C_G(g)/\#H$.
Thus,

$$\rho \sim \rho' \iff \#(< g > \cap H) = \#(< g > \cap H'), \forall g \in G$$

Remark: If $H \lhd G$, $\chi_\rho = \mathbb{1}_H$. Therefore, this phenomenon happens only if $H = H'$.

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

Fact: In $\mathfrak{S}_6$, every product of two disjoint transpositions are conjugates. Therefore, H and H' satisfy the above condition.
But we also have $\#supp(H) = \#supp(gHg^{-1})$ and $\#supp(H) \neq \#supp(H')$, therefore H and H' are not conjugates.

Exercise 6.4.
A correction of this exercise can be found in [Per77].
For the sake of completeness, and because the demonstration is not in [Per77] but is said to be in [Has70] (which seems impossible to find), let's highlight the link between the Galois group and the decomposition of primes. This is all taken from [Kli98] (chapter 1).

Firstly, let's define the decomposition type.

Definitions:

a) Let K/k be an extension of number fields, $\mathfrak{p}$ a prime of k.
If $\mathfrak{p}$ has exactly r prime divisors in K with residue degrees $f_1 \leq ... \leq f_r$, we call

$$A_{K/k}(\mathfrak{p}) = (f_1, ..., f_r)$$

the decomposition type of $\mathfrak{p}$ in K.

b) If a permutation σ of n objects decomposes into a product of r disjoint cycles of length $f_1 \leq ... \leq f_r$ with all fixed points included as cycles of length 1 (hence $f_1 + ... + f_r = n$), then we call $(f_1, ..., f_r)$ the cycle type of σ.

Theorem:
Let $K = k(a)/k$ be a finite extension of number fields. N/k a Galois extension containing K with Galois group $G = Gal(N/k)$.
Then, for any prime ideal $\mathfrak{p}$ of k which is unramified in N the following statements are equivalent:

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

ii) The Frobenius automorphism F of any prime $\mathfrak{O}$ of N over $\mathfrak{p}$ acting on n conjugates of a has cycle type $(f_1, ..., f_r)$.

PROOF: Let $\mathfrak{O}$ prime of N dividing $\mathfrak{p}$, $F = F_{N/k}(\mathfrak{O})$ and $\mathfrak{P}_\sigma = \mathfrak{O}^\sigma \cap K$.
Then

$$\begin{aligned}
\mathfrak{P}_\sigma = \mathfrak{P}_{\sigma'} &\iff \mathfrak{O}^\sigma \text{ conjugate to } \mathfrak{O}^{\sigma'} \text{ over } K \\
&\iff \mathfrak{O}^\sigma = \mathfrak{O}^{\sigma'\tau} \text{ for some } \tau \in Gal(N/K) \\
&\iff \sigma'\tau\sigma^{-1} \in G_{\mathfrak{O}} \text{ for some } \tau \in Gal(N/K) \\
&\iff \sigma'\tau = F^m\sigma \text{ for some } m \in \mathbb{Z}, \tau \in Gal(N/K) \\
&\iff \sigma'(a) = F^m\sigma(a) \text{ for some } m \in \mathbb{Z} \\
&\iff \sigma'(a) \text{ belongs to the orbit of } \sigma(a) \text{ under } < F > \\
&\iff \sigma'(a) \text{ and } \sigma(a) \text{ belongs to the same cycle of } F
\end{aligned}$$

Hence there are as many different prime divisors $\mathfrak{P}_\sigma$ of $\mathfrak{p}$ in K as there are cycles of F under its action on the conjugates of a.
To conclude, we are going to use a combinatorial argument. As the sum of the length of the cycles must be n which is also the sum if the local degrees (as $\mathfrak{p}$ is unramified), it suffices to prove:

$$F^m(\sigma(a)) = \sigma(a) \iff f(\mathfrak{P}_\sigma|\mathfrak{p}) \text{ divides } m$$

And

$$\begin{aligned}
F^m(\sigma(a)) = \sigma(a) &\iff \sigma^{-1}F^m\sigma \in Gal(N/K) \\
&\iff (F^\sigma)^m \in Gal(N/K) \cap G_{\mathfrak{O}^\sigma} = D_{N/K}(\mathfrak{O}^\sigma) \\
&\iff (F^\sigma)^m \in < F_{N/K}(\mathfrak{O}^\sigma) > = < (F^\sigma)^{f(\mathfrak{P}_\sigma|\mathfrak{p})} > \\
&\iff m = df(\mathfrak{P}_\sigma|\mathfrak{p}) \bmod ord(F^\sigma) \\
&\iff f(\mathfrak{P}_\sigma|\mathfrak{p}) | m \qquad \text{(because } ord(F^\sigma) = f(\mathfrak{O}^\sigma|\mathfrak{p}) = f(\mathfrak{O}^\sigma|\mathfrak{P}_\sigma)f(\mathfrak{P}_\sigma|\mathfrak{p})\text{)}
\end{aligned}$$

That concludes.

We have now the following corollary:

Corollary:
Let K/k be a finite extension of number fields, N/k a Galois extension containing K with $G = Gal(N/k)$ its Galois group and $H = Gal(N/K)$ the subgroup corresponding to K.
Let χ_H denote the character of the permutation representation of G corresponding to H.

Then for all primes $\mathfrak{p}$ of K which are unramified in N, the decomposition type in K is uniquely determined by the character χ_H.
Explicitly: If $F = F_{N/k}(\mathfrak{O})$, with $\mathfrak{O}$ dividing a unramified prime $\mathfrak{p}$, then the decomposition type $(f_1, ..., f_r)$ of $\mathfrak{p}$ in K is recursively given by by the formulae:

$$\chi_H(F^s) = \sum_{i \in \{1,...,r\}, f_i | s} f_i$$

for $s \in \mathbb{N}^*$.

PROOF: As G acts transitively on the conjugates of a, and as the stabilizer subgroup of a is H, the action of G on $Conj_{N/k}(a)$ is the same as on G/H.
In fact, we have the following commutative diagram:

$$\begin{array}{ccc} & G & \\ \swarrow & & \searrow \\ G/H & \xrightarrow{\sim} & Conj_{N/k}(a) \end{array}$$

Thus, by the previous theorem, it suffices to show that the cycle type of F acting on G/H is determined by χ_H.
Let $\sigma = \prod_{i=1}^{r} \sigma_i$ and with f_i the length of σ_i, and with the σ_i are of disjoint support.
Then, $\sigma^s = \prod_{i=1}^{r} \sigma_i^s$ and $\chi_H(\sigma^s) = \sum_{i=1}^{r} \chi_i(\sigma_i^s)$, with χ_i compting the number of fixed points by permutations of the elements of the support of σ_i.
As the σ_i are cycles, $\chi_i(\sigma_i^s) = 0$ if $f_i \not| s$ or $\chi_i(\sigma_i^s) = f_i$ if $f_i | s$.
Therefore,

$$\chi(\sigma^s) = \sum_{i \in \{1,...,r\}, f_i | s} f_i$$

That concludes.

Exercise 7: A Lemma on Admissible Maps

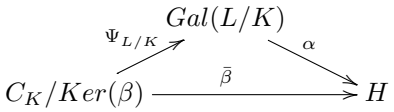
Exercise 7.1.
Let $\varphi : I^S \to H$ be an admissible homomorphism.
By chapter VII, §4.1, there is $\beta : C_K \to H$ such that

- β is continuous
- $\beta(\bar{x}) = \phi((x)^S)$, for all $x \in J_K^S$

As β is continuous and H discrete, $Ker(\beta)$ is open.
By the existence theorem (chapter VII, §5.1), there is an abelian extension L/K such that $Ker(\beta) = N_{L/K}C_L$ and $\Psi_{L/K} : C_K/Ker(\beta) \xrightarrow{\sim} Gal(L/K)$.

Let v be outside S and $x \in U_v$, $\varphi((x)^S) = \varphi(0) = 1$. Thus, the image of $i_v(U_v)$ in C_K is in $Ker(\beta)$. Therefore, by exercise 3.1, v is unramified in L/K.

Let α be such that the following diagram is commutative:



$\alpha = \bar{\beta} \circ \Psi_{L/K}^{-1}$ is injective as $\bar{\beta}$ and $\Psi_{L/K}^{-1}$ are injective.

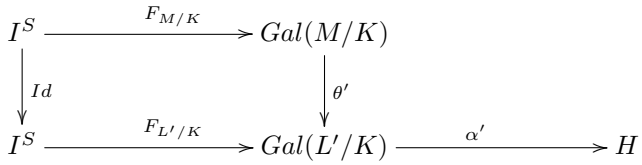
If $\mathfrak{a} \in I^S$ and $x \in J_K^S$ such that $(x)^S = \mathfrak{a}$, then

$$\varphi(\mathfrak{a}) = \varphi((x)^S) = \beta(\bar{x}) = \bar{\beta}(\bar{\bar{x}}) = \alpha \circ \Psi_{L/K}(\bar{\bar{x}}) = \alpha(F_{L/K}((x)^S)) = \alpha(F_{L/K}(\mathfrak{a}))$$

Exercise 7.2.
As α is injective, $\varphi(v) = 1$ for all prime v in a set of density 1 implies $F_{L/K}(v) = 1$ for all prime v in a set of density 1.
But, by Tchebotarev density theorem, $\{v \in \mathfrak{M}_K | F_{L/K}(v) = 1\}$ has density $\frac{1}{\#Gal(L/K)}$.
Therefore, $\#Gal(L/K) = 1$ and $L = K$. And $F_{L/K} = 1$. And $\varphi = \alpha \circ F_{L/K} = 1$.

Exercise 7.3.
By "transport de structure", let's suppose that L and L' live in the same algebraic closure.
Firstly, $\alpha' \circ F_{L'/K}$ is an admissible homomorphism since $F_{L'/K}$ is an admissible homomorphism.
Thus, by exercise 7.2, $\alpha' \circ F_{L'/K} = \varphi = \alpha \circ F_{L/K}$.

Now, let M be the compositum of L and L'.
Then, we have the following diagrams from chapter VII, §3.2:



$$\begin{array}{ccccc} I^S & \xrightarrow{F_{M/K}} & Gal(M/K) & & \\ \downarrow{\scriptstyle Id} & & \downarrow{\scriptstyle \theta} & & \\ I^S & \xrightarrow{F_{L/K}} & Gal(L/K) & \xrightarrow{\alpha} & H \end{array}$$

Thus, $\alpha' \circ \theta' \circ F_{M/K} = \alpha \circ \theta \circ F_{M/K}$.

As $F_{M/K}$ is surjective (consequence of Tchebotarev density theorem) and α, α' is injective, $Ker\theta = Ker\theta'$.
Thus, $Gal(M/L) = Gal(M/L')$, i.e. $L = L'$.
And again by surjectivity, $\alpha' \circ F_{L/K} = \alpha \circ F_{L/K}$ implies $\alpha = \alpha'$.

Thus, in the general case (we do not impose that L and L' are in the same algebraic closure), by "transport de structure" (α, L) and (α', L') share the same properties.

Exercise 8: Norms from Non-abelian Extensions

The following diagram is commutative:

$$\begin{array}{ccc} H^{ab} & \xrightarrow{\sim} & C_E/N_{L/E}C_L \\ \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle N_{E/K}} \\ G^{ab} & \xrightarrow{\sim} & C_K/N_{L/K}C_L \end{array}$$

Thus,

$$Gal(M/K) \simeq G^{ab}/\theta(H^{ab}) \simeq \frac{C_K/N_{L/K}C_L}{N_{E/K}C_E/N_{E/K}N_{L/E}C_L} \simeq C_K/N_{E/K}C_E$$

(As $N_{E/K}N_{L/E} = N_{L/K}$).

As, by class field theory, $Gal(M/K) \simeq C_K/N_{M/K}C_M$, $N_{M/K}C_M$ and $N_{E/K}C_E$ have the same index in C_K.

As $N_{M/K}N_{E/M} = N_{E/K}$, we have $N_{E/K}C_E \subset N_{M/K}C_M$.
Thus,

$$N_E/KC_E = N_{M/K}C_M$$

Appendix

Let's state a useful criterion for a separable extension to be unramified at a certain prime.
A more complete result can be found in [Cox13] (chapter 5, proposition 5.11).

Lemma: Let L/K be a Galois extension, where $L = K(\alpha)$ for some $\alpha \in \mathcal{O}_L$. Let $f(x)$ be the monic minimal polynomial of α over K, so that $f(x) \in \mathcal{O}_K[x]$. If $\mathfrak{p}$ is prime in $\mathcal{O}_K$ and $f(x)$ is separable modulo $\mathfrak{p}$, then $\mathfrak{p}$ is unramified in L.

Proof: Let $\mathfrak{P}$ be a prime of $\mathcal{O}_L$ containing $\mathfrak{p}$, and let $G_{\mathfrak{P}}$ be the associated decomposition subgroup. $G_{\mathfrak{P}}$ is of order ef.

Let $f(x) = f_1(x)...f_r(x) \pmod{\mathfrak{p}}$ where the $f_i(x)$ are distinct and irreducible mod $\mathfrak{p}$. Then as $f(\alpha) = 0$, $f_1(\alpha)...f_g(\alpha) \in \mathfrak{p} \subset \mathfrak{P}$. Thus, $f_i(\alpha) \in \mathfrak{P}$ for some i. Let's assume $f_1(\alpha) \in \mathfrak{P}$, i.e. $f_1(\alpha) = 0$ in $\mathcal{O}_L/\mathfrak{P}$.
Thus, $deg(f_1(x)) = [(\mathcal{O}_K/\mathfrak{p})(\alpha) : \mathcal{O}_K/\mathfrak{p}] \leq [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = f$.

Now, $f_1(\sigma(\alpha)) \in \mathfrak{P}$ for all $\sigma \in G_{\mathfrak{P}}$. As $f(x)$ is separable mod $\mathfrak{p}$, the $\sigma(\alpha)$ for $\sigma \in G = Gal(L/K)$ are all different in $\mathcal{O}_L/\mathfrak{P}$ (they run through all the roots of f mod $\mathfrak{p}$). Therefore $\#G_{\mathfrak{P}} \leq deg(f_1(x))$.
Hence, as $\#G_{\mathfrak{P}} = ef$. We have $e = 1$, $f = deg(f_1(x))$. And $\mathfrak{p}$ is unramified in L.

Furthermore, this reasoning tells us that, for all i, there is an associated coset $\sigma G_{\mathfrak{P}}$ such that the roots of f_i in $\mathcal{O}_L/\mathfrak{P}$ are the images of α by this coset. (You first take σ such that α is a root of $f_i \circ \sigma = 0$ in $\mathcal{O}_L/\mathfrak{P}$ and then $f_i \circ \sigma | f \circ \sigma = f$, thus $f_i \circ \sigma = f_1 \bmod \mathfrak{p}$). Therefore, all polynomial f_i have the same degree f, and therefore the number of polynomial g is the number of prime in L dividing $\mathfrak{p}$.

We can therefore state an easy corollary of this demonstration.

Corollary: In addition, if f has a root in $\mathcal{O}_K/\mathfrak{p}$, then $\mathfrak{p}$ splits completely in L.

References

[Con] Keith Conrad. *Galois groups of cubics and quartics (not in characteristic 2)*. URL: `http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf`.

[Cox13] David A. Cox. *Primes of the Form x2+ny2*. Wiley. 2 edition, 2013.

[Has70] Helmut Hasse. *Zahlbericht*. Physica-Verlag, Wiirzburg/Vienna, 1970.

[Kli98] Norbert Klingen. *Arithmetical similarities : prime decomposition and finite group theory*. Clarendon Press, 1998.

[Per77] Robert Perlis. *On the equation $\zeta_k(s) = \zeta_{k'}(s)$*. 1977. URL: `https://www.sciencedirect.com/science/article/pii/0022314X77900701`.

[Ser94] Jean-Pierre Serre. *Cours d'arithmétique*. PUF, 1994.