① We begin our lecture with some homework., which involves some counting.

1. Count order-2 element in S_6:

form: (12) ..... $C_6^2 = 15$.

(12)(34). $C_6^2 \cdot 3 = 45$.

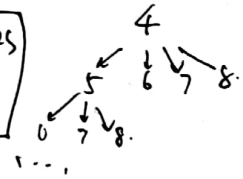
(12)(34)(56) $1 \to 2, 3, 4, 5, 6$ $5 \times 3 = 15$.

Thus $15 + 45 + 15 = 75$.

2. Count the maximal order elements of in A_8.

- What are in A_8?
- the maximal order: (123)(45678). $C_8^3 \cdot 2 \cdot (5 \times 2 = \cdots$

Count 5-cycles with given orbits



3. count elements in S_n that fix no points

Recall De-Morgan's Law:

$$\#(A_1 \cup \cdots \cup A_n) = \sum_{j=1}^{n} (-1)^{j-1} \sum_{\{i_1, \cdots, i_j\} \subset \{1,2,\cdots,n\}} \#(A_{i_1} \cap \cdots \cap A_{i_j})$$

- $\#\{\sigma \in S_n : \exists i \text{ s.t. } \sigma(i) = i\} = \#\bigcup_{k=1}^{n} \{\sigma : \sigma(k) = k\}$

$$= \sum_{j=1}^{n} (-1)^{j-1} \sum_{\{i_1, \cdots, i_j\} \subset \{1, \cdots, n\}} \#\{\sigma(i_1) = i_1 \& \cdots \& \sigma(i_j) = i_j\}$$

$$= \sum_{j=1}^{n} (-1)^{j-1} C_n^j \cdot (n-j)! = \sum_{j=1}^{n} (-1)^{j-1} \cdot \frac{n \cdots (n-j)}{j!} \cdot (n-j)! = (n!) \sum_{j=1}^{n} \frac{(-1)^{j-1}}{j!}$$

$\Rightarrow \#\{\text{the wanted}\} = n!\left(1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^{n-1}\frac{1}{n!}\right)$,

$= n! \sum_{k=0}^{n} \frac{1}{k!}\cdot(-1)^k$

- Next we see an example of the Galois Action on a the set of roots of a polynomial, which lays the foundation of Galois Theory and is the key point of understanding the relation of Symmetry with number field.

· I explain some basic notion in class and give a proposition below

Gauß : Theorem of Symmetric Polynomials. and its corollaries.

·Recall its definition and give some examples.

Theorem : $f \in A[X_1, \cdots, X_n]$, $S_1 = X_1 + \cdots + X_n$, $S_2 = \sum_{i<j} X_i X_j$, $\cdots$, $S_n = X_1 \cdots X_n$

Then $f = g(S_1, \cdots, S_n)$ uniquely ($g \in A[X_1, \cdots X_n]$).

Pf: Some observations : $\sigma : R[X] \to R[X]$.

① $\sigma f(X_1, \cdots, X_n) \mapsto X_{\sigma(1)} \cdots X_{\sigma(n)}$ $\sigma(f_1 f_2) = f_1 f_2(X_{\sigma_1}, \cdots, X_{\sigma n})$

$= f_1(X_{\sigma(1)}, \cdots, X_{\sigma(n)})\, f_2(X_{\sigma(1)}, \cdots, X_{\sigma(n)}) = \sigma(f_1)\,\sigma(f_2)$. in fact, σ behaves like valuation map.

② Thus : if $X_1 \mid f(X_1, \cdots, X_n)$ Then $\sigma(X_1) \mid f(X_{\sigma 1}, \cdots, X_{\sigma n}) \Rightarrow X_1 \mid f(X_1, \cdots, X_n)$ (sym)

· f symmetric, g symetric $\Rightarrow$ $f+g$ is, fg is,

· By induction, on n.

$f(X_1, \cdots, X_n)$ symmetric $\Rightarrow f(X_1, \cdots, X_{n-1}, 0) = g(X_1, \cdots, X_{n-1})$ symetric on $\{X_1, \cdots, X_{n-1}\}$

(15)

$\Rightarrow \quad g(X_1, \cdots, X_{n-1}) = h(\tilde{S}_1, \cdots, \tilde{S}_{n-1})$.

Consider $f(X_1, X_2, \cdots X_n) - h(S_1, \cdots, S_{n-1}) = k(X_1, \cdots X_n)$

Then k is symmetric, moreover: $k(X_1, \cdots X_{n-1}, 0) =$

$f(X_1, \cdots X_{n-1}, 0) - h(\tilde{S}_1, \cdots, \tilde{S}_{n-1}) = 0$.

Thus $X_n \mid k \Rightarrow S_n \mid k$. i.e. $k = S_n u$

A second induction on degree $\Rightarrow u$ is symmetric, and hence $u = V(S_1, \cdots S_n)$.

(degree of multi-variable polynomial)

We give some more remarks: on a field F

- $f(X) = X^n - a_1 X^{n-1} + a_2 X^{n-2} + \cdots + (-1)^n a_n = (x - u_1) \cdots (x - u_n)$

Then one knows that:

$$u_1 + \cdots + u_n = a_1$$
$$\sum_{i<j} u_i u_j = a_2 \qquad u_i \in F$$
$$\vdots$$
$$u_1 \cdots u_n = a_n.$$

What we have proved gives that elements like

$u_1^4 + \cdots + u_n^4 \in F$, being an polynomial of $a_1, \cdots, a_n$.

To generalize this:

$f_1 = f_1(X_1, \cdots X_n)$. $S_n f_1 = \{f_1, \cdots, f_k\}$

$F[Y_1, \cdots Y_k] \ni h(Y_1, \cdots Y_k)$ is symmetric, then

$h(f_1(X_1, \cdots X_n), \cdots, f_n(X_1, \cdots X_n))$ is symmetric.

pf: S_n act on obits gives

$\varphi: S_n \to S_k$.

$\sigma \mapsto \varphi(\sigma)$.

Thus $\sigma \cdot h(f_1(X_1,\cdots,X_n),\cdots f_k(X_1,\cdots,X_n))$.

$= h(f_1(X_{\sigma(1)},\cdots,X_{\sigma(n)}),\cdots f_k(X_{\sigma(1)},\cdots,X_{\sigma(n)}))$.

$= h(f_{\varphi\sigma(1)}(X_1,\cdots,X_n),\cdots,f_{\varphi\sigma(k)}(X_1,\cdots,X_n))$

$= h(f_1(X_1,\cdots,X_n),\cdots,f_k(X_1,\cdots,X_n))$

This above is a way to constract symmetric polynomials.

You can take $P_1(X_1,X_3) = X_1^2 + X_2X_3$.

Since there are some room here, we do an extra exercise.

2.3.18. $K \lhd G$ $\#K=2$ $\bar{G}=\frac{G}{K}$ $\bar{C}$, S,

We assme all are finite

- $S = \varphi^{-1}(\bar{C}) \Rightarrow \#S = 2\#\bar{C}$.
- $\#\bar{C} = \frac{\#\bar{G}}{\#C_{\bar{G}}(\bar{x})} = \frac{1}{2}\cdot\frac{\#G}{\#C_G(\bar{x})}$

$C_{\bar{G}}(\bar{x}) = \{ \overline{gK} : gxg^{-1}x^{-1} \in K, g\in G \}$

$C_G(x) = \{ g\in G : gxg^{-1}x^{-1} = 1 \}$.

$x\in G \Rightarrow \{g_1Kx,\cdots,g_nKx\}$

- $g_iKx = \{g_ix^{g_ik}, x^{g_i}\}$, 可能有两个，可能有1个.
- $g_iKx \neq g_jKx$, $g_iKx \cap g_jKx = \phi$ ✓.

若 $Kx = x$ 则为情况2. 若 $Kx = \{x_1,x_2\}$, 则为情况1

Next we see another discription of S_n, using some notions if the pesentation of a group (§2.5), which leads to the discussion of "Group of. 辫子".

Prop. $S_n \cong \langle s_1, \cdots, s_{n-1} : s_i^2 = 1,\ i = 1, \cdots, n-1,\ s_{i+1} s_i s_{i+1} = s_i s_{i+1} s_i$
$s_i s_j = s_j s_i \quad \forall |i-j| > 1. \rangle$

(Ref: CS)

To begin with, I give some basic facts about S_n:

① β and τ admit a same "cyclic decomposition" (form of) $\Leftrightarrow$ β and τ conjugates in S_n, more over: $\beta^{-1}(123)\beta = (\beta(1)\beta(2)\beta(3))$ as you can check. You may refer to my earlier notes for more about this.

② for ~~cycles~~ cycles, β and τ, $\beta\tau = \tau\beta$ if they are disjoint or they lie in a same cyclic group. One can ask if we only have the two situations.

Now we prove prop.

Observe: $\{(12), (23), \cdots (n-1, n)\}$ generates S_n,

of course: ① $(ij) = (i\ i+1)(i+1\ i+2)\cdots(j-1\ j)\cdots(i+1\ i+2)(i\ i+1)$

② $(i+1\ i+2)(i\ i+1)(i+1\ i+2) = (i\ i+1)(i+1\ i+2)(i\ i+1)$
$(i+2\ \overset{\parallel}{i})$ $(i\ \overset{\parallel}{i+2})$.

③ $(i\ i+1)(j\ j+1) = (j\ j+1)(i\ i+1)$ if $|i-j| \geq 2$.

Now we just keep "$s_i = (i\ i+1)$" in mind and develop our proof.

$\varphi: F(S) \longrightarrow S_n$.

$s_i \mapsto (i\ i+1)$.

since $\{(i\ i+1)\}$ satisfy the relation of $\{s_i\}$, the homomorphism is well-defined.

In fact, what we did is:

$$\begin{array}{ccc} Free[S] & \xrightarrow{\Phi} & S_n \\ \downarrow & \nearrow_{\varphi} & \\ \frac{Free[S]}{\langle Relation \rangle} = F[S] & & \end{array}$$

(Φ: free element, $(s_i \mapsto (i\ i+1))$)

φ exists since $\langle Relation \rangle \subseteq \ker \Phi$

- φ is surjective, using the argument earlier.
  (all generators of S_n are mapped onto)
- To prove φ is injective, we have the sense that the relations of $\{s_i\}$ contain full information of $\{(i\ i+1)\}$ i.e. we have lost no information about $(i\ i+1)$.

  Recall that $\ker \varphi$ measures the loss of information ($\mathbb{Z} \to \frac{\mathbb{Z}}{p\mathbb{Z}}$ means we cannot tell the difference between 0 and p). So we are convinced that φ is injective.

The Argument below is somehow routine, but we need to learn it.

- $0 \to \ker\varphi \to F(S) \to S_n \to 0$

③ The trick is that we count $F(S)$. ~~claim~~:

Claim: $\#(F(S)) \leq n!$

~~Given a tuple, we change it into the form $S_1 \cdots S_n$~~

A further trick is that we use induction and count the decomposition of cosets.

Assume: $\#H = \#\langle S_1, \cdots, S_{n-2} \rangle = (n-1)!$

We claim that $\#F_n[S]/H = n$ (coset decomposition)

We use a further induction method to claim that:

$$F_n[S]/H = \{H, S_{n-1}H, S_{n-2}S_{n-1}H, \cdots, S_1 \cdots S_{n-1}H\}.$$

~~By it we find the~~ minimal length of the tuple

If, length $= 0$: H

length $= 1$: $S_k H = H$ $k \leq n-2$, the only possible choice is $S_{n-1}H$

length 2: by argument of length 1, we find $S_k S_{n-1} H$

notice that ~~S_{n-2}~~ $S_k S_{n-1} H = S_{n-1} H$ $k \leq n-3$

$\Rightarrow$ only $S_{n-2} S_{n-1} H$

⋮

length n: $S_1 S_2 \cdots S_{n-1} H$

the only choice is $S_2 S_1 S_2 S_3 \cdots S_{n-1} H$

But $S_1 S_2 S_1 S_3 \cdots S_{n-1} H = S_1 \cdots S_{n-1} H$

Thus the "algorithm" stops and the only choice is

$\{ H, \cdots s_1 \cdots s_{n-1} H \}$.

We don't need to argue that the above elements are different from one to ~~each~~ another :

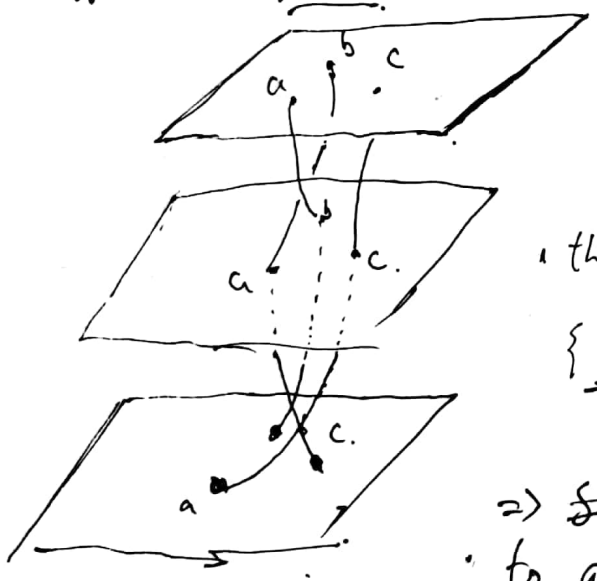
Since $\#(\quad) \leq n$

$\Rightarrow \#F(S) \leq n!$

But $F(S) \twoheadrightarrow S_n$

$\Rightarrow \#F(S) = n!$ & $F(S) \cong S_n$

We now see 2.5.9



· The product is just the gluing of two paths in $\mathbb{C} \times \mathbb{R}$ (x, y, z)

· the generators :

$\{ 1, (ab), (bc), (ac), (abc), (acb) \}$.

generates

$\Rightarrow$ ~~$S_3 + S_4 + S_5 + \cdots$~~.

· to generate the group, first we ~~once~~ remove the restriction

④

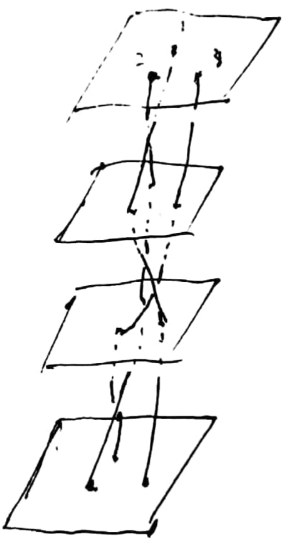
· That $(ab)^2=1$, $(bc)^2=1$.

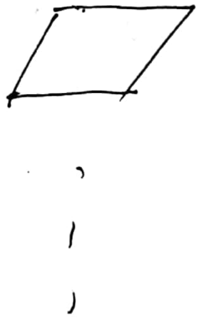
· But we reserve the restrictions:

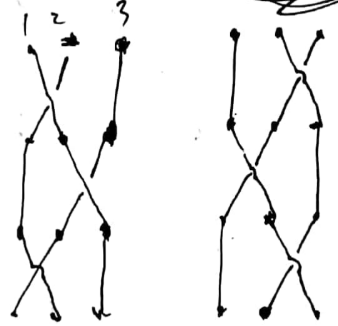
从1出发的个路径.
规定1放在2上面
2放在3上面

平面黑

$s_1 s_2 s_1 = s_2 s_1 s_2$:







这样的两条辫子是等价的:

① 都打到相同的点,

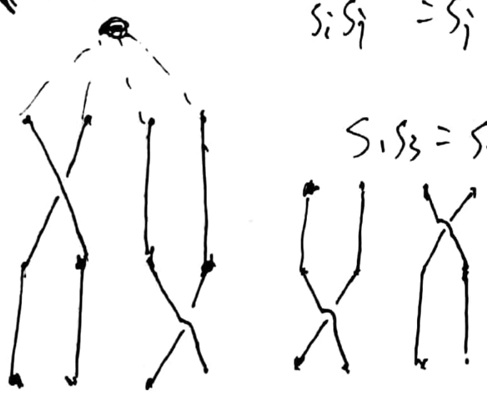
② 每根绳子和其它绳子的覆盖像是相同的

(打出来的结是一样的.

一般的，有

$$B_n = \langle s_1,\dots,s_n : s_{i+1} s_i s_{i+1} = s_i s_{i+1} s_i,\quad s_i s_j = s_j s_i \quad \forall |i-j|>1 \rangle$$

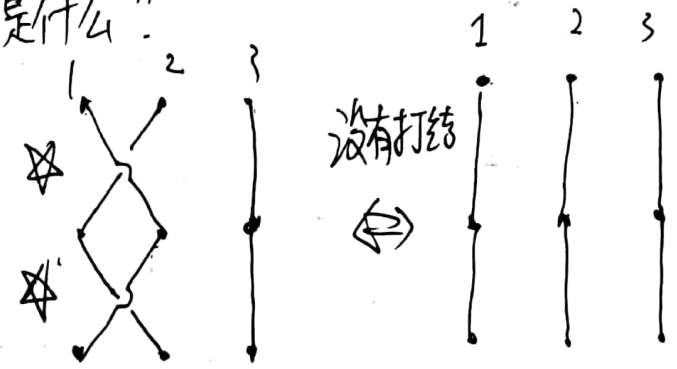
$s_1 s_3 = s_3 s_1$.



打出来的辫子是"一样的.

(以上只是我浅显的理解)

• 商是什么?



• 更多的想法: 把端点最后捏成一个点会是什么? 影长什么样?

Next we see some group actions and with Sylow's Theorem. normal subgroups

• 2.4.2. See my solutions.

• 2.4.6.

$200 = 25 \times 8$.

Take 5-group.

• only one such, done.

• $5+1=6$, : Impossible, since $6 \nmid 200$.

~~21, 26, 31, 36, 41, 46,~~

$224 = 32 \times 7$.

$\#G = 32 \times 7$

Take Sylow-2 group.

① 1 done

② 7 : $\varphi: G \to S_7$. $\ker \varphi \neq 0$: $7 \times 6 \times 5 \times 4 \times 3 \times 2 = 2^4 \times \cdots$

⑤

2.4.9 G. $N \triangleleft G$, P: Sylow p-subgroup.

(1). NP is Sylow p-of N

(2). $\frac{PN}{N}$: $\frac{S}{L}$

(3). $\frac{N_G(P)N}{N} \cong N_{G/N}\left(\frac{PN}{N}\right)$

(1) pf $\frac{\#(NP)}{\#P} = \frac{\#N\,\#P}{\#N\cap P\ \#P} = \frac{\#N}{\#N\cap P}$

(2.) $\frac{\frac{\#G}{\#N}}{\frac{\#P\,\#N}{\#P\cap N\ \#N}} = \frac{\#G\,\#(P\cap N)}{\#N\ \#P} = \frac{\left(\frac{\#G}{\#P}\right)}{\left(\frac{\#N}{\#P\cap N}\right)}$. $\nmid p$ from (1)

(3). $\varphi: N_G(P)N \to N_{G/N}(PN/N)$

$mn \mapsto \overline{mn} = \overline{m}\,\overline{n} = \overline{m}N$

① $\varphi(m) \in N_{G/N}\left(\frac{PN}{N}\right)$.

$\overline{m}\,\overline{p}\,\overline{n}\,\overline{m}^{-1} = \overline{(mpm^{-1})(mnm^{-1})}$

$= \overline{mpm^{-1}} \in \frac{PN}{N}$.

* (lift)

② φ is surjective:

$m \in G$ $\quad \overline{m}\,\frac{PN}{N}\,\overline{m}^{-1} = \frac{PN}{N}$ ①

Claim: $m \in N_G(PN)$:

$mpm^{-1} \in PN$ by ①

$\Rightarrow mpnm^{-1} = mpm^{-1}\,mnm^{-1} \in PNN = PN$

But $\varphi(m) = \overline{m}$.

⑤. $\ker\varphi = N$

obvious. : $N_G(P)N \xrightarrow{\varphi} N_{G/N}(\frac{PN}{N}) \hookrightarrow \frac{G}{N}$.

$\varphi(x)=0 \Leftrightarrow (\varphi(x)=0 \Leftrightarrow x\in N$.

~~Exercise~~ 2: $M \lhd G$, P is a sylow p-group of M. Then $G = MN_G(P)$.

Pf: $P \leq M \lhd G$

$gPg^{-1} \leq gMg^{-1} \leq M$. ($g$)

$\Rightarrow gPg^{-1} = mPm^{-1}$ $m\in M$.

$\Rightarrow m^{-1}g \in N_G(P)$.

3. 2.4.15. $P \overset{\leq G}{\subseteq} N_G(P) \subseteq G$.

$gPg^{-1} \leq gN_G(P)g^{-1} = N_G(P)$, only one.

4 (2.4.3) 首先更正：G 轨道是 Ga.

We have: ~~By the~~ $\Delta = \{x\in Ga : Px = x\}$

$\forall b \in \Delta$:

$b = ga$ $g\in G$.

~~AIM~~: modify g to be an element in $N_G(P)$

$Pb=b \Rightarrow$ $Pb = Pga = b = ga$ i.e. $g^{-1}Pg \in Stab(a) \leq Stab(a)$

$\Rightarrow$ $g^{-1}Pg = hPh^{-1}$, $h\in Stab(a) \Rightarrow gh \in N_G(P)$ and $gha = a$.

⑥ Next we pay attention to some abelian groups and some basic & interesting Homological Algebra.

① $G = G_1 \times G_2 \times \cdots \times G_n$, $i \neq j$, $|G_i|$, $|G_j|$ ~~prime~~ coprime.

$\Rightarrow \forall H \leq G$: $H \cong G_1 \cap H \times \cdots \times G_n \cap H$.

pf: Remark: The underlying idea appears in Chinese Remainder Theorem

① $G_1 \cap H \xrightarrow{i_1} \bigoplus H$ ...

universal property of direct sum $\Rightarrow G_1 \cap H \times \cdots \times G_n \cap H \xrightarrow{i_1 \times i_2 \times \cdots \times i_n = i} H$

② We have to prove:

$$H \longrightarrow G_1 \cap H \qquad (*)$$

is defined.

Then: $H \to G_i \cap H \to \prod G_i \cap H$ (universal property of direct product)

$p \circ i = i \circ p = id$ is checked.

Now we prove (*):

$(h_1, h_2, \cdots, h_n) \mapsto h_1$.

$(|G_1|, |G_i|) = 1 \Rightarrow m_i|G_1| + n_i|G_i| = 1$.

$$\Rightarrow h_1 = \left(\cdots\left(\left(h_1^{m_2|G_1|+n_2G_2}\right)^{m_2G_2+n_1G_3}\right)\cdots\right)^{m_nG_n+n_nG_n}$$

But that gives:

$$\varphi\left[(h_1,h_2,\cdots h_n)^{m_2|G_1|+n_2|G_2|}\right]^{\cdots}$$

$$= \varphi\left[(h_1,\not{e},h_3,\cdots,h_n)\right]^{\cdots} = \varphi(h_1,\not{e},\not{e},\cdots\not{e})$$

$\in G \cap H_1$, done.

2.6.4. $\mathbb{Q}$ is not a free abelic group.

pf: Assume the countrary. $\mathbb{Q} = \bigoplus \mathbb{Z} e_i$.

$\forall e_j \in \mathbb{Q} \Rightarrow \exists q \in \mathbb{Q}$ s.t. $2q = e_j$

$\Rightarrow 2\sum \lambda_i e_i = e_1 \quad 2\lambda_i = 1 \Rightarrow$ contradiction.

- We use ✡ to Get some more interesting properties.

Prop:

$$0 \to A_1 \xrightarrow{\varphi} A_2 \qquad \varphi: A_1 \to \mathbb{Q}$$

A_1, A_2: abelian group.

pf: • 原也多项法: ~~A_2中原~~ $A_1 \subseteq A_2$, $A_1 \to \mathbb{Q}$ 已定义好.

Hard Part: $x \in A_2 \setminus A_1$, $x \mapsto 1 \Rightarrow A_2$ 定义好. ……, 就 A_2 定义好

- Zorn define a partial order on $\{H \mid A_1 \le H \le A_2.$ $f: H \to \mathbb{Q}$, $f|_{A_1} = \varphi\}$

~~$H_1 \le H_2$~~ $\Leftrightarrow H_1 \le H_2$ & $f_2|_{H_1} = f_1$

$(H_1, f_1) \preceq (H_2, f_2)$

(7)

· $(H_1, f_1) \subseteq (H_2, f_2) \cdots \Rightarrow f: \bigcup_{k=1}^{\infty} H_k \to \mathbb{Q}$ is defined $f|_{H_k} = f_k$.

· Maximal element : (H, f).

Claim : $H = A_2$. Otherwise take $x \in A_2 \setminus H$.

- define $H + x \to \mathbb{Q}$.

$\exists\, a \neq 0 \in H \cap \langle x \rangle$ if $H \cap \langle x \rangle \neq \{0\}$,

$a = nx$. Take $\tilde{f}(x) = \frac{1}{n} f(a)$.

$n \neq 0$: $n \neq 0$

Well-defined : $h_1 + n_1 x = h_2 + n_2 x$.

$\Rightarrow \bar{f}(h_2 - h_1) = \frac{n_2 - n_1}{n} f(a) = f(h_1 - h_2)$

$\Rightarrow h_1 - h_2 = \frac{n_2 - n_1}{n} a$. $\Rightarrow f(h_1 - h_2) = \frac{n_2 - n_1}{n} f(a)$

$\Rightarrow \bar{f}(h_1 + n_1 x) = \bar{f}(h_2 + n_2 x)$

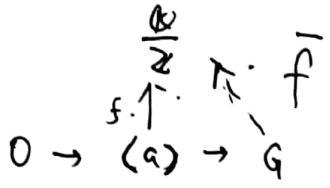
$\Rightarrow$ done.

Further Exercise :

G : abelian group $a \in G$, $a \neq 0 \Rightarrow \exists f \in \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z})$

s.t. $f(a) \neq 0$

pf:



We only need to give $\langle a\rangle \to \frac{\mathbb{Q}}{\mathbb{Z}}$.

if $\langle a\rangle \cong \mathbb{Z}$, easy.

Otherwise: $na=0 \Rightarrow a \mapsto \frac{1}{n}$.

It is left as an exercise to prove that $\bar{f}$ exists.

2.6.6, 2.6.7, 2.6.8, 2.6.9, 2.6.10, 2.6.11, ~~2.6.12~~ 2.6.15&16

是教你如何使用 structure theorem 的好练习，请务必完成.

Some other exercises:

p 为 prime, count # order of p^2 subgroup of $\frac{\mathbb{Z}}{p^2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{p^5\mathbb{Z}}$

我们做一道更难的题. 上面这题留为练习

数 $\frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{9\mathbb{Z}} \oplus \frac{\mathbb{Z}}{9\mathbb{Z}} \oplus \frac{\mathbb{Z}}{243\mathbb{Z}}$ 的 9 阶子群个数.

① 3 阶元: $3^4-1=80$.

② 9 阶元: $3\times9\times9\times9-80-1=2106$

· $\mathbb{Q}$ $\frac{\mathbb{Z}}{9\mathbb{Z}}$ 型: $\frac{2106}{6}=351$

· $\frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{9\mathbb{Z}}$ 型: 把 80 个 3 阶元分成 40 组, $\{e, g^2\}$

则任意两不同组可得到一个 $\frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}$, 每个 $\frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{9\mathbb{Z}}$ 可能中有 4 个不同组, 则

(8)

得 $\mathbb{Z}_{32} \times \mathbb{Z}_{32}$ 共有：

$$\frac{C_{160}^{2}}{C_{4}^{2}} = 130 \text{ 个}.$$

2.6.18. $\mathbb{F}_p$ n 维 $\mathbb{F}_p^n$ ..

(1). $\mathbb{F}_p^n$ p^{n-1} 阶子群.

(2). $\{\mathbb{F}_p^n$ 中 p^k 阶子群 个数$\} = \{p^{n-k}$ 阶子群个数$\}$.

pf: $\{\mathbb{F}_p^n$ 的 subgroups $\} \leftrightarrow \{$Subvector spaces of $\mathbb{F}_p^n$ over $\mathbb{F}_p\}$.

$\{p^k$ ord subgroup $\} \Leftrightarrow \{$Subvector spaces of dimension $k\}$

$\leftrightarrow \{$complement of subvector spaces of dim $k\}$

(direct)

$\leftrightarrow \{$sub vector ~~~ $n-k\}$

$\leftrightarrow \{$subgrp of order $p^{n-k}\}$

In particular: $p^{n-1} \cdots p \cdots \frac{p^n-1}{p-1} = p^{n-1} + \cdots + 1$

2.2.5. Φ 是满足为 $PSL_2(\mathbb{Z})$ 在 $\mathcal{H}^+$ 上作用

$\frac{az+b}{cz+d} = z$ $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $z \in \mathcal{H}^+ = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$

$cz^2 + (d-a)z - b = 0$

$\Leftrightarrow c \neq 0$, 不妨 $c > 0$ ($PSL_2(\mathbb{Z})$)

$(d-a)^2 + 4bc < 0$.

$a^2 + d^2 - 2ad + 4bc$ $\quad ad - bc = 1$

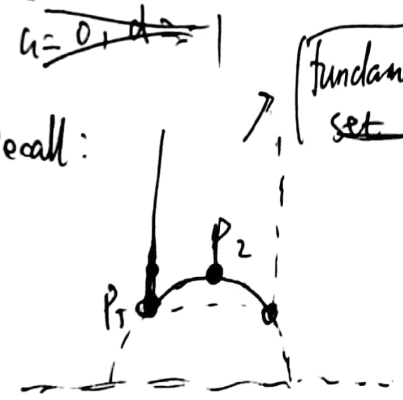
$= a^2 + d^2 - 2ad + 4ad - 4 < 0$

$\Leftrightarrow c > 0$ & $|a+d| < 2$

$a=0, d=0$ $\quad a=1, d=-1$, $\quad a=-1, d=1$, $\quad a=0, d=1$

$a=0, d=1$

Recall:



$z = \frac{a-d+\sqrt{4-(a+d)^2}\,i}{2c}$

- $a+d=1 \Rightarrow c=1$, $a-d=-1$, we get P_1

- $a+d=0 \Rightarrow c=1$

$\Rightarrow |a-d| \leq 2$ $\Rightarrow$ we get P_2

Thus only 2 orbits.