1. Unique Factorisation and Applications

We review the notion of unique factorisation and give some applications of unique factorisation in the ring of integers.

1.1. **Factorisation in integral domains.**

We have studied this topic extensively in Algebra 2B. Here we review some important notions and results. In this lecture we always assume R is a commutative ring with 1, such that $0 \neq 1$. We say R is an *integral domain* if for $a, b \in R$ with $ab = 0$, we have either $a = 0$ or $b = 0$. We recall the definitions of Euclidean domains, principal ideal domains, unique factorisation domains, along with other relevant concepts and notations. (If you learned Algebra 2B in 2013, you have seen the mathematical content of these terminologies without knowing some of the names.)

Definition 1.1. Let R be an integral domain. A *Euclidean valuation* on R is a map

$$\nu : R\backslash\{0\} \to \{0, 1, 2, \cdots\}$$

such that if $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ with the property that $a = qb + r$ and either $r = 0$ or $\nu(r) < \nu(b)$. R is said to be a *Euclidean domain* if it has a Euclidean valuation.

Example 1.2. We recall some important examples of Euclidean domains

(1) The ring of integers $\mathbb{Z}$ is an Euclidean domain, with the absolute value function $\nu(n) = |n|$ being a Euclidean valuation.

(2) For $\Bbbk$ a field, the polynomial ring of a single variable $\Bbbk[x]$ is an Euclidean domain, with the degree function $\nu(f(x)) = \deg f(x)$ being a Euclidean valuation.

(3) The ring of Gaussian integers

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

is an integral domain as it is a subring of the field of complex numbers $\mathbb{C}$. The function

$$\nu(a + bi) = a^2 + b^2$$

provides a Euclidean valuation. See Exercise 1.4.

Definition 1.3. Let R be an integral domain. An ideal I of R is a *principal ideal* if $I = (a)$ for some $a \in R$. R is a *principal ideal domain (PID)* if every ideal of R is principal.

Remark 1.4. Notice that we use a slightly different notation from the one you used in Algebra 2B. Here $(a) = Ra$ is the ideal generated by $a \in R$.

Theorem 1.5. *Every Euclidean domain is a PID.*

Proof. See Theorem 2.5 (2013) or Theorem 3.10 (2014) in Algebra 2B. (The 2013 version only proves this result in special cases, but some minor changes would make it into a complete proof for arbitrary Euclidean domains, which is given in the 2014 version.) □

By Theorem 1.5, all examples discussed in Example 1.2 are PIDs.

Before proceeding we review some basic definitions.

Definition 1.6. Let R be an integral domain. If $a, b \in R$ with $b \neq 0$, we say that b *divides* a if $a = bc$ for some $c \in R$. We denote it by $b \mid a$. (Otherwise we write $b \nmid a$.) An element $u \in R$ is called a *unit* if u divides 1. Two elements $a, b \in R$ are said to be *associated* if $a = bu$ for some unit u.

Remark 1.7. We can restate everything in the language of ideals: $b \mid a$ iff $(a) \subset (b)$; $u \in R$ is a unit iff $(u) = R$; a and b are associates iff $(a) = (b)$. See Lemma 2.9 (2013) or Lemmas 3.15 and 3.16 (2014) in Algebra 2B.

Definition 1.8. Let R be an integral domain. A non-unit $p \in R$ is said to be *irreducible* if $a \mid p$ implies that a is either a unit or an associate of p. A non-unit $p \in R$ is said to be *prime* if $p \neq 0$ and $p \mid ab$ implies that $p \mid a$ or $p \mid b$.

Proposition 1.9. *We have*

1. *Let R be an integral domain. Then every prime element is irreducible.*
2. *Let R be a PID. Then every irreducible element is prime.*

Proof. For (1), see Proposition 2.10 (2013) or Proposition 3.19 (2014) in Algebra 2B. For (2), see Proposition 2.12 (2013) or Proposition 3.21 (2014). □

Clearly, for all examples discussed in Example 1.2, the two notions "prime" and "irreducible" agree, so we can use them interchangeably. For historical reasons we usually say "primes" in $\mathbb{Z}$ and "irreducible polynomials" in $\Bbbk[x]$.

We move on to the definition of unique factorisation domains.

Definition 1.10. An integral domain R is a *unique factorisation domain (UFD)* if the following conditions are satisfied:

1. Every non-zero non-unit element in R can be written as the product of finitely many irreducible elements in R;
2. Given two such factorisations, say $r_1 r_2 \cdots r_s = r'_1 r'_2 \cdots r'_t$, we have $s = t$, and after renumbering if necessary, each r'_i is an associate of r_i for $1 \leqslant i \leqslant s$.

Theorem 1.11. *Every PID is a UFD.*

Proof. See Theorem 2.14 (2013) or Theorem 3.26 (2014) in Algebra 2B. □

By Theorem 1.11, all examples discussed in Example 1.2 are UFDs.

Remark 1.12. Sometimes we prefer to eliminate the ambiguity of the factorisations coming from units. The relation of being associated is an equivalence relation which partitions irreducible elements into equivalence classes. From each equivalence class we pick a representative and denote the set of all representatives (one from each class) by S. For instance, in $\mathbb{Z}$ we can take the set of all positive primes (irreducibles and primes agree in $\mathbb{Z}$); in $\mathbb{k}[x]$ we can take the set of all monic (leading coefficient 1) irreducible polynomials. Then every non-zero element $a \in R$ can be written in the form

$$a = ur_1r_2\cdots r_s$$

where u is a unit and $r_1, \cdots, r_s \in S$. Moreover u is unique and $r_1, r_2, \cdots, r_s$ are unique up to renumbering.

Corollary 1.13 (Fundamental Theorem of Arithmetic)**.** *Every non-zero integer n admits a prime factorisation*

$$n = (-1)^{\epsilon} p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$$

where $\epsilon = 0$ or 1, s is a non-negative integer, $p_1, p_2, \cdots, p_s$ are distinct positive primes, $a_1, a_2, \cdots, a_s$ are positive integers. This factorisation is unique up to the order of factors.

Proof. We have seen that unique factorisation holds for $\mathbb{Z}$. By writing products of repeated factors as powers we get the desired form. □

Remark 1.14. Unique factorisation in the ring of integers has fundamental importance. However, unique factorisation fails for some other integral domains studied in number theory. Understanding why it fails and how to fix it, is an important topic in algebraic number theory. We will come back to this later.

The following famous result of Euclid is a nice application of the fundamental theorem of arithmetic. The proof is simple and clever.

Theorem 1.15. *There are infinitely many primes in $\mathbb{Z}$.*

Proof. It suffices to prove there are infinitely many positive primes in $\mathbb{Z}$. We prove by contradiction. Assume there are only finitely many positive primes. We can label all of them in increasing order $p_1, p_2, \cdots, p_n$. Let $N = p_1p_2\cdots p_n + 1$. Then N is greater than 1 and not divisible by any p_i, $i = 1, 2, \cdots, n$. On the other hand, N can be factored into product of primes and hence is divisible by some prime p, which is different from any p_i. Contradiction! □