Irreducible polynomials: Finite Fields.

Reducible and Irreducible:

A polynomial $f(x) \in F[x]$, where F is a field of degree ≥ 2 is reducible over F, If there exist $g(x), h(x) \in F[x]$, each of degree ≥ 1 such that $f(x) = g(x)h(x)$. If $f(x)$ is not reducible, it is called irreducible (or) prime. $f(x) = x^2 - 1 = \pm 1 \geq 1$

$f(x) = (x+1)(x-1)$
$= g(x)\, h(x) \geq 1$

Theorem: 1

a) Every non-zero polynomial in $F[x]$ of degree ≤ 1 is irreducible.

b) If $f(x) \in F[x]$ with degree 2 or 3, then $f(x)$ is reducible iff $f(x)$ has a root in the field $F[x]$.

Proof:

a) For a polynomial to be reducible it should be of degree ≥ 2. Therefore, every non-zero polynomial of degree ≤ 1 is irreducible.

b) Assume that $f(x)$ is reducible.

Since $f(x)$ is of degree 2 or 3, one of the factors of $f(x)$ is of degree 1,

say $ax+b$ with $a, b \in F$ and $a \neq 0$. $ax+b = 0$, $ax = -b$, $x = -a^{-1}b$.

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

Conversely, assume that $f(x)$ has a root $\alpha \in F$.

Then $x - \alpha$ is a factor of $f(x)$.

$\therefore$ there exists a polynomial $g(x)$ in $F[x]$,

such that $f(x) = (x-\alpha)\, g(x)$.

Hence, $f(x)$ is reducible.

Examples:

1. x^2+1 is irreducible in $\mathbb{Q}[x]$ and $\mathbb{R}[x]$; but it is reducible in $\mathbb{C}[x]$, since $(x^2+1) = (x+i)(x-i)$ where $x-i$ and $x+i$ are in $\mathbb{C}[x]$.

2. $x^4+2x^2+1 \in \mathbb{R}[x]$ has no real roots; but it is reducible over $\mathbb{R}$, since $x^4+2x^2+1 = (x^2+1)(x^2+1)$.

3. $f(x) = x^3+x^2+x+1$ is reducible over $\mathbb{Z}_2$ because $f(0) = 1 \neq 0$, $f(1) = 1+1+1+1 = 0$ and $g(x) = x^2+x+1$ is irreducible over $\mathbb{Z}_2$ because $g(0)=1$ and $g(1) = 3 = 1$.

4. Let $h(x) = x^4+x^3+x^2+x+1$. Then $h(0)=1$ and $h(1) = 5 = 1$. Therefore, $h(x)$ has no first degree factors in $\mathbb{Z}_2[x]$.

Solution:

Given: $x^4+x^3+x^2+x+1 = (x^2+ax+b)(x^2+cx+d)$;

$a, b, c, d \in \mathbb{Z}_2$.

Then $a+c=1$, $ac+b+d=1$, $bc+ad=1$ and $bd=1$.

$bd=1$, $b, d \in \mathbb{Z}_2 \Rightarrow b=1$, $d=1$.

$\therefore ac+1+1 = 1 \Rightarrow ac = -1 = 1 \Rightarrow a=1$, $c=1$.

This contradicts, $a+c=1$, since $1+1=1$ (or) $0=1$.

Hence $h(x)$ has no quadratic factors. $\therefore h(x)$ is irreducible over $\mathbb{Z}_2$.

Theorem: 2 Euclidean Algorithm for polynomials

Let $f(x), g(x) \in F[x]$ with degree $f(x) \leq$ degree $g(x)$, and $f(x) \neq 0$. Then by division algorithm,

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

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

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

$$\vdots \qquad\qquad \vdots$$

$$r_{k-2}(x) = q_k(x) r_{k-1}(x) + r_k(x), \quad \deg r_k(x) < \deg r_{k-1}(x).$$

$$r_{k-1}(x) = q_{k+1}(x) r_k(x) + r_{k+1}(x), \quad r_{k+1}(x) = 0.$$

Then $r_k(x)$, the last non-zero remainder, is a gcd of $f(x)$ and $g(x)$ and is a constant multiple of the monic gcd of $f(x)$ and $g(x)$.

Theorem: 3.

Let $S(x) \in F[x]$, $S(x) \neq 0$. Define relation $\mathcal{R}$ on $F[x]$ by $f(x) \mathcal{R} g(x) \Leftrightarrow S(x)$ divides $f(x) - g(x)$. Then $\mathcal{R}$ is an equivalence relation on $F[x]$.

Proof:

Reflexive: $f(x) - f(x)$ divisible by $S(x)$.

$\Rightarrow f(x) \mathcal{R} f(x), \ \forall f(x) \in F[x]$.

Symmetry:

$f(x) \mathcal{R} g(x) \Rightarrow S(x)$ divides $f(x) - g(x)$

$\Rightarrow S(x)$ divides $g(x) - f(x)$

$\Rightarrow g(x) \mathcal{R} f(x)$.

Transitive:

$f(x) \mathcal{R} g(x)$ and $g(x) \mathcal{R} r(x)$.

$\Rightarrow f(x) - g(x) = q_1(x) s(x)$ and $g(x) - r(x) = q_2(x) s(x)$

$\Rightarrow f(x) - g(x) + g(x) - r(x) = [q_1(x) + q_2(x)] s(x)$.

$\Rightarrow f(x) \mathcal{R} r(x)$. Hence $\mathcal{R}$ is an equivalence relation.

THEOREM: 4

Let $s(x)$ be a non-zero polynomial in $F[x]$.

a) The equivalence classes of $F[x]$ for the relation of congruence modulo $s(x)$ from a commutative ring with unity under the closed binary operations.

$$[f(x)] + [g(x)] = [f(x) + g(x)]$$

and $[f(x)] \cdot [g(x)] = [f(x)\, g(x)] = [r(x)]$.

where $r(x)$ is the remainder obtained when $f(x)\, g(x)$ is divided by $s(x)$.

This ring is denoted by $\frac{F[x]}{(s(x))}$

b) If $s(x)$ is irreducible in $F[x]$,

Then $\frac{F[x]}{(s(x))}$ is a field.

c) If $|F| = q$ and $\deg s(x) = n$, then $\left|\frac{F[x]}{(s(x))}\right| = q^n$.

Proof:

(a) Claim : (1)

The operations + and · are well defined.

Let $[f(x)] = [f_1(x)]$ and $[g(x)] = [g_1(x)]$

Then $f(x) \mathcal{R} f_1(x)$ and $g(x) \mathcal{R} g_1(x)$.

$\Rightarrow f(x) = f_1(x) + p(x)\,s(x)$ and $g(x) = g_1(x) + q(x)\,s(x)$.

$\Rightarrow f(x) + g(x) = f_1(x) + g_1(x) + [p(x) + q(x)]\,s(x)$.

$\Rightarrow f(x) + g(x) \mathcal{R} f_1(x) + g_1(x)$.

$\Rightarrow [f(x) + g(x)] = [f_1(x) + g_1(x)]$.

Further, $f(x)\,g(x) = f_1(x)\,g_1(x) + \{f_1(x)\,q(x) + g_1(x)\,p(x) + p(x)\,q(x)\,s(x)\}\,s(x)$.

$\Rightarrow f(x)\,g(x) \mathcal{R} f_1(x)\,g_1(x)$.

$\Rightarrow [f(x)\,g(x)] = [f_1(x)\,g_1(x)]$

$\therefore$ Both + and · are well-defined.

The Equivalence classes of $F[x]$ relative to congruence modulo $s(x)$ is denoted by $\frac{F[x]}{(s(x))}$.

Claim : (2)

$\frac{F[x]}{(s(x))}$ is a ring with identity.

(1) Closure Axiom w.r. to + :

For $[f(x)], [g(x)] \in \frac{F[x]}{(s(x))}$

$[f(x)] + [g(x)] = [f(x) + g(x)] = [r(x)] \in \frac{F[x]}{(s(x))}$

where $f(x) + g(x) = t(x)s(x) + r(x)$, for some $t(x) \in F[x]$

(ii) Associative Axiom w.r.to +:

For $[f(x)], [g(x)], [h(x)] \in \frac{F[x]}{(s(x))}$.

$$([f(x)] + [g(x)]) + [h(x)] = [f(x) + g(x)] + [h(x)]$$
$$= [(f(x) + g(x)) + h(x)]$$
$$= [f(x) + (g(x) + h(x))]$$
$$= [f(x)] + ([g(x) + h(x)])$$
$$= [f(x)] + ([g(x)] + [h(x)])$$

$\Rightarrow$ + is associative in $\frac{F[x]}{(s(x))}$.

(iii) Existence of zero element:

$[0] \in \frac{F[x]}{(s(x))}$ and $[0]$ is the zero element.

(iv) Existence of Additive Inverse:

For $[f(x)]$, $[-f(x)]$ is the additive inverse.

(v) Commutative Axiom:

For $[f(x)], [g(x)] \in \frac{F[x]}{(s(x))}$

$$[f(x)] + [g(x)] = [f(x) + g(x)]$$
$$= [g(x) + f(x)]$$
$$= [g(x)] + [f(x)].$$

$\Rightarrow$ + is commutative.

vi) closure Axiom w.r.to $*$:

For $[f(x)], [g(x)] \in \frac{F[x]}{(g(x))}$

$$[f(x)][g(x)] = [f(x)\, g(x)] = [r(x)] \in \frac{F[x]}{(g(x))}.$$

vii) Associative Axiom w.r.to $*$:

For $[f(x)], [g(x)], [h(x)] \in \frac{F[x]}{(g(x))}$

$$\begin{aligned}([F(x)].[g(x)]).[h(x)] &= [f(x)\, g(x)][h(x)] \\ &= [(f(x)\, g(x))\, h(x)] \\ &= [f(x)(g(x)\, h(x))] = [f(x)][g(x)\, h(x)] \\ &= [f(x)]\,([g(x)][h(x)]).\end{aligned}$$

$\Rightarrow *$ is associative.

(viii) Distributive Axiom:

$$\begin{aligned}[f(x)]([g(x)+h(x)]) &= [f(x)][g(x)+h(x)] \\ &= [f(x)(g(x)+h(x))] \\ &= [f(x)\, g(x) + f(x)\, h(x)] \\ &= [f(x)][g(x)] + [f(x)][h(x)].\end{aligned}$$

Illy $([g(x)]+[h(x)])[f(x)] = [g(x)][f(x)] + [h(x)][f(x)]$.

$\therefore \frac{F[x]}{(g(x))}$ is a ring

$[1] \in \frac{F[x]}{(g(x))}$ is the identity element.

(b) Let $[f(x)] \neq 0$ be in $\frac{F[x]}{(s(x))}$ and let $s(x)$ be irreducible over F.

$$[f(x)] \in \frac{F[x]}{(s(x))} \Rightarrow \deg f(x) < \deg s(x)$$
$$\Rightarrow s(x) \nmid f(x).$$

$s(x) \nmid f(x)$ and $s(x)$ is irreducible.

$$\Rightarrow (s(x), f(x)) = 1$$

$\Rightarrow$ there exist polynomials $p(x)$ and $q(x)$ in $F[x]$ such that $s(x)q(x) + f(x)p(x) = 1$

$$\Rightarrow f(x)p(x) \equiv 1$$
$$\Rightarrow [f(x)p(x)] = [1]$$
$$\Rightarrow [f(x)][p(x)] = [1]$$
$$\Rightarrow [p(x)] \in \frac{F[x]}{(s(x))} \text{ is the inverse of } [f(x)].$$

$\therefore \frac{F[x]}{(s(x))}$ is a field,

since, $[f(x)][g(x)] = [f(x)g(x)]$
$= [g(x)f(x)]$
$= [g(x)][f(x)]$.

for all $[f(x)], [g(x)]$ in $\frac{F[x]}{(s(x))}$.

c). Let $|F| = q$ and $\deg s(x) = n$.

Let $f(x) \in F[x]$. Then by division algorithm.

$$f(x) = q(x)s(x) + r(x).$$

where $\deg r(x) < \deg s(x) = n$.

Then $f(x) \in [r(x)]$ and $r(x)$ is of the form,

$r(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$,

where each a_i is one of the q elements in F.

$\therefore$ any $f(x)$ in $F[x]$ belongs to one of the q^n equivalence classes $[r(x)]$.

Further, if $r_1(x)$ and $r_2(x)$ of degree $\leq n-1$, then $r_1(x) \not\equiv r_2(x)$.

Hence $\frac{F[x]}{(s(x))}$ contains exactly q^n equivalence classes.

$\therefore \left|\frac{F[x]}{(s(x))}\right| = q^n$.

Definition:

If $f(x), g(x) \in F[x]$ have their gcd 1, then $f(x)$ and $g(x)$ are said to be relatively prime.

THEOREM: 5

If $f(x)$ and $g(x)$ are relatively prime and belong to $F[x]$, where F is any field, show that there is no element $a \in F$ such that $f(a)=0$ and $g(a)=0$.

Proof: Assume the contrary that there is an element $a \in F$ such that $f(a)=0$ and $g(a)=0$.

Then $x-a \in F[x]$ is common factor of $f(x)$ and $g(x)$.

This is a contradiction, since $f(x)$ and $g(x)$ are relatively prime. $\therefore$ There is no element $a \in F$ such that $f(a)=0$ and $g(a)=0$.

Problems:

1. Let $S(x) = 1+x+x^2$ in $Z_2[x]$. Then prove that $Z_2[x]$ can be partitioned into 4 equivalence classes $[0], [1], [x], [1+x]$ Modulo $S(x)$.

Solution:

Given: $S(x) = 1+x+x^2 \in Z_2[x]$.

$$\frac{Z_2[x]}{(S(x))} = \{[0], [1], [x], [1+x]\}$$

To prove that $\frac{Z_2[x]}{(S(x))}$ is a field. → (There exists addition & multiplication. its inverse exist

Now we define addition:

+	[0]	[1]	[x]	[1+x]
[0]	[0]	[1]	[x]	[1+x]
[1]	[1]	[0]	[1+x]	[x]
[x]	[x]	[1+x]	[0]	[1]
[1+x]	[1+x]	[x]	[1]	[0]

From the table, $\frac{Z_2[x]}{(S(x))}$ is an abelian group under addition.

Now we define Multiplication:

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

$$\Rightarrow x^2 = 1(x^2+x+1) - (x+1).$$

$$\Rightarrow x^2 \mathcal{R} -(x+1)$$

x^2+x+1 | 1

x^2

x^2+x+1

$-x-1$.

$[x][x+1] = [x^2+x] = [-1] = [1]$

$[x+1][x+1] = [x^2+2x+1] = [x^2+x+1+x] = [x]$.

*	[0]	[1]	[x]	[1+x]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[x]	[1+x]
[x]	[0]	[x]	[x+1]	[1]
[1+x]	[0]	[1+x]	[1]	[x]

$\Rightarrow \left\{ \frac{Z_2[x]}{S(x)} - [0] \right\}$ is an abelian group under Multiplication.

$\therefore \frac{Z_2[x]}{(S(x))}$ is a field.

2. Let $S(x) = x^2+1 \in R[x]$, where R is the field of real numbers and $S(x)$ is irreducible over R. To prove that the field $\frac{R[x]}{[x^2+1)}$ and the complex field C are isomorphic.

Solution: Given: $S(x) = x^2+1 \in R[x]$.

By the theorem (4), If $S(x)$ is irreducible in R.

Then $\frac{R[x]}{(S(x))}$ is a field $\Rightarrow \frac{R[x]}{(x^2+1)}$ is a field.

TO prove that $\frac{R[x]}{(x^2+1)}$ and C are isomorphic.

Define: $h : \frac{R[x]}{(x^2+1)} \to C.$

$$h([a+bx]) = a+ib.$$

Claim: h is well defined.

Let $[a+bx] = [c+dx]$

Then $(a+bx)\ R\ (c+dx)$

$\Rightarrow a+bx = c+dx \mod (g(x))$

$\Rightarrow a+bx-c-dx = t(x)(x^2+1).$

$\Rightarrow (a-c)+(b-d)x = t(x)(x^2+1).$

This is possible only if $t(x)=0$

$\Rightarrow (a-c)+(b-d)x = 0$

$\Rightarrow a+bx=c+dx \Rightarrow a=c$ and $b=d.$

$\Rightarrow a+ib = c+id \Rightarrow h([a+bx]) = h([c+dx])$

$\Rightarrow h$ is well-defined.

Claim: h is a homomorphism.

For $[a+bx], [c+dx] \in \frac{R[x]}{(x^2+1)}.$

$$h([a+bx]+[c+dx]) = h([(a+c)+(b+d)x])$$
$$= (a+c)+i(b+d)$$
$$= (a+ib)+(c+id)$$
$$= h([a+bx])+h([c+dx])$$

$$h([a+bx][c+dx]) = h([ac+adx+bcx+bdx^2])$$
$$= h([ac+(ad+bc)x]+bd[x^2])$$

$= h([ac + (ad+bc)x] + bd[-1])$, Since $x^2 R(-1)$

$= h([(ac-bd) + (ad+bc)x])$

$= (ac-bd) + i(ad+bc)$

$= (a+ib)(c+id)$

$= h([a+bx])\, h([c+dx])$.

$\Rightarrow$ h is a homomorphism.

Claim: h is 1-1.

Let $h([a+bx]) = h([c+dx])$

Then: $a+ib = c+id$

Equating real and imaginary parts, $a = c$ and $b = d$.

$\Rightarrow [a+ib] = [c+id]$

$\Rightarrow$ h is 1-1.

Claim: h is onto.

Let $a+ib \in C$. Then $a, b \in R$.

$\therefore [a+bx] \in \frac{R[x]}{(x^2+1)}$ and $h([a+bx]) = a+ib$

$\Rightarrow$ h is onto

Hence: $\frac{R[x]}{(x^2+1)} \simeq C$.

3. Show that $s(x) = x^2+x+2$ is Irreducible in $Z_3[x]$.

Solution:

Given: $s(x) = x^2+x+2$ in $Z_3[x]$

$Z_3 = \{0, 1, 2\}$

$s(0) = 2 \neq 0$, $s(1) = 1+1+2 = 4 \neq 0$.

$s(2) = 4+2+2 = 2 \neq 0$.

$\therefore$ $s(x)$ is Irreducible in $Z_3[x]$.

4. Find the equivalence classes for the ring $\frac{Z_3[x]}{(s(x))}$, where $s(x) = x^2+x+2$.

Solution: Given: $s(x) = x^2+x+2$.

$\deg s(x) = 2 = n$

and $|Z_3[x]| = q = 3$.

By the theorem, if $|F| = q$ and $\deg s(x) = n$ then

$\left|\frac{F[x]}{(s(x))}\right| = q^n$.

$\Rightarrow \left|\frac{Z_3[x]}{(s(x))}\right| = 3^2 = 9$.

$\therefore$ The nine equivalence classes are $[0], [1], [2]$, $[x], [2x]$, $[x+1], [x+2], [2x+1], [2x+2]$.

5. Give an example of a polynomial $f(x) \in R[x]$ where $f(x)$ has degree 6, is Irreducible, but has no real roots.

Solution: Let $f(x) = (x^2+1)^3$.

This polynomial has degree 6.

Also $(x^2+1)^3 = (x^2-i^2)^3 = ((x+i)(x-i))^3$

Then, the roots of the polynomial $(x^2+1)^3$ are imaginary

∴ The polynomial that has degree 6 reducible and has no real root is,

$$f(x) = (x^2+1)^3.$$

6. Let $f(x) = (2x^2+1)(5x^3-5x+3)(4x-3) \in \mathbb{Z}_7[x]$ write $f(x)$ as the product of a unit and three Monic polynomials.

Solution:

$$f(x) = (2x^2+1)(5x^3-5x+3)(4x-3).$$

$1 \equiv 8 \pmod 7$

$3 \equiv 10 \pmod 7$

$3 \equiv 24 \pmod 7$

$$= (2x^2+8)(5x^3-5x+10)(4x+4) \quad (4x-24)$$

$$= 2(x^2+4)\,5(x^3-x+2)\,4(x+1) \quad 4(x-6)$$

$$= 40\,(x^2+4)(x^3-x+2)(x+1). \quad (x-6)$$

$40 \equiv 5 \pmod 7$.

$$f(x) = 5\,(x^2+4)(x^3-x+2)(x+1). \quad (x-6).$$

with each ~~of~~ one is Monic and 5 is a unit.

Since $= 5 \cdot 3 = 1$

∴ 5 is a unit.

H.10

1. Show that $S(x) = x^2+1$ is reducible in $\mathbb{Z}_2[x]$
2. Show that $S(x) = x^4+x^3+1 \in \mathbb{Z}_2[x]$ is irreducible.
3. Find the equivalence classes for the ring $\frac{\mathbb{Z}_2[x]}{(S(x))}$, where $S(x) = x^2+1$.
4. What is the order of the field $\frac{\mathbb{Z}_2[x]}{(S(x))}$? Where $S(x) = x^4+x^3+1$.