Algebra: Chapter 0 读书笔记

章小明

更新日期: 2025 年 1 月 2 日

目录

前言

本笔记以 Paolo Aluffi 的 Algebra: Chapter 0 为蓝本, 并参考了一些其它教材, 基于本人的手写自学笔记总结而成, 并不蕴含书的全部内容, 其中对我而言较为简明或显然的部分被略过.

0 范畴论基础

本章旨在记录学习后面的代数内容所必要的范畴论基础内容, 并不包含过多的范畴论知识.

0.1 基础概念

一个范畴 C 包含对象类 $\mathrm{Obj}(\mathsf{C})$ 与态射类 $\mathrm{Mor}(\mathsf{C})$.$\forall X, Y \in \mathrm{Obj}(\mathsf{C})$ 存在态射集合 $\mathrm{Hom}_{\mathsf{C}}(X, Y)$, 其全体并即为 $\mathrm{Mor}(\mathsf{C})$. 态射满足:

(1) $\mathrm{Hom}(X, X) = \mathrm{End}(X)$ 中均存在恒等元素 id_X.

(2) 态射间存在复合, 即存在复合映射 $\circ : \mathrm{Hom}(X, Y) \times \mathrm{Hom}(Y, Z) \to \mathrm{Hom}(X, Z), (f, g) \mapsto gf$.

(3) 复合运算满足结合律.

(4) 恒等元素 (关于复合) 为态射的左/右幺元.

若态射 f(关于复合) 满足左消去律 $f\alpha = f\alpha' \implies \alpha = \alpha'$, 则称 f 为单态射. 相应的右消去律则称为满态射. 若 $f \in \mathrm{Hom}(X, Y)$ 可逆 (即存在 $g \in \mathrm{Hom}(Y, X), fg = \mathrm{id}_Y, gf = \mathrm{id}_X$) 则称 f 为同构. 需要注意的是, 在 Set 中有 "单 + 满 = 同构", 但这在一般的范畴中并不成立.

另外由定义可知,$\mathrm{End}(X)$ 为幺半群且 $\mathrm{Aut}(X)$ 为群. 称所有态射都是同构的范畴为群胚/广群.

范畴 C 有子范畴 C', 若 $\mathrm{Obj}(\mathsf{C}') \subset \mathrm{Obj}(\mathsf{C})$ 且对于 $X, Y \in \mathrm{Obj}(\mathsf{C}')$ 都有 $\mathrm{Hom}_{\mathsf{C}'}(X, Y) \subset \mathrm{Hom}_{\mathsf{C}}(X, Y)$. 若后者为等号则为全子范畴.

最后我们给出反范畴 C^{op}, 其对象与 C 相同而 $\mathrm{Hom}_{\mathsf{C}^{\mathrm{op}}}(X, Y) = \mathrm{Hom}_{\mathsf{C}}(Y, X)$, 且 $f \circ^{\mathrm{op}} g = gf$.

0.2 函子与自然变换

函子 $F : \mathsf{C}_1 \to \mathsf{C}_2$ 表现为对象间的映射 $F : \mathrm{Obj}(\mathsf{C}_1) \to \mathrm{Obj}(\mathsf{C}_2)$ 与态射间的映射, 后者表现为总有映射 $F : \mathrm{Hom}_{\mathsf{C}_1}(X, Y) \to \mathrm{Hom}_{\mathsf{C}_2}(FX, FY)$, 其保持恒等 $\mathrm{id}_X \mapsto \mathrm{id}_{FX}$ 且保持态射间的复合运算 (即关于复合运算 F 成为同态). 另外有其反函子 $F^{\mathrm{op}} : \mathsf{C}_1^{\mathrm{op}} \to \mathsf{C}_2^{\mathrm{op}}$, 其保持对象间映射不变, 而 $F^{\mathrm{op}} : \mathrm{Hom}_{\mathsf{C}_1^{\mathrm{op}}}(X, Y) \to \mathrm{Hom}_{\mathsf{C}_2^{\mathrm{op}}}(FX, FY)$,.

1 群论 (第一部分)

1.1 Grp 范畴

群的基本概念 让我们先从一句抽象废话来描述群的定义:

- 仅含一个对象的群胚 (groupoid)(其所有态射连带态射复合) 构成群. 更进一步的,$\mathrm{Aut}_{\mathsf{C}}(X)$ 是群.

而群之间的同态等价于 Grp 上的态射, 即使
$$\begin{tikzcd} G \times G \arrow[r, "\varphi\times\varphi"] \arrow[d, "m_G"] & H \times H \arrow[d, "m_H"] \\ G \arrow[r, "\varphi"] & H \end{tikzcd}$$
交换的 $\varphi : G \to H$, 这样的 φ 将群上的二元运算 m_G 平移到另一个群上的 m_H, 是很自然的性质. 而这样的交换图给定了 Grp 中的态射,Grp 自然成为范畴.

积与余积 Grp 中的积 (切片范畴 $\mathsf{Grp}_{G,H}$ 的终对象) 和余积 (余切片范畴 $\mathsf{Grp}^{G,H}$ 的始对象) 成为群之间的直积 $G \times H$ 和自由积 $G * H$. 对于前者我们可以直接构造分量 (componentwise) 积运算 $(g, h)(g', h') = (gg', hh')$ 的形式, 后者在自由群中给出构造.

而 Ab 中的积和余积是等价的, 即成为群的直和 $G \oplus H$. 等价性的直接原因是对于任意 $\varphi: G\times H \to A$, 余积定义要求 $\varphi(g,h)=\varphi_G(g)\varphi_H(h)$, 它成为同态需要交换. 但我暂且不知道更深刻的内涵.

最后,$\mathrm{Hom}_{\mathsf{Ab}}(G,H)$ 构成交换群 (态射的加法逐点定义), 此处交换性来源于 G 的交换性, 但构成群的良定性源于 H 的交换性, 因此在 H 是交换群时,$\mathrm{Hom}_{\mathsf{Grp}}(G,H)$ 和 $\mathrm{Hom}_{\mathsf{Set}}(A,H)=H^A$ 都构成群.

范畴中的群对象 范畴 C 若具有有限积和终对象 1, 则其中群对象指 C 中对象 G 连带态射 (二元运算)$m: G\times G \to G$, (幺元)$e: 1\to G$ 和 (取逆)$\iota: G\to G$, 其满足结合律,(双边) 幺和 (双边) 逆:

$$\begin{tikzcd}
(G\times G)\times G \arrow[r, "m\times\mathrm{id}"] \arrow[d, "\cong"] & G\times G \arrow[d, "m"] \\
G\times(G\times G) \arrow[r, "\mathrm{id}\times m"] & G
\end{tikzcd}
\quad
\begin{tikzcd}
1\times G \arrow[r, "e\times\mathrm{id}"] \arrow[dr, "\cong"'] & G\times G \arrow[d, "m"] & G\times 1 \arrow[l, "\mathrm{id}\times e"'] \arrow[dl, "\cong"] \\
& G &
\end{tikzcd}
\quad
\begin{tikzcd}
G \arrow[r, "\mathrm{id}\times\mathrm{id}"] \arrow[d] & G\times G \arrow[r, shift left, "\mathrm{id}\times\iota"] \arrow[r, shift right, "\iota\times\mathrm{id}"'] & G\times G \\
1 \arrow[rr, "e"] & & G \arrow[u, "m"']
\end{tikzcd}$$

从而可以看出, 群是 Set 中的群对象.

1.2 自由群

对于某集合 A, 考虑由集合函数 $j: A\to G$ 作为对象的范畴 $\mathcal{F}^A$, 其中 G 为任意群, 态射由其自然诱导, 即 $j_1 \to j_2$ 为满足 $j_2 = j_1\circ\varphi$ 的群同态 $\varphi: G_1\to G_2$. 我们定义集合 A 生成的自由群 $F(A)$ 为 $\mathcal{F}^A$ 的始对象, 即

$$\begin{tikzcd}
F(A) \arrow[r, "\exists!\varphi"] & G \\
A \arrow[u, "j"] \arrow[ur, "\forall f"'] &
\end{tikzcd}$$

将定义中的 G 改为交换群, 所得到的群即自由交换群 $F^{ab}(A)$.

从范畴论的观点来看, 自由群的泛性质使其构造仅差一个同构, 而 $A\mapsto F(A)$, Set $\to$ Grp 给定了一个自由函子, 其是遗忘函子 For : Grp $\to$ Set 的左伴随.[1]从这一观点 (或直接从泛性质和自由群的构造) 出发, 我们可以得到结果

$$F(A\sqcup B)=F(A)*F(B), F^{ab}(A\sqcup B)=F^{ab}(A)\oplus F^{ab}(B).$$

为了具体刻画 $F(A)$, 我们给出其构造: 用 A 与 A^{-1}(A 的复制) 的无交并构造有限序列 (被称为词 word), 其全集为 $W(A)$, 再用化简/消去的函数 R 将其相邻的互逆元素消去得到化简词,$F(A)=R(W(A))$. 以词的连接并化简作为 $F(A)$ 上的运算, 因此可构造出群 $F(A)$ 的具体形式, 而此时 $j: A\to F(A), a\mapsto (a)$ 成为 $\mathcal{F}^A$ 的始对象.

容易看出 $F(\{*\})=F^{ab}(\{*\})=\mathbb{Z}$, 因此对于 $[n]=\{1,2,\cdots,n\}$,$F^{ab}([n])=\mathbb{Z}^{\oplus n}:=\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}=\mathbb{Z}^n$. 而对于任意集合 A 和交换群 H, 我们定义 H^A 的子群 $H^{\oplus A}:=\left\{\alpha: A\to H \middle| 仅有限个\alpha(a)\neq e_H\right\}$. 事实上我们有 $F^{ab}(A)\cong\mathbb{Z}^{\oplus A}$, 这是因为前者的每个词仅含有限个元素, 而后者也仅有限个元素/分量非零. 可以考虑 $j: A\to\mathbb{Z}^{\oplus A}, a\mapsto\chi_a$, 其中 $\chi_a\in\mathbb{Z}^{\oplus A}: x\mapsto[x=a]$ 是示性函数, 因此 $\displaystyle\sum_{a\in A} m_a j(a)\mapsto\prod_{a\in A} a^{m_a}$ 成为上述同构.

1.3 子群与商群

子群与单同态 我们给出子群一个比较新奇的定义: 群 G 的子集 H 的嵌入映射 $i_H: H\to G$ 是群同态. 这与其一般的定义或 $ab^{-1}\in H$ 等价. 子群的任意交, 直和, 同态像与原像都是子群.

在范畴论视角下, 群同态 $\varphi: G\to G'$ 的核具有某种泛性质: 考虑 Grp 的子范畴 C_φ, 其对象为满足 $\varphi\circ\alpha=0$ 的群同态 $\alpha: K\to G$, 则嵌入 $i: \ker\varphi\to G$ 是其终对象, 即

$$\begin{tikzcd}
\ker\varphi \arrow[d, "i"'] & K \arrow[l, "\exists!\bar{\alpha}"'] \arrow[dl, "\alpha"'] \arrow[d, "\varphi\circ\alpha=0"] \\
G \arrow[r, "\varphi"] & G'
\end{tikzcd}$$

这其实是 "使同态像平凡的子群中 $\ker\varphi$ 是最大的" 的抽象废话式描述.

---

[1]伴随我还没学过, 待补充.

另外, 群的单同态 $\iff$ 核平凡 $\iff$ 同态作为集合函数是单射. 但 Grp 与 Set 中的单同态 (前者是群单同态, 后者是单射) 不同, 尽管存在左逆蕴含单同态, 但 Set 中反之亦然, 而 Grp 中单同态不一定存在左逆.[2]

子集生成的子群 考虑群 G 中的 $A \subset G$, 由泛性质可取出唯一的 $\varphi_A : F(A) \to G$, 我们可以定义 A 生成的子群 $\langle A \rangle := \operatorname{im} \varphi_A < G$.$G$ 交换时取 $F^{ab}(A)$.[3]该定义与其它定义等价, 如 $\langle A \rangle = \bigcap_{A \subset H < G} H$ 或 $\langle A \rangle = \left\{ \prod_{a' \in A'} a' \middle| A' \subset A \right\}$. 若 A 有限, 则称 $\langle A \rangle$ 为有限生成群, 而由定义, 这等价于存在满同态 $F([n]) \to G$. 这一结论也可迁移至交换群上.

商群 对于群 G 商去其上等价关系 $\sim$ 所得到的结构, 我们有结论

- $[a]_\sim [b]_\sim = [ab]_\sim$ 给定了 $G/\sim$ 上的群结构, 等价于 $a \sim a' \implies ag \sim a'g, ga \sim ga'$. 而此时在满足 $a \sim a' \implies \varphi(a) = \varphi(a')$ 的同态 $\varphi : G \to G'$ 构成的范畴中, 典范投影 $\pi : G \to G/\sim$ 成为其始对象.
- 若 $H \lhd G$ 且 $H < \ker \varphi$, 则 (由上泛性质) 有
$$\begin{tikzcd} G/H \arrow[r, "\exists ! \tilde{\varphi}"] & G' \\ G \arrow[u, "\pi_H"] \arrow[ur, "\forall \varphi"'] & \end{tikzcd}$$

实际上商去 (同态给定的) 等价关系与商去 (正规) 子群并没有本质区别, 只有记号差异 $H = [e_G]_\sim$, 尽管同态给定的等价关系内蕴的要求了 $[e_G]_\sim < \ker \varphi$. 而 G/H 的泛性质表明, 它是商去后最普适的, 最小的. 另外, 去掉 $H < \ker \varphi$ 则会导致等价关系不成立, 最小的商群成为 $G/\ker \varphi$.

这一结果也表明, 对于每个同态都能取其核为正规子群, 而对于每个正规子群都存在以其为核的同态, 这表明核与正规子群之间有一定的等价联系.

特征子群 我们可以推广正规子群这一概念: 考虑群 G 的子群 H, 若 $\forall \varphi \in \operatorname{Inn}(G)$(或 $\operatorname{Aut}(G), \operatorname{End}(G)$),$\varphi(H) < H$, 则称 H 是 G 的正规子群 (或特征子群, 全特征子群). 全特征 $\implies$ 特征 $\implies$ 正规. 由上显然正规子群不具有传递性, 但特征与全特征子群具有传递性. 此外, 正规子群的特征子群仍为正规子群, 即 $K < H \lhd G, K$ 是 H 的特征子群, 则 $K \lhd G$.[4]而 $H \lhd G$ 且 G 有限,$|H|$ 与 $|G/H|$ 互素, 则 H 是 G 的特征子群.[5]

导群 群 G 的导群是以其全体交换子 $[g,h] = ghg^{-1}h^{-1}$ 生成的子群, 记为 $G', [G,G]$ 或 G_{der}. 导群保序, 即 $H < G$ 则 $H' < G'$. 对于群同态 $\varphi : G_1 \to G_2$, 显然有 $\varphi([g,h]) = [\varphi(g), \varphi(h)]$ 且 $\varphi(G_1') < G_2'$. 由此可见 G' 是特征子群, 从而 $G' \lhd G$. 若令 $\varphi = \pi_{G'}$ 从而可见 G/G' 交换, 称之为 G 的 Abel 化. 对于 $N \lhd G$,G/N 交换等价于 $G' < N$.

考虑群 G 到任意交换群 A 的群同态 $\alpha : G \to A$, 其构成范畴并自然诱导态射. 由 $\alpha(G') < A' = \{e\}$ 知 $G' < \ker \alpha$, 从而由商群的泛性质可见 $\pi : G \to G/G'$ 为该范畴的始对象.

在自由群上我们有如下结果:$F(A)/F(A)' \cong F^{ab}(A)$.[6][7]

[2]有反例 $\mathbb{Z}/3 \to S_3, k \mapsto (123)^k$.

[3]这其中有什么差异呢? 我想交换应当成为所有普通的群的特例. 但先前自由交换群是较为平凡的情形, 而与一般的自由群有一些区别. 我想这里可能会有一些问题.

[4]$\varphi_g : a \mapsto gag^{-1}, \varphi_g|_H \in \operatorname{Inn}(H) \subset \operatorname{Aut}(H), \varphi_g|_H(K) = gKg^{-1} \subset K$, 反向同理, 故 $gKg^{-1} = K$.

[5]考虑 $\pi_H : G \to G/H, \forall \varphi \in \operatorname{Aut}(G), |\pi_H \circ \varphi(H)|$ 整除 $|\varphi(H)| = |H|$ 以及 $|\operatorname{im} \varphi| = |G/H|$, 故 $\pi_H \circ \varphi(H) = H, \varphi(H) \subset H$.

[6]考虑任意交换群 G 及集合函数 $j : A \to G$, 由 $F(A)$ 的泛性质可得唯一群同态 $\varphi : F(A) \to G, a \mapsto j(a)$, 而核即 $F(A)$ 中次数和为零的词, 显然 $F(A)' < \ker \varphi$, 故由商群泛性质知存在唯一同态 $F(A)/F(A)' \to G$, 故可构造 $j : A \to F(A)/F(A)', a \mapsto aF(A)'$ 为始对象.

[7]这表明包含函子 Ab $\to$ Grp 的左伴随是 Abel 化函子 $G \mapsto G/G'$. 此处需要更多说明.

1.4 典范分解

考虑在 Grp 中的典范分解[8]
$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"] & G' \\ G/\ker\varphi \arrow[r, "\tilde{\varphi}"] & \operatorname{im}\varphi \arrow[u, "i"'] \end{tikzcd}$$
其中 $\tilde{\varphi}$ 是商群关于 φ 诱导的映射, 可以证明其为同构. 此即本节的出发点. 该同构也被称为群同构第一定理. 进一步我们有如下推论:

- 若 $H_1 \lhd G_1, H_2 \lhd G_2$ 则 $\dfrac{G_1 \times G_2}{H_1 \times H_2} \cong \dfrac{G_1}{H_1} \times \dfrac{G_2}{H_2}$.[9]特例是 $(G_1 \times G_2)/G_1 \cong G_2$.
- 对于满同态 $\varphi: G \to H$, 有保序双射 $f: \{K < G | \ker\varphi < K\} \to \{J | J < H\}, K \mapsto \varphi(K)$, 在此对应下正规子群映成正规子群.[10]若令 $\varphi = \pi_N: G \to G/N, N \lhd G$, 则可见 G/N 的子群均为商群形式, 且 $K \lhd G \iff K/N \lhd G/N$.
- (群同构第三定理) 若 $H < N < G$ 且 $H \lhd G$, 则 $N \lhd G \iff \dfrac{N}{H} \lhd \dfrac{G}{H}$, 且此时有 $\dfrac{G/H}{N/H} \cong \dfrac{G}{N}$.[11]
- (群同构第二定理) 若 $K < G$ 且 $H \lhd G$, 则 $H \lhd HK < G, H \cap K < K$ 且 $\dfrac{HK}{H} \cong \dfrac{K}{H \cap K}$.[12]

自由群的关系 群 G 的表示是指同构 $G \cong F(A)/R$ 或 $\rho: F(A) \twoheadrightarrow G, \ker\rho = R$ 是 (词的集合)"关系"$\mathcal{R} \subset F(A)$ 在 $F(A)$ 中生成的正规子群. 记 $G = (A|\mathcal{R})$. 我们有 $F(A) = (A|\varnothing), D_{2n} = (x, y|x^2, y^2, (xy)^n)$. 最后, 由 "自由是遗忘的左伴随" 同样可知 $(A|\mathcal{R}) * (A'|\mathcal{R}') = (A \sqcup A'|\mathcal{R} \sqcup \mathcal{R}')$.

满同态与 coker 在考虑子群与单同态时我们注意到嵌入 $i: \ker\varphi \to G$ 是 Grp 中范畴 C_φ 的终对象. 我们考虑其对偶形式 C^φ:Obj$(\mathsf{C}^\varphi) = \{\alpha: G' \to L | \alpha \circ \varphi = 0\}$, 其始对象即为 $\pi: G' \twoheadrightarrow \operatorname{coker}\varphi$. 综合两者我们有交换图:

$$\begin{tikzcd} \ker\varphi \arrow[d, "i"'] & H \arrow[l, "\exists!\bar{\alpha}"'] \arrow[dl, "\alpha"'] \arrow[d, "\varphi\circ\alpha=0"] \\ G \arrow[r, "\varphi"] \arrow[d, "\beta\circ\varphi=0"'] & G' \arrow[dl, "\beta"'] \arrow[d, two heads, "\pi"] \\ K & \operatorname{coker}\varphi \arrow[l, "\exists!\bar{\beta}"] \end{tikzcd}$$

若在 Ab 中由商群泛性质直接可得 $G'/\operatorname{im}\varphi \cong \operatorname{coker}\varphi$, 而在 Grp 中 $\operatorname{im}\varphi$ 不一定正规于 G', 因此由泛性质仅可得到 $\operatorname{coker}\varphi \cong G'/N$, N 是 $\operatorname{im}\varphi$ 在 G' 中生成的正规子群, 即 G' 中包含 $\operatorname{im}\varphi$ 最小的正规子群.

最后,φ 是满射同态 $\iff$ φ 是满态射 $\implies$ $\operatorname{coker}\varphi$ 平凡. 最后一个箭头的反向需在 Ab 中成立.[13]

1.5 群的作用

基本概念与 G-Set 范畴 群 G 在范畴 C 的对象 A 上的作用即态射 $\sigma: G \to \operatorname{Aut}_{\mathsf{C}}(A)$.[14]称作用是忠实的, 若 σ 是单射; 称作用是自由的, 若 $\ker\sigma$ 平凡. 当 $\mathsf{C} = \mathsf{Set}$ 时我们有记号 $\rho: G \times A \to A, (g, a) \mapsto \sigma(g)(a)$, 记作 ga. 我们有 Cayley 定理: 所有群 G 总能忠实地作用于某集合 A 上, 换言之,G 均同构于某对称群 S_A 的子群.[15]记轨道 $O_G(a) = \{ga | g \in G\}$, 稳定子 $G_a = \operatorname{Stab}_G(a) = \{g \in G | ga = a\}$. 称作用 ρ 可迁, 若 $O_G(a) = A$, 即总能将一个元素迁移为任意另一个. 显然 $G_{ga} = gG_ag^{-1}$, 且作用的核 $\ker\sigma = \bigcap\limits_{a \in A} G_a$.

---

[8]典范分解的更多内容应在补充范畴论内容后继续补充. 参考什么样的范畴具有典范分解?

[9]考虑 $\pi = \pi_1 \times \pi_2$ 即可.

[10]容易验证 $K \mapsto \varphi^{-1}(K)$ 是 f 的逆, 保序显然. 此处应当注意到 $\ker\varphi < K \iff \varphi^{-1}(\varphi(K)) = K$. 最后 $K \lhd G \implies \varphi(K) < H$ 且 $J \lhd H \implies \varphi^{-1}(J) \lhd G$.

[11]$\implies$ 由商群泛性质考虑 $G/H \to G/N$, $\impliedby$ 与同构考虑 $\pi_{N/H} \circ \pi_H: G \to G/H \to \dfrac{G/H}{N/H}$ 即可.

[12]包含关系由考虑 π_H^{-1} 内的包含可得, 再取 $\varphi: K \to HK/H, k \mapsto Hk$ 可证.

[13]反例是嵌入 $H = \{(1), (12)\} \hookrightarrow S_3$ 的 coker 平凡但非满射.

[14]此处以及下面的 G-Set 应当有函子背景, 未来需补全.

[15]其在群作用视角下显然, 因为 G 到自身的左乘作用 $G \to \operatorname{Aut}_{\mathsf{Set}}(G) = S_G, a \mapsto \lambda_a$ 显然是忠实的.

群 G 在集合上的作用构成范畴 G-Set, 其对象是 (ρ, A), 态射为函数 $\varphi: A \to A'$, 其满足
$$\begin{tikzcd} G\times A \arrow[r, "\mathrm{id}_G\times\varphi"] \arrow[d, "\rho"] & G\times A' \arrow[d, "\rho'"] \\ A \arrow[r, "\varphi"] & A' \end{tikzcd}$$
称 G-Set 中态射为 (G-) 等价的, 即 $g\varphi(a)=\varphi(ga)$, 而其中同构即等价双射. 我们有如下结果:G 在 A 上的可迁左作用在 G-Set 中同构于 G 在 $G/_L G_a(\forall a\in A)$ 上的左乘作用.[16]换言之在一般情形下, 在每个轨道 $O_G(a)$ 上都有 $O_G(a)\simeq G/_L G_a$. 因此在 G 和轨道 $O(a)$ 有限时, 我们有 $|G|=|O(a)|\cdot|G_a|$, 此即轨道-稳定子定理. 另外若将 G 视为左乘作用下的 G-集合, 则显然有 $\mathrm{Aut}_{G\text{-Set}}(G)\cong G$.

共轭作用 考虑群 G 作用在有限集 S 上, 定义作用的不动点集 $Z=\{a\in S|\forall g\in G, ga=a\}, a\in Z \iff G_a=G \iff O_a=\{a\}$. 我们有 $|S|=|Z|+\sum_{a\in A}[G:G_a]$, 其中 $A\subset S$ 是 S 的轨道等价类中非平凡轨道的代表元, 即 $a\in A, |O_a|>1$. 这是通过计数得到的: 前项为平凡轨道的数量, 后项为所有非平凡轨道中轨道元素数量之和.

考虑群 G 在自身上的共轭作用, 此时的作用不动点集即中心 $C(G)$, 而稳定子即中心化子 $C_G(a)$, 轨道即共轭类 $[a]=\{gag^{-1}|g\in G\}$. 显然 $C(G)=\bigcap_{a\in G}C_G(a), a\in C(G) \iff C_G(a)=G \iff [a]=\{a\}$. 实际上有 $G/C(G)\cong\mathrm{Inn}(G)$, 且其循环时 G 交换.[17]对共轭作用考虑上述公式可得类数公式:$|G|=|C(G)|+\sum_{a\in A}[G:C_G(a)]$,$A$ 定义同上. 另外注意到 $H\lhd G$ 有 $a\in H$ 则 $[a]\subset H$, 故 $H=\bigcup_{a\in H}[a]$(实则共轭类的不交并).

再考虑群 G 在其幂集上的共轭作用, 即 $\rho(g,A)=gAg^{-1}=\{gag^{-1}|a\in A\}$, 应当注意到 $A\to gAg^{-1}, a\mapsto gag^{-1}$ 是双射. 此作用的稳定化子即正规化子 $N_G(A)=\{g\in G|gAg^{-1}=A\}$, 而 $C_G(A)\subset N_G(A)$ 的每个点在作用下不变. 对于子群 $H<G$ 有 $H\lhd N_G(H)<G$, 且 $N_G(H)$ 是 G 中最大的使 H 正规于之的子群, 即 $H\lhd K$ 则 $K<N_G(H)$, 显然 $H\lhd G \iff N_G(H)=G$. 且由轨道-稳定子定理,H 的共轭子群数量为 $[G:N_G(H)]$.

事实上 $C_G(A)\lhd N_G(A)$, 且 $N_G(A)$ 在 A 上有共轭作用[18], 作用核为 $C_G(A)$, 故 $N_G(A)/C_G(A)$ 同构于 S_A 的某子群. 对于 $H<G$, 该作用成为同态 $N_G(H)\to\mathrm{Aut}_{\mathsf{Grp}}(H)$, 即 $N_G(H)/C_G(H)$ 同构于 $\mathrm{Aut}(H)$ 的某子群, 此即 N/C 定理. 其在 $H=G$ 时即为 $G/C(G)\cong\mathrm{Inn}(G)$, 而对于 $N<N_G(H)$ 在 H 上的共轭作用, 作用核为 $N\cap C_G(H)$.

p-群 p-群即阶为素数 p 幂的群. 由类数公式可知, 其在有限集 S 上作用时有 $|Z|\equiv|S| \bmod p$, 故对于 G 在自身上的共轭作用有 $|G|\equiv|C(G)| \bmod p$, 从而由 $|C(G)|\geq 1$ 可知, 非平凡 p-群必有非平凡中心. 若有限群 G 有 p-子群 H, 则考虑 H 在 $G/_L H$ 上的左乘作用, 可见 $Z=N_G(H)/H$, 即 $[N_G(H):H]\equiv[G:H] \bmod p$.

p^2 阶群总交换, 而 p^n 阶 p-群对 $m\in[n]$ 均有 p^m 阶正规子群.[19]另外, 对于有限群 G 及 $|G|$ 的最小素因子 p, 指数 p 的子群均正规, 而正规 p 阶子群均含于 $C(G)$.[20]

1.6 Sylow 定理

Cauchy 定理 对于有限群 G 及 $|G|$ 的素因子 p,G 中总有 p 阶元.

证明 *(James McKay)*. 考虑 $S=\{(a_1,\cdots,a_p)|a_i\in G, a_1\cdots a_p=e\}$, 由 a_p 由前元素唯一决定, 故 $|S|=|G|^{p-1}\equiv 0 \bmod p$. 令 $\mathbb{Z}/p$ 循环作用于 S 上, 即 $m(a_1,\cdots,a_p)=(a_{m+1},\cdots,a_p,a_1,\cdots,a_m)\in S$(容易验证 $ab=e$ 则 $ba=e$), 显然该作用的稳定点 $Z=\{(a,\cdots,a)|a\in G\}$, 且有 $|Z|\equiv|S|\equiv 0 \bmod p$, 故有 $a^p=e, a\neq e$. □

[16]即考虑函数 $\varphi: G/H\to A, gH\mapsto ga$, 易证其良定等价双射.

[17]前者考虑 $g\mapsto(\varphi_g: a\mapsto gag^{-1})$, 后者考虑 $\varphi_g=\varphi_a^n \implies gag^{-1}=a, a\in C(G)$, 故内自同构均平凡.

[18]即群同态 $N_G(A)\to S_A, n\mapsto(a\mapsto nan^{-1})$

[19]显然 $C(G)$ 的阶为 $p^s, s\leq n$, 故其 p^k 阶子群 $(0\leq k\leq s)$ 均正规. 而考虑 p^m 阶正规子群 H,G/H 仍为 p-群, 故其有非平凡中心. 取其中 p 阶子群 N, 可见 $\pi_H^{-1}(N)$ 是 p^{m+1} 阶正规子群, 归纳可证.

[20](1) 即 $[G:H]=p$,G 在 $G/_L H$ 上的左乘作用即 $\sigma: G\to S_p$, 而 $\ker\sigma\subset H, |G/\ker\sigma|=[G:H][H:\ker\sigma]$, 又有 $|G/\ker\sigma|\,|\,\gcd(|G|,|S_p|)=p$, 故 $[H:\ker\sigma]=1, H=\ker\sigma\lhd G$.(2) 即有共轭作用 $\sigma: G\to\mathrm{Aut}_{\mathsf{Grp}}(H)\cong\mathbb{Z}/(p-1)$, 其中 $\ker\sigma=C_G(H)$, 故 $|G/\ker\sigma|\,|\,\gcd(|G|,p-1)=1$, 即 $G=C_G(H), H<C(G)$.

故由此有推论:G 中 p 阶子群的数量 $N \equiv 1 \bmod p$.[21]此处需要插入看似无关的引理: 若 G 中仅有一个子群 H 同构于某群 K, 则 $H \lhd G$.(共轭不变)

Sylow 第一定理 G 为有限群, 则对 $|G|$ 的任意素因子 p, G 总含 Sylow p-子群.G 中的 Sylow p-子群 P 即 $P < G$ 为 p-群且 p 与 $[G:P]$ 互素, 即 G 中的极大 p-子群. 换言之,$|G| = p^r m, |P| = p^r, \gcd(p,m) = 1$.

定理的等价 (由 p-群性质) 描述为:G 为 $p^n m$ 阶群 (p 为素数且与 m 互素), 则对 $k \in [n]$ 总有 p^k 阶子群, 且该子群是某个 p^{k+1} 阶子群的正规子群.

证明. 首先由 Cauchy 定理,G 中总含 p 阶子群. 下对 k 归纳证明: 若 H 是 G 的 p^k 阶子群 ($k < n$), 则 $0 \equiv [G:H] \equiv [N_G(H):H] \bmod p$, 后项非 0 故 $N_G(H) \neq H$, 且 $N_G(H)/H$ 也含 p 阶子群, 记为 H_1/H, 其中 $H < H_1 < N_G(H)$, 因此 $H \lhd H_1, |H_1| = |H|\,|H_1/H| = p^{k+1}$. □

事实上对于有限交换群有更强的结论: 若 G 是有限交换群且 $d|\,|G|$ 则 G 有 d 阶子群.[22]

Sylow 第二定理 P 是有限群 G 中的 Sylow p-子群,$H < G$ 是 p-子群, 则 H 在 P 的某个共轭中, 即 $H < gPg^{-1}$. 特别的,G 的 Sylow p-子群间互相共轭.

证明. 令 H 左乘作用于 $G/_L P$ 上, 作用不动点集的势 $|Z| \equiv [G:P] \not\equiv 0 \bmod p$, 故有作用不动点 $aP, a^{-1}ha \in P(\forall h \in H), H < aPa^{-1}$. □

事实上有限群 G 的全体 Sylow p-子群之交 $N = \bigcap\limits_{g\in G} gPg^{-1}$ 是 G 中的极大正规 p-子群, 即任意 G 的正规 p-子群均含于 N 中. 换言之, 在 G 的 $|G|/p^\alpha$ 阶同态像中 G/N 是终对象.

Sylow 第三定理 G 为有限群,$|G| = p^n m$, 其中 p 为素数且与 m 互素, 则 G 中的 Sylow p-子群数量 $N_p|m$ 且 $N_p \equiv 1 \bmod p$.

证明. 对任意 Sylow p-子群 P 有 $N_p = [G:N_G(P)]$, 且 $m = [G:P] = N_p[N_G(P):P]$, 而 $m = [G:P] \equiv [N_G(P):P] \bmod p$, 因此 $mN_p \equiv m \bmod p$, 而 m 与 p 互素, 故 $N_p \equiv 1 \bmod p$. □

Sylow 定理的应用

1. 单群即正规子群平凡 (仅有单位元或本身) 的群. 我们有如下命题:
   - mp^r 阶群 ($1 < m < p, p$ 为素数) 不为单群[23]. 若 m 的模 p 余 1 因子仅有 1, 则该命题同样成立.
   - 非平凡交换单群有且仅有 $\mathbb{Z}/p, p$ 为素数.
   - G 为非平凡有限单群 $\iff$ 其同态像平凡或同构于本身[24], 从而非平凡群同态 $\varphi: G \to G'$ 总为单射.
   - 无平方因子群 (即素数平方不能整除阶) 均不是单群.[25]
   - G 是有限单群且 H 是其指数为 N 的真子群, 则 $|G|\,|N!$.[26]特别的, 令 P 是其 Sylow p-子群,$H = N_G(P)$, 则 $|G|\,|N_p!$.
   - 延申阅读:Cole 与有限单群 (I)

[21] 通过计数有 $|Z| = 1 + (p-1)N$, 模 p 即得.

[22] 任取元素生成循环子群再不断商去可得任意素因子, 再如上考虑商群子群, 可得任意因子. 关键在于交换群的子群均正规.

[23] 由 Sylow 第三定理,$1 + kp = N_p|m < p$, 因此 $k = 0, N_p = 1$, 故 Sylow p-子群唯一, 故其正规, 从而非单.

[24] 由定义, 同态核仅有两种选择, 因此同态像也即如此.

[25] 参考Given 3 distinct primes p, q, r, then $|G| = pqr \implies G$ is not simple及Burnside's transfer theorem in group theory.

[26] 令 G 左乘作用于 $G/_L H \cong S_N$ 上, 由 G 单知作用核平凡, 故 $|G|\,|N!$.

2. 对于 pq 阶群 G, 其中 p, q 均为素数且 $p < q$, 若 $q \not\equiv 1 \bmod p$, 则 G 为循环群.[27]反之,G 不交换则有 $N_p = q \equiv 1 \bmod p$
3. 若 p 为奇素数, 则 $2p$ 阶非交换群 $G \cong D_{2p}$.[28]

1.7 合成列与可解群

合成列 群 G 的次正规列 (subnormal series) 是指一列降序子群:

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots$$

其中 $G_i \neq G_{i+1}, G_i \rhd G_{i+1}$, 称 G_i/G_{i+1} 为因子 (群). 若总有 $G_i \lhd G$, 则称之为正规列.[29]列的长度即严格嵌入 $G_i \hookleftarrow G_{i+1}$ 的数量, 也即非平凡因子的数量. 记群 G 的次正规列的最大长度 (若有限) 为 $\ell(G)$, 即 $G_{\ell(G)} = \{e\}$. $\ell(G) = 0$ 即 G 平凡, 而 $\ell(G) = 1$ 即 G 为单群.

次正规列的一步细化 (one-step refinement) 是指比原列仅多一项的次正规列, 次正规列的细化 (refinement) 即有限次一步细化所得次正规列, 若细化比原列长则称为真 (proper) 细化[30]. 换言之, 称某列是另一列的细化, 若后者的项均出现在前者中. 此外, 次正规列之间等价是指次正规列的因子之间仅差一个置换相同 (同构).

对于 G 的有限长次正规列

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}$$

若因子均为单群, 则称之为合成列 (composition series); 若因子均交换 (循环), 则称之为可解列 (solvable series)(循环列). 其中,G/N 为单群等价于 N 在 G 的所有真正规子群中极大, 故称 N 为 G 的极大正规子群. 显然有限群均有合成列, 且次正规列长 $\ell(G)$ 时为合成列.

Jordan-Hölder 定理 若群 G 有二合成列

$$G = G_0 \rhd \underbrace{G_1 \rhd \cdots \rhd G_n = \{e\}}_{G_\bullet}, \qquad G = G_0' \rhd \underbrace{G_1' \rhd \cdots \rhd G_m' = \{e\}}_{G_\bullet'}$$

则 $m = n$, 且两者等价. 换言之合成因子与合成列的选取无关, 即 G_i/G_{i+1} 与 G_i'/G_{i+1}' 间仅差一个置换.

证明. 我们对较短合成列的长度 n 归纳证明之. 显然 $n = 0, 1$ 时命题已成立. 若命题在 $< n$ 时成立, 且 $G_1 = G_1'$, 则两合成列可化为 $G_\bullet$ 和 $G_\bullet'$, 其长度满足归纳假设, 从而命题得证. 故下设 $G_1 \neq G_1'$.

易证 $G_1 \lneq G_1G_1' \lhd G$, 而 G_1 是 G 的极大正规子群, 故可知 $G = G_1G_1'$. 设 $K = G_1 \cap G_1'$, 考虑其任意合成列 (由下定理知存在)$K_\bullet$. 由 $G_1/K \cong G/G_1', G_1'/K \cong G/G_1$ 知两者均为单群, 故可得二合成列 $G \rhd G_1(G_1') \rhd K_\bullet$, 其长度相同且因子间只差一个置换.

最后, 合成列 $G_1 \rhd K_\bullet$ 与 $G_\bullet$ 中较短列的长度满足归纳假设, 从而命题成立, 故 $K_\bullet$ 长 $n-2$, 从而 $G_1' \rhd K_\bullet$ 与 $G_\bullet'$ 也满足归纳假设, 因此命题成立, 综上得证. □

[27]由 Sylow 第三定理及条件有 $N_p = 1$, 即 p 阶子群 H 唯一 (正规). 考虑 G 在 H 上的共轭作用 $\gamma : G \to \mathrm{Aut}(H) \cong \mathbb{Z}/(p-1)$, $|\gamma(G)| \mid \gcd(pq, p-1) = 1$, 故 γ 平凡,$H < C(G)$, 考虑 $G/C(G)$ 的阶从而循环, 即 G 交换. 取其中 p, q 阶元, 乘积必为 pq 阶元, 从而循环.

[28]显然 $N_p = 1$, 令其为正规 p 阶子群 $\langle y \rangle$, 可见 $G - \langle y \rangle$ 的元素均为 2 阶, 任取之为 x, 令 $xyx^{-1} = y^r$, 而 $(y^r)^r = xy^rx^{-1} = x^2yx^{-2} = y$, 从而 $y^{r^2-1} = e, p|(r^2-1)$ 即 $p|(r-1)$ 或 $p|(r+1)$, 即 $r = 1$ 或 $p-1$. 前者则 $xy = yx$ 可得 xy 阶 $2p$, 矛盾. 故可得 $x^2 = y^p = xyxy = e$, 此即 D_{2p}.

[29]该定义在不同资料中略有不同. 此处降序与升序没有本质区别, 仅有下标差别, Chapter 0 与 Hungerford 均使用降序, 而互联网中多见升序. 此外, Chapter 0 中用正规列指 Hungerford 与该笔记中的次正规列, 而没有提到本文的正规列概念. 在 Hungerford 和维基百科中并没有要求 $G_i \neq G_{i+1}$, 但在使用该概念时常需令 G_{i+1} 严格嵌入 G_i, 故在此令两者不等没有本质区别. 最后, 在维基百科中要求子群链结束/开始于 $\{e\}$, 但同样没有本质问题.

[30]在此定义中所有细化均为真细化, 因此我们将混用两概念.

该定理表明合成列若存在则几乎相同且互相等价, 从而可知 G 的合成列均长 $\ell(G)$, 但我们缺乏对存在性的证明. 另外, 上述证明中提到若 K 存在正合列, 则会有 $\ell(G)=n=2+(n-2)=\ell(G/K)+\ell(K)$. 为证明其存在性并推广该结论, 我们有如下定理

Schreier 定理 考虑群 G 及其正规子群 N,G 有合成列等价于 N 与 G/N 有合成列, 此时 $\ell(G)=\ell(N)+\ell(G/N)$, 且 G 的合成因子包含 N 与 G/N 的合成因子.

证明. 一方面, 若 N 与 G/N 均有合成列

$$N \triangleright N_1 \triangleright \cdots \triangleright N_{\ell(N)}=\{e\}, \qquad G/N \triangleright G_1/N \triangleright \cdots \triangleright G_{\ell(G/N)}/N=\{N\}$$

则每个 G_i/N 均可对应到 G 的子群 G_i 上, 且同样有 $G_i \triangleright G_{i+1}, G_i/G_{i+1} \cong (G_i/N)/(G_{i+1}/N)$ 为单群, 从而可以构造 G 的合成列

$$G \triangleright G_1 \triangleright \cdots \triangleright G_{\ell(G/N)}=N \triangleright N_1 \triangleright \cdots \triangleright N_{\ell(N)}=\{e\}$$

并且长度与因子的命题同样得证.

另一方面, 若 G 有合成列

$$G_\bullet : G=G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n=\{e\}$$

则可以构造关于 N 的子群链

$$N \cap G_\bullet : N=N \cap G \triangleright N \cap G_1 \triangleright \cdots \triangleright N \cap \{e\}=\{e\}$$

且 $G_i \cap N \triangleright G_{i+1} \cap N$. 考虑 $\pi : G_i \cap N \to G_i/G_{i+1}, a \mapsto aG_{i+1}, \ker\pi = G_{i+1} \cap N$, 可以证明 $\operatorname{im}\pi \lhd G_i/G_{i+1}$[31], 从而由 G_i/G_{i+1} 是单群知 $\dfrac{G_i \cap N}{G_{i+1} \cap N}$ 平凡或同构于 G_i/G_{i+1}. 由此可见在删去子群链 $N \cap G_\bullet$ 中的重复项后, 其成为 N 的合成列.

对于 G/N 的子群链可以类似构造:

$$\frac{G_\bullet}{N} : \frac{G}{N} \triangleright \frac{G_1 N}{N} \triangleright \cdots \triangleright \frac{\{e\}\,N}{N}=\{e_{G/N}\}$$

且 $G_iN/N \triangleright G_{i+1}N/N$. 同样考虑 $\pi : G_i \to (G_iN)/(G_{i+1}N), a \mapsto aG_{i+1}N$, 易见其为满射, 且 $G_{i+1} < \ker\pi$, 故可由商群的泛性质知有满射 $\varphi : G_i/G_{i+1} \to (G_iN)/(G_{i+1}N), \pi=\varphi \circ \pi_{G_{i+1}}$. 而 G_i/G_{i+1} 为单群, 故 $\dfrac{G_iN/N}{G_{i+1}N/N} \cong \dfrac{G_iN}{G_{i+1}N}$ 平凡或同构于之. 同上可见也有 G/N 的合成列. 最后由 N 与 G/N 的合成列同第一部分可证剩下命题. □

导出列与可解群 回忆导群相关知识, 群 G 的导出列 (derived series) 即子群链 $G \triangleright G' \triangleright G'' \triangleright \cdots$.[32]若 G 交换, 则导出列仅为 $G \triangleright G'=\{e\}$; 若 G 为非交换单群, 则 $G=G'=G''=\cdots$. 可解群 (solvable group) 即导出列终止于 $\{e\}$ 的群, 其等价于具有可解列.[33]

对于有限群 G, 其可解 $\iff$ 合成因子均循环 $\iff$ 有循环列 $\iff$ 有可解列.[34]由此知所有 p-群均可解. 结合 Schreier 定理知, 对于 $N \lhd G$, 有限群 G 可解 $\iff$ N 与 G/N 可解. 此外, 可解群的子群也可解.

幂零群

[31]即证 $\forall g \in G_i \forall a \in G_i \cap N, gag^{-1}G_{i+1} \in \operatorname{im}\pi$, 即 $gag^{-1} \in G_i \cap N$. 显然 $gag^{-1} \in G_i$, 而 $N \lhd G$ 从而 $gag^{-1} \in N$, 故得证.

[32]对于一般资料而言, 次正规列不要求相邻项不等, 故导出列是次正规列.

[33]可解群的导出列显然邻项不等, 故即可解列; 若群有可解列 $G \triangleright G_1 \triangleright \cdots \triangleright G_n=\{e\}$, 则 G/G_1 循环可得 $G_1 > G'$, 同理 $G_2 > G_1' > G''$, 故 $G_i > G^{(i)}, \{e\} > G^{(n)}$, 从而有可解列.

[34]已知 (1) $\iff$ (4), 显然 (2) $\implies$ (3) $\implies$ (4), 仅证 (4) $\implies$ (2): 将可解列细化为合成列, 注意到交换单群仅有素数阶循环群.

2 环与模

2.1 Ring 范畴

环的基本概念 环 $(R,+,\cdot)$ 是交换群 $(R,+,0)$ 与幺半群 $(R,\cdot,1)$[35]关于分配律构成的代数结构.

整环是指无零因子[36]交换 (含幺) 环, 除环是指非零元均可逆的环, 即乘法群 $R* = R-\{0\}$, 域是交换除环. 直观上可以认为域去除可逆性即为整环, 而去除交换性即为除环. 它们之间有一定关系: 整环 $\xRightarrow{\text{有限交换}}$ 域 $\xLeftarrow{\text{有限或交换}}$ 除环 .[37]

关于零因子 (非零元之积为 0) 和正则元 (乘法可逆元)[38]我们有如下结论 (类似对另一边也有):

$$\begin{array}{ccccc}
a\text{不是左零因子} & \Longleftrightarrow & a\text{的左乘作用是}R\to R\text{的单射} & & \\
\Uparrow & & \Uparrow & & \\
a\text{是右正则元} & \Longleftrightarrow & a\text{的右乘作用是}R\to R\text{的满射} & \Longleftrightarrow & R=Ra
\end{array}$$

环 R 的中心 $C(R)=\{r\in R|\forall a\in R, ar=ra\}$ 是 R 的交换子环, 而 a 的中心化子 $C_R(a)=\{r\in R|ar=ra\}$ 是子环, 且 $C(R)=\bigcap\limits_{a\in R}C_R(a)$. 除环的中心化子也是除环, 从而其中心是域.

幺半群环 给定环 R 和幺半群 M, 幺半群环 $R[M]$ 的元素为 $r\cdot m(r\in R, m\in M)$ 的有限线性组合, 其间加法与乘法类似多项式环定义. 可见 $R[x]=R[\mathbb{N}], R[x,x^{-1}]=R[\mathbb{Z}]$.

Ring 的泛对象 Ring 以全体 (含幺) 环为对象, 态射为保持加法交换群与乘法幺半群结构的映射/同态 (需 $1_R\mapsto 1_{R'}$). 其中终对象为零环 $\{0\}$, 始对象为 $\mathbb{Z}$(对每个环都有 $n\mapsto n1_R$).

由于对任意环 R 有唯一环同态 $\iota:\mathbb{Z}\to R, n\mapsto n1_R$, 其核 $\ker\iota=(\operatorname{char}R)\mathbb{Z}$, 我们据此定义环 R 的特征 $\operatorname{char}R\geq 0$. 换言之,$\operatorname{char}R$ 是 1_R 在加法群中的阶 (若阶无限则特征为 0).[39]整环的特征仅有零或质数.

多项式环的泛性质 给定 $A=\{a_1,\cdots,a_n\}$ 与任意交换环 R, 在以 $(j:A\to R,R)$ 为对象的范畴 (态射为诱导的环同态) 中,$(i:a_i\mapsto x_i,\mathbb{Z}[x_1,\cdots,x_n])$ 为始对象. 详细来说, 对于任意 $j:A\to R$, 存在唯一的环同态 $\varphi:\mathbb{Z}[x_1,\cdots,x_n]\to R, n\mapsto n1_R, x_i\mapsto j(x_i)$. 此处要求交换环是因为 R 中的乘法与多项式乘法不一致, 因此需要令不定元的像 $\varphi(x_i)=j(a_i)$ 与任意同态像元素 $\varphi(n)=n1_R$ 交换, 以使 φ 仍保持乘法运算从而成为环同态.

$n=1$ 时, 这一泛性质在任意 (含幺) 环上都存在[40]. 更进一步的, 对于给定环同态 $\alpha:R\to S$, 若有 $s\in S$ 与 $\alpha(r)(\forall r\in R)$ 交换, 则 α 有唯一环同态延拓 $\bar{\alpha}:R[x]\to S, x\mapsto s$.[41]由这一结果, 我们对交换环上的多项式总有取值映射 $\bar{\alpha}:R[x]\mapsto R, f(x)\mapsto\sum\limits_{i\geq 0}a_ir^i=f(r)$, 其由上述 $\alpha=\mathrm{id}_R$ 导出. 换言之, 多项式决定了一个多项式函数 $f:r\mapsto f(r)$.

单满态射与积 单态射的情形与 Grp 中相同: 对于环同态, 单同态 $\iff$ 核平凡 $\iff$ 单射. 同样也有类似的子环定义 (嵌入映射是单同态). 但对于满同态, 我们仅有: 满射 $\implies$ 满同态, 其反例是嵌入 $\iota:\mathbb{Z}\to\mathbb{Q}$ 是满同态[42]而非满射. 从而在 Ring 中 "单 + 满 $\impliedby$ 同构" 但反向不成立.

[35]大部分书都以后者为半群作环的定义, 但由于关于环的大部分讨论都在含幺环上进行讨论, 因此本书中环的定义使乘法半群含幺. 另外, 不一定含幺的环构成的范畴有时记作 Rng.

[36]需要注意的是很多书以零因子为非零元素, 但也有很多书认为 0 也是零因子. 但零因子 = 左零因子 $\cup$ 右零因子.

[37]整环有限交换时为域: 任意元素非零因子则左乘作用为单射, 而有限情况下容易看出其为满射, 这等价于任意元素为正则元 (即可逆). 有限除环为域: 即 Wedderburn 小定理, 后面待证.

[38]a 是左零因子 $\iff\exists b\neq 0, ab=0$; u 是左正则元 $\iff\exists v, uv=1$.

[39]对于不一定含幺的环 R, $\operatorname{char}R=\min\{n\geq 1|\forall a\in R-\{0\}, na=0\}=R$ 中非零元的最大加法阶.

[40]任取 s 作为 $j(a)$, 其总与其它像元素交换, 即 $s\varphi(n)=s(n1_R)=s(1+\cdots+1)=ns=\varphi(n)s$.

[41]存在性容易构造, 唯一性的重点在于 $\bar{\alpha}|_R$ 是否唯一, 以使其与 $x\mapsto s$ 相容. 在 $\mathbb{Z}[x]$ 情形下其唯一性由 $\mathbb{Z}$ 的泛性质保证, 而在此处已固定 $\alpha=\bar{\alpha}|_R$, 故仍唯一.

[42]$\mathbb{Z}$ 到任意环的同态唯一, 故使 $\mathbb{Q}$ 到任意环的同态唯一, 从而有右消去律.

这一问题其实提示我们: 在一般的范畴中, 态射可能过多或过少, 因此可能导致满射态射比满态射要更多. 进一步的, 在具有泛对象的范畴中, 泛对象的性质也可能导致这一结果. 我们看到了 Set 和 Grp 中泛对象都是平凡的, 但 Ring 中的始对象不平凡导致满态射要更少.

对于环的积, 其与群的情形相同, 考虑分量运算的构造即可. 但对于余积, 我们需要在未来考虑张量积运算.

$\mathrm{End}_{\mathsf{Ab}}(G)$　考虑交换群的自同态集, 其关于逐点加法和复合运算构成环. 事实上, 我们有环同构 $\mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}) \cong \mathbb{Z}$[43], 以及类似的 $\mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}/n) \cong \mathbb{Z}/n$. 更进一步, 我们有 Cayley 定理的环版本: 对于任意环 R 中元素的左乘作用 $\lambda_r : a \mapsto ra, \lambda : R \to \mathrm{End}_{\mathsf{Ab}}(R), r \mapsto \lambda_r$ 给出了环单同态.

由于 $\mathbb{Z}$ 上的环自同态与左乘作用完全一致, 因此由 $\lambda : (\mathbb{Z}, +, \circ) \xrightarrow{\sim} \mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}) \cong (\mathbb{Z}, +, \cdot)$ 知,$(\mathbb{Z}, +)$ 上的环 (在同构意义下) 仅有一种. 对于任意环 R, 我们仅有更弱的结论:$C(\mathrm{End}_{\mathsf{Ab}}(R)) \cong C(R)$[44], 从而对于交换环有 $C(\mathrm{End}_{\mathsf{Ab}}(R)) \cong R$.

2.2　理想与商环

环 R 的左理想是指 $I < (R, +)$ 满足 $RI \subset I$, 即 $\forall r \in R \forall a \in I : ra \in I$. 类似定义右理想.(双边) 理想即同时为左理想与右理想. 含幺理想仅有 R 本身, 在不要求含幺的环定义中理想是子环, 而在本书定义中仅为子模. 称 R 的平凡理想为 $\{0\}$ 与 R 本身.

- 对于环同态 $\varphi : R \to S, I \lhd R, J \lhd S$, 则 $\varphi^{-1}(J) \lhd R$, 因此 $\ker\varphi \lhd R$. 而 $\varphi(I) \lhd \operatorname{im}\varphi$ 但非 S 的理想.
- 理想 I_α 的 (有限) 和 $\sum_{\alpha \in A} = \left\{ \sum_{\alpha \in A} r_\alpha \middle| r_\alpha \in I_\alpha \text{仅有限非} 0 \right\}$ 和任意交 $\bigcap_{\alpha \in A} I_\alpha$ 仍为理想.
- 除环等价于仅有平凡 (即零环和本身) 的左/右理想, 而仅有平凡 (双边) 理想的环称为单环, 交换单环即域.
- 交换环 R 中全体幂零元构成理想 N, 称之为诣零根 (nilradical). 非交换环中其不存在.R/N 中不含非零幂零元, 称之为约化环.

若环 R 有理想 I, 其有商环 R/I[45], 其运算直接由 R 的运算导出, 且有环满同态 $\pi : R \to R/I, r \mapsto r + I$. 换言之, 环同态的核与理想的关系是与群的情况一致的: 每个核都是理想, 而每个理想都有自然投影使其成为核.

典范分解　基于上述内容, 我们有其与群的情形完全类似的泛性质与典范分解:

- 商环的泛性质:$I \lhd R, \varphi : R \to S, I \subset \ker\varphi$, 则有交换图
$$\begin{tikzcd} & R \arrow[dl, "\pi"'] \arrow[dr, "\varphi"] & \\ R/I \arrow[rr, "\exists!\tilde{\varphi}"] & & S \end{tikzcd}$$
- 任意环同态 $\varphi : R \to S$ 总有典范分解
$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, two heads, "\pi"] & G' \\ G/\ker\varphi \arrow[r, "\tilde{\varphi}"] & \operatorname{im}\varphi \arrow[u, hook, "i"'] \end{tikzcd}$$
其中 $\tilde{\varphi}$ 是由 φ 诱导的同构.

因此我们也有完全类似的同构定理:

- $\operatorname{im}\varphi \cong R/\ker\varphi$.
- $u : \{J \lhd R | I < J\} \to \left\{J' \lhd R/I\right\}, J \mapsto J/I$ 是保 (包含) 序双射.
- $I \lhd R, I \subset J \lhd R$, 则 $J/I \lhd R/I$ 且 $\dfrac{R/I}{J/I} \cong \dfrac{R}{J}$. 考虑 $\varphi|_{I+\ker\varphi}$ 的典范分解, 有特例 $\dfrac{R/\ker\varphi}{\varphi(I)} \cong \dfrac{R}{I + \ker\varphi}$.
- 第二同构定理略有不同: 若 $S < R, I \lhd R$, 则 $I \lhd S + I < R, S \cap I \lhd S$, 且有 $\dfrac{S}{S \cap I} \cong \dfrac{S + I}{I}$.

[43] 考虑 $\varphi : \mathbb{Z} \to \mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}), n \mapsto n\mathrm{id}_{\mathbb{Z}}, n\mathrm{id}_{\mathbb{Z}} : k \mapsto nk$, 其有逆 $\alpha \mapsto \alpha(1)$.

[44] $\alpha \in C(\mathrm{End}_{\mathsf{Ab}}(R)) \implies \alpha \circ \mu_r = \mu_r \circ \alpha \implies \alpha(r) = \alpha(1)r, \alpha = \lambda_{\alpha(1)}$, 因此可以验证 $C(\mathrm{End}_{\mathsf{Ab}}(R)) \to C(R), \alpha \mapsto \alpha(1)$ 成为 $\lambda|_{C(R)}$ 的逆.

[45] 商环的基础是加法交换群的商群, 其良定下自动成为环, 但为使商良定, 换言之为使 π 成为环同态,I 作为理想是充要的.

2.3 主理想, 素理想与极大理想

主理想 a 的左右主理想为 Ra 和 aR, 定义 a 生成的主理想 $(a)=RaR=\left\{\sum_{i=1}^{n} r_i a s_i \middle| r_i, s_i \in R\right\}$, 其等价定义为 R 中含 a 的最小理想 (或所有理想的交), 这一定义也可类似推广至子集上. 考虑 R 交换的情形, 此时 $(a)=Ra=aR$, 由于总有 $(a_\alpha)_{\alpha\in A}=\sum_{\alpha\in A}(a_\alpha)$, 故有有限生成理想 $(a_1,\cdots,a_n)=(a_1)+\cdots+(a_n)=\left\{\sum_{i=1}^{n} r_i a_i \middle| r_i\in R\right\}$, 基于此我们有同构 $\frac{R/(a)}{(\bar b)}\cong\frac{R}{(a,b)}$, 其中 $\bar b=b+(a)\in R/(a)$. 另外我们对理想 $I_i(i\in[n])$ 有乘积理想 $I_1\cdots I_n=\sum_{a_i\in I_i}(a_1\cdots a_n)\subset\bigcap_{1\le i\le n} I_i$. 若 R 交换时 $\sum_{i=1}^{n} I_i=R$, 或 $R/(I_1\cdots I_n)$ 是约化环, 则乘积理想 $=$ 交理想.

称交换环 R 是 Noether 环 (Noetherian ring), 若每个理想均有限生成, 称整环是主理想整环 (PID), 若每个理想都是主理想. 容易看出,$\mathbb{Z}$ 是 PID, 且 $(n)=n\mathbb{Z},(m,n)=(\gcd(m,n))$, 但 $\mathbb{Z}[x]$ 不是, 因为 $(2,x)$ 不能由一个元素生成.

多项式环的商 任意环 R 上的多项式环 $R[x]$ 中的首一多项式 f 对任意多项式有能良定的带余除法.[46]而对于 R 交换的情形, 带余除法表明对于首一多项式 $f,\forall g\exists! r: g+(f)=r+(f)$ 且 $\deg r<\deg f$. 记 $d=\deg f$, 通过将次数 $<d$ 的多项式 $r(x)=r_0+\cdots r_{d-1}x^{d-1}$ 对应到其系数 $(r_0,\cdots,r_{d-1})\in R^{\oplus d}$, 带余除法给定了关于 f 的群满同态 $\varphi: R[x]\to R^{\oplus d}, g\mapsto(r_0,\cdots,r_{d-1})$ 以及群同构 $R[x]/(f)\cong R^{\oplus\deg f}$.

对某些特别情况我们有更强的结果:

- $\varphi: R[x]\to R, g\mapsto g(a)$ 给出的 $R[x]/(x-a)\cong R$ 是环同构. 换言之即带余除法 $f(x)=q(x)(x-a)+f(a)$.
- 对于 $f(x)=x^2+1$, 通过在 $R\oplus R$ 中定义乘法结构 $(a_0,a_1)\cdot(b_0,b_1)=(a_0b_0-a_1b_1,a_0b_1+a_1b_0)$, 这使 $R\oplus R$ 成为环且上述加法群同态 φ 成为环同态, 故 $R[x]/(x^2+1)\cong R\oplus R$ 成为环同构.
- 对于 $R=\mathbb{R}$, 由此有 $\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$, 由下可说明 (x^2+1) 是 $\mathbb{R}[x]$ 的素 (极大) 理想.
- $\mathbb{Q}[t]/(t^2-d)\cong\mathbb{Q}(\sqrt{d})$.
- 交换环 R 上的多项式 $f_1,\cdots,f_r\in R[x]$ 以及 $a\in R$ 有 $(f_1(x),\cdots,f_r(x),x-a)=(f_1(a),\cdots,f_r(a),x-a)$[47], 因此有 $\frac{R[x]}{(f_1(x),\cdots,f_r(x),x-a)}\cong\frac{R}{(f_1(a),\cdots,f_r(a))}$. 多元情况下也有 $\frac{R[x_1,\cdots,x_n]}{(x_1-a_1,\cdots,x_n-a_n)}\cong R$.

素理想与极大理想 考虑环 R 中的真理想 I, 若 R 交换且 R/I 为整环 (即 $ab\in I\implies a\in I\text{或}b\in I$) 则称 I 为素理想, 其全集即素谱 $\operatorname{Spec}R$; 若 R/I 是单环 (R 交换时即域) 则称 I 为极大理想, 其等价于 R 中没有真包含 I 的真理想. 由定义,R 交换时有极大理想 $\implies$ 素理想, 若此时 R/I 有限则两者等价.R 是整环 $\iff$ (0) 是素理想, 而 R 是 PID 时, 极大理想 $=$ 非零素理想.[48]另外对于交换环, 素理想的原像仍为素理想, 但极大理想没有该性质.[49]

对于 $R[x]$, 上小节同构表明理想 $(x-a)$ 是其素 (极大) 理想等价于 R 是整环 (域), 而 $(2,x)\lhd\mathbb{Z}[x]$ 是素理想, 因为其商环为 $\mathbb{Z}/2$. 对于 PID $\mathbb{Z}$ 中理想 $(n)=n\mathbb{Z}, n$ 为素数 $\iff$ (n) 为非零素 (即极大) 理想. 换言之,$\operatorname{Spec}\mathbb{Z}=\{(p)|p\text{是质数或}0\}$

对于域 $\Bbbk$, 由 $\Bbbk[x]$ 是 PID[50]知其中非零素理想等价于极大理想. 而对于代数闭域 $\Bbbk$(即 $f\in\Bbbk[x]$ 的根均在 $\Bbbk$

[46]即 $\forall g\in R[x]\exists! q,r\in R[x]: g=fq+r$ 且 $\deg r<\deg g$. 存在性: 记 $d=\deg f$, 对于 $\deg g=n>d$ 可构造性的通过 $g=ax^{n-d}f+h,\deg h<\deg g$ 说明这样的操作可以降次, 再归纳的用 f 除 h 可以最终得到余项 $r,\deg r<\deg f$, 因此存在性得证. 唯一性:$fq_1+r_1=fq_2+r_2\implies f(q_1-q_2)=r_1-r_2$, 比较次数说明两个差都是零, 因此唯一.

[47]$f_i(x)=q_i(x)(x-a)+f_i(a)\implies(f_i(x))\subset(f_i(a),x-a)$ 以及 $(f_i(a))\subset(f_i(x),x-a)$, 同理易证等式, 后面同构由上节定理.

[48]前者由有限交换整环为域. 对于后者, 考虑理想 $I=(a)\subset J=(b)$, 由存在 c 使 $a=bc$, 而由素知 $b\in(a)\implies I=J$ 或 $c\in(a)\implies c=da, a=bc=bda\implies bd=1, J=R$.

[49]反例为 $\iota:\mathbb{Z}\hookrightarrow\mathbb{Q}$, 后者的极大理想仅有 (0).

[50]考虑 $I\lhd\Bbbk[x]$ 中次数最小的首一多项式 f, 其唯一, 由带余除法的余项次数小于 $\deg f$ 可知 I 中多项式整除 f, 故 $I=Rf=(f)$.

内),$\Bbbk[x]$ 的极大理想有且仅有 $(x-c), c\in\Bbbk$[51], 故可见 $\operatorname{Spec}\Bbbk[x]=\{(x-c)|c\in\Bbbk\}\cup\{(0)\}$. 对于 $\Bbbk=\mathbb{C}$, 由此可见 $\mathbb{C}[x]$ 的非零素理想分布在一条复 "直线" 上, 这表明其 Krull 维数为 1. 交换环 R 的 (Krull) 维数 $\dim R$ 即素谱中的最大 (包含) 链长.

2.4 R-模

***R*-模** (左)R-模就是环 R 在交换群 M 上的 (左) 环作用, 即环同态 $\sigma: R\to\operatorname{End}_{\mathsf{Ab}}(M)$, 记 $\sigma(r)(m)=rm$.[52]以此言之, 左 R-模即加法交换群 M 连带环 R 与 M 间的运算 $\rho: R\times M\to M, (r,m)\mapsto rm$, 其满足 M-线性 $r(m+n)=rm+rn$, R-线性 $(r+s)m=rm+sm$, (作用) 结合 $(rs)m=r(sm)$, (作用) 含幺 $1m=m$. 所有交换群 M 都能对应到唯一的 $\mathbb{Z}$-模 M 上, 由作用 σ 唯一.

R-模间的态射即保持交换群运算和 R-作用不变的同态[53], 由此全体 R-模构成范畴 R-Mod, 其中有零对象平凡模. 另外,R-Mod 中的双射态射自然成为同构. 易见 $\mathbb{Z}$-Mod 与 Ab 等价, 且 $\operatorname{Hom}_{R\text{-}\mathsf{Mod}}(M,N)\subset\operatorname{Hom}_{\mathsf{Ab}}(M,N)$[54].$R$ 交换时 R-Mod 与 Ab 类似:$\operatorname{Hom}_{\mathsf{Ab}}(M,N)$(关于复合) 构成交换群, 同样的 $\operatorname{Hom}_{R\text{-}\mathsf{Mod}}(M,N)$ 成为 R-模, 且此时有模同构 $\operatorname{Hom}_R(R,M)\cong M$.[55]最后, 若 $R=\Bbbk$ 为域, 称模为 $\Bbbk$-向量空间, 其构成范畴 $\Bbbk$-Vect, 态射即线性映射.

***R*-代数** 对于给定的环同态 $\alpha: R\to S$, 可用同态 $\rho: R\times S\to S, (r,s)\mapsto\alpha(r)s$ 定义 (左)R-模 S. 容易看出, 若令 $S=R, \alpha=\mathrm{id}_R$, 则 R 同样可以成为自身的 R-模. 若 R 交换且 $\alpha(R)<C(S)$, 称此时的环同态 α 是一个 R-代数[56], 其交换即 S 交换. 此时左右模相同, 且可在模上附加环运算 $\rho:(s_1,s_2)\mapsto s_1s_2$, 进而有 $(r_1s_1)(r_2s_2)=(r_1r_2)(s_1s_2)$, 因此称 S 中的乘法是 R-双线性的. 对于域 $\mathbb{K}$ 及其子域 $\Bbbk$, 前者可被视为 $\Bbbk$-代数, 此时称 $\mathbb{K}$ 为 $\Bbbk$ 的扩张.

由上可见,R-代数 α(或 S) 即带有 R-模结构的环 S,R-代数间的态射即同时保持环与模结构的同态[57], 由此构成范畴 R-Alg, 其始对象即 R. 可见 $\mathbb{Z}$-Alg 与 Ring 等价[58]. 环 R 交换时, 复合运算使 $\iota: R\to\operatorname{End}_R(M), r\mapsto r\mathrm{id}_M$ 成为 R-代数. 另外, 交换 R-代数同样构成范畴 R-$\mathsf{CommAlg}$, 其为交换环范畴上的余切片范畴 $\mathsf{CommRing}^R$. 交换环 R 上的多项式环 $R[x_1,\cdots,x_n]$[59]是一个交换 R-代数.

子模与商模 R-模 M 的子模 N 也被自然定义:N 是 R-模且嵌入 $\iota: N\to M$ 是模同态. 换言之,N 是 M 的子群且在 R-作用下封闭:$\forall r\in R\forall a\in N: ra\in N$. 可见 R 若作为自身的 R-模, 则其 (左) 子模即自身的 (左) 理想. 模同态的核与像均为子模, 且子模的和与交均为子模. 若 $r\in C(R), I\lhd R$, 则 rM 与 $IM=\left\{\sum_{i=1}^n r_im_i\middle|r_i\in I, m_i\in M\right\}$ 均为 M 的子模.

对于 M 的子模 N, 容易定义其商模 M/N, 其作为交换群的商且保持 R-作用故同样成为 R-模, 且典范投影成为模同态. 考虑环 R 上的情形,$I\lhd R<$ 环 S, 则 $S, R, I, R/I$ 均为 R-模, 且 R 交换时 R 与 R/I 均成为 R-代数. 而 R 不交换且 I 为其左理想 (即左子模) 时, 商群 R/I 成为左 R-模.

类似群与环, 商模也有泛性质与典范分解:

---

[51]若 $I=(x-c)$ 则 $\Bbbk[x]/I\cong\Bbbk$, 即 I 是极大理想; 若 $I=(f)$ 是极大理想, 则由代数闭域知 $f(x)=q(x)(x-c), I\subset(x-c)$, 由极大知 $I=(x-c)$.

[52]需要注意的是, 对于同样的 R 和 M 也可以有不同的环作用使之成为不同的模, 因此应当认识到模本质上是一个环作用/环同态 σ 或 ρ, 其凭依的 R 和 M 都不是本质的模本身. 但为简便言还是通常称 M 为模, 此时默认其上有一个 R-作用, 而对不同的模也其上的作用不同.

[53]即 $\varphi(m+n)=\varphi(m)+\varphi(n), \varphi(rm)=r\varphi(m)$, 其与 G-Set 中态射一致.

[54]有时记 $\operatorname{Hom}_{R\text{-}\mathsf{Mod}}$ 为 Hom_R.

[55]交换性源于要求 $r\varphi(r'm)=r'[r\varphi(m)]$. 同构可以取 $m\mapsto(\lambda_m: 1_R\mapsto m)$.

[56]出于语言简便, 有时也称 S 是一个 R-代数.

[57]保持加法和乘法运算 $\varphi(s_1s_2)=\varphi(s_1)\varphi(s_2), \varphi(s_1+s_2)=\varphi(s_1)+\varphi(s_2)$, 保持幺元 $\varphi(1)=1$, 保持 R-作用 $\varphi(rs)=r\varphi(s)$. 可见代数同态相当于保持 R-作用的环同态.

[58]上见交换群与附加 $\mathbb{Z}$-模结构的模等价, 而此处仅同时增加了环结构.

[59]准确地说, 是嵌入 $\iota: R\to R[x_1,\cdots,x_n]$.

- N 是 R-模 M 的子模,R-模同态 $\varphi : M \to P$ 满足 $N \subset \ker\varphi$, 则有唯一模同态 $\tilde{\varphi} : M/N \to P$ 使

$$\begin{tikzcd} & M \arrow[dl, two heads, "\pi"'] \arrow[dr, "\varphi"] & \\ M/N \arrow[rr, "\exists!\tilde{\varphi}"] & & P \end{tikzcd}$$

交换. 可见与正规子群或理想的情况类似, 模同态的核与子模等价. 但有所不同的是, 核并不为某个子结构赋予更强的限制, 在未来我们会看到, 这是 R-Mod 作为 Ab-范畴所特有的性质.

- R-模同态也可以被典范分解为满射, 双射与单射的复合, 即

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, two heads, "\pi"] & M' \\ M/\ker\varphi \arrow[r, "\tilde{\varphi}"] & \operatorname{im}\varphi \arrow[u, hook, "i"'] \end{tikzcd}$$

以及由典范分解得来的模同构定理

- $\operatorname{im}\varphi \cong M/\ker\varphi$.
- $u : \{P < M | N < P\} \to \{P' \lhd M/N\}, P \mapsto P/N$ 是保 (包含) 序双射.
- $N < M, N \subset P < M$, 则 $P/N < M/N$ 且 $\dfrac{M/N}{P/N} \cong \dfrac{M}{P}$.
- $N < M, P < M$, 则 $N + P < M, N \cap P < P$ 且 $\dfrac{N+P}{N} \cong \dfrac{P}{N \cap P}$.
- 对于交换环 $R, I, J \lhd R$, 则有 R-模同构 $I \cdot (R/J) \cong (I+J)/J$.

2.5 R-Mod 中的基础概念

积与纤维积 在 Ab-范畴 (如 Ab 或 R-Mod) 中积 (切片范畴的终对象) 与余积 (余切片范畴的始对象) 在任意情形下均存在, 其中积总为直积 (分量积), 而余积总为直和 (或称弱直积, 即仅有限分量非零的积). 两者在有限情形下等价, 而在无限情形下余积为积的子结构.Grp 不是 Ab-范畴, 因此其中余积为自由积.

对于以指标集 A 构造的 R-模 M 的积与余积, 其分别为 $M^A = \prod_{a \in A} M$ 与 $M^{\oplus A}$. 尽管 $M^{\oplus A} < M^A$, 但在 R 交换时有 $\operatorname{Hom}_R(R^{\oplus A}, M) \cong M^A, \varphi \mapsto \{\varphi(a)\}_{a \in A}$, 其有限情形下即 $\operatorname{Hom}_R(R^n, R) \cong R^n$, 此即对偶间的同构.

将上述 (余) 切片范畴改为纤维 (fibered) 形式, 我们有纤维积 (或拉回, pull-back) 与纤维余积 (或推出, push-out), 如下交换图所示: 给定 R-模 M, N, A 及模同态 μ, ν, 存在 R-模 $M \times_A N$ 与模同态 $\pi_M, \pi_N (M \oplus_A N, i_M, i_N)$ 使得对任意 R-模 P 及任意模同态 $\varphi_M, \varphi_N (f_M, f_N)$ 都有唯一模同态满足如下交换图.

$$\begin{tikzcd} P \arrow[dr, dashed, "\exists!"] \arrow[drr, bend left, "\varphi_N"] \arrow[ddr, bend right, "\varphi_M"'] & & \\ & M \times_A N \arrow[r, "\pi_N"] \arrow[d, "\pi_M"] \arrow[dr, phantom, "\square"] & N \arrow[d, "\nu"] \\ & M \arrow[r, "\mu"'] & A \end{tikzcd} \qquad \begin{tikzcd} A \arrow[r, "\nu"] \arrow[d, "\mu"'] \arrow[dr, phantom, "\boxplus"] & N \arrow[d, "i_N"] \arrow[ddr, bend left, "f_N"] & \\ M \arrow[r, "i_M"] \arrow[drr, bend right, "f_M"'] & M \oplus_A N \arrow[dr, dashed, "\exists!"] & \\ & & P \end{tikzcd}$$

可知 $M \times_A N = \{(m, n) \in M \times N | \mu(m) = \nu(n)\}, M \oplus_A N = (M \oplus N)/\{(\mu(a), -\nu(a)) \in M \oplus N | a \in A\}$.

核 R-Mod 中的核与余核也存在: 考虑模同态 $\varphi : M \to N$, 对于满足 $\varphi \circ \alpha = 0$ 的模同态 $\alpha : P \to M$ 为对象的范畴,$\ker\varphi$ 为其终对象; 对于满足 $\beta \circ \varphi = 0$ 的模同态 $\beta : N \to Q$ 为对象的范畴,$\operatorname{coker}\varphi \cong N/\operatorname{im}\varphi$ 为其始对象. 需要注意的是, 这一定义模式可以直接推广到更多范畴中. 对核与余核类似也有交换图:

$$\begin{tikzcd} \ker\varphi \arrow[d, hook, "i"'] & P \arrow[l, "\exists!\bar{\alpha}"'] \arrow[dl, "\alpha"'] \arrow[d, "\varphi\circ\alpha=0"] \\ M \arrow[r, "\varphi"] \arrow[d, "\beta\circ\varphi=0"'] & N \arrow[dl, "\beta"'] \arrow[d, two heads, "\pi"] \\ Q & \operatorname{coker}\varphi \arrow[l, "\exists!\bar{\beta}"] \end{tikzcd}$$

在 R-Mod 中也有关于单满态射的等价关系: 单态射 $\iff$ 核平凡 $\iff$ 单射态射; 满态射 $\iff$ 余核平凡 $\iff$ 满射态射. 这样的等价关系与 Ab 中完全一致, 这也是 Ab-范畴的一般性质. 另外, 尽管存在左 (右) 逆 $\implies$ 单 (满) 态射, 但反之不一定对. 在 R-Mod 中可以仅考虑 $\mathbb{Z} \to \mathbb{Z}, n \mapsto 2n$ 即可.

自由模与自由代数 类似自由群的定义, 考虑集合 A 射到任意 R-模 M 上的集合函数 $f : A \to M$ 构成的范畴 (态射容易诱导), 其中始对象 $j : A \to F^R(A)$ 即 A 生成的自由模, 即交换图 $\begin{tikzcd} F^R(A) \arrow[r, "\exists!\varphi"] & M \\ A \arrow[u, "j"] \arrow[ur, "f"'] & \end{tikzcd}$. 为了详细构造自由模的结构, 我们对 R-模 N 与集合 A 定义直和 $N^{\oplus A} := \{\alpha : A \to N | 仅有限 a \in A 有 \alpha(a) \neq 0\}$[60], 其容易赋有 R-模结构, 且有 $(R^{\oplus A_1})^{\oplus A_2} \cong R^{\oplus A_1 \times A_2}$. 考虑 $j : A \to R^{\oplus A}, a \mapsto \chi_a$. 可以验证 j 即上述始对象, 故 $F^R(A) \cong R^{\oplus A}$. 特别地, 即 $F^R([n]) \cong R^{\oplus n} = R^n$.

可类似定义自由交换 R-代数, 仅考虑 $A = [n]$ 有限情形, 记 $R[A] = R[x_1, \cdots, x_n]$, 考虑函数 $j : A \to R[A], i \mapsto x_i$, 其同样成为所定义范畴的始对象, 换言之 $R[A]$ 即 A 生成的自由交换 R-代数.[61]换言之,(有限不定元的) 多项式环即有限集生成的交换 R-代数, 也因此可见 $\mathbb{Z}[x_1, \cdots, x_n]$ 的泛性质实际是其在交换环范畴 $\mathsf{CommRing}$(即 $\mathbb{Z}$-$\mathsf{CommAlg}$) 中的自由对象.

上述之所以要求代数交换, 是为了不定元之间互相交换, 而 R-Alg 中的自由对象包含不交换多项式环 $R\langle A\rangle$, 其同构于一个 (基于 A 生成的自由幺半群的) 幺半群环, 由 A 中所有有限长字符串构造.

综上我有一个问题:

- 为什么同样对于一个集合 A, 其生成的自由 R-模仅是以 A 中元素为下标的直和 (即弱直积)$R^{\oplus A}$, 而生成的自由交换 R-代数则为以 A 中元素为不定元的多项式环? 准确的说, 为什么是多项式环结构?

在此我给出我的回答:

- 对于自由群与自由交换群, 它们都是被 A 中元素 "生成" 的群, 且生成的方式是取元素构造字符串, 只是交换情形下字符串退化成元素的直和, 字符串连接也成为分量运算.
- 模结构实际上即向量空间的退化, 即数域退化成环, 因此模仍保留大量向量空间的性质. 另一方面,R-模与 (加法) 交换群的本质区别在于 R-作用, 即 $r \in R$ 作用于 $m \in M$ 可以得到 $rm \in M$, 这可以被看做某种 "数乘".
- 综上可见, 自由模是环的直和并不令人意外: 一方面, 模是带有 R-作用的交换群, 因此自由交换群 $\mathbb{Z}^{\oplus A}$(元素为 $\sum\limits_{a\in A} m_a a$, $m_a \in \mathbb{Z}$) 加上 R-作用自然可以成为 $R^{\oplus A}$(元素为 $\sum\limits_{a\in A} r_a a, r_a \in R$). 另一方面, 集合 "生成" 的向量空间即以其为基底的向量空间, 其退化为模时自然带有其分量结构, 即 $R^{\oplus A}$.
- 交换 R-代数可以视为具有交换环结构的 R-模. 限于所学, 下仅讨论 A 有限情形.A 中元素在带有环 (乘法) 的结构中生成, 其可被视作某种不定元, 且应当自然具有幂次与元素间的 (交换) 积. 而加法与 R-作用能自然定义加法和 R 系数, 这些已经自然地给出了多项式, 且其次数总有限 (否则不良定).

子集生成的子模和子代数 生成子模可类似群定义: 考虑 R-模 M 及其子集 A, 上节诱导了唯一模同态 $\varphi_A : R^{\oplus A} \to M$, 其像即 A(作为 R-模) 生成的子模 $\langle A\rangle = \operatorname{im}\varphi_A = \left\{\sum\limits_{a\in A} r_a a \middle| 仅有限 a \in A 有 r_a \neq 0\right\}$, 它也是 M 中含 A 最小子模. 有限生成模即模可由此被有限集生成, 有限生成模 M 的子模 N 不一定有限生成[62], 但 N 与 M/N 为有限生成模时 M 也是 (证明同下). 另外, 有限生成模的同态像也是有限生成模.

可类似定义生成子代数及有限生成代数. 对于 R-代数 S, 其可被视为作为模有限生成或作为代数有限生成, 我们分别称之为 S is finite 与 S is of finite type. 作为有限生成模时 $S \cong R^{\oplus n}/M$, 而作为有限生成代数时 $S \cong R[x_1, \cdots, x_n]/I$.$S$ 作为有限生成 R-模 $\Longrightarrow$ S 作为有限生成 R-代数.[63]

[60]实际上此处 A 即指标集, 也可将该直和中的元素记作 $\{n_a\}_{a\in A}$ 或 $\sum\limits_{a\in A} n_a a$, 其中仅有限个 $n_a \neq 0$, 而这与映射定义完全相同. 这也是上节余积定义的构造形式.

[61]始对象中的唯一性可直接验证, 也可考虑多项式环的泛性质进行唯一延拓.

[62]如无穷不定元多项式环 $\mathbb{Z}[x_1, x_2, \cdots]$, 其是自身的有限生成子模, 但其理想 (即子模)$(x_1, x_2, \cdots)$ 并非有限生成.

[63]$R[x]$ 是有限生成 R-代数, 但非有限生成 R-模.

Noether 模 称一个 R-模是 Noether 模 (Noetherian module), 若其所有子模均作为 R-模有限生成.[64]若 R 是 Noether 环, 可见其即为 Noether R-模. Noether 模的同态像也是 Noether 模. 对于子模 $N < M$, M 是 Noether 模 $\iff$ N 和 M/N 都是 Noether 模.[65]若 R 是 Noether 环, 则有限生成 R-模 M 是 Noether R-模.[66]

单模与循环模 称 R-模 M 为单模 (或不可约模), 若 M 仅有平凡子模. 我们有 Schur 引理: 单模间的非零同态仅有同构, 因此单模的自同态环 $\mathrm{End}_R(M)$ 是除环.[67]称 (左)R-模 M 是循环模, 若 $M = \langle m \rangle = Rm, m \in M$. 单模都是循环模.[68]循环模的商模也都是循环模.[69]模 M 是循环模等价于 $M \cong R/I$, 其中 I 是 R 的 (左) 理想[70], 且此时对 R-模 N 有 $\mathrm{Hom}_R(M, N) = \{n \in N | In = 0\}$[71], 由此可知 $\mathrm{Hom}_{\mathsf{Ab}}(\mathbb{Z}/a, \mathbb{Z}/b) \cong \mathbb{Z}/\gcd(a, b)$.

2.6 链复形与同调

链复形与正合列 R-模的链复形 (chain complex) 是指一列 R-模与 R-模同态:

$$\cdots \xrightarrow{d_{i+2}} M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \cdots$$

其满足 $d_i \circ d_{i+1} = 0$, 换言之即 $\operatorname{im} d_{i+1} \subset \ker d_i$. 常记一列链复形为 $(M_\bullet, d_\bullet)$(或仅 $M_\bullet$), 且下标随箭头减小. 称同态 d_i 为边界或微分, 其也常被记为 d^n, ∂_n. 称链复形在 M_i 处正合, 若 $\operatorname{im} d_{i+1} = \ker d_i$, 正合列 (exact sequence) 即每处正合的链复形. 短正合列即形如

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

的正合列, 其等价于 α 是单同态且 β 是满同态. 由 $\operatorname{im} \alpha = \ker \beta$ 可见 $N \cong M/\operatorname{im} \alpha \cong M/L$. 由此可见, 对于每个模同态 $\varphi : M \to M'$ 可以诱导短正合列

$$0 \longrightarrow \ker \varphi \xrightarrow{i} M \xrightarrow{\varphi} \operatorname{im} \varphi \longrightarrow 0 \qquad 或 \qquad 0 \longrightarrow \ker \varphi \xrightarrow{i} M \xrightarrow{\varphi} M' \xrightarrow{\pi} \operatorname{coker} \varphi \longrightarrow 0$$

应当注意到, 我们可以将每条正合列视作一系列短正合列:

$$\begin{tikzcd}
 & M_{i+2} \arrow[d] \arrow[dr, "d_{i+2}"] & & 0 \arrow[d] & \\
0 \arrow[r] & \operatorname{im} d_{i+2} = \ker d_{i+1} \arrow[r] \arrow[d] & M_{i+1} \arrow[r] \arrow[dr, "d_{i+1}"'] & \operatorname{im} d_{i+1} = \ker d_i \arrow[r] \arrow[d] & 0 \\
 & 0 & & M_i \arrow[d] \arrow[dr, "d_i"] & \\
 & & 0 \arrow[r] & \operatorname{im} d_i = \ker d_{i-1} \arrow[r] \arrow[d] & M_{i-1} \\
 & & & 0 &
\end{tikzcd}$$

---

[64]需要注意的是, 考虑 Noether 模时需要注意其所凭依的环 R, 我们认为一个 R-模是 Noether 模时, 同样将与其相关的模看作 R-模.

[65] $\Longrightarrow$: $M/N = \pi_N(M)$ 显然同样是 Noether 模, 因 N 的子模也是 M 的子模, 故 N 也是 Noether 模. $\Longleftarrow$: 考虑 $P < M$, 注意到 $P \cap N$ 有限生成且 $P/(P \cap N) \cong (P + N)/N < M/N$, 因此 $P/(P \cap N)$ 有限生成, 故 P 有限生成, 即得证.

[66]注意到 M 是某个 $R^{\oplus n}$ 的同态像, 而 $R^{\oplus n}$ 是 Noether 模, 可由上句归纳证明.

[67]注意到同态核与像均为子模, 同态非零则仅有同构情形, 从而自同态均为自同构.

[68]若单模有多个生成元, 可由此给出非平凡子模.

[69] $N < M = Rm, \pi_N : M \to N, N = R\pi_N(m)$.

[70] $\Longrightarrow$: $\varphi_M : R \to \langle m \rangle, 1 \mapsto m$ 是满模同态, 故可取 $I = \ker \varphi_M$. $\Longleftarrow$: 若 $\varphi : R/I \to M$ 是同构, 取 $m_0 = \varphi(1 + I), \forall m \in M \exists! r + I : m = \varphi(r + I) = rm_0$, 故 $M = \langle m_0 \rangle$.

[71]注意到 $\varphi \in \mathrm{Hom}_R(R/I, N)$ 由 $n_0 = \varphi(1 + I) \in \mathrm{RHS}$ 确定, 且需满足 $in_0 = 0, i \in I$ 以确保良定.

分裂正合列　称一个正合列是分裂 (split) 的, 若其满足以下交换图 (即一系列同构):

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r, "\alpha"] \arrow[d, "\sim"] & M \arrow[r, "\beta"] \arrow[d, "\sim"] & N \arrow[r] \arrow[d, "\sim"] & 0 \\
0 \arrow[r] & M_1 \arrow[r, "i_1"] & M_1 \oplus M_2 \arrow[r, "\pi_2"] & M_2 \arrow[r] & 0
\end{tikzcd}$$

分裂正合列可以解答问题 "什么样的同态有左 (右) 逆?" 考虑 R-模同态 $\varphi : M \to N$, 我们有:

- φ 有左逆 $\iff$ 有分裂正合列 $0 \longrightarrow M \xrightarrow{\varphi} N \longrightarrow \operatorname{coker}\varphi \longrightarrow 0$, 此时称 φ 为分裂单同态.
- φ 有右逆 $\iff$ 有分裂正合列 $0 \longrightarrow \ker\varphi \longrightarrow M \xrightarrow{\varphi} N \longrightarrow 0$, 此时称 φ 为分裂满同态.

仅证第一个命题, 第二个类似.

$\Longleftarrow$: 正合列分裂即 φ 是 M 到 $M \oplus M'$ 的嵌入, 因此有左逆 $\psi = \pi_M, \psi\varphi = \mathrm{id}_M$.

$\Longrightarrow$: 令 φ 左逆为 $\psi : N \to M$, 考虑同态 $M \oplus \ker\psi \to N, (m, k) \mapsto \varphi(m) + k$, 其逆为 $n \mapsto (\psi(n), n - \varphi\psi(n))$, 故其为同构, 即 $M \oplus \ker\psi \cong N$, 且由此有 $\varphi : m \mapsto \varphi(m) \leftrightarrow (m, 0)$, 此即嵌入 $i_M : M \mapsto M \oplus \ker\psi$. 最后,$\operatorname{coker}\varphi \to \ker\psi$ 也有同构 $n + \operatorname{im}\varphi \mapsto n - \varphi\psi(n)$, 因此正合列分裂. 有下图所示:

$$\begin{tikzcd}
0 \arrow[r] & \underset{m}{M} \arrow[r, "\varphi"] \arrow[d, "\mathrm{id}_M"] & \underset{n=\varphi(m)}{N} \arrow[r] \arrow[d, "\sim"] & \underset{n+\operatorname{im}\varphi}{\operatorname{coker}\varphi} \arrow[r] \arrow[d, "\sim"] & 0 \\
0 \arrow[r] & \underset{m}{M} \arrow[r, "i_M"] & \underset{(\psi(n), n-\varphi\psi(n))=(m,0)}{M \oplus \ker\psi} \arrow[r] & \underset{n-\varphi\psi(n)}{\ker\psi} \arrow[r] & 0
\end{tikzcd}$$

同调与蛇形引理　对链复形

$$M_\bullet : \cdots \xrightarrow{d_{i+2}} M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \cdots$$

可定义其同调 (模)$H_i(M_\bullet) = \ker d_i / \operatorname{im} d_{i+1}$, 可见 $H_i(M_\bullet) = 0 \iff M_i$ 处正合. 对于链复形

$$M_\bullet : 0 \longrightarrow M_1 \xrightarrow{\varphi} M_0 \longrightarrow 0$$

可见 $H_1(M_\bullet) \cong \ker\varphi, H_0(M_\bullet) \cong \operatorname{coker}\varphi$. 若其正合则同调平凡, 即 φ 是同构.

考虑两正合列, 其间有对应同态:

$$\begin{tikzcd}
0 \arrow[r] & L_1 \arrow[r, "\alpha_1"] \arrow[d, "\lambda"] & M_1 \arrow[r, "\beta_1"] \arrow[d, "\mu"] & N_1 \arrow[r] \arrow[d, "\nu"] & 0 \\
0 \arrow[r] & L_0 \arrow[r, "\alpha_0"] & M_0 \arrow[r, "\beta_0"] & N_0 \arrow[r] & 0
\end{tikzcd}$$

我们有蛇形引理, 即存在正合列[72]

$$0 \longrightarrow \ker\lambda \longrightarrow \ker\mu \longrightarrow \ker\nu \xrightarrow{\delta} \operatorname{coker}\lambda \longrightarrow \operatorname{coker}\mu \longrightarrow \operatorname{coker}\nu \longrightarrow 0$$

或

$$\begin{tikzcd}
0 \arrow[r] & H_1(L_\bullet) \arrow[r] & H_1(M_\bullet) \arrow[r] & H_1(N_\bullet) \arrow[dll, "\delta"'] & \\
& H_0(L_\bullet) \arrow[r] & H_0(M_\bullet) \arrow[r] & H_0(N_\bullet) \arrow[r] & 0
\end{tikzcd}$$

[72]若不令 α_1, β_0 分别为单射与满射, 即去掉交换图左上角与右下角的 0, 则结论也需去掉正合列两端的 0. 这是蛇形引理更一般的版本.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \ker\lambda \arrow[r] \arrow[d] & \ker\mu \arrow[r] \arrow[d] & \underset{a}{\ker\nu} \arrow[d] \arrow[dddll, red, bend left, "\delta"'] & \\
0 \arrow[r] & L_1 \arrow[r, "\alpha_1"] \arrow[d, "\lambda"] & \underset{b}{M_1} \arrow[r, "\beta_1"] \arrow[d, "\mu"] & \underset{a}{N_1} \arrow[r] \arrow[d, "\nu"] & 0 \\
0 \arrow[r] & \underset{c}{L_0} \arrow[r, "\alpha_0"] \arrow[d] & \underset{\mu(b)}{M_0} \arrow[r, "\beta_0"] \arrow[d] & N_0 \arrow[r] \arrow[d] & 0 \\
 & \underset{c+\operatorname{im}\lambda}{\operatorname{coker}\lambda} \arrow[r] \arrow[d] & \operatorname{coker}\mu \arrow[r] \arrow[d] & \operatorname{coker}\nu \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

蛇形引理的证明即对如上交换图的阐释.

1. 首先应注意到图中横纵列均为正合列. 仅需考虑第一行与第四行的正合性. 由 α_1 单与 β_0 满知 $\ker\lambda$ 与 $\operatorname{coker}\nu$ 处正合.

   - 对于 $\ker\mu$ 处, 即证 $\alpha_1(\ker\lambda) = \ker\mu \cap \ker\beta_1 = \ker\mu \cap \operatorname{im}\alpha_1$.$\subset$: $\forall a \in \ker\lambda, \alpha_1(a) \in \operatorname{im}\alpha_1$, 且 $\mu\alpha_1(a) = \alpha_0\lambda(a) = 0, \alpha_1(a) \in \ker\mu$.$\supset$: $\forall b \in \ker\mu \cap \operatorname{im}\alpha_1 \exists a \in L_1, b = \alpha_1(a), \mu(b) = \mu\alpha_1(a) = \alpha_0\lambda(a) = 0$, 由 α_0 单知 $a \in \ker\lambda$.
   - 对于 $\operatorname{coker}\mu$ 处, 由 $\alpha_0(\operatorname{im}\lambda) \subset \operatorname{im}\mu$ 知 $\bar\alpha_0 : a + \operatorname{im}\lambda \mapsto \alpha_0(a) + \operatorname{im}\mu$ 良定,$\bar\beta_0$ 同理. 即证 $\bar\alpha_0(\operatorname{coker}\lambda) = \ker\bar\beta_0$.$\subset$: $\forall a + \operatorname{im}\lambda \in \operatorname{coker}\lambda, \bar\beta_0\bar\alpha_0(a + \operatorname{im}\lambda) = \beta_0\alpha_0(a) + \operatorname{im}\nu = \operatorname{im}\nu$, 因此 $\bar\alpha_0(a + \operatorname{im}\lambda) \in \ker\bar\beta_0$.$\supset$: $\forall b + \operatorname{im}\mu \in \ker\bar\beta_0$, $\beta_0(b) \in \operatorname{im}\nu$, 故 $\exists c \in N_1, \nu(c) = \beta_0(b)$, 又由 β_1 满知 $\exists d \in M_1, c = \beta_1(d)$, 因此 $\beta_0(b) = \nu\beta_1(d) = \beta_0\mu(d), b - \mu(d) \in \ker\beta_0 = \operatorname{im}\alpha_0$. 因此 $\exists a \in L_0, \alpha_0(a) = b - \mu(d), \bar\alpha_0(a + \operatorname{im}\lambda) = b + \operatorname{im}\mu$.

   故该两处正合, 因此得证.
2. $\delta : \ker\nu \to \operatorname{coker}\lambda, a \mapsto \alpha_0^{-1}\mu\beta_1^{-1}(a) + \operatorname{im}\lambda$ 的定义. 如图:$\forall a \in \ker\nu$, 其在嵌入至 N_1 中后由 β_1 满知有原像 $b \in M_1, a = \beta_1(b)$. 由 $\beta_0\mu(b) = \nu\beta_1(b) = \nu(a) = 0$ 知 $\mu(b) \in \ker\beta_0 = \operatorname{im}\alpha_0$, 故有 $c \in L_0, \mu(b) = \alpha_0(c)$. 最后令 $\delta(a) = c + \operatorname{im}\lambda$ 即可. 对于其良定性, 首先由 α_0 单知关于 b 的 c 唯一, 而考虑 a 的不同原像 $b, b' \in M_1, b - b' \in \ker\beta_1 = \operatorname{im}\alpha_1$, 即有 $g \in L_1, b - b' = \alpha_1(g), \mu(b - b') = \mu\alpha_1(g) = \alpha_0\lambda(g)$, 即 $c - c' = \lambda(g)$, 故可知不同的原像 b 仍使 δ 的像 $c + \operatorname{im}\lambda$ 不变.
3. 最后说明 $\ker\nu$ 与 $\operatorname{coker}\lambda$ 处正合.

   - 对于 $\ker\nu$, 即证 $\beta_1(\ker\mu) = \ker\delta$.$\subset$: $\forall a \in \ker\mu, \delta\beta_1(a) = \alpha_0^{-1}\mu(a) + \operatorname{im}\lambda = \operatorname{im}\lambda$.$\supset$: $\forall a \in \ker\delta, \delta(a) = \operatorname{im}\lambda$, $\alpha_0^{-1}\mu\beta_1^{-1}(a) \in \operatorname{im}\lambda$, 故 $\exists b \in L_1, \mu\beta_1^{-1}(a) = \alpha_0\lambda(b) = \mu\alpha_1(b), \beta_1^{-1}(a) - \alpha_1(b) \in \ker\mu, \beta_1(\beta_1^{-1}(a) - \alpha_1(b)) = a$.
   - 对于 $\operatorname{coker}\lambda$, 即证 $\operatorname{im}\delta = \ker\bar\alpha_0$.$\subset$: $\forall a \in \ker\nu, \bar\alpha_0\delta(a) = \mu\beta_1^{-1}(a) + \operatorname{im}\mu = \operatorname{im}\mu$.$\supset$: $\forall c + \operatorname{im}\lambda \in \ker\bar\alpha_0, \alpha_0(c) \in \operatorname{im}\mu$, 即 $\exists b \in M_1, \alpha_0(c) = \mu(b)$, 故有 $a = \beta_1(b), \nu(a) = \beta_0\mu(b) = \beta_0\alpha_0(c) = 0, a \in \ker\nu$, 由 δ 定义知 $\delta(a) = c + \operatorname{im}\lambda$.

蛇形引理有直接推论: 若 μ 满且 ν 单, 则 λ 满且 ν 是同构.[73]以及短五引理:λ, ν 均为同构, 则 μ 也是同构. 由此可见分裂正合列的定义中,$M \cong M_1 \oplus M_2$ 的同构可由其它两同构推出.

正合列的应用

- 若有正合列
  $$\cdots \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow \cdots$$
  且 L, N 是 Noether 模, 则 M 也是.[74]
- 对于 R-模 L, M, N, P 有正合列
  $$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

[73]此条件下即仅有 $0 \longrightarrow \ker\lambda \longrightarrow \ker\mu \longrightarrow \underset{\ker\nu}{0} \xrightarrow{\delta} \operatorname{coker}\lambda \longrightarrow \underset{\operatorname{coker}\mu}{0} \longrightarrow \operatorname{coker}\nu \longrightarrow 0$, 从而结论显然.

[74]注意到 $N \cong M/L$ 及 Noether 模的等价条件.

其可诱导 (交换群,R 交换时则为模) 正合列[75]

$$0 \longrightarrow \mathrm{Hom}_R(N,P) \xrightarrow{\varphi\mapsto\varphi\beta} \mathrm{Hom}_R(M,P) \xrightarrow{\psi\mapsto\psi\alpha} \mathrm{Hom}_R(L,P)$$

而原正合列分裂时, 该诱导的正合列末尾有 $\longrightarrow 0$, 即最右端同态为满射. 而 N 为自由模时, 原正合列分裂.[76]

- 四引理 (four-lemma) 与五引理 (five-lemma): 考虑如下交换图, 其中横行均为正合列.

$$\begin{tikzcd}
A_1 \arrow[r, "f_4"] \arrow[d, "\alpha"] & B_1 \arrow[r, "f_3"] \arrow[d, "\beta"] & C_1 \arrow[r, "f_2"] \arrow[d, "\gamma"] & D_1 \arrow[r, "f_1"] \arrow[d, "\delta"] & E_1 \arrow[d, "\epsilon"] \\
A_0 \arrow[r, "g_4"] & B_0 \arrow[r, "g_3"] & C_0 \arrow[r, "g_2"] & D_0 \arrow[r, "g_1"] & E_0
\end{tikzcd}$$

  四引理即 (1)α 满且 β,δ 单, 则 γ 单;(2)ϵ 单且 β,δ 满, 则 γ 满.[77](其均不涉及第五个态射)

  五引理即其直接推论:β,δ 同构,α 满且 ϵ 单, 则 γ 同构.

- 九引理 (nine-lemma): 考虑如下交换图, 其中横行均为正合列.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & L_2 \arrow[r] \arrow[d] & M_2 \arrow[r] \arrow[d, "\alpha"] & N_2 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & L_1 \arrow[r] \arrow[d] & M_1 \arrow[r] \arrow[d, "\beta"] & N_1 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & L_0 \arrow[r] \arrow[d] & M_0 \arrow[r] \arrow[d] & N_0 \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

  则 (1) 左端两列或右端两列正合, 则剩下一列也正合;(2) 若左右两列正合, 则 α 单且 β 满, 而中间列为链复形时则同样正合;(3) 中间列为链复形时其它列也是, 此时任意两列正合时剩下一列也正合. 其对一般链复形也成立.

---

[75]首先证明 $a:\varphi\mapsto\varphi\beta$ 是单射, 仅需考虑 $\varphi\beta=0=0\beta \implies \varphi=0$. 对于 $\mathrm{Hom}_R(M,P)$ 处的正合, 即证 $\operatorname{im} a=\ker b$, 一方面 $\psi\in\operatorname{im} a, b(\psi)=\psi\alpha=\varphi\beta\alpha=0$, 另一方面由 $N\cong\operatorname{coker}\alpha$ 的泛性质, 对任意 $\psi\in\ker b$ 有唯一 $\varphi, a(\varphi)=\varphi\beta=\psi$.

[76]即证此时 β 有右逆即可使正合列分裂. 由 $N=R^{\oplus A}$ 考虑 $\beta(m_a)=a$, m_a 总存在 (但不唯一), 故可构造 $\sigma:N\to M, n=\sum\limits_{a\in A} r_a a\mapsto \sum\limits_{a\in A} r_a m_a, \beta\circ\sigma=\mathrm{id}_N$, 故有右逆.$\sigma$ 的良定源于 N 自由, 即 $n\in N$ 可被分解为 a 的唯一线性组合.

[77](1) 考虑 $c_1\in C_1,\gamma(c_1)=0$, 则 $g_2\gamma(c_1)=\delta f_2(c_1)=0$, 由 δ 单知 $c_1\in\ker f_2=\operatorname{im} f_3$, 故有 $b_1\in B_1, c_1=f_3(b_1), g_3\beta(b_1)=0$. 故 $\beta(b_1)\in\ker g_3=\operatorname{im} g_4$, 故有 $a_1\in A_1,\beta f_4(a_1)=g_4\alpha(a_1)=\beta(b_1)$, 由 β 单知 $f_4(a_1)=b_1, c_1=f_4f_3(a_1)=0$, 故 γ 单.
(2) 对 $c_0\in C_0$ 有 $d_1\in D_1,\delta(d_1)=g_2(c_0)$, 而 $\epsilon f_1(d_1)=g_1\delta(d_1)=g_1g_2(c_0)=0$, 由 ϵ 单知 $d_1\in\ker f_1=\operatorname{im} f_2$, 故有 $c_1\in C_1, f_2(c_1)=d_1$, 即 $g_2(c_0)=\delta(d_1)=\delta f_2(c_1)=g_2\gamma(c_1), c_0-\gamma(c_1)\in\ker g_2=\operatorname{im} g_3$, 故有 $b_1\in B_1, c_0-\gamma(c_1)=g_3\beta(b_1)=\gamma f_3(b_1), c_0=\gamma(c_1+f_3(b_1))\in\operatorname{im}\gamma$.