Theorem
Let $K = \mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p$. Every non-constant polynomial in $K[x]$ has unique factorisation as a product of one or more irreducible polynomials.

gcd and lcm in K[x]

Definition: For $a(x), b(x) \in K[x]$, $d(x)$ is a greatest common divisor of $a(x), b(x)$ if

1. $d(x) \mid a(x)$, $d(x) \mid b(x)$, and
2. if $c(x) \mid a(x)$ and $c(x) \mid b(x)$ then $c(x) \mid d(x)$.

Theorem: Let $K = \mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p$. Then any two polynomials in $K[x]$ have gcd and lcm. $\gcd(a(x), b(x))$ is a polynomial of smallest degree of the form $a(x)u(x) + b(x)v(x)$.

Note: If $d(x)$ is a greatest common divisor of $a(x), b(x)$, then so is $kd(x)$ for all $k \neq 0$ in K.

Euclidean Algorithm in K[x]

For all $a(x), b(x), q(x), r(x) \in K[x]$, if $a(x) = b(x)q(x) + r(x)$ then $\gcd(a(x), b(x)) = \gcd(b(x), r(x))$.

The same methods for finding gcd and lcm apply as for **Z**.

Factor Theorem

Let $K = \mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z}_p$. For all $f(x) \in K[x]$ and for all $a \in K$,

$$f(a) = 0 \iff f(x) = (x - a)g(x)$$

for some $g(x) \in K[x]$.

Corollary (Remainder Theorem)

If $f(x)$ is divided by $x - a$, the remainder is $f(a)$.

Divisibility and Factorisation in K[x]

Let $K = \mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z}_p$. For $a(x), b(x) \in K[x]$, $a(x) \mid b(x)$ if $b(x) = a(x)q(x)$ for some $q(x) \in K[x]$.

Irreducible polynomials

$f(x) \in K[x]$ (non-constant) is *irreducible* if the only factors of $f(x)$ are trivial, i.e. of the form k or $kf(x)$, ($k \in K$).

MATHS 255 Class Notes

Polynomials

Let $K = \mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_n$. A *polynomial over* K is an expression of the form $a(x) = a_0 + a_1 x + \cdots a_n x^n$ with $n \geq 0$ in $\mathbf{Z}$ and $a_0, \cdots, a_n \in K$.

The set of all such polynomials is denoted $K[x]$.

Degree

The *degree* of $a(x)$ is the largest value of d such that $a_d \neq 0$, or $-\infty$ if all $a_i = 0$.

Addition:

$$\sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i .$$

Multiplication:

$$(\sum a_i x^i)(\sum b_i x^i) = \sum c_k x^k \quad \text{where} \quad c_k = \sum_{i=0}^{k} a_i b_{k-i} .$$

Division algorithm for polynomials

Let $K = \mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p$.
For each $a(x), b(x) \in K[x]$ with $b(x) \neq 0$, there exist unique $q(x), r(x) \in K[x]$ with
$\deg r(x) < \deg b(x)$ such that
$a(x) = b(x)q(x) + r(x)$.

Proof: Let $S = \{a(x) - b(x)n(x) : n(x) \in K[x]\}$.
Let $r(x)$ be a polynomial of smallest degree in *S*.
Proceed as in the proof of the division algorithm for **Z**,

Example: Find quotient and remainder when $3x^5 - 2x^4 + 4x^3 - 1$ is divided by $x^2 - 1$. ($K = \mathbf{Q}$)