现代数学基础丛书·典藏版 8

有限群构造

（上册）

张远达 著

科学出版社

现代数学基础丛书·典藏版 8

有限群构造

上册

张远达 著

科学出版社
北京

内 容 简 介

本书主要论述有限群的构造理论，分上、下两册. 上册是代数领域中关于有限群的一些基本知识. 下册论述有限群的专题部分.

本书可供大专院校数学系高年级学生、研究生及代数研究工作者阅读，也可供其他有关科技工作者参考.

图书在版编目(CIP)数据

有限群构造. 上册/张远达著. —北京：科学出版社，2015.11
(现代数学基础丛书·典藏版；8)
ISBN 978-7-03-046419-4

I. ①有… II. ①张… III. ①有限群—研究 IV. ①O152.1

中国版本图书馆 CIP 数据核字(2015) 第 277007 号

责任编辑：张 扬 / 责任校对：林青梅
责任印制：徐晓晨 / 封面设计：王 浩

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京虎彩印刷科技有限公司 印刷

科学出版社发行 各地新华书店经销
*
2015 年 11 月第 一 版 开本：B5(720×1000)
2016 年 6 月 印 刷 印张：27 1/2
字数：357 000
POD定价： 198.00元
(如有印装质量问题，我社负责调换)

序　　言

有限群是代数学中一个古老的分支，它有十分悠久的历史．它是由解代数方程的需要，也就是由伽罗瓦（Galois）理论的需要而产生的，并且首先是由置换群的概念发展起来的．至于群的抽象的讨论大概是从弗罗比尼斯（Frobenius）开始的，也就是后来发现构成群之特殊材料（置换这个概念）并不重要，而只需注意一集合里面所定义的代数运算这个性质的探讨．正是这样一种发展，才使得有限群的一般理论得以建立在公理基础之上而变得严谨且清晰，并有利于这理论的进一步发展．仅在第二次世界大战后期几年它的研究中断了，但不久又恢复了它的活跃力，现在人们对有限群反而更为重视，考其原因是群论几乎在各个科技领域里都有它的应用．在爱丁堡举行的国际数学会上由维兰德（H. Wielandt）作的题为《有限群构造之发展》的报告（文献[1]），以及由居里亨（C. A. Чунихин）在全苏第三届代数会上作的题为《近年来有限群发展的若干方向》的报告（文献[2]），并由最近出版的虎拍（B. Huppert）的巨著（文献[3]），都足以说明近年来有限群研究的盛行．

有限群之研究大体可分为群表现与群构造两个方面．本书只叙述了有限群表现的基本知识，目的是用它证明 p^aq^b 阶群的可解性．本书主要是叙述有限群的构造理论．有限群构造的内容也非常丰富，不可能在一本书内包括无遗．例如，近年来国际上对于有限单群的研究有很大的发展，而本书对这个问题却未触及．本书仅环绕有限可解群能分解为西洛（Sylow）基底，以之为中心来阐述近来的发展趋势，而对超可解群给以较详尽的论述．

全书分上、下两册．上册共五章．第一章是基础理论；第二章以有限可解群能分解为素数幂阶群之积以及这样分解之唯一性

来说明素数幂阶群（在本书中称为 p-群）之重要性；第三章论述群表现的基本知识，解决 p^aq^b 阶群之可解性；第四章讲扩展理论，其重要性有二：一为借它可由二个群怎样去作另一新的群，二为因有限群存在合成群列，故知研究有限群的根本问题是决定有限单群与探索扩展理论；第五章讨论 p-群的基本性质．总而言之，上册为基本概念，是代数领域中关于有限群的一些基本知识，当然间或有些不是为专攻有限群工作的同志所需的内容；凡是这样的地方均打有星号 *，或用小号字排印，像这样一些地方初学者也可略去．

下册论述有限群的专题部分，诸如弗拉梯尼（Frattini）子群，费丁（Fitting）子群，卡特（Carter）子群，恩格尔（Engel）子群，群之 Π-性质及分解，半单群，超可解群，传输理论等等．概括之，本书是以霍尔（P. Hall），柏额（R. Baer），虎拍，维兰德，居里亨等人的主要工作为基础而阐述的，其间并非无作者的创意在．由于有限群范围过大，而本人学识肤浅，错误难免且取材可能不当，望同好者批评指正．

张远达

武汉大学，1980 年 8 月

目　　录

第一章 基础理论

群的概念在数学各分支与其他科技领域里有广泛的应用. 为使读者阅读方便，本书是从群定义及它的一些基本性质开始来叙述的.

§1. 群的概念

定义 由一些同类的元素(例如数或矩阵等等)组成的一个非空集合 G 满足下列四条件时，就把 G 叫做群:

1°. 在集合 G 内定义了一种代数运算——即对 G 之任二元 a, b(a, b 可为一同元，也可不同) 总可在 G 中找得一元与它们相应. 习惯上叫这样所找得的元素为 a 与 b 的积，记作 ab (或 $a\cdot b$)，并叫 a 与 b 都是积 ab 之因子. 注意，积与它的因子之先后顺序有关，即 ab 与 ba 一般不见得相等.

2°. 结合律成立——即对 G 之任三个元 a, b, c, 常有关系式 $(ab)c = a(bc)$.

3°. G 中至少有这样一元 e, 使 $ex=x$ 恒成立(任 $x\in G$). ——叫这 e 为 G 之一个左单位元.

4°. 对每个 $x\in G$, G 中至少有这样一元 x^{-1} 具有性质 $x^{-1}x = e$, 但这 e 为 3° 中所说的某确定的 e. 于是 x^{-1} 不仅与 x 有关且还与 e 之选择有关叫 x^{-1} 为 x 的一个左逆元(对 e 而言).

说确切些，又把 G 关于 1° 之结合方法叫做群. 1° 中说的结合方法叫**乘法**. 注意，**乘法与积**只是两个术语，说明群元素结合的意义与结合的结果. 如将群元素结合方法写为加法"+"，则 a, b 结合的结果为 $a+b$，叫做**和**，而结合律应改为 $(a+b)+c = a+(b+c)$.

群之左单位元及每元 x 之左逆元 x^{-1} 究竟有怎样的特性呢?

首先,设 e 为群 G 之一左单位元. 对这 e 言,若 $x\in G$(符号 $x\in G$ 表 x 为 G 之元),则由 4° 知有 $x^{-1}\in G$,因之又有 $(x^{-1})^{-1}\in G$,使 $x^{-1}x=e$, $(x^{-1})^{-1}\cdot x^{-1}=e$, 于是 $(x^{-1}x)x^{-1}=ex^{-1}=x^{-1}$, 故再据 2° 得 $x^{-1}(xx^{-1})=x^{-1}$, 据 3° 得 $(x^{-1})^{-1}[x^{-1}(xx^{-1})]=(x^{-1})^{-1}x^{-1}=e$, 复由 2° 与 3° 得 $e=[(x^{-1})^{-1}x^{-1}](xx^{-1})=e(xx^{-1})=xx^{-1}$. 证得了 $x^{-1}x=xx^{-1}=e$, 即对 e 言知 G 中每元 x 之每个左逆元 x^{-1} 必同时为 x 的右逆元. 正因为如此,故无必要把逆元加以左、右之分,干脆叫 x^{-1} 为 x 之逆元,也说明了原先直接用符号 x^{-1} 的用意. 须注意的是, x 的每个逆元 x^{-1}(关于 e 言)还是唯一的, 因若 x_1 是 x 之任一个逆元,则从 $xx_1=e=xx^{-1}$, 得 $x^{-1}(xx_1)=x^{-1}(xx^{-1})$, $(x^{-1}x)x_1=(x^{-1}x)x^{-1}$, $ex_1=ex^{-1}$, $x_1=x^{-1}$, 即证明了逆元的唯一性,且同时证明了 x^{-1} 之逆元为 x, 即 $(x^{-1})^{-1}=x$.

其次,由 $xe=x(x^{-1}x)=(xx^{-1})x=ex=x$, 又知每左单位元 e 同时必为右单位元,因而也无必要将单位元加以左、右之分;干脆叫 e 为 G 之单位元. 群 G 之单位元也是唯一的: 因若 e' 是一单位元,则由 e 与 e' 都可为左、右单位元,就不得不有 $ee'=e'$ 与 $ee'=e$, 故 $e'=e$.

总之,群 G 的单位元 e 只有一个,每元 x 的逆元 x^{-1} 也只有一个.

如将群定义中的条件 3° 与 4° 分别改为:

3_1°. G 中至少有一右单位元 e 使 $xe=x$ 对任 $x\in G$ 常成立;

4_1°. 对每 $x\in G$, G 中至少有一元 x^{-1} 使 $xx^{-1}=e$ (叫 x^{-1} 为 x 的一个右逆元),但 e 是 3_1° 中说的某个 e;那末同样可证由 3_1° 与 4_1° 能得 3° 与 4°. 换言之, 1°, 2°, 3°, 4° 和 1°, 2°, 3_1°, 4_1° 是群定义的等价条件,即把群定义中的"左"字都改为"右"字,是无影响的.

于是我们自然会问: 若将 3° 与 4° 中某个"左"字不变,另一个"左"字改为"右"字,会发生什么现象呢? 如

$$e_1=\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix},\quad e_2=\begin{pmatrix}1 & -1\\ 0 & 0\end{pmatrix},$$

$$a=\begin{pmatrix}-1 & 1\\ 0 & 0\end{pmatrix},\quad b=\begin{pmatrix}-1 & -1\\ 0 & 0\end{pmatrix},$$

这四个 2 级矩阵组成的集合 G 中若定义二元之结合方法为矩阵之通常的乘法，那末 G 中任二元结合之结果如下表所示.

	e_1	e_2	a	b
e_1	e_1	e_2	a	b
e_2	e_1	e_2	a	b
a	b	a	e_2	e_1
b	b	a	e_2	e_1

即先画两条互相垂直的线(一是水平的、另一是竖直的)；再将 G 之元 e_1, e_2, a, b 写在水平线上方，同时又写在竖直线之左方；G 中二元结合时，约定第一个因子取在竖直线的左方，第二个因子取在水平线的上方，并将结合结果写在第一个因子的向右及第二个因子的向下的交叉点处.

从上表看出集合 G 满足群定义条件 1°；因矩阵乘法确满足结合律，故集合 G 满足群定义条件 2°；又从上表已看出 e_1 与 e_2 皆可充当 G 之左单位元，即 3° 成立；但关于 e_1 言确知 e_1, e_2, a, b 的右逆元各为 e_1, e_1, b, b，而对 e_2 言又知它们的右逆元各为 e_2, e_2, a, a 故 G 满足 $4_1°$. 这说明了 G 满足 1°, 2°, 3°, $4_1°$；但 G 不是群，因群之左单位元必为右单位元，而 e_1 与 e_2 都不是右单位元.

由此例可知判断一集合为群时除检验 1°, 2° 外，还需检验 3° 与 4° 同时成立 (或检验 $3_1°$ 与 $4_1°$ 同时成立)，光检验了 3° 与 $4_1°$ (或 $3_1°$ 与 4°) 是不行的.

当结合方法 1° 写为加法“+”时，常用符号“0”表示单位元，用 $-a$ 表示 a 之逆元，习惯上叫这样的群为**加群**. 结合法写为乘法的群叫**乘群**，乘群的单位元有时用 1 表示.

群条件 1° 只是说群之任二元 x，y 结合的结果 xy 与 yx 都是群之元，并不要求 $xy = yx$. 特当群中任二元 x，y 常有关系式 $xy = yx$ 时，叫群为**交换群**. 结合方法写为加法的群习惯上总是表示交换群(即 $x + y = y + x$ 常成立).

只含有限多个元的群 G 叫**有限群**(或叫 G 的**阶**为有限的)，否则就说 G 为**无限群**(或叫 G 的**阶**为无限). 通常用符号 $o(G)$ 表示群 G 的阶，例如 $o(G) = \infty$ 表 G 为无限群，而 $o(G) = n$ 表 G 为有限群，其阶等于 n，或叫 G 为 n 阶群.

有限、无限、交换、非交换群的例很多. 如一切正实数之集合是无限交换(乘)群；一切 n 级满秩矩阵(矩阵的要素即组成分子为某域内的元)的集合是无限非交换(乘)群；1 之 n 个 n 次单位根(即方程 $x^n - 1 = 0$ 之根)之集合是 n 阶(有限阶)交换群；由

$$e = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad a = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$c = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad d = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad f = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

这六个 3 级初等矩阵(满秩的)所成之集合关于矩阵之乘法言确成群，而为六阶(有限阶)非交换群，这可以像前面由四个 2 级矩阵列表那样去检验，这时的表如下(叫做群表)：

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	f	e	d	c	a
c	c	d	f	e	a	b
d	d	c	a	b	f	e
f	f	b	c	a	e	d

与群定义中条件 1°，2°，3°，4° 等价的除了 1°，2°，3_1°，4_1° 外，

还有另一组等价条件，即 1°，2° 与

5°. 对于集合 G 中任二元 a 与 b，方程 $ax = b$ 与 $ya = b$ 在 G 内都有解.

由 1°，2°，3°，4° 易知 5°：因为 $x = a^{-1}b$ 与 $y = ba^{-1}$ 显然分别为 $ax = b$ 与 $ya = b$ 的解. 故需检验的是 1°，2°，5° $\Longrightarrow$ 3°，4°［甲 $\Longrightarrow$ 乙表示由甲可推得乙］. 这也易于了解：因对某 $a \in G$，由 5° 可知 $ya = a$ 在 G 内可解，令 e 为其一解（$ea = a$），于是对 $b \in G$ 而根据 5° 取 $ax = b$ 之一解 c 后（$ac = b$），就有 $eb = e(ac) = (ea)c = ac = b$，证明了 e 为 G 之一左单位元，即 3° 成立；又 $ya = e$ 之解的存在性（条件 5°）即证明了条件 4°.

下一性质很重要，经常引用，即

6°. 在群 G 内方程 $ax = b$ 与 $ya = b$ 的解皆是唯一的.

因从 $ax = b$ 得 $a^{-1}(ax) = a^{-1}b$，而 $a^{-1}(ax) = (a^{-1}a)x = ex = x$，故 $x = a^{-1}b$，即 $ax = b$ 之解只能是 $x = a^{-1}b$. 同样可证 $ya = b$ 之解的唯一性.

注意 这性质 6° 的含义是消去律，即

$$\begin{cases} ax = ax_1 \Rightarrow x = x_1, \\ ya = y_1a \Rightarrow y = y_1. \end{cases}$$

特当 G 为由有限多个元而成之集时，易证 G 成群的充要条件是 1°，2° 与 6°.（即这时不要求 5° 之可解性，而只要求解之唯一性.）

因若 G 成群，则 1°，2°，6° 成立自明. 故需检验的是 1°，2°，6° $\Longrightarrow$ 5°：因集合 G 只含有限多个元，如以 $a_1, a_2, \cdots, a_n$ 表示。故取定了 G 之某元 a 并作 n 个乘积 $aa_1, aa_2, \cdots, aa_n$ 后，则据 1，知 $aa_i \in G (i = 1, 2, \cdots, n)$，再据 6° 又知当 $i \neq j$ 时确有 $aa_i \neq aa_j$，于是 $aa_i (i = 1, 2, \cdots, n)$ 不得不为 G 之全部元素，故不论 b 为 G 之任何元，恒有一 a_i 使 $aa_i = b$（i 随 b 而变化），即 $ax = b$ 在 G 内可解. 同理也知 $ya = b$ 在 G 内可解. 因而 5° 获证.

总之，判定集合 G 成群，有下列三组条件（等价的）：

（一）1°，2°，3°，4°；

（二）1°，2°，3_1°，4_1°；

（二）1°, 2°, 5°.

但判定有限集成群，尚有下面一组等价条件：

（四）1°, 2°, 6°.

可是判定一有限集成群，有时常用群表来说明. 事实上，从群表可看出许多性质：例如单位元的存在从群表的角度言即意味着有一行的元素与水平线上方的元素完全一致（即相应位置的元相同），也有一列的元素与竖直线左方的元素完全一致；消去律则意味着群表之每行和每列都没有相同的元. 于是，当这些现象中有一不合时，则知所给的集合不成群. 但这些现象即令皆适合，要这集成群，还需检验结合律；可惜从群表不易判断结合律，§5 末再叙述检验的方法.

结合律指对 G 之任三元 a, b, c, 常有 $(ab)c = a(bc)$；正因为这样，故干脆将 $(ab)c = a(bc)$ 简写为 abc 而不加括号，并不有损其意义之明确性. 关于

$$\prod_{i=1}^{n} a_i = a_1 a_2 \cdots a_n$$

之多个元素的结合积是用递归公式

$$\prod_{i=1}^{1} a_i = a_1, \quad \prod_{i=1}^{n+1} a_i = \left(\prod_{i=1}^{n} a_i\right) a_{n+1}$$

来定义的. 关于这个，有下列两个引理.

引理 1 $\displaystyle\prod_{i=1}^{m} a_i \cdot \prod_{j=1}^{n} a_{m+j} = \prod_{k=1}^{m+n} a_k.$

事实上，$n = 1$ 时显然成立（这是定义）. 归纳地假定 $n = r$ 时成立，则由条件 2° 及定义，有

$$\begin{aligned}\prod_{i=1}^{m} a_i \cdot \prod_{j=1}^{r+1} a_{m+j} &= \prod_{i=1}^{m} a_i \cdot \left[\left(\prod_{j=1}^{r} a_{m+j}\right) a_{m+r+1}\right] \\ &= \left(\prod_{i=1}^{m} a_i \cdot \prod_{j=1}^{r} a_{m+j}\right) a_{m+r+1} \\ &= \left(\prod_{k=1}^{m+r} a_k\right) a_{m+r+1} = \prod_{k=1}^{m+r+1} a_k,\end{aligned}$$

即证明了引理 1 在 $n = r + 1$ 时是成立的.

引理 1 的实质意义是说两个结合积之积与它们的所有因子在同一顺序下的结合积相等，例如 $(abc)(df) = abcdf$. 于是，n 个元 $a_1, a_2, \cdots, a_n$ 所决定的一切结合积，只要这 n 个元的顺序不改变，不管在它们中间怎样添加括号或去掉括号，结果都一样，总是等于 $\prod_{i=1}^{n} a_i$. 特当这些 a_i 都相等而为 a 时，就用幂 a^n 表示 $a_1 a_2 \cdots a_n = \underbrace{aa\cdots a}_{n\text{个}}$，叫 a^n 为 a 之 n 次幂. 于是由引理 1 又有

$$a^n a^m = a^m a^n = a^{m+n}, \quad (a^m)^n = (a^n)^m = a^{mn}. \tag{1}$$

再定义 $a^0 = 1$，$a^{-n} = (a^{-1})^n (n > 0)$，易证公式 (1) 对任何整数 m, n (正、负或零)皆成立，故又有 $a^{-n} = (a^n)^{-1}$.

又因 $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = 1$，故根据逆元的唯一性可知 $(ab)^{-1} = b^{-1}a^{-1}$，于是用归纳法可知

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}. \tag{2}$$

关于交换群又有下面的

引理 2 设 $a_1, a_2, \cdots, a_n$ 为交换群 G 之任 n 个元. 不论 $p(1), p(2), \cdots, p(n)$ 表示自然数 $1, 2, \cdots, n$ 之任何排列，恒有关系式

$$\prod_{i=1}^{n} a_{p(i)} = \prod_{i=1}^{n} a_i \left(= a_1 a_2 \cdots a_n\right).$$

证明 $n = 1$ 时显然成立. 再归纳地假定引理 2 对 $n - 1$ 个元成立. 因 $p(1), p(2), \cdots, p(n)$ 是 $1, 2, \cdots, n$ 之排列，故必有一 k 使 $p(k) = n$，因之

$$\prod_{i=1}^{n} a_{p(i)} = \left(\prod_{i=1}^{k-1} a_{p(i)}\right) \cdot a_{p(k)} \cdot \left(\prod_{i=k+1}^{n} a_{p(i)}\right)^{1)}$$

---

1) $k=1$ 时无第一个括号 $\left(\prod_{i=1}^{k-1} a_{p(i)}\right)$，$k = n$ 时无后一个括号 $\left(\prod_{i=k+1}^{n} a_{p(i)}\right)$，这些都不影响证明的一般性.

$$= \left(\prod_{i=1}^{k-1} a_{p(i)}\right)\left(\prod_{i=k+1}^{n} a_{p(i)}\right) \cdot a_{p(k)}$$

$$= (a_{p(1)} \cdots a_{p(k-1)} a_{p(k+1)} \cdots a_{p(n)}) a_n .$$

但因 $p(1), \cdots, p(k-1), p(k+1), \cdots, p(n)$ 是 $1, 2, \cdots, n-1$ 的一个排列，故由归纳法的假设可知

$$a_{p(1)} \cdots a_{p(k-1)} a_{p(k+1)} \cdots a_{p(n)} = \prod_{i=1}^{n-1} a_i ,$$

因之就有

$$\prod_{i=1}^{n} a_{p(i)} = \left(\prod_{i=1}^{n-1} a_i\right) a_n = \prod_{i=1}^{n} a_i , \quad \text{证完.}$$

引理 2 是说交换群中 n 个元之结合积的结果只和这 n 个元自身有关，而与其先后顺序无关.

由引理 2 易证交换群 G 中任二元 a, b 恒有

$$(ab)^n = a^n b^n \tag{3}$$

之关系，但 n 为任何整数（正、负或零）. 同样，虽 G 非交换群，只要 $ab = ba$，也可证明 (3) 式为真.

在加群里，用符号 $\sum_{i=1}^{n} a_i$ 代替符号 $\prod_{i=1}^{n} a_i$，用 na 代替 a^n，于是公式 (1) 变为

$$ma + na = (m + n)a, \quad m(na) = (mn)a ,$$

而公式 (3) 变成了 $n(a + b) = na + nb$.

问题　由 $a \neq 0$ 之一切实数偶 (a, b) 所成之集 G 中结合方法为 $(a, b) \cdot (c, d) = (ac, bc + d)$. 试证 G 为无限非交换群.

§2. 同构，同态

群论的任务是研究“有一种代数运算”的集合（当然对这一种代数运算还要附加若干条件，如前节中的 2°, 3°, 4°）. 代数学研究的对象就是具有一种或多种代数运算的集合，但不是孤立地研究集合本身，往往是将集合中的结合方法（即代数运算）一块来考

虑．研究群当然也如此．于是当两群 G，G_1 已给时，可能 G 与 G_1 之结合方法不同（例如一为加群、一为乘群），但若在 G 与 G_1 之元间能建立一种对应关系，使这对应关系仅牵连到结合方法，而与各个群之元究竟是什么具体东西没有关系，那末从抽象的角度言，由某一群只利用其结合方法所推出的性质即得另一群借对应关系应具有的类似性质，这样可使我们的研究能一般化．为此，要引进一个重要概念——同构．下面先从一般情况来谈．

定义 1　设 S 与 T 为任二集合．如有一确定方法（记为 σ）能使 S 之每元 x 得在 T 内有相应的一元 y（记为 $y=x^{\sigma}$，或 $x\sigma$，或 σx），就叫 σ 是 S 在 T 内的一个映射．叫 y 为 x 的像，而叫 x 为 y 的一个原像（借映射 σ）．有时又记为

$$\sigma:\ x\to y.$$

注意这里的确定方法用通俗语言来说就是函数关系，即 y 为 x 之函数；从 x 能找着相应的 y 即表示 y 是 x 的单值函数；σ 为 S 在 T 内的一个映射就是说单值函数 y 的值域在 T 内，而自变量 x 变化的范围（或区域）为全集合 S．

若集 T 之每元 y 是集 S 中至少一个元 x 的像（关于映射 σ），即 T 之每元 y 至少有一个原像（或函数的值域为全集合 T），就叫 σ 是 S 在 T 上的映射．例如当 S 为一切整数之集合，而 T 为一切偶数之集合时，那末使每整数对应于其 2 倍的方法就是 S 在 T 上的映射，而使每整数对应于其 4 倍的方法就是 S 在 T 内的映射．

定义 2　若 S 在 T 上的映射 σ 只能使 T 之每元 y 为 S 之唯一个元 x 的像（即 T 之每元只有唯一个原像），就叫 σ 为 S 在 T 上的一对一的（简称 1-1 的）映射，记为 $\sigma:x\Longleftrightarrow y$．于是 S 与 T 有相同的浓度（或基数）——集合论的术语．

至于 S 在 T 内的 1-1 映射也可同样定义，不过这时 T 之每元不见得有原像，但若有，就只有一个．例如使每整数对应于其 2 倍与 4 倍分别为整数集合 S 在偶数集合 T 上与内的 1-1 映射．

定义 3　设 G 与 G_1 为二个群，其元分别表为 a，b，c，$\cdots$ 与 a_1，b_1，c_1，$\cdots$．若 σ 是 G 到 G_1 内（或上）的这样一个映射即由 σ

只要 $x \to x_1$, $y \to y_1$, 就必有 $xy \to x_1y_1$ [与之等价的是 $(xy)^\sigma = x^\sigma y^\sigma$ 或 $(xy)\sigma = x\sigma \cdot y\sigma$], 那末就叫 σ 是 G 到 G_1 **内**(或**上**)的同态映射而叫 G 同态于 G_1 **内**(或**上**). 特当 G 同态于 G_1 上时, 简称 G 同态于 G_1 (或 G 与 G_1 同态), 表为 $G \overset{\sigma}{\sim} G_1$, 或简写为 $G \sim G_1 (= G^\sigma)$.

当同态映射 σ 为 1-1 映射时, 叫 σ 为**同构映射**并叫 G 同构于 G_1 **内**(或**上**). 若 σ 为 G 到 G_1 **上**之同构映射时, 简称 G 同构于 G_1 (或 G 与 G_1 同构), 表为 $G \overset{\sigma}{\simeq} G_1$, 或简表为 $G \simeq G_1 (= G^\sigma)$.

据同构之义, 欲证映射 σ 为同构, 只需证明

$$(xy)^\sigma = x^\sigma y^\sigma \tag{1}$$

及

$$x^\sigma = y^\sigma \Rightarrow x = y. \tag{2}$$

例如使每整数对应于其 2 倍或 4 倍的映射分别是一切整数之加群在一切偶数之加群**上**或**内**的同构映射. 又如令正实数 a 对应于它的对数 $a_1 = \log a$ 之映射为 $\sigma[a \to a^\sigma = a_1 = \log a]$, 则因 $(ab)^\sigma = \log(ab) = \log a + \log b = a^\sigma + b^\sigma$, 以及 $a^\sigma = b^\sigma$ (即 $\log a = \log b$) $\Rightarrow a = b$, 并因每实数 a_1 可由 $e^{a_1} = a$ (即 $a_1 = \log a$) 得以决定唯一的正数 a, 即每实数 a_1 有唯一个原象 a, 故知一切正实数之乘群 G 与一切实数之加群 G_1 是同构的, 因而从群论的方法又知这二个集合的浓度相同.

设有二群 G 与 G_1, 假定 $G \overset{\sigma}{\sim} G_1$.

若 $x_1 \in G_1$, 则从 $G \overset{\sigma}{\sim} G_1$ 可知至少有一元 $x \in G$ 使 $x^\sigma = x_1$; 又由 $x = ex$ (e 为 G 之单位元) 得 $x_1 = x^\sigma = (ex)^\sigma = e^\sigma x^\sigma = e^\sigma x_1$, 故从 x_1 在 G_1 内的任意性不得不有 $e^\sigma = e_1$ (G_1 之单位元). 再从 $e_1 = e^\sigma = (x^{-1}x)^\sigma = (x^{-1})^\sigma \cdot x^\sigma$ 又知 $(x^{-1})^\sigma = (x^\sigma)^{-1}$. 于是证得

定理 1 若 $G \overset{\sigma}{\sim} G_1$, 则 G 之单位元 e 必对应 G_1 之单位元 e_1, G 之每元 x 的逆元 x^{-1} 必对应于 x 之对应元 x_1 的逆元 x_1^{-1}. 即 $e^\sigma = e_1$, $(x^{-1})^\sigma = (x^\sigma)^{-1}$.

推论 若 $G \simeq G_1$, 则 $e \longleftrightarrow e_1$; 且当 $x \longleftrightarrow x_1$ 时, 又有 $x^{-1} \longleftrightarrow x_1^{-1}$.