近世代数学

熊全淹 編著

上海科学技术出版社

近世代数学

熊全淹 編著

上海科学技术出版社

內 容 提 要

本书是在武汉大学数学系代数专門組历年来所用近世代数学課程讲义的基础上經过修正充实而成。全书共分六章，前三章介紹有关群，环，体的基本概念及性质，第四章专門討論可换体理論，以有穷次代数扩張体为重点．第五章群論，在第二章的基础上作了深入一步的闡述．第六章伽罗华理論，討論有穷次可离正規扩張体上伽罗华理論的基本定理及其应用．书中每节之后均附有相当数量的习題，并列出了近代一些主要的文献，可供高等学校代数专門組作为教材或教学参考书．

近 世 代 数 学

熊 全 淹 編 著

上海科学技术出版社出版（上海瑞金二路 450 号）
上海市书刊出版业营业許可証出 093 号

商务印书館上海厂印刷　新华书店上海发行所发行

开本 850×1168 1/32　印張 8 24/32　排版字数 209,000
1963 年 10 月第 1 版　1963 年 10 月第 1 次印刷　印数 1—4,500

統一书号 13119·534　定价（十二）1.20 元

序　言

本书是系統而比較全面地介紹群，环，体以及伽罗华理論等的基础理論，作为高等院校数学系同学的基本讀物．同学有此基础后，在深入数学其他分支时，对所需要的近世代数理論基本上不致发生問題，此外讀代数方面近代书籍或文献，亦不致有大困难．再适当地介紹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，以便利讀者进一步研究．

在編写时，力求做到叙述簡洁易懂，推理尽可能詳尽，对所引用的理論特殊的都有交代，毋須另参考他书，以减少讀者困难．因为是介紹基础理論，所以专門而联系不大的概念都予削减，因此定理証明宁可长一点，用所謂初等証法，而不因一二証明，另加新概念．譬如§6.3定理3的証明就是如此．編者认为这样做讀者既易理解，又可对已有的基础理論加深认識，一举而二得．但同时也适当地給出一些联系很紧的新概念，以說明現状，主要目的仍是对已有基础理論加深认識．

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，使讀者容易接受而不觉突然．譬如§3.6中介紹理想子环时，事先就說明了我們的企图．为了使問題提得自然，有时不按慣例，譬如西洛定理在§2.3即提出，但証明在§5.5中．又§3.10中代数基本定理的証明引用了后面的定理，即所謂暫时承认的性质．§4.10中的魏特邦定理先运用而后証明，这些都不是一般书中的慣例，但編者认为这样做有它的現实意义．为求目标明确，又不使篇幅过长，很多重要結果列为习題，让讀者自己思考，

书末附有答案，以备讀者查考。

本书系根据自1953年起在武汉大学所用的近世代数学讲义改編而成，次序安排大体上是按照范特瓦登(B. L. van der Waerden)的代数学。第一、二两章曾参考曾宪昌同志原稿，第三章曾参考路見可同志原稿，启发很多，并且某些方面采用了他們的写法，此外，曹和貴同志也提过一些意見，謹此一一致謝。由于水平所限，书中錯誤或不妥之处自属难免，敬求讀者惠予指正。

熊全淹 1963年3月

目　录

第一章

基本概念

这章簡单地介紹集合，映射，分类等几个基本概念，并且解釋記号 $\in$，$\subset$，$\supset$，$\cap$，$\cup$，$\{\cdots\}$等的意义，作为以后各章的基础。

§1.1 集合

数学中討論的对象，如代数中的数，几何中的点，直綫等，我們現在統統叫做**元素**，有时候簡单地就叫做**元**。若干个元的集体，叫做**集合**，或簡单地叫做**集**。

我們要知道一个集，必定要知道它里面所有的元，也就是說我們对于任意一个元要能够判别它是否在这个集中。譬如，所有整数組成一个集，因为我們随便拿一个数来，都可以判别它是否是整数；这个集又叫做**整数集**，我們用 $\mathfrak{C}$ 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，平面上所有点組成的集与平面上所有的圓組成的集都各有各的特性，因此对于一个集，我們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，也就是說它是 M 的元时，我們就用記号

$$a \in M$$

来表示。如果它沒有集合 M 的特性，也就是說它不是 M 的元时，我們就用

$$a \in M$$

来表示。有时，a 在 M 中我們也說 a 属于 M，或者說 M 包含 a；同样，a 不在 M 中我們也說 a 不属于 M，或者說 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**，有穷集的元数当然是自然数。

集合可以用列举它的所有元来表示，譬如整数集 $\mathfrak{C}$ 可以写成 $\mathfrak{C}=\{0, 1, -1, 2, -2, \cdots\}$，或 $\mathfrak{C}=\{\cdots, -2, -1, 0, 1, 2, \cdots\}$。一般，假如 M 含有元 $a, b, c, \cdots$，我們就用記号 $M=\{a, b, c, \cdots\}$ 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个元常常不加区别。为了叙述方便，我們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 中所有的元都是集合 M 的元，也就是說 N 是 M 的一部分，那末 N 就叫做 M 的**子集**，M 又叫做 N 的**包含集**，我們用記号 $N\subseteq M$ 或 $M\supseteq N$ 来表示。子集与包含集的关系可以用图形来說明(图 1.1)。从图上我們很容易看出 N 中所有的元都在 M 中，也就是說任意一个元，如果它有 N 的特性，它一定也有 M 的特性。

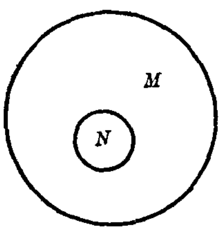

图 1.1

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，我們假定任意集都包含空集，再从 $A\subseteq B$ 及 $B\subseteq C$，我們就得到 $A\subseteq C$。

假如 M 的所有元都属于 N，同时 N 的所有元又都属于 M，即

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

也就是說 M 与 N 的特性完全相同时，我們就說 M 与 N **相等**，用

記号

$$M=N$$

来表示．假如 $N\subseteqq M$，但 N，M 不相等，那末 N 就叫做 M 的**眞子集**，M叫做 N 的**眞包含集**，用記号

$$N\subset M \text{ 或 } M\supset N$$

来表示，这时 N 的所有元都属于 M，但 M 中至少有一个元不属于 N．

上面我們介紹了集合的基本概念，現在介紹它的二个基本結合法．

定义 1　假如 A，B 是两个集，那末属于 A 同时又属于 B 的所有元組成的集 P，就叫做 A 与 B的**交集**，用記号

$$P=A\cap B$$

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，我們可以用图形来說明(見图 1.2)．

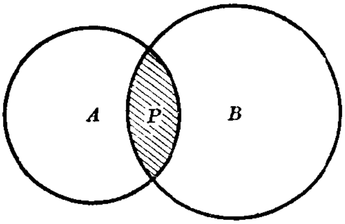

图　1.2

定义 2　假如 A，B 是两个集，那末属于 A 或者属于 B 的所有元組成的集 S，就叫做 A 与 B 的**并集**，用記号

$$S=A\cup B$$

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，我們可以用图形来說明(見图 1.3)．

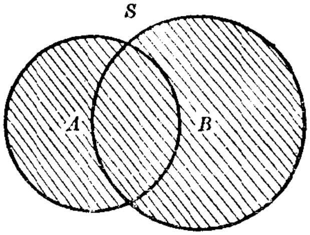

图　1.3

为了区别起見，由元組成的集叫做**第一层集**，把第一层集当作

元組成的集，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 Σ 是由集 $A, B, C, \cdots$ 組成的系，我們用

$$P(\Sigma)=A\cap B\cap C\cap\cdots$$

来表示 Σ 的交集，用

$$S(\Sigma)=A\cup B\cup C\cup\cdots$$

来表示 Σ 的并集. 要注意的是 Σ 虽然是第二层集，但 $P(\Sigma)$, $S(\Sigma)$ 却都是第一层集.

习 題 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，試証
   (i) $A\cap(B\cap C)=(A\cap B)\cap C$,
   (ii) $A\cup(B\cup C)=(A\cup B)\cup C$,
   (iii) $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$,
   (iv) $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$,
   (v) 如果 $A\subseteq C$，那末 $A\cup(B\cap C)=(A\cup B)\cap C$.
4. 假定 M 是元数为 m 的有穷集，Σ 是 M 的所有子集組成的系，試証 Σ 的元数是 2^m.

§1.2 映 射，分 类

我們知道，近世代数学中集合的元是抽象的，因此，两个集如何来进行比較是一个关鍵性問題. 映射这个概念主要用途之一就是用来解决这个問題，它是近世代数学中最基本的工具.

对于集 M 中每一个元 a，如果根据某种规則，我們可以使它与

集 N 中一个唯一的元相对应,那末这对应叫做M射到 N **內的映射**,这个与 a 相对应的元,叫做 a 的**象**,a 又叫做它的象的**象源**,这时 N 中任意元不一定是 M 中某元的象;如果 N 中任意元又都是 M 中某元的象,那末这映射又叫做 M 射到 N **上的映射**. 假如 M 射到 N 內的映射用 σ 来表示,那末 a 的象,我們就用 $\sigma(a)$ 来表示. 有时这映射又表为 $a\to\sigma(a)$.

显然,M射到 N 內的映射就是M射到N中某一子集上的映射. 譬如在整数集 $\mathfrak{C}$ 中,根据自乘这个規則,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已內的映射,也是整数集射到由所有整数平方組成集上的映射.

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**.

我們知道,当 σ 是映射时,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,叫做**一对一的映射**;不是一对一的映射,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 中所有这样的元組成的集,它們的象都是在 B 中的,那末 A 叫做集 B 对于映射 σ 的**完全象源**.

M射到 N 上的一个映射 σ,当 $a_1\neq a_2$ 时,$\sigma(a_1)\neq\sigma(a_2)$,也就是說当 $\sigma(a_1)=\sigma(a_2)$ 时,$a_1=a_2$,那末 σ 就是一对一的映射.

集合 M 射到 N 上面的一对一的映射 σ 有时叫做**可逆一意映射**,用記号

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

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,我們叫它做 σ 的**逆映射**,用記号 σ^{-1} 表示. 因此,任意可逆一意映射都有逆映射,它也是可逆一意映射. 假如 σ 是可逆一意映射,那末它的逆映射 σ^{-1} 的逆映射就是 σ,这

就是說$(\sigma^{-1})^{-1}=\sigma$。

譬如在自然数集中，我們把偶数与 0 对应，奇数与 1 对应，这样就得到自然数集射到集合 $\{0, 1\}$ 上的映射，这个映射是多对一的，0 的完全象源是所有的偶数，1 的完全象源是所有的奇数，它們都沒有唯一的象源．假如我們把自然数 n 与 $2n$ 对应，即 $n\to 2n$，那就得到自然数集射到正偶数集上的映射，这个映射是一对一的，因此它有逆映射，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，譬如說 M，射到他一个 N 上，那末这两个集就叫做**有相等的濃度**（或称势，或参数）．与自然数集或它的子集有相等濃度的集，叫做**可数集**．因此有穷集是可数集．任一可数集中元可以用自然数做标号来排列，于是任意可数集M可以写成

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

一个集如果不是可数集，就叫做**不可数集**。

自然数集与正偶数集有相等的濃度，因此一个集的濃度也可以与它的眞子集的濃度相等，这是无穷集的一个重要性质，任意有穷集是不能够与它的眞子集有相等的濃度的。

假定 $M=N$，那末M射到 N 內的映射，就叫做M射到**自己內的映射**，M 射到 N 上的映射，就叫做M射到**自己上的映射**．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，也就是說不使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，譬如平面上的旋轉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射到自己內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 $n\to 2n$ 就是自然数集射到自己內的一对一的映射，$2n\to n$, $2n+1\to 2n+1$ 就是自然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, $\sigma_1(a)=\sigma_2(a)$,我們就說这两个映射**相等**,用記号$\sigma_1=\sigma_2$表示. 假如τ是A射到B上的映射,σ是B射到C上的映射,$\tau(a)=b$, $\sigma(b)=c$,卽

$$a\rightarrow b,\ b\rightarrow c,$$

我們容易証明对应$a\rightarrow c$就是A射到C上的映射,叫做映射σ,τ的**积**,用記号$\sigma\tau$表示,卽

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

这就是說$\sigma\tau$是先施行τ,再施行σ所得到的映射. 我們容易知道,假如σ, τ都是可逆一意映射,那末σ, τ的积$\sigma\tau$也是可逆一意映射. 显然$\tau^{-1}\sigma^{-1}$就是$\sigma\tau$的逆映射,并且$\sigma\tau$又是$\tau^{-1}\sigma^{-1}$的逆映射. 假如σ是可逆一意映射,那末$\sigma^{-1}\sigma(a)=a$, $\sigma\sigma^{-1}(a)=a$,因此$\sigma^{-1}\sigma=I$, $\sigma\sigma^{-1}=I$,这就是$\sigma^{-1}\sigma$与$\sigma\sigma^{-1}$都是恒等映射.

要注意的是虽然一个集的任意两个变换的积是存在的,但一般两个映射不一定有积;再映射σ, τ的积$\sigma\tau$与τ, σ的积$\tau\sigma$一般不是一致的. 譬如τ是A射到B上的映射,σ是B射到A上的映射,这时,$\sigma\tau$, $\tau\sigma$都有意义,但前者是A射到自己上的映射,而后者則是B射到自己上的映射,两者显然不一致. 卽令$A=B$,一般$\sigma\tau$与$\tau\sigma$也不一定相等,象这样的例子,我們在几何上是很熟悉的.

假定对于集A中任意元a与集B中任意元b,根据某个規則,我們可以把a, b与某集中唯一的元c对应,那末这对应,我們叫做A, B的**結合法**,有时又叫做A, B的**代数运算**. 也就是說,根据这結合法,我們可以把a, b結合得到元c,因此我們又說A, B有一个結合法. 譬如对于整数集$\mathfrak{C}$中任意二数a, b,我們命$a+b$与它們对应,那末这对应就是$\mathfrak{C}$的結合法,它就是普通的加法. 同样,对于a, b我們命$a\cdot b$与它們对应,这对应也是$\mathfrak{C}$的結合法,它

就是普通的乘法。

一个集，假如它具有适合某些法则的結合法，或代数运算，就叫做**代数系**。象上面所示，整数集 $\mathfrak{C}$ 是代数系，因为它所具有的加法，乘法二个結合法适合交换律 $a+b=b+a$, $ab=ba$，結合律 $a+(b+c)=(a+b)+c$, $a(bc)=(ab)c$，分配律 $a(b+c)=ab+ac$ 等法則，近世代数学的目的就是討論某些基本代数系关于結合法的性质，也就是代数性质。因此可以説近世代数学是研究某些基本代数系的理論的学科。

上面我們研究了映射，現在我們再来介紹分类这个新概念。

我們知道，通常我們把两个元看成同一个元，或者説两个元相等，所用的等号"＝"这个記号适合下面三个律：

1° 自反律：$a=a$,

2° 对称律：假如 $a=b$, 那就 $b=a$,

3° 傳递律：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，譬如前面所述的濃度相等就是适合这三个律的一个关系。一般来說，我們有

定义 假如对于一个集的元，我們規定了一个关系 $\sim$，并且我們可以判別其中每对元 a, b 是否有这个关系 $a\sim b$；再这个关系还适合上面的自反，对称，傳递三个律，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 $a\sim c$.

那末这个关系，就叫做这集的**等价关系**。

譬如濃度相等，就是集合間的等价关系，初等几何中的三角形全等、相似也都是三角形間的等价关系，但是整数集 $\mathfrak{C}$ 中不相等，或者大于、小于等关系都不是等价关系。

在一个集中，根据某个观点或者用某种关系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**. 分类所根据的观点或所采用的关系,由上面得知是一个等价关系,因此我們要問一个集的任一等价关系能否用它把这集来分类，这是等价关系的一个重要性质。

定理 假如集M有一个等价关系，所有与一个元等价的元的集,叫做一类,那末M就能够分成为若干个这样沒有公共元的类而无剩余。反过来,假如M能够分成若干个沒有公共元的集,我們叫它做类,而无剩余,那末元素在同一类这个关系就是等价关系。

証明 定理的后半段我們容易知其成立，因此我們只要証明前半段就行了。

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 中所包含的元是所有相互等价的元,这是因为从 $a\sim b$, $a\sim c$,根据对称律,傳递律就得到 $b\sim c$. 显然M中任意元必定属于这样的一类,因此M可以分成这样的类而无剩余.

假如我們能够証明任意这样的两类不是相等就是沒有一个公共元,那末M中任意一元只能在唯一的一类,因此定理的前半段就告成立了。

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 $K_a\subseteq K_b$. 同样我們可以証明 $K_b\subseteq K_a$, 所以 $K_a=K_b$. 这就是說任意两类如果不相等,那末它們就沒有一个公共元,于是定理的前半段成立,因此定理得証.

于是我們得知一个集，如果有一个等价关系，它就有一种分类,反过来,如果它有一种分类,它就有一个等价关系.

假如 m 是一个正整数，在整数集$\mathfrak{C}$中，两数 a , b 的差 $a-b$ 如果能够用 m 整除,即 $m|(a-b)$时,叫做对于模 m, a 与 b **同余**,

用記号

$$a\equiv b(\bmod m) \text{ 或 } a\equiv b(m)$$

表示。显然 $a\equiv a$，并且我們容易証明，假如 $a\equiv b$，那末 $b\equiv a$，再假如 $a\equiv b$，$b\equiv c$，那末 $a\equiv c$，因此同余关系适合等价律，所以它是等价关系。于是对这个关系，整数集 $\mathfrak{C}$ 有一个分类，a 所在的类是所有形状象 $a+km$（k 是任意整数）的数的集，叫做 a 对于 m 的**剩余类**，我們用 $\bar{a}$ 表示。因此 $\mathfrak{C}$ 可以分成为 m 个类

$$\bar{0},\ \bar{1},\ \cdots,\ \overline{m-1},$$

这是因为对于模 m，任意一整数必定与 $0, 1, \cdots, m-1$ 中某一数同余，并且 $0, 1, \cdots, m-1$ 中任意两数都不同余。当 $m=2$ 时，整数集 $\mathfrak{C}$ 就分成为两类，一类是所有偶数形成的偶数类，一类是所有奇数形成的奇数类。相异的元都不同余的同余叫做**零同余**。因此整数集 $\mathfrak{C}$ 自身可以看成是根据零同余确定的分类，它的每个剩余类只有一个元。

上面是为了叙述方便，假定 $m>0$，其实 $m<0$ 时也是同样成立的，这时整数集 $\mathfrak{C}$ 可以分成 $|m|$ 个剩余类。

习 题 1.2

1. 假如 $a\equiv b(m)$，$c\equiv d(m)$，那末

$$a+c\equiv b+d(m),\qquad a-c\equiv b-d(m),$$
$$na\equiv nb(m),\qquad ac\equiv bd(m).$$

2. 試就 $m=-5$ 时，把整数集 $\mathfrak{C}$ 分类。

3. 假如 σ 是 A 射到 B 上的映射，τ 是 B 射到 A 上的映射，如果 $\sigma\tau=I$，那末 σ 是 τ 的逆映射。

4. 假如 σ 是 M 射到 N 上的映射，A，B 分别是 M，N 的子集，試証 $\sigma(A)$ 的完全象源包含 A，而 B 的完全象源的象就是 B。

5. 有人說从对称律和傳遞律可以推出自反律，因此自反律可以不要，他