Kummer Theory and Reciprocity Laws

Peter Stevenhagen

Abstract. Insert abstract here.

1. Introduction

How can we find abelian extensions of a number field? For any such field K, we have the cyclotomic extension $K \subset K(\zeta_m)$; the Galois group will be abelian and a subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$. We might also adjoin a square root, but should we adjoin a general root $\sqrt[n]{a}$, we no longer even have a Galois extension, unless $\zeta_n \in K$ already.

But in fact, for $K = \mathbb{Q}$, all quadratic extensions of $\mathbb{Q}$ are already cyclotomic: for $p \neq 2$, there is only one cyclotomic extension which is ramified only at p and only tamely ramified, namely, $\mathbb{Q}(\zeta_p)$. This field has Galois group $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$, so it has a unique quadratic subfield, which is easily seen to be $\mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{(p-1)/2}p$: it is the unique quadratic field ramified only at p. In addition, we have $\mathbb{Q}(\sqrt{-1}, \sqrt{2}) = \mathbb{Q}(\zeta_8)$, so we find $\mathbb{Q}(\sqrt{a}) \subset \mathbb{Q}(\zeta_{4|a|})$.

Already this discussion of quadratic subextensions of cyclotomic extensions gives us the classical quadratic reciprocity law. Given distinct odd primes p, q, then there is a Legendre symbol (p/q) which is 1 or -1, respectively, depending on whether or not p is a square modulo q or not, respectively. One has the quadratic reciprocity law where

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & p \text{ or } q \equiv 1 \pmod 4, \\ -\left(\frac{q}{p}\right), & \text{else.} \end{cases}$$

We can write this more compactly as

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

To prove this, consider first the case $q \equiv 1 \pmod 4$. We consider the cyclotomic extension $\mathbb{Q}(\zeta_q)/\mathbb{Q}$, with Galois group $(\mathbb{Z}/q\mathbb{Z})^*$. This extension contains the quadratic extension $\mathbb{Q}(\sqrt{q})$. Let $\sigma \in (\mathbb{Z}/q\mathbb{Z})^*$ be the Frobenius at p, and note that $(p/q) = 1$ if and only if $\sigma_p(\sqrt{q})/\sqrt{q} = 1$. By the property of the Frobenius, we

have

$$\sigma_p(\sqrt{q})/\sqrt{q} \equiv (\sqrt{q})^{p-1} \pmod{p},$$

so this is equal to 1 if and only if $q^{(p-1)/2} \equiv 1 \pmod{p}$, which holds if and only if $(q/p) = 1$ by Euler's criterion. This proves quadratic reciprocity. The case when $q \equiv 3 \pmod{4}$ is similar, except now we work in $\mathbb{Q}(\sqrt{-q})$, and we end up with an extra factor $(-1)^{(p-1)/2}$.

Seen one way, then, the quadratic reciprocity law is none other than the statement that the quadratic extensions are all contained in cyclotomic extensions, over which we have control.

2. Kummer Theory

We would like to generalize the quadratic reciprocity law; to do so, we need to construct abelian extensions of number fields K.

Throughout we assume that $\zeta_n \in K$. Then $L = K(\sqrt[n]{a})$ (the splitting field of $X^n - a$) is abelian over K, for we have a map

$$\begin{aligned} \mathrm{Gal}(L/K) &\hookrightarrow \langle \zeta_n \rangle \\ \sigma &\mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}. \end{aligned}$$

Note that this is independent of the choice of $\sqrt[n]{a}$ (they differ by a root of unity, which since they are in K, drops out), and by a little work we see that in fact this is a group homomorphism.

Kummer theory gives a certain converse to this statement: If L/K is cyclic of order n, and $\zeta_n \in K$, then there exists an $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^n \in K$. This was basically discovered by Lagrange: If $G = \langle \sigma \rangle$, then for any x write down the *Lagrange resultant*

$$\alpha = x + \zeta_n^{-1}\sigma(x) + \zeta_n^{-2}\sigma^2(x) + \cdots + \zeta^{1-n}\sigma^{n-1}(x).$$

We see that $\sigma(\alpha) = \zeta_n \alpha$, and if $\alpha \neq 0$, then such an α will generate the extension. We can always find such an $\alpha \neq 0$; this is a result from Galois theory (known as 'Artin-Dedekind' or linear independence of characters).

More generally, Kummer theory tells us that if L/K is Galois with group G which is abelian of exponent n (meaning that for all $\sigma \in G$, $\sigma^n = \mathrm{id}_L$), and $\zeta_n \in K$, then $L = K(\sqrt[n]{W})$ for some subgroup $(K^*)^n \subset W \subset K^*$. Then Kummer theory tells us that (within a fixed algebraic closure) there is a bijection

$$\begin{array}{ccc} \{W : (K^*)^n \subset W \subset K^*\} & \longleftrightarrow & \{L \supset K \text{ abelian, exponent } n \text{ (inside } \overline{K})\} \\ W & \longmapsto & K(\sqrt[n]{W}) \\ (L^*)^n \cap K^* & \longmapsfrom & L. \end{array}$$

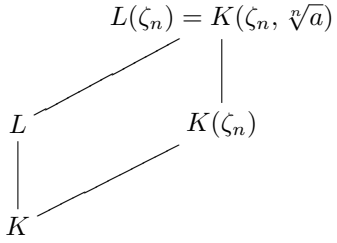
In this case, if $W \leftrightarrow L$, then we have a perfect pairing

$$\begin{aligned} \mathrm{Gal}(L/K) \times W/(K^*)^n &\to \langle \zeta_n \rangle \\ (\sigma, a) &\mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}; \end{aligned}$$

that is to say,

$$\mathrm{Gal}(L/K) \cong \mathrm{Hom}(W/(K^*)^n, \langle \zeta_n \rangle).$$

If L/K is a cyclic extension of degree n but $\zeta_n \notin K$, it can be very hard to describe. However, when one adjoins ζ_n to K, by Kummer theory, the extension $L(\zeta_n)$ is now Kummer over $K(\zeta_n)$, so $L = K(\zeta_n, \sqrt[n]{a})$ for some $a \in K(\zeta_n)$. Note that this extension is not abelian, but it is abelian in two steps, which is usually good enough.



3. Norm Residue Symbol

We now look at the local situation. Recall the statement of local class field theory: if $F = K_{\mathfrak{p}}$ is a local field, and $E \supset F$ is a finite abelian extension, then

$$F^*/N_{E/F}E^* \xrightarrow{\sim} \mathrm{Gal}(E/F)$$

and we have a bijection between open subgroups of F^* and finite abelian extensions of F.

By Kummer theory, if $\zeta_n \in F$, then $E \supset F$ of exponent n arises as $E = F(\sqrt[n]{W})$ where $(F^*)^n \subset W \subset F^*$. But by class field theory, $E \supset F$ of exponent n arises as $(F^*)^n \subset N_{E/F}E^* \subset F^*$. These two ways of viewing extensions are dual to each other.

The maximal exponent n extension by Kummer theory is $E = F(\sqrt[n]{F^*})$. This is a finite extension, for in the local case $(F^*)^n$ has finite index in F^*. Since the bijection in class field theory is inclusion-reversing, $NE^* = (F^*)^n$. By the perfect pairing, we have

$$\begin{aligned} F^*/(F^*)^n \times F^*/(F^*)^n &\to \langle \zeta_n \rangle \\ (\alpha, \beta) &\mapsto \frac{\sigma_\alpha(\sqrt[n]{\beta})}{\sqrt[n]{\beta}} \end{aligned}$$

This is called the *nth power norm residue symbol*, and we denote it F, $(-,-)_{n,F}$.

It has two useful properties:

- From local class field theory, $(\alpha,\beta)_{n,F}=1$ if and only if $\alpha \in N(F(\sqrt[n]{\beta})^*)$.
- Since $A_F^*/N_{E/F}A_E^* \xrightarrow{\sim} I$, the inertia group, if the extension E/F is unramified and $\alpha \in A_F^*$, then $(\alpha,\beta)_{n,F}=1$.

Example 3.1. *Take the case $F=\mathbb{Q}_p$, $n=2$, $p\neq 2$. Then $\mathbb{Q}_p^* = \langle p\rangle \times \mathbb{Z}_p^*$, so $(Q_p^*)^2 = \langle p^2\rangle \times (\mathbb{Z}_p^*)^2$, and so $(\mathbb{Q}_p^*)^2$ has index 4 in $\mathbb{Q}_p^*$, where*

$$\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \cong \langle p\rangle \times \langle \overline{a}\rangle \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},$$

for $a\in\mathbb{Z}$ with $(\overline{a}/p)=-1$.

We have $(x,y)_{2,\mathbb{Q}_p}) = \sigma_x(\sqrt{y})/\sqrt{y}$. In the unramified case, $y=a$, we see that $(a,a)=1$, and since $\pi_F \mapsto \mathrm{Frob}_{E/F}$, we see $(p,a)=-1$. In the ramified case, $y=p$ the norms must generate a subgroup of index 2, so $(a,p)=-1$; and finally we wish to know if $p\in N(\mathbb{Q}_p(\sqrt{p})^*)$: but $(p,p)(-1,p)=(-p,p)=1$ ($N(\sqrt{p})=-p$), so $(p,p)=(-1,p)=(-1)^{(p-1)/2}$. We summarize the values of $(x,y)_{2,\mathbb{Q}_p}$ in the following table:

$x\setminus y$	$\overline{a}$	$-p$
$\overline{a}$	1	-1
p	-1	$(-1)^{(p-1)/2}$

The symbol has other important properties:

- $(-\alpha,\alpha)=1$ for all $\alpha\in F^*$;
- $(1-\alpha,\alpha)=1$ for $\alpha\in F^*\setminus\{1\}$;
- $(\alpha,\beta)=(\beta,\alpha)^{-1}$.

The latter property, for example, follows from

$$(-\alpha\beta,\alpha\beta)=(-\alpha,\alpha)(\beta,\alpha)(\alpha,\beta)(-\beta,\beta)=(\beta,\alpha)(\alpha,\beta)=1.$$

Note that we also have this pairing for archimedean F. For $F=\mathbb{C}$ this is trivial, for $F=\mathbb{R}$ we have the Artin isomorphism

$$\mathbb{R}^*/N\mathbb{C}^* \xrightarrow{\mathrm{Gal}(\mathbb{C}/\mathbb{R})}$$

and a corresponding pairing

$$\mathbb{R}^*/\mathbb{R}^{*2}\times\mathbb{R}^*/\mathbb{R}^{*2}\to\langle -1\rangle$$

with $(-1,-1)_\infty=-1$.

Now, for a number field K such that $\zeta_n\in K$, for any prime $\mathfrak{p}$ of K, there is a norm residue symbol

$$(-,-)_{n,\mathfrak{p}} : K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^n \times K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^n \to \langle\zeta_n\rangle.$$

We then have:

Proposition 3.2 (Product formula)**.** *For $\alpha,\beta\in K^*$,*

$$\prod_{p\le\infty}(\alpha,\beta)_{n,\mathfrak{p}}=1.$$

Example 3.3. *To complete the picture, we compute the quadratic symbols for* $\mathbb{Q}_\infty = \mathbb{R}$ *and* $\mathbb{Q}_2$*. In the first case,* $\mathbb{R}^*/(\mathbb{R}^*)^2 = \langle -1\rangle$*, and* $(-1,-1)_{2,\infty} = -1$*. For* $p = 2$*,* $\mathbb{Q}_2^* = \langle 2\rangle \times \mathbb{Z}_2^*$*, and* $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 = \langle 2^2\rangle \times (\mathbb{Z}_2^*)^2$*, now* $(\mathbb{Z}_2^*)^2 = 1 + 8\mathbb{Z}_2$*, so we see*

$$\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \cong \langle \overline{2}\rangle \times \langle \overline{-1}\rangle \times \langle \overline{5}\rangle.$$

We summarize the values of $(x,y)_{2,2}$ *in the following table:*

$x \setminus y$	$\overline{2}$	$\overline{-1}$	$\overline{5}$
$\overline{2}$	1	1	-1
$\overline{-1}$	1	-1	1
$\overline{5}$	-1	1	1

Proof of the product formula. Consider the following diagram:

$$\begin{array}{ccc} \prod_{p\le\infty}{}' K_{\mathfrak{p}}^* & \longrightarrow & \bigoplus_{\mathfrak{p}\le\infty} \mathrm{Gal}(K_{\mathfrak{p}}(\sqrt[n]{\beta})/K_{\mathfrak{p}}) \\ \downarrow & & \downarrow \\ \mathbf{J} & \longrightarrow & \mathrm{Gal}(K(\sqrt[n]{\beta})/K) \end{array}$$

The left vertical map is the definition of the idèles. The top map is $\alpha \mapsto ((\alpha,\beta)_{n,\mathfrak{p}})_{\mathfrak{p}}$, which one sees is trivial for almost all $\mathfrak{p}$. The horizontal bottom arrow is the Artin map. The right vertical map is $(\sigma_{\mathfrak{p}})_{\mathfrak{p}} \mapsto \prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}$.

The statement is then that for $\alpha \in K^* \subset \mathbf{J}$, the global Artin map (the bottom arrow) factors as $\mathbf{J} \to \mathbf{J}/K^* = C_K \to \mathrm{Gal}(K(\sqrt[n]{\beta})/K)$; this is a nontrivial statement from class field theory. □

Example 3.4. *For the case* $n = 2$*,* $K = \mathbb{Q}$*,* p, q *distinct odd primes, writing* $(p,q)_{2,\ell} = (p,q)_\ell$*, we have*

$$\prod_{\ell\le\infty} (p,q)_\ell = (p,q)_2(p,q)_p(p,q)_q(p,q)_\infty = 1.$$

Since $p, q > 0$*,* $(p,q)_\infty = 1$*. We see from the computation in the above table that* $(p,q)_2 = 1$ *unless* $p, q \equiv 3 \pmod 4$*, i.e.* $(p,q)_2 = (-1)^{(p-1)(q-1)/4}$*. Also, we see*

$$(p,q)_p = \frac{\sqrt{q}^p}{\sqrt{q}} = q^{(p-1)/2} \equiv \left(\frac{q}{p}\right) \pmod p,$$

and similarly $(q,p)_q \equiv \left(\frac{p}{q}\right) \pmod q$*. Altogether,*

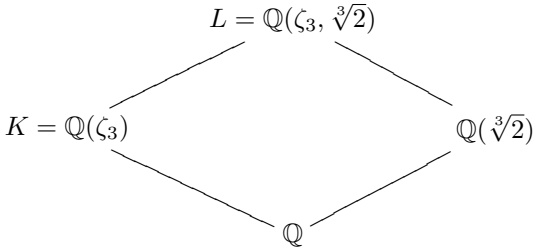
$$(-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = 1$$

which is the statement of quadratic reciprocity.

4. Higher Reciprocity Laws

Are there higher reciprocity laws? In the nineteenth century, such a question was asked. But what should this mean? We begin with the cubic reciprocity law: for which p is 2 a cube modulo p?

For $\mathbb{F}_p^* \supset (\mathbb{F}_p^*)^3$, if $p \equiv 2 \pmod 3$ we see that already $\mathbb{F}_p^* = (\mathbb{F}_p^*)^3$, and this question is not interesting, for 2 is always a cube. We assume therefore that $p \equiv 1 \pmod 3$. Then p splits as $p = \pi\overline{\pi}$ in $\mathbb{Q}(\sqrt{-3})$. In this case, 2 is a cube modulo p if and only if $X^3 - 2$ splits completely modulo p, which happens if and only if p splits completely in $L = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$. This is a Galois extension of degree 6 with Galois group S_3.



But now the extension $L/K = \mathbb{Q}(\zeta_n, \sqrt[3]{2})/\mathbb{Q}(\zeta_3)$ is Kummer, so we can get a handle on it. In fact, one can show that this is the ray class field of $\mathbb{Q}(\zeta_3)$ of conductor 6, and it follows from this that p splits completely in L if and only if $p = x^2 + 27y^2$.

For an nth power reciprocity law, we assume that $\zeta_n \in K$. What is the analogue of the Legendre symbol for nth powers? Given a prime $\mathfrak{p} \nmid n\infty$, we have the unit group $(\mathcal{O}/\mathfrak{p})^*$, which has order divisible by n since $\langle\zeta_n\rangle \hookrightarrow (\mathcal{O}/\mathfrak{p})^*$ (the discriminant of the polynomial $X^n - 1$ is prime to $\mathfrak{p}$). Therefore we define:

$$\left(\frac{-}{\mathfrak{p}}\right)_n : (\mathcal{O}/\mathfrak{p})^* \to \langle\zeta_n\rangle$$

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n \equiv \alpha^{(N\mathfrak{p}-1)/n} \pmod{\mathfrak{p}}.$$

For the primes in

$$S(\alpha) = \{\mathfrak{p} : \mathfrak{p} \mid n\infty \text{ or } \operatorname{ord}_{\mathfrak{p}}(\alpha) \neq 0\}$$

we do not define the symbol. We extend the symbol to any fractional $\mathcal{O}_K$-ideal $\mathfrak{b}$ of K by multiplicativity,

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_n = \prod_{\mathfrak{p}\notin S(\alpha)} \left(\frac{\alpha}{\mathfrak{p}}\right)^{\operatorname{ord}_{\mathfrak{p}}(\mathfrak{b})}.$$

This symbol is then multiplicative in $\mathfrak{b}$ on the group $I(\alpha)$ generated by $\mathfrak{p} \notin S(\alpha)$. For any element $\beta \in K^*$, we also define

$$\left(\frac{\alpha}{\beta}\right)_n = \left(\frac{\alpha}{(\beta)}\right)_n.$$

Lemma 4.1. *For $\alpha, \beta \in K^*$, with $\zeta_n \in K$, we have*

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{\mathfrak{p} \in S(\alpha) \cap S(\beta)} (\alpha, \beta)_{\mathfrak{p}}.$$

In particular, if α and β are coprime, then

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{\mathfrak{p} | n\infty} (\alpha, \beta)_{\mathfrak{p}}.$$

To prove this, we use the following fact:

Lemma 4.2. *If $\mathfrak{b} \in I(\alpha)$, then*

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_n = \frac{\sigma_{\mathfrak{b}}(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}},$$

where $\sigma_{\mathfrak{b}} \in \mathrm{Gal}(K(\sqrt[n]{\alpha})/K)$ is the Artin symbol of $\mathfrak{b}$.

Proof. Suppose $\mathfrak{b} = \mathfrak{p} \in I(\alpha)$. Now α is a unit at $\mathfrak{p}$, so $K_{\mathfrak{p}}(\sqrt[n]{\alpha})$ is an unramified extension of $K_{\mathfrak{p}}$. The Artin symbol of $\mathfrak{p}$ in this case is

$$\sigma_{\mathfrak{p}} \alpha = \frac{(\sqrt[n]{\alpha})^{N\mathfrak{p}}}{\sqrt[n]{\alpha}} = \alpha^{(N\mathfrak{p}-1)/n} \pmod{p}$$

which is exactly the definition of the power residue symbol. □

Proof of power reciprocity. By the lemma,

$$\left(\frac{\alpha}{\beta}\right)_n = \prod_{\mathfrak{p} \notin S(\alpha)} (\beta, \alpha)_{n,\mathfrak{p}}.$$

Similarly,

$$\left(\frac{\beta}{\alpha}\right)_n = \prod_{\mathfrak{p} \notin S(\beta)} (\alpha, \beta)_{n,\mathfrak{p}} = \prod_{\mathfrak{p} \in S(\beta)} (\alpha, \beta)_{n,frakp}^{-1}$$

by the product formula. For $\mathfrak{p} \notin S(\alpha) \cup S(\beta)$, we clearly have $(\alpha, \beta)_{n,\mathfrak{p}} = 1$. For the quotient

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1}$$

we therefore obtain the quantity

$$\prod_{\mathfrak{p} \in S(\beta) \setminus S(\alpha)} (\beta, \alpha)_{n,\mathfrak{p}} \prod_{\mathfrak{p} \in S(\beta)} (\alpha, \beta)_{n,\mathfrak{p}}.$$

Using $(\beta, \alpha)(\alpha, \beta)^{-1} = 1$ at the primes $\mathfrak{p} \in S(\beta) \setminus S(\alpha)$, the result follows. □

The expression for power reciprocity may look complicated, but $F^*/(F^*)^n$ is a finite abelian group, so the norm residue symbol relies on only a finite amount of information. For example, we have the supplementary law for a odd and positive:

$$\left(\frac{2}{a}\right) = (-1)^{(a^2-1)/8} = \begin{cases} 1, & a \equiv \pm 1 \pmod 8 \\ -1, & a \equiv \pm 3 \pmod 8. \end{cases}$$

We may now prove cubic reciprocity, a result originally due to Eisenstein. Suppose that $\alpha, \beta \in \mathbb{Z}[\zeta_3]$ are coprime and coprime to 3. Since the ideal (3) ramifies in $\mathbb{Q}(\zeta_3)$ as $(3) = (1-\zeta_3)^2$, we have a map

$$\mathbb{Z}[\zeta_3] \to \mathbb{Z}[\zeta_3]/3\mathbb{Z}[\zeta_3] = \mathbb{Z}[\zeta_3]/(1-\zeta_3)^2\mathbb{Z}.$$

This latter group is of order 6, so the map takes $\langle \zeta_6 \rangle = \langle -\zeta_3 \rangle$ injectively into the quotient. Replacing α by $\zeta_6^k \alpha$ we may assume $\alpha \equiv 1 \pmod 3$, and similarly with β. In this case, we actually have

$$\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\beta}{\alpha}\right)_3.$$

This follows from the power reciprocity law:

$$\left(\frac{\alpha}{\beta}\right)_3 \left(\frac{\beta}{\alpha}\right)_3^{-1} = (\alpha, \beta)_{3,(1-\zeta_3)};$$

as this field is totally complex, there are no infinite primes. Evaluating this entry, we see that it is equal to 1.

Example 4.1. *As another example, we can take quintic reciprocity. Take $\alpha, \beta \in \mathbb{Z}[\zeta_5]$ coprime to each other and coprime to 5. We have $(5) = (1-\zeta_5)^4$, and*

$$\left(\frac{\alpha}{\beta}\right) \left(\frac{\beta}{\alpha}\right)^{-1} = (\alpha, \beta)_{5,(1-\zeta_5)}.$$

Multiplying α, β by units, for which we have

$$\mathbb{Z}[\zeta_5]^* = \langle -\zeta_5 \rangle \times \langle (1+\sqrt{5})/2 \rangle,$$

we can obtain $\alpha, \beta \equiv 1 \pmod{(1-\zeta_5)^3}$. Then $(\alpha, \beta)_{5,1-\zeta_5} = 1$, and

$$\left(\frac{\alpha}{\beta}\right)_5 = \left(\frac{\beta}{\alpha}\right)_5.$$

Exercises

Exercise 3.1. For odd primes p and q, we showed how to deduce the quadratic reciprocity law

$$\left(\frac{p}{q}\right) = (-1)^{p-\frac{1}{2}q-\frac{1}{2}} \left(\frac{q}{p}\right)$$

from the inclusion $\mathbb{Q}(\sqrt{\left(\frac{-1}{q}\right)q}) \subset \mathbb{Q}(\zeta_q)$ and properties of the Artin symbol. Give a similar proof for the supplementary law

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \bmod 8, \\ -1 & p \equiv \pm 3 \bmod 8, \end{cases}$$

where p denotes an odd prime.

In the next two exercises, let $K = \mathbb{Q}(\sqrt{-3})$ be the number field generated by the cube root of unity $\zeta_3 = (-1+\sqrt{-3})/2$, and $L = K(\sqrt[3]{2})$ the extension of K generated by a root $\sqrt[3]{2}$ of $X^3 - 2$. The unique primes of K lying over 2 and 3 are denoted by 2 and $\mathfrak{t}$, respectively.

Exercise 3.2.

(a) Prove that $K \subset L$ is cyclic of degree 3, and that $\epsilon\colon \mathrm{Gal}(L/K) \to \langle\zeta_3\rangle$ defined by $\epsilon(\sigma) = \sigma(\sqrt[3]{2})/\sqrt[3]{2}$ is a group isomorphism.
(b) Show that the conductor $\mathbb{F}(L/K)$ divides $2\mathfrak{t}^4$.
(c) Let $\mathfrak{p}$ be a finite prime of K not dividing $2\mathfrak{t}$, and let $N\mathfrak{p}$ be the cardinality of its residue class field. Prove that $\epsilon((\mathfrak{p}, L/K))$ is the unique element of $\langle\zeta_3\rangle$ that is congruent to $2^{(N\mathfrak{p}-1)/3}$ modulo $\mathfrak{p}$.
(d) Show that L is the ray class field of K with modulus 6 $(= 2 \cdot \mathfrak{t}^2)$.

Exercise 3.3. Let p be a prime number, and let m be the number of distinct roots of $X^3 - 2$ in $\mathbb{F}_p$. Prove the following:

(a) $m = 0$ if and only if $p \equiv 1 \bmod 3$ and p is not represented by $X^2 + 27Y^2$.
(b) $m = 1$ if and only if $p \not\equiv 1 \bmod 3$.
(c) $m \neq 2$.
(d) $m = 3$ if and only if p is represented by $X^2 + 27Y^2$.

Exercise 3.4. Let K be a number field, and r the number of real primes of K. Denote by Cl the class group of K, and by Cl^* the *strict* (or *narrow*) class group of K; i.e., the ray class group modulo the cycle $\mathfrak{f} = \prod_{\mathfrak{p}\ \mathrm{real}} \mathfrak{p}$. The 2-rank $\mathrm{rk}_2\, A$ of a multiplicatively written abelian group A is defined to be the dimension of the $\mathbb{F}_2$-vector space A/A^2.

(a) Prove that $\mathrm{rk}_2\,\mathrm{Cl} \leq \mathrm{rk}_2\,\mathrm{Cl}^* \leq \mathrm{rk}_2\,\mathrm{Cl} + r - 1$ if $r > 0$.
(b) Let $H = \{x \in K^* : K(\sqrt{x})$ is unramified over K at all finite primes$\}$, and let H^+ be the set of elements of H that are positive at all real primes of K. Prove that $\mathrm{rk}_2\,\mathrm{Cl}^*$ equals the dimension of the $\mathbb{F}_2$-vector space H/K^{*2}, and that $\mathrm{rk}_2\,\mathrm{Cl}$ equals the dimension of the $\mathbb{F}_2$-vector space H^+/K^{*2}.

Exercise 3.5. Let the notation be as in the previous exercise.

(a) Let a, $b \in H$. Prove that the norm residue symbol $(a,b)_{2,\mathbb{Q}}$ equals 1 for every finite prime $\mathbb{Q}$ of K, and that $\prod_{\mathfrak{p}\ \mathrm{real}} (a,b)_{2,\mathfrak{p}} = 1$.
(b) Prove that $\mathrm{rk}_2\,\mathrm{Cl}^* \leq \mathrm{rk}_2\,\mathrm{Cl} + \lfloor r/2 \rfloor$.

Mathematisch Instituut,
Universiteit Leiden,
Postbus 9512,
2300 RA Leiden,
The Netherlands
E-mail address: psh@math.leidenuniv.nl