群论笔记

© 晨沐公[†]

[†] 成都市锦江区嘉祥外国语高级中学

临时笔记

bilibili: 晨沐公 Johnny　github:MATHhahetaDEATH

2024 年 8 月 12 日

请：相信时间的力量，敬畏概率的准则。

Johnny Tang

前言

在数学中, 对于每一个数学对象 (例如极限), 我们会例行公事般地考虑它的一些常见的性质. 比如说, 这个对象最基本的例子是什么, 这种对象是否存在, 如果存在的话它是否具有唯一性, 它的子对象和商对象 (如果有的话) 都具有什么性质 (比如说遗传了原来的对象的什么性质), 这个对象的可计算性以及在特定映射下的行为等等.

目录

Chapter 1

群论

疯狂抄书中……

1.1 基本想法

定义 1.1 二元运算

定义非空集合 S 上的二元运算 $\cdot : S \times S \to S$, 考虑 $(S, \cdot)$ 的如下性质:

- S 是交换的, 如果对任意 $x, y \in S$ 有 $xy = yx$.
- S 是结合的, 如果对任意 $x, y, z \in S$ 有 $(xy)z = x(yz)$.
- S 上的一个幺元 (单位元)e, 满足对任意 $x \in S$ 都有 $xe = ex = e$.
- x 的一个逆元 x^{-1}, 满足 $xx^{-1} = x^{-1}x = e$.

注. 不造成歧义时, $x \cdot y$ 可简写为 xy, $(S, \cdot)$ 可简写为 S. 括号表示优先的运算.

注. 不难 (并且应当) 验证逆元 x^{-1}(相对于 x) 和幺元 e(相对于 S) 的唯一性.

注. 后面会看到, 这些性质的常见程度为结合性质 $\sim$ 存在幺元 $>$ 所有元素存在逆元 $>$ 交换性质.

我们引入自然的 x^n 定义, 其中 n 是整数.

定义 1.2 幺半群, 群

设带有二元运算 $\cdot$ 的非空集合 S, 称 $(S, \cdot)$ 为幺半群, 若运算 $\cdot$ 满足结合律且 S 中存在幺元. 进一步, 称幺半群 G 为群, 如果其所有元素均可逆.

注. 关于交换性质的扩展定义: 称交换的幺半群为交换幺半群, 交换的群为 Abel 群.

定义 1.3 子幺半群, 子群

对于幺半群 S 和非空子集 $T \subset S$, 称 T 是一个*子幺半群*, 如果

- $e \in T$.
- T 对于 $\cdot$ 封闭, 即 $\cdot$ 在 T 上的限制映射之值域包含于 T.

对于群 G 和非空子集 $H \subset G$, 称 H 是一个*子群* (记作 $H < G$), 如果

- $e \in H$.
- H 对于 $\cdot$ 封闭.
- H 对于取逆元映射 $\bullet^{-1}$ 封闭.

注. *子群的后两个条件可以合并为一个: 对任意 $x, y \in H$ 有 $xy^{-1} \in H$.*

例 1.1 幺半群中所有可逆元素构成的子幺半群是一个群.

例 1.2 记 n 阶实矩阵构成集合 $\mathrm{M}(n, \mathbb{R})$, 该集合对矩阵乘法构成幺半群. 考虑其子集 $\mathrm{GL}(n, \mathbb{R}) := \{A \in \mathrm{M}(n, \mathbb{R}) : \det A \neq 0\}$ 和 $\mathrm{SL}(n, \mathbb{R}) := \{A \in \mathrm{M}(n, \mathbb{R}) : \det A = 1\}$, 它们对矩阵乘法构成群, 分别称作*一般线性群*和*特殊线性群*.

例 1.3 对于集合 X, 考虑所有 $X \to X$ 的双射所成集合 $\operatorname{Sym} X$, 这个集合对映射复合构成群, 称为*对称群* (置换群). 参考后文.

记群 G 的阶 $\operatorname{ord} G := |G|$, 当 G 为无限集合时 $|G|$ 表示其基数.

在 G 中任取集合 E, 考虑 E 所生成的“闭包”, 即包含 E 的最小子群 $\langle E \rangle := \bigcap_{H<G, E \subset H} H$. 容易证明, 对于有限集合 $E = \{a_1, \cdots, a_n\}$, $\langle E \rangle = \{a_1^{\alpha_1} \cdots a_n^{\alpha_n} : \alpha_j \in \mathbb{Z}, j = 1, \cdots, n\}$. 特别地, 当 E 是单点集 $\{x\}$ 时, 简记 $\langle x \rangle = \langle \{x\} \rangle$. 此时定义 $\operatorname{ord} x := \operatorname{ord} \langle x \rangle$ 为 x 的阶. 亦可证明, $\operatorname{ord} x$ 有限时即为最小的使得 $x^n = e$ 的正整数 n.

例 1.4 对于群 G, 若存在 $x \in G$ 使得 $G = \langle x \rangle$, 则称 G 为*一个循环群*. 下一节会研究循环群的结构.

我们采用惯常的记号 AB 表示 $\{ab : a \in A, b \in B\}$, 并简记 $\{x\}A$ 为 xA, Bx 同理.

类似于利用等价类和商集对集合进行划分的方法, 这里可以考虑一个群 G 的划分. 选取其任一子群 H, 我们希望利用 H 的某一特征划分 G. 自然的想法是作出 GH 或者 HG 并设法去除其中重复的集合. 这就是定义陪集的动机:

定义 1.4 陪集

设 H, K 为群 G 的子群.

- 定义*左陪集*为 G 中形如 xH 的子集, 并记全体左陪集构成集合 G/H. 类似可得右陪集和 $G \setminus H$ 的定义.
- 定义*双陪集*为 G 中形如 HxK 的子集, 并记全体双陪集构成集合 $H \setminus G / K$.

- 定义 H 在 G 中的指数 $(G:H) := \operatorname{ord} G/H$.

注. 在三种陪集中, 我们也许更偏爱左陪集, 因为左乘一个元素可以自然地视作映射 $H \to G, h \mapsto xh$.

注. 左右陪集是双陪集的特例, 即 H 或 K 为 $\{e\}$ 的情况.

注. 令 $x \sim y$ 当且仅当 $HxK = HyK$, 那么这是一个等价关系.

注. 可以证明 $\operatorname{ord} G/H = \operatorname{ord} G \setminus H$. 因此讨论指数时无需指定左或右.

自然想到, 取映射 $\tau_K : K \to K, k \mapsto y^{-1}xk$, 则 $xK = yK$ 等价于 τ_K 是双射. 同理可得, 令 $\tau_H : H \to H, h \mapsto hyx^{-1}$, 则 $Hx = Hy$ 等价于 τ_H 是双射. 最后, $HxK = HyK$ 等价于 $\tau_H \circ \tau_K$ 是双射.

更进一步, 以 τ_K 为例: 若想要 τ_K 是双射, 由于其本身就是单射, 故只需要求满射, 一个充分条件是 $y^{-1}x \in K$. 反过来, 当 $xK = yK$ 时自然有 $xe = yk$ 即 $y^{-1}x = k \in K$. 这就证明了下面的命题.

另一种证明该命题的方法是考虑 x 驱使 H "平移" 的作用. 如果将 H 想象成向量空间, x 想象成向量并取加法为 $\cdot$, 这一点会非常直观.

命题 1.5

设 H 为群 G 的子群, 则对于 $x \in G$ 有 $xH = H \Leftrightarrow x \in H$. 进而对于 $x, y \in G$ 有 $xH = yH \Leftrightarrow y^{-1}x \in H$. 右陪集和双陪集的情况同理.

证明 必要性: 取 $e \in H$ 即得 $x = xe \in xH = H$. 充分性: 由乘法封闭性可知 $xH \subset H$. 同理有 $x^{-1}H \subset H$, 即 $H \subset xH$. 这说明 $xH = H$.

现在考虑用陪集划分群 G:

命题 1.6

设 H, K 为群 G 的子群, 则

- $G = \bigsqcup_x HxK$, 其中 x 遍历每个双陪集的代表元.
- (Lagrange 定理)$\operatorname{ord} G = (G:H) \operatorname{ord} H$.

证明 (1) 先证明若 HxK, HyK 有交则相等: 记 $hxk = h'yk'$, 则 $x = h^{-1}h'yk'k^{-1} \in HyK$, 由等价关系的传递性可知 $HxK = HyK$. 这就证明了无交部分. 并部分则是显然的.

(2) 将 G 进行无交并分解即 $G = \bigsqcup_x xH$, 记 $E = \{e\}$, 则 $G = \bigsqcup_x x \bigsqcup_y yE = \bigsqcup_{x,y} xyE$. 注意到对于 G, H, $(G:H)$ 就是可能的 x 的个数, 而 $(G:1) = \operatorname{ord} G, (H:1) = \operatorname{ord} H$, 结合 x, y 个数是 x 个数与 y 个数之积, 立得原式成立.

注. 在 (2) 中实际上证明了: 若 $K < H < G$, 则 $(G:K) = (G:H)(H:K)$. 当然这直接由 Lagrange 定理可得.