1. Write all elements of S_4.

identity e

transposition. (12), (13), (14), (23), (24), (34)

double transposition. $(12)(34)$, $(13)(24)$, $(14)(23)$

3-cycle. (123) (132)
(234) (243)
(341) (314)
(412) (421)

4-cycle. (1234), (1243), (1324), (1342), (1423), (1432).

24 elements in total.

2. normal subgroup of D_{20}.

$D_{20} = \langle a, b \mid a^{10} = b^2 = 1, bab = a^{-1} \rangle$

Normal subgroup: $\langle a \rangle$, $\langle a^2 \rangle$, $\langle a^5 \rangle$, $\langle a^2, b \rangle$, $\langle a^2, ab \rangle$

$\{e\}$, D_{20}.

3. Let $H, K \leq G$.

(1). $HK = KH$

$\forall\ h, k \in H, K$ respectively

$hk = hkh^{-1}h$, since $k \in H \lhd G$, $\exists\ k_1 \in H$ s.t. $k_1 = hkh^{-1}$

$\Rightarrow hk = hkh^{-1}h = k_1 h \in kH$

$\Rightarrow HK \subset KH$, vice versa.

(2). $HK \leq G$.

$\forall\ h, k, g \in H, K, G$ respectively

I forgee to prove $HK \leq G$ first. But this is easy. $\forall\ h_1 k_1 h_2 k_2$ consider $h_1 k_1 \cdot h_2 k_2$

Consider. $g^{-1}hkg = g^{-1}hgg^{-1}kg$

Since $H, K \trianglelefteq G$. $\exists\ h_1, k_1 \in H, K$ s.t

$$g^{-1}hg = h_1,\quad g^{-1}kg = k_1$$

i.e. $g^{-1}hkg = g^{-1}hg\ g^{-1}kg = h_1k_1 \in HK$

Thus $HK \trianglelefteq G$

$= h_1k_1h_2k_1^{-1}k_1k_2$

$= h_1h_2'k_1k_2 \in HK$

So $HK \subseteq G$.

(3). If $H \cap K = \{e\}$ then G is iso to subgrup of $G/H \oplus G/K$.

Consider $\varphi: G \longrightarrow G/H \oplus G/K$ s.t

$$g \longmapsto (gH, gK)$$

This is a grup. homomorphism.

$\forall\ g \in \ker\varphi$ then $gH = H$ and $gK = K \Rightarrow g \in H \cap K = \{e\}$

$\Rightarrow \ker\varphi = \{e\}$, thus φ is monomorphism.

By 1st iso thm $G \xrightarrow{\sim} \varphi(G) \leq G/H \oplus G/K$.

4. Let $m, n \in \mathbb{Z}$. $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ iff $(m, n) = 1$.

Step 1. Consider

$$\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

$$k \longmapsto (k \bmod m,\ k \bmod n)$$

① this is grup homo. (check it!)

② this is epimorphism. iff $(m, n) = 1$ (Chinese remainder Thm)

③ $\ker\varphi = mn\mathbb{Z}$

$\Rightarrow \mathbb{Z}/mn\mathbb{Z} \hookrightarrow \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ 当 $(m,n)=1$.

5. H, K finite index. $H\cap K$ also.

Consider $\varphi: \frac{H}{H\cap K} \longrightarrow \frac{G}{K}$

This map is injective.

$\Rightarrow [G: H\cap K] = [G:H][H: H\cap K] \le [G:H][G:K] < \infty$

6. Classify all groups with order 4.

$\mathbb{Z}_4$ $\mathbb{Z}_2\times\mathbb{Z}_2$

7. If $|g|=n$, then $o(g^m) = n/(m,n)$

Let $(m,n)=d$ where $m=kd$, $n=ld$

$$(g^m)^{\frac{n}{(m,n)}} = g^{m\frac{n}{d}} = g^{\frac{mn}{d}} = g^{\frac{kdn}{d}} = g^{kn} = (g^n)^k = 1$$

$\Rightarrow o(g^m) \mid \frac{n}{(m,n)}$

$g^{o(g^m)\cdot m} = (g^m)^{o(g^m)} = 1 \Rightarrow m\,o(g^m) \mid n \Rightarrow o(g^m) \mid \frac{n}{(m,n)}$

$\Rightarrow o(g^m) = \frac{n}{(m,n)}$

8. Prove there there is no subgroup of A_4 with order 6.

If $|H|=6$, $H \le A_4$, since $[A_4 : H] = 2 \Rightarrow H \lhd A_4$.

Consider A_4/H,

P. if H contains all 3-cycle. then $|H| \ge 8$ ↯

Σ^p. $\exists$ a 3-cycle $x \notin H$

we have coset H, xH, x^2H in A_4

Since $[A_4 : H] \geq 2 \Rightarrow$ (i) $xH = H \Rightarrow x \in H$ ↯

(ii) $x^2H = H \Rightarrow x \in H$ ↯.

□

4. fin grp G is D grp iff $G = \langle a, b \rangle$ where $a^2 = b^2 = 1$.

$\Rightarrow$. Let $G = D_{2n} = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1} \rangle$

Consider. $D_{2n} \longrightarrow D_{2n}$.

$b \longmapsto bx$

$ab \longmapsto y$

This is an iso. so $D_{2n} = \langle x, y \rangle$ where $x^2 = y^2 = 1$.

$\Leftarrow$ suppose. $G = \langle a, b \mid a^2 = b^2 = 1 \rangle$

Let $x = ab$, since $|G| < \infty$, assume $|x| = n$

then $G \longrightarrow G$

$ab \longmapsto x$

$b \longmapsto y$ is an iso.

$\Rightarrow G = \langle x, y \mid x^n = y^2 = 1, yxy = x^{-1} \rangle = D_{2n}$.

10. $|g|=rs$, $(r,s)=1$ prove $g=ab$ $|a|=r$ $|b|=s$, g's power.

$(r,s)=1$, $\exists\, m,n\in\mathbb{Z}$ s.t. $mr+ns=1$

$g=g^{mr+ns}=g^{mr}\cdot g^{ns}$ Let $a=g^{ns}$ $b=g^{mr}$

on the one hand

$a^r=g^{nsr}=(g^{sr})^n=1$ $\quad b^s=g^{mrs}=(g^{rs})^m=1$.

$o(a)\mid r$, $o(b)\mid s$

on the other hand.

$a^{o(a)}=1=g^{nso(a)}\Rightarrow rs\mid nso(a)$

$mr+ns=1\Rightarrow ns\equiv 1 \bmod r$ $\quad (s,r)=1\Rightarrow (r,n)=1$

$\Rightarrow r\mid o(a)$

Similarly $s\mid o(b)$

$\Rightarrow o(a)=r$, $o(b)=s$

11. $(o(g),k)=1$. prove $x^k=g$ has only one solution in $\langle g\rangle$

Let $o(g)=r$, $(r,k)=1\Rightarrow \exists\, a,b\in\mathbb{Z}$ s.t. $ar+bk=1$

$x^k=g^{ar+bk}=g^{ar}\cdot g^{bk}=1\cdot g^{bk}=(g^b)^k$

$x=g^b$ is a solution.

Now suppose $\exists\, x=g^i$ s.t. $i\not\equiv b \bmod r$ and

$(g^i)^k=g\Rightarrow r\mid ik-1$

$r\mid bk-1$,

$\Rightarrow ik = bk \equiv 1 \bmod r \overset{(r,k)=1}{\Rightarrow} i \equiv b \bmod r$ ↯

12. fin gene. subgrp of $(\mathbb{Q},+)$ is cyclic.

Sps $H \leq (\mathbb{Q},+)$ H is a fin. gene. subgrp.

We can always write H in following way:

$$H = \left\langle \frac{a_1}{n}, \dots, \frac{a_m}{n} \right\rangle, \quad m, n, a_i \text{ are all integers.}$$

Then $H \simeq \langle a_1, \dots, a_m \rangle \leq (\mathbb{Z},+)$

$$h \longmapsto nh$$

but $(\mathbb{Z},+)$ is a cyclic gnup $\Rightarrow$ H is also cyclic.

13. G. fin. gene. abelian. grp, any generator of G has fin order

$\Rightarrow G$ fin.

Let $G = \langle a_1, \dots a_m \rangle$, $o(a_i) < \infty$

Then $G = \{ a_1^{k_1} \dots a_m^{k_m} \mid k_i \in \mathbb{Z} \}$ is a finite set

14. Prove the subgrp of fin. index of a fin. gene. is fin. gene.

Since G is finitely generated, $G = \langle S \rangle$, $|S| < \infty$

Since $[G:H] < \infty$, $\exists\, x_1, \dots x_n \in G$ s.t

$x_1 = 1$, $Hx_i \cap Hx_j = \emptyset$, $G = Hx_1 \sqcup Hx_2 \sqcup \dots \sqcup Hx_n$.

Now given $g \in G$, $x_i g \in Hx_j$ for some j

$\Rightarrow \exists$ unique $h \in H$ s.t $x_i g = h x_j$

j, h are all uniquely determined

Based on this we can define a map :

$$f: \{1, 2, \dots, n\} \times G \to H$$
$$(i, g) \mapsto h$$

h is associate to an integer i and an element of G

reformulate this to:

given $g \in G$. for each i.

$$x_i \cdot g = f(i, g)\, x_{(i,g)}$$

j is also uniquely determinate by i and g

Now. $\forall h \in H$, $H \leq G \Rightarrow h$ can be writen into

$$h = g_1 \cdots g_m, \quad g_i \in S \cup S^{-1}$$

remember $x_1 = e$

$$h = x_1 \cdot h = x_1 g_1 \cdots g_m$$

$$= f(1, g_1)\, x_{(1,g_1)}\, g_2 \cdots g_m$$

$$= f(1, g_1)\, f((1, g_1), g_2)\, x_{((1,g_1),g_2)}\, g_3 \cdots g_m.$$

$$= \cdots$$

$$= f(1, g_1)\, f((1, g_1), g_2) \cdots f((\cdots(1, g_1), g_2), g_3 \cdots, g_m)\, x$$

$((\cdots(1, g_1), \cdots g_m)$

$h \in H$, all $f(\cdot,\cdot) \in H \Rightarrow x_{(\cdot,\cdot)} \in H$

Only can be $\chi_{C_{\cdots}} = \chi_1 = e$

$\Rightarrow$ H is generated by following finite set

$$\{ f(i,g) : 1 \le i \le n,\ g \in SUS^{-1} \}$$

15. $G^k = \{ g^k \mid g \in G \}$. Prove G cyclic $\Leftrightarrow$ all subgroups of G is of G^k type.

$\Rightarrow$: Sps G cyclic. For any $H \le G$

H is also cyclic

$H = \langle g^k \rangle = \langle g \rangle^k$ is of G^k type.

$\Leftarrow$: Sps all subgroups of G is of G^k type.

Now $\forall\ a \in G$. Sps $\langle a \rangle = G^k$ for some k.

Then $\exists\ x \in G$ s.t $x^k = a$.

Now Let $\langle x \rangle = G^j$ for some j

Then $\exists\ y \in G$ s.t $y^j = x$.

If $j = 1$. Then $G = \langle x \rangle$ is cyclic

if $j \neq 1$ Then $y^k \in G^k$

$\Rightarrow \exists\ i$ s.t $y^k = a^i = y^{ijk} \Rightarrow y^{k(ji-1)} = e$

$\Rightarrow$ order of y is finite

$\Rightarrow$ order of a is finite

$\Rightarrow$ All elements in G are of finite order

Let $b \in G$ with $o(b)$ is the biggest number of all elements in G

Let $\langle b \rangle = G^m$, $o(b) = n$

Since b is of the biggest order, it forces $m = 1$

$\Rightarrow G = \langle b \rangle$ is cyclic.

16. $G = \mathbb{Z}_{p^n}$. identify $\mathrm{Aut}(G)$

1° for $p \neq 2$. Then p^n has primitive root

$\Rightarrow \mathrm{Aut}(G) \cong \mathbb{Z}_{\varphi(p^n)} = \mathbb{Z}_{p^{n-1}(p-1)}$

2° for $p = 2$

1° $n = 1$ $G = \mathbb{Z}_2$. $\mathrm{Aut}(G) = 1$.

2° $n = 2$ $G = \mathbb{Z}_4$. $\mathrm{Aut}(G) = \mathbb{Z}_2$.

3° $n \geq 3$.

$\varphi: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ Automorphism. there are two ways:

1°. $\sigma: x \mapsto x^i$, i : odd $|\sigma| = 2^{n-2}$

2°. $\tau: x \mapsto x^{-1}$ $|\tau| = 2$.

$\mathrm{Aut}(\mathbb{Z}_{2^n}) = \langle \sigma \rangle \times \langle \tau \rangle = \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_2$.

17. Classify order 36 abelian group.

$36 = 2^2 \times 3^2$

Z_{36}

$Z_2 \times Z_2 \times Z_9$

$Z_4 \times Z_3 \times Z_3$

$Z_2 \times Z_2 \times Z_3 \times Z_3$

18. $G = Z_3 \times Z_9 \times Z_9 \times Z_{243}$. find the number

(1) cyclic subgps of order 9 = order 9 elements / $\varphi(9)$

(2) Non-cyclic subgps of order 9. only $Z_3 \times Z_3$

Consider $G_3 = (Z_3)^4$ pick 2 different order 3 elements to count the number

$(3^4-1)(3^4-3)/(3^2-1)(3^2-3) = 130$.

19. Prove. $S_n = \langle (12),(13),\dots,(1n) \rangle$ or $S_n = \langle (12),(23),\dots,(n-1\ n) \rangle$

1°. $\forall \sigma \in S_n$, σ is a production of transposition.

for any transposition (ij), $(ij) = (1i)(1j)(1i)$

2°. By 1°, furthermor

$(1i) = (i-1\ i)\cdots(34)(23)(12)(23)(34)\cdots(i-1\ i)$.

20. $n \geq 2$. n even, $A_n = \langle (123),(124),\dots,(12n) \rangle$

or $A_n = \langle (123),(234),\dots(n-2\ n-1\ n) \rangle$

$\forall \sigma \in A_n$. σ is a production of 3-cycles.

for any 3-cycle

$(ijk) = (1ij)(1ik)(1ij)^{-1}$

and for any $(1ij)$, $(1ij) = (12j)^{-1}(12i)(12j)$

$(1ij) = ((i-1j)(1\,i-1\,i)^2 = \cdots$ production of $(1\,i,i+1)$

for any $(1\,i\,i+1) = (i-1\,i\,i+1)^{-1}(i-2\,i-1\,i)^{-1}\cdots(123k)^{-1}(123)(123k)$

$\cdots (1\,i-1\,i+1)$.

21. $n>2$. even. $A_n = \langle (123), (23\cdots n)\rangle$

odd $A_n = \langle (123), (123\cdots n)\rangle$.

1°. Let $\tau = (23\cdots n)$ $\sigma = (123)$

$\tau\sigma\tau^{-1} = (134)$

$\tau\sigma\tau^{-2} = (145)$ .....

2°. Let $\tau = (123\cdots n)$ $\sigma = (123)$

$\tau\sigma\tau^{-1} = (234)$

$\tau\sigma\tau^{-2} = (345)$ ... -

22. Let $\sigma = (12\cdots n)$. Prove $C_{S_n}(\sigma) = \langle\sigma\rangle$

Prove $|C(\sigma)| = n-1!$

$\forall \alpha \in C_{S_n}(\sigma)$ $\alpha\sigma\alpha^{-1} = \sigma$

$\Rightarrow$ $\alpha = (12\cdots n)^i$ for some i $\rightarrow$ $C_{S_n}(\sigma) = \langle\sigma\rangle$

$|S_n| = |C(\sigma)|\,|C_{S_n}(\sigma)|$ $\Rightarrow$ $|C(\sigma)| = (n-1)!$

Orbit - stabilizer theorem.

23. $n>2$, $Z(S_n)=\{(1),\}$.

By 23. if $\exists\ e\neq\alpha\in Z(S_n)$

$\alpha\in\langle\sigma\rangle$ and $\alpha(12)=(12)\alpha$

but $\forall\ e\neq\beta\in\langle\sigma\rangle$, $\beta(12)\neq(12)\beta$

$\Rightarrow Z(S_n)=\{(1),\}$.

24. $n\geq 5$. S_n has unique normal subgroup A_n.

Sps $\exists\ H\triangleleft S_n$ s.t $H\neq A_n$

Since $H\cap A_n\triangleleft A_n$ and A_n simple

$\Rightarrow H\cap A_n=e$

$\Rightarrow$ all elements in H are odd permutation (except e)

$\Rightarrow |H|=2 \Rightarrow H\triangleleft S_n$ and $|H|=2 \Rightarrow H\leq C(S_n)$

But $C(S_n)=e$ $\lightning$

25. G grp. $N\trianglelefteq G$ $N\cap G'=e \Rightarrow N\leq Z(G)$

$\forall\ g\in G$, $n\in N$ $[g,n]=g^{-1}n^{-1}gn$, $N\trianglelefteq G \Rightarrow [g,n]\in N$

$[g,N]\in G' \Rightarrow [g,n]\in N\cap G'=e \Rightarrow n\in Z(G) \Rightarrow N\leq Z(G)$

26 subgrp and quotient grp of solvable grp G are all solvable.

G solvable $\Rightarrow G^{(n)} = e$

for any $H \leq G$. $H^{(n)} \leq G^{(n)} = e \Rightarrow H^{(n)} = e \Rightarrow H$ solvable.

Consider $\pi \quad G \to G/N$. epi.

$\pi(G^{(n)}) = (G/N)^{(n)} = \bar{e} \Rightarrow G/N$ solvable.

27. $H, K \trianglelefteq G$. G/H, G/K solvable. $\Rightarrow G/H\cap K$ solvable.

Consider: $\varphi : G \to G/H \oplus G/K$, $g \mapsto (gH, gK)$ epi. $\ker\varphi = H\cap K$.

$\Rightarrow G/H\cap K \cong G/H \oplus G/K$

$\uparrow \quad \uparrow$

solvable. $\cong$ solvable $\oplus$ solvable

28. $|\mathrm{Aut}(G)| = 2 \Rightarrow G$ abelian.

Sps G non-abelian, $\Rightarrow G \neq Z(G)$

$\mathrm{Inn}(G) = G/Z(G) \neq e \Rightarrow |\mathrm{Inn}(G)| = |\mathrm{Aut}(G)| = 2$.

$\Rightarrow |G/Z(G)| = 2$

Pure $\swarrow$ force to be cyclic

and then G abelian.

29. if G finite $|G| > 2$ the G has at least 2 automorphism.

If $|\mathrm{Aut}(G)| = 1 \Rightarrow \mathrm{Inn}(G) = \{e\} \Rightarrow Z(G) = G \Rightarrow G$ abelian

Ture for any $|G|>2$.

1°. if $\exists x \in G$ s.t $|x|>2$, $\tau: G \to G$, $g \mapsto g^{-1}$ is also automorphism

and $\tau \neq id$. since $x \neq x^{-1}$

2°. if $exp(G)=2$ then for $G=(\mathbb{Z}_2)^n$ $n \geq 2$. G has

at least 2 generators so has at leas 2 automorphisms.

30. $Aut(\mathbb{Z}_2 \oplus \mathbb{Z}_2) \simeq S_3$

Consider $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{1, i, j, k\}$

Then any automorphism is just a permutation of i, j, k

$\Rightarrow Aut(G) \simeq S_3$.

31. $S_n = \langle (12), (12\cdots n) \rangle$

Let $(12)=\sigma$ $(12\cdots n)=\tau$

$$\tau \sigma \tau^{-1} = (23)$$

$$\tau^2 \sigma \tau^{-2} = (34)$$

$$\cdots$$

And $S_n = \langle (12), (23), \ldots, (n-1\ n) \rangle = \langle (12), (12\cdots n) \rangle$.