An Introduction to Orders of Number Fields

Pace Nielsen

May 3, 2002

1 What is an Order?

One of the first objects of study in algebraic number theory is the ring $\mathcal{O}_K$ of algebraic integers of a number field K. This remarkable invariant has a number of useful properties. We will just list a few:

- $\mathcal{O}_K$ is integrally closed
- $\mathcal{O}_K$ has Krull dimension 1; prime ideals are maximal
- $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, and hence Noetherian
- If $\mathfrak{a} \subseteq \mathcal{O}_K$ is an ideal, then $\mathcal{O}_K/\mathfrak{a}$ is finite
- $\mathcal{O}_K$ has unique factorization of all fractional ideals
- The class group, $Cl(\mathcal{O}_K)$, is finite
- $\mathcal{O}_K^*$ is a finitely generated abelian group
- If L/K is a finite extension of number fields, $\mathcal{O}_L \cap K = \mathcal{O}_K$

These few facts lead to some amazing results. For instance, it isn't too difficult after some work with cyclotomic fields to deduce quadratic reciprocity. With a little more work, cubic and biquadratic reciprocity can be recovered. Using the fact that the ring of integer $\mathbb{Z}[i] \subset \mathbb{Q}(i)$ is a U.F.D. we can deduce Fermat's classical result that an odd number p is the sum of two squares if and only if $p \equiv 1 \pmod 4$ (see Neukirch[4]). Exploiting unique factorization of fractional ideals, we can prove Fermat's last theorem for all but the irregular primes. In particular, we see that the algebraic structure of $\mathcal{O}_K$ provides a key to proving major results in number theory.

Mathematicians are never satisfied when theorems can be strengthened, or when hypotheses can be dropped. Further, more abstract objects can lead to deeper insights (as we will see a little later). We can attempt to generalize the notion of the ring of algebraic integers as follows:

Definition 1. An **order** of an algebraic number field K is a subring $\mathcal{O} \subseteq \mathcal{O}_K$ which is also a $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$.

Example 1. For the field $\mathbb{Q}(\sqrt{5})$, we have the obvious order $\mathbb{Z}[\sqrt{5}] \subseteq \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

First of all, note that $\mathcal{O}_K$ is always an order. In fact, it is the maximal order for any fixed number field K. Second, since K is torsion free, so is any order, $\mathcal{O}$. Hence $\mathcal{O}$ is in fact a free $\mathbb{Z}$-module. Unfortunately, $\mathcal{O}$ is not necessarily integrally closed. This leads to some immediate difficulties. For those familiar with algebraic geometry and schemes, we can look at the affine

space Spec($\mathcal{O}$). Clearly, $\mathcal{O} = \mathcal{O}_K \iff$ our affine space is non-singular. Thus, we can think of the study of orders and the ring of integers as corresponding to the study of singular and non-singular curves, respectively. To see some other dissimilarities we will list characteristics of orders, parallel to our earlier list (proofs are found in Neukirch[4], p. 73-81):

- $\mathcal{O}$ contains only integral elements over it's quotient field K
- $\mathcal{O}$ has Krull dimension 1; prime ideals are maximal
- $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, and hence Noetherian
- If $\mathfrak{a} \subseteq \mathcal{O}$ is an ideal, then $\mathcal{O}/\mathfrak{a}$ is finite
- $\mathcal{O}$ does not have unique factorization of all fractional ideals
- Fractional ideals don't form a group under multiplication
- $\mathcal{O}^*$ is a finitely generated abelian group
- If L/K is a finite extension of number fields, with $\mathcal{O}$ an order for L, then $\mathcal{O} \cap K \subseteq \mathcal{O}_K$

Since orders are not necessarily integrally closed they are not Dedekind domains, and we lose the power of unique factorization of ideals. We can begin to rectify this problem by focusing on a smaller class of ideals. For the following we let R be a commutative domain, with K it's field of fractions.

Definition 2. A **fractional ideal** of R in K is any R-submodule $\mathfrak{a} \subseteq K$ such that $\exists\, r \in R - \{0\}$ so that $r\mathfrak{a} \subseteq R$.

Definition 3. A fractional ideal, $\mathfrak{a} \subseteq \mathcal{O}$, is an **invertible ideal** (or invertible fractional ideal) if there is another fractional ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}$.

Definition 4. The **Picard group**, of a ring R, is the quotient of the group of invertible ideals by the group of principal ideals. It is written $Pic(R)$. In particular, if $R = \mathcal{O}_K$ then all the fractional ideals are invertible, so $Pic(R) = Cl(K)$.

One obvious question we might ask is whether unique factorization of ideals holds for the invertible fractional ideals. Unfortunately, the answer is no. Consider the following (taken from Cox[1]):

Example 2. Look at the order $R = \mathbb{Z}[\sqrt{-3}] \subset \mathbb{Q}(\sqrt{-3})$. It isn't the full ring of integers, so is not integrally closed. Further, by ring theory we know that any U.F.D. is integrally closed (see Lang[2], Prop.7, p. 7.). Hence R is not a U.F.D. It is easy to show that all invertible fractional ideals in R are

principal. So, if unique factorization held at the level of ideals then unique factorization would also hold on elements, a contradiction.

But the situation isn't all bad. We just need to make one more definition.

Definition 5. The **conductor** of $\mathcal{O}$ is the set $\mathfrak{f} = \{\alpha \in \mathcal{O}_K | \, \alpha\mathcal{O}_K \subseteq \mathcal{O}\}$.

Notice that since $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, it is therefore a finitely generated $\mathcal{O}$-module. Hence, $\mathfrak{f} \neq 0$. The following theorems tell us why the conductor is important.

Theorem 1. *Given a prime ideal, $\mathfrak{p} \subset \mathcal{O}$, then*

$$\mathfrak{p} \nmid \mathfrak{f} \iff \mathcal{O}_{\mathfrak{p}} \text{ is integrally closed} \iff \mathfrak{p} \text{ is an invertible ideal.}$$

Proof. See Neukirch[4], p. 81, 84. □

Theorem 2. *The group of invertible fractional ideals relatively prime to the conductor have unique factorization.*

Proof. We can easily adapt Propositions 7.18, 7.20 and exercise 7.26 in Cox[1] to apply to all number fields K, in the case that the conductor is principal. For the general case use Neukirch[4], proposition I.12.6, and the theorem above. □

Theorem 3. *There is a natural exact sequence*

$$1 \longrightarrow \mathcal{O}^* \longrightarrow \mathcal{O}_K^* \longrightarrow (\mathcal{O}_K/\mathfrak{f})^*/(\mathcal{O}/\mathfrak{f})^* \longrightarrow Pic(\mathcal{O}) \longrightarrow Pic(\mathcal{O}_K) \longrightarrow 1.$$

Proof. See Neukirch[4], p. 78-80. □

It is an easy result that every class of ideals in $Pic(\mathcal{O})$ contains a prime ideal relatively prime to the conductor, $\mathfrak{f}$, of $\mathcal{O}$.

2 Orders in Imaginary Quadratic Fields

Just as with the full ring of integers, we can define the discriminant of an order, $\mathcal{O}$, as the discriminant of it's basis as a free $\mathbb{Z}$-module Notice, this basis is also a basis for K over $\mathbb{Q}$. In the case of orders of imaginary quadratic fields, this invariant has some particularly nice properties. For the rest of this section let $K = \mathbb{Q}(\sqrt{-n})$ with $n > 0$, n square-free. Let $\mathcal{O}$ be an order

of K. We know that $\mathcal{O}_K = \mathbb{Z}[\frac{d_K+\sqrt{d_K}}{2}]$ where d_K is the discriminant of K. More concretely:

$$d_K = \begin{cases} -n & \text{if } n \equiv 3 \pmod 4 \\ -4n & \text{otherwise} \end{cases}$$

We then have the following result.

Proposition 4. *Setting $\alpha = \frac{d_K+\sqrt{d_K}}{2}$ then every order in K can be written in the form $\mathcal{O} = \mathbb{Z}[f \cdot \alpha]$ for $f \geq 0$. Further, the ideal (f) is the conductor of $\mathcal{O}$, $f = [\mathcal{O}_K : \mathcal{O}]$, and the discriminant of the order is $f^2 d_K$.*

Proof. See Cox[1], p. 133-134. □

Example 3. Consider the order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$. A simple calculation shows that the discriminant is always $-4n$. The discriminant of $\mathcal{O}_K$ is either $-n$ or $-4n$. Thus, the conductor of this order is always (1) or (2).

This last proposition tells us that the structure of any order of K, in the case K is an imaginary quadratic field, is particularly simple. Namely, the order is generated over $\mathbb{Z}$ by a multiple of the discriminant. But there is something deeper going on. As we saw in the last section, fractional ideals that are prime to the conductor have unique factorization. The proof hinges upon the observation that there is a natural correspondence between ideals $\mathfrak{a} \subseteq \mathcal{O}$ relatively prime to the conductor and ideals of $\mathcal{O}_K$ (where unique factorization holds).

To make this concrete we fix some notation. Let $Cl(\mathcal{O}_K), I_K$, and P_K be the class group, group of fractional ideals, and group of principal fractional ideals of $\mathcal{O}_K$, respectively. Let $Cl(\mathcal{O}), I(\mathcal{O})$, and $P(\mathcal{O})$ be the corresponding groups over the order $\mathcal{O}$ (remember to use *invertible* fractional ideals and the Picard group here). When we wish to limit ourselves to elements relatively prime to f we write $I_K(f), P_K(f), I(\mathcal{O}, f)$, and $P(\mathcal{O}, f)$, in the obvious cases. We now have:

Theorem 5. *Let $\mathcal{O}$ be an order of K of conductor f. Then we have:*
(i) If $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal, prime to f, then $\mathfrak{a} \cap \mathcal{O}$ is an $\mathcal{O}$-ideal, prime to f, of the same norm.
(ii) If $\mathfrak{a}$ is an $\mathcal{O}$-ideal, prime to f, then $\mathfrak{a}\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal, prime to f, of the same norm.
(iii) The correspondences above induce inverse isomorphisms $I_{K,(f)} \cong I(\mathcal{O}, f)$.

Proof. We sketch the proof (found in Cox[1], p. 144-145):

Step 1: Let $\mathfrak{a}$ be an $\mathcal{O}$-ideal. Show that $\mathfrak{a}$ is prime to $f \iff N(\mathfrak{a})$ is prime to f.

Notation: For convenience we are writing f rather than (f) for the conductor. From now on it is understood that $\mathfrak{a}$ is always prime to f. Further we know whether $\mathfrak{a}$ is an $\mathcal{O}$-ideal or an $\mathcal{O}_K$-ideal by considering the context.

Step 2: Show that the map

$$\mathcal{O}/\mathfrak{a} \cap \mathcal{O} \longrightarrow \mathcal{O}_K/\mathfrak{a}$$

is an isomorphism. Injectivity is trivial, and this implies $N(\mathfrak{a} \cap \mathcal{O})$ is prime to f. Surjectivity follows from the fact that $\mathfrak{a}$ is prime to (f), so multiplication by f induces an automorphism of $\mathcal{O}_K/\mathfrak{a}$. Note, $f\mathcal{O}_K \subseteq \mathcal{O}$ by definition of the conductor. Since the map above is an isomorphism this implies $N(\mathfrak{a} \cap \mathcal{O}) = N(\mathfrak{a})$.

Step 3: Prove the following two equations

$$\mathfrak{a}\mathcal{O}_K \cap \mathcal{O} = \mathfrak{a} \quad \text{when } \mathfrak{a} \text{ is an } \mathcal{O}\text{-ideal}$$

$$(\mathfrak{a} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{a} \quad \text{when } \mathfrak{a} \text{ is an } \mathcal{O}_K\text{-ideal.}$$

We will show how to prove the first one.

$$\mathfrak{a} \subseteq \mathfrak{a}\mathcal{O}_K \cap \mathcal{O} = (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})\mathcal{O} = (\mathfrak{a}\mathcal{O}_K \cap \mathcal{O})(\mathfrak{a} + f\mathcal{O})$$

$$\subseteq \mathfrak{a} + f(\mathfrak{a}\mathcal{O}_K \cap \mathcal{O}) \subseteq \mathfrak{a} + \mathfrak{a} \cdot f\mathcal{O}_K \subseteq \mathfrak{a} + \mathfrak{a}\mathcal{O} \subset \mathfrak{a}.$$

Step 4: Notice that the map $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ is multiplicative, so the map of monoids just constructed is in fact a group isomorphism. □

Using part (iii) of this theorem we would hope to find a relationship between the class group (i.e. the Picard group) of $\mathcal{O}$ and the class group of $\mathcal{O}_K$. In fact, this is hoping for too much, since we have to restrict to ideals relatively prime to f. However, the notion of *generalized ideal class groups* provides a way to express the needed information. For clarity, let us recall some definitions. (Note: We do not need to restrict to the case the K is an imaginary quadratic field to make these definitions.)

Definition 6. A **modulus**, $\mathfrak{m}$, is a formal product of places (or primes, if you include the infinite primes), written

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$$

where the $e_{\mathfrak{p}}$ satisfy

$$\begin{cases} e_{\mathfrak{p}} \geq 0 & \text{and almost all are equal to 0} \\ e_{\mathfrak{p}} = 0 & \text{if } \mathfrak{p} \text{ is a complex prime} \\ e_{\mathfrak{p}} \leq 1 & \text{if } \mathfrak{p} \text{ is a real prime.} \end{cases}$$

We write $\mathfrak{m}_0$ for the product of the finite primes in $\mathfrak{m}$. So in fact, $\mathfrak{m}_0$ is an ideal.

Given a modulus, $\mathfrak{m}$, we write $I_K(\mathfrak{m})$ for the group of fractional ideals of $\mathcal{O}_K$ relatively prime to $\mathfrak{m}_0$. We write $P_{K,1}(\mathfrak{m})$ for the group of principal ideals generated by $\alpha\mathcal{O}_K$ such that: (i) $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ and (ii) α is positive in any real embedding dividing $\mathfrak{m}$. Notice, in the case K is a imaginary quadratic number field, that there are no real places so $\mathfrak{m} = \mathfrak{m}_0$.

Definition 7. A **congruence subgroup** for a modulus $\mathfrak{m}$ is a group H where $P_{K,1}(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m})$.

Definition 8. A **generalized ideal class group** for a modulus $\mathfrak{m}$ is the quotient $I_K(\mathfrak{m})/H$ where H is a congruence subgroup.

For references that give explanations and motivations for these definitions, see Cox[1], p. 159-178; Milne[3], p. 113-146; and Neukirch[4], p. 363-368.

Example 4. When we take the smallest congruence subgroup possible, namely $H = P_{K,1}(\mathfrak{m})$, we say that the corresponding generalized ideal class group is the **ray class group** for $\mathfrak{m}$. In the case when $\mathfrak{m} = 1$, the ray class group is just the usual class group $Cl(K)$. When $\mathfrak{m}$ is the product of the real places we call the generalized ideal group the **narrow class group**.

Now comes the wonderful result:

Theorem 6. *We have an isomorphism*

$$Cl(\mathcal{O}) \cong I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I_K(f)/P_K(f).$$

Proof. See Cox[1], p. 145-146. □

Corollary 7. *Let K be an imaginary quadratic field, let $\mathcal{O}$ be an order over K, and let (f) be the conductor of $\mathcal{O}$. Then the class group of $\mathcal{O}$ corresponds to a generalized class group for the modulus $\mathfrak{m} = (f)$.*

Proof. Use the above theorem, with the fact that $P_{K,1}(f) \subseteq P_K(f) \subseteq I_K(f)$. □

Example 5. This example shows that the class group of an order can equal the class group of its integral closure, even for a proper order.

Let $K = \mathbb{Q}(\sqrt{-3})$ and let $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$. As we saw in an earlier example, the conductor for $\mathcal{O}$ is (2) and $Cl(\mathcal{O}) = 1$ (one way to prove this is to relate quadratic forms to ideals, and show that the quadratic forms corresponding to invertible ideals also correspond to principal ideals). With much less work, one can show that $Cl(\mathcal{O}_K) = 1$. This is equivalent to showing that $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is a P.I.D. This follows from the fact that the field norm is actually a Euclidean norm, making $\mathcal{O}_K$ into a Euclidean domain, and hence a P.I.D.

Example 6. It is known that having $Cl(\mathcal{O}) = Cl(\mathcal{O}_K)$, when $\mathcal{O} \subsetneq \mathcal{O}_K$, is rare (over imaginary quadratic fields). In fact, letting $d < 0$ be the discriminant of the order (which, by proposition 4, completely classifies the order) and letting $h(d)$ be the class number (i.e. the order of the class group $Cl(\mathcal{O})$) then $h(d) \to \infty$ as $d \to -\infty$.

3 Class Field Theory and Orders

Class field theory attempts to classify the abelian extensions of arbitrary number fields. In the case $K = \mathbb{Q}$ the answer is the Kronecker-Weber Theorem: any abelian extensions of $\mathbb{Q}$ is a subfield of $\mathbb{Q}(\zeta_m)$, for some m (and conversely). The answer is not nearly as nice when K is arbitrary. There is no known set of elements we can adjoin to K to exhaust the abelian extensions. However, the idea of generalized ideal class group gives us a way of classifying all abelian extensions. This result is commonly called the *Existence Theorem*. It states:

Theorem 8. *Given a modulus $\mathfrak{m}$ for a number field K, and a congruence subgroup H then there is a unique abelian extension L/K so that the Artin map gives an isomorphism*

$$I_K(\mathfrak{m})/H \xrightarrow{\sim} Gal(L/K).$$

For a proof of this theorem, look in any book on class field theory! Note, for the Artin map to even be well-defined it must be the case that all ramified primes (finite or infinite) of L/K must divide $\mathfrak{m}$. For those unfamiliar with

the Artin map (which *basically* sends a prime ideal to its Frobenius) see Milne[3], p. 4-5.

Example 7. In the case that our modulus is just equal to 1, and our congruence subgroup is just $H = P_{K,1}(1) = P_K$, then this theorem says that $Cl(\mathcal{O}_K)$ is isomorphic to $Gal(L/K)$ for some unramified extension L of K. In fact, one can prove it is the maximal unramified abelian extension. This field is called the **Hilbert class field**, in honor of Hilbert's work on these fields.

Example 8. Let $H = P_{K,1}(\mathfrak{m})$. The theorem above then says that the ray class group corresponds to a unique field, called the **ray class field**. Let $K = \mathbb{Q}$. Let our modulus be $\mathfrak{m} = a \cdot \infty$, where ∞ is the unique real embedding of $\mathbb{Q}$ and $a > 0$. Then the ray class field is $\mathbb{Q}(\zeta_a)$. If we take away the infinite prime, then the ray class field becomes $\mathbb{Q}(\zeta_a + \zeta_a^{-1})$.

We now have the immediate corollary:

Corollary 9. *Every order, $\mathcal{O}$, over an imaginary quadratic field, K, gives a unique abelian extension L/K, which is unramified over the conductor, and such that the Artin map induces $Cl(\mathcal{O}) \xrightarrow{\sim} Gal(L/K)$. This field is called the* **ring class field** *of $\mathcal{O}$.*

Proof. Just combine Corollary 7 and Theorem 8. This theorem actually holds for orders over *any* number field. The interested reader is encouraged to work out the details, by modifying the proofs of Theorems 5 and 6 to arbitrary extensions of $\mathbb{Q}$. Warning: In this case, the conductor $\mathfrak{f}$ is not necessarily principal. □

Example 9. It is not a simple matter to determine ring class fields. However, when restricting to imaginary quadratic fields, there are methods to find the explicit ring class field of any order. One of these techniques involve modular functions, elliptic curves, and complex multiplication.

We saw earlier that we could adjoin the roots of unity to find all abelian extension of $K = \mathbb{Q}$. Complex multiplication allows one to similarly find such elements, in the case $K = \mathbb{Q}(\sqrt{-n})$. We direct those wishing a very basic introduction to these ideas to Cox[1].

Example 10. Some explicit computations.

The ring class field of $\mathcal{O} = Z[\sqrt{-3}] \subset \mathbb{Q}(\sqrt{-3})$, is $L = \mathbb{Q}(\sqrt{-3})$ (which is also the Hilbert class field), since $Cl(\mathcal{O}) = 1 = Gal(L/K)$.

The ring class field of $\mathcal{O} = \mathbb{Z}[\sqrt{-27}] \subset \mathbb{Q}(\sqrt{-3})$ is $L = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$. To prove this, show that the class number of $\mathcal{O}$ is 3, and that L/K is unramified.

The ring class field of $\mathcal{O} = \mathbb{Z}[\sqrt{-17}] \subset \mathbb{Q}(\sqrt{-17})$ is $L = \mathbb{Q}(\sqrt{-17}, \sqrt{\frac{1+\sqrt{17}}{2}})$. To prove this, show that $Cl(\mathcal{O}) \cong \mathbb{Z}/4\mathbb{Z}$, and show that L/K is unramified.

We would be remiss not to mention why this theory is developed in Cox[1], and how it applies to number theory. As we mentioned at the beginning of this paper, using the ring of algebraic integers $\mathbb{Z}[i]$, and letting p be an odd prime, one can prove

$$p = a^2 + b^2 \text{ with } a, b \in \mathbb{Z} \iff p \equiv 1 \pmod 4.$$

This was claimed by Fermat, and given a concrete proof by Euler. The question can then be asked: When is a prime of the form $p = a^2 + nb^2$, for $n > 0$? The answer, after work by Fermat, Euler, Gauss, and myriad other mathematicians is the following:

Theorem 10. *Let $n > 0$, let $K = \mathbb{Q}(\sqrt{-n})$, and let $f_n(x) \in \mathbb{Z}[x]$ be a minimal polynomial of any algebraic integer α, so that $L = K(\alpha)$ is the ring class field for the order $\mathbb{Z}[\sqrt{-n}]$. Suppose p is a prime number, relatively prime to n and the discriminant of $f_n(x)$. Then*

$$p = x^2 + ny^2 \iff (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \pmod p.$$

Conversely, if $f(x)$ is any polynomial satisfying the conditions above, it is the minimal polynomial for a generator for the ring class field of $\mathcal{O}$.

Proof. This is Theorem 9.2 in Cox[1]. The proof is amazingly simple in concept. Clearly, letting p be relatively prime to n and the discriminant of $f_n(x)$ makes it so that p is relatively prime to the conductor of $\mathcal{O}$ and the discriminant of L. Then, in this case, one shows that $p = x^2 + ny^2 \iff p$ splits completely in L. The proof makes use of the Artin map, and the fact that $(-n/p) = 1 \iff p$ splits completely in K. □

4 One Final Theorem and Remark

As we have seen, there are some remarkable results concerning orders. We add one more beautiful result:

Theorem 11. *Let $\mathcal{O}$ be an order over K, an imaginary quadratic field. Let L be the ring class field of $\mathcal{O}$. Then*

$$Gal(L/\mathbb{Q}) \cong Gal(L/K) \rtimes (\mathbb{Z}/2\mathbb{Z}) \quad (*)$$

where the semidirect product has the structure where the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ sends an element of $Gal(L/K)$ to its inverse (such an extension of $\mathbb{Q}$ is called a dihedral extension).

Conversely, given an abelian extension L/K satisfying $(*)$, then L is a subfield of some ring class field.

Proof. Lemma 9.3 and Theorem 9.18 in Cox[1]. □

Thus, we see that ring class fields allow us to classify all dihedral extensions of $\mathbb{Q}$. Information about orders converts to information about which Galois extensions are possible.

Results like these show that there is a beautiful, underlying structure to the theory of orders. In this survey we have restricted our attention, for the most part, to orders over imaginary quadratic fields. This is because the theory is nowhere near as coherent over any other field (except trivially, $\mathbb{Q}$) and not nearly as developed. This is a field of study that is both challenging and full of unsolved problems.

References

[1] David A. Cox, *Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication*, John Wiley and Sons, Inc., New York, 1989.

[2] Serge Lang, *Algebraic Number Theory*, 2nd ed., Springer-Verlag, New York, 1994.

[3] J.S. Milne, *Class Field Theory*, http://www.wath.lsa.umich.edu/~jmilne, 1997.

[4] Jürgen Neukirch, *Algebraic Number Theory*, Springer-Verlag, New York, 1999.