IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

Definition:

Let F be a field and $f(x) \in F[x]$ is of degree ≥ 2. We call $f(x)$ is reducible over F if there exist $g(x), h(x) \in F[x]$ such that $f(x) = g(x)\, h(x)$.

where $deg\, g(x)$ and $deg\ h(x)$ are greater than or equal to 1.

i.e., $deg\, g(x) \geq 1$ and $deg\, h(x) \geq 1$.

If $f(x)$ is not reducible, then we call it irreducible (or prime) over F.

Theorem: Reducibility test

Let F be a field and $f(x) \in F[x]$.

Then (i) If $f(x)$ is of degree 1, then $f(x)$ is irreducible.

(ii) *If* $f(x)$ is of degree 2 or 3, then $f(x)$ is reducible iff $f(x)$ has a root F.

Proof:

(i) Let $f(x) = ax + b, a \neq 0$ in $F[x]$.

Suppose $f(x)$ is reducible, then there exist $g(x), h(x) \in F[x]$ such that

$$f(x) = g(x)\, h(x).$$

Where $1 \leq \deg g(x) < \deg f(x)$ and $1 \leq \deg h(x) < \deg f(x)$

therefore $ax + b = g(x)\, h(x)$

therefore $\deg(ax + b) = \deg g(x) + deg\ h(x)$

$\Rightarrow \quad 1 = \deg\ g(x) + deg\ h(x)$

This is impossible, since $\deg g(x) + deg\ h(x) \geq 2$

Therefore $f(x)$ is irreducible over F.

(ii) Let $f(x) \in F[x]$ be of degree 2 or 3

Suppose $f(x)$ is reducible over F, then $f(x) = g(x)\, h(x)$ for some $g(x), h(x) \in F[x]$,

Where $1 \leq \deg g(x) < \deg f(x)$ and $1 \leq \deg h(x) < \deg f(x)$

Since $deg f(x) = \deg g(x) + deg\ h(x)$ and $deg f(x) = 2$ or 3,

we have $\deg g(x) + deg\ h(x) = 2$ or 3

Therefore one of $g(x)$ and $h(x)$ has degree 1.

Let $\deg g(x) = 1 \Rightarrow g(x) = ax + b, \quad a \neq 0$.

Now $-a^{-1} \in F$ and $g(-a^{-1}b) = a(-a^{-1}b) + b$

$$= -(a.a^{-1})b + b$$
$$= -(1.b) + b$$
$$= -b + b$$
$$= 0$$

Therefore $-a^{-1}b$ is a root of $g(x)$

Hence $-a^{-1}b$ is a root of $f(x)$ in F

So, $f(x)$ has a root in F.

Conversely, let $f(x)$ have a root $a \in F$.

Then $(\mathrm{x} - \mathrm{a})$ is a factor of $f(x)$.

Therefore $f(x) = (x - a)\, g(x), \quad g(x) \in F[x]$.

Hence $f(x)$ is reducible over F.

Example 1:

Test whether the polynomial $f(x) = 2x^2 + 4$ is irreducible over Z, Q , R & C.

Solution:

Given, $f(x) = 2x^2 + 4$

$$f(x) = 0 \Rightarrow 2x^2 + 4 = 0$$
$$\Rightarrow x^2 + 2 = 0$$
$$\Rightarrow x^2 = -2$$
$$\Rightarrow x = \pm i\sqrt{2}$$

Therefore the roots do not belong to Z, Q and R

Hence $f(x) = 2x^2 + 4$ is irreducible over Z, Q and R

But the roots $i\sqrt{2}$ and $-i\sqrt{2}$ belong to C

Hence $f(x) = 2x^2 + 4$ is reducible over C.

Example 2:

Let $f(x) = x^3 + x^2 + x + 1 \in Z_2[x]$ is it irreducible or irreducible? If reducible find the other factor.

Solution:

Given $f(x) = x^3 + x^2 + x + 1 \in Z_2[x]$

and $Z_2 = \{0\,,1\}$

Now $f(0) = 1 \neq 0$

$f(1) = 4 \equiv 0 \quad (\text{mod } 2)$

Therefore 1 is a root in Z_2

Hence $x - 1$ is a factor of $f(x)$ in $Z_2[x]$

Therefore $f(x)$ is reducible

By division algorithm $\exists\ q(x), r(x) \in Z_2[x]$

Such that,

$$x^3 + x^2 + x + 1 = (x^2 + 1)(x - 1) + 0$$

Hence $x^3 + x^2 + x + 1 = (x^2 + 1)(x - 1)$.

Example 3:

Test the polynomial $f(x) = x^2 + x + 4$ in $Z_7[x]$ is irreducible over Z_7.

Solution:

Given $f(x) = x^2 + x + 4$

and $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

We search for an element $a \in Z_7 \ni f(a) = 0$

$$f(0) = 4 \neq 0$$

$$f(1) = 6 \neq 0$$

$$f(2) = 10 \equiv 3(mod\ 7) \neq 0$$

$$f(3) = 16 \equiv 2(mod\ 7) \neq 0$$

$$f(4) = 24 \equiv 3(mod\ 7) \neq 0$$

$$f(5) = 34 \equiv 6(mod\ 7) \neq 0$$

$$f(6) = 46 \equiv 4(mod\ 7) \neq 0$$

Therefore there is no root for $f(x)$ in Z_7

Hence $f(x)$ is irreducible over Z_7.

GREATEST COMMON DIVISOR

Definition: (Greatest Common Divisor)

Let F be a field and $f(x), g(x) \in F[x]$. A Greatest Common Divisor of $f(x)\ and\ g(x)$ is a non-zero polynomial $d(x)$ such that $(i)\ d(x)\ divides\ f(x)\ and\ g(x)\ (ii)\ c(x)$ is a divisor of $f(x)\ and\ g(x)$ then $c(x)\ divides\ d(x)$.

Theorem 1: Let F be a field and $f(x), g(x) \in F[x]$ with at least one of them is non-zero polynomial. Then their GCD $d(x)$ can be expressed as $d(x) = a(x)f(x) + b(x)g(x)$, for some $a(x), b(x) \in F[x]$.

Proof:

$Let\ S = \{s(x)f(x) + t(x)g(x) : s(x), t(x) \in F[x]\}$

Then $S \neq \emptyset, since\ f(x) \in S$.

Let $d(x)$ be a polynomial of least degree in S.

Then $d(x) = a(x)f(x) + b(x)g(x)$, for some $a(x), b(x) \in F[x]$. --------(1)

First we prove that $d(x)$ is the g.c.d of $f(x)\ and\ g(x)$

Now consider $f(x), d(x)$

By division algorithm, there exists $q(x)\ and\ r(x)$ such that

$f(x) = q(x)d(x) + r(x)$ --------(2)

Where either $r(x) = 0\ (or) \deg r(x) < \deg d(x)$

$\therefore r(x) = f(x) - q(x)d(x)$

$= f(x) - q(x)[a(x)f(x) + b(x)g(x)]$

$= [1 - q(x)a(x)]f(x) - q(x)b(x)g(x)$

$= [1 - q(x)a(x)]f(x) + [[-q(x)b(x)]g(x)]$

This is of the form $s(x)f(x) + r(x)g(x)$

$\therefore r(x) \in S$

$If\ r(x) \neq 0, then \deg r(x) < \deg d(x)$, which contradicts the choice of $d(x)$.

$\therefore r(x) = 0 \Rightarrow f(x) = q(x)d(x)$ (using (2))

$\therefore d(x)\ divides\ f(x)$.

Similarly, we can prove that $d(x)\ divides\ g(x)$.

Suppose $c(x)\ divides\ f(x)\ and\ g(x)\ then\ c(x)\ divides\ a(x)f(x)\ and\ b(x)g(x)$.

Hence $c(x)\ divides\ a(x)f(x) + b(x)g(x)$.

$\Rightarrow c(x)\ divides\ d(x)$
(using (1))

$\therefore d(x)\ is\ the\ \text{gcd}\ of\ f(x)\ and\ g(x)$

Note: Suppose $d(x)$ is Monic then it will be unique

$Suppose\ d(x) = a_0 + a_1x + a_2x^2 + \cdots \dots . + a_nx^n, a_n \neq 0$

$Then\ a_n^{-1}d(x) = a_n^{-1}a_0 + a_n^{-1}a_1x + a_n^{-1}a_2x^2 + \cdots \dots . + a_n^{-1}a_nx^n$

$= b_0 + b_1x + b_2x^2 + \cdots \dots . + x^n$ is a Monic polynomial.

$and\ a_n^{-1}d(x)$ is also a gcd of $f(x)\ and\ g(x)$.

Suppose $d_1(x)\ and\ d_2(x)$ be two monic polynomials which are the gcd's of $f(x)\ and\ g(x)$

$Then\ d_1(x)\ divides\ d_2(x)$
(treating $d_2(x)$ as gcd)

$and\ d_2(x)\ divides\ d_1(x)$
(treating $d_1(x)$ as gcd)

$\therefore d_1(x) = u\ d_2(x)\ for\ some\ u \neq 0\ in\ F$

Since both $d_1(x)\ and\ d_2(x)$ are monic polynomials by using equality of polynomial and by equating the leading coefficient's, we get $u = 1$

$\therefore d_1(x) = d_2(x)$

Hence the gcd is unique, when it is monic.

Definition:

If the gcd of $f(x)\ and\ g(x) \in F\ is\ 1, then\ f(x)\ and\ g(x)$ are called relatively prime.

$If\ f(x)\ and\ g(x)$ are relatively prime in $F[x]$, then there exists polynomials $a(x)\ and\ b(x)\ in\ F[x]$ such that $a(x)f(x) + g(x)\ b(x) = 1$.

Theorem 2: Let F be a field and $f(x), g(x) \in F[x]$, where $g(x) \neq 0\ and\ \deg r(x) \leq \deg d(x)$.

Applying the division algorithm, we write

$f(x) = q_1(x)g(x) + r_1(x), \quad \deg r_1(x) < \deg g(x)$

$g(x) = q_2(x)r_1(x) + r_2(x), \quad \deg r_2(x) < \deg r_1(x)$

$r_1(x) = q_3(x)r_2(x) + r_3(x), \quad \deg r_3(x) < \deg r_2(x)$

.

.

.

.

$r_{n-2}(x) = q_n(x)r_{n-1}(x) + r_n(x),\ \deg r_n(x) < \deg r_{n-1}(x)$

$r_{n-1}(x) = q_{n+1}(x)r_n(x) + r_{n+1}(x),\ r_{n+1}(x) = 0$

Then $r_n(x)$ is the lasts non-zero remainder.

It can be seen that $r_n(x)$ *is the* gcd *of* $f(x)$ *and* $g(x)$.

Example 1: Find the gcd of $x^4 + x^3 + 2x^2 + x + 1$ *and* $x^3 - 1$ *over* Q.

Solution:

Let $f(x) = x^4 + x^3 + 2x^2 + x + 1$ *and* $g(x) = x^3 - 1$

And $\deg g(x) < \deg f(x)$

Divide $f(x)$ *by* $g(x)$ by division algorithm successively.

$\therefore f(x) = (x+1)(x^3 - 1) + 2(x^2 + x + 1),\ \deg(2x^2 + 2x + 2) < \deg(x^3 - 1).$

$x^3 - 1 = \left(\frac{x}{2} - \frac{1}{2}\right)(2x^2 + 2x + 2) + 0$

$= (x-1)(x^2 + x + 1)$

$\therefore$ The last non-zero remainder is $(x^2 + x + 1)$

$\therefore f(x) = (x+1)(x-1)(x^2 + x + 1) + (x^2 + x + 1)$

$= (x^2 + x + 1)\big((x+1)(x-1) + 1\big)$

$\therefore$ The gcd of $f(x)$ *and* $g(x)$ *is* $(x^2 + x + 1)$.

$$
\begin{array}{r|l}
 & x+1 \\
\hline
x^3 - 1 & x^4 + x^3 + 2x^2 + x + 1 \\
 & x^4 - x \\
\hline
 & x^3 + 2x^2 + 2x + 1 \\
 & x^3 - 1 \\
\hline
 & 2x^2 + 2x + 2
\end{array}
\qquad
\begin{array}{r|l}
 & \frac{1}{2}x - \frac{1}{2} \\
\hline
2x^2 + 2x + 2 & x^3 - 1 \\
 & x^3 + x^2 + x \\
\hline
 & -x^2 - x - 1 \\
 & -x^2 - x - 1 \\
\hline
 & 0
\end{array}
$$

View more GCD examples on YouTube:

https://youtu.be/82nmtNxPaXE

https://youtu.be/q9lKz-cicWI

CHARACTERISTIC OF A RING

Definition: The characteristic of a ring R is the least positive integer n such that $n.a = 0$ for all $a \in R$ and is denoted by $Char(R) = n$. If no such positive integer exists, then R is said to have characteristic 0.

Examples:

- The ring $(Z_3, +, .)$ has characteristic 3.
- The ring $(Z_4, +, .)$ has characteristic 4.
- The ring $(Z, +, .)$ and $(Q, +, .)$ both have characteristic 0.
- The characteristic of a field $(F, +, .)$ is either 0 or a prime number.
- The characteristic of a finite field is a prime number p.

Theorem : The characteristic of a field $(F, +, .)$ is either 0 or a prime number

Proof: Let $(F, +, .)$ be a field.

If $Char(F) = 0$, then there is nothing to prove.

If $Char(F) \neq 0$, then let $Char(F) = n$.

To prove n is prime.

Suppose n is not a prime, then $n = pq$, where $1 < p < n, 1 < q < n$.

i.e p and q are proper factors of n.

Since $Char(F) = n$, we have $na = 0 \ \forall\, a \in F$.

Take $a = 1$, then $n.1 = 0$.(1 is the identity of F)

$\Rightarrow \ (pq).1 = 0 \Rightarrow (p.1)(q.1) = 0$

$$[\because (pq).1 = \underbrace{1 + 1 + \ldots + 1}_{\text{pqterms}} = \underbrace{(1 + 1 + \cdots + 1)}_{\text{pterms}} \underbrace{(1 + 1 + \cdots + 1)}_{\text{qterms}}]$$

Since F is a field, F is an integral domain and so, it has no divisor of zero,

$\therefore$ either $p.1 = 0$ or $q.1 = 0$.

Since p and q are less than n, it contradicts the definition of chararcterics of F.

$\therefore n$ is a prime number.

Note:

1. The characteristic of a ring need not be a prime. For example $Char(Z_6) = 6$, which is not a prime.
2. The characteristic of a finite field is a prime number P.