Section III.3. Factorization in Commutative Rings

Note. In this section, we introduce the concepts of divisibility, irreducibility, and prime elements in a ring. We define a unique factorization domain and show that every principal ideal domain is one ("every PID is a UFD"—Theorem III.3.7). We push the Fundamental Theorem of Arithmetic and the Division Algorithm to new settings.

Definition III.3.1. A nonzero element a of commutative ring R *divides* an element $b \in R$ (denoted $a \mid b$) if there exists $x \in R$ such that $ax = b$. Elements $a, b \in R$ are *associates* if $a \mid b$ and $b \mid a$.

Theorem III.3.2. Let a, b, u be elements of a commutative ring R with identity.

(i) $a \mid b$ if and only if $(b) \subset (a)$.

(ii) a and b are associates if and only if $(a) = (b)$.

(iii) u is a unit if and only if $u \mid r$ for all $r \in R$.

(iv) u is a unit if and only if $(u) = R$.

(v) The relation "a is an associate of b" is an equivalence relation on R.

(vi) If $a = br$ with $r \in R$ a unit, then a and b are associates. If R is an integral domain, the converse is true.

Note. The proof of Theorem III.3.2 is to be given in Exercise III.3.A.

Definition III.3.3. Let R be a commutative ring with identity. An element $c \in R$ is *irreducible* provided that:

(i) c is a nonzero nonunit, and

(ii) $c = ab$ implies that either a is a unit or b is a unit.

An element $p \in R$ is *prime* provided that:

(i) p is a nonzero nonunit, and

(ii) $p \mid ab$ implies that either $p \mid a$ or $p \mid b$.

Example III.3.A. In the ring $\mathbb{Z}$, if p is "prime" then p and $-p$ are both irreducible and prime (in the sense of Definition III.3.3). In the ring $\mathbb{Z}_n$, where $n \equiv 2 \pmod 4$, $\overline{2}$ is prime but not irreducible since $\overline{2} = \overline{2}(\overline{n/2+1})$ but neither $\overline{2}$ nor $\overline{n/2+1}$ are units (since both are "even"). In Exercise III.3.3 you are asked to show that 2 is irreducible but not prime in the ring $\{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ (see III.3 Supplement: The Gaussian Integers for details). So the concepts of prime and irreducible can be very different in general. This is not the case in an integral domain, though (see parts (iii) and (iv) in the next result).

Theorem III.3.4. Let p and c be nonzero elements in an integral domain R.

(i) p is prime if and only if (p) is a nonzero prime ideal,

(ii) c is irreducible if and only if (c) is maximal in the set S of all proper principal ideals of R.

(iii) Every prime element of R is irreducible.

(iv) If R is a principal ideal domain, then p is prime if and only if p is irreducible.

(v) Every associate of an irreducible (respectively, prime) element of R is irreducible (respectively, prime).

(vi) The only divisors of an irreducible element of R are its associates and the units of R.

Notes. We have sort of reached the "mountain top of weirdness" in terms of abstract algebraic structures (in the humble opinion of your instructor). We now introduce a better behaved structure (in which the concepts of prime and irreducible are the same, for example). From this point on, we almost exclusively consider rings with this "unique factorization" behavior.

Definition III.3.5. An integral domain R is a *unique factorization domain* ("UFD") provided that:

(i) every nonzero nonunit element $a \in R$ can be written $a = c_1c_2 \cdots c_n$, with $c_1, c_2, \ldots, c_n$ irreducible, and

(ii) if $a = c_1c_2 \cdots c_n$ and $a = d_1d_2 \cdots d_m$ (where c_i, d_i are all irreducible), then $n = m$ and for some permutation σ of $\{1, 2, \ldots, n\}$, c_i and $d_{\sigma(i)}$ are associates for every i.

Note. Notice that every field is vacuously a unique factorization domain; "vacuously" because a field contains no nonzero nonunits.

Note. The integers are an example of a unique factorization domain (UFD) where the irreducibles are the usual prime numbers in $\mathbb{N}$ (and their negatives), the only units are 1 and -1, the associates are the pairs n and $-n$, and the uniqueness of part (ii) is given by the Fundamental Theorem of Arithmetic. See my online notes for Elementary Number Theory (MATH 3120) on Section 2. Unique Factorization, and notice Theorem 2.2. Also see my online notes for Mathematical Reasoning (MATH 3000) on Section 6.3. Divisibility: The Fundamental Theorem of Arithmetic and notice Theorem 6.29.

Note III.3.A. In the definition of UFD, part (ii) shows that for an irreducible we must have $m = n = 1$. So if c is irreducible and $c \mid ab$, then $cx = ab$ for some $x \in R$. So $a = c_1c_2 \cdots c_n$ and $b = d_1d_2 \cdots d_m$ for irreducible c_i, d_i by (i) of the definition and $ab = (c_1c_2 \cdots c_n)(d_1d_2 \cdots d_m)$. Since $ab = cx = c(x_1x_2 \cdots x_k)$ for some irreducible x_i, we have $k = n + m - 1$ and by (ii) c must be an associate of either some c_i (in which case $c \mid a$) or an associate of some d_i (in which case $c \mid b$). So c is prime. Also, by Theorem III.3.4(iii) every prime is irreducible. So <u>in a UFD irreducible and prime elements coincide</u>.

Note III.3.B. Let $R = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$. In Exercise III.3.4 it is to be shown that this is an integral domain (under the usual addition and multiplication) and that every element can be factored into a product of irreducibles (see III.3 Supplement: The Gaussian Integers for details). So (i) in the definition of UFD holds. However, it is shown that 2, 3, $4-\sqrt{10}$, and $4+\sqrt{10}$ are irreducibles and that neither 2 nor 3 is an associate of $4-\sqrt{10}$ or $4+\sqrt{10}$. Then $6 = 2\cdot 3 = (4-\sqrt{10})(4+\sqrt{10})$ is written as a product of of irreducibles in two different ways (in the sense of Definition 3.5(ii)). So there are integral domains which are not UFDs.

Note. The big result of this section is that every principal ideal domain ("PID") is a unique factorization domain ("UFD"). In this direction, we need the following preliminary result.

Lemma III.3.6. If R is a principal ideal ring and $(a_1) \subset (a_2) \subset \cdots$ is a chain of ideals in R, then for some positive integer n, $(a_j) = (a_n)$ for all $j \geq n$.

Theorem III.3.7. Every principal ideal domain R is a unique factorization domain. That is, "every PID is a UFD."

Note III.3.C. The converse of Theorem III.3.7 (i.e., "Every UFD is a PID") does not hold as established by the fact that $\mathbb{Z}[x]$ is a UFD (as shown in Theorem III.6.14) but $\mathbb{Z}[x]$ is not a PID (as shown in Exercise III.6.1).

Note. We now consider some "special" integral domains.

Definition III.3.8. Let R be a commutative. R is a *Euclidean ring* if there is a function $\varphi : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ such that:

(i) if $a, b \in R$ and $ab \neq 0$, then $\varphi(a) \leq \varphi(ab)$,

(ii) if $a, b \in R$ and $b \neq 0$, then there exist $q, r \in R$ such that either $a = qb + r$ with $r = 0$, or $r \neq 0$ and $\varphi(r) < \varphi(b)$.

A Euclidean ring which is an integral domain is called a *Euclidean domain*.

Note III.3.D. The ring $\mathbb{Z}$ with $\varphi(x) = |x|$ is a Euclidean domain (by the Division Algorithm, Theorem 0.6.3; also see my online notes on for Mathematical Reasoning on Section 6.3. Divisibility: The Fundamental Theorem of Arithmetic and notice Theorem 6.17). If F is a field, then the ring of polynomials $F[x]$ is a Euclidean domain with $\varphi(f) =$ degree of f (as shown in Corollary III.6.4).

Note III.3.E. Let $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Then $\mathbb{Z}[i]$ is an integral domain called the domain of *Gaussian integers*. Define $\varphi(a + bi) = a^2 + b^2$. Then $\mathbb{Z}[i]$ with φ is a Euclidean ring. See III.3 Supplement: The Gaussian Integers for details.

Theorem III.3.9. Every Euclidean ring R is a principal ideal ring with identity. Consequently every Euclidean domain is a unique factorization domain.

Note III.3.F. The converse of Theorem III.3.9 is false—that is, there is a PID that is not a Euclidean domain, as shown in Exercise III.3.8.

Definition III.3.10. Let X be a nonempty subset of a commutative ring R. An element $d \in R$ is a *greatest common divisor* of X provided:

(i) $d \mid a$ for all $a \in X$, and

(ii) $c \mid a$ for all $a \in X$ implies that $c \mid d$.

If R has an identity 1_R and $a_1, a_2, \ldots, a_n$ has 1_R as a greatest common divisor, then $a_1, a_2, \ldots, a_n$ are *relatively prime.*

Note. Greatest common divisors may not exist for a given set (even when it is a finite set) and when a set has a greatest common divisor, it may not be unique (though by part (ii) of Definition III.3.10, two greatest common divisors of a set must be associates). In fact, any associate of a greatest common divisor of a set is itself a greatest common divisor of the set.

Theorem III.3.11. Let $a_1, a_2, \ldots, a_n$ be elements of a commutative ring R with identity.

(i) $d \in R$ is a greatest common divisor of $\{a_1, a_2, \ldots, a_n\}$ such that $d = r_1a_1 + r_2a_2 + \cdots + r_na_n$ for some $r_i \in R$ if and only if $(d) = (a_1) + (a_2) + \cdots + (a_n)$.

(ii) If R is a principal ideal ring, then a greatest common divisor of $a_1, a_2, \ldots, a_n$ exists and every one is of the form $r_1a_1 + r_2a_2 + \cdots r_na_n$, where each $r_i \in R$.

(iii) If R is a unique factorization domain, then there exists a greatest common divisor of $a_1, a_2, \ldots, a_n$.

Revised: 3/22/2024