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,$1 \le p \le q \le n$, 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)

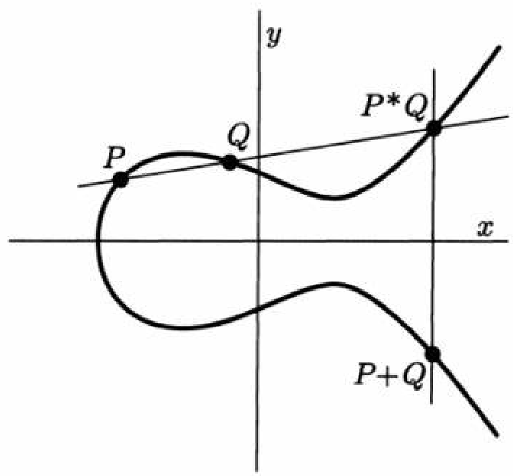
费马于 1630 年左右在 Diophantus 所著《数论》的书页空白处写下“当 $n \geq 3$ 时, 不存在满足 $x^n + y^n = z^n$ 的自然数解”以及“对此我发现了令人惊叹的证明，但这里空白太小写不下了.”由此引出了三百多年的故事. 我们将从椭圆曲线的角度出发浅探其与 FLT 的关系.

$E : y^2 = x^3 + ax + b$ $(a, b \in Q)$，$4a^3 + 27b^2 \neq 0$, 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 $(\frac{x^2z}{y^3})^2 = (\frac{z^2}{y^2})^3 - \frac{z^2}{y^2})$.

(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 $Ker(f)=\{A\in GL_2(\mathbf{Z})|\exists B\in M_{2\times 2}(\mathbf{Z}),A=I+3\cdot B\}$.
(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.