Galois 理论

Ihaku

前言

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

目录

第零章 预备知识 1

0.1 群 1

0.2 环和域 5

索引 9

参考文献 11

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. 与任何元素相乘等于自身的称为**幺元**, 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 与任何元素相乘等于幺元的称为**逆元**, 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, 含幺元, 含逆元四个性质. 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**.

定义 0.6　(i) 一个群的阶是指其势，即其元素的个数；
(ii) 一个群内的一个元素 a 之阶（有时称为周期）是指会使得 $a^m=e$ 的最小正整数 m。若没有此数存在，则称 a 有无限阶. 有限群的所有元素有有限阶.
一个群 G 的阶被记为 $|G|$，而一个元素的阶则记为 $\operatorname{ord} a$。

例 0.7 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 0.8 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** $\mathfrak{S}_X \coloneqq \mathrm{Aut}(X)$. 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 0.9 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 $HxK\coloneqq\{hxk : h\in H, k\in K\}$ 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**

$$[G:H]\coloneqq|G/H|.$$

陪集空间 G/H 未必有限, 在此视 $[G:H]$ 为基数.

定理 0.10 (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 0.11 群 G 中任意元素 g 的阶整除 G 的阶, 即 $\mathrm{ord}\ g\mid|G|$. 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 0.12 设 G 为群.

(i) G 的**中心**定义为 $Z_G\coloneqq\{z\in G:\forall x\in G, xz=zx\}$ [i];
(ii) 设 $E\subset G$ 为任意子集, 定义其**中心化子**为 $Z_G(E)\coloneqq\{z\in G:\forall x\in E, xz=zx\}$ [ii];
(iii) 承上, 定义其**正规化子**为 $N_G(E)\coloneqq\{n\in G : nEn^{-1}=E\}$[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 $N_G(H)=G$.

[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.

定义 0.13 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) $\varphi(1) = 1$.

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 $\mathrm{Im}(\varphi) \coloneqq \{\varphi(x) : x \in M_1\}$, 而其**核**定义为 $\mathrm{Ker}(\varphi) \coloneqq \varphi^{-1}(1)$, 他们分别是 M_1, M_2 的子群.

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**, 记作 $M_1 \cong M_2$. 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 0.14 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

$$\pi : G \twoheadrightarrow G/N^{\text{iv}}, \qquad x \mapsto xN$$

称为**商同态**.

定义 0.15 设幺半群 M 作用于 X. 定义

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

(ii) 对于 $x \in X$, **轨道** $Mx \coloneqq \{mx : m \in M\}$, 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 $M_x \coloneqq \{m \in M : mx = x\}$.

定理 0.16 (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

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

[iv] 一般用 $\hookrightarrow$ 表示单射, 用 $\twoheadrightarrow$ 表示满射. 可类比 $\subset, \supset$ 记忆.

定义 0.17 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

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

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 0.18 (同态基本定理) 设 $\varphi \in \mathrm{Hom}(G, G')$, 则 φ 诱导出同构

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

此同构叫做**正则同构**.

定理 0.19 (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 0.20 (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 0.21 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 0.22 (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 0.23 (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.

有关对称群请参考 [1, 1.6] 或 [2, 4.9], 有关可解群的内容请参考 [1, 附录 1.1] 或 [2, 4.6, 4.7], 这对于 Galois 理论的学习至关重要.

0.2 环和域

定义 0.24 称 $(R,+,\cdot)$ 是 **(含幺) 环**, 如果

(i) $(R,+)$ 是阿贝尔群, 二元运算用加法符号记作 $(a,b)\mapsto a+b$, 加法幺元记为 0, 称之为 R 的加法群;

(ii) $(R,\cdot)$ 是含幺半群;

(iii) $a(b+c)=ab+ac$, $(b+c)a=ba+ca$ (分配律, 或曰双线性)

除去和幺元相关性质得到的 $(R,+,\cdot)$ 称作无幺环. 若子集 $S\subset R$ 对 $(+,\cdot)$ 也构成环, 并且和 R 共用同样的乘法幺元 1, 则称 S 为 R 的**子环**, 或称 R 是 S 的环扩张或扩环. 若乘法也满足交换律则称为**交换环**.

例 0.25 一般将有限个元素 $r_1,\dots,r_n\in R$ 生成的环记为 $\langle r_1,\dots,r_n\rangle$. 在交换环的情形也习惯写作 $(r_1,\dots,r_n)$. 零环 (0) 是无幺环, 也是平凡环.

定义 0.26 设 R,S 为环, 映射 $\varphi:R\to S$ 为**环同态**, 如果 φ 是加法群同态, 且为乘法幺半群同态. 如去掉与 1_R, 1_S 相关的条件, 就得到无幺环之间的同态概念.

由此可导出环的同构 (即可逆同态), 自同态, 自同构, 像与核等概念, 与0.13同一套路, 不再赘述.

定义 0.27 设 R 为环, $I\subset R$ 为加法子群.

(i) 若对每个 $r\in R$ 皆有 $rI\subset I$, 则称 I 为 R 的**左理想**;

(ii) 若对每个 $r\in R$ 皆有 $Ir\subset I$, 则称 I 为 R 的**右理想**;

(iii) 若 I 兼为左, 右理想, 则称作**双边理想**.

满足 $I\neq R$ 的左, 右或双边理想称为真理想. 交换环的左, 右理想不分, 与双边理想一起简称为理想.

定义 0.28 设 I 为 R 的理想, 赋予加法群 R/I 乘法运算如下

$$(r+I)\cdot(s+I)\coloneqq(rs+I),\quad r,s\in R.$$

则 R/I 构成一个环, 称为 R 模 I 的**商环**. 商映射 $R\twoheadrightarrow R/I$ 称为**商同态**.

定理 0.29 (环同态基本定理) 设 $\varphi\in\mathrm{Hom}(R,R')$, 则 $\mathrm{Ker}(\varphi)\coloneqq\varphi^{-1}(0)$ 是 R 的理想, 且诱导同态 $\bar\varphi:R/\mathrm{Ker}(\varphi)\to\mathrm{Im}(\varphi)$ 是环同构.

定义 0.30 既然 R 对乘法构成幺半群, 故可定义其中元素的左逆与右逆. 设 $r\in R$ 非零, 若 r 可逆, 其逆记为 r^{-1}; 全体可逆元构成的乘法群称作**单位**, 记作 $U(R)$, 有时也简记 $R^\times$. 若存在 $r'\neq0$ 使得 $rr'=0$ 则称 r 为**左零因子**; 条件改作 $r'r=0$ 则称**右零因子**. 为 R 中左或右零因子的元素统称为**零因子**. 元素 $r\in R-\{0\}$ 非左零因子当且仅当 r 的左乘满足消去律; 右零因子的情形类似.

定义 0.31 设 R 非零环, 定义其**特征**为加法群元素的最大阶, 记为 $\mathrm{char}(R)$. 若有无限阶元素则特征记为 0.

定义 0.32 无零因子的交换环称为**整环**.

定义 0.33 若环 R 中的每个非零元皆可逆, 则称 R 为**除环**. 交换除环称为**域**[v].

按本节的约定, 除环不能是零环; 某些文献将除环称作**斜域**或**体**, 但体在日本和港澳台地区用以指代域, 所以尽量避免使用体这一说法.

命题 0.34 无零因子的有限环必为除环.

定理 0.35 (Wedderburn 小定理) 对于有限环, 整环等价于除环等价于域.

证明见: https://www.theoremoftheday.org/Docs/WedderburnShamil.pdf

例 0.36 四元数是除环.

定义 0.37 含幺交换环 R 的真理想 I 称为

(i) **素理想**, 如果 $xy \in I$ 蕴涵 $x \in I$ 或 $y \in I$;[vi]

(ii) **极大理想**, 如果 $I \neq R$ 且不存在严格包含 I 的理想.

分别记 R 中素理想和极大理想所成的集合为 $\mathrm{Spec}\ R$ 与 $\mathrm{MaxSpec}\ R$, 称为 R 的素谱和极大理想谱.

命题 0.38 设 I 为含幺交换环 R 的真理想, 则

(i) R/I 为整环当且仅当 I 为素理想;

(ii) R/I 为域当且仅当 I 为极大理想.

推论 0.39 极大理想必为素理想. 其逆一般不成立, 因为整环未必是域.

定义 0.40 设 I 为 R 的理想, 若存在 $a \in R$ 使得 $I = \langle a \rangle = Ra$, 则称 I 为**主理想**. 若整环 R 的所有理想皆为主理想, 则称 R 为**主理想整环**.

定理 0.41 (中国剩余定理) 设 R 为环, $I_1, \dots I_n$ 为一族理想. 假设对每个 $i \neq j$ 皆有 $I_i + I_j = R$, 则环同态

$$\varphi : R \to \prod_{i=1}^{n} R/I_i, \qquad r \mapsto (r \bmod I_i)_{i=1}^{n}$$

诱导出环同构 $R/(\bigcap_{i=1}^{n} I_i) \cong \prod_{i=1}^{n} R/I_i$.

[v] 域在德文中写作 Körper, 因此也有书中用 $\mathbb{K}$ 指代域而非 $\mathbb{F}$.

[vi] 有些书对于一般环的素理想定义为: 对于 R 的理想 I, 如果任意两个理想 A, B 满足 $AB \subset I$, 则 $A \subset I$ 或者 $B \subset P$. 当环是含幺交换环时这两种定义是等价的.

定义 0.42 整环 R 中的非零元 r 称为**不可约**的, 如果 $r \notin R^\times$ 而且在 R 中 $d \mid r$ 蕴涵 $\langle d\rangle = \langle r\rangle$ 或 $d \in R^\times$. 不可约性仅取决于 r 在 $\mathcal{P}$ 中的像. 令 $\mathcal{P} := (R \smallsetminus \{0\})/R^\times$, 以 $\mathring{x} \in \mathcal{P}$ 标记 $x \in R \smallsetminus \{0\}$ 的像如果 $\mathcal{P}$ 的每个元素 $\mathring{r}$ 都能写成

$$\mathring{r} = \prod_{i=1}^{n} \mathring{p}_i, \quad n \in \mathbb{Z}_{\geq 0}$$

其中 $\mathring{p}_i \in \mathcal{P}$ 不可约, 而且 $\{\mathring{p}_1, \ldots, \mathring{p}_n\}$ (计重数但不计顺序) 是唯一的, 则称 R 为**唯一分解整环**; 称 $\mathring{p}_1, \ldots, \mathring{p}_n$ (或其原像 $p_1, \ldots, p_n \in R$) 是 $\mathring{r}$ (或其原像 $r \in R$) 的不可约因子. 约定 $n = 0 \Longleftrightarrow \mathring{r} = 1$. 如果整环 R 中的非零元 p 满足 $p \notin R^\times$ 而且 $p \mid ab \Longleftrightarrow (p \mid a) \vee (p \mid b)$, 则称 p 是**素元**.

(i) p 是素元 $\Longleftrightarrow \langle p\rangle$ 是素理想;
(ii) 素元是不可约元, 当环是 UFD 时反之也成立;
(iii) 整环 R 是 UFD 当且仅当主理想满足升链条件且不可约元皆为素元, 前者保证不可约分解存在, 后者保证此分解唯一.

定义 0.43 设 R 为整环, 若存在良序集 L 和函数 $N : R - \{0\} \to L$, 使得对任意 $x \in R$, $d \in R - \{0\}$ 都存在 $q \in R$ 使 $r := x - qd$ 满足

$$r = 0, \quad \text{或者} \quad r \neq 0 \text{而} N(r) < N(d).$$

满足此条件的 R 称作**欧几里得整环**.

命题 0.44 ED[vii]是 PID, PID 是 UFD.

判定一个环是否为 PID 并不容易. ED 推广了 $\mathbb{Z}$ 中的带余除法, 从而使得判断 PID 变得简易, 比如多项式环即为 ED.

多项式环的内容请参照 [1, 2.5] 或 [2, 5.6, 5.7], 对称多项式环的内容请参照 [1, 附录 2.2] 或 [2, 5.8], 这对于 Galois 理论的学习至关重要.

[vii]此 ED 非彼 ED.

索引

半群 (semigroup), 1
  幺半群 (monoid), 1
不可约 (irreducible), 7

除环 (division ring), 6

单位 (unit), 5

共轭 (conjugation), 4
轨道 (orbit), 3

核 (kernel), 3
环 (ring), 5
  交换环 (commutative ring), 5
  子环 (subring), 5

阶 (order), 1

零因子 (zero divisor), 5
理想 (ideal), 5
  极大理想 (maximal ideal), 6
  素理想 (prime ideal), 6

陪集 (coset), 2

群 (group), 1
  交错群 (alternative group), 2
  商群 (quotient group), 3
  子群 (subgroup), 1
    Sylow p-子群, 4
    正规子群 (normal subgroup), 1
  对称群 (symmetric group), 2
  循环群 (cyclic group), 1
  阿贝尔群 (Abel group), 1

素元 (prime element), 7

特征 (characteristic), 6
同构 (isomorphism), 3
  自同构 (automorphism), 3
同态 (morphism), 3, 5
  自同态 (endomorphism), 3

稳定化子 (stabilizer), 3

域 (field), 6

正规化子 (normalizer), 2
整环 (integral domain), 6
  主理想整环 (PID, principal ideal domain), 6
  唯一分解整环 (UFD, unique factorization domain), 7
  欧几里得整环 (ED, Euclid Domain), 7
中国剩余定理 (CRT, Chinese Remainder Theorem), 6
中心化子 (centralizer), 2

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（卷一：基础架构）, 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.