MATH 433

Applied Algebra

Lecture 36: Factorisation of polynomials (continued). Factorisation in general rings.

Unique factorisation of polynomials

Definition. A non-constant polynomial $f \in \mathbb{F}[x]$ over a field $\mathbb{F}$ is said to be **irreducible** over $\mathbb{F}$ if it cannot be written as $f = gh$, where $g, h \in \mathbb{F}[x]$, and $\deg(g), \deg(h) < \deg(f)$.

Irreducible polynomials are for multiplication of polynomials what prime numbers are for multiplication of integers.

Theorem Any polynomial $f \in \mathbb{F}[x]$ of positive degree admits a factorisation $f = p_1 p_2 \dots p_k$ into irreducible factors over $\mathbb{F}$. This factorisation is unique up to rearranging the factors and multiplying them by non-zero scalars.

Some facts and examples

- Any polynomial of degree 1 is irreducible.

- A polynomial $p(x) \in \mathbb{F}[x]$ is divisible by a polynomial of degree 1 if and only if it has a root.

Indeed, if $p(\alpha) = 0$ for some $\alpha \in \mathbb{F}$, then $p(x)$ is divisible by $x - \alpha$. Conversely, if $p(x)$ is divisible by $ax + b$ for some $a, b \in \mathbb{F}$, $a \neq 0$, then p has a root $-b/a$.

- A polynomial of degree 2 or 3 is irreducible if and only if it has no roots.

If such a polynomial splits into a product of two non-constant polynomials, then at least one of the factors is of degree 1.

- Polynomial $p(x) = (x^2 + 1)^2$ has no real roots, yet it is not irreducible over $\mathbb{R}$.

- Polynomial $p(x) = x^3 + x^2 - 5x + 2$ is irreducible over $\mathbb{Q}$.

We only need to check that $p(x)$ has no rational roots. Since all coefficients are integers and the leading coefficient is 1, possible rational roots are integer divisors of the constant term: ± 1 and ± 2. We check that $p(1) = -1$, $p(-1) = 7$, $p(2) = 9$ and $p(-2) = 8$.

- If a polynomial $p(x) \in \mathbb{R}[x]$ is irreducible over $\mathbb{R}$, then $\deg(p) = 1$ or 2.

Assume $\deg(p) > 1$. Then p has a complex root $\alpha = a + bi$ that is not real: $b \neq 0$. Complex conjugacy $\overline{r + si} = r - si$ commutes with arithmetic operations and preserves real numbers. Therefore $p(\overline{\alpha}) = \overline{p(\alpha)} = 0$ so that $\overline{\alpha}$ is another root of p. It follows that $p(x)$ is divisible by $(x - \alpha)(x - \overline{\alpha})$ $= x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha} = x^2 - 2ax + a^2 + b^2$, which is a real polynomial. Then $p(x)$ must be a scalar multiple of it.

Problem. Find all common roots of real polynomials $p(x) = x^4 + 2x^3 - x^2 - 2x + 1$ and $q(x) = x^4 + x^3 + x - 1$.

Common roots of p and q are exactly roots of their greatest common divisor $\gcd(p, q)$. We can find $\gcd(p, q)$ using the Euclidean algorithm.

First we divide p by q: $x^4 + 2x^3 - x^2 - 2x + 1 =$
$= (x^4 + x^3 + x - 1)(1) + x^3 - x^2 - 3x + 2.$

Next we divide q by the remainder $r_1(x) = x^3 - x^2 - 3x + 2$:
$x^4 + x^3 + x - 1 = (x^3 - x^2 - 3x + 2)(x + 2) + 5x^2 + 5x - 5.$

Next we divide r_1 by the remainder $r_2(x) = 5x^2 + 5x - 5$:
$x^3 - x^2 - 3x + 2 = (5x^2 + 5x - 5)(\frac{1}{5}x - \frac{2}{5}).$

Since r_2 divides r_1, it follows that

$$\gcd(p, q) = \gcd(q, r_1) = \gcd(r_1, r_2) = r_2.$$

The polynomial $r_2(x) = 5x^2 + 5x - 5$ has roots $(-1 - \sqrt{5})/2$ and $(-1 + \sqrt{5})/2$.

Unity and units

Let R be an **integral domain**, i.e., a commutative ring with the multiplicative identity element and no zero-divisors. The multiplicative identity, denoted 1, is also called the **unity** of R. Any element of R that has a multiplicative inverse is called a **unit**. All units of R form a multiplicative group.

Examples. • Integers $\mathbb{Z}$.

Units are 1 and -1.

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

Units are 1, -1, i, and $-i$.

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

Units are all nonzero constants.

- $\mathbb{F}[[x]]$: formal power series in x over a field $\mathbb{F}$.

Units are all formal power series with nonzero constant terms.

Irreducible elements and factorisation

Let R be an integral domain. 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 $x = q_1 q_2 \dots q_k$ of irreducible elements. Equivalently, $x = u q_1 q_2 \dots q_k$, where u is a unit and each q_i is irreducible.

Two non-zero elements $x, y \in R$ are called **associates** of each other if x divides y and y divides x. An equivalent condition is that $y = ux$ for some unit u. Any associate of a unit (non-unit, irreducible, resp.) element is also a unit (non-unit, irreducible, resp.).

Suppose $x = u q_1 q_2 \dots q_k$, 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 $x = u' q_1' q_2' \dots q_k'$ for some unit u'.

Examples of factorisation rings:

- Integers $\mathbb{Z}$.

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

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

Irreducible elements are exactly irreducible polynomials.

Example of a non-factorisation ring:

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

This is a subring of $\mathbb{Q}[x]$. Units are 1 and -1. Irreducible elements are of the form $\pm p$, where p is a prime number, or $\pm q(x)$, where $q(x)$ is an irreducible polynomial over $\mathbb{Q}$ with the constant term 1. No element with zero constant term is irreducible; for example, $x = 2 \cdot \frac{1}{2}x$.