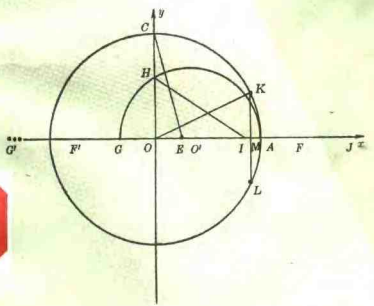
伽罗华理论基础

刘长安　王春森　编著



電子工業出版社

伽罗华理论基础

刘长安　王春森　编著

電子工業出版社

内 容 提 要

本书讲述了伽罗华理论的基本知识，内容包括：群论的有关基础知识——置换群，可解群，可迁群等；域和扩域的基础知识——有限扩域，代数扩域，多项式的分裂域，有限域等；伽罗华理论初步——正规扩域，伽罗华群，伽罗华理论的基本定理等；伽罗华理论的应用——代数方程可用根号解的充要条件，不能用根号解的方程的例子，尺规作图等。

本书可作为高等师范院校的教材，也可供大学数学系函授学员和中学数学教师参考。

伽罗华理论基础

刘长安 王春森 编著

责任编辑：吴金生

电子工业出版社出版（北京海淀区万寿路）

电子工业出版社发行 各地新华书店经销

山东电子工业印刷厂印刷

（淄博市周村）

开本：787×1092毫米 1/32 印张：5.375 字数：124千字

1989年9月第一版 1989年9月第一次印刷

印数：1～2500册 定价：2.40元

ISBN 7-5053-0564-6/O·6

序　言

本书是作者根据多次在河北师范学院讲授伽罗华理论课程的讲义修改编写而成，编写的过程是比较长的。本书第一作者根据1964年和1965年在河北北京师范学院数学系两次给高年级学生讲授伽罗华理论的材料，于1979年写成伽罗华理论讲义初稿，1979年至1982年以此初稿为教材在河北师范学院数学系曾给三届学生讲授。1982年下半年较全面地修改了初稿写成伽罗华理论讲义，于1983年初与全国多数师范院校进行了交流。修改后的讲义由第二作者在河北师范学院数学系继续试用三遍，并做了一些修改。原讲义是在《近世代数基础》(张禾瑞著，1978年修订本，人民教育出版社)一书的基础之上编写了三章。这次修改由第二作者增加编写域和扩域一章作为本书的第二章，并由两作者根据多次讲授伽罗华理论的经验和一些同行的意见共同进行了一次全面的修改，使其成为较完整的一本《伽罗华理论基础》教材。

修改后的《伽罗华理论基础》分为四章，前两章分别介绍群论的有关知识与域和扩域，一方面是对近世代数基础的有关内容作进一步介绍，另一方面是为第三章做好准备。第三章的主要内容是伽罗华理论的基本定理，介绍了伽罗华理论的最基本部分和主要方法，这是本书的核心。第四章是介绍应用伽罗华理论研究方程的根号解和尺规作图等问题。本书力求做到前后呼应，自成系统。

本书读者应具有高等代数和群、环、域的初步知识。在编写时，我们力求做到叙述简明易懂，推理尽可能的详尽，尽量把抽象内容具体化。有些定理的证明是根据作者多次实

践改写的，因此便于读者接受。由于本书对群和代数扩域的叙述较完整，对抽象代数的方法也给予足够的注意，因此，希望对具有一定近世代数基础的读者在学习本书后，对进一步学习和研究抽象代数方面的有关内容，能够有所裨益。

在编写本书时，主要参考以下书目：

〔1〕近世代数基础(张禾瑞著，1978年修订本，人民教育出版社)。

〔2〕近世代数(熊全淹编著，1977年第二版，上海科技出版社)。

〔3〕代数学Ⅰ(B.L范德瓦尔登著，丁石孙等人译，科学出版社)

〔4〕Basic Algebra Ⅰ(Nathan Jacobson，W.H. Freeman and Company，San Francisco，1974)。

原讲义曾参考张禾瑞教授于1954年给研究生班讲域论课的笔记，此次进行修改时，又参考了《古典数学难题与伽罗瓦理论》(徐诚浩著，复旦大学出版社)一书。

本书适合作为高等师范院校讲授伽罗华理论基础课的教材，也可供高等学校数学系函授学员和中学数学教师的参考。

在修改本书时，张禾瑞教授阅读了部分讲义原稿，提出了很好的修改意见，吴品三教授和王仰贤教授审阅了本书的最后修改稿，并提出一些宝贵意见。我们在这里对他们表示感谢。由于作者水平所限，在本书中难免有不当之处，望读者批评指正。

编　者

1987.6

目　录

第一章　群论的初步知识

为了研究伽罗华理论，需要对群论的有关内容进行讨论。本章对群的基本概念作一概括介绍，着重讨论置换群、可解群、可迁群等。

§1·1　群的基本概念

1·1·1 定义　一个具有叫做乘法的代数运算的非空集合G叫做一个群，若是以下条件被满足：

1）乘法满足结合律：即对于G中任意元素a、b、c来说，都有

$$(ab)c=a(bc)。$$

2）存在一个元素$e\in G$，对于任意$a\in G$，均有

$$ae=ea=a,$$

把具有上述性质的e，叫做G的单位元。

3）对于任意元素$a\in G$，存在一个元素$a^{-1}\in G$，具有性质

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

把具有上述性质的a^{-1}，叫做a的逆元。

不难证明，群G的单位元和G中每一个元素a的逆元是唯一的。

如果群G的代数运算还满足交换律，那么就把G叫做一个可换群或阿贝尔(Abel)群。

如果一个群G只含有限个元素，则称G为有限群，元素的个数称为G的阶，记为$|G|$.

设a是群G的一个元素，能使

$$a^m=e$$

的最小正整数m称为a的阶；若这样的m不存在，则称a是无限阶的。

1·1·2 定义 群G的一个子集H叫做G的一个子群，假如H对G的乘法来说作成一个群，记为$H\leqslant G$.

一个群G的一个非空子集H作成G的一个子群的充要条件是：

$$a,\ b\in H\Rightarrow ab^{-1}\in H$$

若群G中的每个元素都是G中某个固定元素a的整数方幂a^n，则称G是由a生成的循环群，记为$G=(a)$。此时，称a是G的一个生成元。由无限阶元生成的循环群称为无限循环群。否则，称为有限阶循环群。

显然，循环群的子群仍为循环群。

对群G的任意两个子集合A，B，规定

$$AB=\{ab\mid a\in A,\ b\in B\}$$

称为A与B的乘积，易知这种群子集的乘法满足结合律。

1·1·3 定理 设A和B是群G的子群，那么，AB是G的子群当且仅当$AB=BA$成立。

证明 假定$AB\leqslant G$，任取$ba\in BA$，由$A\leqslant G$ $B\leqslant G\Rightarrow a^{n-1}b^{-1}\in AB$，因而$(a^{-1}b^{-1})^{-1}=ba\in AB$所以$BA\subseteq AB$.再由$AB\leqslant G$，$AB$的任一元有形式$ab=((ab)^{-1})^{-1}$。但$AB$的任一元$ab$的逆元$(ab)^{-1}=b^{-1}a^{-1}\in BA$，所以$AB\subseteq BA$.故$AB=BA$，

反之，假定$AB=BA$，对任a_1b_1，$a_2b_2\in AB$，我们有

$(a_1b_1)(a_2b_2)^{-1}=a_1(b_1b_2^{-1}a_2^{-1})=a_1a_3b=ab\in AB$。所以

$$AB\leqslant G$$

1·1·4 **定义** 设H是群G的一个子群，且$x\in G$，

$$Hx=\{hx\mid h\in H\}\text{和}xH=\{xh\mid h\in H\}$$

分别称为H在G中的右陪集和左陪集。

1·1·5 **定理** 群G中子群H的任意两个右（左）陪集，或者不相交，或者恒同，且$Hx=Hy\Leftrightarrow xy^{-1}\in H$。当$G$的右陪集的个数有限时，$G$可分解为

$$G=H\cup Hx_2\cup\cdots\cup Hx_t$$

这里t代表H在G中右陪集的个数，当G的右陪集的个数无限时，我们也形式地写为$G=\bigcup_{i=1}^{\infty}Hx_i$。

H在G中的诸左陪集和诸右陪集有相同的基数ν，称ν为H在G中的指数，记为$\nu=|G:H|$。

由以上事实及H和Hx有相同基数便得

1·1·6 **Lagrange定理** 设G为有限群，$H\leqslant G$，则

$$|G|=|G:H|\cdot|H|。$$

特别地，$|H|$和$|G:H|$都是$|G|$的因子。

1·1·7 **定义** 群G的一个子群N叫做一个不变子群，如果对子G的每一元a来说，都有$Na=aN$，用$N\trianglelefteq G$表示N是G的不变子群。

1·1·8 **定理** 设G是一个群，下列三个条件等价：

1）N是G的不变子群；

2）$a\in G$，$n\in N\Rightarrow ana^{-1}\in N$；

3）对子G中的每个元素a都有$aNa^{-1}=N$。

一个群至少有两个不变子群，一个是它自身，一个是单位元群，它们称为平凡不变子群。

1·1·9 定义　不含非平凡不变子群的群，叫做单纯群，简称单群.

显然，单位元群和阶数为素数的群，都是单群. 对于可换群，我们有

1·1·10 定理　可换群G为单群的充要条件是G的阶为1或是一个素数.

证明　充分性是显然的. 现在证明必要性. 设G是无限群. 取$a\in G$，且$a\neq e$，若a的阶有限，则$H=(a)$就是G的一个非平凡不变子群. 若a的阶无限，则$H=(a^2)$就是G的一个非平凡不变子群，故无限阶的可换群皆不是单群.

设G为有限群，且设阶为合数n，取$a\in G$且$a\neq e$，若a的阶为$m<n$，则$H=(a)$就是G的一个非平凡不变子群. 若a的阶$m=n$，则$G=(a)$. 因为n为合数，可设$n=n_1n_2$，而$1<n_1<n$，$1<n_2<n$，则$H=(a^{n_1})$是G的一个阶为n_2的非平凡不变子群. 就阶为合数的有限可换群也不是单群.

非可换单群的例子，我们将在§1·2中给出.

下面我们介绍共轭类的概念.

1·1·11 定义　群G中两个元素a，b称为共轭的，记为$a\sim b$，如果在G中存在元素x使得$b=xax^{-1}$.

共轭关系具有以下性质：

1）反身性：$a\sim a$，a为G中任意元；

2）对称性：$a\sim b\Rightarrow b\sim a$；

3）传递性：$a\sim b$，$b\sim c\Rightarrow a\sim c$.

由此可见，共轭关系是一个等价关系，从而一个群可以按共轭分为共轭类.

设$a\in G$，由a所决定的共轭类记为

$$S_a=\{xax^{-1}\mid a\text{为}G\text{中一个固定元，}\forall x\in G\}.$$ 易得

1·1·8中(2)的一个等价说法：

N是G的不变子群的充分必要条件是：若$a\in N$，则$S_a\subseteq N$（S_a表示a在G中的共轭类）。

若令

$$Z_a=\{x\in G\mid xa=ax\},\quad Z=\{x\in G\mid xa=ax\ \ \forall a\in G\}$$

易见Z_a和Z都是G的子群，称Z_a为a在G中的中心化子，Z为G的中心。

1·1·12 定理 S_a所含元素的个数等于Z_a在G中的指数。

证明 令L表示Z_a在G中左陪集的集合，定义

$$f:\ S_a\to L$$

$$xax^{-1}\mapsto xZ_a$$

我们有 $xax^{-1}=yay^{-1}\Rightarrow(y^{-1}x)a=a(y^{-1}x)^{-1}\Rightarrow y^{-1}x\in Z_a\Rightarrow xZ_a=yZ_a$，所以$f$是$S_a$到$L$的一个映射，易证$f$是单射和满射，因此有

$$|S_a|=|G:Z_a|.$$

设$|G|=m$，那么$|G:Z_a|\,\big|\,m$，从而S_a的元素的个数是m的因子，因此有

1·1·13 推论 设G为有限群，其阶为m，那么每一共轭类中元素的个数是m的因子。

设群G中心Z的阶为z，除Z外G共有r个共轭类S_1，S_2，…，S_r，且S_i所含元素个数为d_i，则有

$$m=z+d_1+\cdots+d_r \tag{1}$$

易见，如果G是非交换群，则$d_i\neq 1$，且$d_i\mid m$。

如果群G的阶为p^n，这里p是素数，则称G是一个p-群。我们有以下

1·1·14 定理 设G是p-群，则G的中心$Z\neq\{e\}$。

证明 设G的阶$m=p^n$，由(1)可知m与$d_i(i=1,2,\cdots$

r)，都被p整除，所以$p|z$，从而$z>1$，即$Z\neq\{e\}$。

习　题

1．设A是群G的子集，$A^{-1}=\{a^{-1}|a\in A\}$。证明：若A，B为群G的子集，则$(AB)^{-1}=B^{-1}A^{-1}$。

2．设G是有限群，且$A\leq G$，$B\leq G$。证明：

$$|AB|=\frac{|A||B|}{|A\cap B|}$$

3．证明指数为2的子群必为不变子群。

4．设G是群，$A\trianglelefteq G$，$B\trianglelefteq G$，且$A\cap B=\{e\}$，证明：对$\forall x\in A$，$\forall y\in B$等式$xy=yx$成立。

5．设P为素数，试证：P^2元群为可换群。

§1.2　置　换　群

这一节主要介绍置换群的基本概念和n次交代群的单性。置换群是最重要的群，因为所有的有限群都可以用之表示。在研究伽罗华理论时，置换群更占有重要地位。

我们知道，一个包含n个元素的集合上的全体置换对置换乘法作成一个群叫做n次对称群，记为S_n。S_n的每一个元素叫做一个n级置换，一般记为

$$\sigma=\begin{pmatrix}1 & 2\cdots n\\ i_1 & i_2\cdots i_n\end{pmatrix},$$

容易证明，$|S_n|=n!$。

下面介绍一种简单的表示置换的方法，先约定一个记号

$$(a_1a_2\cdots a_m)=\begin{pmatrix}a_1 & a_2\cdots a_{m-1} & a_m & a_{m+1}\cdots a_n\\ a_2 & a_3\cdots a_m & a_1 & a_{m+1}\cdots a_n\end{pmatrix},\quad (m\leqslant n),$$

$(a_1a_2\cdots a_m)$叫做m-循环置换，简称m-循环。例如5级置换

$$\begin{pmatrix}1&2&3&4&5\\4&3&1&5&2\end{pmatrix}=(1\ 4\ 5\ 2\ 3),\quad \begin{pmatrix}1&2&3&4&5\\5&2&3&1&4\end{pmatrix}=(1\ 5\ 4)$$

分别是5-循环和3-循环；而$\begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}=(1\ 3\ 2)(4\ 5)$是3-循环和2-循环之积。循环$(1\ 5\ 4)$中2、3不出现，表示2和3保持不变，即$(1\ 5\ 4)=(154)(2)(3)$。

实际上，m-循环$(a_1a_2\cdots a_m)$只与元素相邻状况有关，而与哪个元素为首无关，比如$(1\ 2\ 3)=(2\ 3\ 1)$。如若两个循环$(a_1a_2\cdots a_l)$和$(b_1b_2\cdots b_m)$，没有相同的文字，则称为不相交的。不相交两循环的乘积可以交换。

例如$(1\ 3\ 2)(4\ 5)=(4\ 5)(1\ 3\ 2)$。

1·2·1 定理 任意一个n级置换，都可表成若干个不相交的循环置换的乘积。

证明 对已知置换

$$\sigma=\begin{pmatrix}1&2&3&\cdots&n\\i_1&i_2&i_3&\cdots&i_n\end{pmatrix},$$

从1开始搜索，如$1\to a_1\to a_2\to\cdots\to a_k\to 1$，则得一循环$(1a_1a_2\cdots a_k)$，如若$(1a_1a_2\cdots a_k)$包含了1，2，…，$n$的所有文字，则搜索停止。否则在余下的文字中任意确定一个，如法进行，又得一个循环。如此反复进行直到所有元素都取完为止，这样便得到若干个不相交的循环，σ就等于这些不相交的循环的乘积。除了循环次序可以任意交换外，这种表示是唯一的。

显然k-循环的阶为k，我们有

1·2·2 定理 任意置换σ的阶等于它的不相交循环置换的阶的最小公倍数。

证明　设$\sigma=\sigma_1\sigma_2\cdots\sigma_s$，$\sigma_1$，$\sigma_2$，$\cdots\sigma_s$为不相交的循环置换。因为当$i\neq j$时，$\sigma_i\sigma_j=\sigma_j\sigma_i$，于是$\sigma^n=\sigma_1^n\sigma_2^n\cdots\sigma_s^n$，所以$\sigma^{(n)}=(1)$当且仅当$\sigma_i^n=(1)$，$i=1$，$2$，$\cdots$，$s$。

设σ的阶为k，σ_1，σ_2，$\cdots$，σ_s的阶分别为k_1，k_2，$\cdots$，k_s，且k_1，k_2，$\cdots$，k_s的最小公倍数为l。现在证明，$k=l$。由以上事实，显然有$k|l$。又因为由$\sigma^k=(1)$可得$\sigma_i^k=(1)$，因而$k_i|k$，$i=1$，2，$\cdots$，s。根据整数的性质，$l|k$，所以$k=l$。

由于$(i_1i_2\cdots i_k)=(i_1i_2)(i_1i_3)\cdots(i_1i_k)$，所以每一个$n$级置换都可以表成为若干个对换的乘积，但表法不是唯一的。例如

$$\begin{pmatrix}1&2&3&4&5\\2&1&3&5&4\end{pmatrix}=(1\ 2)(4\ 5)=(1\ 2)(3\ 4)(4\ 3)(4\ 5).$$

但是，我们有

1·2·3 定理　把一个n级置换表为对换的乘积，其对换个数的奇偶性不变。

证明　设n级置换

$$\tau=\begin{pmatrix}1&2&\cdots&n\\i_1&i_2&\cdots&i_n\end{pmatrix}$$

有两种方法表成对换之积，如

$$\tau=(j_1^{(1)}j_1^{(2)})(j_2^{(1)}j_2^{(2)})\cdots(j_s^{(1)}j_s^{(2)})$$

及

$$\tau=(k_1^{(1)}k_1^{(2)})(k_2^{(1)}k_2^{(2)})\cdots(k_t^{(1)}k_t^{(2)}),$$

前者对换的个数为s，后者的个数等于t，现在作n个字母x_1，x_2，$\cdots$，x_n的范德蒙行列式

$$D=\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \cdots & \cdots & \cdots & \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix}$$

我们把置换τ看作是将D的第1列变为第i_1列，第2列变为第i_2列，…，第n列变为第i_n列，于是将置换τ施行在D上便得到

$$D^{\tau}=\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_{i_1} & x_{i_2} & \cdots & x_{i_n} \\ x_{i_1}^2 & x_{i_2}^2 & \cdots & x_{i_n}^2 \\ \cdots & \cdots & \cdots & \cdots \\ x_{i_1}^{n-1} & x_{i_2}^{n-1} & \cdots & x_{i_n}^{n-1} \end{vmatrix}$$

而把τ中每一对换(ij)看作使D中第i、j两列互换，则从τ的前一种用s个对换之积表示，可知连续施行这s个对换于D上，就使D变成$(-1)^sD$，而从τ的后一种用t个对换之积表示，又使D变为$(-1)^tD$。但这两个结果都等于D^{τ}，因因有$(-1)^sD=(-1)^tD$，由于D不恒等于零，故有$(-1)^s=(-1)^t$，即s与t有相同奇偶性。

我们把表为偶数个对换乘积的置换叫做偶置换，表为奇数个对换乘积的置换叫做奇置换。

1·2·4 **定理** S_n的所有偶置换的集合A_n，作成S_n的一个不变子群(叫做n次交代群)。

证明 A_n含有单位元，故不空；两个偶置换的乘积仍是偶置换；由于$(ij)^{-1}=(ij)$，易见偶置换的逆元仍是偶置

换，故A_n是S_n的一个子群．设α是偶置换，不论β是奇是偶，$\beta\alpha\beta^{-1}$总是偶置换，故A_n是S_n的一个不变子群．

以下我们对于不同的n详细讨论A_n．

1）当$n=2$时，偶置换只有(1)，即$A_2=\{(1)\}$，故A_2是单群．

2）当$n=3$时，偶置换有$\frac{3!}{2}$个，即$A_3=\{(1),(1\ 3\ 2),(1\ 2\ 3)\}$．由于3为素数，所以，$A_3$为单群．

3）当$n=4$时，偶置换有$\frac{4!}{2}=12$个．即

$A_4=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3),(1\ 2\ 3),(1\ 2\ 4),(1\ 3\ 2),(1\ 3\ 4),(1\ 4\ 2),(1\ 4\ 3),(2\ 3\ 4),(2\ 4\ 3)\}$．

容易证明$B_4=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$是$A_4$的一个不变子群，故$A_4$不是单群．其次，$C=\{(1),(1\ 2)(3\ 4)\}$是$B_4$的一个不变子群，故$B_4$也不是一个单群．$C$不是$A_4$的不变子群，即一个不变子群的不变子群不一定是原来群的不变子群．

B_4叫做克莱因(Klein)四元群，任一含4个元素的非循环群均与B_4同构．

4）当$n\geqslant 5$时，A_n为单群．

为了证明这个结果，我们先来证明一个引理．

1·2·5 引理 如果群A_n($n\geqslant 5$)的不变子群N含有一个3-循环，则$N=A_n$．

证明 设N含有一个3-循环，例如(1 2 3)，令

$$\gamma=\begin{pmatrix}1&2&3&4&5\cdots\\ i&j&k&l&m\cdots\end{pmatrix}$$

若γ不是偶置换，则另取$\gamma(lm)$代替γ。容易算出$\gamma^{-1}(123)\gamma=(ijk)\in N$，因此$N$包含一切3-循环。另一方面，由于$A_n$的每一元均可表为偶数个对换的乘积，而任意两个对换的乘积均可写成一个3-循环或两个3-循环的乘积：

$$(ab)(ac)=(abc),$$

$$(ab)(cd)=(ab)(ac)(ca)(cd)=(abc)(cad).$$

因之A_n的每一元均可表为若干个3-循环的乘积。由于N包含一切3-循环，故N包含一切3-循环之积，即$N\supseteq A_n$，因之$N=A_n$。

此引理对$n=3$，4亦是成立的，证明留做练习。

1·2·6 **定理** n次交代群$A_n(n\geqslant 5)$是单群。

证明 设N是A_n的一个不交于群，且$N\neq\{(1)\}$，我们要证明$N=A_n$。为此只需证明N含有一个3-循环即可。

假设N不含3-循环。考虑N中$\neq(1)$的使最多个号码保持不动的置换α。由于α是偶置换，故不能只使二个号码变动，α至少要使三个或三个以上号码变动，若α不是3-循环，则α只能有如下两种形式：

$$\text{I}\quad \alpha=(1\ 2\ 3\cdots)(\ \ )\cdots,$$

或

$$\text{II}\quad \alpha=(1\ 2)(3\ 4)\cdots.$$

在第一种情形，α至少还应使另外两个号码(例如说，4，5)变动，因α不是奇置换$(1\ 2\ 3k)$。令$\beta=(3\ 4\ 5)$，于是$\beta^{-1}\alpha\beta=\alpha_1\in N$。如果$\alpha$有I的形式，容易算出，

$$\alpha_1=(1\ 2\ 4\cdots)(\ \ )\cdots$$

如果α有II的形式，那么

$$\alpha_1=(1\ 2)(4\ 5)\cdots$$

如果α使号码$i>5$不动，则α_1也使这个号码i不动。因之，$\alpha_1\alpha^{-1}$也使i不动，$\alpha_1^{-1}\alpha\in N$。当α有I形式时，$\alpha_1\alpha^{-1}$使1不