近世代数作业题

叶郁班

Contents

第一次作业

必做题

1: 对于任何集合 X, 我们用 id_X 表示 X 到自身的恒等映射. 设 $f : A \to B$ 是集合间的映射,A 是非空集合. 试证:

(1) f 是单射当且仅当存在 $g : B \to A$, 使得 $g \circ f = id_A$;
(2) f 是满射当且仅当存在 $h : B \to A$, 使得 $f \circ h = id_B$;
(3) f 是双射当且仅当存在唯一的 $g : B \to A$, 使得 $f \circ g = id_B, g \circ f = id_A$;
(4) 分别举例说明 (1)(2) 不唯一.

2: 设 $P(A)$ 是集合 A 的全部子集所构成的集族,$M(A)$ 为所有 A 到集合 $\{0, 1\}$ 的映射构成的集合. 试构造 $P(A)$ 到 $M(A)$ 的双射. 特别的, 如 A 为有限集, 试证 $|P(A)| = 2^{|A|}$, 换言之,n 元集共有 2^n 个子集.

3: 证明等价关系的三个条件是互相独立的, 即: 已知任意两个条件不能推出第三个条件.

4: 设集合 A 中关系满足对称性和传递性, 且 A 中任意元素都和某个元素有关系, 证明此关系为等价关系.

5: 证明容斥原理:

$$|A_1 \bigcup \cdots \bigcup A_n| = \sum_{j=1}^{n} (-1)^{j-1} \sum_{\{i_1,\cdots,i_j\} \subset \{1,2,\cdots,n\}} |A_{i_1} \bigcap \cdots \bigcap A_{i_j}|$$

其中 $A_i, i = 1, 2, \cdots, n$ 为某个固定集合 U 的有限子集.

选做题

补充 (粗略, 选做):
下面是集合论中三个等价的著名定理 (在集合论的 ZF 公理系统之下):
(1):Zorn 引理: 令 $(A, \leq)$ 是一个偏序集. 若 A 的每一链 S 在 A 中都有上界, 即:

$$\exists a \in A, \forall s \in S, s \leq a,$$

则 A 有极大元.
(2): 选择公理: 令 $T = \{A_i | i \in I\}$ 为一族非空集合. 则存在映射:

$$\phi : T \longrightarrow \bigcup_{i \in I} A_i$$

$$A_i \longrightarrow \phi(A_i) \in A_i.$$

称 ϕ 为一选择函数.
(3): 任何集合上都可以定义起一个良序 (称一偏序集 $(A, \leq)$ 为良序集, 或称偏序 $\leq$ 为一个良序, 如果 A 的任意非空子集关于 $\leq$ 有最小元).

6: 利用 Zorn 引理或者良序公理证明非空集合 A 上存在极大偏序 (称 A 上的偏序 α 为一极大偏序, 如果关于 A 上的任一偏序 β,$\alpha \subset \beta$ 蕴含着 $\alpha = \beta$, 即将 A 上的一个二元关系看成是 $A \times A$ 的子集).

7: 尝试寻找实数集 $\mathbb{R}$ 上的一个良序.

8: 令 $T = \{A_i | i \in I\}$ 是一族非空集合, 证明 $\prod_{i\in I} A_i$ 非空, 其中:

$$\prod_{i\in I} A_i = \{f : I \to \bigcup_{i\in I} A_i | \forall i \in I, f(i) \in A_i\}.$$

反之是否成立? 即 $\prod_{i\in I} A_i$ 非空, 则 T 有选择函数.

第二次作业

必做题 (周三)

一: 基础 (定义验证)
1: 令 G 是实数对 $(a, b), a \neq 0$ 的集合. 在 G 上定义:$(a, b)(c, d) = (ac, ad + b)$. 试证 G 是群.

2: 令 Ω 是任意一个集合,G 是一个群,Ω^G 是 Ω 到 G 的所有映射的集合. 对任意两个映射 $f, g \in \Omega^G$, 定义乘积是如下映射:

$$\forall \alpha \in \Omega, (fg)(\alpha) = f(\alpha)g(\alpha).$$

试证 Ω^G 是群.

3: 令 G 是所有秩不大于 r 的 n 阶复方阵的集合, 试证在矩阵的乘法下 G 成半群.

4: 设 G 是一个半群, 如果:
(1) G 中含有左幺元 e, 即 $\forall x \in G, ex = x$;
(2) G 的每个元素 x 有左逆元 x^{-1} 使得 $x^{-1}x = e$.
试证 G 是群.

5:b 是含幺半群中元素 a 的逆元素当且仅当成立 $aba = a$ 和 $ab^2a = 1$.

二: 进阶 (思考思考)
6: 设 G 是一个有限半群, 如果在其内满足左右消去律 ($ax = ay$ 或者 $xa = ya$ 意味着 $x = y$) 则 G 是群, 即有限双消半群是群. 并举例说明一个半群如果只满足单边消去律则不一定是一个群.

7: 令 G 是 n 阶有限群,$a_1, a_2 \cdots, a_n$ 是群 G 的任意 n 个元素, 不一定两两不同, 试证: 存在整数 p 和 q,$1 \leq p \leq q \leq n$, 使得 $a_p a_{p+1} \cdots a_q = 1$.

8: 举例:
(1) 举出一个半群的例子, 其中存在元素有左逆元但是没有右逆元;
(2) 举出一个半群的例子, 其中存在元素有两个左逆元;
(3) 举出一个半群的例子, 其中存在元素有无数个左逆元.

选做题

9: 令 S 是一非空集. 定义 S 上的运算:$a \cdot b = a(a \cdot b = b)$. 则 $(S, \cdot)$ 是一个半群, 称其为左 (右) 零半群. 若 S 是一半群, 证明如下三款等价:

(1) S 是一左零半群, 或者 S 是一右零半群;

(2) $ab = cd \Rightarrow a = c$ 或者 $b = d$;

(3) 任意映射 $f : S \to S$,$f(ab) = f(a)f(b)$.

10: 令 G 是一个半群. 则 G 是一个群当且仅当

$$\forall a \in G, \exists! b \in G, (ab)^2 = ab.$$

必做题 (周五)

11: (1) 一个 n 阶矩阵称为一个单项矩阵, 如果该方阵的每一行, 每一列都恰有一个非零元素. 证明所有 n 阶单项矩阵构成的集合对于通常的矩阵乘法构成群.

(2) 所有 n 阶严格对角占优矩阵对于通常的矩阵乘法是否构成群?

(3) 定义 $GL_n(R)$ 上运算 $A \circ B = AB - BA$, 那么 $(GL_n(R), \circ)$ 是否构成一个群?

12: 偶数阶群必定存在 $a(\neq e)$ 满足 $a^2 = e$.

13: 令 G 是 n 阶有限群,S 是 G 的一个子集,$|S| > n/2$. 试证:对任意 $g \in G$, 存在 $a, b \in S$ 使得 $g = ab$.

第 e 次作业
(阅读材料，不用做)

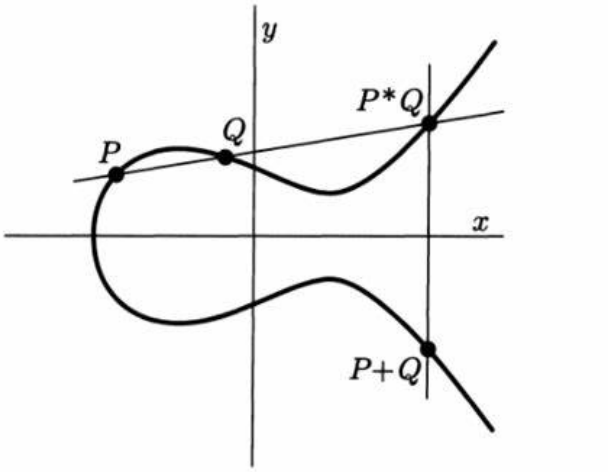
费马于 1630 年左右在 Diophantus 所著《数论》的书页空白处写下 “当 $n \geq 3$ 时, 不存在满足 $x^n + y^n = z^n$ 的自然数解” 以及 “对此我发现了令人惊叹的证明, 但这里空白太小写不下了.” 由此引出了三百多年的故事. 我们将从椭圆曲线的角度出发浅探其与 FLT 的关系.

$E : y^2 = x^3 + ax + b$ $(a, b \in Q)$, $4a^3 + 27b^2 \neq 0$, 则称 E 为 Q 上的椭圆曲线. 考虑 E 的解集 $E(Q) = \{(x, y) \in Q \times Q | y^2 = x^3 + ax + b\}$. 我们在 $E(Q)$ 中添加一个特殊的元素 O 并定义:

(i)O 为单位元

(ii)$P, Q \in E(Q), P \neq O, Q \neq O$. 连接 P, Q 的直线与 E 交于第三点 $P^*Q = (x, y)$, 则令 $(x, -y) \in E(Q)$ 为 $P + Q$.

(iii)$P \in E(Q), P \neq O$. 设其坐标为 (x, y), 则 P 的逆元为 $(x, -y)$.



试解决以下问题 (* 题目仅供娱乐)

$*$[1] 验证 $E(Q)$ 在上述定义下构成阿贝尔群.

$*$[2] (Siegel's Theorem) 若 $a,b\in Z$, 令 $E(Z)=\{(x,y)\in Z\times Z|(x,y)\in E(Q)\}$, 证明 $E(Z)$ 为有限阿贝尔群.(更一般的，Mordell 证明了 $E(Q)$ 为有限生成阿贝尔群.)

[3] 费马曾写下“除 1 以外的 3 角数均非立方数”且未给出证明, 其中 3 角数为形如 $\frac{n(n+1)}{2}$ 的自然数.

(1) 试说明该论断与 $E:y^2=x^3+1$ 之间的关系.(提示：将 $\frac{n(n+1)}{2}=m^3$ 改写成 $y^2=x^3+1$)

(2) 证明 $\{(0,\pm1),(-1,0),(2,\pm3)\}\in E(Z)$.

(3) 利用 [2] 以及如下定理说明 $E(Z)$ 除 (2) 中解外无其余整数解.

$*$(Nagell-Lutz Theorem) 对于椭圆曲线 $y^2=x^3+ax^2+bx+c$ $(a,b,c\in Z)$, 令 $D=-4a^3c+a^2b^2+18abc-4b^3-27c^2$, 若 $P=(x,y)\in E(Q)$ 且作为阿贝尔群中的元素其阶数有限, 则 $P\in E(Z)$ 并且要么 $y=0$, 要么 $y|D$.

(4) 证明费马的论断.

[4] 有学者认为费马利用“无穷递降法”证明了 $n=4$ 的情形并认为其余情形类似，因此宣称自己有一个“美妙的证明”. 以下将采用椭圆曲线的知识并利用“无穷递降法”证明费马关于 $n=4$ 时的论断.

(1) 说明 $x^4+y^4=z^4$ 的自然数解与 $E:y^2=x^3-x$ 的有理数解之间的关系.(提示: 改写成 $(\frac{x^2z}{y^3})^2=(\frac{z^2}{y^2})^3-\frac{z^2}{y^2}$).

(2) 验证 $\{(0,0),(\pm1,0)\}\in E(Q)$ 并证明 E 除此之外无其余有理数解.

提示：

对于有理数 $a=\frac{m}{n}$ 其中 m,n 互素, 定义其高 (Height) 为 $H(a)=max(|n|,|m|)$. 例如,$H(\frac{-5}{8})=8,H(\frac{7}{2})=7,H(0)=H(\frac{0}{1})=1$. 假设 E 还有其他有理数解，选取其中 x 坐标的高最小者，记为 (x_0,y_0), 则证明此时存在 $(x_1,y_1)\in E(Q)$ 满足 $H(x_1)<H(x_0)$, 因此得到矛盾.

(i) 证明可以取 $x_0>1$.

(ii) 于是取 $x_0>1$, 证明从 $(x_0-1)x_0(x_0+1)=x_0^3-x_0=y_0^2$ 为有理数的平方推导出 x_0-1,x_0,x_0+1 都是有理数的平方.

(iii) 此时存在 $(x_1,y_1)\in E(Q)$ 并且 $x_0=\frac{(x_1^2+1)^2}{4(x_1^3-x_1)}$, 说明 $H(x_1)<H(x_0)$. (3) 证明费马的论断.

$*$(4) 验证 $E(Q)=Z_2\oplus Z_2$.(Mazur，1977 给出了 $E(Q)$ 所有可能的群结构)

椭圆曲线在 FLT 的证明过程中发挥了重要作用，对该问题感兴趣的同学可以翻阅加藤和也, 黑川信重以及斋藤毅所著的《数论 1》.
[5] 假定 ABC 猜想成立，证明费马大定理.
$*(ABC\ conjecture)$ 对于任意实数 $\epsilon > 0$, 存在与 ϵ 有关的常数 $C(\epsilon)$ 使得: 若互素的 $a, b, c \in Z - \{0\}$ 满足 $a + b + c = 0$, 则 $max\{|a|, |b|, |c|\} < C(\epsilon) rad(abc)^{1+\epsilon}$, 其中 $rad(N) := \prod p$, p 为满足 $p|N$ 的所有素数.

第三次作业

必做题 (周三)

一: 基础 (定义验证)
1: 对于群同态 $f : G \longrightarrow H$, 定义 f 的核为 $Ker(f) = \{a \in G | f(a) = e \in H\}$,$f$ 的像为 $Im(f) = \{b \in H | \exists a \in G, b = f(a)\}$. 证明 $Ker(f)$ 与 $Im(f)$ 分别为 G 与 H 的子群并且 f 为单射当且仅当 $Ker(f) = \{e\}$.

2:a,b,c 为群 G 的元素，证明 $ord(a) = ord(a^{-1}), ord(ab) = ord(ba), ord(a) = ord(cac^{-1})$.

3: 求有理数加法群 $\mathbf{Q}$ 的自同构群 $Aut(\mathbf{Q})$.

二: 进阶 (思考思考)
4: 找出 $(\mathbf{Z}/4\mathbf{Z}, +)$, $(Aut(\mathbf{Z}/5\mathbf{Z}), \cdot\ )$, $(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, +)$ 与 $(Aut(\mathbf{Z}/8\mathbf{Z}), \cdot\ )$ 之间的同构关系.

选做题

5: 对任意整数 $m, n, r > 1$, 存在有限群 G 以及其中的元素 a, b 满足 $ord(a) = m, ord(b) = n, ord(ab) = r$.

必做题 (周五)

一: 基础 (定义验证)
1: 设

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

试求 A, B, AB 和 BA 在 $GL_2(\mathbf{R})$ 中的阶

2: 设 a, b 是群 G 的两个元素,a 的阶是 7 且 $a^3 b = ba^3$. 证明 $ab = ba$.

3:(1) 设 G 是有限阿贝尔群. 证明:

$$\prod_{g \in G} g = \prod_{a \in G, a^2 = 1} a$$

(2) 证明 $Wilson$ 定理: 如果 p 是素数，则 $(p-1)! \equiv -1\ mod\ p$.

4: 证明 $SL_2(\mathbf{Z})$ 可以由

$$S=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}, T=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$$

生成.

二: 进阶 (思考思考)
5: 设 H 和 K 分别是有限群 G 的两个子群,$HgK=\{hgk|h\in H,k\in K\}$. 试证:
$|HgK|=|H|\cdot|K:g^{-1}Hg\cap K|$.

6: 设 A 是群 G 的具有有限指数的子群. 试证: 存在 G 的一组元素 $g_1,g_2,\cdots,g_n$, 它们既可以作为 A 在 G 中的右陪集代表元系, 又可以作为 A 在 G 中的左陪集代表元系.

7: 群论在晶体结构的分类中有着重要应用, 例如二维结晶类对应于 $GL_2(\mathbf{Z})$ 的有限子群 (参见沙法列维奇《代数基本概念》). 我们将分以下几步说明只有有限多个二维结晶类.
(1) 求 $|GL_2(\mathbf{Z}/3\mathbf{Z})|$.
(2) 证明商映射 $\mathbf{Z}\longrightarrow\mathbf{Z}/3\mathbf{Z}$ 诱导的映射 $f:GL_2(\mathbf{Z})\longrightarrow GL_2(\mathbf{Z}/3\mathbf{Z})$ 为乘法群同态且 $Ker(f)=\{A\in GL_2(\mathbf{Z})|\exists B\in M_{2\times2}(\mathbf{Z}),A=I+3\cdot B\}$.
(3) 若 $A\in Ker(f)$ 且 A 的阶有限, 则 $B=0$.(提示: 二项式展开后考虑 3 的指数)
(4)$GL_2(\mathbf{Z})$ 的任意有限子群 G 都同构于 $f(G)$, 从而 $|G|$ 整除 $|GL_2(\mathbf{Z}/3\mathbf{Z})|$(提示: 说明 f 限制在 G 上为单射)
(5) 证明 $GL_2(\mathbf{Z})$ 只有有限多个互不同构的有限子群.

选做题

8:$SO_2(\mathbf{R})$ 的任何有限子群都是循环群.

9:$SL_n(\mathbf{Z})$ 有限生成.

第四次作业

必做题 (周三)

一: 基础 (定义验证)

1: 群 G 的指数为 2 的子群 N 一定是 G 的正规子群.

2: 设 G 为群, 证明以下问题:
(1) 如果 $N\lhd G,N<M,M<G$, 则 $N\lhd M$.
(2) 如果 $N\lhd M$,$M\lhd G$,N 是否一定是 G 的正规子群?
(3) 如果 $K<G,N\lhd G$, 令 $N\vee K$ 表示 G 中包含 N,K 的最小的子群, 证明:
(i)$NK=N\vee K=KN$.(提示:$N\vee K$ 中元素为一些 $n_1k_1\cdots n_rk_r$ 的乘积, 利用 N 的正规性说明可以改写成 nk 的形式)
(ii) 如果 $K\lhd G,N\lhd G$ 且 $K\cap N=\{e\}$, 则对于任意的 $k\in K,n\in N$ 都有 $kn=nk$.
(4) 如果 $K<G,N<G$, 说明 $[N\vee K:N]\geq[K:N\cap K]$.(提示:$[N\vee K:N\cap K]=[N\vee K:K][K:$

$N \cap K]$)

二: 进阶 (思考思考)
3: 共轭作用 σ_g 给出了 $\sigma : G \mapsto Aut(G)$ 的群同态, 其像为 $Inn(G)$.
(1) 证明 $Ker(\sigma) = Z(G)$.
(2) 若 G 有一个阶不为 1 或 2 的元素, 说明 $Aut(G) \neq \{e\}$.(提示: 反证, 得到 $Ker(\sigma) = G$, 从而 $g \mapsto g^{-1}$ 是一个非平凡自同构)

4: 以下证明 pq 阶群 G 非单群.($p > q$, 皆为素数)
(1)G 有 p 阶子群 H.(提示: 选做题 5)
(2)G 至多只有一个 p 阶子群.(提示: 假设另一个为 K, 则 $K \cap H = \{e\}$, 应用第 2 题 (4) 得到矛盾)
(3)H 是正规子群.(提示: 对任意 $g \in G, H \cong gHg^{-1}$, 利用 (2))

选做题

5: 令 G 为 $p^r m$ 阶群 (p 为素数且 $(p, m) = 1$), 我们称 p^r 阶子群 P 为 G 的西罗 p 子群. 以下证明 P 存在:
(1) 若 H, K 为 G 的子群, 定义 H, K 的双陪集为 $HaK = \{hak | h \in H, k \in K\}$, 其中 $a \in G$; 说明存在 G 关于 H, K 的双陪集分解即有 $\{g_i\}_{i=1}^s$ 使得 $G = \bigcup_{i=1}^s Hg_iK$ 且若 $g_i \neq g_j$ 则 $Hg_iK \cap Hg_jK = \{\varnothing\}$.
(2) 利用第三次作业 (周五) 第 5 题证明 $|HgK| = \frac{|H||K|}{|H \cap gKg^{-1}|}$.
(3) 若西罗 p 子群 P 存在, 则对 G 的任意子群 H 有 $g \in G$ 使得 $H \cap gPg^{-1}$ 为 H 的西罗 p 子群.(提示: 利用 (1),(2) 说明存在某个 $g \in G$ 使得 p 不整除 $[H : H \cap gPg^{-1}]$, 从而 $H \cap gPg^{-1}$ 为 H 的西罗 p 子群)
(4) 任意有限群可作为某个 $GL_n(\mathbf{Z}/p\mathbf{Z})$ 的子群.(提示: 矩阵表示)
(5) 令 U 为 $GL_n(\mathbf{Z}/p\mathbf{Z})$ 中主对角线全为 1 的上三角矩阵全体, 说明 U 为西罗 p 子群.(提示: 容易计算 $|U|$, 第二次习题课讲义计算了 $GL_n(\mathbf{Z}/p\mathbf{Z})$)
(6) 利用 (3),(4) 以及 (5) 证明任意有限群 G 存在西罗 p 子群.

必做题 (周五)

一: 基础 (定义验证)

6: 令 $G = \{(a, b) | a \in \mathbf{R}^\times, b \in \mathbf{R}\}$, 乘法定义为

$$(a, b)(c, d) = (ac, ad + b)$$

试证:$K = \{(1, b) | b \in \mathbf{R}\}$ 是 G 的正规子群且 $G/K \cong \mathbf{R}^\times$.

7: 如果 $f : G \mapsto H$ 是满射群同态, 则 G 中包含 $Ker(f)$ 的正规子群一一对应于 H 的正规子群.

8: 设 $G_i (n \geq i \geq 1)$ 为群, 则:
(1)$Z(G_1 \times G_2 \times \cdots \times G_n) = Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n)$:
(2)$G_1 \times G_2 \times \cdots \times G_n$ 为阿贝尔群当且仅当每个 G_i 为阿贝尔群.

9: 如果 $N_1 \lhd G_1, N_2 \lhd G_2$, 则 $N_1 \times N_2 \lhd G_1 \times G_2$ 且 $(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$.

10: 假设已知 $|GL_n(\mathbf{Z}/m\mathbf{Z})|$, 计算 $|SL_n(\mathbf{Z}/m\mathbf{Z})|$.

二: 进阶 (思考思考)

11:(1) 如果 $G/Z(G)$ 是循环群, 则 G 是阿贝尔群.
(2) 试证非阿贝尔群 G 的自同构群 $Aut(G)$ 不是循环群.

12: 求 $GL_n(\mathbf{R})$ 关于 $O_n(\mathbf{R})$ 的右陪集代表元系.(提示: 应用矩阵的 QR 分解)

第五次作业

必做题 (周五)

(a) 每周三交作业, 周五可以补交, 都放在教室最后一排. 电子版在一周内任何时间都可提交; (b) 每周答疑习题课时间为周六下午 14:30-16:00, 地点为 5301; (c) 有不会的题目可以在群里讨论或者和助教讨论; (d) 习题可能会给一些提示, 但是并非只有提示的做法, 能做出来就行, 无需拘泥.
一: 基础 (定义验证)
1: 将置换 $f:\mathbb{Z}_{29}\to\mathbb{Z}_{29}, n\mapsto n^3$ 写成 S_{29} 中两两不相交轮换的积.

2: (1) 设 $\sigma=(i_1i_2\cdots i_r)\in S_n, \tau\in S_n$, 证明 $\tau\sigma\tau^{-1}=(\tau(i_1)\tau(i_2)\cdots\tau(i_r))$;
(2) 设 $\sigma=(i_1i_2\cdots i_n)\in S_n$, 证明 $C_{S_n}(\sigma):=\{\tau\in S_n|\sigma\tau=\tau\sigma\}=<\sigma>$;
(3) $C(S_n)=\{1\}(n\geq 3)$.

3: (1) 设 $N\lhd G$,g 是群 G 的任意一个元素. 如果 g 的阶和 $|G/H|$ 互素, 则 $g\in N$;
(2) 如果 N 是 $S_n(n\geq 3)$ 的指数为 2 的正规子群, 证明其包含所有的 3-轮换.
因此 $A_n(n\geq 2)$ 是 S_n 中唯一的指数为 2 的子群.

4: (1) 确定 S_4 中所有置换的型;
(2) 确定 S_4 的全部正规子群 (注意到正规子群是共轭类的并, 而两个置换共轭当且仅当其有相同的型).
二: 进阶 (思考思考)
5: 证明 S_n 中型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换共有 $n!/\prod_{i=1}^n\lambda_i!i^{\lambda_i}$ 个, 由此证明:

$$\sum_{\lambda_i\geq 0,\lambda_1+2\lambda_2+\cdots n\lambda_n=n}\frac{1}{\prod_{i=1}^n\lambda_i!i^{\lambda_i}}=1.$$

(注意到型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换是对 $\{i_1,i_2,\cdots,i_n\}(\{1,2,\cdots,n\}$ 的一个乱序) 的一个划分, 再除掉重复次数.)

6: (1) 证明 $GL_2(\mathbb{Z}_2)$ 同构于 S_3 (考察 $GL_2(\mathbb{Z}_2)$ 在 $\mathbb{Z}_2\oplus\mathbb{Z}_2=\{(a,b)|a,b\in\mathbb{Z}_2\}$ 的三个非零元上的作用. 当然, 也可以说明 6 阶非交换群只有 S_3, 由 Cauchy 定理知道 6 阶群有 2,3 阶元, 然后正常分析即可);
(2)(选做) 证明 $PGL_2(\mathbb{F}_3)\cong S_4$, 此处 $\mathbb{F}_3$ 是三元域, 实际就是大家熟知的 $\mathbb{Z}_3$(自然的加法和乘法运算).(类似于上一题, 注意到 $\mathbb{F}_3\oplus\mathbb{F}_3$ 有四个一维 $\mathbb{F}_3$-子空间, 记为 $S=\{V_1,V_2,V_3,V_4\}$, $GL_2(F_3)$ 中元素自然给出在 S 上置换, 而且标量矩阵作用平凡, 只需要证明不同的非标量矩阵作用不同再计

算阶数即可);
(3) 证明 $SL_2(\mathbb{Z}_3) \ncong S_4$(尝试说明 $SL_2(\mathbb{Z}_3)$ 的中心非平凡, 而我们知道 $PGL_2(\mathbb{Z}_3)$ 的中心是平凡的, 和第二题 (3) 吻合).

选做题

定义: 称一个群 G 是单群, 如果其没有平凡的正规子群.

8: 旋转群 SO(3) 是单群 (我们在前面的习题证明了 $PSU(2) \cong SO(3)$, 因此利用标准型考虑 $SU(2)$ 或许是一个思路).

7: 如果域 F 有至少四个元素, 则 $SL_2(F)/\{\pm I_2\}$ 是单群 (一般的, $PSL_n(F_p)$ 呢?).

第六次作业

必做题 (周三)

一: 基础 (定义验证)

1: 试证 A_4 没有 6 阶子群.

2: 对 $f(x_1,x_2,x_3,x_4) \in \mathbb{R}[x_1,x_2,x_3,x_4]$, 令 $G_f = \{\sigma \in S_4 | f(x_{\sigma(1)},x_{\sigma(2)},x_{\sigma(3)},x_{\sigma(4)}) = f(x_1,x_2,x_3,x_4)\}$.
(1) 证明 G_f 为 S_4 的一个子群.
(2) 求以下情形的 G_f:
$(i)f = x_1x_2+x_3x_4$, $(ii)f = x_1x_2x_3$, $(iii)f = x_1+x_2$, $(iv)f = x_1x_2x_3x_4$, $(v)f = \prod_{1\le j<i\le 4}(x_i-x_j)$.

3:(1)S_n 可由 $(12),(13),(14),\cdots,(1n)$ 生成.
(2)S_n 可由 $(12),(23),(34),\cdots,(n-1\ n)$ 生成.
(3)S_n 可由 $(12),(123\cdots n)$ 生成.

二: 进阶 (思考思考)

4: 试证:
(1) 对称群 S_n 是交错群 A_{2n} 的子群.
(2) 对称群 S_n 是交错群 A_{n+2} 的子群.(remark: 当 $n \ge 2$ 时 S_n 不为 A_{n+1} 的子群)
(3) 每个有限群均是某个交错群的子群.

5:(1)$|Aut(S_3)| \le 6$.(提示: 利用必做题 3 的 (3), 考虑他们在自同构下的像的可能情况)
(2)$Inn(S_3) \cong S_3$.(提示: 利用第五次作业第 2 题 (3))
(3)$Aut(S_3) \cong S_3$.

6: 令 G 为 S_{999} 的阶为 1111 的循环子群, 证明存在 $i \in \{1,\cdots,999\}$ 使得对任意的 $\sigma \in G$ 都有 $\sigma(i) = i$.(提示: 考虑 G 的生成元的型)

选做题

7:(1) 构造 S_6 的一个不属于 $Inn(S_6)$ 的自同构.
(2) 证明 $n \neq 6$ 时有 $Aut(S_n) = Inn(S_n)$.
(3) 当 $n \neq 2, 6$ 时 $Aut(S_n) \cong S_n$.

必做题（周五）

一: 基础 (定义验证)

8: 若群 G 在集合 S 上的作用是可迁的, 则 G 的子群 N 是正规子群当且仅当任意 S 在 N 的作用下的每个轨道有同样多的元素.(提示: 反过来考虑到左陪集的左乘作用)

9: 二面体群 D_n 是由满足 $ord(a) = n, ord(b) = 2, ba = a^{-1}b$ 的元素 a, b 生成的群，证明以下问题:
(1)$D_2 \cong K_4, D_3 \cong S_3$.
(2) $< a > \lhd D_n, D_n/ < a > \cong Z_2$.
(3)(选做) 找出 D_n 的共轭类以及正规子群.
(4)(选做) 当 n 为奇数时 $Z(D_n)$ 为 e, 当 n 为偶数时 $Z(D_n) \cong Z_2$.
(5)(选做) 若有限群 G 有两个 2 阶元 a, b, 则存在某个自然数 n 使得 $< a, b > \cong D_n$.
.
10:($Burnside\ Lemma$) 设群 G 作用在集合 S 上, 令 t 表示 S 在 G 作用下的轨道条数. 对任意 $g \in G$,$F(g)$ 表示 S 在 g 作用下不动点的个数. 即 $F(g) = |\{x \in S | gx = x\}|$. 试证明:

$$t = \frac{\sum_{g \in G} F(g)}{|G|}$$

这就是说,G 的每个元在 S 上的作用平均使得 t 个文字不动.

11: 集合 $A \subseteq \mathbb{R}^n$ 的旋转群是将 A 映为自身的所有关于原点的旋转构成的群, 而对称群是将 A 映为自身的所有刚体变换构成的群. 求正四面体, 正六面体，正八面体，正十二面体和正二十面体的旋转群和对称群各有多少个元?

二: 进阶 (思考思考)

12: 用四种颜色对正四面体的每个面进行染色, 保证四种颜色均出现且在旋转下相同的染色方案记为同一种，则有多少种不同的染色方案? (提示: 利用第 10, 11 题)

13: 考虑 $SL_2(\mathbb{R})$ 在上半平面 $H = \{z = x + yi | y > 0\}$ 上的作用:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z = \frac{az + b}{cz + d}$$

(1) 验证上述作用为群作用.(需要说明 $gz \in H$)
(2) 证明 $\forall z \in H$, 有 $g \in SL_2(\mathbb{R})$ 使得 $z = gi$ 从而该作用可迁.
(3) 求 i 的稳定子群.
(4) 证明 $SL_2(\mathbb{R})$ 关于 $SO_2(\mathbb{R})$ 的左陪集代表元系与 H 一一对应.(提示:$gSO_2(\mathbb{R}) \mapsto gi, x + yi \mapsto \begin{bmatrix} y^{\frac{1}{2}} & xy^{-\frac{1}{2}} \\ 0 & y^{-\frac{1}{2}} \end{bmatrix} SO_2(\mathbb{R})$)

(5) 证明任意 $g \in SL_2(\mathbb{R})$ 可写成

$$\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix}$$

的形式, 其中 $a > 0, b \in \mathbb{R}, \theta \in [0, 2\pi)$.(提示: 利用 (4))

选做题

14: 对于 $\mathbb{R}^2$ 上的任意内积 $< , >_i$, 考虑 $GL_2(\mathbb{R})$ 在其上的作用:$g < w, v >_i =< gw, gv >_i$, 其中 w, v 为任意向量. 若 G 为 $GL_2(\mathbb{R})$ 的有限子群, 定义 $< w, v >_G = \sum_{g \in G} \frac{g<w,v>}{|G|}$, 其中 $< , >$ 为标准内积.
(1) 说明 $< , >_G$ 为 $\mathbb{R}^2$ 上的内积且存在 $h \in GL_2(\mathbb{R})$ 使得 $< w, v >_G = h < w, v >$.(提示: 欧式空间中的任意内积都有到标准内积的保距同构)
(2) 令 S, S_G 分别为 $< , >, < , >_G$ 的稳定子群, 说明存在 $h \in GL_2(\mathbb{R})$ 使得 $S_G = hSh^{-1}$.
(3) 证明 $\forall g \in G$ 都有 $g < w, v >_G =< w, v >_G$, 从而 g 是关于内积 $< , >_G$ 的正交矩阵.
(4) 利用 (2), (3) 说明存在 $h \in GL_2(\mathbb{R})$ 使得 $hGh^{-1} \subseteq O_2(\mathbb{R})$.
(5) 证明 $SL_2(\mathbb{R})$ 的有限子群为循环群.(提示: 利用 (5) 以及第三次作业选做题 8)
(6) 尝试找出哪些 D_n 可作为 $GL_2(\mathbb{Z})$ 的子群.(提示: 参考第二次习题课讲义问题 4)

第七次作业

必做题 (周三)

一: 基础 (定义验证)

1: 设 p 是一个素数，G 的阶是 p 的方幂。证 G 的非正规子群个数是 p 的倍数。

2: 设 p 是 G 的阶的最小素因子。若有 p 阶子群 $A \lhd G$，则 $A \leq Z(G)$。

3: 设 N 是有限群 G 的正规子群。若素数 p 与 $|G/N|$ 互素，则 N 包含 G 的所有 Sylow p-子群。

4: 设 P 是有限群 G 的 Sylow p-子群。若 $N_G(P) \lhd G$，则 $P \lhd G$。

二: 进阶 (思考思考)

5: 设 G 为有限群，对 $g \in G$，令 C_g 为 g 所在的共轭类，若 $C_g = C_{g^{-1}}$，称 C_g 为一个实共轭类。证 G 只有一个实共轭类当且仅当 G 的阶为奇数。

6: 确定 S_4 的 Sylow 子群。

必做题 (周五)

一: 基础 (定义验证)

7: 设 N 是有限群 G 的正规子群，P 是 G 的 Sylow p-子群。则
(1) $N \cap P$ 是 N 的 Sylow p-子群。
(2) PN/N 是 G/N 的 Sylow p-子群。
(3) $N_G(P)N/N = N_{G/N}(PN/N)$。

8: 设 P 是 G 的 Sylow p-子群，H 是 G 的子群且 $p||H|$，则存在 $a \in G$ 使得 $aPa^{-1} \cap H$ 是 H 的 Sylow p-子群。

9: 证明 24，36，48 阶群非单群。

10: 设 G 为群，$X \subset G$，$G_X = \{g \in G | gX = X\}$。若 $1 \in X$，则 $X \leq G$ 当且仅当 $|X| = |G_X|$。

二: 进阶 (思考思考)

11: 给出 $GL_n(\mathbb{Z}_p)$，$SL_n(\mathbb{Z}_p)$ 的一个 Sylow p-子群，并计算 $GL_n(\mathbb{Z}_p)$ 的 Sylow p-子群的个数。

12：确定 S_4 的自同构群 $Aut(S_4)$。(考虑所有 Sylow 3-子群的集合)

选做题

13: 若有限群 G 的每一个 Sylow 子群都是正规子群，则 G 是它 Sylow 子群的直积。

14: 若 G 为 24 阶群且中心平凡，则 $G \cong S_4$。

第八次作业

必做题 (周三)

一: 基础
1: 若有限群 G 的每一个子群都是正规子群 (Dedekind group), 证明若 $d||G|$, 则 G 有 d 阶子群. 也就是说 Lagrange 定理的逆在 dedekind 群上是成立的, 特别地, 有限阿贝尔群.

2: 证明 $S_n(n \geq 5)$ 没有指数为 i 的子群, 其中 $2 < i < n$. 而且 S_n(任意 n) 的指数为 n 的子群同构于 S_{n-1}(在以前的问题中我们已经知道 $S_n(n \geq 2)$ 指数为 2 的子群只有 A_n).

3: 一般线性群 $GL(n, \mathbb{C})$ 不含有指数有限的真子群.

二: 进阶 (思考思考)
4: 我们已经知道最小的非阿贝尔单群阶数为 60, 实际上其同构于 A_5. 设 G 为 60 阶单群, 试证明:
(1)G 没有指数为 4 的子群, 进而 G 的 Sylow 2-group 的个数不能为 3;
(2)G 有 12 阶子群;
(3)G 同构于 A_5.

5: 试证有限群 G 的一个真子群的全部共轭子群不能覆盖整个群 G. 该结论对无限群不成立, 能否举出一例? (可以考虑线性代数的例子)

必做题（周五）

一: 基础

1:(1) 设 $G = G_1 \times G_2 \times \cdots \times G_n$,$H$ 是 G 的子群.H 是否形如 $H = H_1 \times H_2 \times \cdots \times H_n$? 其中 H_i 是 G_i 的子群,$1 \leq i \leq n$.

(2) 令 $G = G_1 \times G_2 \times \cdots \times G_n$, 且对于任意的 $i \neq j$,$|G_i|$ 和 $|G_j|$ 互素. 证明 G 的任意子群 H 都是它的子群 $H \bigcap G_i (1 \leq i \leq n)$ 的直积.

(3) $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ 当且仅当 $(m, n) = 1$.

2: 试证 20230501 阶群是循环群.

3: 设 p 是一素数.

(1) 证明 $p^n, n \geq 1$ 阶群有非平凡的中心.

(2) 分类 p^2 阶群.

(3) 利用群的表现证明总存在 p^3 阶非阿贝尔群.

4: 令 $G = \langle x_i, i \in \mathbb{Z}_{>0} | \, x_n^n = x_{n-1}, n > 1 \rangle$, 证明 $(G, \cdot) \cong (\mathbb{Q}, +)$.

定义: 设 S 是任意集合, 表现为

$$F = \langle S | ab = ba, \forall a, b \in S \rangle$$

的群叫做以 S 为基的自由阿贝尔群 (除了交换性条件外没有其他条件). 我们可以证明 $F \cong \oplus_{a \in S} \mathbb{Z}$(群的直和).

5: 给定生成元 $X = \{x_0, x_1, \cdots, x_n, \cdots\}$, 令 F 是 X 上的自由阿贝尔群,R 为包含 $\{px_0, x_0 - px_1, x_1 - px_2, \cdots, x_{n-1} - px_n, \cdots\}$ 的最小正规子群,p 为一素数,$G = F/R$, 记 $a_n = x_n + R$.

(1) 证明:$\forall x \in G, \exists n \geq 0$ 使得 $p^n x = 0$.

(2) $a_n \neq 0, \forall n \geq 0$ 且所有的 a_n 是互异的, 从而 G 是一个无限群.

(3) 证明 G 的每个真子群都是有限循环群.

(4) 对于每一个正整数 n,G 有唯一的 p^n 阶子群.

(5) 令 $U_p = \{e^{\frac{2\pi ik}{p^n}} | k \in \mathbb{Z}, n \geq 0\} \leq \mathbb{C}$ 是所有 p^n 次单位根构成的乘法群, 证明 $G \cong U_p$.

我们将上述群 G 记为 $\mathbb{Z}(p^\infty)$.

思考:4,5 两题的描述有何异同? $Z(p^\infty)$ 和 $\mathbb{Q}$ 有何联系? 不用做.

二: 进阶

6: (1) (A_{n-1} 型 Coxeter group) 证明 S_n 与下述群同构:

$$\langle x_1, x_2, \cdots x_{n-1} | \, x_i^2 = (x_j x_{j+1})^3 = (x_k x_l)^2 = 1, 1 \leq i \leq n-1, 1 \leq j \leq n-2, 1 \leq l < k-1 < n-1 \rangle.$$

(2) 令 $A = (a_{ij}), 1 \leq i, j \leq n-1$, 其中 $a_{ij} = -cos(\frac{\pi}{m_{ij}})$,$m_{ij}$ 是 (1) 中群内元素 $x_i x_j$ 的阶. 证明 A 是正定矩阵.

7: 令 $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, 我们在第三次作业证明了 A, B 是 $SL_2(\mathbb{Z})$ 的一组生成元. 令 $C = AB^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$, 则 $SL_2(\mathbb{Z})$ 也可以由 A, C 生成. 因此我们有自然群同态 $f : \langle x, y | x^4 = 1, x^2 = y^3 \rangle \to SL_2(\mathbb{Z}) (x \mapsto A, y \mapsto C)$ 并且 f 诱导出群同态 $g : \langle x, y | x^2 = y^3 = 1 \rangle \to PSL_2(\mathbb{Z})$.

(1) 证明 $\langle x,y|x^4=1,x^2=y^3\rangle \cong \langle a,b|aba=bab,(aba)^4=1\rangle$.
(2) 证明 f 是单射当且仅当 g 是单射, 证明 f 是满射当且仅当 g 是满射.
(3) 尝试证明 f 和 g 都是群同构.

选做题

8: 尝试给出 A_n 的一个表示.

9: 设 G 是一个无限阿贝尔群.
(1) 若 G 的每一个真子群是有限群, 则存在素数 p 使得 $G \cong \mathbb{Z}(p^\infty)$.
(2) 若 G 同构于每一个真子群, 则 $G \cong \mathbb{Z}$.
(3) 若 G 同构于每个非平凡商群, 则 $G \cong \mathbb{Z}(p^\infty)$.
(4) 若 G 的每个非平凡商群是有限的, 则 $G \cong \mathbb{Z}$.

第九次作业

必做题（周五）

一: 基础 (定义验证)

1:(1)$n \geq 3$ 时,$A_n \times \mathbb{Z}_2$ 是否同构于 S_n.
(2) 若 n 为奇数, 证明:$D_{2n} \cong D_n \times \mathbb{Z}_2$.

2:(1)$G =< x,y|x^5y^3 = x^8y^5 = 1 >$,$G$ 是否平凡.
(2)$G =< x,y|ab^3 = b^2a, a^2b = ba^3 >$,$G$ 是否平凡.

3: 设 $\mathbb{Q}^+$ 是正有理数乘法群, 试证:
(1)$\mathbb{Q}^+$ 是自由阿贝尔群.
(2)$\mathbb{Q}^+$ 不是有限生成的.

4: 设 $\mathbb{Q}$ 是有理数加法群, 试证:
(1)$\mathbb{Q}$ 不是自由阿贝尔群.
(2)$\mathbb{Q}$ 的任意有限生成的子群都是循环群，但 $\mathbb{Q}$ 不是循环群.

二: 进阶 (思考思考)

5: 令 F_2 为集合 y_1, y_2 生成的自由群:
(1) 考虑自同态 $f: y_1 \mapsto y_2, y_2 \mapsto y_1y_2$, 令 $|*|$ 表示 F_2 中字的长度, 例如 $|y_1y_2| = 2$, 证明 $lim_{k\to\infty}\frac{|f^{k+1}(y_1)|}{|f^k(y_1)|} = \lambda$, 其中 $\lambda = \frac{1+\sqrt{5}}{2}$.
(2) 证明 F_2 中关于每个 y_i 的指数和都能被 n 整除的所有字全体 N 构成正规子群.
(3)$F_2/N \cong \mathbb{Z}_n \times \mathbb{Z}_n$.(提示: 需要考虑换位子)

6:(1) 设 G 是有限生成自由阿贝尔群,$rank(G) = r$. 如果 $g_1, \cdots, g_n$ 是 G 的一组生成元, 则 $n \geq r$.
(2) 令 G 为 $\{x_i\}_{i=1}^n$ 生成的阿贝尔群, 证明 G 的任意子群 H 最多由 n 个元素生成.(提示: 若 $H \subset < x_2, \cdots, x_n >$, 归纳知成立. 若不然, 取 H 的元素 $x = m_1x_1 + \cdots + m_nx_n$, 其中 $m_1 > 0$ 且最小, 说明 $H =< x, K >, K = H \cap < x_2, \cdots, x_n >$).

(3)(选做) 令 F 为 $\{a_i\}_{i=1}^m$ 生成的自由阿贝尔群. 令 K 为 $b_1 = r_{11}a_1 + r_{1m}a_m, \cdots, b_n = r_{n1}a_1 + r_{nm}a_m$ ($r_{ij} \in \mathbb{Z}$) 生成的子群
(i) 对任意 i,$\{b_1, \cdots, b_{i-1}, -b_i, b_{i+1}, \cdots, b_n\}$ 与 $\{b_1, \cdots, b_{i-1}, b_i + rb_j, b_{i+1}, \cdots, b_n\}(r \in \mathbb{Z}, i \neq j)$ 都能生成 K.
(ii) 对任意 i,F 可由 $\{a_1, \cdots, a_{i-1}, -a_i, a_{i+1}, \cdots, a_n\}$ 生成, 此时 K 由 $\{b_j = r_{j1}a_1 + \cdots + r_{j,i-1}a_{i-1} - r_{ij}(-a_i) + r_{j,i+1}a_{i+1} + \cdots + r_{jm}a_m\}$ 生成.
(iii) 对任意 i 以及 $j \neq i$,$\{a_1, \cdots, a_{j-1}, a_j - ra_i, a_{j+1}, \cdots, a_m\}(r \in \mathbb{Z})$ 可生成 F, 此时 K 由 $\{b_k = r_{k1}a_1 + \cdots + r_{k,i-1}a_{i-1} + (r_{ki} + rr_{kj})a_i + r_{k,i+1}a_{i+1} + \cdots + r_{k,j-1}a_{j-1} + r_{kj}(a_j - ra_i) + r_{k,j+1}a_{j+1} + \cdots + r_{km}a_m\}$.
(iv) 若记矩阵 $A = (r_{ij})$, 其表示 F 在某组基下 K 的生成元. 说明 (i)(ii)(iii) 描述的是 F 以及 K 在 A 的初等行列变换下不变.
(4)(选做) 证明如下定理: 设 G 是有限生成自由阿贝尔群,H 为 G 的非零子群, 则 H 也是有限生成自由阿贝尔群且 $rank(H) \leq rank(G)$. 更具体地说, 存在 G 的一组基 $\{x_1, x_2, \cdots, x_n\}$, 正整数 $r \leq n$, 正整数 $d_1|d_2|\cdots|d_r$, 使得 H 是以 $\{d_1x_1, d_2x_2, \cdots, d_rx_r\}$ 为基的自由阿贝群.(提示: 利用 (2),(iv) 以及第二次习题课讲义 $Lemma1$ 也即 A 可经过初等行列变换化为对角矩阵.)
(5)(选做)(i) 若 $rank(F) = 3$,$b_1 = 9a_1 + 3a_2 + 6a_3, b_2 = 3a_1 + 3a_2, b_3 = 3a_1 - 3a_2 + 6a_3$. 将商群 F/K 写成循环群的直和.
(ii) 证明商群 F/K 有限当且仅当 $det(A) \neq 0$, 此时 $|F/K| = |det(A)|$.

必做题 (周六)

7: 判断以下命题是否成立, 若不然则给出反例:
(1)$H_1 \times H_2 \cong K_1 \times K_2$,$H_1$ 与某个 K_i 同构.
(2) 以下 $H_i \lhd G_i$ $(i = 1, 2)$:
(i) 如果 $G_1 \cong G_2$ 并且 $H_1 \cong H_2$, 则 $G_1/H_1 \cong G_2/H_2$.
(ii) 如果 $G_1 \cong G_2$ 并且 $G_1/H_1 \cong G_2/H_2$, 则 $H_1 \cong H_2$.
(iii) 如果 $H_1 \cong H_2$ 并且 $G_1/H_1 \cong G_2/H_2$, 则 $G_1 \cong G_2$.

8:$S_3, \mathbb{Z}, \mathbb{Z}_{p^n}$ $(n \geq 1, p\ prime)$ 都不能写成它们真子群的直积.

9: 自由阿贝尔群 $\{F_i\}_{i\in I}$ 的直和 $\oplus_{i\in I}F_i$ 是自由阿贝尔群.(remark: 该结论对直积不一定成立.)

10: 设 $G = G_1 \times G_2, H \lhd G$ 且 $H \cap G_i = \{1\}, i = 1, 2$. 试证 $H \leq Z(G)$. 特别的,H 是阿贝尔群.(三百题原题)

11:(1) 自由阿贝尔群 F 是自由群当且仅当其是循环群.
(2) 有限生成阿贝尔群 G 是有限群当且仅当 G 的一组生成元均是有限阶元.(三百题原题)
(3) 有限生成阿贝尔群 G 是自由阿贝尔群当且仅当 G 的每个非零元都是无限阶元.(三百题原题)

二: 进阶 (思考思考)

12: 令 $G =< g_1, g_2, \cdots, g_n >$. 如果 G 的子群 A 具有有限指数 m, 则 A 可以由 $2nm$ 个元素生成.(三百题原题)

13: 设 G_1 和 G_2 是非交换单群, 试证明 $G_1 \times G_2$ 的非平凡正规子群只有 G_1 和 G_2.(三百题原题)

选做题

13: 若 A, B, C 为阿贝尔群, 试赋予 $Hom(A, B)$ 阿贝尔群结构, 并解决以下问题:
(1) 求 $Hom(\mathbb{Z}_m, \mathbb{Z}_n), Hom(\mathbb{Z}_m, \mathbb{Q}), Hom(\mathbb{Z}, A), Hom(\mathbb{Z}_m, \mathbb{Q}/\mathbb{Z})$.
(2) 证明 $Hom(A \oplus B, C) \cong Hom(A, C) \oplus Hom(B, C)$ 以及 $Hom(C, A \oplus B) \cong Hom(C, A) \oplus Hom(C, B)$.
(3) 求 $Hom(\mathbb{Z}_{114} \oplus \mathbb{Z}_{514}, \mathbb{Z}_{1919} \oplus \mathbb{Z}_{810})$.

14: 设 N, H 为群, 给定群同态 $\theta : H \mapsto Aut(N)$. 定义它们的半直积为 $G = N \rtimes_\theta H$ 为如下定义的群:
(i) 作为集合 G 为 $N \times H$.(ii) 二元运算为:$(n_1, h_1)(n_2, h_2) = (n_1\theta(h_1)(n_2), h_1h_2)$, 其中 $n_i \in N, h_i \in H$.
(1) 验证 $N \rtimes_\theta H$ 为群且 $G/N \cong H$.
(2) 若 H 为 G 的子群,N 为 G 的正规子群, 且满足 $G = NH, H \cap N = \{e\}$, 则 $G = N \rtimes_\theta H$, 其中 θ 为共轭.
(3) 构造 θ 使得 $D_n \cong \mathbb{Z}_n \rtimes_\theta \mathbb{Z}_2$ $(n \geq 2)$,$S_n = A_n \rtimes_\theta \mathbb{Z}_2$ 以及构造非交换 p^3 阶群 (有或者没有 p^2 阶元素).

第十次作业

必做题 (周三)

一: 基础
1: 在同构意义下给出所有 108 阶交换群。

2: 若 m, n 互素，证明 $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$，当 m, n 不互素时，$\mathbb{Z}_m \oplus \mathbb{Z}_n$ 不变因子为 $(m, n), [m, n]$。

二: 进阶 (思考思考)
3: 设 H 是有限阿贝尔群 A 的子群，则有 A 的子群同构于 A/H。

4: 设 A 为有限阿贝尔群，则对 $|A|$ 的每个正因子 d，A 都有 d 阶子群和 d 阶商群。

选做题

1: 设 G 为有限交换 p-群，若 G 只有一个 p 阶子群，则 G 为循环群。

2: 设 G 为有限交换 p-群，若 G 只有一个指数为 p 的子群，则 G 为循环群。

3: 设 G 为有限 p-群，若 G 只有一个指数为 p 的子群，则 G 为循环群。

必做题 (周五)

一: 基础 (定义验证)

5: 证明对于含幺环，加法适合交换律可由定义中其他条件给出。

6: 对于下列情形，各给一个例子。
(1) 既无左单位元也无右单位元。
(2) 只有左单位元，无右单位元。
(3) 只有右单位元，无左单位元。

二: 进阶 (思考思考)

7: 对于下列情形，各给一个例子。
(1) 环 R 有单位元，但一个子环 S 无单位元。
(2) 环 R 无单位元，但一个子环 S 有单位元。
(3) 环 R 及其一子环有单位元，但单位元不同。

8: 设 $\mathbb{F}$ 为数域, $M_n(\mathbb{F})$ 为 $\mathbb{F}$ 上的 n 阶全矩阵环, 则 $A \in M_n(\mathbb{F})$ 为左零因子当且仅当 A 为右零因子。

选做题

4: 分类 18 阶群。

5: 设 R 为含幺环，若 $a, b \in R$，且 $a, b, ab-1$ 都可逆，则 $ba-1, a-b^{-1}, (a-b^{-1})^{-1}-a^{-1}$ 也可逆。

第十一次作业

必做题 (周三)

一: 基础
1: 设 R 是一不含幺元素的环, 考虑集合 $S = R \times \mathbb{Z}$, 定义 S 上两种运算: $(r_1, n_1) + (r_2, n_2) = (r_1 + r_2, n_1 + n_2), (r_1, n_1)(r_2, n_2) = (r_1 r_2 + n_2 r_1 + n_1 r_2, n_1 n_2)$. 试证明 S 对于如此定义的加法和乘法是含幺环.

2: 设 G 是阿贝尔群,$End(G)$ 是群 G 的全部自同态构成的集合. 对于 $f, g \in End(G)$, 定义 $(f+g)(a) = f(a) + g(a), (f \cdot g)(a) = f(g(a)), a \in G$. 求证 $End(G)$ 对于上述运算是含幺环.

3: (1) 证明有限整环是域;
(2) $\mathbb{Z}_m$ 什么时候是整环,i.e, 域.

4: (1) 求证 $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ 是实数域 $\mathbb{R}$ 的子域;
(2) 求 $\mathbb{Z}_m$ 的全部子环;
(3) 求 $\mathbb{Q}[\sqrt{2}]$ 的全部子域.

二: 进阶
5: 含幺环中某元素若有至少两个右逆, 则它必然有无限多个右逆.

6: 设 a,b 都是含幺环 R 中的元, 则 $1-ab$ 可逆当且仅当 $1-ba$ 可逆.

三: 选做
1:$\mathbb{R}$ 上的有限维可除结合代数只有三种 $\mathbb{R},\mathbb{C},\mathbb{H}$. 非结合代数呢?

必做题 (周五)

一: 基础
7: 对任何幺环 S 和环同态 $f:R\to S$, 证明 f 可以唯一地分解为 $R\xrightarrow{i}R\times\mathbb{Z}\xrightarrow{g}S$,$g((0,1))=1_S$. 此处 $R\times\mathbb{Z}$ 是我们第一题定义的环,$i:R\to R\times\mathbb{Z},r\mapsto(r,0)$ 是环嵌入.

8: 令 $L=\left\{\begin{pmatrix} z & w \\ -\bar{w} & \bar{z}\end{pmatrix}\in M_2(\mathbb{C})|z,w\in\mathbb{C}\right\}$, 证明 L 是除环且其同构于实四元数体 (课堂讲过).

9:(1) 给出环的非零环同态 $f:R\to S$ 的例子, 使得 $f(1_R)\neq 1_S$.
(2) 给出一个环同态 $f:R\to S$ 的例子, 使得 R 中可逆元不映成 S 中可逆元.
(3) 如果 $f:R\to S$ 是含幺环之间的环满同态, 则 $f(1_R)=1_S$.
(4) 如果 $f:R\to S$ 是含幺环之间的环同态,u 是 R 中的可逆元, 且 $f(u)$ 也是 S 中的可逆元, 则 $f(1_R)=1_S$, 且 $f(u)^{-1}=f(u^{-1})$.

10: (1) 若 I,J 是环 R 的理想, 证明 $IJ,I\bigcap J$ 也是环 R 的理想, 且 $IJ\subset I\bigcap J$. 举例说明该包含关系可能是真包含, 也可能是相等.
(2) 证明 $I+J$ 是 R 中包含 I 和 J 的最小的理想.
(3) 若 I,J,K 是环 R 的理想, 证明 $(IJ)K=I(JK)$. 分配率 $I(J+K)=IJ+IK$ 是否成立?

二: 进阶
11: 设 I 是 R 的一个理想, 令 $M_n(I)$ 表示元素都位于 I 中的 n 阶方阵.
(1) 证明 $M_n(I)$ 是 $M_n(R)$ 的理想.
(2) 若 J 是 $M_n(R)$ 的理想, 令 $E(J)$ 是 J 中所有矩阵的所有位置的元素构成的集合, 证明 $E(J)$ 是 R 的理想且 $J=M_n(E(J))$.
(3)$I\mapsto M_n(I)$ 给出了一个从 R 的全体理想集合到 $M_n(R)$ 的全体理想集合的双射.

三: 选做 (可阅读)
2:(1) 设 R 是一含幺环,$f:R\to\mathbb{Z}$ 是任意一个幺环同态 $f(1_R)=1$. 证明作为群, 有同构 $R\cong kerf\oplus\mathbb{Z}$.
(2) $\varphi:R\to kerf\oplus\mathbb{Z},r\mapsto(r-f(r)1_R,f(r))$ 给出一个群同构. 我们可以给 $kerf\oplus\mathbb{Z}$ 赋予环结构使得 φ 是环同构, 即满足 $\varphi(r_1r_2)=\varphi(r_1)\varphi(r_2)$, 请给出 $kerf\oplus\mathbb{Z}$ 上的乘法结构满足上述性质. 你发现了什么? 1:$\mathbb{R}$ 上的有限维可除结合代数只有三种 $\mathbb{R},\mathbb{C},\mathbb{H}$. 非结合代数呢?

第十二次作业

周三

Warning: 标有*(必做)*的题目必做, 余下选做. 每题的大问用蓝色标注以便于区分, 必做部分大都改编自三百题.

1(必做): 说明每组环 (代数) 是否同构:
(a)$\mathbb{Z}[x]/(x^2-2), \mathbb{Z}[x]/(x^2-3)$.
(b)$\mathbb{C}[\mathbb{Z}_2], \mathbb{C}\times\mathbb{C}$.(可以思考幂等元是什么)
(c)$\mathbb{Z}[x]/(x^2-3, 2x+4), \mathbb{Z}_2[x]/(x^2)$.

2(必做): 除环相关的讨论:
(a)若非平凡含幺有限环 R 没有零除子, 则 R 为除环.
(b)证明除环 K 是单环, 从而任意环同态 $f: K\mapsto R$, 要么 $f=0$, 要么 f 是单射.($M_n(K)$ 是否也单呢?)
(c)令 m 为非平凡环 R 的理想, 若 R/m 为除环, 则 m 是极大理想.
(d)(选做) 非平凡含幺环 R 为除环当且仅当 R 没有真左理想.(提示: 反过来说明元素右可逆需要用到第二次作业第 4 题)
(e)(选做) 只有有限多个自同构的除环是域.

3(必做):
(a)(i) 若 R 是主理想环, 则 R 的每个同态像也是主理想环.
(ii) 当 $m>0$ 时,$\mathbb{Z}_m$ 是主理想环.
(iii) 设 $f: R\mapsto S$ 是环的满同态 (特别的,S 为 R 的商环), 求证:
(1) 若 P 是 R 的素理想并且 $Ker(f)\subseteq P$, 则 $f(P)$ 也是 S 的素理想.
(2) 若 Q 是 S 的素理想, 则 $f^{-1}(Q)$ 也是 R 的素理想.
(3)S 中素理想与 R 中包含 $Ker(f)$ 的素理想一一对应.
将素理想改为极大理想则以上论断皆成立.
(iv) 当 $m\geq 2$ 时确定 $\mathbb{Z}_m$ 的全部素理想与极大理想.(提示: 利用以上或者 6(c)(i))
(b)求 $\mathbb{C}[[x]]$ 的全部理想 (并选做求 $\mathbb{Z}[x]$ 的极大理想).
(c)(选做) 以下假设 R 为含幺交换环, 若 R 只有唯一极大理想, 则称其为局部环, 解决以下问题:
(i)R 为局部环当且仅当其不可逆元构成理想, 试举出一个局部环的例子.
(ii)R 为局部环当且仅当 $M_n(R)$ 为局部环.(能得到关于 $M_n(\mathbb{C}[[x]])$ 的什么性质呢?)
(iii) 若 m 为极大理想, 则对任意正整数 n 有 $R/(m^n)$ 为局部环.(比如 $\mathbb{Z}_{p^n}$)

4(必做): 极大理想与素理想相关讨论:
(a)(i) 含幺环 R 的子集 S 若满足 $1\in S, 0\notin S$ 且 S 在乘法下封闭则称 S 为乘法子集. 说明若理想 I 为满足 $I\cap S=\emptyset$ 的所有理想中的极大元, 则 I 为素理想.
(ii)(选做) 令 T 为含幺交换环 R 中 0 以及所有零除子构成的子集, 说明 T 至少包含一个素理想.(利用 (i))
(b)令 R 为含幺交换环, 则真理想 m 为极大理想当且仅当对任意 $r\notin m, \exists x\in R$ 使得 $1-rx\in m$.(提示:R/m 为域)
(c)(i) 在环 $4\mathbb{Z}$ 中考虑极大理想 (8), 说明 $4\mathbb{Z}/(8)$ 不是域.
(ii) 设 I 是含幺交换环 R 中的理想, 求证有环同构:$M_n(R)/M_n(I)\cong M_n(R/I)$. 利用此说明 $M_2(p\mathbb{Z})$ 是 $M_2(\mathbb{Z})$ 的极大理想, 但 $M_2(\mathbb{Z})/M_2(p\mathbb{Z})$ 不是域.
(d)(i) 若 R 为含幺环, 则 R 的极大理想为素理想.R 不含幺时是否成立呢?
(ii) 含幺交换有限环 R 的素理想 I 必为极大理想.

5(必做): 设 R 为含幺交换环,S 为 R 的乘法子集, 定义 $S^{-1}R=\{\frac{t}{s}|t\in R, s\in S\}/\sim$, 其中等价关系 $\sim$ 定义为:$\frac{t}{s}\sim\frac{t'}{s'}\Leftrightarrow\exists u\in S, s.t.\ ust'=uts'$. 定义 $S^{-1}R$ 的环结构为:$\frac{t}{s}\frac{t'}{s'}=\frac{tt'}{ss'}, \frac{t}{s}+\frac{t'}{s'}=\frac{ts'+st'}{ss'}$.
(a)说明 $S^{-1}R$ 为环.(验证良定义即加法和乘法不依赖于代表元的选取).
(b)(选做) 验证 $\phi_S: R\mapsto S^{-1}R, r\mapsto\frac{r}{1}$ 为环同态. 并说明 R 为整环时 ϕ_S 为单射且 $S^{-1}R$ 也为整

环，若取 $S=R-0$,$S^{-1}R$ 是什么呢? 两个整环同构是否等价于商域同构呢?
(c)(选做)(i)$S^{-1}R$ 的素理想具有形式 $S^{-1}P=\{\frac{p}{s}|p\in P,s\in S\}$, 其中 P 为 R 中素理想.
(ii)R 中与 S 不交的素理想一一对应与 $S^{-1}R$ 中的素理想并说明 $S=R-P$ 时 $S^{-1}R$ 是局部环.
(d)(选做) 求 $\mathbb{Q}$ 所有的含幺子环.($S^{-1}\mathbb{Z}$,S 为 $\mathbb{Z}$ 的乘法子集)

6:$nilpotent, radical\ and\ semisimple$:
(a)(必做)环 R 中元素 a 称为幂零的，是指存在正整数 m 使得 $a^m=0$.
(i) 若 R 为交换环,a 和 b 均为幂零元, 则 $a+b$ 也是幂零元.R 非交换时是否成立呢?
(ii) 交换环 R 中幂零元的集合 $nil(R)$ 是 R 的理想, 且商环 $R/nil(R)$ 中无非平凡幂零元.
(iii) 设 I 是交换环 R 中的理想, 求证集合 $\sqrt{I}=\{r\in R|\exists n\geq 1, r^n\in I\}$ 也是环 R 的理想. 并说明 $\sqrt{0}$ 是什么?
(iv)(选做) 含幺交换环中 $\sqrt{I}=\cap_{I\subset P}P$, 其中 P 皆为素理想.
(v) 若 x 为含幺交换环 R 中幂零元, 则 $1+x$ 可逆, 由此说明幂零元与可逆元的和依旧可逆.
(vi)(选做) 考虑含幺交换环 R 的多项式环 $R[x]$, 取 $f=\sum_{i=0}^{n}a_ix^i\in R[x]$.
(1)f 在 $R[x]$ 中可逆等价于 a_0 可逆且 $a_1,\cdots,a_n$ 幂零.
(2)f 幂零等价于 a_i 皆幂零.
(b)环 R 中的理想 J 称为幂零的, 是指存在正整数 n 使得 $J^n=0$.
(i) 若 J 为含幺交换环 R 的幂零理想, 说明 $f: GL_n(R)\mapsto GL_n(R/J)$ 是满射且 $Ker(f)=I+M_n(J)$.
(ii) 求 $GL_n(\mathbb{Z}_{p^m})$ 的阶.(第三次习题课用类似方法也计算过)
(c)(必做)
(i) 设 $R_i(i\in I)$ 是一个非空环族,$R=\prod_{i\in I}R_i$. 求证:
(1)R 为含幺环当且仅当每个 R_i 为含幺环.
(2)R 为交换环当且仅当每个 R_i 为交换环.
(3)$x=(x_i)$ 是 R 中可逆元当且仅当每个 x_i 均为 R_i 中可逆元.
(4) 若 R 为含幺环且 I 有限, 则 R 中理想 A 均形如 $I=\prod_{i\in I}A_i$, 其中每个 A_i 是 R_i 的理想.(假如含幺环 R 可写成理想的和, 那么理想个数是否有限呢?)
(ii) 对于含幺环 R,S，证明 $M_2(R\times S)\cong M_2(R)\times M_2(S)$. 并据此以及 (i),(b), 第四次作业 10 求 $SL_2(\mathbb{Z}_n)$ 的阶.
(d)令 $rad(R)$ 为含幺环 R 的所有极大左理想的交, 说明 $y\in rad(R)$ 当且仅当对于任意 $x\in R$ 都有 $1-xy$ 左可逆.
(i)(必做)求 $rad(\mathbb{Z}_n), nil(\mathbb{Z}_n), rad(\mathbb{C}[[x]]), nil(\mathbb{C}[[x]])$.
(ii) 令 T 为 $M_n\mathbb{C}$ 中所有上三角矩阵构成的子环, 求 $rad(T)$ 以及 $T/rad(T)$.
(iii) 对于含幺环 R 证明 $rad(M_n(R))=M_n(rad(R))$.
(iv) 对于含幺交换环 R, 证明 $rad(R[x])=nil(R[x])$.(参考 (a)(vi))
(v) 含幺环 R 的左理想 J 幂零, 则 $J\subset rad(R)$.
(vi) 对于含幺环 R,$rad(R/rad(R))=0$. 将理想 I 视作子环则有 $rad(I)=I\cap rad(R)$.
(e)(必做)
(i) 环 R 的左理想 $I\neq 0$ 称为极小左理想若其不包含 R 的其他非零左理想. 举例说明不是所有环都有极小左理想.(比如 $\mathbb{Z}$)
(ii) 令 $soc(R)$ 为 R 的所有极小左理想的和. 求 $soc(\mathbb{Z}_n)$ 并选做求 $soc(M_n(K)), K$ 为除环.(提示: 若 $n=st$, 则有群同构 $s\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}/t\mathbb{Z}$)
(iii)(选做) 环 R 为整环, 则 R 为域当且仅当 $soc(R)\neq 0$.
(f)(i) 若环 $R=soc(R)$, 则称其为左半单环, 说明以下等价:
(1)R 左半单.
(2)R 可写成极小左理想的直和.

(3)R 的任意左理想为其直和项.
(ii)(必做)试求 $\mathbb{Z}_n$ 为左半单环的充分必要条件, 计算此时的 $rad(\mathbb{Z}_n)$ 并将 $\mathbb{Z}_n$ 写成一些除环的直积.
(iii) 环 R 左半单当且仅当 $rad(R)=0$ 且 R 左 $Artin$.
(iv) 环 R 左半单当且仅当 $M_n(R)$ 左半单.(能得到 $M_n(K), K$ 为除环的什么性质?)
(v)(Maschke 定理) 对于有限群 G, 说明 $\mathbb{C}[G]$ 半单.
(vi)(Wedderburn-Artin 定理) 环 R 左半单则 $R\cong M_{n_1}(K_1)\times\cdots\times M_{n_r}(K_r)$, 其中 n_i 为正整数,K_i 为除环.(推广了 6(f)(ii))

第十三次作业

必做题（周三）

一: 基础
1: 设 R 为环, 称 N 为 R 的一个诣零理想, 若 $\forall a\in N$ 存在正整数 n，使得 $a^n=0$。
（1）N 为 R 的一个诣零理想, 则 R 诣零当且仅当 R/N 诣零。
（2）R 的两个诣零理想之和仍为诣零理想。

2: 设 R 为 UFD，则 R 中每一个非零素理想均包含一个非零主素理想。

3: 设 R 为 UFD,$a,b\ c\in R-\{0\}$ 则
（1）ab 与 $(a,b)[a,b]$ 相伴。
（2）若 $a|bc,(a,b)=1$，则 $a|c$。

4：设 R 为 PID, 证明
（1）$(a)\cap(b)=([a,b])$, 且 $(a)\cap(b)=(a)(b)$ 当且仅当 $(a,b)=1$。
（2）方乘 $ax+by=c$ 在 R 中有解当且仅当 $(a,b)|c$。

二: 进阶
5: 设 R 为环,P 为 R 的一个素理想。
（1）$S_P=R-P$ 为一个乘性子集。
（2）$S_P^{-1}R$ 有唯一极大理想 $S_P^{-1}P$。

6: 设 R 为含幺整环，$|R|>1$，则 R 为域当且仅当 $R[x]$ 为主理想环。

必做题（周五）

一: 基础
7: 主理想环 R 中元素 $a_1,\cdots,a_n$ 互素当且仅当存在 $b_1,\cdots,b_n\in R$ 使得 $a_1b_1+\cdots+a_nb_n=1$。

8: 设 $a_1,\cdots,a_n$ 是唯一因子分解整环 R 的非零元素，若 $a_1=db_1,\cdots,a_n=db_n\in R$，则 $(a_1,\cdots,a_n)=d$ 当且仅当 $(b_1,\cdots,b_n)=1$。

9: 设 p 是唯一因子分解整环 R 的素元，则 p 也是 $R[x]$ 的素元。

二: 进阶
10: 设 R 是一个无零因子交换环，若有一个 R^* 到非负整数集的映射 ϕ 满足，

(i) 对 R 中任意元素 a 及 $b \neq 0$，有 $q, r \in R$ 使得 $a = bq + r$，$r = 0$ 或 $\phi(r) < \phi(b)$。
(ii) 对 R 中任意非零元素 a, b 有 $\phi(ab) \geq \phi(a)$。
则称 R 为一个 V 欧式环。下面设 R 为一个 V 欧式环。
(1)R 的理想必为主理想。
(2)R 必有单位元从而是欧式环。
(3)(选做) 对欧式环可定义一个映射使其为 V 欧式环。

11:(选做) 设 $\mathbb{Z}[i]$ 为高斯整环，
(1)$\mathbb{Z}[i]/(m + ni)$ 有 $m^2 + n^2$ 个元素。
(2)$\mathbb{Z}[i]/(m + ni) \cong \mathbb{Z}_{m^2+n^2}$ 当且仅当 $(m, n) = 1$。
(3) 当 $mn \neq 0$ 时，$m + ni$ 是素元当且仅当 $m^2 + n^2$ 为素数。
(4) 当 $mn = 0$ 时，$m + ni$ 是素元当且仅当 $|m + ni|$ 为素数且 $4||m + ni| - 3$。

第十四次作业

一: 基础
0: 有空自己多看看近世代数 300 题.

1: 严格写出环、理想、左右零因子、左右单位、整环、除环、域、商域、环同态、UFD、PID、ED、素理想、极大理想、多项式环等课堂学过的主要知识的定义. 有疑问及时查书, 你能确保你写的是正确的吗? 其他的可以自行回顾.

2: 严格写出并证明中国剩余定理 (注意定理条件).

3: 若 D 是整环但不是域, 求证 $D[x]$ 不是主理想环.

4: 设 D 是整环,$f(x) \in D[x], c \in D, g(x) = f(x + c) \in D[x]$, 求证:
(1)$f(x)$ 在 $D[x]$ 中本原当且仅当 $g(x)$ 在 $D[x]$ 中本原;
(2)$f(x)$ 在 $D[x]$ 中不可约当且仅当 $g(x)$ 在 $D[x]$ 中不可约;
(3) 证明 $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ 是 $\mathbb{Z}[x]$ 中不可约多项式, 其中 p 为任意素数.
(4)$y^3 + x^2y^2 + x^3y + x$ 是否是 $R[x, y]$ 中不可约元? 其中 R 是 UFD.

5:(1) 设 K 是一个域, 试问 $K[x]$ 中哪些理想是素理想和极大理想?
(2)(选做) 思考:$\mathbb{Z}[x]$ 呢?

二: 进阶
5:(1) 证明 $\mathbb{Z}[\sqrt{-2}]$ 是欧式整环.$\mathbb{Z}[\sqrt{-3}]$,$\mathbb{Z}[\sqrt{-4}]$,$\mathbb{Z}[\sqrt{-5}]$ 是吗?
(2) (选做) 思考 $\mathbb{Z}[\sqrt{n}], n \in \mathbb{Z}$ 什么时候是 ED?

6: 设 D 是 UFD,K 是其商域,$f(x)$ 是 $D[x]$ 中本原多项式且 $degf(x) \geq 1$. 则 $f(x)$ 在 $D[x]$ 中不可约当且仅当 $f(x)$ 在 $K[x]$ 中不可约.

近世代数作业

Fir1247

2023 年 03 月-2022 年 7 月

前言

本文档为 2023 年春季学期叶郁老师的《近世代数》课程第四次开始的作业，都交的电子版，所以汇总了一下。突出一个折磨！叶老师的课作业实在太多了。

为避免歧义，本文档中的 $\subset$，相当于 $\subseteq, \subseteqq$，均表示“包含于”的意思，且只使用第一种形式；本文档中的 $\subsetneq$，相当于 $\subsetneqq$，均表示“真包含于”的意思，且只使用第一种形式。

Fir1247

第四次作业

1 $\forall g \in G$，如果 $g \in N$，则 $gN = Ng = N$；如果 $g \notin N$，则 $G = N \sqcup gN = N \sqcup Ng$，也有 $gN = Ng$. 于是对于 $\forall g \in G$ 都有 $gN = Ng$，N 是 G 的正规子群。

2 (1) $N \triangleleft G, M < G \Rightarrow \forall g \in M \subset G, gN = Ng$，所以 N 是 M 的正规子群。

(2) 不一定，反例：$\mathbb{Z}_2 \triangleleft K_4 \triangleleft S_4$，但 $\mathbb{Z}_2$ 不是 S_4 的正规子群。

(3) *(i).* 先证明，$NK = \{nk | n \in N, k \in K\}$ 是 G 的子群：

1° $\forall n_1k_1, n_2k_2 \in NK, N \triangleleft G \Rightarrow k_1n_2k_1^{-1} \in N \Rightarrow n_1k_1n_2k_2 = n_1k_1n_2k_1^{-1} \cdot k_1k_2 \in NK$，满足封闭性；

2° N, K 都是 G 的子群，故 $e \in N, e \in K \Rightarrow e = ee \in NK$，有单位元；

3° $\forall nk \in NK, k^{-1}n^{-1} = k^{-1}n^{-1}k \cdot k^{-1} \in NK$ 且 $nk \cdot k^{-1}n^{-1} = e$，有逆元。

再证明 NK 就是包含 N, K 的最小子群，即 $NK = N \vee K$：设 $H \leqslant G$ 且 $N, K \subset H$，$\forall n, k \in NK, n \in N \subset H, k \in K \subset H \Rightarrow nk \in H \Rightarrow NK \subset H$. 结论得证。

同理可证 $KN = N \vee K$.

(ii). $\forall n \in N, k \in K, nkn^{-1} \in K \Rightarrow nkn^{-1}k^{-1} \in K$，同时 $kn^{-1}k^{-1} \in N \Rightarrow nkn^{-1}k^{-1} \in N$. 因此 $nkn^{-1}k^{-1} \in N \cap K \Rightarrow nkn^{-1}k^{-1} = e \Rightarrow nk = kn$.

(4) 记 $M = N \vee K$. 因为

$$[M : N \cap K] = [M : K][K : N \cap K]$$

且

$$[M : N \cap K] \leqslant [M : N][M : K]$$

所以 $[K : N \cap K] \leqslant [M : N]$.

5.

(1) 定义 $x \sim y \Leftrightarrow x \in HyK$，$\sim$ 是等价关系，因为

1° $e \in H \cap K, x = exe \in HyK \Rightarrow x \sim x$.

2° $x \sim y \Rightarrow x = hyk, y = h^{-1}yk^{-1} \in HxK \Rightarrow y \sim x$.

3° $x \sim y, y \sim z \Rightarrow x = h_1yk_1 = h_1h_2zk_2k_2 \in HzK \Rightarrow x \sim z$.

所以可把 G 划分为若干等价类的不交并

$$G = \bigsqcup_{i \in R} Hg_iK.$$

(2) 和第三次作业 5. 类似，可得

$$|HgK| = |H||K : K \cap gHg^{-1}| = \frac{|H||K|}{|K \cap gHg^{-1}|}.$$

(3) 定义 H 上的等价关系：$h_a \sim h_b \Leftrightarrow h_a^{-1}h_b \in H \cap gPg^{-1}$，$H$ 对子群 $H \cap gPg^{-1}$ 的左陪集分解为

$$H = \bigsqcup_{h \in R} h \cdot H \cap gPg^{-1}$$

其中 $R = \{h_1, \cdots, h_t\}$. $HgK = \bigcup_{h \in H} hgK$，如果 $h_a \sim h_b, h_a = h_bgp_0^{-1}g^{-1}$，则

$$h_agP = h_bgp_0^{-1}g^{-1}gP = h_bgp_0^{-1}P = h_bgP.$$

也就是说

$$HgP = \bigsqcup_{h\in R} hgP$$

$|HgP| = t\cdot|hgP|$，此时如果取 $g\in P$，就有 $|HgP| = t\cdot|hP| = t\cdot p^r$，由 (1) 可知，$|G| = |HgP|\cdot s = p^r\cdot t\cdot s = p^r\cdot m$，于是 p 不整除 t.

而 $|HgP| = |P|[H : H\cap gPg^{-1}] = p^r[H : H\cap gPg^{-1}] \Rightarrow [H : H\cap gPg^{-1}] = t$，因此 p 不整除 $[H : H\cap gPg^{-1}]$，从而 $H\cap gPg^{-1} = H\cap P$ 是 H 的西罗 p 子群。

(4)（放弃了，没看懂群表示论 QAQ）

(5)

$$|GL_n(\mathbb{Z}/p\mathbb{Z})| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = p^{\frac{1}{2}(n-1)n}(p^n-1)(p^{n-1}-1)\cdots(p-1)$$

$$|U| = p^{\frac{1}{2}(n-1)n}$$

所以 U 是 $GL_n(\mathbb{Z}/p\mathbb{Z})$ 的西罗 p 子群。

(6) 由 (3)(4)(5) 知，$G\cap U$ 就是有限群 G 的西罗 p 子群。

3 (1) 由 *5.* 的结论可知 G 有西罗 p 子群 H，也就是 p 阶子群。

(2)（反证）假设另外一个 p 阶子群为 K，不妨设 H, K 分别由 h, k 生成，$H\neq K \Rightarrow h\neq k \Rightarrow H\cap K = \{e\}$. 由 2(4). 结论可知，$|H\vee K| \geqslant |H||K : e| = p^2 > |G| = pq$，矛盾。

(3) gHg^{-1} 也是 G 的 p 阶子群，但是由 (2). 可知 $H = gHg^{-1}$，因此 H 是 G 的正规子群。

4 (1) 定义 $x\sim y \Leftrightarrow x\in HyK$，$\sim$ 是等价关系，因为

1° $e\in H\cap K, x = exe\in HyK \Rightarrow x\sim x$.

2° $x\sim y \Rightarrow x = hyk, y = h^{-1}yk^{-1}\in HxK \Rightarrow y\sim x$.

3° $x\sim y, y\sim z \Rightarrow x = h_1yk_1 = h_1h_2zk_2k_2\in HzK \Rightarrow x\sim z$.

所以可把 G 划分为若干等价类的不交并

$$G = \bigsqcup_{i\in R} Hg_iK.$$

(2) 和第三次作业 *5.* 类似，可得

$$|HgK| = |H||K : K\cap gHg^{-1}| = \frac{|H||K|}{|K\cap gHg^{-1}|}.$$

(3) 定义 H 上的等价关系：$h_a\sim h_b \Leftrightarrow h_a^{-1}h_b\in H\cap gPg^{-1}$，$H$ 对子群 $H\cap gPg^{-1}$ 的左陪集分解为

$$H = \bigsqcup_{h\in R} h\cdot H\cap gPg^{-1}$$

其中 $R = \{h_1,\cdots,h_t\}$.$HgK = \bigcup_{h\in H} hgK$，如果 $h_a\sim h_b, h_a = h_bgp_0^{-1}g^{-1}$，则

$$h_agP = h_bgp_0^{-1}g^{-1}gP = h_bgp_0^{-1}P = h_bgP.$$

也就是说

$$HgP = \bigsqcup_{h\in R} hgP$$

$|HgP| = t\cdot|hgP|$，此时如果取 $g\in P$，就有 $|HgP| = t\cdot|hP| = t\cdot p^r$，由 (1) 可知，$|G| = |HgP|\cdot s = p^r\cdot t\cdot s = p^r\cdot m$，于是 p 不整除 t.

而 $|HgP| = |P|[H : H\cap gPg^{-1}] = p^r[H : H\cap gPg^{-1}] \Rightarrow [H : H\cap gPg^{-1}] = t$，因此 p 不整除 $[H : H\cap gPg^{-1}]$，从而 $H\cap gPg^{-1} = H\cap P$ 是 H 的西罗 p 子群。

(4)（放弃了，没看懂群表示论 QAQ）
(5)

$$|GL_n(\mathbb{Z}/p\mathbb{Z})| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = p^{\frac{1}{2}(n-1)n}(p^n-1)(p^{n-1}-1)\cdots(p-1)$$

$$|U| = p^{\frac{1}{2}(n-1)n}$$

所以 U 是 $GL_n(\mathbb{Z}/p\mathbb{Z})$ 的西罗 p 子群。
(6) 由 (3)(4)(5) 知，$G \cap U$ 就是有限群 G 的西罗 p 子群。

5 $K = \{(1,b)|b \in R\} \subset G$ 先证明 K 是子群：
1° $(1,b_1),(1,b_2) \in K \Rightarrow (1,b_1)(1,b_2) = (1,b_1+b_2) \in K$. 满足封闭性；
2° $(1,b) \in K, \exists (1,0) \in K$ $s.t.$ $(1,b)(1,0) = (1,0)(1,b) = (1,b)$，存在单位元；
3° $(1,b) \in K, \exists (1,-b) \in K$ $s.t.$ $(1,b)(1,-b) = (1,-b)(1,b) = (1,0)$，存在逆元。
因此 $K < G$. 再证明 K 正规：$\forall (a,b) \in G$,

$$(a,b)K = \{(a,ac+b)|c \in R\} = \{(a,d)|d \in R\}$$
$$K(a,b) = \{(a,b+c)|c \in R\} = \{(a,d)|d \in R\}$$

因此 $(a,b)K = K(a,b)$，并且选定 $b, \{(a,b)|a \in R^\times\}$ 就是 G 对 K 作陪集分解的一个代表元系。

取映射 $\sigma : G/K \to R^\times, (a,b)K = \{(a,d)|d \in R\} \mapsto a$. 易证它是一个同构，所以 $G/K \cong R^\times$.

6 设 G 包含了 $Ker(f)$ 的正规子群为 G_1，则 $Ker(f) \triangleleft G_1$，f 诱导了同构映射：

$$\overline{f} : G_1/Ker(f) \to f(G_1)$$

$f(G_1)$ 是 H 的某个正规子群，因为：
1° f 是群同态，G_1 是群，故 $f(G_1)$ 是 H 的子群；
2° f 是群同态满射，所以 $\forall h \in H, \exists g \in G, f(g) = h \Rightarrow hf(G_1) = f(gG_1) = f(G_1g) = f(G_1)h$，故 $f(G_1)$ 是 H 的正规子群。
反之，任何一个 H 的正规子群 H_1 都可以表示成某个 $f(G_1)$，因为：f 是满射，所以可设 $G_1 = f^{-1}(H_1) = \{g \in G|f(g) \in H_1\}$，下证 G_1 就是 G 的包含了 $Ker(f)$ 的正规子群：
1° $g_1, g_2 \in G \Rightarrow f(g_1g_2) = f(g_1)f(g_2) \in H \Rightarrow g_1g_2 \in G_1$，满足封闭性；存在单位元 e_G；存在逆元 $g^{-1}, f(g^{-1}) = f(g)^{-1} \in H_1$. 故 G_1 是 G 的子群；
2° $\forall g \in G, g_0 \in gG_1g^{-1} \Rightarrow f(g)f(g_1)f(g^{-1}) = f(g_1) \in H_1 \Rightarrow gG_1g^{-1} \subset G_1$，故 G_1 是正规子群。
3° $e \in H \Rightarrow Ker(f) = f^{-1}(e_H) \subset f^{-1}(H_1) = G_1$.
综上可知，如果取映射

$$f' : \{G_1|Ker(f) \triangleleft G_1 \triangleleft G\} \to \{H_1|H_1 \triangleleft H\}$$

$$f'(G_1) = \overline{f}(G_1/Ker(f)) = f(G_1)$$

则 f' 是一个双射，所以结论得证。

7 (1) 设 $(a_1,\cdots,a_n) \in Z(G_1 \times \cdots \times G_n)$，则对于任意的 $(b_1,\cdots,b_n) \in G_1 \times \cdots \times G_n$，有 $(a_1,\cdots,a_n)(b_1,\cdots,b_n) = (b_1,\cdots,b_n)(a_1,\cdots,a_n) \Leftrightarrow a_ib_i = b_ia_i, i = 1,2,\cdot,n \Leftrightarrow a_i \in Z(G_i), i = 1,\cdots,n$，因此 $Z(G_1 \times \cdots \times G_n) = Z(G_1) \times \cdots \times Z(G_n)$。

(2) $G_1 \times \cdots \times G_n$ 是阿贝尔群 $\Leftrightarrow G_1 \times \cdots \times G_n = Z(G_1 \times \cdots \times G_n) = Z(G_1) \times \cdots \times Z(G_n)$ $\Leftrightarrow Z(G_i) = G_i, \forall i \Leftrightarrow$ 每个 G_i 都是阿贝尔群。

8 由群乘积的定义可得 $N_1 \times N_2 \triangleleft G_1 \times G_2$;

取映射 $\sigma : G_1 \times G_2/N_1 \times N_2 \to (G_1/N_1) \times (G_2/N_2), (g_1, g_2)N_1 \times N_2 = g_1N_1 \times g_2N_2 \mapsto (g_1, g_2)$，显然它是一个同构，所以 $G_1 \times G_2/N_1 \times N_2 \cong (G_1/N_1) \times (G_2/N_2)$.

9 $SL_n(\mathbb{Z}/m\mathbb{Z})$ 是由行列式为 *1* 的矩阵全体，所以有 $SL_n(\mathbb{Z}) = Ker(det)$，其中 $det : GL_n(\mathbb{Z}/m\mathbb{Z}) \to \mathbb{Z}/m\mathbb{Z}^\times$ 为行列式映射，它是群同态映射，所以

$$|SL_n(\mathbb{Z}/m\mathbb{Z})| = \frac{|GL_n(\mathbb{Z}/m\mathbb{Z})|}{|\mathbb{Z}/m\mathbb{Z}^\times|} = \frac{|GL_n(\mathbb{Z}/m\mathbb{Z})|}{\phi(m)}$$

其中 $\phi(m)$ 为在模 m 意义下乘法可逆元个数，也就是所有与 m 互质且不大于 m 的正整数个数。

10 (1) 设 $G/Z(G)$ 是循环群，且 $xZ(G)$ 生成 $G/Z(G)$。则

$$G = \bigsqcup_{i \in I} x^i Z(G)$$

对于 $g, h \in G$，存在 $i, j \in \mathbb{Z}$，使得 $g \in x^iZ(G), h \in x^jZ(G)$，所以 $g = x^iz_1, h = x^jz_2$，其中 $z_1, z_2 \in Z(G)$，则 z_1, z_2, x^i, x^j 相互可交换，所以 $gh = hg$. 由于 g, h 的任意性，G 是阿贝尔群。

(2) 否则，G 的内自同构群 $G/Z(G)$ 是循环群，由上一问可知 G 是阿贝尔群，矛盾。

11 任意可逆方阵 P，对列向量作施密特正交化得到 $P = OR$，其中 $O \in O_n(\mathbb{R})$ 为正交阵，R 为上三角阵，记全体上三角阵为 T.。所以 $GL_n(\mathbb{R}) = \bigcup_{R \in T} O_n(\mathbb{R})R$. 定义 T 上的等价关系：$R_1 \sim R_2 \Leftrightarrow R_1R_2^{-1} \in O_n(\mathbb{R})$，所以

$$\begin{aligned} R_1 \sim R_2 &\Leftrightarrow (R_1R_2^{-1})^T R_1R_2^{-1} = I \\ &\Leftrightarrow R_1^T R_1 = R_2^T R_2 \end{aligned}$$

考察 $R_1^T R_1, R_2^T R_2$ 的第一行：

$$\begin{aligned} &(a_{11}^2, a_{11}a_{12}, \cdots, a_{11}a_{1n}) = (b_{11}^2, b_{11}b_{12}, \cdots, b_{11}b_{1n}) \\ &\Rightarrow (a_{11}, a_{12}, \cdots, a_{1n}) = \pm(b_{11}, b_{12}, \cdots, b_{1n}) \end{aligned}$$

C 再考察第二行：

$$\begin{aligned} &(a_{12}a_{11}, a_{12}a_{12} + a_{22}a_{22}, \cdots, a_{12}a_{1n} + a_{22}a_{2n}) = (b_{12}b_{11}, b_{12}b_{12} + b_{22}b_{22}, \cdots, b_{12}b_{1n} + b_{22}b_{2n}) \\ &\Rightarrow (0, a_{22}a_{22}, \cdots, a_{22}a_{2n}) = (0, b_{22}b_{22}, \cdots, b_{22}b_{2n}) \\ &\Rightarrow (0a_{22}, \cdots, a_{2n}) = \pm(0, b_{22}, \cdots, b_{2n}) \end{aligned}$$

以此类推，可知 R_1, R_2 每一行都差一个正负号，并且这些正负号之间无关。由此等价关系对全体上三角阵作划分，代表元系即为

$$R_T = \{R = (r_{ij})_{n \times n} \in T | r_{ii} > 0, i = 1, \cdots, n\}$$

也就是全体正定上三角阵，这也是 $GL_n(\mathbb{R})$ 对 $O_n(\mathbb{R})$ 的右陪集代表元系。

第五次作业

1 每个箭头代表一次置换 f，

$$
\begin{aligned}
&0 \to 0\\
&1 \to 1\\
&2 \to 8 \to 19 \to 15 \to 11 \to 26 \to 2\\
&3 \to 27 \to 21 \to 10 \to 14 \to 18 \to 3\\
&4 \to 6 \to 13 \to 22 \to 5 \to 9 \to 4\\
&7 \to 24 \to 20 \to 25 \to 23 \to 16 \to 7\\
&12 \to 17 \to 12\\
&28 \to 28
\end{aligned}
$$

省略掉 1-轮换，

$$f = (2,8,19,15,11,26)(3,27,21,10,14,18)(4,6,13,22,5,9)(7,24,20,25,23,16)(12,17).$$

2 (1) $\forall k \in \{1,2,\cdots,r\}$，不妨认为 $i_{r+1} = i_1$，则

$$\tau\sigma\tau^{-1}(\tau(i_k)) = \tau\sigma(i_k) = \tau(i_{k+1})$$

所以 $\tau\sigma\tau^{-1} = (\tau(i_1)\cdots\tau(i_k))$.

(2) 为了叙述方便，在某一个轮换中，$\forall k \in N_+$，$\exists l \in \{1,2,\cdots,n\}, l \equiv k(\mathrm{mod}\ n)$，规定 $i_k \overset{\text{def}}{=} i_l$.
回到本题，如果 $\tau \in C_{S_n}$，则 $\tau\sigma = \sigma\tau \Rightarrow \tau\sigma\tau^{-1} = \sigma \overset{(1)}{=} (\tau(i_1)\cdots\tau(i_n))$，也就是

$$(i_1 i_2 \cdots i_n) = (\tau(i_1)\cdots\tau(i_n))$$

而 $\forall k \in N_+$，有

$$(i_1 i_2 \cdots i_n) = (i_{1+k} i_{2+k} \cdots i_{n+k})$$

所以存在 $k \in N_+$ 使得 $\tau(i_j) = \tau(i_{j+k}), \forall j \in \{1,2,\cdots,n\}$，此时 $\tau = (i_1 i_2 \cdots i_n)^k = \sigma^k \in \langle\sigma\rangle$. 于是 $C_{S_n} \subset \langle\sigma\rangle$，显然有 $\langle\sigma\rangle \subset C_{S_n}$，于是二者相等得证。

(3) $n \geqslant 3$ 时，若 $1 \neq \sigma \in C(S_n)$，则根据 (2) 结论可知 $S_n =< \sigma >$，但 S_n 中包含 $n-1$-轮换，而 $< \sigma >$ 中没有，故矛盾。

3 (1) 设 g 的阶数为 n，$|G/N| = m$，考虑 gN 在 G/N 中的阶数，设为 r，$(gN)^r = g^r N = N \Rightarrow g^r \in N$.
因为 m, n 互素，r 是 m 的因数，所以 n, r 互素，于是存在整数 s, t 使得 $sn + rt = 1$，从而

$$g = g^{sn+rt} = (g^n)^s \cdot (g^r)^t = (g^r)^t \in N$$

(2) 任何一个 3-轮换 $\sigma \in S_n$ 的阶都是 3，与 $|S_n/N| = 2$ 互素，所以 $\sigma \in N$，进而 N 包含所有的 3-轮换。由于 A_n 由 3-轮换生成，$|A_n| = |N|$，所以 $A_n = N$，于是 $A_n (n \geqslant 3)$ 便是 S_n 中唯一的指数为 2 的正规子群。至于 $n = 2$ 的情况，$A_2 = \{\mathrm{Id}, (12)\}$，$\{\mathrm{Id}\}$ 是它唯一地指数为 2 的正规子群。

4 (1) S_4 中元素的型设为：$1^{\lambda_1}2^{\lambda_2}3^{\lambda_3}4^{\lambda_4}$，所有可能的 $(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ 有：

$$(4,0,0,0), (2,1,0,0), (1,0,1,0), (0,2,0,0), (0,0,0,1)$$

(2) 每个型对应的共轭类为：

$$\begin{aligned}
[1^4] &: (1)，即恒等变换，共\ 1\ 个\\
[1^2 2^1] &: (12),(13),(14),(23),(24),(34)共\ 6\ 个\\
[1^1 3^1] &: (123),(132),(124),(142),(134),(143),(234),(243)共\ 8\ 个\\
[2^2] &: (12)(34),(13)(24),(14)(23)共\ 3\ 个\\
[4^1] &: (1234),(1243),(1324),(1342),(1423),(1432)共\ 6\ 个
\end{aligned}$$

$|S_4| = 24$，设 N 是正规子群，则 $|N|$ 只能是 $1, 2, 3, 4, 6, 8, 12, 24$. 除去平凡的 1 和 24（对应 $\{1\}$ 和 S_4 本身），则只有 $12 = 1 + 3 + 8$ 和 $4 = 1 + 3$（对应 A_4 和 K_4）. 所以 S_4 的所有正规子群包括：$\{1\}, S_4, A_4, K_4$.

5 $1^{\lambda_1} 2^{\lambda_2} \cdots n^{\lambda_n}$ 对应的共轭类中元素，是 λ_1 个 1-轮换、λ_2 个 2-轮换、$\cdots$、λ_n 个 n-轮换互不相交的积，所以相当于是对 $\{i_1 i_2 \cdots i_n\}$（此排列个数为 $n!$）的一个划分，每个 i-轮换自身重复了 i 次，顺序上因为可交换所以重复了 $\lambda_i!$ 次，所以一共重复了 $\prod_{i=1}^n \lambda_i! \cdot i^{\lambda_i}$ 次，因此型的个数为

$$\frac{n!}{\prod_{i=1}^n \lambda_i! \cdot i^{\lambda_i}}$$

如果把型的全体记作 M，$m \in M$ 对应的共轭类元素个数为 N_m，则

$$\mathrm{LHS} = \sum_{m \in M} \frac{N_m}{n!} = \frac{\sum_{m \in M} N_m}{n!} = \frac{|S_n|}{n!} = 1 = \mathrm{RHS}$$

6 (1) 考虑 $GL_2(\mathbb{Z}_2) \circlearrowleft X = \left\{ \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \right\}$，于是 $S(X) = S_3$，从而 $\rho : GL_2(\mathbb{Z}_2) \to S_3$ 是群同态。而 $\mathrm{Ker}\rho = \{I_2\}$，所以是单射，进而是群同构。

(2) $\mathbb{F} \oplus \mathbb{F}$ 有 4 个一维子空间，分别记作 V_1, V_2, V_3, V_4，并设

$$\begin{aligned}
V_1 &= \left\{ \begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix} \right\}\\
V_2 &= \left\{ \begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}2\\0\end{pmatrix} \right\}\\
V_3 &= \left\{ \begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}2\\2\end{pmatrix} \right\}\\
V_4 &= \left\{ \begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix} \right\}
\end{aligned}$$

设 $X = \{V_1, V_2, V_3, V_4\}$，考虑群作用 $GL_2(\mathbb{F}_3) \circlearrowleft X$，诱导了群同态 $\rho : GL_2(\mathbb{F}_3) \to S_4$，如果能证明 $\mathrm{Ker}\rho$ 等于所有纯量阵全体 $P = \{rI : r \in \mathbb{F}_3\} = Z(GL_2(\mathbb{F}_3))$，由第一同构定理可知

$$PGL_2(\mathbb{F}_3) = (GL_2(\mathbb{F}_3))/Z(GL_2(\mathbb{F}_3)) \cong S_4$$

下面完成补充证明：纯量阵作用到子空间上显然是恒等变换（即相当于伸缩变换），所以 $P \subset \mathrm{Ker}\rho$.

设 $A=(a_{ij})\in GL_2(\mathbb{F}_3)$，$x=\begin{pmatrix}b_1\\b_2\end{pmatrix}$ 是 V_i 的基，假设 $Ax\in V_i$，则 $\exists r\in\mathbb{F}_3, Ax=rx$，即

$$\begin{aligned}(a_{11}-r)b_1+a_{12}b_2&=0\\a_{21}b_1+(a_{22}-r)b_2&=0\end{aligned}$$

考虑：

$i=1$： $b_1=0,b_2=1$，解得 $a_{12}=0$，$a_{22}=r$.

$i=2$： $b_1=1,b_2=0$，解得 $a_{11}=r$，$a_{21}=0$.

所以 $A=rI$ 是纯量阵，所以 $\mathrm{Ker}\rho\subset P$，进而二者相等。

(3) $2I\in GL_2(\mathbb{Z}_3)$ 与 $GL_2(\mathbb{Z}_3)$ 中所有元素都可交换,所以 $GL_2(\mathbb{Z}_3)$ 中心非平凡,但 $PGL_2(\mathbb{F}_3)$ 中心只有单位阵，$PGL_2(\mathbb{F}_3)\cong S_4$，故 $GL_2(\mathbb{Z}_3)\ncong S_4$.

第六次作业

1 假设 A_4 的 6 阶子群是 H，不妨设 $A_4=H\sqcup gH$.

先证明：$\forall a\in A_4$，$a^2\in H$. 如果 $a\in H$，则成立；如果 $a\notin H$，则 $a=gh\in gH$，如果 $a^2\notin H$，则 $a^2=gh_1\in gH$，从而 $h_1=hgh$，$g=h^{-1}h_1h^{-1}\in H$，矛盾。

于是，所有的 3-轮换都在 H 里，这是因为 3-轮换的平方都是自身的逆，全体 3-轮换的逆也就是全体 3-轮换。但由于 3-轮换有 8 个，H 中元素只有 6 个，所以假设不成立。

2 (1) 先证明 G_f 是群：

1° $\forall a_1,a_2\in G_f$，$f(a_2\circ a_1(x_1),\cdots)=f(a_2(a_1(x_1)),\cdots)=f(a_1(x_1),\cdots)=f(x_1,\cdots)\Rightarrow a_2\circ a_1\in G_f$.

2° 单位元，即恒等变换 $\mathrm{Id}\in G_f$.

3° 任取置换 $a\in G_f$，逆置换 a^{-1} 就是 a 在 G_f 中的逆元。

进而 G_f 是 S_4 的子群。

(2) 用 $abcd$ 表示置换 $\begin{pmatrix}1&2&3&4\\a&b&c&d\end{pmatrix}$,

(i) $G_f=\{1234,2134,1243,2143,3412,3421,4312,4321\}$

(ii) $G_f=\{1234,1324,2134,2314,3124,3214\}$

(iii) $G_f=\{1234,2134,1243,2143\}$

(iv) $G_f=S_4$

(v) 为所有的偶置换，即 $G_f=A_4$

3 (1) 任何一个置换能被写成不交的轮换之积,轮换 $(a_1a_2\cdots a_k)=(a_1a_k)(a_1a_{k-1})\cdots(a_1a_2)$，对换 $(ij)=(1i)(1j)(1i)$，所以 S_n 由 $\{(12),\cdots,(1n)\}$ 生成。

(2) $(1k)=(12)(23)\cdots(k-2\ k-1)(k-1\ k)(k-2\ k-1)\cdots(23)(12),\forall k\in\{2,3,\cdots,n\}$.

(3) $(k\ k+1)=(12\cdots n)^{-(k-1)}(12)(12\cdots n)^{k-1},\forall k\in\{1,2,\cdots,n-1\}$.

4 (1) 见 (2)

(2) 定义映射 $f:S_n\to A_{n+2}$，

$$f(\sigma)=\begin{cases}\begin{pmatrix}1&2&\cdots&n&n+1&n+2\\\sigma(1)&\sigma(2)&\cdots&\sigma(n)&n+1&n+2\end{pmatrix}, & \sigma\text{ 是偶置换}\\[2ex]\begin{pmatrix}1&2&\cdots&n&n+1&n+2\\\sigma(1)&\sigma(2)&\cdots&\sigma(n)&n+2&n+1\end{pmatrix}, & \sigma\text{ 是奇置换}\end{cases}$$

下面验证 f 是一个群同态：

$$f(\sigma\mu)=\begin{cases}\sigma\mu\cdot(n+1\ n+2) & ,\ \sigma\mu \text{ 是奇置换}\\ \sigma\mu & ,\ \sigma\mu \text{ 是偶置换}\end{cases}=f(\sigma)f(\mu)$$

(3) 任取一 n 阶有限群 G，考虑群乘法左乘 m 作用于自身，$G\circlearrowleft G$ 诱导的群同态 $\rho:G\to S(G)=S_n$，那么根据 $\mathrm{Ker}\rho=\rho^{-1}(\mathrm{Id})=\rho^{-1}(m(1_G,*))=\{1_G\}$ 可知 ρ 是单射，进而是群同构。因此每个有限群都是某个对称群的子群，由 (2) 知也是某个交错群的子群。

5 (1) $S_3=<(12),(123)>$，实际上

$$\begin{aligned}S_3&=\{(1),(12),(123),(13),(23),(132)\}\\&=\{(1),(12),(123),(12)(123),(12)(123)^2,(123)^2\}\end{aligned}$$

希望找如下对应关系，使得 σ 是一个同构：

$$\sigma=\begin{cases}(1)\to(1)\\(12)\to?_1\\(123)\to?_2\end{cases}$$

列举：$?_2$ 处不能是偶置换，否则 $\sigma((132))=(1)$，不保证单射，因此只能是 (123) 或 (132).

$?_1$ 处不能与 $?_2$ 相同，也不能是 (1)，只剩下三种选择，因此可能构成同构的情况最多只有 6 种，即 $|Aut(S_3)|\leqslant 6$.

(2) 先证明：任何一个群 G，都有 $Inn(G)\cong G/Z(G)$.

考虑同态映射：$\varphi:G\to Inn(G),g\mapsto\sigma_g:x\mapsto gxg^{-1}$ 的核

$$\mathrm{Ker}\varphi=\{g\in G:gxg^{-1}=x,\forall x\in G\}=Z(G)$$

由第一同构定理可知结论得证。

于是 $Inn(S_3)\cong S_3/Z(S_3)=S_3$.

(3) 因为 $Inn(S_3)\leqslant Aut(S_3)$，而 $|Inn(S_3)|=|S_3|=6\geqslant Aut(S_3)$，故 $Inn(S_3)=Aut(S_3)$，进而 $Aut(S_3)\cong S_3$.

6 $1111=11\times101$，所以 G 的生成元的型只可能是：$1^c11^a101^b$，$11a+101b+c=999$. 存在一个元素 i 使得任何 $\sigma(i)=i$，也就是生成元对这个元素不产生影响，只需证 $c>0$.

假设不成立，即 $c=0$，那么非负整数 a,b 满足 $11a+101b=999$. 因此

$$a=\frac{999-101b}{11}=\frac{9-2b}{11}+90-9b\in N_+$$

$\frac{9-2b}{11}$ 是整数时，$b=\frac{9+11k}{2}\geqslant 10$，然而此时 $a<0$，矛盾。

7 ($\Rightarrow$) 设 $a\in S$ 满足 $S=Ga$，对于任意 $x\in S,x=ga,g\in G$，x 在 N 中的稳定子群

$$\begin{aligned}N_x=&\{n\in N:nx=x\}=\{n\in N:nga=ga\}=\{n\in N:g^{-1}ng\cdot a=a\}\\=&\{n\in N:g^{-1}ng\in G_a\}=N\cap gG_ag^{-1}\end{aligned}$$

又因为 $N\triangleleft G$，故 $N_x=N\cap gG_ag^{-1}=gNg^{-1}\cap gG_ag^{-1}=g(N\cap G_a)g^{-1}=gN_ag^{-1}$，从而

$$|Nx|=\frac{|N|}{|N_x|}=\frac{|N|}{|gN_ag^{-1}|}=\frac{|N|}{|N_a|}=|Na|$$

即 S 在 N 作用下的每个轨道有相同多的元。

($\Leftarrow$) 没想出来...

8 (1). 关于 D_2，因为 $aba = aa^{-1}b = b, bab = a^{-1}b^2 = a^{-1} = a$，所以 $D_2 = \{1, a, b, ab\} \cong K_4$.
关于 D_3，构造

$$f : D_3 =< a, b >\to S_3 =< (12), (123) >,$$
$$a \mapsto (123), b \mapsto (12)$$

因为 $(12)(123) = (13) = (123)^{-1}(12)$，两个群的生成结构相同，所以 f 是一个同构。
(2). 因为 $\forall k, a \cdot a^k \cdot a^{-1} \in < a >, b \cdot a^k \cdot b^{-1} = (bab^{-1})^k = a^{-k} \in < a >$，所以 $< a > \triangleleft D_n$.
D_n 中的元素总可以表示成：$d = a^{n_1}ba^{n_2}\cdots$ 由于 $bab^{-1} = a^{-1} \Rightarrow ba^tb = a^{-t}$，

$$\begin{aligned} d &= a^{n_1}(ba^{n_2}b)a^{n_3}ba^{n_4}b\cdots \\ &= a^{n_1}a^{-n_2}a^{n_3}ba^{n_4}b\cdots \\ &= a^{n_1-n_2+n_3-n_4}\cdots \end{aligned}$$

如此一来，或者 $d \in < a >$，或者 $d \in < a > b$，于是 $D_n/ < a > \cong \{1, b\}^\times \cong \mathbb{Z}_2^+$

9 令 $\Omega = \{(g, x) \in G \times S : gx = x\}$.
先固定 $g \in G$，得到

$$|\Omega| = \sum_{g\in G} F(g)$$

同时，固定 $x \in S$，设 $S = \bigcup_{1\leqslant i\leqslant t} Gx_i$ 是 S 的按轨道的划分，注意到若 $x \in Gx_i$，则 $|Gx| = |Gx_i|$，于是

$$\begin{aligned} |\Omega| =& \sum_{x\in S} |G_x| = \sum_{x\in S} \frac{|G|}{|Gx|} = \sum_{i=1}^{t} \sum_{x\in Gx_i} \frac{|G|}{|Gx|} \\ =& \sum_{i=1}^{t} \sum_{x\in Gx_i} \frac{|G|}{|Gx_i|} = \sum_{i=1}^{t} |Gx_i| \frac{|G|}{|Gx_i|} = t|G| \end{aligned}$$

故 $\sum_{g\in G} F(g) = t|G|$.

10 这五个正多面体分别有 $4, 8, 6, 20, 12$ 个顶点，对于旋转群或对称群 G，固定一个顶点得到的稳定子群 G_1 满足 $|G| = |\Sigma||G_1|$，其中 $|\Sigma|$ 为顶点数。

如果 G 是旋转群，则 G_1 相当于是正三角形、正三角形、正四边形、正三角形、正五边形的旋转群，阶数分别为 $3, 3, 4, 3, 5$，进而得到旋转群的阶数分别为 $12, 24, 24, 60, 60$.

如果 G 是对称群，则 G_1 相当于是正三角形、正三角形、正四边形、正三角形、正五边形的对称群，阶数分别为 $6, 6, 8, 6, 10$，进而得到对称群的阶数分别为 $24, 48, 48, 120, 120$.

11 正四面体的旋转群 A 有 12 个元，从而得知 A 作用于四面体的轨道数为 12，而不考虑旋转的染色方案有 $4! = 24$ 种，也就是对称群 B 的所有元，$A \triangleleft B$，B 对 A 作陪集分解得到的代表元系只有 2 个元素，这两个元素就是旋转意义下不相同的两种染色方案。

12 (1).

$$gz = \begin{bmatrix} a & b \\ c & d \end{bmatrix} (x + y\mathrm{i}) = \frac{ax + b + ay\mathrm{i}}{cx + d + cy\mathrm{i}} = \frac{(ax + b + ay\mathrm{i}) \cdot (cx + d - cy\mathrm{i})}{|cx + d + cy\mathrm{i}|^2}$$
$$\mathrm{Im}gz = \frac{-(ax + b)cy + ay(cx + d)}{|cx + d + cy\mathrm{i}|^2} = \frac{(-bc + ad)y}{|cx + d + cy\mathrm{i}|^2} = \frac{y}{|cx + d + cy\mathrm{i}|^2} > 0.$$

所以 $gz \in H$.

(2). 任取 $z = x + y\mathrm{i}$,

$$x + y\mathrm{i} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} i = \frac{ac + bd + \mathrm{i}}{c^2 + d^2}$$
$$\Rightarrow x = \frac{ac + bd}{c^2 + d^2}, y = \frac{1}{c^2 + d^2}$$

取 $a = \sqrt{y}, b = \frac{x}{\sqrt{y}}, c = 0, d = \frac{1}{\sqrt{y}}$ 即可。

(3). 若 $g \in G_{\mathrm{i}}$，则

$$\frac{ac + bd}{c^2 + d^2} = 0, \frac{1}{c^2 + d^2} = 1$$
$$\Rightarrow ac + bd = 0, c^2 + d^2 = 1$$

设 $c = \sin\theta$，$d = \cos\theta$，于是解得 $a = \cos\theta, b = -\sin\theta$. 即

$$G_{\mathrm{i}} = \left\{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} : \theta \in [0, 2\pi) \right\}$$

(4). 任意 $z = x + y\mathrm{i} \in H$，存在 $g = \begin{bmatrix} x^{\frac{1}{2}} & xy^{-\frac{1}{2}} \\ 0 & y^{-\frac{1}{2}} \end{bmatrix}$ 使得 $z = gi$.

由 (3) 可知，i 的稳定子群实际上就是 $SO_2(\mathbb{R})$，从而 $SL_2(\mathbb{R})$ 中的每一个元素，都可以分解为两个部分：把点 i 移动到目标点 z 的（分式线性）变换 $\circ$ 保持 i 不动的（旋转）变换，

即目标点 $z = x + y\mathrm{i} \in H$ 一一对应陪集 $\begin{bmatrix} x^{\frac{1}{2}} & xy^{-\frac{1}{2}} \\ 0 & y^{-\frac{1}{2}} \end{bmatrix} SO_2(\mathbb{R})$，于是 $SL_2(\mathbb{R})$ 关于 $SO_2(\mathbb{R})$ 的陪集分解的代表元系就是所有的目标点 z，即上半平面 H.

(5). 由 (4) 可知，任意 $g \in SL_2(\mathbb{R})$，存在 $x + y\mathrm{i} \in H$ 和 $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \in SO_2(\mathbb{R})$ 使得

$$\begin{aligned} g &= \begin{bmatrix} x^{\frac{1}{2}} & xy^{-\frac{1}{2}} \\ 0 & y^{-\frac{1}{2}} \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \\ &= \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, a = \sqrt{y} > 0, b = x \in \mathbb{R}, \theta \in [0, 2\pi) \end{aligned}$$

第七次作业

1 设 $|G| = p^k$，S 是 G 的非正规子群全体，考虑 G 在 S 上的共轭作用：

$$G \circlearrowright S : G \times S \to S$$
$$(g, S_i) \mapsto gS_ig^{-1}$$

由轨道公式，

$$|S| = \sum_{H \in I} |\mathcal{O}_H| = \sum_{H \in I} [G : G_H]$$

其中，$G_H = \{g \in G | gHg^{-1} = H\}$ 是 H 的稳定子群，亦即 H 在 G 中的正规化子，I 是轨道代表元系.

$G_H \neq G$，否则 $H \triangleleft G$，与 $H \in S$ 矛盾。故 $|G_H| = p^r$，$r < k$，进而 $|G : G_H|$ 是 p 的倍数，所以 $|S|$ 是 p 的倍数。

2 A 是正规子群，所以可以考虑 G 在 A 上的共轭作用：

$$G \circlearrowleft A : G \times A \to A$$

$$(g, a) \mapsto gag^{-1}$$

对应的表示是群同态：$\rho : G \to S(A) = S_p$.

素数 p 阶群的自同构群同构于 $\mathbb{Z}_{p-1}$，所以

$$\mathrm{Im}\rho = \rho(G) \subset \mathrm{Aut}(A) \cong \mathbb{Z}_{p-1}$$

$$\mathrm{Ker}\rho = \{g \in G | gag^{-1} = a, \forall a \in A\} = Z_G(A)$$

所以

$$|G \backslash Z_G(A)| = |\mathrm{Im}\rho| \leqslant p - 1$$

但是 $|G\backslash Z_G(A)|$ 是 G 的因子，所以只能是 1，即 $G = Z_G(A)$，所以 $A \leqslant Z(G)$.

我不会证“素数 p 阶群的自同构群同构于 $\mathbb{Z}_{p-1}$”这个结论。另一种思路是：素数 p 阶群 A 一定是 p 阶循环群，有 $\varphi(p) = p - 1$ 个生成元，则 A 有 $p - 1$ 个自同构。

3 $G = |G\backslash N| \cdot |N|$，$p$ 与 $|G\backslash N|$ 互素，则 N 的 Sylow$p$ 子群也是 G 的 Sylow$p$ 子群。

设 $P \in \mathrm{Syl}_p(N) \subset \mathrm{Syl}_p(G)$，则由 Sylow 定理，

$$\forall Q \in \mathrm{Syl}_p(G), \exists g \in G \text{ s.t. } Q \leqslant gPg^{-1} \leqslant gNg^{-1} = N$$

这就证明了 N 包含所有 G 的 Sylow$p$ 子群。

4 $N_G(P) = \{g \in G | gPg^{-1} = P\} \triangleleft G$，所以

$$\forall g \in G, x \in N_G(P), gxg^{-1}Pgx^{-1}g^{-1} = P$$

即

$$x(g^{-1}Pg)x^{-1} = g^{-1}Pg$$

也就是说 $N_G(P) = N_G(g^{-1}Pg), \forall g \in G$.

显然地，$P \leqslant N_G(P)$，$g^{-1}Pg \leqslant N_G(g^{-1}Pg) = N_G(P)$，而 P 以及 $g^{-1}Pg$ 又是 G 的 Sylow$p$-子群，所以 P 和 $g^{-1}Pg$ 是 $N_G(P)$ 的 Sylow$p$-子群，由 Sylow 定理可知 P 和 $g^{-1}Pg$ 在 $N_G(P)$ 中是共轭的，所以

$$\exists n \in N_G(P), g^{-1}Pg = nPn^{-1} = P$$

即 P 的共轭子群是它本身，所以 P 是 G 的正规子群。

5 必要性：假设 G 的阶是偶数，由 Cauthy 定理，G 存在二阶元 $g = g^{-1}$，则 $C_g = C_{g^{-1}}$，而 1 所在的共轭类也是实共轭类，矛盾。

充分性：设 $C \neq \{1\}$ 是一个实共轭类，设有 $g, g^{-1} \in C$，存在 $h \in G$ 使得 $hgh^{-1} = g$. 则

$$\begin{aligned} h^2gh^{-2} &= h(hgh^{-1})h^{-1} = hg^{-1}h^{-1} \\ &= (hgh^{-1})^{-1} = (g^{-1})^{-1} = g \end{aligned}$$

若 h 的阶为偶数，即 $h^{2n} = 1$，从而 $2n||G|$，矛盾。若 h 的阶为奇数，设 $h^n = 1$，有 $h = h^{1-n}$，从而 $hg = g^{1-n}g = gh^{1-n} = gh$，从而 $g = g^{-1}$，g 为二阶元，矛盾。因此 G 是有一个实共轭类。

6 $|S_4| = 2^3 \times 3$，则 S_4 的 Sylow3-子群个数为 $3k+1|24$，于是 $k=0$ 或 1. 而 S_4 有 4 个 3-轮换生成的子群，所以 $k=1$，于是确定了所有的 Sylow3-子群：

$$\langle(123)\rangle, \langle(124)\rangle, \langle(134)\rangle, \langle(234)\rangle$$

Sylow2-子群个数为 $2k+1|24$，于是 $k=0$ 或 1，第五次作业 4. 计算过 S_4 没有 8 阶正规子群，所以 $k=1$，Sylow2-子群个数为 3. 也就是：

$$\{1,(13),(24),(12)(34),(13)(24),(14)(23),(1234),(1432)\}$$
$$\{1,(12),(34),(12)(34),(13)(24),(14)(23),(1324),(1423)\}$$
$$\{1,(14),(23),(12)(34),(13)(24),(14)(23),(1243),(1342)\}$$

7 (1). $N \triangleleft G$，所以 $NP = PN$ 是 G 的子群，且

$$[N : N \cap P] = [NP : P]$$

设 $|G| = p^k \cdot n$，$(p, n) = 1$，

$$|N \cap P| = \frac{|N||P|}{|NP|} = \frac{p^{r_1} \cdot n_1 \cdot p^k}{p^{r_2} \cdot n_2} = \frac{n_1}{n_2} p^{k+r_1-r_2}$$

$r_2 \leqslant k$，所以 $k + r_1 - r_2 \geqslant r_1$，而 $N \cap P \leqslant N \Rightarrow k + r_1 - r_2 = r_1$，即 $N \cap P$ 是 N 的 Sylow$p$-子群。

(2). 因为

$$[G/N : PN/N] = [G : PN]$$

而 $|P|||PN| \Rightarrow [G : PN]|[G : P] = n$，所以 $[G : PN]$ 即 $[G/N : PN/N]$ 与 p 互素，命题得证。

(3). 由定义可知，$(N_G(P)N)/N \subset N_{G/N}(PN/N)$. 设 $N_{G/N}(PN/N) = T/N$，$T \leqslant G$，由定义可知

$$tPt^{-1} \subset PN, \forall t \in T.$$

从而 P 和 tPt^{-1} 均是 PN 的 Sylow$p$-子群，故由 Sylow 定理知 P 和 tPt^{-1} 在 PN 中共轭。由此可推得 $t \in N_G(P)N$，即 $T \subset N_G(P)N$.

8 取 H 的某个 Sylow$p$-子群 A，由 Sylow 定理知，A 含于 G 的某个 Sylow$p$-子群 aPa^{-1}，从而 $A \subset aPa^{-1} \cap H$. 而 $aPa^{-1} \cap H$ 是 H 的阶为 p 的幂的子群，故 $|aPa^{-1} \cap H| \leqslant |A|$. 于是 $A = aPa^{-1} \cap H$，即 $aPa^{-1} \cap H$ 是 H 的 Sylow$p$-子群。

9 设 $|G| = 24 = 2^3 \times 3$. 不妨设 G 的 Sylow2-子群非正规，则由 Sylow 定理知，G 有 3 个 Sylow2-子群 P_1, P_2, P_3. 考虑 G 在 $\{P_1, P_2, P_3\}$ 上的共轭作用，它诱导了群同态 $\rho : G \to S_3$.
$\mathrm{Ker}\rho \neq \{1\}$，否则 $\rho : G \to S_3$ 是单射，但 $|G| > |S_3|$，矛盾。
$\mathrm{Ker}\rho \neq G$，否则 $gP_ig^{-1} = P_i, \forall g \in G, i = 1, 2, 3$. 这与 G 的 Sylow2-子群互相共轭矛盾。
因此 $\mathrm{Ker}\rho$ 是 G 的非平凡正规子群，从而 G 非单群。

同样地，$36 = 3^2 \times 4$，考虑它的 Sylow3-子群，如果非正规，则个数为 4；$48 = 2^4 \times 3$，考虑它的 Sylow2-子群，如果非正规，则个数为 3.

10 $1 \in X \Rightarrow g \in gX$，所以 $g \in G_X \Rightarrow g \in gX = X$，即 $G_X \subset X$.

回到本题，充分性：

$$|G_X| = |X| \Rightarrow X = G_X \leqslant G$$

必要性：

$$X \leqslant G \Rightarrow X \leqslant G_X \Rightarrow X = G_X \Rightarrow |X| = |G_X|$$

11 令 $G = GL_n(\mathbb{Z}_p)$，则

$$|G| = p^{\frac{n(n-1)}{2}}(p^n-1)(p^{n-1}-1)\cdots(p-1)$$

所以 G 的 Sylow$p$-子群的阶为 $p^{\frac{n(n-1)}{2}}$. 令 A 为 G 中所有对角元为 1 的上三角矩阵集合，易证 A 是 G 的子群。第一列有 1 种取法，第二列有 p 种取法，第三列有 p^2 种取法，以此类推可知 A 的阶为 $p^{\frac{n(n-1)}{2}}$，所以是 G 的 Sylow$p$-子群。

$SL_n(\mathbb{Z}_p)$ 是 G 的子群，而 A 是 G 的 Sylow$p$-子群，所以 A 也是 $SL_n(\mathbb{Z}_p)$ 的 Sylow$p$-子群。

由 Sylow 定理，G 的 Sylow$p$-子群的个数是 $[G : N_G(A)]$，而且

$$N_G(A) = \{g \in G | gAg^{-1} = A\}$$

所以 $N_G(A)$ 是 $GL_n(\mathbb{Z}_p)$ 上的全体上三角阵，第一列有 $p-1$ 种取法，第二列有 $p(p-1)$ 种取法，第 k 列有 $p^{k-1}(p-1)$ 种取法，所以

$$|N_G(A)| = p^{\frac{n(n-1)}{2}}(p-1)^n$$

$$[G : N_G(A)] = \frac{(p^n-1)(p^{n-1}-1)\cdots(p-1)}{(p-1)^n}$$

12 由第 6 题可知，S_4 的 Sylow3-子群全体为

$$N = \{\langle(123)\rangle, \langle(124)\rangle, \langle(134)\rangle, \langle(234)\rangle\} = \{P_1, \cdots, P_4\}$$

设 $G = \mathrm{Aut}(S_4)$，因为 S_4 的中心平凡，所以 $Z(S_4) \cong S_4$. 考虑 G 在 N 上的群作用（因为自同构把 Sylow3-子群仍映为 Sylow3-子群）诱导的群同态为：

$$\rho : G \to S(N) = S_4$$

$$\mathrm{Ker}\rho = \{\alpha \in G | \alpha(P_i) = P_i, i = 1, 2, 3, 4\}$$

设 $\alpha \in \mathrm{Ker}\rho$，希望证明 $\forall A \leqslant S_4$，$\alpha(A) = A$，也就是说 α 是恒等变换，从而 $G \cong S_4$.

α 把 S_4 的 12 阶子群变成 12 阶子群，故 $\alpha(A_4) = A_4$.

考虑 S_4 的 2 阶元，α 把对换变成对换，或变成两个不相交对换的乘积。后者属于 A_4，故 α 只能把对换变成对换。

因为 $\alpha(\langle(123)\rangle) = \langle(123)\rangle$，所以 $\alpha((123)) = (123)$ or (132)，而 $(123) = (13)(12),$，故 $\alpha((12)) = (12), (13)$ or (23).

同样地考虑 $\alpha(\langle(124)\rangle) = \langle(124)\rangle$，可知 $\alpha((12)) = (12), (14)$ or (24). 综上可知 $\alpha((12)) = (12)$.

同理，任何对换 $a \in S_4$ 都有 $\alpha(a) = a$，因此 α 是恒等变换。

第八次作业

1 设 G 的阶质因数分解为 $|G| = p_1^{r_1}\cdots p_n^{r_n}$，由 Sylow 定理，$G$ 存在 $p_1^{r_1}, \cdots, p_n^{r_n}$ 阶子群，记作 $P_1, \cdots, P_n$，并且由题设可知都是 $P_1, \cdots, P_n$ 正规子群。

Claim:

$$\forall 1 < m \leqslant n, (P_1P_2\cdots P_{m-1}) \cap P_m = \{1\}$$

这是因为 $P_1P_2\cdots P_{m-1}$ 中元素的阶只能是 $p_1^{r_1}\cdots p_{m-1}^{r_{m-1}}$ 的因数，而 P_m 中元素的阶只能是 $p_m^{r_m}$ 的因数，所以只能是 1，即二者交集为 $\{1\}$. 由课本定理 44 页定理 2，$G=P_1\times\cdots\times P_n$.

设 $d=p_1^{m_1}\cdots p_n^{m_n}$，只需取 P_i 的 $p_i^{m_i}$ 阶子群 $Q_i, 1\leqslant i\leqslant n$，则 $Q=Q_1\times\cdots\times Q_n\leqslant P_1\times\cdots\times P_n=G$，同样地有

$$\bigcap_{i=1}^{n}Q_i=\{1\}$$

所以 $|Q|=p_1^{m_1}\cdots p_n^{m_n}=d$，$Q$ 就是 G 的 d 阶子群。

2 设 H 是 S_n 的指数为 i 的子群，且 $2\leqslant i\leqslant n$. 左陪集分解：

$$S_n=\bigsqcup_{k=1}^{i}a_kH$$

令

$$R=\{a_k|1\leqslant k\leqslant i\}$$

考虑 S_n 在 R 上的作用，定义

$$(g,a_k)\mapsto a_m\Leftrightarrow a_m^{-1}ga_k\in H$$

这样的 a_m 一定存在，因为 $ga_k\in S_n\Rightarrow ga_k$ in some a_mH. 其诱导的群同态为

$$\varphi:S_n\to S(R)\cong S_i$$

$n\geqslant 5$ 时 S_n 的非平凡正规子群只有 A_n，$\mathrm{Ker}\varphi\triangleleft S_n$ 所以 $\mathrm{Ker}\varphi\in\{\{1\},A_n,S_n\}$. 对于 $g\in\mathrm{Ker}\varphi$，等价于

$$g\in a_kHa_k^{-1},\forall k$$

存在某个 $a_k\in H$，否则群 G 中没有单位元。所以 $\mathrm{Ker}\varphi\subset H$. 因此，$\mathrm{Ker}\varphi\in\{\{1\},A_n\}$. 根据同态基本定理，

$$S_n/\mathrm{Ker}\varphi\cong\mathrm{Im}\varphi\subset S_i$$

如果 $\mathrm{Ker}\varphi=\{1\}$，则由上式得到 $i=n$；如果 $\mathrm{Ker}\varphi=A_n$，则由 $\mathrm{Ker}\varphi\subset H$ 得到 $i=2$.

若 H 是指数为 n 的子群，考虑 H 在 R 上的左乘作用，还是因为存在某个 $a_k\in H$，所以该作用至少有一个不动点 a_k. 又因为 $\mathrm{Ker}\varphi=\{1\}$，$\varphi$ 是一个同构，H 中的不同元素给出了不同的 $R-\{a_k\}$ 上的置换。于是可以给出一个 $H\to S_{n-1}$ 的嵌入，比较阶数可得 $H\cong S_{n-1}$.

3 设 $G=GL(n,\mathbb{C})$，H 是 G 的指数为 m 的真子群，左陪集分解：

$$G=\bigsqcup_{k=1}^{m}a_kH$$

令

$$R=\{a_kH|1\leqslant k\leqslant m\}$$

考虑 G 在 R 上的作用，诱导的群同态为

$$f:G\to S_m$$

设 $|G/\mathrm{Ker}f|=s|m!$，则 $\forall B\in G$，$B^s\in\mathrm{Ker}f$.（这里我其实没看懂）又因为 $\forall A\in G$，都存在 A' 满足 $A'^s=A$，所以 $\mathrm{Ker}f=G$，也就是说 $H=G$，这与 H 是真子群的条件矛盾。

4

(1) 假设 H 是 G 的指数为 4 的子群，那么考虑 G 在 H 左陪集上的作用诱导的群同态：

$$G \to S_4$$

$$G/\mathrm{Ker}f \leqslant S_4$$

由于 G 是单群，$\mathrm{Ker}f \triangleleft G$ 只能是平凡的，所以 $G \leqslant S_4$，显然不可能。假设 G 的 Sylow2-子群的个数为 3，记作 $P = \{P_1, P_2, P_3\}$，因为 Sylow2-子群都是共轭的，考虑 G 在 P 上的共轭作用诱导的群同态：

$$G \to S_3$$

同理可得 $G \leqslant S_3$，这显然不可能。

(2) G 的 Sylow2-子群 P 的个数 $N(2) = 2k+1|15$ 且不为 3，而且 G 是单群所以不为 1，则 $N(2) \in \{5, 15\}$. 如果 $N(2) = 5$，则 $[G : N_G(P)] = 5$，$N_G(P)$ 就是 G 的 12 阶子群；如果 $N(2) = 15$，如果这些 4 阶子群除了单位元两两不相交，考虑到 $N(5) = 5k+1|12 \Rightarrow N(5) = 6$，那么它们的并一共有至少 $1 + 15 \times 3 + 5 \times 5 = 71$ 个元素，矛盾。因此必然存在两个不同的 4 阶群 $P_1 \cap P_2 = K \neq \{1\}$，我们考虑

$$Z_G(K) = \{g \in G | gk = kg, \forall k \in K\} \leqslant G$$

因为 P_1, P_2 都是阿贝尔群，则 $P_1P_2 \leqslant Z_G(K)$，则 $|P_1P_2| = 4k|60, k > 1 \Rightarrow k \geqslant 3$. 可知 $|Z_G(K)| \geqslant 12$，又因为 G 不存在指数为 4（第一问结论）或者 2（因为单群）的子群，所以 $|Z_G(K)| = 12$. 综上所述 G 一定有 12 阶子群。

(3) 考虑 G 在 12 阶子群的左陪集上的作用诱导的群同态

$$G \to S_5$$

G 是单群，所以 $G \leqslant S_5$. 而我们知道 A_5 是 S_5 的唯一 60 阶（非平凡正规）子群，所以 $G \cong A_5$.

5 不妨设 $H < G$ 满足题目要求，如果 a, b 属于 H 在 G 中的同一左陪集，则 $b^{-1}a \in H$，记 $h = b^{-1}a$，则 $aHa^{-1} = bhHh^{-1}b^{-1} = bHb^{-1}$. 于是，$H$ 的共轭子群个数不会超过 $|G : H|$. 所有不同的共轭子群的并集大小不会超过

$$1 + (|H| - 1)|G : H| = 1 + |G| - |G : H| \leqslant |G| - 1$$

所以 G 不可能为所有 H 的共轭子群的并。

无限群的例子：$G = GL(2, \mathbb{C})$，H 为 G 中满足 $(1, 0)$ 是特征向量的矩阵构成的子群，因为 C 上的矩阵一定有特征向量，所以任意 G 中的矩阵可以由 H 中的矩阵共轭得到，因此 H 的所有共轭子群的并就是 G。

下面 6-12 题是周五的 1-7 题

6

(1) 不一定，例如 $G = \mathbb{Z}_2 \times \mathbb{Z}_4 = \langle a \rangle \times \langle b \rangle$，令

$$K = \{(1, 1), (a, b), (1, b^2), (a, b^3)\} = \langle (a, b) \rangle$$

不难验证 K 不能写成 $\langle a \rangle, \langle b \rangle$ 子群的直积。

(2) 设 $h \in H$，$h = h_1 \cdots h_n, h_i \in G_i$. 因 G_i 中任一元与 $G_j (i \neq j)$ 中任一元可换，故对任一整数 t，有 $h^t = h_1^t \cdots h_n^t$. 令 $a = |G_i|$，$b = \prod_{j \neq i} |G_j|$，则 $h_i^a = 1$，$h_j^b = 1 (j \neq i)$. 因 $(a, b) = 1$，故有整数 l 和 k，使得 $la + kn = 1$. 故

$$h_i = h_i^{la+kb} = h_i^{kb} = h^{kb} \in H \cap G_i, i = 1, \cdots, n$$

从而

$$H = (H \cap G_1) \cdots (H \cap G_n) = (H \cap G_1) \times \cdots \times (H \cap G_n)$$

结论得证。

(3) 充分性：考虑映射

$$f : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_{mn}$$
$$(s, t) \to ns + mt$$

容易验证这 f 是加法群同态，下面证明是同构：

$$\begin{aligned} f(s_1, t_1) = f(s_2, t_2) &\Rightarrow n(s_1 - s_2) + m(t_1 - t_2) = knm \\ (m, n) = 1 &\Rightarrow n|(s_1 - s_2), m|(t_1 - t_2) \\ &\Rightarrow (s_1, t_1) = (s_2, t_2) \end{aligned}$$

$$\begin{aligned} &\forall l \in \mathbb{Z}_{mn}, \exists s, t \in \mathbb{Z} \text{ s.t. } ns + mt = 1 \\ &\Rightarrow n(sl) + m(tl) = l \\ &\Rightarrow l = f(sl, tl) \end{aligned}$$

必要性：如果 $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} = \langle a \rangle$，因为循环群的固定阶的子群是唯一地，故

$$\mathbb{Z}_m = \langle a^n \rangle, \mathbb{Z}_n = \langle a^m \rangle$$

而且 $\langle a^n \rangle \cap \langle a^m \rangle = \{1\}$，故 $(n_1, n_2) = 1$.

7 $|G| = 20230501 = 23 \times 89 \times 9883$，

$$N(23) = 23k + 1 | 879587 \Rightarrow 23k | 23 \times 38242 + 21 \Rightarrow k = 1$$

同理 $N(89) = N(9883) = 1$. 于是 $\mathbb{Z}_{23}, \mathbb{Z}_{89}, \mathbb{Z}_{9883}$ 都是 G 的正规子群，且只相交于 $\{1\}$，于是

$$G = \mathbb{Z}_{23} \times \mathbb{Z}_{89} \times \mathbb{Z}_{9883} \cong \mathbb{Z}_{20230501}$$

所以是循环群。

8

(1) 考虑 p^n 阶群 G 在集合 $X = G - \{1\}$ 上的共轭作用，

$$|X| = \sum_{i \in I} |\mathcal{O}_x|$$

因为 $\mathcal{O}_x \leqslant G \Rightarrow |\mathcal{O}_x| = p^i$，而 $(|X|, p) = 1$，所以存在某个 $x \in X$ s.t. $|\mathcal{O}_x| = 1$，从而 $1 \neq x \in Z(G)$，G 有非平凡中心。

(2) p^2 阶群 G 必为交换群，否则 $|Z(G)|=p$，G 中没有 p^2 阶元，$Z(G)$ 是 p 阶正规子群且是循环群，元素 $y\notin Z(G)$，那么 y 只能是 p 阶元，于是 G 由 x,y 生成，进而可知 G 交换，矛盾。因此 p^2 阶群同构于 $\mathbb{Z}_{p^2}$ 或 $\mathbb{Z}_p\times\mathbb{Z}_p$.

(3) (a) 如果 $p\neq 2$，G 有非平凡中心 $Z(G)\leqslant G$，G 非阿贝尔群，那么 $Z(G)\neq G$，所以只能 $|Z(G)|=p$ 或 p^2. 于是 $G/Z(G)$ 是 p^2 或者 p 阶群。第四次作业 11 证明了一个群商掉其中心是循环群则群可交换，所以只能 $|Z(G)|=p$，

$$G/Z(G)=\langle a,b|a^p=b^p=1,ab=ba\rangle\cong\mathbb{Z}_p\times\mathbb{Z}_p$$

取 a,b 在 G 中得原像 x,y，定义

$$[x,y]:=xyx^{-1}y^{-1}\in Z(G)$$

1° 若 $[x,y]=1$，则 $\langle x,y,Z(G)\rangle$ 生成 G，故 G 是阿贝尔群，排除。因此应当有 $\langle[x,y]\rangle=Z(G)$.

2° 若 $\mathrm{ord}(x)=\mathrm{ord}(y)=p$，则由于 $xy=[x,y]yx=yx[x,y]$，G 中得元素都可以写成 $x^iy^j[x,y]^k,1\leqslant i,j,k\leqslant p$ 的性质，因此

$$\begin{aligned}G&\cong\langle x,y|x^p=y^p=[x,y]^p=1,[[x,y],x]=[[x,y],y]=1\rangle\\&\cong\langle x,y,z|z=[x,y],x^p=y^p=z^p=1,[z,x]=[z,y]=1\rangle\end{aligned}$$

此类非阿贝尔群等价于 $GL(3,\mathbb{F}_p)$ 的 Sylow$p$-子群：

$$\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\middle|\,a,b,c\in\mathbb{F}_p\right\}$$

3° 若 G 中存在元素 x 满足 $\mathrm{ord}(x)=p^2$，令 $X=\langle x\rangle$，则总存在 $y\in G-X$ 使得 $y^p\in X$. 为了证明这个论断，对 y 的阶分类讨论：

(i) 如果 $y^p=1$，则 $y^{p^2}=1$，由于 $x^iy^j,1\leqslant i,j\leqslant p^2$ 共计数 p^4 次，故存在 i_1,i_2,j_1,j_2 使得

$$x^{i_1}y^{j_1}=x^{i_2}y^{j_2}\Rightarrow x^{i_3}=y^{j_3}$$

同时意味着 $(i_3,p^2)=(j_3,p^2)=p$，也就是说 $y^p\in\langle x^p\rangle\leqslant X$. 由于 G 非交换，因此 $C_G(X)=X$ 是指数为 p 的子群，p 是群阶最小素因子所以 $C_G(X)$ 是正规子群，考虑 y 在 X 上的共轭作用：

$$\sigma_y:x\mapsto y^{-1}xy$$

则这是一个非平凡的自同构，因为 $\mathrm{ord}(y^{-1}xy)=\mathrm{ord}(x)=p^2,y\notin X$. 又因为 $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})=\mathbb{Z}_p\times\mathbb{Z}_{p-1}$ or $\mathbb{Z}_2$. 所以 $y^p\in X$ 意味着 σ_y 是 p 阶自同构，因此 $\sigma_y(x)=x^{kp},1\leqslant k\leqslant p-1$，通过选取适当的 y 可以使得 $k=1$，因此

$$y^{-1}xy=x^{p+1}\Rightarrow x^py=yx^{p(p+1)}=yx^p$$

从而 $Z(G)=\langle x^p\rangle=\langle[x,y]\rangle$. 因此 x^iy^j 形式的不同元素正好有 p^3 个，构成非阿贝尔群 G.

(*ii*) 如果 $y^{p^2}=1$，则有 $y^p=x^{kp}, 1\leqslant k\leqslant p-1$，令 $z=y^{-1}x^k\notin X$，则因为 $y^{-1}xy=x^{p+1}$，即 $[x^{-1},y^{-1}]=x^p$，有

$$z^p=(y^{-1}x^k)^p=x^{k\sum_{i=1}^p(p+1)^i}y^{-p}=x^{kp}y^{-p}=1$$

此处

$$\sum_{i=1}^{p}(p+1)^i=(p+1)\frac{(p+1)^p-1}{p}\equiv p(p+1)\equiv p(\mathrm{mod}\ p^2, p\neq 2)$$

因此总可以找到 $G-X$ 中的 p 阶元 y_1 满足 $y_1^{-1}xy_1=x^{p+1}$. 因此此时

$$G\cong\left\langle x,y|x^{p^2}=y^p=1,y^{-1}xy^{p+1}\right\rangle$$

(*b*) 如果 $p=2$，不存在 8 阶元，也不会都是 2 阶元，否则是阿贝尔群，故其一定存在 4 阶元 x，记 $X=\langle x\rangle$，取 $y\in G-X$，若 $\mathrm{ord}(y)=2$，则结论类似，有

$$G\cong\left\langle x,y|x^4=y^2=1,y^{-1}xy=x^3\right\rangle\cong D_4$$

若 $G-X$ 中都是四阶元，这里无法将其转化成 $G-X$ 中的二阶元，但是同样可以通过共轭作用，y 诱导了一个 X 的非平凡自同构，$y^{-1}xy=x^3$，有

$$G\cong\left\langle x,y|x^4=y^4=1,y^{-1}xy=x^3\right\rangle\cong Q_8$$

9 考虑群同态 $\varphi:G\to Q$，$x_n\mapsto\frac{1}{n!}, n>0$，因为 $\{\frac{1}{n!}\}$ 生成 $\mathbb{Q}$，因此只需要证明 φ 是单同态即可。由于 $x_n^n=x_{n-1}$，因此 G 是交换群，且其中元素 x 都有形式：

$$\prod_{i=1}^{k}x_{n_i}^{s_i}, 0\leqslant s_i<n_i, 1\leqslant i\leqslant k, s_i\in\mathbb{Z}$$

因此 $\varphi(x)=\sum_{i=1}^k\frac{s_i}{n_i!}.\varphi(x)=0$ 当且仅当 $\sum_{i=1}^k\frac{s_i}{n_i!}=0$ 当且仅当 $m+\frac{s_k}{n_k}=0, m\in\mathbb{Z}$，因此 $n_k=1, s_k=0$，即 $x=1$.

10

(1) $p^{n+1}x_n=px_0\in R$，因此 $p^{n+1}a_n=0,\forall n\geqslant 0$. 由于 $pa_{n+1}=a_n$，因此 G 是交换群，其中元素都有 $a=\sum_{i=1}^k m_ia_i$ 的形式，故 p^{k+1} 零化 a.

(2) 若 $a_0=0$，则 $x_0\in R$. 而我们知道 $F\cong\otimes_{i\in X}\mathbb{Z}$，因此

$$\begin{aligned}x_0&=\sum_{i=1}^{k}m_i(x_{i-1}-px_i)+m_0px_0\\&=(m_0p+m_1)x_0+\sum_{i=1}^{k-1}(m_{i+1}-m_ip)x_i+n_kpx_k, m_j\in\mathbb{Z}, j\geqslant 0.\end{aligned}$$

故

$$m_0p+m_1=1, m_{i+1}=m_ip, 1\leqslant i\leqslant k-1, m_kp=0.$$

因此 $1=m_0p$，矛盾。类似地可以证明 $a_n\neq 0$. 若 $a_n=a_m, m\geqslant n$，则 $a_n=p^{m-n}a_m\Rightarrow(1-p^{m-n})a_m=0$，乘以一个合适的 $p^i(\neq 0)$ 可以得到 $p^i=0$，矛盾。因此 a_n 是互异的，从而 G 是一个无限群。

(3) 设 $H \leqslant G$，若 H 含有无限个 a_n，则由 $pa_n = a_{n-1}$ 可知 H 含有所有的 a_n，$H = G$. 若其只含有有限个 a_n. 若

$$a = \sum_{i=1}^{k} m_i a_i \in H, 0 \leqslant m_i < p, m_k \neq 0$$

则

$$\begin{aligned} p^k a = p^k m_k a_k = m_k a_0 \in H &\Rightarrow a_0 \in H \\ &\Rightarrow m_k a_1 = p^{n-1} a - m_{k-1} a_0 \in H \\ &\Rightarrow a_1 \in H \end{aligned}$$

依次即可得 $H = \langle a_0, a_1, \cdots, a_m \rangle = \langle a_m \rangle$，即 H 是有限循环群。

(4) 由 (3) 可得 G 的有限子群都是形如 $\langle a_m \rangle$ 的 p^{m+1} 阶循环群，因此 p^n 阶子群是唯一的。

(5) 易知 $R_p \cong Z[\frac{1}{p}]/ \cong G$. 第一个同构是自然的，第二个同构类似于上面的证明。

11

(1) 考虑 S_n，$(12), (23), \cdots, ((n-1)n)$ 是它的一组生成元，记作 $S = \{x_1, x_2, \cdots, x_{n-1}\}$，满足：

$$x_i^2 = (x_j x_{j+1})^3 = (x_k x_l)^2 = 1, 1 \leqslant i \leqslant n-1, 1 \leqslant j \leqslant n-2, 1 \leqslant l < k-1 < n-1$$

考虑 S 上的自由群 F，则有满的群同态：

$$f : F \to S_n \tag{1}$$

由同态基本定理可知

$$S_n \cong F_n / \mathrm{Ker} f \tag{2}$$

注意到 $f(x_i^2) = f((x_j x_{j+1})^3) = f((x_k x_l)^2) = 1$，令 K 是 F 中 $\{x_i^2, (x_j x_{j+1})^3, (x_k x_l)^2\}$ 生成的正规子群，则 $K \leqslant \mathrm{Ker} f$. 注意到题目中给出的群 $G_n \cong F_n / K$，可以证明

$$G_n = G_{n-1} \sqcup G_{n-1} x_{n-1} \sqcup \cdots \sqcup G_{n-1} x_{n-1} \cdots x_1$$

所以 $[G_n : G_{n-1}] = n \Rightarrow |G_n| = n!$，

$$n! = |S_n| = |F_n / \mathrm{Ker} f| = \frac{|F/K|}{|\mathrm{Ker} f|/|K|} = \frac{n!}{|\mathrm{Ker} f|/|K|}$$

于是 $K = \mathrm{Ker} f$，$S_n \cong F/K \cong G_n$.

(2) 实际上

$$m_{ij} = \begin{cases} 1 & , 1 \leqslant i = j \leqslant n \\ 3 & , |i-j| = 1 \\ 2 & , \text{otherwise} \end{cases}$$

所以

$$A = \begin{pmatrix} 1 & -\frac{1}{2} & 0 & \cdots & 0 \\ -\frac{1}{2} & 1 & -\frac{1}{2} & \cdots & 0 \\ 0 & -\frac{1}{2} & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & -\frac{1}{2} \\ 0 & 0 & \cdots & -\frac{1}{2} & 1 \end{pmatrix}$$

记 A 的 i 阶顺序主子式为 d_i，则满足关系式

$$d_{i+2} = d_{i+1} - \frac{1}{4}d_i, d_1 = 1, d_2 = \frac{3}{4}$$

可得

$$d_i = \frac{i+1}{2^i} > 0$$

所以 A 正定。

12 由题设可知：$A^4 = 1$，$A^2 = C^3$. 设

$$G = \langle x, y | x^4 = 1, x^2 = y^3 \rangle$$

$$H = G/\langle x^2 \rangle = \langle x, y | x^2 = y^3 = 1 \rangle$$

(1) 考虑 $\varphi : x \mapsto aba, y \mapsto ab$ 和 $\psi : a \mapsto y^{-1}x, b \mapsto xy^{-1}$ 即可。

(2) $SL_2(\mathbb{Z})$ 的中心是 $\{\pm I\}$，因为 $x^2 \in C(G)$，且 $x^2 = -1$，因此 $\langle x^2 \rangle = \{\pm 1\}$，$f$ 诱导出的群同态即两边同时商掉同构的群：

$$g : H = G/\{\pm 1\} \to SL_2(\mathbb{Z})/\{\pm I_2\} \cong PSL_2(\mathbb{Z})$$

可知如果 f 是单射、满射，则 g 亦然。
f 如果不是单射，注意到 $f(x^2) = -I$，$x^2 \notin \mathrm{Ker}f$，存在另一个不是 x^2 的元素 $y \in \mathrm{Ker}f$，这就导致所以 g 不是单射；g 是满射时，注意到有两个自然的满同态

$$\pi_1 : G \to H, g \mapsto \overline{g}$$

$$\pi_2 : SL_2(\mathbb{Z}) \to PSL_2(\mathbb{Z}), A \mapsto \overline{A}$$

则根据定义有 $g \circ \pi_1 = \pi_2 \circ f$. 于是

$$\begin{aligned}
&\forall A \in SL_2(\mathbb{Z}), \exists X \in H, g(X) = \overline{A} \\
&\exists Y \in G, \pi_2(A) = \overline{A} = g(X) = g \circ \pi_1(Y) = \pi_2 \circ f(Y) \\
&\Rightarrow A^{-1}f(Y) \in \mathrm{Ker}\pi_2 = \{\pm I_2\} \\
&\Rightarrow f(Y) = \pm A
\end{aligned}$$

$f(Y) = -A$ 取 $-Y$ 即可，故 f 是满射。

(3) 只需证明 f 是满射且 g 是单射，从而二者都是同构。f 满显然，因为 A, C 可以生成 $SL_2(\mathbb{Z})$. 下面说明 g 是单射：H 中的非单位元元素都可以写成如下形式：

$$\begin{aligned}
w = y^{\varepsilon_1}xy^{\varepsilon_2}x\cdots y^{\varepsilon_{r-1}}xy^{\varepsilon_r} \\
\text{or } x \text{ or } wx \text{ or } xw \text{ or } xwx (\varepsilon_i \in \{\pm 1\}, 1 \leqslant i \leqslant r)
\end{aligned}$$

我们要验证的是这五种形式的元素都不属于 $\mathrm{Ker}g$. 显然的是 $x \notin \mathrm{Ker}g$，又有

$$xwx = xw \cdot x^{-1}, xwx \cdot x^{-1} = xw$$

所以只需证明 $\{w, wx\} \cap \mathrm{Ker}g = \varnothing$ 即可。我们有

$$g(y^{-1}x) = g(y^2)g(x) = \overline{A^2B} = \overline{B},$$

$$g(yx) = \overline{AB^{-1}A} = \overline{\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}} = \overline{D^{-1}}$$

其中 $D = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$，则 $B^n D^{-m} = \begin{pmatrix} 1-nm & n \\ -m & 1 \end{pmatrix}$

$$\begin{aligned} g(wx) &= g(y^{\varepsilon_1} x y^{\varepsilon_2} x \cdots y^{\varepsilon_{r-1}} x y^{\varepsilon_r} x) \\ &= \prod_{i=1}^{r} g(y^{\varepsilon_i} x) = \overline{B^{t_1} D^{-t_2} \cdots} \neq \overline{1} \end{aligned}$$

这是因为 $B^{t_1} D^{-t_2} \cdots$ 的非对角元素非零。若 $g(w) = \overline{1}$，则 $g(wx) = g(w)g(x) = g(x)$，矛盾，因为 $B^{t_1} D^{-t_2} \cdots$ 的元素全正，因此 $g(wx)$ 对应元素的代表元里的元素全正或全负，综上可知 g 是单射。
（最后这段完全没看明白，应该是我线代没学好。）

第九次作业

1 (1) $n \geqslant 3$ 时，$(\mathrm{id}, 1) \in C(A_n \times \mathbb{Z}_2)$，所以有非平凡中心，而 S_n 没有。
(2) 设

$$D_{2n} = \left\langle a, b | a^{2n} = b^2 = 1, ba = a^{2n-1} b \right\rangle$$

考虑 D_{2n} 的子群 $\langle a^n \rangle$ 和 $\langle a^2, b \rangle$，因为

$$\left\langle a^2, b \right\rangle = \{a^{2i}, a^{2i} b | 0 \leqslant i \leqslant n-1\}$$

所以阶为 $2n$，是 D_{2n} 的指数为 2 的子群，故为正规子群。设

$$f : \left\langle a^2, b \right\rangle \to D_n$$

$$a^2 \mapsto a, b \mapsto b$$

容易验证这是一个群同构。同时

$$\langle a^n \rangle \cong \mathbb{Z}_2$$

D_{2n} 中任一元素都可以写成 $a^i b$ 的形式，则

$$(a^i b) a^n (a^i b)^{-1} = a^i \cdot (bab^{-1})^n \cdot a^{-i} = a^i a^{-n} a^{-i} = a^{-n} \in \langle a^n \rangle$$

所以是 $\langle a^n \rangle$ 正规子群，而且 $\langle a^n \rangle \cap \langle a^2, b \rangle = \{1\}$，于是

$$D_{2n} \cong \left\langle a^2, b \right\rangle \times \langle a^n \rangle \cong D_n \times \mathbb{Z}_2$$

2 (1)

$$\begin{aligned} x^5 y^3 = x^8 y^5 = 1 &\Rightarrow x^5 y^3 = x^3 y^2 = 1 \Rightarrow x^2 y = x^3 y^2 = 1 \\ &\Rightarrow x^2 y = xy = 1 \\ &\Rightarrow x = y = 1 \end{aligned}$$

所以 G 平凡。

(2)

$$\begin{aligned} xy^3 = y^2x, x^2y = yx^3 &\Rightarrow y^3 = x^{-1}y^2x, x^3 = y^{-1}x^2y \\ &\Rightarrow y^{27} = x^{-1}y^{18}x = x^{-2}y^{12}x^2 = x^{-3}y^8x^3 = y^{-1}x^{-2}y^8x^2y \\ &\Rightarrow y^{27} = x^{-2}y^8x^2 = x^{-2}y^{12}x^2 \\ &\Rightarrow y^8 = y^{12} \Rightarrow y^4 = 1 \end{aligned}$$

同理也有 $x^4 = 1$，所以

$$\begin{aligned} xy^3 = y^2x, x^2y = yx^3 &\Rightarrow xy^{-1}x^{-1} = y^2, yx^{-1}y^{-1} = x^2 \\ &\Rightarrow 1 = xy^{-2}x^{-1} = yx^{-2}y^{-1} \\ &\Rightarrow x^2 = y^2 = 1 \\ &\Rightarrow x = y = 1 \end{aligned}$$

所以 G 平凡。

3 (1) 任一正有理数 x 可以被表示成两个不可约整数的分式，再进行质因数分解，即

$$x = \frac{p}{q} = \frac{p_1^{s_1} \cdots p_n^{s_n}}{q_1^{r_m} \cdots q_t^{r_m}} = p_1^{s_1} \cdots p_n^{s_n} q_1^{-r_1} \cdots q_t^{-r_m}$$

p_i, q_j 是素数，s_i, r_j 是正整数，上述分解是唯一的。

(2) 有限个有理数中的分子分母所包含的素因子是有限多个，而素数有无穷多个，一定存在某个素数不能被生成，故 $\mathbb{Q}^+$ 不是有限生成的。

4 (1) 假设 $\mathbb{Q}$ 是自由阿贝尔群，

$$\left\{ \frac{b_i}{a_i} | i \in J \right\}$$

是它的一组基，于是对于任一有理数 x 存在唯一的 J 的有限子集 I 和唯一的一组整数 $r_i, i \in I$ 使得

$$r = \sum_{i \in I} r_i \frac{b_i}{a_i}$$

则

$$\left\{ \frac{1}{a_i} | i \in J \right\}$$

也是一组基。而因为 $1 = a_i \cdot \frac{1}{a_i}, \forall i \in J$，故 J 只能含有一个元，这意味着 $\mathbb{Q}$ 是循环群，显然矛盾。

(2) 任取一个 $\mathbb{Q}$ 的有限生成子群

$$H = \left\langle \frac{b_1}{a_1}, \cdots, \frac{b_n}{a_n} \right\rangle$$

同理可证

$$H = \left\langle \frac{1}{a_1}, \cdots, \frac{1}{a_n} \right\rangle$$

设 $a = \mathrm{lcm}(a_1, \cdots, a)_n$，那么存在正整数 m_i 使得 $a_i m_i = a$，于是

$$H = \left\langle \frac{m_1}{a}, \cdots, \frac{m_n}{a} \right\rangle = \left\langle \frac{1}{a} \right\rangle$$

所以 H 是循环群。

5 (1) 对于文字 $f^k(y_1)$，$a_k = |f^k(y_1)| = n_k^1 + n_k^2$，$n^i$ 代表 y_i 的个数，$i = 1, 2$. 则

$$a_{k+1} = |f^{k+1}(y_1)| = n_{k+1}^1 + n_{k+1}^2 = (n_k^2) + (n_k^1 + n_k^2)$$

所以

$$\begin{aligned} n_{k+1}^1 &= n_k^2 \\ n_{k+1}^2 &= n_k^1 + n_k^2 = n_{k-1}^2 + n_k^2 \end{aligned}$$

所以是斐波那契数列，因为 $n_1^2 = 1$，$n_2^2 = 1$，所以

$$n_k^2 = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k}{\sqrt{5}} = n_{k+1}^1$$

$$\frac{|f^{k+1}(y_1)|}{|f^k(y_1)|} = \frac{n_{k+1}^1 + n_{k+1}^2}{n_k^1 + n_k^2} = \frac{n_k^2 + n_{k+1}^2}{n_{k-1}^2 + n_k^2} = \frac{n_{k+2}^2}{n_{k+1}^2} \to \frac{1+\sqrt{5}}{2} \text{ as } k \to \infty$$

(2) 共轭作用上元素 y 不改变每个 y_i 的指数和，因此 N 正规。

(3) $\forall x, y \in F_2, xyx^{-1}y^{-1} \in N$，因此 F_2/N 是阿贝尔群；又因为 $y_1^n, y_2^n \in N$，因此 F_2/N 中的元素具有 $y_1^i y_2^j (0 \leqslant i, j < n)$ 的形式且 $\langle y_1 \rangle \cap \langle y_2 \rangle = \{1\}$，于是

$$F_2/N \cong \langle y_1 \rangle \times \langle y_2 \rangle \cong \mathbb{Z}_n \times \mathbb{Z}_n$$

6 (1) 设 G 的一组基是 $e_1, \cdots, e_r$，设

$$g_i = \sum_{j=1}^{r} a_{ij} e_j, 1 \leqslant i \leqslant n$$

$$e_i = \sum_{j=1}^{n} b_{ij} g_j, 1 \leqslant i \leqslant r$$

令 $A = (a_{ij}) \in M_{n \times r}(\mathbb{Z})$，$B = (b_{ij}) \in M_{r \times n}(\mathbb{Z})$，于是 $BA = I_r$，

$$r = \text{rank}(BA) \leqslant \text{rank}(A) \leqslant n$$

(2) 归纳：$n = 1$ 时是循环群的情形，成立；
如果 $n-1$ 的情形成立，若 $H \subset \langle x_2, \cdots, x_n \rangle$ 则可知结论得证，否则，取

$$S = \{m_1 x_1 + \cdots + m_n x_n \in H | m_1 > 0\} \subset H$$

中 m_1 最小的元素 x. $\forall y = s_1 x_1 + \cdots + s_n x_n \in S$，因为 $s_1 \geqslant m_1$，存在 $q \in \mathbb{N}_+, r (0 \leqslant r < m_1)$ 使得 $s_1 = q m_1 + r$，此时

$$y - qx = r x_1 + \cdots + (s_n - q m_n) x_n \in S$$

只能 $r = 0$，否则与 m_1 最小矛盾，从而

$$\forall y \in S, y = qx + (s_2 - q m_{n_2}) x_2 + \cdots + (s_n - q m_n) x_n$$

$m_1 < 0$ 的情况同理，因此 $H = \langle x, K \rangle$，$K = H \cap \langle x_2, \cdots, x_n \rangle$，由于 K 最多由 $n-1$ 个元素生成，所以 H 最多由 n 个元素生成。

7 都不正确，下面给出反例：
(1) $\mathbb{Z}_2 \times \mathbb{Z}_{15} \cong \mathbb{Z}_6 \cong \mathbb{Z}_5$
(2) 设 $\mathbb{Z}_2 = \langle a \rangle$，$\mathbb{Z}_4 = \langle b \rangle$.
(i) $G_1 = G_2 = \langle a \rangle \times \langle b \rangle$，取 $H_1 = \langle a \rangle \cong H_2 = \langle 2b \rangle$，于是

$$G_1/H_1 \cong \mathbb{Z}_4, G_2/H_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

并不同构。
(ii) G_1 和 G_2 定义与 (i) 相同，令 $H_1 = \langle a \rangle \times \langle 2b \rangle$，$H_2 = \langle b \rangle$，则

$$G_1/H_1 \cong \mathbb{Z}_2 \cong G_2/H_2$$

但 H_1 和 H_2 不同构。
(iii) 取 $\langle c \rangle \cong \langle a \rangle$，令

$$G_1 = \langle a \rangle \times \langle c \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$G_2 = \langle b \rangle, H_1 = \langle a \rangle \cong \mathbb{Z}_2, H_2 = \langle 2b \rangle \cong \mathbb{Z}_2$$

此时 $G_1/H_1 \cong G_2/H_2 \cong \mathbb{Z}_2$，但是 G_1 和 G_2 不同构。

8 对于 S_3，同构意义下其非平凡子群只有两个：三轮换和对换循环群，分别同构于 $\mathbb{Z}_3$ 和 $\mathbb{Z}_2$. 由于 $\mathbb{Z}_2 \times \mathbb{Z}_3$ 是交换群，而 S_3 不是，从而可知不可分解。

对于 $\mathbb{Z}$ 是无限循环群，其非平凡子群同构于 $\mathbb{Z}$，如果可分解则有子群 $\mathbb{Z} \cong \mathbb{Z} \times \mathbb{Z}$，但秩不相等，所以不可分解。

对于 $\mathbb{Z}_{p^n}$，其非平凡子群同构于 $\mathbb{Z}_{p^k}(0 < k < n)$，如果可分解，则 $\mathbb{Z}_{p^n} = \mathbb{Z}_{p^{k_1}} \times \cdots \times \mathbb{Z}_{p^{k_m}}$，前者有 p^n 阶元，后者元的最大阶数就是 $\{p^{\max(k_i)}\}$ 不互素，所以没有 p^n 阶元。

9 设 F_i 是由集合 S_i 生成的自由阿贝尔群，记

$$F = \bigoplus_{i \in I} F_i = \{(f_i)_{i \in I} | f_i \in F_i, \text{finite } f_i \neq 0\}$$

可交换性是显然的，如果令

$$S = \{(s_i)_{i \in I} | s_i \in S_i, \text{finite } s_i \neq 0\}$$

那么 S 中任意元素不可约，因为单独地来看某个分量不可约。F 中的某个元素 f 的非 0 分量有限，所以可以表示成形如

$$(s_i)_{i \in I}, \text{only } 0 \neq s_{n_k} \in S_{n_k}$$

的有限和，而这些元素都可以被 S 中的自由元生成，所以 F 是自由群，进而是自由阿贝尔群。

10 因为 $H, G_1, G_2 \triangleleft G, H \cap G_i = \{1\}$，故 H 中任一元与 G_i 中任一元可交换，因此 H 与 G 中元素可交换，即 $H \leqslant Z(G)$.

11 (1) 充分性：设 $F = \langle a \rangle$，则 $F = F(\{a\})$，是自由阿贝尔群。
必要性：设 $F = F(S)$，假设 $a, b \in S$，则文字 $ab = ba \Rightarrow a = b$，所以只能 $S = \{a\}$，进而 $F = \langle a \rangle$ 是循环群。

(2) 必要性：否则有无限阶元，则 G 一定是无限群。
充分性：设 $g_1,\cdots,g_n$ 是阿贝尔群 G 的一族生成元，且阶分别为 $m_1,\cdots,m_n$. 则 $G=\mathbb{Z}g_1+\cdots+\mathbb{Z}g_n$. 令 $F=\mathbb{Z}x_1\oplus\cdots\oplus\mathbb{Z}x_n$ 是 n 秩自由阿贝尔群，

$$\pi:F\to G$$

$$\pi(x_i)=g_i,\forall i=1,2,\cdots,n$$

是满的群同态，则由题设可知

$$\mathrm{Ker}\pi\supset m_1\mathbb{Z}x_1\oplus\cdots\oplus m_n\mathbb{Z}x_n$$

因此下列群同态是满的：

$$\mathbb{Z}_1\oplus\cdots\oplus\mathbb{Z}_n\cong\mathbb{Z}x_1\oplus\cdots\oplus\mathbb{Z}x_n/m_1\mathbb{Z}x_1\oplus\cdots\oplus m_n\mathbb{Z}x_n\to G$$

左边是有限群，故 G 是有限群。
(3) 必要性：由定义可知自由阿贝尔群的每个非零元都是无限阶的。
充分性：设 $G=\langle g_1,\cdots,g_n\rangle$，$G=\mathbb{Z}g_1+\cdots+\mathbb{Z}g_n$. 不妨设 $\{g_1,\cdots,g_m\}$ 是 $\{g_1,\cdots,g_m\}$ 的一个极大 $\mathbb{Z}$-线性无关组，于是对于任一 $g_{m+i},1\leqslant i\leqslant n-m$，存在非零的 $\lambda_i\in\mathbb{Z}$ 使得

$$\lambda_i g_{m+i}\in\mathbb{Z}g_1+\cdots+\mathbb{Z}g_m=\mathbb{Z}g_1\oplus\cdots\oplus\mathbb{Z}g_m$$

令 $\lambda=\lambda_1\cdots\lambda_{n-m}\in\mathbb{Z}$，则

$$\lambda G\leqslant\mathbb{Z}g_1\oplus\cdots\oplus\mathbb{Z}g_m$$

但是 $\mathbb{Z}g_1\oplus\cdots\oplus\mathbb{Z}g_m$ 是有限生成自由阿贝尔群，故 λG 亦是有限生成自由阿贝尔群。令

$$\pi:G\to\lambda G,g\mapsto\lambda g$$

由题设知 $\mathrm{Ker}\pi=0$. 即 $G\cong\lambda G$，故 G 是自由群。

12 记 $g_{n+i}=g_i^{-1}$，右陪集分解：

$$G=Aa_1\sqcup\cdot\sqcup Aa_m$$

并设 $a_1=1$. 则对于任意的 i,j，$1\leqslant i\leqslant m$，$1\leqslant j\leqslant 2n$，存在唯一的 k，$1\leqslant k\leqslant m$ 和 $b_{ij}\in A$ 使得

$$a_ig_j=b_{ij}a_k$$

令 B 是由 $2nm$ 个元 b_{ij} 生成的子群，则 B 是 A 的子群。因为 $g_j=a_i^{-1}b_{ij}a_k$，故 G 可以由 b_{ij} 和 a_i 生成，$1\leqslant i\leqslant m,1\leqslant j\leqslant 2n$，即 G 由 B 和 $a_1,\cdots,a_m$ 生成。

下证 $G=Ba_1\cup\cdots\cup Ba_m$ 是 G 关于 B 的右陪集分解。

因为 $Aa_i\cap Aa_j=\varnothing,i\neq j$，故 $Ba_i\cap Ba_j=\varnothing,i\neq j$.

其次要证 G 中任一元属于某一 Ba_i. 因为 $G=\langle g_1,\cdots,g_n\rangle$，故 G 中任一元可以写成 $g_1,\cdots,g_n,g_{n+1},\cdots,g_{2n}$ 的某种积。因为任一 $g_j=b_{1j}a_k$，故只要证形如 a_sx 的元属于某一 Ba_i，其中 x 是 $g_1,\cdots,g_n,g_{n+1},\cdots,g_{2n}$ 的某种积，不断应用 $a_sg_j=b_{sj}a_k$ 即可。

因此 $[G:B]=m$，而 $[G:B]=[G:A][A:B]=m[A:B]$，于是 $[A:B]=1$，即 $A=B$，所以 A 是由 $2nm$ 个元 b_{ij} 生成的。

13 设 N 是 $G_1 \times G_2$ 的非平凡正规子群。

若 $G_1 \cap N = G_1$，也就是 $G_1 \leqslant N$，则 $N = G_1 \times (N \cap G_2)$，由于 G_2 是单群，而且 $N \neq G_1 \times G_2 \Rightarrow N \cap G_2 \neq G_2$，因此 $N \cap G_2$ 只能是 $\{1\}$，从而 $N = G_1$.

若 $G_1 \cap N = \{1\}$，则 G_1 中任一元与 N 中任一元可交换。令

$$H_1 = \{g_1 \in G_1 | 存在 g_2 \in G_2 使得 g_1 g_2 \in N\}$$

则 $H_1 \triangleleft G_1$. 于是 $H_1 = \{1\}$ 或者 G_1，如果是前者则 $N = G_2$，如果是后者，则对于任一 $x \in G_1$ 和任一 $g_1 \in G_1$，存在 $g_2 \in G_2$ 使得 $g_1 g_2 \in N$，从而 x 与 $g_1 g_2$ 可交换。但 x 与 g_2 也可交换，因此 x 与 g_1 可交换。所以 G_1 是阿贝尔群，与题设不合。

第十次作业

1 类比三百题 1.10.1.

$108 = 2^2 \times 3^3$，共有 6 个互不同构的 108 阶交换群，如下：

$$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^3} \cong \mathbb{Z}_{108}$$

$$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_{3^1} \cong \mathbb{Z}_{36} \oplus \mathbb{Z}_3$$

$$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{3^1} \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

$$\mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{3^3} \cong \mathbb{Z}_{54} \oplus \mathbb{Z}_2$$

$$\mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_{3^1} \cong \mathbb{Z}_{18} \oplus \mathbb{Z}_6$$

$$\mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{3^1} \oplus \mathbb{Z}_{3^1} \cong \mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_3$$

2 三百题 1.10.9.

若 $(m, n) = 1$，则互质，于是 $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$，故其不变因子组为 $\{mn\}$.

若 $(m, n) > 1$，不妨设

$$m = p_1^{t_1} \cdots p_l^{t_1}, n = p_1^{s_1} \cdots p_l^{s_l}$$

这里 $p_1, \cdots, p_l$ 是互不相同的素数，$t_1, \cdots, t_l, s_1, \cdots, s_l$ 是非负整数，对于 $\forall i$，t_i 和 s_i 不同时为零。于是

$$\mathbb{Z}_m = \mathbb{Z}_{p_1^{t_1}} \oplus \cdots \oplus \mathbb{Z}_{p_l^{t_l}}$$

$$\mathbb{Z}_n = \mathbb{Z}_{p_1^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p_l^{s_l}}$$

因此，$\mathbb{Z}_m$ 和 $\mathbb{Z}_n$ 的初等因子组是从

$$(p_1^{t_1}, p_1^{s_1}, \cdots, p_l^{t_l}, p_l^{s_l})$$

中删去为 1 的因子后得到的数组，从而其不变因子为

$$\prod_{i=1}^{l} p_i^{\min(t_i, s_i)}, \prod_{i=1}^{l} p_i^{\max(t_i, s_i)}$$

前者即 (m, n)，后者为最小公倍数 $[m, n]$，故不变因子组为 $\{(m, n), [m, n]\}$.

3 三百题 1.10.7.

设 $A=G_1\oplus\cdots\oplus G_m$，其中 G_i 是 A 的 Sylow$p$-子群。则

$$H=H_1\oplus\cdots\oplus H_m, H_i=H\cap G_i, 1\leqslant i\leqslant m$$

因为

$$A\backslash H\cong G_1\backslash H_1\oplus\cdots\oplus G_m\backslash H_m$$

故只要证明 G_i 有子群与 $G_i\backslash H_i$ 同构即可，不妨设 $|A|=p^n, n\geqslant 1, |H|=p^m, m\leqslant n$.

由 Abel$p$-群的结构可知

$$A=\mathbb{Z}_{p^{r_1}}\oplus\cdots\oplus\mathbb{Z}_{p^{r_t}}$$

$$H=\mathbb{Z}_{p^{s_1}}\oplus\cdots\oplus\mathbb{Z}_{p^{s_t}}$$

其中 $\mathbb{Z}_{p^{s_i}}\leqslant\mathbb{Z}_{p^{r_i}}, \forall 1\leqslant i\leqslant t, r_1+\cdots+r_t=n, s_1+\cdots+s_t=m, r_i\in\mathbb{N}_+, s_i\in\mathbb{N}, s_i\leqslant r_i$. 因此

$$A\backslash H\cong\mathbb{Z}_{p^{r_1-s_1}}\oplus\cdots\oplus\mathbb{Z}_{p^{r_t-s_t}}\leqslant A$$

4 三百题 1.10.6.

只需证明因为 A 是其 Slyow$p$-子群的直和，故只需要对 p-群证明此结论即可。

$$H=H_1\oplus\cdots\oplus H_m, H_i=H\cap G_i, 1\leqslant i\leqslant m$$

因为

$$A/H\cong G_1/H_1\oplus\cdots\oplus G_m/H_m$$

故只要证明 G_i 有子群与 G_i/H_i 同构即可，不妨设 $|A|=p^n, |H|=p^m$. 由 Abel$p$-群的结构知

$$A=\mathbb{Z}_{p^{r_1}}\oplus\cdots\oplus\mathbb{Z}_{p^{r_t}}, H=\mathbb{Z}_{p^{s_1}}\oplus\cdots\oplus\mathbb{Z}_{p^{s_t}}$$

其中 $\mathbb{Z}_{p^{s_i}}\leqslant\mathbb{Z}_{p^{r_i}}, 1\leqslant i\leqslant t, r_1+\cdots+r_t=n, s_1+\cdots+s_t=m, r_i\in\mathbb{N}_+, s_i\in\mathbb{N}, s_i\leqslant r_i$. 因此

$$A/H\cong\mathbb{Z}_{p^{r_1-s_1}}\oplus\cdots\oplus\mathbb{Z}_{p^{r_t-s_t}}\leqslant A$$

5 记乘法幺元 1 的加法逆元为 -1，

$$\begin{aligned}a+b+(-1)(a+b)&=0\\ a+b+(-a-b)&=0\\ a+b&=b+a\end{aligned}$$

加法交换律得证。

6 习题课九 4.

(1) 全体偶数 $2\mathbb{Z}$ 对整数加法和乘法构成环，无左单位元也无右单位元。

(2) 对于数域 $\mathbb{F}$，定义

$$R=\left\{\begin{pmatrix}a&b\\0&0\end{pmatrix}:a,b\in\mathbb{F}\right\}$$

R 对于矩阵加法和乘法构成环，$\begin{pmatrix}1&0\\0&0\end{pmatrix}$ 是左单位元之一，假设存在右单位元 $\begin{pmatrix}x&y\\0&0\end{pmatrix}$，但

$$\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}x&y\\0&0\end{pmatrix}=\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}1&1\\0&0\end{pmatrix}\begin{pmatrix}x&y\\0&0\end{pmatrix}=\begin{pmatrix}1&1\\0&0\end{pmatrix}$$

矛盾。

(3) 对于数域 $\mathbb{F}$，定义

$$R=\left\{\begin{pmatrix}a & 0\\ b & 0\end{pmatrix}:a,b\in\mathbb{F}\right\}$$

类似地可证 R 无左单位元。

7 习题课九 5.

(1) $R=\mathbb{Z}$，其子环 $S=2\mathbb{Z}$ 无单位元。

(2) 上一题第二问里的 $R=\left\{\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}:a,b\in\mathbb{F}\right\}$ 无单位元，其子环 $S=\left\{\begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix}:a\in\mathbb{F}\right\}$ 有单位元。

(3) $R=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}:a,b,c,d\in\mathbb{Z}\right\}$ 的单位元是

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

但是其子环 $S=\left\{\begin{pmatrix}a & a\\ 0 & 0\end{pmatrix}:a\in\mathbb{Z}\right\}$，其单位元之一是

$$\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix}$$

8 A 是左零因子，即 $\exists B$ s.t. $AB=0\Leftrightarrow Ax=0$ 有非零解 $\Leftrightarrow \mathrm{rank}(A)<n\Leftrightarrow A$ 的行向量线性相关 $\Leftrightarrow xA=0$ 有非零解 $\Leftrightarrow \exists B$ s.t. $BA=0$，即 A 是右零因子。

第十一次作业

1

(a) 因为 $(R,+)$ 和 $(\mathbb{Z},+)$ 为加法群，所以 $(S,+)$ 也是加法群。

(b) $\forall(r_1,n_1),(r_2,n_2),(r_3,n_3)\in S$，

$$\begin{aligned}&[(r_1,n_1)\cdot(r_2,n_2)]\cdot(r_3,n_3)\\ &=(r_1r_2+n_2r_1+n_1r_2,n_1n_2)\cdot(r_3,n_3)\\ &=(r_1r_2r_3+n_2r_1r_3+n_1r_2r_3+r_1r_2n_3+n_2r_1n_3+n_1r_2n_3+n_1n_2r_3,n_1n_2n_3)\\ &=(r_1,n_1)\cdot(r_2r_3+n_3r_2+n_2r_3,n_2n_3)\\ &=(r_1,n_1)\cdot[(r_2,n_2)\cdot(r_3,n_3)]\end{aligned}$$

满足结合律，故 $(S,\cdot)$ 为半群。

(c) $\forall(r_1,n_1),(r_2,n_2),(r_3,n_3)\in S$，

$$\begin{aligned}(r_1,n_1)\cdot[(r_2,n_2)+(r_3,n_3)]&=(r_1,n_1)\cdot(r_2+r_3,n_2+n_3)\\ &=(r_1r_2+r_1r_3+r_1n_2+r_1n_3+n_1r_2+n_1r_3,n_1n_2+n_1n_3)\\ &=(r_1r_2+r_1n_2+n_1r_2,n_1n_2)+(r_1r_3+r_1n_3+n_1r_3,n_1n_3)\\ &=(r_1,n_1)\cdot(r_2,n_2)+(r_1,n_1)\cdot(r_3,n_3)\end{aligned}$$

满足分配律。

(d) $(0,1)$ 是一个乘法幺元，因为 $\forall(r,n)\in S$，

$$(0,1)(r,n)=(0r+0n+1r,1n)=(r,n)$$

$$(r,n)(0,1)=(0r+0n+1r,1n)=(r,n)$$

所以 $(R,+,\cdot)$ 是一个含幺环。

2 记 $R=\mathrm{End}(G)$，

(a) 因为 G 是加法群，R 关于映射的加法满足：

1° 封闭：$(f+g)(a)=f(a)+g(a)\in G,\forall a\in G\Rightarrow f+g\in R.$

2° 结合律：$[(f+g)+h](a)=f(a)+g(a)+h(a)=[f+(g+h)](a),\forall a\in G\Rightarrow (f+g)+h=f+(g+h).$

3° 存在加法零元：定义群 G 的同态 $0_R:a\mapsto 0_G$，则 $\forall f\in R, f+0_R=0_R+f=f.$

4° 存在加法逆元：对于 $f\in R:a\mapsto f(a)$，定义 $-f:G\to G,a\mapsto -f(a)$，则 $f+(-f)=(-f)+f=0_R.$

5° 交换律：$(f+g)(a)=f(a)+g(a)=g(a)+f(a)=(g+f)(a),\forall a\in G\Rightarrow f+g=g+f.$

所以 $(R,+)$ 是一个加法群。

(b) 乘法半群：封闭性显然；题目中定义的映射的乘法即映射的复合，满足结合律。

(c) 分配律：$f\cdot(g+h)(a)=f(g(a)+h(a))=f\cdot g(a)+f\cdot h(a),\forall a\in G\Rightarrow f\cdot(g+h)=f\cdot g+f\cdot h.$ 满足分配律。

(d) 乘法幺元：恒等映射 $\mathrm{Id}_G\in R$，满足 $\mathrm{Id}_G\cdot f=f\cdot\mathrm{Id}_G=f$，为乘法幺元。

所以 $(R,+,\cdot)$ 是一个含幺环。

3 (1) 设 R 是有限整环，不妨设 $R=\{r_0,r_1,\cdots,r_n\}$，且 $r_0=0_R,r_1=1_R$，令 $G=\{r_1,\cdots,r_n\}$，由于 R 不含零因子，所以 G 关于乘法封闭，且满足结合律，且含幺即 r_1，所以 G 构成一个有限含幺半群。又因为 $\forall r_a,r_b,r_c\in G$，

$$\begin{aligned} r_a\neq r_b\Rightarrow r_a-r_b\neq 0_G &\Rightarrow r_a-r_b\in G\\ &\Rightarrow (r_a-r_b)r_c=r_ar_c-r_br_c\neq 0_G\\ &\Rightarrow r_ar_c\neq r_br_c \end{aligned}$$

所以

$$r_ar_c=r_br_c\Rightarrow r_a=r_b$$

为左消去律，同理可证右消去律。由第二次作业 6. 可知有限半群满足双边消去律则为群，进而可知 $G=u(R)$，从而 R 是一个域。

(2) $\mathbb{Z}_m$ 是域当且仅当 m 是质数。

充分性：当 m 是质数，则任意 $0\neq\overline{n}\in\mathbb{Z}_m$，$n$ 与 m 互质，存在整数 p,q 使得 $pn+qm=1$，则 $pn=1-qm$，$\overline{pn}=\overline{1}$，$\overline{p}$ 即为 $\overline{n}$ 的乘法逆元，所以环 $\mathbb{Z}_m$ 任意非零元素都可逆，所以是域。

必要性：$\mathbb{Z}_m$ 是域时，假设 m 不是质数，不妨设 $m=pn$，$p<m$ 为质数，则 $0\neq\overline{p}\in\mathbb{Z}_m$ 存在乘法逆元，不妨 $pq=m+1\Rightarrow p(n-q)=1\Rightarrow p=n-q=1$，矛盾。所以 m 是质数。

4 (1) 只需证明 $\mathbb{Q}[\sqrt{2}]\subset\mathbb{R}$ 关于实数加法和乘法构成域。因为

(a) $\mathbb{Q}[\sqrt{2}]$ 是加法群：

1° 封闭：$(f+g)(a)=f(a)+g(a)\in G,\forall a\in G\Rightarrow f+g\in R.$

2° 结合律：实数加法满足结合律。

3° 存在加法零元：$\exists 0 \in \mathbb{Q}[\sqrt{2}]$.
4° 存在加法逆元：$\exists(-a-b\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$，$a+b\sqrt{2}+(-a-b\sqrt{2})=0$.
5° 交换律：实数加法满足交换律。

(b) 乘法半群：实数乘法满足结合律，只需验证封闭性：

$$(a+b\sqrt{2})(c+d\sqrt{2}) = ac+2bd+(ad+bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

(c) 分配律：实数加法、乘法满足分配律。
(d) 乘法幺元：$\exists 1 \in \mathbb{Q}[\sqrt{2}]$.
所以 $\mathbb{Q}[\sqrt{2}]$ 构成环，其非零元 $a+b\sqrt{2}$ 存在逆元

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} \in \mathbb{Q}[\sqrt{2}]$$

所以是域。

(2) $\mathbb{Z}_m$ 的子环必为循环群 $\mathbb{Z}_m$ 的子群，从而形如 $\mathbb{Z}_r$. 设 m 的所有因数为

$$1 = m_0 < m_1 < \cdots < m_k < m_{k+1} = m$$

于是

$$m_i\mathbb{Z}_m = \{\overline{0}, \overline{m_i}, \cdots, \overline{m/m_i - 1}\} \cong \mathbb{Z}_{m/m_i}, i = 1, 2, \cdots, k$$

为 $\mathbb{Z}$ 的所有子环。

(3) 由于 $\mathbb{Q}$ 的子域只有其本身，所以 $\mathbb{Q}[\sqrt{2}]$ 的子域 T 都包含 $\mathbb{Q}$，若存在 $t = a+b\sqrt{2} \in T$，则 $\sqrt{2} = \frac{t-a}{b} \in T$，从而 $T = \mathbb{Q}[\sqrt{2}]$，所以 $\mathbb{Q}[\sqrt{2}]$ 的子域只有 $\mathbb{Q}[\sqrt{2}]$ 和 $\mathbb{Q}$.

5 如果 $b \neq c$ 都是 a 的右逆，则 $a(b-c)=0$，a 是左零因子，且 $b-c \in I = \{x \in R : ax = 0\} \neq \{0\}$，则 $\forall x \in I$，$a(x+b) = ax+ab = 1$，$x+b$ 是 a 的右逆。只需证明 I 为无限集即可。
否则，假设 $I = \{0, x_1, \cdots, x_n\}$，$\forall i$，

$$a \cdot x_i a = 0a = 0 \Rightarrow x_i a \in I$$

$$x_i a \cdot b = x_i \neq 0 \Rightarrow x_i a \neq 0$$

所以 $(x_i x_1, \cdots, x_i x_n)$ 是 $(x_1, \cdots, x_n)$ 的置换。又因为

$$a \cdot (ba-1) = aba - a = 0 \Rightarrow ba - 1 \in I$$

因为 a 没有左逆，所以 $ba-1 \neq 0$，不妨 $ba-1 = x_i$，

$$x_i b = (ba-1)b = 0$$

而存在 x_j 使得 $x_i = x_j a$，从而 $x_i b = x_j ab = x_j \neq 0$，矛盾。

6 设 $1-ab$ 的逆元为 c，则

$$(1-ba)(1+bca) = 1-ba+(b-bab)ca = 1-ba+b(1-ab)ca = 1-ba+ba = 1$$

$$(1+bca)(1-ba) = 1-ba+bc(a-aba) = 1-ba+bc(1-ab)a = 1-ba+ba = 1$$

即 $1+bca$ 就是 $1-ba$ 的逆元。

7 由题设可知，映射 i 是唯一的，而 $\forall(r,n)\in R\times\mathbb{Z}$，只能是

$$g(r,n)=g(r,0)+n\cdot g(0,1)=f(r)+n\cdot 1_S$$

于是 g 由 f 唯一确定。下面证明 $g:(r,n)\mapsto f(r)+n\cdot 1_S$ 是一个同态：

$$g(r_1,n_1)+g(r_2,n_2)=f(r_1+r_2)+(n_1+n_2)\cdot 1_S=g(r_1+r_2,n_1+n_2)$$

$$\begin{aligned}g(r_1,n_1)g(r_2,n_2)&=f(r_1)f(r_2)+n_2\cdot f(r_1)+n_1\cdot f(r_2)+n_1n_2\cdot 1_S\\&=g(r_1r_2+n_2r_1+n_1r_2,n_1n_2)=g((r_1,n_1)(r_2,n_2))\end{aligned}$$

8 L 中非零元都可逆：$\forall 0\neq\begin{pmatrix}z&w\\-\overline{w}&\overline{z}\end{pmatrix}\in L$，$|z|^2+|w|^2>0$，

$$\begin{pmatrix}z&w\\-\overline{w}&\overline{z}\end{pmatrix}^{-1}=\frac{1}{|z|^2+|w|^2}\begin{pmatrix}\overline{z}&-w\\\overline{w}&z\end{pmatrix}$$

所以是除环。

定义映射 $f:\mathbb{H}\to L$，

$$a+bi+cj+dk\mapsto\begin{pmatrix}a+bi&c+di\\-c+di&a-bi\end{pmatrix}$$

则 f 是一个环同构。

9

(1) $f:\mathbb{Z}\to 2\mathbb{Z},n\mapsto 2n.$

(2) $f:\mathbb{Z}_m\to 2\mathbb{Z}_m,\overline{n}\mapsto\overline{2n}.$

(3) 假设 $f(1_R)=s\neq 1_S$，因为是满射所以存在 $f(r)=1_S$，进而 $f(r)f(1_R)=s=f(r)$，矛盾。

(4) 假设 $f(1_R)=s$，设 $u\in R$ 可逆，于是 $f(u)f(u^{-1})=s$，则

$$s=f(u)f(u^{-1})=f(1_R)\cdot f(u)f(u^{-1})=s\cdot f(u)f(u^{-1})$$

$\Rightarrow f(u)f(u^{-1})=s=1_S$，故 $f(1_R)=1_S$，$f(u)f(u^{-1})=1_S\Rightarrow f(u)^{-1}=f(u^{-1}).$

10

(1) $ij\in IJ,r\in R\Rightarrow ijr=i\cdot(jr)\in IJ,rij=(ri)\cdot j\in IJ$；$i\in I\cap J,r\in R\Rightarrow ir\in I,ir\in J\Rightarrow ir\in I\cap J$，所以 IJ 和 $I\cap J$ 也是 R 的理想。$\forall ij\in IJ,ij\in I,ij\in J\Rightarrow ij\in I\cap J$，所以 $IJ\subset I\cap J$，例子：取整数环 $\mathbb{Z}$ 的两个理想：$I_1=n\mathbb{Z},I_2=m\mathbb{Z}$，则 $I_1I_2=nm\mathbb{Z}$，$I_1\cap I_2=[n,m]\mathbb{Z}$，如果 n,m 互素则相等，不互素时不相等。

(2) $i+j\in I+J,r\in R\Rightarrow(i+j)r=ir+jr\in I+J$，所以 $I+J$ 是理想，而 $I,J\subset I+J$，所以是包含 I，J 的最小理想。

(3) $\forall ij\in IJ,k\in K$，$ij\cdot k=i\cdot jk\in I(JK)\Rightarrow(IJ)K\subset I(JK)$，反之同理。
分配律也成立：由环的分配律可得 $I(J+K)\subset IJ+IK$，设 $i_1,i_2\in I,j\in J,k\in K$，则

$$i_1j+i_2k=i_1(j+k)+(i_2-i_1)k\in I(J+K)+IK$$

$$\Rightarrow IJ+IK\subset I(J+K)+IK$$

由于 $IK\subset I(J+K)$，所以实际上 $I(J+K)+IK=I(J+K)$，故 $IJ+IK=I(J+k).$

11

(1) $\forall A=(a_{ij})\in M_n(I), B=(b_{ij})\in M_n(R)$

$$C=AB=(c_{ij}), c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj}\in I\Rightarrow C\in M_n(I)$$

同理 $BA\in M_n(I)$，所以 $M_n(I)$ 是 $M_n(R)$ 的理想。

(2) 任取 $r\in R, a\in E(J)$，考虑 $A=\mathrm{diag}(a,0,\cdots,0)\in J$，$S=\mathrm{diag}(r,0,\cdots,0)\in M_n(R)\Rightarrow AS=\mathrm{diag}(ar,0,\cdots,0)\in J\Rightarrow ar\in E(J)$，同理 $ra\in E(J)$，所以 $E(J)$ 是 R 的理想。要证明 $J=M_n(E(J))$，显然 $J\subset M_n(E(J))$，只需说明 $M_n(E(J))$ 是 R 的理想，由第一问结论可知得证。

(3) 由前两问可知，I 是 R 的理想 $\Leftrightarrow M_n(I)$ 是 $M_n(R)$ 的理想，所以 $I\mapsto M_n(I)$ 是满射，由 $I\mapsto M_n(I)$ 的构造方式可知是单射，故为双射。

第十二次作业

1

(a) 设 $p(x)=a_nx^n+\cdots+a_0\in\mathbb{Z}[x]$，

$$\begin{aligned}p(\sqrt{2})&=a_n(\sqrt{2})^n+\cdots+a_0\\&=\sqrt{2}(a_1+2a_3+\cdots)+(a_0+2a_2+\cdots)\in\mathbb{Z}[\sqrt{2}]\end{aligned}$$

于是构造环同态：

$$f:\mathbb{Z}[x]\to\mathbb{Z}[\sqrt{2}], p(x)\mapsto p(\sqrt{2})$$

f 满显然，因为 $a+bx\mapsto a+b\sqrt{2}$，而 $\mathrm{Ker}f=(x^2-2)\mathbb{Z}[x]$，即 x^2-2 生成的理想，由环同态基本定理可知 $\mathbb{Z}[x]/(x^2-2)\cong\mathbb{Z}[\sqrt{2}]$. 同理可知 $\mathbb{Z}[x]/(x^2-3)\cong\mathbb{Z}[\sqrt{3}]$，但 $\forall x\in\mathbb{Z}[\sqrt{3}]$，$x^2\neq 2$，故不同构。

(b) 设 $a=z_1\cdot\overline{0}+z_2\cdot\overline{1}=z_1x+z_2y\in\mathbb{C}[\mathbb{Z}_2]$ 是幂等元，则

$$(z_1x+z_2y)^2=(z_1^2+2z_1z_2)x+z_2^2y$$

$\Rightarrow a=0,x,y,-x+y$ 是幂等元。其中 y 是乘法幺元，x 是中心幂等元，因此由三百题 2.3.7，

$$\mathbb{C}[\mathbb{Z}_2]\cong x\mathbb{C}[\mathbb{Z}_2]\cong(y-x)\mathbb{C}[\mathbb{Z}_2]\cong\mathbb{C}[x]\times\mathbb{C}[y-x]\cong\mathbb{C}\times\mathbb{C}$$

最后一步的同构，由 x 和 $y-x$ 都是幂等元得到。

(c) $2(x^2-3)+(2-x)(2x+4)(2x+4)=2$，所以 $2\in(x^2-3,2x+4)$，因此

$$\mathbb{Z}[x]/(x^2-3,2x+4)\cong\mathbb{Z}/(x^2-1,2)\cong\mathbb{Z}_2/(x^2-1)$$

实际上，$\mathbb{Z}_2$ 中 $x^2-3=x^2-2x+1=(x-1)^2$，所以 $\mathbb{Z}_2/(x^2-1)\cong\mathbb{Z}_2/((x-1)^2)\cong(\mathbb{Z}_2+1)/(x^2)=\mathbb{Z}_2/(x^2)$.

2

(a) 第十一次作业 3.(1) 里“有限整环 $\Rightarrow$ 域”，实际上证明了含幺有限环且不含零因子 $\Rightarrow$ 非零元都可逆，即除环。

(b) 除环 K 是单环，则 K 只有平凡理想，所以 $\mathrm{Ker}f=\{0\}$ or K，进而 f 是单射或者 $f=0$. $M_n(K)$ 是否单？

(c) R/m 是除环，则一定只有平凡理想，因为任一非零理想 $I \ni x \neq 0$，$x \cdot x^{-1} = 1 \in I \Rightarrow I = R/m$. 因此 m 是极大理想。

3

(a) (i) 不妨设 $f : R \to S = \mathrm{Im}f$，$I$ 是 S 的一个理想，则考虑 $J = f^{-1}(I)$，给定 $a \in J, \forall r \in R$ 有

$$f(ar) = f(a)f(r) \in I \Rightarrow ar \in J$$

同理 $ra \in J$，因此 J 是 R 的理想，不妨 $J = r_1R$，于是 $I = f(r)S$，S 也是主理想环。

(ii) $\mathbb{Z}_1$ 平凡，考虑 $m \geqslant 2$，不妨设 $\mathbb{Z}_m$ 的一个理想是 $I = (a, b)$，$\exists n_1, n_2$ s.t. $n_1a + n_2b = \gcd(a, b) = c$，进而 $I = (c)$，所以 $\mathbb{Z}_m$ 是主理想整环。

(iii) 一个基本事实是：环的满同态把理想映到理想，把子环映到子环。

(1) 设 $s_1s_2 \in f(P)$, 因为是满同态, 所以存在 $r_1, r_2 \in R$ 使得 $f(r_1) = s_1, f(r_2) = s_2$，进而 $s_1s_2 = f(r_1r_2) \in f(P)$，此时可得存在一个 $r \in P$ 使得

$$f(r) - f(r_1r_2) = 0 \Rightarrow r - r_1r_2 \in \mathrm{Ker}f \subset P \Rightarrow r_1r_2 \in P$$

因为 P 是素理想，可得 $r_1 \in P$ or $r_2 \in P$，所以 $s_1 \in f(P)$ or $s_2 \in f(P)$，进而 $f(P)$ 是素理想。

(2) $r_1r_2 \in f^{-1}(Q) \in f(r_1r_2) = f(r_1)f(r_2) \in Q \Rightarrow f(r_i) \in Q \Rightarrow r_i \in f^{-1}(Q) \Rightarrow r_i \in f^{-1}(Q) \Rightarrow f^{-1}(Q)$ 为素理想。其中 r_i 代表 r_1 或 r_2.

(3) 结合前两问结论即得证。

关于极大理想：(1) 实际上证明了 $\mathrm{Ker}f \subset P$ 则 $f(r) \in f(P) \Rightarrow r \in P$，即 $f^{-1}(f(P)) = P$. 所以如果有一个比 $f(P)$ 更大的理想 Q，$f^{-1}(Q)$ 就是一个比 P 更大的理想，从而矛盾；(2) 则自然地满足这个性质，因为 $\mathrm{Ker}f^{-1} = 0 \subset Q$.

(iv) $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$，考虑满的环同态：

$$f = \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, n \mapsto \overline{n}$$

$\mathbb{Z}$ 的非零素理想都为 $p\mathbb{Z}$，p 为素数，$m\mathbb{Z} \subset p\mathbb{Z}$ 当且仅当 $p|m$，由 (iii) 可知，$\mathbb{Z}$ 的素理想全体为

$$\{\{0\}, p\mathbb{Z}/m\mathbb{Z} : p|m, p\text{素}\}$$

极大理想亦然。

(b) 令 I 是 $\mathbb{C}[[x]]$ 的非零理想，$f = \sum_{i=s}^{\infty} a_i x^i \in I$ 是其中 s 最小的元素，则 $I \subset (x^s)$. 另一方面，$f = x^s \sum_{i=0}^{\infty} a_{i+s}x^i = x^s g$，且 g 可逆，故 $(x^s) \subset I$，从而 $I = (x^s)$. 因此，$\mathbb{C}[[x]]$ 的全体非零理想就是 $\{\{0\}, (x^s) : s \in \mathbb{N}\}$

4 (a) 设 $(a), (b)$ 是 R 的理想，且 $a \notin I, b \notin I$，由 I 的极大性可知，$((a) + I) \cap S$ 和 $((b) + I) \cap S$ 非空，不妨其分别包含元素 s_1, s_2，由于 S 是乘法子集，$s_1s_2 \in S$，同时 $s_1s_2 \in ((a) + I)((b) + I)$，因此 $s_1s_2 \in S \cap ((a) + I)((b) + I)$，进而 $s_1s_2 \in (a)(b) + I$，而 $s_1s_2 \notin I \Rightarrow (a)(b) \nsubseteq I$，即 $ab \notin I$，所以 I 是素理想。

(b) R 含幺交换，m 是真极大理想 $\Rightarrow R/m$ 为非平凡域，所以 $\forall r \notin m$，不妨 $r \neq 0$，则存在 r^{-1}，取 $x \in R$ 使得 $x = r^{-1} - m_0, m_0 \in m, r^{-1} - x \in m$，则

$$(r^{-1} - x)r = 1 - rx \in m$$

反之，假设存在一个更大的理想 M，$r \in M$ 但 $r \notin m$，则存在一个 $x \in R$ 使得 $1 - rx \in m \subset M$，$rx \in M \Rightarrow 1 \in M \Rightarrow R = M$，故 m 是极大理想。

(c) (i) $4\mathbb{Z}/(8)=\{\overline{0},\overline{4}\}$，非零元 $\overline{4}$ 不可逆。
(ii)
(d) (i) 假设 $ab\in I$，且 $a\notin I$，考虑极大理想的定义一定有，$I+(a)=R$，由此，存在 $x\in I$ 和 $y\in R$，使得 $x+ay=1$。将等式两边同时左乘 b，得到 $xb+aby=b$。由于 $ab\in I$，而 xb 和 aby 都属于 I，所以 b 属于 I。因此 I 是素理想。
不含幺则不一定，例如 $2\mathbb{Z}_4$ 的极大理想 (4) 不是素理想。
(ii) 含幺交换有限环 R 的素理想 $I\Rightarrow R\backslash I$ 是有限整环 $\Rightarrow R\backslash I$ 是域 $\Rightarrow I$ 是极大理想。

5

$$\frac{r_1'}{s_1'}=\frac{r_1}{s_1},\frac{r_2'}{s_2'}=\frac{r_2}{s_2}\Rightarrow\exists s,t\text{ s.t. }s(r_1's_1-r_1s_1')=t(r_2's_2-r_2s_2')=0$$

令 $s'=st$，不难验证：

$$s'((r_1s_2+r_2s_1)s_1's_2'-(r_1's_2'+r_2's_1')s_1s_2)=0$$

$$s'(r_1r_2s_1's_2'-r_1'r_2's_1s_2)=0$$

可知

$$\frac{r_1}{s_1}+\frac{r_2}{s_2}=\frac{r_1'}{s_1'}+\frac{r_2'}{s_2'}$$

$$\frac{r_1}{s_1}\frac{r_2}{s_2}=\frac{r_1'}{s_1'}\frac{r_2'}{s_2'}$$

6 (a) 前两问三百题 2.2.1，第三问 2.2.2，第五问未知。
(b) 习题课 11.
(c) 第一问三百题 2.3.3，第二问习题课。
(d) 习题课 11.
(e) 第一问未知，第二问习题课。
(f)

写不动了。

第十三次作业

1 (1) 必要性：R 诣零可得 $\forall r\in R$，存在 $r^n=0$，自然 $\overline{r}=r+N\in R/N$ 满足 $\overline{r}^n=\overline{0}$，$R/N$ 诣零；充分性：任何一个 $r_0\in R$ 可以写成 $r+p\in\overline{r}$，其中 $p\in N$，R/N 诣零可知 $\forall r+p\in\overline{r}$，存在

$$\overline{r}^n=\overline{0}=N\Rightarrow(r+p)^n\in\overline{0}=N$$

由于 N 诣零，所以存在 m 使得 $(r+p)^{nm}=0$，因此 R 诣零。
(2) 设 R 的两个诣零理想是 N 和 I，任取 $r\in N+I$，自然有 $r\in I$，由于 I 诣零所以存在 $r^n=0$，从而 $N+I$ 诣零。

2 设 I 是 R 的一个非零素理想，考虑 $a\in I$，如果 a 是一个可逆元，则 $1\in(a)$，进而主素理想 $(a)\subset I=R$；如果 a 不是单位，则 a 可以唯一分解为不可约元的乘积，设 $a=p_1p_2\cdots p_n$，因为 R 是交换的，所以一定存在某个 $p_i\in I$，进而使得主素理想 $(p_i)\subset I$.

综上，I 总包含了一个非零主素理想。

3 (1) 设 $[a,b]=pa=qb=r(a,b)$，$a=p'(a,b)$，$b=q'(a,b)$，则可得 $pp'=qq'=r$，$ab=p'q'(a,b)^2$，$[a,b](a,b)=r(a,b)^2$. 于是只需证明 $p'q'\sim r$. 由定义，p' 与 q' 最大公因子为 1，p 与 q 的最大公因子为 1，于是由第二问结论，由 $pp'=qq'\Rightarrow q'|pp'\Rightarrow q'|p$，同理 $q|p'$，$p|q'$，$p'|q$，所以 $q\sim p'$，$p\sim q'$，于是 $r=pp'\sim p'q'$.

(2) $a|bc$，把右边写成素因子相乘的形式：

$$p_1^{k_1}\cdots p_n^{k_n}\cdot q_1^{l_1}\cdots q_m^{l_m}$$

其中 $k_i,l_i\geqslant 1$，并设 $a=p_1^{k_1'}\cdots p_n^{k_n'}\cdot q_1^{l_1'}\cdots q_m^{l_m'}$，其中 $0\leqslant k_i'\leqslant k_i$，$0\leqslant l_i'\leqslant l_i$.
由于 $(a,b)=1$，所以 $k_1'=\cdots=k_n'=0$，所以

$$a=q_1^{l_1'}\cdots q_m^{l_m'}|q_1^{l_1}\cdots q_m^{l_m}=c$$

4 (1) $x\in\langle a\rangle\cap\langle b\rangle\Rightarrow x=am=bn\Rightarrow a|x,b|x\Rightarrow[a,b]|x\Rightarrow x=p[a,b]\in\langle[a,b]\rangle$，反过来：$x\in\langle[a,b]\rangle\Rightarrow x=p[a,b]=pma=pnb\Rightarrow x\in\langle a\rangle\cap\langle b\rangle$. 因此 $\langle a\rangle\cap\langle b\rangle=\langle[a,b]\rangle$.
$\langle a\rangle\cap\langle b\rangle=\langle a\rangle\langle b\rangle\Leftrightarrow\langle a\rangle\langle b\rangle=\langle[a,b]\rangle\Leftrightarrow[a,b]\in\langle a\rangle\langle b\rangle,ab\in\langle[a,b]\rangle\Leftrightarrow[a,b]|ab,ab|[a,b]\Leftrightarrow ab\sim[a,b]$，由于 PID⇒UFD，由上一题结论可知 $ab\sim(a,b)[a,b]$，所以 $\langle a\rangle\cap\langle b\rangle=\langle a\rangle\langle b\rangle$ 当且仅当 $(a,b)\sim 1$.

(2) 必要性：如果方程 $ax+by=c$ 有解，$c=mx(a,b)+ny(a,b)\Rightarrow(a,b)|c$.
充分性：设 $c=k(a,b)$，主理想整环里成立裴蜀定理，即存在 $an+bm=(a,b)$，所以 $x=nk,y=mk$ 是方程的解。

5 (1) $1\notin P$，否则 $P=R$，于是 $1\in S_P$. 任取 $x,y\in S_P$，如果 $xy\notin S_P$，则 $xy\in P\Rightarrow x\in P$ 或者 $y\in P$，这与 $x,y\in R-P$ 矛盾。

(2) 先证明一个引理（其实是第十二次作业 5.(c)）：设 P 是 R 的素理想，S 是 R 的乘法子群，且 $P\subset R\backslash S$，同时设 Q 是 $S^{-1}R$ 的素理想，则

1° $S^{-1}P\cap R=\{r\in R|\frac{r}{1}\in S^{-1}P\}=P$. 证明：显然有 $S^{-1}P\cap R\supset P$；设 $r=\in S^{-1}P\cap R$，$\frac{r}{1}=\frac{rs}{s}=\frac{p}{s}\in S^{-1}P$，于是 $rs=p\in P$，P 是素理想所以 $r\in P$ 或 $s\in P$，又因为 $P\subset R\backslash S$，所以 $s\notin P$，从而有 $r\in P$，即 $S^{-1}P\cap R\subset P$，所以二者相等。

2° $S^{-1}(Q\cap R)=\{\frac{r}{s}|r\in R,\frac{r}{1}\in Q\}=Q$. 证明：$\{\frac{r}{1}\in Q|r\in R\}\subset Q$，可知 $S^{-1}(Q\cap R)\subset Q$；设 $\frac{r}{s}\in Q$，则因为 Q 是理想，$\frac{r}{s}\cdot\frac{s}{1}=\frac{r}{1}\in Q$，因此 $\frac{r}{s}\in S^{-1}(Q\cap R)$，于是 $S^{-1}(Q\cap R)\supset Q$，从而二者相等。

3° 结合 1°2°，可知 R 的与 S 无交的素理想 P 与 $S^{-1}R$ 的素理想 $S^{-1}P$ 一一对应。
然后我们来证明 $S_P^{-1}R$ 有唯一极大理想 $S_P^{-1}P$：设 A 是 $S_P^{-1}R$ 的极大理想，进而也是素理想，由引理可得有 R 的素理想 $B\subset R\backslash S=P$ 使得 $A=S_P^{-1}B$，从而

$$A=S_P^{-1}B\subset S_P^{-1}P=S_P^{-1}RP=S_P^{-1}P$$

6 充分性：不妨设 D 中存在非零不可逆元 d，则设 $\langle d,x\rangle=\langle f(x)\rangle$，由 $d\in\langle f(x)\rangle$ 可知 $f(x)$ 是常数，记作 c，于是 $x\in\langle d,x\rangle=\langle c\rangle\Rightarrow c$ 是 D 中可逆元，从而 $\langle d,x\rangle=D[x]$，这表明 $(d,x)=1$，于是存在 $g(x),h(x)\in D[x]$ 使得 $1=dg(x)+xh(x)$，比较两边常数项可知 $1=dg_0$，这与 d 不可逆相矛盾。

必要性：D 是域，取映射 $\varphi:D[x]\to\mathbb{N}$，$\deg f(x)\geqslant 0$，$\varphi(f(x))=\deg f(x)+1$；$\varphi(0)=0$. 如果任意的 $f(x),g(x)\in F[x],g(x)\neq 0$，存在多项式 $q(x)$ 和 $r(x)$ 使得 $f(x)=q(x)g(x)+r(x)$，且 $\deg r(x)<\deg g(x)$，进而 $\varphi(r(x))<\varphi(g(x))$，从而 $D[x]$ 是一个欧式整环，进而是主理想整环。证明如下：

若 $f(x)=0$, 那取 $r(x)=q(x)=0$ 即可; 若 $f(x)=c$, $g(x)=a\neq 0$, D 是域所以 a 可逆, 则取 $q(x)=ca^{-1}, r(x)=0$ 即可; 如果 $0\leqslant \deg f(x)<\deg g(x)$, 则取 $q(x)=0, r(x)=f(x)$; 于是只剩下一种情况: $\deg f(x)\geqslant \deg g(x)$, 不妨设

$$f(x)=a_nx^n+\cdots+a_1x+a_0$$

$$g(x)=b_mx^m+\cdots+b_1x+b_0$$

并且最高次项系数非零, 取 $q_0(x)=a_nb_m^{-1}x^{n-m}$, 令

$$f_1(x)=f(x)-q_0(x)g(x)$$

于是 $\deg f_1(x)\leqslant n-1<\deg g(x)$, 此时存在 $q_1(x)$ 和 $r_1(x)$ 使得

$$f(x)=f_1(x)+q_0g(x)=(q_1(x)+q_0(x))g(x)+r_1(x)$$

则满足要求。

7 考虑 $n=3$ 的情况, 更多元的情况证明类似:

必要性: a_1,a_2,a_3 互素, 则 $((a_1,a_2),a_3)=1$, 于是存在 $x(a_1,a_2)+ya_3=1$, 又因为存在 m,n 使得 $ma_1+na_2=(a_1,a_2)$, 所以 $xma_1+xna_2+ya_3=1$, 取 $b_1=xm, b_2=xn, b_3=y$.

充分性: $b_1a_1+b_2a_2+b_3a_3=(b_1x+b_2y)(a_1,a_2)+b_3a_3=1$, 于是 (a_1,a_2) 和 a_3 互素, 进而 a_1,a_2,a_3 互素。

8 对于二元的情况, 成立 $(db_1,db_2)=d(b_1,b_2)$, 因此

$$\begin{aligned}(a_1,\cdots,a_n)&=((\cdots((a_1,a_2),a_3),\cdots),a_n)\\&=((\cdots(d(b_1,b_2),db_3),\cdots),a_n)=\cdots=d(b_1,\cdots,b_n)=d\\\Leftrightarrow (b_1,\cdots,b_n)&=1\end{aligned}$$

9 设 $f(x),g(x)\in R[x]$, 则 $f(x)g(x)|p\Rightarrow f(x)g(x)=$ 常数 c 且 $c|p$, 于是 $f(x)=c_1, g(x)=c_2, c_1c_2=c|p\Rightarrow c_1|p$ 或 $c_2|p$, 即 $f(x)|p$ 或者 $g(x)|p$, 从而 p 也是 $R[x]$ 的素元。

10 (1) 设 R 是 V 欧式整环, I 是其理想, 取非零元 $r\in I$ 使得 $\varphi(r)$ 最小, 则必须有 $I=(r)$, 这是因为 I 中元素 x 都被 r 整除, 即写成 $x=rq$ 的形式, 否则有余数 r_0, 即总存在 q,r_0 使得 $x=rq+r_0$ 且 $\varphi(r_0)<\varphi(r)$, 这与 r 的取法矛盾。因此 R 的理想都是主理想。

(2) 设