A BRIEF INTRODUCTION TO COMMUTATIVE RINGS

FELIX GOTTI

Background

General Notation. In what follows, $\mathbb{P}$, $\mathbb{N}$, and $\mathbb{N}_0$ denote the sets of primes, positive integers, and nonnegative integers, respectively. As it is customary, we let $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ denote the set of integers, rational numbers, and real numbers, respectively. In addition, for any $b, c \in \mathbb{Z}$ with $b \le c$, we let $[\![b, c]\!]$ denote the discrete interval from b to c:

$$[\![b, c]\!] := \{n \in \mathbb{Z} : b \le n \le c\}.$$

Commutative Semigroups and Abelian Groups. A *binary operation* on a set S is a function $*\colon S \times S \to S$. When $*$ si a binary operation on a set S, it is customary to write $s * t$ instead of $*(s, t)$ for any $s, t \in S$. A pair $(S, *)$, where S is a set and $*$ is a binary operation on S is called a semigroup provided that the operation $*$ is associate: $r * (s * t) = (r * s) * t$ for all $r, s, t \in S$.

Let $(S, *)$ be a semigroup. An element $e \in S$ is called an *identity element* of S if $e * s = s * e = s$ for all $s \in S$. Every semigroup has at most one identity element: indeed, if $e_1, e_2 \in S$ are both identity elements, then $e_1 = e_1 * e_2 = e_2$. The semigroup $(S, *)$ is said to be *commutative* if $s * t = t * s$ for all $s, t \in S$. A semigroup having an identity element is called a *monoid*.

Let $(M, *)$ be a monoid with identity element denoted by e, and let us denote $(M, *)$ simply by M. An element $u \in M$ is called *invertible* or a *unit* if $u * v = v * u = e$ for some $v \in M$, in which case such an element v is called an *inverse* of u. As the identity element $e \in M$ satisfies $e * e = e$, it is its own inverse and, therefore, a unit. In a monoid, every unit has a unique inverse: indeed, if $v_1, v_2 \in M$ are two inverses of a unit u, then $v_1 = v_1 * (u * v_2) = (v_1 * u) * v_2 = v_2$. The monoid M is called a *group* if every element of M is a unit. A group is said to be *abelian* if it is a commutative monoid.

A subset S of M is called a *submonoid* of M if S contains the identity element of M and is *closed* under the operation of M, which means that $b * c \in S$ for all $b, c \in S$. A submonoid of M which is a group is called a *subgroup* of M. If S is a submonoid (resp., a subgroup) of M such that $S \neq M$, then S is called a *proper* submonoid (resp., subgroup) of M. It is routine to prove that the property of being submonoids of a given monoid is preserved under taking arbitrary intersections.

Let N denote a monoid $(N, *')$ with identity element e_N. A function $\varphi\colon M \to N$ is called a *monoid homomorphism* if $\varphi(e) = e_N$ and $\varphi(b * c) = \varphi(b) *' \varphi(c)$ for all $b, c \in M$. If $\varphi\colon M \to N$ is a bijective homomorphism, then φ is called a *monoid isomorphism* and, in this case, we say that the monoids M and N are *isomorphic*. If both M and N are groups, a monoid homomorphism $\varphi\colon M \to N$ is called a *group homomorphism*, and a bijective group homomorphism is called a *group isomorphism*.

Let $(G, *)$ be an abelian group with identity element e, and let H be a subgroup of G. For each $g \in G$, the subset $\{g * h : h \in H\}$ of G, which is denoted by $g * H$, is called a *coset* of G by H. Let G/H denote the set consisting of all the cosets of G by H, and define $*'$ on G/H as follows:

$$g_1 H *' g_2 H := (g_1 * g_2) * H$$

for any cosets g_1H and g_2H of G/H. It is routine to verify that $*'$ is well defined and also that G/H is an abelian group with respect to $*'$, which is called the *quotient group* of G by H. The binary operation of the quotient group G/H is often denote as that of G, in this case, $*$. The following theorem is known as the First Isomorphism Theorem.

Theorem 1. *Let G and G' be abelian groups (multiplicatively written), and let $\varphi\colon G \to G'$ be a group homomorphism. Then $\varphi(G)$ and $\ker\varphi := \{g \in G : \varphi(g) = 1\}$ are subgroups of G' and G, respectively, In addition, $G/\ker\varphi$ and $\varphi(G)$ are isomorphic abelian groups.*

Proof. This is routine, and we leave it as an exercise. □

1. Commutative Rings: Homomorphisms and Ideals

1.1. **What is a Commutative Ring?** We are in a position to bring the definition of a commutative ring with identity, the most relevant algebraic objects in the scope of this exposition.

Definition 2. A triple $(R, +, \cdot)$, where R is a set and $+$ and $\cdot$ are two binary operations on R, is called a *ring* if the following conditions hold:

- $(R, +)$ is an abelian group,
- $(R, \cdot)$ is a semigroup, and
- $r \cdot (s + t) = r \cdot s + r \cdot t$ and $(s + t) \cdot r = s \cdot r + t \cdot r$ for all $r, s, t \in R$.

Let $(R, +, \cdot)$ be a ring and, from now on, let us denote this triple simply by R (this is customary in the literature). The identity of the monoid $(R, +)$, is denoted by 0 and called the *zero element* of R or simply *zero*. For all $r \in R$, the equality $0\cdot r = 0$ holds: it can be deduced from $0\cdot r = (0+0)\cdot r = 0\cdot r+0\cdot r$, as $0 \cdot r$ has an additive inverse. Similarly, $r \cdot 0 = 0$ for all $r \in R$. For $r, s \in R$, we write rs instead of $r \cdot s$ if we see not risk of confusion. We say that R is *commutative* if the semigroup $(R, \cdot)$ is commutative. In addition, we say that an element of R is an *identity* if it is an identity of the semigroup $(S, \cdot)$. Thus, if R contains an identity, then it must be unique and we denote it by either 1_R or 1 and refers to it as *the* identity element. In the scope of this exposition, we are only interested in commutative rings with identity, and we tacitly assume that the identity is not the zero element (otherwise, R is a singleton, which is not an interesting case to consider).

For a commutative ring R with identity, we let $R^\times$ denote its group of units (i.e., invertible elements) of R. 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 $u \in R^\times$.

An additive subgroup S of R is called a *subring* if S is closed under multiplication and contains 1. Clearly, a subring of R is a commutative ring with identity under the binary operations it inherits from R.

1.2. **Ideals.** Let R be a commutative ring with identity 1. An additive subgroup I of R is called an *ideal* if $ra \in I$ for all $r \in R$ and $a \in I$. It is clear that $\{0\}$ and R are ideals of R, and we call $\{0\}$ the *zero ideal* of R. An ideal I of R is called *proper* if $I \subsetneq R$. An ideal I of R is proper if and only if $I \cap R^\times$ is empty: for the less trivial direction, observe that if $u \in I \cap R^\times$ then $R = u(u^{-1}R) \subseteq IR = I$. Hence the only ideals of a field are the zero ideal and the whole field.

For any $a \in R$, we can verify that $aR := \{ar : r \in R\}$ is the smallest ideal of R containing a: ideals of the form aR are called *principal ideals*. When often write (a) instead of aR. The zero ideal and the whole ideal R are both principal ideals as $\{0\} = 0R$ and $R = 1R$.

Example 3. We verify that the every ideal of $\mathbb{Z}$ is principal. Let I be a nonzero proper ideal, and take $m \in I \setminus \{0\}$ such that $|m| := \min\{|a| : a \in I \setminus \{0\}\}$. Then $m\mathbb{Z} \subseteq I\mathbb{Z} = I$. Conversely, for any $a \in I$ we can take $q, r \in \mathbb{Z}$ with $|r| < |m|$ such that $a = qm + r$ and, as $r = a - qm \in I - m\mathbb{Z} \subseteq I$, and $r = 0$ must hold by the minimality of $|m|$, whence $a = mq \in m\mathbb{Z}$. Hence $I = m\mathbb{Z}$ is a principal ideal.

Given ideals I and J of R, we can produce new ideals operating I and J in various ways. The set

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

is an ideal of R, called the *sum* or *addition* of I and J. The sum of finitely many ideals is defined similarly. An ideal I of R is called *finitely generated* if $I = Ra_1 + \cdots + Ra_n$ for some $a_1, \ldots, a_n \in R$. The set

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

is an ideal of R, called the *product* of I and J. We can naturally extend this to the *product* of finitely many ideals. It is clear that $IJ \subseteq I \cap J \subseteq I + J$.

1.3. **Quotients and Homomorphisms.** The main relevance of ideals in ring theory is that we can quotient by them. For an ideal I of R, we let R/I denote the set of *cosets* by I:

$$R/I := \{r + I : r \in R\},$$

and then we define addition and multiplication on R/I as follows: for all $r, s \in R$,

$$(r + I) + (s + I) := (r + s) + I \quad \text{and} \quad (r + I)(s + I) := rs + I.$$

It is routine to verify that, under the defined binary operations, R/I is a commutative ring with identity $1 + I$ (the absorbing property of the ideal I is needed for the multiplication to be well defined). We call R/I the *quotient ring* of R by I.

The group homomorphism $\pi\colon R \to R/I$ is indeed a ring homomorphism. If $f\colon R \to S$ is a ring homomorphism, 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 $R/\ker f \cong f(R)$. (this is often called the First Isomorphism Theorem). 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 $f = \varphi \circ \pi$.

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).

Prime and Maximal Ideals. 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 $J \subseteq P$. The set of prime ideals of R is denoted $\operatorname{Spec}(R)$. One can readily check that a proper ideal P is prime if and only if for all $r, s \in R$ with $rs \in P$, either $r \in P$ or $s \in P$.

Example 4. We have seen before that the ideals of $\mathbb{Z}$ are those of the form $m\mathbb{Z}$ such that $m \in \mathbb{N}_0$. It is clear that $\{0\}$ is a prime ideal and $\mathbb{Z}$ is not. We can write any other ideal of $\mathbb{Z}$ as $m\mathbb{Z}$ for some $m \in \mathbb{N}_{\geq 2}$: note that $m\mathbb{Z}$ is not a prime ideal if and only if there exist $a, b \in \mathbb{N}$ such that $ab \in m\mathbb{Z}$ but neither $a \in m\mathbb{Z}$ nor $b \in m\mathbb{Z}$, which is equivalent to say that $m \notin \mathbb{P}$. Hence $\operatorname{Spec}(\mathbb{Z}) = \big\{\{0\}, p\mathbb{Z} : p \in \mathbb{P}\big\}$.

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 $I = R$.

Example 5. Let us determine the maximal ideals of $\mathbb{Z}$. Clearly $\{0\}$ and $\mathbb{Z}$ are not maximal. If $m \in \mathbb{N}$ is composite, then $a \mid m$ for some $a \in [\![2, m-1]\!]$, and so $m\mathbb{Z} \subsetneq a\mathbb{Z} \subsetneq \mathbb{Z}$, whence $m\mathbb{Z}$ is not maximal. On the other hand, if $p \in \mathbb{P}$, for any $m \in \mathbb{N}$ such that $p\mathbb{Z} \subseteq m\mathbb{Z} \subseteq \mathbb{Z}$, we see that $m \mid p$ and so $m \in \{1, p\}$ or, equivalently, $m\mathbb{Z} \in \{p\mathbb{Z}, \mathbb{Z}\}$. Thus, the maximal ideals of $\mathbb{Z}$ are the $p\mathbb{Z}$ with $p \in \mathbb{P}$.

Proposition 6. *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 7. *Every maximal ideal is prime.*

Not every prime ideal, however, is maximal.

Example 8. For instance, in the ring $\mathbb{Z}[x]$ the principal 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 $\mathbb{Z}[x]$.

It turns out that every proper ideal of R is contained in a maximal ideal (Corollary 10). To argue such a result, one needs to appeal to Zorn's lemma, which is a statement equivalent to the Axiom of Choice. Zorn's lemma states that a nonempty partially ordered set (poset) S contains a maximal element provided that every totally ordered subset of S has an upper bound. One can actually use Zorn's lemma to argue the following result, which is stronger than the fact that every proper ideal is contained in a maximal ideal.

Theorem 9. *Let R be a commutative ring with identity, and let I be a proper ideal of R. If M is a multiplicative submonoid of R disjoint from I, then there exists an ideal P that is maximal in the set consisting of all ideals of R disjoint from M and containing I. Moreover, P is prime.*

Proof. Let $\mathscr{S}$ be the set of all ideals of R disjoint from M and containing I. The set $\mathscr{S}$ is nonempty because $I \in \mathscr{S}$. Clearly, $\mathscr{S}$ is a partially ordered set (under inclusion). In addition, if $\mathscr{T} := \{I_\gamma : \gamma \in \Gamma\}$ is a totally ordered subset of $\mathscr{S}$, then it is not hard to verify that $J = \bigcup_{\gamma \in \Gamma} I_\gamma$ is an ideal of R disjoint from M and containing I. Thus, J is an upper bound of $\mathscr{T}$ in $\mathscr{S}$. Therefore Zorn's lemma guarantees the existence of a maximal element P in $\mathscr{S}$, which yields the first part of the theorem.

Now we show that P is indeed a prime ideal. Suppose, by way of contradiction, that $J_1 J_2 \subseteq P$ for ideals J_1 and J_2 of R none of them contained in P. Then both ideals $J_1 + P$ and $J_2 + P$ properly contain P, which means that they both intersect M. Take $p_1, p_2 \in P$, $j_1 \in J_1$ and $j_2 \in J_2$ such that $m_1 := p_1 + j_1 \in M$ and $m_2 := p_2 + j_2 \in M$. Thus, we see that

$$m_1 m_2 = p_1 p_2 + j_2 p_1 + j_1 p_2 + j_1 j_2 \in P + J_1 J_2 \subseteq P.$$

Since M is closed under multiplication, $m_1 m_2 \in P \cap M$, contradicting that P is disjoint from M. Hence P is a prime ideal. □

As an immediate consequence of Theorem 9, we obtain the following result.

Corollary 10. *Let R be a commutative ring with identity. Then every proper ideal of R is contained in a maximal ideal.*

Corollary 11. *Every commutative ring with identity contains a minimal prime ideal.*

2. Integral Domains: UFDs, PIDs, and Euclidean Domains

Let R be an integral domain, that is, a commutative ring with identity with no nonzero zero-divisors. We say that a nonzero nonunit $r \in R$ is *irreducible* if whenever $r = uv$ for some $u, v \in R$ either $u \in R^\times$ or $v \in R^\times$.

Example 12. The prototypical integral domain is $\mathbb{Z}$, the ring of integers.

According the most standard version of the Fundamental Theorem of Arithmetic (FTA), every nonzero integer z with $z \notin \{\pm 1\}$ can be factored as $z = p_1 \cdots p_n$ for some $p_1, \ldots, p_n \in \pm\mathbb{P}$ and such a factorization is unique (up to permuting and multiplying the factors by ± 1).

UFDs, PIDs, and Euclidean Domains

A nonzero element $r \in R \setminus R^\times$ is *prime* if whenever $r \mid_R st$ for some $s, t \in R$ either $r \mid_R s$. It is not hard to verify that every prime is irreducible (prove this!).

Definition 13. 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 $p_1, \ldots, p_m \in R$, and
(2) if $r = q_1 \cdots q_n$ for irreducibles $q_1, \ldots, q_n \in R$, 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 14. *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 15. 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 22 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 17, this lemma will become a special case of Proposition 14).

Lemma 16. *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 17. *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 $q_1, \ldots, q_n$ 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 $p_1, \ldots, p_{m+1}$ in R. Suppose that $r = q_1 \cdots q_n$ for irreducibles $q_1, \ldots, q_n$. Since p_{m+1} is prime by Lemma 16, one of the irreducibles $q_1, \ldots, q_n$ is divisible by p_{m+1}. After relabeling $q_1, \ldots, q_n$, 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 $q_1, \ldots, q_m$ such that p_i and q_i are associates for every $i \in [\![1, m]\!]$. Hence R is a UFD. □

The converse of Theorem 17 does not hold.

Example 18. 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 19. An integral domain R is called a *Euclidean domain* if there is a map $N\colon R \to \mathbb{N}_0$, called a *norm*, such that $N(0) = 0$ and 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.

Example 20. 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 $|q_1 - m| \leq 1/2$ and $|q_2 - n| \leq 1/2$, and then set $q = m + in \in \mathbb{Z}[i]$ and $r = \alpha - q\beta \in \mathbb{Z}[i]$. Since

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

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

Polynomial rings over fields are also examples of Euclidean domains.

Proposition 21. *If F is a field, then $F[x]$ is a Euclidean domain.*

Proof. Let F be a field. Define $N\colon F[x] \to \mathbb{N}_0$ by $N(0) = 0$ and $N(p(x)) = \deg p(x)$. Now, let $f(x)$ and $g(x)$ be any two polynomials in $F[x]$ with $g(x) \neq 0$. We want to find $q(x)$ and $r(x)$ in $F[x]$ with $f(x) = g(x)q(x) + r(x)$ such that either $r(x) = 0$ or $N(r(x)) < N(g(x))$. We proceed by induction on $\deg f(x)$. If $\deg f(x) = 0$, then $f(x) \in F$, and so we take $q(x) = r(x) = 0$ if $f(x) = 0$ or $q(x) = f(x)/g(x)$ and $r(x) = 0$ if $f(x) \in F^\times$. Therefore assume that $n := \deg f(x) \in \mathbb{N}$ and also that the statement of the proposition follows for any pair of polynomials $f'(x), g'(x) \in F[x]$ with $\deg f'(x) < n$ and $g'(x) \neq 0$. If $n < \deg g(x)$, then we simply take $q(x) = 0$ and $r(x) = f(x)$. Thus, we assume that $\deg f(x) \geq \deg g(x)$.

Set $m := \deg g(x)$, and let a_n and b_m be the leading coefficients of $f(x)$ and $g(x)$, respectively. Observe that $f_1(x) := f(x) - (a_n b_m^{-1})x^{n-m}g(x)$ has degree strictly less than $\deg f(x)$. By the induction hypothesis, we can find polynomials $q_1(x)$ and $r(x)$ in $F[x]$ with $f_1(x) = g(x)q_1(x) + r(x)$ such that either $r(x) = 0$ or $\deg r(x) < \deg g(x)$. Now, set $q(x) := q_1(x) + (a_n b_m^{-1})x^{n-m}$, and observe that

$$\begin{aligned} f(x) &= f_1(x) + (a_n b_m^{-1})x^{n-m}g(x) \\ &= g(x)q_1(x) + r(x) + (a_n b_m^{-1})x^{n-m}g(x) \\ &= g(x)q(x) + r(x). \end{aligned}$$

Hence our proof is complete. □

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

Theorem 22. *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. □

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].

Localization

Let R be a commutative ring with identity. A *multiplicative subset* of R is a submonoid of $(R\backslash\{0\}, \cdot)$, that is, a subset of $R\backslash\{0\}$ that contains 1 and is closed under multiplication. Let S be a multiplicative subset of R. One can define the following relation on $R \times S$: $(r_1, s_1) \sim (r_2, s_2)$ for $(r_1, s_1), (r_2, s_2) \in R \times S$ provided that $(r_1 s_2 - r_2 s_1)s = 0$ for some $s \in S$. It is not hard to check that $\sim$ is indeed an equivalence relation on $R \times S$. We let $S^{-1}R$ denote the set of equivalence classes of $\sim$ and, for $r \in R$ and $s \in S$, we let r/s denote the equivalence class of (r, s). Motivated by the standard addition and multiplication of rational numbers, we can now define for r_1/s_1 and r_2/s_2 in $S^{-1}R$ the following operations:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \quad \text{and} \quad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}.$$

It is routine to verify that both operations are well defined and that $(S^{-1}R, +, \cdot)$ is a commutative ring with identity $1/1$.

Proposition 23. *$(S^{-1}R, +, \cdot)$ is a commutative ring with identity.*

The ring $S^{-1}R$ is called the *localization* of R at S. We can easily see that the map $\pi\colon R \to S^{-1}R$ defined by $\pi(r) = r/1$ satisfies the properties in the following proposition.

Proposition 24. *Let R be a commutative ring with identity, and let S be a multiplicative subset of R. Then the following statements hold.*

(1) *The map $\pi\colon R \to S^{-1}R$ is a ring homomorphism satisfying that $\pi(s)$ is a unit in $S^{-1}R$ for every $s \in S$. In addition, π is injective if and only if S contains no zero-divisors of R.*

(2) *If $\varphi\colon R \to T$ is a ring homomorphism such that $\varphi(s)$ is a unit in T for every $s \in S$, then there exists a unique ring homomorphism $\theta\colon S^{-1}R \to T$ such that $\varphi = \theta \circ \pi$.*

Proof. (1) One can readily see that π is a ring homomorphism. For every $s \in S$, it is clear that $1/s \in S^{-1}R$ and, therefore, $\pi(s) = s/1$ is a unit in $S^{-1}R$. If $s \in S$ is a zero-divisor in R, then taking $r \in R \setminus \{0\}$ with $sr = 0$, we can see that $\pi(r) = 0$ and so π is not injective. Conversely, if $\pi(r) = 0$ for some $r \in R \setminus \{0\}$, then $r/1 = 0/1$ and so there is an $s \in S$ such that $sr = 0$.

(2) For φ as in (2), define $\theta\colon S^{-1}R \to T$ by $\theta(r/s) = \varphi(r)\varphi(s)^{-1}$. Since $\varphi(s) \in T^\times$ for every $s \in S$, the element $\varphi(r)\varphi(s)^{-1}$ belongs to T, and it is easy to check that θ is a well-defined ring homomorphism. Since $\theta(\pi(r)) = \theta(r/1) = \varphi(r)$, the equality $\theta \circ \pi = \varphi$ holds. Finally, for any ring homomorphism $\theta'\colon S^{-1}R \to T$ with $\varphi = \theta' \circ \pi$, we see that $\theta'(r/s) = \theta'(r/1)\theta'(1/s) = \theta'(\pi(r))\theta'(\pi(s))^{-1} = \varphi(r)\varphi(s)^{-1} = \theta(r/s)$ for all $r/s \in S^{-1}R$. Hence $\theta' = \theta$, and the uniqueness follows. □

If R is an integral domain, then the localization of R at the multiplicative subset $(R \setminus \{0\}, \cdot)$ is the quotient field $\mathrm{qf}(R)$ of R. The following two examples of localizations often show up in commutative ring theory.

Example 25. Let R be a commutative ring with identity, and let P be a prime ideal of R. Since R is prime, $S := R \setminus P$ is a multiplicative subset of R. The ring $S^{-1}R$ is called the *localization of R at P* and is denoted by R_P.

(1) For instance, if $p \in \mathbb{P}$, then

$$\mathbb{Z}_{(p)} = \big\{m/n : m, n \in \mathbb{Z} \text{ and } p \nmid n\big\};$$

observe that the units of $\mathbb{Z}_{(p)}$ are the elements m/n such that $m, n \in \mathbb{Z}$ and $p \nmid mn$.

(2) Set $R = \mathbb{C}[x, y]$ and $P = (x, y)$. Then P is a prime ideal, and the localization R_P of R at P consists of all rational expressions f/g, where $f, g \in R$ and $g \notin P$, that is, $g(0, 0) \neq 0$. The units of R_P are the rational expressions f/g satisfying $f(0, 0)g(0, 0) \neq 0$.

In general, the units of R_P have the form r/s with $r, s \in R$ such that $rs \notin P$.

Example 26. Let R be a commutative ring with identity, and let f be an element of R such that $f^n \neq 0$ for any $n \in \mathbb{N}_0$. For $S := \{f^n : n \in \mathbb{N}_0\}$, the ring $S^{-1}R = R[1/f]$ is often denoted by R_f. It is not hard to argue that R_f is isomorphic to the ring $R[x]/(xf - 1)$. For instance, $\mathbb{Z}[x]_x = \mathbb{Z}[x, 1/x]$, which is the ring of Laurent polynomials in one variable over $\mathbb{Z}$.

An integral domain is the intersection of all its localizations at prime ideals.

Proposition 27. *If R is an integral domain, then $R = \bigcap_P R_P = \bigcap_M R_M$, where the first intersection runs over all prime ideals of R and the second intersection runs over all maximal ideals of R.*

Proof. It is clear that $R \subseteq \bigcap_P R_P \subseteq \bigcap_M R_M$. To show that $\bigcap_M R_M \subseteq R$, take $a \in \bigcap_M R_M$ and suppose, by way of contradiction, that $a \notin R$. The set $I_a := \{r \in R : ra \in R\}$ is an ideal of R, which is a proper ideal because $a \notin R$. Let M be a maximal ideal of R containing I_a. Then $a \in R_M$, and we can take $r \in R$ and $s \in R \setminus M$ such that $a = r/s$. As $sa = r \in R$, we see that $s \in I_a \subseteq M$, which is a contradiction. □

Localization and Ideals. For an ideal I of R, the ideal $S^{-1}R\,\pi(I)$ of $S^{-1}R$ is called the *extension* of I by π and is denoted by $S^{-1}I$. Observe that every element of $S^{-1}I$ can be written as a/s for some $a \in I$ and $s \in S$.

Proposition 28. *Let R be a commutative ring with identity, and let S be a multiplicative subset of R. Then the following statements hold.*

(1) *For any ideal J of $S^{-1}R$ the equality $S^{-1}\pi^{-1}(J) = J$ holds. In particular, every ideal of $S^{-1}R$ is the extension of an ideal in R.*
(2) *For an ideal I of R, the equality $S^{-1}I = S^{-1}R$ holds if and only if $I \cap S \neq \emptyset$.*
(3) *The assignment $I \mapsto S^{-1}I$ induces a bijection between the set of prime ideals of R disjoint from S and the set of prime ideals of $S^{-1}R$.*

Proof. (1) It suffices to show that J is contained in the ideal $J' := S^{-1}\pi^{-1}(J)$. Take $r/s \in J$. As $r/1 = (s/1)(r/s) \in J$, it follows that $r \in \pi^{-1}(J)$, and so $r/1 \in S^{-1}\pi^{-1}(J)$. Since J' is an ideal of $S^{-1}R$, we see that $r/s = (1/s)(r/1) \in J'$. Hence $J' = J$. The second statement is an immediate consequence of the first one.

(2) If $S^{-1}I = S^{-1}R$, then $a/s = 1/1$ for some $a \in I$ and $s \in S$. So we can take $s' \in S$ such that $(a - s)s' = 0$. This means that $ss' = as' \in I$, whence $I \cap S = \emptyset$. Conversely, assume that $I \cap S \neq \emptyset$ and take $a \in I \cap S$. Then for all $r/s \in S^{-1}R$, we see that $ra \in I$ while $sa \in S$, which implies that $r/s = (ra)/(sa) \in S^{-1}I$. Thus, $S^{-1}I = S^{-1}R$.

(3) Let $\mathscr{I}$ be the set of prime ideals in R that are disjoint from S, and let $\mathscr{J}$ be the set of prime ideals in $S^{-1}R$. Let $e\colon \mathscr{I} \to \mathscr{J}$ and $c\colon \mathscr{J} \to \mathscr{I}$ be the maps given by the assignments $I \mapsto S^{-1}I$ and $J \mapsto \pi^{-1}(J)$, respectively. Since homomorphic inverse images of prime ideals are prime ideals, c is well defined. To check that e is also well defined, take $P \in \mathscr{I}$ and let us verify that $S^{-1}P$ is a prime ideal. Take $r_1, r_2 \in R$ and $s_1, s_2 \in S$ such that $(r_1/s_1)(r_2/s_2) \in S^{-1}P$. Then there are elements $a \in P$ and $s, s' \in S$ such that $(r_1r_2s - as_1s_2)s' = 0$, which implies that $r_1r_2ss' \in P$. As P is prime and disjoint from S, we obtain that either $r_1 \in P$ or $r_2 \in P$, from which we deduce that either $r_1/s_1 \in S^{-1}P$ or $r_2/s_2 \in S^{-1}P$. Hence $S^{-1}P$ is a prime ideal, and so the map e is well defined. Part (1) guarantees that $e \circ c$ is the identity of $\mathscr{J}$. Proving that $c \circ e$ is the identity of $\mathscr{I}$ amounts to arguing that $c(e(P)) \subseteq P$ for every $P \in \mathscr{I}$. To do so, take $a_3/s_3 \in e(P) = S^{-1}P$ for $a_3 \in P$ and $s_3 \in S$. If $r \in \pi^{-1}(a_3/s_3)$, then $r/1 = a_3/s_3$ and there is an $s'' \in S$ with $(rs_3 - a_3)s'' = 0$. This implies that $rs_3 \in P$, from which we deduce that $r \in P$. Hence $c(e(P)) \subseteq P$, as desired. Thus, $c \circ e$ is the identity of $\mathscr{I}$, which completes the proof. □

3. Polynomials Rings: Irreducibility and Factorization

We turn our attention to rings of polynomials over UFDs. The following criterion is quite useful to argue the irreducibility of polynomials over UFDs.

Theorem 29 (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 $p_1, \ldots, p_n$ 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 $d_1 d_2 = d$ such that both $a'(x)/d_1$ and $b'(x)/d_2$ belong to $R[x]$. Now we just need to take $c = d_1^{-1} a'(x)/a(x)$. □

Corollary 30. *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 31. *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 uniquely 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, $p(x) = p_1'(x) \cdots p_m'(x)$ for unique irreducibles $p_1'(x), \dots, p_m'(x)$ in $\mathrm{qf}(R)[x]$. It follows now by Gauss's lemma that $p(x) = p_1(x) \cdots p_m(x)$, 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 30 that $p_1(x), \dots, p_m(x)$ are irreducibles in $R[x]$.

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 30 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 $b_i = u a_i$ 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 30 and Proposition 32 (known as Eisenstein's criterion) are practical tools to argue that certain polynomials are irreducibles.

Proposition 32. *Let R be an integral domain, and let $p(x) = a_n x^n + \cdots + a_1 x + a_0$ 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 $a_0 \notin P^2$. □

We conclude with an application of Eisenstein's criterion.

Example 33. 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 30 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

$$f(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}. \tag{3.1}$$

From the summation in (3.1), 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.

4. Noetherian Rings

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

Definition 34. 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 35. *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 $I = Ra_1 + \cdots + Ra_n$ for some $a_1, \ldots, a_n \in I$. After taking $N \in \mathbb{N}$ such that $a_1, \ldots, a_n \in I_N$, 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. □

Example 36. 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 37. *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. □

The property of being Noetherian is preserved under localization.

Proposition 38. *Let R be a Noetherian domain, and let S be a multiplicative subset of R. Then $S^{-1}R$ is also Noetherian.*

Proof. By Proposition 28, any ideal of $S^{-1}R$ has the form $S^{-1}I$ for some ideal I of R. Since R is Noetherian, $I = Ra_1 + \cdots + Ra_n$ for some $a_1, \dots, a_n \in R$. Then for each $a/s \in S^{-1}I$ with $a \in I$ and $s \in S$, we can write $a = \sum_{i=1}^n r_i a_i$ for some $r_1, \dots, r_n \in R$ to obtain the equality $a/s = \sum_{i=1}^n (r_i/s)(a_i/1)$. Thus, $S^{-1}I$ is the ideal of $S^{-1}R$ generated by $a_1/1, \dots, a_n/1$. Hence $S^{-1}R$ is a Noetherian ring. □

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

Theorem 39 (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 for each nonzero $f \in R[x]$, the element $LC(xf) \in I_{n+1}$ provided that $LC(f) \in I_n$. 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 $r_1, \ldots, r_k \in R$ and $\ell_1, \ldots, \ell_k \in L_m$. 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 40. *If R is a Noetherian ring, then $R[x_1, \ldots, x_n]$ is a Noetherian ring.*

Exercises

Exercise 1. Prove that every finite integral domain is a field.

Exercise 2. Let R be a commutative ring with identity, and let $\mathscr{C}$ be a chain of prime ideals of R. Prove that $\bigcap_{I \in \mathscr{C}} I$ and $\bigcup_{I \in \mathscr{C}} I$ are also prime ideals.

Exercise 3. Prove that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Exercise 4. Prove that every Noetherian domain is atomic.

Exercise 5. Does every nonzero element of a Noetherian domain has finitely many factorizations into irreducibles?

Exercise 6. Prove that $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ is a Euclidean domain.

Exercise 7. Set $R := \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$.

(1) Prove that R is not a Euclidean domain.
(2) Prove that R is a PID.

Exercise 8.

(1) Find a Noetherian domain that is not a UFD.
(2) Find a UFD that is not a Noetherian domain.

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