1. Group & subgroup

Z_n, $\mathbb{Z}/n\mathbb{Z}$: 模n加法群
$U(p)$, 模p乘法群
⊕ 外直积, × 内直积, "·" 群运算.

① def: group, subgroup, order of g and G

② prop of group
1) unique identity: $ee' = e = e'$
2) cancellation: ∃ inverse
3) unique inverse: I. $(a^{-1} = b = b')$ $bab' = b = b'$ II. just by cancelling
4) socks-shoes $(ab)^{-1} = b^{-1}a^{-1}$

③ subgroup test 1) $ab^{-1} \in H$ 2) $ab \in H \wedge a^{-1} \in H$ 3) $ab \in H \wedge |H| < \infty$

④ $A < G, B < G \Rightarrow A \cap B < G$; $A \cup B \neq A \cdot B$, $A \cdot B < G$

2. Center & centralizer

① $Z(G) := \{a \mid \forall x \in G, ax = xa\}$
$C(x) := \{a \mid ax = xa\}$

② $Z(G), C(x)$ is subgroup of G

3. Cyclic group: $\langle a \rangle$, $|\langle a \rangle| = n$.

prop: ① $a^i = a^j \Leftrightarrow n \mid i-j$: write as $kn + r\ (r<0)$ Cor: $|a^b| \,\big|\, |a|$ $|b|$ for general finite group

② $\langle a^k \rangle = \langle a^{(n,k)} \rangle$: (Bézout's lemma) $xn + yk = d$ Cor: $|\langle a^k \rangle| = \frac{n}{(k,n)}$

③ FTCG: 1) subgroup is cyclic : take smallest positive m s.t. $a^m \in H$. then $H = \langle a^m \rangle$
2) divisors of n $\overset{1\text{-to-}1}{\longleftrightarrow}$ subgroups of G.

④ # elements of order $d = \varphi(d)$ [Euler function] Cor: in general finite group, # is multiple of $\varphi(d)$

⑤ $|\langle a \rangle|$ is prime: a) every $x \in \langle a \rangle$ is generator;

⑥ $|\langle a \rangle \cap \langle b \rangle| \leq (|\langle a \rangle|, |\langle b \rangle|)$ cor: ① $\langle a \rangle \cap \langle b \rangle \neq \emptyset \Rightarrow \langle a \rangle \subseteq \langle b \rangle$ or $\langle b \rangle \subseteq \langle a \rangle$
② G has only elements of order p (prime) $\Rightarrow |G| = k(p-1)+1$

4. Permutation Groups

Notation: $(1\ 3\ 2) = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$, "3-cycle"

Prop: ① per ⇔ product of disjoint cycles → commutes; → order = lcm (length of cycles)

rmk: "odd-length cycle" is "even perm."

② per ↔ product of 2-cycles → e must be even → $e = \dots(x,y)(a,b)$ →
- $(a,b)(a,b)$ → induction
- $(a,c)(a,b) = (a,b)(b,c)$
- $(b,c)(a,b) = (a,c)(b,c)$
- $(c,d)(a,b) = (a,b)(c,d)$

continue until → must happen. otherwise $e = (a,x)(\ )\dots$ no 'a'

even per. form a subgroup; a per. is either even or odd

A_n, "alternating group of degree n", has order $\frac{n!}{2}$

Cayley's Theorem: $T_g: G \to per(G)$, $g \mapsto (T_g(x) = gx)$

rmk: op in per(G) is $T_{g_1} \cdot T_{g_2} = T_{g_1 g_2}$

5.1) Isomorphism : bijection + preserve operation

prop: ① preserve identity, order ("if cyclic"), commutativity ("if Abelian")
↳ $\phi(x) = \phi(ex) = \phi(e)\cdot\phi(x)$.

② preserve number of sol for $x^k = b$: "$\leq$" and "$\nleq$"

③ preserve subgroup, center

④ ϕ is isomorphism $G \to \bar{G} \Leftrightarrow \phi^{-1}$ is isomorphism $\bar{G} \to G$.

2) Automorphism : isomorphism from G to G; "$Aut(G)$" ; is a group by composition

Inner Automorphism : $\forall a \in G$, $\phi_a : x \mapsto axa^{-1}$; "$Inn(G)$" ; is a group $\phi_a \circ \phi_b = \phi_{ab}$

eg. $Aut(\mathbb{Z}_n) \cong U(n)$ by $\phi : \alpha \mapsto \alpha(1)$, $\alpha\circ\beta \mapsto \alpha(1)\cdot\beta(1)$.

6.1) Cosets

rmk: aH, Ha, aH, HK, $H+K$ are defined namely, not necessarily with any property

def: eg aH, is a left coset of H (subgroup) with a being representative.

prop: ① $aH = bH$ or $aH \cap bH = \emptyset$: $ah_1 = bh_2 \Rightarrow ax' = (bh_2h_1^{-1})x' = b\cdot(h_2h_1^{-1}x')$

② criteria for equivalence : $aH = bH \Leftrightarrow ab^{-1} \in H$.

③ respect op : $(ab)H = a(bH)$. $H(ab) = (Ha)b$

Cor: i) $aH = bH \Leftrightarrow a \in bH$; $aH = H \Leftrightarrow a \in H$

ii) $aH = Ha \Leftrightarrow H = aHa^{-1}$

④ criteria for subgroup: aH is subgroup of $G \Leftrightarrow a \in H$.

2) Lagrange's Theorem : $H < G \Rightarrow |H| \,|\, |G| \wedge |G:H| = \frac{|G|}{|H|}$

Cor: i) $|a| \,|\, |G|$, $a^{|G|} = e$

ii) $|G|$ is prime $\Rightarrow$ G is cyclic (hence Abelian). [Cor: Fermat's little theorem]

★iii) $|HK| = \frac{|H||K|}{|H\cap K|}$ a) number $|HK|$ appears to be $|H:H\cap K|\cdot|K:H\cap K|\cdot|H\cap K|$ by intuition

b) every $hk \in HK$ is counted $|H\cap K|$ times : "$\Rightarrow$" $hk = h'k' \Rightarrow (h')^{-1}h = k\cdot k^{-1} \in H\cap K$; "$\Leftarrow$" $t \in H\cap K \Rightarrow hk = (ht)(t^{-1}k)$

iv) $|G| = 2p \Rightarrow G \cong \mathbb{Z}_{2p}$ or $G \cong D_p \cong \mathbb{Z}_p \oplus \mathbb{Z}_2$ rmk: G doesn't need be Abelian in premise.

Pf: ① all order 2 $\Rightarrow ab = (ba)^{-1} = ba \Rightarrow$ Abelian $\leftrightarrow$ FTA: $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_p$ → contradiction → $\exists\, |a| = p$ ($|\{e, a, b, ab\}| \nmid |G|$)

② $p^2 > p \,\not|\, |G| \Rightarrow \forall b \notin \langle a\rangle$, $|b| = 2 \Rightarrow (b\langle a\rangle) \cup \langle a\rangle = G$

③ G has unique ~~multi~~ Cayley table as $|ab| = 2 \Rightarrow ab = (b^{-1}a^{-1}) = ba^{-1} \Rightarrow (b^n a^k)\cdot(b^n a^i) = b^{m+n}a^{i+k}$

rmk: $stab(x)$ is subgroup $\Rightarrow$ all non-cyclic G with $|G| = 2p$ are isomorphic.

App: i) $G \curvearrowright S$, $\forall x \in G$. T: $\underbrace{\phi\cdot stab(x)}_{\text{coset}} \mapsto \phi(x)$ is well-defined and bijective $\Rightarrow |G| = |G:stab(x)|\cdot|stab(x)|$
$= |orb(x)|\,|stab(x)|$

App: count $|G|$

7. External Direct Product : $(G_1, \cdots G_n)$, "$\oplus$"

prop: ① $|(g_1, \cdots g_n)| = \mathrm{lcm}(|g_1|, \cdots |g_n|)$

② When G_i is cyclic, $G_1 \oplus \cdots \oplus G_n$ is cyclic iff $|G_i|$ are pairwise relatively prime.

Cor: $\mathbb{Z}_{n_1 n_2 \cdots n_k} \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$, $n_i \perp n_j$ $(\forall i \neq j)$.

③ $U(n_1 n_2 \cdots n_k) \cong U(n_1) \oplus \cdots \oplus U(n_k)$, $n_i \perp n_j$ $(\forall i \neq j)$.

8. Normal Subgroup & Factor ~~Ring~~ Ring

Def: $H \lhd G$ iff $aH = Ha$ for all $a \in G$.

criterion: $xHx^{-1} \subseteq H$ $\forall x \in G$.

联想：在共轭运算下"absorb" G into H

prop: ① $(aH)(bH) = abH$ iff H is normal.

When H is not normal, $(aH)(bH)$ depends on the representative

"$\Leftarrow$": obvious. "$\Rightarrow$": $ah_1 bh_2 \in abH \Rightarrow h_1 b h_2 \in bH \Rightarrow h_1 b \in bH$ $\forall b, h_1 \Rightarrow H \lhd G$.

$\Rightarrow$ Def: $G/H = \{aH \mid a \in G\}$, where $H \lhd G$, is a group with $(aH) * (bH) = (aH)(bH) = (ab)H$.

Cor: $G/Z(G) \cong \mathrm{Inn}(G)$ Consider: $\forall g, xgx^{-1} = ygy^{-1} \Leftrightarrow \forall g, (y^{-1}x)g(y^{-1}x)^{-1} = g \Leftrightarrow y^{-1}x \in Z(G) \Leftrightarrow xZ = yZ$

② Every subgroup is normal for Abelian group

Cor (Cauchy's Theorem): "prime" $\mid |G| \Rightarrow G$ has an element of order "prime" [Take arbitrary x and induct]

Cor: $a \in G$ then $\langle a \rangle \lhd G$, $x\langle a \rangle = y\langle a \rangle$ iff $xy^{-1} \in \langle a \rangle$

9. Internal Direct product "$\times$"

Def: ① $H \lhd G$, $K \lhd G$, $H \cap K = \{e\}$, $H \cdot K = G \Rightarrow G = H \times K$ (internal direct product)

② $H_i \lhd G$, $(H_1 H_2 \cdots H_i) \cap H_{i+1} = \{e\}$, $H_1 \cdot H_2 \cdots H_n = G \Rightarrow G = H_1 \times H_2 \times \cdots \times H_n$

prop: $H_1 \times \cdots \times H_n \cong H_1 \oplus \cdots \oplus H_n$

① H_i, H_j $(i \neq j)$ commutes: $h_i h_j = h_j h_i \Leftrightarrow h_i h_j (h_i^{-1} h_j^{-1}) = h_i (h_j h_i^{-1} h_j^{-1}) (\in H_i) = (h_i h_j h_i^{-1}) h_j^{-1} (\in H_j) \in H_i \cap H_j = \{e\}$

② $h \in G$ has unique representation as $h_1 h_2 \cdots h_n$, as $h_i (h_i')^{-1} \neq e \Rightarrow \prod h_i (h_i')^{-1} \neq e \Rightarrow \prod h_i \neq \prod h_i'$

(Cor: $|G| = p^2_{\text{prime}} \Rightarrow G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$) take $b \notin \langle a \rangle$, prove $G \cong \langle a \rangle \times \langle b \rangle$ as $a^i b^j = a^k b^l \Leftrightarrow i=k, j=l$

10. Group Homomorphism : preserve operation

inverse image / pullback

def: $\ker\phi$ (is a subgroup), $\phi^{-1}(g)=\{x\in G \mid \phi(x)=g\}$ when $|G|$ is finite

$\phi(e)\in\ker\phi$ $|\phi(g)| \mid |g|$ $ab=ba \Rightarrow \phi(a)\phi(b)=\phi(b)\phi(a)$ The other direction does not hold

prop: ① "almost preserve" identity, order; commutativity / Abelian / cyclic in one direction

② $\phi^{-1}(\phi(g))=g\ker\phi$ pf: $\phi(a)=\phi(b)\Rightarrow ab^{-1}\in\ker\phi \Rightarrow a\ker\phi=b\ker\phi$

Cor: $\phi(a)=\phi(b) \iff \phi^{-1}(\phi(a))=\phi^{-1}(\phi(b)) \iff a\ker\phi=b\ker\phi$

③ "preserve" normality, subgroup, in both directions.

normality: $\bar H\lhd\bar G \Rightarrow$ consider $x\phi^{-1}(\bar H)x^{-1}=\{xkx^{-1}\mid\phi(k)\in\bar H\}$, $\phi(xhx^{-1})=\phi(x)\phi(h)(\phi(x))^{-1}\in\phi^{-1}(\bar H)$

subgroup: $\bar H<\bar G \Rightarrow$ consider xy^{-1} where $x,y\in\phi^{-1}(\bar H)$, $\phi(xy^{-1})=\phi(x)\phi(y^{-1})\in\bar H \Rightarrow xy^{-1}\in\phi^{-1}(\bar H)$. $\Rightarrow \phi^{-1}(\bar H)\lhd G$.

Cor: $\ker\phi\lhd G$, $G/\ker\phi\cong\bar G$ First Isomorphism Theorem

Cor Cor ① $|\ker\phi|=n$, ϕ is n-to-1

② $|\phi(H)| \mid |H|$, as $|\phi(H)|=\frac{|H|}{n}$

③ $\ker\phi=e \Rightarrow \phi$ is isomorphism

thm 19.4

Inverse is true : Every normal subgroup can be kernel of some ϕ: $\phi: g\mapsto gN$, $G\to G/N$

Clarify about def: "ϕ is hom. $G\to\bar G$" means $\phi(G)<\bar G$, not $\phi(G)=\bar G$...

11. FT of finite Abelian groups: $\exists!$ decomposition into direct product of cyclic group rmk: $\langle a\rangle\times\langle b\rangle$ doesn't have to be Abelian (inverse doesn't hold).

Algorithm to find $|G|_{p^k}\to\oplus\mathbb{Z}_{p^{k_i}}$: take $a\in G$ with $\max|a|$, $G\to G/\langle a\rangle$ normal by Abelian

② $|G|_{\prod p_i^{k_i}}\to |G|_{p_i^{k_i}}$: Take out $\{a\mid |a|\mid p_i^{k_i}\}$ only (we don't need $|a|=\prod_j p_j^{k_j}$ to construct $\mathbb{Z}_{p^{n_i}}$)

Cor: $d\mid|G|\Rightarrow\exists H<G$, s.t. $|H|=d$

Pf: ① $|G|=pq$, $p\perp q \Rightarrow \begin{cases}|H=\{x\mid x^p=e\}|=q,\ |K=\{x\mid x^q=e\}|,\\ G=H\times K\end{cases}$

pf: $x\in G$, $x^z=x^{sp+tq}\in K\times H$; $sp+t'q=sp+tq\Rightarrow q\mid(t'-t)$, $p\mid(t'-t)\Rightarrow x^{sp}=x^{sp}x^{tq}=x^{t'q}$

Cor: $G=H_{p_1^{k_1}}\times\cdots\times H_{p_m^{k_m}}$ for Abelian G.

② $|G|=p^n$, $|a|=p^m$ is maximum order $\Rightarrow G=\langle a\rangle\times K$

pf: ① Notice $\exists b\in K$, $|b|=p$ ② Induction with $\bar G=G/\langle b\rangle$

$b\in\langle a\rangle$, $b^p\in\langle a^p\rangle \Rightarrow b^{p^m}=a^{jp^{m-1}}=e\Rightarrow |a^{\frac{j}{p}}\cdot b|=p$ (a^j is not generator)

Why $p=|b|$: ① preserve max order ② intersection implies inclusion (would generate whole)

$\langle b\rangle\cap\langle a\rangle=\{e\}$ as any intersection would generate a whole

Cor: exist decomposition into internal product of cyclic groups.

③ Uniqueness of decomposition

Up to isomorphism / size of the cyclic groups

$H_1\times H_2\cdots\times H_m=K_1\times\cdots\times K_n$

$|H_i|>p\Rightarrow |H_i^p|>1\Rightarrow$ done $|H_i|=p\cdot|H_i^p|$; Count $|G|$ we know $\sum[|H_i|=p]=\sum[|K_i|=p]$

$\bar G=G^p$, induction

12. Tools for Analyzing Group structure

① $|G|$; ② $|g|$ and number of elements with specific order

③ $G\to G^k$: ① Cl holds for non-Abelian group, ② when $(k,n)=1\Rightarrow g\mapsto g^k$ is bijection:

$g_1^k=g_2^k$, $g_1^n=g_2^n\Rightarrow g_1=g_2$ (Bezout's theorem)

② for Abelian group this is homomorphism (automorphism if $(k,n)=1$)