AN OVERVIEW OF RINGS AND MODULES

FELIX GOTTI

Preliminary on Rings

Here we assume the reader has had at least a brief exposure to the notions of a group, a ring, and their corresponding substructures and homomorphisms. In what follows, $\mathbb{P}$, $\mathbb{N}$, and $\mathbb{N}_0$ denote the sets of primes, positive integers, and nonnegative integers, respectively. In addition, we set $[\![a, b]\!] := \{n \in \mathbb{Z} : a \le n \le b\}$ for all $a, b \in \mathbb{Z}$.

Ideals and Quotient Rings. Let R be a commutative ring with identity element 1. An additive subgroup I of R is called an *ideal* if $ra \in I$ for all $r \in R$ and $a \in I$. Let I be an ideal. The quotient group R/I is a ring under the operation $(r+I)(s+I) := rs+I$, which is called the *quotient ring* of R by I. It is clear that R/I is a commutative ring with identity element $1 + I$. The group homomorphism $\pi \colon R \to R/I$ is indeed a ring homomorphism. If $f \colon R \to S$ is a ring homomorphsim, then $\ker f = \{r \in R : f(r) = 0\}$ is an ideal of R, the set $f(R)$ is a subring of S, and the assignment $r + \ker f \mapsto f(r)$ determines a ring isomorphism $R/\ker f \cong f(R)$. On the other hand, if $I \subseteq \ker f$, then f factors through π, that is, there exists a unique ring homomorphism $\varphi \colon R/I \to S$ such that $f = \varphi \circ \pi$.

The intersection of ideals of R is again an ideal. We can also add, multiply, and take quotients of ideals. Let I and J be ideals of R. The set

$$I + J := \{a + b : a \in I \text{ and } b \in J\}$$

is an ideal of R, which is called the *sum* of I and J. The sum of finitely many ideals is defined similarly. If $I = Ra$ for some $a \in R$, then I is called *principal*, in which case, we also write $I = (a)$. More generally, if $I = Ra_1 + \cdots + Ra_n$ for some $a_1, \dots, a_n \in R$, then I is called *finitely generated*. The set

$$IJ := \bigg\{ \sum_{i=1}^{n} a_i b_i : n \in \mathbb{N},\ a_i \in I, \text{ and } b_i \in J \bigg\}$$

is an ideal of R, which is called the *product* of I and J. We can naturally extend this to the *product* of finitely many ideals and, accordingly, we let I^n denote the product of n copies of I and call it the *n-th power* of I. It is clear that $IJ \subseteq I \cap J$. Finally,

$$(J : I) := \big\{ r \in R : rI \subseteq J \big\}$$

is also an ideal of R, and it is often called the *colon* or the *quotient* ideal of J by I. The verification that $I \cap J$, $I + J$, IJ, and $(J : I)$ are ideals of R is routine, and we leave this task to the reader.

If I is an ideal of R and S is a subring of R, then $I + S$ is a subring of R and $I \cap S$ is an ideal of S. In addition, it is not hard to verify that the assignment $s \mapsto s + I$ determines a surjective ring homomorphism $S \to (I + S)/I$ with kernel $I \cap S$ (this is often called the Second Isomorphism Theorem). On the other hand, if J is an ideal of R with $I \subseteq J$, then the assignment $r + I \mapsto r + J$ determines a surjective ring homomorphism $R/I \to R/J$ with kernel J/I (this is often called the Third Isomorphism Theorem). Finally, the assignment $T \mapsto T/I$ for any subring (resp., ideal) T of R induces an inclusion-preserving bijection from the set of all subrings (resp., ideals) of R containing I to the set of all subrings (resp., ideals) of R/I.

A proper ideal P of R is *prime* if whenever $IJ \subseteq P$ for ideals I and J in R, either $I \subseteq P$ or $J \subseteq P$. In addition, a proper ideal M of R is *maximal* if for any ideal I with $M \subseteq I \subseteq R$, either $I = M$ or $I = R$.

Proposition 1. *Let R be a commutative ring with identity, and let I be an ideal of R. Then the following statements hold.*

(1) *I is prime if and only if R/I is an integral domain.*
(2) *I is maximal if and only if R/I is a field.*

Proof. (1) Since $r \in I$ if and only if $r + I = I$ for all $r \in R$, this part follows immediately from the fact that $rs \in I$ if and only if $(r + I)(s + I) = I$ for all $r, s \in R$.

(2) It is clear that a commutative ring with identity is a field if and only if it has precisely two ideals (the trivial ideals). Thus, this part is a direct consequence from the fact that the assignment $J \mapsto J/I$ induces a bijection from the set of ideals of R containing I to the set of ideals of R/I. □

Corollary 2. *Every maximal ideal is prime.*

Not every prime ideal, however, is maximal. For instance, in the ring $\mathbb{Z}[x]$ the ideal (x) is prime, but it is not maximal because (x) is strictly contained in the ideal $(x, 2)$, which is a proper ideal of $\mathbb{Z}[x]$.

UFDs, PIDs, and Euclidean Domains. For a commutative ring R with identity, we let $R^\times$ denote its group of units (i.e., invertible elements) of R. Let R be an integral domain, that is, a commutative ring with identity with no nonzero zero-divisors. For $r, s \in R$, we say that s *divides* r and write $s \mid_R r$ if $r = st$ for some $t \in R$. Elements $r, s \in R$ are *associates* if $s = ur$ for some $u \in R^\times$. A nonzero element $r \in R \setminus R^\times$ is *prime* if whenever $r \mid_R st$ for some $s, t \in R$ either $r \mid_R s$ or $r \mid_R t$, and we say that r is *irreducible* if whenever $r = uv$ for some $u, v \in R$ either $u \in R^\times$ or $v \in R^\times$. It is not hard to verify that every prime is irreducible (prove this!).

Definition 3. An integral domain is a *unique factorization domain (UFD)* if for every nonzero $r \in R \setminus R^\times$, the following statements hold:

(1) $r = p_1 \cdots p_m$ for some irreducibles $p_1, \dots, p_m \in R$, and
(2) if $r = q_1 \cdots q_n$ for irreducibles $q_1, \dots, q_n \in R$, then $n = m$ and there is a bijection $\varphi \colon [\![1, m]\!] \to [\![1, m]\!]$ such that $q_{\varphi(j)}$ and p_j are associates for every $j \in [\![1, m]\!]$.

Every field is trivially a UFD, and $\mathbb{Z}$ is a UFD by the Fundamental Theorem of Arithmetic. We will prove in the next subsection that the rings of polynomials $\mathbb{Z}[x]$ and $\mathbb{Z}[x, y]$ are UFDs.

Proposition 4. *Let R be a UFD. An element of R is prime if and only if it is irreducible.*

Proof. In every integral domain, primes are irreducibles, and we leave the verification of this fact to the reader. Now suppose that $p \in R$ is an irreducible. To check that p is prime, take $r, s \in R$ such that $p \mid_R rs$, and then write $pt = rs$ for some $t \in R$. As R is a UFD, we can factor t, r, and s into irreducibles to obtain factorizations of the same element in both sides of the equality $pt = rs$. Since p is irreducible and R is a UFD, p is associate with one of the irreducibles in the factorization of rs, and so either $p \mid_R r$ or $p \mid_R s$. Hence p is prime. □

Integral domains whose ideals are principal play an important role in commutative ring theory.

Definition 5. An integral domain R is called a *principal ideal domain (PID)* if every ideal of R is principal.

Every field is clearly a PID. It is not hard to verify that $\mathbb{Z}$ is a PID, although it follows from Theorem 11 below. We will prove in the next theorem that every PID is a UFD. First, we need to collect the following temporary result (once we prove Theorem 7, this lemma will become a special case of Proposition 4).

Lemma 6. *If R is a PID, then every irreducible in R must be prime.*

Proof. Let p be an irreducible in R, and let I be an ideal containing Rp. Since R is a PID, $I = Ra$ for some $a \in R$. After writing $p = ab$ for some $b \in R$, we see that either $a \in R^\times$ or $b \in R^\times$. Accordingly, we find that $I = R$ or $I = Rp$. Hence the only ideal properly containing Rp is R, which means that Rp is a maximal ideal and, therefore, a prime ideal. Hence p is prime. □

Theorem 7. *Every PID is a UFD.*

Proof. Let R be a PID. Suppose, by way of contradiction, that there is a nonzero element $r_0 \in R \setminus R^\times$ that does not factor into irreducibles. So $r_0 = r_1 s_1$ for some $r_1, s_1 \in R \setminus R^\times$ such that r_1 does not factor into irreducibles. As before, we can write $r_1 = r_2 s_2$ for some $r_2, s_2 \in R \setminus R^\times$ such that r_2 does not factor into irreducibles.

Going on in a similar fashion, we can construct sequences $(r_n)_{n\in\mathbb{N}_0}$ and $(s_n)_{n\in\mathbb{N}}$ with $r_n, s_n \in R \setminus R^\times$ such that $r_n = r_{n+1}s_{n+1}$. Thus, the sequence $(Rr_n)_{n\in\mathbb{N}_0}$ of ideals satisfies that $Rr_n \subsetneq Rr_{n+1}$ and, therefore, $I = \bigcup_{n\in\mathbb{N}_0} Rr_n$ is an ideal. Since R is a PID, there is an $a \in R$ such that $I = Ra$. Take an $m \in \mathbb{N}$ such that $a \in Rr_m$. This implies that $I = R_m$, and so $Rr_{m+1} = Rr_m$. In this case, r_m and r_{m+1} are associates, which contradicts that Rr_{n+1} strictly contains Rr_n. Hence every nonzero element of $R \setminus R^\times$ is a product of irreducibles.

Let us prove now that every nonzero element in $R \setminus R^\times$ has a unique factorization up to permutation and associate. To do so we use induction on the number of irreducible factors (counting repetitions). If a nonzero r in $R \setminus R^\times$ has a factorization consisting of only one irreducible, then r itself must be irreducible and $r = q_1 \cdots q_n$ for irreducibles $q_1, \dots, q_n$ immediately implies that $n = 1$ and $q_1 = r$. So assume that there is an $m \in \mathbb{N}$ such that every nonzero in $R \setminus R^\times$ having a factorization with at most m irreducibles (counting repetitions) must have a unique factorization. Take $r \in R \setminus R^\times$ such that $r = p_1 \cdots p_{m+1}$ for irreducibles $p_1, \dots, p_{m+1}$ in R. Suppose that $r = q_1 \cdots q_n$ for irreducibles $q_1, \dots, q_n$. Since p_{m+1} is prime by Lemma 6, one of the irreducibles $q_1, \dots, q_n$ is divisible by p_{m+1}. After relabeling $q_1, \dots, q_n$, one can assume that $p_{m+1} \mid_R q_n$ and so that p_{m+1} and q_n are associates. Take $u \in R^\times$ such that $q_n = up_{m+1}$. Then $p_1 \cdots p_m = (uq_1)q_2 \cdots q_{n-1}$. By induction hypothesis, $n - 1 = m$ and we can relabel $q_1, \dots, q_m$ such that p_i and q_i are associates for every $i \in [\![1, m]\!]$. Hence R is a UFD. $\square$

The converse of Theorem 7 does not hold.

Example 8. Consider the ring $\mathbb{Z}[x]$. We will show in the next section that $R[x]$ is a UFD provided that R is a UFD. Therefore $\mathbb{Z}[x]$ is a UFD. On the other hand, one can easily verify that the ideal $(2, x)$ is not principal (check this!). Hence $\mathbb{Z}[x]$ is not a PID.

The Euclidean division algorithm is an important tool we have at our disposal in $\mathbb{Z}$. We can consider generalizations of the ring $\mathbb{Z}$ where still we can perform the Euclidean division algorithm. Such rings are called Euclidean domains.

Definition 9. An integral domain R is called a *Euclidean domain* if there is a map $N\colon R \to \mathbb{N}_0$ with $N(0) = 0$, called a *norm*, such that for any elements $a, b \in R$ with $b \neq 0$, there are elements $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $N(r) < N(b)$.

Every field F is a Euclidean domain under the norm $N(\alpha) = 0$ for every $\alpha \in F$ (indeed, any norm can be taken). In addition, $\mathbb{Z}$ is a Euclidean domain under the norm $N(m) = |m|$. The ring $\mathbb{Z}[i] := \{a + ib : a, b \in \mathbb{Z}\}$ of *Gaussian integers* is also a Euclidean domain under the norm $N(a + ib) = a^2 + b^2$.

Example 10. Let us argue that the ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain. Consider $N\colon \mathbb{Z}[i] \to \mathbb{N}_0$ defined by $N(a + ib) = a^2 + b^2$. As $N(\alpha) = \alpha\bar{\alpha}$, it is clear that $N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2)$. Take $\alpha, \beta \in \mathbb{Z}[i]$ such that $\beta \neq 0$, and write

$\alpha/\beta = q_1 + iq_2$, where $q_1, q_2 \in \mathbb{Q}$. Now take $m, n \in \mathbb{Z}$ such that $|q_1 - m| \le 1/2$ and $|q_2 - n| \le 1/2$, and then set $q = m + in \in \mathbb{Z}[i]$ and $r = \alpha - q\beta \in \mathbb{Z}[i]$. Since

$$N(r) = N(\beta)N\Big(\frac{\alpha}{\beta} - q\Big) = N(\beta)\big(|q_1 - m|^2 + |q_2 - n|^2\big) \le \frac{N(\beta)}{2} < N(\beta),$$

we obtain that $\mathbb{Z}[i]$ is a Euclidean domain.

We proceed to show that every Euclidean domain is a PID.

Theorem 11. *Every Euclidean domain is a PID.*

Proof. Let R be a Euclidean domain with norm $N \colon R \to \mathbb{N}_0$. Take a nonzero ideal I of R. Let b be a nonzero element of I having minimum norm. We claim that $I = Rb$. Clearly, $Rb \subseteq I$. For the reverse inclusion, consider $a \in I$. Since R is a Euclidean domain, $a = qb + r$ for some $q, r \in R$, where either $r = 0$ or $N(r) < N(b)$. Since $r = a - qb \in I$, the minimality of $N(b)$ ensures that $r = 0$, and so $a = qb \in I$. As a result, the inclusion $I \subseteq Rb$ holds and, therefore, I is principal. Hence R is a PID. $\square$

We conclude this subsection emphasizing that not every PID is a Euclidean domain. However, examples witnessing this are not that easy to construct. One of the most tractable examples is $\mathbb{Z}[\omega]$, where $\omega := (1 + i\sqrt{19})/2$. The fact that $\mathbb{Z}[\omega]$ is a PID that is not a Euclidean domain is discussed in [1, Subsections 8.1 and 8.2].

Polynomial Rings and Irreducibility. Polynomial rings over fields are also examples of Euclidean domains.

Proposition 12. *If F is a field, then $F[x]$ is a Euclidean domain.*

Proof. Exercise (Hint: Use induction.). $\square$

The following criterion is quite useful to argue the irreducibility of a polynomial.

Theorem 13 (Gauss's lemma)**.** *Let R be a UFD, and let $p(x)$ be a polynomial in $R[x]$. If $p(x) = a(x)b(x)$ for some $a(x), b(x) \in \mathrm{qf}(R)[x]$, then there exists $c \in \mathrm{qf}(R)^\times$ such that $ca(x) \in R[x]$ and $c^{-1}b(x) \in R[x]$.*

Proof. Assume that $p(x) = a(x)b(x)$ for some $a(x), b(x) \in \mathrm{qf}(R)[x]$. If $a(x), b(x) \in R[x]$, then we can take $c = 1$. We will assume, therefore, that this is not the case, and write $dp(x) = a'(x)b'(x)$ for some $d \in R \setminus R^\times$ and $a'(x), b'(x) \in R[x]$. Since R is a UFD, we can take irreducibles $p_1, \dots, p_n$ such that $d = p_1 \cdots p_n$. Set $J = p_nR[x]$ and observe that $R[x]/J \cong (R/Rp_n)[x]$ is an integral domain, and so J is a prime ideal of $R[x]$. Since $(a'(x) + J)(b'(x) + J) = dp(x) + J = J$, the fact that $R[x]/J$ is an integral domain implies that either $a'(x) \in J$ or $b'(x) \in J$. Assuming the former, we obtain that $a'(x)/p_n \in R[x]$ and so the equality $(d/p_n)p(x) = (a'(x)/p_n)b'(x)$ takes place in $R[x]$. One can proceed similarly with the rest of the irreducibles $p_1, \dots, p_{n-1}$ in the factorization of d to find $d_1, d_2 \in R$ with $d_1d_2 = d$ such that both $a'(x)/d_1$ and $b'(x)/d_2$ belong to $R[x]$. Now we just need to take $c = d_1^{-1}a'(x)/a(x)$. $\square$

Corollary 14. *Let R be a UFD, and let $p(x)$ be a nonzero polynomial in $R[x]$ such that 1 is a greatest common divisor of the coefficients of $p(x)$. Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in* $\mathrm{qf}(R)[x]$.

We are in a position now to prove the following promised result.

Theorem 15. *If R is a UFD, then $R[x]$ is a UFD.*

Proof. Let R be a UFD, and take a nonzero polynomial $p(x) \in R[x]$. It is not hard to see that the irreducibles of R are still irreducibles in $R[x]$. Therefore if $p(x) \in R$, then $p(x)$ factors uniquely into irreducibles. Accordingly, assume that $p(x)$ is a non-constant polynomial. In addition, if d is a greatest common divisor of the coefficients of $p(x)$ and $p'(x) := p(x)/d$, then $p(x) = dp'(x)$ factors uniquely into irreducibles in $R[x]$ provided that $p'(x)$ factors into irreducibles in $R[x]$. So we can further assume that 1 is a greatest common divisor of the coefficients of $p(x)$. As $\mathrm{qf}(R)[x]$ is a Euclidean domain and so a UFD, $p(x) = p'_1(x) \dots p'_m(x)$ for unique irreducibles $p'_1(x), \dots, p'_m(x)$ in $\mathrm{qf}(R)[x]$. It follows now by Gauss's lemma that $p(x) = p_1(x) \dots p_m(x)$, where the polynomials $p_1(x), \dots, p_m(x) \in R[x]$ are F-multiples of $p'_1(x), \dots, p'_m(x)$, respectively. Since 1 is a greatest common divisor of the coefficients of $p(x)$, the same holds for $p_1(x), \dots, p_m(x)$. So it follows from Corollary 14 that $p_1(x), \dots, p_m(x)$ are irreducibles.

In order to argue the uniqueness, suppose that $p(x) = q_1(x) \dots q_n(x)$ for irreducibles polynomials $q_1(x), \dots, q_n(x)$ in $R[x]$. Since 1 is a greatest common divisor of the coefficients of $p(x)$, the same holds for $q_1(x), \dots, q_n(x)$. In particular, $q_1(x), \dots, q_n(x)$ are non-constant, and it follows from Corollary 14 that they are irreducibles in $\mathrm{qf}(R)[x]$. Since $\mathrm{qf}(R)[x]$ is a UFD, $n = m$ and, after relabeling the indices of $q_1(x), \dots, q_m(x)$, we obtain that $a_i p_i(x) = b_i q_i(x)$, where $a_i, b_i \in R$, for every $i \in [\![1, m]\!]$. Fix $i \in [\![1, m]\!]$. Since 1 is a greatest common divisor of the coefficients of $q_i(x)$, every prime in a factorization of a_i in R, which is also a prime in $R[x]$, must divide b_i, and so a_i divides b_i in R. Similarly, b_i divides a_i in R, and so $b_i = ua_i$ for some $u \in R^\times$. This implies that $p_i(x)$ and $q_i(x)$ are associates in $R[x]$. Hence the uniqueness follows, and so $R[x]$ is a UFD. ∎

When used in tandem, Corollary 14 and Proposition 16 (known as Eisenstein's criterion) are practical tools to argue that certain polynomials are irreducibles.

Proposition 16. *Let R be an integral domain, and let $p(x) = a_n x^n + \dots + a_1 x + a_0$ be a polynomial in $R[x]$. If there exists a prime ideal P of R such that*

(1) $a_n \notin P$,

(2) $a_0, \dots, a_{n-1} \in P$, *and*

(3) $a_0 \notin P^2$,

then $p(x)$ cannot be written in $R[x]$ as a product of two non-constant polynomials. In addition, if 1 is a greatest common divisor of the coefficients of $p(x)$, then $p(x)$ is irreducible.

Proof. Suppose, by way of contradiction, that $p(x) = a(x)b(x)$ for non-constant polynomials $a(x), b(x) \in R[x]$. Then $a'(x)b'(x) = (a_n+P)x^n$ in $(R/P)[x]$, where $a'(x)$ and $b'(x)$ are the images of $a(x)$ and $b(x)$ under the canonical homomorphism $R[x] \to (R/P)[x]$. Since $(R/P)[x]$ is an integral domain and $(a_n+P)x^n$ is nonzero in $(R/P)[x]$, both $a'(x)$ and $b'(x)$ are nonzero. This, together with the fact that $(a_n + P)x^n$ is a monomial, ensures that the constant coefficients of both $a'(x)$ and $b'(x)$ equal P in $(R/P)[x]$, that is, $a(0) \in P$ and $b(0) \in P$. However, this contradicts that $a_0 \notin P^2$. $\square$

We conclude with an application of Eisenstein's criterion.

Example 17. For each $p \in \mathbb{P}$, we will argue that the polynomial $f(x) = x^{p-1}+\cdots+x+1$ is irreducible in $\mathbb{Q}[x]$. Since $f(x)$ is monic, in light of Corollary 14 it suffices to show that $f(x)$ is irreducible in $\mathbb{Z}[x]$. Observe that $f(x)$ is irreducible if and only if $f(x+1)$ is irreducible. Since $x^p - 1 = (x-1)f(x)$, we see that

$$f(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}. \tag{0.1}$$

From the summation in (0.1), it is clear that $f(x+1)$ is a monic polynomial having all its non-leading coefficients divisible by p. In addition, the constant coefficient of $f(x+1)$ is p, which is not divisible by p^2. So by virtue of Eisenstein's criterion, $f(x+1)$ is irreducible, as desired. Moreover, for every $n \geq 2$, it is easy to verify that the polynomial $x^{n-1} + \cdots + x + 1$ is irreducible if and only if n is prime.

Noetherian Rings. In this subsection, we introduce one of the most relevant classes of rings in commutative algebra, Noetherian rings.

Definition 18. A commutative ring R with identity is *Noetherian* if every ascending chain of ideals of R eventually stabilizes, that is, for every sequence $(I_n)_{n\in\mathbb{N}}$ of ideals of R with $I_n \subseteq I_{n+1}$ for every $n \in \mathbb{N}$, there exists $N \in \mathbb{N}$ such that $I_n = I_N$ for every $n \geq N$.

The term "Noetherian" honors Emmy Noether, who first investigated chain conditions on commutative rings in her celebrated paper [3]. We can characterize Noetherian rings as follows.

Proposition 19. *For a commutative ring R, the following statements are equivalent.*

(a) *R is Noetherian.*
(b) *Every nonempty set of ideals of R contains a maximal element (under inclusion).*
(c) *Every ideal of R is finitely generated; that is, if I is an ideal of R, then there exist $a_1, \ldots, a_n \in R$ such that $I = Ra_1 + \cdots + Ra_n$.*

Proof. (a) $\Rightarrow$ (b): Assume, by way of contradiction, that there is a nonempty set $\mathscr{S}$ consisting of ideals of R that does not contain a maximal member. Take $I_1 \in \mathscr{S}$. Since I_1 is not a maximal member in $\mathscr{S}$, we can take $I_2 \in \mathscr{S}$ such that $I_1 \subsetneq I_2$. Since I_2 is not a maximal member of $\mathscr{S}$, we can take $I_3 \in \mathscr{S}$ such that $I_2 \subsetneq I_3$. Continuing in this matter we can produce an ascending chain $(I_n)_{n \in \mathbb{N}}$ that does not stabilize, which contradicts that R is Noetherian.

(b) $\Rightarrow$ (c): Let I be an ideal of R, and let $\mathscr{F}$ be the set of finitely generated ideals of R contained in I. Observe that $\mathscr{F}$ is not empty because it contains the zero ideal. Therefore $\mathscr{F}$ contains a maximal member M by assumption. We can see now that $I = M$ as, otherwise, for any $x \in I \setminus M$ the existence of the finitely generated ideal $M + xR$ would contradict the maximality of M. Hence I is finitely generated.

(c) $\Rightarrow$ (a): Let $(I_n)_{n \in \mathbb{N}}$ be an ascending chain of ideals of R. Then $I := \bigcup_{n \in \mathbb{N}} I_n$ is also an ideal of R, and since R is Noetherian we can write $I = Ra_1 + \dots + Ra_n$ for some $a_1, \dots, a_n \in I$. After taking $N \in \mathbb{N}$ such that $a_1, \dots, a_n \in I_N$, we see that $I \subseteq I_N$ and so that $I_N = I$. This clearly implies that $I_n = I$ for every $n \geq N$, and so $(I_n)_{n \in \mathbb{N}}$ eventually stabilizes. Hence R is Noetherian. $\square$

Example 20. PIDs and, in particular, Euclidean domains are Noetherian rings. In addition, the rings of integers of algebraic number fields are Noetherian, even though many of them are not PIDs. On the other hand, not every UFD is Noetherian; for instance, $\mathbb{Z}[x_1, x_2, \dots]$ is a UFD but its prime ideal $(x_1, x_2, \dots)$ is not finitely generated.

It is not hard to verify that quotients and, therefore, homomorphic images of Noetherian rings are Noetherian rings.

Proposition 21. *Let R be a Noetherian ring. Then R/I is also a Noetherian ring for every ideal I of R.*

Proof. Every ideal of R/I has the form J/I, where J is an ideal of R containing I. Fix an ideal J/I of R/I. Since R is Noetherian, we can take $r_1, \dots, r_n \in R$ such that $J = (r_1, \dots, r_n)$. Hence $J/I = (r_1 + I, \dots, r_n + I)$, and so it is a finitely generated ideal. Thus, R/I is also Noetherian. $\square$

A crucial tool to produce Noetherian rings is Hilbert Basis Theorem, which was established by D. Hilbert [2] back in 1890.

Theorem 22 (Hilbert Basis Theorem)**.** *If R is a Noetherian ring, then $R[x]$ is also a Noetherian ring.*

Proof. For a nonzero $f \in R[x]$, we let $LC(f)$ denote the leading coefficient of f. Let J be an ideal of $R[x]$. For each $n \in \mathbb{N}_0$, consider the set

$$I_n := \{0\} \cup \{LC(f) : f \in J \setminus \{0\} \text{ and } \deg f = n\}.$$

Using that J is an ideal of $R[x]$, we can easily verify that I_n is an ideal of R for every $n \in \mathbb{N}_0$. In addition, observe that $(I_n)_{n \in \mathbb{N}_0}$ is an ascending chain of ideals of R; indeed, it follows from the fact that $xf \in I_{n+1}$ when $f \in I_n$. As R is a Noetherian ring, I_n is generated by a finite set L_n for every $n \in \mathbb{N}_0$ and there is an $m \in \mathbb{N}$ such that $I_n = I_m$ for every $n \geq m$. For each $n \in \mathbb{N}_0$ and $c \in L_n$, there exists $g_c \in J$ with $\deg g_c = n$ such that $LC(g_c) = c$. Consider the subset $L := \{g_c : c \in \bigcup_{n=1}^m L_n\}$ of J, and let us argue that J can be generated by L.

Let J_ℓ be the ideal generated by L. As $L \subseteq J$, it follows that $J_\ell \subseteq J$. For the reverse implication, we will argue that every nonzero polynomial f in J belongs to J_ℓ by induction on the degree of f. If $\deg f = 0$, then $f = LC(f) \in I_0 \subseteq J_\ell$. Now assume that $\deg f \geq 1$ and write $f = c_n x^n + \cdots + c_1 x + c_0$ for some $c_0, \dots, c_n \in R$ with $c_n \neq 0$, in which case, $c_n \in I_n$. We consider the following two cases.

Case 1: $n \leq m$. Write $c_n = \sum_{i=1}^k r_i \ell_i$ for some $r_1, \dots, r_k \in R$ and $\ell_1, \dots, \ell_k \in L_n$. Since $n \leq m$, the polynomial $g := \sum_{i=1}^k r_i g_{\ell_i}$ belongs to J_ℓ and has degree at most n. Indeed, $\deg g = n$ because the coefficient of x^n in g is c_n. As $J_\ell \subseteq J$, the polynomial $f - g$ belongs to J and, in addition, it has degree strictly less than n. Hence $f - g \in J_\ell$ by the induction hypothesis, and so f must belong J_ℓ.

Case 2: $n > m$. In this case, $c_n \in I_n = I_m$, and we can write $c_n = \sum_{i=1}^k r_i \ell_i$ for some $r_1, \dots, r_k \in R$ and $\ell_1, \dots, \ell_k \in L_m$. Consider the polynomial $g := \sum_{i=1}^k r_i g_{\ell_i}$, and note that it belongs to J_ℓ and it has degree at most m. Also, the coefficient of x^m in g is c_n. Therefore $x^{n-m} g$ is a polynomial of J_ℓ of degree at most n, which ensures that $\deg x^{n-m} g = n$ because the coefficient of x^n in $x^{n-m} g$ is c_n. This implies that $f - x^{n-m} g$ is a polynomial in J of degree less than n, and then it follows by the induction hypothesis that $f - x^{n-m} g \in J_\ell$. Hence f must belong to J_ℓ.

As a result, $J \subseteq J_\ell$, and so J is finitely generated. Thus, we can conclude that $R[x]$ is a Noetherian ring. □

The following corollary is an immediate consequence of Hilbert Basis Theorem.

Corollary 23. *If R is a Noetherian ring, then $R[x_1, \dots, x_n]$ is a Noetherian ring.*

Preliminary on Modules

Definitions and Examples. Modules over commutative rings are generalizations of vector spaces that play a fundamental role in commutative algebra and, in particular, in ideal theory. For the rest of this section, let R be a commutative ring with identity.

Definition 24. An additive abelian group M is a *module* over R (or an *R-module*) if there is an action of R on M, that is a map $R \times M \to M$ given by $(r, m) \mapsto rm$, satisfying the following properties:

(1) $r(m_1 + m_2) = rm_1 + rm_2$ for all $r \in R$ and $m_1, m_2 \in M$,
(2) $(r_1 + r_2)m = r_1 m + r_2 m$ for all $r_1, r_2 \in R$ and $m \in M$,

(3) $(r_1r_2)m = r_1(r_2m)$ for all $r_1, r_2 \in R$ and $m \in M$, and
(4) $1m = m$ for all $m \in M$.

It is clear from the above definition that vector spaces are precisely modules over fields. On the other hand, it is not hard to see that there is a canonical action of $\mathbb{Z}$ over any abelian group A turning A into a $\mathbb{Z}$-module, namely, $na := a + \cdots + a$ (the addition of n copies of a) and $(-n)a := -na$ for all $n \in \mathbb{N}_0$ and $a \in A$. Also, for $n \in \mathbb{N}$, it is easy to verify that the additive abelian group R^n is an R-module over R under the action $r(a_1, \dots, a_n) := (ra_1, \dots, ra_n)$. Under this action, R^n is called the *free module of rank* n over R.

Let M be an R-module. A subgroup N of M is called an *R-submodule* of M if it is is closed under the action of R, that is, $rn \in N$ for all $r \in R$ and $n \in N$. One can readily prove that N is a submodule of M if and only if N is nonempty and $x + ry \in N$ for all $r \in R$ and $x, y \in N$. Every commutative ring R is an R-module over itself, and every ideal I of R is clearly an R-submodule. If N is an R-submodule of M, then the quotient group M/N is an R-module under the action $r(m + N) := rm + N$.

For R-modules M_1 and M_2, a map $\varphi\colon M_1 \to M_2$ is called an *R-module homomorphism* if φ is a group homomorphism satisfying that $\varphi(rm) = r\varphi(m)$ for all $r \in R$ and $m \in M$. In this case, $\ker \varphi$ is an R-submodule of M_1, and it follows that φ is injective if and only if $\ker \varphi = \{0\}$. When φ is bijective, it is called an *isomorphism* of R-modules. The canonical group isomorphism $M_1/\ker \varphi \cong \varphi(M_1)$ (from the First Isomorphism Theorem) is, indeed, an isomorphism of R-modules. If N_1 and N_2 are two R-submodules of M, then the subgroups $N_1 + N_2$ and $N_1 \cap N_2$ are R-submodules, and the canonical group isomorphism $(N_1 + N_2)/N_1 \cong N_2/(N_1 \cap N_2)$ is also an isomorphism of R-modules.

Finitely Generated Modules and Noetherian Modules. The R-module M is *finitely generated* if there exist $m_1, \dots, m_n \in M$ such that $M = Rm_1 + \cdots + Rm_n$. Clearly, every commutative ring R with identity is a finitely generated R-module over itself (generated by 1). In addition, quotient and so homomorphic images of finitely generated R-modules are finitely generated.

Proposition 25. *If N is an R-submodule of a finitely generated R-module M, then the quotient M/N is also a finitely generated R-module.*

Proof. See the proof of Proposition 21. □

Being finitely generated is transitive in the following sense.

Proposition 26. *Let R, S, and T be commutative rings with identities. If S is a finitely generated R-module and T is a finitely generated S-module, then T is a finitely generated R-module.*

Proof. Since S is a finitely generated R-module, we can take $s_1, \dots, s_m \in S$ such that $S = \sum_{i=1}^m Rs_i$. In addition, since T is a finitely generated S-module, we can take $t_1, \dots, t_n \in T$ such that $T = \sum_{j=1}^n St_j$. Thus, $T = \sum_{j=1}^n \big(\sum_{i=1}^m Rs_i \big) t_j = \sum_{i=1}^m \sum_{j=1}^n Rs_i t_j$, whence T is a finitely generated R-module. □

An R-module M is called *Noetherian* if every R-submodule of M is finitely generated. Not every finitely generated R-module is Noetherian. For instance, although the ring $R := \mathbb{Z}[x_n : n \in \mathbb{N}]$ in countably many variables over $\mathbb{Z}$ is a finitely generated R-module, its ideal $(x_1, x_2, \dots)$ is an R-submodule that is not finitely generated.

Example 27. Let V be a finite-dimensional vector space over a field F. Then every F-submodule of V is a vector space of dimension at most $\dim V$ and, therefore, is finitely generated. As a result, V is a Noetherian F-module.

As in the case of commutative rings, one can characterize Noetherian modules as follows.

Proposition 28. *For an R-module M, the following statements are equivalent.*

(a) *M is Noetherian.*
(b) *M satisfies the ascending chain condition (ACC) on submodules: every ascending chain of R-submodules of M eventually stabilizes.*
(c) *Every nonempty set of R-submodules of M contains a maximal element (under inclusion).*

Proof. Exercise. □

As for commutative rings, quotients of Noetherian modules are Noetherian. Moreover, we have the following result.

Proposition 29. *Let M be an R-module, and let N be a submodule of M. Then M is Noetherian if and only if both N and M/N are Noetherian.*

Proof. Suppose first that M is Noetherian. Clearly, every R-submodule of N is also an R-submodule of M and, therefore, is finitely generated. Hence N is Noetherian. To verify that M/N is Noetherian, take an R-submodule S/N of M/N, where S is an R-submodule of M. Since M is Noetherian $S = Rs_1 + \dots + Rs_k$ for some $s_1, \dots, s_k \in S$. Hence it immediately follows that $S/N = R(s_1 + N) + \dots + R(s_k + N)$, and so S/N is finitely generated. Thus, R/N is also Noetherian.

Conversely, suppose that both N and M/N are Noetherian R-modules. Let S be an R-submodule of M, and let S' be the R-submodule $(S+N)/N$ of M/N. Since both N and M/N is Noetherian, $S \cap N = Rm_1 + \dots + Rm_k$ and $S' = R(m'_1 + N) + \dots + R(m'_\ell + N)$ for some $m_1, \dots, m_k \in S \cap N$ and $m'_1, \dots, m'_\ell \in S + N$. Indeed, we can assume that $m'_1, \dots, m'_\ell \in S$. Now take $s \in S$ and write $s + N = r'_1(m'_1 + N) + \dots + r'_\ell(m'_\ell + N)$, where $r'_1, \dots, r'_\ell \in R$. As $s - \sum_{j=1}^\ell r'_j m'_j \in N$, we can write $s - \sum_{j=1}^\ell r'_j m'_j = \sum_{i=1}^k r_i m_i$ for some

$r_1, \dots, r_k \in R$. Thus, $s = \sum_{i=1}^k r_i m_i + \sum_{j=1}^\ell r'_j m'_j$. Hence S can be generated by the elements $m_1, \dots, m_k, m'_1, \dots, m'_\ell$. Since each R-submodule of M is finitely generated, we conclude that M is Noetherian. $\square$

As a corollary of the previous proposition, we can obtain that the direct sum of finitely many Noetherian R-modules is also Noetherian.

Corollary 30. *Let $M_1, \dots, M_n$ be R-modules. If $M_1, \dots, M_n$ are Noetherian, then $M_1 \oplus \cdots \oplus M_n$ is Noetherian.*

Proof. It suffices to prove the statement for $n = 2$. It is clear that $M_1 \cong M_1 \oplus 0$. Also, since the projection $M_1 \oplus M_2 \to M_2$ has kernel $M_1 \oplus 0$, it follows from the First Isomorphism Theorem that $M_2 \cong (M_1 \oplus M_2)/(M_1 \oplus 0)$. Since both M_1 and M_2 are Noetherian, Proposition 29 guarantees that $M_1 \oplus M_2$ is Noetherian. $\square$

We have pointed out before that not every finitely generated module is Noetherian. However, finitely generated modules over Noetherian rings are Noetherian, as the following proposition indicates.

Proposition 31. *Let M be a finitely generated R-module. If R is Noetherian, then M is Noetherian.*

Proof. Take $m_1, \dots, m_k \in M$ such that $M = Rm_1 + \cdots + Rm_k$, and consider the map $\varphi \colon R^k \to M$ given by the assignment $(r_1, \dots, r_k) \mapsto r_1 m_1 + \cdots + r_k m_k$. Clearly, φ is a surjective R-module homomorphism, and so the First Isomorphism Theorem ensures that $M \cong R^k / \ker \varphi$. Now observe that $R^k / \ker \varphi$ is a Noetherian R-module because direct sums and quotients of Noetherian modules remain Noetherian by Corollary 30 and Proposition 29, respectively. Hence M is Noetherian. $\square$

Nakayama's Lemma. The main purpose of this section is to prove Nakayama's Lemma, which is an important result of commutative algebra that we shall be using in future lectures. Let M be an R-module. If I is an ideal of R, then

$$IM := \Big\{ \sum_{i=1}^n r_i m_i : r_1, \dots, r_n \in I \text{ and } m_1, \dots, m_n \in M \Big\}$$

is an R-submodule of M. Let us argue the following useful result, known as Nakayama's Lemma.

Lemma 32 (Nakayama's Lemma)**.** *Let R be a commutative ring with identity, and let I be an ideal of R. Then the following statements are equivalent.*

(a) *I is contained in every maximal ideal of R.*
(b) *If M is a finitely generated R-module such that $IM = M$, then $M = \{0\}$.*
(c) *If S is a submodule of a finitely generated R-module M such that $IM + S = M$, then $S = M$*

Proof. (a) $\Rightarrow$ (b): Suppose that M is a finitely generated R-module such that $IM = M$. Now assume, by way of contradiction, that $M \neq \{0\}$. Write $M = Rm_1 + \cdots + Rm_n$ for $m_1, \dots, m_n \in M$ assuming that $n \in \mathbb{N}$ is taken as smallest as possible. Since $M \neq \{0\}$, we see that $m_1 \neq 0$. As $m_1 \in M = IM$, we can take $a_1, \dots, a_n \in I$ such that $m_1 = \sum_{i=1}^n a_i m_i$. Then $(1 - a_1)m_1 = \sum_{i=2}^n a_i m_i$. Since $a_1 \in I$ belongs to every maximal ideal, one can easily see that $1 - a_1 \in R^\times$. This implies that $n \geq 2$ and also that $a_1 = \sum_{i=2}^n (1 - a_1)^{-1} a_i m_i$, which contradicts the minimality of n.

(b) $\Rightarrow$ (c) Let M be a finitely generated R-module, and let S be an R-submodule of M satisfying $IM + S = M$. Then M/S is also a finitely generated R-module. In addition, since $IM + S = M$, it follows that $M/S = (IM + S)/S = I(M/S)$. Therefore M/S is trivial by our hypothesis in part (b), which implies that $S = M$.

(c) $\Rightarrow$ (a) Let J be a maximal ideal of R. Then J is an R-submodule of the finitely generated R-module of R. Since $IR + J$ is an ideal of R containing the maximal ideal J, either $IR + J = R$ or $IR + J = J$. Since $J \neq R$, part (c) ensures that $IR + J \neq R$. As a result, $I + J = IR + J = J$, which implies that $I \subseteq J$. $\square$

References

[1] D. S. Dummit and R. M. Foote: *Abstract Algebra* (Third Edition), John Wiley & Sons, 2004.
[2] D. Hilbert: *Über die Theorie der algebraishen Formen*, Math. Ann. **36** (1890) 473–534.
[3] E. Noether: *Idealtheorie in Ringbereichen*, Math. Ann. **83** (1921) 24–66.

Department of Mathematics, MIT, Cambridge, MA 02139
Email address: fgotti@mit.edu