Math 129: Algebraic Number Theory
Lecture 2

William Stein

Tuesday, February 10, 2004

`Announcements:` (1) Barry Mazur will talk about his popular math book "Imagining Numbers" at the Harvard COOP tonight at 7pm. (2) I have office hours Tuesdays and Thursdays 2–3pm in SC 515.

We will do some serious commutative algebra today, which will provide a powerful algebraic foundation for understanding the more refined number-theoretic structures associated to number fields.

In the first section we establish the standard properties of Noetherian rings and modules, including the Hilbert basis theorem. We also observe that finitely generated abelian groups are Noetherian $\mathbf{Z}$-modules, which fills the gap in our proof of the structure theorem for finitely generated abelian groups. After establishing properties of Noetherian rings, we consider the rings of algebraic integers and discuss some of their properties.

1 Noetherian Rings and Modules

Let R be a commutative ring with unit element. We will frequently work with R-modules, which are like vector spaces but over a ring. More precisely, recall that an *R-module* is an additive abelian group M equipped with a map $R \times M \to M$ such that for all $r, r' \in R$ and all $m, m' \in M$ we have $(rr')m = r(r'm)$, $(r + r')m = rm + r'm$, $r(m + m') = rm + rm'$, and $1m = m$. A *submodule* is a subgroup of M that is preserved by the action of R.

Example 1.1. The set of abelian groups are in natural bijection with $\mathbf{Z}$-modules.

A *homomorphism* of R-modules $\varphi : M \to N$ is a abelian group homomorphism such that for any $r \in R$ and $m \in M$ we have $\varphi(rm) = r\varphi(m)$. A *short exact sequence* of R-modules

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$$

is a specific choice of injective homomorphism $f : L \to M$ and a surjective homomorphism $g : M \to N$ such that $\mathrm{im}(f) = \ker(g)$.

Definition 1.2 (Noetherian). An R-module M is *Noetherian* if every submodule of M is finitely generated. A ring R is *Noetherian* if R is Noetherian as a module over itself, i.e., if every ideal of R is finitely generated.

Notice that any submodule M' of M is Noetherian, because if every submodule of M is finitely generated then so is every submodule of M', since submodules of M' are also submodules of M.

Definition 1.3 (Ascending chain condition). An R-module M *satisfies the ascending chain condition* if every sequences $M_1 \subset M_2 \subset M_3 \subset \cdots$ of submodules of M eventually stabilizes, i.e., there is some n such that $M_n = M_{n+1} = M_{n+2} = \cdots$.

Proposition 1.4. *If M is an R-module, then the following are equivalent:*

1. *M is Noetherian,*
2. *M satisfies the ascending chain condition, and*
3. *Every nonempty set of submodules of M contains at least one maximal element.*

Proof. $1 \implies 2$**:** Suppose $M_1 \subset M_2 \subset \cdots$ is a sequence of submodules of M. Then $M_\infty = \cup_{n=1}^{\infty} M_n$ is a submodule of M. Since M is Noetherian, there is a finite set $a_1, \ldots, a_m$ of generators for M. Each a_i must be contained in some M_j, so there is an n such that $a_1, \ldots, a_m \in M_n$. But then $M_k = M_n$ for all $k \geq n$, which proves that the ascending chain condition holds for M.
$2 \implies 3$**:** Suppose 3 were false, so there exists a nonempty set S of submodules of M that does not contain a maximal element. We will use S to construct an infinite ascending chain of submodules of M that does not stabilize. Note that S is infinite, otherwise it would contain a maximal element. Let M_1 be any element of S. Then there is an M_2 in S that contains M_1, otherwise S would contain the maximal element M_1. Continuing inductively in this way we find an M_3 in S that properly contains M_2, etc., and we produce an infinite ascending chain of submodules of M, which contradicts the ascending chain condition.

$3 \implies 1$**:** Suppose 1 is false, so there is a submodule M' of M that is not finitely generated. We will show that the set S of all finitely generated submodules of M' does not have a maximal element, which will be a contradiction. Suppose S does have a maximal element L. Since L is finitely generated and $L \subset M'$, and M' is not finitely generated, there is an $a \in M'$ such that $a \notin L$. Then $L' = L + Ra$ is an element of S that strictly contains the presumed maximal element L, a contradiction. $\square$

Lemma 1.5. *If*

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$$

is a short exact sequence of R-modules, then M is Noetherian if and only if both L and N are Noetherian.

Proof. First suppose that M is Noetherian. Then L is a submodule of M, so L is Noetherian. If N' is a submodule of N, then the inverse image of N' in M is a submodule of M, so it is finitely generated, hence its image N' is finitely generated. Thus N is Noetherian as well.

Next assume nothing about M, but suppose that both L and N are Noetherian. If M' is a submodule of M, then $M_0 = \varphi(L) \cap M'$ is isomorphic to a submodule of the Noetherian module L, so M_0 is generated by finitely many elements $a_1, \ldots, a_n$. The quotient M'/M_0 is isomorphic (via g) to a submodule of the Noetherian module N, so M'/M_0 is generated by finitely many elements $b_1, \ldots, b_m$. For each $i \leq m$, let c_i be a lift of b_i to M', modulo M_0. Then the elements $a_1, \ldots, a_n, c_1, \ldots, c_m$ generate M', for if $x \in M'$, then there is some element $y \in M_0$ such that $x - y$ is an R-linear combination of the c_i, and y is an R-linear combination of the a_i. $\square$

Proposition 1.6. *Suppose R is a Noetherian ring. Then an R-module M is Noetherian if and only if it is finitely generated.*

Proof. If M is Noetherian then every submodule of M is finitely generated so M is finitely generated. Conversely, suppose M is finitely generated, say by elements $a_1, \ldots, a_n$. Then there is a surjective homomorphism from $R^n = R \oplus \cdots \oplus R$ to M that sends $(0, \ldots, 0, 1, 0, \ldots, 0)$ (1 in ith factor) to a_i. Using Lemma 1.5 and exact sequences of R-modules such as $0 \to R \to R \oplus R \to R \to 0$, we see inductively that R^n is Noetherian. Again by Lemma 1.5, homomorphic images of Noetherian modules are Noetherian, so M is Noetherian. $\square$

Lemma 1.7. *Suppose $\varphi : R \to S$ is a surjective homomorphism of rings and R is Noetherian. Then S is Noetherian.*

Proof. The kernel of φ is an ideal I in R, and we have an exact sequence

$$0 \to I \to R \to S \to 0$$

with R Noetherian. By Lemma 1.5, it follows that S is a Noetherian R-modules. Suppose J is an ideal of S. Since J is an R-submodule of S, if we view J as an R-module, then J is finitely generated. Since R acts on J through S, the R-generators of J are also S-generators of J, so J is finitely generated as an ideal. Thus S is Noetherian. $\square$

Theorem 1.8 (Hilbert Basis Theorem). *If R is a Noetherian ring and S is finitely generated as a ring over R, then S is Noetherian. In particular, for any n the polynomial ring $R[x_1, \ldots, x_n]$ and any of its quotients are Noetherian.*

Proof. Assume first that we have already shown that for any n the polynomial ring $R[x_1, \ldots, x_n]$ is Noetherian. Suppose S is finitely generated as a ring over R, so there are generators $s_1, \ldots, s_n$ for S. Then the map $x_i \mapsto s_i$ extends uniquely to a surjective homomorphism $\pi : R[x_1, \ldots, x_n] \to S$, and Lemma 1.7 implies that S is Noetherian.

The rings $R[x_1, \dots, x_n]$ and $(R[x_1, \dots, x_{n-1}])[x_n]$ are isomorphic, so it suffices to prove that if R is Noetherian then $R[x]$ is also Noetherian. (Our proof follows §12.5 of Artin's *Algebra*.) Thus suppose I is an ideal of $R[x]$ and that R is Noetherian. We will show that I is finitely generated.

Let A be the set of leading coefficients of polynomials in I along with 0. If $a, b \in A$ are nonzero with $a + b \neq 0$, then there are polynomials f and g in I with leading coefficients a and b. If $\deg(f) \leq \deg(g)$, then $a + b$ is the leading coefficient of $x^{\deg(g)-\deg(f)} f + g$, so $a + b \in A$. If $r \in R$ and $a \in A$ with $ra \neq 0$, then ra is the leading coefficient of rf, so $ra \in A$. Thus A is an ideal in R, so since R is Noetherian there exists $a_1, \dots, a_n$ that generate A as an ideal. Since A is the set of leading coefficients of elements of I, and the a_j are in I, we can choose for each $j \leq n$ an element $f_j \in I$ with leading coefficient a_j. By multipying the f_j by some power of x, we may assume that the f_j all have the same degree d.

Let $S_{<d}$ be the set of elements of I that have degree strictly less than d. This set is closed under addition and under multiplication by elements of R, so $S_{<d}$ is a module over R. The module $S_{<d}$ is submodule of the R-module of polynomials of degree less than n, which is Noetherian because it is generated by $1, x, \dots, x^{n-1}$. Thus $S_{<d}$ is finitely generated, and we may choose generators $h_1, \dots, h_m$ for $S_{<d}$.

Suppose $g \in I$ is an arbitrary element. We will show by induction on the degree of g that g is an $R[x]$-linear combination of $f_1, \dots, f_n, h_1, \dots h_m$. Thus suppose this statement is true for all elements of I of degree less than the degree of g. If the degree of g is less than d, then $g \in S_{<d}$, so g is in the $R[x]$-ideal generated by $h_1, \dots, h_m$. Next suppose that g has degree $e \geq d$. Then the leading coefficient b of g lies in the ideal A of leading coefficients of g, so there exist $r_i \in R$ such that $b = r_1 a_1 + \cdots + r_n a_n$. Since f_i has leading coefficient a_i, the difference $g - x^{e-d} r_i f_i$ has degree less than the degree e of g. By induction $g - x^{e-d} r_i f_i$ is an $R[x]$ linear combination of $f_1, \dots, f_n, h_1, \dots h_m$, so g is also an $R[x]$ linear combination of $f_1, \dots, f_n, h_1, \dots h_m$. Since each f_i and h_j lies in I, it follows that I is generated by $f_1, \dots, f_n, h_1, \dots h_m$, so I is finitely generated, as required. $\square$

Properties of Noetherian rings and modules will be crucial in the rest of this course. We have proved above that Noetherian rings have many desirable properties.

1.1 Z is Noetherian

The ring $\mathbf{Z}$ of integers is Noetherian because every ideal of $\mathbf{Z}$ is generated by one element.

Proposition 1.9. *Every ideal of the ring* $\mathbf{Z}$ *of integers is principal.*

Proof. Suppose I is a nonzero ideal in $\mathbf{Z}$. Let d the least positive element of I. Suppose that $a \in I$ is any nonzero element of I. Using the division algorithm, write $a = dq + r$, where q is an integer and $0 \leq r < d$. We have $r = a - dq \in I$ and $r < d$, so our assumption that d is minimal implies that $r = 0$, so $a = dq$ is in the ideal generated by d. Thus I is the principal ideal generated by d. $\square$

Proposition 1.6 and 1.9 together imply that any finitely generated abelian group is Noetherian. This means that subgroups of finitely generated abelian groups are finitely generated, which provides the missing step in our proof of the structure theorem for finitely generated abelian groups.

2 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 2.1 (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 2.2 (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 2.3. *If α is an algebraic integer, then the minimal polynomial of α has coefficients in $\mathbf{Z}$.*

Proof. (From S-D, page 2.) 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 any denominator of f, and likewise let p^j be the largest power of p that divides any denominator 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 2.4. *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 2.3). 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 2.5. *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 2.6 (Ring of Integers). The *ring of integers* of a number field K is the ring

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

Example 2.7. 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 $\mathcal{O}_K = \mathbf{Z}[(1+\sqrt{5})/2]$. According to MAGMA, the ring of integers of $K = \mathbf{Q}(\sqrt[3]{9})$ is $\mathbf{Z}[\sqrt[3]{3}]$, where $\sqrt[3]{3} = \frac{1}{3}(\sqrt[3]{9})^2$.

Lemma 2.8. *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. If $\alpha \in \mathcal{O}_K \cap \mathbf{Q}$, write $\alpha = a/b$ in lowest terms. Since a/b is integral, by Proposition 2.4, the ring $\mathbf{Z}[a/b]$ is finitely generated as a $\mathbf{Z}$-module. If $b \neq 0$, then $G = \mathbf{Z}[a/b]$ is not even finitely generated as an abelian group, since G is torsion free and $G/bG = 0$. Thus $\mathcal{O}_K \cap \mathbf{Q} = \mathbf{Z}$.

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 $\mathbf{Q}\mathcal{O}_K = K$. $\square$

Next time we will prove the following proposition:

Proposition 2.9. *The ring of integers $\mathcal{O}_K$ of a number field is Noetherian.*

We will also develop some basic properties of norms, traces, and discriminants, and give more properties of rings of integers in the general context of Dedekind domains.