Chapter 4

Unique Factorization Domains

4.1 Lecture 15: 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 51. *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.

Notes

1. A non-zero non-unit element is prime if and only if the principal ideal that it generates is a prime ideal.

2. 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. If two elements are associates, they generate the same prinicipal ideal.

3. 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 see in Lecture 16.

4. In any commutative ring R, an element a is irreducible if and only if the principal ideal $\langle a \rangle$ is maximal among *prinicipal* ideals of R. This is becasue if $\langle a \rangle \subsetneq \langle b \rangle \subsetneq R$ for some $b \in R$, then b is a divisor of a that is neither an associate of a nor a unit. In the special case where R is a PID, it follows that $a \in R$ is irreducible if and only if $\langle a \rangle$ is a maximal ideal of R. Since every maximal ideal is prime, it follows that every irreducible element of a PID is a prime element.

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 a prime number.

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.

Definition 52. *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 $a = p_1 p_2 \dots p_r$ and $a = q_1 q_2 \dots q_s$ 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.*

Theorem 53. *(Fundamental Theorem of Arithmetic). $\mathbb{Z}$ is a UFD.*

Proof. Let n be a non-zero non-unit element of $\mathbb{Z}$ (we may assume that n is positive after replacing n with its associate $-n$ if necessary). There are two things to show: that n can be written as a product of irreducible elements, and that this can be done in a unique way.

For the first part, if n is irreducible then the statement holds. If not, then $n = rs$ for some positive integers r and s, both strictly less than n. This step can be repeated for r and s - each of them is either irreducible or the product of two strictly lesser positive integers. This factorization process cannot contiune indefinitely since the only possible factors are integers in the range 2 to n and they decrease at each step - so it ends with an description of n as a product of (positive) irreducible elements (prime numbers).

For the uniqueness, suppose that

$$n = p_1 \dots p_t = q_1 \dots q_s$$

are alternative expressions for n as products of irreducibles. Then p_1 divides the product $q_1 \dots q_s$. Since p_1 is irreducible and $\mathbb{Z}$ is a PID, p_1 is prime. So p_1 divides one of the q_j. After reordering we can assume $p_1 | q_1$, which means $p_1 = q_1$ since p_1 and q_1 are both irreducible. Since $\mathbb{Z}$ is an integral domain, we can cancel p_1 from both sides, leaving $p_2 \dots p_t = q_2 \dots q_s$. Continuing in this manner we deduce that all primes appear with the same multplicity in both expressions. □

Remark: In the first part of this proof, we made heavy use of the order relation in $\mathbb{Z}$ to argue that every non-zero non-unit integer is the product of finitely many irreducible elements. We don't have an order relation in every integral domain.
In the second part, we used the fact that $\mathbb{Z}$ is a PID to conclude that irreducible elements are prime. If we didn't know this, we could use the division algorithm/Euclidean algorithm in $\mathbb{Z}$.