Abstract Algebra

Hwichang Jeong

July 14, 2020

Outline

- Group
- Ring
- Field
- Finite field

Group

- A **group** $< G, * >$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied
  - $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$ (Associativity)
  - There is an element $e \in G$ such that for all $x \in G$,

    $$e * x = x * e = x \text{ (Identity element)}$$

  - Corresponding to each $a \in G$, there is an element a' in G such that

    $$a * a' = a' * a = e \text{ (Inverse)}$$

- If a subset H of a group G is closed under the binary operation of G and if H with the induced operation from G is itself a group, then H is **subgroup** of G denoted by $H \leq G$.

Cyclic group

Theorem - Cyclic subgroup

Let $< G, * >$ be a group and let $a \in G$. Then

$$H = \{g^n | n \in \mathbb{Z}\}$$

is a subgroup of G and is the smallest subgroup of G contains g.
Note : $m \in \mathbb{N}$, $g^m = g * g * \cdots * g$, $g^0 = e$, g^{-m} is inverse of g^m

- H is called the cyclic subgroup $< g >$ of G **generated by** g.
- We call g is **generator** of $< g >$.
- If $| < g > | = m$, i.e. $< g >$ is of finite order(Cardinality of group) m, m is the smallest positive integer such that $g^m = e$ (Order of g is m)

Theorem - Cyclic group

A subgroup of a cyclic group is cyclic.

Cyclic group / $\mathbb{Z}_m$

- Every Cyclic group is **abelian group**(commutative group).
- $\mathbb{Z}_m = \{0, 1, \cdots, m-1\} := \mathbb{Z}/_\sim$ such that $a \sim b \Leftrightarrow a \equiv b \ (mod \ m)$
  - $a \equiv b \ (mod \ m)$ means the remainder when a and b are divided by m are the same.
- $< \mathbb{Z}_m, +_m >$ is cyclic group of order m.
  - For $\mathbb{Z}_5$, 1$+_5$2=3, 2$+_5$3=0, 3$+_5$4=2, 4$+_5$4=3

Group isomorphism

- Two groups $< G, * >$, $< G', *' >$ are isomorphic, if there exists one-to-one function ϕ mapping G onto G' such that

$$\phi(x * y) = \phi(x) *' \phi(y) \text{ for all } x, y \in G.$$

Theorem - Cyclic group

Let G be a cyclic group with generator a. If order of G is infinite, then G is isomorphic to $< \mathbb{Z}, + >$. If G has finite order n, then G is isomorphic to $< \mathbb{Z}_n, +_n >$.

Lagrange Theorem

Lagrange Theorem

Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.

Corollary

Every group of prime order is cyclic.

Ring

- A ring $< R, +, \cdot >$ is a set R together with two binary operations $+$ and $\cdot$, which we call addition and multiplication, defined on R such that the following axioms are satisfied
  - $< R, + >$ is an abelian group.
  - Multiplication is associative.
  - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (a \cdot b)$
- $< \mathbb{Z}_n, +_n, \cdot_n >$ is a Ring.
- Let F be the set of all functions $f : \mathbb{R} \to \mathbb{R}$. Then $< F, +, \cdot >$ is a ring. where

$$(f + g)(x) = f(x) + g(x),$$

$$(fg)(x) = f(x)g(x).$$

Ring / Field

- A ring which the multiplication is commutative is a **commutative ring.**
- A ring with a multiplicative identity element is a **ring with unity**; the multiplicative identity element 1 is called **unity**.
- Let R be a ring with unity $1 \neq 0$. An element u in R is a **unit** of R if it has a multiplicative inverse in R.
- If every nonzero element of R is a unit, then R is a **division ring.**
- A field is **commutative division ring.**

0 Divisor

- When we want to find roots of $x^2 - 5x + 6 = 0$ in $\mathbb{Z}_{12}$, the factorization $(x-2)(x-3)$ is still valid.
- But in $\mathbb{Z}_{12}$, not only is $0a = a0 = 0$ for all $\mathbb{Z}_{12}$, but also $(2)(6) = (3)(4) = (3)(8) = (4)(6) = (4)(9) = \cdots = (8)(9) = 0$
- So equation has not only 2 and 3 as solutions, but also 6 and 11.
- If a and b are two nonzero elements of a ring R such that $ab = 0$, then a and b are **0 divisors**.

0 Divisor

Theorem - 0 divisor

In the ring $\mathbb{Z}_n$, the divisors of 0 are precisely those nonzero elements that are not relatively prime to n.

pf) Let $m \in \mathbb{Z}_n$, where $m \neq 0$, and let the gcd of m and n be $d \neq 1$. Then

$$m\left(\frac{n}{d}\right) = \left(\frac{m}{d}\right)n.$$

Thus $m\left(\frac{n}{d}\right) = 0$ in $\mathbb{Z}_n$, while neither m nor n/d is 0, so m is a 0 divisor.

Corollary

If p is prime, then $\mathbb{Z}_p$ has no 0 divisors.

Cancellation law

- The cancellation laws hold in R if $ab = ac$ with $a \neq 0$ implies $b = c$, and $ba = ca$ with $a \neq 0$ implies $b = c$.

Theorem

The cancellation laws hold in a ring R if and only if R has no 0 divisors.

Integral Domain

- An Integral Domain D is a commutative ring with unity $1 \neq 0$ and containing no 0 divisors.

Theorem

Every field F is an integral domain.

Theorem

Every finite integral domain is a field.

Corollary

If p is prime, then $\mathbb{Z}_p$ is a field.

Characteristic of a Ring

- If for a ring R a positive integer n exists such that $n \cdot a$ $(a + a + \cdots + a$ for n summands$) = 0$ for all $a \in R$, then the least such positive integer is the **characteristic of the ring** R. If no such positive integer exists, then R is of characteristic 0.
- The ring $\mathbb{Z}_m$ is of characteristic m, while $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ all have characteristic 0.

Fermat's Theorem

Theorem - Fermat's Theorem

If $a \in \mathbb{Z}$ and p is a prime not dividing a, then

$$a^{p-1} \equiv 1(\text{mod p}).$$

pf) For $\mathbb{Z}_p$, the elements

$$1, 2, 3, \cdots, p-1$$

form a group of order $p-1$ under $\cdot_p$. By Lagrange Theorem, for $a \neq 0$ and $a \in \mathbb{Z}_p$, we have $a^{p-1} = 1$ in $\mathbb{Z}_p$.

Corollary

If $a \in \mathbb{Z}$ then

$$a^p \equiv a(\text{mod p}).$$

Congruent Equation

- $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, then $a \pm c \equiv b \pm d \pmod{m}$
- $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
- $a \equiv b \pmod{m}$, then $a^k \equiv b^k (\text{mod } m)$
- $ab \equiv ac \pmod{m}$, $d = gcd(a, m)$, then $b \equiv c\ (\text{mod}\frac{m}{d})$
- $a \equiv b \pmod{m}$, d is common divisor of a, b, m, then $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

Example of Fermat's Theorem

Example1

Show that $2^{11,213} - 1$ is not divisible by 11.

By Fermat's Theorem $2^{10} \equiv 1 \pmod{11}$, so

$$2^{11,213} - 1 \equiv [(2^{10})^{1,121} \cdot 2^3] - 1 \equiv 2^3 - 1 \equiv 7 \pmod{11}$$

Example2

Show that $n^{33} - n$ is not divisible by 15.

If n divides 3 and 5, clear.
If not by Fermat's Theorem $n^2 \equiv 1 \pmod{3}$, so

$$n^{32} - 1 \equiv (n^2)^{16} - 1 \equiv 0 \pmod{3}$$

By Fermat's Theorem $n^4 \equiv 1 \pmod{5}$, so

$$n^{32} - 1 \equiv (n^4)^8 - 1 \equiv 0 \pmod{5}$$

Field

Theorem - Prime field

A field F is either of prime characteristic p and contains a subfield isomorphic to $\mathbb{Z}_p$ or of characteristic 0 and contains a subfield isomorphic to $\mathbb{Q}$.

Corollary

$\mathbb{Z}_p, \mathbb{Q}$ contains no proper subfields.(Prime Field).

Extension Field

- A field E is an extension field of a field F if $F \leq E$.
- Let E be an extenstion field of F, then E is a vector space over F.
    - If $a, b \in E$ then $a + b \in E$
    - If $a \in F$, $b \in E$, then $ab \in E$
- If an extension field E of a field F is of finite dimension n as a vector space over E, E is a finite extension of degree n over F.
- $[E : F]$ be the degree n of E over F.

Finite Field (Galois Field)

Theorem

Let E be a finite extension of degree n over a finite field F. If F has q elements, then E has q^n elements.

pf) Let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis for E as a vector space over F. Then $\beta \in E$ can be uniquely written in the form

$$\beta = b_1\alpha_1 + \cdots + b_n\alpha_n$$

for $b_i \in F$. So the total number of such distinct linear combinations of the α_i is q^n.

Finite Field (Galois Field)

Corollary

If E is a finite field of characteristic p, then E contains exactly p^n elements for some positive integer n.

Theorem

The multiplicative group $< F^*, \cdot >$ of nonzero elements of a finite field F is cyclic.
$\therefore \mathbb{Z}_p^\times =< \mathbb{Z}_p \setminus \{0\}, \cdot_p >$ is cyclic group.

GF(p^n)

- We showed that the order of finite fields must be p^n for some prime p, $n \in \mathbb{N}$.
- A finite field of order p^n exists for every prime power p^n
- If E and E' are fields of order p^n then $E \approx E'$.
    - Two fields E and E' are isomorphic($E \approx E'$) if there exist bijective function ϕ such that

$$\phi(a+b) = \phi(a) + \phi(b)$$
$$\phi(ab) = \phi(a)\phi(b)$$
$$\phi(1) = 1 \text{ or } \phi \neq 0$$

- The field of order p^n is called Galois field of order p^n denoted by GF(p^n).
- GF(p) is cyclic additive group. But GF(p^n) is cyclic additive group when $n > 1$.

Euler phi-function

- Euler phi-funtion $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is function such that $\varphi(n)$ is the number of nonzero elements of $\mathbb{Z}_n$ that are not 0 divisors.
- (Euler's Theorem) If a is an integer relatively prime to n, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.
- It is known that the number of generators of GF(p^n) is $\varphi(p^n - 1)$.
    - For example, the number of generators of $\mathbb{Z}_{11}$ is $\varphi(10) = 4(\because 1, 3, 7, 9)$.
    - In fact, 2,6,7,8 are generator of $\mathbb{Z}_7$.
- It is not easy to find all generators of GF(p^n).

Discrete Logarithm

- The discrete logarithm $\log_a b$ is an integer k such that $a^k = b$.
    - For example, since $3^5 \equiv 5 \pmod 7$, $\log_3 5 = 5$ in $\mathbb{Z}_7$.
- Discrete logarithm is quickly computable in a few special cases. However, no efficient method is known for computing them in general.
- There is not only no efficient algorithm known for the worst case, but the average case complexity can be shown to be about as hard as the worst case using random self-reducibility.