MATH 433

Applied Algebra

Lecture 38:
Factorisation in general rings (continued).

Factorisation into irreducible elements

Let R be an **integral domain**, i.e., a commutative ring with the multiplicative identity element and no zero-divisors.

Any element of R that has a multiplicative inverse is called a **unit**. All units of R form a multiplicative group.

A non-zero, non-unit element of R is called **irreducible** if it cannot be represented as a product of two non-units.

The ring R is called a **factorisation ring** if every non-zero, non-unit element x can be expanded into a product $x = uq_1q_2 \dots q_k$, where u is a unit and each q_i is irreducible.

If x is an irreducible element and u is a unit, then $y = ux$ is irreducible as well (y is called an **associate** of x).

Suppose $x = uq_1q_2 \dots q_k$, where u is a unit and each q_i is irreducible. If $q'_1, q'_2, \dots, q'_k$ are associates of $q_1, q_2, \dots, q_k$, resp., then $x = u'q'_1q'_2 \dots q'_k$ for some unit u'.

Examples of factorisation rings:

- Integers $\mathbb{Z}$.

Units are 1 and -1. Irreducible elements are primes and negative primes. Factorisation into irreducibles is, up to a sign, the usual prime factorisation. It is unique up to rearranging the factors and changing their signs. For example, $-6 = (-1) \cdot 2 \cdot 3 = (-2) \cdot 3 = 2 \cdot (-3) = (-3) \cdot 2$.

- Polynomials $\mathbb{F}[x]$.

Units are all nonzero constants. Irreducible elements are exactly irreducible polynomials. Factorisation into irreducibles is unique up to rearranging the factors and multiplying them by constants.

Example of a non-factorisation ring:

- $\mathbb{Z} + x\mathbb{Q}[x]$: polynomials over $\mathbb{Q}$ with integer constant terms.

Factorisation into irreducibles is not possible for polynomials with zero constant term.

Integral norm

Let R be an integral domain. A function $N : R \setminus \{0\} \to \mathbb{Z}$ is called an **integral norm** on R if

- $N(xy) = N(x)N(y)$ for all $x, y \in R \setminus \{0\}$,
- $N(x) > 0$ for all $x \in R \setminus \{0\}$,
- $N(x) = 1$ if and only if x is a unit.

Theorem If R admits an integral norm N then it is a factorisation ring.

Proof: The proof is by strong induction on $n = N(x)$, where x is a non-unit. Assume that factorisation is possible for all non-units y with $N(y) < n$. If x is irreducible, we are done. Otherwise $x = yz$, where y and z are non-units. Then $N(y), N(z) > 1$ and $N(y)N(z) = n$, hence $N(y), N(z) < n$. By the inductive assumption, $y = uq_1q_2 \dots q_k$ and $z = u'q'_1q'_2 \dots q'_s$, where all q_i and q'_j are irreducible and u, u' are units. Then $x = (uu')q_1q_2 \dots q_kq'_1q'_2 \dots q'_s$, which completes the induction step.

Examples of integral norms

- Integers $\mathbb{Z}$.

$N(n) = |n|$.

- $\mathbb{F}[x]$: polynomials in a variable x over a field $\mathbb{F}$.

$N(p) = 2^{\deg(p)}$.

- Gaussian integers $\mathbb{Z}[\sqrt{-1}] = \{m + ni \in \mathbb{C} \mid m, n \in \mathbb{Z}\}$.

$N(m + ni) = (m + ni)(\overline{m + ni}) = m^2 + n^2$. If $N(m + ni) = 1$ then $(m + ni)^{-1} = m - ni \in \mathbb{Z}[\sqrt{-1}]$ so that $m + ni$ is a unit. Not every prime integer is irreducible in this ring. For example, $2 = (1 + i)(1 - i)$, $5 = (2 + i)(2 - i)$.

- $\mathbb{Z}[\sqrt{3}] = \{m + n\sqrt{3} \mid m, n \in \mathbb{Z}\}$.

$N(m + n\sqrt{3}) = |(m + n\sqrt{3})(m - n\sqrt{3})| = |m^2 - 3n^2|$.
It turns out that the map $\phi : \mathbb{Z}[\sqrt{3}] \to \mathbb{Z}[\sqrt{3}]$ defined by $\phi(m + n\sqrt{3}) = m - n\sqrt{3}$ for all $m, n \in \mathbb{Z}$ satisfies $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in \mathbb{Z}[\sqrt{3}]$.

Unique factorisation

Let R be a factorisation ring. We say that R is a **unique factorisation domain** if factorisation of any non-unit element of R into a product of irreducible elements is unique up to rearranging the factors and multiplying them by units.

A non-zero, non-unit element $x \in R$ is called **prime** if, whenever x divides a product yz of two non-zero elements, it actually divides one of the factors y and z.

Proposition Every prime element is irreducible.

Theorem A factorisation ring is a unique factorisation domain if and only if every irreducible element is prime.

Example of non-unique factorisation:

- $\mathbb{Z}[\sqrt{-5}] = \{m + ni\sqrt{5} \in \mathbb{C} \mid m, n \in \mathbb{Z}\}$.

Integral norm: $N(z) = z\overline{z}$, $N(m + ni\sqrt{5}) = m^2 + 5n^2$. The norm can never equal 2 or 3. Hence any element of norm 4, 6 or 9 is irreducible. Now $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$.

Euclidean rings

Let R be an integral domain. A function $E : R \setminus \{0\} \to \mathbb{Z}_+$ is called a **Euclidean function** on R if for any $x, y \in R \setminus \{0\}$ we have $x = qy + r$ for some $q, r \in R$ such that $r = 0$ or $E(r) < E(y)$.

In a Euclidean ring, division with remainder is well defined.

Many Euclidean rings admit a **multiplicative Euclidean function**, which is both a Euclidean function and an integral norm.

Theorem 1 Any Euclidean ring is a factorisation ring.

Theorem 2 In a Euclidean ring, any irreducible element is prime.

Corollary Any Euclidean ring is a unique factorisation domain.

Greatest common divisor

In a Euclidean ring R, any two non-zero elements $x, y \in R$ admit a **greatest common divisor** $\gcd(x, y)$, that is, a common divisor divisible by any other common divisor. $\gcd(x, y)$ is unique up to multiplication by a unit. It can be found by the Euclidean algorithm, which also leads to a representation $\gcd(x, y) = ax + by$, where $a, b \in R$.

Theorem In a Euclidean ring R, any irreducible element is prime.

Proof: Suppose $x \in R$ is an irreducible element that divides a product yz of two non-zero elements. We need to show that x divides one of the factors y and z.

Since x is irreducible, it follows that $\gcd(x, y) = 1$ or x. If $\gcd(x, y) = x$ then x divides y. If $\gcd(x, y) = 1$ then $1 = ax + by$ for some $a, b \in R$. Consequently, $z = (ax + by)z = (az)x + b(yz)$, which is divisible by x.