Mersenne primes and class field theory

Jansen, B.J.H.

Chapter 6

Class field theory

Theorem 5.6 relates the Lehmer symbol to the Frobenius symbol. For abelian extensions of number fields one can calculate the Frobenius symbol using the Artin map of class field theory. In this chapter we will introduce class field theory. In the next chapter we will apply class field theory to prove properties of the Lehmer symbol.

The Artin map

In this section we will briefly explain the Artin map. We also state the theorems of class field theory concerning the Artin map that we apply in the next chapter.

Let F/E be a finite abelian extension of number fields with Galois group G and discriminant Δ. Let $\mathfrak{p} \neq 0$ be a prime of E relatively prime to Δ, so that $\mathfrak{p}$ is unramified in F/E. Let $\mathfrak{P}$ be a prime ideal of the ring of integers of F such that $\mathfrak{P} \cap \mathcal{O}_E = \mathfrak{p}$, i.e. $\mathfrak{P}$ lies above $\mathfrak{p}$. In the previous chapter we introduced the Frobenius symbol. The Frobenius symbol has the property $\sigma(\mathfrak{P}, F/E)\sigma^{-1} = (\sigma(\mathfrak{P}), F/E)$ for any $\sigma \in G$. The extension F/E is abelian, so the Frobenius symbol does not depend on the choice of the prime $\mathfrak{P}$. Hence we can define $\mathrm{Frob}_{\mathfrak{p}}$ by $(\mathfrak{P}, F/E)$.

Let $I = I_E(\Delta)$ be the group of fractional ideals generated by the prime ideals $\mathfrak{p} \nmid \Delta$ of $\mathcal{O}_E$. The group I is a free abelian group generated by the set of primes of E relatively prime to Δ. The *Artin map* is the group homomorphism

$$I \to G$$

defined on the generators $\mathfrak{p}$ of I by

$$\mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}}.$$

From class field theory it follows that the Artin map is surjective. This theory also gives a description of the kernel of the Artin map.

In order to describe the kernel of the Artin map we will use the notion of a totally positive element. A real embedding of E is a ring homomorphism from

E to the field of real numbers $\mathbb{R}$. An element $x \in E$ is called *totally positive* in F/E if for every real embedding σ of E which is not induced by a real embedding of F we have $\sigma(x) > 0$.

Theorem 6.1. *Let F/E be a finite abelian extension of number fields. Let $\mathcal{O}_E$ be the ring of integers of E. Then there exists a non-zero ideal $\mathfrak{f}$ in $\mathcal{O}_E$, which is divisible by all ramified primes in F/E, such that for each $x \in E^*$ with*

(i) $\operatorname{ord}_{\mathfrak{p}}(x-1) \geq \operatorname{ord}_{\mathfrak{p}}(\mathfrak{f})$ *for all prime ideals $\mathfrak{p} \mid \mathfrak{f}$,*
(ii) *x is totally positive in F/E,*

the ideal $(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(x)}$ is in the kernel of the Artin map, where the product runs over all prime ideals $\mathfrak{p}$ of $\mathcal{O}_E$. Furthermore, the Artin map is surjective.

For a proof of Theorem 6.1 see [7, Chapter X, §1, Theorem 1] and [7, Chapter X, §2, Theorem 2]. We call an ideal $\mathfrak{f}$ for which the conclusion of Theorem 6.1 holds a *modulus* for F/E.

Theorem 6.2. *If $\mathfrak{f}_1$ and $\mathfrak{f}_2$ are two moduli for F/E then their greatest common divisor $\gcd(\mathfrak{f}_1, \mathfrak{f}_2)$ is also a modulus.*

For a proof of Theorem 6.2 see [5, Chapter V, §6]. From Theorem 6.2 it follows that for every extension F/E of number fields, we have a unique modulus $\mathfrak{f}$ for F/E such that every modulus of F/E is divisible by $\mathfrak{f}$. We call this modulus $\mathfrak{f}$ the *conductor* of F/E. (Readers already familiar with class field theory should note that we give a different definition of modulus here than one would find in the literature, since our definition of modulus does not allow the modulus to "contain" the so-called infinite primes.) The following theorem gives an upper bound for the conductor.

Theorem 6.3. *Let F/E be a finite abelian extension of number fields. Let Δ be the discriminant of F/E. Let $\mathfrak{f}$ be the conductor of the extension. Then*

$$\mathfrak{f} \mid \gcd(\Delta, [F:E] \cdot \Big(\prod_{p \mid [F:E]} p \Big) \prod_{\mathfrak{p} \mid \Delta} \mathfrak{p}),$$

where the first product runs over all primes of $\mathbb{Z}$ which divide $[F:E]$ and the second product runs over all primes $\mathfrak{p}$ of E which divide Δ.

We will prove Theorem 6.3 in the next section, assuming the well-known fact that $\mathfrak{f}$ divides Δ (see [11, Chapter 5, §3, Theorem 3.27]).

The following corollary gives an upper-bound of the 2-part of the conductor in a special case.

Corollary 6.4. *Let $n \in \mathbb{Z}_{>0}$, let $L/\mathbb{Q}(\sqrt[n]{2})$ be an abelian extension of degree 8, let $\mathfrak{f}$ be the conductor of $L/\mathbb{Q}(\sqrt[n]{2})$, and let $m \in \mathbb{Z}_{\geq 0}$ be such that $\sqrt[n]{2}^m \parallel \mathfrak{f}$. Then we have $m \leq 4n+1$.*

Corollary 6.4 follows directly from Theorem 6.3. Indeed by Theorem 6.3 we have $(\sqrt[n]{2})^m \mid 8 \cdot 2 \cdot (\sqrt[n]{2}) = (\sqrt[n]{2})^{4n+1}$ where $m = \operatorname{ord}_{(\sqrt[n]{2})}(\mathfrak{f})$.

An example: primes of the form $x^2 + 23y^2$

To illustrate how one can apply class field theory we will prove that we can write a prime p as $p = x^2 + 23y^2$ with $x, y \in \mathbb{Z}$ if and only if $x^3 - x + 1$ has three zeros in $\mathbb{F}_p$ or $p = 23$ (for more examples see [1]).

The statement above is clear for $p = 23$. For the remaining part of this section assume $p \neq 23$.

Let L be the splitting field of the polynomial $f = x^3 - x + 1$. The polynomial f has no zeros in $\mathbb{F}_2$, hence f is irreducible over $\mathbb{Q}$. The discriminant of f is -23. Therefore $\sqrt{-23} \in L$. Hence $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to the full symmetric group of degree 3. Let $F = \mathbb{Q}(\sqrt{-23})$. Now we show that the conductor of L/F is 1. The only primes that ramify in $L/\mathbb{Q}$ divide the discriminant of f, so only the prime $(\sqrt{-23})$ can ramify in L/F. Suppose for a contradiction that $(\sqrt{-23})$ ramifies in L/F. Then 23 is totally ramified in $L/\mathbb{Q}$, since $L/\mathbb{Q}$ is Galois. Hence the inertia group of 23 in L/F is $\mathrm{Gal}(L/\mathbb{Q})$. However by Proposition 5.8(v) and (vi) the inertia group of a tamely ramified prime is cyclic, hence we have a contradiction. Therefore no prime ramifies in the extension L/F.

By Theorem 6.3 the conductor of L/F is 1. Note that F cannot be embedded in the field of real numbers, so every element of F is totally positive. Now the Artin Reciprocity Law implies that all principal ideals of F are in the kernel of the (surjective) Artin map $I_F \to \mathrm{Gal}(L/F)$. Let Cl_F be the class group of F. The class number of F is 3. Hence the Artin map induces a isomorphism from Cl_F to $\mathrm{Gal}(L/F)$. This isomorphism implies that the Frobenius symbol of every principal ideal in F in the extension L/F is trivial. Therefore every principal prime ideal of F splits completely in L. Let $p \in \mathbb{Z}$ be a prime number. Then p splits in F completely into principal ideals if and only if p splits completely in L. Proposition 5.8(iii) implies: p splits completely in L if and only if f has three zeros in $\mathbb{F}_p$. Hence p splits in principal ideals in F if and only if f has three zeros in $\mathbb{F}_p$.

Let $\alpha = (1 + \sqrt{-23})/2$ and $\overline{\alpha} = (1 - \sqrt{-23})/2$. The ring of integers $\mathcal{O}_F$ is $\mathbb{Z}[\alpha]$. Suppose $p = x^2 + 23y^2$. Then (p) is the product of the principal ideals $(x + \sqrt{-23}y)$ and $(x - \sqrt{-23}y)$ of $\mathcal{O}_F$. Now suppose that p splits into principal ideals in $\mathcal{O}_F$. Then we have $p = (a + b\alpha)(a + b\overline{\alpha}) = a^2 + ab + 6b^2$. If b is odd, then p is divisible by 2. Since p is an odd prime, b is even. Therefore we get $a + b\alpha \in \mathbb{Z}[\sqrt{-23}]$, so p can be written in the form $x^2 + 23y^2$. Hence p can be written as $x^2 + 23y^2$ if and only if p splits into principal ideals in F.

Now we can conclude that p can be written as $x^2 + 23y^2$ if and only if f has three zeros in $\mathbb{F}_p$.

Estimating conductors

In this section we give a proof of Theorem 6.3 based on well-known theorems of local class field theory and Newton polygons.

Let F/E be an abelian extension of number fields. Let $\mathfrak{f}$ be the conductor of F/E and let Δ be the discriminant of F/E. A rough approximation of the

conductor is given by the following theorem.

Theorem 6.5. *We have* $\mathfrak{f} \mid \Delta$.

Proof. See [14, Chapter VI, §3, Corollary 2] or [11, Chapter 5, §3, Theorem 3.27]. □

The next theorem we state enables us to calculate the conductor.

Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_E$ and let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_F$ above $\mathfrak{p}$. Let $F_{\mathfrak{P}}/E_{\mathfrak{p}}$ be the corresponding abelian extension of local fields. Let $\mathcal{O}_{E_{\mathfrak{p}}}$ be the ring of integers of $E_{\mathfrak{p}}$. For $i \in \mathbb{Z}_{>0}$ we define the multiplicative group U_i by $1 + \mathfrak{p}^i$ and we let $U_0 = \mathcal{O}_{E_{\mathfrak{p}}}^*$. Denote the norm map from $F_{\mathfrak{P}}^*$ to $E_{\mathfrak{p}}^*$ by $\mathrm{N}_{F_{\mathfrak{P}}/E_{\mathfrak{p}}}$. Denote the subgroup $\mathrm{N}_{F_{\mathfrak{P}}/E_{\mathfrak{p}}}(F_{\mathfrak{P}}^*)$ of $E_{\mathfrak{p}}^*$ by N, so

$$N = \mathrm{N}_{F_{\mathfrak{P}}/E_{\mathfrak{p}}}(F_{\mathfrak{P}}^*).$$

Theorem 6.6. *Let* $i \in \mathbb{Z}_{\geq 0}$ *be the smallest integer such that* $U_i \subset N$. *Then we have* $\mathfrak{p}^i \parallel \mathfrak{f}$.

Proof. See [14, Chapter XV, §2, Corollary 2]. □

In order to apply Theorem 6.6 efficiently we will use one of the main theorems of local class field theory.

Let G be the Galois group of F/E. Since F/E is abelian, Proposition 5.8(ii) implies that the decomposition group $G_{\mathfrak{P}}$ does not depend on the prime $\mathfrak{P}$ above $\mathfrak{p}$. Hence we can denote the decomposition group by $G_{\mathfrak{p}}$. Similarly we denote the ramification groups by $V_{\mathfrak{p},i}$. An element σ of the Galois group of $F_{\mathfrak{P}}/E_{\mathfrak{p}}$ can be restricted to F. Since $E \subset E_{\mathfrak{p}}$, the element σ acts as the identity on E. Therefore we have a restriction map $r : \mathrm{Gal}(F_{\mathfrak{P}}/E_{\mathfrak{p}}) \to G$. This map is injective and the image of r is $G_{\mathfrak{p}}$ (see [14, Chapter II, §3, Corollary 4]). Hence we can identify $\mathrm{Gal}(F_{\mathfrak{P}}/E_{\mathfrak{p}})$ with $G_{\mathfrak{p}}$.

Theorem 6.7. *We have a group isomorphism* $E_{\mathfrak{p}}^*/N \to G_{\mathfrak{p}}$ *that for* $n \in \{0, 1\}$ *maps* $U_n N/N$ *bijectively to* $V_{\mathfrak{p},n}$.

Proof. For $n = 0$ see [14, Chapter IV, §3] and [14, Chapter XV, §2]. Suppose $n = 1$. Then $U_1 N/N$ is the Sylow p-subgroup of $U_0 N/N$ (see [7, Chapter 2, §3]). By Proposition 5.8(vi) the group $V_{\mathfrak{p},1}$ is a Sylow p-subgroup of $V_{\mathfrak{p},0}$. Hence for $n = 1$ the theorem also holds. □

Theorem 6.8. *The prime ideal* $\mathfrak{p}$ *is unramified in* F *if and only if* $\mathfrak{p} \nmid \mathfrak{f}$. *Suppose* $\mathfrak{p}$ *is ramified in* F. *Then* $\mathfrak{p}$ *is tamely ramified in* F *if and only if* $\mathfrak{p} \parallel \mathfrak{f}$.

Proof. Assume $\mathfrak{p}$ is unramified in F/E. Then Proposition 5.8(iv) implies that $V_{\mathfrak{p},0}$ is the trivial group. Hence the group isomorphism of Theorem 6.7 maps $U_0 N/N$ to the identity element of $G_{\mathfrak{p}}$. Therefore $U_0 \subset N$. Now Theorem 6.6 implies $\mathfrak{p} \nmid \mathfrak{f}$.

Assume $\mathfrak{p} \nmid \mathfrak{f}$. Then Theorem 6.6 implies $U_0 \subset N$. Therefore $U_0 N/N$ is the trivial group. By Theorem 6.7 the group $V_{\mathfrak{p},0}$ is trivial. Hence Proposition 5.8(iv) implies $\mathfrak{p}$ is unramified.

Assume $\mathfrak{p}$ is tamely ramified in F. Then Proposition 5.8(vi) implies that $V_{\mathfrak{p},1}$ is the trivial group. Hence the group isomorphism of Theorem 6.7 maps U_1N/N to the identity element of $G_{\mathfrak{p}}$. Therefore $U_1 \subset N$. Since $\mathfrak{p}$ is ramified, Proposition 5.8(iv) implies that $V_{\mathfrak{p},0}$ is a non-trivial group. From Theorem 6.7 we get that the group U_0 is not contained in N. Now Theorem 6.6 implies $\mathfrak{p} \parallel \mathfrak{f}$.

Assume $\mathfrak{p} \parallel \mathfrak{f}$. Then Theorem 6.6 implies $U_1 \subset N$. Therefore U_1N/N is the trivial group, so Theorem 6.7 implies that $V_{\mathfrak{p},1}$ is the trivial group. Now Proposition 5.8(vi) implies that $\mathfrak{p}$ is tamely ramified. □

Let $p \in \mathbb{Z}$ be the prime under $\mathfrak{p}$. Let $e = e(\mathfrak{p}/p) = \mathrm{ord}_{\mathfrak{p}}(p)$ be the ramification index of $\mathfrak{p}$ in $E/\mathbb{Q}$. Let $\lfloor \frac{e}{p-1} \rfloor \in \mathbb{Z}$ be such that $0 \leq \frac{e}{p-1} - \lfloor \frac{e}{p-1} \rfloor < 1$.

Lemma 6.9. *Let $i \in \mathbb{Z}_{\geq 0}$. If $i \geq \lfloor \frac{e}{p-1} \rfloor + 1$ then the map $U_i \to U_{i+e}$ defined by $x \mapsto x^p$ is a group isomorphism.*

Proof. Let $\mathcal{O} = \mathcal{O}_{E_{\mathfrak{p}}}$ be the ring of integers of $E_{\mathfrak{p}}$. Let $\pi \in \mathcal{O}$ be such that $(\pi) = \mathfrak{p}$. Note that $i \geq \lfloor \frac{e}{p-1} \rfloor + 1$ implies $i(p-1) \geq e+1$. Hence $p \cdot i \geq i + e + 1$. Therefore $\pi^{i+e+1} \mid \pi^{ip}$. We will use this result in order to apply Hensel's Lemma.

Since $(p) = (\pi)^e$ and $\pi^{i+e+1} \mid \pi^{ip}$, the coefficients of the polynomial $(1 + \pi^i y)^p - 1 = p\pi^i y + \ldots + \pi^{p \cdot i} y^p \in \mathcal{O}[y]$ are elements of $(\pi)^{i+e} \cdot \mathcal{O}$. Hence for all $x \in U_i$ we have $x^p \in U_{i+e}$, so the map $\phi : x \mapsto x^p$ from U_i to U_{i+e} is well-defined.

To show that ϕ is a group isomorphism it suffices to prove that ϕ is a bijection. First we show that ϕ is surjective. Let $u \in U_{i+e}$. Then we see $g(y) = (1 + \pi^i y)^p - u \in (\pi)^{i+e} \cdot \mathcal{O}[y]$, so $f(y) = g(y)/\pi^{i+e} \in \mathcal{O}[y]$. Let $a \in \mathcal{O}$ be such that $u = 1 + p\pi^i a$. Since $\pi^{i+e+1} \mid \pi^{pi}$, we have $g(a) = \frac{1}{2}p(p-1)\pi^{2i}a^2 + \ldots + \pi^{pi}a^p \in \pi^{i+e+1} \cdot \mathcal{O}$. Hence we have $\pi | f(a)$. The derivative of $f(y)$ equals $f'(y) = p \cdot (1+\pi^i y)^{p-1} \cdot \pi^i \cdot \pi^{-i-e} \in (1+\pi^i y)^{p-1} \cdot \mathcal{O}^*$, so $\pi \nmid f'(a)$. Therefore Hensel's Lemma implies that there exists an element $\alpha \in \mathcal{O}$ such that $f(\alpha) = 0$. By definition of $f(y)$ we see that $g(y)$ also has a zero in $\mathcal{O}$. This proves that ϕ is surjective.

Let ζ_p be a primitive p-th root of unity. To show that ϕ is injective it suffices to prove that $\zeta_p \notin U_i$. From above we know $i(p-1) \geq e+1$. Hence we have $(\pi)^{i(p-1)} \nmid (\pi)^e = (p) = (1-\zeta_p)^{p-1}$. This implies $1 - \zeta_p \notin \pi^i \cdot \mathcal{O}$. Therefore we can conclude that $\zeta_p \notin U_i$. This finishes the proof of Lemma 6.9. □

Proof of Theorem 6.3. By Theorem 6.8 only primes $\mathfrak{p}$ that ramify in F/E can divide the conductor $\mathfrak{f}$ of F/E. We recall from Proposition 5.8(vi) that $V_{\mathfrak{p},1}$ is the p-part of the inertia group $V_{\mathfrak{p},0}$ in F/E. We define ϵ by $\epsilon = \epsilon(\mathfrak{p}) = \mathrm{ord}_p(\text{exponent of } V_{\mathfrak{p},1})$, where p is the prime of $\mathbb{Q}$ below $\mathfrak{p}$. Now we prove that

$$U_{\lfloor \frac{e}{p-1} \rfloor + 1 + e\epsilon} = U_{\lfloor \frac{e}{p-1} \rfloor + 1}^{p^\epsilon} \subset U_1^{p^\epsilon} \subset N$$

hold (see just above Theorem 6.6 for the definition of N). The equality follows from applying Lemma 6.9 precisely ϵ times starting with $i = \lfloor \frac{e}{p-1} \rfloor + 1$. The first inclusion follows from $U_{\lfloor \frac{e}{p-1} \rfloor + 1} \subset U_1$. Now we prove the second inclusion.

By definition of ϵ we have that p^ϵ annihilates $V_{\mathfrak{p},1}$. Hence by Theorem 6.7 the integer p^ϵ annihilates U_1N/N. Therefore we have $U_1^{p^\epsilon} \subset N$.

From Theorem 6.6 we get $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}) \leq \lfloor \frac{e}{p-1} \rfloor + 1 + e\epsilon$. Hence together with Theorem 6.5 we have

$$\mathfrak{f} \mid \gcd(\Delta, \prod_{\mathfrak{p}\mid\Delta} \mathfrak{p}^{\lfloor \frac{e(\mathfrak{p})}{p-1} \rfloor + 1 + e(\mathfrak{p})\epsilon(\mathfrak{p})}).$$

Now we prove that this result implies Theorem 6.3.

Assume that $\mathfrak{p}$ is wildly ramified. Then $\mathfrak{p} \mid \Delta$ implies $\mathfrak{p} \mid [F : E]$. Hence we have

$$\prod_{\mathfrak{p}\mid\Delta} \mathfrak{p}^{\lfloor \frac{e(\mathfrak{p})}{p-1} \rfloor} \Big| \prod_{p\mid[F:E]} \prod_{\mathfrak{p}\mid p} \mathfrak{p}^{e(\mathfrak{p})} \Big| \prod_{p\mid[F:E]} p.$$

Let $m(p)$ be the maximum of the set $\{\epsilon(\mathfrak{p}) : \mathfrak{p} \mid p\}$. The order of $V_{\mathfrak{p},1}$ divides the order of G, so

$$m(p) \leq \mathrm{ord}_p([F : E]).$$

Hence we have

$$\prod_{\mathfrak{p}\mid\Delta} \mathfrak{p}^{\epsilon(\mathfrak{p})e(\mathfrak{p})} \Big| \prod_{p\mid[F:E]} \prod_{\mathfrak{p}\mid p} \mathfrak{p}^{e(\mathfrak{p})\epsilon(\mathfrak{p})} \Big| \prod_{p\mid[F:E]} \Big(\prod_{\mathfrak{p}\mid p} \mathfrak{p}^{e(\mathfrak{p})}\Big)^{m(p)} \Big| \prod_{p\mid[F:E]} p^{m(p)} \mid [F : E].$$

Theorem 6.8 implies $\mathfrak{f}$ divides $\prod_{p\mid[F:E]} p \cdot \prod_{\mathfrak{p}\mid\Delta} \mathfrak{p} \cdot [F : E]$. □