MATH 254A: RING CLASS FIELDS AND $p = x^2 + ny^2$

BRIAN OSSERMAN

1. Ring class groups and ring class fields

Recall that we had shown that given $n \in \mathbb{N}$, and p a prime number, then $p = x^2 + ny^2$ if and only if $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ in $\mathbb{Z}[\sqrt{-n}]$, and $\mathfrak{p}$ is principal. The first condition is easy to analyze: we saw that at least for p not dividing $2n$, $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ if and only if $\left(\frac{-n}{p}\right) = 1$, which in turn can be described very concretely for any given n by quadratic reciprocity. The condition that $\mathfrak{p}$ be principal is subtler, and requires class field theory.

We will see:

Theorem 1.1. *Given $n \in \mathbb{N}$, there exists an irreducible monic polynomial $f_n(x) \in \mathbb{Z}[x]$ such that for any prime p not dividing $2n \operatorname{disc} f_n(x)$,*

$$p = x^2 + ny^2 \Leftrightarrow \begin{cases} (-n/p) = 1 \text{ and } f_n(x_0) \equiv 0 \pmod{p} \\ \text{for some } x_0 \in \mathbb{Z}. \end{cases}$$

In the case that $\mathbb{Z}[\sqrt{-n}] = \mathscr{O}_{\mathbb{Q}(\sqrt{-n})}$, we know that $\mathfrak{p}$ is principal if and only if it splits completely in the Hilbert class field of $\mathbb{Q}(\sqrt{-n})$. From there, some elementary manipulations give the desired result. However, for the general case, we will need to see how class field theory interacts with orders in imaginary quadratic fields.

Recall the notion of orders:

Definition 1.2. An **order** $\mathscr{O}$ of **conductor** f in an imaginary quadratic field K is the unique subring of $\mathscr{O}_K$ of index f, given explicitly as $\mathscr{O} = \{x + yf\omega : x, y \in \mathbb{Z}\}$, where ω is such that $\mathscr{O}_K = \mathbb{Z}[\omega]$.

It turns out that the key to dealing with ideals in orders is to restrict to ideals prime to the conductor; i.e., $I \subset \mathscr{O}$ such that $I + (f) = \mathscr{O}$.

Definition 1.3. The **ideal class group** of $\mathscr{O}$ is the group obtained by considering ideals prime to f modulo principal ideals prime to f.

It will follow that this is a group from the following:

Proposition 1.4. *Given $\mathscr{O}$ of conductor f in $\mathscr{O}_K$, the maps $I \mapsto I\mathscr{O}_K$ and $I \mapsto I \cap \mathscr{O}$ are mutually inverse on ideals prime to f, and induce a multiplicative bijection between ideals of $\mathscr{O}$ prime to f and ideals of $\mathscr{O}_K$ to prime to f.*

The image in $\mathscr{O}_K$ of the principal ideals of $\mathscr{O}$ prime to f is exactly $P_{K,\mathbb{Z}}(f)$, the group of principal ideals of $\mathscr{O}_K$ generated by x with $x \equiv n \pmod{f\mathscr{O}_K}$, for some $n \in \mathbb{Z}$ (and relatively prime to f).

See [1, Prop. 7.20, Prop. 7.22] for the proof.

We can thus define:

Definition 1.5. If $\mathscr{O}$ is the order in $\mathscr{O}_K$ of conductor f, we define the **ring class group** to be $I_K(f)/P_{K,\mathbb{Z}}(f)$, which is naturally isomorphic to the group of ideals of $\mathscr{O}$ prime to f modulo principal ideals of $\mathscr{O}$ prime to f. We define the **class number** $h_{\mathscr{O}}$ of $\mathscr{O}$ to be the order of the ring class group.

The proposition gives a natural isomorphism between the ideal class group of $\mathscr{O}$ and the ring class group of $\mathscr{O}$.

Remark 1.6. Note that having trivial class group does not imply that $\mathscr{O}$ is a PID. In fact, for $f > 1$, $\mathscr{O}$ is never Dedekind, and in particular never a PID.

Definition 1.7. Given $\mathscr{O}$, the **ring class field** $K_{\mathscr{O}}$ is the abelian extension of K associated by the existence theorem of class field theory to the ring class group of $\mathscr{O}$.

From the definitions, it is not hard to see that $K_{\mathscr{O}}$ has the following property generalizing the Hilbert class field:

Theorem 1.8. *A prime $\mathfrak{p}$ of $\mathscr{O}$ which is prime to f is principal if and only if it splits completely in $K_{\mathscr{O}}$.*

It is then not hard to deduce:

Theorem 1.9. *Fix $n > 0$. Then for p not dividing $2n$, we have*

$$p = x^2 + ny^2 \Leftrightarrow p \text{ splits completely in } \mathbb{Q}(\sqrt{-n})_{\mathbb{Z}[\sqrt{-n}]}.$$

From here, one finishes the proof of Theorem 1.1 by showing that $\mathbb{Q}(\sqrt{-n})_{\mathbb{Z}[\sqrt{-n}]}$ is Galois over $\mathbb{Q}$, and the theorem is satisfied by setting $f_n(x)$ to be the minimal polynomial of a primitive element for $\mathbb{Q}(\sqrt{-n})_{\mathbb{Z}[\sqrt{-n}]} \cap \mathbb{R}$ over $\mathbb{Q}$. See [1, §9 A].

Remark 1.10. In fact, the condition that p is prime to $\operatorname{disc} f_n(x)$ in Theorem 1.1 can be dropped if $f_n(x)$ is chosen appropriately; this is a consequence of the explicit methods discussed below.

The theory we have discussed thus far is sufficient to compute a number of examples. The basic idea is to use that we can compute the degree of $f_n(x)$ as a class number, and to use our knowledge of where the ring class field is ramified, to reduce down to a finite set of possibilities for the ring class field, and then check one by one whether they agree with the theorem. For instance:

Example 1.11. In the theorem, for $n = 27$, the polynomial $f_n(x)$ may be taken to be $x^3 - 2$, while for $n = 64$, we may take $f_n(x) = x^4 - 2$. For the method of finding and proving the correctness of these polynomials, see [1, §9 B].

2. The theory of complex multiplication

Recall that we used abstract class field theory to show the Kronecker-Weber theorem, that every abelian extension of $\mathbb{Q}$ is a subfield of some cyclotomic extension. This is the first case of an *explicit* class field theory, where the abelian extensions, described abstractly by class field theory, are somehow made explicit. We could rephrase the Kronecker-Weber theorem as saying rational values of the function $e^{2\pi ix}$ generate abelian extensions of $\mathbb{Q}$, and every abelian extension of $\mathbb{Q}$ is contained in the field generated by some rational value. If we want to have a more constructive form of Theorem 1.1, we need an explicit class field theory for imaginary quadratic fields, and that is what we now discuss.

In the discussion that follows, we always take our lattices to be of full rank. Recall that any order may be viewed as a lattice in $\mathbb{R}^n$; in our case, if $\mathscr{O}$ is an order of an imaginary quadratic field, it is naturally a lattice inside $\mathbb{C}$. The same is true of any non-zero ideal of $\mathscr{O}$ prime to the conductor, and it is easy to check that two such ideals $I, J \in \mathscr{O}$ are equivalent in the class group if and only if $\exists \alpha \in \mathbb{C}$ such that $\alpha I = J$ (the main point to check is that $\alpha I = J$ implies that $\alpha \in K$).

Definition 2.1. We say that two lattices $L, L' \subset \mathbb{C}$ are **homothetic** if $\exists \alpha \in \mathbb{C}$ with $\alpha L = L'$.

We define certain functions on complex lattices as follows:

Definition 2.2. Let $L \subset \mathbb{C}$ be a lattice. Then we define:

$$g_2(L) = 60 \sum_{\omega \in L \smallsetminus \{0\}} \frac{1}{\omega^4},$$

$$g_3(L) = 140 \sum_{\omega \in L \smallsetminus \{0\}} \frac{1}{\omega^6},$$

$$\Delta(L) = g_2(L)^3 - 27 g_3(L)^2,$$

and

$$j(L) = 1728 \frac{g_2(L)^3}{\Delta(L)}.$$

It is not too difficult to prove:

Theorem 2.3. *For two lattices $L, L' \in \mathbb{C}$, we have $j(L) = j(L')$ if and only if L, L' are homothetic.*

It is then easy to establish a relationship between ideal classes of $\mathscr{O}$ and values $j(I)$ for I an (*) ideal of $\mathscr{O}$. It is not too hard to prove: condition

Theorem 2.4. *Given $\sigma \in \mathrm{Aut}(\mathbb{C})$, and I an ideal of $\mathscr{O}$ prime to the conductor, then $\sigma(j(I)) = j(I')$ for I' some other ideal of $\mathscr{O}$.*

Corollary 2.5. *$j(\mathscr{O})$ generates an extension of $\mathbb{Q}$ of degree at most equal to $h_{\mathscr{O}}$.*

We thus start to suspect a relationship between the j-function and the ring class field of $\mathscr{O}$. Indeed, we have the following far deeper theorem:

Theorem 2.6. *If K is an imaginary quadratic field, and $\mathscr{O}$ an order of $\mathscr{O}_K$, then $j(\mathscr{O})$ generates the ring class field of $\mathscr{O}$ over K.*

More precisely, $j(\mathscr{O})$ is an algebraic integer, and we may take the $f_n(x)$ of Theorem 1.1 to be the minimal polynomial of $j(\mathscr{O})$, which is given explicitly as $\prod(x - j(I))$ as I ranges over the ideal classes of $\mathscr{O}$. Moreover, for this choice of $f_n(x)$, the hypothesis of Theorem 1.1 that p not divide $\operatorname{disc} f_n(x)$ *may be dropped.*

See [1, Thm. 11.1, Exer. 11.1, Thm. 9.2, Prop. 13.2, Thm. 13.23].

One rather involved algorithm for finding the minimal polynomial of $j(\mathscr{O})$, called the **class equation**, is described in [1, §13 A,B]. However, it is also possible to compute more efficiently by finding representatives I_i for each ideal class of $\mathscr{O}$, computing each $j(I_i)$ to within a certain precision, and taking advantage of the fact that the minimal polynomial of $j(\mathscr{O})$ has integer coefficients.

This discussion has produced an explicit class field theory for ring class fields. We conclude by mentioning that a slight generalization gives the full collection of ray class fields of imaginary quadratic fields.

Definition 2.7. Given a lattice $L \subset \mathbb{C}$, let

$$\wp(z, L) = \frac{1}{z^2} + \sum_{\omega \in L \smallsetminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

be the Weierstass $\wp$-function, and

$$\tau(z, L) = \begin{cases} \frac{g_2(L)^2}{\Delta(L)} \wp(z, L)^2 : & g_3(L) = 0; \\ \frac{g_3(L)}{\Delta(L)} \wp(z, L)^3 : & g_2(L) = 0; \\ \frac{g_2(L) g_3(L)}{\Delta(L)} \wp(z, L) : & \text{otherwise} \end{cases}$$

be the Weber function.

We then have the following explicit class field theory for imaginary quadratic fields:

Theorem 2.8. *Given K an imaginary quadratic field and $N \in \mathbb{N}$, the ray class field of K of conductor N is generated by $j(\mathscr{O}_K), \tau(1/N, \mathscr{O}_K)$.*

In particular, these are all abelian extensions of K, and every abelian extension of K is contained in one of these.

Remark 2.9. The entire theory of complex multiplication can be understood in the context of elliptic curves. Indeed, elliptic curves over $\mathbb{C}$ are closely related to lattices in $\mathbb{C}$, and our j-function simply becomes the j-invariant of the elliptic curve in question. The order $\mathscr{O}$ corresponds to the endomorphism ring of the elliptic curve. Ultimately, we find that we are generating ring class fields by adjoining the j-invariants of elliptic curves having endomorphism ring $\mathscr{O}$, and that to generate all ray class fields for K, we further adjoin the x-coordinates of N-torsion points of the curve.

References

1. David A. Cox, *Primes of the form $x^2 + ny^2$*, Wiley-Interscience, 1989.