Solutions 27

Class Fields, Reciprocity Laws

1. Let K be a number field. Call an element $x \in K^\times$ *totally positive* if it becomes positive under every real embedding of K. Let $\mathrm{Cl}'(\mathcal{O}_K)$ denote the group of all fractional ideals of $\mathcal{O}_K$ modulo the subgroup of principal ideals generated by totally positive elements of $K^\times$. Show that the maximal abelian extension H/K that is everywhere unramified possesses a natural isomorphism

$$\mathrm{Gal}(H/K) \;\cong\; \mathrm{Cl}'(\mathcal{O}_K).$$

Solution The field H is the big Hilbert class field of K, and by the reciprocity isomorphism we have

$$\mathrm{Gal}(H/K) \;\cong\; C_K/\operatorname{Nm}_{L/K} C_L \;\cong\; I_K/I_K^{(1)}K^\times \tag{$*$}$$

for the subgroup

$$I_K^{(1)} \;:=\; \bigtimes_{v\in S_\infty}(K_v^\times)^\circ \times \bigtimes_{v\in M_K\smallsetminus S_\infty}\mathcal{O}_{K_v}^\times \;\subset\; I_K.$$

This subgroup is contained in the subgroup

$$I_K' \;:=\; I_K \cap \Big(\bigtimes_{v\in S_\infty}(K_v^\times)^\circ \times \bigtimes_{v\in M_K\smallsetminus S_\infty}K_v^\times\Big) \;\subset\; I_K.$$

Since K is dense in $K\otimes_{\mathbb{Q}}\mathbb{R} = \bigtimes_{v\in S_\infty}K_v$, we have

$$\Big(\bigtimes_{v\in S_\infty}(K_v^\times)^\circ\Big)\cdot K^\times \;=\; \bigtimes_{v\in S_\infty}K_v^\times$$

and thus $I_K'K^\times = I_K$. By the first isomorphism theorem we therefore have

$$I_K/K^\times \;\cong\; I_K'/(I_K'\cap K^\times),$$

where $I_K'\cap K^\times$ is the subgroup of all totally positive elements of $K^\times$. With $(*)$ we deduce that

$$\mathrm{Gal}(H/K) \;\cong\; I_K/I_K^{(1)}K^\times \;\cong\; I_K'\big/ I_K^{(1)}(I_K'\cap K^\times). \tag{$**$}$$

On the other hand, as in Proposition 13.2.2 we have a natural surjective homomorphism

$$\begin{aligned} I_K' &\longrightarrow \mathrm{Frac}(\mathcal{O}_K) \;:=\; \{\text{fractional ideals of } \mathcal{O}_K\},\\ (x_v)_v &\longmapsto \prod_{v\in M_K\smallsetminus S_\infty}\mathfrak{p}_v^{v(x_v)} \end{aligned}$$

whose kernel is the subgroup I_K'. The image of $I_K'\cap K^\times$ under this homomorphism is precisely the subgroup of principal ideals generated by totally positive elements of $K^\times$. From $(**)$ we therefore obtain a natural isomorphism $\mathrm{Gal}(H/K)\cong \mathrm{Cl}'(\mathcal{O}_K)$.

2. Deduce the two supplements of the quadratic reciprocity law from the reciprocity isomorphism of global class field theory.

Solution Consider an odd prime number p.

(a) For the first supplement take $K := \mathbb{Q}(i)$ with $i = \sqrt{-1}$. From Example 6.2.6 of the lecture we already know that $(\frac{-1}{p}) = 1$ if and only if p splits in K. By global class field theory this is equivalent to the equality

$$[(1,\ldots,1,p,1,\ldots)] \;=\; 1 \quad \text{in} \quad I_{\mathbb{Q}} \,/\, \mathbb{Q}^\times \cdot \mathrm{Nm}_{K/\mathbb{Q}}\, I_K,$$

where the entry p is at the place p. As the idele classes are taken modulo $\mathbb{Q}^\times$, this is equivalent to

$$[(p^{-1},\ldots,p^{-1},1,p^{-1},\ldots)] \;=\; 1 \quad \text{in} \quad I_{\mathbb{Q}} \,/\, \mathbb{Q}^\times \cdot \mathrm{Nm}_{K/\mathbb{Q}}\, I_K,$$

where the entry 1 is at the place p. Since every prime $\ell \neq 2, p$ is unramified in K, the unit p^{-1} is already a local norm at ℓ. Also $p^{-1} > 0$ is a local norm at ∞. The condition is therefore equivalent to

$$[(1,\ldots,1,p^{-1},1,)] \;=\; 1 \quad \text{in} \quad I_{\mathbb{Q}} \,/\, \mathbb{Q}^\times \cdot \mathrm{Nm}_{K/\mathbb{Q}}\, I_K,$$

where the entry p^{-1} is at the place 2. Now recall that 2 is ramified in K and let $\mathfrak{p}$ be the prime of K above it. Under the reciprocity isomorphism $I_{\mathbb{Q}}/\mathbb{Q}^\times \cdot \mathrm{Nm}_{K/\mathbb{Q}}\, I_K \cong \mathrm{Gal}(K/\mathbb{Q})$ the idele class in question is the image of

$$[p^{-1}] \;\in \mathbb{Q}_2^\times / \,\mathrm{Nm}_{K_{\mathfrak{p}}/\mathbb{Q}_2}(K_{\mathfrak{p}}^\times) \;\cong\; \mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_2).$$

But by the solution of exercise 1 (a) of sheet 25 we have

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

Since p is odd, this class therefore vanishes if and only if $p \equiv 1 \bmod (4)$, or again if $(-1)^{\frac{p-1}{2}} = 1$. Altogether this proves the desired equality

$$(\tfrac{-1}{p}) \;=\; (-1)^{\frac{p-1}{2}}.$$

(b) For the second supplement take $K := \mathbb{Q}(\sqrt{2})$. Then from Example 6.2.6 of the lecture we already know that $(\frac{2}{p}) = 1$ if and only if p splits in K. By global class field theory this is equivalent to the equality

$$[(1,\ldots,1,p,1,\ldots)] \;=\; 1 \quad \text{in} \quad I_{\mathbb{Q}} \,/\, \mathbb{Q}^\times \cdot \mathrm{Nm}_{K/\mathbb{Q}}\, I_K,$$

where the entry p is at the place p. As the idele classes are taken modulo $\mathbb{Q}^\times$, this is equivalent to

$$[(p^{-1},\ldots,p^{-1},1,p^{-1},\ldots)] \;=\; 1 \quad \text{in} \quad I_{\mathbb{Q}} \,/\, \mathbb{Q}^\times \cdot \mathrm{Nm}_{K/\mathbb{Q}}\, I_K,$$

where the entry 1 is at the place p. Since every prime $\ell \neq 2, p$ is unramified in K, the unit p^{-1} is already a local norm at ℓ. Also $p^{-1} > 0$ is a local norm at ∞. The condition is therefore equivalent to

$$[(1, \ldots, 1, p^{-1}, 1,)] \;=\; 1 \quad \text{in} \quad I_{\mathbb{Q}} \,/\, \mathbb{Q}^\times \cdot \mathrm{Nm}_{K/\mathbb{Q}} I_K,$$

where the entry p^{-1} is at the place 2. Now recall that 2 is ramified in K and let $\mathfrak{p}$ be the prime of K above it. Under the reciprocity isomorphism $I_{\mathbb{Q}}/\mathbb{Q}^\times \cdot \mathrm{Nm}_{K/\mathbb{Q}} I_K \cong \mathrm{Gal}(K/\mathbb{Q})$ the idele class in question is the image of

$$[p^{-1}] \;\in \mathbb{Q}_2^\times / \mathrm{Nm}_{K_\mathfrak{p}/\mathbb{Q}_2}(K_\mathfrak{p}^\times) \;\cong\; \mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_2).$$

But by the solution of exercise 1 (b) of sheet 25 we have

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

Since p is odd, this class therefore vanishes if and only if $p \equiv \pm 1 \bmod (8)$. This is equivalent to $p^2 \equiv 1 \bmod (16)$ or again to $(-1)^{\frac{p^2-1}{8}} = 1$. Altogether this proves the desired equality

$$\left(\tfrac{-1}{p}\right) \;=\; (-1)^{\frac{p^2-1}{8}}.$$

3. *(A cubic reciprocity law)* Recall that the number field $K := \mathbb{Q}(\mu_3) = \mathbb{Q}(\sqrt{-3})$ is imaginary quadratic, that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is a principal ideal domain, and that $3\mathcal{O}_K = \mathfrak{m}^2$ for the maximal ideal $\mathfrak{m} := (\sqrt{-3})$. Take inequivalent primes $\pi, \rho \in \mathcal{O}_K \smallsetminus \mathfrak{m}$ and consider the extension $L := K(\sqrt[3]{\pi})$ of K, which by Kummer theory is cyclic with Galois group μ_3.

   (a) Show that all primes $\neq \mathfrak{m}, (\pi)$ of $\mathcal{O}_K$ are unramified in L.

   (b) Show that $\mathfrak{m}$ is unramified in L if and only if $\pi \equiv \pm 1 \bmod \mathfrak{m}^3$.

   (c) Assuming this, prove that the residue class of π is a cube in the residue field $\mathcal{O}_K/(\rho)$ if and only if the residue class of ρ is a cube in $\mathcal{O}_K/(\pi)$.

Solution

   (a) It suffices to show that (ρ) is unramified in L. Since ρ is coprime to 3π, the polynomial $X^3 - \pi$ is separable modulo (ρ). Therefore $\mathcal{O}_L \cdot \mathcal{O}_{K,(\rho)} \cong \mathcal{O}_{K,(\rho)}[X]/(X^3 - \pi)$ by Proposition 9.5.6 of the lecture, and (ρ) is unramified in L.

   (b) From $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ we deduce that $\mathcal{O}_{K_\mathfrak{m}} = \mathbb{Z}_3[\sqrt{-3}]$ and hence

$$\mathcal{O}_{K_\mathfrak{m}}[\sqrt[3]{\pi}] \;\cong\; \mathbb{Z}_3[\sqrt{-3}, X]/(X^3 - \pi).$$

Substituting $X = Y + \pi$ we can rewrite this as

$$\mathcal{O}_{K_\mathfrak{m}}[\sqrt[3]{\pi}] \;\cong\; \mathbb{Z}_3[\sqrt{-3}, Y]/(Y^3 + 3\pi Y^2 + 3\pi^2 Y + \pi^3 - \pi).$$

Here $\pi^3 - \pi \in \mathfrak{m}$, because the residue field $\mathcal{O}_K/\mathfrak{m}$ has order 3. Therefore $\mathrm{ord}_\mathfrak{m}(\pi^3 - \pi) \geqslant 1$.

Suppose first that $\mathrm{ord}_\mathfrak{m}(\pi^3 - \pi) \leqslant 2$. Then $\mathrm{ord}_\mathfrak{m}(3) = 2$ and $\mathrm{ord}_\mathfrak{m}(\pi) = 0$ imply that the Newton polygon of the polynomial $Y^3+3\pi Y^2+3\pi^2 Y+\pi^3-\pi$ is a straight line segment of slope $-1/3$ or $-2/3$. Thus the image $\sqrt[3]{\pi}-\pi \in L$ of Y acquires valuation $1/3$ or $2/3$ above $\mathfrak{m}$, and so $\mathfrak{m}$ is ramified in L.

Suppose now that $\mathrm{ord}_\mathfrak{m}(\pi^3 - \pi) \geqslant 3$. Then substituting $Y = \sqrt{-3}\,Z$ and dividing by $(\sqrt{-3})^3$ implies that

$$\mathcal{O}_{K_\mathfrak{m}}\big[\tfrac{\sqrt[3]{\pi}-\pi}{\sqrt{-3}}\big] \;\cong\; \mathbb{Z}_3\big[\sqrt{-3}, Z\big] \big/ \big(Z^3 - \sqrt{-3}\,\pi Z^2 - \pi^2 Z + \tfrac{\pi^3-\pi}{-3\sqrt{-3}}\big),$$

where the polynomial has coefficients in $\mathbb{Z}_3[\sqrt{-3}]$. In particular $\frac{\sqrt[3]{\pi}-\pi}{\sqrt{-3}}$ is integral over $\mathbb{Z}_3[\sqrt{-3}]$. Also, the polynomial in Z reduces to $Z^3 - \pi^2 Z + a$ modulo $\mathfrak{m}$ for some value of a. The derivative thereof is $-\pi^2$ and therefore a unit modulo $\mathfrak{m}$. Thus the polynomial is separable modulo $\mathfrak{m}$, which implies that $\mathfrak{m}$ is unramified in L.

Finally, we have $\pi^3 - \pi = \pi(\pi - 1)(\pi + 1)$ with $\pi \notin \mathfrak{m}$ and $\pi \pm 1$ being pairwise coprime modulo $\mathfrak{m}$. This implies that $\mathrm{ord}_\mathfrak{m}(\pi^3 - \pi) \geqslant 3$ if and only if $\mathrm{ord}_\mathfrak{m}(\pi \mp 1) \geqslant 3$ for some choice of sign.

(c) From (a) we know that (ρ) is unramified in L, and the primes of L above (ρ) are in bijection with the irreducible factors of $X^3 - \pi$ modulo (ρ). Since the residue field of (ρ) already contains μ_3, either ρ splits completely in L or it is inert. Moreover, the former case happens if and only if $X^3 - \pi$ has a root in the residue field $\mathcal{O}_K/(\rho)$. Thus the residue class of π is a cube in $\mathcal{O}_K/(\rho)$ if and only if (ρ) splits completely in L.

By global class field theory the latter is equivalent to the equality

$$[(1, \ldots, 1, \rho, 1, \ldots)] \;=\; 1 \quad \text{in} \quad I_K \big/ K^\times \cdot \mathrm{Nm}_{L/K}\, I_L,$$

where the entry ρ is at the place (ρ). As the idele classes are taken modulo $K^\times$, this is equivalent to

$$[(\rho^{-1}, \ldots, \rho^{-1}, 1, \rho^{-1}, \ldots)] \;=\; 1 \quad \text{in} \quad I_K \big/ K^\times \cdot \mathrm{Nm}_{L/K}\, I_L,$$

where the entry 1 is at the place (ρ). By (a) and (b) the element ρ^{-1} is already a local norm at all finite primes $\neq (\pi)$ of K. Since K is totally imaginary, the element ρ^{-1} is also a local norm at the infinite prime of K. The condition is therefore equivalent to

$$[(1, \ldots, 1, \rho^{-1}, 1,)] \;=\; 1 \quad \text{in} \quad I_K \big/ K^\times \cdot \mathrm{Nm}_{L/K}\, I_L,$$

where the entry ρ^{-1} is at the place (π).

Now observe that the prime $\mathfrak{p} := (\pi)$ of K is totally ramified in L with the unique prime $\mathfrak{q} := (\sqrt[3]{\pi}\,)$ above it. Under the reciprocity isomorphism $I_K/K^\times \cdot \mathrm{Nm}_{L/K} I_K \cong \mathrm{Gal}(L/K)$ the idele class in question is the image of

$$[\rho^{-1}] \ \in K_\mathfrak{p}^\times/\,\mathrm{Nm}_{L_\mathfrak{q}/K_\mathfrak{p}}(L_\mathfrak{q}^\times) \ \cong \ \mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p}).$$

Since ρ is a local unit at $\mathfrak{p}$, the above condition is therefore equivalent to

$$\rho \ \in \mathrm{Nm}_{L_\mathfrak{q}/K_\mathfrak{p}}(\mathcal{O}_{L_\mathfrak{q}}^\times).$$

As $L_\mathfrak{q}/K_\mathfrak{p}$ is totally ramified of degree 3, this is a subgroup of index 3 of $\mathcal{O}_{K_\mathfrak{p}}^\times$. But as $K_\mathfrak{p}$ has residue characteristic $\neq 3$, every element of $1+\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$ is already a third power. Since the multiplicative group of the residue field $\mathcal{O}_K/(\pi)$ is cyclic of order divisible by 3, it follows that $(\mathcal{O}_{K_\mathfrak{p}}^\times)^3$ is the unique subgroup of index 3 of $\mathcal{O}_{K_\mathfrak{p}}^\times$. Moreover ρ lies in it if and only if its residue class is a third power in $\mathcal{O}_K/(\pi)$. The condition is therefore equivalent to saying that the residue class of ρ is a cube in $\mathcal{O}_K/(\pi)$, as desired.