代数 1 H Lecture Notes

Instructor: 余成龙
Notes Taker: 唐龙天

Qiuzhen College, Tsinghua University
2022 Spring

课程信息:

- 授课人: 余成龙;
- 办公室: 近春园西楼 260;
- 邮箱: yuchenglong@mail.tsinghua.edu.cn;
- 成绩分布: 作业 (20%) + 期中 (30%) + 期末 (50%), 习题课讲题加分项;
- 参考书: M.Artin *Algebra*, 姚慕生 抽象代数学, S.Lang *Algebra*.

内容大纲:

- 群;
- 环 (交换环);
- 模 (环上的线性代数);
- 二次型.

目录

第一章　第一周

1.1　九月十三日

定义 1.1.1. 群 $(G,\cdot)$ 是指一个非空集合 G, 有一个 “二元运算”. 这里运算是指映射

$$G\times G\to G$$
$$(a,b)\mapsto a\cdot b=:ab.$$

输入一个有序对 (a,b), 输出 $ab\in G$. 且 $\cdot$ 满足

1. 结合律 (Associativity): 对任意 $a,b,c\in G$ 有 $(a\cdot b)\cdot c=a\cdot(b\cdot c)$.
2. 单位元/恒等元 (Identity element): 存在 $e\in G$ 使得对任意 $a\in G$ 有 $ae=ea=a$.
3. 逆 (Inverse) 对任意 $a\in G$, 存在 $b\in G$ 使得 $ab=ba=e$.

注记. 结合律保证记号 $a_1a_2\cdots a_n$ 无歧义.

例子.
- $(\mathbb{Z},+)$, 0 是单位元;
- 对正整数 n, 模 n 同余类有群结构 $(\mathbb{Z}/n\mathbb{Z},+)$.
- $(\mathbb{Q},+)$ 和 $(\mathbb{Q}^\times=\mathbb{Q}\backslash\{0\},\times)$ 是群.
- 对素数 p, $(\mathbb{F}_p^\times=\mathbb{Z}/p\mathbb{Z}\backslash\{\bar{0}\},\times)$ 是群.

同样有许多反例:
- (奇数, $+$) 不是群, 因为 “二元运算” 不良定义;
- $\mathbb{Z}_{\geq 0}$ 不是群, 因为不存在逆元;
- $(\mathbb{R}^3$, 叉乘) 不是群, 因为没有结合律.

问题 1.1.2. 思考是否存在不满足结合律, 但有单位元和逆的结构?

命题 1.1.3. 单位元唯一, 即 $e_1,e_2\in G$ 都是单位元, 则有 $e_1=e_2$.

证明: 注意到 $e_1=e_1e_2=e_2$. □

命题 1.1.4. 逆元唯一, 即若 b,c 都是 a 的逆元, 则 $b=c$

证明: 考虑 bac, 我们有

$$c=ec=(ba)c=b(ac)=be=b.\quad\square$$

我们现在可以记 a^{-1} 为 a 的逆元. 对任意 $n\in\mathbb{Z}_{>0}$, 令 $a^n=\underbrace{a\cdots a}_{n\text{ 个}}$, 令 $a^{-n}=(a^{-1})^n$; 对 $n=0$, 令 $a^0=e$.

练习. 验证: $a^{-n}=(a^{-1})^n$, $(a^m)^n=a^{mn}$, $a^ma^n=a^{m+n}$.

一个重要的例子是 n 元置换群 (Permutation group/Symmetric group). 用 $[n]$ 表示 n 元集合 $\{1,2,\cdots,n\}$.

定义 1.1.5. 集合 $S_n=\{\sigma\colon [n]\to[n]\mid \sigma \text{ 双射}\}$ 可以定义二元算

$$\sigma\tau:=\sigma\cdot\tau$$

是映射的复合, 即 $(\sigma\cdot\tau)(i)=\sigma(\tau(i))$.

例子. 通常将置换记为

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix},$$

也可以记为 $\sigma=\sigma(1),\cdot,\sigma(n)$, 通常称为 $1,\cdots,n$ 的排列.

命题 1.1.6. $(S_n,\cdot)$ 是群.

证明:

(0) 二元运算良定义, 因为单射复合单射还是单射, 满射复合满射还是满射.

(1) 结合性. 对任意 $\sigma_1,\sigma_2,\sigma_3\in S_n$, 我们有

$$\begin{aligned}((\sigma_1\sigma_2)\sigma_3)(i)&=(\sigma_1\sigma_2)(\sigma_3(i))\\ &=\sigma_1(\sigma_2(\sigma_3(i)))\\ (\sigma_1(\sigma_2\sigma_3))(i)&=\sigma_1(\sigma_2(\sigma_3(i))).\end{aligned}$$

从而有 $(\sigma_1\sigma_2)\sigma_3=\sigma_1(\sigma_2\sigma_3)$.

(2) 恒等元. 定义 $e\colon[n]\to[n]$ 满足 $e(i)=i$. 验证知

$$\begin{aligned}\sigma e(i)&=\sigma(e(i))=\sigma(i)\\ e\sigma(i)&=e(\sigma(i))=\sigma(i)\end{aligned}$$

从而有 $e\sigma=\sigma e=\sigma$.

(3) 逆. σ 满射, 则对任意 $i\in[n]$, 存在 $j\in[n]$ 使得 $\sigma(j)=i$. 定义

$$\begin{aligned}\tau\colon[n]&\to[n]\\ i&\mapsto j\end{aligned}$$

由于 σ 是双射, 知 τ 也是双射. 且 $\sigma\tau(i)=\sigma(j)=i$. 利用结合律, 有

$$\sigma(\tau(\sigma(i)))=(\sigma\tau)(\sigma(i))=\sigma(i).$$

又由于 σ 是双射, 则有 $\tau\sigma(i)=i$, 从而 $\tau\sigma=\sigma\tau=e$. □

注记. 对一般 $f\colon X\to Y$ 双射, 存在 $g\colon Y\to X$ 使得 $f\circ g=\mathrm{Id}_Y$ 及 $g\circ f=\mathrm{Id}_X$. g 记作 f^{-1}. τ 也是如此定义, 记作 σ^{-1}, 无歧义.

定义 1.1.7. 群 G 的元素个数称为阶 (order), 记作 $|G|$.

命题 1.1.8. 对于置换群有 $|S_n| = n!$.

例子. 考虑 S_3, 令

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

计算得

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 1 & 3 & 2 \end{pmatrix} = (132), \ \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix} = (213)$$

这告诉我们 $\sigma\tau \neq \tau\sigma$, 即 S_3 不是交换群. 我们也可以用另外一种看法, 即 σ 交换 $1,3$ 位置. 因此 $\sigma\tau = 213$. 而 τ 是向后平移次, 从而

$$\tau\sigma = \text{ 平移 } 321 = 132 \neq \sigma\tau.$$

定义 1.1.9. 群 $(G, \cdot)$ 称为 Abel 群, 若满足对任意 $a, b \in G$ 都有 $ab = ba$. 此时通常将二元运算记作 $+$, 单位元记作 0.

命题 1.1.10. 对于 $n \geq 3$, S_n 不是 *Abel* 群.

例子. 考虑 $D_n = \{$二维平面上将正 n 边形映到自身的旋转和反射, 包括恒等映射$\}$, 二元运算是映射的复合, D_n 构成群, 称为二面体群 *(Dihedral group)*.

练习. 验证 D_n 是群.

例子. 对于 $\mathbb{R}$ 线性空间 V, 定义

$$\mathrm{GL}(V) = \{f \colon V \to V \mid f \text{ 是可逆线性变换}\},$$

二元运算是复合, $\mathrm{GL}(V)$ 构成群, 称为一般线性群 *(General linear group)*. 特别地, $\mathrm{GL}(n;\mathbb{R})$ 是所有 $n \times n$ 可逆矩阵的群, 运算时矩阵乘法. 对于域 $F = \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_p$, $\mathrm{GL}(n;F)$ 只在 $n = 1$ 时是 *Abel* 群.

定义 1.1.11. 对于群 $(G_1, \cdot)$ 和 $(G_2, \cdot)$, 定义

$$G_1 \times G_2 = \{(a, b) \mid a \in G_1, \ b \in G_2\},$$

二元运算是逐分量乘法, 即

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2).$$

$(G_1 \times G_2, \cdot)$ 是群, 称为 G_1 与 G_2 的积群 (Product group).

1.2 九月十四日

定义 1.2.1. 对群 G 的子集 H, 若 H 在 G 的乘法下构成群, 称 H 为 G 的子群 (subgroup).

例子. 对 $G = S_n$, 我们令

$$H = \{\sigma \in S_n \mid \sigma(n) = n\},$$

有 H 是 G 的子群. 我们只需验证 H 在 G 的运算下封闭, 并且对取逆封闭.

- 对 $\sigma, \tau \in H$, 有 $\sigma(\tau(n)) = \sigma(n) = n$, 即 $\sigma\tau \in H$;
- 若 $\sigma(n) = n$, 则有 $\sigma^{-1}(n) = \sigma^{-1}(\sigma(n)) = n$, 即 $\sigma^{-1} \in S_n$.

事实上, 我们还能证明 $H \simeq S_{n-1}$.

定理 1.2.2 (Lagrange)**.** G 是有限群, 对任意子群 $H \subset G$ 都有 $|H| \big| |G|$.

为证明此定理, 我们引入陪集 (coset) 的概念. 这里考虑左陪集 (left coset).

定义 1.2.3. 对群 G, H 是正规子群. G 中形如 $gH = \{gh \mid h \in H\}$ 的子集称为 G 的左 H-陪集.

例子. 1. $eH = H$ 是左 H-陪集.

2. 考虑 $H = \{\sigma \mid \sigma(n) = n\} \subset S_n$. 左 H 陪集的分类如下

$$X_i = \{\sigma \in S_n \mid \sigma(n) = i\},\ i = 1, 2, \cdots, n.$$

对任意给定 $g \in S_n$, 令 $i = g(n)$, 我们证明 $gH = X_i$. 首先对任意 $h \in H$, 有 $gh(n) = g(n) = i$, 即有 $gH \subset X_i$. 另一方面, 对任意 $\sigma \in X_i$, 有

$$\sigma = (g^{-1}g)\sigma = g(g^{-1}\sigma).$$

令 $h = g^{-1}\sigma$, 有 $h(n) = g^{-1}(i) = n$, 即 $h \in H$, 从而 $X_i \subset gH$. 因此有 $gH = X_i$.

定义 1.2.4. 定义集合 $G/H = \{gH \mid g \in G\}$, 每一个元素都是 G 的子集, 称为商集 (quotient set).

例子. 考虑 S_n, $H = \{\sigma \in S_n \mid \sigma(n) = n\}$, 有 $S_n/H = \{X_1, \cdots, X_n\}$.

定理 1.2.5. G 有左陪集分解

$$G = \coprod_{gH \in G/H} gH.$$

证明:

1. 无交, 若有 $gH \cap g'H \neq 0$, 即存在 $a \in gH \cap g'H$. 断言, 若 $a \in gH$, 则有 $aH = gH$. 设 $a = gh$, 对任意 $h' \in H$, 有

$$ah' = ghh' = g(hh') \in gH,$$

即 $aH \subset gH$. 另一方面, 对任意 $h'/ \in H$, 有

$$gh' = ah^{-1}h' = a(h^{-1}h') \in aH,$$

即 $gH \subset aH$. 从而 $aH = gH$. 因此 $gH = gH'$.

2. 并, 因为 $g = ge \in gH$. □

命题 1.2.6. $H \to gH : h \mapsto gh$ 是双射.

证明: 若 $gh = gh'$, 则有

$$h = g^{-1}gh = g^{-1}gh' = h'.$$

而满射由定义保证. □

证明:(定理 1.2.2) 由于 $|G| < \infty$, 因此我们有 $|H| = |gH|$. 利用左陪集分解

$$G = \coprod_{gH \in G/H} gH,$$

我们有 $|G| = |G/H| \cdot |H|$, 即得 $|H| \big| |G|$. □

定义 1.2.7. 对集合 S, $X \subset S \times S$ 是子集. 若 $(a, b) \in X$, 记为 $a \sim b$. 若 $\sim$ 满足

(1) 传递性 (transitive): $\forall\, a, b, c \in S$, 若 $a \sim b, b \sim c$, 则有 $a \sim c$.

(2) 对称性 (symmetric): 若 $a \sim b$, 则有 $b \sim a$.

(3) 自反性 (reflextive): 对任意 a, 有 $a \sim a$.

则称 $\sim$ 为 S 上的等价关系 (equivalence relation).

把 S 分成非空子集的无交并称为 S 的一个划分 (partition). 从等价关系我们可以自然诱导一个划分. 考虑 S 上的等价关系 $\sim$, 对任意 $a \in S$, 定义

$$C_a = \{b \in S \mid a \sim b\} \subset S.$$

令 $\bar{S} = \{C_a \mid a \in S\}$ 是所有等价类构成的集合. 我们有划分

$$S = \coprod_{C_a \bar{S}} C_a,$$

且有满射 $S \to \bar{S} : a \mapsto C_a$. 反过来, 从一个给定划分也可以定义等价关系.

特别地, 设 $H \subset G$ 是子群, 我们可以定义等价关系, 即

$$a \sim g \text{ 当且仅当 } \exists\, h \in H, \text{ 使得 } a = gh.$$

有满射 $G \twoheadrightarrow G/H$, 称为商映射 (quotient map). 一个自然的问题是 G/H 上是否有自然的群结构? 我们先尝试定义运算

$$\begin{aligned} G/H \times G/H &\longrightarrow G/H \\ (aH, bH) &\longmapsto abH \end{aligned}$$

我们希望这是良定义的, 即对

$$a' = ah_1,\ b' = bh_2,$$

需要 $a'b'H = abH$. 注意到

$$\begin{aligned} a'b' &= ah_1bh_2 = abb^{-1}h_1bh_2 \\ &= ab(b^{-1}h_1b)h_2, \end{aligned}$$

因此只需要, 对任意 $b \in G$, $h \in H$ 有 $b^{-1}hb \in H$. 如果假设这一点, 我们容易发现 G/H 确实有群结构, 因为有单位元 eH 和逆元 $g^{-1}H$. 因此, 从中抽取出正规子群的概念.

定义 1.2.8. 若子群 $H \subset G$ 满足对任意 $h \in H$, $g \in G$ 都有 $ghg^{-1} \in H$, 则称 H 为正规子群 (normal subgroup). 此时 G/H 有群结构, 称为商群 (quotient group).

注记. 可以定价定义为, 对任意 $g \in G$, 有 $gHg^{-1} = \{ghg^{-1} \mid h \in H\} = H$.

命题 1.2.9. *Abel 群的子群都是正规子群.*

证明: 对任意 $h \in H$, $g \in G$, 有 $ghg^{-1} = gg^{-1}h = h \in H$. □

例子. 考虑加法群 $(\mathbb{Z}, +)$, $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\} \subset \mathbb{Z}$ 是正规子群. 有商群 $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \cdots, \overline{n-1}\}$, 其中 $\bar{i} = \{i + na \mid a \in \mathbb{Z}\}$.

例子. 也容易给出非正规子群的例子. 考虑 $G = S_3$, $H = \{\sigma \in S_3 \mid \sigma(3) = 3\}$. 取

$$h = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \ g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \ g^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

我们有 $(ghg^{-1})(3) = gh(2) = g(1) = 1$, 即 $ghg^{-1} \in H$. 因此 H 不是正规子群.

定义 1.2.10. 群 G_1, G_2, 映射 $f\colon G_1 \to G_2$ 称为群同构 (group isomorphism), 若对任意 $a, b \in G_1$ 都有 $f(ab) = f(a)f(b)$.

注记. 此时对于子群 $H = \{\sigma \in S_n \mid \sigma(n) = n\} \subset S_n$, 我们知道有群同构 $H \simeq S_{n-1}$.

1.3 作业 1

练习. 计算下列 S_6 中的元素的乘积. 其中 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 4 & 6 & 5 & 2 \end{pmatrix}$ 和 $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$

- ◇ $\sigma \cdot \tau$.
- ◇ $\sigma \cdot \tau \cdot \sigma^{-1}$.

练习. 列出 S_4 的所有子群, 并指出哪些是正规子群.

练习. 对群 G 中的任意元素 g, h, 证明 $(gh)^{-1} = h^{-1}g^{-1}$.

练习. 分类 $(\mathbb{Z}, +)$ 的所有子群.

练习. 构造同构 $f\colon \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$.

练习. D_n 是二面体群, 计算 $|D_n|$ 并判断 D_n 是否为 *Abel* 群, 给出论证.

练习. 对给定素数 p, 群 $G = GL(n, \mathbb{F}_p)$. 考虑 G 的如下子集

- ◇ B 是 G 中上三角矩阵的全体.
- ◇ W 是每行每列有且仅有一个 1，其余位置是 0 的方阵全体. *(请说明为什么 W 是 G 的子集)*
- ◇ H 是每行每列有且仅有一个位置非零, 其余位置是 0 的方阵全体. *(请说明为什么 H 是 G 的子集)*
- ◇ T 是 G 中的对角阵全体.

◇ U 是 G 中对角线都是 1 的上三角矩阵全体.

◇ D 是 G 中纯量矩阵全体，即 $D = \{\lambda I_n \mid \lambda \neq 0\}$.

◇ $\mathrm{SL}(n, \mathbb{F}_q)$ 是 G 中行列式等于 1 的矩阵全体.

请完成以下证明或者计算:

1. 证明以上子集都是 G 的子群.
2. 判断这些子群和 G 本身是不是 *Abel* 群.
3. 求这些子群和 G 的阶数.
4. 判断哪些子群是 G 的正规子群.
5. 对于有严格包含关系的子群，判断小的群是否是大的群的正规子群.

练习. 判断 $\mathrm{GL}(2, \mathbb{F}_2)$ 是否与 S_3 同构, 给出论证.

练习. 对群 G, H 是其子群, 完成如下问题:

◇ 给出右 H-陪集的定义. 证明右 H-陪集数量等于左 H-陪集数量 *(假设有限)*.

◇ 证明 H 是正规子群当且仅当对任意 $g \in G$ 都有 $gH = Hg$.

◇ 左 H-陪集的数量称为 H 在 G 中的指数 *(index)*, 记作 $[G : H]$. 证明若 $[G : H] = 2$, 则 H 为正规子群.

我们下面需要用到所谓半群的概念. 集合 S 和运算 $\cdot : S \times S \to S$ 构成的对 $(S, \cdot)$ 称为半群 (semi group), 若 $\cdot : S \times S \to S$ 满足结合律.

练习. G 是所有秩小于等于 r 的 $n \times n$ 矩阵构成的集合. 证明 G 关于矩阵乘法构成半群.

练习. 对半群 G, 假设:

1. 存在左单位. 即存在 $e \in G$ 对任意 $a \in G$, 都有 $ea = a$;
2. 存在左逆. 即对任意 $a \in G$, 存在 $a^{-1} \in G$ 使得 $a^{-1}a = e$.

练习. 令 $G = \{(a, b) \mid a \neq 0\}$, 定义运算

$$\begin{aligned} \cdot : G \times G &\longrightarrow G \\ (a, b) \cdot (c, d) &\longmapsto (ac, ad + b). \end{aligned}$$

证明 $(G, \cdot)$ 是群.

练习. 设 G 是偶数阶群, 证明 $x^2 = e$ 的解数也是偶数.

练习. 对群 G, $a, b \in G$. 若有 $a^5 = e$, $a^3 b = ba^3$, 求证 $ab = ba$.

练习. 证明 $(\mathbb{R}, +)$ 与 $(\mathbb{R}_{>0}, \times)$ 同构.

练习. 对有限群群 G, $H \subsetneq G$ 是真子群. 证明

$$G \neq \bigcup_{g \in G} gHg^{-1}.$$

注记. 对于无限群, G 可能等于某个子群的全体共轭的并.

索引