Math 129: Algebraic Number Theory
Lecture 3

William Stein

Thursday, February 12, 2004

`Announcements:` I will be giving a talk on my research on computing with modular abelian varieties at 3pm in SC 507 today. If you're interested in finding out what my research is about, feel free to attend. The first half will be less technical, and you could leave halfway through.

`-----------------------------------------------------------------------`

Today we will learn about rings of algebraic integers and discuss some of their properties.

1 Rings of Algebraic Integers

Fix an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. For example, $\overline{\mathbf{Q}}$ could be the subfield of the complex numbers $\mathbf{C}$ generated by all roots in $\mathbf{C}$ of all polynomials with coefficients in $\mathbf{Q}$.

Much of this course is about algebraic integers.

Definition 1.1 (Algebraic Integer). An element $\alpha \in \overline{\mathbf{Q}}$ is an *algebraic integer* if it is a root of some monic polynomial with coefficients in $\mathbf{Z}$.

Definition 1.2 (Minimal Polynomial). The *minimal polynomial* of $\alpha \in \mathbf{Q}$ is the monic polynomial $f \in \mathbf{Q}[x]$ of least positive degree such that $f(\alpha) = 0$.

The minimal polynomial of α divides any polynomial h such that $h(\alpha) = 0$, for the following reason. If $h(\alpha) = 0$, use the division algorithm to write $h = qf + r$, where $0 \leq \deg(r) < \deg(f)$. We have $r(\alpha) = h(\alpha) - q(\alpha)f(\alpha) = 0$, so α is a root of r. However, f is the polynomial of least positive degree with root α, so $r = 0$.

Lemma 1.3. *If α is an algebraic integer, then the minimal polynomial of α has coefficients in $\mathbf{Z}$.*

Proof. Suppose $f \in \mathbf{Q}[x]$ is the minimal polynomial of α and $g \in \mathbf{Z}[x]$ is a monic integral polynomial such that $g(\alpha) = 0$. As mentioned after the definition of minimal polynomial, we have $g = fh$, for some $h \in \mathbf{Q}[x]$. If $f \notin \mathbf{Z}[x]$, then some prime p

divides the denominator of some coefficient of f. Let p^i be the largest power of p that divides some denominator of some coefficient f, and likewise let p^j be the largest power of p that divides some denominator of a coefficient of g. Then $p^{i+j}g = (p^i f)(p^j g)$, and if we reduce both sides modulo p, then the left hand side is 0 but the right hand side is a product of two nonzero polynomials in $\mathbf{F}_p[x]$, hence nonzero, a contradiction. $\square$

Proposition 1.4. *An element $\alpha \in \overline{\mathbf{Q}}$ is integral if and only if $\mathbf{Z}[\alpha]$ is finitely generated as a $\mathbf{Z}$-module.*

Proof. Suppose α is integral and let $f \in \mathbf{Z}[x]$ be the monic minimal polynomial of α (that $f \in \mathbf{Z}[x]$ is Lemma 1.3). Then $\mathbf{Z}[\alpha]$ is generated by $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$, where d is the degree of f. Conversely, suppose $\alpha \in \overline{\mathbf{Q}}$ is such that $\mathbf{Z}[\alpha]$ is finitely generated, say by elements $f_1(\alpha), \ldots, f_n(\alpha)$. Let d be any integer bigger than the degree of any f_i. Then there exist integers a_i such that $\alpha^d = \sum a_i f_i(\alpha)$, hence α satisfies the monic polynomial $x^d - \sum a_i f_i(x) \in \mathbf{Z}[x]$, so α is integral. $\square$

The rational number $\alpha = 1/2$ is not integral. Note that $G = \mathbf{Z}[1/2]$ is not a finitely generated $\mathbf{Z}$-module, since G is infinite and $G/2G = 0$.

Proposition 1.5. *The set $\overline{\mathbf{Z}}$ of all algebraic integers is a ring, i.e., the sum and product of two algebraic integers is again an algebraic integer.*

Proof. Suppose $\alpha, \beta \in \mathbf{Z}$, and let m, n be the degrees of the minimal polynomials of α, β, respectively. Then $1, \alpha, \ldots, \alpha^{m-1}$ span $\mathbf{Z}[\alpha]$ and $1, \beta, \ldots, \beta^{n-1}$ span $\mathbf{Z}[\beta]$ as $\mathbf{Z}$-module. Thus the elements $\alpha^i\beta^j$ for $i \leq m, j \leq n$ span $\mathbf{Z}[\alpha, \beta]$. Since $\mathbf{Z}[\alpha+\beta]$ is a submodule of the finitely-generated module $\mathbf{Z}[\alpha, \beta]$, it is finitely generated, so $\alpha+\beta$ is integral. Likewise, $\mathbf{Z}[\alpha\beta]$ is a submodule of $\mathbf{Z}[\alpha, \beta]$, so it is also finitely generated and $\alpha\beta$ is integral. $\square$

Recall that a *number field* is a subfield K of $\overline{\mathbf{Q}}$ such that the degree $[K : \mathbf{Q}] := \dim_{\mathbf{Q}}(K)$ is finite.

Definition 1.6 (Ring of Integers). The *ring of integers* of a number field K is the ring

$$\mathcal{O}_K = K \cap \overline{\mathbf{Z}} = \{x \in K : \ x \text{ is an algebraic integer}\}.$$

The field $\mathbf{Q}$ of rational numbers is a number field of degree 1, and the ring of integers of $\mathbf{Q}$ is $\mathbf{Z}$. The field $K = \mathbf{Q}(i)$ of Gaussian integers has degree 2 and $\mathcal{O}_K = \mathbf{Z}[i]$. The field $K = \mathbf{Q}(\sqrt{5})$ has ring of integers $\mathcal{O}_K = \mathbf{Z}[(1+\sqrt{5})/2]$. Note that the Golden ratio $(1+\sqrt{5})/2$ satisfies $x^2 - x - 1$. According to MAGMA, the ring of integers of $K = \mathbf{Q}(\sqrt[3]{9})$ is $\mathbf{Z}[\sqrt[3]{3}]$, where $\sqrt[3]{3} = \frac{1}{3}(\sqrt[3]{9})^2$.

Definition 1.7 (Order). An *order* in $\mathcal{O}_K$ is any subring R of $\mathcal{O}_K$ such that the quotient $\mathcal{O}_K/R$ of abelian groups is finite. (Note that R must contain 1 because it is a ring, and for us every ring has a 1.)

As noted above, $\mathbf{Z}[i]$ is the ring of integers of $\mathbf{Q}(i)$. For every nonzero integer n, the subring $\mathbf{Z} + ni\mathbf{Z}$ of $\mathbf{Z}[i]$ is an order. The subring $\mathbf{Z}$ of $\mathbf{Z}[i]$ is not an order, because $\mathbf{Z}$ does not have finite index in $\mathbf{Z}[i]$. Also the subgroup $2\mathbf{Z} + i\mathbf{Z}$ of $\mathbf{Z}[i]$ is not an order because it is not a ring.

We will frequently consider orders in practice because they are often much easier to write down explicitly than $\mathcal{O}_K$. For example, if $K = \mathbf{Q}(\alpha)$ and α is an algebraic integer, then $\mathbf{Z}[\alpha]$ is an order in $\mathcal{O}_K$, but frequently $\mathbf{Z}[\alpha] \neq \mathcal{O}_K$.

Lemma 1.8. *Let $\mathcal{O}_K$ be the ring of integers of a number field. Then $\mathcal{O}_K \cap \mathbf{Q} = \mathbf{Z}$ and $\mathbf{Q}\mathcal{O}_K = K$.*

Proof. Suppose $\alpha \in \mathcal{O}_K \cap \mathbf{Q}$ with $\alpha = a/b$ in lowest terms and $b > 0$. The monic minimal polynomial of α is $bx - a \in \mathbf{Z}[x]$, so if $b \neq 1$ then Lemma 1.3 implies that α is not an algebraic integer, a contradiction.

To prove that $\mathbf{Q}\mathcal{O}_K = K$, suppose $\alpha \in K$, and let $f(x) \in \mathbf{Q}[x]$ be the minimal monic polynomial of α. For any positive integer d, the minimal monic polynomial of $d\alpha$ is $d^{\deg(f)} f(x/d)$, i.e., the polynomial obtained from $f(x)$ by multiplying the coefficient of $x^{\deg(f)}$ by 1, multiplying the coefficient of $x^{\deg(f)-1}$ by d, multiplying the coefficient of $x^{\deg(f)-2}$ by d^2, etc. If d is the least common multiple of the denominators of the coefficients of f, then the minimal monic polynomial of $d\alpha$ has integer coefficients, so $d\alpha$ is integral and $d\alpha \in \mathcal{O}_K$. This proves that $\mathbf{Q}\mathcal{O}_K = K$. □

In the next two sections we will develop some basic properties of norms and traces, and deduce further properties of rings of integers.

2 Norms and Traces

Before discussing norms and traces we introduce some notation for field extensions. If $K \subset L$ are number fields, we let $[L : K]$ denote the dimension of L viewed as a K-vector space. If K is a number field and $a \in \overline{\mathbf{Q}}$, let $K(a)$ be the number field generated by a, which is the smallest number field that contains a. If $a \in \overline{\mathbf{Q}}$ then a has a minimal polynomial $f(x) \in \mathbf{Q}[x]$, and the *Galois conjugates* of a are the roots of f. For example the element $\sqrt{2}$ has minimal polynomial $x^2 - 2$ and the Galois conjugates of $\sqrt{2}$ are $\pm\sqrt{2}$.

Suppose $K \subset L$ is an inclusion of number fields and let $a \in L$. Then left multiplication by a defines a K-linear transformation $\ell_a : L \to L$. (The transformation ℓ_a is K-linear because L is commutative.)

Definition 2.1 (Norm and Trace). The *norm* and *trace* of a from L to K are

$$\mathrm{norm}_{L/K}(a) = \det(\ell_a) \quad \text{and} \quad \mathrm{tr}_{L/K}(a) = \mathrm{tr}(\ell_a).$$

It is standard from linear algebra that determinants are multiplicative and traces are additive, so for $a, b \in L$ we have

$$\mathrm{norm}_{L/K}(ab) = \mathrm{norm}_{L/K}(a) \cdot \mathrm{norm}_{L/K}(b)$$

and

$$\mathrm{tr}_{L/K}(a+b) = \mathrm{tr}_{L/K}(a) + \mathrm{tr}_{L/K}(b).$$

Note that if $f \in \mathbf{Q}[x]$ is the characteristic polynomial of ℓ_a, then the constant term of f is $(-1)^{\deg(f)} \det(\ell_a)$, and the coefficient of $x^{\deg(f)-1}$ is $-\mathrm{tr}(\ell_a)$.

Proposition 2.2. *Let $a \in L$ and let $\sigma_1, \ldots, \sigma_d$, where $d = [L : K]$, be the distinct field embeddings $L \hookrightarrow \overline{\mathbf{Q}}$ that fix every element of K. Then*

$$\mathrm{norm}_{L/K}(a) = \prod_{i=1}^{d} \sigma_i(a) \quad \text{and} \quad \mathrm{tr}_{L/K}(a) = \sum_{i=1}^{d} \sigma_i(a).$$

Proof. We prove the proposition by computing the characteristic polynomial F of a. Let $f \in K[x]$ be the minimal polynomial of a over K, and note that f has distinct roots (since it is the polynomial in $K[x]$ of least degree that is satisfied by a). Since f is irreducible, $[K(a) : K] = \deg(f)$, and a satisfies a polynomial if and only if ℓ_a does, the characteristic polynomial of ℓ_a acting on $K(a)$ is f. Let $b_1, \ldots, b_n$ be a basis for L over $K(a)$ and note that $1, \ldots, a^m$ is a basis for $K(a)/K$, where $m = \deg(f) - 1$. Then $a^i b_j$ is a basis for L over K, and left multiplication by a acts the same way on the span of $b_j, ab_j, \ldots, a^m b_j$ as on the span of $b_k, ab_k, \ldots, a^m b_k$, for any pair $j, k \leq n$. Thus the matrix of ℓ_a on L is a block direct sum of copies of the matrix of ℓ_a acting on $K(a)$, so the characteristic polynomial of ℓ_a on L is $f^{[L:K(a)]}$. The proposition follows because the roots of $f^{[L:K(a)]}$ are exactly the images $\sigma_i(a)$, with multiplicity $[L : K(a)]$ (since each embedding of $K(a)$ into $\overline{\mathbf{Q}}$ extends in exactly $[L : K(a)]$ ways to L by Exercise ??). □

The following corollary asserts that the norm and trace behave well in towers.

Corollary 2.3. *Suppose $K \subset L \subset M$ is a tower of number fields, and let $a \in M$. Then*

$$\mathrm{norm}_{M/K}(a) = \mathrm{norm}_{L/K}(\mathrm{norm}_{M/L}(a)) \quad \text{and} \quad \mathrm{tr}_{M/K}(a) = \mathrm{tr}_{L/K}(\mathrm{tr}_{M/L}(a)).$$

Proof. For the first equation, both sides are the product of $\sigma_i(a)$, where σ_i runs through the embeddings of M into K. To see this, suppose $\sigma : L \to \overline{\mathbf{Q}}$ fixes K. If σ' is an extension of σ to M, and $\tau_1, \ldots, \tau_d$ are the embeddings of M into $\overline{\mathbf{Q}}$ that fix L, then $\tau_1\sigma', \ldots, \tau_d\sigma'$ are exactly the extensions of σ to M. For the second statement, both sides are the sum of the $\sigma_i(a)$. □

The norm and trace down to $\mathbf{Q}$ of an algebraic integer a is an element of $\mathbf{Z}$, because the minimal polynomial of a has integer coefficients, and the characteristic polynomial of a is a power of the minimal polynomial, as we saw in the proof of Proposition 2.2.

Proposition 2.4. *Let K be a number field. The ring of integers $\mathcal{O}_K$ is a lattice in K, i.e., $\mathbf{Q}\mathcal{O}_K = K$ and $\mathcal{O}_K$ is an abelian group of rank $[K : \mathbf{Q}]$.*

Proof. We saw in Lemma 1.8 that $\mathbf{Q}\mathcal{O}_K = K$. Thus there exists a basis $a_1, \ldots, a_n$ for K, where each a_i is in $\mathcal{O}_K$. Suppose that as $x = \sum c_i a_i \in \mathcal{O}_K$ varies over all elements of $\mathcal{O}_K$ the denominators of the coefficients c_i are arbitrarily large. Then subtracting off integer multiples of the a_i, we see that as $x = \sum c_i a_i \in \mathcal{O}_K$ varies over elements of $\mathcal{O}_K$ with c_i between 0 and 1, the denominators of the c_i are also arbitrarily large. This implies that there are infinitely many elements of $\mathcal{O}_K$ in the bounded subset

$$S = \{c_1 a_1 + \cdots + c_n a_n : c_i \in \mathbf{Q},\ 0 \leq c_i \leq 1\} \subset K.$$

Thus for any $\varepsilon > 0$, there are elements $a, b \in \mathcal{O}_K$ such that the coefficients of $a - b$ are all less than ε (otherwise the elements of $\mathcal{O}_K$ would all be a "distance" of least ε from each other, so only finitely many of them would fit in S).

As mentioned above, the norms of elements of $\mathcal{O}_K$ are integers. Since the norm of an element is the determinant of left multiplication by that element, the norm is a homogenous polynomial of degree n in the indeterminate coefficients c_i. If the c_i get arbitrarily small for elements of $\mathcal{O}_K$, then the values of the norm polynomial get arbitrarily small, which would imply that there are elements of $\mathcal{O}_K$ with positive norm too small to be in $\mathbf{Z}$, a contradiction. So the set S contains only finitely many elements of $\mathcal{O}_K$. Thus the denominators of the c_i are bounded, so for some d, we have that $\mathcal{O}_K$ has finite index in $A = \frac{1}{d}\mathbf{Z}a_1 + \cdots + \frac{1}{d}\mathbf{Z}a_n$. Since A is isomorphic to $\mathbf{Z}^n$, it follows from the structure theorem for finitely generated abelian groups that $\mathcal{O}_K$ is isomorphic as a $\mathbf{Z}$-module to $\mathbf{Z}^n$, as claimed. □

Corollary 2.5. *The ring of integers $\mathcal{O}_K$ of a number field is Noetherian.*

Proof. By Proposition 2.4, 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. □

Definition 2.6 (Integrally Closed). An integral domain R is *integrally closed* 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 2.7. *If K is any number field, then $\mathcal{O}_K$ is integrally closed. Also, $\overline{\mathbf{Z}}$ is integrally closed.*

Proof. It suffices to prove that $\overline{\mathbf{Z}}$ is integrally closed, since if $c \in K$ is integral over $\mathcal{O}_K$, then c would be an element of $\overline{\mathbf{Z}}$, so $c \in K \cap \overline{\mathbf{Z}} = \mathcal{O}_K$, as required.

Now 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 by Proposition 2.4, 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. Then $\mathbf{Z}[c]$ 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 $\mathbf{Z}$. □

3 Dedekind Domains

Definition 3.1 (Dedekind Domain). A ring R is a *Dedekind domain* if it is Noetherian, integrally closed, and every nonzero prime ideal of R is maximal.

Proposition 3.2. *The ring of integers $\mathcal{O}_K$ of a number field is a Dedekind domain.*

Proof. By Proposition 2.7, the ring $\mathcal{O}_K$ is integrally closed, and by Proposition 2.5 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 (see Exercise ?), so $\mathfrak{p}$ is maximal, which completes the proof. $\square$

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:

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

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.

Next Tuesday we will start by proving the crucial Theorem 3.4 below, 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.

Definition 3.3 (Fractional Ideal). A *fractional ideal* is an $\mathcal{O}_K$-submodule of K that is finitely generated. 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 emphasis, we will sometimes call a genuine ideal $I \subset \mathcal{O}_K$ an *integral ideal.*

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

Theorem 3.4. *The set of nonzero fractional ideals of a Dedekind domain R is an abelian group under ideal multiplication.*