Polynomial Rings

Sanhan M. S. Khasraw

Salahaddin University-Erbil
13th March, 2017

Polynomial Rings

Definition: Let R be a commutative ring with 1. The **polynomial ring** $R[x]$ in indeterminate x with coefficients from R is the set of all formal sums $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $n \geq 0$ and $a_i \in R$. That is,
$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0; n \geq 0; a_i \in R\}$.

Polynomial Rings

Definition: Let R be a commutative ring with 1. The **polynomial ring** $R[x]$ in indeterminate x with coefficients from R is the set of all formal sums $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with $n \geq 0$ and $a_i \in R$. That is,
$R[x] = \{a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0; n \geq 0; a_i \in R\}$.

In order to make a ring out of $R[x]$ we must be able to recognize when two elements in it are **equal**, we must be able to **add** and **multiply** elements of $R[x]$ so that the axioms defining a ring hold true for $R[x]$. This will be our initial goal.

Operations on $R[x]$

Definition: If $f(x) = a_0 + a_1x + ... + a_mx^m$ and $g(x) = b_0 + b_1x + ... + b_nx^n$ are in $R[x]$, then $f(x) = g(x)$ if and only if for every integer $i \geq 0, a_i = b_i$.

Definition: If $f(x) = a_0 + a_1x + ... + a_mx^m$ and $g(x) = b_0 + b_1x + ... + b_nx^n$ are in $R[x]$, then $f(x) = g(x)$ if and only if for every integer $i \geq 0, a_i = b_i$.

Thus, two polynomials are said to be equal if and only if their corresponding coefficients are equal.

Operations on $R[x]$

Definition: If $f(x) = a_0 + a_1x + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$ are both in $R[x]$, then $f(x) + g(x) = c_0 + c_1x + \cdots + c_tx^t$ where for each i, $c_i = a_i + b_i$.

Operations on $R[x]$

Definition: If $f(x) = a_0 + a_1x + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$ are both in $R[x]$, then $f(x) + g(x) = c_0 + c_1x + \cdots + c_tx^t$ where for each i, $c_i = a_i + b_i$.

In other words, add two polynomials by adding their coefficients and collecting terms. To add $1 + x$ and $3 - 2x + x^2$ we consider $1 + x$ as $1 + x + 0x^2$ and add, according to the recipe given in the definition, to obtain as their sum $4 - x + x^2$.

Operations on $R[x]$

The most complicated item to define for $R[x]$ is the multiplication.

Operations on $R[x]$

The most complicated item to define for $R[x]$ is the multiplication.

Definition: If $f(x) = a_0 + a_1x + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$, then

$$f(x)g(x) = c_0 + c_1x + \cdots + c_kx^k$$

where

$$c_t = a_tb_0 + a_{t-1}b_1 + a_{t-2}b_2 + \cdots + a_0b_t.$$

Operations on $R[x]$

The most complicated item to define for $R[x]$ is the multiplication.

Definition: If $f(x) = a_0 + a_1x + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$, then

$$f(x)g(x) = c_0 + c_1x + \cdots + c_kx^k$$

where

$$c_t = a_tb_0 + a_{t-1}b_1 + a_{t-2}b_2 + \cdots + a_0b_t.$$

This definition says nothing more than: multiply the two polynomials by multiplying out the symbols formally, use the relation $x^\alpha x^\beta = x^{\alpha+\beta}$ and collect terms.

Degree of Polynomials

Definition: If $f(x) = a_0 + a_1x + \cdots + a_nx^n \neq 0$ and $a_n \neq 0$, is in $R[x]$, then the **degree** of $f(x)$, written as $degf(x)$, is n.

That is, the degree of $f(x)$ is the largest integer i for which the ith coefficient of $f(x)$ is not 0.

Degree of Polynomials

Definition: If $f(x) = a_0 + a_1 x + \cdots + a_n x^n \neq 0$ and $a_n \neq 0$, is in $R[x]$, then the **degree** of $f(x)$, written as $degf(x)$, is n.

That is, the degree of $f(x)$ is the largest integer i for which the ith coefficient of $f(x)$ is not 0.

We say a polynomial is **constant** if its degree is 0.

Degree of Polynomials

Definition: If $f(x) = a_0 + a_1x + \cdots + a_nx^n \neq 0$ and $a_n \neq 0$, is in $R[x]$, then the **degree** of $f(x)$, written as $degf(x)$, is n.

That is, the degree of $f(x)$ is the largest integer i for which the ith coefficient of $f(x)$ is not 0.

We say a polynomial is **constant** if its degree is 0.

We say a polynomial is **monic** if $a_n = 1$.

Degree of Polynomials

Definition: If $f(x) = a_0 + a_1x + \cdots + a_nx^n \neq 0$ and $a_n \neq 0$, is in $R[x]$, then the **degree** of $f(x)$, written as $degf(x)$, is n.

That is, the degree of $f(x)$ is the largest integer i for which the ith coefficient of $f(x)$ is not 0.

We say a polynomial is **constant** if its degree is 0.

We say a polynomial is **monic** if $a_n = 1$.

We say a polynomial is **linear** if $n = 1$.

Degree of Polynomials

Definition: If $f(x) = a_0 + a_1x + \cdots + a_nx^n \neq 0$ and $a_n \neq 0$, is in $R[x]$, then the **degree** of $f(x)$, written as $degf(x)$, is n.

That is, the degree of $f(x)$ is the largest integer i for which the ith coefficient of $f(x)$ is not 0.

We say a polynomial is **constant** if its degree is 0.

We say a polynomial is **monic** if $a_n = 1$.

We say a polynomial is **linear** if $n = 1$.

We **do not** define the degree of the zero polynomial.

Degree of Polynomials

Remark: If $f(x)$ and $g(x)$ are two polynomials over a ring R, then
(1) $deg(f(x)+g(x)) \leq max\{degf(x), degg(x)\}$.
(2) $deg(f(x)\cdot g(x)) \leq degf(x)+degg(x)$.

Degree of Polynomials

Remark: If $f(x)$ and $g(x)$ are two polynomials over a ring R, then
(1) $deg(f(x)+g(x)) \leq max\{degf(x), degg(x)\}$.
(2) $deg(f(x) \cdot g(x)) \leq degf(x) + degg(x)$.

Example: Let $f(x) = 1 + 3x + 2x^5$ and $g(x) = x + 3x^2$ be two polynomials in $Z_6[x]$ for which $degf(x) = 5$ and $degg(x) = 2$.

Then $f(x) \cdot g(x) = x + 3x^3 + 2x^6$ has degree 6. Thus,
$degf(x) + degg(x) = 7 \neq deg(f(x) \cdot g(x)) = 6$.

Degree of Polynomials

Theorem: Let R be an integral domain and $f(x), g(x)$ be two nonzero elements of $R[x]$. Then

1. $deg(f(x) \cdot g(x)) = degf(x) + degg(x)$, and
2. either $f(x) + g(x) = 0$ or $deg(f(x) + g(x)) \leq max\{degf(x), degg(x)\}$.

Degree of Polynomials

Theorem: Let R be an integral domain and $f(x), g(x)$ be two nonzero elements of $R[x]$. Then

1. $deg(f(x) \cdot g(x)) = degf(x) + degg(x)$, and
2. either $f(x) + g(x) = 0$ or $deg(f(x) + g(x)) \leq max\{degf(x), degg(x)\}$.

Corollary: If the ring R is an integral domain, then so is $R[x]$.

Division Algorithm Theorem

Theorem(Division Algorithm): Let R be a commutative ring with 1 and $f(x), g(x) \neq 0$ be polynomials in $R[x]$, with the leading coefficient of $g(x)$ an invertible element. Then there exist unique polynomials $q(x), r(x) \in R[x]$ such that $f(x) = q(x) \cdot g(x) + r(x)$, where either $r(x) = 0$ or $deg r(x) < deg g(x)$.

Division Algorithm Theorem

Theorem(Division Algorithm): Let R be a commutative ring with 1 and $f(x), g(x) \neq 0$ be polynomials in $R[x]$, with the leading coefficient of $g(x)$ an invertible element. Then there exist unique polynomials $q(x), r(x) \in R[x]$ such that $f(x) = q(x) \cdot g(x) + r(x)$, where either $r(x) = 0$ or $degr(x) < degg(x)$.

Example: Let $f(x) = x^4 + 4x^3 + x^2 + 4x + 1, g(x) = x^2 + 2x + 1$ be polynomials in $Z_7[x]$. Then
$f(x) = x^4+4x^3+x^2+4x+1 = (x^2+2x+3)(x^2+2x+1)+(3x+5)$.

Definition: Let R be a commutative ring with 1 and r be an arbitrary element of R. For each polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$ in $R[x]$, we may define $f(r) = a_0 + a_1r + \cdots + a_nr^n$.
If $f(r) = 0$, we call the element r a **root** or **zero** of f(x).

Root of Polynomials

Definition: Let R be a commutative ring with 1 and r be an arbitrary element of R. For each polynomial
$f(x) = a_0 + a_1x + \cdots + a_nx^n$ in $R[x]$, we may define
$f(r) = a_0 + a_1r + \cdots + a_nr^n$.
If $f(r) = 0$, we call the element r a **root** or **zero** of f(x).

Example: In $Z_2[x]$, each of 1 and 0 is root of the polynomial $f(x) = x^2 + x$.

Factors

Definition: Let R be a commutative ring with 1. If $f(x)$ and $g(x) \neq 0$ are in $R[x]$, we say that $g(x)$ is a **factor** of $f(x)$ [or $g(x)$ *divides* $f(x)$] if there exists some polynomial $h(x) \in R[x]$ for which $f(x) = h(x) \cdot g(x)$.

Factors

Definition: Let R be a commutative ring with 1. If $f(x)$ and $g(x) \neq 0$ are in $R[x]$, we say that $g(x)$ is a **factor** of $f(x)$ [or $g(x)$ *divides* $f(x)$] if there exists some polynomial $h(x) \in R[x]$ for which $f(x) = h(x) \cdot g(x)$.

Example: If $f(x) \in \mathbb{Z}[x]$, where $f(x) = x^2 + 2x - 3 = (x - 1)(x + 3)$, then $(x - 1)$ is a factor of $f(x)$.

Remainder Theorem

Theorem(Remainder Theorem): Let R be a commutative ring with 1. If $f(x) \in R[x]$ and $a \in R$, then there is a unique polynomial $q(x) \in R[x]$ such that $f(x) = (x - a)q(x) + f(a)$.

Remainder Theorem

Theorem(Remainder Theorem): Let R be a commutative ring with 1. If $f(x) \in R[x]$ and $a \in R$, then there is a unique polynomial $q(x) \in R[x]$ such that $f(x) = (x - a)q(x) + f(a)$.

Corollary (Factorization Theorem): The polynomial $f(x) \in R[x]$ is divisible by $x - a$ if and only if a is a root of $f(x)$.

More about roots

Theorem: Let R be an integral domain and $f(x) \in R[x]$ be a nonzero polynomial of degree n. Then $f(x)$ has at most n distinct roots in R.

More about roots

Theorem: Let R be an integral domain and $f(x) \in R[x]$ be a nonzero polynomial of degree n. Then $f(x)$ has at most n distinct roots in R.

Example: consider the polynomial $x^p - x \in Z_p[x]$, where p is a prime.
Since the nonzero elements of Z_p form a cyclic group under multiplication of order $p-1$, we must have $a^{p-1} = 1$ or $a^p = a$ for every $0 \neq a \in Z_p$.
But the last equation clearly holds when $a = 0$, so that every element of Z_p is a root of the polynomial $x^p - x$.

More Examples

Remark: The theorem is not true if R is not an integral domain.

More Examples

Remark: The theorem is not true if R is not an integral domain.

For example, $R = Z_2 \times Z_2 = \{(0,0),(1,0),(0,1),(1,1)\}$. Then R has divisors of zero. Let $f(x) = x^2 + x \in R[x]$. Then every element in R is a root of $f(x)$.

More Examples

Remark: The theorem is not true if R is not an integral domain.

For example, $R = Z_2 \times Z_2 = \{(0,0),(1,0),(0,1),(1,1)\}$. Then R has divisors of zero. Let $f(x) = x^2 + x \in R[x]$. Then every element in R is a root of $f(x)$.

Example: Let the polynomial $f(x) = x^2 + 1$ be in $H[\mathbb{R}]$. Then i, j, k are roots for $f(x)$ in $H[\mathbb{R}]$.

More Examples

Remark: The theorem is not true if R is not an integral domain.

For example, $R = Z_2 \times Z_2 = \{(0,0),(1,0),(0,1),(1,1)\}$. Then R has divisors of zero. Let $f(x) = x^2 + x \in R[x]$. Then every element in R is a root of $f(x)$.

Example: Let the polynomial $f(x) = x^2 + 1$ be in $H[\mathbb{R}]$. Then i, j, k are roots for $f(x)$ in $H[\mathbb{R}]$.

In fact it has infinite roots in $H[\mathbb{R}]$.

More Theorems

Theorem: Let $\mathbb{C}$ be the field of complex numbers. If $f(x) \in \mathbb{C}[x]$ is a polynomial of positive degree, then $f(x)$ has at least one root in $\mathbb{C}$.

More Theorems

Theorem: Let $\mathbb{C}$ be the field of complex numbers. If $f(x) \in \mathbb{C}[x]$ is a polynomial of positive degree, then $f(x)$ has at least one root in $\mathbb{C}$.

Corollary: If $f(x) \in \mathbb{C}[x]$ is a polynomial of degree $n>0$, then $f(x)$ can be expressed in $\mathbb{C}[x]$ as a product of n (not necessarily distinct) linear factors.

More Theorems

Theorem: Let $\mathbb{C}$ be the field of complex numbers. If $f(x) \in \mathbb{C}[x]$ is a polynomial of positive degree, then $f(x)$ has at least one root in $\mathbb{C}$.

Corollary: If $f(x) \in \mathbb{C}[x]$ is a polynomial of degree $n>0$, then $f(x)$ can be expressed in $\mathbb{C}[x]$ as a product of n (not necessarily distinct) linear factors.

Remark: For any ring R, $R[x]$ is not a field. That is, no element of $R[x]$ which has positive degree can have a multiplicative inverse.

More Theorems

Theorem: Let $\mathbb{C}$ be the field of complex numbers. If $f(x) \in \mathbb{C}[x]$ is a polynomial of positive degree, then $f(x)$ has at least one root in $\mathbb{C}$.

Corollary: If $f(x) \in \mathbb{C}[x]$ is a polynomial of degree $n>0$, then $f(x)$ can be expressed in $\mathbb{C}[x]$ as a product of n (not necessarily distinct) linear factors.

Remark: For any ring R, $R[x]$ is not a field. That is, no element of $R[x]$ which has positive degree can have a multiplicative inverse.

Suppose $f(x) \in R[x]$ with $deg f(x)>0$. If $f(x) \cdot g(x) = 1$ for some $g(x) \in R[x]$, then
$0 = deg 1 = deg(f(x) \cdot g(x)) = deg f(x) + deg g(x) \neq 0$, a contradiction.

Principal Ideal Domain

Theorem: If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a principal ideal domain.

Principal Ideal Domain

Theorem: If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a principal ideal domain.

Corollary: A nontrivial ideal of $\mathbb{F}[x]$ is maximal if and only if it is a prime ideal.

Principal Ideal Domain

Theorem: If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a principal ideal domain.

Corollary: A nontrivial ideal of $\mathbb{F}[x]$ is maximal if and only if it is a prime ideal.

Definition: A nonconstant polynomial $f(x) \in \mathbb{F}[x]$ is said to be **irreducible** in $\mathbb{F}[x]$ if and only if $f(x)$ cannot be expressed as the product of two polynomials of positive degree. Otherwise, $f(x)$ is **reducible** in $\mathbb{F}[x]$.

Principal Ideal Domain

Theorem: If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a principal ideal domain.

Corollary: A nontrivial ideal of $\mathbb{F}[x]$ is maximal if and only if it is a prime ideal.

Definition: A nonconstant polynomial $f(x) \in \mathbb{F}[x]$ is said to be **irreducible** in $\mathbb{F}[x]$ if and only if $f(x)$ cannot be expressed as the product of two polynomials of positive degree. Otherwise, $f(x)$ is **reducible** in $\mathbb{F}[x]$.

Example: $f(x) = x^2 + 1$ is irreducible in $\mathbb{R}[x]$, but it is reducible in both $\mathbb{C}[x]$ and $Z_2[x]$.

Irreducibility

Example: Any linear polynomial $f(x) = ax + b, a \neq 0$, is irreducible in $\mathbb{F}[x]$.

Irreducibility

Example: Any linear polynomial $f(x) = ax + b, a \neq 0$, is irreducible in $\mathbb{F}[x]$.
Since the degree of a product of two nonzero polynomials is the sum of the degrees of the factors, it follows that a representation $ax + b = g(x) \cdot h(x)$ with $0 < deg g(x) < 1$, $0 < deg h(x) < 1$ is impossible. Thus, every reducible polynomial has degree at least 2.

Example: Any linear polynomial $f(x) = ax + b, a \neq 0$, is irreducible in $\mathbb{F}[x]$.
Since the degree of a product of two nonzero polynomials is the sum of the degrees of the factors, it follows that a representation $ax + b = g(x) \cdot h(x)$ with $0 < degg(x) < 1$, $0 < degh(x) < 1$ is impossible. Thus, every reducible polynomial has degree at least 2.

Remark: If $f(x)$ is a polynomial over $\mathbb{F}$ which has a root in $\mathbb{F}$, then $f(x)$ is reducible in $\mathbb{F}[x]$.

Irreducibility

Example: Any linear polynomial $f(x) = ax + b, a \neq 0$, is irreducible in $\mathbb{F}[x]$.
Since the degree of a product of two nonzero polynomials is the sum of the degrees of the factors, it follows that a representation $ax + b = g(x) \cdot h(x)$ with $0 < deg g(x) < 1$, $0 < deg h(x) < 1$ is impossible. Thus, every reducible polynomial has degree at least 2.

Remark: If $f(x)$ is a polynomial over $\mathbb{F}$ which has a root in $\mathbb{F}$, then $f(x)$ is reducible in $\mathbb{F}[x]$.

Theorem: Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$ be of degree 2 or 3. Then $f(x)$ is reducible in $\mathbb{F}[x]$ if and only if $f(x)$ has a root in $\mathbb{F}$.

Theorem: If $\mathbb{F}$ is a field, the following statements are equivalent:

1. $f(x)$ is an irreducible polynomial in $\mathbb{F}[x]$.
2. The principal ideal $(f(x))$ is a maximal(prime) ideal of $\mathbb{F}[x]$.
3. The quotient ring $\mathbb{F}[x]/(f(x))$ is a field.

Unique Factorization Theorem

Theorem: If $\mathbb{F}$ is a field, the following statements are equivalent:

1. $f(x)$ is an irreducible polynomial in $\mathbb{F}[x]$.
2. The principal ideal $(f(x))$ is a maximal(prime) ideal of $\mathbb{F}[x]$.
3. The quotient ring $\mathbb{F}[x]/(f(x))$ is a field.

Unique Factorization Theorem: Each polynomial $f(x) \in \mathbb{F}[x]$ of positive degree is the product of a nonzero element of $\mathbb{F}$ and irreducible monic polynomials of $\mathbb{F}[x]$.

Eisenstein Criterion

Theorem(Eisenstein Criterion): Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial in $\mathbb{Z}[x]$. Suppose that for some prime number p, $p \nmid a_n$, $p \mid a_0$, $p \mid a_1$, $\cdots$, $p \mid a_{n-1}$ and $p^2 \nmid a_0$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Theorem(Eisenstein Criterion): Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial in $\mathbb{Z}[x]$. Suppose that for some prime number p, $p \nmid a_n$, $p \mid a_0$, $p \mid a_1$, $\cdots$, $p \mid a_{n-1}$ and $p^2 \nmid a_0$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example: The polynomial $f(x) = 3 - 45x + 18x^2 + 2x^5$ is irreducible in $\mathbb{Q}[x]$.
If we take $p = 3$, then $3 \mid 3$, $3 \mid -45$, $3 \mid 18$, $3 \nmid 2$ and $3^2 \nmid 3$. By Eisenstein Criterion, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Theorem(Eisenstein Criterion): Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial in $\mathbb{Z}[x]$. Suppose that for some prime number p, $p \nmid a_n$, $p \mid a_0$, $p \mid a_1$, $\cdots$, $p \mid a_{n-1}$ and $p^2 \nmid a_0$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example: The polynomial $f(x) = 3 - 45x + 18x^2 + 2x^5$ is irreducible in $\mathbb{Q}[x]$.
If we take $p = 3$, then $3 \mid 3$, $3 \mid -45$, $3 \mid 18$, $3 \nmid 2$ and $3^2 \nmid 3$. By Eisenstein Criterion, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Remark: If the condition of Eisenstein Criterion is not satisfied in a polynomial, this does not mean that the polynomial is reducible.
For example: $f(x) = x^2 + 1$ in $\mathbb{Q}[x]$ is irreducible and the condition of Eisenstein Criterion is not satisfied.

More about irreducibility

Theorem: If $\frac{r}{s}$ is a root of the polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ in $\mathbb{Q}[x]$ in which $gcd(r, s) = 1$, then $r \mid a_0$ and $s \mid a_n$.

More about irreducibility

Theorem: If $\frac{r}{s}$ is a root of the polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ in $\mathbb{Q}[x]$ in which $gcd(r, s) = 1$, then $r \mid a_0$ and $s \mid a_n$.

Example: The polynomial $f(x) = x^4 + 2x^3 - 2$ has no roots in $\mathbb{Q}$. Let $\frac{r}{s}$ is a root of $f(x)$ with $gcd(r, s) = 1$, then by above theorem $r \mid -2$ and $s \mid 1$. Then we have four values for $\frac{r}{s}$, which are 1, -1, 2, -2. But none of them is a root of $f(x)$.

More about irreducibility

Theorem(Kronecker): If $f(x)$ is an irreducible polynomial in $\mathbb{F}[x]$, then there is an **extension field** of $\mathbb{F}$ in which $f(x)$ has a root.

The Use of GAP

To create, for example, the polynomial ring $P = Z_7[x]$:

gap> R:= Integers mod 7;

$GF(7)$

gap>P:= PolynomialRing(R);

$GF(7)$([x_1])

To create, for example, the polynomial ring $P = Z_7[x]$:
gap> R:= Integers mod 7;
$GF(7)$
gap>P:= PolynomialRing(R);
$GF(7)$([x_1])

Suppose we want to factor the polynomial $x^2 - 2 \in Z_7[x]$.
The command
gap> x:= X(R, "x");
x
creates the indeterminate x over the ring R.
gap> f:= x^2-2;
x^2+Z(7)^5
gap> Factors(f);
$[x + Z(7), x + Z(7)^4]$

The Use of GAP

To create, for example, the polynomial ring $P = Z_7[x]$:
gap> R:= Integers mod 7;
$GF(7)$
gap>P:= PolynomialRing(R);
$GF(7)$([x_1])

Suppose we want to factor the polynomial $x^2 - 2 \in Z_7[x]$.
The command
gap> x:= X(R, "x");
x
creates the indeterminate x over the ring R.
gap> f:= x^2-2;
x^2+Z(7)^5
gap> Factors(f);
$[x + Z(7), x + Z(7)^4]$
gap> IsIrreducible(f);
false

The Use of GAP

```
gap> R:= Rationals;
Rationals
```

The Use of GAP

gap> R:= Rationals;
Rationals

Suppose we want to factor the polynomial $z^2 - 2 \in \mathbb{Q}[x]$.
gap> z:= X(R, "z");
z
gap> f:= z^2-1;
z^2-1
gap> Factors(f);
$[z - 1, z + 1]$
gap> IsIrreducible(f);
false

Definition: Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{C}[x]$. The **height** $H(f)$ is defined to be the maximum of the magnitudes of its coefficients: $H(f) = max\{|a_i|\}$, $i = 0, 1, \cdots, n$.

Definition: Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{C}[x]$. The **height** $H(f)$ is defined to be the maximum of the magnitudes of its coefficients: $H(f) = max\{|a_i|\}$, $i = 0, 1, \cdots, n$.

Definition: Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{C}[x]$. The **length** $L(f)$ is similarly defined as the sum of the magnitudes of the coefficients: $L(f) = \sum_{i=0}^{n} |a_i|$.

Height and Length

Definition: Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{C}[x]$. The **height** $H(f)$ is defined to be the maximum of the magnitudes of its coefficients: $H(f) = max\{|a_i|\}$, $i = 0, 1, \cdots, n$.

Definition: Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{C}[x]$. The **length** $L(f)$ is similarly defined as the sum of the magnitudes of the coefficients: $L(f) = \sum_{i=0}^{n} |a_i|$.

Example: Let $f(x) = 1 + 2x^2 \in \mathbb{C}[x]$. Then $H(f) = 2$ and $L(f) = 3$.

Mahler Measure

Definition: Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{C}[x]$. The **Mahler measure** of $f(x) = \sum_{k=0}^{n} a_kx^k = a_n\prod_{k=1}^{n}(x-\alpha_k)$ is

$M(f) = |a_n|\prod_{k=1}^{n} max\{1, |\alpha_k|\}$.

Mahler Measure

Definition: Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{C}[x]$. The **Mahler measure** of $f(x) = \sum_{k=0}^{n} a_kx^k = a_n \prod_{k=1}^{n}(x - \alpha_k)$ is
$M(f) = |a_n| \prod_{k=1}^{n} max\{1, |\alpha_k|\}$.

Example: Let $f(x) = 1 + 2x^2 \in \mathbb{C}[x]$. Then
$f(x) = 2(x - \frac{i}{\sqrt{2}})(x + \frac{i}{\sqrt{2}})$. So, $M(f) = 2 \times 1 \times 1 = 2$.

Definition: Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{C}[x]$. The **Mahler measure** of $f(x) = \sum_{k=0}^{n} a_kx^k = a_n \prod_{k=1}^{n}(x - \alpha_k)$ is
$M(f) = |a_n| \prod_{k=1}^{n} max\{1, |\alpha_k|\}$.

Example: Let $f(x) = 1 + 2x^2 \in \mathbb{C}[x]$. Then
$f(x) = 2(x - \frac{i}{\sqrt{2}})(x + \frac{i}{\sqrt{2}})$. So, $M(f) = 2 \times 1 \times 1 = 2$.

Remark:
$\binom{n}{\lfloor \frac{n}{2} \rfloor} H(f) \leq M(f) \leq H(f)\sqrt{n+1}$;
$L(f) \leq 2^n M(f) \leq 2^n L(f)$;
$H(f) \leq L(f) \leq nH(f)$.

Definition: The **detour distance** $D(u, v)$ between two distinct vertices u and v in a connected graph Γ is the length of a longest $u - v$ path in Γ.

Definition: The **detour distance** $D(u, v)$ between two distinct vertices u and v in a connected graph Γ is the length of a longest $u - v$ path in Γ.

Definition: The **detour polynomial** of Γ is defined by $D(\Gamma; x) = \sum_{\{u,v\}} x^{D(u,v)}$.

Definition: The **detour distance** $D(u, v)$ between two distinct vertices u and v in a connected graph Γ is the length of a longest $u - v$ path in Γ.

Definition: The **detour polynomial** of Γ is defined by $D(\Gamma; x) = \sum_{\{u,v\}} x^{D(u,v)}$.

Example: Ladder.

Definition: The **detour distance** $D(u, v)$ between two distinct vertices u and v in a connected graph Γ is the length of a longest $u - v$ path in Γ.

Definition: The **detour polynomial** of Γ is defined by $D(\Gamma; x) = \sum_{\{u,v\}} x^{D(u,v)}$.

Example: Ladder.

Example: Connect to group theory. Take S_3 as an example and associate a commuting graph with it

Thanks for your attention