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. 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. 此为群中的拓扑, 反之, 拓扑中亦有群, 称为拓扑群.

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 $X = \{1,\dots,n\}$ $(n \in \mathbb{Z}_{\geq 1})$ 时也称为 n 次**对称群**, 记为 $\mathfrak{S}_n$[i], 它的每个子群称作**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 $\mathfrak{A}_n$[ii], 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 $Z_G \coloneqq \{z \in G : \forall x \in G, xz = zx\}$ [iii];
(ii) 设 $E \subset G$ 为任意子集, 定义其**中心化子**为 $Z_G(E) \coloneqq \{z \in G : \forall x \in E, xz = zx\}$ [iv];
(iii) 承上, 定义其**正规化子**为 $N_G(E) \coloneqq \{n \in G : nEn^{-1} = E\}$[v].

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] 德文尖角体 S, 对应德语 Symmetrische Gruppe 或英语的首字母 S.
[ii] 德文尖角体 A, 对应德语 Alternierende Gruppe 或英语的首字母 A.
[iii] 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.
[iv] 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.
[v] 因其德文 Normalisator 和英文 normalizer, 首字母为 N.

注记 0.13 若 $N, H \leqslant G$, 而且 $H \subset N_G(N)$, 则 $HN = NH$ 是 G 的子群且 $N \lhd HN$.

定义 0.14 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 $\mathrm{Ker}(\varphi) \coloneqq \varphi^{-1}(1)$. 若 M_1, M_2 是群, 则他们分别是 M_1, M_2 的正规子群.

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 0.15 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

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

称为**商同态**.

定义 0.16 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 0.17 (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

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

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

(iv) 对所有 $x \in X$ 和 $g \in G$, 有

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

定义 0.18 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

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

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. 易知正规子群仅与自身共轭.

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 0.19 (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 0.20 (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 0.21 (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 0.22 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 0.23 (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 0.24 (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 0.25 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 0.26 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 0.27 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0.14同一套路, 不再赘述.

定义 0.28 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 0.29 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 0.30 (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 0.31 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 0.32 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.

例 0.33 有限域$\mathbb{F}_p$ 的特征是 p, 利用二项式定理和数论中的有关结论可知 $\forall x, y \in \mathbb{F}_p$,

$$(x+y)^p = x^p + y^p.$$

定义 0.34 无零因子的交换环称为**整环**. 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**[vii].

例 0.35 按本节的约定, 除环不能是零环, 四元数 $\mathbb{H}$ 是除环; 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 0.36 无零因子的有限环必为除环.

定理 0.37 (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

定义 0.38 设 R 为交换环. 子集 $S \subset R$ 若对环的乘法构成幺半群, 则称 S 为 R 的**乘性子集**. 构作对乘性子集 S 的**局部化** $R[S^{-1}]$ 如下. 首先在集合 $R \times S$ 上定义关系

$$(r,s) \sim (r',s') \Leftrightarrow [\exists t \in S, trs' = tr's] .$$

易证 $\sim$ 是等价关系, 相应的商集记为 $R[S^{-1}]$, 其中的等价类 $[r,s]$ 应该设想为 "商" r/s, 且对任意 $t \in S$ 皆有 $[r,s] = [rt,st]$. 以下定义的环运算因而是顺理成章的:

$$[r,s] + [r',s'] = [rs' + r's, ss'],$$
$$[r,s] \cdot [r',s'] = [rr', ss'].$$

$R[S^{-1}]$ 对此成交换环, 零元为 $0 = [0,s]$ 而幺元为 $1 = [s,s]$, 其中 $s \in S$ 可任取. 由此得到

$$[r,s] = 0 \Leftrightarrow [\exists t \in S, tr = 0] .$$

因此 $R[S^{-1}]$ 是零环当且仅当存在 $s \in S$ 使得 $sR = 0$, 我们既假定 R 含幺元, 这也相当于说 $0 \in S$; 一般总排除这种情形.

另一方面, $r \mapsto [r,1]$ 给出环同态 $R \to R[S^{-1}]$. 注意到 $s \in S$ 的像落在 $R[S^{-1}]^\times$ 中, 其逆无非是 $[1,s]$. 局部化应当同态射 $R \to R[S^{-1}]$ 一并考量.

引理 0.39 设 $S \subset R$ 为乘性子集, $0 \notin S$, 则 $[r,s] \in R[S^{-1}]$ 可逆当且仅当存在 $r_1 \in R$ 使得 $rr_1 \in S$.

证明 若 $rr_1 \in S$ 则 $[r,s][r_1 s, rr_1] = 1$. 反之设存在 $[r',s']$ 使得 $[r,s][r',s'] = 1$, 则存在 $t \in S$ 使得 $trr' = tss'$, 因而 $r(tr') \in S$.

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

原环 R 的部分信息可能在局部化过程中丢失. 可知

$$\operatorname{Ker}\left[R \to R[S^{-1}]\right] = \{r \in R : \exists s \in R, sr = 0\}.$$

我们希望取尽可能大的 S 使得 $R[S^{-1}]$ 是 R 的扩环. 前述讨论自然引向以下结果.

引理 0.40 设 $S \subset R$ 为乘性子集, $0 \notin S$. 则局部化态射 $R \to R[S^{-1}]$ 是单射当且仅当 S 不含零因子. 另一方面, $R - \{0\}$ 中的所有非零因子构成 R 的乘性子集, 相应的局部化记为

$$R \hookrightarrow \operatorname{Frac}(R),$$

而 $\operatorname{Frac}(R)$ 称为 R 的**全分式环**.

当 R 是整环时, $\operatorname{Frac}(R)$ 无非是对 $S := R - \{0\}$ 的局部化; 此时由引理 0.39 知 $\operatorname{Frac}(R)$ 是域: 事实上 $r \neq 0$ 时 $[r, s]^{-1} = [s, r]$; 称此为 R 的**分式域**.

局部化是交换代数中的常见操作, 它把环里一些元素变得可逆, 是分式域概念的推广. 在代数几何的观点下, 局部化所得的环是原来的环的某些 "局部", 其谱自然地是原来环的谱的子集. 既然如此, 局部化的环通常会变得更简单. 我们也常常通过研究环的各个局部化来研究环本身.

定义 0.41 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 $y \in I$;[viii]

(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 $\operatorname{Spec} R$ 与 $\operatorname{MaxSpec} R$, 称为 R 的素谱和极大理想谱.

命题 0.42 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 0.43 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 0.44 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 0.45 (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 $R/\left(\bigcap_{i=1}^{n} I_i\right) \cong \prod_{i=1}^{n} R/I_i$.

[viii] 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 0.46 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 $\mathcal{P} := (R - \{0\})/R^\times$, 以 $\mathring{x} \in \mathcal{P}$ 标记 $x \in R - \{0\}$ 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**.

有以下结论:

(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 0.47 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

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

满足此条件的 R 称作**欧几里得整环**.

命题 0.48 ED[ix]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, 比如域上多项式环即为 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.

[ix] 此 ED 非彼 ED.

附录 A　要点知识

A.1　对称群

定义 A.1 设 $a_1,\dots,a_m$ 是 X 中相异的元素. 对称群 $\mathfrak{S}_X$(见0.8) 中的 m-**轮换** $(a_1\cdots a_m)$ 是下述映射 $\sigma: X\to X$

$$\sigma(a_i)=a_{i+1},\quad i\in\mathbb{Z}/m\mathbb{Z},$$
$$\sigma(x)=x,\quad x\notin\{a_1,\dots,a_m\},$$

在此将下标 $\{1,\dots,m\}$ 方便地视为 $\mathbb{Z}/m\mathbb{Z}$ 中元素, 即模 m 的同余类. 称 m 为该轮换的长度; 2-轮换 (ab) 又称**对换**. 我们称 $\mathfrak{S}_X$ 中两个轮换 $(a_1\cdots a_m),(b_1\cdots b_k)$ 不交, 如果 $\{a_1,\dots,a_m\}\cap\{b_1,\dots,b_k\}=\varnothing$.

由先前讨论可知不交的轮换对乘法相交换. 同样显然的是 $\operatorname{ord}(a_1\cdots a_m)=m$.

命题 A.2 (轮换分解) 每个 $\sigma\in\mathfrak{S}_X$ 都能表成不交的轮换之积

$$\sigma=(a_1a_2\cdots)(b_1b_2\cdots)\cdots$$

其中的轮换 $(a_1\cdots),(b_1\cdots)$ 在至多差一个顺序的意义下唯一. 由于 1-轮换是单位元, 乘积中可以省去.

这无非是 X 在 σ 生成的有限轮换群 $\langle\sigma\rangle$ 下的轨道分解 (引理 0.17), 每个轮换对应到一个轨道, 描述了 σ 在该轨道上的作用.

我们称轮换分解中出现的轮换长度 $n_1,n_2,\dots$ (包括长度为一的轮换) 为 σ 的**轮换型**, 计重数不计顺序. 为了得到唯一性, 不妨排成 $n_1\geq n_2\geq\cdots$, 轮换型因之对应于整数 $n:=|X|$ 的**分拆**: $n=n_1+n_2+\cdots$. 上面对阶数的讨论蕴涵 σ 的阶数等于 $n_1,n_2,\dots$ 的最小公倍数.

推论 A.3 (对换分解) 每个 $\sigma\in\mathfrak{S}_n$ 都能表成若干对换的积, 但不唯一. 且群 $\mathfrak{S}_n$ 由对换 $(1i)$ 或 $(i-1\ i)$ 生成, 这里 $1<i\leqslant n$.

我们既可以将 m-轮换拆分成 $m-1$ 个对换之积, 也可以直接通过排序算法 (如冒泡排序) 将其拆分, 行列式中的逆序数可看为选择排序. 由于对换分解不唯一, 且两两不可交换, 故不如轮换分解方便.

据此, 共轭作用 (见0.18) 在对称群情形下有干净的陈述.

引理 A.4 设 $\tau=(a_1a_2\cdots)(b_1\cdots)\cdots$ 为上述的轮换分解, $\tau\in\mathfrak{S}_X$, 则

$$\sigma\tau\sigma^{-1}=(\sigma(a_1)\sigma(a_2)\cdots)(\sigma(b_1)\cdots)\cdots.$$

作为推论, 元素 τ 的共轭类由其轮换型确定; $\mathfrak{S}_X$ 中的共轭类一一对应于轮换型 $n_1\geq n_2\geq\cdots$, 后者又一一对应于整数 $n=|X|$ 的分拆.

这无非是先给一个新序, 置换后再回到旧序, 等价于在新序下的置换.

引理 A.5 存在唯一的群同态 $\mathrm{sgn}:\mathfrak{S}_n\to\{\pm1\}$ 使得 $\mathrm{sgn}((ab))=-1$.

若置换 $\sigma\in\mathrm{Ker}(\mathrm{sgn})$, 则称为偶置换, 否则为奇置换. 虽然对换分解不唯一, 但对换分解个数的奇偶性将始终保持一致 (因为两个对换之积为一个 3-轮换, 不可能退化成一个对换), 如何得到置换的奇偶性在交错代数 (比如行列式) 中将非常关键.

显然奇偶置换个数相同, 为此我们可以构造一个映射, 将每个偶置换乘上随意一个对换则为奇置换, 容易验证这是一个双射. 因此 $|\mathfrak{A}_n|=n!/2$.

定义 A.6 只有平凡正规子群的群称为**单群**.

例 A.7 (i) 素数阶循环群是单群, 而 $p^n(n\geqslant2,p$为素数$)$ 阶群有非平凡中心, 故不是单群;
(ii) $pq,p^2q(p,q$为素数$)$ 阶群不是单群;
(iii) $2m(m$为大于 3 奇数$)$ 阶群不是单群.

以下记任意置换 σ 的不动点集为 $\mathrm{Fix}(\sigma)\coloneqq\{i:\sigma(i)=i\}$.

定理 A.8 (É. Galois) 当 $n\geq5$ 时 $\mathfrak{A}_n$ 是单群.

证明 设 $H\lhd\mathfrak{A}_n$, $H\neq\{1\}$. 从以上性质可知找出一个 3-轮换 $\sigma\in H$ 即足. 兹断言取 $\sigma\in H-\{1\}$ 使得 $|\mathrm{Fix}(\sigma)|$ 极大便是.

如果 σ 的轮换分解中只有对换, 那么分解中至少含两项如 $(ij)(kl)$, 其中 $\{i,j\}\cap\{k,l\}=\emptyset$. 由于 $n\geq5$, 可取 $r\notin\{i,j,k,l\}$ 并定义

$$\tau\coloneqq(klr),\quad \sigma'\coloneqq[\tau,\sigma]=\tau\sigma\tau^{-1}\sigma^{-1}\in H\quad(\because H\lhd\mathfrak{A}_n).\tag{A.1}$$

可直接验证 $i,j\in\mathrm{Fix}(\sigma')-\mathrm{Fix}(\sigma)$, $\sigma'(k)=r\neq k$, 以及

$$\mathrm{Fix}(\sigma)-\{r\}=\mathrm{Fix}(\sigma)-\{k,l,r\}=\mathrm{Fix}(\sigma)\cap\mathrm{Fix}(\tau)\subset\mathrm{Fix}(\sigma').$$

综之 $|\mathrm{Fix}(\sigma')|>|\mathrm{Fix}(\sigma)|$, 矛盾.

设 σ 的轮换分解中包含长度 >2 的项 $(ijk\cdots)$. 假若 $\sigma=(ijk)$ 则是所求的 3-轮换; 否则因为 σ 不可能是 4-轮换, σ 除了 i,j,k 之外还挪动至少两个相异元 r,l. 依然以 (A.1) 式定义 $\sigma'\in H$. 可以验证 $j\in\mathrm{Fix}(\sigma')$, $\sigma'(k)=l\neq k$ 和

$$\mathrm{Fix}(\sigma)=\mathrm{Fix}(\sigma)-\{k,l,r\}=\mathrm{Fix}(\sigma)\cap\mathrm{Fix}(\tau)\subset\mathrm{Fix}(\sigma').$$

仍得到矛盾 $|\mathrm{Fix}(\sigma')|>|\mathrm{Fix}(\sigma)|$. 明所欲证.

推论 A.9 当 $n\geqslant5$ 时,$\mathfrak{A}_n$ 是 $\mathfrak{S}_n$ 的唯一非平凡正规子群.

利用以上结果和 Sylow 定理可知最小非阿贝尔单群的阶数是 60, 且必同构于 $\mathfrak{A}_n$.

A.2 群列

定义 A.10 考虑一列群同态

$$\cdots \xrightarrow{f_0} G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} \cdots \xrightarrow{f_i} G_{i+1} \to \cdots,$$

长度或有限或无限. 若对所有 i 都有

$$\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1}),$$

则称此列**正合**. 我们经常把 $\{1\}$ 简写为 1, 或用加性符号记为 0. 举例明之, 对于任意同态

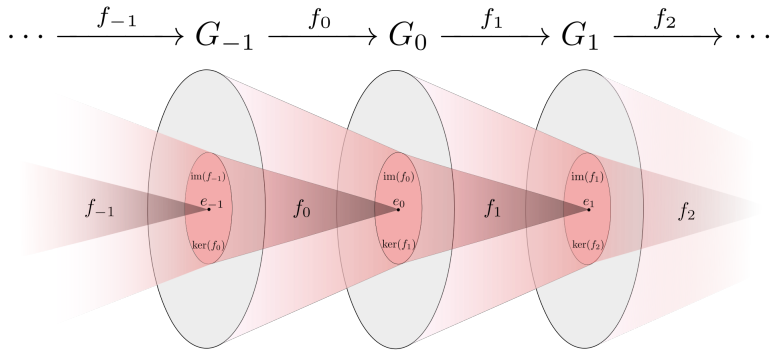

图 A.1: Illustration of an exact sequence of groups G_i using Venn diagrams

$\varphi : G \to G'$, 列 $G \to G' \to 1$ 正合当且仅当 φ 是满的, 列 $1 \to G \to G'$ 正合当且仅当 φ 是单的. **短正合列**为具有下列形式的正合列

$$1 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 1$$

如上所述, 对任何一个短正合序列,f 一定为单射, 且 g 一定为满射, 且 f 的像会等于 g 的核. 有时也称 G 为 G'' 经由 G' 的**扩张**。

正合列经常和交换图表搭配. 其妙用在同调代数中才会完全彰显, 在 Galois 理论中将不会用到.

定义 A.11 群 G 的递降子群链

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_n = \{1\}$$

如满足 $\forall 0 \leq i < n, G_{i+1} \lhd G_i$, 则称之为**正规列**, 而群族

$$G_i/G_{i+1}, \quad i = 0, \ldots, n-1$$

称为该列的**子商**. 正规列的**加细**是透过形如

$$[\cdots \rhd G_i \rhd G_{i+1} \rhd \cdots] \rightsquigarrow [\cdots \rhd G_i \rhd G' \rhd G_{i+1} \rhd \cdots]$$

的反复插项得到的新列. 插入 $G' = G_i$ 或 G_{i+1} 得到的加细是平凡的; 反之则称为**真加细**.

下节将考虑一种特殊的正规列, 在此一并定义.

定义 A.12 群 G 的正规列 $G = G_0 \rhd G_1 \rhd \cdots$ 如对每个 i 都满足

$$G_i \lhd G,$$
$$G_i/G_{i+1} \subset Z_{G/G_{i+1}},$$

则称为**中心列**.

定义 A.13 若群 G 的正规列 $G = G_0 \rhd G_1 \rhd \cdots$ 满足 $G_{i+1} \subsetneq G_i$, 而且子商皆为单群, 则称之为**合成列**[i].

细观单群定义可见合成列正是无冗余项, 而且无法再 (真) 加细的列. 有限群总有合成列, 一般的群则未必.

引理 A.14 (Zassenhaus 引理) 固定群 G, 考虑子群 U, V 及各自的正规子群 $u \lhd U$, $v \lhd V$. 则有

$$u(U \cap v) \lhd u(U \cap V),$$
$$(u \cap V)v \lhd (U \cap V)v,$$

其中各项在注记 0.13 的意义下都是子群, 而且有自然的同构

$$\frac{u(U \cap V)}{u(U \cap v)} \cong \frac{(U \cap V)v}{(u \cap V)v}.$$

定义 A.15 设 $G = G_0 \rhd \cdots$ 为正规列, 我们视其子商 $(G_i/G_{i+1})_{i \geq 0}$ 为不计顺序, 但计入重数的集合. 如果两个正规列长度相同, 而且其子商在上述意义下相等, 则称两正规列**等价**.

定理 A.16 (Schreier 加细定理) 设

$$G = G_0 \rhd \cdots \rhd G_r \rhd G_{r+1} = \{1\},$$
$$G = H_0 \rhd \cdots \rhd H_s \rhd H_{s+1} = \{1\}$$

为 G 的两个正规列, 则两者有等价的加细.

证明 对每个 $0 \leq i \leq r$, $0 \leq j \leq s$ 定义

$$G_{i,j} \coloneqq G_{i+1}(H_j \cap G_i),$$
$$H_{j,i} \coloneqq (G_i \cap H_j)H_{j+1}.$$

先看 $G_{i,j}$, 由 $G_{i+1} \lhd G_i$ 知其为子群. 包含关系 $G_{i,j+1} \lhd G_{i,j}$ 成立, 而且

$$G_{i,0} = G_{i+1}(G \cap G_i) = G_i, \quad G_{i,s+1} = G_{i+1},$$

[i] 有书也译作组成列

遂得到 $(G_i)_{i=0}^r$ 的加细

$$\mathcal{G} \coloneqq [\cdots \rhd G_i = G_{i,0} \rhd G_{i,1} \rhd \cdots G_{i,s} \rhd G_{i,s+1} = G_{i+1} \rhd \cdots].$$

同理可见 $H_{j,i}$ 给出 $(H_j)_{j=0}^s$ 的加细, 记为 $\mathcal{H}$. 在引理 A.14 中取 $u \coloneqq G_{i+1}$, $U \coloneqq G_i$ 和 $v \coloneqq H_{j+1}$, $V \coloneqq H_j$, 遂导出

$$\frac{G_{i,j}}{G_{i,j+1}} = \frac{u(U\cap V)}{u(U\cap v)} \cong \frac{(U\cap V)v}{(u\cap V)v} = \frac{H_{j,i}}{H_{j,i+1}}.$$

当 (i,j) 取遍所有可能, 正规列 $\mathcal{G}$, $\mathcal{H}$ 的各个子商在同构两边都恰好出现一次. 证毕.

推论 A.17 (Jordan–Hölder 定理) 群 G 的任两个合成列皆等价.

因此, 一旦群 G 有合成列, 则其子商在定义 A.15 的意义下无关合成列的选取.

A.3 可解群

定义 A.18 设 G 为群.

(i) 若存在正规列 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$ 使得每个子商都交换, 则称之为**可解群**;
(ii) 承上, 若对每个 i 皆有 $G_i \lhd G$, 且 G_i/G_{i+1} 是素数阶循环群, 则称之为**超可解群**;
(iii) 如果存在中心列 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$, 则称之为**幂零群**.

我们希望在上述定义中找到一类典则的正规列/中心列, 借以检验一个群是否可解或幂零. 以下概念是必要的.

定义 A.19 对于 $x, y \in G$, 定义**换位子**

$$[x,y] \coloneqq xyx^{-1}y^{-1}.$$

对任意子集 $A, B \subset G$, 置 $[A,B] \lhd G$ 为包含 $\{[a,b] : a \in A, b \in B\}$ 的最小正规子群, 或简称为它们生成的正规子群. 递归地定义 G 之

- **导出列**: $\mathscr{D}^0 G \coloneqq G, \mathscr{D}^{i+1}G \coloneqq [\mathscr{D}^i G, \mathscr{D}^i G]$;
- **降中心列**: $\mathscr{C}^0 G \coloneqq G, \mathscr{C}^{i+1}G \coloneqq [\mathscr{C}^i G, G]$.

容易验证以下性质. 设 $i \in \mathbb{Z}_{\geq 0}$:

(i) $xy = yx \Longleftrightarrow [x,y] = 1$, 而 $[x,y]^{-1} = [y,x]$;
(ii) 对于任意群同态 $\varphi : G_1 \to G_2$, 有 $\varphi[x,y] = [\varphi(x), \varphi(y)]$;
(iii) $\mathscr{D}^i G \subset \mathscr{C}^i G$;
(iv) $\mathscr{D}^i G \lhd G$, $\mathscr{C}^i G \lhd G$: 事实上 G 的任何自同构都保持子群 $\mathscr{D}^i G$ 和 $\mathscr{C}^i G$.

关于 $\mathscr{D}^i G$, $\mathscr{C}^i G$ 的性质可以递归地证明. 我们也称 $G_{\mathrm{der}} \coloneqq \mathscr{D}^1 G$ 为 G 的**导出子群**或**换位子群**. 而 $G_{\mathrm{ab}} \coloneqq G/G_{\mathrm{der}}$ 称为 G 的**交换化**.

命题 A.20 群 $\mathfrak{S}_n$ 的导出子群 $\mathscr{D}^1\mathfrak{S}_n$ 等于 $\mathfrak{A}_n$. 当 $n=1$ 时此为显然. 以下解释 $n\geq 2$ 情形: $\mathfrak{S}_n$ 由对换生成, 每个对换都共轭于 (12), 故交换商 $\mathfrak{S}_n/\mathscr{D}^1\mathfrak{S}_n$ 由 (12) 的像生成, 这是二阶元. 给出商同态

$$\mathfrak{S}_n/\mathscr{D}^1\mathfrak{S}_n \twoheadrightarrow \mathfrak{S}_n/\mathfrak{A}_n \cong \{\pm 1\}.$$

比较阶数可见以上同态实为同构, 亦即 $\mathscr{D}^1\mathfrak{S}_n=\mathfrak{A}_n$.

引理 A.21 对任意群 G,

(i) 对每个 i, 商群 $\mathscr{D}^iG/\mathscr{D}^{i+1}G$ 交换, 而 $\mathscr{C}^iG/\mathscr{C}^{i+1}G$ 包含于 $Z_{G/\mathscr{C}^{i+1}G}$;
(ii) 群 G 可解当且仅当 n 充分大时 $\mathscr{D}^nG=\{1\}$;
(iii) 群 G 幂零当且仅当 n 充分大时 $\mathscr{C}^nG=\{1\}$.

设 G 为幂零群, $\mathscr{C}^nG=\{1\}$, 则对任意 $x\in G$, 映射 $[x,\cdot]: g\mapsto [x,g]$ 迭代 n 次后的像落在 $\mathscr{C}^nG$, 故成为平凡映射 $g\mapsto 1$. 这解释了 "幂零" 一词的来由.

引理 A.22 设 G 为群, 用 $\mathcal{P}$ 代表可解, 超可解或幂零三种性质之一.

(i) 若 G 具有性质 $\mathcal{P}$, 则 G 的子群和商群都有性质 $\mathcal{P}$;
(ii) 设 $N\lhd G$, 令 $\bar{G}\coloneqq G/N$, 则 G 可解当且仅当 $N,\bar{G}$ 皆可解.

当 $n\geq 5$ 时 $\mathfrak{A}_n$ 是非交换单群, 因此它必然等于自身的导出子群 $\mathscr{D}^1\mathfrak{A}_n$, 故不可解. 下述推论是证明五次以上方程无根式解的群论钥匙.

推论 A.23 当 $n\geq 5$ 时 $\mathfrak{S}_n$ 不可解.

由 $\mathscr{D}^iG\subset\mathscr{C}^iG$ 知幂零蕴涵可解. 事实上还有下述稍强的结果.

命题 A.24 对于有限群,

循环群 $\subset$ 阿贝尔群 $\subset$ 幂零群 $\subset$ 超可解群 $\subset$ 多循环群 $\subset$ 可解群 $\subset$ 有限生成群.

定理 A.25 (Burnside p^aq^b 定理) $p^aq^b(p,q$ 是素数,a,b 是正整数) 阶群是可解群.

关于可解有限群最著名的结果当属英国数学家 Burnside 的猜想, 该猜想于 1963 年由 Walter Feit 和 John Griggs Thompson 证明.

定理 A.26 (Feit–Thompson 定理) 任意奇数阶有限群皆可解.

该定理曾经有力地推动了有限群的分类工作; 作为一篇有限群论的论文, 其 255 页的长度与繁复亦属空前, 然而还远远不是绝后的.

推论 A.27 除素数阶循环群外, 所有有限单群的阶都是偶数.

索引

兹给出名词索引及其英文翻译, 以供参考. 中文术语按汉语拼音排序.

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.