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)

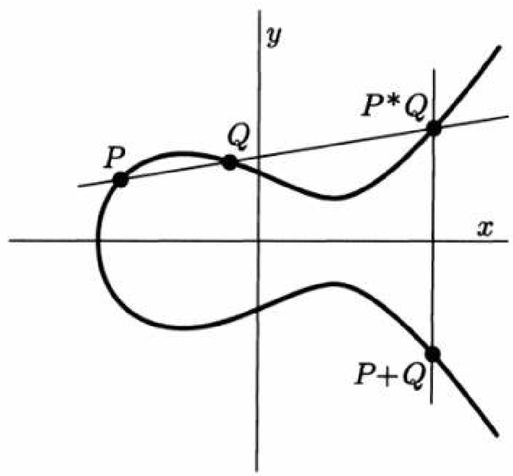
费马于 1630 年左右在 Diophantus 所著《数论》的书页空白处写下“当 $n \geq 3$ 时, 不存在满足 $x^n + y^n = z^n$ 的自然数解”以及“对此我发现了令人惊叹的证明，但这里空白太小写不下了.”由此引出了三百多年的故事. 我们将从椭圆曲线的角度出发浅探其与 FLT 的关系.

$E : y^2 = x^3 + ax + b\ (a, b \in Q)$，$4a^3 + 27b^2 \neq 0$, 则称 E 为 Q 上的椭圆曲线. 考虑 E 的解集 $E(Q) = \left\{(x, y) \in Q \times Q | y^2 = x^3 + ax + b\right\}$. 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 $\{(0, \pm 1), (-1, 0), (2, \pm 3)\} \in E(Z)$.
(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 $(\frac{x^2 z}{y^3})^2 = (\frac{z^2}{y^2})^3 - \frac{z^2}{y^2})$.
(2) 验证 $\{(0, 0), (\pm 1, 0)\} \in E(Q)$ 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 $a^3b = ba^3$. 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,$1\le i\le n$.

(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 $H\bigcap G_i(1\le i\le n)$ 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 $p^n,n\ge 1$ 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:$\forall x\in G,\exists n\ge 0$ 使得 $p^nx=0$.

(2) $a_n\neq 0,\forall n\ge 0$ 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 $U_p=\{e^{\frac{2\pi ik}{p^n}}|k\in\mathbb{Z},n\ge 0\}\le\mathbb{C}$ 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:

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

(2) 令 $A=(a_{ij}),1\le i,j\le n-1$, 其中 $a_{ij}=-cos(\frac{\pi}{m_{ij}})$,$m_{ij}$ 是（1）中群内元素 x_ix_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 $\{d_1x_1, d_2x_2, \cdots, d_rx_r\}$ 为基的自由阿贝尔群.(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 $R \cong ker f \oplus \mathbb{Z}$.
(2) $\varphi: R \to ker f \oplus \mathbb{Z}, r \mapsto (r - f(r)1_R, f(r))$ 给出一个群同构. 我们可以给 $ker f \oplus \mathbb{Z}$ 赋予环结构使得 φ 是环同构, 即满足 $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$, 请给出 $ker f \oplus \mathbb{Z}$ 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.