Chapter 4

Unique Factorization Domains (UFDs)

4.1 Unique Factorization Domains (UFDs)

Throughout this section R will denote an integral domain (i.e. a commutative ring with identity containing no zero-divisors). Recall that a *unit* of R is an element that has an inverse with respect to multiplication. If a is any element of R and u is a unit, we can write

$$a = u(u^{-1}a).$$

This is not considered to be a proper factorization of a. For example we do not consider $5 = 1(5)$ or $5 = (-1)(-5)$ to be proper factorizations of 5 in $\mathbb{Z}$. We do not consider

$$x^2 + 2 = 2\left(\frac{1}{2}x^2 + 1\right)$$

to be a proper factorization of $x^2 + 2$ in $\mathbb{Q}[x]$.

Definition 4.1.1 *An element a in an integral domain R is called* irreducible *if it is not zero or a unit, and if whenever a is written as the product of two elements of R, one of these is a unit.*

An element p of an integral domain R is called prime *if p is not zero or a unit, and whenever p divides ab for elements a, b of R, either p divides a or p divides b.*

Note

1. Elements r and s are called *associates* of each other if $s = ur$ for a unit u of R. So $a \in R$ is irreducible if it can only be factorized as the product of a unit and one of its own associates.

2. If R is an integral domain, every prime element of R is irreducible. To see this let $p \in R$ be prime and suppose that $p = rs$ is a factorisation of p in R. Then since p divides rs, either p divides r or $p|s$. There is no loss of generality in assuming p divides r. Then $r = pa$ for some element a of R, and $p = rs$ so $p = pas$. Then $p - pas = 0$ so $p(1 - as) = 0$ in R. Thus $as = 1$ since R is an integral domain and $p \neq 0$. Then s is a unit and $p = rs$ is not a proper factorisation of p. Hence p is irreducible in R.

   It is *not* true that every irreducible element of an integral domain must be prime, as we will shortly see.

Examples:

1. In $\mathbb{Z}$ the units are 1 and -1 and each non-zero non-unit element has two associates, namely itself and its negative. SO 5 and -5 are associates, 6 and -6 are associates, and so on. The irreducible elements of $\mathbb{Z}$ are p and $-p$, for p prime.

2. In $\mathbb{Q}[x]$, the units are the non-zero constant polynomials. The associates of a non-zero non-constant polynomial $f(x)$ are the polynomials of the form $af(x)$ where $a \in \mathbb{Q}^\times$. So x^2+2 is associate to $3x^2+6$, $\frac{1}{2}x^2+1$, etc.

3. In $\mathbb{Z}$ the irreducible elements are the integers p and $-p$ where p is a prime numbers. The prime elements of $\mathbb{Z}$ are exactly the irreducible elements - the prime numbers and their negatives.

Definition 4.1.2 *An integral domain R is a* unique factorization domain *if the following conditions hold for each element a of R that is neither zero nor a unit.*

1. *a can be written as the product of a finite number of irreducible elements of R.*

2. *This can be done in an essentially unique way. If $a = p_1p_2\dots p_r$ and $a = q_1q_2\dots q_s$ are two expressions for a as a product of irreducible elements, then $s = r$ and $q_1, \dots, q_s$ can be reordered so that for each i, q_i is an associate of p_i.*

Example 4.1.3 *$\mathbb{Z}$ is a UFD.*

(This is the Fundamental Theorem of Arithmetic).

Example 4.1.4 *Let $\mathbb{Z}[\sqrt{-5}$ denote the set of complex numbers of the form $a+b\sqrt{-5}$ where a and b are integers (and $\sqrt{-5}$ denotes the complex number $\sqrt{5}i$. We will show that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD (it is easily shown to be a ring under the usual addition and multiplication of complex numbers).*

Claim: $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.
The proof if this claim will involve a number of steps.

1. We define a function $\phi : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}_{\geq 0}$ by $\phi(\alpha) = \alpha\bar{\alpha}$ where $\bar{\alpha}$ denotes the complex conjugate of α. Thus

$$\phi(a+b\sqrt{-5}) = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2.$$

   Let $\alpha,\ \beta \in \mathbb{Z}\sqrt{-5}$. Then

$$\phi(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = \phi(\alpha)\phi(\beta).$$

   So ϕ is multiplicative.

2. Suppose α is a unit of $\mathbb{Z}[\sqrt{-5}]$ and let β be its inverse. Then $\phi(\alpha\beta) = \phi(1) = 1 = \phi(\alpha)\phi(\beta)$. Since $\phi(\alpha)$ and $\phi(\beta)$ are positive integers this means $\phi(\alpha) = 1$ and $\phi(\beta) = 1$. So $\phi(\alpha) = 1$ whenever α is a unit.

   On the other hand $\phi(a+b\sqrt{-5}) = 1$ implies $a^2+5b^2 = 1$ for integers a and b which means $b = 0$ and $a = \pm 1$. So the only units of $\mathbb{Z}[\sqrt{-5}]$ are 1 and -1.

3. Suppose $\phi(\alpha) = 9$ for some $\alpha \in \mathbb{Z}[\sqrt{-5}]$. If α is not irreducible in $\mathbb{Z}[\sqrt{-5}]$ then it factorizes as $\alpha_1\alpha_2$ where α_1 and α_2 are non-units. Then we must have

$$\phi(\alpha_1) = \phi(\alpha_2) = 3.$$

   Now this would means $3 = c^2+5d^2$ for integers c and d which is impossible. So if $\phi(\alpha) = 9$ then α is irreducible in $\mathbb{Z}[\sqrt{-5}]$.

4. Now $9 = 3 \times 3$ and $9 = (2+\sqrt{-5})(2-\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. The elements 3, $2+\sqrt{-5}$ and $2-\sqrt{-5}$ are all irreducible in $\mathbb{Z}[\sqrt{-5}]$ by item 3. above. Furthermore 3 is not an associate of either $2+\sqrt{-5}$ or $2-\sqrt{-5}$ as the only units in $\mathbb{Z}[\sqrt{-5}]$ are 1 and -1. We conclude that the factorizations of 9 above are genuinely different, and $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Note that 3 is an example of an element of $\mathbb{Z}[\sqrt{-5}]$ that is irreducible but not prime.
Remark: The ring $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$ *is* a UFD.

Theorem 4.1.5 *Let F be a field. Then the polynomial ring $F[x]$ is a UFD.*

Proof: We need to show that every non-zero non-unit in $F[x]$ can be written as a product of irreducible polynomials in a manner that is unique up to order and associates.

So let $f(x)$ be a polynomial of degree $n \geq 1$ in $F[x]$. If $f(x)$ is irreducible there is nothing to do. If not then $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ both have degree less than n. If $g(x)$ or $h(x)$ is reducible further factorization is possible; the process ends after at most n steps with an expression for $f(x)$ as a product of irreducibles.

To see the uniqueness, suppose that

$$\begin{aligned} f(x) &= p_1(x)p_2(x)\dots p_r(x) \text{ and} \\ f(x) &= q_1(x)q_2(x)\dots q_s(x) \end{aligned}$$

are two such expressions, with $s \geq r$. Then $q_1(x)q_2(x)\dots q_s(x)$ belongs to the ideal $\langle p_1(x)\rangle$ of $F[x]$. Since this ideal is prime (as $p_1(x)$ is irreducible) this means that either $q_1(x) \in \langle p_1(x)\rangle$ or $q_2(x)\dots q_s(x) \in \langle p_1(x)\rangle$. Repeating this step leads to the conclusion that at least one of the $q_i(x)$ belongs to $\langle p_1(x)\rangle$. After reordering the $q_i(x)$ if necessary we have $q_1(x) \in \langle p_1(x)\rangle$. Since $q_1(x)$ is irreducible this means $q_1(x) = u_1 p_1(x)$ for some unit u_1. Then

$$p_1(x)p_2(x)\dots p_r(x) = u_1 p_1(x)q_2(x)\dots q_s(x).$$

Since $F[x]$ is an integral domain we can cancel $p_1(x)$ from both sides to obtain

$$p_2(x)\dots p_r(x) = u_1 q_2(x)\dots q_s(x).$$

After repeating this step a further $r-1$ times we have

$$1 = u_1 u_2 \dots u_r q_{r+1}(x)\dots q_s(x),$$

where $u_1, \dots, u_r$ are units in $F[x]$ (i.e. non-zero elements of F). This means $s = r$, since the polynomial on the right in the above expression must have degree zero. We conclude that $q_1(x), \dots, q_s(x)$ are associates (in some order) of $p_1(x), \dots, p_r(x)$. This completes the proof. □