~~About Symplectic Group~~: Exlecture Note

1. definition: · ~~标准辛矩阵 $J = \begin{pmatrix} & I \\ -I & \end{pmatrix}$ $\det(J)=1$, $J^2=-I$, $J^T=J^{-1}=-J$~~

· $Sp(2n,\mathbb{R}) = \{ S : S^TJS = SJS^T = J \}$

· S symplectic $\Rightarrow$ $(S^{-1})^TJS^{-1} = -S^{-1T}J^TS^{-1} = -(SJS^T)^{-1} = J$

$S^{-1}JS^{-1T} = (S^TJ^{-1}S)^{-1} = -(S^TJ^{-1}S)^{-1} = J.$

Prop:

i. $S \in S_p(2n,\mathbb{R}) \Leftrightarrow S^TJS = J \Leftrightarrow SJS^T = J$

pf: $(\Leftarrow)$: $S^TJS = J \Rightarrow S^{-1}JS^{-1T} = J \xRightarrow{\text{取逆}} JS^{-1T} = SJ$

$\Rightarrow J = SJS^T$

$S = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$ $SP_{2n} = \{ P \in GL_{2n}(\mathbb{R}) \mid P^TSP = S \}$

§ Linear Groups (Some Calculation).

① $SP_{2n}(\mathbb{R})$ is a group:

$P^TSP = S.$ (i)

$\Rightarrow S = P^{-1T}SP^{-1}$. $P^{T-1} = P^{-1T}$. $\Rightarrow P^{-1} \in S$

Multiplication-closed is trivial.

② $P \in SP_{2n}(\mathbb{R}) \Leftrightarrow P^T \in SP_{2n}(\mathbb{R})$

Take inverse in (i), we have $P^{-1}S^{-1}P^{T-1} = S^{-1}$

But $S^{-1} = S^T = -S$, as you notice.

Thus $S = PSP^T$ Hence $P \in SP_{2n}$.

③ $P \in SP_{2n}(\mathbb{R}) \Rightarrow \det P = 1$.

It's not hard to prove in the case when $n=1$.

For general n, we refer to 王新茂《线性代数讲义》

④ $SP_2 = SL_2$ $SP_4 \neq SL_4$.

Notice that SL_2 is generated by $\left\{ \begin{pmatrix} 1 & a \\ & 1 \end{pmatrix}, \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}, \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \right\}$ $a \neq 0$ here.

We ~~reduce~~ to check these 3 class of matrices are in SP_2.

$\begin{pmatrix}1&a\\&1\end{pmatrix}\begin{pmatrix}&-1\\1&\end{pmatrix}.\begin{pmatrix}1&\\a&1\end{pmatrix}=\begin{pmatrix}a&-1\\1&0\end{pmatrix}\begin{pmatrix}1&\\a&1\end{pmatrix}=\begin{pmatrix}0&-1\\1&0\end{pmatrix}!$

$\begin{pmatrix}&-1\\1&\end{pmatrix}\begin{pmatrix}&-1\\1&\end{pmatrix}\begin{pmatrix}&1\\-1&\end{pmatrix}=\begin{pmatrix}&-1\\1&\end{pmatrix}!$

$\begin{pmatrix}a&\\&a^{-1}\end{pmatrix}.\begin{pmatrix}&-1\\1&\end{pmatrix}\begin{pmatrix}a&\\&a^{-1}\end{pmatrix}=\begin{pmatrix}&-a\\a^{-1}&\end{pmatrix}\begin{pmatrix}a&\\&a^{-1}\end{pmatrix}=\begin{pmatrix}&-1\\1&\end{pmatrix}.$

Remark: $\begin{pmatrix}a&b\\c&d\end{pmatrix}\xmapsto{a\neq 0}\begin{pmatrix}a&\\c&d-a^{-1}bc\end{pmatrix}\longmapsto\begin{pmatrix}a&\\&a^{-1}\end{pmatrix}$,

$ad-bc=1$ multply $\begin{pmatrix}&-1\\1&\end{pmatrix}$ if necessary. Infact: notice that $ab-cd=1$ $\Rightarrow$ ~~prime~~ coprime $\Rightarrow$ easy to do with $n=2$

By the same tone we check that $SL_2(\mathbb{Z})=\left\langle\begin{pmatrix}0&-1\\1&0\end{pmatrix},\begin{pmatrix}1&1\\&1\end{pmatrix}\right\rangle$

since $(a, a^{-1}\in\mathbb{Z}\Rightarrow a=\pm 1)$. (P32 / 1.3.24.)

The reason why we want to ~~reduce~~ find generators as small as possible is presented above.

- $Sp_4(\mathbb{R})\neq SL_4(\mathbb{R})$

It's not such hard as it seems to find an example, right! Just try $\begin{pmatrix}&-1&&\\1&&&\\&&1&\\&&&1\end{pmatrix}$. The reason I put an -1 here is to make the det $=1$.

Having got some taste of calculation in matrix groups, we begin our discussion of a nice theorem.

Theorem: F : $|F|\geq 4$. (& finite, order: q).

a). The only proper normal subgroup of $SL_2(F)$ is its center $Z=\{\pm I\}$

b). $PSL_2(F)$ is a simple group

Lemma. q: $\mathbb{F}_q$; Then $|SL_2(\mathbb{F}_q)|=q^3-q$. , infact here we can calculate SL_n.

if q is not power of 2. $PSL_2(\mathbb{F}_q)=\frac{1}{2}(q^3-q)$

if q is a — — — , — — — — $|PSL_2(\mathbb{F}_q)|=SL_2(\mathbb{F}_q)$!

Pf: Recall a famous group homomorphisms: ~~SL~~ $GL_n\to F^\times$ with kernal SL_n. , $|F^\times|=q-1$ thus we are reduced to calculate $\#(GL_n)$

Here is a trick. "GL" means the column vectors of matrix A should be linear independent with each other. Thus:

4>: why is "q" here? Note that $\#\{\lambda V\} = q$, where $\lambda \in \mathbb{F}_q$.

$\begin{pmatrix} (\ ) & (\ ) & (\ ) & \cdots \end{pmatrix}_{n \times n}$

Step 1 $q^n - 1$

Step 2: $\underbrace{q^n - q}_{4>}$.

Step 3: $q^n - q \cdot q$. ..... Step n: $q^n - q^{n-1}$.

Thus we have done: $(q^n - 1) \cdots (q^n - q^{n-1}) = q^{\frac{n(n-1)}{2}} (q^n - 1) \cdots (q - 1)$

Hence $\# SL_2(\mathbb{F}_q) = \dfrac{(q^2 - 1)(q^2 - q)}{q - 1} = q(q^2 - 1)$

$PSL_2(\mathbb{F}_q)$ doesn't lose half of its weight since $1 = -1$ in that case. (when $q = 2^m$, $m \in \mathbb{N}^+$)

It is left as an exercise to check that $Z = \{\pm I\}$ where Z is the center of SL_2

Lemma: F field, $\# F > 5$. Then $\exists\, r$: $r^2 \neq 0, 1, -1$.

Pf: $r^2 = 0 \Rightarrow r = 0$ $\quad r^2 = 1 \Rightarrow (r+1)(r-1) = 0 \Rightarrow r = 1$ or -1.

$a^2 = b^2 = -1 \Rightarrow (a+b)(a-b) = 0 \Leftarrow$ Cancel Law Holds in Field. $\Rightarrow a = -b$ or $a = b$,

at most $\underbrace{2}_{}$.

$2 + 2 + 1 = 5$.

(This Lemma should be put forward when it is needed.)

We prove the case for ~~...~~ $q > 5$, here we can ~~use~~ enjoy the lemma above.

We take an arbitrary $A \neq \pm I$ and $r \in F$, $r^2 = s \neq \pm 1$, then we try to "generate" the whole group SL_2. Or more precisely, to generate the generators of SL_2.

What kind of generators? $\left\{ \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix}, \begin{pmatrix} 1 & \\ x & 1 \end{pmatrix}, x \in F \right\}$

To see why ~~this~~ is true:

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \xrightarrow[\substack{\text{for } c \neq 0, \\ \text{similarly.}}]{a \neq 0} \begin{pmatrix} a & \\ d & a^{-1} \end{pmatrix} \Rightarrow \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \Rightarrow \begin{pmatrix} a & 1 \\ & a^{-1} \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 1 \\ a^{-1}-1 & a^{-1} \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & \\ * & 1 \end{pmatrix}$$

Next, How to generate? We use A, and then conjugation operation (action) (i.e. similarity) → since we are given a normal subgroup.
in $SL_2(\mathbb{R})$ (Not $GL_2(\mathbb{R})$), and then matrix multiplication and inverse.

There're some tricks here: we think about eigenvalues.
We claim1 that at least one matrix with s, s^{-1} as e-v is in SL_2.
And then we claim2 that all (s, s^{-1}) can be generated by conjugation in SL_2. Then we observe that:

$$\begin{pmatrix} s^{-1} & \\ & s \end{pmatrix}\begin{pmatrix} s & sx \\ & s^{-1} \end{pmatrix} = \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix}$$ is what we want.

Thus, it remains to prove claim 1 and 2.

1. (Nice trick). choose vector $v_1 \in \mathbb{F}_q^2$ & v_1 is not eigenvector of A.
Then $(v_1\ Av_1) = B$ is invertible ~~and det = 1, WLOG~~.
This can be achieved since $A \neq \pm I$..
Let $P = B\begin{pmatrix} r & \\ & r^{-1} \end{pmatrix}B^{-1}$ (recall $r^2 = s \neq \pm 1, 0$) $\Rightarrow P \in SL_2$
Then $P(v_1, Av_1) = PB = B\begin{pmatrix} r & \\ & r^{-1} \end{pmatrix}BB^{-1} = B\begin{pmatrix} r & \\ & r^{-1} \end{pmatrix} = (rv_1, r^{-1}Av_1)$.
Then $C = A\underbrace{(PA^{-1}P^{-1})}_{\in N}$: $C(Av_1) = APA^{-1}P^{-1}Av_1 = r\,APA^{-1}Av_1$
$= rAPv_1 = r^2Av_1 = s(Av_1)$

C is with eigenvalue s and s^{-1}.

2. Note that any matrix M with s, s^{-1} can be conjugated to $\begin{pmatrix} s & \\ & s^{-1} \end{pmatrix}$ with $Q \in GL_2(\mathbb{F})$.
$M = Q^{-1}\begin{pmatrix} s & \\ & s^{-1} \end{pmatrix}Q$. But $\begin{pmatrix} s & \\ & s^{-1} \end{pmatrix}$ can commute with any diagonal matrix in $GL_2(\mathbb{F})$, thus Q can be choose with det $= 1$. $\blacksquare$

§ $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.

We have learned in class that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \begin{cases} \{\pm 1\} & n=0 \\ (\mathbb{Z}/n\mathbb{Z})^\times & \text{otherwise} \end{cases}$

where $(\mathbb{Z}/n\mathbb{Z})^\times$ is the unit group of the ring $\mathbb{Z}/n\mathbb{Z}$. We develope ~~more~~ finer discussions about the group

Prop: $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ where p is a prime.

Here is a trick.

Let $d \mid p-1$ and assum $r \in (\mathbb{Z}/p\mathbb{Z})^\times$ s.t. $\mathrm{ord}(r) = d$.

That is, ~~$r^d-1=0$ and r is a root of $f(x)=x^d-1$,~~
~~where $f(x) \in \mathbb{F}_p[x]$. It is easily seen (or you will see it in 2 months)~~
~~f can't claim more than d roots. Thus:~~

$$\cancel{f_d = \#\{r \in (\mathbb{Z}/p\mathbb{Z})^\times,\ \mathrm{ord}(r)=d\} \le d}$$

$r^d-1=0 \Rightarrow r$ is a root of $f(x)=x^d-1 \in \mathbb{F}_p[x]$

f has at most d roots and all elements of $\langle r\rangle = \mu_d$ are distinguished roots of $f(x)$. Hence those are all the elemets that satisfy $x^d-1=0$

What's more, the only elements of order d are the generators of μ_d. And $\#\mu_d^\times = \varphi(d)$.

Hence, let $f_d = \#\{r \in (\mathbb{Z}/p\mathbb{Z})^\times,\ \mathrm{ord}(r) = d\}$

Then $f_d = 0$ or $\varphi(d)$.

But $\sum_{d \mid p-1} f_d = \#(\mathbb{Z}/p\mathbb{Z})^\times = p-1 = \sum_{d \mid p-1} \varphi(d)$, this makes $f_d = \varphi(d)\ \forall d \mid p-1$

In particular, $f_{n-1} = \varphi(n-1) > 0$, which means that $\mathbb{Z}/p\mathbb{Z}$ is cyclic

Prop 2. Let $p > 2$ and m be a primitive root modulo p.

Then:

either m or $m+p$ is a primitive root modulo p^2.

In particular, $\left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^\times$ is cyclic.

pf: m exists due to previous prop.

Then $m^{p-1} \equiv 1 \bmod p$. and $m^k \not\equiv 1 \bmod p$ $\forall\, 0<k < p-1$.

$\Rightarrow$ $\mathrm{ord}_{p^2}(m) \geq p-1$. But $\mathrm{ord}_{p^2}(m) \mid p(p-1)$, where

we know that $\#\left(\frac{\mathbb{Z}}{p^2\mathbb{Z}}\right)^\times = p(p-1)$

Thus either $\mathrm{ord}_{p^2}(m) = p-1$ or $p(p-1)$ by Lagrange Theorem.

If $m^{p-1} \not\equiv 1 \bmod p^2$, then we are done.

Otherwise, $m+p$:

first notice that $m+p \equiv m \bmod p$ $\underset{\text{(why?)}}{\Longrightarrow}$ $\mathrm{ord}_{p^2}(p+m) \geq p-1$.

think about it.

But $(p+m)^{p-1} = m^{p-1} + (p-1)pm + \cdots \equiv 1 - pm \bmod p^2$.

$pm \not\equiv 1$ since $p^2 \equiv 0 \bmod p^2$. Thus we are done.

Prop 3. $\mathrm{Aut}\,\frac{\mathbb{Z}}{8\mathbb{Z}} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$

Pf: $\mathrm{Aut}\,\frac{\mathbb{Z}}{8\mathbb{Z}} = \left(\frac{\mathbb{Z}}{8\mathbb{Z}}\right)^\times = \left(\{1,3,5,7\}, \times \pmod 8\right) \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$

Prop: $\left(\frac{\mathbb{Z}}{2^m\mathbb{Z}}\right)^\times \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^{m-2}\mathbb{Z}}$

§. Semi-product ~~Ø~~.

Motivation: ① Given to generators a, b, what information should be known to get the whole structure of the group? $\boxed{\text{We hope } g = a^m b^n}$ factoring as in $\mathbb{Z}$.

② We have learn that let $H, N \trianglelefteq G$, $HN = G$, $H \cap N = \{1\}$, then $H \times N \cong HN = G$.

It still make sense, if H fails to be normal, to write HN. HN is still a subgroup of G.

Notice that $\langle (12) \rangle \cdot \langle (123) \rangle = S_3$ but

$S_3 \neq \mu_2 \times \mu_3$. since S_3 is not abelian.

Can we learn more of structure of G using HN?

We develop our observations.

① G "uniquely factor" into elements of H and N.

② $|G| = |N||H|$ and we have: $\boxed{G = H \times N \text{ as sets}}$

③ we hope: $(h_1, n_1) \cdot (h_2, n_2) = h_1 \underline{n_1 h_2} n_2 = h' n' = (h', n')$.

Then we have to commute $n_1 h_2$.

But $n \in N$, normal subgroup! Hence the above becomes

$$h_1 n_1 h_2 n_2 = h_1 h_2 \underbrace{(h_2^{-1} n_1 h_2) n_2} = (h_1 h_2, n_1^{h_2} n_2).$$

just a convenient notation

④ Then Recall: $\varphi: H \to \mathrm{Aut}(N)$
$h \mapsto \varphi_h(n) = n^h = h^{-1} n h$.

We have: $\mathrm{Hom}_{\mathrm{Group}}(H, \mathrm{Aut}(N)) \overset{?}{\leftrightarrow} \mathrm{Semi}(H, N)$

~~"≅" is functorial~~" On the other hand, given N and H.

We can construct a group G with each φ: $H \times_\varphi N$.

It is checked that: ~~N~~ $\{1_H\} \times N \lhd H \ltimes_\varphi N$.
left as an exercise to

Conclusion: $G \leftrightarrows (H \to \mathrm{Inn}(N))$. Useful: $(n,h) \longleftrightarrow$ elements in G

but the multiplication is not the trivial one ~~that good~~.

A Basic Example: D_n, the dihedral group of order $2n$.
(二面体群).

It is convenient to write a reflection by τ, and a rotation by ζ.
(or whatever tradition you like). To understand the group:

① order: $\tau^2 = 1$, $\zeta^n = 1$ and $\langle \tau, \zeta \rangle = D_n$.
② How to compute? We would like elements to be the form of $\zeta^m \tau^n$, thus we try to find out min m, n 对: $\tau\zeta = \zeta^m \tau^n$. If this m, n is got, we can compute it using ζ and τ freely.

Fortunately, we have the following facts:

the relation betw (or "torsion") ζ and τ

- $\tau\zeta\tau = \underbrace{\tau\zeta\tau^{-1}} = \zeta^{-1} = \zeta^{n-1}$ $\boxed{\tau\zeta = \zeta^{-1}\tau}$.
- $\langle \zeta \rangle \lhd D_n$, as the above formula shows (or $[D_n : \langle \zeta \rangle] = 2$).

And thus $D_n = H \ltimes_\varphi N$, where $H = \langle \tau \rangle$, $N = \langle \zeta \rangle$.

Then we give a ~~further~~ finer structure of D_n. We try to decide:

① the order of every elements.
② Every subgroup / Normal subgroup structure
③ Every conjugate class

We first explain ③: Given an element g ~~belongs~~ $\in G$, we push it to $h^{-1}gh$ $\forall h \in G$ to get $\{h^{-1}gh : h \in G\}$. This will lead to a partition (划分) of G. The equivalent relation corresponding to that is: $x \sim y \Leftrightarrow \exists z : x = z^{-1}yz$. You see that ~~$G_g$~~ $C_g = \{x : x \text{ "fix" } g, \text{ namely } g = x^{-1}gx\}$ is the subgroup of elements that commutes with g. You see that

$$\sum_{g \text{ over a representative set}} \#K(g) = \#G$$ and:

$K(g)$ means the conjugacy class of g.

$$\#K(g) = \frac{\#G}{\#C(g)}.$$

In fact, that's ~~the~~ a most important group action on a set (in fact, ~~groups~~ on the group itself) in group theory. In the proof of Sylow's theorem, a variant type of it (act on a subgroup class) plays important role.

On the other hand, computing the conjugacy class of a group is standard if you want to attain a "~~repre~~ character table" of ~~the~~ it [see GTM162 or Artin for further].

For ②: every element can written as $z^m\tau$ or z^n.

$(z^m\tau)^2 = z^m\tau z^m\tau = z^m(\tau z \tau^{-1})^m = z^m z^{-m} = 1$, done.

For ①. Forget ~~it~~ at this step. The key is: how does generators behave:

For ③ Observation: $\tau z \tau = z^{-1}$, we have to consider $\boxed{\text{odd or even}}$

$\boxed{\text{case } n \text{ is odd}}$. $z^k \neq z^{-k}$ $\forall k$. ① You first need to consider how τ or z push z^k: $\tau z^k \tau^{-1} = z^{-k}$, $z z^k z^{-1} = z^k$. Thus the conjugacy class of z^k is $\{z^k, z^{-k}\}$, as you can check using z^m, τz^m.

For τ and other order 2 elements: $\boxed{z^{-1}\tau z = z^{-1}\cdot z^{-1}\tau = z^{-2}\tau}$

$\tau^{-1}\tau\tau = \tau$.

n is odd

You then see an orbit: $\tau \xrightarrow{z} z^{-2}\tau \xrightarrow{z} z^{-4}\tau \xrightarrow{z} \cdots \xrightarrow{z} z^{-2n}\tau = \tau$, n elements here.

They form a conjugacy class. Select a remaining element, $z\tau$, for example, you ~~see~~ see similarly: $z\tau \mapsto z^{-1}\tau \mapsto \cdots \mapsto z^{-2n+1}\tau = \tau$.

① For n even, it is left as an exercise.

For ②, at least you can find all normal subgroups using the above observations.

After you learn Sylow's theorem, it is suggested that you do the same ~~calcul~~ calculations for pq groups, where p and q are prime.

§ Factorization of a Group: Normal ~~Series~~ Towers.

· Of course: $12 = 3 \times 2^2$.

You can do a similar thing for groups: e.g. $S_4 \triangleright A_4 \triangleright K_4 \triangleright \mu_2 \triangleright \{1\}$.

It's hopeless to write $S_4 = \underset{\sim}{\frac{S_4}{A_4}} \overset{?}{\times} \underset{\sim}{\frac{A_4}{K_4}} \times \underset{\sim}{\frac{K_4}{\mu_2}} \times \underset{\sim}{\frac{\mu_2}{1}}$. But there are still interesting things here: all "$\sim$" above are simple groups, namely μ_2, μ_3, μ_2, μ_2. In what meaning do they play the role of prime decomposition? Is it unique (in some way)?

On the other hand, it's famous that Galois combined the normal series of Galois Group with the extension field to prove the insolubility of polynomials with degree ≥ 5. Also you will see many "series" here and after..

Definition:

① Tower. $G = G_0 \supset G_1 \supset \cdots \supset G_m$. · Normal tower: "$\supset$" $\Rightarrow$ $\triangleright$.

② Abelian / Cyclic tower: Normal & G_i / G_{i+1} is cyclic.

③ refinement: just insert some into a given tower.

④ soluble: abelian tower & the ending element is trivial.

⑤ $G = G_1 \supset G_2 \supset \cdots \supset G_r = \{e\}$
$G = H_1 \supset H_2 \supset \cdots \supset H_s = \{e\}$ equivalent if:

$r = s$ and $\exists\, \sigma : S\{1, \dots, r-1\}$ $i \mapsto i'$ s.t.

$$\frac{G_i}{G_{i+1}} = \frac{H_{i'}}{H_{i'+1}}$$

Theorem: G : group. Two normall towers of subgroups ending with the trivial group have equivalent refinements (Schrier)

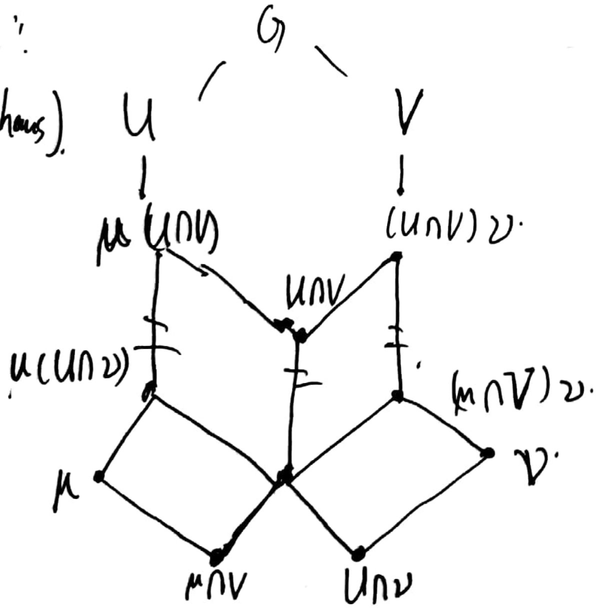
Theorem: $G = G_1 \supset G_2 \supset \cdots \supset G_r = \{e\}$, normal tower $\frac{G_i}{G_{i+1}}$ is simple $G_i \neq G_{i+1}$. Any other "factorizations" of G is equivalent to it.

Lemma 1. $f : G \to G'$; $G' = G_0' \triangleright G_1' \triangleright \cdots \triangleright G_m'$

Then: Let $G_i = f^{-1}(G_i')$, we have $G = G_0 \triangleright G_1 \cdots \triangleright G_m$.

"Pull back".

Lemma 2. (Zassenhaus).



μ, ν: $\mu \triangleleft U$
$\nu \triangleleft V$.

Then: $\mu(U\cap\nu) \triangleleft \mu(U\cap V)$
$(\mu\cap V)\nu \triangleleft (U\cap V)\nu$.

and: $\dfrac{\mu(U\cap V)}{\mu(U\cap\nu)} \cong \dfrac{(U\cap V)\nu}{(\mu\cap V)\nu}$

Proof: Add a point: $(\mu \cap V)(U \cap v)$. Check: normal.

Check: $(\mu \cap V)(U \cap v) \triangleleft U \cap V$.

Check: $\frac{\mu(U \cap V)}{\mu(U \cap v)} \simeq \frac{U \cap V}{(\mu \cap V)(U \cap v)} \simeq \frac{(U \cap V)\nu}{(\mu \cap V)\nu}$

symmetric.

Use isomorphism theorems.

$$\frac{\mu(U \cap V)}{\mu(U \cap v)} = \frac{(\mu U \cap v)(U \cap V)}{\mu U \cap v} \overset{2nd}{=} \frac{U \cap V}{\mu U \cap v \cap (U \cap V)} = \frac{U \cap V}{(\mu \cap V)(U \cap v)}$$

Observation: Every Normal Tower can be refined so that $\frac{G_i}{G_{i+1}}$ is simply.

Pf of thm 1: $G_1 \triangleright G_2 \triangleright G_3 \triangleright$ Trick.

insert $H_1 \supset H_2 \supset \cdots$

See butterfly.

Namely: $G_1 \triangleright G_{11} = G_2(H_1 \cap G_1) \boxed{\triangleright} G_{12} = G_2(H_2 \cap G_1) \triangleright \cdots \triangleright G_2 \triangleright \cdots$

$G_{ij} = G_{i+1}(H_j \cap G_i)$

Similarly: $H_{ji} = H_{j+1}(G_i \cap H_j)$.

$$\frac{G_{ij}}{G_{i,j+1}} \simeq \frac{H_{ji}}{H_{j,i+1}}$$ By Butterfly.

- $(r-1)(s-1)+1$ elements
- end with $\{e\}$

Proof of thm 2: Do refinement As above.

$\forall i \ \exists$ one j: $\frac{G_i}{G_{i+1}} = \frac{G_{ij}}{G_{i,j+1}}$ (You got many "trivial refinement")

You may refer to P144 for more about "solvable groups".

群论 课本习题解答（part）

$1.2.1.$ 幺：$f: \begin{matrix} \alpha \mapsto 1 \\ A \to G. \end{matrix}$ 逆：$(f^{-1})(\alpha) = (f(\alpha))^{-1}$.

$1.2.2.$

$1.2.3$ 解析几何.

$1.2.5.$ 只有 (3)

$1.2.6.$ $\forall x,y \in \bigcup_{n\geq 1} \mu_n \quad \exists N: \quad x,y \in \mu_N$.

$1.2.7$ 例子：$\{(n,n) : n \in \mathbb{Z}\}$.

$1.2.8.$ ✓

$1.2.9.$ $a,b \in G^\times$ 则 $ab^{-1} \in G^\times$.

$1.2.10.$ $a_1,\cdots,a_n \in G \quad |G|=n \Rightarrow \exists\ 1\leq p\leq q\leq n: \quad a_p a_{p+1}\cdots a_q = 1$.

Pf: 考虑集合 $\{a_1, a_1a_2, \cdots, a_1\cdots a_n\} = S$ 若 $1\in S$, done.
若不然，$\exists\ i<j$: $a_1\cdots a_i = a_1\cdots a_j$ 从而 $a_i\cdots a_j = 1$

$1.2.11$ 若不然，取 $a\in A\setminus B \quad b\in B\setminus A$ 则 $a^{-1}\in A \quad b^{-1}\in B \Rightarrow ab\notin A\cup B$, 矛盾.

$1.2.12.$ $x^2=1$ 偶数阶群. 总有偶数个解.

$G - \{1\} - \underbrace{\{2\text{阶元}\}}_{\{x^2=1\}}$ 是偶数 [g 和 g^{-1} 配对]

$1.2.13.$ $O_{p,q}(\mathbb{R}) := \{A\in GL_n(\mathbb{R}) : A^T \begin{pmatrix} I_p & \\ & -I_q \end{pmatrix} A = \begin{pmatrix} I_p & \\ & -I_q \end{pmatrix}\}$.

Pf: $A^{T-1} = A^{-1T} \qquad \begin{pmatrix} I_p & \\ & -I_q \end{pmatrix}^{-1} = \begin{pmatrix} I_p & \\ & -I_q \end{pmatrix}$.

$Sp_{2n}(\mathbb{R}) = \left\{A : A^T \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} A = \begin{pmatrix} & I_n \\ -I_n & \end{pmatrix}\right\}$

$1.2.14$ 、$1.2.15$: easy (由 $1.2.11$)

$1.2.16.$ ($\Rightarrow$). AB 是 G 的子群 $\Rightarrow$ ($ba = [a^{-1}b^{-1}]^{-1} \in AB \Rightarrow BA \subseteq AB$)

$AB = (AB)^{-1} = B^{-1}A^{-1} = BA$.

($\Leftarrow$) $AB = BA \Rightarrow \forall\ a_1,a_2\in A;\ b_1,b_2\in B: (a_1b_1)(b_2^{-1}a_2^{-1}) = a_1(b_1b_2^{-1})a_2^{-1} = a_1a_3b_3 \in AB$

1.2.17 $A \to A^{-1} \to A^{-1}g$ 是双射，

从而 $|A^{-1}g| + |B| > |G|$

$\Rightarrow A^{-1}g \cap B \neq \emptyset \Rightarrow$ $\exists a \in A\ b \in B$ $a^{-1}g = b$ i.e. $g = a$

1.2.18. (1) ~~[illegible]~~ 利用欧几里得除法 + 最小 argument.

(2) $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle_n = \langle \mu_n \rangle$ 故所有子群为 $\langle \mu_n^k \rangle$ $k=1,\cdots,n$.

1.2.19 1.1.20 easy.

1.2.21 (1) $H \times K \to \mathbb{R}^\times$
$(a, b) \mapsto ab$.

(2) $\mathrm{Diag}_n(F) \times T_n(F) \to B_n(F)$
$(\lambda I, A) \mapsto \lambda A$.

(3). $H \times K \to G$.
$(e^{i\theta}, r) \mapsto re^{i\theta}$ $r>0$.

1.2.22. ~~$(\mathbb{Q},+)$ 中每个元素都是有限阶元~~ $(\mathbb{Q},+)$中的有限阶元 ✓
~~$(\mathbb{Q}^*,\times)$ 中，2 不是有限阶元~~ $(\mathbb{Q},\times)$ 中有限阶元：只有 ± 1

1.2.23. $\varphi: (a,b) \mapsto \begin{pmatrix} a & b \\ & 1 \end{pmatrix}$. $(a,b): a \neq 0$

$$\begin{pmatrix} a & b \\ & 1 \end{pmatrix}\begin{pmatrix} c & d \\ & 1 \end{pmatrix} = \begin{pmatrix} ac & ad+b \\ & 1 \end{pmatrix} = \varphi(ac, ad+b) = \varphi((a,b)\cdot(c,d))$$

1.2.24 G 有一个无不动点的自同构 α. 且 $\alpha^2=1$. 证明：G 是奇数阶阿贝尔群.

Pf: 只需证明 $\alpha(g) = g^{-1}$ $\forall g \in G$.
为此注意到 α 无不动点，从而 $h \to \alpha(h)h^{-1}$ 是双射（单⇒满），故 $g = \alpha(h)h^{-1}$ ($\exists h$)
两边用 α 作用，得 $\alpha(g) \underset{\alpha^2=1}{=} h\alpha(h)^{-1} = g^{-1}$ 得证.

1.3.1. A = 4阶 B: 3阶. AB: 无穷 BA: 无穷阶.

1.3.4. $k=0 \cdots\cdots 1$ 不变: d_G $\bar{n}\bar{k}^{-1}$, $d \le n$.

1.3.6. $f^2 = 1_G$ $g^3 = \dfrac{\dfrac{\frac{x-1}{x}-1}{\frac{x-1}{x}}-1}{\dfrac{\frac{x-1}{x}-1}{x}} = 1$

Check: $fgf^{-1} = g^{-1}$.

1.3.7. (1). $g=e^{i\theta}$ 取 θ最小的那个元素，它是生成元.

(2) $\mathbb{Q}$不是循环群：设 $\mathbb{Q}=\langle \frac{p}{q} \rangle$ 则 $\frac{1}{q+1}$ 无法生成. (注：运算是加法)

有限生成子群：$\langle \frac{1}{a_1}, \cdots, \frac{1}{a_n} \rangle$ 取 $g=\frac{1}{\mathrm{lcm}(a_1,\cdots,a_n)}$ 即为生成元.

(3) 注意到 G的子群有链的结构：

$\{1\} \le G_1 \le G_2 \le G_3 \le \cdots\cdots$

$G_i = \{x \in G : x^{p^i} = 1\}$.

1.3.3 $aba^{-1} = a^5ba^{-5} = a^3 \cdots (a^3ba^{-3}) \cdot a^{-3} = b$

$\Rightarrow ab=ba$.

1.3.8. $(ab)^k=1 \Rightarrow a^kb^k=1 \xRightarrow{k最小} m|k, n|k \xRightarrow{(m,n)=1} mn|k$ & $(ab)^{mn}=1$

$\Rightarrow$ order of ab is 1.

1.3.9. TBD

1.3.11. $n = \sum_{d|n} \varphi(d) = \sum_{d|n} \psi(d)$. $\psi(d)$是d阶元的个数

则由 $\psi(d) \le \varphi(d)$ [d阶元有一个 $\Rightarrow$ 至少有$\varphi(d)$个]. 由条件, $\psi(d) \le d$.

故$\psi(d) = \varphi(d)$或0, 特别, $\psi(n) = 1$

1.3.12: $n\mathbb{Z}$.

1.3.13. (1). $(ab^{-1})^{mn} = a^m b^{-n} = 0$.

(2) 由1.3.1利得.

1.3.14. (1) Abel $\Rightarrow$ $\varphi \in End(G)$.

- $x^2 = y^2 \Rightarrow (x^{-1}y)^2 = 1 \xrightarrow{odd} x = y$.
- injective & finite $\Rightarrow$ surjective.

(2). $\varphi_d(x) = x^d$. $(d, n) = 1$ when $n = |G| < \infty$.

1.3.15. G abel $\alpha \in Aut(G)$. $\alpha \circ \alpha = id$.

$G_1 = \{g \in G : \alpha(g) = g\}$ $G_{-1} = \{g \in G : \alpha(g) = g^{-1}\}$

(1). $\alpha g = g = g^{-1} \Rightarrow g = 1$ since $|G|$ odd.

$g = [g\alpha(g^{-1})]\alpha(g)$

$= h \quad k$ $\quad \alpha(h) = \alpha(g) g^{-1} = h^{-1}$ since $\alpha \circ \alpha = 1$.

$\alpha(k) = g$

(2) 特别: $\exists! h \in G : h^2 = 1 \Rightarrow h = 1 \Rightarrow$ no non-trivial order-2-element.

$\Rightarrow G_1 \cap G_{-1} = 1$

(i) (ii): 取 α 为转置, $x \mapsto -x$.

1.3.16. (1) $Aut(\mathbb{Q}, +)$: $\varphi \in Aut(\mathbb{Q}, +)$

Classical Problem for Beginners determin $GL(\mathbb{F}_p^n)$?

q_φ: $\varphi(1) = q_\varphi$ Then $q_\varphi \leftrightarrow \varphi$. correspondence.

$\psi \circ \varphi(1) = q_\varphi q_\psi$ Thus $Aut(\mathbb{Q}, +) \cong \mathbb{Q}^\times$.

(2). $\varphi(1) = \pm 1. \Rightarrow Aut(\mathbb{Z}) \cong \mu_2$.

(3). $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \cong \mathbb{F}^2$ $Aut(K_4) \cong GL_{\mathbb{Z}}(\mathbb{F}_2^2)$ 加法群同构,即Z模同构

$\cong GL_{\mathbb{F}_2}(\mathbb{F}_2^2)$. And hence we consider Matrix Group. of.

We have: $\left\{ \begin{pmatrix} 1 & \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}, \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, \begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} & \\ 1 & 1 \end{pmatrix}. \right\} \cong S_3$

~~$A f_i$~~ ~~$\hookrightarrow$~~ ~~$\mathcal{O}\ x f_i$~~

New:

1.4.1. $(a,b)(c,d) = (ac, ad+b)$ $a \in \mathbb{R}^\times, b \in \mathbb{R}$

注意到 $G \cong \left\{ \begin{pmatrix} a & b \\ & 1 \end{pmatrix} \dots \right\}$

1.4.2 $G = GL_n(\mathbb{R})$ $H: \det > 0$

$\frac{G}{H} =$ $G \to \mathbb{R} \to \mathbb{F}_2$.

1.4.3. (2) 反例: $K_4 \triangleleft A_4 \triangleleft S_4$ 但 $K_4 \ntriangleleft S_4$

1.4.4.

(1) $aba^{-1}b^{-1} \underset{\forall b}{=} 1 \Rightarrow \tau^{-1}a\underbrace{\tau b \tau^{-1}}_{b'}a^{-1}\underbrace{\tau b^{-1}\tau^{-1}}_{b'}\tau = \tau^{-1}aa^{-1}\tau =$

(2) 注意到 $aN = Na$ $\forall a$.

1.4.5. 显然

1.4.6. $\boxed{\text{反证法.}}$ $Z(G) \subsetneq G$ $\Rightarrow \frac{G}{Z(G)} = \langle a + Z(G) \rangle$

$a \notin Z(G)$. Claim: $ab = ba$ $\forall b$ 于是矛盾.

- $\forall b \in Z(G) \Rightarrow ab = ba$
- $\forall b \notin Z(G) \Rightarrow b = a^n c$ $c \in Z(G)$ 由循环群
  $\Rightarrow ab = aa^n c = ca^n = (ca^n)a = ba$.

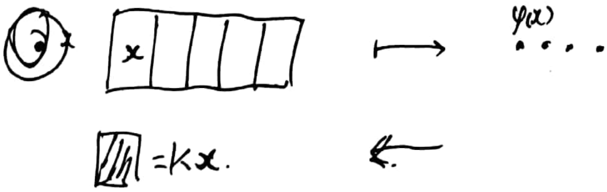
1.4.7 (外直积) 显然.

1.4.8. (2) $\mathrm{Inn}(G)$: $\langle \partial_x \partial_y, g \rangle = \langle \partial_x, yg y^{-1} \rangle = xygy^{-1}x^{-1}$
$= \langle \partial_{xy}, g \rangle$.

(3) $I(G) \cong \frac{G}{Z(G)}$; $G \to Z(G)$, $x \mapsto \partial_x$.

1.4.9. $GL_n(\mathbb{R})$: 先用 $I+E_{ij}$, 再用 $I+E_{ii}$ 作为 "test function".

1.4.10.



1.4.11. (1) $M\cap N=\{1\}$ $a\in M$ $b\in N$ $ab=ba$.

注意到 $aba^{-1}b^{-1}\in M\cap N$

(2) φ $M\times N\to G$ Check: φ 是群同态 (用到了(1))

$(m,n)\mapsto mn.$ $\ker\varphi=1.$

1.4.12. $\mathrm{ord}(g)\,m+n|G/N|=1.$

$\Rightarrow g=g^{\mathrm{ord}(g)\cdot m+n|G/N|}=(g^n)^{|G/N|}\in N.$ why?

1.4.13 利用1.4.6 和1.4.8之得.

1.4.14 TBP

1.3.20 & 1.3.24

20 · 用群作用更容易理解：$G/K\triangleq G$关于K的左陪集.

· H act on $G/K\Rightarrow HxK=\cancel{\mathrm{orbit}(xK)}\bigsqcup_{y\text{遍代表元}} yK$. (轨道中并起来)

· $\mathrm{Stab}(xK)=\{g\in H:\ gxK=xK\}=\{g\in H:\ x^{-1}gx\in K\}$
$=H\cap xKx^{-1}.$

从而：$|HxK|=|K|\cdot\#\mathrm{orbit}=|K|\cdot\dfrac{|H|}{\#\mathrm{Stab}}=\dfrac{|K|\,|H|}{|H\cap xKx^{-1}|}=\dfrac{|K|\,|H|}{|x^{-1}Hx\cap K|}.$

$[g(S\cap T)g^{-1}=gSg^{-1}\cap gTg^{-1}\quad\forall g\in G,\ S,T\leq G]$

1.3.24 $x\sim y\Leftrightarrow x\in HyK.$ $\Rightarrow G=\bigcup_{g_i\in R}Hg_iK.$

$G=\bigcup_{g\in R}AgA$ $AgA=\bigcup Aga_i=\bigcup b_igA$ 而 $A=Ab_i=a_iA.$ $\{b_iga_i;\ g,i\text{ varies}\}$ 即

$\Rightarrow AgA=\bigcup Ab_iga_i=b_iga_iA$