Galois 理论

Ihaku

前言

... [1] [2] [3]

目录

第零章　预备知识

0.1　群

定义 0.1 集合 S 和 S 上满足结合律的二元运算 $\cdot$ 所形成的代数结构叫做**半群**. 这个半群记成 $(S,\cdot)$ 或者简记成 S, 运算 $x\cdot y$ 也尝尝简写成 xy. 若含有幺元则称为**幺半群**, 幺元通常记作 e 或 1. 若满足交换律则称为**交换半群**.

例 0.2 $(\mathbb{Z},-)$ 不满足结合律, 故不是半群.

对于交换幺半群, 惯例是将其二元运算 $\cdot$ 写成加法 $+$, 并将幺元 1 写成 0, 元素 x 的逆写成 $-x$; 但一些场合仍适用乘法记号. 必要时另外申明.

定义 0.3 若含幺半群 $(G,\cdot)$ 中每一个元素都存在逆元, 则 G 叫做**群**. 若满足交换律则称为**交换群**或**阿贝尔群**.

简言之, 群内的元素满足封闭性, 结合律, 单位元, 逆元四个性质. 其中逆元往往难以满足, 结合律通常难以验证. 向量空间的前四条性质即是群的定义.

例 0.4 一个拓扑 $(\tau,\cup)$ 是一个幺半群, 而拓扑 $(\tau,\triangle)$ 是一个群. 单位元都为 $\varnothing$, 后者逆元为自身, 亦即 $\forall A\in\tau, A^2=\varnothing$, 该群每一个非单位元的阶都为 2.

定义 0.5 设 G 为群, 子集 $H\subset G$ 被称为 G 的**子群**, 如果

(i) H 是子幺半群,
(ii) 对任意 $x\in H$ 有 $x^{-1}\in H$.

表示成 $H\leqslant G$. 假若子群 H 对所有 $x\in G$ 满足 $xH=Hx$, 则称 H 为 G 的**正规子群**, 记作 $H\lhd G$. 子群 $\{1\}\lhd G$ 称作 G 的**平凡子群**.

例 0.6 包含 x 的最小群叫做由 x **生成**的群, 记作 $\langle x\rangle$. 若群 G 中存在元素 x 使得 $G=\langle x\rangle$, 则称 G 为**循环群**. 循环群又叫单位生成群, 且都同构于 $\mathbb{Z}$ 的子群.

例 0.7 从任意集合 X 映到自身的全体双射构成一个群, 称为 X 上的**对称群** $\mathfrak{S}_X:=\mathrm{Aut}(X)$. 其中的二元运算是双射的合成 $(f,g)\mapsto f\circ g$, 幺元为恒等映射 $\mathrm{id}_X:X\to X$, 而逆元无非是逆映射. 当 $X=\{1,\dots,n\}$ $(n\in\mathbb{Z}_{\geq 1})$ 时也记为 $\mathfrak{S}_n$, 称为 n 次的**对称群**或**置换群**. 注意到 $|\mathfrak{S}_n|=n!$. 其所有偶置换元素组成的子群称为**交错群**, 记作 $\mathfrak{A}_n$, 且 $\mathfrak{A}_n\lhd\mathfrak{S}_n$.

定义 0.8 设 H 为群 G 的子群. 定义:

(i) **左陪集**: G 中形如 xH 的子集, 全体左陪集构成的集合记作 G/H;

(ii) **右陪集**: G 中形如 Hx 的子集, 全体右陪集构成的集合记作 $H\backslash G$;

(iii) **双陪集**: 设 K 为另一子群, 则 G 中形如 $HxK := \{hxk : h \in H, k \in K\}$ 的子集称为 G 对 (H, K) 的双陪集, 全体双陪集构成的集合记作 $H\backslash G/K$.

陪集中的元素称为该陪集的一个代表元. $H \lhd G$ 等价于左, 右陪集相同. 由于陪集的左右之分总能从符号辨明, 以下不再申明. 定义 H 在 G 中的**指数**

$$[G : H] := |G/H|.$$

陪集空间 G/H 未必有限, 在此视 $[G : H]$ 为基数.

定理 0.9 (Lagrange 定理) 设 H 为群 G 的子群, 则

(i) $|G| = [G : H]|H|$, 特别地, 当 G 有限时 $|H|$ 必整除 $|G|$;

(ii) 若 K 是 H 的子群, 则 $[G : K] = [G : H][H : K]$.

推论 0.10 群 G 中任意元素 g 的阶整除 G 的阶, 即 $\operatorname{ord} g \mid |G|$. 由此直接得费马小定理.

拉格朗日定理的逆命题并不成立. 给定一个有限群 G 和一个整除 G 的阶的整数 d,G 并不一定有阶数为 d 的子群. 最简单的例子是 4 次交替群 $\mathfrak{A}_4$, 它的阶是 12, 但对于 12 的因数 6, $\mathfrak{A}_4$ 没有 6 阶的子群. 对于这样的子群的存在性, Cauchy 定理和 Sylow 定理给出了一个部分的回答.

定义 0.11 设 G 为群.

(i) G 的**中心**定义为 $Z_G := \{z \in G : \forall x \in G, xz = zx\}$ [i];

(ii) 设 $E \subset G$ 为任意子集, 定义其**中心化子**为 $Z_G(E) := \{z \in G : \forall x \in E, xz = zx\}$ [ii];

(iii) 承上, 定义其**正规化子**为 $N_G(E) := \{n \in G : nEn^{-1} = E\}$[iii].

当 E 是独点集 $\{x\}$ 时, 使用简写 $Z_G(x)$ 和 $N_G(x)$.

显然有

$$Z_G = Z_G(G) \leqslant Z_G(E) \leqslant N_G(E) \leqslant G.$$

阿贝尔群等价于中心是自身的群. $H \lhd G$ 等价于 $N_G(H) = G$.

定义 0.12 设 M_1, M_2 为幺半群. 映射 $\varphi : M_1 \to M_2$ 如满足下述性质即称为**同态**

(i) $\forall x, y \in M_1, \varphi(xy) = \varphi(x)\varphi(y)$;

(ii) $\varphi(1) = 1$.

[i] 因其德文 Zentrum(注意德文中名词首字母应大写), 首字母为 Z, 也有部分书采用英文 center 的首字母 C 表示.

[ii] 因其德文 Zentralisator, 首字母为 Z, 也有部分书采用英文 centralizer 的首字母 C 表示.

[iii] 因其德文 Normalisator 和英文 normalizer, 首字母为 N.

从 M_1 到 M_2 的同态所成集合写作 $\mathrm{Hom}(M_1, M_2)$. 设 $\varphi \in \mathrm{Hom}(M_1, M_2)$. 它的**像**记作 $\mathrm{Im}(\varphi) := \{\varphi(x) : x \in M_1\}$, 而其**核**定义为 $\mathrm{Ker}(\varphi) := \varphi^{-1}(1)$.

从幺半群 M 映至自身的同态称为**自同态**, 自同态全体构成一个群, 叫做**自同态群**, 记作 $\mathrm{End}(M) = \mathrm{Hom}(M, M)$.同态的合成仍为同态. 取常值 1 的同态称作**平凡同态**.

若存在同态 $\psi : M_2 \to M_1$ 使得 $\varphi\psi = \mathrm{id}_{M_2}$, $\psi\varphi = \mathrm{id}_{M_1}$, 则称 φ 可逆而 ψ 是 φ 的逆; 可逆同态称作**同构**. 此时我们也称 M_1 与 M_2 同构. 从幺半群映至自身的同构称为**自同构**, 自同构全体构成一个群, 叫做**自同构群**, 记作 $\mathrm{Aut}(M)$, 如恒等映射 $\mathrm{id}_M \in \mathrm{Aut}(M)$.

定义 0.13 设 G 为群, N 为其正规子群. 在陪集空间 G/N 上定义二元运算

$$xN \cdot yN = xyN, \quad x, y \in G.$$

这使得 G/N 构成一个群, 称为 G 模 N 的**商群**, 其中的幺元是 $1 \cdot N$ 而逆由 $(xN)^{-1} = x^{-1}N$ 给出. 群同态

$$\pi : G \to G/N, \qquad x \mapsto xN$$

称为**商同态**.

定义 0.14 设幺半群 M 作用于 X. 定义

(i) **不动点**集 $X^M := \{x \in X : \forall m \in M, mx = x\}$;

(ii) 对于 $x \in X$, **轨道** $Mx := \{mx : m \in M\}$, 其元素称为该轨道的代表元, 轨道 Mx 是 X 的 M-子集;

(iii) 承上, 其**稳定化子**定为 M 的子幺半群 $M_x := \{m \in M : mx = x\}$.

定理 0.15 (轨道分解定理) 设群 G 作用于 X, 则

(i) 有轨道分解 $X = \bigsqcup_x Gx$, 其中我们对每个轨道选定代表元 x;

(ii) 对每个 $x \in X$, 映射

$$G/G_x \to Gx, \qquad g \cdot G_x \mapsto gx$$

是 G-集间的同构;

(iii) 特别地, 我们有基数的等式

$$|X| = \sum_x [G : G_x]\,;$$

(iv) 对所有 $x \in X$ 和 $g \in G$, 有

$$G_{gx} = gG_xg^{-1}.$$

定义 0.16 依旧设 G 为群. 伴随自同构 $\mathrm{Ad} : G \to \mathrm{Aut}(G)$ 给出的作用称为 G 的**共轭作用** $G \times G \to G$ (在此考虑左作用). 定义展开后无非是

$$(g, x) \longmapsto {}^gx := gxg^{-1}.$$

共轭作用下的轨道称为 G 中的**共轭类**.

推而广之, 对任意子集 $E \subset G$ 我们业已定义子群 $N_G(E)$, 它在 E 上的作用也叫共轭. 若两子集 E, E' 满足 $\exists g \in G, E' = gEg^{-1}$, 则称 E 与 E' 共轭.

非交换群共轭作用的性状一般相当复杂. 对于 $x \in G$, 其稳定化子群正是中心化子 $Z_G(x)$, 而不动点集则是中心 Z_G. 剖析 G 的共轭作用是了解其群结构的必由之路.

定理 0.17 (同态基本定理) 设 $\varphi \in \mathrm{Hom}(G_1, G_2)$, 则 φ 诱导出同构

$$\bar{\varphi} : G_1/\operatorname{Ker}(\varphi) \to \operatorname{Im}(\varphi), \qquad g \cdot \operatorname{Ker}(\varphi) \mapsto \varphi(g).$$

此同构叫做**正则同构**.

定理 0.18 (Caylay 定理) 对任意有限群 G, 同态

$$\rho : G \to \mathfrak{S}_G, \qquad \rho(g)a = ga$$

是单的, 故 $\operatorname{Ker}(\rho) = \{1\}$, 利用同态基本定理得: 每个群均同构于某个对称群的子群.

定理 0.19 (Cauchy 定理) 设 G 为有限群, 素数 p 整除 $|G|$, 则存在 $x \in G$ 使得 $\operatorname{ord} x = p$.

定义 0.20 设 G 为 n 阶有限群, p 为素数. 设 $p^m \mid n$, 满足 $|H| = p^m$ 的子群 H 称为 G 的 Sylow p-子群.

定理 0.21 (Sylow 定理) 对任意有限群 G 和任意素数 p,

(i) G 含有 Sylow p-子群.

(ii) (a) 任意 p-子群 $H \subset G$ 皆包含于某个 Sylow p-子群;

(b) G 的任两个 Sylow p-子群 P, P' 皆共轭;

特别地, G 中存在正规的 Sylow p-子群当且仅当 G 有唯一的 Sylow p-子群.

(iii) G 中 Sylow p-子群的个数 $\equiv 1 \pmod{p}$.

定理 0.22 (有限生成阿贝尔群结构定理) 有限生成阿贝尔群都同构于若干 $\mathbb{Z}$ 子群的直和.

有关对称群和可解群的内容请参考 [1, 1.6, 1.11], 这对于 Galois 理论的学习至关重要.

0.2 环

索引

参考文献

[1] 冯克勤. 近世代数引论. 合肥: 中国科学技术大学出版社, 2009.

[2] 李文威. 代数学方法 *(第一卷)*, volume 67.1 of 现代数学基础丛书. 北京: 高等教育出版社, 2019.

[3] 章璞. 伽罗瓦理论：天才的激情, volume 37 of 现代数学基础丛书. 北京: 高等教育出版社, 2013.