Abstract Algebra (H). 20% + 30% + 5%.
Mid Final

Caiheng Li. Office hour: Wed. 16:00~18:00.

2024. 9. 10. Lecture 1.

$\mathbb{N}$: 1, 2, 3, $\cdots$, n, $n+1$, $\cdots$ $+, \times$.

$\mathbb{Z}$: $0, \pm 1, \pm 2, \cdots, \pm n, \pm(n+1), \cdots$ $+, -, \times$.

$\mathbb{Q}$: $0, \frac{n}{m}$ with $n, m \in \mathbb{Z} \setminus \{0\}$. $+, -, \times, \div$.

$\mathbb{R}$: $+, -, \times, \div$.

$\mathbb{C}$: $+, -, \times, \div$.

$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ where $a_i \in \mathbb{Q}$.

$\mathbb{Q}[x] = \{ f(x)$ with rational coefficients $\}$. $+, -, \times$.

$M_n(F)$: $n \times n$ matrices $[a_{ij}]_{n \times n}$, with $a_{ij} \in F$. $+, -, \times$. $(M_n(F), +, \times)$. — mat. ring.

$Inv_n(F)$: invertible mat. $\times$.

$\begin{cases} p \text{ prime} \\ 1 \le a < p \end{cases} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$.

$\begin{cases} p \text{ prime} \Rightarrow \\ p = a^2 + b^2 \iff p \equiv 1 \pmod{4} \end{cases}$.

Groups

Def. A set G with a multiplication $*$ ($a, b \in G \Rightarrow a*b \in G$, $b*a \in G$. (closed).)

is called a group if

(1) $a*(b*c) = (a*b)*c$. "$a*b*c$." association.

(2) $\exists\, e \in G$, s.t. $a*e = e*a = a$. "e": identity.

(3) For any $a \in G$, $\exists\, b \in G$, s.t.

$a*b = b*a = e$. "b": the inverse of a.

denote by $(G, *)$.

Further, if $a*b = b*a$ for all $a, b \in G$, then $(G, *)$ is called an abelian group.

Ex: $\mathbb{N}$: $1, 2, 3, \cdots, n, n+1, \cdots$

$\mathbb{Z}$: $0, \pm 1, \pm 2, \cdots, \pm n, \pm(n+1), \cdots$

$\mathbb{Q}$: $0, \frac{n}{m}$ with $n, m \in \mathbb{Z} \setminus \{0\}$.

$\mathbb{R}$:

$\mathbb{C}$:

$(\mathbb{Z}, +)$ is a gp. $(\mathbb{Z}, -)$ is not a group. $\{\mathbb{Z} \setminus \{0\}, \times\}$ is not a group.

$(\mathbb{Q}, +)$ is a gp. $(\mathbb{Q}, -)$ is not a group. $\{\mathbb{Q} \setminus \{0\}, \times\}$ is a group.

$\mathbb{R}$	$\mathbb{R}$	$\mathbb{R} \setminus \{0\}$
$\mathbb{C}$	$\mathbb{C}$	$\mathbb{C} \setminus \{0\}$.

$\mathbb{Q}[x]$, $+$, $-$, $\times$.

$(\mathbb{Q}[x], +)$ is a group. $(\mathbb{Q}[x], -)$ is not a group. $(\mathbb{Q}[x], \times)$ is not a group.

$(M_n(\mathbb{R}), +)$ is an abelian group.

$-$ not a group.

$\times$ not a group.

$(Inv_n(\mathbb{R}), \times)$ is a group. not abelian.

Fields

Def. A set F with "$+$" and "$\times$" is called a *field* if

(1) $(F, +)$ is an abelian group. with 0 being addition identity.

(2) $(F \setminus \{0\}, \times)$ is an abelian group. (→ ensure that addition identity $\neq$ multiplicity identity.; ↳ ensure there exists a multiplicity identity.)

(3). $a \times (b+c) = (a \times b) + (a \times c)$

$(b+c) \times a = (b \times a) + (c \times a)$.

denote by $(F, +, \times)$.

Ex. ① $(\mathbb{Z}, +, \times)$ is not a field as $(\mathbb{Z} \setminus \{0\}, \times)$ is not a group.

② $(\mathbb{Q}, +, \times)$ is a field.

$\mathbb{R}$

$\mathbb{C}$

③ $(\mathbb{Q}[x], +, \times)$ is not a field.

④ $(M_n(\mathbb{R}), +, \times)$ is not a field as $(M_n(\mathbb{R}) \setminus \{0\}, \times)$ is not a gp.

Rings

Def. A set R with "$+$" and "$\times$" is called a *ring* if

(1) $(R, +)$ is an abelian group.

(2). $a \times (b \times c) = (a \times b) \times c$. associativity.

(3). $a \times (b+c) = a \times b + a \times c$.

$(b+c) \times a = b \times a + c \times a$. distribution.

denote by $(R, +, \times)$.

Moreover, (i) if $a \times b = b \times a$ for all $a, b \in R$. then R is called a *commutative ring*.

(ii) if $e \in R$ is s.t $a \times e = e \times a = a$ for each $a \in R$, then e is called *the multiplication identity* of R.

firstly def. what is a multiplicity identity then prove its unique and we can use the word "the".

Observations:

① A field is a ring.

② A ring is not necessarily a field.

Ex. ① $(\mathbb{Z}, +, \times)$ is not a field, but a ring. integer ring.

② $(\mathbb{Q}, +, \times)$ is a field.

$\mathbb{R}$

$\mathbb{C}$

③ $(\mathbb{Q}[x], +, \times)$ is not a field. but it's a ring. polynomial ring.

④ $(M_n(\mathbb{R}), +, \times)$ is not a field as $(M_n(\mathbb{R}) \setminus \{0\}, \times)$ is not a gp.

but is a ring, called a matrix ring.

Question: ① How can we construct a group G? ⟶ Given two groups $(G, \times), (H, *)$

② What do we ask about a group G?

eg. $(M_n(\mathbb{R}), +)$ —— ?

Let $(G, \times), (H, *)$ be groups.

Define $X = G \times H = \{(g, h) \mid g \in G, h \in H\}$.

multiplication "$\cdot$": $(g_1, h_1) \cdot (g_2, h_2) := (g_1 \times g_2, h_1 * h_2)$.

Claim: $(G \times H, \cdot)$ is a group, called the direct product of G and H.

Prove $(G \times H, \cdot)$ is a group:

① closed: √.

② associativity: $[(g_1, h_1) \cdot (g_2, h_2)] \cdot (g_3, h_3)$

$= (g_1 \times g_2, h_1 * h_2) \cdot (g_3, h_3) = (g_1 \times g_2 \times g_3, h_1 * h_2 * h_3)$.

$(g_1, h_1) \cdot [(g_2, h_2) \cdot (g_3, h_3)] = (g_1, h_1) \cdot (g_2 \times g_3, h_2 * h_3)$ ✓

③ identity: Claim: (e_1, e_2) is $(G \times H, \cdot)$'s identity where e_1, e_2 denote the identity of G, H.

$$(g,h)\cdot(e_1,e_2) = (g\times e_1,\ h * e_2) = (g,h)$$
$$\|$$
$$(e_1,e_2)\cdot(g,h) = (e_1\times g,\ e_2\times h)\ \checkmark$$

④ inverse: every element's inverse is made of two components which are the inverses of the two componets that make up the element. ✓

□.

2024.09.12 Lecture 2.

More examples.

① Let $\mathbb{Z}_n = \{0,1,2,\cdots,n-1\}$.

Define $\oplus$ and $\otimes$ as:

$$i\oplus j = i+j \pmod n.$$
$$i\otimes j = i\times j \pmod n.$$

Proposition: $(\mathbb{Z}_n, \oplus, \otimes)$ is a commutative ring.

Moreover, if $n=p$ is a prime, then $(\mathbb{Z}_p\setminus\{0\}, \otimes)$ is an abelian group.

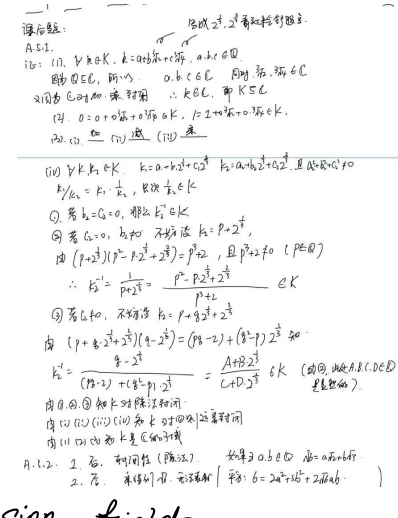
$(\mathbb{Z}_p, \oplus, \otimes)$ is a field, denoted by $\mathbb{F}_p$, $GF(p)$.

proof:

$a\in\{1,2,\cdots,p-1\}$.

$\gcd(a,p)=1$, so there exists $x,y\in\mathbb{Z}$ s.t. $ax+py=1$.

$\Rightarrow$ $a\otimes x = ax = 1 \pmod p$. $x=a^{-1}$.



Fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$.

② Let $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\} \subsetneq \mathbb{R}$.

$(\mathbb{Q}[\sqrt{2}], +, \times)$ is a field. Check box: ✓.

③. Let $\mathbb{Q}[2^{\frac{1}{3}}] = \{a+b\cdot 2^{\frac{1}{3}} + c\cdot 2^{\frac{2}{3}} \mid a,b,c\in\mathbb{Q}\}$.

inverse.

extension fields of $\mathbb{Q}$.

$(\mathbb{Q}[2^{\frac{1}{3}}], +, \times)$ is a field.

④ Let $\mathbb{Q}[\pi] = \left\{ \dfrac{a_0 + a_1\pi + \cdots + a_n\pi^n + \cdots}{b_0 + b_1\pi + \cdots + b_m\pi^m + \cdots} \;\middle|\; a_i, b_j \in \mathbb{Q} \right\}$.

$(\mathbb{Q}[\pi], +, \times)$ is a field.

⑤ Let $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, where $i = \sqrt{-1}$.

Claim: $(\mathbb{Z}[i], +, \times)$ is a ring, Gaussian ring. (Later used to prove $p = a^2 + b^2 \iff p \equiv 1 \pmod 4$).

Let F be a field, and let

$G := M_n(F) = \{$ invertible matrices of degree n over $F\}$.

$(G, \times)$ is a group, <u>General Linear group.</u>

$GL_n(F)$ or $GL(n, F)$

$GL_n(\mathbb{F}_p) = GL_n(p)$.

Let $(G, \times)$ be a group.

<u>Def.</u> A subset $H \subseteq G$ is called a <u>subgroup of G</u> if

$(H, \times)$ is a group. denoted by $H \leq G$.

↓

the operation need to be the same. eg. $(\mathbb{Z}_n, \oplus)$ is not a subgp of $(\mathbb{Z}, +)$.

<u>Lemma.</u> $H \subset G$ is a subgp

$\iff$ ① for any $x, y \in H$, we have

$xy \in H$ & $x^{-1} \in H$. If G is finite, only $xy \in H$ is needed.

$H \subseteq G$, $|G| < \infty$.

$H \leq G \iff H^2 \subseteq H$. (don't need $H^{-1} \subseteq H$)

Pf: $\forall x \in H$. $\{x, x^2, \cdots\}$.

$x^i = x^j$. $x \cdot x^{i-j-1} = e$.

$\Leftrightarrow$ ② for any $x, y \in H$, we have $xy^{-1} \in H$.

If G is infinite, $x^{-1} \in H$ is required.

Moreover, if $|G|$ is finite, then $H \subset G$ is a subgp $\Leftrightarrow xy \in H$ for any $x, y \in H$.

this is because for $x \in G$, $\langle x \rangle$ is finite, $|\langle x \rangle|$ is finite $\Rightarrow x^{-1} = x^{|\langle x \rangle| - 1}$

Ex. Let $G := \{ A \in M_n(F) \mid \det(A) = 1 \}$.

then $G \subset M_n(F)$, and $(G, \times)$ is a group.

also a subgp of $GL_n(F)$.

called Special Linear group.

$SL_n(F)$ or $SL(n, F)$.

Problem. $|GL_n(p)| = ?$

$|SL_n(p)| = ?$

G: group.

$H \leq G$. $K \leq G$.

Then $G = HK \Leftrightarrow HK = KH$ and $|G| = |H||K|$.

or $HK \leq G \Leftrightarrow HK = KH$.

$$C = \left\{ \begin{bmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{bmatrix} \middle| \, 0 \neq a \in F \right\} \subset GL_n(F)$$

$(C, \times)$ is a subgroup of $GL_n(F)$.

Claim: C is the center of $GL_n(F)$.

denoted by $Z(GL_n(F))$.

Def. A subgp $H \leq G$ is called the center of G if

$hg = gh$ for all $h \in H$ and $g \in G$.

Let G be a group. $H < G$.

$aH = bH \Leftrightarrow a^{-1}b \in H$.

Def. Let $Hg := \{ hg \mid h \in H \}$, where $g \in G$.

$gH := \{gh \mid h \in H\}$.

right coset　　left coset.

If $Hg = H$, $g \notin H$.
Suppose $g \notin H$, $e \cdot g = g \in H$. contrary.

Prop.

① For $g_1, g_2 \in G$, $Hg_1 \cap Hg_2 \neq \emptyset \iff Hg_1 = Hg_2$.

Pf: suppose $h_1 g_1 = h_2 g_2$ so $Hg_1 = (Hh_1)g_1 = H(h_1 g_1) = H(h_2 g_2) = (Hh_2)g_2 = Hg_2$.

Prop. $Hh = H$ for $h \in H$. (Pf: $x = (xh^{-1})h \in Hh$).

Cor. either $Hg_1 = Hg_2$ or $Hg_1 \cap Hg_2 = \emptyset$.

② If H is finite then $|Hg| = |H|$. (Pf: $\varphi: H \to Hg$, $h \to hg$, bij.)

$H \leq G$. $a, b \in G$. $|aH| = |bH|$.

Theorem (Lagrange).

If G is a finite group, then the order of a subgroup divides the order $|G|$. i.e. for $H \leq G$, we have $|H| \mid |G|$.

In particular, each element of G has its order dividing $|G|$.

Pf: Write all different right cosets of H in G.

$Hg_1, Hg_2, \cdots, Hg_m$.　$G = a_1H \sqcup a_2H \sqcup a_3H \cdots \sqcup a_mH$.　$\left(G = \dot{\bigcup_g} (Hg).\right)$

$G = (Hg_1) \dot\cup (Hg_2) \dot\cup \cdots \dot\cup (Hg_m)$.　$\{a_1, \cdots, a_m\}$ is called a (left) coset representative system of H in G.

↳ union with vacous intersection.

and $|G| = |Hg_1| + |Hg_2| + \cdots + |Hg_m| = m|H|$, so $|H| \mid |G|$. □.

Upshot: $H \leq G \Rightarrow |H| \mid |G|$.　The # of cosets := index of H.

denoted by $|G:H|$ or $[G:H]$

$H, K \leq G$.

Cor: $|HK| = \dfrac{|H|\,|K|}{|H \cap K|}$.

G: finite group.

For $g \in G$, $g, g^2, \cdots, g^n, \cdots$　the sequence is finite.

i.e. for some m, $g^m \in \{g, g^2, \cdots, g^{m-1}\}$.

So $g^m = g^j$ for $1 \le j \le m-1$. $\Rightarrow g^{m-j} = 1 \Rightarrow g^{-1} = g^{m-j-1}$.

$\Rightarrow \{1, g, g^2, \cdots, g^{m-j-1}\}$ form a subgp. of G, denoted by $\langle g \rangle$.

denote the order of g: $|\langle g \rangle|$ or $|g|$. (left as HW for a more detailed pf.)

Theorem (Fermat Little Theorem)

Let p be a prime, and $a \in \{1, \cdots, p-1\}$.

Then, $a^{p-1} \equiv 1 \pmod p$.

Pf: Let $G = (\mathbb{Z}_p \setminus \{0\}, \otimes) = (\{1, 2, \cdots p-1\}, \otimes)$, a gp of order $p-1$.

Then $a \in G$, so $k = |a| \mid |G|$, i.e. → Lagrange.

$a^{p-1} = a^{km} = (a^k)^m = 1^m = 1 \in G$.

$a^{p-1} \equiv 1 \pmod p$. □.

Recall. $(\mathbb{Z}_n, \oplus, \otimes)$ is a rng.

$(\mathbb{Z}_n \setminus \{0\}, \otimes)$ is not necessarily a group.

Let $U(n) = \{x \in \mathbb{Z}_n \mid \gcd(x, n) = 1\}$.

Then $(U(n), \otimes)$ is a group of order $\phi(n)$.

Theorem (Euler Theorem).

Let n be a positive integer, and let x be an integer coprime to n,

if $1 \le x < n$, then $x^{\phi(n)} \equiv 1 \pmod{n}$. (Pf left as HW)

Recall. $SL_n(F) < GL_n(F)$.

Ψ $\quad$ Ψ

x $\quad$ g.

we have $g^{-1}xg \in SL_n(F)$, since $\det(g^{-1}xg) = \det(g^{-1})\det(x)\det(g) = 1$.

Def. Let $H \le G$. then H is called a normal subgroup of G if

$H^g \subseteq H$.

$g^{-1}hg \in H$, for all $h \in H$ and all $g \in G$. denoted by $H \triangleleft G$.

$g^{-1}Hg = H$.

Prop. $Z(G) \triangleleft G$. (Pf left as HW).

Pf: $Z(G)$: $hg = gh$ for all $h \in Z(G)$, $g \in G$.

$\Rightarrow g^{-1}hg = g^{-1}gh = h \in H \Rightarrow Z(G) \triangleleft G$. □

2024.9.19. Lecture 3.

$g^{-1}Hg$

Lemma ① $H \triangleleft G$.

our def. ② $g^{-1}Hg = H$

③ $g^{-1}hg \in H \quad \forall h \in H$.

④ $gH = Hg$

$gH = (gHg^{-1})g$

③⇒④: $g^{-1}hg \in H \Rightarrow gg^{-1}hg = hg \in gH \Rightarrow Hg \subset gH$.

Similarly. $gH \subset Hg \Rightarrow gH = Hg$

①, ②, ③, ④ are equivalent.

Eg. $SL_n(F) \triangleleft GL_n(F)$.

Def. Let $N \triangleleft G$, and let $G/N = \{gN \mid g \in G\} = [G:N]$.

and define $(g_1N)\cdot(g_2N) = (g_1g_2)N$. So $(G/N, \cdot)$.

Prop. $(G/N, \cdot)$ is a group. called factor group or quotient group.

Pf: "$\cdot$" is well-defined. (This quotient may have different representatives.)

① $\left(gN\cdot(g_1N)\right)\cdot(g_2N) = (gN)\cdot\left((g_1N)\cdot(g_2N)\right)$.

② N is the identity for $(G/N,\cdot)$.

③ $(gN)^{-1} = g^{-1}N$. □.

Eg. $\left|GL_n(\mathbb{F}_p)/SL_n(\mathbb{F}_p)\right| = p-1$.

$g\in GL_n(\mathbb{F}_p) \Rightarrow g = g_1h$, where $|h|=1$, and

$g_1 = \begin{bmatrix} a & & 0 \\ & 1 & \\ 0 & & \ddots \end{bmatrix}$, with $|a| = \det(g)$.

Claim: $\left(GL_n(\mathbb{F}_p)/SL_n(\mathbb{F}_p),\cdot\right)$ is a cyclic of order $p-1$.

$g = \begin{bmatrix} a & & 0 \\ & 1 & \\ 0 & & \ddots \end{bmatrix}\begin{bmatrix} a^{-1} & & 0 \\ & 1 & \\ 0 & & \ddots \end{bmatrix}\begin{bmatrix} a_{ij} \end{bmatrix}$ where $a = \det(g)\neq 0$.

g_1 $\quad$ h.

$\left\{\begin{bmatrix} a & & \\ & 1 & \\ & & \ddots \end{bmatrix}\middle| a\in\mathbb{F}_p\setminus\{0\}\right\} \subset GL_n(\mathbb{F}_p)$ (also $<$)

$V = F^3$.

$\{(a,0,0)\mid a\in F\}$.

$\{(0,b,0)\mid b\in F\}$.

$\{(a,a,0)\mid a\in F\}$.

"essentially the same".

Def. Two groups $(G,\cdot)$ and $(H,*)$ are said to be isomorphic if there is a one-to-one (bij.) mapping $\phi: G\to H$, $g\mapsto h$, such that $(g_1\cdot g_2)^\phi = g_1^\phi * g_2^\phi$ for all elts $g_1,g_2\in G$. (preserve the operation) $G\cong H$. ϕ: isomorphism.

Eg. Let $G = \left\{\begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix}\middle| c\in\mathbb{F}_p\right\}$. $(G,\cdot)\cong(\mathbb{F}_p,+)$.

HW: $GL_n(p)/SL_n(p)\cong\mathbb{Z}_{p-1}$.

$\phi: \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix}\to c$.

$\begin{bmatrix} 1 & c_1 \\ 0 & 1 \end{bmatrix}\cdot\begin{bmatrix} 1 & c_2 \\ 0 & 1 \end{bmatrix}\overset{\phi}{=}\begin{bmatrix} 1 & c_1+c_2 \\ 0 & 1 \end{bmatrix}$

c_1 + c_2 $=$ c_1+c_2

Def. G is homomorphic to H if a mapping $\phi: G\to H$ st.

$\phi: g_1 \cdot g_2 \to g_1^\phi g_2^\phi$ or $(g_1 g_2)^\phi = g_1^\phi g_2^\phi$. ϕ is a homomorphism.

Eg. Let $G = \left\{ \begin{bmatrix} a & \\ b & \end{bmatrix} \middle| \ a,b \in F \setminus \{0\} \right\}$.

$H = \left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \middle| \ a \in F \setminus \{0\} \right\}$.

$\phi: \begin{bmatrix} a & \\ b & \end{bmatrix} \mapsto \begin{bmatrix} a & \\ 1 & \end{bmatrix}$ homomorphism.

Eg. Let $N \lhd G$. Then G is homomorphic to G/N.

natural homomorphism: $\phi: G \longrightarrow G/N$. by

$g \longmapsto gN$. $\forall g \in G$.

$(g_1 g_2)^\phi \overset{?}{=} g_1^\phi g_2^\phi$

$\| \qquad\qquad \|$

$g_1 g_2 N \qquad (g_1 N)(g_2 N)$

N : normal subgroup $\Rightarrow gN = Ng$.

$(g_1 N)(g_2 N) = g_1 (g_2 N) N = g_1 g_2 (NN) = g_1 g_2 N$.

$(G, \cdot)$ is a group. ϕ: homomorphism.

Def. Let $K = \{ g \in G \mid g^\phi = 1 \} \subset G$. called the kernal of ϕ.

Prop. Then 1° $K \lhd G$ ($G/\ker\phi \cong \mathrm{Im}\,\phi$)

2° $G/K \cong \mathrm{Im}\,\phi$. (The first isomorphism theorem)

1° Proof: ① $K \leq G$ as K is closed under multiplication "$\cdot$".

For $g_1, g_2 \in K$, we have $g_1^\phi = 1$, $g_2^\phi = 1$. so

$(g_1 g_2)^\phi = g_1^\phi \cdot g_2^\phi = 1 \cdot 1 = 1$.

② For $x \in G$ and $h \in K$.

$x^{-1} h x \in K$ as

$(x^{-1} h x)^\phi = (x^{-1})^\phi h^\phi (x)^\phi = (x^{-1})^\phi \cdot 1 \cdot (x)^\phi = (x^{-1})^\phi \cdot (x)^\phi = (x^{-1} \cdot x)^\phi$

$= 1^\phi = 1$.

2° Proof: Define $\Phi: G/K \to \mathrm{Im}\phi$ by $gK \mapsto g^{\phi}$

$gK \mapsto h$

First. Φ is a homomorphism.

Then Φ is an injection.

Clearly, Φ is a surjection.

For any $h \in \mathrm{Im}\phi$, we have $h = g^{\phi}$ for some $g \in G$.

So $\Phi: gK \to h$ is surjective. □.

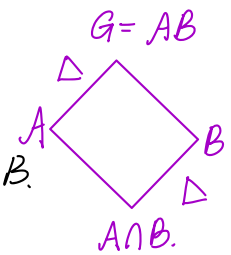
(The second isomorphism theorem).

Let $G = AB = \{ab \mid a \in A, b \in B\}$. (HW)

→ If $G = AB$, then $G = BA$.

Assume $A \lhd G$. then $A \cap B \lhd B$

and $G/A \cong B/(A \cap B)$.



Pf: ① Take $x \in A \cap B$ and $g \in B$.

Then $g^{-1}xg \in A, B$. so $g^{-1}xg \in A \cap B$.

and $A \cap B \lhd B$.

② Define $\varphi: B \longrightarrow G/A$.

$b \longmapsto bA$.

Claim: 1° φ is homomorphism.

2° the kernal of ϕ is $A \cap B$.

$\ker\phi$.

by the first isomorphism thm.

$B/A \cap B \cong G/A$. □.

Let $A, B < G$, then

① $AB = \{ab \mid a \in A, b \in B\} \subseteq G$.

② if $A \lhd G$, then $AB \leq G$.

Pf of ②: Let $a_1b_1, a_2b_2 \in AB$.

where $a_1, a_2 \in A$ and $b_1, b_2 \in B$.

Then $(a_1b_1)(a_2b_2) = a_1b_1a_2b_2$.

$= a_1 b_1 a_2 b_1^{-1} b_1 b_2$

$= (a_1 a_2')(b_1 b_2) \in AB$.

$ab \in AB \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$

$= b^{-1}a^{-1}b\, b^{-1} = a'b^{-1} \in AB$.

So AB is a subgp. of G.

2024. 9. 24. Lecture 4.

Let $H, K \triangleleft G$, we have G/H, G/K.

If $H < K$, then G/H is homomorphic to G/K (surjective) with kernel K/H.
check.

so $(G/H)/(K/H) = G/K$.

Theorem (3rd iso. thm)

Let $H, K \triangleleft G$ s.t. $H < K$. then $(G/H)/(K/H) \cong G/K$.

Idea of pf: $\phi: gH \mapsto gK$

$G/H \longrightarrow G/K$

$\downarrow$ $\quad\quad$ $\searrow$ i.k.

kernal $= K/H$.

Thm 1 If $\phi: G \to H$ is a homo, then $G/\ker\phi \cong G^{\phi} (\leq H)$.

Thm 2 If $G = HK$ and $K \triangleleft G$, then $G/K \cong H/(H \cap K)$. $(H \cap K \triangleleft H)$

Def. Let G, H be groups. Let $X = G \times H = \{(g,h) \mid g \in G, h \in H\}$.

s.t. $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$.

Then. $G \times H$ is a group called a direct product of G and H.

direct sum $G \oplus H$.

Cyclic group: $G = \langle g \rangle$ $\quad$ g: generator.

$= \{g^{\pm i} \mid i \in \mathbb{N}\}$.

Ex. ① $(\mathbb{Z}, +) = \{(\pm i) \cdot 1 \mid i \in \mathbb{N}\}$.

$= \{\pm i \mid i \in \mathbb{N}\}$

② $(\mathbb{Z}_p, \oplus) = \{(\pm i)\cdot 1 \mid i \in \mathbb{N}\}$.

$= \{0, \cdots, p-1\}$.

↳ every element can be a generator.

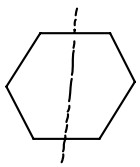
Dihedral group. 二面体群.

Def. Let $G = \{1, a, \cdots, a^{n-1}, b, ab, \cdots, a^{n-1}b \mid |a|=n, |b|=2\}$. where $b^{-1}ab = a^{-1}$.

(a^n; $b = b^{-1}$; $a^{n-1} = a^{-1}$, $b = b^{-1}$)

Claim: G is a group of order $2n$. denoted by D_{2n} or D_n.

Ex.



6 rotations, 60°.

$|a| = 6$.

$|b| = 2$.

$\langle a, b\rangle = D_{12}$. or D_6.

$a^i b = b a^{-i}$.

Pf: $\langle a\rangle = \{1, a, a^2, \cdots, a^{n-1}\}$.

$a^i \cdot a^j = a^{i+j}$ reading $i+j$ modulo n.

$(a^i)^{-1} = a^{n-i}$

① $a^i \cdot (a^j b) = a^{i+j} \cdot b \in G$.

$(a^i b)\cdot(a^j b) = a^i b a^j b = a^i b^{-1} a^j b = a^i a^{-j} = a^{i-j} \in G$.

② $(a^i b)^{-1} = b^{-1} a^{-i} b b = a^i b \in G$.

In particular, $a^i b$ is of order 2. "involution": element of order 2.

Let $\Omega = \{1, 2, \cdots, n\}$.

A 1-1 map from Ω to Ω is called a permutation on Ω.

Let $\mathrm{Sym}(\Omega) = \{$all permutations on $\Omega\}$. $|\mathrm{Sym}(\Omega)| = n!$.

Define multiplication "$\cdot$" by "composition".

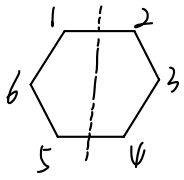
Then, $(\mathrm{Sym}(\Omega), \cdot)$ is a group. called the symmetric group on Ω. denoted S_n.

$\Omega = \{1, 2, 3, 4\}$.

ϕ: $1 \to 2$, $2 \to 4$, $3 \to 3$, $4 \to 1$. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$.

$(1\ 2\ 4)(3)$ cycle form. ↓ simplified. $(1\ 2\ 4)$.

eg. $(2\ 4\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ = $\begin{cases} 2 \to 4 \\ 4 \to 3 \\ 3 \to 2. \end{cases}$



6 rotations, 60°. $|a| = 6$. $|b| = 2$. $\langle a, b \rangle = D_{12}$.

$\begin{cases} a = (1\ 2\ 3\ 4\ 5\ 6) \\ b = (1\ 2)(3\ 6)(4\ 5) \end{cases} \in \mathrm{Sym}(\Omega)$ $\Omega = \{1, 2, 3, 4, 5, 6\}$.

group operation. written as: $i^{ab} = (i^a)^b$.

ab are permutations, not functions.

$ab = (1\ 2\ 3\ 4\ 5\ 6)(1\ 2)(3\ 6)(4\ 5)$ so we compute ab from left to right.

$= (2\ 6)(3\ 5)$.

1	2	3	4	5	6
2	3	4	5	6	1
1	6	5	4	3	2

$(1)(2\ 6)(3\ 5)(4) = (2\ 6)(3\ 5)$

$bab = a^{-1}$.

1	2	3	4	5	6
2	1	6	5	4	3
3	2	1	6	5	4
6	1	2	3	4	5

$(1\ 6\ 5\ 4\ 3\ 2\ 1)$

$bab = (1\ 6\ 5\ 4\ 3\ 2\ 1) = (1\ 6\ 5\ 4\ 3\ 2\ 1)$

$= (1\ 2\ 3\ 4\ 5\ 6)^{-1} = a^{-1}$.

$= (5\ 4\ 3\ 2\ 1\ 6) = \cdots\cdots$

HW: write all elements of S_4.

Lemma! Each permutation of $\Omega = \{1, 2, \cdots, n\}$ can be written as a product of disjoint cycles.

eg. ϕ: $1 \to 6$, $2 \to 3$, $3 \to 4$, $4 \to 2$, $5 \to 5$, $6 \to 1$

Then $\phi = (1\ 6)(2\ 3\ 4)(5)$.

$= (1\ 6)(2\ 3\ 4)$

$= (1\ 6)(2)(3)(4)(5)\ (1)(2\ 3\ 4)(5)(6)$

$|\phi| = 2 \times 3$ → $\phi_1 \sim \phi_m$ are disjoint

If $\phi = \phi_1 \phi_2 \cdots \phi_m$. $|\phi| =$ least common multiple of $(|\phi_1|, |\phi_2|, \cdots, |\phi_m|)$

$(i\ j)$ —— transposition.

Lemma 2. Each permutation can be written as a product of transpositions. (not uniquely).

$(2\ 3\ 1) = (2\ 3)(2\ 1) = (2\ 3)(1\ 2)$.

eg. $(1\ 2\ 3) = (1\ 2)(1\ 3)$.

$(1\ 2\ 3\ 4) = (1\ 2)(1\ 3)(1\ 4)$

$(i_1\ i_2 \cdots i_m) = (i_1\ i_2)(i_1\ i_3) \cdots (i_1\ i_m)$.

The number of transpositions is unique modulo 2.

(parity).

eg. $(1\ 2\ 3) = (1\ 2)(1\ 3)$

$= (1\ 2)(2\ 3)\underbrace{(3\ 2)(1\ 3)(3\ 2)}_{(1\ 2)}(3\ 2)$

$= (1\ 2)(2\ 3)(1\ 2)(3\ 2)$.

$(1\ 2\ 3\ 4) = (1\ 2)(1\ 3)(1\ 4)$

$= (1\ 2)(2\ 3)\underbrace{(2\ 3)(1\ 3)(2\ 3)}_{(1\ 2)}(2\ 3)(1\ 4)$

$= (1\ 2)(2\ 3)(1\ 2)(2\ 3)(1\ 4)$.

Definition. If the number of transpositions appear in a permutation is even, then the permutation is called an even permutation. otherwise, odd permutation.

Lemma. All even permutations in $Sym(\Omega)$ form a proper subgroup of $Sym(\Omega)$. called the alternating group, denote $Alt(\Omega)$ or A_n.

Claim: $A_n \triangleleft S_n$, and $|S_n| = 2|A_n|$. $|A_n| = \frac{1}{2}n!$.

$\Omega = \{1, 2, \cdots, n\}$ Observation: any ele. in A_n is a prod. of 3-cycle.

If ϕ is odd, then $(12)\phi$ is even.

So each odd permutation g of S_n has the form $g = (12)h$, where $h \in A_n$.

Lecture 5. 2024. 9.26.

$A, B \longrightarrow A \times B$.
$A \oplus B$.

$G = (\mathbb{Z}_{15}, \oplus)$. $|G| = 15$.

$= \langle 1 \rangle = \{1, 2, 3, \cdots, 14, \overset{\circ}{15}\}$

Let $A = \langle 3 \rangle = \{3, 6, 9, 12, \overset{\circ}{15}\}$. $|A| = 5$.

$B = \langle 5 \rangle = \{5, 10, \overset{\circ}{15}\}$ $|B| = 3$.

Correspond with HW3 Prob. 10.

Claim: $G = AB$. $G \cong A \times B$. (Chinese Remainder Thm ?).

$g = a \oplus b$.

Thm. Let $H, K \triangleleft G$ such that $G = HK$. TFAE.

(1) $\phi: H \times K \longrightarrow G$
$(h, k) \longmapsto hk$ is an isomorphism.

(2). $H \cap K = \{e\}$, where e is the identity.

Proof: (1) $\Rightarrow$ (2). Assume ϕ is iso.

Suppose $x \in H \cap K$ st $x \neq e$.

Then, $\phi: (x, e) \longmapsto xe = x$
$\neq$ $\quad$ $\|$
$(e, x) \longmapsto ex = x$. Contradiction. So $H \cap K = \{e\}$.

(2) $\Rightarrow$ (1). Assume $H \cap K = \{e\}$.

We need to prove that ϕ is a homomophism and a bijection.

Claim: $hk = kh$ for any $h \in H,\ k \in K$.

Consider $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = k'k^{-1} \in K$.

and $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) = hh' \in H$.

$\Rightarrow hkh^{-1}k^{-1} \in H \cap K \Rightarrow hkh^{-1}k^{-1} = e. \Rightarrow hk = kh.$

① homo.

$$\left((h_1,k_1)(h_2,k_2)\right)^{\phi} = (h_1h_2, k_1k_2)^{\phi} = (h_1h_2)(k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2$$

$$= (h_1k_1)(h_2k_2) = (h_1,k_1)^{\phi}(h_2,k_2)^{\phi}.$$

② by def, ϕ is surj. as $G = HK$.

③ The kernal of $\phi = \{(h,k) \in H \cap K \mid (h,k)^{\phi} = e\}$

$$= \{(h,k) \in H \cap K \mid hk = e\}$$

Then, $k = h^{-1} \in H \cap K = \{e\}$. Similarly $h = e$. $\Rightarrow$ the kernal is trivial.

$\Rightarrow \phi$ is inj.

Thus, ϕ is iso. and $H \times K \cong G$. $\square$.

$H \times K \cong G$ ↓ inner direct prod.

Notation: $G = H \times K = HK$. (H, K are diff. subgp.)

Warning: $G = Z_3 \times Z_3$

$$= H \times H = \{(h_1,h_2) \mid h_1,h_2 \in H\}.$$

$$\neq \underbrace{HH}_{=H}.$$

Let $G = \left\{ \begin{bmatrix} a & 0 & 0 \\ 0 & b_1 & b_2 \\ 0 & b_3 & b_4 \end{bmatrix} \;\middle|\; \begin{array}{l} a_i \in \mathbb{F}_p \setminus \{0\}. \\ b_i \in \mathbb{F}_p. \\ b_1b_4 - b_2b_3 \neq 0. \end{array} \right\}$.

Then G is a group with mat. mult. $G < GL_3(\mathbb{F}_p)$.

Claim: $G \cong \mathbb{Z}_{p-1} \times GL_2(\mathbb{F}_p)$. (thinking about block mat.)

Let $A = \left\{ \begin{bmatrix} a & 0 \\ 0 & I_2 \end{bmatrix} \middle| \; a \in \mathbb{F}_p \setminus \{0\} \right\}$

$$B = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & \begin{matrix} b_1 & b_2 \\ b_3 & b_4 \end{matrix} \end{bmatrix} \middle| \begin{matrix} b_i \in \mathbb{F}_p \\ b_1 b_4 - b_2 b_3 \neq 0 \end{matrix} \right\}$$

Then $G = A \times B \cong \mathbb{Z}_{p-1} \times GL_2(\mathbb{F}_p)$.

$H < G$

/

maximal subgroup: If $H \leq K \leq G$, then $K = H$ or $K = G$.

Def. subgps. of $Sym(\Omega)$ are called permutation groups on Ω.

Let $G \leq Sym(\Omega)$, then G is called transitive on Ω 可迁的.

if for any $\omega_1, \omega_2 \in \Omega$, there is a $g \in G$ s.t. $\omega_1 g = \omega_2$.

Otherwise, G is intransitive on Ω.

HW. ① Let $G = S_n$. Describe maximal intransitive subgps of G.

② Let $G = GL_n(\mathbb{F}_p)$ Describe max. subgroups of G which fixes a 1-subspace of $\mathbb{F}_p^n$. (1 dimentional subspace.)

Let $G = \langle g \rangle = \mathbb{Z}_n$.

(1) If $n = lm$ s.t. $\gcd(l, m) = 1$. then $\mathbb{Z}_n = \mathbb{Z}_l \times \mathbb{Z}_m$.

(2) If $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ where $p_1, p_2, \cdots, p_r$ are distinct primes.

then $\mathbb{Z}_n = \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}}$.

Let G be a group of order p^2, where p is a prime.

Then, either $G \cong \mathbb{Z}_{p^2}$, or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Observe that $g \in G$ has order p or p^2.

If $|g| = p^2$, then $\langle g \rangle = \{g, g^2, \cdots\cdots, \underset{\| }{g^{p^2}}\}$. So $G = \langle g \rangle$ is cyclic.
1.

Suppose G does not have elts of order p^2.

Let $a \in G \setminus \{1\}$. then $\langle a \rangle \cong \mathbb{Z}_p$.

Let $b \in G \setminus \langle a \rangle$. then $\langle b \rangle \cong \mathbb{Z}_p$.

Further, $\langle a \rangle \cap \langle b \rangle = \{1\}$ and $G = \langle a \rangle \langle b \rangle$. (Prove G Abelian).

HW. Prove $G = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Thm (Fundamental Theorem for Finite Abelian Groups).

Let G be a finite abelian group of order n, and let $n = p_1^{e_1} \cdots p_r^{e_r}$.

Then (1) $G = G_1 \times G_2 \times \cdots\cdots \times G_r$, where $|G_i| = p_i^{e_i}$.

(2) G is a direct product of cyclic subgroups.

Proof: (1) Let $n = p^e m$ s.t p is a prime and $p \nmid m$. otherwise $|H| \neq p^e$.

Let $H = \{g^m \mid g \in G\}$. then H is a subgroup, and every elt of H has order p-power. ($|G| = p^e m$. $H^{p^e} \subseteq G$).

Moreover, $|H| = p^e$, and $G = H \times K$. where $|K| = m$.

Repeat this process, we'll finish the proof of (1).

(2). Assume that $|G| = p^e$

Let $g \in G$ which has the largest order. i.e $|g| \geq |h|$ for any $h \in G$.

If $G = \langle g \rangle$, then we are done.

Suppose $G \neq \langle g \rangle$.

Claim: $G = \langle g \rangle \times H$ for some $H < G$.

(i). Let $h \in G \setminus \langle g \rangle$ s.t. $h^p \in \langle g \rangle$.

$h \in G \setminus \langle g \rangle$.

If $h^p \notin \langle g \rangle$. then $h^{p^2} \in \langle g \rangle$ or $h^{p^2} \notin \langle g \rangle$.

$(h^p)^p$.

$(h^{p^2})^p$ keep going.

So $h^p = g^k$ for some integer k. Since $|g| \geq |h|$, $k = pl$.

for some integer l.

Let $x = h^{-1} g^l$. Then $|x| = p$ as $x^p = h^{-p} g^{lp} = h^{-p} g^k = 1$.

and $x \notin \langle g \rangle$ since $h \notin \langle g \rangle$.

(iii). Let $\bar{G} = G/\langle x \rangle$. then $|\bar{G}| < |G|$.

$|\bar{g}|$ is the largest order in $|\bar{G}|$. By induction, we may

assume $\bar{G} = \langle \bar{g} \rangle \times \bar{H}$ where $\bar{g}$ is the image of g in $\bar{G}$.

(iii). Let H be the full preimage of $\bar{H}$ under $\bar{H}$ under $G \to \bar{G}$.

i.e. $H = \{h \in G \mid \bar{h} \in \bar{H}\}$.

Then $H < G$ and $\langle g \rangle \cap H = \{1\}$.

Thus, $G = \langle g \rangle H = \langle g \rangle \times H$, as claimed.

Lecture 6. 2024.10.8. (Back to gps later).

Ring $(R, +, \cdot)$

$(R, +)$ abelian group.

$(R, \cdot)$ semi-groups. (only have associativity).

$a \cdot (b+c) = a \cdot b + a \cdot c$.

$(b+c) \cdot a = b \cdot a + c \cdot a$.

(left & right distributivity).

Note: $0 \cdot a = 0$. → identity of addition

Given $a \in R$.

if $ba = 1$. then b is <u>left inverse</u>.

if $ab = 1$. then b is <u>right inverse</u>.

Further. if $ab = ba = 1$. b is a's <u>inverse</u>

Sometimes, $a \neq 0, b \neq 0$ but $ab = 0$. e.g. in mat. ring. $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ & $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$.

a, b: <u>zero factor</u> of each other.

① If $ab = ba$, $\forall a, b \in R$. then R is a <u>commutative ring</u>.

② If each elt of R is invertible, then R is a <u>division ring</u>. 除环.

③ If R is commutative (with identity) and has no zero factor, then R is an <u>integral domain</u> 整环.

(R should also have <u>at least 2 elts</u> and identity for multiplication). $0 \neq 1$

e.g. ① $(\mathbb{Z}, +, \cdot)$ integral domain.

② $(\mathbb{Z}/m\mathbb{Z}, \oplus, \otimes)$ commutative ring. for all m.

{ division ring / integral domain } for prime m.

③ $(M_n(\mathbb{F}), +, \times)$ neither commutative nor division ring.

④ $(\mathbb{F}[x], +, \times)$ integral domain.

<u>Def</u>. A subset S of a ring $(R, +, \times)$ is called a subring if $(S, +, \times)$ is a ring ($S \leq R$.)

e.g. ① $(2\mathbb{Z}, +, \times)$ is a subring of $(\mathbb{Z}, +, \times)$.

$(3\mathbb{Z}, +, \times)$ is a subring of $(\mathbb{Z}, +, \times)$.

.....

② diagonal matrices in $(M_n(\mathbb{F}), +, \times)$ form a subgroup of $(M_n(\mathbb{F}), +, \times)$

③ $\{ f(x) \cdot x \mid f(x) \in \mathbb{F}[x] \}$ form a subgroup of $(\mathbb{F}[x], +, \times)$.

常数项为0的全体A'.

Def. A subring I of R is called an ideal (理想) if $rI, Ir \subset I$ for all elts. $r \in R$. $(I \lhd R)$

e.g. ① $(2\mathbb{Z}, +, \times)$ is a subring of $(\mathbb{Z}, +, \times)$. ideal.

$(3\mathbb{Z}, +, \times)$ is a subring of $(\mathbb{Z}, +, \times)$. ideal.

.....

$rI = \{rx \mid x \in I\}$.

Note: $rI \neq I$.

$5(2\mathbb{Z}) \subsetneq 2\mathbb{Z}$.

② diagonal matrices in $(M_n(\mathbb{F}), +, \times)$ form a subgroup of $(M_n(\mathbb{F}), +, \times)$ × ideal.

③ $\{f(x)\cdot x \mid f(x) \in \mathbb{F}[x]\}$ form a subgroup of $(\mathbb{F}[x], +, \times)$. ideal.

($f(x)$: 无常数项的多项式)

Def. For a ring R and an ideal I of R, Let $R/I := \{r+I \mid r \in R\}$, and (additive) quotient ring

$(r_1+I) \oplus (r_2+I) = (r_1+r_2)+I$.

$(r_1+I) \otimes (r_2+I) = (r_1 \cdot r_2)+I$.

Rmk: why ideal?

$(r_1+I)\times(r_2+I) = r_1r_2 + r_1I + Ir_2 + II = r_1r_2 + I$.

$II \neq I$. ×

$I = 2\mathbb{Z}$.

$II = 4\mathbb{Z}$.

we only have $II \subseteq I$.

But I is considered as $\bar{0}$.

- $(R/I, \oplus, \otimes)$ is a ring. (⊕, ⊗: Formal symbol. actually + & ×.)

e.g. $\mathbb{Z}/2\mathbb{Z} = \{2\mathbb{Z}, 1+2\mathbb{Z}\}$.

$= \{0, 1\}$. also a field.

$\mathbb{Z}/m\mathbb{Z} = \{\bar{1}, 1+I, \cdots, (m-1)+I\}$.

$\mathbb{F}[x]/x\mathbb{F}[x] = \{I, r+I\}$. (r: const.)

$\mathbb{F}[x]/x^2\mathbb{F}[x] = \{a+I, bx+I\}$

$= \{a+bx \mid a,b \in \mathbb{F}\}$.

$\mathbb{F}[x]/x^3\mathbb{F}[x] = \{a+bx+cx^2 \mid a,b,c \in \mathbb{F}\}$.

Proposition 6. Let R be a ring and let I be an ideal of R. Then the (additive) quotient group R/I is a ring under the binary operations:

$$(r+I)+(s+I) = (r+s)+I \quad \text{and} \quad (r+I)\times(s+I) = (rs)+I$$

for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well defined, then I is an ideal of R.

$rs + rI + Is + II$.

$2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$

$= (2)$. generated by 2.

(a): ma, $-ma$, na^k

$(a) = \{\sum_{\text{finite}} r_i a^i + a^j s_j + r_1 a^k r_2 + ma^l \mid i,j,k,l \in \mathbb{N}, r_i, s_j, r_1, r_2 \in R\}$.

Def. Let $M \subset R$. The ideal generated by M is the intersection of the ideals which contain M. denoted by (M).

$(R_1, +_1, \times_1)$, $(R_2, +_2, \times_2)$.

$\varphi: R_1 \to R_2$ is a homomorphism if

- $(r_1 + r_2)^\varphi = r_1^\varphi +_2 r_2^\varphi$, $\forall r_1, r_2 \in R_1$.
- $(r_1 \times r_2)^\varphi = r_1^\varphi \times_2 r_2^\varphi$, $\forall r_1, r_2 \in R_1$.

$\ker\varphi = \{r \in R_1 \mid r^\varphi = 0_2\} \subseteq R_1$.

$\operatorname{im}\varphi = \{r^\varphi \mid r \in R_1\} \subseteq R_2$.

Definition. Let R and S be rings.

(1) A *ring homomorphism* is a map $\varphi : R \to S$ satisfying

- **(i)** $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$ (so φ is a group homomorphism on the additive groups) and
- **(ii)** $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

(2) The *kernel* of the ring homomorphism φ, denoted $\ker\varphi$, is the set of elements of R that map to 0 in S (i.e., the kernel of φ viewed as a homomorphism of additive groups).

(3) A bijective ring homomorphism is called an *isomorphism.*

consider as the "same".

Lemma. ① $\ker\varphi$ is an ideal of R_1.

② $\operatorname{im}\varphi$ is a subring of R_2.

Moreover, $R_1/\ker\varphi \cong \operatorname{im}\varphi \leq R_2$.

Proof: ① If $r \in \ker\varphi$ and $s \in R$, then $rs \in \ker\varphi$

since $(rs)^\varphi = r^\varphi s^\varphi = 0 \cdot s^\varphi = 0$.

(Also check: subring).

Theorem 7.

(1) *(The First Isomorphism Theorem for Rings)* If $\varphi : R \to S$ is a homomorphism of rings, then the kernel of φ is an ideal of R, the image of φ is a subring of S and $R/\ker\varphi$ is isomorphic as a ring to $\varphi(R)$.

(2) If I is any ideal of R, then the map

$R \to R/I$ defined by $r \mapsto r + I$

is a surjective ring homomorphism with kernel I (this homomorphism is called the *natural projection* of R onto R/I). Thus every ideal is the kernel of a ring homomorphism and vice versa.

R之沐恩.

$\bar{\varphi}: R_1/\ker\varphi \longrightarrow \operatorname{Im}\varphi$.

$r + \ker\varphi \longmapsto r^\varphi$. Claim: $r_1 + \ker\varphi = r_2 + \ker\varphi \iff r_1^\varphi = r_2^\varphi$.

$r_1 + \ker\varphi,\ r_2 + \ker\varphi \longmapsto r_1^\varphi, r_2^\varphi$. $\bar{\varphi}$ iso ✓.

I is an ideal of R.

Thm 1. Let $I \lhd R$ and let

$\pi: R \to R/I$.

$r \mapsto r + I$. (natural homo.)

Then, (1) The ideals of R containing I and ideals of R/I are one-to-one correspondence.

(2) If $I \lhd J \lhd R$, then $R/J \cong (R/I)/(J/I)$.

Thm 2. Let $I \lhd R$, $S \leq R$. Then $I+S$ is a subring of R, and

(1) $S \cap I \lhd S$, & $I \lhd I+S$.

(2) $(I+S)/I \cong S/(S \cap I)$.

$i + s + I \mapsto s + S \cap I$. iso ✓.

Theorem 8. Let R be a ring.

(1) *(The Second Isomorphism Theorem for Rings)* Let A be a subring and let B be an ideal of R. Then $A + B = \{a + b \mid a \in A,\ b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and $(A + B)/B \cong A/(A \cap B)$.

$S \neq I$

$(R,+,\times)$, $(S,+,\times)$ are rings.

$R \times S = \{(r,s) \mid r \in R, s \in S\}$.

$(r_1,s_1)+(r_2,s_2) = (r_1+r_2, s_1+s_2)$.

$(r_1,s_1)\times(r_2,s_2) = (r_1 r_2, s_1 s_2)$.

$R \times S$ is a ring.

$$\frac{\{(r,0) \mid r \in R\}}{I} \oplus \frac{\{(0,s) \mid s \in S\}}{J}$$

Lecture 7. 2024. 10. 10.

Division ring R: 体

each none-zero elt. of R has inverse.

Further, a commutative division ring is a field.

Ex. (a division ring, not field).

Let $R = \left\{ \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} \middle| \alpha, \beta \in \mathbb{C} \right\}$.

where $\bar{\alpha} = \overline{a+bi} = a-bi$.

Then $R \subsetneq M_2(\mathbb{C})$. and R is a division ring, which is not commutative. Quaternion Ring 四元素环.

$\mathbb{C} = \{a+bi \mid a,b \in \mathbb{R}\}$

$= \mathbb{R}(i)$. $i = \sqrt{-1}$.

Check: ① R is a ring. ✓.

② $\begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix}^{-1} = \frac{1}{\alpha^2+\beta^2} \begin{bmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{bmatrix} \in R$.

③ R is not commutative ring.

Let E be a field. $F \subset E$ be a subfield. Then E is called an extension field of F.

- $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. $\mathbb{Q}$ is the smallest field: $1 \in S$ (any field) $\Rightarrow 1, 1+1, 1+1+1, \cdots \in S$.

  $-1, -2, -3, \cdots \in S$.

  $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \cdots \in S$.

  $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \cdots \in S$. $\mathbb{Q} \subset S$.

$\mathbb{Q} \subset S \subset \mathbb{R}$.

① $S_1 = \mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$. $\quad S_2 = \mathbb{Q}(\sqrt{3}) = \{a+b\sqrt{3} \mid a,b \in \mathbb{Q}\}$.

↓ commutative ring.

$\frac{1}{a+b\sqrt{2}} = \frac{1}{a^2+2b^2}(a-b\sqrt{2}) \in S_1$.

$S_3 = \mathbb{Q}(\sqrt{n}) = \{a+b\sqrt{n} \mid a,b \in \mathbb{Q}\}$.

$S_1 \ncong S_2$ Suppose iso $\phi : S_1 \to S_2$.

$1 \mapsto 1$

$\sqrt{2}\cdot\sqrt{2} = 2 \mapsto 2 = (\sqrt{2})^\phi \cdot (\sqrt{2})^\phi$.

$(\sqrt{2})^\phi \in \mathbb{Q}(\sqrt{3})$.

$=$ $a+b\sqrt{3}$ for some $a,b \in \mathbb{Q}$

$2 = 2^\phi = (\sqrt{2})^\phi \cdot (\sqrt{2})^\phi = a^2+3b^2+2ab\sqrt{3}$. $\Rightarrow ab=0$.

$\Rightarrow a=0$ or $b=0$. $\quad 2=a^2+3b^2 = a^2$ or $3b^2$.

where $a,b \in \mathbb{Q}$. $\quad 2=a^2$. ↯. $\quad 2=3b^2$. ↯.

② $S = \mathbb{Q}(2^{\frac{1}{3}})$, the smallest subfield of $\mathbb{R}$ which contains $\mathbb{Q}$ and $2^{\frac{1}{3}}$.

$S = \mathbb{Q}(2^{\frac{1}{3}}) = \{a+b2^{\frac{1}{3}}+c2^{\frac{2}{3}} \mid a,b,c \in \mathbb{Q}\}$.

Check: $(a+b2^{\frac{1}{3}}+c2^{\frac{2}{3}})^{-1} = a_1+b_1 2^{\frac{1}{3}}+c_1 2^{\frac{2}{3}} \in S$.

Let $F = \mathbb{Q}$ or $\mathbb{F}_p$.

Let $R = F[x]$. → commutative ring.

Take $p(x) \in R$ such that $p(x)$ is irreducible. ← If $p(x) = f(x)g(x)$ then $f(x) = a$ or $g(x) = b$, a,b const.

$2^{\frac{1}{3}}$

$p(x) = x^3-2$. irreducible.

Let $I = (p(x))$. → $\{f(x)p(x) \mid f(x) \in R\}$. 主理想.

$I = (p(x)) = (x^3-2) = \{(x^3-2)f(x) \mid f(x) \in R\}$.

Theorem. R/I is a field. (We have already known the quotient ring is a ring.)

Proof: The elts of R/I have the form $f(x)+(p(x))$. where $f(x) \in R$.

Suppose $f(x)+I$ has an inverse, say $g(x)+I = (f(x)+I)^{-1}$.

Then, $g(x)+I \in R/I$.

$g(x)+(x^3-2) \subset R$.

view $x^3 = 2$. Since $I = (x^3-2)$.

i.e. $(f(x)+I)(g(x)+I) = 1+I$.

$\quad\quad$ ‖ ⟶ I is an ideal.

$\quad\quad f(x)g(x)+I$

e.g. $g(x) = x^4+ax^3+bx^2+cx+d$.

$g(x)+I = \underbrace{(bx^2+(c+2)x+d+2a)}_{g_0(x)} + I$.

$\Rightarrow f(x)g(x) = 1 + p(x)q(x)$ for some $q(x) \in R$.

i.e. $f(x)g(x) - p(x)q(x) = 1$.

This is true due to $\gcd(f(x), p(x)) = 1$. as $p(x)$ is irreducible.

So $R/I = \{g_0(x)+I \mid g_0 \in R \text{ and } \deg g_0 \le 2\}$.

$\cong \{g_0(2^{\frac{1}{3}}) \mid g_0 \in R \text{ and } \deg g_0 \le 2\}$.

$= \{a(2^{\frac{1}{3}})^2 + b2^{\frac{1}{3}} + c \mid a,b,c \in \mathbb{Q}\}$.

We know $\mathbb{F}_p$. p prime.

Is there a field of order 6? 8? 9? 10?

Let $F = \mathbb{F}_3 = (\{0,1,2\}, \oplus_3, \otimes_3)$.

Let $p(x) = x^2+1$. irreducible (need check). If $x^2+1 = (ax+b)(a_1x+b_1)$. $a_1a x^2 + (ab_1+ba_1)x + bb_1 = x^2+1$.

$F[x]/(x^2+1) = \{a+b\alpha \mid a,b \in F,\ \alpha^2 = -1 = 2\}$. 9 elts. is a field of order 3^2.

Thm. If F is a finite field, then $|F| = p^d$, where p prime, $d \geq 1$.

Find a irreducible polynomial of deg 2 over $\mathbb{F}_2 = \{0,1\}$.

$x^2+1 = x^2-1 = (x+1)(x-1) = (x+1)^2$ not irr.

$p(x) = x^2+x+1$ irr.

$\Rightarrow \mathbb{F}_2[x]/(x^2+x+1)$ is a field of order 4.

Is there a field of order 6?

Let F be a field. Let n be the smallest positive integer s.t. $n \cdot 1 \equiv 0$. (If such n doesn't exist, define $\mathrm{char}(F) = 0$.)
Then n is called the characteristic of F. denoted $\mathrm{char}(F)$

Lemma. The char of a field is either 0 or a prime number.

Proof: If n exists and $n = pq$. then $(p\cdot 1)\cdot(q\cdot 1) = (pq)\cdot 1 = 0$

Since $p\cdot 1 \neq 0$. $q\cdot 1 \neq 0$. this is not possible. $p\cdot 1$, $q\cdot 1$ are zero factors.
But they are in a field.

e.g. $\mathrm{char}(\mathbb{Q}) = 0$. $\mathrm{char}(\mathbb{F}_3) = 3$.
$\mathrm{char}(\mathbb{R}) = 0$. $\mathrm{char}(\mathbb{F}_9) = 9$. $\mathbb{F}_9 \triangleq \mathbb{F}_3(\alpha) = \{a+b\alpha \mid a,b \in \{0,1,2\}\}$.
$\mathrm{char}(\mathbb{C}) = 0$.

The characteristic of a field of order p^d is p.

Thus there is no order 6 field.

→ prime fields.

Theorem. Any field F contains a subfield which is iso to $\mathbb{Q}$ or $\mathbb{F}_p$ for some prime p

Proof: Let E be the smallest subfield of F. Then $0, 1 \in E$. and hence $n\cdot 1 \in E$ and $\frac{n}{n}\cdot 1 \in E$.

If char $F=0$, then $E \cong \mathbb{Q}$
$n\cdot 1 \mapsto n$.

If char $F=p$, then $E \cong \mathbb{F}_p$.

Lecture 8. 2024.10.17

Thm. Let G be a finite abelian group.

Then G is direct prod. of cyclic groups of order prime number.

Proof: $|G| = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$.

① $G = G_{p_1} \times G_{p_2} \times \cdots \times G_{p_t}$, where $|G_{p_i}| = p_i^{e_i}$.

② Assume $|G| = p^e$. and G is not cyclic.

$g \in G$.
$|g| = p_1^{f_1} p_2^{f_2} \cdots p_t^{f_t}$
$g = g_{p_1} g_{p_2} \cdots g_{p_t}$ with $|g_{p_i}| = p_i^{f_i}$.

Lemma: Let $g \in G$, which has the largest order.

Then $G = \langle g \rangle \times H$ for some $H < G$.

Induction: order: $|G| = p^1 \Rightarrow |G|$ cyclic. ✓.
$|G| = \langle g \rangle \times \langle 1 \rangle$, $|g| = p$.

Suppose $|G| = p^{e-1}$, $G = \langle g \rangle \times H$ for some $H < G$.
Prove for $|G| = p^e$. induction.

Proof of Lemm:

Claim: There exists $h \in G$ s.t. $\langle h \rangle \cap \langle g \rangle = 1$ and $|h| = p$.

Since $G \neq \langle g \rangle$, there is $y \in G \setminus \langle g \rangle$ such that $y^p \in \langle g \rangle$.

Then $y^p = g^j = g^{pk}$. (Since $|g|$ is the largest).

Let $h = y^{-1} g^k$, then $h \neq 1$ and $h^p = y^{-p} g^{pk} = 1$. So $|h| = p$.

If $h \in \langle g \rangle$, then $y^{-1} g^k \in \langle g \rangle$, so $y^{-1} \in \langle g \rangle$ ↯.

So $h \notin \langle g \rangle$.

$\langle \bar{g} \rangle$.
$\langle g \rangle < G$.
$\frac{\langle g \rangle}{\langle g \rangle \cap \langle h \rangle} \cong \frac{\langle g \rangle \langle h \rangle}{\langle h \rangle} < \frac{G}{\langle h \rangle}$.
$\| S$
$\langle g \rangle$.

Let $\bar{G} = G/\langle h \rangle$. Then $|\bar{G}| < |G|$ and $|\bar{g}| = |g|$ is the largest order of elts in $\bar{G}$.

By induction. $\bar{G} = \langle \bar{g} \rangle \times \bar{H}$.

$|g| = |\bar{g}|$.

Let H be the full preimage of $\bar{H}$ under $G \to \bar{G}$. $|\bar{G}| = |\bar{g}|\,|\bar{H}|$

Then $|H| = |\bar{H}|\,p$. $|G| = |g|\,|H|$

Claim: $\langle g \rangle \cap H = 1$.

Suppose $1 \neq x \in \langle g \rangle \cap H$. Then $\bar{x} = \bar{1}$ as $\langle \bar{g} \rangle \cap \bar{H} = \bar{1}$.

So $x \in \langle h \rangle$ and $x = h^i$, with $(i,p) = 1$. Thus $h \in \langle g \rangle$ ↯. ($h^i \in \langle g \rangle$.)

Therefore, $\langle g \rangle \cap H = 1$, and $G = \langle g \rangle \times H$. ($|G| = |g| \cdot |H|$.)

The lemma is proved. #.

Proof of thm: $G = \langle g \rangle \times H$

$= \langle g \rangle \times (\langle g_1 \rangle \times \cdots \times \langle g_t \rangle)$. □.

Solvable group

G: finite group.

For $x, y \in G$, let $[x,y] = x^{-1}y^{-1}xy$. called the commutator of x and y.

Def. Let $G' = \langle [x,y] \mid x,y \in G \rangle$.

Then $G' \lhd G$. called the commutator subgroup, denoted by G'. 換位子群.

For any $g \in G$. $g^{-1}[x,y]g = g^{-1}x^{-1}y^{-1}xyg = g^{-1}x^{-1}g\ g^{-1}y^{-1}g\ g^{-1}xg\ g^{-1}yg$.

$= (x^g)^{-1}(y^g)^{-1}x^g y^g = [x^g, y^g] \in G'$.

eg. ① Let $G = \langle a, b \rangle = D_{2n}$. where $|a| = n$, $|b| = 2$. $a^b = a^{-1} = b^{-1}ab$.

Then $G' = \begin{cases} \langle a \rangle, & \text{if } n \text{ odd.} \\ \langle a^2 \rangle, & \text{if } n \text{ even.} \end{cases}$ and $G/G' = \begin{cases} \langle \bar{b} \rangle = C_2. \\ \langle \bar{a}, \bar{b} \rangle = C_2 \times C_2. \end{cases}$

② If G is abelian, then $G' = \{1\}$.

Lemma 1 $G' \lhd G$. and G/G' is abelian.

Proof: Let $\bar{x}, \bar{y} \in \bar{G} = G/G'$.

Let x, y be the preimages of $\bar{x}, \bar{y}$ under $G \to \bar{G}$ respectively.

Then $[x,y] = x^{-1}y^{-1}xy \in G'$ by def. and

$$\overline{x^{-1}y^{-1}xy} = \bar{1}$$
$$\| $$
$$\bar{x}^{-1}\bar{y}^{-1}\bar{x}\bar{y}$$

$\Rightarrow \bar{x}\bar{y} = \bar{y}\bar{x}$. and $\bar{G}$ abelian. $\square$.

Lemma 2. For any $H \lhd G$. G/H is abelian $\Leftrightarrow G' \leq H$.

G' is the least normal subgroup of G. s.t. G/G' abelian.

Proof: ($\Leftarrow$)

If $G' \leq H$, then $G/H \cong \dfrac{G/G'}{H/G'}$ is abelian,

($\Rightarrow$). Assume G/H is abelian.

$xyH = yxH$. $x^{-1}y^{-1}xyH = H \Rightarrow [x,y] \in H$.

Then for any $\bar{x}, \bar{y} \in \bar{G} = G/H$. $\bar{x}\bar{y} = \bar{y}\bar{x}$. i.e. $\bar{x}^{-1}\bar{y}^{-1}\bar{x}\bar{y} = \bar{1}$.

Let x, y be preimages of $\bar{x}, \bar{y}$ respectively.

Then $x^{-1}y^{-1}xy \in H$.

Solvable groups.

$G \rhd G' \rhd (G')' = G'' \rhd \cdots \rhd G^{(n)} \rhd \cdots$, where $G^{(n)} = (G^{(n-1)})'$.

Since G finite, there exists n. s.t. either $G^{(n)} = 1$. or $G^{(n)} = G^{(n+1)}$.

Def. A finite group G is called a solvable group if $G^{(n)} = 1$ for some integer n.

Otherwise, G is non-solvable. Specifically, if $G' = G$, G is a perfect group.

Prop. A group G is solvable $\Leftrightarrow$ there exists a subgroup chain $G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_s = 1$.

s.t. G_i/G_{i+1} is abelian for all i. $G/G_1, G/G_2, \cdots, G/G_s$.

abelian.

Proof: ($\Rightarrow$) clearly true.

($\Leftarrow$) Assume $G = G_0 \rhd G_1 \rhd \cdots G_s = 1$ exists s.t. G_i/G_{i+1} is abelian.

Claim: $G^{(i)} \leq G_i \ \forall i$. (by induction).

First. $G' \leq G_1$ as G/G_1 is abelian, and by Lem. 2.

Suppose $G^{(i)} \leq G_i$ for some $i \geq 1$.

Since G_i/G_{i+1} is abelian, $G_i' \leq G_{i+1}$.

Thus $G^{(i+1)} = \left(G^{(i)}\right)' \leq G_i' \leq G_{i+1}$. so the claim holds.

and $G^{(s)} \leq G_s = 1$. G is solvable. #.

$x \overset{g}{\mapsto} g^{-1}xg$ $\quad G \to G$ $\quad g, x \in G$.

conjugate $\quad$ 1-1.

induces an automorphism of G called an inner automorphism.

Theorem 20. *(The Fourth or Lattice Isomorphism Theorem)* Let G be a group and let N be a normal subgroup of G. Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\overline{A} = A/N$ of G/N. In particular, every subgroup of $\overline{G}$ is of the form A/N for some subgroup A of G containing N (namely, its preimage in G under the natural projection homomorphism from G to G/N). This bijection has the following properties: for all $A, B \leq G$ with $N \leq A$ and $N \leq B$,

(1) $A \leq B$ if and only if $\overline{A} \leq \overline{B}$, ✓.
(2) if $A \leq B$, then $|B : A| = |\overline{B} : \overline{A}|$, ✓.
(3) $\overline{\langle A, B \rangle} = \langle \overline{A}, \overline{B} \rangle$, ✓.
(4) $\overline{A \cap B} = \overline{A} \cap \overline{B}$, and ✓.
(5) $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$. ✓.

one-to-one correspondence.

everything corresponds!