Algebra

Group : G (nonempty) , $+ : G \times G \to G$ is a group if

① $a+(b+c) = (a+b)+c \quad \forall a, b, c \in G$

② $\exists\, e \in G$ (identity)

$$x+e = e+x = x \quad \forall x \in G$$

③ For every $x \in G$, $\exists\, \bar{x} \in G$ st

$$x+\bar{x} = \bar{x}+x = e$$

If $+$ is commutative then G is called a commutative/ Abelian group

Eg: ① $(\mathbb{Z}, +)$

② $(\mathbb{N}, +)$ X

③ Set of all invertible $n \times n$ matrices, x

④

Properties:

(P1) For any group G, the identity is unique

Suppose e, e' are identities

$$e = e + e' = e'$$

(P2) Inverses are unique

Let $\bar{x}$, $\tilde{x}$ be inverses of x

$$x + \tilde{x} = e$$

$$\bar{x} + (x + \tilde{x}) = \bar{x} + e = \bar{x}$$

$$(\bar{x} + x) + \tilde{x} = \bar{x}$$

$$e + \tilde{x} = \bar{x}$$

$$\tilde{x} = \bar{x}$$

Subgroup $(G,+)$ & $H \subseteq G$ is a group under $+$

Then H is a subgroup of G.

Eg: $(2\mathbb{Z},+)$ is a subgroup of $(\mathbb{Z},+)$

$(a\mathbb{Z},+)$ is a s.g. of $(\mathbb{Z},+)$ for any $a \in \mathbb{Z}\setminus\{0\}$

Lemma: $H \subseteq G$ is a subgroup if

① $a+b \in H$ for all $a,b \in H$

② For every $a \in H$, $\bar{a} \in H$

$a \in H, \Rightarrow \bar{a} \in H \Rightarrow a+\bar{a} \in H \Rightarrow e \in H$

If $H \subsetneq G$, then H is called a proper subgroup of G.

Coset : Let H be a subgroup of G & $a \in G$

$a + H = \{a + h : h \in H\}$ is called a left coset of H

$H + a = \{h + a : h \in H\}$ is a right coset of H

Claim 1 : All elements of a coset are distinct

Proof : $a + h_1 = a + h_2$ for some $h_1, h_2 \in H$

$\Rightarrow h_1 = h_2$

$\therefore$ $\exists$ bijection b/w H & $a+H$.

$$|a+H| = |H|$$

Order of H = No of elements in H.

<u>Claim</u>: Distinct cosets of H are disjoint

$a+H$ $\quad$ $b+H$

Suppose $a+h_1 = b+h_2$ $\qquad$ $h_1, h_2 \in H$

$$a = b+h_2+\bar{h}_1$$

$$a = b+h' \qquad \text{for } h' = h_2+\bar{h}_1 \in H$$

$$\begin{aligned} a+H &= (b+h')+H \\ &= b+(h'+H) \\ &= b+H \end{aligned}$$

∴ The cosets of H have the same size & form a partition of G

(non intersecting & union equals G)

Lagrange's thm: Consider any G with order n & subgroup $H \subseteq G$ of order m. Then m must divide n & there are n/m cosets of H.

Division: $a, b \in \mathbb{Z}$, we can always write

$$\underbrace{b = a\underset{\downarrow}{q} + r}_{} \longrightarrow \text{remainder} \qquad 0 \leq r < |a|$$

Quotient

Ring: $(R, +, \times)$ is a ring if

⓪ R is closed under $\times$

① $(R, +)$ is a group

② $\times$ is associative

③ $\exists$ 1 identity

④ Distributive $a(b+c) = ab + ac$

Eg: ① $\mathbb{Z}$ is a ring

② Given any field $\mathbb{F}$, the ring of polynomials with coefficients from $\mathbb{F}$ is

$$\mathbb{F}[x] = \left\{ \sum_{i=0}^{n} a_i x^i \; ; \; a_i \in \mathbb{F}, \; n \text{ is finite} \right\}$$

Claim: $\mathbb{F}[x]$ is a ring

- Closed under $+, \cdot$
- Additive identity: 0
- Multiplicative : $e \in \mathbb{F}$
- Additive inverse : $a(x) = a_0 + a_1 x + \cdots + a_m x^m$

  $\bar{a}(x) = \bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_m x^m$

- Associative
- Distributive

③ $2\mathbb{Z}$ is a group, but not a ring.

Division in the integers

Given $(a,b) \in \mathbb{Z}^2$

$b = aq + r$; $q \in \mathbb{Z}$

$0 \leq r < a$

$b \in \mathbb{Z}$ $\quad a\mathbb{Z}$

$b \in a\mathbb{Z} + r$ for some $0 \leq r < a$

Cosets : $a\mathbb{Z},\ a\mathbb{Z}+1,\ a\mathbb{Z}+2,\ \ldots,\ a\mathbb{Z}+(a-1)$

Consider $\mathbb{F}[x]$

$a(x) \in \mathbb{F}[x]$ $\qquad\qquad$ x^2+2x+1

$$(x^2+2x+1)\mathbb{F}[x] = \{(x^2+2x+1)\alpha(x) : \alpha(x) \in \mathbb{F}[x]\}$$

$a(x)\mathbb{F}[x]$ is a subgroup of $\mathbb{F}[x]$

What will the cosets be?

Claim: $a(x)\mathbb{F}(x) + \alpha(x)$ for $\alpha(x) \to$ set of all polynomials of degree < deg(a)

Given any $a(x)$, $b(x)$, we can write

$$b(x) = a(x)\underset{\substack{\downarrow \\ \text{quotient}}}{q(x)} + \underset{\substack{\downarrow \\ \text{remainder}}}{r(x)}$$

$$0 \leq \deg(r(x)) < \deg(a(x))$$

Eg: $a(x) = x^2+1$ $\quad b(x) = x^4+x+1$ over $\mathbb{F}_2$

$$\begin{array}{r|l}
 & \underline{\;x^2+1\;} \\
x^2+1 & x^4+x+1 \\
 & \underline{x^4+x^2} \\
 & 0+x^2+x+1 \\
 & \quad \underline{x^2+1} \\
 & \quad 0+x
\end{array}$$

$$x^4+x+1 = (x^2+1)(x^2+1) + x$$

Defn: We say that $a(x)$ divides $b(x)$ if $\exists\, q(x)$ st

$$b(x) = a(x)\, q(x)$$

Defn: $\text{GCD}(a(x), b(x))$ is a polynomial of max degree that divides both $a(x)$ & $b(x)$

Claim: GCD is not unique

Only unique up to scalar multiple.

$$x^2+x \;,\; x^2+2x$$

$$\frac{x^2+x}{x/2} = 2x+2$$

$69, 33$

$$\frac{x^2+2x}{x/2} = 2x+4$$

$$\begin{array}{rl} & 2 \\ 33 & \overline{)\,69} \\ & \underline{66} \end{array}$$

$$\begin{array}{rl} & 11 \\ 3 & \overline{)\,33} \\ & \underline{33} \\ & \underline{0} \end{array}$$

$$3 = 69 - 33 \times 2$$

$$= 69(1) + 33(-2)$$

$a(x) = x^4 + x^2 + x + 1, \qquad b(x) = x^3 + 1$

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

$$\begin{array}{r|l} & x \\ \hline x^2+1 & x^3+1 \\ & x^3+x \\ \hline & x+1 \end{array}$$

$$\begin{array}{r|l} & x+1 \\ \hline x+1 & x^2+1 \\ & x^2+x \\ \hline & x+1 \\ & x+1 \\ \hline & 0 \end{array}$$

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

$$= (x^3+1) + \left[(x^4+x^2+x+1) + x \times (x^3+1)\right] \times x$$

$$= (x^3+1)(1+x^2) + (x^4+x^2+x+1)\,x$$

$$\frac{x^4+x^2+x+1}{x+1} = x^3+x^2+1$$

Irreducible polynomial : $a(x) \in \mathbb{F}[x]$ is irreducible if

$$b(x) \mid a(x) \Rightarrow \deg(b(x)) = 0 \quad \text{OR}$$

$$\underbrace{b(x) = \alpha\, a(x)}_{\deg(b(x)) = \deg(a(x))}$$

$\mathbb{F} = \mathbb{R} \rightarrow$ $x+1$, All deg(1) polynomials

x^2+1

If $a \in \mathbb{C} \setminus \mathbb{R}$ is a root of $f(x)$,
a^* is also a root

$$(x-a)(x-a^*) = x^2 - |a|^2$$

$$f(x) = (x^2-|a_1|^2)(x^2-|a_2|^2)\cdots(x^2-|a_m|^2)\ (x-\alpha_1)(x-\alpha_2)\cdots(\ )$$

$\therefore$ There are no irreducible polynomials of deg > 2 in $\mathbb{R}[x]$

Irreducible polynomials in $\mathbb{F}_2[x]$:

① $x,\ x+1$

② x^2+x+1

③ $x^3+x+1,\ x^3+x^2+1$

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

<u>Claim</u>: For any $\mathbb{F}_p$, p a prime & any $m \in \mathbb{Z}_+$, $\exists$ an irreducible polynomial of deg m in $\mathbb{F}_p[x]$

Given $a(x), b(x)$ $\quad GCD(a(x), b(x)) = 1$

$\Leftrightarrow \exists\ \alpha(x), \beta(x)$

$$a(x)\alpha(x) + b(x)\beta(x) = 1$$

Given a, b, $\exists\ c$ & d

$$ac + bd = GCD(a, b)$$

Theorem: Given any $a(x), b(x) \in \mathbb{F}[x]$,

$GCD(a(x), b(x)) = 1$ iff $\exists\ c(x), d(x)$ st

$$a(x)c(x) + b(x)d(x) = 1$$

Proof: Consider $a(x)c(x) + b(x)d(x) = 1$

& $GCD(a(x), b(x)) = \alpha(x)$

$\Rightarrow \alpha(x) \mid a(x)$ & $\alpha(x) \mid b(x)$

$\Rightarrow \alpha(x) \mid a(x)c(x) + b(x)d(x)$

$\Rightarrow \alpha(x) \mid 1$

$\Rightarrow \alpha(x) \in \mathbb{F}$ $\alpha(x) = 1 \Rightarrow GCD = 1$

Now, suppose $GCD(a(x), b(x)) = 1$

Let $G = \{ a(x) c(x) + b(x) d(x) : c(x), d(x) \in \mathbb{F}[x] \}$

Take any $f(x) \in G$

$$\alpha(x) f(x) \in G \quad \forall \ \alpha(x) \in \mathbb{F}[x]$$

G is a group

(If $1 \in G \Rightarrow G = \mathbb{F}[x]$)

Let $\beta(x)$ is the polynomial of lowest degree in G

Since $\beta(x) \in G$, $\exists$ $c(x)$ & $d(x)$ st

$$\beta(x) = a(x)\,c(x) + b(x)\,d(x)$$

$$a(x) = \beta(x)\,q_a(x) + r_a(x)$$

$$\deg(r_a(x)) < \deg(\beta(x))$$

$$r_a(x) = \underbrace{a(x)}_{\in G} - \underbrace{\beta(x)\,q_a(x)}_{\in G} \in G$$

$\Rightarrow$ $r_a(x) = 0$ (since β is nonzero poly of lowdeg

$\Rightarrow$ $a(x) = \beta(x)\,q_a(x)$ or $\beta(x) \mid a(x)$

$$b(x) = \beta(x)\,q_b(x) + r_b(x) \Rightarrow r_b(x) = 0$$

$\Rightarrow \quad \beta(x) \mid b(x)$

$\beta(x) \mid a(x) \quad \& \quad \beta(x) \mid b(x)$

$\Rightarrow \quad \beta(x) = 1$

$1 = a(x)\, c(x) + b(x)\, d(x)$

Definition : We say that $a(x) \equiv b(x) \mod f(x)$

if remainder of $a(x)$ when divided by $f(x)$

= rem of $b(x)$ when divided by $f(x)$

$[a(x)] \mod f(x)$ = remainder of $a(x)$ when divided by $f(x)$

$$[a(x) + b(x)] \mod f(x) = [a(x)] \mod f(x) + [b(x)] \mod f$$

Unique Factorization Theorem

Every $f(x) \in \mathbb{F}[x]$ can be uniquely factorized as a product of irreducible polynomials (up to scalars)

Proof: Suppose

$$f(x) = a_1(x)\, a_2(x) - a_m(x) \times \alpha$$

$$= b_1(x)\, b_2(x) - b_n(x) \times \beta$$

$$a_1(x) \mid b_1(x)\, b_2(x) - b_n(x)$$

$\Rightarrow \quad a_1(x) \mid b_i(x)$ for some i

$a_1(x) = b_i(x)$ for some i

$\forall i,$

$\therefore \quad a_i(x) = b_j(x)$ for some j

If α is a root of $f(x)$

$f(\alpha) = 0$

$x - \alpha \mid f(x)$

$\mathbb{C}[x]$

Extension field If $\mathbb{F} \subsetneq \mathbb{F}'$ where $\mathbb{F}$ & $\mathbb{F}'$ are fields,

then $\mathbb{F}$ is a subfield of $\mathbb{F}'$

$\mathbb{F}'$ is an extension field of $\mathbb{F}$.

Theorem Take any $\mathbb{F}$. $\mathbb{F}[x]$

& any irreducible polynomial $f(x) \in \mathbb{F}[x]$

$(\mathbb{F}[x]) \bmod f(x)$ is a field.

$$\shortparallel$$

$$\{ [a(x)] \bmod f(x) \; : \; a(x) \in \mathbb{F}[x] \}$$

Proof : $\mathbb{F}_f[x] = \left(\mathbb{F}[x]\right) \bmod f(x)$ is an Abelian group

$\times$ is commutative, associative & distributive over +.

$$\left[a(x) \cdot 1\right] \bmod f(x) = a(x)$$

$f(x)$ is irreducible,

for any $a(x) \in \mathbb{F}_f(x)$, $\deg(f(x)) > \deg(a(x))$

$$\mathrm{GCD}(a(x), f(x)) = 1$$

$\Rightarrow \exists \; c(x), d(x)$ st

$$a(x)\, c(x) + f(x)\, d(x) = 1$$

$$[a(x)\, c(x) + f(x)\, d(x)] \bmod f(x) = 1$$

$$[a(x)\, c(x)] \bmod f(x) = 1$$

$[c(x)] \bmod f(x)$ is the multiplicative inverse of $a(x)$

Example 1 : $\mathbb{F} = \mathbb{R}$

$x^2 + 1$ is irreducible

$$(\mathbb{R}[x]) \bmod (x^2+1)$$

$$\shortparallel$$

$$\{ a + bx \ : \ a, b \in \mathbb{R} \}$$

$$\left[(a_1 + b_1 x) + (a_2 + b_2 x) \right] \bmod (x^2+1)$$

$$\shortparallel$$

$$(a_1 + a_2) + (b_1 + b_2) x$$

$$\left[(a_1 + b_1 x)(a_2 + b_2 x)\right] \bmod (x^2+1)$$

$$\|$$

$$\left[a_1 a_2 + (a_2 b_1 + a_1 b_2)x + b_1 b_2 x^2\right] \bmod (x^2+1)$$

$$\|$$

$$a_1 a_2 + (a_2 b_1 + a_1 b_2) x + b_1 b_2 (x^2) \bmod (x^2+1)$$

$$= (a_1 a_2 - b_1 b_2) + (a_2 b_1 + a_1 b_2) x$$

$$\begin{array}{rl} & b_1 b_2 \\ x^2+1 \,\big) & \overline{b_1 b_2 x^2} \\ & \underline{b_1 b_2 x^2 + b_1 b_2} \\ & -b_1 b_2 \end{array}$$

Example 2

$\mathbb{F}_2$

$\mathbb{Z}_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

x^2+x+1 is irreducible.

$$(\mathbb{F}_2[x]) \bmod (x^2+x+1)$$

$$\|$$

$$\{ a_1 + a_2 x \; : \; a_1, a_2 \in \mathbb{F}_2 \}$$

$\times$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

$\mathbb{F}_{2^2}$ $\mathbb{F}_8$

Isomorphism : Given $\mathbb{F}$ & $\mathbb{F}'$ $\mathbb{F}$ & $\mathbb{F}'$ are isomorphic if $\exists$ bijection $\phi : \mathbb{F} \to \mathbb{F}'$

$$\phi(a+b) = \phi(a) + \phi(b) \quad \forall a,b \in \mathbb{F}$$

$$\phi(ab) = \phi(a)\,\phi(b) \quad \forall a,b \in \mathbb{F}$$

Claim: For any prime p & +ve integer n, there exists an irreducible polynomial of degree n in $\mathbb{F}_p[x]$

Consider $\underbrace{\left(\mathbb{F}_p(x)\right) \bmod a(x)}$ for some poly $a(x)$ of degree n

$$\shortparallel$$

$$\{ \alpha_0 + \alpha_1 x + \dots + \alpha_{n-1} x^{n-1} ; \quad \alpha_i \in \mathbb{F}_p \}$$

$$p^n$$

The order of every finite field is of the form p^n for some prime p & +ve integer n.

$0, 1, x, 1+x, x^2, 1+x^2, 1+x+x^2, x+x^2$