抽象代数学

● 辛 林 编著

福建教育出版社

抽象代数学

辛 林 编著

福建教育出版社

抽象代数学

辛　林　编著

福建教育出版社出版发行
（福州梦山巷27号　邮编350001）
福州市鼓楼印刷精装厂印刷
（福州北大路钱塘巷9号　邮编350003）

开本850×1168　1/32　8.125印张　200千字
1998年7月第一版　1998年7月第一次印刷
印数：1—1000

ISBN7—5334—2497—2/G·2026　定价：17.00元

序　言

本书原稿是福建师大数学系基础数学硕士研究生抽象代数学的讲义，这几年又在教学实践中经过了多次修改而形成。基本意图是使得一年级研究生或高年级数学本科生，能够在一个学期的教学时间（周时数为4）内，掌握代数学的一些基本理论和基本方法，也能够使有兴趣的读者在掌握近世代数基础上，通过自学，了解或掌握抽象代数学的基本内容。

本书共分为六章。第一章介绍群的基本理论，内容有置换群、西洛定理、有限交换群、可解群、可除群等。第二章阐述伽罗瓦理论，我们认为，伽罗瓦理论是域论中最基本的部分，虽然其发展历史似乎是为了解决古代的几个数学问题，但其实际意义远远超出了这些范围，他的基本理论和基本方法对现代数学都产生了极其重要的影响。作为数学工作者有必要了解和掌握这些内容。因此，在内容的安排上，以伽罗瓦理论为重点，将古代几个数学问题，如几何作图问题、n 次方程公式解问题在附录或正文中阐述。第三章格论，在代数结构的共性研究中，它起到了重要作用。第四章讨论模的一些基本概念、基本性质。作为大学线性代数中向量空间的自然拓展以及内容的衔接，我们还专门讨论了除环上的模等。第五章讨论交换环上线性代数，将数域或一般域上的线性代数推广到一般交换环上，如交换环上行列式理论、交换环上线性方程组解、矩阵的秩、相似关系等。第六章范畴，这是一个在现代数学中应用广泛的概念，限于篇幅以及本书之目的，只介绍

基础部分。尽管如此，也能够从中领略到如何从各种不同的总体中，找到共同的规律，建立起统一的数学系统这样一条认识规律。

在各节末均配备了大量的习题，难易均有安排，能适应于不同程度不同层次的读者。这些练习对于巩固学习内容，加强代数训练都有启发意义，何况有些练习本身还是后面定理、命题等证明上的依据。

本书内容由浅入深，通俗易懂，只要求有大学近世代数基础就能够自学下去。本书可供高等院校作为高年级本科生或一年级研究生基础课教材或参考用书，也可取舍部分章节作为选修教材。

本书从始至终得到福建师大数学系薛卫民教授的鼓励和指导，并承蒙福建师范大学陈德仁育才基金资助出版，在此深表感谢。

限于作者水平，书中错漏之处恳请读者批评指正。

作　者

福建师范大学数学系

部分常用符号说明

第一章

$\boldsymbol{Z}$：整数集(环).

$\boldsymbol{Q}$：有理数集(域).

$\boldsymbol{R}$：实数集(域).

$\boldsymbol{C}$：复数集(域).

$\boldsymbol{N}$：自然数集.

$a|b$：a 整除 b.

$[G:H]$：子群 H 在 G 中的指数.

$|G|$：群 G 的阶数.

$\langle S\rangle$：由 S 生成的子群.

$\mathrm{Im}f$：f 的象集.

$\mathrm{Ker}f$：f 的核.

$\mathrm{Coker}f$：f 的上核.

$\mathrm{Hom}(G_1,G_2)$：G_1 到 G_2 的所有同态组成的集合.

$H\lhd G$：H 是 G 的正规子群.

$\mathrm{End}(G)$：$\mathrm{Hom}(G,G)$.

$\boldsymbol{Z}_p$：$\boldsymbol{Z}/p\boldsymbol{Z}$ 是 $\boldsymbol{Z}$ 模 p 的剩余类加群(环).

$\boldsymbol{Z}(p^\infty)$：拟循环 p 群，这是 $\boldsymbol{Q}/\boldsymbol{Z}$ 的一个子群.

$\cup$：集合并.

$\cap$：集合交.

$A-B$(或 $A\backslash B$)：集合 A 与 B 的差集.

第二章

$\mathrm{Ch}F$：域 F 的特征.

$[K:F]$(或 $\dim_F K$)：K 作为 F－向量空间的维数.

$F\leqslant K$：K 是域 F 的扩域.

$F[x_1,x_2,\cdots,x_n]$：域 F 上关于 $x_1,\cdots,x_n$ 的多项式环.

$F(x_1,x_2,\cdots,x_n)$：$F[x_1,\cdots,x_n]$的分式域.

K^H：H 在 K 中的固定域.

$\mathrm{Aut}(_FK)$：域扩张 $F\leqslant K$ 的伽罗瓦群.

$\triangle$：素域.

$|\cdot|$元素周期.

第三章

$x\vee y$：格上的并运算，表示 x 与 y 的最小上界.

$x\wedge y$：格上的交运算，表示 x 与 y 的最大下界.

D_1：$x\wedge(y\vee z)=(x\wedge y)\vee(x\wedge z)$.

D_2：$x\vee(y\wedge z)=(x\vee y)\wedge(x\vee z)$.

x'：x 的补元.

2^X：集合 X 的幂集.

第四章

$_RM$，(M_R)：左 R(右 R)－模.

$_RM_S$：左 R－右 S－双模.

$\mathrm{Hom}_R(M,N)=\mathrm{Hom}(_RM,{}_RN)$：模 M 到 N 的所有 R－同态构成的加法群.

End_RM：$\mathrm{Hom}_R(M,M)$.

第五章

$R^{n\times m}$：环 R 上 $n\times m$ 阶矩阵的集合.

R^n：$R^{n\times 1}$或 $R^{1\times n}$.

$r(A)$：矩阵 A 的秩.

$r_R(A)$：矩阵 A 的 McCoy 秩(这里称弱秩).

$F_t(A)$：矩阵 A 中所有 t 阶子式生成的理想.

$\mathrm{Ann}_R(S)$：S 在 R 上的零化子.

$|A|$（或 $\det(A)$）：矩阵 A 的行列式.

I：单位矩阵.

$A\left(\begin{matrix} i_1 \cdots i_t \\ j_1 \cdots j_t \end{matrix}\right)$：从矩阵 A 中取(i_s, j_p)位置上元素构成的子矩阵.

$(-1)^\tau$：当 τ 为奇置换时为-1，τ 为偶置换时为 1.

A^*：矩阵 A 的伴随矩阵.

A'：矩阵 A 的转置矩阵.

$\wedge(M)$：模 M 的 Grassmann 外代数.

$x \wedge y$：x 与 y 的外积.

$AX=B$：以 A 为系数矩阵的线性方程组.

第六章

ζ, ξ：范畴.

$\mathrm{M}_\zeta(A,B)$：范畴 ζ 上从对象 A 到 B 的一切态射构成的集合.

$\mathrm{obj}\zeta$：ζ 上一切对象构成的类.

$R-\mathrm{Mod}$（$\mathrm{Mod}-R$）：左 $R-$模（右 $R-$模）范畴.

ζ^{op}：范畴 ζ 的对偶范畴.

$\varinjlim F$：F 的正向极限.

$\varprojlim F$：F 的逆向极限.

目　录

第一章　群…… (1)

§1　预备知识 …… (1)

§2　群的直积 …… (8)

§3　置换群…… (13)

§4　作用在集合上的群…… (18)

§5　西洛(*sylow*)定理 …… (21)

§6　有限交换群…… (26)

§7　可解群与幂零群…… (30)

§8　可除群…… (33)

第二章　伽罗瓦理论 …… (38)

§1　域扩张…… (38)

附录:尺规作图问题 …… (45)

§2　分裂域和有限域…… (50)

§3　可离扩张、正规扩张、伽罗瓦扩张…… (55)

§4　伽罗瓦理论基本定理…… (64)

附录:代数基本定理 …… (68)

§5　根式扩张与用根式解方程…… (70)

第三章　格 …… (78)

§1　偏序集…… (78)

§2　格的基本性质…… (81)

§3　分配格、模格、可补格…… (88)

§4 布尔代数 …… (97)
第四章 模 …… (106)
§1 基本概念 …… (106)
§2 直积与直和 …… (118)
§3 自由模 …… (125)
附录:向量空间维数 …… (129)
§4 投射模 …… (135)
§5 内射模 …… (142)
§6 Noether 模与 Artin 模 …… (147)
§7 模的张量积 …… (153)
§8 可除代数 …… (160)
第五章 交换环上线性代数 …… (167)
§1 行列式 …… (167)
§2 自同态行列式 …… (175)
§3 线性方程组 …… (181)
§4 齐次线性方程组 …… (187)
§5 主理想整环上的模 R^n …… (190)
§6 相似关系 …… (198)
第六章 范畴 …… (205)
§1 基本概念 …… (205)
§2 单态射与满态射 …… (211)
§3 直积与直和 …… (217)
§4 函子与自然变换 …… (225)
§5 正向极限与逆向极限 …… (231)
§6 范畴等价 …… (242)
参考文献 …… (246)

第一章　群

群论，不仅是一个具有丰富内容的代数系统，而且也是研究其他代数系统以及其他邻近学科所常常涉及到的一个基础理论. 它以丰富的内容，严谨而清晰的理论体系渗透到许多数学分支，并起着重要作用. 群论研究的内容广泛，有一般群论、交换群论、有限群论等. 此外还形成了一些边缘性学科，如拓扑群、*Lie* 群、代数群等.

本章主要介绍群论中的一些基本概念，包括置换群、p 群、群在集合上的作用、可解群、幂零群和可除群等，为进一步学习代数或其他相近学科打下一个基础.

§1　预备知识

本节将介绍群论的最基本概念及其简单的性质，这些内容在任何一本“近世代数”教材中都能找到. 因此，我们对所列出的定理不予详证甚至不作证明.

设 G 是一个非空集合，如果 G 中有一个二元代数运算“$\cdot$”，使之满足结合律，则称$(G,\cdot)$是一个半群，常常简称 G 是半群，而将元素运算 $x\cdot y$ 记为 xy. 如果半群$(G,\cdot)$中，任意两个元素 x，y，恒有 $xy=yx$ 成立，则称$(G,\cdot)$是交换半群或 *Abel* 半群.

定义 1　设 G 是一个半群，如果 G 还满足下列两个条件：

(1) G 中有左(右)单位元 1，即 $1\in G$ 并且 $1x=x$ $(x1=x)$，

$\forall\ x\in G$,

(2)对任意一个元素 $x\in G$,关于左(右)单位元 1 有左(右)逆元 y,即 $y\in G$ 并且 $yx=1(xy=1)$.

那么称 G 是一个群. 满足(1)、(2)条件的交换半群称为交换群或 *Abel* 群. 对交换群,我们常常将运算符号"·"改为"+",而将单位元 1 改写为零元"0".

需要指出的是:如果 G 是群,则 G 的左(右)单位元 1 实际上是双边的,因此是 G 的单位元,从而唯一;而每一个元素 x 的左(右)逆元也是双边的,因此是 x 的逆元,也是唯一的,记为 x^{-1}. 下面例子表明,存在半群 G,有左(右)单位元,并且每一个元素 x 有右(左)逆元,但 G 不是群.

例 2 设 $\boldsymbol{Q}$ 是有理数域,

$$G=\left\{\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}\middle|\ x\neq 0, y\in \boldsymbol{Q}\right\}$$

G 关于矩阵的乘法构成半群,但不是群.

定义 3 设 A 是群 G 的非空子集,如果 A 关于 G 的运算构成群,则称 A 是 G 的一个子群.

显然,任意群 G 有两个平凡子群,一个由单位元 1 构成的单位元子群$\{1\}$,另一个是 G 自身.

如果 A 是群 G 的一个非空子集,不难证明,A 是 G 的子群当且仅当对任意 $x,y\in A$ 有 $xy^{-1}\in A$ 成立.

设 S 是群 G 的一个非空子集,记

$$S^{-1}=\{x^{-1}\mid x\in S\}$$

和

$$\langle S\rangle=\{a_1a_2\cdots a_m\mid m\geqslant 0, a_i\in S\cup S^{-1}\}$$

(当 $m=0$ 时,理解为 $a_1a_2\cdots a_m=1$),那么$\langle S\rangle$ 是 G 的包含 S 的最小子群,称$\langle S\rangle$是由 S 生成的子群,而 S 称为生成元系.

如果群 G 是由它的一个 n 元子集 $\{x_1,\cdots,x_n\}$ 生成的群，称 G 是 n－生成群，这种由有限个元素生成的群称为有限生成群. 特别地，1－生成群 $\langle x\rangle\equiv\langle\{x\}\rangle$ 称为循环群.

根据上面说明，$\langle x\rangle=\{x^m\mid m\in\mathbf{Z}\}$. 整数加群 $\mathbf{Z}$ 是无限循环群，而模 n 的剩余类加群 $\mathbf{Z}_n$ 是有限循环群.

设 $x\in G$，如果存在最小自然数 n，使 $x^n=1$，1 是 G 的单位元，则称 x 的周期为 n，如果这样的 n 不存在，称 x 的周期为 0. 显然，有限循环群中元素的周期有限，而无限循环群中元素 $x(x\neq1)$ 的周期为 0.

如果 H 是群 G 的一个子群，G 上定义一个二元关系“$\sim_H$”如下：

$$x\sim_H y\Leftrightarrow\text{存在 } h\in H,\text{使 } x=yh,$$

那么，“$\sim_H$”是 G 上的一个等价关系，包含 x 的等价类记为 xH. 不难知道，

$$xH=\{xh\mid h\in H\}$$

称之为包含 x 的 H 左陪集. 关于左陪集有如下性质：

(1) $xH=yH\Leftrightarrow x^{-1}y\in H\Leftrightarrow xH\cap yH\neq\varnothing$；

(2) H 与 xH 等势：$h\mapsto xh$ 是 H 到 xH 上双射；

(3) $G=\bigcup xH$.

相类似地定义右陪集 Hx，而且 H 的所有左陪集的集合与所有右陪集的集合有相等的势，这个势称为 H 在 G 中的指数，记为 $[G:H]$. G 的势常称为 G 的阶数，记为 $|G|$.

设 $K\subseteq H\subseteq G$ 是子群，则 $[G:K]=[G:H][H:K]$，这是因为，若 $G=\bigcup xH$ 和 $H=\bigcup yK$，则 $G=\bigcup xyK$，详细的证明留给读者练习.

取 $K=\{1\}$，得到

定理 4(*Lagrange* 定理) 如果 G 是群，H 是 G 的子群，则

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

如果 X、Y 是群 G 的二个非空子集，定义 X 与 Y 的积

$$XY=\{xy|x\in X,y\in Y\}.$$

如果 $XY=YX$，称 X 与 Y 可交换.

定理 5 如果 H,K 是群 G 的子群，则 HK 是 G 的子群当且仅当 H 与 K 可交换，这时

$$HK=\langle H\cup K\rangle=KH.$$

证：若 HK 是子群，由 $H\subseteq HK,K\subseteq HK$ 得 $KH\subseteq HK$. 另一方面，$HK=(HK)^{-1}\subseteq KH$，故 $HK=KH$.

反之，如果 $h_i\in H,k_i\in K$，则存在 $h_3\in H,k_3\in K$ 使得

$$h_1k_1(h_2k_2)^{-1}=(h_1k_1)(k_2^{-1}h_2^{-1})=h_1((k_1k_2^{-1})h_2^{-1})=h_1h_3k_3,$$

故 $h_1k_1(h_2k_2)^{-1}=h_1h_3k_3\in HK$. □

群 G 中与所有单元子集可交换的子群 H 称为 G 的正规子群. 显然正规子群与所有子群可交换. 正规子群有如下性质：

定理 6 如果 H、K 是 G 的子群，那么

Ⅰ. 下列等价

(1) $xH=Hx,\forall\ x\in G$；

(2) $x^{-1}Hx=H,\forall\ x\in G$；

(3) $x^{-1}hx\in H,\forall\ x\in G,h\in H$.

Ⅱ. 若 H 是 G 的正规子群，则

(1) $H\cap K$ 是 K 的正规子群；

(2) H 是 $\langle H\cup K\rangle$ 的正规子群；

(3) $HK=\langle H\cup K\rangle=KH$；

(4) 若 K 也是 G 的正规子群，并且 $K\cap H=\{1\}$，则 $\forall\ a\in H,b\in K$ 有 $ab=ba$.

我们用 $H\lhd G$ 表示 H 是 G 的正规子群.

设 $H\lhd G$，记

$$G/H=\{xH\mid x\in G\}$$

并规定:$(xH)\cdot(yH)=xyH$.

直接验证表明,这个规定的运算是 G/H 的一个二元代数运算,并且 G/H 是一个群,称这个群为 G 关于 H 的商群,显然,$|G/H|=[G:H]$.

定义 7 设 G_1,G_2 是两个群,f 是 G_1 到 G_2 的映射,如果 f 保持群的运算,即

$$f(xy)=f(x)f(y),\quad \forall\ x,y\in G_1,$$

那么称 f 为 G_1 到 G_2 的一个同态. 特别,当 f 又是单射时,称 f 为单同态;当 f 又是满射时,称 f 为满同态;当 f 又是双射时,称 f 为同构映射,这时也记 $G_1\overset{f}{\cong}G_2$,或记 $f:G_1\cong G_2$.

用 $\mathrm{Hom}(G_1,G_2)$ 表示 G_1 到 G_2 的所有同态的集合,这个集合总是非空的. 因为它至少含有零同态 $0:G_1\to G_2:x\mapsto 1$. G 到 G 的同态(同构映射)称为自同态(自同构).

设 $f:G_1\to G_2$ 是同态,如果 K 是 G_1 的子群,记 $f(K)=\{f(k)\mid k\in K\}$,特别地,当 $K=G_1$ 时,记 $\mathrm{Im}f=f(G_1)=\{f(x)\mid x\in G_1\}$,这是 G_2 的子群,但未必是 G_2 的正规子群.

$\mathrm{Ker}f=\{x\in G_1\mid f(x)=1\}$(称为 f 的核)是 G_1 的正规子群.

定理 8(同态基本定理) 设 G 是一个群,则 G 的任一商群都是 G 的同态象;反之,若 G' 是 G 的同态象,比如 $\mathrm{Im}f=G'$,则 $G'\cong G/\mathrm{Ker}f$.

如果 $H\lhd G$,则 $\eta:G\to G/H:x\mapsto xH$ 是群同态,$Ker\eta=H$,这个同态称为 G 到商群 G/H 的自然同态.

作为同态基本定理的应用,我们再给出两个群的同构定理.

定理 9 设 $H\lhd G,N$ 是 G 的子群,则 $N\cap H\lhd N$ 并且 $x(N\cap H)\mapsto xH$ 是 $N/N\cap H$ 到 NH/H 上的同构映射.

定理 10 设 $H \lhd G, N \lhd G, N \subseteq H$，则 $H/N \lhd G/N$，并且

$$(G/N)/(H/N) \cong G/H.$$

证：设 $f: G/N \to G/H: xN \mapsto xH$，则 f 是满同态映射，并且 $\mathrm{Ker} f = H/N$. □

同态基本定理有很多应用，而且在环，模等其他代数系统中也有相应的同态基本定理，因此要特别注意这一定理的理解.

习　题

1. 设 G 是群，H 是 G 的子群，证明：H 的所有左陪集构成的集合与 H 的所有右陪集构成的集合有相同的势.

2. 设 G 是群，a, b 是 G 的两个周期分别为 m, n 的元素，这里 m, n 是自然数，如果 $ab = ba$，证明：元素 ab 的周期为 m, n 的最小公倍数 q 的一个因数，并且 G 中含有周期为 q 的元素，当 m, n 互质时，ab 的周期为 mn. 举一个 $ab \neq ba$ 的例子，使这个结果不成立.

3. 设 G 是 n－生成群，H 是有限群，证明：

$$|\mathrm{Hom}(G, H)| \leqslant |H|^n$$

4. 证明定理 6.

5. 证明：指数为 2 的子群总是正规子群.

6. 如果 H, K 是群 G 的子群，且 $H \subseteq K$，若 N 是 G 的正规子群，且 $HN = KN, H \cap N = K \cap N$，证明：$H = K$.

7. 设 $\boldsymbol{Q}$ 是有理数加法群，证明：

(1) $\boldsymbol{Q}$ 不是有限生成的；

(2) 描述 $\mathrm{End}(\boldsymbol{Q}) \equiv \mathrm{Hom}(\boldsymbol{Q}, \boldsymbol{Q})$；

(3) 取定素数 p，令 $\boldsymbol{Q}_p = \left\{ \dfrac{m}{p^n} \,\middle|\, m, n \in \boldsymbol{Z} \right\}$，将 $\boldsymbol{Q}_p$ 作为加法群，描述 $\mathrm{End}(\boldsymbol{Q}_p)$.

8. 证明：只有有限个子群的群是有限群.

9. 设 G 是半群，证明：下列条件等价：

(1) G 是群；

(2) G 满足下面两个条件：

(i)G 有唯一的左单位元 1，

(ii)$\forall\ a\in G$，存在 $a'\in G$，使得 $aa'=1$；

(3) G 满足下面两个条件：

(i)G 有唯一的右单位元 1，

(ii)$\forall\ a\in G$，存在 $a'\in G$，使得 $a'a=1$；

(4) $\forall\ a\in G$，存在唯一的 $a'\in G$，使得对$\forall\ b\in G$，有

$$a'(ab)=b=(ba)a';$$

(5) G 有单位元 1，并且$\forall\ a\in G$，存在 $b\in G$，使得

$$aba=a,\quad ab^2a=1.$$

10. 设 G 是一个非空集合，并且有一个二元代数运算“$\cdot$”. 证明：$(G,\cdot)$是交换群的充分必要条件是：

(1)$\forall\ a,b,c\in G$，有$(ab)c=a(cb)$，

(2)G 有左单位元 1，

(3)对于左单位元 1，$\forall\ a\in G$，存在 $a'\in G$，使 $aa'=1$.

11. 设 G 是一个非空集合，并有一个二元代数运算“$\cdot$”. 对$(G,\cdot)$，考察下列条件：

(i)$\forall\ a,b,c\in G$，有 $a(bc)=(ac)b$；

(ii)$\forall\ a,b,c\in G$，有 $a(bc)=(ca)b$；

(iii)$\forall\ a,b\in G$，方程 $ax=b$ 在 G 中有解；

(iv)$\forall\ a,b\in G$，方程 $xa=b$ 在 G 中有解.

则下列条件等价：

(1) $(G,\cdot)$是交换群；

(2) $(G,\cdot)$满足(i)，(iii)；