伽罗华理论

JIALUOHUALILUN

孙本旺编著

湖南科学技术出版社

伽罗华理论

孙本旺编著

湖南科学技术出版社

伽罗华理论

孙本旺 编著

责任编辑：胡海清

*

湖南科学技术出版社出版
（长沙市展览馆路14号）
湖南省新华书店发行　湖南省新华印刷二厂印刷

*

1984年4月第1版第1次印刷
开本：787×1092毫米 1/32　印张：6.25　字数：139,000
印数：1——5,700
统一书号：13204·97　　定价：0.99元

前　言

本书是为初学代数的人自学用的，其内容是根据作者于1948年在美国听代数学家E·阿丁（E.Artin）讲课的笔记改编而成．作者原想重写一遍，使其内容更完善一些，但一则阿丁的讲课有人比之于象讲诗一般，完全将数学这个比较严密的科学艺术化，读之引人入胜；再则作者身患重病，如果大改一番，反而失其精彩，同时也无此精力．阿丁本人很多年前已出版与本书内容基本相同的书，为什么还要出版这本书呢？这是因为本书讲得更通俗、更透彻一些，并且还增加了一些内容，这对初学的人更有益处．本来阿丁的讲稿比本书内容还要多得多：第一部分讲赋值论与希尔伯特（Hilbet）理论，第二部分讲代数数与代数函数，第四部分讲上同调理论及达特（Tate）定理．最后讲类域论，本书内容是他的第二部分．本想将这些内容全部整理出来付诸印刷，以供代数学者参考，但由于上述原因，这些计划不能实现了．

付印前曾请湘潭大学陈仲沪教授校阅本书原稿，对本书内容作了一些修改和润色，为本书的出版作了不少工作，作者特致深切的谢意．

由于作者重病住院，本书出版前未能作仔细推敲，一定存在不少错误和缺点，请读者批评指正．

孙本旺

1983.7.7于北京301医院

目　录

第一章 群

§1 乘法的定义及结合律

考虑一组元素，这些元素本身具有什么性质，我们暂不考虑它。元素用英文小写字母a，b，c，等等记它；元素的集合则用英文大写字母A，B，C，等等记它，符号$a\in G$表示：a属于G。在G内定义一种运算，叫做乘法：即对于G内每一对有次序的元素a，b（以下简称序偶），我们用某种方法（究竟什么方法无关紧要）规定一个元素c与序偶(a, b)对应，这种对应可用符号$(a, b)\longrightarrow c$记它，我们称c为a，b的乘积，有时写作$c=ab$（或$a\cdot b$），这里的c与序很有关系，一般说来，ab与ba不一定是相同的元素。

现在我们给出乘法封闭性定义如下：

定义1 集合G对于乘法运算而言是封闭的，就是说，如果a，$b\in G$，则$ab\in G$。

例1 命G为正整数（自然数）的集合，G内通常的减法作为上述的乘法，则对于这种乘法来说，G不是封闭的，事实上，$3\cdot 5=3-5=-2$不属于G。

例2 G同例1，如果取两个正整数a，b的最大公约数作为它们的乘积$a\cdot b$，显然G对于这种乘法运算是封闭的。

例3 G同例1，如取G的通常乘法作为上述乘法，则G对于这种乘法显然也是封闭的。

例4 取G为全体一元函数组成的集合如果f，$g\in G$，定义$(f\circ g)(x)=f[g(x)]$，显然对于这种乘法而言，G也是封闭的。

例5 命G为下列元素组成的集合

$$f_1=x,\ f_2=\frac{1}{x},\ f_3=1-x,\ f_4=\frac{1}{1-x},\ f_5=\frac{x}{x-1},$$

$f_6=\frac{x-1}{x}$，乘法定义为 $(f_i\circ f_j)(x)=f_i[f_j(x)]$，写出乘法表，得到

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_2	f_6	f_3	f_1
f_5	f_5	f_4	f_6	f_2	f_1	f_3
f_6	f_6	f_3	f_5	f_1	f_2	f_4

由此可知：G对于乘法$f_i\circ f_j$而言是封闭的，又注意一般地$f_i\circ f_j\neq f_j\circ f_i$。

现在对乘法再作第二个要求

定义11 乘法服从结合律，就是说，对于任意三个元素a，b，$c\in G$恒有$(ab)c=a(bc)$。

这是一个相当强的条件，一般是不被满足的，例如整数之间的减法就不满足结合律，但上述例4中G为一元函数的集合，乘法$f\circ g$就满足结合律：如$f(x)$，$g(x)$，$h(x)$为G中任意三个函数，则有

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

习题1 从定义11导出关于四个元素的结合律，即证明下列5个乘积，$a(b(cd))$，$((ab)c)d$，$(ab)(cd)$，$a((bc)d)$，$(a(bc))d$

都相等。

习题2 给出 n 个元素$a_1,\cdots a_n$，并按此序排列，问有多少种可能的乘积？

提示 命a_n为$a_1,\cdots,a_n$按此序排列所有可能得出的乘积数目，求出关于a_n的递推公式，并利用拉格朗日发生函数

$$f(x)=a_1x+a_2x^2+\cdots a_nx^n+\cdots$$

于是 $$(f(x))^2=a_1^2x^2+(a_2a_1+a_1a_2)x^3+\cdots$$
$$=a_2x^2+a_3x^3+\cdots$$

因为 $a_1=1$，这就给出

$$f^2-f+x=0,$$

故 $$f(x)=\frac{1-(1-4x)^{1/2}}{2}=\sum_{n=1}^{\infty}\frac{1\cdot3\cdots(2n-3)}{1\cdot2\cdots n}2^{n-1}x^n,$$

从而得出$a_n=\frac{1\cdot3\cdots(2n-3)}{1\cdot2\cdots n}2^{n-1}$。

这也可简写如下

$$a_n=\frac{(2n-3)!}{n!(n-1)!}。$$

习题3 n 个元素的结合律就是说：n 个元素按着写定的次序，可得出的所有可能的乘积都相同。如果对于三个元素的结合律成立的话，那么，对于任意多个元素的结合律都成立，试证明之。

证明：假设对于m 个因子的一切乘积结合律已成立，其中$m\leqslant n$，我们要证对于 $n+1$ 个因子的乘积结合律也成立。考虑特殊的乘积$\prod_{k=1}^{n+1}a_k$，这里是$n+1$个元素$a_1,a_2,\cdots a_{n+1}$顺次从右边相乘所得的乘积，即

$$\prod_{k=1}^{1} a_k = a_1,$$

$$\prod_{k=1}^{n+1} a_k = \left(\prod_{k=1}^{n} a_k\right) a_{n+1}.$$

命P_{n+1}为$n+1$个元素a_1，a_2，$\cdots a_{n+1}$按着某一个顺序相乘的一个乘积，因为P_{n+1}是至少一种乘法的结果，故可写

$$P_{n+1} = P_1^m P_{m+1}^{n+1} \qquad 1 \leqslant m \leqslant n.$$

这里P_1^m是元素a_1，$\cdots a_m$在这顺次下的某一个乘积，而P_{m+1}^{n+1}是其余元素a_{m+1}，$\cdots a_{n+1}$在这顺次下的某一个乘积，由归纳法，则有

$$P_\mu^\nu = \prod_{k=\mu}^{\nu} a_k.$$

对于任意的μ，ν，只要$\nu-\mu+1 \leqslant n$都真，特别有

$$P_{n+1} = \prod_{j=1}^{m} a_j \prod_{k=m+1}^{n+1} a_k$$

$$= \prod_{j=1}^{m} a_j \left(\prod_{k=m+1}^{n} a_k \cdot a_{n+1}\right) = \left(\prod_{j=1}^{m} a_j \cdot \prod_{k=m+1}^{n} a_k\right) a_{n+1}$$

$$= \prod_{k=1}^{n} a_k \cdot a_{n+1} = \prod_{k=1}^{n+1} a_k.$$

这里每一步骤都应用定义 II。

§2 群的定义

一个非空集合G，叫做一个群，如果集合G满足下列公理（或称为条件）。

（1）封闭性；在G内存在一种运算叫做乘法：对于任一对

有序的元素a，$b\in G$，对应于G中一个唯一的元素c，c叫做a与b的乘积，用$c=$表示之。

（2）结合律；如果a，b，$c\in G$，则

$$(ab)c=a(bc).$$

（3）单位元：存在一个元素 $e\in G$，使得

$$ea=a$$

对于一切$a\in G$成立，元素e叫做G的左单位元。

（4）逆元；对于每一元$a\in G$有一元$a^{-1}\in G$使得

$$a^{-1}a=e,$$

元素a^{-1}叫做元素 a 的左逆元。

让我们考虑乘积

$$(a^{-1})^{-1}a^{-1}aa^{-1}.$$

一方面，这个乘积可以写做

$$[(a^{-1})^{-1}a^{-1}](aa^{-1})=e(aa^{-1})=aa^{-1}.$$

另一方面 $[(a^{-1})^{-1}][(a^{-1}a)a^{-1}]=(a^{-1})^{-1}(ea^{-1})=(a^{-1})^{-1}a^{-1}=e$，从而得到 $aa^{-1}=e$，

故左逆元的存在意味着右逆元的存在，而且他们相同，这个元素就称为 a 的逆元。

同样结果对于单位元亦成立，事实上，考虑乘积

$$aa^{-1}a,$$

首先有$aa^{-1}a=(aa^{-1})a=ea=a$，

但又有 $aa^{-1}a=a(a^{-1}a)=ae$，

结果的：$ae=a$。

因此，左单位元的存在意味着右单位元的存在，且左、右单位元相同，这个元就称为G的单位元。

习题1 我们说两组公理系统是等价的，这是指其中一组可以从另一组用逻辑方法推导出来，现在把上面公理(3) 与(4)

分别用下面的公理来代替：

（3′）有一右单位元$e\in G$存在，使得

$$ae=a$$

对于一切的元$a\in G$成立。

（4′）对于每一元$a\in G$，有一右逆元$a\in G$，使得

$$aa^{-1}=e.$$

证明：（1），（2），（3），（4）与(1)，(2)，(3′)（4′)等价。

习题2 再考虑一组公理系统，其中(3）与(4）分别换作

（3″）存在一个左单位元$e\in G$，使得

$$ea=a$$

对于一切$a\in G$成立。

（4″）对于每一元$a\in G$，存在一个右逆元$a^{-1}\in G$，使得

$$aa^{-1}=e.$$

问满足（1），（2），（3″）与（4″）公理系统的集合G是否仍是一个群？如不是，请举一反例。

提示 对任一元$a\in G$，用$ax=x$（x取遍G中一切元）定义一个乘积，证明这个系统满足公理（1），（2），（3″），（4″），但不满足公理系统（1），（2），（3），（4），问那一性质不被满足？

对于通常的数，商可以看作是方程$ax=b$的解，现在考虑群G中类似的方程，

a）$ax=b$；b）$xa=b$；c）$axb=c$。如果方程a）对某一元$x\in G$成立，则

$$a^{-1}b=ex=x.$$

因此，如果方程a）有解，这个解不是别的，而就是$a^{-1}b$，并且是唯一的解，$a^{-1}b$事实上也确是方程的解，因为$a(a^{-1}b)=(aa^{-1})b=eb=b$，同理方程（b）有唯一的解$x=ba^{-1}$及方程c）也有唯一的解$a^{-1}cb^{-1}$，故上述方程的唯一的解的存在反映

群里具有与除法相似的一种性质。

因为a^{-1}是方程$xa=e$的一个解，且a^{-1}是唯一的，同样，e是方程$xa=a$的一个解，并且也是唯一的。注意方程$x(ab)=e$的解是 $(ab)^{-1}=b^{-1}a^{-1}$，因为 $(b^{-1}a^{-1})(ab)=b^{-1}(a^{-1}a)b=b^{-1}eb=b^{-1}b=e$，一般乘积的逆元

$$(a_1a_2\cdots a_n)^{-1}=a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}。$$

如果$x=(a^{-1})^{-1}$，则x满足方程$xa^{-1}=e$，但后一方程有唯一的解$x=a$，故$(a^{-1})^{-1}=a$，即元素的逆元的逆元仍为该元素本身。

习题3 证明公理（3）与(4）可以用下面的公理来代替

(3′）如果a，$b\in G$则方程

$$xa=b,\qquad ay=b$$

在G中都有解。

如果群的乘法还满足交换律

(5）若a，$b\in G$，则$ab=ba$。

那么称G为交换群，或叫做阿贝尔群。

习题4 证明§1例5组成一个不可交换（或称非交换）的群，并确定单位元与每一个函数的逆元。

§3 子　群

命G为一子群，S为它的一个子集，如果S自身在G的同样运算之下是一个群，则称S为G的一个子群。

例1 命G为除去零以外的一切有理数的集合，运算就是普通的乘法，则G是一个群，且G有下列子群，

(i) 正有理数的集合；

(ii) 任一元素的全体幂；

(iii) 只含-1与1的集合；

(iv) 只含单位元 1 的集合$\{1\}$。

命题1 命S为群G的一个子集，要使S成为G的一个子群，其充要条件是：

(A) 封闭性：若$s_1s_2\in S$，则$s_1s_2\in S$。

(B) 逆性：如果$s\in S$，则$s^{-1}\in S$。

证明 必要性：如果S是一个子群，则由群的公理 (1)，(A) 必成立，单位元$e\in S$是由方程$xs=s$在S内有解所保证的，而唯一性则由G中单位元的唯一性所保证，条件 (B) 通过方程$xs=e$亦容易建立。

充分性：如果 (A) 与 (B) 成立，我们要证明S是一个子群，从 (B) 则知若$s\in S$，则s^{-1}也属于S，再由 (A)，$s^{-1}s=e\in S$，结合律对于S的元素成立，因为结合律在G内成立。

如果S是G的子群，及$a\in G$，我们定义aS为所有元素as的集合，其中s取遍S中的一切元素，我们记$aS=\{as|s\in S\}$，as叫做傍系（或称陪系），因为$e\in S$，故$a=ae\in aS$。

例2 命G为一切非零的有理数集合，运算为通常的乘法，命S为G中一切正有理数的集合，显然S是G的一个子群，S在G内有两个傍系，即S与$-S=(-1)S$，这两个傍系没有公共元，它们合起来就是集合G。如果我们取S为$\{-1, 1\}$，则傍系$aS=\{a, -a\}$，注意在这情形下，仍然具有，任两个傍系若有公共元，则完全相同，它们合起来就是集合G，这结果在一般情形下都成立。

命S为群G的一个子群，并取$a, b\in G$。

引理1 如果傍系aS与bS有一公共元c，则$aS=bS$。

证明 假设对于某两个元素$s, s'\in S$有$as=bs'$，则$b=ass'^{-1}$，由命题 1，$ss'^{-1}=s''\in S$，因此$bS=as''S$，现在要证$s''S=S$，事实上，由于S是一个子群，而$s''\in S$，故$s''S\subset S$（意

思是说，集$s''S$中每一元素都含在S内），又$s''^{-1}S\subset S$，这意味着，$S\subset s''S$，因此$s''S=S$，故$bS=aS$。

引理2 群G的每一元素都必会在某一个傍系内。

证明 因为单位元$e\in S$，所以$ae=a\in aS$

如果群G只含有有限多个元素，则称G为一有限群；否则称为一无限群，有限群的元素数目叫做群G的阶。

命题2 设G为一有限群，且设它的阶为N，又设S为G的一个子群，其阶为n，则n是N的一个因子，就是说，n整除N，记作$n|N$。

证明 傍系aS与S含有相同数目的元素，事实上，命S中互异元素的全体为s_1，s_2，$\cdots s_n$则aS包含下列元素as_1，$as_2\cdots as_n$，它们也是互异的，因为如果$as_i=as_j$，则用a^{-1}左乘，就得$s_i=s_j$，这与假设不合，事实上，如果$s_i\neq s_j$则$as_i\neq as_j$。因此aS也含有n个元素，命j为傍系的数目，由引理1与引理2，则知这些傍系互不重叠，且它们合起来复盖G集，故有$N=jn$。

取一元素$a\in G$，用a^2记aa，一般定义a^n如下：

若n是正整数，则$a^n=a\cdots a$（n个因子）；

若$n=0$，则$a^0=e$；

若n是负整数，则$a^n=a^{-1}\cdots a^{-1}$（$-n$个因子）。

a的一切幂的集合是一个群，并且显然是包含a的最小子群，我们称这个群为由元素a生成的循环群，以(a)记之，至于含两个元素的最小群，那是另一种性质的问题，例如

$$(ab)^n=ab\cdot ab\cdots ab\qquad (n次)$$

如果乘法是可交换的，那么$(ab)^n=a^nb^n$，如果乘法是不可交换的，则$(ab)^n$的讨论一般讲来要麻烦得多。

习题1 证明元素a的幂a^n服从通常的指数定律：

$$a^\mu a^\nu=a^{\mu+\nu}\qquad (a^\nu)^\mu=a^{\nu\mu}$$

第一个性质意味着a的幂的乘法是可交换的。

a的所有幂的集合S组成群G的一个子群，因为S对于乘法是封闭的，而且每一元素的逆元存在，因此由命题1可知，S为群G的一个子群，现在考虑两种情形：

情形1)，a的幂都是互异的，在这种情形下，S是一个无限循环群。

情形2)，存在两个整数i与k，不妨设$i<k$，使得$a^i=a^k$，将两边乘以a^{-i}则得$e=a^{k-i}$，因此，使$a^\mu=e$成立的正整数μ的集合是非空的，因$a^\mu=e$可推出$a^{-\mu}=e$，命d为这个集合中的最小的正整数，则

$$a^d=e\Longrightarrow a^{\varepsilon d}=e$$

对一切整数ε成立，（$\Longrightarrow$读作“从…推出”或“蕴涵”），反之，如果$a^m=e$，则m必为d的倍数，事实上，若$m=qd+r$此处$0\leqslant r<d$，则

$$a^r=a^{m-qd}=a^m a^{-qd}=ee=e,$$

但d是使$a^d=e$成立的最小正整数，故必有$r=0$，由此得$m=qd$。

诸幂a^0，a^1，$\cdots a^{d-1}$

必两两互异，因为否则的话，将有$a^i=a^k$，其中$0\leqslant i<k<d$，即$a^{k-i}=e$，但这是不可能的，因为$0<k-i<d$，a的其它幂也必等于它们之中的某一个。例如，$a^d=e$，$a^{d+1}=e$，等等，一般地

$$a^{qd+r}=a^r \qquad (0\leqslant r<d),$$

故只有d个互异的a的幂。在这情形下，称$S=\{a^\mu\mid\mu=0.1\cdots d-1\}$为阶为$d$的循环群，并称$d$为$a$的周期。

命题3 有限群的任一元素的周期必为群的阶的因子。

证明 这是命题2的一个直接结果、命G为有限群，其阶为N，且a是G的一个元素，如果d是a的周期，则

$$S=\{a^0,\ a^1,\ \cdots a^{d-1}\}$$

是G的一个子群，其阶为d，因此，由命题2立即得知，$d|N$。

推论 如果群G的阶是一素数p，则G必为循环群。

证明 群的任一元素的周期必为p的因子，因此，它必为1或p，周期为1的元素只有单位元e，因此，如$a\in G$，$a\neq e$，则a的周期为p，于是易知$G=\{e, a, a^2\cdots a^{p-1}\}$。

以n为阶的循环群实际上只有一种，所谓一种是指阶数同为n的循环群必有相同的结构，但什么叫做相同的结构，这个问题留待以后再讲。

例3 让我们确定阶为4的群的一切可能的构造。任何元素的周期必为1、2或4，如果恰有一个元素a具有周期4，则e，a，a^2，a^3走遍群G中所有的元素，在这种情形下，G必是由a生成的循环群，即$G=(a)$，另一方面，如果没有周期为4的元素，则除去单位元e外（它的周期是1）其它3个元素的周期都是2，因此，如果e，a，b，c是群G的4个互异元素，则有$a^2=b^2=c^2=e$，现在考虑元素$x=ab\in G$，由$ax=aab=a^2b=eb=b$，显然$x\neq e$及$x\neq a$(因为$a\neq e$，$b\neq e$，$a\neq b$)，由方程$yb=b$的唯一解$y=e$便知$x\neq b$（因为若$x=b$，则$ab=b$从而$a=e$这与$a\neq e$相违）故x必为c，在这群内交换律也一定成立，因为若$x\in G$，则$x=x^{-1}$从而$ab=(ab)^{-1}=b^{-1}a^{-1}=ba$容易写出乘法表

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

故阶为4的群实际上只有两种：一种是循环群(a)；另一种是上