Notes on Algebra I

FE enthusiast enthusiast

2025.09.13

课程概要

- 课程名：代数学 I (Honor)
- 周课时：3+单周习题课
- 授课教师：袁新意
- 给分方法：作业 20% + 期中 30% + 期末 50%，作业每两周一次
- 课程大纲：（完全从网站上抄下来的）
  - 群：子群、商群、同态、群作用、西罗子群、群的直积和半直积、可解群、合成群列
  - 环：理想、同态、商环、分式域、欧几里得整环、主理想整环、唯一分解整环
  - 模直和、自由模、主理想整环上模结构定理、正合列、张量积、局部化
  - 域扩张、分裂域、伽罗华理论、分圆域、五次方程分裂域、无穷伽罗华群
- 参考资料：肖梁老师的 2023 年代数实验班讲义，写的非常非常清楚，以至于我感觉自己整理笔记只是无意义 translation……

  精确到每一周的进度，往年题以及往年题的答案都完全且清晰地在肖梁老师的网页上出现.

Week 1: 2025/9/8

我们为什么学习群/环/域?

- 严格地描述对称性;
- 比较不同的对称性（如正二十面体的对称群核五次方程的根的对称性）
- 确定最“common”的结构的什么样的，即什么样的结构是重要的.

Example 0.0.1. Pell 方程的解可以被写成 $\pm(x_0 + y_0\sqrt{D})^N$，它的解构成一个群 $\mathbb{Z} \times C_2$.（我们把 $\epsilon \cdot (x_0 + y_0\sqrt{D})^N$ 打到 (N, ϵ)，然后给出显然的加法运算）

更不平凡地，椭圆曲线的解构成一个 Abel 群，通过把 $P + Q$ 定义为它们所在的那条直线核椭圆曲线的第三个交点的反射点.

1 群论

1.1 定义，群同构，置换群，生成集

Definition 1.1.1. 一个群包含下述资料:

- 一个非空集合 G,
- 一个二元运算 $\star : G \times G \to G$,

使得以下三条公理成立.

- $(a \star b) \star c = a \star (b \star c)$;
- 存在单位元 $e \in G$ 使得对任意 $a \in G$ 均有 $a \star e = e \star a = a$.
- 对任意 $a \in G$，存在 a 的逆元 a^{-1} 使得 $a \star a^{-1} = e = a^{-1} \star a$.

一个群被称为**交换的**如果对任意 $a, b \in G$ 均有 $a \star b = b \star a$.

我们将 $\#G$ 或者 $|G|$ 定义为 G 的阶，它可能是 $+\infty$.

Remark. 给定群 G 和 n 个元素 $a_1, \ldots, a_n \in G$，我们想计算 $a_1 a_2 \ldots a_n$. 任意钦定乘法的顺序，所得的最终乘积相同.

Example 1.1.2. $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(Z_n, +)$（也被称为 $\mathbb{Z}/n\mathbb{Z}$） 都是群. 我们也可以建构一些不一样的：比如 $\mathbb{Q} \setminus \{-1\} : a \star b = ab + a + b$，它就是错一位的 $\mathbb{Q} \setminus \{0\}$.

Definition 1.1.3. 给定两个群 $(G, \star)$ 和 $(H, \circ)$，可以定义它们的直积 $(G \times H, *)$，其运算定义为

$$(g, h) * (g', h') = (g \star g', h \circ h').$$

Proposition 1.1.4. 下面是一些基本性质:

- 单位元是唯一的；
- 任何元素的逆元是唯一的；
- $(a \star b)^{-1} = b^{-1} \star a^{-1}$；
- 消去律：$a \star u = a \star v$ 可推出 $u = v$.

Remark (Important convention). 我们在群中会频繁地使用 $+$ 和 $\cdot$ 记号. 如果我们不知道 G 是否是 Abelian 的，那么我们一般习惯用 $\cdot$ 来表示运算 $\star$，然后用 1 来表示单位元.

如果我们已经知道 G 是 Abelian 的，那么我们用加号来表示运算 $\star$，用 0 来表示单位元，然后用 $-a$ 来表示 a 在群中的逆元.

Example 1.1.5 (二面体群). 我们用 D_{2n} 来表示正 n 边形的对称群，即把这个图形映回自身的映射构成的群.

首先，$e = \mathrm{id}$ 是把恒同映射，它一定处于这个对称群中.

其次，对称群中有旋转. （顺时针看）角度为 $\frac{2k\pi}{n}$ 的旋转均落在对称群中.把它们记为 $r^1, r^2, \ldots, r^{n-1}$.

最后，有一些翻转也落在对称群中，可以找到它们的对称轴 $l_1, l_2, \ldots, l_n$，并且把“以 l_i 为对称轴的翻转”标记为 s_i.

由此我们可以枚举出群中的所有元素，但是为了描述它们之间的乘法关系还是要费点功夫. 此外，很明显我们可以用一个旋转来表示所有旋转，用一个翻转和一个旋转来表示所有翻转. 它的严格表达就是利用生成元的语言.

$$D_{2n} = \left\langle r, s \mid r^n = 1,\, s^2 = 1,\, srs = r^{-1} \right\rangle.$$

我们可以直观来理解 $srs = r^{-1}$，我们把图形画在一张纸上，翻转，旋转，再翻回去相当于在这个图形的背面作了一次（反方向的）旋转.

Definition 1.1.6 (生成集). 一个群 G 的子集 S 被称为**生成集**，如果 G 中任何元素都可以被写成 S 中**有限个**元素及其逆的乘积.（一般来说我们并不要求 S 的元素个数有限） 生成集中一个关于**生成元**和它们的逆的等式叫做**生成关系**. 我们用 $G = \langle s_1, \ldots, s_n \mid R_1, \ldots, R_m \rangle$ 来表示通过 $s_1, \ldots, s_n$ 这些生成元，$R_1, \ldots, R_m$ 这些关系所生成的群.

Example 1.1.7. 生成关系未必是好的. 比如说我们可以给 Z_6 一个非常 awkward 的用生成元和生成关系的表达：

$$Z_6 = \left\langle r, s \mid r^3 = s^2 = 1,\, rs = sr \right\rangle.$$

这说明我们需要寻找好的生成关系来看出群的性质.

Definition 1.1.8 (置换群). 设 Ω 是一个集合，那么 $S_\Omega = \{\sigma : \Omega \to \Omega \text{ 的双射}\}$ 具有群的结构.

乘法被定义为复合运算. $(\sigma\tau)(x) = \sigma(\tau(x))$，单位元是 id，逆元就是映射的逆.

我们把 S_Ω 称为 Ω 的对称群或者置换群. 当 $\Omega = [n]$ 时我们记其为 S_n.

置换群中的元素有多种表现方式，比如写成两行，第一行分别是 Ω 的元素，a 的下方写 $\sigma(a)$；

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix}$$

或者循环圈的表达形式：我们称 $\sigma = (a_1, a_2, \ldots, a_r)$ 是一个循环圈，它表示

$$a_1 \overset{\sigma}{\longmapsto} a_2 \overset{\sigma}{\longmapsto} \ldots \overset{\sigma}{\longmapsto} a_n \overset{\sigma}{\longmapsto} a_1.$$

任何 S_n 中的元素都可以写成一些互不相交的循环圈的乘积，并且这个乘积是可交换的.

Proposition 1.1.9. 下面有一些关于 S_n 生成元的命题：

- S_n 可以被全体对换生成；
- S_n 可以被全体相邻对换生成；
- S_n 可以被两个元素 $(1,2)$ 和 $(1,2,3,4,\ldots,n)$ 生成.

Definition 1.1.10 (群同构). 我们称两个群 $(G, \star)$ 和 $(H, \circ)$ 是同构的，如果存在同构 $\phi : G \xrightarrow{\sim} H$ 使得

- ϕ 作为集合间的映射是双射；
- ϕ 保持结构，即

  (i) $\forall\, g, h \in G$，$\phi(g \star h) = \phi(g) \circ \phi(h)$；

  (ii) $\phi(e_G) = e_H$；

  (iii) $\forall\, g \in G$，$\phi(g^{-1}) = \phi(g)^{-1}$.

  但是 (i) 蕴含了 (ii) 和 (iii)，所以我们一般看到的定义就只含有 (i).

Example 1.1.11.

- 指数函数 $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ 是群同构；
- $(Z_n, +) \to \{z \in \mathbb{C},\, z^n = 1\}$ 存在一个群同构，比如把 a 打到 $\zeta_n^a = e^{2\pi \mathbf{i} a/n}$.

群论中一个基本的问题是，我们想在同构的意义下把群进行**分类**. 比如 6 阶群在同构的意义下只有 Z_6, S_3 两种.

Definition 1.1.12. 一个群 H 被称为**循环群**，如果它能够被一个元素所生成，即存在 $x \in H$ 使得 H 中所有元素都能被表示成某个 x^n. 换句话说，$H = \langle x \rangle$.

循环群一共只有两类：如果是有限的 n 阶群那么它同构于 Z_n，如果是无限群那么它同构于 $\mathbb{Z}$.

Definition 1.1.13. 一个群 G 的子集 H 被称为一个子群，如果它在 G 附带的结构下构成一个群，即

- $e \in H$;
- $\forall\, a, b \in H,\ a \cdot b \in H$;
- $\forall\, a \in H,\ a^{-1} \in H$.

记作 $H \leqslant G$. 我们也有一种偷懒的验证方法：只要对任意 $a, b \in H$ 可推出 $ab^{-1} \in H$ 就能验证 H 是一个子群.

Remark (Notation). 设 A 是 G 的一个子集，我们记 $\langle A \rangle$ 为 G 中由 A 生成的子群，它的具体表达形式是

$$\{a_1^{\epsilon_1} \dots a_r^{\epsilon_r} \mid a_1, \dots, a_r \in A,\ \epsilon_i \in \{\pm 1\}\} = \bigcup_{A \subset H \leqslant G} H.$$

Definition 1.1.14. 设 G 是一个群，$x \in G$. 定义 G 中元素 x 的阶为 $|\langle x \rangle|$，简记为 $|x|$. 那么 $|x|$ 是一个有限群当且仅当对任意 $n \geq 1$ 均有 $x^n = 1$，满足要求的最小的 n 就是 $|x|$. 同时我们有 $\langle x \rangle \simeq Z_n$. 如果 $|x|$ 是无穷群，则 $\langle x \rangle \simeq \mathbb{Z} \leqslant G$.

Week 2: 2025/9/15 2025/9/18

1.2 陪集，Lagrange 定理，正规子群和商群，群同态

Definition 1.2.1. 设 $H < G$ 是 G 的子群. g 对应的左陪集是指集合

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

同样地，可以定义 Hg 是 g 对应的右陪集. 我们通常如果说陪集就是指“左陪集”.

Example 1.2.2.

- 若 $g = e$ 是 G 的单位元，则 $gH = eH = H$ 是一个陪集（称为平凡陪集）. 对任意 $g \in H$ 我们都有 $gH = H$.
- 设 $G = \mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$ 是加法群，$H < G$ 是 $y = 0$ 给出的子群，则对任意 $(a, b) \in \mathbb{R}^2$，$g + H = (a, b) + H = (0, b) + H$ 就是一个陪集. 几何上来看，这时陪集就是平面中平行于 $y = 0$ 的直线. 另外我们注意到，这里的陪集完全对应于 $\mathbb{R}^2$ 和 $\mathbb{R}$ 作为线性空间时所对应的商空间.（但注意在群中我们只能说它是一个集合.）

Proposition 1.2.3. 两个陪集 g_1H，g_2H 要么相等，要么不交.

Proof. 只需证明 $g_1H = g_2H$ 等价于 $g_1^{-1}g_2 \in H$，而 g_1H 和 g_2H 不交等价于 $g_1^{-1}g_2 \notin H$. 

我们需要给全体左陪集构成的集合下一个定义.

Definition 1.2.4 (左商 left quotient). 设 $H < G$ 是一个子群，定义**左商** $G/H := \{gH \mid g \in G\} = \{\text{left cosets}\}$. 同理也可以定义右商 $H\backslash G$. 记 $[G : H] = |G/H|$，称为 H 在 G 中的**指标**.

Theorem 1.2.5 (Lagrange Theorem). 如果有限群 H, G 满足 $H < G$，则 $|H| \mid |G|$.

Proof. 这是因为

$$G = \coprod_{gH \in G/H} gH = \text{陪集的无交并}.$$

容易证明 gH 中元素个数和 H 中元素个数相等（只需利用双射 $h \mapsto gh$），所以

$$|G| = \sum |gH| = |H| \cdot |G/H|.$$

这推出了整除性. 

Corollary 1.2.6. (1) 若 G 是有限群，$g \in G$，则 $|g|$ 整除 $|G|$.

(2) 在上一问的条件下有 $g^{|G|} = e$.

Proof. 这是因为 $\langle g \rangle$ 是 G 的子群，并且 $|\langle g \rangle| = |g|$. 然后利用 Lagrange 定理即可. 

Example 1.2.7. 设 n 是一个正整数，我们知道

$$\left|Z_n^\times\right| = \#\{a \in \{0,\dots,n-1\} : \gcd(a,n) = 1\} = \varphi(n)$$

所以对群中任何元素 $\bar{a}$ 均有 $\bar{a}^{\varphi(n)} = \bar{1}$. 这等价于在 mod n 的意义下有

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Theorem 1.2.8. *如果 G 的阶数为 p，那么 G 是（同构于 C_p 的）循环群.*

Definition 1.2.9. *如果 $a, g \in G$，称 gag^{-1} 是 a 关于 g 的共轭.*

若 $H < G$ 是一个子群，$g \in G$. 设 $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ 被称为 H 关于 g 的共轭. 实际上，gHg^{-1} 也是 G 的一个子群.

通过明显的同构，我们可以得到 $H \cong gHg^{-1}$，但是它们未必相等.

Definition 1.2.10 (正规子群). *一个 G 的子群 H 被称为**正规的**，如果 $H = gHg^{-1}$ 对任意 $g \in G$ 成立. 记作 $H \lhd G$ 或者 $H \trianglelefteq G$.*

Definition 1.2.11 (商群). *如果 $H \lhd G$ 是正规子群，那么可以良定义 $aH \cdot bH = abH$.*

*这时，我们可以把 G/H 实现为一个群，称为**商群**.*

事实上，如果我们希望 $aH \cdot bH = abH$ 良定义，就需要对任意 $h_1, h_2 \in H$，均有

$$ah_1bh_2 = abh \text{ for some } h \in H,$$

这等价于要求 $b^{-1}h_1b \in H$，综合下来就是 $b^{-1}Hb \subset H$. 如果这个要求对任意 b 均成立，这就推出了 $bH = Hb$，从而“正规子群”确实是一个自然的定义.（这里有一个有趣的事实，光有 $bHb^{-1} \subset H$ 无法推出两者相等，一个反例见作业 5.）

Example 1.2.12. 我们之前所说的 Z_n 可被实现为 $\mathbb{Z}/n\mathbb{Z}$，其中模 n 的第 i 个剩余类就是元素 i 对应的商群. 在记号上我们其实会更喜欢 $a + n\mathbb{Z}$ 而不是 $\bar{a}$.

Remark. *我们可能现在会觉得商群的记号很冗余，想要用代表元来表示商群中的结构. 但是 aH 或者 $a + H$ 这样的记号真正体现了商群是“集合族上钦定了群结构”：即在一些问题中我们会同时把 aH 看作一个“集合”和商群里的“一个元素”，这样的写法就会更清楚一些*（不过我们有时也希望陪集不凸显某个代表元的地位，这时往往会直接设成某个 H_i）

接下来我们考虑两个群之间的关系.

Definition 1.2.13 (群同态 homomorphism). *设 G, H 是群，映射 $f : G \to H$ 是一个**同态**如果*

(i) $\forall\, x, y \in G$, $\phi(xy) = \phi(x)\phi(y)$;

(ii) $\phi(e_G) = e_H$;

(iii) $\forall\, g \in G$, $\phi(g^{-1}) = \phi(g)^{-1}$.

可以看到，同构就是双射+同态.

Example 1.2.14.
- 当 $H \lhd G$ 时，G/H 具有群结构. 并且，$\phi : G \to G/H$, $g \mapsto gH$ 是群同态.
- 特别地，$\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto a + n\mathbb{Z}$ 是群同态，也即“把 a 打到它所在的剩余类 $\overline{a}$”是群同态.

Lemma 1.2.15. 如果 $G \xrightarrow{\phi} H$, $H \xrightarrow{P\psi} K$ 是群同态，那么 $G \xrightarrow{\psi\circ\phi} K$ 也是群同态.

Lemma 1.2.16. 设 $\phi : G \to H$ 是群同态.

(i) $\operatorname{im}\phi = \phi(G)$ 是 H 的子群;

(ii) $\ker\phi = \phi^{-1}(e_H)$ 是 G 的正规子群.

(iii) 对任意 $h \in H$，它的原像 $\phi^{-1}(h)$ 是 G 中 $\ker\phi$ 的一个陪集.

Proof. 我们只证明 (ii). 如果 $x \in \ker\phi$ 那么对任意 $g \in G$ 均有 $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e_H$. 从而 $g(\ker\phi)g^{-1} \subset \ker\phi$. 这推出 $\ker\phi \subset g^{-1}(\ker\phi)g$，然后用 g^{-1} 代替 g 就得到证明. 

Remark. 在这个引理之后，我们可以这样子想正规子群：正规子群是所有能作为某个群同态的 kernel 的东西. 这个观点似乎在之后可用来理解 ideal 之类的概念.

Lemma 1.2.17. 一个同态 $\phi : G \to H$ 是单射当且仅当 $\ker\phi = \{e_G\}$.

1.3 同构定理，单群与合成列，Hölder 计划

Theorem 1.3.1 (第一同构定理). 设 $\phi : G \to H$ 是群同态，则

$$G/\ker\phi \cong \operatorname{im}\phi.$$

Remark. 把定义逐条验证即可. 线性空间中也有类似的结论，你甚至可以在证明时想象这是一个线性空间. 这个定理在群论中的地位相当于这个定理陈述在线性代数中的地位（在题目中也是最常见的）.

Theorem 1.3.2 (第二同构定理). 设 $A < G$ 是子群，$B \lhd G$ 是正规子群，那么 $AB < G$ 是子群，$B \lhd AB$ 是正规子群，$A \cap B \lhd A$ 是正规子群. 并且有下述同构

$$(AB)/B \cong A/(A \cap B).$$

Proof. 考虑同态的复合

$$A \longrightarrow AB \longrightarrow (AB)/B; \quad a \mapsto a \mapsto aB.$$

并且证明这是一个同态；这个同态的 kernel 是 $A \cap B$，并且整个同态是满射. 然后利用第一同态定理即可. 

Remark. 当 $A < G, B \lhd G$ 时，实际上 $AB = BA$. 这是因为此时 $ab = (aba^{-1}a)$，而 $aba^{-1} \in B$. 这导致群的乘法可交换.

Theorem 1.3.3 (第三同构定理). 设 H, K 是 G 的正规子群，满足 $H \lhd K \lhd G$，那么 $(K/H) \lhd (G/H)$ 并且

$$(G/H)\big/(K/H) \cong G/K.$$

Proof. 只需要建构同态 $\varphi : G/H \to G/K, gH \mapsto gK$（真的非常自然!），证明同态，满射，以及 kernel 是 K/H 即可. 

Example 1.3.4. 用初等数论来做例子：假设 $a, b \in \mathbb{Z}_{>0}$ 并且 $a \mid b$，那么先模 b，再模 a 和直接模 b 所得的结果是一样的，这两种操作得到的群相同，即

$$(\mathbb{Z}/b\mathbb{Z})\big/(a\mathbb{Z}/b\mathbb{Z}) \cong \mathbb{Z}/a\mathbb{Z}.$$

Theorem 1.3.5 (第四同构定理). 设 $N \lhd G$ 是正规子群，则

$$\{G \text{ 包含 } H \text{ 的正规子群}\} \xrightarrow{\sim} \{G/N \text{ 的子群}\};$$

$$A \longmapsto A/N;$$

$$\pi^{-1}(\overline{A}) \longmapsto \overline{A}.$$

这个双射保持很多结构（不止写出来的一个对应关系），比如群的包含关系，比如群的 index，比如群的相交关系，比如正规性，等等……

Remark. 讲义上把 G 包含 H 的正规子群称为一个“格”（lattice），这个格就不仅表示这些群构成的集合，也包含了上面所述的群之间的各种关系等等.

Proposition 1.3.6 (商群的泛性质 Universal property). 给定群同态 $\phi : G \to H$，假设 $N \lhd G$. 则我们可以定义出自然的群同态 $G/N \to H, gN \mapsto \phi(g)$ 当且仅当 $N \subset \ker \phi$. 反过来说，给定 N，“G/N”满足对任意群同态 $\phi : G \to H$ 使得 $N \subset \ker \phi$ 均存在唯一的 $\Phi : G/N \to H$ 使得图表交换.

$$\begin{array}{ccc} G & \xrightarrow{\phi} & H \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \Phi} & \\ G/N & & \end{array}$$

我们以及看到群的结构十分复杂，群论学家的终极目标就是把有限群进行分类. 根据前面的第四同构定理，只要 G 有非平凡的正规子群 N，对 G 的学习可以转化为对 N 和 G/N 两个群的研究，直到这样的正规子群无法找到为止. 这引出了单群的概念：

Definition 1.3.7 (单群 simple group). *群 G 被称为**单群**，如果 $|G| > 1$ 并且 G 所含的正规子群只有 $\{e\}$ 和 G.*

这便给出了**Hölder 计划**的想法：

- 分类所有有限单群；
- 用有限单群得到所有的有限群.

（后者的情况并非所述的那么简单，因为只有 N 和 G/N 这两个群肯定是复原不出 G 的. 但这不妨碍我们形而上地认为单群是一个“基本模块”.）

有限单群分类的工作在上个世纪已经被完成（which is surprising），有 18 个家族和 26 个散在单群，其中的“家族”是指有规律的一个无限群族，比如 $\mathbb{Z}/p\mathbb{Z}$，$A_n (n \geq 5)$ 之类的。大量的群族都来源于 Lie 群理论（不会在这门课上出现）. 关于有限单群分类的历史，Banana Space 上有一些有趣的说明.

Week 3: 2025/9/22 2025/9/25

受 Hölder 计划的启发，我们可以把“G 分解为 H 和 G/H，每个小群再继续这样分解”所得的所有结果写在一起，这就得到了合成列的定义.

Definition 1.3.8. *在群 G 中，一列子群*

$$\{1\} = N_0 \leq N_1 \leq \cdots \leq N_k = G$$

*被称为***合成列***如果 $N_{i-1} \lhd N_i$ 并且每个 N_i/N_{i-1} 都是单群.*

$$N_1/N_0,\ N_2/N_1, \ldots, N_k/N_{k-1}$$

*被称为***合成因子***或者* **Jordan-Hölder 因子**.

简单来说，当我们把 G 拆分为对 N 和 G/N 的研究时，根据第四同态定理，G/N 的合成列对应于 G 中包含 N 的一个合成列，把两者合起来就得到了 G 的合成列，确实和我们的想法相吻合.

Example 1.3.9. 考虑二面体群 $D_8 = \langle r, s \mid r^4 = s^2 = 1, \quad srs = r^{-1} \rangle$，其中 r 是 90° 的旋转而 s 是反射. 它有以下两个合成列：

- $1 \lhd \langle s \rangle \lhd \langle s, r^2 \rangle \lhd D_8$；
- $1 \lhd \langle r^2 \rangle \lhd \langle r \rangle \lhd D_8$.

前一个可以归结为先把 D_8 拆为 D_4，再只剩下反射；后者可以归结为先把 D_8 拆为 C_4，再把循环群进行拆分.

Theorem 1.3.10 (Jordan-Hölder). *设 G 是一个有限群，则*

(1) *G 存在合成列.*

(2) *合成因子在差一个置换的意义下是唯一的，即如果我们有两个合成列*

$$\{1\} = A_0 \lhd A_1 \lhd \cdots \lhd A_m = G, \quad \{1\} = A_0 \lhd B_1 \lhd \cdots \lhd B_n = G$$

则 $m = n$，并且存在置换 $\sigma \in S_m$ 使得

$$A_i/A_{i-1} \cong B_{\sigma(i)}/B_{\sigma(i)-1}, \quad \forall\, i = 1, \ldots, m.$$

（我更喜欢的表述是合成因子构成的可重集相等）

Proof. 先来证 (1). 如果 G 是单群那么已经成立，若不然则 G 存在正规子群 $H \neq \{1\}, G$，因此 H 和 G/H 都存在合成列. 设

$$\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_r = H; \tag{1}$$

$$\{1\} = N_0 \lhd N_1 \lhd \cdots \lhd N_s = G/H. \tag{2}$$

我们可以把它“嵌入”到 $\{1\} \lhd H \lhd G$ 中：利用第四同态定理，(2) 告诉我们存在一些包含 H 的正规子群 $\tilde{N}_i$ 使得

$$H = \tilde{N}_0 \lhd \tilde{N}_1 \lhd \cdots \lhd \tilde{N}_s = G.$$

所以两项拼起来就是

$$\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_r = H = \tilde{N}_0 \lhd \tilde{N}_1 \lhd \cdots \lhd \tilde{N}_s = G.$$

接下来证明第二部分，讲义上证明较为复杂，课上采用了 [丁,聂] 上的证明：

Proof. 对 $|G|$ 归纳. 我们考虑两个 G 的合成列的最后一项：

$$\{1\} \lhd A \lhd G, \quad \{1\} \lhd B \lhd G.$$

那么 G/A 和 G/B 都是单群. 如果 $A = B$，根据归纳我们已经证完了. 下考虑 $A \neq B$ 的情形，此时根据正规性 AB 是 G 的正规子群，且满足 $A \cup B \subset AB$. 所以根据 $A \lhd AB \lhd G$ 且第一个等号不成立可知 $AB = G$. 所以

$$G/A = AB/A \cong B/(A \cap B), \quad G/B = AB/B \cong A/(A \cap B).$$

最后的两个群都是单群，所以我们得到更长的合成列

$$1 \lhd (A \cap B) \lhd A \lhd AB = G,$$
$$1 \lhd (A \cap B) \lhd B \lhd AB = G.$$

根据归纳假设，A 的合成因子所成可重集是

$$\{(A \cap B) \text{ 的合成因子 }, A/(A \cap B) \cong G/B\}$$

B 的合成因子所成可重集是

$$\{(A \cap B) \text{ 的合成因子 }, B/(A \cap B) \cong G/A\}$$

所以一开始两个关于 G 的合成列的合成因子所成可重集（在同构的意义下）都是

$$\{(A \cap B) \text{ 的合成因子}, G/B, G/A\}.$$

于是归纳成立，证毕. 

讲义上证明了更强的命题，这是一个局部结论：

Lemma 1.3.11 (Zassenhaus). *设 H, K 都是 G 的子群，H^* 和 K^* 分别是 H 和 K 的正规子群. 那么*

(1) $H^*(H\cap K^*)$ 是 $H^*(H\cap K)$ 的正规子群;

(2) $K^*(H^*\cap K)$ 是 $K^*(H\cap K)$ 的正规子群;

(3) $\dfrac{H^*(H\cap K)}{H^*(H\cap K^*)}\cong\dfrac{H\cap K}{(H^*\cap K)(H\cap K^*)}\cong\dfrac{K^*(H\cap K)}{K^*(H^*\cap K)}$.

Proof. (1) 如果我们直接上手考虑正规性，会遇到如下的问题：设 $a,c\in H^*$, $b\in H\cap K^*$, $d\in H\cap K$，

$$(cd)(ab)(cd)^{-1}=c(dad^{-1})(dbd^{-1})c^{-1}\in H^*(H\cap K^*)H^*.$$

其中 $dad^{-1}\in H^*$ 和 $dbd^{-1}\in H\cap K^*$ 分别用到了 $H^*\lhd H$ 以及 $H\cap K^*\lhd H\cap K$. 但是我们发现 c 这个元素没法和左边直接进行交互. 但我们注意到 $H^*\lhd H$ 以及 $H\cap K^*<H$，所以有子群交换

$$H^*(H\cap K^*)=(H\cap K^*)H^*.$$

换句话说，

$$c(dad^{-1})(dbd^{-1})c^{-1}=c(dad^{-1})\big[(dbd^{-1})c^{-1}(dbd^{-1})^{-1}\big](dbd^{-1})\in H^*(H\cap K^*).$$

因此正规性成立，(2) 的证明是完全对称的.

(3) 我们想利用第二同态定理. 令 $A=H\cap K$，$B=H^*(H\cap K^*)$，那么

$$A=H\cap K<H^*(H\cap K),\quad B=H^*\lhd H^*(H\cap K),\quad H^*(H\cap K)<BA=AB.$$

从而 $AB=H^*(H\cap K)$. 再考虑 $A\cap B$：很明显 $a\in H^*$ 和 $b\in H\cap K^*$ 满足 $ab\in H\cap K$ 等价于 $a\in K$，所以 $A\cap B=(H^*\cap K)(H\cap K^*)$. 所以 (3) 完全就是第二同态定理 1.3.2 的推论，证毕. 

接下来回到原问题.

Proof. 我们考虑任何的两个正规列：（不一定要求是合成列）

$$\{1\}=A_0\lhd A_1\lhd\cdots\lhd A_m=G,\quad \{1\}=B_0\lhd B_1\lhd\cdots\lhd B_n=G.$$

我们对 $(H,K,H^*,K^*)=(A_{i+1},B_{j+1},A_i,B_j)$ 使用 Zassenhaus Lemma 1.3.11，首先固定 i 移动 j：

$$A_i=A_i(A_{i+1}\cap B_0)\lhd A_i(A_{i+1}\cap B_1)\lhd\cdots\lhd A_i(A_{i+1}\cap B_n)=A_{i+1}.$$

这完美地嵌入在了 $A_i\lhd A_{i+1}$ 之中，在 $B_j\lhd B_{j+1}$ 之中可以做类似的操作嵌入一些 $B_j(B_{j+1}\cap A_i)$ 得到一个更长的正规列，并且根据引理的 (3) 可知

$$\frac{A_i(A_{i+1}\cap B_{j+1})}{A_i(A_{i+1}\cap B_j)}\cong\frac{B_j(B_{j+1}\cap A_{i+1})}{B_j(B_{j+1}\cap A_i)}.$$

如果我们记 A_i 和 A_{i+1} 之间插入的第 j 个商 $\dfrac{A_i(A_{i+1}\cap B_{j+1})}{A_i(A_{i+1}\cap B_j)}$ 为 a_{ij}， B_j 和 B_{j+1} 之间插入的第 i 个商 $\dfrac{B_j(B_{j+1}\cap A_{i+1})}{B_j(B_{j+1}\cap A_i)}$ 为 b_{ji}，那么上面的同构告诉我们

$$a_{ij}\cong b_{ji},$$

并且两个新的正规列的正规因子分别是 $\{a_{ij}:0\le i<m,0\le j<n\}$ 和 $\{b_{ji}:0\le i<m,0\le j<n\}$，这样两个可重集是相同的.

特别地，如果两个正规列都是合成列，那么任意两个群之间只能插入平凡的子群. 因此对每个 i，$\{a_{ij}:0\le j<n\}$ 中恰有 $n-1$ 个是 1，剩下一个是 A_{i+1}/A_i. 所以 $\{a_{ij}\}_{i,j}$ 作为可重集是 $m(n-1)$ 个 1 和 A 侧的合成因子。 $\{b_{ji}\}_{j,i}$ 作为可重集是 $n(m-1)$ 个 1 和 B 侧的合成因子，这两个可重集相等. 由于合成因子中无 1，故 $m=n$ 并且两侧的合成因子所成可重集相同，证毕. 

有一个很类似合成列定义的很古老的概念：

Definition 1.3.12 (可解 solvable). 一个群 G 被称为**可解的**如果存在一列子群

$$\{1\}=G_0\lhd G_1\lhd\cdots\lhd G_s=G$$

使得 G_i/G_{i-1} 对 $i=1,2,\dots,s$ 都 abelian. 称满足要求的列为**可解列**.

Corollary 1.3.13. 对任意群 G，G 可解当且仅当它的合成列的每个因子都是某个循环群 $\mathbb{Z}/p\mathbb{Z}$.

Proof. $\Leftarrow$ 方向显然，至于 $\Rightarrow$ 方向，证明方法是线找出一个可解列，然后将它细化. 交换群的子群和商群都是交换群，所以细化后每个合成因子都是交换的单群，只有 $\mathbb{Z}/p\mathbb{Z}$. 

Example 1.3.14. 考虑

$$G=\left\{\begin{pmatrix}*&*&*\\0&*&*\\0&0&*\end{pmatrix}\in \mathrm{GL}_3(\mathbb{C})\right\}\text{ 是上三角矩阵群.}$$

我们证明它可解：考虑

$$N=\left\{\begin{pmatrix}1&*&*\\0&1&*\\0&0&1\end{pmatrix}\in \mathrm{GL}_3(\mathbb{C})\right\}\text{ 是严格上三角矩阵群,}$$

$$N'=\left\{\begin{pmatrix}1&0&*\\0&1&0\\0&0&1\end{pmatrix}\in \mathrm{GL}_3(\mathbb{C})\right\}.$$

首先 $N \lhd G$，因为对 $g \in G$ 和 $n \in N$，gng^{-1} 对角元上元素就是 $g_{ii}n_{ii}g_{ii}^{-1} = n_{ii}$. 此外，$G/N$ 就完全是对交矩阵群，这同构于 $\mathbb{C}^3$ 是交换群.

同理可以证明 $N' \lhd N$：N 中元素形如 $I + A_1 + A_2$，N' 中元素形如 $I + B_2$，

$$\begin{aligned}(I + A_1 + A_2)^{-1}(I + B_2)(I + A_1 + A_2) &= (I + A_1 + A_2)^{-1}(I + A_1 + A_2 + B_2) \\ &= I + (I + A_1 + A_2)^{-1}B_2 = I + B_2.\end{aligned}$$

所以 $N/N' \cong \mathbb{C}^2$. 最后 $N' \cong \mathbb{C}$，就完成了证明. 容易看到任意阶的上三角矩阵群都是可解的.

Remark. 也可以从线性空间的视角来看，考虑一个 Flag $V = V_0 \supset V_1 \supset \cdots \supset \{0\}$，然后考虑这个 Flag 的自同构，它作为矩阵就对应着可逆的上三角阵. 之后的过程完全可以用线性空间的语言叙述（$T - \mathrm{id}$ 把 V_i 映到更小的 V_{i+r} 内）.

作业中展现了可解群的如下性质：

Proposition 1.3.15. 可解群的子群和商群都是可解的.

我们接下来具体讨论一类单群，即交错群 A_n. 接下来我们会把 S_n 中的置换分为两类，这乍一看其实并不显然. 但是我们已经对逆序数和圈的对换拆分这样的概念很熟悉了，所以这里仅仅列出定义.

Definition 1.3.16 (置换的奇偶性). 以下几种方式都能定义出置换 $\sigma \in S_n$ 的**奇偶性**，或者说**符号** $\mathrm{sgn}(\sigma) \in \{\pm 1\}$（奇置换对应 -1，偶置换对应 1）：

- 称 σ 的**逆序数**为 $\#\{(i,j) : 1 \le i < j \le n, \sigma(i) > \sigma(i)\}$，$\sigma$ 的逆序数的奇偶性就可以定义成置换的奇偶性；
- 也可以直接写出代数表达式：
$$\mathrm{sgn}(\sigma) = \frac{\prod_{1 \le i < j \le n}(x_{\sigma(i)} - x_{\sigma(j)})}{\prod_{1 \le i < j \le n}(x_i - x_j)}.$$
- 每个置换 σ 都可以被写成一些 2-对换的乘积，如果 σ 是奇数/偶数个 2-对换的乘积，就称其为奇/偶置换.
- 每个置换 σ 都可以被写成一些不交的循环圈的乘积. $(n -$ 循环圈个数$)$ 的奇偶性就可以定义为置换的奇偶性.

可证明 $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau)$，因此

Proposition 1.3.17. $\mathrm{sgn} : G \to (\{\pm 1\}, \times)$ 是群同态.

Definition 1.3.18 (交错群 alternating group). 定义 $A_n = \ker(\mathrm{sgn}) = \{\sigma \in S_n : \mathrm{sgn}(\sigma) = 1\}$，即所有 n 阶偶置换构成的群. A_n 作为 S_n 的 index 为 2 的子群，是一个正规子群.

Theorem 1.3.19. 对 $n \ge 5$，A_n 是单群.

Proof. 证明太炜了……

1.4 群直积，群作用，半直积

我们接下来来讨论群的直积. 这是一种非常自然的用两个群构建一个更大的群的方式. 在 1.1 节我们已经定义过两个群的直积，这里我们正式地对任意多个群来定义.

Definition 1.4.1 (群直积 direct product). 设 I 是指标集，为每个 $i \in I$ 选定一个 $G_i \in \mathsf{Grp}$，定义它们的**直积** $\prod_{i\in I} G_i$ 为：

- 在集合的层面上，$\prod_{i\in I} G_i$ 就是 $(G_i)_{i\in G}$ 作为集合的 Cartesian 积.
- 在群结构的层面上，我们定义群运算 $(g_i)_{i\in I} \cdot (h_i)_{i\in I} = (g_i h_i)_{h\in I}$. 容易验证群运算的良定性.

在群直积中，对两个不同的指标 i, j，G_i 中的元素和 G_j 中的元素是完全交换的，它们之间“完全互不干涉”. 特别地 G_i 是 $\prod_{i\in I} G_i$ 的正规子群.

从群直积 $\prod_{i\in I} G_i$ 到每个分量 G_j 有典范投影态射 $\pi_j : (g_i)_{i\in I} \mapsto g_j$，从每个分量都直积也有含入态射 $\iota_j : g_j \mapsto (\dots, 1, 1, g_j, 1, \dots)$. 注意直积对象所包含的自然的资料是投影.（基于 product 的泛性质）

由于直积结构的交换性很强，我们很难在一般的群内找到直积项，但是对 Abel 群来说有以下非常著名的有限生成 Abel 群结构定理：

Theorem 1.4.2 (有限生成 Abel 群结构定理). 设 G 是有限生成 Abel 群. 则**存在唯一的**和 $r \geq 0$（称为 G 的**秩**）和 $2 \leq n_1 \leq n_2 \leq \cdots \leq n_s$，满足

$$n_1 \mid n_2 \mid \cdots \mid n_s$$

以及

$$G \cong \mathbb{Z}^r \times (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_s\mathbb{Z}).$$

其证明是把 Abel 群看成 $\mathbb{Z}$-模，然后对一般的 PID 讨论 R-模的结构（另一个常用的推论是“存在有理标准型”）. 虽然我们这里还不能给出完整的证明，但是我们可以对其结构进行一些讨论：

Theorem 1.4.3 (中国剩余定理 CRT). 若 $m, n \in \mathbb{Z}$，$\gcd(m, n) = 1$，则

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}).$$

Proof. 构建群同态 $\phi : \mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$：$x \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$，那么

$$\ker\phi = \{x : x + m\mathbb{Z} = 0 + m\mathbb{Z},\, x + n\mathbb{Z} = 0 + n\mathbb{Z}\} = \{x : m \mid x,\, n \mid x\} = mn\mathbb{Z}.$$

从而得到单同态 $\tilde{\phi} : \mathbb{Z}/mn\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$. 根据两边元素个数相同，$\phi$ 自然是群同构. 

那么我们可以把上面的结构定理进一步作拆分到最细致的形式：

Theorem 1.4.4 (最细形式的结构定理). *对任何有限生成 Abel 群 G，存在 $r \geq 0$ 和（允许相同的）素数幂 $p_1^{\alpha_1}, \ldots, p_s^{\alpha_s}$ 使得*

$$G \cong \mathbb{Z}^r \times (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{\alpha_s}\mathbb{Z}).$$

其中可重集 $\{p_i^{\alpha_i}\}_{1\leq i\leq s}$ 是被 G 所唯一确定的.

Remark. 两个形式的结构定理都是非常有用的，对应到线性代数中，就是有理标准型（循环分解）和 Jordan 标准型（准素循环分解）之间的关系. 后者划分地更细致，适合对每个准素部分分开考虑问题，前者的唯一性更强（n_i 有一个大小关系导致整个序列具有绝对唯一的表达方式）而且可以过渡到更一般的命题上去，理论价值更强.

不过比较有意思的是如何快速在两者之间转化：只看 torsion 部分，考虑可重集 $\{p_i^{\alpha_i}\}$ 如何与序列 $(n_1 \mid n_2 \mid \cdots \mid n_s)$ 之间进行对应. 从前者到后者像是把积木一块一块搭起来：首先把不同素数的幂分离（它们互不干扰），只对固定的 p 考虑每个 $\mathbb{Z}/p^{\alpha_i}\mathbb{Z}$ 如何出现在 n_i 序列中. 先把它们根据大小关系排好 $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_t$，根据整除关系以及每个 $\mathbb{Z}/n_i\mathbb{Z}$ 中至多有一个素数幂部分，n_s 必须包含最大的一项 $\mathbb{Z}/p^{\alpha_t}\mathbb{Z}$， $\mathbb{Z}/n_{s-1}\mathbb{Z}$ 中包含次大的一项 $\mathbb{Z}/p^{\alpha_{t-1}}\mathbb{Z}$，依此类推直到 $\mathbb{Z}/n_{s-t+1}\mathbb{Z}$ 中包含 $\mathbb{Z}/p^{\alpha_1}\mathbb{Z}$，而再往前的 $\mathbb{Z}/n_i\mathbb{Z}$ 就不再含有 p 进部分. 看成积木的话，就是先把每种颜色的积木分类，然后每类从小到大排好，把最大的块对齐，再把次大的块对齐，如果某种颜色的积木用完了之后就忽略之.

如果是从右边得到左边，就需要把每种不同的块分离：一个方法如下（可以之间从 G 本身得到所有 $p_i^{\alpha_i}$）：考虑

$$G[p^\alpha] = \{g \in G : p^\alpha g = 0\}.$$

这里采用加法记号，$p^\alpha g = 0$ 指的是 g 自相加 p^α 次后得到零. 我们发现

$$(\mathbb{Z}/q^\beta\mathbb{Z})[p^\alpha] \cong \begin{cases} \mathbb{Z}/p^{\min(\beta,\alpha)}\mathbb{Z}, & q = p, \\ 0, & q \neq p. \end{cases}$$

因此如果设 G 中含有的 p 幂部分为 $\mathbb{Z}/p^{r_1}\mathbb{Z}, \ldots, \mathbb{Z}/p^{r_t}\mathbb{Z}$，那么

$$\#(G[p^\alpha]) = p^{\#\{r_i=1\}+2\#\{r_i=2\}+\cdots+(\alpha-1)\#\{r_i=\alpha-1\}+\alpha\#\{r_i\geq\alpha\}}.$$

从而

$$\#(G[p^\alpha])/\#(G[p^{\alpha-1}]) = p^{\#\{r_i\geq\alpha\}}.$$

从而所有 $\#\{r_i \geq \alpha\}$ 都能被读出，进而所有 r_i 的具体值都能被读出.

接下来回到一般的群讨论群直积，$H \times K$ 实际上是 HK 的最简单结构形式. 下面的识别定理可以完全告诉我们什么时候有 $HK \cong H \times K$.

Theorem 1.4.5 (识别群直积). 设 G 是群，G 的子群 H, K 满足

(1) $H, K \lhd G$;

(2) $H \cap K = \{e\}$;

那么存在群同构 $HK \cong H \times K$.（(1) 可推出 HK 是一个正规子群.）

Remark. 实际上这两个条件经常会出现，比如在考虑 Sylow 子群的时候，可能会得到 $\gcd(|K|, |H|) = 1$ 这个条件，这直接推出 $|K \cap H| = 1$. 这样就立即能推得定理的适用条件成立.

Proof. 我们先来证明直积必须满足的很好的条件成立：$\forall h \in H, k \in K, hk = kh$. 这是因为考虑 $hkh^{-1}k^{-1}$：

$$hkh^{-1}k^{-1} = \begin{cases} (hkh^{-1})k^{-1} \in K \cdot K = K; \\ h(kh^{-1}k^{-1}) \in H \cdot H = H. \end{cases}$$

所以必须有 $hkh^{-1}k^{-1} = e$. 接下来验证显然的映射 $f : H \times K \to HK, (h, k) \mapsto hk$ 是群同构.

- f 是群同构，即

$$f((h,k)(h',k')) = f(hh', kk') = hh'kk' = (hk)(h'k') = f(k,h)f(k',h').$$

- f 是单射，如果 $hk = e$，则 $h = k^{-1} \in H \cap K \Rightarrow h = k^{-1} = e$.

- f 是满射，这好像是显然的.

接下来介绍群作用，是群论中非常重要的一个分支，因为它真正告诉我们群如何被直观地“展现”出来（而不是只有抽象的定义），称为某种对称性，或者反过来考虑某种作用能反过来给出一个群. 比如说置换群就有明显的群作用意义.

Definition 1.4.6 (群作用 Group Action). 设 G 是一个群，X 是一个集合. 一个在 X 上的左 G-群作用是指

$$G \times X \to X, \quad (g, x) \mapsto g \cdot x$$

使得

- $e \cdot x = x, \quad \forall x \in X$;

- $g \cdot (h \cdot x) = (g \cdot h) \cdot x, \ \forall g, h \in G, x \in X$.

群作用的记号可写作 $G \curvearrowright X$. 可以这样考虑它的意义：$G \circlearrowright X$ 即 X 有一个通过 G 到自身的映射.（当然好像是没有专门一个群作用的记号，我们会更多地直接说 G 作用在 X 上或者 X 是一个 G-轨道空间 $X \in \mathsf{G-Set}$.）

Remark. 对每个固定的 g，群作用相当于给出了一个双射 $\rho_g : X \to X$，$x \mapsto g \cdot x$（因为存在逆元 $\rho_{g^{-1}} : X \to X$）. 这是一个非常重要的“转换视角”，我们也经常把一个元素的作用单独拿出来考虑.

群作用有非常多的例子：

Example 1.4.7.

- S_n 作用在 $\{1., \dots, n\}$ 上，表达为

$$S_n \times \{1, \dots, n\} \to \{1, \dots, n\}, \quad (\sigma, i) \mapsto \sigma(i).$$

- $\mathrm{GL}_n(\mathbb{C})$ 可以通过 $(M, v) \mapsto Mv$ 作用在全体列向量 $\mathbb{C}^{1\times n}$ 上.
- D_{2n} 可以作用在平面上的正 n 边形上，r 被打到平面上的旋转，s 被打到沿对称轴的翻折.
- G 作用在自己上，即考虑 $G \times G \to G$，$(g, h) \mapsto gh$. 以下两个作用都是左作用：

$$\ell_g : G \to G, \quad x \mapsto gx;$$
$$r_g : G \to G, \quad x \mapsto xg^{-1}.$$

  它们分别被称为左移和右移.

- G 还可以通过共轭作用作用于自身：

$$\mathrm{Ad}_g : G \to G, \quad \mathrm{Ad}_g(x) = gxg^{-1}.$$

  共轭作用是比左移右移更“好”的群作用，因为 $x \mapsto gxg^{-1}$ 是一个群同态，但是左移和右移都不满足这点，之后会有进一步的说明.

当然我们可以定义右乘作用：

Definition 1.4.8 (右作用 right action). 称 G 右作用于 X 是指

$$X \times G \to X, \quad (x, g) \mapsto x \cdot g,$$

满足 $x \cdot e = x$ 以及 $(x \cdot g) \cdot h = x \cdot (g \cdot h)$，注意右作用和左作用是不完全相同的东西，但是能互相转化.

Proposition 1.4.9. 如果 G 左作用于 X，那么存在一个自然的同态

$$\Phi : G \to S_X, \quad g \mapsto (\Phi_g : X \to X, x \mapsto gx).$$

“G 在 X 上的左作用”可以和“群同态 $G \to S_X$”之间建立双射关系，两者意义相同.

其证明就是群作用定义的一种重述

Definition 1.4.10. 称一个群作用是**忠实的**（faithful）如果 $\ker\Phi = \{e_G\}$. 称其是**平凡的**如果 $\operatorname{im}\Phi = \{\mathrm{id}_X\}$.

Theorem 1.4.11 (Cayley). 任何群 G 都是某个置换群的子群. 如果 $|G| = n$，那么 G 是 S_n 的一个子群.

Proof. 只需考虑 G 关于自身的左移群作用即可. 这个群作用是忠实的，所以 Φ 是单同态，故 G 能实现为 S_G 的一个子群. 

Remark. 这个命题具有更多的历史意义，因为在历史上群的定义就是置换群的子群（置换群的实际意义更明显），这个定理说明这样定义没有损失说明信息. 注意如果对置换群 S_X 使用 Cayley 定理，得到的是 $S_X \hookrightarrow S_{S_X}$. 这说明如果一个群 G 能作用在一个更小的集合 X 上，它的结构能被研究地更清楚.（要有这样的感觉：一个群在一个集合上的作用“存在”这件事本身就不平凡.）

Definition 1.4.12 (自同构群 Automorphism Group). 定义 G 的**自同构群**为所有同构 $\phi : G \xrightarrow{\sim} G$（称为自同构）构成的群，记作 $\mathrm{Aut}(G)$.

Example 1.4.13. 共轭作用是一个很好的作用，因为 Φ 不仅给出了 $G \to S_G$ 的同态，它实际上也是 $G \to \mathrm{Aut}(G)$ 的群同态，即每个 Ad_g 都是群同态. 注意左移作用就不是 G 的自同态.

接下来我们定义半直积. 在群中会广泛出现这样的对象：有两个子群 $N \lhd G$ 和 $H < G$ 满足 $N \cap H = \{e\}$，那么 NH 是 G 的一个子群，集合层面上每对 (n, h) 恰对应 NH 中一个元素，但它未必在群层面上是 $N \times H$. 我们可以定义半直积 $N \rtimes H$ 来描述这件事.

Definition 1.4.14 (半直积 Semiproduct). 给定群 N, H 以及群同态 $\phi : H \to \mathrm{Aut}(N)$. 定义半直积 $N \rtimes H = N \rtimes_\phi H$ 如下：

- 作为集合而言 $N \rtimes H = N \times H = \{(n, h) \mid n \in N, h \in H\}$.
- 群乘法如下定义：

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \phi_{h_1}(n_2), h_1 h_2).$$

可以验证 (e_N, e_H) 是这个群的单位元，而 $(\phi_{h^{-1}}(n^{-1}), h^{-1})$ 是 (n, h) 的逆元.

特别地，当 ϕ 是平凡同态时 $N \rtimes H$ 就是 $N \times H$.

Remark. 半直积的想法其实就是一般的 NH 中的元素如何作相乘：

$$(n_1 h_1) \cdot (n_2 h_2) = n_1 (h_1 n_2 h_1^{-1}) \cdot h_1 h_2 = (h_1 \ \mathrm{Ad}_{h_1}(n_2)) \cdot (h_1 h_2).$$

所以我们其实就是想刻画 H 让 N 如何扭曲从而给出了半直积的抽象定义（注意到这个定义抹去了作为背景的大群 G，如果这样的 G 存在，那么 ϕ 由 G 中 H 在 N 上的共轭作用诱导. 这两者的关系类似内直和和外直和.）

Remark. 半直积也有 $H \ltimes N$ 的记号，我们可以从两方面来理解这个记号：粗略来讲 ϕ 是一个 H 在 N 上的群作用，所以它的记号意谓从 N 出发，经过 H 的“扭曲作用”后重新抵达 N，H 只是 N 的结构所附带的一个“扭曲因子”. 另一方面，也可以看作 $\lhd$ 和 $\rhd$ 记号的延伸，尖角指向的位置就是正规子群.

Proposition 1.4.15. H 是 $N \rtimes H$ 的子群，N 是 $N \rtimes H$ 的正规子群. 类似同构定理，我们能给出

$$(N \rtimes H)/N \cong H.$$

这很好理解，因为 $N \rtimes H$ 在 H 分量上的乘法没有经过扭曲.

Example 1.4.16. 如何把半直积所得的群可视化为一个容易理解的方式是有趣的问题. $(\mathbb{Z}/n\mathbb{Z})^+$ 的自同构群意义对应于合法的生成元 $1+n\mathbb{Z}$ 的像，因此只需把 1 送到和 n 互素的某个 $k+n\mathbb{Z}$ 即可. 这样我们就得到同构 $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})^+$. 于是可考虑半直积 $(\mathbb{Z}/n\mathbb{Z})^+ \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$. 它的运算满足：

$$(a,b)\cdot(c,d) = (a+bc, bd).$$

它可对应为矩阵乘法

$$\begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} d & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} bd & bc+a \\ 0 & 1 \end{pmatrix}.$$

于是就可以把它同构为一个矩阵群.

Example 1.4.17 (pq 阶群). 讲义上还举了关于 pq 阶群建构的例子. 我们之后会证明任何一个 pq 阶群中都含有一个 C_p 和 C_q 作为子群，并且其中较大的是正规子群（这可以参考作业 29），不妨设为 C_p. 那么群可以实现为一个半直积 $C_p \rtimes C_q$. 除了最简单的 Abel 群 $C_p \times C_q$ 之外，如果 $q \mid p-1$，可按下述方法建构非平凡的半直积：上一个例子说过 $\mathrm{Aut}(C_p) \cong (\mathbb{Z}/p\mathbb{Z})^\times$，我们可以证明 $(\mathbb{Z}\times p\mathbb{Z})^\times \cong C_{p-1}$（利用原根），于是 C_q 可实现为 C_{p-1} 的一个子群，从而给出群同态 $C_q \to \mathrm{Aut}(C_p)$. 比如说 $p=7, q=3$ 时，3 是 mod 7 意义下的原根，$3^2+7\mathbb{Z} = 2+7\mathbb{Z}$. 因此可考虑群同态

$$C_3 \to (\mathbb{Z}/7\mathbb{Z})^\times \cong \mathrm{Aut}(C_7),\ \{0,1,2\} \to \{1,2,4\} \to \{\mathrm{id}, x\mapsto 2x, x\mapsto 4x\}.$$

构建出的半直积满足乘法

$$(a,b),(c,d) \in C_7 \rtimes C_3, \quad (a,b)(c,d) = (a+2^b c, c+d).$$

并且它显然是非 Abel 的：$a+2^b c \neq c+2^d a$. 由此可见，半直积是简单有限群分类时，用于构造的一个有力工具.

Example 1.4.18. 我们又可以拿 D_{2n} 作为例子：D_{2n} 在有一个 n 阶循环子群 $N = \langle r\rangle \cong C_n$. 由于它的 index 为 2，所以是 G 的正规子群. 另一个生成元 s 满足

$H = \langle s \rangle \cong \mathbb{Z}/2\mathbb{Z}$. 根据生成元关系我们容易得到 $N \cap H = \{e\}$，以及 $NH = D_{2n}$，从而 D_{2n} 是 N 和 H 的某种半直积. G 中的共轭关系给出 $srs = r^{-1}$，于是 $\mathbb{Z}/2\mathbb{Z}$ 在 C_n 上的群作用是 $[r \mapsto -r] = -\mathrm{id}$.

$$D_{2n} = C_n \rtimes_\phi \mathbb{Z}/2\mathbb{Z}, \quad \phi = -\mathrm{id}\,.$$

Week 5:2025/10/9

1.5 稳定子，轨道，类

回忆上周讲过的群作用的概念，它由一个 $\Phi : G \times X \to X$ 确定. 如果我们想更加强调把 $(G, X, G$ 在 X 上的群作用$)$ 作为一个整体，我们可以说 X 是一个 G-set，把 G 的群作用本身就作为 X 上所附带的资料. G 的 X 上的两个不同作用给出不同的两个 G-set.

实际上，每个 G-set 都可以被实现为一个**群胚** $\mathfrak{X}$：

$$\begin{cases} \text{Obj: } X; \\ \text{Mor: 对每个 } g \in G,\, x \in X\text{，引一条从 } x \text{ 到 } gx \text{ 的箭头.} \end{cases}$$

群作用的性质立刻能让我们验证这是一个群胚：

- 对两个箭头 $x \xrightarrow{g} y$ 和 $y \xrightarrow{h} z$，根据 $hgx = z$ 可定义它们的复合是 $x \xrightarrow{hg} z$. 根据群满足结合律可验证这里的复合满足结合律.
- 单位元 e 诱导出单位态射 $x \xrightarrow{e} x$.
- 每个态射都是同构，是因为每个 $x \xrightarrow{g} y$ 有逆 $y \xrightarrow{g^{-1}} x$,

个人认为，这里最后一条性质虽然没有直接出现在群作用的定义里，但是它是群作用能发挥出很大作用的重要的性质.

对任意一个群胚，每点处的自同态就是自同构，因此每个 $\mathrm{Hom}(x)$ 都是群. 如果 x, y 在同一连通分支中，任意选定一个 $x \xrightarrow{g} y$ 就可给出

$$\mathrm{Hom}(x, y) = g\,\mathrm{Hom}(x), \quad \mathrm{Hom}(y) = g\,\mathrm{Hom}(x)g^{-1}.$$

如果另有一个 $x \xrightarrow{h} z$，那么 $\mathrm{Hom}(y, z) = h\,\mathrm{Hom}(x)g^{-1}$. 这是因为任何两个在同一连通分支中的对象都是同构的. 特别地，上述所有集合都具有相同的基数. 基于这些考虑，下面关于稳定化子和轨道的讨论就非常自然：

Definition 1.5.1 (稳定子群，轨道). *给定 G 在集合 X 上的作用. 对任意 $x \in X$，定义 x 的* ***稳定子群*** *为*

$$\mathrm{Stab}_G(x) = \{g \in G : gx = x\}.$$

定义 x 所在的**轨道**为

$$\mathrm{Orb}_G(x) := Gx = \{gx : g \in G\}.$$

记 $G\backslash X = \text{set of orbits} = \{Gx : x \in X\}$. 对右作用 G，以 X/G 记之.

Proposition 1.5.2. 关于稳定化子和轨道由如下的事实：

- $\mathrm{Stab}_G(x)$ 是 G 的子群.
- X 可以被写为一些轨道的无交并.
- 如果 $y = gx$，那么 $\mathrm{Stab}_G(y) = g \cdot \mathrm{Stab}_G(x) \cdot g^{-1}$.

Example 1.5.3. 关于轨道的各种性质和记号都让我们想起子群对应的陪集. 如果 X 是一个群，G 是 X 的子群，那么 G 在 X 上的左作用得到的轨道就是全体右陪集 Gx. 上面的命题就直接对应到陪集的无交并分拆，或者说陪集的无交并分拆是上述结论的一个推论.

我们之后会发现，上面几乎显然的事实会有非常好的理论用途，这就是因为群作用存在本身就不平凡，所以只要我能建构出一个好的群作用，它就能给我们很好的信息.（后面也是如此：我们研究群表示时，比如像 regular representation 这种表示存在本身就能带来好的性质.） 下面的**共轭作用**就是一例：

Definition 1.5.4 (共轭作用). 给定群 G，它通过**共轭作用**作用在自己身上：

$$\mathrm{Ad}_g : G \to G, \quad \mathrm{Ad}_g(x) = gxg^{-1}.$$

出于其重要性，我们值得给共轭作用下的轨道和稳定子下一个定义：

- 称 $a, b \in G$ 是**共轭**的如果它们落在共轭作用的同一个轨道内. 即存在 $g \in G$ 使得 $b = gag^{-1}$.
- 一个轨道被称为 G 的一个**共轭类**.（它绝非子群）.
- 元素 a 的稳定子群被称为关于它的**中心化子**，即所有满足 $ga = ag$ 的元素构成的子群.

Example 1.5.5.

- 当 G 是 Abel 群时，每个共轭类都是单元集.
- 如果我们在矩阵群 $G = \mathrm{GL}_n(\mathbb{C})$ 中考虑共轭类，我们发现在线性代数中的标准型理论就相当于在每个共轭类中选择一个好的代表元. 比如说有理标准型，Jordan 标准型. 全体有理标准型可以和全体共轭类一一对应.
- 考虑 S_n 的共轭类. 则只有两个置换是共轭的当且仅当拥有相同的**圈种类**. σ 的圈种类就是指把它写成循环圈的形式，然后看各种长度的圈分别出现多少个. 这等价于考虑 n 的一个拆分 $n = n_1 + n_2 + \cdots + n_r$, $n_i \in \mathbb{N}^*$，表示 σ 中恰有长为 $n_1, \ldots, n_r$ 的圈各一个.

Definition 1.5.6 (中心化子). 设 $H < G$ 是子群，$S \subset G$ 是 G 中一个子集. 定义

- S 在 G 中的**中心化子**就是全体和 S 中每个元素都交换的群元素，

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

- G 的**中心**是指和 G 中全体元素都交换的群元素.

$$Z(G) = \{g \in G : ghg^{-1} = h, \forall\, h \in G\}.$$

- H 在 G 中的**正规化子**是在共轭作用下把 H 映回 H 的群元素，

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

  特别地，H 是 G 中的正规子群当且仅当 $N_G(H) = G$.

其中，集合的中心化子是元素中心化子的推广，满足 $C_G(S) = \bigcap_{g\in S} C_G(g)$. 中心 $Z(G)$ 是 G 的正规子群，它是共轭作用诱导出的群同态 $G \to \mathrm{Aut}(G)$ 的核. 正规化子也可以看作某种意义上稳定子群的推广，它满足 $H < N_G(H)$.

我们回到关于 G-set 的讨论. 首先我们可以定义 G-set 之间的同态，即保 G 作用的群同态.

Definition 1.5.7 (G-等变映射). 设 X, Y 都是 G-set. 称 $\phi : X \to Y$ 是 **G-等变的**，如果

$$\phi(gx) = g\phi(x), \quad \forall\, g \in G, x \in X.$$

这就给出一个范畴 G-Set.

G-set 的本质情况是只有一个连通分支的情形，即群作用只有一个轨道. 我们也给它一个定义：

Definition 1.5.8 (可递作用). 设 G 作用在集合 X 上，称该作用是**传递的**，如果对任意 $x, y \in X$，存在 $g \in G$ 使得 $y = gx$.

Example 1.5.9. G 在自身上的左移作用就是传递的，但是共轭作用就不一定是传递的.

之前我们说在群胚中，每个同连通分支中的 $\mathrm{Hom}(x, y)$ 都是某个 $g\,\mathrm{Hom}(x)$. 它们合起来就给出了整个 G 在 x 处的作用，于是恰好每个 $\mathrm{Hom}(x) = \mathrm{Stab}(x)$ 的左陪集对应一个轨道中的元素.

Proposition 1.5.10. 如果 G 作用在 X 上，则对任意 $x \in X$，存在集合间的双射

$$G/\mathrm{Stab}_G(x) \cong \mathrm{Orb}_G(x).$$

Corollary 1.5.11. 设 G 作用在 X 上，$\{x_i\}$ 是在每个轨道 $\mathcal{O}_i$ 中选取一个代表元构成的集合. 则

$$X = \coprod_{\text{orbits}} \mathcal{O} \cong \coprod_i G/\mathrm{Stab}_G(x_i).$$

接下来令 G 有限，我们把上面的公式应用在共轭作用上，给出一些在群论中有用的计数等式.

Theorem 1.5.12 (Class Equation). 设 G 是有限群，考虑 G 在自身上的共轭作用. 则对每个元素 g，它所在的轨道就是包含 g 的共轭类，稳定化子就是它的中心化子. 所以

$$\#\{hgh^{-1} : h \in G\} = |G| \,/\, |C_G(g)| = [G : C_G(g)].$$

设 $g_1, \ldots, g_r$ 分别为 G 的每个共轭类的一个代表元，则

$$|G| = \sum_{i=1}^{r} [G : C_G(g_i)].$$

这个公式看上去只是一个平凡的推论，但是它其实能得到很多不平凡的结果. 比如说 $[G : C_G(g_i)] = 1$ 当且仅当 G 中每个元素都和 g_i 交换，这就是说 g_i 落在 G 的中心内. 另一方面，右侧的每一项都是 $|G|$ 的因数. 所以当 $\#G$ 是比较好的数时，上式能给出意想不到的效果.

Definition 1.5.13 (p-group). 对素数 p，称 G 是 p-群，如果 $|G| = p^n$ 对某个 n 成立.

接下来的结论非常神奇!

Proposition 1.5.14. 如果 G 是非平凡的 p-群，那么其中心是非平凡的.

Proof. 我们考察共轭作用给出的轨道，每个轨道长度都是 p^n 的因子，从而是 p 的方幂. $|Z(G)|$ 就是长为 1 的轨道的个数，而只要轨道长度不为 1，就必须是 p 的倍数. 因此根据类公式，

$$p^n = |Z(G)| + \text{一些 } p \text{ 的倍数}.$$

所以 $|Z(G)|$ 是 p 的倍数，结合 $e \in Z(G)$ 可知 $|Z(G)| \geq p$，因此 $Z(G)$ 非平凡.

Proposition 1.5.15. p^2 阶群必是 Abel 群.

Proof. 假设 G 满足 $|G| = p^2$ 并且 G 不交换，根据上题结论，$Z(G)$ 非平凡且非 G，所以只能 $|Z(G)| = p$. 任取 $g \notin Z(G)$，则 g 和 $Z(G)$ 中任何元素都是交换的，所以它们生成的子群 $\langle g, Z(G)\rangle$ 也是交换的. 但是它真包含 $Z(G)$，所以只能是 G 本身. 因此 G 是 Abel 群.

我们接下来再研究一下自同构群. 回忆 $\mathrm{Aut}(G)$ 是全体从 G 到自身的群同构构成的群. 我们通过共轭作用可得到一个从 G 到 $\mathrm{Aut}(G)$ 的群同态：

$$\mathrm{Ad} : G \to \mathrm{Aut}(G), \quad g \mapsto (\mathrm{Ad}_g : h \mapsto ghg^{-1}).$$

根据同态定理，$\mathrm{Ad}_g = \mathrm{id}$ 当且仅当 $g \in Z(G)$，所以有单同态 $G/Z(G) \hookrightarrow \mathrm{Aut}(G)$. 由于这样由 G 本身诱导出的自同构总存在，我们把 $\mathrm{Ad}(G)$ 称为 G 的内自同构群，记作 $\mathrm{Inn}(G)$. 可证明 $\mathrm{Inn}(G)$ 是 $\mathrm{Aut}(G)$ 的一个正规子群：

$$\sigma \mathrm{Ad}_g \sigma^{-1}(h) = \sigma\big(g\sigma^{-1}(h)g^{-1}\big) = \sigma(g)h\sigma(g)^{-1} = \mathrm{Ad}_{\sigma(g)}.$$

Example 1.5.16. 对矩阵群 $G = \mathrm{GL}_n(\mathbb{Q})$，它的中心为

$$\{A \in \mathrm{GL}_n(\mathbb{Q}) : AB = BA \text{ for all } B \in \mathrm{GL}_n(\mathbb{Q})\} = \{\lambda \cdot I_n : \lambda \in \mathbb{Q}^\times\}.$$

从而 $\mathrm{Inn}(G) \cong \mathrm{GL}_n(\mathbb{Q})/\mathbb{Q}^\times =: \mathrm{PGL}_n(\mathbb{Q})$. 有一个外自同构

$$\psi : A \mapsto {}^tA^{-1}.$$

这是因为转置作用和取逆作用同时是反变的. 从而我们可给出群作用

$$\mathrm{PGL}_n(\mathbb{Q}) \rtimes \{1, \psi\} \curvearrowright \mathrm{GL}_n(\mathbb{Q}).$$

Example 1.5.17. 作业中有一个有趣的例子：当 $n \neq 6$ 时 S_n 只有内自同构，见.

我们可以讨论在全体自同构下不变的子群，这被称为 G 的**特征子群**.

Definition 1.5.18 (特征子群 Characteristic Subgroup). *称 H 为 G 的特征子群，如果对任意 $\sigma \in \mathrm{Aut}(G)$ 均有 $\sigma(H) = H$. 特别地，特征子群一定是正规子群.*

Week 6:2025/10/16

1.6 Sylow 定理

回忆我们定义过如果一个群的阶为素数 p 的某个幂次，则称其为 p-群. 我们今天研究的对象就是有限群 G 中的 p-群.

Definition 1.6.1 (Sylow p-子群). *如果 G 的阶数为 $|G| = p^r m$，其中 $p \nmid m$. 则 G 的 p^r 阶子群被称为它的* **Sylow-p 子群**. *我们在本节中记*

$$\mathrm{Syl}_p(G) = \{G \text{ 的 Sylow } p\text{-子群}\}, \quad n_p = \left|\mathrm{Syl}_p(G)\right|.$$

下面的结果初见时是令人震惊的：

Theorem 1.6.2 (Sylow). *若 G 是有限群，$|G| = p^r m$，$p \nmid m$，$r > 0$.*

(1) (First Sylow Thm) Sylow p-子群存在.

(2) (Second Sylow Thm) 设 P, Q 是 G 的两个 p-群，其中 P 是 Sylow-p 群. 则存在 $g \in G$ 使得 $Q < gPg^{-1}$.

换句话说，所有 Sylow p-子群是两两共轭的，任意 p-子群都落在某个 Sylow p-子群中.

(3) (Third Sylow Thm) n_p 满足 $n_p \equiv 1 \pmod{p}$ 并且 $n_p \mid m$.

Corollary 1.6.3. G 的 Sylow 子群是正规子群当且仅当 $n_p = 1$，此时它也是唯一的正规子群.

Example 1.6.4. 设 $|G| = pq$，p, q 为素数，$p < q$. 我们分类所有 pq 阶群.

取 G_p, G_q 分别是 G 的 Sylow p-子群和 Sylow q-子群. 则 $G_p \cong \mathbb{Z}/p\mathbb{Z}$，$G_q \cong \mathbb{Z}/q\mathbb{Z}$. 根据第三 Sylow 定理，$n_q \mid p$ 并且 $n_q \equiv 1 \pmod{q}$，根据 $p < q$ 可知 $n_q = 1$，所以 G_q 是 G 的正规子群.

另一方面，$n_p \mid q$ 并且 $n_p \equiv 1 \pmod{p}$. 所以 $n_p = 1$ 或 q. 如果 $n_p = 1$，则 G_p 也是 G 的正规子群，由于 $|G_p \cap G_q| \mid \gcd(p, q) = 1$，所以 $G_p \cap G_q = \{1\}$，再根据 $|G| = pq$ 可知 $G = G_p \times G_q = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$.

如果 $n_p = q$，则我们要求 $p \mid q - 1$. 根据 $G_p < G$ 和 $G_q \lhd G$，$|G_p \cap G_q| = 1$ 可得 $G \cong G_p \ltimes_\varphi G_q$. 我们只需考虑对 $\varphi : G_p \to \mathrm{Aut}(G_q)$ 分类. 由于

$$G_p \cong \mathbb{Z}/p\mathbb{Z}, \quad \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/(q-1)\mathbb{Z};$$

根据 $p \mid q - 1$，$\mathrm{Aut}(G_q)$ 存在唯一一个元素个数为 p 的子群，记为 H. 所以 φ 要么是平凡的（从而 $G_p \ltimes_\varphi G_q \cong G_p \times G_q$），要么它给出群同构

$$\varphi_i : G_p \to H,\ a \mapsto b^i.$$

其中 a 为 G_p 的一个生成元，$H = \{1, b, \ldots, b^{p-1}\}$. $G_p \xrightarrow{\sim} H$. 这给出 $p - 1$ 种群同构，我们可以证明它们给出的群是两两同构的. 所以在同构的意义下有两种 pq 阶群.

Proof for First Sylow Theorem. 对 $|G|$ 归纳，$|G| = 1$ 时显然成立，我们只考虑 $p \mid |G|$ 的情形. 如果 $p \mid |Z(G)|$，则根据有限 Abel 群结构定理，$Z(G)$ 存在 Sylow p-子群，记为 W. 我们考虑商同态 $\varphi : G \to G/W$，由归纳假设 G/W 存在 Sylow p-子群 H，于是计算阶数可知 $\varphi^{-1}(H)$ 是 G 的 Sylow p-子群.

如果 $p \nmid |Z(G)|$，则根据共轭作用所得的类公式，

$$|G| = \sum_{\mathcal{O} \text{ orbits}} |\mathcal{O}| = |Z(G)| + \sum_{i=1}^{s} \frac{|G|}{|\mathrm{Stab}_G(x_i)|}.$$

其中 x_i 是每个长度不为 1 的轨道中的代表元. 由于 $p \nmid |Z(G)|$，因此存在 x_i 使得

$$p \nmid \frac{|G|}{|\mathrm{Stab}_G(x_i)|} \Rightarrow p^r \mid |\mathrm{Stab}_G(x_i)|.$$

又根据 $|\mathrm{Stab}_G(x_i)| < |G|$（否则轨道长为 1） 可知 $\mathrm{Stab}_G(x_i)$ 是 G 的真子群且其含 p 的幂次和 G 相同. 由归纳假设，$\mathrm{Stab}_G(x_i)$ 存在 Sylow p-子群 H，那么它也是 G 的 Sylow p-子群，证毕.

Proof for Second Sylow Theorem. 考虑 Q 在 G/P 上的左乘作用. 考虑该作用的类公式：

$$|G/P| = \sum_{g_iP} \mathrm{Orb}_Q(g_iP) = \sum_{g_iP} \frac{|Q|}{|\mathrm{Stab}_Q(g_iP)|}.$$

其中 $\{g_iP\}$ 是每个轨道中的一个生成元. 稳定子的具体意义是：

$$\begin{aligned}\mathrm{Stab}_Q(g_iP) &= \{q \in Q : qg_iP = g_iP\} = \{q \in Q : qg_i \in g_iP\} \\ &= \{q \in Q : q \in g_iPg_i^{-1}\} = Q \cap g_iPg_i^{-1}.\end{aligned}$$

由于 P 是 Sylow p-群，故 $p \nmid |G/P|$，所以存在某个 i 使得

$$p \nmid \frac{|Q|}{|\mathrm{Stab}_Q(g_iP)|}.$$

由于 Q 是 p-群，因此 RHS 是 p 的幂次，因此 RHS $= 1$，即 $\left|Q \cap g_iPg_i^{-1}\right| = |\mathrm{Stab}_Q(g_iP)| = |Q|$. 所以 $Q < g_iPg_i^{-1}$，证毕. ∎

Proof for Third Sylow Theorem. 由于我们要计算 $\left|\mathrm{Syl}_p(G)\right|$，其中是一些互相共轭的子群，因此考虑 G 在 $\mathrm{Syl}_p(G)$ 上的共轭作用.

根据第一 Sylow 定理 $\left|\mathrm{Syl}_p(G)\right| \neq 0$，取 P 为其 Sylow p-子群. 根据第二 Sylow 定理该作用是传递的. 所以

$$\left|\mathrm{Syl}_p(G)\right| = \frac{|G|}{|\mathrm{Stab}_G(P)|}.$$

又根据 $P < \mathrm{Stab}_G(P)$ 可知 $|P| \mid |\mathrm{Stab}_G(P)|$，所以 $n_p \mid p^rm/p^r = m$.

再考虑 P 在 $\mathrm{Syl}_p(G)$ 上的共轭作用. 考虑该作用给出的类公式：

$$|\mathrm{Syl}_P(G)| = \sum_{P_i} |\mathrm{Orb}_P(P_i)| = \sum_{P_i} \frac{|P_i|}{|\mathrm{Stab}_P(P_i)|}.$$

其中 $\{P_i\}$ 是每个轨道中的一个代表元. 由于 $|P|$ 是 p-群，因此

$$p \nmid \frac{|P_i|}{|\mathrm{Stab}_P(P_i)|} \Leftrightarrow \mathrm{Stab}_P(P_i) = P_i \Leftrightarrow P \subset N_G(P_i).$$

所以 P 和 P_i 都是 $N_G(P_i)$ 的 Sylow p-子群，而且 $P_i \lhd N_G(P_i)$. 于是根据第二 Sylow 定理，P_i 是 $N_G(P_i)$ 中唯一的 Sylow 子群. 所以只能 $P_i = P$. 因此恰有一个 i 使得 $p \nmid \frac{|P_i|}{|\mathrm{Stab}_P(P_i)|}$，所以 RHS 模 p 余 1，证毕. ∎

讲义上还有一种神秘的 First Sylow Theorem 的证明方法（我记得 Artin 好像就用了类似的方法？）：

Proof. 设 $|G| = p^rm$，$\mathcal{X}$ 为全体 G 中 p^k 元集构成的集合，则可定义 G 在 X 上的左作用. 设该作用所得轨道为 $\mathcal{O}_1, \ldots, \mathcal{O}_l$. 由于

$$|\mathcal{X}| \binom{n}{p^k},$$

故 $p^{r-k} \parallel |\mathcal{X}|$，因此存在某个 $\mathcal{O}$ 使得 $p^{r-k+1} \nmid |\mathcal{O}|$. 从而对某个 $A \in \mathcal{O}$，

$$p^k \mid \frac{|G|}{|\mathcal{O}|} = |\mathrm{Stab}A|.$$

另一方面，由于 $|A| = p^k$，则对每个 $g \in \mathrm{Stab}(A)$，ga 给出 A 中不同的元素，于是 $|\mathrm{Stab}A| \leq p^k$. 因此 $\mathrm{Stab}A$ 是 G 的 p^k 阶子群，特别地 Sylow p-子群存在，证毕.

关于 Sylow 定理的应用，其实作业里会给出更多，这里就不再多说了.

Week 7:2025/10/20

1.7 交换子和幂零群

Definition 1.7.1 (交换子和导出子群). 设 G 是群，对任意 $x, y \in G$ 定义它们的**交换子**为 $[x, y] = xyx^{-1}y^{-1} \in G$.（它用来衡量 x, y 是否交换，如果交换那么取值为 1.）

对 $H_1, H_2 < G$，定义 $[H_1, H_2]$ 为由全体 $\{[x_1, x_2] : x_1 \in H_1,\ x_2 \in H_2\}$ **生成**的子群.

特别地，当 $H_1 = H_2 = G$ 时定义 G 的**导出子群**或者**交换子群**为

$$G^{\mathrm{der}} = G' = [G, G].$$

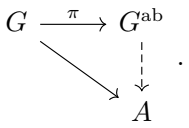
还是注意 G^{der} 是由全体 $[x, y]$ **生成**的子群.

Proposition 1.7.2. G^{der} 是 G 的正规子群. G/G^{der} 是 Abel 群，称为 G 的**交换化** G^{ab}.

Proof. 这是因为对任意 $g \in G$ 和 $[a, b]$ 均有 $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}] \in G^{\mathrm{der}}$.

另一方面，$abG^{\mathrm{der}} = baG^{\mathrm{der}} \Leftrightarrow [a, b] \in G^{\mathrm{der}}$，所以二者相等.

Proposition 1.7.3 (交换化的泛性质). 对任意从 $G \in \mathsf{Grp}$ 到 $A \in \mathsf{Ab}$ 的群同态，存在唯一的 Abel 群同态 $G^{\mathrm{ab}} \to A$ 使得



Proof. 给定任意群同态 $\varphi : G \to A$，都有 $\varphi([a, b]) = \varphi(a)\varphi(b)\varphi^{-1}(a)\varphi^{-1}(b) = 1$，从而每个 $[a, b] \in \ker\phi$，故 $G^{\mathrm{ab}} \subset \ker\phi$. 然后利用 kernel 的泛性质即可.

Example 1.7.4. 考虑 $\mathrm{Hom}_{\mathsf{Grp}}(D_{2n}, \mathbb{C}^\times)$. 则由于 $\mathbb{C}^\times$ 是交换群，我们只需考虑 $\mathrm{Hom}_{\mathsf{Ab}}(D_{2n}^{\mathrm{ab}}, \mathbb{C}^\times)$. 根据生成元关系，$srs = r^{-1} \Rightarrow srsr^{-1} = r^{-2}$，因此 $r^2 \in G^{\mathrm{der}}$. 这导致 $\langle r^2 \rangle < G^{\mathrm{der}}$.

若 n 为奇数，则 $\langle r \rangle < G^{\mathrm{der}}$，由此我们可以验证 $G^{\mathrm{der}} = \langle r \rangle$ 并且 $G^{\mathrm{ab}} \cong \{\pm 1\}$. 若 n 为偶数，则 $\langle r^2 \rangle < G^{\mathrm{der}}$，同样可以验证 $G^{\mathrm{der}} = \langle r^2 \rangle$ 并且 $G^{\mathrm{ab}} \cong \{\pm 1\} \times \{\pm 1\}$.

从而 $\mathrm{Hom}_{\mathsf{Grp}}(D_{2n}, \mathbb{C}^\times) \cong \mathbb{Z}/2\mathbb{Z}$ 或 $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Definition 1.7.5 (导出序列). 定义 $G^{(0)} = G$，对每个 $i \geq 0$ 定义 $G^{(i+1)} = [G^{(i)}, G^{(i)}]$. 我们称

$$G = G^{(0)} \rhd G^{(1)} \rhd G^{(2)} \rhd \dots$$

为 G 的导出序列.

Example 1.7.6. 我们考虑 $G = \begin{pmatrix} \mathbb{C}^\times & \mathbb{C} & \mathbb{C} \\ 0 & \mathbb{C}^\times & \mathbb{C} \\ 0 & 0 & \mathbb{C}^\times \end{pmatrix}$，它的导出序列为

$$G^{(1)} = \begin{pmatrix} 1 & \mathbb{C} & \mathbb{C} \\ 0 & 1 & \mathbb{C} \\ 0 & 0 & 1 \end{pmatrix}, G^{(2)} = \begin{pmatrix} 1 & 0 & \mathbb{C} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, G^{(3)} = \{I\}.$$

这和之前例子中取 G 的一个合成列证明其可解是一样的. 事实上可证明这两个命题的等价性.

Proposition 1.7.7. G 可解当且仅当 $G^{(n)} = \{1\}$ 对某个 $n \geq 1$ 成立. 称使得 $G^{(n)} = \{1\}$ 成立的最小的 n 为 G 的**可解长度**.

Proof. $\Leftarrow$ 方向显然. 考虑 $\Rightarrow$ 方向，如果由合成列

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_r = \{1\}$$

使得每个 H_i/H_{i+1} 均交换. 根据泛性质，$G^{(1)} < H_1$. 又因为

$$[H_1, H_1] < H_2,\ G^{(1)} < H_1 \Rightarrow G^{(2)} = [G^{(1)}, G^{(1)}] < [H_1, H_1] < H_2.$$

这样下去会得到 $G^{(i)} < H_i$ 总成立，所以 $G^{(r)} = 1$，证毕. 

Remark. 实际上，这证明了导出列 $G^{(i)}$ 就是典范的“下降最快”可解列，因此验证一个群可解只需要对导出序列验证还不需要担心是否会有更好的下降列满足要求.

有了上面的结论后，可更容易证明下述可解群的性质.

Proposition 1.7.8. 可解群的子群和商群均可解.

Proof. 若 $H < G$，则 $H^{(i)} < G^{(i)}$，从而 G 的导出序列可下降到 $\{1\}$ 自动推出 H 的导出序列可下降到 $\{1\}$.

若 $\varphi : G \to G/N$，则 $(G/N)^{(i)} = \varphi(G^{(i)})$（注意这里真的是等号而非包含关系，商映射是保导出子群的），从而 G 的导出序列可下降到 $\{1\}$ 自动推出 G/N 的导出序列可下降到 $\{1\}$. 

Proposition 1.7.9. 所有 $G^{(i)}$ 都是 G 的特征子群. 特别地，所有 $G^{(i)}$ 都是 G 的正规子群.（不依靠于特征子群的传递性，后者的证明不容易看出.）

Proof. 只需证明 G^{der} 是 G 的特征子群，然后根据特征子群的特征子群是特征子群（注意正规子群没有类似的传递性）即可. 设有 G 的自同构 φ，则

$$\varphi([g,h]) = \varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi^{-1}(g)\varphi^{-1}(h) = [\varphi(g),\varphi(h)].$$

因此根据 φ 的同构性 $\varphi(G^{\mathrm{der}}) = G^{\mathrm{der}}$. 证毕. 

接下来我们考虑的这一类群，它介于可解群和 Abel 群之间（强于可解性，弱于 Abel 性）.

Definition 1.7.10 (中心列，幂零群 Nilpotent Group). *若群 G 的正规列 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_m = \{1\}$ 满足*

$$G_i \lhd G, \quad G_i/G_{i+1} < Z_{G/G_{i+1}}$$

*对每个 i 成立，则称该序列为 G 的**中心列**. 如果 G 存在中心列，称其为**幂零群**.*

中心列满足的条件等价于

$$[g, g_i] \in G_{i+1}, \quad \forall\, g \in G,\, g_i \in G_i.$$

因此如果 G 是幂零群，那么算子 $[g,\cdot]$ 的某个幂为平凡同态. 对比 Abel 群满足每个 $[g,\cdot]$ 都是平凡同态，这解释了“幂零”的来源.

与可解群类似，幂零群有更典范的判定方法，而且有互为对偶的两个序列.

Definition 1.7.11 (下中心序列). *对群 G 定义下述正规列*

$$G^0 = G,\, G^1 = [G,G], \ldots,\, G^{i+1} = [G, G^i] (i \geq 1).$$

*将 $G = G^0 > G^1 > \ldots$ 称为 G 的**下中心序列**.*

Definition 1.7.12 (上中心序列). *对群 G 定义 $Z_0(G) = \{1\}$，$Z_1(G) = Z(G)$. 对 $i \geq 1$ 定义 $Z_{i+1}(G)$ 是 $G/Z_i(G)$ 的中心在 $\pi_i : G \twoheadrightarrow G/Z_i(G)$ 下的原像*

$$Z_{i+1}(G) = \pi_i^{-1}(Z(G/Z_i(G))).$$

*称 $\{1\} = Z_0(G) < Z_1(G) < Z_2(G) < \ldots$ 为 G 的**上中心序列**.*

Proposition 1.7.13. *G 幂零当且仅当 G 的下中心序列下降到 0.*

Proof. 我们先来证明下中心序列是中心列. 归纳证明 G^i 是 G 的特征子群，当 $i = 0$ 时显然，假设 i 时成立，$i+1$ 时 G 的任意自同构 σ 是保 G^i 的，从而对任意 $[a,b] \in [G,G^i]$，

$$\sigma[a,b] = [\sigma(a),\sigma(b)] \in [G,G^i].$$

从而 σ 保 G^{i+1} 的所有生成元，因此保 G^{i+1} 本身. 特别地有 $G^i \lhd G$. 此时对 $a \in G$，$b \in G^i$ 有 $aba^{-1} \in G^i$，从而 $[a,b] \in G^i$，故 $G^{i+1} < G^i$，再根据 $G^{i+1} \lhd G$ 可得 $G^{i+1} \lhd G^i$. 最后中心列额外满足的条件等价于 $[G,G_i] \subset G_{i+1}$，这即是此处的定义.

另一方面，如果存在一个中心列 $G = G[0] \rhd G[1] \rhd \cdots \rhd G[m] = \{1\}$，则根据性质 $[G, G[i]] \subset G[i+1]$ 可归纳证明 $G^i < G[i]$.

$$G^i < G[i] \Rightarrow G^{i+1} = [G, G^i] \subset [G, G[i]] \subset G[i+1].$$

故两命题等价.

Proposition 1.7.14. *G 幂零可推出 G 可解.*

Proof. 直接利用中心列性质可知 G_i/G_{i+1} 均交换，或者可归纳证明 $G^{(i)} < G^i$.

$$G^{(i)} < G^i \Rightarrow G^{(i+1)} = [G^{(i)}, G^{(i)}] \subset [G, G^i] = G^{i+1}.$$

从而 $G^{(i)}$ 是比 G^i 下降更快的序列.

Proposition 1.7.15. *G 幂零推出 G 的子群和商群均幂零.*

Proof. 证明和可解时完全类似.（ref 1.7.8）

接下来证明上中心列和下中心列两种建构是对偶的.

Proposition 1.7.16. *G 幂零当且仅当 G 的上中心序列上升到 G. 具体而言，$G^c = \{1\}$ 当且仅当 $Z_c(G) = G$，并且有 $G^{c-i} < Z_i(G)$ 对任意 i 成立.*

Proof. 我们重新观察 $Z_{i+1}(G)$ 的定义：

$$\begin{aligned} Z_{i+1}(G) &= \{g \in G : gZ_i(G) \in Z(G/Z_i(G))\} \\ &= \{g \in G : \forall\, h \in G,\, ghZ_i(G) = hgZ_i(G)\} \\ &= \{g \in G : [g, G] \subset Z_i(G)\}. \end{aligned}$$

如果 $G^c = \{1\} = Z_0(G)$，那么 $[G, G^{c-1}] = G^c = Z_0(G)$，从而 $G^{c-1} \subset Z_1(G)$. 因此归纳易得：

$$G^{c-i} < Z_i(G) \Rightarrow [G, G^{c-i-1}] = G^{c-i} < Z_i(G) \Rightarrow G^{c-i-1} < Z_{i+1}(G).$$

特别地，令 $i = c$ 推出 $Z_c(G) = G$. 反之，如果 $Z_c(G) = G = G^0$，那么 $[Z_c(G), G] \subset Z_{c-1}(G)$ 推出 $G^1 = [G, G^0] \subset Z_{c-1}(G)$. 同样地归纳可以反推

$$G^i < Z_{c-i}(G) \Rightarrow G^{i+1} = [G^i, G] \subset [Z_{c-i}(G), G] \subset Z_{c-i-1}(G).$$

特别地，令 $i = c$ 推出 $G^c = Z_0(G) = \{1\}$. 从而两个序列的存在性是等价的.

诚然考虑“中心”要比考虑“交换子群”来的容易分析不少，比如我们立马就可以得到如下的：

Proposition 1.7.17. *p-群都是幂零群.*

Proof. 当 G 平凡时显然. 对任意非平凡 p-群 G，均有 $Z(G) \neq \{1\}$（ref 1.5.14）. 从而只要 $Z_i(G) \neq G$，则 $G/Z_i(G)$ 也是非平凡 p 群，故 $Z(G/Z_i(G))$ 非平凡. 因此 $Z_i(G) \lneq Z_{i+1}(G)$，所以上中心列一定会上升到 G. 

我们为证明幂零群的结构定理做一些准备.

Proposition 1.7.18. *设 P 是一个非平凡 p-群，则*

(1) $Z(P) \neq \{1\}$.

(2) *如果 H 是 P 的非平凡正规子群，则 $H \cap Z(P) \neq \{1\}$.*

(3) *如果 H 是 P 的真子群，则 H 是 $N_P(H)$ 的真子群.*

Proof. (1) 已经在 1.5.14 中证明.

(2) 这只不过是更精细地考虑 (1) 的证明. 考虑 P 在 H 上的共轭作用. 由于 P 的 p-群，因此每个轨道长度都是 p 的幂次，并且轨道长度之和 $|H|$ 是 p 的倍数. 由于至少有 1 个长为 1 的轨道，故至少有 p 个长为 1 的轨道. 而若 a 位于长为 1 的轨道中，则 $a \in H \cap Z(P)$. 因此 $|H \cap Z(P)| \geq p > 1$，证毕.

(3) 我们只利用 (1) 就可完成证明. 对 $|P|$ 归纳.

- 若 $Z(P) \not\leq H$，则根据 $Z(P) < N_P(H)$ 可知 $H \neq N_P(H)$，从而 H 是 $N_P(H)$ 的真子群.
- 若 $Z(P) < H$，考虑商映射 $\phi : P \to P/Z(P)$，则根据归纳假设 $N_{P/Z(P)}(\phi(H)) \neq \phi(H)$. 由于 $N_P(H) = \phi^{-1}\big(N_{P/Z(P)}(\phi(H))\big)$，故这导致 $N_P(H) \neq H$，证毕. 

Corollary 1.7.19. *若 P 是 p-群，$H < P$ 是 P 的 index p 子群，则 H 是 P 的正规子群.*（更一般的结论在作业 29 中出现过.）

我们接下来证明下述神奇的结论：有限幂零群一定是一些 p-群的直积.

Theorem 1.7.20. *设有限群 G 满足 $|G| = n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$，任取 $P_i \in \mathrm{Syl}_{p_i}(G)$. 则下述叙述等价：*

(1) *G 幂零；*

(2) *对任意 $H \lneq G$ 均有 $H \lneq N_G(H)$.*

(3) *所有 Sylow p-子群 P_i 是正规子群.*

(4) $G \cong P_1 \times \cdots \times P_r$.

Proof. (1)⇒(2)：我们在 1.7.18 (3) 中对 p-群证明这条性质，只用到了 P 含有非平凡中心和 P 的商群还是 p-群（从而可进行归纳）这两条性质. 现在对幂零群来说，这

两条性质仍然成立. 幂零群的上中心序列上升到 G 保证了 $Z(G)$ 一定非平凡；命题 1.7.15 中已经证明了幂零群的商群也是幂零群. 所以我们完全可以照搬上面的证明.

(2)⇒(3)：我们证明对所有 Sylow p-子群 P_i 均有 $N_G(N_G(P_i)) = N_G(P_i)$.（实际上该证明过程在第三 Sylow 定理的证明中是出现过的.） 由于 $P_i \lhd N(P_i) < G$，故 P_i 是 $N(P_i)$ 的 Sylow p-子群，并且是 $N(P_i)$ 中唯一的 Sylow p-子群（根据第二 Sylow 定理）. 因此如果 $g \in G$ 满足 $gN_G(P_i)g^{-1} = N_G(P_i)$，那么 gP_ig^{-1} 仍然是 $N_G(P_i)$ 中的 Sylow p-子群，从而 $gP_ig^{-1} = P_i \Rightarrow g \in N_G(P_i)$. 现在利用 (2) 可知 $N_G(P_i) = G$，从而 P_i 是 G 的正规子群.

(3)⇒(4)：这是因为任两个 Sylow p-子群的交均平凡，所以任两个 P_i, P_j 之间均交换，从而直积 $P_1 \times \cdots \times P_r$ 可嵌入在 G 中. 对比元素个数就可知相等关系.

(4)⇒(1)：这是因为每个 P_i 都是幂零的，于是它们的直积也幂零. 比如说根据 $Z(\prod P_i) = \prod Z(P_i)$，可归纳证明 $Z_k(\prod P_i) = \prod Z_k(P_i)$，所以 $Z_k(P_i)$ 都上升到 P_i 可推出 $Z_k(\prod P_i)$ 上升到 $\prod P_i$.

2 Appendix A: Homeworks

2.1 第一次作业

T/F problems

TFTFF

FTFFF

FFTTF

Standard Problems

Problem 1: P1.3.2

设 $n, m \in \mathbb{N}_{\geq 2}$. 确定所有群同态 $\phi : \mathbb{Z}/n\mathbb{Z} \to D_{2m}$.

Sol. 我们考虑 D^{2m} 中元素的阶. D^{2m} 中有 m 个反射，每个反射的阶都是 2. 剩下 m 个旋转构成一个同构于 $\mathbb{Z}/m\mathbb{Z}$ 的子群，设为 $\langle\rho\rangle$. 那么 ρ^k 的阶就是 $m/\gcd(k,m)$.

一个同态 $\phi : \mathbb{Z}/n\mathbb{Z} \to D_{2m}$ 完全由 $\phi(\overline{1})$ 确定，并且要求 $\phi(\overline{1})^n = \mathrm{id}$，即 $\operatorname{ord}\phi(\overline{1}) \mid n$. 根据上面的讨论：

- 如果 $2 \mid n$ 那么对任意反射 r 存在一个 ϕ 使得 $\phi(\overline{1}) = r$.
- 对所有 ρ^k 使得 $\frac{n}{\gcd(m,n)} \mid k$，存在一个 ϕ 使得 $\phi(\overline{1}) = \rho^k$.

Problem 2: P1.3.3

证明 S_n 可由 $(1\ 2)$ 和 $(1\ 2\ \dots\ n)$ 生成.

Proof. 我们先证明 S_n 可由相邻对换 $(i\ i+1)$ 生成，$n = 1$ 时显然，假设 $n \geq 2$. 只需要证明对任意 $\sigma \in S_n$ 可以右复合上一些对换得到 id. 设当前面临的状态为 $\sigma_m = \sigma\tau_1 \dots \tau_{m-1}\tau_m$，我们来定义 τ_{m+1}.

- 如果对任意 i 均有 $\sigma_m(i) < \sigma_m(i+1)$，那么 $\{\sigma_m(i)\}_{1\leq i\leq n}$ 是递增列，从而已经是 id，无需再选择 τ_{m+1}.
- 若不然，存在 i 使得 $\sigma_m(i) > \sigma_m(i+1)$，右复合上一个 $\tau_{m+1} = (i\ i+1)$，得到的新的 σ_{m+1} 的逆序数 $\#\{(i,j) : i < j, \sigma(i) > \sigma(j)\}$ 严格减少. 所以有限次后会回到上一种情形.

经过上述算法就证明了存在 $\tau_1, \dots, \tau_m$ 使得 $\sigma = \tau_m\tau_{m-1}\dots\tau_1$，证毕.

再证明 $(i\ i+1)$ 可以被 $a = (1\ 2)$ 和 $b = (1\ 2\ \dots\ n)$ 生成. 当 $n = 1, 2$ 时显然，当 $n \geq 3$ 时，注意到 $b^i(1) = i+1$ 而 $b^i(2) = i+2$，所以 $b^{i-1}ab^{-i+1} = (b^{i-1}(1)\ b^{i-1}(2)) = (i\ i+1)$. 这就证明了 a 和 b 可生成 S_n.

Problem 3: P1.3.5

证明 D_8 和 Q_8 是不同构的. 其中 Q_8 指四元数群 $\{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$.

Proof. D_8 有四个阶为 2 的元素，但是 Q_8 只有 -1 是阶为 2 的元素. 

Problem 4: P1.3.7

设 G 是群. 定义 G^{op} 和 G^{op} 上的运算 $\star$ 满足作为集合 G^{op} 和 G 相同，运算满足 $a \star b = ba$.

(1) 证明 $(G^{\mathrm{op}}, \star)$ 是一个群.

(2) 证明 G 和 G^{op} 同构.

Proof. (1) 验证群公理：1 仍然是 G^{op} 的单位元，a^{-1} 仍然是 a 在 G^{op} 中的逆元，结合律由

$$(a \star b) \star c = (ba) \star c = c(ba) = (cb)a = (b \star c)a = a \star (b \star c).$$

(2) 考虑映射 $\varphi : G \to G^{\mathrm{op}}$，$g \mapsto g^{-1}$. 它在集合层面上是一个对合，从而是双射. 验证群同态：

$$\varphi(g) \star \varphi(h) = g^{-1} \star h^{-1} = h^{-1}g^{-1} = (gh)^{-1} = \varphi(gh).$$

证毕. 

Problem 5: P1.3.10

设 N 是 G 的有限子群. 证明对元素 $g \in G$，$gNg^{-1} \subset N$ 当且仅当 $gNg^{-1} = N$. 能否举例说明这对无穷子群 N 是错误的?

Proof. 当 $|N| < +\infty$ 时命题显然，因为 $|gNg^{-1}| = |N|$，所以 $gNg^{-1} \subset N$ 可推出 $gNg^{-1} = N$.

当 $|N| = +\infty$ 时，考虑

$$G = \{f : \mathbb{Z} \to \mathbb{Z} \text{ 的双射}\}, \quad N = \{f \in G \mid f(x) = x, x \leq 0\}.$$

那么 N 是 G 的子群. 现在考虑 $g : [x \mapsto x + 1]$，则 $g \in G$. 但是对任意 $n \leq 1$ 和 $f \in N$ 均有

$$(gfg^{-1})(n) = gf(n-1) = g(n-1) = n.$$

从而 gfg^{-1} 需以所有 $n \leq 1$ 为不动点，所以 $gNg^{-1} \lneq N$. 这就给出了反例. 

Problem 6: P1.3.12

G 的任意指数为 2 的子群 H 都是正规子群.

Proof. 设 $G = H \sqcup H'$. 对 $g \in H$，有 $gH = H$，这推出 $gH' = H'$.（因为 gH' 一定是某个陪集）对 $g \in H'$，有 $gH = H'$，这推出 $gH' = H$.

考虑 $\varphi : G \to S_2$，$\varphi(g) = [f : (H, H') \mapsto (gH, gH')]$，这是一个群同态，并且 $\ker \varphi = H$. 所以 $H \lhd G$.

Problem 7: P1.3.13

设 H_1, H_2 是 G 的子群，N 是 G 的包含在 $H_1 \cap H_2$ 中的正规子群. 证明

$$(H_1/N) \cap (H_2/N) \cong (H_1 \cap H_2)/N.$$

Proof. 我们先证明：如果 $h_1 \in H_1$ 和 $h_2 \in H_2$ 满足 $h_1 N = h_2 N$，那么 $h_1, h_2 \in H_1 \cap H_2$. 注意到 $N \subset H_1 \cap H_2$，于是

$$h_1 \in H_1 \cap H_2 \Leftrightarrow h_1 N \subset H_1 \cap H_2 \Leftrightarrow h_2 N \subset H_1 \cap H_2 \Leftrightarrow h_2 \in H_1 \cap H_2.$$

这里的 $\subset$ 都是把 $h_i N$ 看作一个集合而言. 从而

$$\begin{array}{ccc} h_1 \notin H_1 \cap H_2 & \Longleftrightarrow & h_2 \notin H_1 \cap H_2 \\ \Updownarrow & & \Updownarrow \\ h_1 N \subset H_1 \setminus (H_1 \cap H_2) & & h_2 N \subset H_2 \setminus (H_1 \cap H_2) \end{array}$$

第二行的两个事件不能同时发生，所以整个图表中的事件都不可能同时发生，从而 $h_1, h_2 \in H_1 \cap H_2$.

回到原题，两侧都可以通过单同态嵌入为 G/N 的子群，我们下面就典范地认为它们是 G/N 的子群. 因此只需证明集合上的等同关系. $(H_1 \cap H_2)/N \subset (H_1/N) \cap (H_2/N)$ 是显然的. 至于 $\supset$ 方向，设某个 $(H_1/N) \cap (H_2/N)$ 中元素在 H_1/N 中表示为 $h_1 N$，在 H_2/N 中被表示为 $h_2 N$. 所以根据上面的论述 $h_1 N = h_2 N \subset (H_1 \cap H_2)/N$. 这就证明了群同构成立.

Problem 8: P1.3.15

设 H, K, N 为 G 的子群，满足

$$H < K, \quad H \cap N = K \cap N, \quad HN = KN.$$

证明 $H = K$.

Proof. 对 $k_1, k_2 \in K$，

$$k_1 N = k_2 N \Leftrightarrow k_1 k_2^{-1} \in N \Leftrightarrow k_1 k_2^{-1} \in K \cap N \Leftrightarrow k_1 (K \cap N) = k_2 (K \cap N).$$

假设存在 $a \in K \setminus H$，则对任意 $h \in H < K$ 均有 $a(K \cap N) \neq h(K \cap N)$，否则根据 $K \cap N = H \cap N$ 可推出 $a \in H$，矛盾.

于是 $aN \neq hN$. 所以作为集合而言，

$$aN \cap \bigcup_{h\in H} hN = \varnothing \Rightarrow \bigcup_{k\in K} kN \neq \bigcup_{h\in H} hN.$$

这与 $KN = HN$ 矛盾！从而 a 不存在，即 $H = K$.

Problem 9: P1.3.18

(1) 设 G 是有限 Abel 群，其中元素为 $a_1, a_2, \ldots, a_n$. 我们在此题中采用乘法记号. 证明 $a_1a_2\ldots a_n$ 这个元素的平方是单位元.

(2) 如果 G 不存在阶为 2 的元素或者多于 1 个阶为 2 的元素，证明 $a_1a_2\ldots a_n = e$.

(3) 如果 G 恰有一个阶为 2 的元素 y，证明 $a_1a_2\ldots a_n = y$.

(4) (Wilson's Theorem) 如果 p 是素数，证明 $(p-1)! \equiv -1 \pmod p$.

Proof. (1) 考虑 $\sigma : \{1,\ldots,n\} \to \{1,\ldots,n\}$，$i$ 被打到 $\sigma(i)$ 使得 $a_{\sigma(i)}$ 是 a_i 的逆元. 则 $\sigma^2 = \mathrm{id}$，所以 σ 是一个置换. 因此

$$(a_1a_2\ldots a_n)^2 = \prod_{i=1}^{n}(a_ia_{\sigma(i)}) = \prod_{i=1}^{n} e = e.$$

(2) 如果 G 不存在阶为 2 的元素，那么上述置换 σ 就不存在不动点. 也就是 σ 给出了 G 中元素的一个配对，每一对的两个数乘积都是 e. 从而 $a_1a_2\ldots a_n = e$.

如果 G 存在大于一个阶为 2 的元素，根据上面的讨论，我们得到

$$\prod_{i=1}^{n} a_i = \prod_{i:\sigma(i)=i} a_i = \prod_{a_i^2=e} a_i.$$

$H = \{a \in G : a^2 = e\}$ 构成 G 的一个子群. 条件告诉我们有至少两个元素 a, b 阶为 2，再加上 $e \in H$ 得到 $|H| > 2$. 考虑 $\langle a, b\rangle$，根据 G 是交换群和 $a^2 = b^2 = e$ 立即得到

$$\langle a, b\rangle = \{e, a, b, ab\} < H.$$

所以 $4 \mid |H|$. 最后我们考虑 H 关于 $\langle a\rangle$ 的陪集分拆，每个陪集中有 $\{h, ha\}$ 两个元素，这两个元素之积为 a. 从而

$$\prod_{a_i^2=e} a_i = a^{[H:\langle a\rangle]} = a^{|H|/2} = e.$$

这由 $4 \mid |H|$ 保证.

(3) 当 G 恰有一个阶为 2 的元素时，$H = \{1, y\}$. 故

$$\prod_{i=1}^{n} a_i = 1 \cdot y = y.$$

(4) 考虑乘法群 $(\mathbb{Z}/p\mathbb{Z})^\times$. 它是一个有限交换群，我们只需证明 $(\mathbb{Z}/p\mathbb{Z})^\times$ 恰含有一个阶为 2 的元素 $\overline{-1}$. 这是因为 $\overline{x}$ 阶为 2 等价于

$$p \mid x^2 - 1, \quad p \nmid x - 1 \Rightarrow p \mid x + 1.$$

所以能且只能 $\overline{x} = \overline{-1}$. 这可推出

$$\overline{(p-1)!} = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} a = \overline{-1}.$$

证毕.

Problem 10: P1.3.19

设 G 是群，$A < G$，$N \lhd G$. 证明 AN 可解当且仅当 A 可解且 N 可解.

Proof. 我们先证明：可解群的子群可解. 给定 $A < G$ 以及合成列

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}.$$

我们证明

$$A = A_0 \rhd A \cap G_1 \rhd \cdots \rhd A \cap G_n = \{1\}$$

是 A 的合成列. 首先需证 $A \cap G_i \rhd A \cap G_{i+1}$. 对 $x \in A \cap G_{i+1}$ 和 $y \in A \cap G_i$，首先根据 $x \in G_{i+1}$ 和 $y \in G_i$ 推出 $yxy^{-1} \in G_{i+1}$，再根据 $x \in A$ 和 $y \in A$ 推出 $yxy^{-1} \in A$.

再证明 $(A \cap G_i)/(A \cap G_{i+1})$ 是 Abel 群. 考虑同态 $\varphi : A \cap G_i \hookrightarrow G_i \twoheadrightarrow G_i/G_{i+1}$. 那么 $\ker \varphi = A \cap G_i \cap G_{i+1} = A \cap G_{i+1}$，因此有单同态

$$(A \cap G_i)/(A \cap G_{i+1}) \to G_i/G_{i+1}.$$

由于 Abel 群的子群是 Abel 群，这推出 $(A \cap G_i)/(A \cap G_{i+1})$ 是 Abel 群. 从而上述的合成列是可解列，证毕!

回到原题，由于 $A, N < AN$，这立即推出 AN 可解 $\Rightarrow$ A 可解且 N 可解.

另一方面，如果 A 可解且 N 可解，我们写出 A 的可解列

$$A = A_0 \rhd A_1 \rhd \cdots \rhd A_n = \{1\}.$$

我们证明

$$AN = A_0N \rhd A_1N \rhd \cdots \rhd A_nN = N \rhd N_1 \rhd \cdots \rhd A_m = \{1\}$$

是 AN 的可解列. 后半段完全由 N 的可解性保证，前半段这样看：首先根据 $A_{i+1} \lhd A_i$ 以及 $N \lhd G$ 我们来证 $A_{i+1}N \lhd A_iN$. 取 $an \in A_iN$，则

$$an(A_{i+1}N)n^{-1}a^{-1} = aA_{i+1}Na^{-1} = aA_{i+1}a^{-1}N = A_{i+1}N.$$

这通过 $aN = Na$ 和 $aA_{i+1} = A_{i+1}a$ 得到. 再考虑 $A_iN/A_{i+1}N$. 考虑群同态

$$\psi : A_i \hookrightarrow A_iN \twoheadrightarrow A_iN/A_{i+1}N.$$

那么 $A_{i+1} \subset \ker\psi$. ψ 还是满同态，因为我们可以把 $A_iN/A_{i+1}N$ 利用同态定理写作

$$(A_i/A_i \cap N)\big/(A_{i+1}/(A_{i+1} \cap N))$$

那么

$$A_i \twoheadrightarrow A_i/(A_i \cap N) \twoheadrightarrow (A_i/A_i \cap N)\big/(A_{i+1}/(A_{i+1} \cap N))$$

就是满同态. 所以 $A_iN/A_{i+1}N$ 可被实现为 A_i/A_{i+1} 的商群，这是一个 Abel 群，因此这是一个可解列，证毕.

More Challenging Problems

Problem 11: P1.4.8 Yau 2011

考虑群

$$\mathrm{SL}_2(\mathbb{Z}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid ad - bc = 1\}.$$

证明 $\mathrm{SL}_2(\mathbb{Z})$ 被 $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 和 $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ 生成.

Proof. 显然 $T, S \in \mathrm{SL}_2(\mathbb{Z})$，因此只需证明 $\mathrm{SL}_2(\mathbb{Z}) \subset \langle T, S\rangle$. 构建下述同态

$$\phi : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{Iso}(\mathbb{C} \cup \{\infty\}), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto [z \mapsto \frac{az + b}{cz + d}].$$

那么 $\ker\phi = \{\pm I\}$. 由于 $S^2 = -I$，因此只需证明 $\phi(SL_2(\mathbb{Z})) \subset \langle\phi(S), \phi(T)\rangle$.

$$\phi(T) = [z \mapsto z + 1], \quad \phi(S) = [z \mapsto -\frac{1}{z}].$$

现在给定任意的 $f \in \mathrm{im}\,\phi$，接下来我们把 f 左复合上一些 $\phi(T), \phi(S)$ 或者 $\phi(T)^{-1}$ 得到 id. 使用下述算法：

- 如果当前 $|c| > |a|$，就左复合一个 $\phi(S)$，复合后所得结果满足 $|a| \geq |c|$.
- 如果 $|c| \neq 0$，进行辗转相除：设 $|a| = q \cdot |c| + r$，$0 \leq r < |c|$，然后左复合上 $\phi(T)^q$ 或者 $\phi(T)^{-q}$，这样就把 $|a|$ 变成了 $|r|$.
- 这样操作下去 $\min\{|a|, |c|\}$ 会严格减，所以一定存在一个时刻使得 $|c| = 0$. 此时根据 $ad - bc = 1$ 可知 $ad = 1$，所以 $|a| = |d| = 1$，也就是此时的变换能写成 $z \mapsto z + bd$，这很明显可左复合上 $\phi(T)^{-bd}$ 使其变为 id.

进过上述算法我们得到：存在一列 $g_1, g_2, \ldots, g_m$，其中 $g_i \in \{\phi(T), \phi(S), \phi(T)^{-1}\}$ 使得

$$g_m \circ g_{m-1} \circ \cdots \circ g_1 \circ f = \mathrm{id}\,.$$

因此 $f \in \langle \phi(T), \phi(S) \rangle$. 根据 f 的任意性，$\mathrm{SL}_2(\mathbb{Z}) \subset \langle T, S \rangle$，证毕.

Problem 12: P1.4.9 Yau 2014

设 S 和 T 是非交换有限单群，$G = S \times T$.

(1) 证明 G 恰有 4 个正规子群.

(2) 证明如果 S 和 T 同构，那么存在 G 的以及极大真子群不包含任何一个直积分量（$\{1\} \times H$ 或者 $G \times \{1\}$）.

(3) 证明如果存在 G 的极大真子群不含任何一个 G 的直积分量，那么 S 和 T 同构.

Proof. 首先考虑 $Z(S)$，则有 $Z(S) \lhd S$. 由于 S 是有限非交换单群，故 $Z(S) = \{1\}$ 或 S. 但是 $Z(S) = S$ 推出 S 是交换群，所以 $Z(S) = 1$，即对任意 $s \in S$, $s \neq 1_S$ 都存在 $g \in S$ 使得 $gs \neq sg$. $(*)$

我们对固定的子群 $A < G$，考虑如下四个群：

$$A_S = \{s \in S : (s, 1) \in A\}, \quad A_T = \{t \in T : (1, t) \in A\}.$$

容易验证 $A_S \cong A \cap (S \times \{1\})$ 从而是群，A_T 同理. 以及对满同态 $\pi_S : S \times T \to S$, $(s, t) \mapsto s$ 和 $\pi_T : S \times T \to T$, $(s, t) \mapsto t$，考虑 $\pi_S(A)$ 和 $\pi_T(A)$ 两个群.

(1) 如果 $A \lhd G$，那么 $A_S, \pi_S(A) \lhd S$，$A_T, \pi_T(A) \lhd T$. 这些正规性直接根据 $(g, 1)(s, t)(g, 1)^{-1} = (gsg^{-1}, t)$ 得到.

从而由于 S, T 是单群，$A_S, \pi_S(A) = \{1\}$ 或 S，并且 $A_T, \pi_T(A) = \{1\}$ 或 T. 如果 $\pi_S(A) = S$，那么存在 $s \in S$, $s \neq 1$，使得存在 $t \in T$ 满足 $(s, t) \in A$. 根据性质 $(*)$，取 $g \in S$ 使得 $gs \neq sg$，那么

$$(g, 1)(s, t)(g, 1)^{-1}(s, t)^{-1} = (gsg^{-1}s^{-1}, 1) \in A.$$

而 $gsg^{-1}s^{-1} \neq 1$，所以 $A_S \neq \{1\}$，这推出 $A_S = S$. 同理，$\pi_T(A) = T$ 可推出 $A_T = T$. 接下来分类讨论：

- 如果 $\pi_S(A) = \{1_S\}$，$\pi_T(A) = \{1_T\}$，那么只能 $A = \{1_G\}$，此时是正规子群.
- 如果 $\pi_S(A) = S$，$\pi_T(A) = \{1_T\}$，那么前者推出 $S \times \{1_T\} < A$，后者推出 $A < S \times \{1_T\}$，所以 $A = S \times \{1_T\}$ 是正规子群.
- 如果 $\pi_S(A) = \{1_S\}$，$\pi_T(A) = T$，同理可知 $A = \{1_S\} \times T$ 是正规子群.

- 如果 $\pi_S(A) = S$ 且 $\pi_T(A) = T$，那么 $A_S = S$ 且 $A_T = T$. 这给出 $\{1_S\} \times T < A$ 以及 $S \times \{1_T\} < A$，这推出 $A = S \times T = G$.

综上，恰好有四个正规子群.

(2) 设一个 $S \to T$ 的同构为 φ. 取

$$H = \{(s, \varphi(s)) : s \in S\}.$$

φ 是群同态立即推出 H 是一个子群. 至于极大性，考虑满足 $H \lneq H' < G$ 的一个群. 首先证明 H'_S, H'_T 仍然是正规子群，因为对任意 $c \in H'_S$ 和 $t \in S$，

$$(t, \varphi(t)^{-1})(c, 1)(t^{-1}, \varphi(t^{-1})) = (tct^{-1}, 1) \in H' \Rightarrow tct^{-1} \in H'_S.$$

同理根据 φ 的满性可推得 $H'_T \lhd T$.

下假设存在 $(s, t) \in H'$ 使得 $t \neq \phi(s)$，那么

$$(s, t) \cdot (s, \varphi(s))^{-1} = (1, t\varphi(s)^{-1}) \in H'.$$

所以 $H'_T \neq \{1\}$，从而 $H'_T = T$，同理 $H'_S = S$. 这已经足以推出 $H' = G$，所以 H 的确是极大子群.

(3) 设这个群为 H. 首先证明 $\pi_S(H) = S$ 且 $\pi_T(H) = T$. 否则假设 $\pi_S(H) \lneq S$，那么 $H < \pi_S(H) \times T \lneq G$，这要么和 H 不包含 $\{1\} \times T$ 矛盾，要么和极大性矛盾，另一侧是同理的.

然后我们证明 $H_S \lhd S$ 以及 $H_T \lhd T$. 这是因为对任意 $s \in S$，存在 $t \in T$ 使得 $(s, t) \in H$，从而对任意 $c \in H_S$，都有

$$(s, t)(c, 1)(s, t)^{-1} = (scs^{-1}, 1) \in H \Rightarrow scs^{-1} \in H_S.$$

再说明对任意 $s \in S$，恰好有一个 $t \in T$ 使得 $(s, t) \in H$. 存在性已经由 $\pi_S(H) = S$ 保证. 假设存在两个不同元素 t, t' 使得 $(s, t), (s, t') \in H$，那么 $(1, t^{-1}t') \in H$，从而 $H_T \neq \{1_T\}$，所以 $H_T = T$，这推出 $\{1_S\} \times T < H$，矛盾!

所以可以建立一个映射 $\varphi : S \to T$，把 s 打到唯一的 t 使得 $(s, t) \in H$. 又因为对每个 t 同理也存在唯一的 s 使得 $(s, t) \in H$，所以 φ 在集合层面上是双射，只需要验证它是个群同态. 这是因为 $(s, \varphi(s)), (t, \varphi(t)) \in H$ 推出 $(st, \varphi(s)\varphi(t)) \in H$，根据定义就有 $\varphi(st) = \varphi(s)\varphi(t)$. 综上，$S \cong T$. 

Problem 13: P1.4.10 Yau 2017

设 G 是一个群，g 是 G 中的一个 n 阶元素. 设 $n = rs$，其中 $\gcd(r, s) = 1$.

(1) 证明存在一组 $(g_1, g_2) \in G \times G$ 使得 $g_1^r = g_2^s = 1$ 并且 $g_1 g_2 = g_2 g_1 = g$.

(2) 证明 (g_1, g_2) 是唯一的.

Proof. (1) 根据 Bezout 定理，存在 $a,b\in\mathbb{Z}$ 使得 $ar+bs=1$. 从而我们取 $g_1=g^{bs}$，$g_2=g^{ar}$. 那么

$$g_1^r=g^{brs}=g^{bn}=1,\quad g_2^s=g^{ars}=g^{an}=1.$$
$$g_1g_2=g_2g_1=g^{ar+bs}=g.$$

(2) 考虑 $g_1^{ar}g_2^{ar-1}$. 一方面，

$$g_1^{ar}g_2^{ar-1}=(g_1g_2)^{ar}g_2^{-1}=g^{ar}g_2^{-1},$$

另一方面 $g_1^{ar}g_2^{ar-1}=g_1^{ar}g_2^{-bs}=1$. 从而 $g_2=g^{ar}$. 类似的推理给出 $g_1=g^{bs}$，所以根据条件可以唯一决定出 (g_1,g_2).

Problem 14: P1.4.2 Jacobson page 53

设 H 是有限群 G 的子群. 证明存在 $z_1,\dots,z_n$ 同时可以作为左陪集 G/H 和右陪集 $H\backslash G$ 的代表元.

Proof. 记 $[G:H]=k$，将 k 个左陪集看作 k 个集合，标记为 $S_1,\dots,S_k$. k 个右陪集分别标记为 $T_1,\dots,T_k$. 则 $|S_i|=|T_j|=|H|$ 并且 $S_1,\dots,S_k$ 和 $T_1,\dots,T_k$ 作为集合分别构成集合 G 的两组分拆.

构建二部图 $G=(\mathscr{S},\mathscr{T},E)$，$\mathscr{S}=\{S_1,\dots,S_k\}$，$\mathscr{T}=\{T_1,\dots,T_k\}$，在 S_i 和 T_j 之间连一条边当且仅当 $S_i\cap T_j\neq\varnothing$. 对任意子集族 $\mathscr{A}\subset\mathscr{S}$，我们考虑

$$N(\mathscr{A})=\{T_j\in\mathscr{T}:\exists S_i\in\mathscr{A}\ \text{s.t.}\ S_i\sim T_j\}.$$

$S_i\sim T_j$ 表示 S_i,T_j 之间有边. 根据连边关系，如果 $T_j\notin N(\mathscr{A})$ 那么

$$T_j\cap\bigcup_{S_i\in\mathscr{A}}S_i=\varnothing\Rightarrow\left(\bigcup_{T_j\notin N(\mathscr{A})}T_j\right)\cap\left(\bigcup_{S_i\in\mathscr{A}}S_i\right)=\varnothing.$$

从而对元素计数可知：

$$\sum_{T_j\notin N(\mathscr{A})}|T_j|+\sum_{S_i\in\mathscr{A}}\leq|G|\Rightarrow(k-|N(\mathscr{A})|)\,|H|+|\mathscr{A}|\,|H|\leq|G|$$
$$\Rightarrow k-|N(\mathscr{A})|+|\mathscr{A}|\leq k\Rightarrow|\mathscr{A}|\leq|N(\mathscr{A})|\,.\qquad(*)$$

$(*)$ 使得我们可以运用 Hall 二部图匹配定理，得到图 G 存在完美匹配. 也就是存在一个置换 $\sigma\in\mathfrak{S}_k$ 使得 $S_i\cap T_{\sigma(i)}\neq\varnothing$，记其中一个元素为 z_i，那么根据分拆性可知 z_i 两两不同. 翻译成群论语言就是：$z_1,\dots,z_k$ 同时构成了左陪集和右陪集的一组代表元，证毕.

Remark. 还有另一种解法是使用双陪集：考察 $HgH=\{h_1gh_2\mid h_1,h_2\in H\}$，所有双陪集给出了 G 的一个拆分，我们看其中一个双陪集. 注意到

$$HgH=\bigcup_{i=1}^{s}x_igH=\bigcup_{j=1}^{t}Hgy_j\Rightarrow s=t.$$

取元素 $\{x_igy_i\mid i=1,2,\dots,s\}$ 就满足要求.

Problem 15: P1.4.4 H, page 29, page 30, page 37

(1) 给一个一行证明，说明 $(\mathbb{Z},+)$ 是 $(\mathbb{Q},+)$ 的一个正规子群.

(2) 设 p 是素数，定义 $Z(p^\infty)$ 是 $\mathbb{Q}/\mathbb{Z}$ 的子集：

$$Z(p^\infty)=\{\overline{a/b}\in\mathbb{Q}/\mathbb{Z}\mid a,b\in\mathbb{Z},\exists,\, i\geq 0 \text{ s.t. } b=p^i\}.$$

证明 $Z(p^\infty)$ 是 $\mathbb{Q}/\mathbb{Z}$ 的无穷子群.

(3) 证明 $Z(p^\infty)$ 中的每个元素有有限阶 p^n 对某个 $n\geq 0$ 成立.

(4) 证明 $H_n:=\{z\in Z(p^\infty)\mid p^n\cdot z=0\}$ 和 $\mathbb{Z}/p^n\mathbb{Z}$ 同构.

(5) 由此推断 $Z(p^\infty)=\bigcup_n H_n$.

(6) 证明 $Z(p^\infty)$ 是可除的，即对任意元素 $x\in Z(p^\infty)$ 和 $n\in\mathbb{N}$ 均存在 $y\in Z(p^\infty)$ 使得 $x=ny$.

Proof. (1) 利用 Abel 群的子群总是正规子群以及 $\mathbb{Z}<\mathbb{Q}$?

(2) 首先证明是群：

$$\left(\frac{a}{p^i}+\mathbb{Z}\right)+\left(\frac{b}{p^j}+\mathbb{Z}\right)=\frac{ap^{\max(i,j)-i}+bp^{\max(i,j)-j}}{p^{\max(i,j)}}+\mathbb{Z}.$$

然后证明无穷性：$\{1/p^i\}_{i\geq 0}$ 是群中两两不同的无穷个元素.

(3) 这是因为对元素 $\overline{a/p^i}\in Z(p^\infty)$，$p^i\cdot\overline{a/p^i}=\overline{a}=\overline{0}$.

(4) 建立映射 $\varphi:\mathbb{Z}\to Z(p^\infty)$，$\varphi(m)=m/p^n+\mathbb{Z}$. 那么 $\operatorname{im}\varphi\subset H_n$，而对 $z+\mathbb{Z}\in H_n$ 有 $p^n\cdot z\in\mathbb{Z}$，从而 $\varphi(p^n z)=z+\mathbb{Z}$，所以 $H_n=\operatorname{im}\varphi$.

另一方面，$\ker\varphi=\{m\in\mathbb{Z}:m/p^n\in\mathbb{Z}\}$，即 $p^n\mathbb{Z}$. 根据第一同构定理，$\mathbb{Z}/p^n\mathbb{Z}\cong H_n$.

(5) 在集合层面上，根据 (3) 可知对每个 $g\in Z(p^\infty)$ 存在 n 使得 $g\in H_n$，所以 $Z(p^\infty)\subset\bigcup_n H_n$. 反方向的包含关系显然成立.

(6) 设 $n=p^\alpha m$，其中 $\gcd(p,m)=1$. 设 $x=z/p^i+\mathbb{Z}$，则存在 $a\in\mathbb{Z}$ 使得 $m\mid x+ap^i$. 于是我们取

$$y=\left(\frac{x+ap^i}{m}\right)/p^{i+\alpha}+\mathbb{Z}.$$

则 $ny=x$，证毕. ∎

2.2 第二次作业

True/False Problems

FTTTF FTFFT TFFFT FTFFT

Standard Problems

Problem 16: P2.3.1

将 $C_{12} \times C_{12} / \langle (2,6) \rangle$ 写成循环群直积的形式.

Proof. 设该群为 G，则 $|G| = 144/6 = 24$，由于它是 Abel 群，所以它必有一个 C_3 分量，我们计算其 2 挠部分.

- 在 mod 12 的意义下，$2(a + 12\mathbb{Z}, b + 12\mathbb{Z}) = n(2 + 12\mathbb{Z}, 6 + 12\mathbb{Z})$ 当且仅当 $a+6\mathbb{Z} = n+6\mathbb{Z}$, $b+6\mathbb{Z} = 3n+6\mathbb{Z}$，所以只需 $b+6\mathbb{Z} = 3a+6\mathbb{Z}$，有 $2\times2\times6 = 24$ 个元素满足要求. 所以 $|G[2]| = 4$.
- 在 mod 12 的意义下，$4(a + 12\mathbb{Z}, b + 12\mathbb{Z}) = n(2 + 12\mathbb{Z}, 6 + 12\mathbb{Z})$ 当且仅当 $2a + 6\mathbb{Z} = n + 6\mathbb{Z}$, $2b + 6\mathbb{Z} = 3n + 6\mathbb{Z}$. 所以只需 $2b + 6\mathbb{Z} = 6\mathbb{Z}$，有 $4 \times 12 = 48$ 个元素满足要求. 所以 $|G[4]| = 8$.

因此 G 的分解中恰有一个 C_2 和一个 C_4. 故 $G = C_2 \times C_4 \times C_3$.

Problem 17: P2.3.3

设 G, H 是两个群，设有单同态 $i : H \to G$ 和 $\pi : G \to H$ 使得 $\pi \circ i = \mathrm{id}_H$. 证明 G 可被实现为某个 $H \ltimes \ker \pi$，使得 i 是到第一个分量的嵌入，π 是到第一个分量的投影.

Proof. $i(H)$ 是 G 的子群，$\ker \pi$ 是 G 的正规子群，则 G 中的共轭作用诱导出半直积结构 $i(H) \ltimes \ker \pi$. 根据 $\pi \circ i = \mathrm{id}_H$ 可知 $\ker \pi \cap i(H) = \{e\}$，所以 $i(H) \ltimes \ker \pi$ 和 G 中两子群相乘是同构的.

对任意 $g \in G$，$\pi \circ i(\pi(g)) = \pi(g)$，于是存在 $h \in \ker \pi$ 使得 $g = i(\pi(g)) \cdot h$，前者是 $i(H)$ 中的元素，因此 $i(H) \cdot \ker \pi = G$，所以 $i(H) \ltimes \ker \pi$ 到 G 有群同构.

由于 i 是单同态，因此从 H 到 $i(H)$ 有群同构，故有群同构 $H \ltimes \ker \pi \cong i(H) \ltimes \ker \pi \cong G$.

Remark. 本题说明了如果有正规子群 $N \lhd G$ 以及商映射的右逆 $G/N \hookrightarrow G$ （或者说从每个陪集中选取一个代表元使得它们构成群结构），那么 G 就能表示成半直积 $G/N \ltimes N$.

Problem 18: P2.3.5

对任何群 G，定义其对偶群 $\widehat{G}$ 为从 G 到 $\mathbb{C}$ 中全体单位元构成的乘法群的群同态构成的集合（这样的群同态被称为 G 的特征），并赋予群结构

$$(\chi\psi)(g)=\chi(g)\psi(g),\quad g\in G.$$

(1) 证明这一乘法结构把 $\widehat{G}$ 实现为了一个 Abel 群，并且指出其单位元和某个元素的逆.

(2) 证明如果 G,H 都是 Abel 群，那么 $\widehat{G\times H}\cong\widehat{G}\times\widehat{H}$.

(3) 具体计算群 $\widehat{\mathbb{Z}/n\mathbb{Z}}$.

(4) 如果 G 是有限 Abel 群，证明 $G\cong\widehat{G}$.

G 和 $\widehat{G}$ 之间不存在典范的群同构，上面选取的群同构依赖于一组生成元的选取.

Proof. (1) 首先验证 $\chi\phi$ 是一个群同态：

$$(\chi\psi)(gh)=\chi(gh)\psi(gh)=\chi(g)\chi(h)\psi(g)\psi(h)=(\chi\psi)(g)(\chi\psi)(h).$$

结合律和交换律都是逐点验证的：

$$\begin{aligned}((\chi_1\chi_2)\chi_3)(g)&=(\chi_1\chi_2)(g)\chi_3(g)=\chi_1(g)\chi_2(g)\chi_3(g)\\&=\chi_1(g)(\chi_2\chi_3)(g)=(\chi_1(\chi_2\chi_3))(g).\\(\chi_1\chi_2)(g)&=\chi_1(g)\chi_2(g)=\chi_2(g)\chi_1(g)=(\chi_2\chi_1)(g).\end{aligned}$$

单位元是把所有元素都送到 1 的平凡映射 χ_1. 定义 $\chi^{-1}(g):=\chi(g)^{-1}$，则 $\chi^{-1}(gh)=\chi(gh)^{-1}=\chi(g)^{-1}\chi(h)^{-1}=\chi^{-1}(g)\chi^{-1}(h)$，所以 $\chi^{-1}\in\widehat{G}$ 并且 χ^{-1} 为 χ 的逆元. 因此 $\widehat{G}$ 可实现为一个 Abel 群.

(2) 为每个 $\phi\in\widehat{G}$ 和 $\psi\in\widehat{H}$，定义 $f(\phi,\psi)$ 满足

$$f(\phi,\psi)(g,h)=\phi(g)\psi(h).$$

- 验证 $f(\phi,\psi)$ 是群同态：

$$\begin{aligned}f(\phi,\psi)(g_1g_2,h_1h_2)&=\phi(g_1g_2)\psi(h_1h_2)=\phi(g_1)\psi(h_1)\phi(g_2)\psi(h_2)\\&=f(\phi,\psi)(g_1,h_1)f(\phi,\psi)(g_2,h_2).\end{aligned}$$

- 验证 f 是群同态：

$$\begin{aligned}f(\phi_1\phi_2,\psi_1\psi_2)(g,h)&=(\phi_1\phi_2)(g)(\psi_1\psi_2)(h)=\phi_1(g)\psi_1(h)\phi_2(g)\psi_2(h)\\&=f(\phi_1,\psi_1)(g,h)f(\phi_2,\psi_2)(g,h).\end{aligned}$$

- 验证 f 是单射：已知 $f(\phi,\psi)(g,h)=1$ 对任意 $g\in G,\ h\in H$ 成立. 令 $h=1$ 得 $\phi(g)=1$ 恒成立，令 $g=1$ 得 $\psi(h)=1$ 恒成立，所以 ϕ,ψ 都是平凡特征标.
- 验证 f 是满射：对每个 $G\times H$ 的特征标 χ，考虑 $\phi(g)=\chi(g,1)$，$\psi(h)=\chi(1,h)$，则 ϕ,ψ 分别是 G,H 上的特征标，且

$$f(\phi,\psi)(g,h)=\phi(g)\psi(h)=\chi(g,1)\chi(1,h)=\chi(g,h).$$

于是 f 给出同构 $\widehat{G}\times\widehat{H}\to\widehat{G\times H}$.

(3) 考虑 $\mathbb{Z}/n\mathbb{Z}\to\mathbb{C}^\times$ 的群同态相当于选取 $1+n\mathbb{Z}$ 的合适的像，相当于选取 $\mathbb{C}^\times$ 的一个 n 阶元，相当于选取一个 n 次单位根 $e^{\frac{2\pi ik}{n}}$. 设本原单位根为 $\omega=e^{\frac{2\pi i}{n}}$，则 $\widehat{\mathbb{Z}/n\mathbb{Z}}$ 同构于全体 n 次单位根 $\{1,\omega,\dots,\omega^{n-1}\}$ 构成的乘法群，后者显然再次同构于 $\mathbb{Z}/n\mathbb{Z}$ 本身，于是 $\widehat{\mathbb{Z}/n\mathbb{Z}}\cong\mathbb{Z}/n\mathbb{Z}$.

(4) 任意有限 Abel 群可被写为有限个循环群的直积，因此 G 的对偶群同构于每个循环群的对偶群的直积. 而每个循环群的对偶群都同构于其自身，所以 G 的对偶群也同构于自身.

Problem 19: P2.3.6

设 I 是非空指标集，每个 $i\in I$ 对应一个群 G_i. 定义 $(G_i)_{i\in I}$ 的直和为 $\prod_{i\in I}G_i$ 中除有限项外均为单位元的元素构成的子群.

(1) 证明 $(G_i)_{i\in I}$ 的直和是直积的正规子群.

(2) 令 $I=\mathbb{N}$ 并且 p_i 是自然数中的第 i 个素数，考虑 $G_i=\mathbb{Z}/p_i\mathbb{Z}$. 那么它们的直和中的任意元素都具有有限阶，但是直积中存在无穷阶的元素. 证明在这个例子中，$(G_i)_{i\in I}$ 的直和是直积的挠子群.

Proof. (1) 我们把直和记作 $\bigoplus_{i\in I}G_i$，将其中每个元素记为 $g=(g_i)_{i\in I}$. 对 $g,h\in\bigoplus_{i\in I}G_i$，除有限个 i 外其余每处均有 $g_i=h_i=1_{G_i}$，所以 $g_ih_i=1_{G_i}$. 所以 gh 在这些位处也都是单位元，因此 $gh\in\bigoplus_{i\in I}G_i$. 再证明正规性：对任意 $g\in\bigoplus_{i\in I}G_i$ 和 $h\in\prod_{i\in I}G_i$，除有限个 i 外均有 $h_ig_ih_i^{-1}=h_ih_i^{-1}=1_{G_i}$. 从而 hgh^{-1} 除有限项外均为单位元，故 $hgh^{-1}\in\bigoplus_{i\in I}G_i$.

(2) 直和中任意元素都在某个有限指标集 J 中有非平凡元素，从而它的阶整除 $\prod_{j\in J}p_j$. 直积中考虑 $g=(1+p_i\mathbb{Z})_{i\in\mathbb{Z}}$，则如果 $g^r=e$，那么 $p_i\mid r$ 对每个 i 均成立，所以 g 拥有无穷阶.

如果 $g\in G_i$ 拥有有限阶，设其阶为 r. 则对任意 $p_i>r$，g 在 $\mathbb{Z}/p_i\mathbb{Z}$ 中投影均为 $0+p_i\mathbb{Z}$，否则会导致 $p_i\mid r$，矛盾. 因此从这项之后所有的分量均平凡，所以 g 落在直和中. 从而直和是直积的挠子群.

Problem 20: P2.3.10

(1) 证明在 D_8 的任意自同构下，r 有至多两个可能的像，s 有至多四个可能的像. 证明 $\#\mathrm{Aut}(D_8) \leq 8$.

(2) 利用 $D_8 \lhd D_{16}$ 证明：$\mathrm{Aut}(D_8) \cong D_8$.

Proof. (1) D_8 中只有 r 和 r^3 是四阶元，其余所有元素都至多是两阶元，所以 r 在自同构下被打到 r 或者 r^3，从而 $\langle r\rangle$ 还是被打到 $\langle r\rangle$，于是 s 的像只能是四个反射之一. 由于每个 $\sigma \in \mathrm{Aut}(D_8)$ 都被 $\sigma(r)$ 和 $\sigma(s)$ 唯一确定，所以至多有 $2\times 4 = 8$ 个不同的自同构.

(2) 根据 $D_8 \lhd D_{16}$ 可知存在群同态 $D_{16}/C(D_{16}) \xrightarrow{\sim} \mathrm{Inn}(D_{16}) \to \mathrm{Aut}(D_8)$，因为每个共轭作用都给出 D_8 的一个自同构. 考虑这个群同态的 kernel，即考虑和 D_8 交换的元素 g. 由于每个反射地位对等，并且 $sr^2s = r^{-2} \neq r^2$，所以所有反射都不和 $r^2 \in D_8$ 交换，因此 g 只能是某个旋转，旋转自动和所有旋转交换. 根据对称性，$g = r^k$ 需和 s 交换，所以 $sr^ks = r^{-k} = r^k \Rightarrow 4 \mid k$. r^4 实际上和 D_{16} 中所有元素交换，因此 $C(D_8) = C(D_{16}) = \langle r^4\rangle$，于是有单同态

$$D_{16}/\langle r^4\rangle \xrightarrow{\sim} \mathrm{Inn}D_{16} \to \mathrm{Aut}(D_8)$$

但根据第一问结论 $\#\mathrm{Aut}(D_4) \leq 8$，所以只能 $\mathrm{Aut}(D_4) = 8$，于是上述群同态是群同构，$\mathrm{Aut}(D_8) \cong D_{16}/\langle r^4\rangle \cong D_8$，证毕. 

Problem 21: P2.3.13

设 F 是域，n 是正整数，G 是 $\mathrm{GL}_n(F)$ 中上三角矩阵构成的子群.

(1) 证明 G 是半直积 $U \rtimes D$，其中 U 是对角线全 1 的上三角矩阵构成的子群，D 是可逆对角矩阵构成的子群.

(2) 令 $n = 2$，则 $U \cong F^\times$，$D \cong F^\times \times F^\times$. 具体写出群同态 $D \to \mathrm{Aut}(U)$.

Proof. (1) 这是因为 U 是 G 的正规子群，并且 $G/U \cong D$，D 中每个矩阵恰好对应 G 中一个 U-陪集. 于是子群乘积 $UD = G$，所以考虑 ϕ 是 D 在 U 上的共轭群作用可知 $G = U \rtimes D$.

(2) 具体来说，共轭作用是

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a^{-1} & 0 \\ 0 & b^{-1} \end{pmatrix} = \begin{pmatrix} 1 & ac/b \\ 0 & 1 \end{pmatrix}.$$

所以 $F^\times \times F^\times \to \mathrm{Aut}(F)$ 可表示为 $(a,b) \mapsto [c \mapsto ac/b]$. 

Problem 22: P2.3.16

设 G 可迁作用在集合 A 上，H 是 G 的一个正规子群. 设 $\mathcal{O}_1, \ldots, \mathcal{O}_r$ 是 H 在 A 上作用给出的轨道.

(1) 证明 G 可作用在集合 $\{\mathcal{O}_1, \ldots, \mathcal{O}_r\}$ 上. 即对每个 $g \in G$，它将每个 $\mathcal{O}_i$ 都打到某个 $\mathcal{O}_j$，满足 $g\mathcal{O}_i = \mathcal{O}_j$. 证明 G 在 $\{\mathcal{O}_1, \ldots, \mathcal{O}_r\}$ 上的作用是可迁的，从而每个轨道都有相同的基数.

(2) 证明如果 $a \in \mathcal{O}_1$ 则 $\#\mathcal{O}_1 = [H : H \cap \mathrm{Stab}_G(a)]$，证明 $r = [G : H\mathrm{Stab}_G(a)]$.

Proof. (1) 这是因为如果设 $\mathcal{O}_i = Ha$，则 $g\mathcal{O}_i = gHa = Hga$，后者恰好是 ga 所在的 H-轨道，所以 G 确实通过左作用将一个轨道映为另一个轨道. 由于 G 在 A 上作用是可迁的，孤对任意 j 和 $b \in \mathcal{O}_j$ 均存在 g 使得 $ga = b$，从而 $g\mathcal{O}_i = \mathcal{O}_j$. 所以 G 在轨道上的作用是可迁的，所有它们拥有相同的基数.

(2) 这是因为 $\mathrm{Stab}_H(a) = \{g \in H : ga = a\} = H \cap \mathrm{Stab}_G(a)$，所以 $\#\mathcal{O}_1 = \mathrm{Orb}_H(a) = [H : H \cap \mathrm{Stab}_G(a)]$. 又因为 $r = |A| / \#\mathcal{O}_1$，而 G 在 A 上可迁作用给出 $|A| = [G : \mathrm{Stab}_G(a)]$，于是

$$r = \frac{[G : \mathrm{Stab}_G(a)]}{[H : H \cap \mathrm{Stab}_G(a)]}$$

根据群同构

$$H/(H \cap \mathrm{Stab}_G(a)) \cong H\ \mathrm{Stab}_G(a)/\ \mathrm{Stab}_G(a)$$

可知 $[H : H \cap \mathrm{Stab}_G(a)] = [H\ \mathrm{Stab}_G(a) :\ \mathrm{Stab}_G(a)]$，于是

$$r = \frac{[G : \mathrm{Stab}_G(a)]}{[H\ \mathrm{Stab}_G(a) :\ \mathrm{Stab}_G(a)]} = [G : H\mathrm{Stab}_G(a)].$$

Problem 23: P2.3.18

证明如果 H 是 G 的指数为 n 的子群，则存在 G 的正规子群 K 满足 $K \leq H$ 并且 $[G : K] \leq n!$.

Proof. 考虑 G 在 H 的左陪集上的作用，这给出群同态 $\phi : G \to S_n$，并且 $h \in H$ 当且仅当 $h \in \mathrm{Stab}(H)$. 考虑 $\ker\phi$，根据群同构 $G/\ker\phi \xrightarrow{\sim} \mathrm{im}\,\phi$ 可知 $[G : \ker\phi] = |\mathrm{im}\,\phi|\ |\ |S_n| = n!$ 并且 $\ker\phi$ 是 G 的正规子群. 由于 $\ker\phi \subset \mathrm{Stab}(H)$，故 $\ker\phi \leq H$. 因此 $\ker\phi$ 就满足题目条件.

Problem 24: P2.3.19

设 G 是一个群，H, K 是 G 的子群，满足 $H < K$.

(1) 证明如果 H 是 K 的特征子群，K 是 G 的特征子群，则 H 是 G 的特征子群.

(2) 构造一个例子，说明 H 是 K 的正规子群，K 是 G 的特征子群推不出 H 是 G 的正规子群.

Proof. (1) 对任意自同构 $\sigma \in \mathrm{Aut}(G)$，$\sigma|_K$ 是 K 的自同构，从而 $(\sigma|_K)|_H$ 是 H 的自同构，即 $\sigma|_H$ 是 H 的自同构，故 H 是 G 的特征子群。

(2) 考虑 $G = A_4$，$K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$，$H = \{\mathrm{id}, (12)(34)\}$. 验证条件：

- K 是 G 的特征子群，因为 G 只有 3 个二阶元，它们都落在 K 中.
- H 是 K 的正规子群，因为 H 是 K 的二阶子群.
- H 不是 G 的正规子群，因为 $(123)(12)(34)(123)^{-1} = (14)(23)$.

Remark. 另一个例子：$G = (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$. 对每个 $(a, b, 0) \in G$，它的阶为 1 或者 p. 对 $(a, b, 1) \in G$，$(a, b, 1)^n = (a + b + a + \ldots, b + a + b + \ldots, n + 2\mathbb{Z})$，从而它的阶一定为偶数，所以 $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ 是 G 的特征子群. 显然 $\mathbb{Z}/p\mathbb{Z}$ 是 $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ 的正规子群（但不是特征子群）. $\mathbb{Z}/p\mathbb{Z}$ 不是 G 的正规子群，因为 $(a, b, 1)(c, 0, 0)(-b, -a, 1) = (a, b + c, 1)(-b, -a, 1) = (0, c, 0)$ 会交换两个分量.

Problem 25: P2.3.20

设 N 是 G 的正规子群，假设 $\#N = 5$ 并且 $\#G$ 为奇数. 证明 N 落在 G 的中心中.

Proof. 考虑 G 在 $N = \{1, a, a^2, a^3, a^4\}$ 上的共轭作用. 如果 $|\mathrm{Orb}(a)| \neq 1$，那么存在 $g \in G$ 使得 $gag^{-1} = a^k$ 且 $k \neq 1$. 则 $g^\alpha a g^{-\alpha} = a^{k^\alpha}$，则由于 $\{2^\alpha\}$ 和 $\{3^\alpha\}$ 都跑遍 mod 5 的缩系，因此 $\mathrm{Orb}(a)$ 中不能恰好含 a^2, a^3 中的一个，所以 $|\mathrm{Orb}(a)| \neq 3$. 但根据 $|\mathrm{Orb}(a)|\,|\mathrm{Stab}(a)| = |G|$ 可知 $|\mathrm{Orb}(a)|$ 为奇数，矛盾.

所以 $|\mathrm{Orb}(a)| = 1$，即 a 和 G 中所有元素均交换，所以 N 和 G 中所有元素均交换，于是 N 落在 G 的中心中，证毕.

More Difficult Problems

Problem 26: P2.4.5

设 A 是有限 Abel 群，$\phi : A \to A$ 是群同态. 设

$$A_{\text{nil}} := \{x \in A : \phi^k(x) = 0 \text{ 对某个 } k \geq 1 \text{ 成立}\}$$

证明存在 A 的唯一子群 A_0 使得 $\phi|_{A_0}$ 是自同构并且 $A = A_0 \times A_{\text{nil}}$.

Proof. 由于 ϕ 把子群映到子群，因此有下降子群列

$$A > \phi(A) > \phi^2(A) > \cdots > \phi^n(A) > \dots$$

由于 A 是有限群，故一定存在 m 使得 $|\phi^m(A)| = |\phi^{m+1}(A)| = \dots$，即从 $\phi^m(A)$ 后每项均相等. 我们声称 $A_0 = \phi^m(A)$.

- $A_0 \subset \phi^m(A)$：因为 $A_0 = \phi(A_0) = \cdots = \phi^m(A_0) \subset \phi^m(A)$.
- $\phi^m(A) \subset A_0$：首先根据 $\phi^m(A) = \phi^{m+1}(A)$ 可知 ϕ 在 $\phi^m(A)$ 上是自同构，于是 $\ker \phi^m = \ker \phi^{m+1} = \dots$. 所以根据 A_{nil} 的定义可知 $A_{\text{nil}} = \ker \phi^m$. 这导致 $A/A_{\text{nil}} \cong \phi^m(A)$，于是 $|\phi^m(A)|\,|A_{\text{nil}}| = |A|$. 又根据 $A = A_0 \times A_{\text{nil}}$ 可知 $|A_0| = |\phi^m(A)|$，即得结论.

最后根据同构关系可得 $\ker \phi^m \cap \phi^m(A) = \{e\}$，所以 $A_0 \cap A_{\text{nil}} = \{e\}$，于是 $A_0 \times A_{\text{nil}}$ 是 A 的子群且两者元素个数相等，故两者相同. 

Problem 27: P2.4.7

我们将证明：对任意 $n \geq 2$ 且 $n \neq 6$，S_n 只含内自同构.

(1) 证明 G 的自同构给出 G 的共轭类上的置换. 即对任意 $\sigma \in \text{Aut}(G)$ 和 G 的共轭类 C，$\sigma(C)$ 也是 G 的共轭类.

(2) 设 C 是 S_n 中对换所在的共轭类，C' 是 S_n 中任意某个阶为 2 的非对换元素所在的共轭类. 证明 $|C| \neq |C'|$. 从而 S_n 的所有自同构都把对换映为对换.

(3) 证明对任意 $\sigma \in \text{Aut}(S_n)$，

$$\sigma : (12) \mapsto (ab_2), \quad \sigma : (13) \mapsto (ab_3), \quad \sigma : (1n) \mapsto (ab_n)$$

对某些两两不同的 $a, b_2, b_3, \dots, b_n \in \{1, \dots, n\}$ 成立.

(4) 证明任何 S_n 的自同构都由它在 $(12), \dots, (1n)$ 上的作用唯一确定，从而 S_n 至多有 $n!$ 个自同构，故 $\text{Aut}(S_n) = \text{Inn}(S_n)$ 对 $n \neq 6$ 总成立.

Proof. (1) 设 $C = \{hgh^{-1} : h \in G\}$，则 $\sigma(C) = \{\sigma(h)\sigma(g)\sigma(h)^{-1} : h \in G\}$. 根据 σ 的满性，$\sigma(C) = \{h\sigma(g)h^{-1} : h \in G\} = C(\sigma(g))$.

(2) S_n 中所有阶为 2 的元素都形如一些不相交的对换之积. 设 σ 是 k 个不交对换之积，则 C' 就是所有能写为 k 个不交对换之积的元素构成的集合，这相当于从 n 个数中选择 k 组数，组之间不计次序，总共有

$$\frac{1}{k!}\binom{n}{2,2,\ldots,2,n-2k}=\frac{(n)_{2k}}{2^k k!}$$

个. 令 $k=1$ 就得到 C 中元素个数. 假设存在 $k\geq 2$ 使得 $|C|=|C'|$，则

$$\frac{(n)_{2k}}{2^k k!}=\frac{n(n-1)}{2}\Rightarrow (n-2)_{2k-2}=2^{k-1}k!\Rightarrow (n-2)_{k-2}\binom{n-k}{k}=2^{k-1}.$$

因此如果 $k\geq 5$ 则 LHS 一定是 3 的倍数，矛盾. 因此只需讨论 $k=2,3,4$ 的情形.

- $k=2$：$(n-2)(n-3)=4$，这不可能.
- $k=3$：$(n-2)(n-3)(n-4)=24$，其唯一解是 $n=6$.
- $k=4$：$(n-2)(n-3)(n-4)(n-5)=192$，没有满足要求的 n.

所以对任意 $n\neq 6$ 和 $k\geq 2$ 均有 $|C|\neq|C'|$，所以自同构把对换映到对换.

(3) 根据上一问结论，对换被映到对换. 根据 $(ij)(ik)=(ikj)$，$\sigma(ij)\sigma(ik)$ 应当也是个三阶元素，所以 $\sigma(ij)$ 和 $\sigma(jk)$ 必须是两个有交的对换. 由于这对任何一个三元组都成立，因此 $\sigma(ij),\sigma(jk),\sigma(ki)$ 应两两有交. 设 $\sigma(ij)=(b_ib_j)$, $\sigma(ik)=(b_ib_k)$，那么只能有 $\sigma(jk)=(b_jb_k)$.

另一方面，可以固定 $i=1$，对任意一组 $2\leq j<k\leq n$ 应用上述结论. 如果 $n=2$ 则命题已经成立，不妨 $n\geq 3$. 设 $\sigma(12)=(ab_2)$，$\sigma(13)=(ab_3)$，于是 $\sigma(23)=(b_2b_3)$. 而所有 $\sigma(1k)$ 都和上述两个对换有交，因此根据 σ 的可逆性只能含有元素 a，于是存在 k 使得 $\sigma(1k)=(ab_k)$，这些元素的互异性是明显的.

(4) 根据第 (3) 问结论，考察 $\tau:1\mapsto a,\ k\mapsto b_k\ (k\geq 2)$. 则 $\sigma(1k)=\tau(1k)\tau^{-1}$. 对任意 $g\in S_n$，它可被写为

$$g=(1i_1)(1i_2)\ldots(1i_l)\Rightarrow\sigma(g)=\sigma(1i_1)\ldots\sigma(1i_l)=\tau(1i_1)\ldots(1i_l)\tau^{-1}=\tau g\tau^{-1}.$$

于是 σ 在 S_n 上的作用被唯一确定，并且就是共轭作用 $\mathrm{Ad}(\tau)$. 所以 S_n 仅存在内自同构，即 $\mathrm{Aut}(S_n)=\mathrm{Inn}(S_n)$ 对 $n\neq 6$ 恒成立.

Problem 28: P2.4.8

证明如果 G 是有限生成的，那么 G 的任何指标有限的子群都是有限生成的.

Proof. 设有子群 $H<G$ 满足 $[G:H]<+\infty$，记 G 关于 H 的左陪集分别为 $H=H_1,H_2,\ldots,H_n$. 那么可以考虑 G 在这些陪集上的左作用得到 $\phi:G\to S_n$，并且 $h\in H$ 当且仅当 $\phi(h)$ 把 H_1 映到 H_1.

现在设 G 的有限生成集为 $A=\{a_1,\ldots,a_m\}$，则 G 中所有元素都能被写为单词 $a_{i_1}\ldots a_{i_d}$ 的形式. 考虑

$$B=\{g\in H\mid g=a_{i_1}^{\epsilon_1}\ldots a_{i_d}^{\epsilon_d},\ d\leq 3n,\ \epsilon_i\in\{\pm 1\}\}.$$

我们证明 B 是 H 的生成集. 对任意 $g \in H$，将其写为 $g = g_1 g_2 \dots g_s$，其中 $g_i \in A \cup A^{-1}$. 如果 $s \le 3n$ 则已经有 $s \in B$. 如果 $s > 3n$，考虑 $\sigma(g) = \sigma(g_1) \dots \sigma(g_s)$，每个 $\sigma(g_i)$ 是一个置换. 追踪 H_1 的像，每次进行一个 $\sigma(g_{s-i})\,(0 \le i \le s-1)$ 的左作用给出一个从 H_1 出发的陪集序列. 根据 $s > 3n$，由抽屉原理存在某个 H_i 在序列中出现了至少三次，这会把整个序列分为四段，记为 $g = ABCD$，其中

$$\sigma(D)(H_1) = H_i,\ \sigma(C)(H_i) = H_i,\ \sigma(B)(H_i) = H_i,\ \sigma(A)(H_i) = H_1.$$

因此 $\sigma(AD)(H_1) = \sigma(D^{-1}BA^{-1})(H_1) = \sigma(ACD)(H_1) = H_1$，所以这三段都是 H 中元素. 而

$$g = AD \cdot D^{-1}BA^{-1} \cdot ACD.$$

所以 g 能写成三个序列长度严格更短的在 H 中元素之积. 有限次操作后，可以证明 g 能写成一些序列长度至多为 $3n$ 的 H 中元素之积，即写成 B 中元素的乘积. 综上，H 是有限生成群.

Problem 29: P2.4.10

设 G 是有限群，它的阶为合数 n. 如果对任意 $k \mid n$，G 都含有一个 k 阶子群，证明 G 不是单群.

Proof. 我们证明更强的结论：如果 p 是 n 的最小素因子，且 G 的子群 H 满足 $[G : H] = p$，那么 H 是 G 的正规子群.

根据 $[G : H] = p$，G 左作用于全体左陪集上，给出群同态 $\phi : G \to S_p$. 根据第一同构定理，$G/\ker\phi \cong \operatorname{im}\phi$，于是

$$|G| = |\ker\phi| \cdot |\operatorname{im}\phi|.$$

所以 $|\operatorname{im}\phi| \mid |G|$. 另一方面，$\operatorname{im}\phi$ 是 S_p 的子群，所以 $|\operatorname{im}\phi| \mid |S_p| = p!$. 由于 p 是 $|G|$ 的最小素因子，故只能 $|\operatorname{im}\phi| = 1$ or p. 但由于 H 是 G 的真子群，左陪集作用不可能平凡，所以 $|\operatorname{im}\phi| = p$，于是 $|\ker\phi| = |G|/p = |H|$.

另一方面，对 $g \in \ker\phi$ 有 $gH = H$，所以 $g \in H$. 因此 $\ker\phi < H$，所以 $\ker\phi = H$. 而群同态的核必为正规子群，所以 H 是 G 的正规子群，证毕.

回到原题，当 n 是合数时，存在其子群 H 使得 $|G : H| = p$ 并且 H 非平凡，所以 G 不是单群.

Problem 30: P2.4.12

(1) 设 p 是素数，计算下述自同构群的阶数：

$$\#\operatorname{Aut}(\mathbb{Z}/p^{n_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p^{n_r}\mathbb{Z}),$$

其中 $n_1\le\cdots\le n_r$.

(2) 定义 $(p)_r:=\prod_{i=1}^r(1-p^{-i})$，证明

$$\sum_{\substack{G\,p\text{-abelian}\\ \#G\le p^r}}\frac{1}{\#\operatorname{Aut}(G)}=\frac{1}{(p)_r}.$$

Proof. (1) 设 $G=\mathbb{Z}/p^{n_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p^{n_r}\mathbb{Z}$ 的 r 个生成元为 $g_1,g_2,\dots,g_r$，g_i 的第 i 个分量为 $1+p^{n_i}\mathbb{Z}$，其余分量均为零. 那么自同构 $\sigma\in\operatorname{Aut}(G)$ 完全由所有 $\sigma(g_i)$ 决定. 设 $\sigma(g_i)=a_{1i}g_1+a_{2i}g_2+\cdots+a_{ri}g_i$，其中每个 $a_{ji}\in\mathbb{Z}$，在差一个 $p^{n_j}\mathbb{Z}$ 的意义下 a_{ji} 的意义相同. 则 $p^{n_i}\sigma(g_i)=0$，这保证了 σ 给出一个群同态. 除了满足这个条件之外，只需满足 $\operatorname{im}\sigma=G$ 就可给出 σ 是群同构. 即对每个 i，存在 $b_1,\dots,b_n\in\mathbb{Z}$ 使得 $b_1\sigma(g_1)+\cdots+b_r\sigma(g_r)=g_i$，即

$$\begin{pmatrix}a_{11}&a_{12}&\dots&a_{1r}\\ a_{21}&a_{22}&\dots&a_{2r}\\ \vdots&\vdots&\ddots&\vdots\\ a_{r1}&a_{r2}&\dots&a_{rr}\end{pmatrix}\begin{pmatrix}b_1\\ b_2\\ \vdots\\ b_r\end{pmatrix}=\begin{pmatrix}c_1\\ c_2\\ \vdots\\ c_r\end{pmatrix},c_j\equiv\mathbf{1}_{i=j}\pmod{p^{n_i}}.\tag{$*$}$$

记上述 $r\times r$ 矩阵为 A，下证明 σ 是自同构当且仅当在 $\mathbb{F}_p$ 中 A 可逆.

- 已知 σ 是自同构，记一个元素 a，向量 $\boldsymbol{v}$，或矩阵 A 在 $\mathbb{F}_p$ 上的投影为 $\overline{a},\overline{\boldsymbol{v}},\overline{A}$. 把关系式 $(*)$ 投影到 $\mathbb{F}_p$ 可知，对任意单位向量 $\overline{\boldsymbol{e}}_i\in\mathbb{F}_p^r$，存在 $\overline{\boldsymbol{v}}_i\in\mathbb{F}_p^r$ 使得

  $$\overline{A}\overline{\boldsymbol{v}}_i=\overline{\boldsymbol{e}}_i.$$

  于是存在矩阵 $\overline{B}$ 使得

  $$\overline{AB}=I\in\mathbb{F}_p^{r\times r}.$$

  所以 $\overline{A}$ 是 $\mathbb{F}_p^{r\times r}$ 中的可逆矩阵.

- 已知 $\overline{A}$ 是 $\mathbb{F}_p^{r\times r}$ 中的可逆矩阵，则对每个 i 都存在 $\overline{v_i}\in\mathbb{F}_p^r$ 使得

  $$\overline{A}\overline{\boldsymbol{v}}_i=\overline{\boldsymbol{e}}_i.$$

  考虑它在 $\mathbb{Z}$ 中的原像可知，存在 $\boldsymbol{x}_i\in\mathbb{Z}^r$ 使得

  $$A\boldsymbol{v}_i=\boldsymbol{e}_i+p\boldsymbol{x}_i.$$

  我们来证明用这些 $\boldsymbol{e}_i+p\boldsymbol{x}_i$ 能够在模足够大的 p^N 的意义下表示所有 r 维向量，记它们张成的格为 L. 则 $p^{N-1}(\boldsymbol{e}_i+p\boldsymbol{x}_i)\in L\Rightarrow p^{N-1}\boldsymbol{e}_i\in L$，因此 L 中含有被

p^{N-1} 整除的所有向量. 再结合上 $p^{N-2}(\boldsymbol{e}_i + p\boldsymbol{x}_i) \in L$ 可知 $p^{N-2}\boldsymbol{e}_i \in L$，因此 L 中含有被 p^{N-2} 整除的所有向量. 依此类推，从上至下归纳可知 L 含有 mod p^N 意义下所有向量，取 $N > n_r$ 就可知存在 $\boldsymbol{v}_i$ 满足 $(*)$，因此 σ 是群同构.

接下来为满足 $\overline{A}$ 在 $\mathbb{F}_p^{r\times r}$ 中可逆的矩阵计数，我们让 a_{ji} 限制在 $\{0, 1, \ldots, p^{n_j} - 1\}$ 内，这样满足要求的矩阵就和群同构是一对一的. 首先 $p^{n_i}\sigma(g_i) = 0$ 的条件等价于 $p^{n_j-n_i} \mid a_{ji}$ 对每组 $n_j > n_i$ 成立，进而在 $\mathbb{F}_p$ 上 $\overline{a_{ji}} = 0$. 所以 $\overline{A}$ 形如分块上三角矩阵. 设 $n_1, \ldots, n_r$ 中有 d_1 个 m_1，d_2 个 m_2，$\ldots$，d_t 个 m_t，其中 $m_1 < m_2 < \cdots < m_t$. 则 $\overline{A}$ 为对角线上从上到下分别为 $d_1 \times d_1$ 块，$d_2 \times d_2$ 块，$\ldots$，$d_t \times d_t$ 块的分块上三角矩阵. $\overline{A}$ 可逆当且仅当 $\det(\overline{A}) \neq 0$，而根据分块结构

$$\det(\overline{A}) = \det(\overline{A_1}) \det(\overline{A_2}) \ldots \det(\overline{A_t}),$$

其中 A_i 是 $d_i \times d_i$ 矩阵. 故 $\overline{A}$ 可逆当且仅当每个 $\det(\overline{A_i})$ 可逆.

于是我们先在 $\mathbb{F}_p$ 中对 d_i 阶可逆矩阵计数，这等价于选取 d_i 个向量，使得每个都不落在之前向量张成的线性空间中，共有

$$(p^{d_i} - 1)(p^{d_i} - p) \ldots (p^{d_i} - p^{d_i-1}) = p^{d_i^2}(p)_{d_i}$$

种选择. 现在回到 A 中，我们考虑每部分贡献的可能数：

- A_i 部分：在 mod p 意义下有 $p^{d_i^2}(p)_{d_i}$ 种选择，而固定 mod p 下的一组选择后，每个位置又有 p^{m_i-1} 种可能的选择，总计

$$\#A_i = p^{d_i^2 m_i}(p)_{d_i}.$$

- 对角线以上的部分：没有任何限制. 对每一组 $i < j$，有一个大小为 $d_i \times d_j$ 的矩阵落在对角线以上，每个位置贡献为 p^{m_i}，从而这个子阵贡献了 $p^{d_i d_j m_i}$ 种可能的选择，总计

$$\#\{\text{对角线以上}\} = \prod_{i<j} p^{d_i d_j m_i}.$$

- 对角线以下的部分：对每一组 $i < j$，有一个大小为 $d_j \times d_i$ 的矩阵落在对角线以下，每个位置原本有 p^{m_j} 种取值，但它需是 $p^{m_j-m_i}$ 的倍数，所以只剩下 p^{m_i} 种取值. 因此总计为

$$\#\{\text{对角线以下}\} = \prod_{i<j} p^{d_i d_j m_i}.$$

综上所述，

$$\#\operatorname{Aut}(G) = \prod_{1\le i,j\le t} p^{d_i d_j \min(m_i,m_j)} \cdot \prod_{i=1}^{t} (p)_{d_i}.$$

(2) 所有满足 $\#G \leq p^r$ 的 p-Abel 群 G 都能被写成一些 $\mathbb{Z}/p^n\mathbb{Z}$ 的直积，因此我们只需对 (1) 中所有满足 $\sum d_i m_i \leq r$ 的群 G 求和（它代表 G 中含有 d_i 个 $\mathbb{Z}/p^{m_i}\mathbb{Z}$），即证

$$\sum_{\sum d_i m_i \leq r} \prod_{1\leq i,j\leq t} p^{-d_i d_j \min(m_i,m_j)} \cdot \prod_{i=1}^{t} (p)_{d_i}^{-1} = (p)_r^{-1}.$$

其中求和对所有 $t \in \mathbb{N}$ 和 $d_i, m_i \in \mathbb{N}^*$, $(1 \leq i \leq t)$ 进行. 因此只需证

$$\sum_{\sum d_i m_i = r} \prod_{1\leq i,j\leq t} p^{-d_i d_j \min(m_i,m_j)} \cdot \prod_{i=1}^{t} (p)_{d_i}^{-1} = (p)_r^{-1} = (p)_{r-1}^{-1} = p^{-r}(p)_r^{-1}.$$

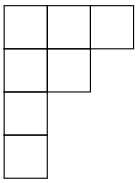
只需证明有下述形式幂级数之间的恒等式：

$$\sum_{\sum d_i m_i = r} \prod_{1\leq i,j\leq t} x^{d_i d_j \min(m_i,m_j)} \cdot \prod_{i=1}^{t} \frac{1}{(1-x)\dots(1-x^{d_i})} = \frac{x^r}{(1-x)\dots(1-x^r)}.$$

首先

$$\begin{aligned}\sum_{1\leq i,j\leq t} d_i d_j \min(m_i,m_j) &= \sum_{1\leq i,j\leq t} \sum_{k=1}^{\infty} d_i d_j \mathbf{1}_{m_i\geq k}\mathbf{1}_{m_j\geq k} \\ &= \sum_{k=1}^{\infty} \left(\sum_{i=1}^{t} d_i \mathbf{1}_{m_i\geq k}\right)^2.\end{aligned}$$

其次，每一组满足 $\sum d_i m_i = r$ 的资料都一一对应于 r 的一个无序分拆，也一一对应于一张 r 阶 Young 表，它从上到下分别是 d_t 个 m_t，d_{t-1} 个 m_{t-1}，$\dots$，d_1 个 m_1. 比如下述例子：

$\lambda : 7 = 3+2+1+1 \leftrightarrow$  $\leftrightarrow$ 2 个 1, 1 个 2, 1 个 3.

所以左边的求和对所有 r 阶 Young 表 λ 进行. 注意到 $\mu_k = \sum_{i=1}^{t} d_i \mathbf{1}_{m_i\geq k}$ 其实就是 λ 对应的 Young 表的第 k 列，而列信息 $\mu = (\mu_1, \mu_2, \dots, \mu_l)$ 也是一个 r 的无序分拆，并且可以从列的角度一一对应于 r 阶 Young 表，所以求和可以改为对所有 r 的无序分拆 μ 进行（下记作对 $\mu \vdash r$ 求和）. 因此只需证：

$$\sum_{\mu\vdash r} \prod_{i=1}^{l} x^{\mu_i^2} \cdot \prod_{k=1}^{l} \frac{1}{(1-x)\dots(1-x^{\mu_k-\mu_{k+1}})} = \frac{x^r}{(1-x)\dots(1-x^r)}.$$

这里我们额外规定 $\mu_{l+1} = \mu_{l+2} = \dots = 0$. 现在考虑两边的 $[x^N]$ 项系数的组合意义：

- RHS：N 的无序分拆且分拆中最大项恰好为 r 的方法数，即所有首行恰有 r 个方格的 N 阶 Young 表个数.
- LHS：对每个 $\mu \vdash r$，记 $S(\mu)$ 为先把 $N - \sum \mu_i^2$ 分为 l 部分，然后再把第 k 部分进行最大项至多为 $\mu_k - \mu_{k+1}$ 的无序分拆的方法数，LHS 是对全体 $S(\mu)$ 求和的结果.

用 n 代替上面的 $N-\sum\mu_i^2$，得到的计数结果记为 $S(\mu,n)$，它关于 n 的生成函数记为 S. 对每个首行恰有 r 个方格的 N 阶 Young 表，我们按下述方式确定一个分拆 μ：

- μ_1 被选择为从以 $(1,1)$ 为左上格的的最大可嵌入 Young 表的正方形边长，比如在上 $7=3+2+1+1$ 的例子中，至多能在左上角放入一个 2×2 的正方形，所以它对应 $\mu_1=2$.
- 假设已经确定 $\mu_1,\dots,\mu_k$ 并且 $\mu_1+\cdots+\mu_k<r$. 考虑以 $(\mu_1+\cdots+\mu_k+1)$ 为左上格的最大可嵌入 Young 表的正方形边长，记为 μ_{k+1}. 比如在上述例子中，$\mu_2=1$，对应的分拆为 $3=2+1$.

这样，RHS 的每个 Young 表都唯一对应一个拆分 $\mu\vdash n$，设这样的拆分个数为 $T(\mu)$，接下来只需证明 $S(\mu)=T(\mu)$. 首先如果 Young 表 P 对应于 μ，那么 P 中已经嵌入一列大小分别为 $\mu_1\times\mu_1$, $\mu_2\times\mu_2$, …, $\mu_l\times\mu_l$ 的正方形，它们的底边从左到右排列在第一行上. 还剩下 $N-\sum\mu_i^2$ 个格子，它们只有如下一些位置可以摆放：

- 在正方形 $\mu_1\times\mu_1$ 的下侧摆放，对应于首行至多为 μ_1 的一张 Young 表；
- 对 $2\le k\le l$，在正方形 $\mu_k\times\mu_k$ 的下侧，$\mu_{k-1}\times\mu_{k-1}$ 的右侧的那个 $(\mu_{k-1}-\mu_k)\times\mu_k$ 区域内摆放，对应于一张包含在区域 $(\mu_{k-1}-\mu_k)\times\mu_k$ 内的 Young 表.

用 n 代替上面的 $N-\sum\mu_i^2$，得到的计数结果记为 $T(\mu,n)$，它关于 n 的生成函数记为 T. 为了进行最后的计数，我们证明一个引理：

Lemma. *记广义二项式系数*

$$\begin{bmatrix}n\\m\end{bmatrix}=\frac{(1-x^n)(1-x^{n-1})\dots(1-x^{n-m+1})}{(1-x^m)(1-x^{m-1})\dots(1-x)}.$$

设包含在区域 $m\times n$ 中的 N 阶 Young 表个数为 $y_{m,n}(N)$，则

$$\begin{bmatrix}n+m\\m\end{bmatrix}=\sum_{N=0}^{\infty}y_{m,n}(N)x^N.$$

Proof. 我们对 $n+m$ 归纳. 当 $m=1$ 时 Young 表只有一行 n 列，所以生成函数恰好为

$$1+x+\cdots+x^n=\frac{1-x^{n+1}}{1-x}=\begin{bmatrix}n+1\\1\end{bmatrix}.$$

同理 $n=1$ 时生成函数也是 $1+x+\cdots+x^n$，它和 $\begin{bmatrix}n+1\\n\end{bmatrix}=\begin{bmatrix}n+1\\1\end{bmatrix}$ 相等.

给定 (m,n)，假设对满足 $r+s<m+n$ 的 (r,s) 均有命题成立. 则对任何一个包含在 $m\times n$ 中的 Young 表 P，考虑其左下角的格子.

- 如果 P 包含这个格子，则 P 包含整个第一列，于是一一对应于 $m\times(n-1)$ 中含有 $N-m$ 个格子的 Young 表.

- 如果 P 不包含这个格子，则 P 不包含整个最后一列，于是一一对应于 $(m-1)\times n$ 中含有 N 个格子的 Young 表.

因此

$$y_{m,n}(N)=y_{m,n-1}(N-m)+y_{m-1,n}(N).$$

所以

$$\begin{aligned}\sum_{N=0}^{\infty}y_{m,n}(N)x^N&=\sum_{N=0}^{\infty}y_{m,n-1}(N-m)x^N+\sum_{N=0}^{\infty}y_{m-1,n}(N)x^N\\&=x^m\begin{bmatrix}m+n-1\\m\end{bmatrix}+\begin{bmatrix}m+n-1\\m-1\end{bmatrix}\\&=x^m\frac{(1-x^{m+n-1})\dots(1-x^n)}{(1-x^m)\dots(1-x)}+\frac{(1-x^{m+n-1})\dots(1-x^{n+1})}{(1-x^{m-1})\dots(1-x)}\\&=\frac{(1-x^{m+n-1})\dots(1-x^{n+1})}{(1-x^m)\dots(1-x)}[x^m(1-x^n)+(1-x^m)]\\&=\frac{(1-x^{m+n})\dots(1-x^{n+1})}{(1-x^m)\dots(1-x)}=\begin{bmatrix}m+n\\m\end{bmatrix}.\end{aligned}$$

证毕.

回到原题，T 的生成函数为：

$$\begin{aligned}T&=\frac{1}{(1-x)\dots(1-x^{\mu_1})}\cdot\begin{bmatrix}\mu_1\\\mu_2\end{bmatrix}\cdot\dots\cdot\begin{bmatrix}\mu_{l-1}\\\mu_l\end{bmatrix}\\&=\frac{1}{(1-x)\dots(1-x^{\mu_1})}\cdot\prod_{k=1}^{l-1}\frac{(1-x)\dots(1-x^{\mu_k})}{(1-x)\dots(1-x^{\mu_{k+1}})(1-x)\dots(1-x^{\mu_k-\mu_{k+1}})}\\&=\prod_{k=1}^{l}\frac{1}{(1-x)\dots(1-x^{\mu_k-\mu_{k+1}})}=S.\end{aligned}$$

而 $T(\mu)=[x^{N-\sum\mu_i^2}]T=[x^{N-\sum\mu_i^2}]S=S(\mu)$，这就完成了整个证明.

Problem 31: P2.4.13

设 $n\geq 2$，$G_1,G_2,\dots,G_n$ 是非 Abel 单群. 设 H 是 $G_1\times\dots\times G_n$ 的子群，并且对每对 $i<j$，H 在每个 $G_i\times G_j$ 上的投影都是满射. 证明 $H=G_1\times\dots\times G_n$.

Proof. 我们归纳证明对任何 $2\leq k\leq n$ 均有 H 在每个 $G_{i_1}\times G_{i_2}\times\dots\times G_{i_k}$ 上的投影均为满射. 归纳奠基就是题目条件. 假设 k 时成立，考虑 $k+1$ 时情形. 不失一般性，我们就考虑 H 在 $G_1\times\dots\times G_{k+1}$ 上的投影，记为 H'. 根据归纳假设，H' 在任意 k 个分量上的投影均满，故对任意 $h,h'\in G_1$，存在 $h_2\in G_2$ 和 $h_3\in G_3$ 使得

$$(h,h_2,1,1,\dots,1)\in H',\quad (h',1,h_3,1,\dots,1)\in H'.$$

所以

$$\begin{aligned}&(h,h_2,1,\dots)(h',1,h_3,\dots)(h,h_2,1,\dots)^{-1}(h',1,h_3,\dots)^{-1}\\=&(hh'h^{-1}h'^{-1},1,\dots,1)\in H'.\end{aligned}$$

因此我们考虑

$$H_1' = \{g \in G_1 : (g, 1, \dots, 1) \in H'\}.$$

则对任意 $h, h' \in G_1$ 有 $hh'h^{-1}h'^{-1} \in H_1'$. 我们证明 H_1' 是 G_1 的正规子群：这是因为对任意 $g \in H_1'$ 和 $h \in G_1$ 均有

$$(h, h_2, 1, \dots)(g, 1, 1, \dots)(h, h_2, 1, \dots)^{-1} = (hgh^{-1}, 1, 1, \dots) \in H' \Rightarrow hgh^{-1} \in H_1'.$$

于是根据 G_1 的单性，$H_1' = \{e\}$ 或者 G_1. 若是前者，则 $hh'h^{-1}h'^{-1} = e$ 对一切 $h, h' \in G_1$ 成立，故 G_1 是 Abel 群，矛盾。所以 $H_1' = G_1$. 同理可证明对任意 i 和 $g_i \in G_i$，$(1, \dots, g_1, \dots, 1) \in H'$. 于是 $H' = G_1 \times \cdots \times G_{k+1}$，归纳成立，令 $k = n$ 即得结论.