Primes Presentation

Thomas Browning

November 6, 2018

1 Algebraic Number Theory

Recall that a number field is a finite extension of $\mathbb{Q}$. If K is a number field then we define $\mathcal{O}_K$ to be the ring of algebraic integers of K or, equivalently, the integral closure of $\mathbb{Z}$ in K. For every nonzero ideal I of $\mathcal{O}_K$, the quotient $\mathcal{O}_K/I$ is finite and we define the norm of I to be the cardinality $|\mathcal{O}_K/I|$. The ring $\mathcal{O}_K$ is a Dedekind domain. This means that every nonzero prime ideal of $\mathcal{O}_K$ is maximal and that every nonzero ideal of $\mathcal{O}_K$ factors as a finite product of nonzero prime ideals. Furthermore, this factorization is unique up to permutation. In other words, every nonzero ideal of $\mathcal{O}_K$ is of the form $\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_g^{e_g}$ for distinct nonzero prime ideals $\mathfrak{p}_1,\dots,\mathfrak{p}_g$ of $\mathcal{O}_K$ and positive integers $e_1,\dots,e_g$. A fractional ideal of $\mathcal{O}_K$ is a nonzero finitely-generated $\mathcal{O}_K$-submodule of K. Fractional ideals of $\mathcal{O}_K$ can always be expressed as αI for a nonzero $\alpha\in K$ and a nonzero ideal I of $\mathcal{O}_K$. The fractional ideals of $\mathcal{O}_K$ form a group I_K under multiplication with $\mathcal{O}_K$ as the identity element. The group of fractional ideals of $\mathcal{O}_K$ is a free abelian group with the nonzero prime ideals of $\mathcal{O}_K$ as a basis. In other words, every fractional ideal of $\mathcal{O}_K$ is of the form $\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_g^{e_g}$ for distinct nonzero prime ideals $\mathfrak{p}_1,\dots,\mathfrak{p}_g$ of $\mathcal{O}_K$ and integers $e_1,\dots,e_g$. A principal fractional ideal of $\mathcal{O}_K$ is a fractional ideal of the form $\alpha\mathcal{O}_K$ for a nonzero $\alpha\in K$. The principal fractional ideals form a subgroup P_K of I_K. The quotient I_K/P_K is called the ideal class group of K and is denoted by $\mathrm{C}(\mathcal{O}_K)$. The ideal class group of K will always be a finite abelian group.

Example 1. Let $n\neq 0,1$ be a squarefree integer and let $K=\mathbb{Q}(\sqrt{n})$. Consider an element $\alpha=a+b\sqrt{n}\in K$ with b nonzero. The minimal polynomial of α is given by $x^2-2ax+a^2-nb^2$. As a consequence, $\alpha\in\mathcal{O}_K$ if and only if both $2a\in\mathbb{Z}$ and $a^2-nb^2\in\mathbb{Z}$. From this, it can be shown that

$$\mathcal{O}_K=\begin{cases}\mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right] & n\equiv 1 \pmod 4\\ \mathbb{Z}[\sqrt{n}] & n\equiv 2,3 \pmod 4\end{cases}.$$

If $n=-5$ then $\mathcal{O}_K=\mathbb{Z}[\sqrt{-5}]$. We have the factoriation $6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$ where the elements $\{2,3,1+\sqrt{-5},1-\sqrt{-5}\}\subseteq\mathcal{O}_K$ are all irreducible. This shows that $\mathcal{O}_K$ is not a UFD. In terms of ideals, we have the factorization $(6)=(2)(3)=(1+\sqrt{-5})(1-\sqrt{-5})$. This does not contradict the uniqueness of prime factorization since none of these ideals are prime. In fact, we have the prime factorizations

$$\begin{aligned}(2)&=\left(2,1-\sqrt{-5}\right)\left(2,1+\sqrt{-5}\right)\\(3)&=\left(3,1-\sqrt{-5}\right)\left(3,1+\sqrt{-5}\right)\\\left(1+\sqrt{-5}\right)&=\left(2,1+\sqrt{-5}\right)\left(3,1+\sqrt{-5}\right),\\\left(1-\sqrt{-5}\right)&=\left(2,1-\sqrt{-5}\right)\left(3,1-\sqrt{-5}\right).\end{aligned}$$

Let K be a number field and let L be a finite extension of K. If $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$ then $\mathfrak{p}\mathcal{O}_L$ is a nonzero ideal of $\mathcal{O}_L$ and has a factorization $\mathfrak{p}\mathcal{O}_L=\mathfrak{q}_1^{e_1}\dots\mathfrak{q}_g^{e_g}$ for distinct nonzero prime ideals $\mathfrak{q}_1,\dots\mathfrak{q}_g$ of $\mathcal{O}_L$ and positive integers $e_1,\dots,e_g$. The integer $e_i=e_{\mathfrak{q}_i|\mathfrak{p}}$ is called the ramification index of $\mathfrak{q}_i|\mathfrak{p}$.

The inclusion $\mathfrak{p} \subseteq \mathfrak{q}_i$ gives a residue field extension $\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{q}_i$ of degree $f_i = f_{\mathfrak{q}_i|\mathfrak{p}}$ which is called the inertia degree of $\mathfrak{q}_i|\mathfrak{p}$. We have the relation

$$\sum_{i=1}^{f} e_i f_i = [L : K].$$

We say that $\mathfrak{p}$ is ramified in L if any ramification index e_i is larger than 1. There will only be finitely many nonzero prime ideals of $\mathcal{O}_K$ that ramify in L. We say that $\mathfrak{p}$ is totally ramified in L if $e_1 = [L : K]$ and $f_1 = 1$ and $g = 1$. We say that $\mathfrak{p}$ is inert in L if $e_1 = 1$ and $f_1 = [L : K]$ and $g = 1$. We say that $\mathfrak{p}$ splits completely in L if $e_i = f_i = 1$ for all i and $g = [L : K]$. If L/K is Galois with Galois group $G = \mathrm{Gal}(L/K)$ then G acts transitively on the $\mathfrak{q}_i$ so $e_1 = \ldots = e_g$ and $f_1 = \ldots = f_g$. In this case, $efg = [L : K]$.

Example 2. Let $K = \mathbb{Q}$ and let $L = \mathbb{Q}(\sqrt{-5})$. Then we have the prime factorizations

$$\begin{aligned}
2\mathcal{O}_L &= \left(2, 1 + \sqrt{-5}\right)^2, \\
3\mathcal{O}_L &= \left(3, 1 - \sqrt{-5}\right)\left(3, 1 + \sqrt{-5}\right), \\
5\mathcal{O}_L &= \left(\sqrt{-5}\right)^2, \\
7\mathcal{O}_L &= \left(7, 3 - \sqrt{-5}\right)\left(7, 3 + \sqrt{-5}\right), \\
11\mathcal{O}_L &= (11),
\end{aligned}$$

so 2 and 5 ramify, 3 and 7 split, 11 is inert. Every number field K has a nonzero integer discriminant d_K. A prime p ramifies in $K/\mathbb{Q}$ if and only if p divides d_K. For the quadratic field, the discriminant is given by

$$d_{\mathbb{Q}(\sqrt{-n})} = \begin{cases} n & n \equiv 1 \pmod 4 \\ 4n & n \equiv 2, 3 \pmod 4 \end{cases}.$$

In our case, $d_K = -20$ so only 2 and 5 ramify in $K/\mathbb{Q}$.

Let K be a number field, let L be a finite Galois extension of K, let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$, and let $\mathfrak{q}$ be a nonzero prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$. The stabilizer subgroup

$$D_{\mathfrak{q}|\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(L/K) \colon \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

is called the decomposition group of $\mathfrak{q}|\mathfrak{p}$. If $\sigma \in D_{\mathfrak{q}|\mathfrak{p}}$ then σ induces an automorphism $\overline{\sigma}$ of $\mathcal{O}_L/\mathfrak{q}$ which is the identity on $\mathcal{O}_K/\mathfrak{p}$. We obtain a homomorphism $\varphi_{\mathfrak{q}|\mathfrak{p}} \colon D_{\mathfrak{q}|\mathfrak{p}} \to \widetilde{G}$ where $\widetilde{G} = \mathrm{Gal}((\mathcal{O}_L/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p}))$. The homomorphism $\varphi_{\mathfrak{q}|\mathfrak{p}}$ is surjective with kernel

$$I_{\mathfrak{q}|\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(L/K) \colon \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}} \text{ for all } \alpha \in \mathcal{O}_L\}$$

which is called the inertia group of $\mathfrak{q}|\mathfrak{p}$. We obtain a short exact sequence of finite abelian groups

$$1 \longrightarrow I_{\mathfrak{q}|\mathfrak{p}} \longrightarrow D_{\mathfrak{q}|\mathfrak{p}} \xrightarrow{\varphi_{\mathfrak{q}|\mathfrak{p}}} \widetilde{G} \longrightarrow 1 \ .$$

The orbit-stabilizer theorem shows that $|D_{\mathfrak{q}|\mathfrak{p}}| = [L : K]/g_{\mathfrak{q}|\mathfrak{p}} = e_{\mathfrak{q}|\mathfrak{p}} f_{\mathfrak{q}|\mathfrak{p}}$. Also, $\left|\widetilde{G}\right| = f_{\mathfrak{q}|\mathfrak{p}}$ by the definition of $f_{\mathfrak{q}|\mathfrak{p}}$. Thus, $|I_{\mathfrak{q}|\mathfrak{p}}| = e_{\mathfrak{q}|\mathfrak{p}}$. Now suppose that $\mathfrak{p}$ is unramified in L. Then $e_{\mathfrak{q}|\mathfrak{p}} = 1$ so $I_{\mathfrak{q}|\mathfrak{p}} = 1$ and $\varphi_{\mathfrak{q}|\mathfrak{p}}$ is an isomorphism. The group $\widetilde{G}$ is cyclic and is generated by the Frobenius automorphism $x \mapsto x^{N(\mathfrak{p})}$. The corresponding element $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}} \in D_{\mathfrak{q}|\mathfrak{p}}$ is the unique element of G such that

$$\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{q}}$$

for all $\alpha \in \mathcal{O}_K$. For each $\sigma \in G$,

$$\sigma\left(\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}\left(\sigma^{-1}(\alpha)\right)\right) - \alpha^{N(\mathfrak{p})} = \sigma\left(\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}\left(\sigma^{-1}(\alpha)\right) - \sigma^{-1}(\alpha)^{N(\mathfrak{p})}\right) \in \sigma(\mathfrak{p})$$

which shows that $\mathrm{Frob}_{\sigma(\mathfrak{q})|\mathfrak{p}} = \sigma \, \mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}} \, \sigma^{-1}$. If G is abelian, then $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$ does not depend on $\mathfrak{q}$ and we obtain the Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right) \in G$. If L/K is abelian and unramified then the Artin symbol is defined for all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ and we obtain the Artin homomorphism

$$\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K).$$

The Artin homomorphism is always surjective.

Let K be a number field. There exists a maximal abelian unramified extension L of K called the Hilbert class field of K. The Artin reciprocity theorem for the Hilbert class field states that the kernel of the Artin homomorphism is P_K. We obtain a short exact sequence of abelian groups

$$1 \longrightarrow P_K \longrightarrow I_K \longrightarrow \mathrm{Gal}(L/K) \longrightarrow 1 \ .$$

Thus, $\mathrm{Gal}(L/K) \cong \mathrm{C}(\mathcal{O}_K)$. Then the Galois correspondence gives an inclusion-reversing bijection between unramified abelian extensions of K and subgroups of $C(\mathcal{O}_K)$. If M is an unramified abelian extension of K with $\mathrm{Gal}(L/M) \cong H \subseteq \mathrm{C}(\mathcal{O}_K)$ then we have the isomorphism

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/M) \cong C(\mathcal{O}_K)/H.$$

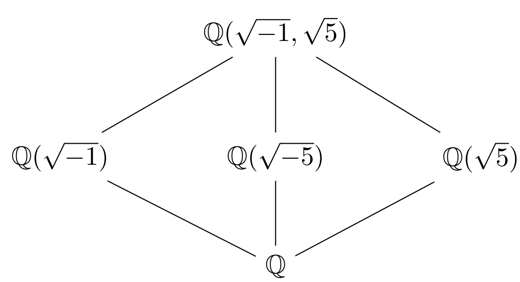
This is known as class field theory for unramified abelian extensions.

Theorem 1 (Corollary 5.24 in [1])**.** *Let K be a number field. Then there is an inclusion-reversing bijection between unramified abelian extensions of K and subgroups of $C(\mathcal{O}_K)$. If M is the unramified abelian extension of K that corresponds to the subgroup H of $\mathrm{C}(\mathcal{O}_K)$ then we have an isomorphism* $\mathrm{C}(\mathcal{O}_K)/H \cong \mathrm{Gal}(M/K)$.

Let K be a number field, let L be the Hilbert class field of K, and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Then we have the following chain of biconditionals:

$$\begin{aligned}
\mathfrak{p} \text{ splits completely in } L &\iff f_{\mathfrak{q}|\mathfrak{p}} = 1 \\
&\iff \mathrm{Gal}((\mathcal{O}_L/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p})) = 1 \\
&\iff \mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}} = 1 \\
&\iff \left(\frac{L/K}{\mathfrak{p}}\right) = 1 \\
&\iff \mathfrak{p} \in P_K.
\end{aligned}$$

Example 3. Consider the following lattice of fields:



Only 2 and 5 ramify in $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$. However, 2 does not ramify in $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ and 5 does not ramify in $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$. Since ramification index is multiplicative, $\mathbb{Q}(\sqrt{-1}, \sqrt{5})$ is an unramified abelian extension of $\mathbb{Q}(\sqrt{-5})$. The class number of $\mathbb{Q}(\sqrt{-5})$ is 2 so $\mathbb{Q}(\sqrt{-1}, \sqrt{5})$ is the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$.

References

[1] Cox, David. *Primes of the Form* $x^2 + ny^2$. Wiley, 1989.