Math 129: Algebraic Number Theory
Lecture 4

William Stein

Tuesday, February 17, 2004

Note: There's a book called *Algebraic Number Theory and Fermat's Last Theorem* by Stewart and Tall, which appears to have a detailed introduction to algebraic number theory and assumes little background on the part of the reader. There is a discussion of the definition of module, and proofs of basic facts about number fields, and many exercises. If you find Swinnerton-Dyer's book difficult, you might want to try to get your hands on Stewart and Tall, which costs about $38 new. (Hand around a copy.)

Today we will deduce, with complete proofs, the most important basic property of the ring of integers $\mathcal{O}_K$ of an algebraic number, namely that every nonzero ideals can be written uniquely as products of prime ideals. After proving this fundamental theorem, we will compute some examples using MAGMA. On Thursday the lecture will consist mostly of examples illustrating the substantial theory we will have already developed, so hang in there!

1 Dedekind Domains

Corollary 1.1. *The ring of integers $\mathcal{O}_K$ of a number field is Noetherian.*

Proof. As we saw before using norms, the ring $\mathcal{O}_K$ is finitely generated as a module over $\mathbf{Z}$, so it is certainly finitely generated as a ring over $\mathbf{Z}$. By the Hilbert Basis Theorem, $\mathcal{O}_K$ is Noetherian. $\square$

If R is an integral domain, the *field of fractions* of R is the field of all elements a/b, where $a, b \in R$. The field of fractions of R is the smallest field that contains R. For example, the field of fractions of $\mathbf{Z}$ is $\mathbf{Q}$ and of $\mathbf{Z}[(1+\sqrt{5})/2]$ is $\mathbf{Q}(\sqrt{5})$.

Definition 1.2 (Integrally Closed). An integral domain R is *integrally closed in its field of fractions* if whenever α is in the field of fractions of R and α satisfies a monic polynomial $f \in R[x]$, then $\alpha \in R$.

Proposition 1.3. *If K is any number field, then $\mathcal{O}_K$ is integrally closed. Also, the ring $\overline{\mathbf{Z}}$ of all algebraic integers is integrally closed.*

Proof. We first prove that $\overline{\mathbf{Z}}$ is integrally closed. Suppose $c \in \overline{\mathbf{Q}}$ is integral over $\overline{\mathbf{Z}}$, so there is a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in \overline{\mathbf{Z}}$ and $f(c) = 0$. The a_i all lie in the ring of integers $\mathcal{O}_K$ of the number field $K = \mathbf{Q}(a_0, a_1, \ldots a_{n-1})$, and $\mathcal{O}_K$ is finitely generated as a $\mathbf{Z}$-module, so $\mathbf{Z}[a_0, \ldots, a_{n-1}]$ is finitely generated as a $\mathbf{Z}$-module. Since $f(c) = 0$, we can write c^n as a $\mathbf{Z}[a_0, \ldots, a_{n-1}]$-linear combination of c^i for $i < n$, so the ring $\mathbf{Z}[a_0, \ldots, a_{n-1}, c]$ is also finitely generated as a $\mathbf{Z}$-module. Thus $\mathbf{Z}[c]$ is finitely generated as $\mathbf{Z}$-module because it is a submodule of a finitely generated $\mathbf{Z}$-module, which implies that c is integral over $\mathbf{Z}$.

Suppose $c \in K$ is integral over $\mathcal{O}_K$. Then since $\overline{\mathbf{Z}}$ is integrally closed, c is an element of $\overline{\mathbf{Z}}$, so $c \in K \cap \overline{\mathbf{Z}} = \mathcal{O}_K$, as required. □

Definition 1.4 (Dedekind Domain). An integral domain R is a *Dedekind domain* if it is Noetherian, integrally closed in its field of fractions, and every nonzero prime ideal of R is maximal.

The ring $\mathbf{Q} \oplus \mathbf{Q}$ is Noetherian, integrally closed in its field of fractions, and the two prime ideals are maximal. However, it is not a Dedekind domain because it is not an integral domain. The ring $\mathbf{Z}[\sqrt{5}]$ is not a Dedekind domain because it is not integrally closed in its field of fractions, as $(1 + \sqrt{5})/2$ is integrally over $\mathbf{Z}$ and lies in $\mathbf{Q}(\sqrt{5})$, but not in $\mathbf{Z}[\sqrt{5}]$. The ring $\mathbf{Z}$ is a Dedekind domain, as is any ring of integers $\mathcal{O}_K$ of a number field, as we will see below. Also, any field K is a Dedekind domain, since it is a domain, it is trivially integrally closed in itself, and there are no nonzero prime ideals so that condition that they be maximal is empty.

Proposition 1.5. *The ring of integers $\mathcal{O}_K$ of a number field is a Dedekind domain.*

Proof. By Proposition 1.3, the ring $\mathcal{O}_K$ is integrally closed, and by Proposition 1.1 it is Noetherian. Suppose that $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$. Let $\alpha \in \mathfrak{p}$ be a nonzero element, and let $f(x) \in \mathbf{Z}[x]$ be the minimal polynomial of α. Then

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

so $a_0 = -(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha) \in \mathfrak{p}$. Since f is irreducible, a_0 is a nonzero element of $\mathbf{Z}$ that lies in $\mathfrak{p}$. Every element of the finitely generated abelian group $\mathcal{O}_K/\mathfrak{p}$ is killed by a_0, so $\mathcal{O}_K/\mathfrak{p}$ is a finite set. Since $\mathfrak{p}$ is prime, $\mathcal{O}_K/\mathfrak{p}$ is an integral domain. Every finite integral domain is a field, so $\mathfrak{p}$ is maximal, which completes the proof. □

If I and J are ideals in a ring R, the product IJ is the ideal generated by all products of elements in I with elements in J:

$$IJ = (ab : a \in I, b \in J) \subset R.$$

Note that the set of all products ab, with $a \in I$ and $b \in J$, need not be an ideal, so it is important to take the ideal generated by that set. (See the homework problems for examples.)

Definition 1.6 (Fractional Ideal). A *fractional ideal* is an $\mathcal{O}_K$-submodule of $I \subset K$ that is finitely generated as an $\mathcal{O}_K$-module.

To avoid confusion, we will sometimes call a genuine ideal $I \subset \mathcal{O}_K$ an *integral ideal*. Also, since fractional ideals are finitely generated, we can clear denominators of a generating set to see that every fractional ideal is of the form $aI = \{ab : b \in I\}$ for some $a \in K$ and ideal $I \subset \mathcal{O}_K$.

For example, the collection $\frac{1}{2}\mathbf{Z}$ of rational numbers with denominator 1 or 2 is a fractional ideal of $\mathbf{Z}$.

Theorem 1.7. *The set of nonzero fractional ideals of a Dedekind domain R is an abelian group under ideal multiplication.*

Before proving Theorem 1.7 we prove a lemma. For the rest of this section $\mathcal{O}_K$ is the ring of integers of a number field K.

Definition 1.8 (Divides for Ideals). Suppose that I, J are ideals of $\mathcal{O}_K$. Then I *divides* J if $I \supset J$.

To see that this notion of divides is sensible, suppose $K = \mathbf{Q}$, so $\mathcal{O}_K = \mathbf{Z}$. Then $I = (n)$ and $J = (m)$ for some integer n and m, and I divides J means that $(n) \supset (m)$, i.e., that there exists an integer c such that $m = cn$, which exactly means that n divides m, as expected.

Lemma 1.9. *Suppose I is an ideal of $\mathcal{O}_K$. Then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_n \subset I$. In other words, I divides a product of prime ideals. (By convention the empty product is the unit ideal. Also, if $I = 0$, then we take $\mathfrak{p}_1 = (0)$, which is a prime ideal.)*

Proof. The key idea is to use that $\mathcal{O}_K$ is Noetherian to deduce that the set S of ideals that do not satisfy the lemma is empty. If S is nonempty, then because $\mathcal{O}_K$ is Noetherian, there is an ideal $I \in S$ that is maximal as an element of S. If I were prime, then I would trivially contain a product of primes, so I is not prime. By definition of prime ideal, there exists $a, b \in \mathcal{O}_K$ such that $ab \in I$ but $a \notin I$ and $b \notin I$. Let $J_1 = I + (a)$ and $J_2 = I + (b)$. Then neither J_1 nor J_2 is in S, since I is maximal, so both J_1 and J_2 contain a product of prime ideals. Thus so does I, since

$$J_1 J_2 = I^2 + I(b) + (a)I + (ab) \subset I,$$

which is a contradiction. Thus S is empty, which completes the proof. $\square$

We are now ready to prove the theorem.

Proof of Theorem 1.7. The product of two fractional ideals is again finitely generated, so it is a fractional ideal, and $I\mathcal{O}_K = \mathcal{O}_K$ for any nonzero ideal I, so to prove that the set of fractional ideals under multiplication is a group it suffices to show the existence of inverses. We will first prove that if $\mathfrak{p}$ is a prime ideal, then $\mathfrak{p}$ has an inverse, then we will prove that nonzero integral ideals have inverses, and finally observe that every fractional ideal has an inverse.

Suppose $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$. We will show that the $\mathcal{O}_K$-module

$$I = \{a \in K : a\mathfrak{p} \subset \mathcal{O}_K\}$$

is a fractional ideal of $\mathcal{O}_K$ such that $I\mathfrak{p} = \mathcal{O}_K$, so that I is an inverse of $\mathfrak{p}$.

For the rest of the proof, fix a nonzero element $b \in \mathfrak{p}$. Since I is an $\mathcal{O}_K$-module, $bI \subset \mathcal{O}_K$ is an $\mathcal{O}_K$ ideal, hence I is a fractional ideal. Since $\mathcal{O}_K \subset I$ we have $\mathfrak{p} \subset I\mathfrak{p} \subset \mathcal{O}_K$, hence either $\mathfrak{p} = I\mathfrak{p}$ or $I\mathfrak{p} = \mathcal{O}_K$. If $I\mathfrak{p} = \mathcal{O}_K$, we are done since then I is an inverse of $\mathfrak{p}$. Thus suppose that $I\mathfrak{p} = \mathfrak{p}$. Our strategy is to show that there is some $d \in I$ not in $\mathcal{O}_K$; such a d would leave $\mathfrak{p}$ invariant (i.e., $d\mathfrak{p} \subset \mathfrak{p}$), so since $\mathfrak{p}$ is an $\mathcal{O}_K$-module it will follow that $d \in \mathcal{O}_K$, a contradiction.

By Lemma 1.9, we can choose a product $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$, with m minimal, such that

$$\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m \subset (b) \subset \mathfrak{p}.$$

If no $\mathfrak{p}_i$ is contained in $\mathfrak{p}$, then we can choose for each i an $a_i \in \mathfrak{p}_i$ with $a_i \notin \mathfrak{p}$; but then $\prod a_i \in \mathfrak{p}$, which contradicts that $\mathfrak{p}$ is a prime ideal. Thus some $\mathfrak{p}_i$, say $\mathfrak{p}_1$, is contained in $\mathfrak{p}$, which implies that $\mathfrak{p}_1 = \mathfrak{p}$ since every nonzero prime ideal is maximal. Because m is minimal, $\mathfrak{p}_2\cdots\mathfrak{p}_m$ is not a subset of (b), so there exists $c \in \mathfrak{p}_2\cdots\mathfrak{p}_m$ that does not lie in (b). Then $\mathfrak{p}(c) \subset (b)$, so by definition of I we have $d = c/b \in I$. However, $d \notin \mathcal{O}_K$, since if it were then c would be in (b). We have thus found our element $d \in I$ that does not lie in $\mathcal{O}_K$. To finish the proof that $\mathfrak{p}$ has an inverse, we observe that d preserves the $\mathcal{O}_K$-module $\mathfrak{p}$, and is hence in $\mathcal{O}_K$, a contradiction. More precisely, if $b_1, \ldots, b_n$ is a basis for $\mathfrak{p}$ as a $\mathbf{Z}$-module, then the action of d on $\mathfrak{p}$ is given by a matrix with entries in $\mathbf{Z}$, so the minimal polynomial of d has coefficients in $\mathbf{Z}$. This implies that d is integral over $\mathbf{Z}$, so $d \in \mathcal{O}_K$, since $\mathcal{O}_K$ is integrally closed by Proposition 1.3. (Note how this argument depends strongly on the fact that $\mathcal{O}_K$ is integrally closed!)

So far we have proved that if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then $\mathfrak{p}^{-1} = \{a \in \mathbf{K} : a\mathfrak{p} \subset \mathcal{O}_K\}$ is the inverse of $\mathfrak{p}$ in the monoid of nonzero fractional ideals of $\mathcal{O}_K$. As mentioned after Definition 1.6, every nonzero fractional ideal is of the form aI for $a \in K$ and I an integral ideal, so since (a) has inverse $(1/a)$, it suffices to show that every integral ideal I has an inverse. If not, then there is a nonzero integral ideal I that is maximal among all nonzero integral ideals that do not have an inverse. Every ideal is contained in a maximal ideal, so there is a nonzero prime ideal $\mathfrak{p}$ such that $I \subset \mathfrak{p}$. Then $I \subset \mathfrak{p}^{-1}I \subset \mathcal{O}_K$. If $I = \mathfrak{p}^{-1}I$, then (arguing as in the previous paragraph) each element of $\mathfrak{p}^{-1}$ preserves that $\mathcal{O}_K$-ideal I and is hence integral, so $\mathfrak{p}^{-1} \subset \mathcal{O}_K$, which implies that $\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^{-1} \subset \mathfrak{p}$, a contradiction. Thus $I \neq \mathfrak{p}^{-1}I$. Because I is maximal among ideals that do not have an inverse, the ideal $\mathfrak{p}^{-1}I$ does have an inverse, call it J. Then $\mathfrak{p}J$ is the inverse of I, since $\mathcal{O}_K = (\mathfrak{p}J)(\mathfrak{p}^{-1}I) = JI$. □

We can finally deduce the crucial Theorem 1.11, which will allow us to show that any nonzero ideal of a Dedekind domain can be expressed uniquely as a product of primes (up to order). Thus unique factorization holds for ideals in a Dedekind domain, and it is this unique factorization that initially motivated the introduction of rings of integers of number fields over a century ago.

Theorem 1.10. *Suppose I is an integral ideal of $\mathcal{O}_K$. Then I can be written as a product*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_n$$

of prime ideals of $\mathcal{O}_K$, and this representation is unique up to order. (Exception: If $I = 0$, then the representation is not unique.)

Proof. Suppose I is an ideal that is maximal among the set of all ideals in $\mathcal{O}_K$ that can not be written as a product of primes. Every ideal is contained in a maximal ideal, so I is contained in a nonzero prime ideal $\mathfrak{p}$. If $I\mathfrak{p}^{-1} = I$, then by Theorem 1.7 we can cancel I from both sides of this equation to see that $\mathfrak{p}^{-1} = \mathcal{O}_K$, a contradiction. Thus I is strictly contained in $I\mathfrak{p}^{-1}$, so by our maximality assumption on I there are maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $I\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Then $I = \mathfrak{p} \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_n$, a contradiction. Thus every ideal can be written as a product of primes.

Suppose $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m$. If no $\mathfrak{q}_i$ is contained in $\mathfrak{p}_1$, then for each i there is an $a_i \in \mathfrak{q}_i$ such that $a_i \notin \mathfrak{p}_1$. But the product of the a_i is in the $\mathfrak{p}_1 \cdots \mathfrak{p}_n$, which is a subset of $\mathfrak{p}_1$, which contradicts the fact that $\mathfrak{p}_1$ is a prime ideal. Thus $\mathfrak{q}_i = \mathfrak{p}_1$ for some i. We can thus cancel $\mathfrak{q}_i$ and $\mathfrak{p}_1$ from both sides of the equation. Repeating this argument finishes the proof of uniqueness. □

Corollary 1.11. *If I is a fractional ideal of $\mathcal{O}_K$ then there exists prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$, unique up to order, such that*

$$I = (\mathfrak{p}_1 \cdots \mathfrak{p}_n)(\mathfrak{q}_1 \cdots \mathfrak{q}_m)^{-1}.$$

Proof. We have $I = (a/b)J$ for some $a, b \in \mathcal{O}_K$ and integral ideal J. Applying Theorem 1.11 to (a), (b), and J gives an expression as claimed. For uniqueness, if one has two such product expressions, multiply through by the denominators and use the uniqueness part of Theorem 1.11 □

2 Using MAGMA

This section is a first introduction to MAGMA, which is an excellent package for doing algebraic number theory computations. You can use it via the web page `http://modular.fas.harvard.edu/calc`. MAGMA is not free, but if you would like a copy for your personal computer, send me an email, and I can arrange for you to obtain a legal copy for free. (Say something about my visiting MAGMA in Sydney three times, and how MAGMA compares to Maple, Mathematica, and PARI.)

1. MAGMA web page

2. Example code to illustrate things so far in course, and relevant to each homework problems. Experiment with students suggesting what examples to try.

3 Algorithms for Algebraic Number Theory

The best overall reference for algorithms for doing basic algebraic number theory computations is Henri Cohen's book *A Course in Computational Algebraic Number Theory*, Springer, GTM 138.

Our main long-term algorithmic goals for this course are to understand good algorithms for solving the following problems in particular cases:

- **Ring of integers:** Given a number field K (by giving a polynomial), compute the full ring $\mathcal{O}_K$ of integers.

- **Decomposition of primes:** Given a prime number $p \in \mathbf{Z}$, find the decomposition of the ideal $p\mathcal{O}_K$ as a product of prime ideals of $\mathcal{O}_K$.

- **Class group:** Compute the group of equivalence classes of nonzero ideals of $\mathcal{O}_K$, where I and J are equivalent if there exists $\alpha \in \mathcal{O}_K$ such that $IJ^{-1} = (\alpha)$.

- **Units:** Compute generators for the group of units of $\mathcal{O}_K$.

As we will see, somewhat surprisingly it turns out that algorithmically by far the most time-consuming step in computing the ring of integers $\mathcal{O}_K$ is to factor the discriminant of a polynomial whose root generates the field K. The algorithm(s) for computing $\mathcal{O}_K$ are quite complicated to describe, but the first step is to factor this discriminant, and it takes much longer in practice than all the other complicated steps.