近世代数引论

冯克勤
李尚志
查建国

JINSHI DAISHU YINLUN

中国科学技术大学出版社

近世代数引论

冯克勤
李尚志
查建国

中国科学技术大学出版社
1988·合肥

内 容 提 要

近世代数是代数学一个基础学科，讲述代数基本结构的特性。本书除系统介绍群、环和域的基础知识（包括域的有限伽罗瓦扩张理论）之外，还力图强调近世代数中的思想和方法，书中有大量习题。除主线内容之外，还增加一些附录用来开拓和深化所学内容。

本书在中国科学技术大学讲授多年的讲义基础上修改写成。可作为高等学校数学系基础课教材，也可供数学工作者和通信、计算机科学等领域的工程技术人员参考。

近 世 代 数 引 论

冯克勤　李尚志　查建国

责任编辑：严镇军　封面设计：盛琴琴

中国科学技术大学出版社出版

（安徽省合肥市金寨路 96 号）

中国科学技术大学印刷厂印刷

安徽省新华书店发行　各地新华书店经售

开本：850×1168/32　印张：7.5　字数：194千

1988年 9 月第 1 版　1988年 9 月第 1 次印刷

印数：1—3000册

ISBN7-312-00041-x/O·14 统一书号：13474·14　定价：1.65元

前　言

近世代数是讲述群、环、域（以及模）等代数对象基本性质的一门大学课程。它是今后学习和研究代数学的基础，也是研究其他数学、物理学和计算机科学等不可缺少的工具。

本书是我们于一九八二年在中国科技大学授课讲义基础上，经过五年教学实践改写而成。原讲义共五章，为了在一学期（周四学时）内讲完，这次删去了模论和线性代数两章。

近世代数从它产生的年代起就明显有别于古典代数学。它的主要研究对象不是代数结构中的元素特性，而是各种代数结构本身和不同代数结构之间的相互联系（同态）。掌握近世代数中所体现的丰富的数学思想和方法，比背诵一些代数学定义和名词字典要重要得多。我们在教学中几乎用半个学期讲述第一章群论，这是因为在群论中体现了近世代数的基本研究思想和方法，而这些思想和方法在学生过去学习中是不熟悉的。群论中的定理基本上可分为定量和定性两类：前者的典型例子是拉格朗日定理，后者的典型例子是同态基本定理。我们着重讲授定性内容，特别是同态基本定理和群在集合上的作用，这是群论的关键所在。

第二章讲述环论和域论初步，正文中的内容是标准的。但是在几个附录中，我们介绍了在数学发展中有历史意义的几个课题（高斯二平方和问题，代数基本定理，尺规作图，三等分角等），最后一章向学生展示关于域的有限伽罗瓦扩张的优美理论。

最后，我们向过去几年里对此书的前身提供意见的许多学者、教师和学生表示深深的谢意，我们也欢迎大家今后对此书给予更多的批评和指正。

作者　一九八七年三月于合肥

目　录

第一章 群

§1 集合论预备知识

群是集合上赋予某种二元运算的一种代数结构. 所以在讲述什么是群之前，先要介绍集合论中我们所需要的一些预备知识.

一些特定的对象放在一起就叫作一个**集合**. 例如全体正整数构成一个集合，表示成$\boldsymbol{N}$. 全体整数构成整数集合，表示成$\boldsymbol{Z}$. 类似地有复数集合$\boldsymbol{C}$，实数集合$\boldsymbol{R}$，有理数集合$\boldsymbol{Q}$等等. 集合A中每个对象a叫作A中的**元素**，表示成$a\in A$，说成a**属于**A. 否则，如果某个对象b不属于A，则表成$b\notin A$.

设A和B是两个集合，如果A中每个元素均是B中元素，即

$$a\in A\Rightarrow a\in B,$$

则A叫作B的一个**子集**，表示成$A\subseteq B$或者$B\supseteq A$. 如果$A\subseteq B$并且$B\subseteq A$，即

$$a\in A\Leftrightarrow a\in B,$$

这也相当于说集合A与B包含同样的元素，这时叫作集合A与B相等，表示成$A=B$. 如果A是B的子集并且不等于B，则A叫B的**真子集**，表示成$A\subset B$或者$B\supset A$. 不包含任何元素的集合叫作**空集**，表示成$\varnothing$. 空集显然是每个集合的子集.

可以有许多方式来表达一个确定的集合. 例如若集合A只有有限多（不同）元素$a_1,\cdots,a_n$（$n\in N$），则这个集合可表成

$$A=\{a_1,\cdots,a_n\}.$$

只有有限多个元素的集合叫**有限集**，否则叫**无限集**. 具有n个元素的集合叫n**元集**，元素个数表示成$|A|=n$. 在一般情形下，集合S中具有某种性质P的全体元素构成的集合通常表成

$$\{x\in S \mid x \text{ 有性质 } P\}.$$

例如：偶数集合$\{0,\pm 2,\pm 4,\cdots\}$可以表成

$$\{n\in Z \mid n\equiv 0 \pmod 2\}.$$

由一些已知集合构作新的集合通常用集合上的运算来实现。下面是集合的一些最基本运算，设A和B是两个集合，它们的公共元素组成的集合叫作A和B的**交**，表示成$A\cap B$，即

$$A\cap B=\{x\mid x\in A \text{ 并且 } x\in B\}.$$

类似地，n个集合$A_1,\cdots,A_n$的交为

$$\bigcap_{i=1}^{n} A_i = A_1\cap A_2\cap\cdots\cap A_n=\{x\mid x\in A_i\ (1\leqslant i\leqslant n)\}.$$

更一般地，对于任意多个集合形成的集族$\{A_i\mid i\in I\}$，（其中I是一个集合，叫该集族的**下标集合**，对于每个$i\in I$，A_i是该集族中的一个集合），它们的交为

$$\bigcap_{i\in I} A_i=\{x\mid x\in A_i \text{ (对每个 } i\in I)\}.$$

第二个集合运算是集合的**并**，集合A与B的并表示成$A\cup B$，定义为

$$A\cup B=\{x\mid x\in A \text{ 或者 } x\in B\}.$$

类似地：

$$\bigcup_{i=1}^{n} A_i = A_1\cup A_2\cup\cdots\cup A_n=\{x\mid x\in A_i \text{ (对某个 } i,1\leqslant i\leqslant n)\}$$

$$\bigcup_{i\in I} A_i=\{x\mid x\in A_i \text{ (对某个 } i\in I)\}.$$

设A是B的子集，则$B-A\doteqdot\{x\mid x\in B, x\notin A\}$叫作子集$A$（关于$B$）的**补集**。如果在讨论问题中所涉及的集合均是某个固定集合Ω的子集，则$\Omega-A$也常常简称作A的补集，表示成$\bar{A}$。

设A和B是两个集合，我们把集合

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

叫作A和B的直积．在$A\times B$中，$(a,b)=(a',b')$当且仅当$a=a'$并且$b=b'$．类似可定义多个集合的直积

$$A_1\times\cdots\times A_n=\prod_{i=1}^{n}A_i=\{(a_1,\cdots,a_n)\mid a_i\in A_i\ (1\leqslant i\leqslant n)\}.$$

$$\prod_{i\in I}A_i=\{(a_i)_{i\in I}\mid a_i\in A_i\ (\text{对每个 } i\in I)\}$$

为了比较不同的集合，需要将不同集合发生联系，这就是集合之间的映射．f叫作从集合A到集合B的**映射**，是指对每个$a\in A$均有确定办法给出集合B中唯一的对应元素，这个对应元素叫作a在映射f之下的象，表示成$f(a)$．而“f把a映成$f(a)$”这件事表示成$a\to f(a)$．从A到B的映射f表示成$f:A\to B$或者$A\xrightarrow{f}B$．

设$f:A\to B$和$g:B\to C$都是集合之间的映射．则可经过连续作用，得到一个从A到C的映射

$$g\circ f:A\to C,\quad (g\circ f)(a)=g(f(a)).$$

映射$g\circ f$叫作f与g的**合成**映射．

设f和g均是从集合A到集合B的映射，我们称f和g**相等**（表示成$f=g$），是指对于每个$a\in A$，均有$f(a)=g(a)$．

引理 （合成运算满足结合律）设$f:A\to B$，$g:B\to C$，$h:C\to D$均是集合的映射，则

$$h\circ(g\circ f)=(h\circ g)\circ f.$$

证明 对于$a\in A$，令$f(a)=b$，$g(b)=c$，$h(c)=d$．则

$$(g\circ f)(a)=c,\quad (h\circ g)(b)=d.$$

于是

$$(h\circ(g\circ f))(a)=h(c)=d,\quad ((h\circ g)\circ f)(a)=(h\circ g)(b)=d.$$

从而对每个$a\in A$，$(h\circ(g\circ f))(a)=((h\circ g)\circ f)(a)$．这就表明$h\circ(g\circ f)=(h\circ g)\circ f$．证毕．

设$f:A\to B$是集合的映射．对于A的每个子集A'，令

$$f(A')=\{f(x)\mid x\in A'\},$$

这是B的子集，叫作A'在f之下的**象**。另一方面，对于B的子集B'，令$f^{-1}(B')=\{x\in A\mid f(x)\in B'\}$，这是$A$的子集，叫作$B'$的原象。如果$f(A)=B$，即$B$中每个元素均是$A$中某个元素（在$f$之下）的象，则$f$叫作**满射**。另一方面，如果$A$中不同元素被$f$映成$B$中不同元素，即：$a,a'\in A$，$a\neq a'\Rightarrow f(a)\neq f(a')$，则$f$叫作单射。最后，若$f:A\to B$同时是单射和满射，则$f$叫作**一一映射**或**一一对应**。例如：将集合A中每个元素均映成其自身的映射

$$1_A:\ A\to A,\ 1_A(a)=a.$$

就是A到A的一一对应。映射1_A叫作集合A的**恒等映射**。通常采用下面引理来判断一个映射是否为一一对应。

引理 2 映射$f:A\to B$是一一对应的充分必要条件是存在映射$g:B\to A$，使得$f\circ g=1_B$，$g\circ f=1_A$。

证明 如果f是一一对应，由定义知这意味着对每个$b\in B$，均存在唯一的$a\in A$使得$f^{-1}(b)=a$（存在性由于f是满射，唯一性由于f是单射）于是可定义映射

$$g:\ B\to A,\ g(b)=f^{-1}(b).$$

直接验证$g\circ f=1_A$和$f\circ g=1_B$成立。

另一方面，如果f不是满射，则存在$b\in B$，使得$f^{-1}(b)=\varnothing$。所以对每个映射$g:B\to A$，均有$(f\circ g)(b)=f(g(b))\neq b$。于是$f\circ g\neq 1_B$。如果$f$不是单射，则存在$a$，$a'\in A$，$a\neq a'$，使得$f(a)=f(a')=b$。那么对于每个映射$g:B\to A$，$(g\circ f)(a)=g(b)=(g\circ f)(a')$，于是$g\circ f\neq 1_A$。所以若存在$g:B\to A$使得$f\circ g=1_B$并且$g\circ f=1_A$。则必然$f$是一一对应。证毕。

当$f:A\to B$是一一对应时，满足$f\circ g=1_B$和$g\circ f=1_A$的映射$g:B\to A$是唯一的。这是因为：若$g':B\to A$也有性质$f\circ g'=1_B$，$g'\circ f=1_A$，

则 $$g'=g'\circ 1_B=g'\circ(f\circ g)=(g'\circ f)\circ g=1_A\circ g=g.$$

我们将这个唯一存在的映射 g 叫作 f 的逆映射，表示成 f^{-1}。

设 A 是集合。集合 $A\times A$ 的每个子集 R 叫作集合 A 上的一个**关系**。如果 $(a,b)\in R$，便称 a 和 b 有关系 R，写成 aRb。例如 $\boldsymbol{R}\times\boldsymbol{R}$ 中子集

$$R=\{(a,b)\in\boldsymbol{R}\times\boldsymbol{R}\mid a\text{ 比 }b\text{ 大}\}$$

则实数 a 和 b 有关系 R 即指 a 比 b 大，这就是“大于”关系。通常将这个关系记成 $a>b$。同样还有 R 上的关系 $\geqslant$（大于或等于），$<$（小于），$\leqslant$（小于或等于），$=$（等于）。集合 A 上的关系 $\sim$ 叫作**等价关系**，是指它满足如下三个条件：

（1）自反性：$a\sim a$（对于每个 $a\in A$）

（2）对称性：若 $a\sim b$，则 $b\sim a$。

（3）传递性：若 $a\sim b$，$b\sim c$，则 $a\sim c$。

设 $\sim$ 是集合 A 上的等价关系。如果 $a\sim b$，由对称性知 $b\sim a$。这时称元素 a 和 b 等价。对于每个 $a\in A$，以 $[a]$ 表示 A 中与 a 等价的全部元素构成的集合，即

$$[a]=\{b\in A\mid b\sim a\}.$$

由自反性知 $a\in[a]$，称 $[a]$ 为 a 所在的**等价类**，由传递性可知同一等价类中任意二元素彼此等价（设 b，$c\in[a]$，则 $b\sim a$，$a\sim c$，于是 $b\sim c$）。不同等价类之间没有公共元素（为什么？）因此集合 A 是一些等价类 $\{[a_i]\mid i\in I\}$ 的并，而这些等价类是两两不相交的。我们从每个等价类 $[a_i]$ 中取出一个元素 b_i（即 $b_i\in[a_i]$），则 $R=\{b_i\mid i\in I\}$ 具有如下性质：A 中每个元素均等价于某个 b_i，而不同的 b_i 彼此不等价。我们把具有这样性质的 R 叫作 A 对于等价关系 $\sim$ 的**完全代表系**。于是

$$A=\bigcup_{a\in R}[a]\text{（两两不相交之并）}.\qquad(*)$$

一般地，若集合 A 是它的某些子集 $\{A_i\mid i\in I\}$ 之并，并且 A_i 两两不相交，便称 $\{A_i\mid i\in I\}$ 是集合 A 的一个**分拆**。如上所述，A 上的每个等价关系给出集合 A 的一个分拆 $(*)$，反过来，如果

$\{A_i \mid i\in I\}$是集合A的一个分拆，可如下定义A上一个关系：对于a，$b\in A$，

$$a\sim b \Leftrightarrow a \text{和} b \text{在同一} A_i \text{之中},$$

请读者证明这是等价关系．以E表示A的全部等价关系，以P表示A的全部分拆，则上面由等价关系到分拆的映射f：$E\to P$和从分拆到等价关系的映射g：$P\to E$满足$f\circ g=1_P$，$g\circ f=1_E$，从而f是一一对应（引理2）．换句话说，集合A上的等价关系和A的分拆是一一对应的．

例如，设F是由某些集合构成的集族．在F上定义如下的关系：对于A，$B\in F$，

$$A\sim B \Leftrightarrow \text{存在从} A \text{到} B \text{的一一对应}.$$

这是F上的等价关系（自反性：1_A：$A\to A$是一一对应，从而$A\sim A$．对称性：若f：$A\to B$是一一对应，则f^{-1}：$B\to A$是一一对应，从而$A\sim B\Rightarrow B\sim A$．传递性基于习题3．）对于这种等价关系，彼此等价的集合叫作是**等势**的．比如说，两个有限集合等势（即存在一一对应）的充要条件是它们有同样多元素，即$|A|=|B|$．与正整数集合$\boldsymbol{N}$等势的集合叫作**可数无限集合**，其他无限集合叫作**不可数集合**．熟知实数集合$\boldsymbol{R}$是不可数集合．而正偶整数的全体E是可数（无穷）集合，因为存在着一一对应$\boldsymbol{N}\to E$，$n\to 2n$．这个例子也表明，无限集合A的一个真子集可以与A等势！

设A是集合．从$A\times A$到A的映射

$$f: A\times A\to A$$

叫作集合A上的一个（二元）运算．例如，通常复数加法就是运算

$$f: \boldsymbol{C}\times\boldsymbol{C}\to\boldsymbol{C},\ f(\alpha,\beta)=\alpha+\beta.$$

我们经常把集合A上的运算表示成$\cdot$，即对于a，$b\in A$，$f(a,b)$写成$a\cdot b(\in A)$或者更简单写成ab．

运算$\cdot$叫作满足结合律，是指

$$a\cdot(b\cdot c)=(a\cdot b)\cdot c \text{（对任意} a,b,c\in A\text{）}.$$

运算·叫作满足交换律，是指

$$a\cdot b=b\cdot a\ (\text{对任意 } a,b\in A)\ .$$

一个集合赋予满足某些特定性质的（一个或多个）二元运算，便得到各种代数结构。本书讲述群、环和域三种代数结构。

习　题

1. 设 B，$A_i\ (i\in I)$ 均是集合。试证：

i) $B\cap\left(\bigcup_{i\in I}A_i\right)=\bigcup_{i\in I}(B\cap A_i)$，

ii) $B\cup\left(\bigcap_{i\in I}A_i\right)=\bigcap_{i\in I}(B\cup A_i)$，

iii) $\overline{\bigcup_{i\in I}A_i}=\bigcap_{i\in I}\bar{A}_i$，$\overline{\bigcap_{i\in I}A_i}=\bigcup_{i\in I}\bar{A}_i$。

2. 设 $f: A\to B$ 是集合的映射，A 是非空集合。试证：

i) f 为单射⇔存在 $g: B\to A$，使得 $g\circ f=1_A$。

ii) f 为满射⇔存在 $h: B\to A$，使得 $f\circ h=1_B$。

3. 如果 $f: A\to B$，$g: B\to C$ 均是一一对应，则 $g\circ f: A\to C$ 也是一一对应，且 $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$。

4. 设 A 是有限集，$P(A)$ 是 A 的全部子集（包括空集）所构成的集族，试证 $|P(A)|=2^{|A|}$。换句话说，n 元集合共有 2^n 个不同的子集。

5. 设 $f: A\to B$ 是集合的映射。在集合 A 上如下定义一个关系：对任意 $a,a'\in A$，$a\sim a'$ 当且仅当 $f(a)=f(a')$。试证：这样定义的关系是一个等价关系。

6. 证明等价关系的三个条件是互相独立的，也就是说，已知任意两个条件不能推出第三个条件。

7. 设 A，B 是两个有限集合。

i) A 到 B 的不同映射共有多少个？

ii) A 上不同的二元运算共有多少个？

§2 什么是群

让我们先从半群讲起。

定义 集合S和S上满足结合律的二元运算$\cdot$所形成的代数结构叫作**半群**。这个半群记成$(S,\cdot)$或者简记成S，运算$x\cdot y$也常常简写成xy。

如果运算又满足交换律，则$(S,\cdot)$叫作**交换半群**。象通常那样令$x^2=x\cdot x$，$x^{n+1}=x^n\cdot x(=x\cdot x^n,\ n\geqslant 1)$

定义 设S是半群，元素$e\in S$叫作半群S的么元素，是指对每个$x\in S$，$xe=ex=x$。

如果半群S有么元素e，则它是唯一的，因若e'也是么元素，则$e'=e'e=e$。我们将半群S中这个唯一的么元素（如果存在的话）通常记成1_S或者1，具有么元素的半群叫**含么半群**。

定义 设S是含么半群。元素$x\in S$叫作元素$y\in S$的逆元素，是指$xy=yx=1$。

如果x有逆元素，则它一定唯一。因为若y'也是x的逆元素，则$xy'=y'x=1$。于是

$$y=y\cdot 1=y(xy')=(yx)y'=1\cdot y'=y'.$$

所以若x具有逆元素，我们把这个唯一的逆元素记作x^{-1}，则$xx^{-1}=x^{-1}x=1$。

定义 半群G如果有么元素，并且每个元素均可逆，则G叫作**群**。此外，若运算又满足交换律，则G叫作**交换群**或叫**阿贝耳**（Abel）**群**。

下面给出半群和群的一些例子。

例 1 设M为非负整数全体，$(M,+)$是含么交换半群，么元素是数0，但它不是群，因为只有0对于加法在M中才可逆。

Z，Q，R，C对于加法均是阿贝耳群，叫作整数加法群，

有理数加法群等等。

$(N,\cdot)$ 是含么交换（乘法）半群，么元素为 1。它不是群。令 Q^* 为非零有理数全体，则 $(Q^*,\cdot)$ 是交换群，么元素为 1，非零有理数的乘法逆为 α^{-1}。这叫非零有理数乘法群，同样有 $(R^*,\cdot)$ 和 $(C^*,\cdot)$，这些都是阿贝耳群。

例 2 以 $M_{m,n}(C)$ 表示全体 m 行 n 列复矩阵组成的集合，它对矩阵加法形成阿贝耳群。么元素是全零矩阵，而矩阵 $A=(\alpha_{ij})$ 的加法逆是 $-A=(-\alpha_{ij})$。以 $M_n(C)$ 表示 n 阶复方阵全体，它对乘法形成含么半群，么元素是单位方阵 I_n。由线性代数可知，n 阶复方阵 A 有乘法逆的充要条件是 $\det A\neq 0$。从而 $M_n(C)$ 不是群，并且当 $n\geqslant 2$ 时，易知半群 $M_n(C)$ 不是交换的。类似有加法交换群 $M_{m,n}(R)$，含么半群 $M_n(Q)$ 等等。

例 3 设 A 是非空集合，以 $\Sigma(A)$ 表示从 A 到 A 全体映射组成的集合。则 $\Sigma(A)$ 对于映射合成运算形成含么半群。么元素为 A 上恒等映射 1_A。由§1的引理 2 可知，$\Sigma(A)$ 中映射 f 可逆的充要条件是 f 为一一对应。所以当 $|A|>1$ 时，$\Sigma(A)$ 不是群，并且半群 $\Sigma(A)$ 不是交换的。

例 4 欧氏平面 R^2 中保持欧氏距离不变的运动叫作**欧氏运动**。由于欧氏运动必为 R^2 到自身之上的一一对应，并且它的逆仍是欧氏运动，而两个欧氏运动的合成仍是欧氏运动，从而全体欧氏运动形成群，叫作平面上的**欧氏运动群**，这也是非阿贝耳群。

例 5 设 n 为正整数，我们在 Z 上定义如下关系：对于整数 a 和 b，

$$a\sim b\Leftrightarrow n\mid a-b\ (\text{即 } a\equiv b\ (\mathrm{mod}n))$$

易知这是等价关系，于是整数集合 Z 分拆成 n 个等价类：$\overline{0}$，$\overline{1}$，…，$\overline{n-1}$，其中 $\overline{i}$ 表示 i 所在的等价类，即 $\overline{i}=\{m\in Z\mid m\equiv i\ (\mathrm{mod}n)\}$。而 $\{0,1,2,\cdots,n-1\}$ 是 Z 对于上述模 m 同余关系的一个完全代表系。

以 Z_n 表示上述 n 个等价类组成的集合。在 Z_n 上定义加法：

$$\overline{a}+\overline{b}=\overline{a+b}$$

由同余式基本性质可知这个加法运算是可以定义的，即与等价类（或叫模 n 同余类）中代表元的取法无关，并且 Z_n 对于这个运算形成交换群，么元素是 $\overline{0}$，这叫**整数模 n 加法群**。

如果 Z_n 中定义乘法

$$\overline{a}\ \overline{b}=\overline{ab}$$

则 Z_n 对此乘法是含么交换半群，么元素为 $\overline{1}$。由于等式 $\overline{a}\ \overline{b}=\overline{1}$ 相当于同余式 $ab\equiv 1\pmod{n}$。从初等数论知道，对于给定的 a，存在 b 满足 $ab\equiv 1(\mathrm{mod}n)$ 的充要条件是 $(a,n)=1$，从而 $\overline{a}$ 对于上述乘法可逆的充要条件是 $(a,n)=1$。

设 $(M,\cdot)$ 是含么半群，我们以 $U(M)$ 或者 M^* 表示半群 M 中可逆元素全体。

定理 1 若 $(M,\cdot)$ 是含么半群，则 $(U(M),\cdot)$ 是群。

证明 由 $1_M^{-1}=1_M$ 可知 $1=1_M\in U(M)$。若 $a,b\in U(M)$，则 a，b 均可逆，易知 $b^{-1}a^{-1}$ 是 ab 的逆元素，从而 $ab\in U(M)$。因此·是 $U(M)$ 上的二元运算。这运算在 $U(M)$ 中当然也满足结合律，于是 $(U(M),\cdot)$ 是含么半群。由于 $U(M)$ 中每个元素 a 均可逆，从而 $a^{-1}\in M$ 也可逆（因为 a 是 a^{-1} 的逆），因此 $a^{-1}\in U(M)$。从而 $U(M)$ 中每个元素在 $U(M)$ 中均可逆。根据定义，$U(M)$ 为群。证毕。

于是由前面的例子便知：

(*a*) 全体 n 阶可逆复方阵形成乘法群，叫作复数上的 n 次**一般线性群**，表示成 $GL(n,\boldsymbol{C})$。同样有群 $GL(n,\boldsymbol{R})$，$GL(n,\boldsymbol{Q})$ 等。

(*b*) 设 A 为非空集合，A 到自身之上的所有一一对应对于合成运算形成群，叫作集合 A 上的**对称群**或**全置换群**，表示成

$S(A)$，其中元素（即A到A的一一对应）叫作集合A上的**置换**。

（c）设n为正整数，$\bar{a}$为整数a的模n同余类。则集合

$$Z_n^* = \{\bar{a} \mid (a,n) = 1\}$$

对于乘法形成阿贝耳群。这个群有$\varphi(n)$个元素，其中$\varphi(n)$是1到n中与n互素的整数个数（$\varphi(n)$叫**欧拉函数**）

设G是群。若集合G有限，称G为有限群，否则叫无限群。若有限群G共有n个元素，则G叫n**阶群**或叫n**元群**，$n = |G|$叫有限群G的**阶**。

为了考查各种群之间的联系，我们要研究群之间的映射。但是群不仅是集合还有运算，所以我们需要映射与群运算保持协调。确切地说：

定义 设$(G,\cdot)$和$(G',\circ)$是两个群。映射$f: G \to G'$叫作群G到群G'的**同态**，是指对$a,b \in G$

$$f(a\cdot b) = f(a)\circ f(b) \quad (\text{简记成 } f(ab) = f(a)f(b)).$$

此外，若f又为单射或满射，则f分别叫**单同态**或**满同态**。如果同态f是一一对应，则称f是群G到群G'的**同构**。这时，称群G和G'是**同构**的，表示成$G \cong G'$或者$f: G \xrightarrow{\sim} G'$。

彼此同构的群具有完全相同的群结构。在群论中，同构的群认为本质上是同一个群，我们更主要是研究本质不同的群之间的联系，所以同态是群论中更重要的研究手段。

例 1 考虑映射

$$\det: GL(n,\boldsymbol{C}) \to \boldsymbol{C}^*, \quad A \mapsto \det(A).$$

即把每个n阶可逆复方阵A映成它的行列式$\det(A)$（这是非负复数）。由于$\det(AB) = (\det A)(\det B)$，可知det是乘法群同态，并且易知这是满同态。当$n \geqslant 2$时，这不是单同态。

例 2 设n为正整数。$C_n = \{e^{\frac{2\pi i a}{n}} \mid 0 \leqslant a \leqslant n-1\}$。则$C_n$中$n$个复数形成乘法群（叫$n$**次单位根群**）作映射

$$f: C_n \to (Z_n,+), \quad e^{\frac{2\pi i}{n}a} \mapsto \bar{a}.$$