近 世 代 数

第 二 版

熊 全 淹 编著

上海科学技术出版社

内 容 提 要

本书第一版于 1963 年印行，现在是第二版．

全书共七章．前三章介绍群、环、体等基本概念及性质．第四章讨论可换体，以有穷次代数扩张讠[illegible]深入一步讨论群，第六章伽罗瓦理论，讨论有穷次[illegible]罗瓦理论的基本定理及其应用．第七章是新增加的，讨论环的构造．书中每节之后均附有相当数量的习题，并列出了近代一些主要的文献，可供高等学校作为代数专门组的教材或教学参考书．

近 世 代 数

第 二 版

熊全淹 编著

上海科学技术出版社出版

（上海瑞金二路 450 号）

新华书店上海发行所发行 上海市印刷六厂印刷

开本 850×1156 1/32 印张 11 字数 260,000

963 年 10 月第 1 版 1978 年 8 月第 2 版 1978 年 8 月第 3 次印刷

书号：13119·534 定价：1.25 元

序　言

本书是系统而比较全面地介绍群、环、体以及伽罗瓦理论等的基础理论，作为高等院校数学系学生的基本读物．学生有此基础后，在深入数学其他分支时，对所需要的近世代数理论基本上不致发生问题，此外读代数方面近代书籍或文献，亦不致有大困难．再适当地介绍近代有关方面的发展及我国在这方面的成就，列举参考文献，以便读者参考．

在编写时，力求做到叙述简洁易懂，推理尽可能详尽，对所引用的理论，特殊的都有交代，毋须另参考他书，以减少读者困难．因为是介绍基础理论，所以专门而联系不大的概念都予削减，因此定理证明宁可长一点，用所谓初等证法，而不因一、二证明，另加新概念．譬如§6.3定理3的证明就是如此．编者认为这样做，读者既易理解，又可对已有的基础理论加深认识，一举而二得．但同时也适当地给出一些联系很紧的新概念，以说明现状，主要目的仍是对已有基础理论加深认识．

再对于重要概念或定理的引进，力求做到前后联系，要求明确，有本有源，使读者容易接受而不觉突然．譬如§3.6中介绍理想子环时，事先就说明了我们的企图．为了使问题提得自然，有时不按惯例，譬如西洛定理在§2.3即提出，但证明在§5.5中．又§3.10中代数基本定理的证明引用了后面的定理，即所谓暂时承认的性质．§4.9中魏特邦定理先运用而后证明，这些都不是一般书中的惯例，但编者认为这样做有它的现实意义．为求目标明确，又不使篇幅过长，很多重要结果列为习题，让读者自己思考，书末

附有答案，以备读者查对.

本书系根据自1953年起在武汉大学所用的近世代数讲义改编而成，次序安排大体上是按照范特瓦登(B. L. van der Waerden 1905～)的代数学(1943年武汉大学故教授肖君绎曾将该书(第二版)译出. 译文是文言，读者多感不便. 1962年丁石孙等根据第四版另译)，第一、二两章曾参考曾宪昌同志原稿，第三章曾参考路见可同志原稿，启发很多，并且某些方面采用了他们的写法. 此外，曹和贵同志也提过一些意见，谨此一一致谢. 由于水平所限，书中错误、不妥处自属难免，敬求读者惠予指正.

编者 1963年3月

再 版 序 言

文化大革命后开始对本书进行全面修改. 这次修改变动很大，也可以说是重写，另外还添加了一章环论. 为了便于初学，叙述宁可长一点，不用表现理论. 原来六章，就内容言，基本上没有改动，只是以前写得过简的，加详细了，罗嗦了的删去了，有些地方为了便于说明，改变了前后的顺序. 此外，在个别地方，加了一些例子，还添了一些参考文献. 所有这些改变，大都是根据读者反映，在这里谨向他们表示衷心感谢.

编者 1977年8月

目　录

第一章

基本概念

这章简单地介绍集合、映射、分类等几个基本概念，并且解释记号 $\in$，$\subset$，$\supset$，$\cap$，$\cup$，$\{\cdots\}$等的意义，作为以后各章的基础.

§1.1 集合

数学中讨论的对象，如代数中的数，几何中的点，直线等，我们现在统统叫做**元素**，有时就简单地叫做**元**．若干个或无穷多个元的集体，叫做**集合**，或简单地叫做**集**.

我们要知道一个集，必定要知道它里面所有的元，也就是说，我们对于任意一个元，要能够判别它是否在这个集中．譬如，所有整数组成一个集，因为我们随便拿一个数来，都可以判别它是否是整数；这个集又叫做**整数集**，我们用 Z 来表示.

一个集一定有它的特性，譬如整数集中任意元，都有整数这个特性，平面上所有点组成的集与平面上所有圆组成的集都各有各的特性，因此对于一个集，我们可以用它的特性来判别任意元是否在它里面.

任意一个元 a，如果它有集合 M 的特性，也就是说，它是 M 的元时，我们就用记号

$$a\in M$$

来表示．如果它没有集合 M 的特性，也就是说，它不是 M 的元

时，我们就用

$$a \in M$$

来表示．有时，a 在 M 中我们也说 a 属于 M，或者说 M 包含 a．同样，a 不在 M 中我们也说 a 不属于 M，或者说 M 不包含 a．

一个集所包含的元假如是有穷个，就叫做**有穷集**，否则就叫做**无穷集**．一个集所包含的元的个数，叫做这集的**元数**或**浓度**．有穷集的元数当然是正整数．

集合可以用列举它的所有元来表示，譬如整数集 Z 可以写成

$$Z=\{0,\ 1,\ -1,\ 2,\ -2,\ \cdots\},$$

或

$$Z=\{\cdots,\ -2,\ -1,\ 0,\ 1,\ 2,\ \cdots\}.$$

一般，假如 M 含有元 $a,\ b,\ c,\ \cdots$，我们就用记号 $M=\{a,\ b,\ c,\ \cdots\}$ 来表示．

通常一个集都含有一个以上的元，但是当它只含一个元时，这个集就与它所含的那唯一一个元常常不加区别．为了叙述方便，我们更假定不包含任何元的也成为一个集，叫做空集，它的元数是零．譬如大于 1 而小于 2 的整数集合就是空集．

假如集合 N 中所有元都是集合 M 中元，也就是说 N 是 M 的一部分，或者说任意一个元，如果它有 N 的特性，它一定也有 M 的特性，那末 N 就叫做 M 的**子集**，M 又叫做 N 的**包含集**．我们用记号 $N \subseteq M$ 或 $M \supseteq N$ 来表示．子集与包含集的关系可以用图形(图 1.1)来说明．

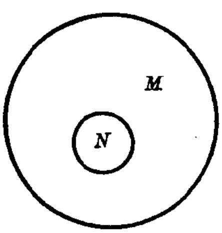

图　1.1

有穷集的子集是有穷集，无穷集的包含集又是无穷集．

为了方便，我们假定任意集都包含空集．再从 $A \subseteq B$ 及 $B \subseteq C$，我们就得到 $A \subseteq C$．

假如 M 的所有元都属于 N，同时 N 的所有元又都属于 M，即

$$M \subseteq N, \quad N \subseteq M,$$

也就是说，M 与 N 的特性完全相同时，我们就说 M 与 N **相等**，用记号

$$M = N$$

表示．假如 $N \subseteq M$，但 M，N 不相等，那末 N 就叫做 M 的**真子集**，M 叫做 N 的**真包含集**，用记号

$$N \subset M \text{ 或 } M \supset N$$

表示，这时 N 的所有元都属于 M，但 M 中至少有一个元不属于 N.

上面我们介绍了集合的基本概念，现在介绍它的二个结合法．

定义 1　假如 A，B 是两个集，那末属于 A 同时又属于 B 的所有元组成的集 P，叫做 A 与 B 的**交集**，用记号

$$P = A \cap B$$

表示．

于是 P 是 A，B 的子集，并且任何集只要它同时是 A，B 的子集，它一定是 P 的子集，因此 P 是包含在 A，B 中的**最大集**．关于交集的概念，我们可以用图形(图 1.2)来说明．

定义 2　假如 A，B 是两个集，那末属于 A 或者属于 B 的所

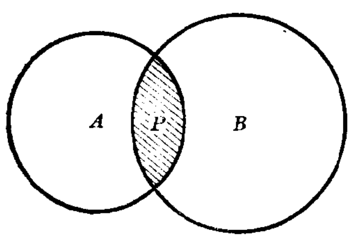

图　1.2

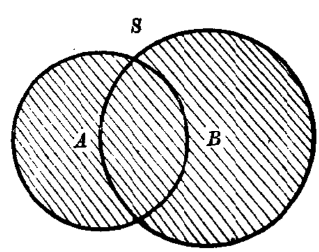

图　1.3

有元组成的集 S, 叫做 A 与 B 的**并集**,用记号

$$S=A\cup B$$

表示.

于是 S 是 A, B 的包含集,并且任何集只要它同时是 A, B 的包含集,它一定也是 S 的包含集,因此 S 是包含 A, B 的**最小集**.关于并集的概念,我们可以用图形(图 1.3)来说明.

假如 A, B, C 是三个集,显然

$$(A\cap B)\cap C=A\cap(B\cap C),\quad (A\cup B)\cup C=A\cup(B\cup C).$$

它们的交集与并集之间有下关系:

定理 $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.

证明 首先因为 $B\subseteqq B\cup C$, 所以 $A\cap B\subseteqq A\cap(B\cup C)$. 同样我们有 $A\cap C\subseteqq A\cap(B\cup C)$,因此

$$(A\cap B)\cup(A\cap C)\subseteqq A\cap(B\cup C).$$

再假如 $a\in A\cap(B\cup C)$,那末 $a\in A$, $a\in B\cup C$, 于是 $a\in B$ 或 $a\in C$. 从前者言,$a\in A\cap B$; 从后者言,$a\in A\cap C$. 因此 $a\in(A\cap B)\cup(A\cap C)$,这就是说

$$A\cap(B\cup C)\subseteqq(A\cap B)\cup(A\cap C).$$

所以定理成立.

同样我们有

$$A\cup(B\cap C)=(A\cup B)\cap(A\cup C).$$

为了区别,由元组成的集,叫做**第一层集**,把第一层集当作元组成的集,叫做**第二层集**. 第二层集又常叫做**系**.

若干个集的交集与并集可以按两个集的情形同样定义. 假定 L 是由集 A, B, C, …组成的系,我们用

$$A\cap B\cap C\cap\cdots$$

来表示 L 的交集,用

$$A\cup B\cup C\cup\cdots$$

来表示 L 的并集．要注意的是 L 虽然是第二层集，但交集、并集却都是第一层集．

定义 3 假如 M, N 是两个集，那末属于 M 同时又不属于 N 的所有元形成的集 D，叫做 M 与 N 的差集，用记号

$$D=M-N$$

表示．

关于差集的概念，我们可以用图形（图 1.4）来说明．

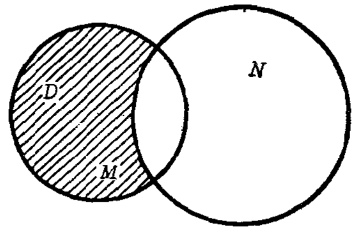

图 1.4

由定义，我们容易得知 $N\cap(M-N)$ 是空集，又

$$M=(M\cap N)\cup(M-N).$$

习 题 1.1

1．任意两个集是否都有交集与并集？

2．假定 $A\subseteq B$，那末 $A\cup B=$? $A\cap B=$?

3．假定 A, B, C 是三个集，试证

(i) $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$,

(ii) $(A-B)\cup(B-A)=(A\cup B)-(A\cap B)$.

4．假定 M 是元数为 n 的有穷集，L 是 M 的所有子集组成的系，试证 L 的元数是 2^n.

§1.2 映射，分类

我们知道，近世代数中集合的元是抽象的，因此，两个集合如何进行比较是一个重要问题．映射这个概念主要用途之一就是用来解决这个问题，它是近世代数中最基本的工具．

下面是一些最基本的概念．

对于集 M 中每一个元 a，如果根据某种规则，我们可以使它

与集 N 中唯一个元对应，那末这对应叫做 M 射到 N **的映射**，那个与 a 对应的元，叫做 a 的**象**，a 又叫做它的象的**象源**．这时 M 中任意元在 N 中都有象，但 N 中任意元在 M 中不一定都有象源．如果 N 中元在 M 中不都有象源，那末这映射叫做 M 射到 N **内的映射**．如果 N 中任意元在 M 中都有象源，那末这映射叫做 M 射到 N **上的映射**．

假如 M 射到 N 的映射用 σ 来表示，那末 a 的象，我们就用 $\sigma(a)$ 来表示，有时这映射又表为 $a\to\sigma(a)$．映射这个概念与数学分析中函数的概念一致，因此 $\sigma(a)$ 又常叫做 a 的**函数**．

显然，M 射到 N 内的映射就是 M 射到 N 中某一子集上的映射．譬如在整数集 Z 中，根据自乘这个规则，把任意整数 a 与它的自乘 a^2 对应，即 $a\to a^2$，那末这对应是整数集射到自己内的映射，也是整数集射到由所有整数平方组成集上的映射．

我们知道，对于映射 σ，象源 a 固然只有唯一的象 $\sigma(a)$，但是象 $\sigma(a)$ 就不一定只有一个象源 a，它可能有一个以上的象源．任意象只有一个象源的映射，有时又叫做**一对一的映射**；不是一对一的映射，有时又叫做**多对一的映射**．假如 σ 是 M 射到 N 上的映射，B 是 N 的子集，A 是 M 中所有这样元组成的集，它们的象都在 B 中，那末 A 叫做 B 对于映射 σ 的**完全象源**．

M 射到 N 上的映射 σ，当 $a_1\neq a_2$ 时，$\sigma(a_1)\neq\sigma(a_2)$，也就是说当 $\sigma(a_1)=\sigma(a_2)$ 时，$a_1=a_2$，那末 σ 就是一对一的映射．

集合 M 射到 N 上的一对一的映射 σ 有时叫做**可逆映射**，用记号

$$a\leftrightarrow\sigma(a)$$

表示．这时 N 中元 b 的象源用 $\sigma^{-1}(b)$ 来表示．显然 $b\to\sigma^{-1}(b)$ 是 N 射到 M 上的映射，我们叫它做 σ 的**逆映射**，用记号 σ^{-1} 表示．**因此，任意可逆映射都有唯一个逆映射，这逆映射也是可逆映射．**

假如 σ 是可逆映射，那末它的逆映射 σ^{-1} 的逆映射就是 σ，这就是说 $(\sigma^{-1})^{-1}=\sigma$.

譬如在整数集中，我们把偶数与 0 对应，奇数与 1 对应，这样就得到整数集射到集合 $\{0, 1\}$ 上的映射，这映射是多对一的，0 的完全象源是所有偶数，1 的完全象源是所有奇数，它们都没有唯一的象源. 假如我们把整数 n 与 $2n$ 对应，即 $n\to 2n$，那就得到整数集射到偶数集上的映射，这映射是一对一的，因此它是可逆映射，它的逆映射就是 $2n\to n$.

假如有一个一对一的映射把两个集 M、N 中的一个，譬如说 M，射到另一个 N 上，那末这两个集就叫做**有相等的浓度**，或**元数**. 与正整数集或它的子集有相等浓度的集，叫做**可数集**. 一个集如果不是可数集，就叫做**不可数集**. 因此有穷集是可数集. 任一可数集中元可以用正整数做标号来排列，于是任意可数集 M 可以写成

$$M=\{a_1,\ a_2,\ \cdots,\ a_n,\ \cdots\}.$$

显然整数集与偶数集有相等的浓度，因此一个集的浓度也可以与它的真子集的浓度相等，这是无穷集的一个重要性质. 任意有穷集是没有这个性质的.

假定 $M=N$，那末 M 射到 N 的映射，就叫做 M 射到**自己的映射**，M 射到 N 上(内)的映射，就叫做 M 射到**自己上(内)的映射**. M 射到自己上的一对一的映射，有时又叫做 M 的**变换**. 对于 M 中任意元使自身与它对应，也就是说不使 M 中任意元变动，是 M 射到自己上的一个映射，叫做 M 的**恒等映射**，用 I 表示，即 $I(a)=a$. 很多重要的映射都是射到自己上的映射，譬如平面上的旋转就可以看成为平面上的点集射到自己上的映射. 要注意的是 M 射到自己内的映射有时是一对一的，而 M 射到自己上的映射却有时是多对一的. 譬如 $n\to 2n$ 就是整数集射到自己内的一对一

的映射，$2n \to n, 2n+1 \to 2n+1$ 是整数集射到自己上的多对一的映射.

假如 σ_1, σ_2 都是 M 射到 N 上的映射，如果对于 M 中任意元 a，而 $\sigma_1(a)=\sigma_2(a)$，我们就说这两个映射**相等**，用记号 $\sigma_1=\sigma_2$ 表示. 假如 σ 是 A 射到 B 上的映射，τ 是 B 射到 C 上的映射，$\sigma(a)=b$, $\tau(b)=c$，即

$$a \to b, \quad b \to c,$$

我们容易证明，对应 $a \to c$ 就是 A 射到 C 上的映射，叫做映射 τ, σ 的**积**，用记号 $\tau\sigma$ 表示，即

$$\tau\sigma(a)=\tau(\sigma(a)).$$

这就是说，$\tau\sigma$ 是先施行 σ，后施行 τ 得到的映射.

要注意的是，虽然一个集的任意两个变换的积是存在的，但一般对于不同集的两个映射不一定有积. 再映射 τ, σ 的积 $\tau\sigma$ 与 σ, τ 的积 $\sigma\tau$ 一般不是一致的. 譬如 σ 是 M 射到 N 的映射，τ 是 N 射到 M 的映射，这时，$\tau\sigma$, $\sigma\tau$ 都有意义，但前者是 M 射到自己的映射，而后者则是 N 射到自己的映射，两者显然不一致. 即令 $M=N$，一般 $\tau\sigma$ 与 $\sigma\tau$ 也不一定相等，象这样的例子，我们在几何上是很熟悉的.

假如 σ 是可逆映射，那末 $\sigma^{-1}\sigma(a)=a$，因此 $\sigma^{-1}\sigma=I$，这就是说 $\sigma^{-1}\sigma$ 是恒等映射. 同样，$\sigma\sigma^{-1}$ 也是恒等映射. 再假如 σ, τ 都是可逆映射，那末 $\tau\sigma$, $\sigma\tau$ 又都是可逆映射. 显然 $\sigma^{-1}\tau^{-1}$, $\tau^{-1}\sigma^{-1}$ 就分别是它们的逆映射.

假定对于集 M 中任意两元 a, b，根据某个规则，我们可以把 a, b 与某集中唯一个元 c 对应，那末这对应，我们叫做 M 的**结合法**，有时又叫做 M 的**代数运算**. 这时我们又常常说根据这结合法，可以把 a, b 结合得到元 c，因此我们又说 M 有一个结合法. 譬如对于整数集 Z 中任意两数 a, b，我们命 $a+b$ 与它们对应，那末

这对应就是 Z 的结合法，它就是普通的加法．同样，对于 a, b，我们命 $a\cdot b$ 与它们对应，这对应也是 Z 的结合法，它就是普通的乘法．

一个集，假如它具有适合某些法则的结合法，或代数运算，就叫做**代数系**．象上面所示，整数集 Z 是代数系，因为它的加法，乘法两个结合法适合交换律 $a+b=b+a$, $ab=ba$，结合律 $a+(b+c)=(a+b)+c$, $a(bc)=(ab)c$，分配律 $a(b+c)=ab+ac$ 等法则．近世代数的目的就是讨论某些基本代数系关于结合法的性质，也就是代数性质．因此可以说，近世代数是研究某些基本代数系的理论学科．

上面我们介绍了映射，现在再来介绍分类这个概念．

我们知道，通常我们把两个元看成为一个元，或者说两个元相等，所用的等号“=”这个记号适合下面三个律：

1° 自反律：$a=a$,

2° 对称律：假如 $a=b$，那就 $b=a$,

3° 传递律：假如 $a=b$, $b=c$，那就 $a=c$.

并且引用等号时也只是引用了这三个律，但是适合这三个律的关系还有很多．一般来说，我们有：

定义 假如对于一个集的元，规定了一个关系～，并且可以判别其中每对元 a, b 是否有这关系 $a\sim b$；再这关系还适合自反，对称，传递三个律，即

1° $a\sim a$,

2° 假如 $a\sim b$，那就 $b\sim a$,

3° 假如 $a\sim b$, $b\sim c$，那就 $a\sim c$.

那末这关系，叫做这集的**等价关系**．

譬如初等几何中的三角形全等、相似都是三角形间的等价关系，但是整数集中不相等，或者大于、小于等关系都不是等价关

系．又如在有穷集 $M=\{1, 2, 4, 6, 10\}$ 中，假定两个数的和能够被 4 整除这个关系是～，即当 $4|a+b$ 时 $a\sim b$，显然对称律成立．再我们不难证明传递律也成立，但自反律不成立，因此这关系不是 M 的等价关系[1]．

在一个集中，根据某种关系或者用某个观点把某些元看成相等或同类，把某些元看成不相等或不同类，叫做**分类**．下面是分类与等价关系之间的一个重要性质．

定理 假如集 M 有一个等价关系，所有与一个元等价的元形成的集，叫做一类，那末 M 就能够分成为若干个这样没有公共元的类而无剩余．反过来，假如 M 能够分成若干个没有公共元的集而无剩余，这种集我们叫它做类，那末元素在同一类这个关系就是等价关系．

证明 定理的后半段我们容易知其成立，因此我们只要证明前半段就行了．

假定集 K_a 是 M 中所有与元 a 等价的元形成的类，那末类 K_a 中包含的元是相互等价的，这是因为从 $a\sim b$, $a\sim c$，根据对称律，传递律就得到 $b\sim c$．显然 M 中任意元必定属于这样的某一类，因此 M 可以分成这样的类而无剩余．

假如我们能够证明任意这样的两类不是相等就是没有一个公共元，那末 M 中任意一元只能在唯一类，因此定理的前半段就告成立．

假定两类 K_a, K_b 有一个公共元 c，那末 $a\sim c$, $b\sim c$，因此 $b\sim a$．如果元 $x\in K_a$，因为 $a\sim x$，所以 $b\sim x$，于是 $x\in K_b$．因此 $K_a\subseteq K_b$．同样我们可以证明 $K_b\subseteq K_a$，所以 $K_a=K_b$．这就是说，任意两类如果不相等，那末它们就没有一个公共元，于是定理的前半段成立，因此定理得证．

于是我们得知一个集，如果有一个等价关系，它就有一种分