抽象代数学

Modern Algebra

● 姚慕生 编

复旦大学出版社

抽象代数学

姚慕生 编

复旦大学出版社

抽象代数学

姚慕生　编

责任编辑　范仁梅
责任校对　张利勇
装帧设计　赵丽丽
出版发行　复旦大学出版社
　　　　　上海市国权路579号　200433
　　　　　86-21-65102941(发行部)　86-21-65642892(编辑部)
　　　　　fupnet@fudan.edu.cn
经　　销　新华书店上海发行所
印　　刷　复旦大学印刷厂
开　　本　850×1168　1/32
印　　张　7.625
字　　数　198千
版　　次　1998年11月第一版　1998年11月第一次印刷
印　　数　1—1 000
　　　　　ISBN 7-309-02096-0/O·183
定　　价　10.00元

内容提要

本书系统地介绍了抽象代数最基本的内容，其中包括群论、环论与域论。在域论这一章中还比较全面地介绍了有限 Galois 理论。书中配备了一定数量、难易不一的习题，习题均有解答或提示。

本书可供综合性大学、师范大学数学系学生阅读，也可供理科各系以及通讯工程的大学生、研究生及教师参考。

前　言

抽象代数是数学的一门重要分支。众所周知，初等代数研究的是数集上的运算，高等代数把数集扩展为向量空间、矩阵集和多项式集。抽象代数则以一般集合上的运算作为研究对象。

历史上，抽象代数起源于纯粹理性的思考。19 世纪 30 年代法国天才的青年数学家 Galois 在研究困惑了人类几百年的用根式求解五次方程问题时，发现了群。Galois 不仅彻底地解决了一元 n 次方程用根式求解是否可能的问题，而且更重要的是他使人们认识到，除了熟知的数外，在其他集合(如置换集)上也可能存在着代数结构，即满足一定规则的运算。Galois 虽然只活了 21 岁，但是他的发现为数学开辟了一个崭新的研究领域。随着 19 世纪末 Cantor 集合论的建立，各种代数结构被定义在一般的集合上，抽象代数的奠基工作完成了。

20 世纪是抽象代数学蓬勃发展的世纪。Lie 群、Lie 代数的出现使几何学和代数学再次结成了亲密的伙伴，也给抽象代数带来了强大的发展动力。拓扑学因为有了抽象代数而得到了突飞猛进的发展，群、环、模成了研究拓扑空间性质的基本工具，代数拓扑成了 20 世纪最引人注目的数学分支之一，而从代数拓扑学产生的同调代数为代数学宝库增添了强有力的工具。数论、代数几何由于抽象代数概念的导入彻底地改变了面貌。代数学从与其他数学分支的结合中获得了前所未有的生命力，新概念不断出现，新的代数学分支不断生长。数学这棵古老的常青树从来没有像现在这样枝繁叶茂，生机勃勃。

通常人们认为抽象代数很抽象，似乎离现实很远，没有多少用处。其实这是一种误解。一切科学的抽象不是对现实的背离，而是对现实世界更深刻的反映。科学研究的对象扩大了，它的应用也就更广

泛了，代数学也是如此。抽象代数不仅是现代数学不可缺少的组成部分，也是现代物理学、化学、计算机科学、通讯科学不可缺少的工具。举例来说，有限域理论是抽象代数中相当“抽象”的理论，但是数字通讯中的编码理论(特别是纠错码)却是以它为基础的。因此当我们舒适地聆听CD唱片或是欣赏VCD(DVD)数码音像节目时，请记住其中也凝聚着数学家们的辛劳。今天，有志于在现代数学、现代物理学、计算机科学等领域作出贡献的年轻人，都应该懂得抽象代数的知识，在人类这一知识宝库中吸取营养，寻求自己的发展。

本书原是编者为复旦大学数学系学生编写的教材，它适用于已修完高等代数的本科生。本书内容按所讨论的代数结构分为4个部分。第一章为预备知识。第二章讨论群，在详细介绍了群、子群、正规子群、商群、同态和同构等基本概念的基础上，着重介绍了循环群、置换群，介绍了有限群的几个基本定理，如Sylow定理等。利用群的直积可以把复杂的群分解为比较简单的群，有限生成Abel群基本定理就是这一思想的体现，这个定理在代数拓扑学中有重要的应用，我们作了详细的介绍。群列和可解群是为第四章Galois理论作准备的。第三章介绍环论。环论，主要是交换环理论，它是代数几何的基础。我们除了介绍环、理想、商环、同态与同构外，还着重介绍了整环及其分式域、唯一分解环和多项式环。第四章讨论域和Galois理论。我们首先介绍了各种域扩张及其性质，然后介绍了Galois对应和Galois理论基本定理，这是Galois理论的核心。运用域的扩张理论和Galois基本定理，我们给出了一元n次方程可用根式求解的充分必要条件。我们还讨论了初等几何中尺规作图的可能性问题，如证明了用圆规和直尺不可能将一个任意角三等分，给出了正n边形可用圆规和直尺作图的充分必要条件。这些美妙的应用是Galois理论的辉煌篇章，读者从中可以充分领略到数学的美。本教程的内容通常分两学期授完，第一学期(每周3节课)讲完群论和环论两章，第二学期(作为选修)讲完第四章。目录中带*的内容可作为选修。

本书力求深入浅出，对抽象的概念尽量用较多的例子加以说明。

为了帮助读者理解抽象代数习题的解题思路，本书附有书内习题的简答或提示。虽然本书是在编者多年从事教学的基础上编成的，但不当之处仍然难免，敬请读者和同行专家批评指正。

编　者

1997 年 6 月于复旦大学

目　　录

第一章 预备知识

我们从中学就开始学习代数学这门课程，初等代数以数(整数、有理数、实数、复数等)及其运算作为基本的研究对象。数集上的运算有加、减、乘、除等。在高等代数的课程中，我们研究了向量、矩阵及其运算。现在我们要研究一般集合及其上的运算。对一般集合上运算的研究可以大大拓广数学研究的领域，为数学的应用开辟广阔的道路。

为了更好地理解抽象代数的内容，有必要先介绍一下集合论的一些基本概念。我们不打算“严格”地阐述这些数学中最基本的概念(读者可以在公理集合论的课程中学到它们的严格定义)，我们只打算“朴素”地叙述其含义。

§1.1 集　　合

读者已经在中学里学习过集合的概念。所谓一个集合，我们把它理解为某一些事物的总体。比如整数集就是指整数全体；有理数集是指有理数全体等等。集合常常用英文大写字母来表示，如 A, B, C 等。一个集合中的某个具体的事物，称为元素。元素常用小写英文字母表示，如 a, b, c 等。我们用$\in$表示属于，$a \in A$ 表示 a 是集合 A 中的元素。若 a 不是集合 A 中的元素，我们用 $a \overline{\in} A$ 来表示。不含有任何元素的集合称为空集，用$\varnothing$表示。一个集合如果只含有有限个元素，则称之为有限集，反之则称为无限集。集合 A 中一部分元素组成的集合称为 A 的子集。若 B 是 A 的子集，我们用符号 $B \subseteq A$ 来表示。两个集合如果含有相同的元素，则称为相等，换句话说，

若 $A \subseteq B$，又 $B \subseteq A$，则 $A = B$。若 A，B 不相等，则用 $A \neq B$ 表示。为了清楚地表示一个集合，我们还经常采用下列表示方法：

$$A = \{a \in S \mid P(a)\},$$

这里表示 A 中的元素来自 S 且具有性质 P。举例来说，集合 $A = \{a \in Z \mid a > 1\}$ 表示大于 1 的自然数，其中 Z 表示整数集。又若记 D 是平面上点的集合且 D 中元素用通常的实数偶(x,y)来表示(即 D 是 Descartes 平面上点的集合)，集合 $S = \{(x,y) \in D \mid x^2 + y^2 = 1\}$ 就表示该平面上的单位圆。

为了方便起见，我们在本书中采用下列固定的记号来表示一些常用的数集：

Z，表示整数集$\{0, \pm 1, \pm 2, \cdots\}$；

N，表示自然数集$\{1, 2, 3, \cdots\}$；

Q，表示有理数集；

R，表示实数集；

C，表示复数集。

定义 1-1 设 A，B 是两个集合，记 $A \cup B$ 为 A，B 中所有元素组成的集合，即

$$A \cup B = \{x \mid x \in A \text{ 或 } x \in B\},$$

称 $A \cup B$ 为集合 A 与 B 的并。

例 1 若 $A = \{a, b, c\}$，$B = \{b, c, d, e\}$，则 $A \cup B = \{a, b, c, d, e\}$。

定义 1-2 设 A，B 是两个集合，记 $A \cap B$ 为既属于集合 A 又属于集合 B 的元素组成的集合，即

$$A \cap B = \{x \mid x \in A \text{ 又 } x \in B\},$$

称 $A \cap B$ 为集合 A 与 B 的交。

例 2 记 A，B 为例 1 中的两个集合，则 $A \cap B = \{b, c\}$。

若两个集合 A，B 无公共元素，即 $A \cap B = \varnothing$，则称 A 与 B 不

相交。

定义 1-3 设 B 是 A 的子集，记 $A-B=\{a\in A \quad a\overline{\in} B\}$，即 $A-B$ 是由 A 中不属于 B 的元素构成的集合，称 $A-B$ 为 B 在 A 中的余集或补集。$A-B$ 有时也记为 $A\backslash B$。

并、交、补都是集合之间的最常用的运算，它们有下列性质。

命题 1-1 设 A, B, C 都是集合，则有下列性质：

(1) 若 $A\subseteq B$，则 $A\bigcup B=B$, $A\bigcap B=A$，特别，

$A\bigcup A=A$, $A\bigcap A=A$；

(2) $A\bigcup B=B\bigcup A$, $A\bigcap B=B\bigcap A$；

(3) $(A\bigcup B)\bigcup C=A\bigcup(B\bigcup C)$，

$(A\bigcap B)\bigcap C=A\bigcap(B\bigcap C)$；

(4) $A\bigcup(B\bigcap C)=(A\bigcup B)\bigcap(A\bigcup C)$，

$A\bigcap(B\bigcup C)=(A\bigcap B)\bigcup(A\bigcap C)$；

(5) 若 A、B 是 C 的子集，则

$C-(C-A)=A$，

$C-(A\bigcap B)=(C-A)\bigcup(C-B)$，

$C-(A\bigcup B)=(C-A)\bigcap(C-B)$。

证明 我们只证(5)中的第二个式子，其余的式子请读者自己证明。现设元素 $x\in C-(A\bigcap B)$，这时若 $x\overline{\in} C-A$，则 $x\in C-(C-A)=A$，但由假定 $x\overline{\in} A\bigcap B$，故 $x\overline{\in} B$，也就是说 $x\in C-B$，从而 $C-(A\bigcap B)\subseteq(C-A)\bigcup(C-B)$。

反之，若 $x\in(C-A)\bigcup(C-B)$，不妨设 $x\in C-A$，显然 $C-A\subseteq C-(A\bigcap B)$，故 $x\in C-(A\bigcap B)$，于是 $(C-A)\bigcup(C-B)\subseteq C-(A\bigcap B)$。这就证明了

$$C-(A\bigcap B)=(C-A)\bigcup(C-B)。$$

证毕。

注 性质(2)称为交换律，性质(3)称为结合律，性质(4)称为分配律，性质(5)中的式子通常称为 Morgan 公式。由于结合律成立，

$(A\cup B)\cup C$及$(A\cap B)\cap C$分别记为$A\cup B\cup C$及$A\cap B\cap C$，即括号可以被省略掉。

并与交的概念可以推广到任意个集合上。为此，我们先引进所谓的“指标集”的概念。设有集合I及一族集合$F=\{A_\alpha, A_\beta,\cdots\}$。对每个$\alpha\in I$，均可在$F$中找到唯一的一个集合$A_\alpha$与之对应，反之$F$中任一集合也可在$I$中找到唯一的一个元素与之对应。粗略地说，$F$中的集合可以用$I$来标记。这样的集合$I$被称为是集族$F$的指标集。举例来说，设数学系二年级有四个班，称为甲班、乙班、丙班、丁班，若设$F=\{$甲班、乙班、丙班、丁班$\}$，则集合$I=\{$甲、乙、丙、丁$\}$就是F的指标集。指标集I可以是无穷集。比如若$I=N$(自然数集)，$F=\{A_i\}_{i\in I}$，则表示$F=\{A_1, A_2, A_3,\cdots\}$。

现令$\bigcup\limits_{\alpha\in I}A_\alpha$表示所有$A_\alpha(\alpha\in I)$的元素组成的集合，即

$$\bigcup_{\alpha\in I}A_\alpha=\{x\mid x\text{ 属于某个 }A_\alpha\},$$

称$\bigcup\limits_{\alpha\in I}A_\alpha$为$\{A_\alpha,\alpha\in I\}$的并。类似地令$\bigcap\limits_{\alpha\in I}A_\alpha$表示所有$A_\alpha(\alpha\in I)$中公共元素组成的集合，即

$$\bigcap_{\alpha\in I}A_\alpha=\{x\mid x\text{ 属于每个 }A_\alpha\},$$

称$\bigcap\limits_{\alpha\in I}A_\alpha$为$\{A_\alpha,\alpha\in I\}$的交。

§1.2　Cartesian 积

定义 2-1　设A，B是集合，有序偶(a,b)(其中$a\in A$，$b\in B$)全体组成的集合称为A与B的Cartesian(简称为A与B的积)，记为$A\times B$，即：

$$A\times B=\{(a,b)\mid a\in A,\ b\in B\}。$$

注意$A\times B$中两个元素$(a,b)=(c,d)$的充要条件是$a=c$且$b=d$。

例 1 $A=\{a, b, c\}$, $S=\{u, v\}$, 则 $A\times S=\{(a, u), (a, v), (b, u), (b, v), (c, u), (c, v)\}$。

例 2 若 $A=B=R$,即实数集,则 $A\times B=R\times R=\{(x, y)\mid x, y\in R\}$, 就是 Descartes 平面。

积集合的概念也可以推广到 n 个甚至无穷多个集合。设 A_1, A_2, …, A_n 是 n 个集,令

$$A_1\times A_2\times\cdots\times A_n=\{(a_1,a_2,\cdots, a_n)\mid a_i\in A_i\},$$

即 n 元有序序列全体的集合(第 i 个元取自 A_i),就称为 A_1,…, A_n 的 Cartesian 积。

对一族集 $\{A_\alpha, \alpha\in I\}$, 也可以定义所有 A_α 的 Cartesian 积。令 A 是这样一个集,它是集合 I 上这样的函数 a 的全体: 对每个 $\alpha\in I$, $a(\alpha)\in A_\alpha$, 则 A 称为$\{A_\alpha\}$的 Cartesian 积,记为 $\underset{\alpha\in I}{X}A_\alpha$。这个定义适合于一般的指标集 I, 无论 I 为有限或无限。比如 A_1,…, A_n 的 Cartesian 积,这时 $I=\{1, 2, \cdots, n\}$, 对 $i\in I$, $a(i)=a_i\in A_i$。这样得到的 A 与上面定义的 $A_1\times\cdots\times A_n$ 完全一致。

利用积集合,我们不仅可以从已知集合构造出新的集合来,还可以定义在数学中起着极其重要作用的等价关系、映射等基本概念。

§1.3 等价关系与商集

定义 3-1 设 A, B 是集合,积集合 $A\times B$ 的一个子集 R 就称为 A 到 B 的一个关系,特别 $A\times A$ 的子集称为 A 上的一个关系。

若 $(a,b)\in R\subset A\times B$, 则称 a 与 b 为 R 相关,记为 aRb。

定义 3-2 设 R 是 A 上的一个关系,若 R 适合下列条件:

(1) 自反性,若 $a\in A$, 则 $(a,a)\in R$;

(2) 对称性,若 $(a, b)\in R$,则$(b, a)\in R$;

(3) 传递性,若 $(a, b)\in R$,$(b, c)\in R$, 则$(a, c)\in R$;

则关系 R 称为 A 上的等价关系。

等价关系常用～表示，即 $a \sim b$ 表示 $(a,b) \in R$。

例 1 设 S 是任意一个集合。$S \times S$ 中所有形为 (a,a) 的元素的全体构成的集合 R 是一个等价关系，称为 S 上的恒等关系，这时 $a \sim b$ 当且仅当 $a = b$。

例 2 设 Z 是全体整数集，定义 $a \sim b$ 当且仅当 $a-b$ 为偶数，即 $R = \{(a, b) \in Z \times Z \mid a - b$ 为偶数$\}$，不难验证这也是一个等价关系。

例 3 设 D 是 Descartes 平面，定义 D 中两点 $a \sim b$ 当且仅当 a 与 b 到原点的距离相等，则～也是一个等价关系。

例 4 设 S 是平面上的一个圆，定义 S 上两点 $a \sim b$ 当且仅当这两点同在一根直径上，则～也是一个等价关系。

例 5 设 Z 是整数集，n 是固定的自然数。定义整数 $a \sim b$ 当且仅当 $a-b$ 可以被 n 整除，则～也是 Z 上的一个等价关系，当 $n = 2$ 时就是例 2。

现设～是集合 A 中的一个等价关系，a 是 A 的一个元素，与 a 等价的元素全体组成 A 的一个子集，称为 a 的一个等价类，我们用 $[a]$ 表示 a 的等价类。例 1 中 a 的等价类只含有一个元素。例 2 中 a 的等价类为形如 $a + 2k(k \in Z)$ 的元素全体，这时 Z 只含有两个等价类：奇数与偶数。例 3 中 a 的等价类为以原点为圆心过 a 点的圆。例 4 中每个等价类都含有两个元素。例 5 中的 Z 一共有 n 个等价类：$[0],[1],\cdots,[n-1]$。

我们注意到，一个集合中由两个元素所在的等价类如不重合，则必不相交。即若 $[a] \neq [b]$，则 $[a] \cap [b] = \varnothing$。因为如存在 $c \in [a] \cap [b]$，则 $a \sim c, c \sim b$。但由传递性知 $a \sim b$，于是 $[a] = [b]$，引出矛盾。由此我们看出如果一个集合上定义了一个等价关系，则这个集合可以被划分成互不相交的等价类(子集)之并。一个集合如果能表示为两两互不相交的子集之并，则称这些子集族为该集合的一个分划。上面的分析表明集合上一个等价关系决定了该集合的一个分划。

反过来，如果 $\{A_i\}_{i \in I}$ 是集合 A 的一个分划，即

$$A_i \cap A_j = \varnothing (i \neq j), \quad A = \bigcup_{i \in I} A_i,$$

在 A 上定义关系 R 如下：

$$R = \{(a, b) \in A \times A \mid a, b \text{ 属于同一个 } A_i\},$$

则容易验证 R 是 A 上的一个等价关系。因此，给定 A 的一个分划，可以得到 A 上的一个等价关系。事实上我们有如下的命题。

命题 3-1 设 R 是集合 A 上的一个等价关系，则 R 决定了 A 的一个分划 P，且由 P 导出的等价关系就是 R。反之给定 A 的一个分划 P，则可得到 A 上的一个等价关系 R，且由这个等价关系 R 决定的 A 的分划就是 P。

证明 设 R 是 A 的等价关系，P 是由上述方法得到的分划，又记 R' 是由 P 决定的 A 的等价关系，若 $(a, b) \in R$，则 a, b 同属于 P 的某个元素(等价类)，于是 $(a, b) \in R'$，故 $R \subseteq R'$。反过来若 $(a, b) \in R'$，则 a, b 同属于 P 中某个等价类，从而 $(a, b) \in R$，即 $R' \subseteq R$，由此即得 $R' = R$。

另一方面设 $P = \{A_i\}_I$ 是 A 的一个分划，它决定的 A 的等价关系记为 R。再由 R 导出的分划记为 $P' = \{B_j\}_J$，设 $a \in A$，且 a 所在的等价类为 A_i，由于 $A = \bigcup_J B_j$，故 a 属于某个 B_j，现只需证明 $A_i = B_j$ 即可。对 A_i 中任一元 c，有 $c \sim a$。另一方面由于 B_j 是 a 的等价类，故 $c \in B_j$，于是 $A_i \subseteq B_j$。反之，若 $b \in B_j$，则 $b \sim a$。但凡与 a 等价的元素必须在 A_i 之中，故 $B_j \subseteq A_i$。由此即推出 $A_i = B_j$，$P' = P$。证毕。

定义 3-3 设～是集 A 上的一个等价关系，A 上的所有等价类的集合称为 A 关于等价关系～的商集，记之为 $A/\sim$ 或 $\overline{A}$。

注意 $\overline{A}$ 实际上是 A 的某些子集(全体等价类)的集合，$\overline{A}$ 中的元素是 A 中某个元素所在的等价类。若 $a \in A$，则 a 的等价类作为 $\overline{A}$ 的元素通常记为 $\overline{a}$。

例 1 中的商集 $\overline{S}$ 为 S 中单点子集(即只含有一个元素的子集)组

成的集。例 2 中的商集只含有 2 个元素，即奇数集与偶数集。例 3 中的商集为 Descartes 平面上以原点为中心的圆全体组成的集合。例 4 中的商集是所谓的射影直线。例 5 中的商集含有 n 个元素，分别记为 $\overline{0}$，$\overline{1}$，$\overline{2}$，…，$\overline{n-1}$，其中 $\overline{i}$ 表示由所有被 n 除后余数等于 i 的整数全体，这个商集记为 Z_n，称为模 n 剩余类集，我们以后还要来研究它。

§1.4 映　　射

定义 4-1 设 A，B 是两个非空集合，M 是 A 到 B 的一个关系（即 $M \subseteq A \times B$），若 M 适合下列条件：对 A 中任一元素 a，有且只有一个 B 中的元素 b，使 $(a, b) \in M$，则称 M 是集合 A 到 B 的一个映射或映照。A 称为这个映射的定义域，B 称为映射的值域。

从映射的定义我们可以看出，对 A 中任一元 a，有且仅有一个元 b 与 a 对应。这个对应关系有时记为 $a \to b$，映射习惯上用小写英文字母 f，g 等来表示。如上述映射记为 f，则 $b = f(a)$。A 到 B 的映射 f 简记为

$$f: A \to B。$$

读者不难看出，映射是函数概念在集合上的推广。与函数一样，A 到 B 的两个映射 f 与 g 相等当且仅当 $f(a) = g(a)$ 对一切 $a \in A$ 成立。

例 1 $S \to S$ 的映射 $a \to a$ 称为恒等映射，记为 Id_S 或 I_S。

例 2 A，B 是两个非空集，$b_0 \in B$，若令 $f: A \to B$ 为 $f(a) = b_0$ 对一切 $a \in A$，则 f 是一个映射，称为常值映射。

例 3 设 R 是实数集，$f(x) = x^2$ 定义了 $R \to R$ 的一个映射。

例 4 设 Z 是整数集，定义 $Z \times Z \to Z$ 的映射为 $(m,n) \to m + n$。这也是一个映射，实际上它是一个运算。

例 5 设 A，B 是非空集，作 $A \times B \to A$ 的映射 $(a, b) \to a$。这个映射称为 $A \times B$ 到 A 上的投影。同样也可以定义 $A \times B$ 到 B 上