D-MATH
Prof. Richard Pink

Number Theory II

FS 2024

Solutions 25

Local Class Field Theory

1. Determine the group of norms $\mathrm{Nm}_{K/\mathbb{Q}_2} K^\times$ for

   (a) $K = \mathbb{Q}_2(\sqrt{-1})$.

   (b) $K = \mathbb{Q}_2(\sqrt{2})$.

   Solution

   (a) Setting $i := \sqrt{-1}$, as in exercise 3 of sheet 23 the extension $K/\mathbb{Q}_2$ is ramified of degree 2 and $\mathcal{O}_K = \mathbb{Z}_2[i]$. The computation $(1-i)^2 = -2i$ implies that $\mathfrak{m}_K := (1-i)$ is the maximal ideal of $\mathcal{O}_K$. Also $1+1=2$ and $1+(-1)=0$ and $1-(\pm i)$ are representatives of $\mathfrak{m}_K/\mathfrak{m}_K^3$; hence the residue classes of ± 1 and $\pm i$ make up the group of units $(\mathcal{O}_K/\mathfrak{m}_K^3)^\times$. Together this implies that

   $$K^\times \;=\; (1-i)^{\mathbb{Z}} \times \mu_4 \times (1+\mathfrak{m}_K^3).$$

   Moreover, since $v((1-i)^3) > v(2)$, the maps exp and log induce a natural isomorphism

   $$(1+\mathfrak{m}_K^3, \cdot) \;\cong\; (\mathfrak{m}_K^3, +) \;=\; 2(1-i)\mathbb{Z}_2 \oplus 4\mathbb{Z}_2.$$

   Since $\mathrm{Tr}_{K/\mathbb{Q}_2}(2(1-i)) = 4$ and $\mathrm{Tr}_{K/\mathbb{Q}_2}(4) = 8$ this implies that $\mathrm{Tr}_{K/\mathbb{Q}_2}(\mathfrak{m}_K^3)) = 4\mathbb{Z}_2$ and hence

   $$\mathrm{Nm}_{K/\mathbb{Q}_2}(1+\mathfrak{m}_K^3) \;=\; \exp(\mathrm{Tr}_{K/\mathbb{Q}_2}(\mathfrak{m}_K^3)) \;=\; \exp(4\mathbb{Z}_2) \;=\; 1+4\mathbb{Z}_2.$$

   On the other hand μ_4 is generated by i with $\mathrm{Nm}_{K/\mathbb{Q}_2}(i) = 1$, and we have $\mathrm{Nm}_{K/\mathbb{Q}_2}(1-i) = (1-i)(1+i) = 2$. Together this shows that

   $$\mathrm{Nm}_{K/\mathbb{Q}_2}(K^\times) \;=\; 2^{\mathbb{Z}} \times (1+4\mathbb{Z}_2).$$

   (b) Here $(\sqrt{2})^2 = 2$ shows that $K/\mathbb{Q}_2$ is ramified of degree 2 with the maximal ideal $\mathfrak{m}_K = (\sqrt{2})$ and $\mathcal{O}_K = \mathbb{Z}_2[\sqrt{2}]$. Also the images of $1+\sqrt{2}$ and -1 generate the group of units $(\mathcal{O}_K/\mathfrak{m}_K^3)^\times$. Together this implies that

   $$K^\times \;=\; \sqrt{2}^{\mathbb{Z}} \cdot (1+\sqrt{2})^{\mathbb{Z}} \cdot \mu_2 \cdot (1+\mathfrak{m}_K^3).$$

   Again, since $v(\sqrt{2}^3) > v(2)$, the maps exp and log induce a natural isomorphism

   $$(1+\mathfrak{m}_K^3, \cdot) \;\cong\; (\mathfrak{m}_K^3, +) \;=\; 2\sqrt{2}\mathbb{Z}_2 \oplus 4\mathbb{Z}_2.$$

Since $\mathrm{Tr}_{K/\mathbb{Q}_2}(\sqrt{2}) = 0$ and $\mathrm{Tr}_{K/\mathbb{Q}_2}(4) = 8$ this implies that $\mathrm{Tr}_{K/\mathbb{Q}_2}(\mathfrak{m}_K^3)) = 8\mathbb{Z}_2$ and hence

$$\mathrm{Nm}_{K/\mathbb{Q}_2}(1+\mathfrak{m}_K^3) \;=\; \exp(\mathrm{Tr}_{K/\mathbb{Q}_2}(\mathfrak{m}_K^3)) \;=\; \exp(8\mathbb{Z}_2) \;=\; 1+8\mathbb{Z}_2.$$

On the other hand we have $\mathrm{Nm}_{K/\mathbb{Q}_2}(\sqrt{2}) = -2$ and $\mathrm{Nm}_{K/\mathbb{Q}_2}(-1) = 1$ and $\mathrm{Nm}_{K/\mathbb{Q}_2}(1+\sqrt{2}) = (1+\sqrt{2})(1-\sqrt{2}) = -1$. Together we therefore find that

$$\mathrm{Nm}_{K/\mathbb{Q}_2}(K^\times) \;=\; (-2)^{\mathbb{Z}} \cdot \{\pm 1\} \cdot (1+8\mathbb{Z}_2).$$

2. Set $K := \mathbb{Q}_p$ and $L := \mathbb{Q}_p(\mu_p)$ for an odd prime p.

   (a) Determine the group of norms $\mathrm{Nm}_{L/K} L^\times < K^\times$.

   (b) Express the reciprocity isomorphism $\mathrm{Gal}(L/K) \cong K^\times / \mathrm{Nm}_{L/K} L^\times$ from local class field theory in terms of the cyclotomic character $\mathrm{Gal}(L/K) \cong \mathbb{F}_p^\times$.

Solution Fix a primitive p-th root of unity $\zeta \in L$. Then L/K is totally ramified and $\mathcal{O}_L = \mathbb{Z}_p[\zeta]$ with maximal ideal $(1-\zeta)$.

(a) By local class field theory $\mathrm{Nm}_{L/K} L^\times$ is a subgroup of index $[L/K] = p-1$ of $K^\times = p^{\mathbb{Z}} \times \mathbb{Z}_p^\times$. Computing

$$\prod_{a=1}^{p-1}(X-\zeta^a) \;=\; \frac{1}{X-1}\cdot\prod_{a=0}^{p-1}(X-\zeta^a) \;=\; \frac{X^p-1}{X-1} \;=\; \sum_{a=0}^{p-1} X^a$$

and setting $X=1$ we deduce that

$$\mathrm{Nm}_{L/K}(1-\zeta) \;=\; \prod_{a=1}^{p-1}(1-\zeta^a) \;=\; \sum_{a=0}^{p-1} 1^a \;=\; p.$$

Thus p is already a norm; hence the subgroup $\mathrm{Nm}_{L/K} L^\times$ must be $p^{\mathbb{Z}}$ times a subgroup of index $p-1$ of $\mathbb{Z}_p^\times$. The only such subgroup is

$$p^{\mathbb{Z}} \times (1+p\mathbb{Z}_p).$$

(b) Since L/K is totally ramified, it is linearly disjoint from $\tilde{K} := \mathbb{Q}_p^{\mathrm{nr}}$ over K. With $\tilde{L} := \mathbb{Q}_p^{\mathrm{nr}}(\mu_p)$ the restriction maps thus induce isomorphisms

$$\mathrm{Gal}(\tilde{L}/\tilde{K}) \xrightarrow{\sim} \mathrm{Gal}(L/K) \quad\text{and}\quad \mathrm{Gal}(\tilde{L}/L) \xrightarrow{\sim} \mathrm{Gal}(\tilde{K}/K)$$

Fix a generator $\sigma \in \mathrm{Gal}(L/K)$ that corresponds to $a \in \mathbb{F}_p^\times$ under the cyclotomic character, that is, with ${}^\sigma\zeta = \zeta^a$. Via the above isomorphism we view it as an element of $\mathrm{Gal}(\tilde{L}/\tilde{K})$. Let $\varphi \in \mathrm{Gal}(\tilde{L}/L)$ be the Frobenius substitution.

Set $\tilde{\sigma} := \sigma\varphi$ and consider the fixed field $L_{\tilde{\sigma}} := \tilde{L}^{\langle\tilde{\sigma}\rangle}$. Then the reciprocity isomorphism is given by

$$r_{L/K}(\sigma) \;=\; [\mathrm{Nm}_{L_{\tilde{\sigma}}/K}(\pi_{L_{\tilde{\sigma}}})] \;\in\; K^\times/\,\mathrm{Nm}_{L/K}\,L^\times$$

for any uniformizer $\pi_{L_{\tilde{\sigma}}}$ of $L_{\tilde{\sigma}}$.

To compute this explicitly note first that $\tilde{\sigma}^{p-1} = \varphi^{p-1}$, whose fixed field in $\tilde{L}$ is the unramified extension of degree $p-1$ of L and therefore equal to $L(\mu_m)$ for $m := p^{p-1}-1$. Thus we have $L_{\tilde{\sigma}} \subset L(\mu_m)$, and $\tilde{\sigma}|L(\mu_m)$ has order $p-1$. Also, by construction $\tilde{L}$ and $L(\mu_m)$ are unramified over both L and $L_{\tilde{\sigma}}$. In particular $1-\zeta \in L$ is also a uniformizer of $L(\mu_m)$. Choose an element $\xi \in \mathcal{O}_{K(\mu_m)}$ whose residue class yields a normal basis of the residue field extension $\mathbb{F}_p(\mu_m)/\mathbb{F}_p$, and set

$$\pi_{L_{\tilde{\sigma}}} \;:=\; \sum_{i=0}^{p-2}(1-\zeta^{a^i})\xi^{p^i}.$$

Claim: The element $\pi_{L_{\tilde{\sigma}}}$ is a uniformizer of $L_{\tilde{\sigma}}$ and satisfies

$$\mathrm{Nm}_{L_{\tilde{\sigma}}/K}(\pi_{L_{\tilde{\sigma}}}) \;\equiv\; a^{-1}p \mod (p^2).$$

Proof: By the choice of $\tilde{\sigma}$ we have ${}^{\tilde{\sigma}}\zeta = {}^{\sigma}\zeta = \zeta^a$ and ${}^{\tilde{\sigma}}\xi = {}^{\varphi}\xi = \xi^p$ and thus

$$\pi_{L_{\tilde{\sigma}}} \;=\; \sum_{i=0}^{p-2} {}^{\tilde{\sigma}^i}\big((1-\zeta)\xi\big) \;=\; \mathrm{Tr}_{L(\mu_m)/L_{\tilde{\sigma}}}((1-\zeta)\xi) \in L_{\tilde{\sigma}}.$$

Moreover the computation

$$1-\zeta^{a^i} \;=\; 1-\sum_{k=0}^{a^i}\binom{a^i}{k}(\zeta-1)^k \;\equiv\; 1-(1+a^i(\zeta-1)) \;=\; a^i(1-\zeta) \mod (1-\zeta)^2$$

shows that

$$(*) \qquad \pi_{L_{\tilde{\sigma}}} \;\equiv\; b(1-\zeta) \mod (1-\zeta)^2$$

for

$$(**) \qquad b \;:=\; \sum_{i=0}^{p-2} a^i\xi^{p^i}.$$

By the choice of ξ the residue classes ξ^{p^i} for $0 \leqslant i \leqslant p-2$ are $\mathbb{F}_p$-linearly independent. Since $a \not\equiv 0 \bmod (p)$, we therefore have $b \not\equiv 0 \bmod (p)$. The formula $(*)$ thus implies that $\pi_{L_{\tilde{\sigma}}}$ is a unit times $1-\zeta$ and therefore a uniformizer of L and hence also of $L_{\tilde{\sigma}}$.

Next $L_{\tilde\sigma}/K$ is totally ramified of degree $p-1$ and the restriction induces an isomorphism $\mathrm{Gal}(\tilde L/\tilde K) \xrightarrow{\sim} \mathrm{Gal}(L_{\tilde\sigma}/K)$. Thus from $(*)$ we deduce that

$$\mathrm{Nm}_{L_{\tilde\sigma}/K}(\pi_{L_{\tilde\sigma}}) \;=\; \prod_{\tau\in\mathrm{Gal}(\tilde L/\tilde K)} {}^\tau\pi_{L_{\tilde\sigma}} \;\equiv\; \prod_{\tau\in\mathrm{Gal}(\tilde L/\tilde K)} {}^\tau b(1-{}^\tau\zeta) \mod (1-\zeta)^p.$$

Here, on the one hand, by the computation in (a) we have

$$\prod_{\tau\in\mathrm{Gal}(\tilde L/\tilde K)} (1-{}^\tau\zeta) \;=\; \mathrm{Nm}_{L/K}(1-\zeta) \;=\; p.$$

On the other hand b is fixed by $\mathrm{Gal}(\tilde L/\tilde K)$; hence $\mathrm{Nm}_{L_{\tilde\sigma}/K}(b) = b^{p-1}$. To identify this value we note that the formula $(**)$ is reminiscent of Kummer theory. Indeed, the equations $a^{p-1}=a^0$ and $\xi^{p^{p-1}}=\xi$ imply that

$$b^p \;\equiv\; \sum_{i=0}^{p-2} a^i\xi^{p^{i+1}} \;=\; \sum_{i=1}^{p-1} a^{i-1}\xi^{p^i} \;=\; a^{-1}\sum_{i=1}^{p-1} a^i\xi^{p^i} \;\equiv\; a^{-1}b \mod (p)$$

and hence $b^{p-1}\equiv a^{-1} \mod (p)$. Since $(p)=(1-\zeta)^{p-1}$, together we get

$$\mathrm{Nm}_{L_{\tilde\sigma}/K}(\pi_{L_{\tilde\sigma}}) \;\equiv\; a^{-1}p \mod (1-\zeta)^p.$$

Here both sides are elements of $\mathbb{Z}_p$, and since $(1-\zeta)^p\mathcal{O}_{\tilde L}\cap\mathbb{Z}_p = p^2\mathbb{Z}_p$, the claim follows. □

Finally, since $\mathrm{Nm}_{L/K} L^\times = p^{\mathbb{Z}}\times(1+p\mathbb{Z}_p)$ by (a), the claim implies that

$$r_{L/K}(\sigma) \;=\; [\mathrm{Nm}_{L_{\tilde\sigma}/K}(\pi_{L_{\tilde\sigma}})] \;=\; [a^{-1}] \;\in\; K^\times/\,\mathrm{Nm}_{L/K} L^\times.$$

As σ was a generator of $\mathrm{Gal}(L/K)$, it follows that the local reciprocity isomorphism $\mathrm{Gal}(L/K) \cong K^\times/\,\mathrm{Nm}_{L/K} L^\times$ is the reciprocal (!) of that obtained from the cyclotomic character $\sigma\mapsto a$.

3. Consider a local field K, a finite cyclic extension L/K, and a finite abelian extension M/L. Let σ be a generator of $\mathrm{Gal}(L/K)$.

   (a) Show that M/K is Galois if and only if ${}^\sigma(\mathrm{Nm}_{M/L} M^\times) = \mathrm{Nm}_{M/L} M^\times$.

   (b) Show that M/K is abelian if and only if $\{{}^\sigma b/b : b\in L^\times\} \subset \mathrm{Nm}_{M/L} M^\times$.

Solution

(a) Choose an algebraic closure $\bar K$ of K that contains M, and lift σ to an automorphism $\tilde\sigma$ of $\bar K$. Then ${}^{\tilde\sigma}M$ is another finite abelian extension of L, and M is galois over K if and only if ${}^{\tilde\sigma}M = M$. Since ${}^{\tilde\sigma}M$ and M are galois over L, that is so if and only if they are isomorphic as extensions of L. But the local reciprocity isomorphism yields a bijection between finite abelian extensions of L up to isomorphism and closed subgroups of finite index of $L^\times$. Thus M is galois over K if and only if

$$ {}^{\sigma}(\operatorname{Nm}_{M/L} M^\times) \;=\; \operatorname{Nm}_{{}^{\tilde\sigma}M/L} {}^{\tilde\sigma}M^\times \;=\; \operatorname{Nm}_{M/L} M^\times. \qquad (*) $$

(b) If M/K is abelian, it is Galois, and we have a short exact sequence

$$ \begin{array}{ccccccccc} 1 & \longrightarrow & \operatorname{Gal}(M/L) & \longrightarrow & \operatorname{Gal}(M/K) & \longrightarrow & \operatorname{Gal}(L/K) & \longrightarrow & 1. \\ & & \| & & \Cup & & \Cup & & \\ & & \text{abelian} & & \tilde\sigma|M & \longmapsto & \sigma & & \end{array} $$

Thus the group in the middle is generated by the one on the left together with the element $\tilde\sigma|M$. As the one on the left is already abelian, the whole group is abelian if and only if conjugation by $\tilde\sigma|M$ is trivial on $\operatorname{Gal}(M/L)$. By the functoriality of the local reciprocity isomorphism $\operatorname{Gal}(M/L) \cong L^\times/\operatorname{Nm}_{M/L} M^\times$ and the first equality in $(*)$ this is equivalent to saying that σ acts trivially on $L^\times/\operatorname{Nm}_{M/L} M^\times$. But that is equivalent to $\{{}^{\sigma}b/b : b \in L^\times\} \subset \operatorname{Nm}_{M/L} M^\times$, proving the implication "$\Rightarrow$".

For the converse observe that $\{{}^{\sigma}b/b : b \in L^\times\} \subset \operatorname{Nm}_{M/L} M^\times$ already implies the condition in $(*)$. Thus M/K is Galois by (a), and so $\operatorname{Gal}(M/K)$ is abelian by the equivalence above.