Part IX. Factorization

Section IX.45. Unique Factorization Domains

Note. In this section we return to integral domains and concern ourselves with factoring (with respect to the multiplication binary operation). We define *irreducible* and *prime*. Many of the results are motivated by the behavior of integral domain $\langle \mathbb{Z}, +, \cdot \rangle$. We show that "every PID is a UFD"(!) and give a proof of the Fundamental Theorem of Arithmetic in $\mathbb{Z}$.

Note. Recall that an *integral domain* is a commutative ring (that is, in $\langle R, +, \cdot \rangle$, multiplication $\cdot$ is commutative) with unity $1 \neq 0$ and containing no divisors of 0 (so $a \cdot b = 0$ implies that either $a = 0$ or $b = 0$). $\langle \mathbb{Z}, +, \cdot \rangle$ is an example of an integral domain.

Definition 45.1. Let R be a commutative ring with unity and let $a, b \in R$. If there exists $c \in R$ such that $b = a$, then a *divides* b (or equivalently, a is a *factor* of b), denoted $a \mid b$. If for given a and b, no such c exists then we say a *does not divide* b, denoted $a \nmid b$.

Definition 45.2. An element u of a commutative ring with unity is a *unit* if u divides 1; that is, if u has a multiplicative inverse in the ring. Two elements a and b in a ring are *associates* if $a = bu$ where u is a unit in the ring.

Example 45.3. In ring $\langle \mathbb{Z}, +, \cdot \rangle$, the only units are 1 and -1. Distinct $a, b \in \mathbb{Z}$ are associates if and only if $a = -b$.

Definition 45.4. A nonzero element p that is not a unit in an integral domain D is an *irreducible* of D if in every factorization $p = ab$ in D implies that either a or b is a unit.

Note. If p and q are associates in an integral domain then p is irreducible if an only if q is irreducible.

Note. As with the Fundamental Theorem of Arithmetic in $\mathbb{N}$, we are interested in uniquely factoring elements of an integral domain into irreducibles. Since $\mathbb{N}$ is not a ring (it has no additive inverses), we need to extend the Fundamental Theorem of Arithmetic to $\mathbb{Z}$. However, uniqueness is affected by the existence of negative primes (which are, of course, associates of positive primes in $\mathbb{Z}$). This idea is the inspiration for the next definition.

Definition 45.5. An integral domain D is a *unique factorization domain* (or "UFD") is the following hold:

1. Every element of D that is neither 0 nor a unit can be factored into a product of a finite number of irreducibles.

2. If $p_1, p_2, \ldots, p_r$ and $q_1, q_2, \ldots, q_r$ are two factorizations of the same element of D into irreducibles, then $r = s$ and the q_j can be renumbered so that p_i and g_i are associates for each i.

Note. We have met the idea of unique factorization in Section 23. Recall:

Theorem 23.20. If F is a field, then every nonconstant polynomial in $F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials being unique except for order and for unit (that is, nonzero constant) factors in F.

In the words used here, if F is a field then $F[x]$ is a UFD.

Note. Recall that an additive subgroup N of a ring R which satisfies $aN \subseteq N$ and $Nb \subseteq N$ for all $a, b \in R$ is an *ideal.* (If N is an ideal of ring R, then we can make the factor ring or quotient ring R/N.) An ideal N of ring R is a *principal ideal* if for some $a \in R$ we have $N = \{ra \mid r \in R\} = \langle a \rangle$.

Definition 45.7. An integral domain D is a *principal ideal domain* (or "PID") if every ideal in D is a principal ideal.

Note. In integral domain $D = \mathbb{Z}$, every ideal is of the form $n\mathbb{Z}$ (see Corollary 6.7 and Example 26.11) and since $n\mathbb{Z} = \langle n \rangle = \langle -n \rangle$, then every ideal is a principal ideal. So $\mathbb{Z}$ is a PID.

Note. Theorem 27.24 says that if F is a field then every ideal of $F[x]$ is principal. So for every field F, the integral domain $F[x]$ is a PID.

Note. The goal of this section is to prove two results (the first of which is poetically brief):

1. **Theorem 45.17.** Every PID is a UFD.
2. **Theorem 45.29.** If D is a UFD, then $D[x]$ is a UFD.

We need a few more definitions before completing the lengthy proofs.

Definition 45.8. If $\{A_i \mid i \in I\}$ is a collection of sets, then the *union* of the sets, denoted $\cup_{i\in I} A_i$, is the set of all x such that $x \in A_i$ for some $i \in I$.

Lemma 45.9. Let R be a commutative ring and let $N_1 \subseteq N_2 \subseteq \cdots$ be an ascending chain of ideals N_i in R. Then $N = \sup_i N_i$ is an ideal of R.

Lemma 45.10. The Ascending Chain Condition for a PID.

Let D be a PID. If $N_1 \subseteq N_2 \subseteq \cdots$ is an ascending chain of ideals, then there exists a positive integer r such that $N_r = N_s$ for all $s \geq r$. Equivalently , every strictly ascending chain of ideals in a PID is of finite length. Under such conditions it is said that the *ascending chain condition* holds for ideals in a PID.

Note 1. In the following proofs we will use the facts that:

(1) $\langle a \rangle \subseteq \langle b \rangle$ if and only if $b \mid a$.

proof. If $\langle a \rangle \subseteq \langle b \rangle$ then $a \in \langle b \rangle$ and then $a = bd$ for some $d \in D$. Then $b \mid a$. If $b \mid a$ then $a = bd$ for some $d \in D$ and then $a \in \langle b \rangle$, or $\langle a \rangle \subseteq \langle b \rangle$. □

(2) $\langle a \rangle = \langle b \rangle$ if and only if a and b are associates.

proof. We have $\langle a \rangle = \langle b \rangle$ if and only if $a \mid b$ and $b \mid a$ by (1). This is the case if and only if $a = bc$ and $b = ad$ for some $c, d \in D$, or $a = bc = (ad)c$ and then $dc = 1$. So d and c are units and a and b are associates (and conversely). □

Note. The following gives us the first condition in the definition of UFD for a PID.

Theorem 45.11. Let D be a PID. Every element that is neither 0 nor a unit of D is a product of irreducibles.

Note. To prove that every PID is a UFD, we now need to show that every PID satisfies the second condition in the definition of a UFD. That is, we need to show that the product of irreducibles of Theorem 45.11 is unique (in the sense explained in the definition of UFD).

Note. Let R be a ring. Recall that an ideal M of R, where $M \neq R$, is a *maximal ideal* of R if there is no proper ideal N of R properly containing M. Recall that Theorem 27.25 says that ideal $\langle p(x) \rangle \neq \{0\}$ or ring $F[x]$ (where F is a field) is maximal if and only if $p(x)$ is irreducible over F. (This result was an important part of the proof of Kronecker's Theorem [Theorem 29.3].) The following result is analogous to Theorem 27.25 but is in the setting of PIDs.

Lemma 45.12. An ideal $\langle p \rangle$ is a PID is maximal if and only if p is irreducible.

Note. Recall that Theorem 27.27 says that for irreducible $p(x) \in F[x]$ (F a field), if $p(x)$ divides $r(x)s(x)$ for $r(x), s(x) \in F[x]$ then either $p(x)$ divides $r(x)$ or $s(x)$. The following result is analogous to Theorem 27.27 but is in the setting of PIDs. Recall that an ideal $N \neq R$ is a commutative ring R is a *prime ideal* if $ab \in N$ implies that either $a \in N$ or $b \in N$ for $a, b \in R$.

Lemma 45.13. In a PID, if an irreducible p divides ab then either $p \mid a$ or $p \mid b$.

Corollary 45.14. If p is an irreducible in a PID and p divides the product $a_1 a_2 \cdots a_n$ for $a_i \in D$, then $p \mid a_i$ for at least on i.

Proof. This follows by induction from Lemma 45.13. ∎

Definition 45.15. A nonzero nonunit element p of an integral domain D is a *prime* if, for all $a, b \in D$, $p \mid ab$ implies either $p \mid a$ or $p \mid b$.

Note. In Exercises 25 and 26, it is shown that a prime in an integral domain is irreducible and that in a UFD an irreducible is a prime. Since a UFD is a type of integral comain, then "prime" and "irreducible" are the same in a UFD. The next example shows that in some integral domains there are irreducibles that are not primes.

Example 45.16. Let F be a field and let D be the subdomain $F[x^3, xy, y^3]$ of $F[x, y]$. (That is, x^3, xy, y^3, x, y are indeterminates [not something involving free groups, though the notation is similar].) Then x^3, xy, y^3 are irreducibles in D ("clearly"), but $(x^3) = (y^3) = (xy)(xy)(xy)$. So xy divides x^3y^3 but xy divides neither x^3 nor y^3. So xy is not prime. (Elements x^3 and y^3 are also irreducible and not prime.)

Theorem 45.17. Every PID is a UFD.

Note. A natural question to ask now is: "Is every UFD a PID" (that is, are UFDs and PIDs equivalent)? We will see in Example 45.31 a UFD which is *not* a PID.

Corollary 45.18. Fundamental Theorem of Arithmetic.
The integral domain $\mathbb{Z}$ is a UFD.

Note. We normally think of the Fundamental Theorem of Arithmetic as stating that every *natural number* can be uniquely written as a product of primes. The units in $\mathbb{Z}$ are 1 and -1 and the irreducibles in $\mathbb{Z}$ are the positive primes and the negative primes. So the only associate of a prime is its negative. Since $\mathbb{Z}$ is a UFD, every element can be expressed as a product of irreducibles (i.e., positive and negative primes) uniquely in the sense of Property 2 of the definition of UFD (that is, different products of irreducibles involve pairwise associates). So if $a = p_1 p_2 p \cdots p_r$ in $\mathbb{Z}$ and $a \in \mathbb{N}$, then there must be an even number of negative p_i's and we can replace these with corresponding positive associates to produce a unique factorization of a into a product of positive primes in $\mathbb{N}$. So Corollary 45.18 implies the traditional Fundamental Theorem of Arithmetic in $\mathbb{N}$.

Note. We now show that if D is a UFD then $D[x]$ is a UFD. This requires some new definitions and several preliminary results.

Definition 45.19. Let D be a UFD and let $a_1, a_2, \ldots, a_n$ be nonzero elements in D. An element $d \in D$ is a *greatest common divisor* (or "gcd") of all the a_i if $d \mid a_i$ for $i = 1, 2, \ldots, n$ and any other $d' \in D$ that divides all the a_i also divides d.

Note. If both d and d' are gcd's of the a_i then $d \mid d'$ and $d' \mid d$. Thus $d = q'd'$ and $d' = qd$ for some $q, q' \in D$. Then $d = q'd' = q'qd$ and by cancellation in D (by Theorem 19.5) $1 = q'q$ and q and q' are units and d and d' are associates. So gcd's are not unique in a UFD, but different gcd's must be associates. In $\mathbb{Z}$, this means that different gcd's differ by a multiple of -1.

Example 45.20. Consider 420, -168, and 252 in $\mathbb{D}$. We know $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$, $-168 = -1 \cdot 2^3 \cdot 3 \cdot 7$ and $252 = 2^2 \cdot 3^2 \cdot 7$. To find a gcd, we algorithmically choose the highest power of each irreducible common to to each number: $2^2 \cdot 3 \cdot 7 = 84$. So a gcd is 84. Another is -84 (notice that -1 is not an irreducible since it is a unit).

Definition 45.21. Let D be a UFD. A noncontant polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ in $D[x]$ is *primitive* if 1 is a gcd of the a_i for $i = 0, 1, \ldots, n$.

Example 45.22. In $\mathbb{Z}[x]$, $4x^2 + 3x + 2$ is primitive but $4x^2 + 6x + 2$ is not. Notice that a nonconstant irreducible in $D[x]$ must be a primitive polynomial.

Lemma 45.23. If D is a UFD then for every nonconstant $f(x) \in D[x]$ we have $f(x) = cg(x)$ where $c \in D$, $g(x) \in D[x]$ and $g(x)$ is a primitive. The element c is unique up to a unit factor in D and is the *content* of $f(x)$. Also $g(x)$ is unique up to a unit factor in D.

Lemma 45.25. Gauss's Lemma.
If D is a UFD, then a product of two primitive polynomials in $D[x]$ is again primitive.

Corollary 45.26. If D is a UFD, then a finite product of primitive polynomials in $D[x]$ is again primitive.

Proof. This follows by induction from Lemma 45.25. ∎

Note. In the following result, D is a UFD and F is field of quotients of D (see Section 21). By Theorem 23.20, $F[x]$ is also a UFD. In our last major result of this section (Theorem 45.29) we'll show that $D[x]$ is a UFD. In the proof, we will relate factorization of polynomials in $F[x]$ to factorization in $D[x]$.

Lemma 45.27. Let D be a UFD and let F be a field of quotients of D. Let $f(x) \in D[x]$ where (degree $f(x)) > 0$. If $f(x)$ is an irreducible in $D[x]$, then $f(x)$ is also an irreducible in $F[x]$. Also, if $f(x)$ is primitive in $D[x]$ and irreducible in $F[x]$, then $f(x)$ is irreducible in $D[x]$.

Corollary 45.28. If D is a UFD and F is a field of quotients of D, then a nonconstant $f(x) \in D[x]$ factors into a product of two polynomials of lower degrees r and s in $F[x]$ if and only if it has a factorization into polynomials of the same degrees r and s in $D[x]$.

Theorem 45.29. If D is a UFD, then $D[x]$ is a UFD.

Corollary 45.30. If F is a field and $x_1, x_2, \ldots, x_n$ are indeterminates, then $F[x_1, x_2, \ldots, x_n]$ is a UFD.

Example 45.31. Now for an example of a UFD which is not a PID. Let F be a field and let x and y be indeterminates. Then $F[x, y]$ is a UFD by Corollary 45.30. Consider the set N of all polynomials in x and y in $F[x, y]$ having constant term 0. Then N is an ideal (since $aN \subseteq N$ and $Nb \subseteq N$ for all $a, b \in F$). A principal ideal is of the form $N = \{ar \mid r \in F\} = \langle a \rangle$ and so includes 0. So our N cannot be a principal ideal. Thus $F[x, y]$ is not a PID.

Note. Since $\mathbb{Z}$ is a UFD by the Fundamental Theorem of Arithmetic (Corollary 45.18), by Theorem 45.29 $\mathbb{Z}[x]$ is a UFD. In Exercise 46.12 it is shown that $\mathbb{Z}[x]$ is not a PID.

Revised: 3/21/2024