

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.....	(1)
§ 1.1 群的基本概念	(1)
§ 1.2 置换群	(6)
§ 1.3 同态和同构定理	(14)
§ 1.4 正规群列与合成群列	(17)
§ 1.5 可解群	(23)
§ 1.6 可迁群	(28)
第二章 域、扩域.....	(32)
§ 2.1 域的基本概念	(32)
§ 2.2 有限扩域、代数扩域	(41)
§ 2.3 多项式的分裂域	(54)
§ 2.4 有限可分扩域的单纯性	(61)
§ 2.5 有限域	(66)
第三章 伽罗华理论初步.....	(73)
§ 3.1 正规扩域	(73)
§ 3.2 伽罗华群	(78)
§ 3.3 方程的伽罗华群	(85)
§ 3.4 伽罗华理论的基本定理	(93)
第四章 伽罗华理论的应用.....	(103)
§ 4.1 单位根和循环扩域	(103)
§ 4.2 方程可用根号解的充要条件	(107)
§ 4.3 不能用根号解的方程的例子	(115)
§ 4.4 三次方程和它的不可约情形	(118)
§ 4.5 尺规作图.....	(125)
§ 4.6 分圆多项式和正n边形作图	(133)
附：习题答案	(145)

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 的乘法来说作成一群,记为 $H \leq G$.

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 $AB \leq G$, 任取 $ba \in BA$, 由 $A \leq G \ B \leq G \Rightarrow a^{-1}b^{-1} \in AB$, 因而 $(a^{-1}b^{-1})^{-1} = ba \in AB$ 所以 $BA \subseteq AB$. 再由 $AB \leq G$, 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

$(a_1 b_1)(a_2 b_2)^{-1} = a_1(b_1 b_2^{-1} a_2^{-1}) = a_1 a_3 b = ab \in AB$. 所以
 $AB \leq G$

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 $Hx = Hy \iff xy^{-1} \in H$. 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, $H \leq G$, 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, 如果对于 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) 对于 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 $n = n_1 n_2$, 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. 故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

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

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

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

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

$$\begin{aligned} f: S_a &\rightarrow L \\ xax^{-1} &\mapsto xZ_a \end{aligned}$$

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 $|G : Z_a| \mid m$, 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, \dots, S_r , 且 S_i 所含元素个数为 d_i , 则有

$$(1) \quad m = z + d_1 + \dots + d_r$$

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 $d_i (i = 1, 2, \dots$

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

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

$(a_1 a_2 \cdots a_m)$ 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 $(a_1 a_2 \cdots a_m)$ 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 $(a_1 a_2 \cdots a_l)$ 和 $(b_1 b_2 \cdots b_m)$, 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 $1 \rightarrow a_1 \rightarrow a_2 \rightarrow \cdots \rightarrow a_k \rightarrow 1$, 则得一循环 $(1 a_1 a_2 \cdots a_k)$, 如若 $(1 a_1 a_2 \cdots a_k)$ 包含了 1, 2, \cdots , 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 , $\sigma_1, \sigma_2, \cdots, \sigma_s$ 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 $(i_1 i_2 \cdots i_k) = (i_1 i_2)(i_1 i_3) \cdots (i_1 i_k)$, 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

$$\tau = (j^{(\frac{1}{1})} j^{(\frac{1}{2})})(j^{(\frac{2}{1})} j^{(\frac{2}{2})}) \cdots (j^{(\frac{i}{1})} j^{(\frac{i}{2})})$$

及

$$\tau = (k^{(\frac{1}{1})} k^{(\frac{1}{2})})(k^{(\frac{2}{1})} k^{(\frac{2}{2})}) \cdots (k^{(\frac{i}{1})} k^{(\frac{i}{2})}),$$

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

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

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， \cdots ，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 $(-1)^s D$ ，而从 τ 的后一种用 t 个对换之积表示，又使 D 变为 $(-1)^t D$ 。但这两个结果都等于 D^τ ，因而有 $(-1)^s D = (-1)^t D$ ，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.

下面我们对于不同的 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 $n \geq 5$ 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 ($n \geq 5$) 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 $A_n (n \geq 5)$ 是单群.

证明 设 N 是 A_n 的一个不变子群, 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:

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

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

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 α 有I的形式, 容易算出,

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

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

动, 当 α 有 Π 形式时, $\alpha_1\alpha^{-1}$ 使1和2不动. 总之, $\alpha_1\alpha^{-1}$ 比 α 能保持更多的号码不动. 这与我们对 α 的选择相矛盾. 此矛盾说明 N 必须含有一个3-循环. 因之, $N = A_n$. 即 A_n 没有非平凡的不变子群, 故 A_n 为单群.

当 $n \geq 4$ 时, A_n 是非可换群, 这样我们就得到一批非可换的有限单群的例子.

最后, 我们介绍求一个置换的共轭置换的方法.

设 $\sigma, \tau \in S_n$, 写

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}.$$

我们可以把 τ 的第一行数字连同它的象, 作适当的排列, 将 τ 写成为如下形式

$$\tau = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ i_1' & i_2' & \cdots & i_n' \end{pmatrix}$$

于是

$$\begin{aligned} \tau^{-1}\sigma\tau &= \begin{pmatrix} j_1 & j_2 & \cdots & j_n \\ 1 & 2 & \cdots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ i_1' & i_2' & \cdots & i_n' \end{pmatrix} \\ &= \begin{pmatrix} j_1 & j_2 & \cdots & j_n \\ i_1' & i_2' & \cdots & i_n' \end{pmatrix} = \begin{pmatrix} 1' & 2' & \cdots & n' \\ i_1' & i_2' & \cdots & i_n' \end{pmatrix} \end{aligned}$$

此即

1.2.7 定理 在 S_n 中置换 σ 的共轭置换 $\tau^{-1}\sigma\tau$ 可以这样得到, 即把置换 σ 的上下两行文字同时施行置换 τ .

若将置换 σ 写为不相交的循环置换的乘积, 如

$$\beta = (k_1 k_2 \cdots k_s)(l_1 l_2 \cdots l_t) \cdots,$$

则同样可得

$$\tau^{-1}\sigma\tau = (k_1' k_2' \cdots k_s')(l_1' l_2' \cdots l_t') \cdots,$$

即把 σ 的各循环中每个数字 k 都换成 k' , 就得到 $\tau^{-1}\sigma\tau$. 这样

1.2.7 定理可以叙述为

1.2.8 定理 在置换群中, 置换 σ 的共轭置换 $\tau^{-1}\sigma\tau$ 可以这样得到, 即先把 σ 写为不相交的循环置换之积, 再将各循环置换中每个数字 k 都换成 $k\tau$ 即可.

由 σ 和 $\tau^{-1}\sigma\tau$ 的循环表示, 还可以看出它们所包含的 s -循环、 t -循环等等的个数都分别相等, 象这样的置换叫做同型的置换. 由1.2.8知二共轭置换是同型的. 反之, 设 σ 与 τ 为二同型置换, 写为循环表示应有

$$\sigma = (i_1 i_2 \cdots i_s)(j_1 j_2 \cdots j_t) \cdots$$

$$\tau = (i'_1 i'_2 \cdots i'_s)(j'_1 j'_2 \cdots j'_t) \cdots$$

此时取

$$\rho = \begin{pmatrix} i_1 i_2 \cdots i_s j_1 j_2 \cdots j_t \cdots \\ i'_1 i'_2 \cdots i'_s j'_1 j'_2 \cdots j'_t \cdots \end{pmatrix} \in S_n,$$

则由1.2.8即得 $\rho^{-1}\sigma\rho = \tau$, 即 σ 与 τ 为共轭置换, 故得

1.2.9 定理 n 次对称群中二置换 σ 和 τ 是共轭的(在 S_n 内)当且仅当它们是同型的置换.

习 题

1. 试证任一 n 阶有限群都和一个 n 次置换群同构.
2. 试证对称群 S_4 的不变子群除自身及单位元群外, 只有交代群 A_4 及克莱因四元群 B_4 .
3. 试证当 $n \neq 4$ 时, 对称群 S_n 除平凡不变子群外, 只有 A_n 是它的唯一不变子群.
4. 写出 S_5 的各共轭类元素(用循环置换表示).

§ 1.3 同态和同构定理

同态和同构是研究群的两个重要概念，这一节我们介绍同态定理和同构定理。

设 G, H 是两个群， $\varphi: x \mapsto \varphi(x)$ 是 G 到 H 内的一个映射。若对任 $x, y \in G$ ，都有

$$\varphi(xy) = \varphi(x)\varphi(y)$$

则称 φ 是 G 到 H 内的同态映射，简称同态。同态 φ 称为满同态，如果 φ 是一个满射；而同态 φ 称为同构，如果 φ 是一个满单射。满同态记为 $G \sim H$ ，同构记为 $G \cong H$ 。

如果两个群同态，则单位元对应单位元，一个元的逆元对应该元的象的逆元，子群对应子群。

1.3.1 定理 设 $N \leq G$ ， G 关于 N 的所有陪集所成集合 $G/N = \{Nx \mid x \in G\}$ ，对于群子集乘法来说作成一个群，叫做 G 关于 N 的商群。

显然， $\varphi: a \mapsto Na \quad \forall a \in G$ 是 G 到 G/N 的满同态，称此 φ 为自然同态。

假定 φ 是一个群 G 到另一个群 \overline{G} 的一个同态满射， \overline{G} 的单位元 \overline{e} 在 φ 之下的所有逆象所作成 G 的子集叫做同态满射 φ 的核。

1.3.2 定理 假定 G 和 \overline{G} 是两个群，且

$$G \sim \overline{G}$$

那么这个同态的核 N 是 G 的一个不变子群，并且

$$G/N \cong \overline{G}$$

1.3.2 定理 通常称为同态基本定理。利用上述这些性质

我们来研究群的同构定理。

下面是第一同构定理，它表示一个群中两个子群的积与它们的交之间的同构关系。

1.3.3 定理 假设 $H \trianglelefteq G$, $K \leq G$, 那么 $K \cap H \trianglelefteq K$, 并且 $KH/H \cong K/K \cap H$.

证明 因为 $G \sim G/H = \overline{G}$, 假定 K 在 \overline{G} 中的象是 \overline{K} , 则 $K \sim \overline{K}$, 并且同态核是 $K \cap H$, 故 $K \cap H$ 是 K 的不变子群, 且 $K/K \cap H \cong \overline{K}$. 又因为 $G \sim \overline{G}$ 的同态核是 H , 且在这个同态下有 $KH \sim \overline{K}$, 于是就有 $\overline{K} \cong KH/H$. 故

$$KH/H \cong K/K \cap H.$$

例如 $K = ((1\ 3\ 2\ 4))$, $H = B_4$ (克莱因四元群).

$$KH = ((1\ 2), (1\ 4)(2\ 3)), K \cap H = \{(1), (1\ 2)(3\ 4)\}$$

由计算容易得知 KH/H 及 $K/K \cap H$ 都是阶为 2 的循环群, 所以它们同构.

特别, 当 $K \cap H$ 是单位元群时, 我们即得

$$KH/H \cong K$$

也就是说, 这时我们简直可以把 H 消去.

下面是第二同构定理, 它表示两个同态群间商群的同构关系.

1.3.4 定理 假定 G, \overline{G} 是群, $G \sim \overline{G}$, $\overline{H} \trianglelefteq \overline{G}$, 那么 H 在 G 中的完全逆象 (\overline{H} 的所有元的逆象做成之集合) H 是 G 的不变子群, 并且

$$G/H \cong \overline{G}/\overline{H}$$

证明 因为 $G \sim \overline{G}$, $\overline{G} \sim \overline{G}/\overline{H}$, 所以 $G \sim \overline{G}/\overline{H}$. 由 $G \sim \overline{G}/\overline{H}$, 我们得知 G/H 的单位元在 \overline{G} 中的完全逆象是 \overline{H} . 由假设, \overline{H} 在 \overline{G} 中的完全逆象是 H , 因此 G/H 的单位元在 G 中

的完全逆象就是 H ，也就是说 $G \sim \overline{G}/\overline{H}$ 时，同态核是 H 。于是由同态基本定理， H 是 G 的不变子群，并且 $G/H \cong \overline{G}/\overline{H}$ 。

此定理显然是同态基本定理的推广，因为假如 $\overline{H} = \{\overline{e}\}$ ，那么， $\overline{G}/\overline{H} \cong \overline{G}$ ，而 H 就是 \overline{e} 的完全逆象，即 H 是 $G \sim \overline{G}$ 的核。

假如 $G \sim \overline{G}$ ， H 是 G 的不变子群， \overline{H} 是 H 在 \overline{G} 中的象，由同态对应关系，我们容易得知 \overline{H} 是 \overline{G} 的不变子群。要注意的是这时 H 不一定是 \overline{H} 的完全逆象。因此 G/H 和 $\overline{G}/\overline{H}$ 一般是不同构的，但是它们是同态的，这一点在下一节我们给出证明。

假如 K, H 是群 G 的不变子群，并且 $K \supseteq H$ ，因为 $G \sim G/H$ ，而 K 在 G/H 中的象是 K/H ，所以 K/H 是 G/H 的不变子群，又因为 K/H 在 G 中的完全逆象是 K ，由1.3.4我们有

$$G/K \cong G/H/K/H$$

这就是第二同构定理的另一种形式。

下面我们证明下节将要用到的一个定理，为此先介绍一个概念。

1.3.5 定义 不变子群 N 称为群 G 的一个极大不变子群，若是不存在 G 的不变子群 N_1 ，使 $N \subset N_1 \subset G$ 。

1.3.6 定理 设 G 是群， $H \leq G$ ， K 是 H 的一个极大不变子群，而 $N \trianglelefteq G$ 。若 $H \cap N \neq K \cap N$ ，则

$$H/K \cong H \cap N / K \cap N$$

证明 显然有 K 是 $(N \cap H)K$ 的一个子群，而 $(N \cap H)K$ 是 H 的一个不变子群。因为 K 是 H 的极大不变子群，所以， $K = (N \cap H)K$ 或 $(N \cap H)K = H$ 。若 $K = (N \cap H)K$ ，则 $N \cap K = (N \cap H)K \cap N = N \cap H$ 与 $H \cap N \neq K \cap N$ ，导致矛盾。所以，

$(N \cap H)K = H$ 。于是由第一同构定理得

$$H/K = (N \cap H)K/K \cong N \cap H/K \cap (N \cap H) = N \cap H/N \cap K$$

习 题

1. 试用第一同构定理, 证明对称群 S_4 关于 B_4 的商群与 S_3 同构。
2. 用同样的方法证明: 如果某个置换群, 不是完全由偶置换组成的, 那么它里面的偶置换组成一个指数为 2 的不变子群。
3. 设 G 是群, H, K, N 如 1.3.6 所设, 证明若 $H \cap N = K \cap N$, 则 $H/K \cong HN/KN$ 。

§ 1.4 正规群列与合成群列

在研究不是单群的群时, 常常要考虑它的不变子群。因此常常引用由不变子群及不变子群的不变子群组成的不变子群列, 这节我们就来讨论这种重要的子群列。

1.4.1 定义 群 G 的一个正规群列 (简称正规列), 是指适合下述条件的 G 的子群的有限列:

$$(1) \quad G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_{i-1} \supseteq G_i \supseteq \cdots \supseteq G_s = \{e\},$$

而 G_{i-1}/G_i 叫做正规列的因子, $i = 1, 2, \cdots, s$ 。

(1) 叫做一个无重项的正规列, 如果对于任意 i , 均有 $G_{i-1} \supsetneq G_i$ 。无重项正规列的因子个数叫做该正规列的长度。这样, 每一个无重项的正规列均有一个确定的长度, 而对有重项的正规列, 长度没有定义。注意: 无重项正规列的长度并不是群列 (1) 中的项的个数, 而是因子 G_{i-1}/G_i 的个数。

例如, $S_4 \supset A_4 \supset B_4 \supset \{(1)\}$ 是 S_4 的一个长度为 3 的正规列; $S_4 \supset A_4 \supset \{(1)\}$ 是 S_4 的一个长度为 2 的正规列。

由上面例子可以看出, 一个群的正规列, 一般来说并不

是唯一的。

设 G 是有限群， G 的正规列的每一因子均为有限群，我们说，这个事实的逆命题也是正确的。

1.4.2 定理 若 G 的正规列(1)的每一因子均为有限群。则 G 亦为有限群。并且，若 G_{i-1}/G_i 的阶为 n_i ，则 G 的阶 $n = n_1 n_2 \cdots n_s$ 。

证明 不妨假定(1)是无重项的正规列，我们对正规列的长度 s 用数学归纳法。

当 $s = 1$ 时，定理显然成立。

假定对 $s - 1$ ，定理成立。我们考虑 G_1 ，因 G_1 是有长为 $s - 1$ 的正规列，由归纳假设知 G_1 的阶为 $n_2 n_3 \cdots n_s$ 。故 G 的阶为 $n_1 n_2 \cdots n_s$ ，即定理对任意 s 均成立。

以下我们讨论正规列的同态以及完全逆象的问题。

1.4.3 定理 设 φ 是群 G 到群 \bar{G} 的一个满同态，(1)是 G 的一个正规列，则

$$(2) \quad \bar{G} = \varphi(G_0) \supseteq \cdots \supseteq \varphi(G_{i-1}) \supseteq \varphi(G_i) \supseteq \cdots \supseteq \varphi(G_s)$$

是 \bar{G} 的一个正规列，并且

$$G_{i-1}/G_i \sim \varphi(G_{i-1})/\varphi(G_i), i = 1, 2, \cdots, s.$$

证明 因 G_i 是 G_{i-1} 的不变子群，故 $\varphi(G_i)$ 是 $\varphi(G_{i-1})$ 的不变子群，由于 $G_s = \{e\}$ ，故 $\varphi(G_s) = \{\bar{e}\}$ ，即(2)确为 \bar{G} 的一个正规列。

从 G_{i-1}/G_i 中任取一元 x ，则 $x = G_i a$ ， $a \in G_{i-1}$ ，令 $\varphi_i(x) = \varphi(G_i)\varphi(a)$ ，则 $\varphi_i(x) \in \varphi(G_{i-1})/\varphi(G_i)$ ，并且，当 $G_i a = G_i b$ 时，有 $ab^{-1} \in G_i$ ，由此得， $\varphi(ab^{-1}) \in \varphi(G_i)$ ，即 $\varphi(G_i)\varphi(a) = \varphi(G_i)\varphi(b)$ ，故 φ_i 是 G_{i-1}/G_i 到 $\varphi(G_{i-1})/\varphi(G_i)$ 的一个映射。

其次, 从 $\varphi(G_{i-1})/\varphi(G_i)$ 中任取一元 y , 则 $y = \varphi(G_i) \times \varphi(a)$, $a \in G_{i-1}$, 于是, 存在 $x \in G_{i-1}/G_i$, $x = G_i a$, $\varphi_i(x) = y$. 这就是说 φ_i 是 G_{i-1}/G_i 到 $\varphi(G_{i-1})/\varphi(G_i)$ 的满射.

再次, $\varphi_i(G_i a G_i b) = \varphi_i(G_i ab) = \varphi(G_i) \varphi(ab) = \varphi(G_i) \times \varphi(a) \varphi(b) = \varphi(G_i) \varphi(a) \cdot \varphi(G_i) \varphi(b) = \varphi(G_i a) \cdot \varphi(G_i b)$. 故 φ_i 是 G_{i-1}/G_i 到 $\varphi(G_{i-1})/\varphi(G_i)$ 的满同态, 即

$$G_{i-1}/G_i \sim \varphi(G_{i-1})/\varphi(G_i).$$

1.4.4 定理 设 φ 是 G 到 \overline{G} 的满同态, 且设

(3) $\overline{G} = \overline{G}_0 \triangleright \overline{G}_1 \triangleright \cdots \triangleright \overline{G}_{i-1} \triangleright \overline{G}_i \triangleright \cdots \triangleright \overline{G}_s = \{\overline{e}\}$ 是 \overline{G} 的一个无重项的正规列, 命 $\varphi^{-1}(\overline{G}_i) = G_i$, 则有

(4) $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{i-1} \triangleright G_i \triangleright \cdots \triangleright G_s$,

并且,

$$G_{i-1}/G_i \cong \overline{G}_{i-1}/\overline{G}_i, \quad i = 1, 2, \dots, s.$$

当 $\varphi^{-1}(\overline{e}) = \{e\}$ 时 (即 φ 是同构对应), (4) 是 G 的无重项的正规列.

证明 由第二同构定理直接得到.

对于任意群 G , G 的正规列总是存在的, 例如, $G \triangleright \{e\}$ 便是, 我们把长为 1 的正规列叫做平凡正规列, 长不为 1 的正规列叫做非平凡的正规列. 容易证明下述事实:

G 有非平凡正规列的充要条件是: G 不是单群.

下面我们介绍加细正规列的概念.

1.4.5 定义 设 G 有一个无重项的正规列,

(5) $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{i-1} \triangleright G_i \triangleright \cdots \triangleright G_s = \{e\}$

若 (5) 有一个因子 G_{i-1}/G_i 不是单群, 则 G_{i-1}/G_i 有一个非平凡的正规列.

$$(6) \quad G_{i-1}/G_i = K_{i,0} \triangleright K_{i,1} \triangleright \cdots \triangleright K_{i,j-1} \triangleright K_{i,j} \triangleright \cdots \triangleright K_{i,t} = \{e\}.$$

命 φ_i 是 G_{i-1} 到 G_{i-1}/G_i 的自然同态, 则由 1.4.4 得

$$(7) \quad G_{i-1} = \varphi_i^{-1}(K_{i,0}) \triangleright \cdots \triangleright \varphi_i^{-1}(K_{i,j-1}) \triangleright \varphi_i^{-1}(K_{i,j}) \triangleright \cdots \triangleright \varphi_i^{-1}(K_{i,t}) = G_i$$

将 (7) 插入 (5), 得出 G 的一个较 (5) 更长的正规列, 称之为 (5) 的加细.

由上述事实可知, G 的一个正规列不能加细的充要条件为: 每一个因子群都是单群.

1.4.6 定义 G 的一个不能加细的无重项正规群列叫做 G 的一个合成群列 (简称合成列), 合成列的因子叫做合成因子.

例如, 在 S_4 中群列

$$S_4 \triangleright A_4 \triangleright B_4 \triangleright C = \{(1), (1\ 2)(3\ 4)\} \triangleright \{(1)\}$$

就是 S_4 的一个合成列.

注意1 并不是每一个群都有合成列, 例如, G 是整数加群, 则 G 没有合成列, 因为, 对于 G 的任一正规列 (5) 来说, $G_{i-1}/G_i \cong G_{i-1}$ 均不是单群之故.

注意2 一个群如果有合成列, 其合成列也未必是唯一的. 例如, G 是阶为 6 的循环群, 其生成元为 a , 则 G 有两个合成列:

$$(a) \triangleright (a^2) \triangleright \{e\}$$

$$(a) \triangleright (a^3) \triangleright \{e\}$$

但是可以证明: G 的任意两个合成列, 其长度必然相同. 并且, 可以适当调换合成因子的次序, 使对应因子是同构的.

1.4.7 定义 群 G 的两个合成列

$$(8) \quad G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{i-1} \triangleright G_i \triangleright \cdots \triangleright G_n = \{e\}$$

和

$$(9) \quad G = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_{i-1} \triangleright N_i \triangleright \cdots \triangleright N_s = \{e\}$$

称为同构的, 如果 $n = s$, 且存在一个在 $\{1, 2, \dots, n\}$ 上的置换 σ 使得

$$G_{i-1}/G_i \cong N_{i^\sigma-1}/N_{i^\sigma} \quad i = 1, 2, \dots, n.$$

1.4.8 Jordan-Holder 定理 如果群 G 有合成列, 那么这个群 G 的任意两个合成列是同构的.

证明 设 (8) 和 (9) 是群 G 的两个合成列, 我们对 (8) 的长度 n 用数学归纳法.

当 $n = 1$ 时, 即 $G = G_0 \triangleright G_1 = \{e\}$ 是合成列, 于是 G 为单群, 这时 G 只有唯一的一个合成列, 论断自然成立.

下面设 $n \geq 2$, 假设对于长度 $< n$ 的合成列来说, 结论成立. 区别以下两种情况讨论之.

$$(I) \quad G_1 = N_1$$

考虑 G_1 的合成列 $G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{e\}$, 它的长度为 $n-1$, 因为 $G_1 = N_1$, 所以

$G_1 = N_1 \triangleright N_2 \triangleright \cdots \triangleright N_s = \{e\}$ 也是 G_1 的合成列, 由归纳假设 $n-1 = s-1$, 因而 $n = s$ 以及存在一个在 $\{1, 2, \dots, n\}$ 上的置换 σ 使 $1^\sigma = 1$, 且

$$G_{i-1}/G_i \cong N_{i^\sigma-1}/N_{i^\sigma}$$

$$(II) \quad G_1 \neq N_1$$

令 $K_2 = G_1 \cap N_1$, 因为 G_1 和 N_1 是 G 的不变子群, 所以 $G_1 N_1$ 是 G 的不变子群, 又因 $G_1 \neq N_1$, 所以 $G_1 N_1 \supset G_1$, 因而 $G_1 N_1 = G_0$, 这样由第一同构定理知

$$G_0/G_1 = G_1 N_1/G_1 \cong N_1/G_1 \cap N_1 = N_1/K_2$$

同理 $N_0/N_1 \cong G_1/K_2$, 且

$$(10) \quad K_2 = G_0 \cap K_2 \supseteq G_1 \cap K_2 \supseteq \cdots \supseteq G_n \cap K_2 = \{e\}$$

是 K_2 的一个正规列, 因为 G_{i-1}/G_i 为单群, 故 G_i 是 G_{i-1} 的极大不变子群. 由1·3·6知, 若

$$G_{i-1} \cap K_2 \cong G_i \cap K_2,$$

则 $G_{i-1}/G_i \cong G_{i-1} \cap K_2 / G_i \cap K_2$

于是将(10)去掉重复项后, 就得到 K_2 的一个合成列, 设其为

$$(11) \quad K_2 \triangleright K_3 \triangleright \cdots \triangleright K_t = \{e\}$$

又因为 N_1/K_2 和 G_1/K_2 为单群, 这样我们就得到如下四个合成列:

$$(i) \quad G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{e\}$$

$$(ii) \quad G = G_0 \triangleright G_1 \triangleright K_2 \triangleright \cdots \triangleright K_t = \{e\}$$

$$(iii) \quad G = N_0 \triangleright N_1 \triangleright K_2 \triangleright \cdots \triangleright K_t = \{e\}$$

$$(iv) \quad G = N_0 \triangleright N_1 \triangleright N_2 \triangleright \cdots \triangleright N_s = \{e\}$$

对于(i)和(ii), 由(I)知 $n=t$, 而且存在一个置换 η , 使

$$G_{i-1}/G_i \cong K_{i^{\eta}-1}/K_{i^{\eta}}$$

这里 $K_0 = G_0$, $K_1 = G_1$. 对于(iii)和(iv)类似地可以得到 $t=s$, 而且适当调换因子的次序, 使对应因子彼此同构, 对于(ii)和(iii), 因为

$$G_0/G_1 \cong N_1/K_2 \quad N_0/N_1 \cong G_1/K_2$$

且从第三个因子开始完全相同, 所以(ii)和(iii)的因子也是彼此同构的. 于是, 我们得到 $n=s$, 且存在一个在 $\{1, 2, 3, \cdots, n\}$ 上的置换 σ , 使

$$G_{i-1}/G_i \cong N_{i^{\sigma}-1}/N_{i^{\sigma}}$$

这样情形(II)也成立.

习 题

1. 决定阶为12的循环群的所有合成列.
2. 在 S_4 中, 写出包含 B_4 以及 $(1 \ 2)$ 的最小子群 H 的所有合成列.

3. 设 G 是阶为 2^n 的循环群, 证明 G 只有一个合成列.

4. 证明: 若可换群 G 有合成列, 那么 G 是有限群.

§ 1.5 可解群

为了给第四章讨论伽罗华理论的应用做准备, 我们在这一节来介绍可解群. 可解群也是群论中一类极其重要的群.

1.5.1 定义 群 G 的一个正规列

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{i-1} \triangleright G_i \triangleright \cdots \triangleright G_s = \{e\}$$

叫做一个可解列, 如果 G_{i-1}/G_i , $i = 1, 2, \dots, s$, 都是可换群. 具有可解列的群 G 叫做一个可解群.

例1 可换群都是可解群.

例2 S_3 和 S_4 是可解群.

因为 $S_3 \triangleright A_3 \triangleright \{e\}$ 是 S_3 的一个可解列, 而 $S_4 \triangleright A_4 \triangleright B_4 \triangleright \{e\}$ 是 S_4 的一个可解列.

例3 设 G 是一个单群, 但 G 不是可换群, 则 G 不是可解群. 由此得出 A_n ($n \geq 5$)不是可解群. 后面我们将证明 S_n ($n \geq 5$)不是可解群.

设 G 为群, 对任意 $a, b \in G$, $aba^{-1}b^{-1}$ 叫做 a, b 的换位子, 群 G 中所有换位子生成的群, 叫做 G 的换位子群, 记作 $G^{(1)}$.

1.5.2 定理 设 $G^{(1)}$ 是群 G 的换位子群, 则

1) $G^{(1)}$ 是 G 的不变子群;

2) $G/G^{(1)}$ 是可换群;

3) 如果 N 是 G 的不变子群, 且 G/N 是可换群, 则 $N \supseteq G^{(1)}$.

证明 1) e 是有限个换位子的乘积: $e = eee^{-1}e^{-1}$, 故

$e \in G^{(1)}$ 。又因为

(有限个换位子的乘积)·(有限个换位子的乘积)=有限个换位子的乘积。故 $G^{(1)}$ 对 G 的乘法是封闭的。

由于 $(aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1}$ 是换位子,故有限个换位子的乘积的逆仍为有限个换位子的乘积,即 $c \in G^{(1)}$ 有 $c^{-1} \in G^{(1)}$ 。

故 $G^{(1)}$ 是 G 的子群。

设 $c \in G^{(1)}$, $g \in G$, 由于 $gcg^{-1}c^{-1} \in G^{(1)}$, $(gcg^{-1}c^{-1})c \in G^{(1)}$, 即 $gcg^{-1} \in G^{(1)}$, 所以 $G^{(1)}$ 是 G 的不变子群。

2) 任取 $aG^{(1)}$ 、 $bG^{(1)} \in G/G^{(1)}$, $a, b \in G$, 于是 $a^{-1}b^{-1}ab = c \in G^{(1)}$, $ab = bac$, 从而 $(ab)G^{(1)} = baG^{(1)}$, 即 $(aG^{(1)})(bG^{(1)}) = (bG^{(1)})(aG^{(1)})$, 所以, $G/G^{(1)}$ 是可换群。

3) 因为, G/N 是可换群, 所以,
 $(aN)(bN) = (bN)(aN)$, $(ab)N = (ba)N$, $ab \in baN$, 从而,
 $a^{-1}b^{-1}ab = n \in N$ 。又由于 N 是子群, 所以 N 包含有限个换位子的乘积, 即 $N \supseteq G^{(1)}$ 。

为了更好地刻划可解群的特征, 下面引入 G 的各级换位子群:

$G^{(1)}$ = 由 G 的一切换位子生成的群。

$G^{(2)} = (G^{(1)})^{(1)}$,

.....

$G^{(l)} = (G^{(l-1)})^{(1)}$,

.....

我们把 $G^{(l)}$ 叫做群 G 的 l 级换位子群。

于是我们有下面的

1.5.3 定理 群 G 是可解群的充分必要条件是存在一个

正整数 k 使得 $G^{(k)} = \{e\}$.

证明 设 G 是可解群, 则 G 有一个可解列

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{i-1} \triangleright G_i \triangleright \cdots \triangleright G_k = \{e\}$$

其中 G_{i-1}/G_i 都是可换群.

因为 G/G_1 可换, 知 $G_1 \supseteq G^{(1)}$, 又因 G_1/G_2 可换, 知 $G_2 \supseteq G^{(1)} \supseteq (G^{(1)})^{(1)} = G^{(2)}$. 一般我们有 $G_i \supseteq G^{(i)}$, 所以, 由 $G_k = \{e\}$, 于是有 $G^{(k)} = \{e\}$.

反之, 假如有一个正整数 k 使 $G^{(k)} = \{e\}$, 则我们得到 $G \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots \supseteq G^{(i-1)} \supseteq G^{(i)} \supseteq \cdots \supseteq G^{(k)} = \{e\}$ 其中 $G^{(i)}$ 是 $G^{(i-1)}$ 的不变子群, 并且 $G^{(i-1)}/G^{(i)}$ 是可换群, 即 G 有一个可解列, 于是 G 为可解群.

关于可解群, 我们有以下诸定理.

1.5.4 定理 1) 可解群 G 的同态象 \bar{G} 是可解群;

2) 可解群 G 的子群 H 是可解群.

证明 1) 设

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{i-1} \triangleright G_i \triangleright \cdots \triangleright G_s = \{e\}$$

是 G 的一个可解列, 则有

$$\begin{aligned} \bar{G} &= \varphi(G_0) \triangleright \varphi(G_1) \triangleright \cdots \triangleright \varphi(G_{i-1}) \triangleright \varphi(G_i) \triangleright \cdots \triangleright \varphi(G_s) \\ &= \{\bar{e}\} \end{aligned}$$

因正规列的同态象仍是正规列, 且

$G_{i-1}/G_i \sim \varphi(G_{i-1})/\varphi(G_i)$, 又由于 G_{i-1}/G_i 可换, 所以, $\varphi(G_{i-1})/\varphi(G_i)$ 也是可换群, 因而 \bar{G} 是可解群.

2) 因为 G 是可解群, 所以存在一个正整数 k 使 $G^{(k)} = \{e\}$, 又因 H 是 G 的一个子群, 所以

$H^{(1)} \subseteq G^{(1)}, H^{(2)} = (H^{(1)})^{(1)} \subseteq (G^{(1)})^{(1)} = G^{(2)}, \cdots$, 一般有 $H^{(k)} \subseteq G^{(k)} = \{e\}$, 于是 $H^{(k)} = \{e\}$, 所以 H 是可解群.

1.5.5 推论 当 $n \geq 5$ 时, S_n 不是可解群.

1.5.6 推论 可解群的正规列的每一因子是可解群.

上述结果的逆命题也是正确的. 即

1.5.7 定理 如果群 G 有一个每一因子均为可解群的正规列, 则 G 是一个可解群.

证明 设 G 的正规列

$$(1) \quad G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{i-1} \triangleright G_i \triangleright \cdots \triangleright G_r = \{e\}$$

的每一因子 G_{i-1}/G_i 均可解, 于是 G_{i-1}/G_i 有可解列

$$G_{i-1}/G_i = K_{i,0} \triangleright K_{i,1} \triangleright \cdots \triangleright K_{i,j-1} \triangleright K_{i,j} \triangleright \cdots \triangleright K_{i,r} \\ = \{\bar{e}\}$$

又 $G_{i-1} \varphi_i G_{i-1}/G_i$, 则由 1.4.4 知

$$(2) \quad G_{i-1} = \varphi_i^{-1}(K_{i,0}) \triangleright \varphi_i^{-1}(K_{i,1}) \triangleright \cdots \triangleright \varphi_i^{-1}(K_{i,j-1}) \triangleright \\ \varphi_i^{-1}(K_{i,j}) \triangleright \cdots \triangleright \varphi_i^{-1}(K_{i,r}) = G_i$$

且 $\varphi_i^{-1}(K_{i,j-1})/\varphi_i^{-1}(K_{i,j}) \cong K_{i,j-1}/K_{i,j}$, 因而, $\varphi_i^{-1}(K_{i,j-1})/\varphi_i^{-1}(K_{i,j})$ 是可换群.

这样利用 (2) 将 (1) 加细, 得到加细正规列是可解列. 故 G 是可解群.

由 1.5.7 又可得

1.5.8 推论 若 G 的不变子群 H 是可解群, 且 G/H 也是可解群, 则 G 是可解群.

证明 由题设条件, G 有正规列

$$G \triangleright H \triangleright \{e\}$$

每一因子 G/H , H 均为可解群, 由 1.5.7 知 G 为可解群.

下面我们研究一类有限群是可解群的例子. 由 1.1.14 易得

1.5.9 定理 p -群是可解群.

证明 设 p -群 G 的阶为 p^n , 今对 n 应用数学归纳法.

当 $n=1$ 时, p -群是含有 p 个元的循环群, 论断自然成立.

假设对 $<n$ 来说, p -群是可解群, 今证对 n 来说 p -群亦为可解群.

设 Z 是 G 的中心, 因为 $Z \neq \{e\}$, 则 G/Z 的阶为 p^k , 而 $k < n$, 由归纳假定, G/Z 是可解群; 又 Z 是可解群, 由 3.5.8, 知 G 为可解群.

最后, 我们证明关于有限群 G 为可解群的一个重要性质.

1.5.10 定理 设 G 为有限群, 且 G 可解, 则 G 必有一个合成列, 而这个合成列的每个因子群的阶都是素数.

证明 因为 G 可解, 则 G 有可解列

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{i-1} \triangleright G_i \triangleright \cdots \triangleright G_r = \{e\}$$

其中 G_{i-1}/G_i 是可换群, 若 G_{i-1}/G_i 的阶不是素数, 则 G_{i-1}/G_i 有真因子群 \bar{H} , 于是 $G_{i-1}/G_i \supset \bar{H} \supset \{e\}$, 利用 $G_{i-1} \varphi_i G_{i-1}/G_i$ 和 1.4.4 可以将上述可解列加细, 这样一直做下去, 必然得到因子群是阶为素数的单群, 即群 G 有一个合成列, 这个合成列的每个因子群的阶都是素数.

习 题

1. 假如 H, K 都是群 G 的子群, 并且 K 是不变子群, 如果 H, K 都是可解群, 那末 HK 也是可解群.

2. 利用第一同构定理证明可解群 G 的子群仍是可解群.

*3. 设 G 为群, 再设 H_1, H_2 是 G 的子群, 用 $[H_1, H_2]$ 表示所有 H_1 中元素 a 与 H_2 中元素 b 的换位子所生成的子群, 我们利用归纳法定义

$$G_0 = G, G_1 = [G, G_0], \dots, G_n = [G, G_{n-1}], \dots$$

显然有

$$G_0 \geq G_1 \geq \cdots \geq G_n \geq \cdots$$

若是存在一个正整数 m 使 $G_m = [G, G_{m-1}] = \{e\}$, 那么, G 叫做
幂零群.

证明: 幂零群是可解群.

§ 1.6 可 迁 群

可迁群是指 S_n 的一类特殊子群.

设 S_n 作用在集合 $M = \{a_1, a_2, \dots, a_n\}$ 上, $\alpha \in S_n$, α 可
表为

$$\alpha = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_{i_1} & a_{i_2} & \cdots & a_{i_n} \end{pmatrix}$$

我们说 a_i 经 α 作用后变为 a_{i_1} , 记为 $a_i \alpha = a_{i_1}$.

1.6.1 定义 S_n 的一个子群 G 叫做在 M 上可迁, 或称 n 次
可迁, 如果对于任意 a_i, a_j 存在 $\alpha \in G$ 使得 $a_i \alpha = a_j$.

如果群 G 在 M 上不是可迁的(非可迁群), 则集合 M 将分
解为许多可迁区, 即那样一些子集, 它们被群中的置换变成
其自身, 而在每个这样的集合上群是可迁的. 这种子集可以
这样来确定: M 中两元素 a_i 和 a_j 属于同一个子集, 当且仅当
 G 中可以找到一个置换 α 使得 $a_i \alpha = a_j$.

例1 S_n 本身显然是一个可迁群, $A_n (n > 2)$ 也是一个可
迁群. 因为, 当 $n = 2$ 时, $A_2 = \{(1)\}$. 故非可迁; 当 $n > 2$
时, 对任意 $a_i, a_j, a_i \neq a_j$, 命 $\alpha = (a_i a_j)(a_i a_k)$, $k \neq i, j$,
则 $\alpha \in A_n$ 且 $a_i \alpha = a_j$.

例2 $B_4 = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ 是四次可迁群. 而 $C = \{(1), (1\ 2)(3\ 4)\}$, 则不是四
次可迁群. 因为 C 中没有置换能将1变到3.

例3 $G = \{(1), (1\ 2)(3\ 4\ 5), (3\ 4\ 5), (1\ 2)(3\ 5\ 4),$

$(1\ 2), (3\ 5\ 4)\}$ 不是五次可迁群. 因为 G 中没有置换能将 1 变到 3.

1.6.2 定理 设 G 是 n 次可迁群, 那么 G 中所有使 a 不变的置换的全体

$$G_a = \{\sigma \in G \mid a^\sigma = a\}$$

作成 G 的一个子群(叫做关于 a 的稳定子群), 并且对任意 $\tau \in G$ 有 $G_{a^\tau} = \tau^{-1} G_a \tau$.

证明 $\sigma, \tau \in G_a$, 由 $a^{\sigma\tau} = (a^\sigma)^\tau = a^\tau = a$ 得 $\sigma\tau \in G_a$, 所以 G_a 是 G 的一个子群.

设 $\sigma, \tau \in G$, 如果, $\sigma \in G_a$, 则 $(a^\tau)^\sigma = a^\tau \Rightarrow a^{\tau\sigma\tau^{-1}} = a \Rightarrow \tau\sigma\tau^{-1} \in G_a \Rightarrow \sigma \in \tau^{-1} G_a \tau$, 故 $G_a \subseteq \tau^{-1} G_a \tau$. 将上面推导过程逆推回去可得 $\tau^{-1} G_a \tau \subseteq G_a$, 所以 $G_{a^\tau} = \tau^{-1} G_a \tau$.

1.6.3 定理 设 p 是素数, 在 p 个文字上的可迁群 G 的不变子群 $H \neq \{e\}$, 仍是 p 次可迁群.

证明 设 $\{1, 2, \dots, k\}$ 为 H 的一个可迁区. 因为 $H \neq \{e\}$, 故 $k > 1$, 于是这 k 个数字中每个数字在 H 的作用下变成为另一个数字, 而除这 k 个数字外, 其它数字不能再为这 k 个数字的象. 现在令 j 为任一数字, 因为 G 是可迁的, 故有一个置换 $\sigma \in G$ 使 $1^\sigma = j$. 由 $\sigma^{-1} H \sigma = H$ 知 $j^H = j^{\sigma^{-1} H \sigma} = 1^{H^\sigma}$. 但由于 1 在 H 的作用下变为从 1 到 k 的全部数字, 故

$$1^{H^\sigma} = \{1^\sigma, 2^\sigma, \dots, k^\sigma\}$$

因此, j 会在这 k 个数字的某一个可迁区里, 故知 $k \mid p$. 但是 p 是素数, 而 $k > 1$, 故 $k = p$, 所以 H 是 p 次可迁的.

最后我们证明第四章将要用到的一个定理.

1.6.4 定理 设 p 是素数, G 是 p 次可迁群, 且 G 含有一个对换, 则 $G = S_p$.

证明 设 $(a_1 a_2) \in G$, 命 $(a_1 a_2), (a_1 a_3), \dots, (a_1 a_i)$ 是

G 中所有含 a_1 的对换, 并命 $A = \{a_1, a_2, \dots, a_l\}$, 由于 $(a_1 a_2) \in G$, 故 $l > 1$.

首先证明 $l = p$. 若 $l < p$, 则存在 $b_1 \in \{a_1, a_2, \dots, a_p\}$, 而 $b_1 \notin A$. 因 G 可迁, 故存在 $\alpha \in G$, $a_1^\alpha = b_1$. 设

$$\alpha = \begin{pmatrix} a_1 & a_2 \cdots a_l & u_1 & u_2 \cdots u_{p-l} \\ b_1 & b_2 \cdots b_l & v_1 & v_2 \cdots v_{p-l} \end{pmatrix}$$

命 $B = \{b_1, b_2, \dots, b_l\}$ (b_1, b_2, \dots, b_l 互异), 则 $A \cap B = \emptyset$. 这是由于 $b_1 \notin A$, 若 $b_i \in A$ ($2 \leq i \leq l$) 则 $(a_1 b_i) \in G$, 由此得

$$(a_1 b_i) \alpha^{-1} (a_1 a_i) \alpha (a_1 b_i) = (a_1 b_i) \in G. \quad \text{矛盾.}$$

集合 $A \cup B$ 含有 $2l$ 个不同数字, 又皆在 $\{a_1, a_2, \dots, a_p\}$ 中, 故 $2l \leq p$. 但 p 为素数, 且 $l > 1$, 故只能是 $2l < p$, 即 $A \cup B \neq \{a_1, a_2, \dots, a_p\}$.

任取 $c_1 \notin A \cup B$, $c_1 \in \{a_1, a_2, \dots, a_p\}$. 因 G 可迁, 故存在 $\beta \in G$, $a_1^\beta = c_1$, 设

$$\beta = \begin{pmatrix} a_1 & a_2 \cdots a_l & s_1 & s_2 \cdots s_{p-l} \\ c_1 & c_2 \cdots c_l & t_1 & t_2 \cdots t_{p-l} \end{pmatrix}$$

命 $C = \{c_1, c_2, \dots, c_l\}$ (c_1, c_2, \dots, c_l 互异). 与前面证明类似, 知 $A \cap C = \emptyset$, 并且, 可证明 $B \cap C = \emptyset$. 因为已经知道 $c_1 \notin B$, 假定有 $c_i \in B$, $2 \leq i \leq l$. 设 $c_i = b_j$, 则 $a_i^\beta \alpha^{-1} = c_i^{\alpha^{-1}} = b_j^{\alpha^{-1}} = a_j$, 若 $\beta \alpha^{-1}$ 变 a_1 为不属于 A 的数字, 则 $\beta \alpha^{-1}$ 必然把 a_i 变为不属于 A 的数字 (证明与前面第一步类似), 矛盾. 故 $a_i^\beta \alpha^{-1} = a_k \in A$, 因之 $a_1^{(\beta \alpha^{-1})^\alpha} = a_i^\alpha = b_k$. 又 $a_1^{(\beta \alpha^{-1})^\alpha} = a_1^\beta = c_1$, 于是 $c_1 = b_k \in B$, 与 c_1 的取法不合, $B \cap C = \emptyset$. 于是 $A \cup B \cup C$ 含有 $3l$ 个不同数字, 同样有 $3l < p$. 如此下去, 得 $4l < p$, $5l < p$, \dots , 这是不可能的. 故 $l = p$.

其次, 可证 G 含有任一对换.

由于 $l = p$, 知 $A = \{a_1, a_2, \dots, a_p\}$, 于是知 $(a_1 a_2), (a_1 a_3), \dots, (a_1 a_p) \in G$. 因之

$$(a_i a_j) = (a_1 a_i)(a_1 a_j)(a_1 a_i) \in G$$

这样 G 含有任一对换, 但又知 S_p 由对换生成, 所以, $G = S_p$.

习 题

1. 设 G 是 S_n 的一个子群, 并且对于任意 a_i , 存在 $\alpha \in G$, 使得 $a_1^\alpha = a_i$. 证明: G 是可迁群.
2. 假如 G 是 m 次可迁群, G 的阶为 n , 试证 m 整除 n .

第二章 域、扩域

伽罗华理论是利用群论的方法来研究代数方程的根号解，而要研究代数方程的根号解，不仅需要群论的有关内容，而且还需要对域作进一步的研究。这一章主要讨论域的基本概念、扩域、有限扩域、代数扩域、多项式的分裂域和有限域等。

§ 2.1 域的基本概念

2.1.1 定义 设 R 是一个具有叫做加法和乘法的两个代数运算的集合，如果

1) R 对于加法作成交换群(通常称为加群)

2) R 的乘法满足结合律：

$$(ab)c = a(bc), \forall a, b, c \in R$$

3) 乘法关于加法满足两个分配律

$$a(b+c) = ab+ac$$

$$(b+c)a = ba+ca$$

$$\forall a, b, c \in R$$

那么称 R 对于所给的加法和乘法作成环。

如果 R 对乘法还满足交换律：

$$ab = ba, \forall a, b \in R$$

则称 R 为交换环

如果 R 中有一个元 e 对于任意 $a \in R$ 都有

$$ae = ea = a$$

则称 e 为 R 的单位元。容易证明一个环 R 如果有单位元，那么单位元是唯一的。环的单位元记为 1 。

2.1.2 定义 环 R 的一个非空子集 I 叫做一个理想子环，简称理想，如果

1) 若 $a, b \in I$ ，则 $a - b \in I$ ，

2) 若 $a \in I, r \in R$ ，则 $ra, ar \in I$ 。

如果 R 是一个有单位元 1 的交换环，在 R 中任取元 a ，那么一切 $ra, (r \in R)$ 所组成的集合

$$I = \{ra | r \in R\}$$

作成 R 的一个理想，记为 $I = (a)$ ，称为由 a 生成的主理想。

2.1.3 定义 交换环 R 称为整环，如果 R 具有单位元并且没有零因子。

例1 整数环 \mathbb{Z} 是一个整环。

例2 域 F 上一元多项式环 $F[x]$ 是一个整环。

2.1.4 定义 如果一个整环 F 的每一个非零元都有逆元，则称 F 是一个域。

由此定义可以看出来，域 F 对加法来说作成一个加群，所有非零元的集合 F^* 对乘法来说作成一个可换群。加法和乘法被分配律联系着。

例3 设 p 是素数，用 \mathbb{Z}_p 表示整数模 p 的剩余类所组成的集合：

$$\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$$

那么 \mathbb{Z}_p 对剩余类的加法和乘法作成一个域，其加法表和乘法表如下：

	$\overline{0}$	$\overline{1}$	$\overline{2}$	\cdots	$\overline{p-1}$		$\overline{0}$	$\overline{1}$	$\overline{2}$	\cdots	$\overline{p-1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	\cdots	$\overline{p-1}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	\cdots	$\overline{0}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	\cdots	$\overline{0}$	$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	\cdots	$\overline{p-1}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	\cdots	$\overline{1}$	$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	\cdots	$\overline{p-2}$
\vdots	\cdots	\cdots	\cdots	\cdots	\cdots	\vdots	\cdots	\cdots	\cdots	\cdots	\cdots
$\overline{p-1}$	$\overline{p-1}$	$\overline{0}$	$\overline{1}$	\cdots	$\overline{p-2}$	$\overline{p-1}$	$\overline{0}$	$\overline{p-1}$	$\overline{p-2}$	\cdots	$\overline{1}$

例4 令 $F[x]$ 表示域 F 上的一元多项式环, $p(x)$ 为 $F[x]$ 中一个不可约多项式, 令 $E = F[x]/(p(x))$, 而 E 中每个元具有形式: $\overline{f(x)} = f(x) + (p(x))$, 则 E 对于如下定义的加法和乘法

$$\begin{aligned} \overline{f(x)} + \overline{g(x)} &= \overline{f(x) + g(x)}, \\ \overline{f(x)} \overline{g(x)} &= \overline{f(x)g(x)}, \end{aligned} \quad \forall \overline{f(x)}, \overline{g(x)} \in E,$$

作成成一个域。

容易验证 E 对于加法和乘法作成成一个整环。因此欲证 E 是一个域只需证明 E 中非零元有逆元。事实上, 任意取 $\overline{f(x)} \in E$, 并且 $\overline{f(x)} \neq \overline{0}$, 即 $p(x) \nmid f(x)$, 由于 $p(x)$ 是不可约多项式, 所以 $(f(x), p(x)) = 1$, 于是在 $F[x]$ 中存在 $u(x)$, $v(x)$, 使得

$$f(x)u(x) + p(x)v(x) = 1$$

即

$$\overline{f(x)}\overline{u(x)} = \overline{1 - p(x)v(x)} = \overline{1}$$

由此可得

$$\overline{f(x)} \overline{u(x)} = \overline{1}$$

即

$$\overline{f(x)}^{-1} = \overline{u(x)}$$

所以 E 中非零元都有逆元，故 E 是一个域。

2.1.5 定义 如果域 E 的一个非空子集 F 对于 E 的加法和乘法作成是一个域，则称 F 为 E 的一个子域。

如果 F 是域 E 的子域，称 E 是 F 的一个扩域，记为 E/F 。

任意域都有子域，因为自身是一个子域。一个域除去自身之外，如果还有子域的话，则称其为真子域。

如何判别子域，我们有

2.1.6 定理 设 F 是域 E 的一个子集， F 含有非零元。 F 是 E 的子域的充分必要条件是

- 1) 若 $a, b \in F$ ，则 $a - b \in F$ ；
- 2) 若 $a, b \in F$ ，且 $b \neq 0$ ，则 $ab^{-1} \in F$ 。

由此即得

2.1.7 定理 设 E 为域， F 表示 E 的一切子域的交，则 F 是 E 的一个子域。

易见，这个子域不含真子域，事实上若 F 含有子域 F_1 ，则 F_1 也是 E 的子域，由 F 的构成知 $F_1 \supseteq F$ ，这与 F_1 是 F 的真子域矛盾，所以 F 不含真子域。

2.1.8 定义 不含真子域的域称为素域。

例如有理数域 \mathbb{Q} 为素域。

为了研究素域的类型，我们介绍域的特征，为此我们先证明

2.1.9 定理 任意域 F 的非零元在加群中有相同的阶。

证明 如果 F 的非零元在加群中都是无限阶元，定理成立。假设 F 的某一个非零元 a 的阶为 n ，在 F 中任取非零元 b ，则有

$$\begin{aligned}(na)b &= (a + a + \cdots + a)b = ab + \cdots + ab \\ &= a(b + b + \cdots + b) = a(nb)\end{aligned}$$

由于 $na=0$ 可得 $a(nb)=(na)b=0$. 又因为 $a\neq 0$, 所以 $nb=0$, b 的阶 $\leq a$ 的阶 n , 同理可证 a 的阶 $\leq b$ 的阶, 所以 b 的阶 $=n$.

由以上定理我们知道, 域的所有非零元在加群中的阶都等于域的单位元 1 在加群中的阶.

2.1.10 定义 域 F 的单位元 1 在 F 的加群中的阶称 F 的特征, 记为 $\text{char} F$.

设 F 是域 E 的子域, 由 F 与 E 有相同的单位元和零元, 所以我们有

2.1.11 定理 如果 F 是域 E 的子域, 则有 $\text{char} F = \text{char} E$.

2.1.12 定理 域 F 的特征或为 ∞ , 或为素数.

证明 若 F 的单位元 1 在加群中的阶是无限, 则 $\text{char} F = \infty$.

若 $\text{char} F = p$, p 为有限正整数. 如果 p 是合数, 则 $p = mn$, $1 < m < p$, $1 < n < p$, 于是

$$0 = p1 = (mn)1 = (m1)(n1)$$

因而 $m1 = 0$ 或 $n1 = 0$, 这与域的特征的定义矛盾. 所以 p 是素数.

显然, 任何数域的特征皆为 ∞ , \mathbb{Z}_p 的特征为 p .

2.1.13 定义 设 F 和 \overline{F} 是两个域, 映射 $\sigma: F \rightarrow \overline{F}$ 称为同构映射, 如果

1) σ 是满单射;

2) $(a+b)^\sigma = a^\sigma + b^\sigma$, $(ab)^\sigma = a^\sigma b^\sigma$, $\forall a, b \in F$.

如果 $\overline{F} = F$ 则称 σ 是域 F 的自同构.

为了方便, 我们把域的同构映射的符号写在 a 的右上角, 即用 a^σ 以代替 $\sigma(a)$.

设 F 是一个域, 由2.1.7和2.1.8可知, 域 F 必含有一个素域 Δ . 又由2.1.11, $\text{char}\Delta = \text{char}F$, 而 $\text{char}F$ 或为 ∞ , 或为素数. 我们将看到, Δ 的结构完全决定于它的特征. 下面分别加以讨论.

(i) 当 $\text{char}\Delta = \infty$ 时, 令

$$\Delta_1 = \{(n1)(m1)^{-1} \mid m, n \in \mathbb{Z}, 1 \text{ 是 } \Delta \text{ 的单位元}\}$$

利用2.1.6可以证明 Δ_1 是 Δ 的一个子域, 但是 Δ 是素域, 所以 $\Delta_1 = \Delta$. 如果我们定义映射

$$\sigma: \mathbb{Q} \longrightarrow \Delta$$

$$\frac{n}{m} \longmapsto (n1)(m1)^{-1}, m \neq 0 \quad \forall \frac{n}{m} \in \mathbb{Q}$$

可以验证 σ 是一个同构映射, 即 $\mathbb{Q} \cong \Delta$.

(ii) 当 $\text{char}\Delta = p$ 时, 令

$$\Delta_1 = \{0 = p \cdot 1, 1, 2 \cdot 1, \dots, (p-1) \cdot 1\}$$

这里1为 Δ 的单位元. 易证 Δ_1 是 Δ 的一个子域, 从而 $\Delta_1 = \Delta$, 我们定义映射

$$\tau: \mathbb{Z}_p \longrightarrow \Delta$$

$$\overline{i} \longmapsto i \cdot 1, i = 1, 2, \dots, p.$$

可以验证 τ 是一个同构映射, 即 $\mathbb{Z}_p \cong \Delta$.

总结以上讨论, 我们可以得到

2.1.14 定理 设 F 是一个域, 那么

1) 若 $\text{char}F = \infty$, 则 F 包含一个与有理数域同构的素域;

2) 若 $\text{char}F = p$, 则 F 包含一个与 \mathbb{Z}_p 同构的素域.

最后, 我们简要地介绍一下整环的商域.

设 R 是一个整环, 作集合

$$A = \{(a, b) \mid a, b \in R, \text{ 且 } b \neq 0\}$$

在A中定义关系 \sim 如下:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

可以证明, “ \sim ” 满足

1° 反身性: $(a, b) \sim (a, b)$

2° 对称性: 若 $(a, b) \sim (c, d)$, 则 $(c, d) \sim (a, b)$

3° 传递性: 若 $(a, b) \sim (c, d)$, $(c, d) \sim (e, f)$, 则
 $(a, b) \sim (e, f)$

事实上1° 和2° 显然成立, 只需证3°. 如果 $(a, b) \sim (c, d)$, $(c, d) \sim (e, f)$, 那么 $ad = bc$, $cf = de$, 于是 $adf = bcf = bde$, $(af - be)d = 0$, 因为R中无零因子, 而 $d \neq 0$, 所以 $af = be$, $(a, b) \sim (e, f)$, 因此 \sim 是一个等价关系.

这样, 由等价关系 \sim , 将A分成若干个等价类, 所有等价类作成一集合, 记为F. 今以 $\frac{a}{b}$ 表示 (a, b) 所在的类.

在F中定义加法和乘法:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

首先, 由于 $(a, b), (c, d) \in A$, $b \neq 0, d \neq 0$, 所以 $bd \neq 0$, 又 $ad + bc \in R$, $ac \in R$, 因而 $(ad + bc, bd), (ac, bd) \in A$. 所以上两式右端属于F.

其次证明这样定义是良好的, 即与代表选择无关.

设 $(a_1, b_1) \sim (a, b)$, $(c_1, d_1) \sim (c, d)$, 则 $a_1b = b_1a$, $c_1d = d_1c$, 于是 $a_1bd_1d = b_1ad_1d$, $c_1db_1b = d_1cb_1b$, 将此两式相加得

$$a_1bd_1d + c_1db_1b = b_1ad_1d + d_1cb_1b$$

或

$$(a_1 d_1 + c_1 b_1) b d = b_1 d_1 (a d + b c)$$

所以

$$(a_1 d_1 + c_1 b_1, b_1 d_1) \sim (a d + b c, b d)$$

即

$$\frac{a_1}{b_1} + \frac{c_1}{d_1} = \frac{a}{b} + \frac{c}{d}.$$

类似地可证

$$\frac{a_1}{b_1} \frac{c_1}{d_1} = \frac{a}{b} \frac{c}{d}.$$

F 对于加法作成加群:

$$1) \frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}.$$

$$2) \text{ 因 } \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f} \right) = \frac{a}{b} + \frac{cf + de}{df} = \frac{adf + bcf + bde}{bdf}$$

$$\left(\frac{a}{b} + \frac{c}{d} \right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{adf + bcf + bde}{bdf}$$

$$\text{故 } \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f} \right) = \left(\frac{a}{b} + \frac{c}{d} \right) + \frac{e}{f}.$$

$$3) \frac{0}{b} + \frac{c}{d} = \frac{bc}{bd} = \frac{c}{d}.$$

$$4) \frac{a}{b} + \frac{-a}{b} = \frac{0}{b}.$$

F^* 作成一個交換群:

5) 乘法滿足交換律和結合律.

6) $\frac{a}{a}$ 是單位元.

7) $\frac{a}{b}(a \neq 0)$ 的逆元是 $\frac{b}{a}$.

易验证乘法对加法适合分配律.

这样, F 作成成一个域.

在 $\frac{ac}{c} = a(c \neq 0)$ 的假定下(这样的假定是合理的), 域 F 含有 R 作为其自己的子环, 同样在 $\frac{c}{bc} = b^{-1}(c \neq 0)$ 的假定下, 域 F 是含有 R 的最小域.

按照以上方法所得到的域 F 称为整环 R 的商域. 于是有

2.1.15 定理 任何整环必存在一个商域.

例 5 有理数域 \mathbb{Q} 是整数环 \mathbb{Z} 的商域.

例 6 设 F 是域, $F[x]$ 是整环, 则 $F[x]$ 也存在一个商域, 称为一元有理分式域, 记为 $F(x)$, 且有

$$F(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x], g(x) \neq 0 \right\}$$

例 7 设 F 是域, $F[x_1, x_2, \dots, x_n]$ 是整环, 则 $F[x_1, x_2, \dots, x_n]$ 也存在一个商域, 称为 n 元有理分式域, 记为 $F(x_1, x_2, \dots, x_n)$, 且有

$$F(x_1, \dots, x_n) = \left\{ \frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)} \mid f(x_1, \dots, x_n), \right.$$

$$\left. g(x_1, \dots, x_n) \in F[x_1, \dots, x_n], g(x_1, \dots, x_n) \neq 0 \right\}$$

以上两例中的“有理”二字指的是分子分母都是多项式.

习 题

1. 令 Δ 是素域, $\text{char} \Delta = \infty$, 设 $\Delta_1 = \{(n1)(m1)^{-1} | m, n \in \mathbb{Z}, m \neq 0, 1 \text{ 是 } \Delta \text{ 的单位元}\}$, 证明 Δ_1 是 Δ 的子域.
2. 证明2.1.7定理.
3. 在特征为 p 的域中, 证明
 - 1) $(a+b)^p = a^p + b^p$;
 - 2) $(a-b)^p = a^p - b^p$.
4. 在 \mathbb{Z}_{11} 中, 计算
 - 1) $\overline{3} \times \overline{6} - \overline{4} \times \overline{8}$;
 - 2) $\overline{2} \times \overline{3}^{-1} + \overline{5} \times \overline{7}^{-1}$.
5. 证明下列数集作成域:
 - 1) $F = \{a + b\sqrt{3} | a, b \in \mathbb{Q}\}$;
 - 2) $F = \{a + bi | a, b \in \mathbb{Q}, i^2 = -1\}$.

§ 2.2 有限扩域、代数扩域

从本节开始, 我们主要研究代数扩域的结构; 特别是有限扩域的结构.

首先介绍扩域的次数.

设 E 是 F 的一个扩域, 那么对于 E 的加法和 $F \times E$ 到 E 的纯量乘法, E 作成 F 上的一个向量空间, 于是 E 作为 F 上的向量空间就有维数的概念, 我们有

2.2.1 定义 如果域 F 的一个扩域 E 作成 F 上的向量空间有有限维数 n (n 为正整数), 那么 n 叫做扩域 E 在 F 上的次数, 记作 $[E : F]$, 这时 E 叫做域 F 的有限扩域, 否则 E 叫做域 F 的一个无限扩域.

例 1 设

$$F = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

那么 F 属于实数域 \mathbb{R} , 容易证明 F 是 \mathbb{R} 的一个子域, 并且 F 是 \mathbb{Q} 的一个扩域. 由于 F 中任意元可以表为

$$a1 + b\sqrt{2}$$

进一步, 可以证明 $1, \sqrt{2}$ 在 \mathbb{Q} 上线性无关. 事实上, 假设

$$a1 + b\sqrt{2} = 0$$

这里 $a, b \in \mathbb{Q}$. 今断言 $b = 0$, 假如 $b \neq 0$, 则有 $\sqrt{2} = -\frac{a}{b}$, 而 $-\frac{a}{b}$ 是有理数, 这就导致矛盾. 于是由 $b = 0$ 即得 $a = 0$. 所以

$1, \sqrt{2}$ 是 F 在 \mathbb{Q} 上的一个基. 故 $[F : \mathbb{Q}] = 2$, 即 F 是 \mathbb{Q} 的二次扩域.

例 2 设 F 如例 1 所述, 令

$$E = \{(a + b\sqrt{2}) + (c + d\sqrt{2})i \mid a, b, c, d \in \mathbb{Q}, i^2 = -1\}$$

易证 E 是复数域 \mathbb{C} 的一个子域, 且有

$$\mathbb{Q} \subseteq F \subseteq E$$

可以证明 $1, i$ 是 E 在 F 上的一个基, 所以 $[E : F] = 2$. E 也是 \mathbb{Q} 的一个扩域, $1, \sqrt{2}, i, \sqrt{2}i$ 是 E 在 \mathbb{Q} 上的一个基, $[E : \mathbb{Q}] = 4$. 于是

$$[E : \mathbb{Q}] = [E : F][F : \mathbb{Q}]$$

这个结论对任意有限扩域是否成立呢? 回答是肯定的.

2.2.2 定理 设 E 是 F 的有限扩域, K 是 E 的有限扩域, 则 K 是 F 的有限扩域, 且有

$$[K : F] = [K : E][E : F]$$

证明 设 $[E : F] = m$, $[K : E] = n$, 而 $\alpha_1, \alpha_2, \dots, \alpha_m$ 是 E 在域 F 上的基, $\beta_1, \beta_2, \dots, \beta_n$ 是 K 在域 E 上的基. 今证

$\alpha_i \beta_j, i=1, 2, \dots, m, j=1, 2, \dots, n$
是 K 在域 F 上的基. 任取 $\alpha \in K$, 则

$$\alpha = \sum_{j=1}^n b_j \beta_j, b_j \in E$$

同样 $b_j = \sum_{i=1}^m a_{ij} \alpha_i, j=1, 2, \dots, n, a_{ij} \in F$. 所以

$$\alpha = \sum_{i=1}^m \sum_{j=1}^n a_{ij} \alpha_i \beta_j$$

即 α 可由 $\alpha_1 \beta_1, \dots, \alpha_1 \beta_n, \dots, \alpha_m \beta_1, \dots, \alpha_m \beta_n$ 线性表示.

现证 $\alpha_1 \beta_1, \dots, \alpha_1 \beta_n, \dots, \alpha_m \beta_1, \dots, \alpha_m \beta_n$ 在 F 上线性无关, 假设

$$\sum_{i=1}^m \sum_{j=1}^n a_{ij} \alpha_i \beta_j = 0, a_{ij} \in F$$

上式可写为

$$\sum_{j=1}^n \left(\sum_{i=1}^m a_{ij} \alpha_i \right) \beta_j = 0,$$

$\sum_{i=1}^m a_{ij} \alpha_i \in E, j=1, \dots, n$. 由 β_1, \dots, β_n 在 E 上线性无

关, 所以 $\sum_{i=1}^m a_{ij} \alpha_i = 0, j=1, 2, \dots, n$.

又因为 $\alpha_1, \dots, \alpha_m$ 在 F 上线性无关, 故

$$a_{ij} = 0, i=1, 2, \dots, m, j=1, 2, \dots, n$$

从而 $\alpha_1 \beta_1, \dots, \alpha_1 \beta_n, \dots, \alpha_m \beta_1, \dots, \alpha_m \beta_n$ 是 K 在 F 上的基,

于是, $[K:F] = mn$, 即

$$[K:F] = [K:E][E:F].$$

2.2.3 推论 令 F_0, F_1, \dots, F_s 都是域且 F_i 是 F_{i-1} 的有限扩域, $i=1, 2, \dots, s$, 则 F_s 是 F_0 的有限扩域, 且有

$$[F_s : F_0] = [F_s : F_{s-1}][F_{s-1} : F_{s-2}] \cdots [F_1 : F_0].$$

设 K 是 E 的扩域, E 是 F 的扩域, 则称 E 是 K 和 F 的中间域.

2·2·4 推论 设 K 是 F 的扩域, $[K : F] = n$, E 是 K 和 F 的中间域, 则 $[E : F]$ 是 n 的因子.

由2·2·4可知, 当 $[K : F] = n$ 是素数时, E 是 K 和 F 的中间域, 那么或者 $E = K$ 或者 $E = F$.

下面介绍单代数扩域的概念, 它在代数扩域理论中占有很重要的地位.

设 E 是 F 的一个扩域, α 是 E 的一个元.

2·2·5 定义 α 称为 F 上的代数元, 如果在 $F[x]$ 中存在一个非零多项式 $f(x)$ 使得 $f(\alpha) = 0$, 否则称 α 为 F 上的超越元.

例3 设 \mathbb{Q} 表示有理数域, 由于 $\sqrt{2}$ 是 $\mathbb{Q}[x]$ 中 $f(x) = x^2 - 2$ 的一个根, 所以 $\sqrt{2}$ 是 \mathbb{Q} 上的代数元.

例4 π 是实数域 \mathbb{R} 上的代数元, 但不是 \mathbb{Q} 上的代数元, 这是因为 π 不是 $\mathbb{Q}[x]$ 中任何非零多项式的根.

由此可见, 当我们说 α 是代数元还是超越元时, 必须指明是在哪个域上.

如果 α 是域 F 上的代数元, 那么在 $F[x]$ 中存在一个多项式 $f(x)$ 以 α 为根, 从而在 $F[x]$ 中有无穷个多项式以 α 为根. 这无穷个多项式中必有一个次数最低者, 我们有

2·2·6 定义 设 α 是域 F 上的一个代数元, $F[x]$ 中一个多项式 $p(x)$ 称为 α 在 F 上的极小多项式, 如果 $p(x)$ 是首项系数为1并且 $p(x)$ 是 $F[x]$ 中以 α 为根的多项式中的次数最低者.

2·2·7 定理 设 $p(x)$ 是 α 在域 F 上的极小多项式, 那么

1) $p(x)$ 是 $F[x]$ 中不可约多项式;

2) 若 $f(x) \in F[x]$, 且 $f(\alpha) = 0$, 则 $p(x) | f(x)$;

3) $p(x)$ 是唯一的.

证明 1) 由于 $p(x)$ 是 α 的极小多项式, 所以 $p(x) \neq 0$ 且 $\partial^\circ(p(x)) \geq 1$. 若 $\partial^\circ(p(x)) = 1$, 则 $p(x)$ 显然不可约. 若 $\partial^\circ(p(x)) > 1$, 假设 $p(x)$ 可约, 则 $p(x) = p_1(x)p_2(x)$, $p_1(x)$, $p_2(x)$ 均为 $F[x]$ 中的多项式, 且 $1 \leq \partial^\circ(p_1(x)) < \partial^\circ(p(x))$, $1 \leq \partial^\circ(p_2(x)) < \partial^\circ(p(x))$, 由于 $p(\alpha) = p_1(\alpha)p_2(\alpha) = 0$, 所以 $p_1(\alpha) = 0$, 或 $p_2(\alpha) = 0$, 这与 $p(x)$ 是 α 的极小多项式矛盾, 故 $p(x)$ 不可约.

2) $f(x), p(x) \in F[x]$, 且 $p(x) \neq 0$, 由多项式的带余除法可得

$$f(x) = p(x)q(x) + r(x)$$

这里或者 $r(x) = 0$ 或者 $0 \leq \partial^\circ(r(x)) < \partial^\circ(p(x))$. 我们断言 $r(x) = 0$, 如若不然, 将 α 代入上式得 $r(\alpha) = 0$, 这是不可能的. 所以 $p(x) | f(x)$.

3) 假设 $p(x)$ 与 $p_1(x)$ 都是 α 的极小多项式, 由 2) 可得

$$p(x) | p_1(x), p_1(x) | p(x)$$

又因为 $p(x)$ 与 $p_1(x)$ 的首项系数都是 1, 所以 $p_1(x) = p(x)$, 即 α 的极小多项式是唯一的.

2·2·8 推论 设 $p(x)$ 是 $F[x]$ 中首项系数为 1 的不可约多项式, 且 $p(\alpha) = 0$, 则 $p(x)$ 是 α 在 F 上的极小多项式.

证明 假设 $p_1(x)$ 是 α 在 $F[x]$ 中的极小多项式, 由 2·2·7, $p_1(x) | p(x)$, 而 $\partial^\circ(p_1(x)) \geq 1$, $p(x)$ 不可约, 且它们的首项系数都是 1, 所以 $p(x) = p_1(x)$, 从而 $p(x)$ 是 α 的极小多项式.

设 E 是域 F 的扩域, $\alpha \in E$ 并且 α 是 F 上的代数元, 考虑 E 中包含 F 与 α 的子域, 用 $F(\alpha)$ 表示一切这样子域的交. 于是 $F(\alpha)$

也是 E 的一个子域,它是 E 中包含 F 和 α 的最小子域,因而 $F(\alpha)$ 刚好包含一切形如下列的元素.

$$(1) \quad \frac{f(\alpha)}{g(\alpha)}$$

这里 $f(x), g(x) \in F[x]$, 且 $g(\alpha) \neq 0$. 一方面, 因为 $F(\alpha)$ 是包含 F 和 α 的一个子域, 它必然含有一切形式为(1)的元, 另一方面, E 中一切可以表为形式(1)的元的集合作成一个包含 F 和 α 的子域. 因此有

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f(x), g(x) \in F[x], g(\alpha) \neq 0 \right\}$$

我们称 $F(\alpha)$ 为在 F 上添加 α 得到的扩域(扩张).

2.2.9 定义 添加一个代数元 α 于域 F 所得的扩域 $F(\alpha)$ 叫做 F 的一个单代数扩域(扩张).

下面我们研究单代数扩域的存在性和结构. 首先介绍在单代数扩域的研究中起着非常重要作用的一个定理:

2.2.10 定理 设 $p(x)$ 是 $F[x]$ 中首项系数为1的不可约多项式, 则 $\overline{E} = F[x]/(p(x))$ 是一个域, 并且在与 \overline{E} 同构的一个域中 $p(x)$ 有根. 反之设域 L 是域 F 的扩域, $p(x)$ 在 L 中有根 α , 则 $F(\alpha) \cong F[x]/(p(x))$.

证明 由于 $p(x)$ 是 $F[x]$ 中不可约多项式, 由§2.1的例4知道 \overline{E} 是一个域.

在自然同态

$$\pi: F[x] \longrightarrow F[x]/(p(x))$$

之下, 令 $F^* = \overline{F}$, 于是, 映射

$$\begin{aligned} \pi|_F: F &\longrightarrow \overline{F} \\ a &\longmapsto \overline{a} \end{aligned}$$

是满射，又因为如果 $\overline{a} = \overline{b}$ ，即 $p(x) | a - b$ ，则有 $a = b$ ，所以 $\pi|_F$ 是单射， $\pi|_F$ 显然保持运算，即

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

所以 $F \cong \overline{F}$

显然 $F \cap \overline{E} = \phi$ ，今作一集合 E ：

$$E = (\overline{E} \setminus \overline{F}) \cup F$$

这里 $\overline{E} \setminus \overline{F}$ 表示 \overline{F} 在 \overline{E} 中的补集。我们定义

$$\varphi: E \longrightarrow \overline{E}$$

$$f \longmapsto \overline{f} = \begin{cases} f & \text{若 } f \in \overline{E} \setminus \overline{F}, \\ \overline{f} & \text{若 } f \in F \end{cases}, \forall f \in E$$

由于 $F \cong \overline{F}$ 且 $F \cap \overline{E} = \phi$ ，所以 φ 是满单射。

在 E 中我们如下规定加法和乘法运算：

$$f + e = h, \text{ 如果 } \overline{f} + \overline{e} = \overline{h};$$

$$fe = h, \text{ 如果 } \overline{f} \overline{e} = \overline{h}.$$

于是有

$$(f + e)^\varphi = h^\varphi = \overline{f} + \overline{e} = \overline{f + e}, (fe)^\varphi = h^\varphi = \overline{f} \overline{e} = \overline{fe}$$

因此 $E \cong \overline{E}$

令 α 是 x 在 φ 之下的原象，设

$$p(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0$$

因为 $\overline{p(x)} = \overline{0}$ ，即

$$\overline{x^n} + \overline{a_{n-1}} \overline{x^{n-1}} + \cdots + \overline{a_0} = \overline{0}$$

这里 $\overline{a_0}, \cdots, \overline{a_{n-1}} \in \overline{F}$ ，于是有

$$a^n + a_{n-1}a^{n-1} + \cdots + a_0 = 0$$

即 $p(\alpha) = 0$, 而 $\alpha \in E$.

设 L 是 F 的扩域, $\alpha \in L$, 且 $p(\alpha) = 0$, 由 2.2.8 知 $p(x)$ 是 α 在 F 上的极小多项式, 定义映射

$$\varphi: F[x] \longrightarrow L$$

$$f(x) \longmapsto f(\alpha)$$

显然 φ 是从 $F[x]$ 到 $F[\alpha] \subseteq L$ 的同态映射, 由环的同态基本定理可得

$$F[\alpha] \cong F[x]/I$$

这里 $I = \{f(x) \in F[x] \mid f(\alpha) = 0\}$. 由 2.2.7, 任取 $f(x) \in I$, 都有 $p(x) \mid f(x)$, 所以 $I = (p(x))$, 即得

$$F[\alpha] \cong F[x]/(p(x))$$

由以上的证明, 可以把 $F[\alpha]$ 的结构说得更具体一些. 令 $\partial^\circ(p(x)) = n$, 任取 $f(x) \in F[\alpha]$, 则有 $f(x) \in F[x]$, 根据多项式的带余除法,

$$f(x) = p(x)q(x) + r(x)$$

这里 $r(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. 由于 $p(\alpha) = 0$, 于是

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

即 $F[\alpha]$ 中每个元都可以表成 $1, \alpha, \cdots, \alpha^{n-1}$ 的线性组合. 我们还可以证明 $1, \alpha, \cdots, \alpha^{n-1}$ 在 F 上必线性无关. 事实上, 假设在 F 中有不全为零的元 $a_0, a_1, \cdots, a_{n-1}$, 使得

$$a_0 1 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1} = 0,$$

即在 $F[x]$ 中有非零多项式

$$g(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$$

以 α 为根, 则 $p(x) \mid g(x)$, 而 $\partial^\circ(g(x)) < \partial^\circ(p(x))$, 所以 $g(x) = 0$, 即 $a_0 = a_1 = \cdots = a_{n-1} = 0$, 这就导致矛盾, 所以

$1, \alpha, \dots, \alpha^{n-1}$ 在 F 上线性无关. 因而, $f(\alpha)$ 可以唯一地表为 $1, \alpha, \dots, \alpha^{n-1}$ 的线性组合.

2.2.11 推论 设 F 是一个域, α 是 F 上的代数元, $p(x)$ 是 α 在 F 上的极小多项式, 且 $\partial^\circ(p(x)) = n$, 那么

1) $F[\alpha]$ 中每个元可以唯一地表为

$$a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}$$

这里 $a_i \in F, i = 0, 1, 2, \dots, n-1$.

2) $F[\alpha]$ 中运算法则如下:

(i) 设 $f(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^i, g(\alpha) = \sum_{i=0}^{n-1} b_i \alpha^i$, 则

$$f(\alpha) + g(\alpha) = \sum_{i=0}^{n-1} (a_i + b_i) \alpha^i;$$

(ii) 设 $f(\alpha), g(\alpha) \in F[\alpha], f(x)g(x) = p(x)q(x) + r(x)$, 则 $f(\alpha)g(\alpha) = r(\alpha)$;

(iii) 设 $f(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^i \neq 0$, 当 $f(\alpha) \in F$, 则 $f(\alpha)^{-1} = 1/f(\alpha)$.

当 $f(\alpha) \notin F, \partial^\circ(f(x)) \geq 1$, 存在 $u(x), v(x) \in F[x]$ 使得 $f(x)u(x) + p(x)v(x) = 1$, 且 $\partial^\circ(u(x)) < \partial^\circ(p(x)), \partial^\circ(v(x)) < \partial^\circ(f(x))$, 则 $f(\alpha)^{-1} = u(\alpha)$.

2.2.12 推论 设 α 是域 F 上的代数元, 则 $F(\alpha) = F[\alpha]$.

证明 由 2.2.10, $F[\alpha]$ 是一个域, 而且 $F[\alpha]$ 包含 F 和 α , 从而 $F[\alpha] \supseteq F(\alpha)$. 又显然有 $F(\alpha) \supseteq F[\alpha]$, 所以

$$F(\alpha) = F[\alpha].$$

由 2.2.11 立得

2.2.13 推论 设 α 是域 F 上的代数元, α 在 F 上的极小多项式为 $p(x)$, 且 $\partial^\circ(p(x)) = n$, 则

1) $F(\alpha)$ 中每个元可以唯一地表为

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

这里 $a_i \in F$, $i = 0, 1, \cdots, n-1$. $1, \alpha, \cdots, \alpha^{n-1}$ 称为 $F(\alpha)$ 在 F 上的通常基.

2) $[F(\alpha) : F] = \partial^\circ(p(x))$

2.2.14 定理 设 $F(\alpha)$ 和 $F(\beta)$ 是域 F 上两个单代数扩域, 并且 α 和 β 在 F 上有相同的极小多项式 $p(x)$, 那么 $F(\alpha) \cong F(\beta)$.

证明 设 $\partial^\circ(p(x)) = n$, 那么 $F(\alpha)$ 的元可唯一地表为

$$\sum_{i=0}^{n-1} a_i \alpha^i \quad a_i \in F, i = 0, 1, \cdots, n-1$$

$F(\beta)$ 的元可唯一地表为

$$\sum_{i=0}^{n-1} a_i \beta^i \quad a_i \in F, i = 0, 1, \cdots, n-1.$$

定义

$$\varphi: F(\alpha) \longrightarrow F(\beta)$$

$$\sum_{i=0}^{n-1} a_i \alpha^i \longmapsto \sum_{i=0}^{n-1} a_i \beta^i$$

由 2.2.11 容易验证 φ 是一个同构映射, 即

$$F(\alpha) \cong F(\beta).$$

由以上讨论自然想到这样一个问题: $F(\alpha)$ 是单代数扩域, F 中的元当然是 F 上的代数元, α 也是 F 上的代数元, 那么 $F(\alpha)$ 中除去 F 和 α 外, 其余的元是否为 F 上的代数元呢? 为了回答这个问题, 需要引入以下概念.

2.2.15 定义 设 E 是域 F 的扩域, 如果 E 的每一个元都是 F 上的代数元, 那么 E 叫做 F 的一个代数扩域(扩张).

2.2.16 定理 如果 E 是 F 的有限扩域, 那么 E 是 F 的代数

扩域.

证明 设 $[E:F]=n$, 任取 $\alpha \in E$, 则

$$1, \alpha, \alpha^2, \dots, \alpha^n$$

必在 F 上线性相关, 即 F 中存在不完全为零的元 a_0, a_1, \dots, a_n 使得

$$a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$$

即 α 是 $F[x]$ 中非零多项式

$$f(x) = a_0 + a_1x + \dots + a_nx^n$$

的根, 从而 α 是 F 上的代数元, 所以 E 是 F 的代数扩域.

由2.2.13立得

2.2.17 推论 域 F 的单代数扩域 $F(\alpha)$ 是 F 的代数扩域.

既然在域 F 上添加一个代数元 α_1 得到的单代数扩域 $F(\alpha_1)$ 是代数扩域, 那么在 $F(\alpha_1)$ 上再添加 $F(\alpha_1)$ 上的代数元 α_2 得到 $F(\alpha_1)$ 上的单代数扩域 $F(\alpha_1)(\alpha_2)$. 由于 $[F(\alpha_1):F]$ 与 $[F(\alpha_1)(\alpha_2):F(\alpha_1)]$ 皆有限, 故 $[F(\alpha_1)(\alpha_2):F]$ 有限, $F(\alpha_1)(\alpha_2)$ 是 F 的代数扩域, 从而 α_2 是 F 上的代数元, 对于 $F(\alpha_2)(\alpha_1)$ 也可以作同样的讨论, 自然想到, $F(\alpha_1)(\alpha_2)$ 与 $F(\alpha_2)(\alpha_1)$ 有什么关系?

设扩域 E/F , α_1, α_2 是 F 上的代数元, $\alpha_1, \alpha_2 \in E$, 令 $F(\alpha_1, \alpha_2)$ 表示 E 中包含 F 和 α_1, α_2 的最小子域, 于是

$$F(\alpha_1, \alpha_2) = \left\{ \frac{f(\alpha_1, \alpha_2)}{g(\alpha_1, \alpha_2)} \mid f(x_1, x_2), g(x_1, x_2) \in F[x_1, x_2], g(\alpha_1, \alpha_2) \neq 0 \right\}$$

由于 $F(\alpha_1)(\alpha_2)$ 是包含 F, α_1, α_2 的域, 而 $F(\alpha_1, \alpha_2)$ 是包含 F, α_1, α_2 的最小子域, 于是 $F(\alpha_1)(\alpha_2) \supseteq F(\alpha_1, \alpha_2)$, 又因为 $F(\alpha_1, \alpha_2)$ 是包含 $F(\alpha_1)$ 与 α_2 的域而 $F(\alpha_1)(\alpha_2)$ 是包含

$F(a_1)$, a_2 的最小子域, 所以 $F(a_1, a_2) \supseteq F(a_1)(a_2)$, 这样就得到 $F(a_1, a_2) = F(a_1)(a_2)$, 同理可得

$$F(a_1, a_2) = F(a_2)(a_1), \text{ 于是}$$

$$F(a_1, a_2) = F(a_1)(a_2) = F(a_2, a_1)$$

推广这个结果可得

$$F(a_1, a_2, \dots, a_n) = F(a_{i_1})(a_{i_2}) \cdots (a_{i_n})$$

这里 i_1, i_2, \dots, i_n 是 $1, 2, \dots, n$ 的一个排列, 而

$$F(a_1, a_2, \dots, a_n) = \left\{ \frac{f(a_1, a_2, \dots, a_n)}{g(a_1, a_2, \dots, a_n)} \right\}$$

$$\left. \begin{array}{l} f(x_1, x_2, \dots, x_n), g(x_1, \dots, x_n) \in F[x_1, \dots, x_n] \\ g(a_1, a_2, \dots, a_n) \neq 0 \end{array} \right\}$$

由以上讨论, 利用2.2.3可得

2.2.18 定理 设 F 是域, a_1 是 F 上的代数元, 而 a_i 是 $F(a_1, a_2, \dots, a_{i-1})$ 上的代数元, $i = 2, \dots, n$, 则 a_2, \dots, a_n 皆为 F 上的代数元, 且 $F(a_1, a_2, \dots, a_n)$ 是 F 的代数扩域.

2.2.19 推论 设 F 是域, a_1, a_2, \dots, a_n 是 F 上的代数元, 则 $F(a_1, a_2, \dots, a_n)$ 是 F 的有限扩域, 因而是代数扩域.

上述结论, 反过来也是正确的.

2.2.20 定理 设 E 是 F 的有限扩域, 则 E 必是 F 的有限次添加代数元的扩域: $E = F(a_1, a_2, \dots, a_n)$, a_i 都是 F 上的代数元.

证明 设 $[E : F] = n$, a_1, a_2, \dots, a_n 是 E 在 F 上的基, 显然 $F(a_1, a_2, \dots, a_n) \subseteq E$. 任取 $\alpha \in E$, 则

$$\alpha = \sum_{i=1}^n a_i \alpha_i, \alpha_i \in F(a_1, a_2, \dots, a_n), \text{ 而 } E \subseteq F(a_1, a_2, \dots, a_n),$$

所以 $E = F(a_1, a_2, \dots, a_n)$.

由2.2.19可得

2.2.21 定理 设 α, β 是域 F 上的代数元, 则 $\alpha \pm \beta, \alpha\beta, \alpha\beta^{-1} (\beta \neq 0)$ 是 F 上的代数元.

由此可知, 设 E 是域 F 的一个扩域, 在 E 中 F 的全体代数元作成 E 的子域并且是 F 的代数扩域. 例如有理数域 \mathbb{Q} 上的在复数域 \mathbb{C} 中全体代数元组成集合 A 作成 \mathbb{C} 的一个子域. A 中的每个元都是 $\mathbb{Q}[x]$ 中某个非零多项式的根. A 是 \mathbb{Q} 的代数扩域. 有趣的是 A 不是 \mathbb{Q} 的有限扩域. 事实上, $\sqrt[n]{2} \in A$, n 为任意正整数, 我们有 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[n]{2}) \subseteq A, [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$, 而由 n 的任意性可知, A 不是 \mathbb{Q} 的有限扩域, 即 A 是 \mathbb{Q} 的无限扩域. 这就是说, 代数扩域是比有限扩域更广泛的一类扩域. 但是代数扩域也有类似于2.2.3的性质, 就是如下:

2.2.22 定理 设 E 是 F 的代数扩域, K 是 E 的代数扩域, 则 K 是 F 的代数扩域.

证明 设 α 是 K 中任意元, 则 α 是 $E[x]$ 中一个非零多项式 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ 的根. 由于 $a_0, a_1, \cdots, a_n \in E$, 所以它们是 F 上的代数元, 由2.2.18 $F(a_0, a_1, \cdots, a_n)$ 是 F 的有限扩域, 从而 $F(a_0, a_1, \cdots, a_n)(\alpha)$ 是 F 的有限扩域, 因此是 F 的代数扩域, α 是 F 上的代数元, 即 K 中每个元都是 F 上的代数元, E 是 F 的代数扩域.

习 题

1. 试求 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$. 并给出各扩域的一个基.

2. 设 K 是 \mathbb{Z}_p 的扩域, $[K : \mathbb{Z}_p] = n$, 试确定 K 所含元素的个数.

3. 设 \mathbb{Q} 是有理数域, α 是 $f(x) = x^3 - 6x^2 + 9x + 3$ 的实根, 试求 $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, 并将 $\alpha^4, 3\alpha^5 - \alpha^4 + 2, (\alpha + 1)^{-1}$ 用 $\mathbb{Q}(\alpha)$ 在 \mathbb{Q} 上的通常基表示出来.

4. 设 E, F 是域 K 的子域, $F \subseteq E$, 且 $[K : E] = [K : F]$, 试证

$$E \cong F.$$

5. 设 E 是 F 的有限扩域, $[E:F]=p$, p 是素数, 试证 E 是 F 的单代数扩域.

6. 设扩域 E/F , $\alpha \in E$ 是 F 上的代数元并且次数是奇数(即 $[F(\alpha):F]$ 为奇数), 试证 α^2 也是 F 上的奇数次代数元, 并且 $F(\alpha) = F(\alpha^2)$.

7. 设扩域 E/F , $\alpha, \beta \in E$, α, β 在 F 上分别是 m 次和 n 次代数元, 试证

$$(1) [K(\alpha, \beta):K] \leq mn.$$

$$(2) \text{ 若 } (m, n) = 1, \text{ 则 } [K(\alpha, \beta):K] = mn.$$

8. 设扩域 E/F , $\text{char} F \neq 2$ 并且 $[E:F]=4$. 试证存在一个满足条件 $F \subset L \subset E$ 的 F 的二次扩域 L 的充分必要条件是 $E = F(\alpha)$, 而 α 在 F 上的极小多项式是 $x^4 + ax^2 + b$.

§ 2.3 多项式的分裂域

在有限扩域的研究中, 除单代数扩域外, 多项式的分裂域也特别重要.

让我们先看一个例子.

例1 $f(x) = x^2 - 2$ 是 $\mathbb{Q}[x]$ 中的一个多项式, 因为 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约, 所以 $f(x)$ 在 $\mathbb{Q}[x]$ 中不能完全分解, 而 $f(x)$ 在 $\mathbb{Q}(\sqrt{2})$ 中能分解为一次因式的乘积:

$$f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

由于 $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ 为素数, 由2.2.4可知 $\mathbb{Q}(\sqrt{2})$ 与 \mathbb{Q} 之间的中间域只有它们自己, 因此 $\mathbb{Q}(\sqrt{2})$ 没有真子域使得 $f(x)$ 能分解为一次因式的乘积, 也就是说 $\mathbb{Q}(\sqrt{2})$ 是使得 $f(x)$ 能够分解为一次因式乘积的 \mathbb{Q} 的最小扩域, 像这样的扩

域在 $f(x)$ 的因式分解和求根中占有特殊的位置。

本节所谈及的多项式总假定首项系数为1，这是因为域上多项式的首项系数对多项式的因式分解和根都没有影响。

2.3.1 定义 设 $f(x)$ 是 $F[x]$ 中的一个 n 次多项式，域 F 的扩域 E 称为 $f(x)$ 在 F 上的分裂域，如果 $f(x)$ 在 E 中能分解成一次因式的乘积：

$$(1) \quad f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n), \quad \alpha_i \in E$$

但在 E 的任一真子域中， $f(x)$ 不能分解成一次因式的乘积。

这里“分裂”的含义指的是， $f(x)$ 能在这个域中分解成一次因式的乘积。由例1我们可以看到，同一多项式看作不同域上的多项式时分裂域可能不同，如 $f(x) = x^2 - 2$ 看作 $R[x]$ 中多项式时，其分裂域就是 R ，而看作 $Q[x]$ 中多项式时，其分裂域为 $Q(\sqrt{2})$ ，因此在谈到多项式的分裂域时必须指明是在哪个域上的分裂域。另外，不能把分裂域与在其上能够完全分解的域等同起来，例如，虽然 $Q[x]$ 中多项式 $f(x) = x^2 - 2$ 在 R 中能够完全分解，但 R 不是 $f(x)$ 的分裂域，因为 R 不是使得 $f(x)$ 分解为一次因式的乘积的 Q 的最小扩域。

由多项式的分裂域定义我们看到 $f(x)$ 的所有根 $\alpha_1, \alpha_2, \dots, \alpha_n$ 都包含在分裂域 E 中，于是

$$F \subseteq F(\alpha_1, \alpha_2, \dots, \alpha_n) \subseteq E$$

在 $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ 上 $f(x)$ 可以分解成(1)的形式，而 E 是使得 $f(x)$ 能够分解成形式(1)的 F 的最小扩域，于是

$$E = F(\alpha_1, \alpha_2, \dots, \alpha_n).$$

这样我们得到

2.3.2 定理 设 E 是域 F 上多项式 $f(x)$ 的一个分裂域，令

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_n), a_i \in E$$

那么 $E = F(a_1, a_2, \dots, a_n)$.

根据这个定理, 如果域 F 上的多项式 $f(x)$ 的分裂域 E 存在, 那么 E 恰好是把 $f(x) = 0$ 所有根添加于 F 所得到的扩域. 因此我们也把多项式的分裂域叫做方程 $f(x) = 0$ 的根域.

由 2.3.2, 如果 E 是 $f(x)$ 在 F 上的分裂域, 则 E 是 F 的有限扩域, 从而是 F 的代数扩域.

下面我们证明一个多项式的分裂域的存在性, 先通过一个例子加以说明.

例 2 设 $f(x) = x^4 - 5x^2 + 6$ 是 $\mathbb{Q}[x]$ 中的多项式, 求 $f(x)$ 在 \mathbb{Q} 上的分裂域.

解 首先在 $\mathbb{Q}[x]$ 中将 $f(x)$ 分解为不可约多项式的乘积:

$$f(x) = (x^2 - 2)(x^2 - 3)$$

由于 $x^2 - 2, x^2 - 3$ 在 \mathbb{Q} 中无根, 所以它们都是 $\mathbb{Q}[x]$ 中不可约多项式. 根据 2.2.10, 存在 \mathbb{Q} 的单代数扩域 $E = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(x^2 - 2)$, 这里 $E = \mathbb{Q}(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$. α 是 $x^2 - 2$ 的一个根, 因而包含 $x^2 - 2$ 的所有根. 而 $x^2 - 3$ 在 $E[x]$ 中仍为不可约多项式. 事实上, 若 $x^2 - 3$ 在 $E[x]$ 中可约, 则 $x^2 - 3$ 在 E 中有根, 设为 $a + b\alpha, a, b \in \mathbb{Q}$. 我们断言 a, b 全不为零 (读者自证), 于是 $(a + b\alpha)^2 - 3 = 0$, 经整理得

$$a = \frac{3 - a^2 - 2b^2}{2ab}$$

从而 $a \in \mathbb{Q}$, 这与 $a \notin \mathbb{Q}$ 矛盾. 因此 $x^2 - 3$ 在 E 上不可约. 再利用 2.2.10, 可作出 E 的单代数扩域 $L, L = E(\beta) \cong E[x]/(x^2 - 3)$, 这里 $E(\beta) = \{(a + b\alpha) + (c + d\alpha)\beta \mid a, b, c, d \in \mathbb{Q}\}$, β 是 $x^2 - 3$ 的根, 从而 L 包含 $x^2 - 3$ 的两个根. 于是 L 含 $f(x)$ 的所有根, 且 $[L : \mathbb{Q}] = 4$. 由以上证明知, L 是包含 $f(x)$ 的

所有根的 \mathbb{Q} 的最小扩域, L 是 $f(x)$ 在 \mathbb{Q} 上的分裂域.

将例2的方法推广到一般情形, 便得到

2.3.3 定理 设 F 是一个域. $F[x]$ 中任一 $n(n \geq 1)$ 次多项式 $f(x)$ 一定存在 $f(x)$ 在 F 上的分裂域.

证明 当 $n=1$ 时, F 即是 $f(x)$ 在 F 上的分裂域.

当 $n \geq 2$ 时, 首先把 $f(x)$ 在 $F[x]$ 中分解为不可约因式的乘积:

$$f(x) = p_1(x)p_2(x)\cdots p_s(x)$$

作 F 的单代数扩域 $F(\alpha_1)$, 使 α_1 在 F 上的极小多项式为 $p_1(x)$.

在 $F(\alpha_1)$ 上, 把 $f(x)$ 分解为不可约因式的乘积:

$$f(x) = (x - \alpha_1)\varphi_2(x)\cdots\varphi_s(x)$$

再作 $F(\alpha_1)$ 的单代数扩域 $F(\alpha_1)(\alpha_2) = F(\alpha_1, \alpha_2)$, 使 α_2 在 $F(\alpha_1)$ 上的极小多项式是 $\varphi_2(x)$.

按照这种方法逐步做下去, 最后得到

$$E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

且多项式 $f(x)$ 在 E 上能分解成一次因式的乘积:

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$$

由2.3.2知, E 是 $f(x)$ 在 F 上的一个分裂域.

2.3.3解决了域 F 上一个多项式的分裂域的存在性, 但是一个多项式可能由于使用方法不同而得到不同的分裂域, 那么它们在同构的意义下是否唯一呢? 为了解决这个问题需要同构开拓的概念.

2.3.4 定义 设 E 和 \overline{E} 分别是域 F 和 \overline{F} 的两个扩张, σ 是域 F 和 \overline{F} 间的同构映射. 如果 σ' 是 E 与 \overline{E} 间的同构映射, 使得

$$a^{\sigma'} = a^{\sigma}, \quad \forall a \in F$$

则 σ' 是 σ 的同构开拓.

设

$$\sigma: F \longrightarrow \overline{F}$$

$$a \longmapsto \overline{a}$$

是域 F 与 \overline{F} 间的同构映射。设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

是 $F[x]$ 中多项式, 那么 $\overline{F}[x]$ 中多项式

$$\overline{f}(x) = \overline{a_n} x^n + \overline{a_{n-1}} x^{n-1} + \cdots + \overline{a_1} x + \overline{a_0}$$

称为 $f(x)$ 在 σ 之下的对应多项式, 而 $\overline{f}(x)$ 也称为 $f(x)$ 在 σ 之下的对应多项式。

容易验证, 映射

$$f(x) \longmapsto \overline{f}(x), \quad \forall f(x) \in F[x]$$

是 $F[x]$ 与 $\overline{F}[x]$ 间的同构映射。此即

2.3.5 引理 设 F, \overline{F} 为域且 $F \cong \overline{F}$, 则

$$F[x] \cong \overline{F}[x].$$

2.3.6 定理 设 F, \overline{F} 为域且 $F \cong \overline{F}$, $p(x)$ 是 $F[x]$ 中不可约多项式, 则 $p(x)$ 对应多项式 $\overline{p}(x)$ 为 $\overline{F}[x]$ 中不可约多项式。又设 $F(\alpha)$ 和 $\overline{F}(\overline{\alpha})$ 分别是 F 和 \overline{F} 的单扩域, 满足条件 $p(\alpha) = 0$ 和 $\overline{p}(\overline{\alpha}) = 0$, 则 $F(\alpha) \cong \overline{F}(\overline{\alpha})$ 可以是 $F \cong \overline{F}$ 的同构开拓, 它将 α 映为 $\overline{\alpha}$ 。

证明 先证 $\overline{p}(x)$ 在 $\overline{F}[x]$ 中不可约。事实上, 假设 $\overline{p}(x)$ 在 $\overline{F}[x]$ 中是可约的:

$\overline{p}(x) = \overline{p}_1(x) \overline{p}_2(x)$, 其中 $\partial^\circ(\overline{p}_1(x)), \partial^\circ(\overline{p}_2(x)) < \partial^\circ(\overline{p}(x))$, $\overline{p}_1(x)$ 与 $\overline{p}_2(x)$ 在 σ 之下对应 $F[x]$ 中多项式为

$p_1(x), p_2(x)$, 在 $F[x]$ 中有

$p(x) = p_1(x)p_2(x)$, 其中 $\partial^\circ(p_1(x)), \partial^\circ(p_2(x)) < \partial^\circ(p(x))$. 这与 $p(x)$ 在 $F[x]$ 中不可约矛盾.

假设 $\sigma: F \longrightarrow \overline{F}, a \longmapsto \overline{a}$ 是 F 与 \overline{F} 间的同构映射.

设 $\partial^\circ(p(x)) = n$, 则 $\partial^\circ(\overline{p(x)}) = n$. 于是 $F(\alpha)$ 中的元可唯一地表为

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

$\overline{F}(\overline{\alpha})$ 中的元可唯一地表为

$$\overline{a_0} + \overline{a_1}\overline{\alpha} + \cdots + \overline{a_{n-1}}\overline{\alpha}^{n-1}$$

定义

$$\sigma': F(\alpha) \longrightarrow \overline{F}(\overline{\alpha})$$

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \longmapsto \overline{a_0} + \overline{a_1}\overline{\alpha} + \cdots + \overline{a_{n-1}}\overline{\alpha}^{n-1}$$

易证 σ' 是 $F(\alpha)$ 与 $\overline{F}(\overline{\alpha})$ 间的满单射. 并且

$$(2) \quad \alpha^{\sigma'} = (0 + 1\alpha)^{\sigma'} = \overline{0} + \overline{1}\overline{\alpha} = \overline{\alpha}.$$

$$(3) \quad a^{\sigma'} = \overline{a} = a^\sigma, \quad \forall a \in F.$$

又因为 $F(\alpha)$ 与 $\overline{F}(\overline{\alpha})$ 元素的运算, 除了横线之外是完全一样的, 因而 σ' 是 $F(\alpha)$ 与 $\overline{F}(\overline{\alpha})$ 间的同构映射, 且由 (3), σ' 是 σ 的一个同构开拓, 且有 $\alpha^{\sigma'} = \overline{\alpha}$.

2.3.7 定理 设 F, \overline{F} 是域, 且有 $F \cong \overline{F}$, $f(x) \in F[x]$, $\overline{f(x)}$ 是 $\overline{F}[x]$ 中在 σ 之下与 $f(x)$ 对应的多项式, 则 $f(x)$ 在 F 上的分裂域与 $\overline{f(x)}$ 在 \overline{F} 上的分裂域同构, 并且这个同构映射是 σ 的同构开拓.

证明 设 $f(x)$ 在 F 上分解成不可约因式之积:

$$f(x) = p_1(x)p_2(x)\cdots p_r(x)$$

如果在 σ 之下, $p_1(x), p_2(x), \dots, p_r(x)$ 分别对应 $\overline{p_1}(x), \overline{p_2}(x), \dots, \overline{p_r}(x)$, 则有

$$\overline{f}(x) = \overline{p_1}(x) \overline{p_2}(x) \cdots \overline{p_r}(x)$$

是 $\overline{f}(x)$ 在 \overline{F} 上的不可约因式分解. 不妨设 α_1 与 $\overline{\alpha_1}$ 分别是 $p_1(x)$ 与 $\overline{p_1}(x)$ 的根, 由2·3·6, σ 可以开拓成 $F(\alpha_1)$ 与 $\overline{F}(\overline{\alpha_1})$ 的同构映射 σ_1 , 并且有 $\alpha_1^{\sigma_1} = \overline{\alpha_1}$

在 $F(\alpha_1)$ 上的 $f(x)$ 的不可约因式分解为

$$f(x) = (x - \alpha_1) \varphi_2(x) \cdots \varphi_s(x)$$

在 σ_1 之下, $\varphi_2(x), \dots, \varphi_s(x)$ 分别对应 $\overline{\varphi_2}(x), \dots, \overline{\varphi_s}(x)$, 则有

$$\overline{f}(x) = (x - \overline{\alpha_1}) \overline{\varphi_2}(x) \cdots \overline{\varphi_s}(x)$$

是 $\overline{f}(x)$ 在 $\overline{F}(\overline{\alpha_1})$ 上的不可约因式分解. 于是可令 α_2 和 $\overline{\alpha_2}$ 分别为 $\varphi_2(x)$ 与 $\overline{\varphi_2}(x)$ 的根. 再由2·3·6, $F(\alpha_1)$ 与 $\overline{F}(\overline{\alpha_1})$ 的同构映射 σ_1 可以开拓成 $F(\alpha_1, \alpha_2)$ 与 $\overline{F}(\overline{\alpha_1}, \overline{\alpha_2})$ 的同构映射 σ_2 , 并且 $\alpha_2^{\sigma_2} = \overline{\alpha_2}$.

如此继续下去, 便得到 σ 的同构开拓 σ' :

$$F(\alpha_1, \alpha_2, \dots, \alpha_n) \cong \overline{F}(\overline{\alpha_1}, \overline{\alpha_2}, \dots, \overline{\alpha_n})$$

并且 $\alpha_i^{\sigma'} = \overline{\alpha_i}$, $i = 1, 2, \dots, n$.

特别地, 当 $F = \overline{F}$, σ 为恒等自同构时我们有

2·3·8 定理 $F[x]$ 中任一多项式 $f(x)$ 在 F 上的任意两个分裂域都同构, 且使 F 的元素保持不变.

习 题

1. 设 Q 为有理数域, $f(x) = x^3 - 2$ 是 $Q[x]$ 中的多项式, 求 $f(x)$ 在 Q 上的分裂域 L 和 $[L : Q]$.

2. 求证: 域 F 上的一个 n 次多项式在 F 上的分裂域关于 F 的次数至多是 $n!$.

3. 设 $f(x) = x^p - 1$, p 为素数, E 为 $f(x)$ 在 Q 上的分裂域, 求证 $[E : Q] = p - 1$.

4. 设 $p_1(x), p_2(x), \dots, p_s(x)$ 是域 F 上 s 个首项系数为1的不可约多项式, 求证存在 F 的有限扩域 $F(\alpha_1, \alpha_2, \dots, \alpha_s)$, 其中 α_i 在 F 上的极小多项式是 $p_i(x)$, $i = 1, 2, \dots, s$.

§ 2.4 有限可分扩域的单纯性

本节我们利用一个多项式的分裂域理论研究一种特殊类型的有限扩域. 关于有限扩域, § 2.2 给出一个很好的结果: E 是域 F 的有限扩域, 当且仅当 $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$, 其中 $\alpha_1, \alpha_2, \dots, \alpha_n$ 为 F 上的代数元. 然而这类扩域的结构还远未解决, 但是这类扩域的一种特殊情形, 即单代数扩域的结构问题已经得到彻底解决. 自然, 我们会提出这样的问题: 对于域 F 的一般的有限扩域 E , 能否选择一个适当的元素 β , 使得

$$E = F(\alpha_1, \alpha_2, \dots, \alpha_n) = F(\beta)$$

这样就可以使很多问题的研究简单化. 我们还是先从一个具体问题谈起.

例如, 在 § 2.3 例 2 中, $f(x) = x^4 - 5x + 6$ 在 Q 上的分裂域 $L = Q(\sqrt{2}, \sqrt{3})$, 不难看出

$$(1) \quad Q \subseteq Q(\sqrt{2} + \sqrt{3}) \subseteq Q(\sqrt{2}, \sqrt{3}).$$

如果令 $x = \sqrt{2} + \sqrt{3}$, 通过实际计算可得 $x^4 - 10x^2 + 1 = 0$, 即 $\sqrt{2} + \sqrt{3}$ 是 $Q[x]$ 中的多项式 $p(x) = x^4 - 10x^2 + 1$ 的一个根. 我们说 $p(x)$ 是 $Q[x]$ 中不可约多项式. 事实上, 多项式 $p(x)$ 在 $Q(\sqrt{2}, \sqrt{3})$ 中可以分解为 $p(x) = (x - \sqrt{2} -$

$\sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3})$,
 易见, $p(x)$ 的每一次因式及每次取两个因式的积都不是有理系数多项式, 故 $p(x)$ 是 $\mathbb{Q}[x]$ 上不可约多项式. 由 $2 \cdot 2 \cdot 8$,
 $p(x)$ 为 $\sqrt{2} + \sqrt{3}$ 在 \mathbb{Q} 上的极小多项式. $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$, 而由例 2, $[L : \mathbb{Q}] = 4$, 再考虑到 (1), $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. 也就是说, \mathbb{Q} 的有限扩域 $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 是一个添加 $\sqrt{2} + \sqrt{3}$ 于 \mathbb{Q} 的单代数扩域.

为了研究一般情形, 我们引入如下概念.

2.4.1 定义 设 E 是 F 的一个代数扩域, $\alpha \in E$. 如果 α 在 F 上的极小多项式没有重根, 则称 α 是 F 上的一个可分元. 如果 E 中每一个元都是 F 上的可分元, 那么称 E 为 F 的一个可分扩域, 否则称 E 为 F 的一个不可分扩域.

例 1 $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 是 \mathbb{Q} 的可分扩域. 事实上 $\sqrt{2}, \sqrt{3}$ 在 \mathbb{Q} 上的极小多项式分别为 $x^2 - 2$ 和 $x^2 - 3$, 因为数域上的不可约多项式都没有重根 (指在多项式的分裂域中), 所以 $x^2 - 2$ 和 $x^2 - 3$ 没有重根, 故 $\sqrt{2}, \sqrt{3}$ 都是 \mathbb{Q} 上的可分元. 又 $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 中每个元都是 \mathbb{Q} 上的代数元, 于是每一个元在 \mathbb{Q} 上都有一个极小多项式, 并且每个极小多项式都没有重根, 所以 $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 中每个元都是 \mathbb{Q} 上的可分元. 故 $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 是 \mathbb{Q} 上的可分扩域.

由前面的讨论, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, 这个结论可否推广到一般情形, 回答是肯定的. 我们首先把数域上不可约多项式没有重根的结果加以推广.

2.4.2 定理 设 F 是一个域, $\text{char } F = \infty$, $f(x)$ 是 $F[x]$ 中的一个不可约多项式, 则 $f(x)$ 没有重根.

证明 $f(x)$ 有重根当且仅当 $f(x)$ 与它的导数 $f'(x)$ 在

$F[x]$ 中有次数 ≥ 1 的公因式. 由于 $f(x)$ 不可约, 因此这个条件只有在 $f'(x)=0$ 时才能被满足. 设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

则

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1$$

假设 $f(x)$ 有重根, 则 $f'(x)=0$, 由于 $\text{char } F = \infty$, 所以必有

$$a_n = a_{n-1} = \cdots = a_1 = 0$$

于是 $f(x) = a_0$, 这与 $f(x)$ 不可约矛盾. 故 $f(x)$ 没有重根.

由 2.4.1 立得

2.4.3 推论 特征为 ∞ 的域上任何代数扩域都是可分扩域.

利用分裂域的理论可以证明如下重要的结论.

2.4.4 定理 设 F 是域, $\text{char } F = \infty$, 那么域 F 的任一有限扩域是单代数扩域.

证明 设 E 是 F 的有限扩域, 根据 2.2.20, $E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$, $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是 F 上的代数元.

我们用数学归纳法来证明. 先考虑添加两个元素的情形: $E = F(\alpha, \beta)$, α, β 是 F 上的代数元. 由 2.4.3, E 是 F 的可分扩域. 令 $f(x), g(x)$ 分别是 α, β 在 F 上的极小多项式. 作多项式 $f(x)g(x)$ 在 E 上的分裂域 L , 在 L 上有

$$(2) \quad f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_s)$$

$$(3) \quad g(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_t)$$

这里 $\alpha_1 = \alpha, \beta_1 = \beta$.

在 F 中任意选定某个非零元 c 使得

$$(4) \quad c \neq \frac{\alpha - \alpha_i}{\beta_i - \beta}, \quad \forall i = 2, \cdots, s, \quad \forall j = 2, \cdots, t$$

由于 β 是 F 上的可分元, 所以 $\beta_i - \beta \neq 0$, 又由于 $\frac{\alpha - \alpha_i}{\beta_i - \beta}$ 这种

元最多有 $(s-1)(t-1)$ 个, 而 F 有无限多个元, 所以这样的 c 可以取到. 令

$$\theta = \alpha + c\beta$$

由于 $c \in F$, 所以 $F(\theta) \subseteq F(\alpha, \beta)$. 欲证 $F(\theta) = F(\alpha, \beta)$, 只需证 $F(\theta) \supseteq F(\alpha, \beta)$. 为此作多项式

$$h(x) = f(\theta - cx) \in F(\theta)[x]$$

这里 $f(\theta - cx)$ 表示把 $f(x)$ 中的文字 x 换成 $\theta - cx$ 而得到的新多项式. 因为 $F(\theta) \subseteq L$, 所以 $h(x) \in L[x]$. 由(2)有

$$\begin{aligned} (5) \quad h(x) &= (\theta - cx - \alpha_1)(\theta - cx - \alpha_2) \cdots (\theta - cx - \alpha_s) \\ &= (-1)^s [c(x - \beta_1)] [c(x - \beta_1) - (\alpha_1 - \alpha_2)] \\ &\quad \cdots [c(x - \beta_1) - (\alpha_1 - \alpha_s)] \end{aligned}$$

显然 $h(\beta_1) = 0$, 由于 c 的取法可知, $h(\beta_j) \neq 0$, $j = 2, \dots, t$, 又由于 $\alpha_1, \dots, \alpha_s$ 互不相同, β_1, \dots, β_t 也互不相同, 比较(3)和(5)知, β 是 $h(x)$ 与 $g(x)$ 的唯一的公根, 因此 $x - \beta$ 是 $h(x)$ 与 $g(x)$ 在 $L[x]$ 中的最大公因式. 又因为 L 是 $F(\theta)$ 的扩域, 所以 $h(x)$ 与 $g(x)$ 在 $F(\theta)$ 上的最大公因式也是 $x - \beta$, 从而 $\beta \in F(\theta)$, 而 $\alpha = \theta - c\beta$, $c \in F$, 所以 $\alpha \in F(\theta)$, 故 $F(\alpha, \beta) \subseteq F(\theta)$. 于是 $F(\theta) = F(\alpha, \beta)$.

假定在 $n-1$ 时定理成立. 于是可令

$$F(\alpha_1, \alpha_2, \dots, \alpha_{n-1}) = F(\alpha),$$

那么在 n 时,

$$\begin{aligned} F(\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \alpha_n) &= F(\alpha_1, \alpha_2, \dots, \alpha_{n-1})(\alpha_n) \\ &= F(\alpha)(\alpha_n) = F(\alpha, \alpha_n) = F(\theta). \end{aligned}$$

这就是说, 在 n 时定理也成立. 于是定理得证.

与2.4.4的证明方法完全类似, 可得如下

2.4.5 定理 设 F 是一个含有无限个元素的域, $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ 是 F 的有限扩张, 而 $\alpha_1, \alpha_2, \dots, \alpha_n$ 都是 F

上的可分元, 则 E 是 F 的一个单代数扩张.

由 2.4.4 立得

2.4.6 定理 设 F 是一个域, $\text{char} F = \infty$, 则 $F[x]$ 中的任一 n 次多项式 $f(x)$ 在 F 上的分裂域 $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$ 是单代数扩域, 即

$$E = F(\alpha_1, \alpha_2, \dots, \alpha_n) = F(\theta).$$

这里 $\alpha_1, \alpha_2, \dots, \alpha_n$ 为 $f(x)$ 的根.

2.4.4 的证明也告诉我们对于 α, β 如何求 c , 当 c 求出后便得到了 θ . 特别, 对 α, β 若能求到 $c = 1$ (在很多情况下可以取到), 则必有 $F(\alpha, \beta) = F(\alpha + \beta)$, 例如, 我们所做过的, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, 经验证取 $c = 1$ 完全满足条件(4).

对于特征为 p 的域的代数扩域确实有可分扩域和不可分扩域. 限于本教材所讨论的内容, 这方面问题就不做进一步讨论了.

习 题

1. 求证有理数域 \mathbb{Q} 上多项式 $f(x) = x^4 + 1$ 在 \mathbb{Q} 上的分裂域是一个单代数 $\mathbb{Q}(\alpha)$, 其中 α 是 $f(x)$ 的一个根.

2. 设 \mathbb{Q} 为有理数域.

(1) 求 θ , 使得 $\mathbb{Q}(\sqrt{3}, \sqrt[3]{2}) = \mathbb{Q}(\theta)$

(2) 求 θ , 使 $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$, 其中 α 是 $x^2 + x + 1$ 的根, β 是 $x^2 + 4$ 的根

3. 在 $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ 中, 用 $\sqrt{2} + \sqrt{3}$ 将 $\sqrt{2}$ 和 $\sqrt{3}$ 在 \mathbb{Q} 上表示出来.

4. 设域 F 的所有扩域都是可分的, 求证 F 的任意代数扩域的所有扩域也是可分的.

§ 2.5 有 限 域

有限域是一类很重要的域，这一节我们来讨论有限域的结构。

2.5.1 定义 一个只含有限个元素的域称为有限域。

例如， \mathbb{Z}_p 是有限域，从而特征为 p 的素域皆为有限域。

有限域 E 的特征一定是一个素数 p 。如若不然， E 的特征为 ∞ ，则 E 包含一个与有理数域 \mathbb{Q} 同构的素域 Δ ，而 Δ 含有无限多个元，这与 E 的元素个数有限相矛盾。

这样，关于有限域所含元的个数，我们有

2.5.2 定理 有限域 E 中元素个数是其特征的正整数方幂。

证明 设 $\text{char} E = p$ ， E 所含素域为 Δ ，根据 2.1.14， $\Delta \cong \mathbb{Z}_p$ ，因而 Δ 含有 p 个元素。 E 是 Δ 的有限扩域，设 $[E : \Delta] = n$ ，则 E 中每个元可唯一地表示：

$$a_1 \alpha_1 + a_2 \alpha_2 + \cdots + a_n \alpha_n$$

这里 $a_1, a_2, \dots, a_n \in \Delta$ ， $\alpha_1, \alpha_2, \dots, \alpha_n$ 是 E 在 Δ 上的一个基。由于每个 a_i 可以独立地取 Δ 中 p 个不同元素，所以 E 中共有 p^n 个不同的元。

2.5.3 定理 设 E 是有限域， $\text{char} E = p$ ， E 所含素域为 Δ ， E 有 $q = p^n$ 个元，则 E 是多项式

$$x^q - x$$

在 Δ 上的分裂域。

证明 因为 E 含有 q 个元，所以 E 的乘法群 E^* 的阶为 $q - 1$ 。从而

$$a^{q-1} = 1, a \in E^*$$

这里 1 为 E 的单位元。又因为 $0^q = 0$, 所以

$$a^q = a, a \in E$$

也就是说, E 中每个元都是 Δ 上多项式

$$x^q - x$$

的根。因此, 若用 a_1, a_2, \dots, a_q 表示 E 的元, 则在 $E[x]$ 里

$$x^q - x = (x - a_1)(x - a_2) \cdots (x - a_q)$$

于是 $x^q - x$ 在 Δ 上的分裂域 L 为

$$L = \Delta(a_1, a_2, \dots, a_q)$$

显然 $\Delta \subseteq L \subseteq E$, 又有 $E \subseteq L$, 所以

$$E = \Delta(a_1, a_2, \dots, a_q)$$

即 E 是多项式 $x^q - x$ 在 Δ 上的分裂域。

利用一个多项式的分裂域的唯一性, 可以证明

2·5·4 定理 两个元素个数相等的有限域必同构。

证明 设 E_1 和 E_2 是两个有限域, 它们所含的元素个数分别为 $p_1^{n_1}$ 和 $p_2^{n_2}$, p_1 和 p_2 为素数, 由于 $p_1^{n_1} = p_2^{n_2}$, 所以 $p_1 = p_2$, 从而 $n_1 = n_2$ 。这样 E_1 和 E_2 所含的素域同构。 E_1 和 E_2 分别是多项式 $x^{p_1^{n_1}} - x$ 在两个同构的素域上的分裂域, 因此 $E_1 \cong E_2$ 。

由此可见, 元素个数相同的有限域在同构意义下是唯一的。

由 2·4·4 知道, 特征为 ∞ 的域上的一个多项式的分裂域都是单代数扩域, 既然有限域都是它所含素域上的多项式 $x^q - x$ (q 为有限域的元的个数) 的分裂域, 那么有限域是否为所含素域的单代数扩域呢? 为了回答这个问题, 我们需要研究有限域的非零元所作成的乘法群的一个重要性质。为此, 先考虑有限交换群的一个性质。

设 G 是一个有限交换群, 则 G 中每个元的阶皆有限。故 G

中的元的阶必有最大的,不妨设为 $a \in G$, a 的阶为 s ,且 G 的任意元 x 的阶不超过 s ,我们断言, G 中任意元的阶必定整除 s .事实上,设 $b \in G$, b 的阶为 t ,则必有 $t \leq s$,假如 $t \nmid s$,则存在素数 p 使得:

$$s = p^k r_1, t = p^l r_2, (p, r_1 r_2) = 1 \text{ 且 } l > k$$

于是 a^{p^k} 的阶是 r_1 , b^{r_2} 的阶是 p^l ,但 $(p^l, r_1) = 1$,所以 $a^{p^k} b^{r_2}$ 的阶为 $p^l r_1 > s$,这说明 G 中还有元 $a^{p^k} b^{r_2}$ 的阶大于 s ,这与 s 为 G 中元的阶的最大者矛盾,所以 $t \mid s$.故得

2.5.5 引理 有限交换群中每个元的阶必为其元素的阶数中的最大者之因数.

由2.5.5,就有

2.5.6 定理 设 E 是有限域,则 E 的非零元作成的乘法群 E^* 是循环群.

证明 设 E 所含元的个数为 q ,则 E^* 的阶为 $q-1$, E^* 是有限交换群,令 m 是 G 的元的阶中的最大者,由2.5.5,对于任意 $a_i \in E^*$ 都有

$$a_i^m = 1$$

即 E^* 中所有元都是 $E[x]$ 中多项式 $x^m - 1$ 的根,这就说明 $x^m - 1$ 在 E 中至少有 $q-1$ 个不同的根.从而 $q-1 \leq m$,而 m 为群 E^* 中某个元的阶,又 $m \leq q-1$,于是 $m = q-1$,这就是说 E^* 中有一元 a 它的阶是 $q-1$,即 $E^* = (a)$, E^* 是一个循环群.

由2.5.3和2.5.6立得

2.5.7 定理 一个有限域 E 是它的素域 Δ 的一个单代数扩域.

证明 因为 E 的乘法群 E^* 是循环群,所以 E^* 由一个元 a 生成,即 $E^* = (a)$,于是 $E = \Delta(a)$.

根据2.5.7的证明得到,任何有限域 E 是它的素域 Δ 添加

循环群 E^* 的生成元而得到的单代数扩域。但反之不真。

由 2.2.10, $E = \Delta(\alpha) \cong \Delta[x]/(\varphi(x))$, 这里 $\varphi(x)$ 是 $\Delta[x]$ 中首项系数为 1 (1 为 Δ 的单位元) 的不可约多项式且 $\varphi(\alpha) = 0$ 。又因为 α 是 Δ 上多项式 $x^{p^n} - x$ 的根, 根据 2.2.7, $\varphi(x) | (x^{p^n} - x)$ 。由此得

2.5.8 推论 设 $\varphi(x)$ 为 $\Delta[x]$ 的 n 次不可约多项式, 这里 Δ 是特征为 p 的素域, 则 $\varphi(x) | (x^{p^n} - x)$ 。

为证明有限域的存在, 我们先来研究 $\Delta[x]$ 中不可约多项式的一些性质。

2.5.9 引理 设 Δ 是特征为 p 的素域, 则 $\Delta[x]$ 中多项式 $x^{p^n-1} - 1$ 不可能有次数大于 n 的不可约多项式为其因式。

证明 设 $g(x)$ (不妨设其首项系数为 1) 是 $\Delta[x]$ 中一个 r 次不可约多项式且 $r > n$ 。则 $\Delta[x]/(g(x))$ 是含 p^r 个元的有限域, 记 $E = \Delta[x]/(g(x))$ 。

假设 $g(x) | x^{p^n-1} - 1$, 则 $x^{p^n-1} - 1 = \overline{0}$, 即 $x^{p^n-1} = \overline{1}$, $x^{p^n} = \overline{x}$ 。由 2.5.3, 任一 $a \in \Delta$, 则有 $a^p = a$ 。 E 中任一元可唯一表示为

$$a_0 \overline{1} + a_1 \overline{x} + \cdots + a_{r-1} \overline{x}^{r-1} \quad a_i \in \Delta$$

而

$$\begin{aligned} & (a_0 \overline{1} + a_1 \overline{x} + \cdots + a_{r-1} \overline{x}^{r-1})^{p^n} \\ &= a_0^{p^n} \overline{1}^{p^n} + a_1^{p^n} \overline{x}^{p^n} + \cdots + a_{r-1}^{p^n} (\overline{x}^{r-1})^{p^n} \\ &= a_0 \overline{1} + a_1 \overline{x} + \cdots + a_{r-1} \overline{x}^{r-1} \end{aligned}$$

这就是说 E 中任一元 a 都有 $a^{p^n} = a$, 故 $a \neq 0$ 时, $a^{p^n-1} = 1$, 即 E^* 的每个元的阶 $\leq p^n - 1$ 。但由 $n < r$ 可得 $p^n - 1 < p^r - 1$, 由此推出 E^* 设有 $p^r - 1$ 阶元, 即 E^* 非循环群, 这与 2.5.6 的结果

矛盾。因此 $\Delta[x]$ 的多项式 $x^{p^n-1}-1$ 不可能有次数大于 n 的不可约多项式为其因式。

2·5·10 引理 对任意素数 p ，不论 n 为任何自然数， $\Delta[x]$ 恒有 n 次不可约多项式，这里 Δ 是特征为 p 的素域。

证明 当 $n=1$ 时， $x-a(a \in \Delta)$ 显然为 $\Delta[x]$ 中一次不可约多项式。此时定理成立。

下面假定 $n>1$ 。

我们考查 $\Delta[x]$ 中 $x^{p^t-1}-1$ 的次数 $<n$ 的不可约多项式。令 $t<n$ ，设 $g_1(x), \dots, g_s(x)$ 是 $\Delta[x]$ 中首项系数为1且彼此互异的 t 次不可约多项式的全体，由2·5·8， $g_i(x)|(x^{p^t-1}-1)$ ， $i=1, 2, \dots, s$ 。但要除掉 $t=1$ 时及这时某唯一的 $g_i(x)=x$ 这个例外情况。而且当 $i \neq j$ 时 $(g_i(x), g_j(x))=1$ ，所以 $\prod_{i=1}^s g_i(x)|(x^{p^t-1}-1)$ 。故在 $t>1$ 有

$$\partial^\circ(g_1(x) \cdots g_s(x)) = \sum_{i=1}^s \partial^\circ(g_i(x)) \leq p^t - 1$$

由于 $p \nmid p^t - 1$ ，所以 $x^{p^t-1}-1$ 无重因式，故在 $x^{p^n-1}-1$ 的不可约因式的分解中，次数小于 n 的一切不可约因式的次数的和最多等于

$$\begin{aligned} & p + (p^2 - 1) + (p^3 - 1) + \cdots + (p^{n-1} - 1) \\ &= (1 + p + p^2 + \cdots + p^{n-1}) - (n - 1) \\ &= \frac{p^n - 1}{p - 1} - (n - 1) < \frac{p^n - 1}{p - 1} \leq p^n - 1 \end{aligned}$$

即小于 $x^{p^n-1}-1$ 的次数，故 $x^{p^n-1}-1$ 的不可约因式中必有次数大于或等于 n 的不可约多项式。但由2·5·9， $x^{p^n-1}-1$ 没有次数大于 n 的不可约因式。因此 $x^{p^n-1}-1$ 一定有次数等于 n 的不可约因式，即 $\Delta[x]$ 必有 n 次不可约多项式。

由此即得

2·5·11 定理 设 Δ 是特征为 p 的素域, 而 $q = p^n (n \geq 1)$, 那么在 $\Delta[x]$ 中必存在一个 n 次不可约多项式 $\varphi(x)$, 因而 $\Delta[x]/(\varphi(x))$ 即为含有 q 个元的有限域.

此即为有限域的存在定理.

由2·5·11和2·5·4 我们得到如下结论, 任意给定一个素数 p 和正整数 n , 必存在一个恰含 p^n 个元的有限域, 而且在同构意义下是唯一的.

当然有限域的存在性定理也可以利用一个多项式的分裂域的存在定理得到, 这里不再叙述了.

解决含有 p^n 个元的域的存在性关键是在 $\Delta[x]$ 中必有 n 次不可约多项式. 上面只说了存在性, 如何去找呢? 任何一次多项式当然是不可约的, 因此关键是怎样去找 $n(>1)$ 次的不可约多项式.

由2·5·8, n 次不可约多项式必整除 $x^{p^n} - x$, 而当 $n > 1$, 易得 n 次不可约多项式必整除 $x^{p^n-1} - 1$, 而由2·5·10的证明中又知, $x^{p^n-1} - 1$ 至少必有一个 n 次不可约因式, 于是这就告诉我们, n 次不可约多项式永远可在 $x^{p^n-1} - 1$ 的不可约因式中找到.

例1 求作含 2^2 个元的域.

解 设 Δ 是特征为2的素域, 为方便计, 令 $\Delta = \{0, 1\}$.

在 $\Delta[x]$ 中求 $x^{2^2-1} - 1 = x^3 - 1$ 的二次不可约因式. 在 $\Delta[x]$ 中 $x^3 - 1$ 分解为:

$$x^3 - 1 = (x - 1)(x^2 + x + 1)$$

而 $x^3 - 1$ 又必有一个二次不可约多项式. 故 $x^2 + x + 1$ 即为 $\Delta[x]$ 中一个二次不可约多项式. 于是 $\Delta[x]/(x^2 + x + 1)$ 就是含 2^2 个元的域. 由2·2·10的证明

$$\begin{aligned}\Delta[x]/(x^2 + x + 1) &= \{a\overline{1} + b\overline{x} \mid a, b \in \Delta\} \\ &= \{\overline{0}, \overline{1}, \overline{x}, \overline{1+x}\}\end{aligned}$$

它的加法表和乘法表如下:

	$\overline{0}$	$\overline{1}$	\overline{x}	$\overline{1+x}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	\overline{x}	$\overline{1+x}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{1+x}$	\overline{x}
\overline{x}	\overline{x}	$\overline{1+x}$	$\overline{0}$	$\overline{1}$
$\overline{1+x}$	$\overline{1+x}$	\overline{x}	$\overline{1}$	$\overline{0}$

	$\overline{0}$	$\overline{1}$	\overline{x}	$\overline{1+x}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	\overline{x}	$\overline{1+x}$
\overline{x}	$\overline{0}$	\overline{x}	$\overline{1+x}$	$\overline{1}$
$\overline{1+x}$	$\overline{0}$	$\overline{1+x}$	$\overline{1}$	\overline{x}

由 § 2.2 可得 $E = \Delta(\alpha) \cong \Delta[x]/(x^2 + x + 1)$, $E \supseteq \Delta$, α 为 $x^2 + x + 1$ 的根, 则

$$E = \{a + b\alpha \mid a, b \in \Delta\}$$

E 的加法表和乘法表与 $\Delta[x]/(x^2 + x + 1)$ 完全相同(不计元素的表示形式).

习 题

1. 设 F 是一个有限域, 且 $F = \Delta(\alpha)$, α 是否必须是 F^* 的一个生成元?
2. 试作特征为 3 的含有 9 个元的有限域, 并写出它的加法表和乘法表.
3. 设 E 是一个含有 p^n 个元的有限域, 求证对于 n 的每个因数 $m > 0$, 存在并且只存在 E 的一个有 p^m 个元的子域 F .

第三章 伽罗华理论初步

本章先介绍正规扩域。然后引入正规扩域的同构群的概念，使域与群发生映射关系。最后在这个基础上介绍伽罗华理论的基本定理。这个定理主要在一个域的若干扩域与一个群的若干子群间建立一种映射，根据这种映射，可以由群的某些性质推测域的某些性质，反之亦然，它在代数中有很多应用。

为了讨论简便起见，从本章开始，我们只对特征为 ∞ 的域进行讨论。

§ 3.1 正规扩域

正规扩域和多项式的分裂域有着密切的关系，它是伽罗华理论的主要研究对象之一。为了研究正规扩域，我们先研究一个多项式的分裂域的一个重要性质。看一个具体例子。

设 Q 是有理数域，当添加 $p(x) = x^2 - 2$ 的一个根 $\sqrt{2}$ 于 Q 而得到 Q 的单代数扩域 $Q(\sqrt{2})$ 时，不难看出， $-\sqrt{2}$ 也含于其中，这就是说 $p(x)$ 在 $Q(\sqrt{2})$ 上可分解为一次因式的乘积：

$$p(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}),$$

那么 $Q(\sqrt{2})$ 对于 Q 上其他的不可约多项式是否也有这样的性质呢？回答是肯定的。设 $f(x)$ （不妨假定首项系数为

1) 是 \mathbb{Q} 上任意一个不可约多项式, 今证明 $f(x)$ 只要在 $\mathbb{Q}(\sqrt{2})$ 中有一个根, $f(x)$ 的所有根就含于 $\mathbb{Q}(\sqrt{2})$. 我们说 $f(x)$ 的次数不能大于 2, 否则, 设 $\mathbb{Q}(\sqrt{2})$ 含 $f(x)$ 的根为 α , 由 $\partial^\circ(f(x)) > 2$ 可得, $[\mathbb{Q}(\alpha) : \mathbb{Q}] > 2$. 但是, 由 $\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}(\alpha)$ 可知, $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, 这是一个矛盾. 因之, $\partial^\circ(f(x)) \leq 2$. 当 $\partial^\circ(f(x)) = 1$ 时, 显然 $\mathbb{Q}(\sqrt{2})$ 含有 $f(x)$ 的所有根; 当 $\partial^\circ(f(x)) = 2$ 时, $2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}(\alpha)]2$, 所以 $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\alpha)$, $\alpha \in \mathbb{Q}(\sqrt{2})$, 于是在 $\mathbb{Q}(\sqrt{2})$ 上有 $f(x) = (x - \alpha)f_1(x)$, $\partial^\circ(f_1(x)) = 1$, 因此 $f(x)$ 的另一个根也含于 $\mathbb{Q}(\sqrt{2})$ 中, 故 $\mathbb{Q}(\sqrt{2})$ 含有 $f(x)$ 的全部根.

实际上, 一个多项式的分裂域就有 $\mathbb{Q}(\sqrt{2})$ 这样的性质, 我们有

3.1.1 定理 令 E 是多项式 $f(x)$ 在 F 上的分裂域, 而 β 是 E 中任意元, 那么 β 在 F 上的极小多项式在 E 里分解成一次因式的乘积.

证明 设 $f(x)$ 在域 F 上的分裂域 $E = F(\alpha_1, \alpha_2, \dots, \alpha_n)$, β 在 F 上的极小多项式为 $g(x)$.

假设 $g(x)$ 不能在 $E[x]$ 里分解为一次因式的乘积, 那么在 $E[x]$ 中,

$$(1) \quad g(x) = (x - \beta)p_1(x) \cdots p_s(x)$$

这里 $p_i(x)$, $i = 1, 2, \dots, s$, 都是 $E[x]$ 中首项系数为 1 的不可约多项式, 且它们的次数不能皆为 1, 从它们中选一个次数最高者, 设为 $p(x)$, 其余的 $s - 1$ 个多项式的乘积记为 $g_1(x)$, 则(1)式可写为

$$g(x) = (x - \beta)p(x)g_1(x)$$

我们假定 $\partial^\circ(p(x)) = m > 1$. 作 E 的单代数扩域

$$\begin{aligned} E(\beta') &= F(\alpha_1, \alpha_2, \dots, \alpha_n)(\beta') \\ &= F(\alpha_1, \alpha_2, \dots, \alpha_n, \beta') \end{aligned}$$

使得 $p(\beta') = 0$ 。则有

$$(2) \quad [E(\beta') : E] = [F(\alpha_1, \dots, \alpha_n, \beta') : E] = m$$

由于

$$g(\beta') = (\beta' - \beta)p(\beta')g_1(\beta') = 0,$$

由 2.2.14,

$$F(\beta) \cong F(\beta'),$$

再由 2.3.5, 可得

$$F(\beta)[x] \cong F(\beta')[x],$$

并且在这个同构映射之下,

$$f(x) \mapsto f(x),$$

这样, 根据 2.3.7, $f(x)$ 在 $F(\beta')$ 上的分裂域与 $f(x)$ 在 $F(\beta)$ 上的分裂域同构。但 $F(\beta', \alpha_1, \dots, \alpha_n)$ 是 $f(x)$ 在 $F(\beta')$ 上的一个分裂域, 而 $F(\beta, \alpha_1, \dots, \alpha_n)$ 是 $f(x)$ 在 $F(\beta)$ 上的一个分裂域, 所以

$$F(\beta', \alpha_1, \dots, \alpha_n) \cong F(\beta, \alpha_1, \dots, \alpha_n),$$

$$[F(\beta', \alpha_1, \dots, \alpha_n) : F] = [F(\beta, \alpha_1, \dots, \alpha_n) : F]$$

由于 $F(\beta', \alpha_1, \dots, \alpha_n) = E(\beta')$, 再根据 (2) 式可得

$$\begin{aligned} [F(\beta', \alpha_1, \dots, \alpha_n) : F] &= [E(\beta') : E][E : F] \\ &= m[E : F] \end{aligned}$$

而

$$[F(\beta, \alpha_1, \dots, \alpha_n) : F] = [E : F]$$

由此得 $m = 1$, 这与 $m > 1$ 矛盾。故 $g(x)$ 在 $E[x]$ 里可以分解为一次因式的乘积。

根据 2.2.8, 我们有

3.1.2 推论 令 E 是多项式 $f(x)$ 在 F 上的分裂域,

$p(x)$ 是 $F[x]$ 中任意不可约多项式. 如果 $p(x)$ 在 E 中有一个根, 那么 E 包含 $p(x)$ 的所有根.

具有 3.1.2 所述性质的代数扩域是非常重要的, 它在伽罗华理论的研究中扮演着重要角色, 我们引入如下概念.

3.1.3 定义 设 N 是域 F 的有限扩域. N 称为 F 的一个正规扩域, 如果对于 F 上的任一不可约多项式 $f(x)$, 只要 $f(x)$ 在 N 中有一个根, 那么就有 N 含有 $f(x)$ 的分裂域.

域 F 的一个正规扩域简称为 F 的正规域, 也称为 F 的伽罗华扩域.

例 1 设 \mathbb{Q} 是有理数域, 则 \mathbb{Q} 是 \mathbb{Q} 的一个正规域. 事实上, 设 $f(x)$ 是 \mathbb{Q} 上任一不可约多项式, 只要 $f(x)$ 在 \mathbb{Q} 中有一个根, 由于 $f(x)$ 不可约, 则必有 $\partial^\circ(f(x)) = 1$, 因而 \mathbb{Q} 就是 $f(x)$ 在 \mathbb{Q} 上的分裂域, 故 \mathbb{Q} 是 \mathbb{Q} 的正规域.

例 2 $\mathbb{Q}(\sqrt{2})$ 是 \mathbb{Q} 的正规域.

例 3 实数域 \mathbb{R} 不是有理数域 \mathbb{Q} 的正规域, 因为 \mathbb{R} 不是 \mathbb{Q} 的有限扩域. 同样, 复数域 \mathbb{C} 也不是 \mathbb{Q} 的正规域.

根据 3.1.2, 域 F 上的一个多项式在 F 上的分裂域是 F 的正规域. 反之也真. 事实上, 设 N 是 F 的正规域, 因为 N 是 F 的有限扩域, 所以 $N = F(a_1, \dots, a_s)$, a_1, \dots, a_s 为 F 上的代数元. 设 a_i 在 F 上的极小多项式为 $p_i(x)$, 则 $p_i(x)$ 在 F 上不可约, 令

$$f(x) = p_1(x)p_2(x)\cdots p_s(x),$$

由于 $p_i(x)$ 在 N 中有根 a_i , 所以 $p_i(x)$ 在 N 中完全分解, 故 N 包含 $f(x)$ 在 F 上的分裂域 P . 另一方面, 因为 $P \supseteq F$, P 含有 a_1, \dots, a_s , 所以 $P \supseteq F(a_1, \dots, a_s) = N$, 故 $N = P$, N 是 $f(x)$ 在 F 上的分裂域. 于是有

3.1.4 定理 设 N 是域 F 的扩域, 则 N 是 F 的正规域的

充分必要条件是 N 为 F 上某个多项式的分裂域。

利用 3.1.4 很容易判断 $\mathbb{Q}(\sqrt{2})$ 是 \mathbb{Q} 的正规域，因其为多项式 $f(x) = x^2 - 2$ 在 \mathbb{Q} 上的分裂域。

例 4 $\mathbb{Q}(\sqrt{3}, i)$ 是 \mathbb{Q} 的一个正规域，因其为 \mathbb{Q} 上多项式 $f(x) = x^4 - 2x^2 - 3$ 的分裂域。

最后，我们再给出一个域是正规域的充分必要条件。设 E 是域 F 的扩域， $\alpha, \beta \in E$ ，我们有如下

3.1.5 定义 域 F 上的两个代数元 α 和 β 称为在 F 上共轭，如果 α 和 β 在 F 上的极小多项式相同。

3.1.6 定理 设 N 是域 F 的有限扩域，那么 N 是 F 的正规域的充分必要条件是：若 $\alpha \in N$ ，则 α 的共轭元 $\beta \in N$ 。

证明 设 N 是 F 的正规域， β 与 α 在 F 上共轭， α, β 在 F 上的极小多项式为 $p(x)$ ，若 $\alpha \in N$ ，由 3.1.3， N 含有 $p(x)$ 的分裂域，因之 $\beta \in N$ 。

反之，设 $\alpha \in N$ ， α 在 F 上的极小多项式为 $p(x)$ ，而 $p(x)$ 的其余的根皆为 α 在 F 上的共轭元，从而均含于 N 中，因之 N 含有 $p(x)$ 的分裂域，故 N 是 F 的正规域。

例 5 复数域 \mathbb{C} 是实数域 \mathbb{R} 的正规域。事实上，已知 $\mathbb{C} = \mathbb{R}(i)$ ，而 $[\mathbb{C} : \mathbb{R}] = 2$ 。设 $\alpha = a + bi \in \mathbb{C}$ ，这里 $a, b \in \mathbb{R}$ ，则 α 的共轭元 $\alpha - bi \in \mathbb{C}$ ，所以 \mathbb{C} 是 \mathbb{R} 的正规域。

例 6 $\mathbb{Q}(\sqrt[3]{2})$ 不是 \mathbb{Q} 的正规域。因为 $\sqrt[3]{2}$ 在 \mathbb{Q} 上的共轭元 $\sqrt[3]{2} \omega \notin \mathbb{Q}(\sqrt[3]{2})$ ，这里 $\omega = \frac{-1 + \sqrt{3}i}{2}$ 。

习 题

1. 设 \mathbb{Q} 是有理数域， E 为 \mathbb{Q} 的任意一个二次扩域，则 E 必有如下形式：

$$E = Q(\sqrt{m})$$

这里 $m = -1$ 或 $m = \pm p_1 p_2 \cdots p_s$, p_i 为素数且当 $i \neq j$ 时, $p_i \neq p_j$.

2. 举出有理数域 Q 的一个三次域和一个四次域不是 Q 的正规域的例子.

3. 设 $P_2 \supset P_1 \supset F$, P_2, P_1, F 皆为域, 证明, 若 P_2 是 F 的正规域, 则 P_2 也是 P_1 的正规域. 若 P_2 是 F 的正规域, 是否有 P_1 也是 F 的正规域?

§ 3.2 伽罗华群

由一个域的所有自同构作成的集合是一种特殊的一一变换的集合, 我们可以证明它对于变换的乘法作成一群. 而我们更感兴趣的是, 正规域的一些特殊的自同构所作成的群, 即所谓伽罗华群. 它是伽罗华理论的主要研究对象.

设 F 是一个域, F 的所有自同构作成一群, 记为 $\text{Aut } F$.

任取 $\tau_1, \tau_2 \in \text{Aut } F$, 规定

$$\sigma: F \longrightarrow F$$

$$a \longmapsto (a^{\tau_1})^{\tau_2}, \quad \forall a \in F$$

由于 τ_1, τ_2 是 F 上的双射, 所以 σ 也是 F 上的双射. 由变换的乘法可知 $\sigma = \tau_1 \tau_2$, 并且有

$$(a+b)^\sigma = ((a+b)^{\tau_1})^{\tau_2} = (a^{\tau_1} + b^{\tau_1})^{\tau_2}$$

$$= (a^{\tau_1})^{\tau_2} + (b^{\tau_1})^{\tau_2} = a^\sigma + b^\sigma$$

$$(ab)^\sigma = ((ab)^{\tau_1})^{\tau_2} = (a^{\tau_1} b^{\tau_1})^{\tau_2}$$

$$= (a^{\tau_1})^{\tau_2} (b^{\tau_1})^{\tau_2} = a^\sigma b^\sigma$$

$$\forall a, b \in F,$$

我们有

3.2.1 定理 设 F 是一个域, 则 $\text{Aut } F$ 对变换的乘法作成一群, 称之为 F 的自同构群.

证明 我们证明 $\text{Aut } F$ 对上述的乘法满足 1.1.1 中的三个条件.

1) 乘法满足结合律:

任取 $\tau_1, \tau_2, \tau_3 \in \text{Aut } F, a \in F$, 由于

$$a^{(\tau_1 \tau_2) \tau_3} = (a^{\tau_1 \tau_2})^{\tau_3} = ((a^{\tau_1})^{\tau_2})^{\tau_3},$$

$$a^{\tau_1 (\tau_2 \tau_3)} = (a^{\tau_1})^{\tau_2 \tau_3} = ((a^{\tau_1})^{\tau_2})^{\tau_3}$$

所以 $(\tau_1 \tau_2) \tau_3 = \tau_1 (\tau_2 \tau_3)$.

2) $\text{Aut } F$ 中有单位元:

设 ε 表示 F 的恒等自同构, 即 $a^\varepsilon = a, \forall a \in F$. 对于任意 $\tau \in \text{Aut } F$ 显然有

$$\tau \varepsilon = \varepsilon \tau = \tau$$

即 ε 为 $\text{Aut } F$ 的单位元.

3) $\text{Aut } F$ 的每个元有逆元:

任取 $\tau \in \text{Aut } F$, 令 τ^{-1} 表示 τ 的逆映射, 即若 $a^\tau = \overline{a}$, 则 $\overline{a}^{\tau^{-1}} = a$. 于是由

$$\overline{a + b} = a^\tau + b^\tau = (a + b)^\tau, \quad \overline{ab} = a^\tau b^\tau = (ab)^\tau$$

可得

$$(\overline{a + b})^{\tau^{-1}} = a + b = \overline{a}^{\tau^{-1}} + \overline{b}^{\tau^{-1}},$$

$$(\overline{ab})^{\tau^{-1}} = ab = \overline{a}^{\tau^{-1}} \overline{b}^{\tau^{-1}}.$$

所以 $\tau^{-1} \in \text{Aut } F$, 且 $\tau^{-1} \tau = \tau \tau^{-1} = \varepsilon$.

故 $\text{Aut } F$ 对自同构的乘法作成群, 称为 F 的自同构群.

设 σ 是 $\text{Aut } F$ 中的任意元, 则 $1^\sigma = 1$, 由 F 的素域的结构可知, $a^\sigma = a$, a 为 F 的素域 Δ 中任意元, 即 σ 限制在 Δ 上是恒等自同构, 因而有

例 1 有理数域 \mathbb{Q} 的自同构群只含一个元素 ε .

例 2 设 $E = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2})$ 中每个元可唯一地表示为

$$a + b\sqrt{2}, \quad a, b \in \mathbb{Q}$$

任取 $\tau \in \text{Aut } E$, 则

$$(a + b\sqrt{2})^\tau = a^\tau + b^\tau(\sqrt{2})^\tau = a + b(\sqrt{2})^\tau$$

设 $(\sqrt{2})^\tau = a$, 则 $((\sqrt{2})^\tau)^2 = a^2$, $a^2 = 2^\tau = 2$, 于是 $a = \pm\sqrt{2}$. 这样, 我们有

1) 当 $\sqrt{2}^\tau = \sqrt{2}$ 时, $\tau = \varepsilon$: $a + b\sqrt{2} \mapsto a + b\sqrt{2}$;

2) 当 $\sqrt{2}^\tau = -\sqrt{2}$ 时, τ : $a + b\sqrt{2} \mapsto a - b\sqrt{2}$.

因此 $\text{Aut } E = \{\varepsilon, \tau\}$, 这里 $\tau^2 = \varepsilon$.

例 3 设 θ 是 $f(x) = x^4 + x^3 + x^2 + x + 1$ 的一个根. 令 $N = \mathbb{Q}(\theta)$. 由于 $x^5 - 1 = (x - 1)f(x)$, 所以 $\theta^5 = 1$, 且 $\theta \neq 1$. 又由于 $f(x)$ 在 \mathbb{Q} 上不可约, 显然, $\theta^2, \theta^3, \theta^4$ 是 θ 在 \mathbb{Q} 上的全部共轭元. N 中每个元可唯一表成

$$a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3, \quad a_i \in \mathbb{Q}$$

设 $\tau \in \text{Aut } N$, 则

$$(a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3)^\tau = a_0 + a_1\theta^\tau + a_2(\theta^\tau)^2 + a_3(\theta^\tau)^3$$

令 $\theta^\tau = \beta$, 则易证 β 是 θ 的共轭元, 于是 β 是 $\theta, \theta^2, \theta^3, \theta^4$ 之一, 对于 β 的四种取法我们有

$$\tau_1 = \varepsilon: a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 \mapsto a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3,$$

$$\tau_2: a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 \mapsto a_0 + a_1\theta^2 + a_2\theta^4 + a_3\theta^6,$$

$$\tau_3: a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 \mapsto a_0 + a_1\theta^3 + a_2\theta^6 + a_3\theta^9,$$

$$\tau_4: a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 \mapsto a_0 + a_1\theta^4 + a_2\theta^8 + a_3\theta^{12}.$$

所以 $\text{Aut}N$ 恰含四个元 $\tau_1 = \varepsilon, \tau_2, \tau_3, \tau_4$, 其乘法表如下:

	τ_1	τ_2	τ_3	τ_4
τ_1	τ_1	τ_2	τ_3	τ_4
τ_2	τ_2	τ_4	τ_1	τ_3
τ_3	τ_3	τ_1	τ_4	τ_2
τ_4	τ_4	τ_3	τ_2	τ_1

易见 $\text{Aut}N \cong Z_2^*$.

现在我们讨论域 P 的特殊的自同构.

3.2.2 定义 设 P 是域 F 的扩域, P 的一个自同构 τ 称为 P 在 F 上的自同构, 如果对于任意 $a \in F$, 都有 $a^\tau = a$.

3.2.3 定理 P 在 F 上的一切自同构的集合 H 作成 P 的自同构群 $\text{Aut}P$ 的一个子群.

证明 由于 $\text{Aut}P$ 的单位元 ε 是 P 在 F 上的自同构, 所以 H 有单位元 ε . 设 $\sigma, \tau \in H$, 则对于任意 $a \in F$ 均有 $a^{\sigma\tau} = (a^\sigma)^\tau = a^\tau = a$, 故 $\sigma\tau \in H$, 再者, $a^{\sigma^{-1}} = (a^\sigma)^{\sigma^{-1}} = a^\varepsilon = a$, 故 $\sigma^{-1} \in H$, 所以 H 是 $\text{Aut}P$ 的一个子群.

3.2.4 定义 设 N 是 F 的正规域, N 在 F 上的所有自同构作成的子群称为 N 在 F 上的伽罗华群, 并用符号 $\text{Gal}N/F$ 表示.

值得注意的是，我们说到 N 在 F 上的伽罗华群时， N 必须是 F 的正规域，伽罗华群只对正规域定义。

下面我们证明伽罗华群的一个重要定理，为此先证明一个引理。

3.2.5 引理 设 τ 是 N 在 F 上的一个自同构， $\alpha \in N$ ，令 $\beta = \alpha^\tau$ ，则对于 $F[x]$ 中一个多项式 $f(x)$ ，如果 $f(\alpha) = 0$ ，就有 $f(\beta) = 0$ 。

特别， α 与 β 在 F 上的极小多项式相同。

证明 设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_i \in F$$

由 $f(\alpha) = 0$ 可得

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0 = 0$$

$$(a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0)^\tau = 0$$

$$a_n^\tau (\alpha^\tau)^n + a_{n-1}^\tau (\alpha^\tau)^{n-1} + \cdots + a_1^\tau \alpha^\tau + a_0^\tau = 0$$

但 $a_i^\tau = a_i$ ， $i = 0, 1, \cdots, n$ ， $\alpha^\tau = \beta$ ，于是

$$a_n \beta^n + a_{n-1} \beta^{n-1} + \cdots + a_1 \beta + a_0 = 0,$$

即

$$f(\beta) = 0.$$

3.2.6 定理 设 N 是域 F 的正规域，则

$$|\text{Gal}N/F| = [N : F].$$

证明 由于 N 是 F 的正规域，根据 3.1.4 定理， N 是 F 上多项式 $f(x)$ 的分裂域， $N = F(\alpha_1, \cdots, \alpha_n)$ ，进一步有 $N = F(\theta)$ ， θ 是 F 上 m 次不可约多项式 $g(x)$ 的根，再由 3.1.6 定理， θ 在 F 上的共轭元均属于 N 。设 $g(x)$ 的 m 个根为 $\theta_1 = \theta, \theta_2, \cdots, \theta_m$ ，对于 N 中任意元

$$\alpha = a_0 + a_1 \theta + \cdots + a_{m-1} \theta^{m-1}, \quad a_i \in F,$$

规定

$\alpha^{\tau_i} = a_0 + a_1\theta_i + \cdots + a_{m-1}\theta_i^{m-1}$, $i = 1, 2, \dots, m$,
 则 τ_i 是 N 到 N 的子域 $F(\theta_i)$ 的满射, 但 θ_i 是 F 上 m 次不可约多项式 $g(x)$ 的根, 故

$$[F(\theta_i) : F] = m,$$

因之 $F(\theta_i) = N$, $i = 1, 2, \dots, m$. 即 τ_i 是 N 到自身的满射.

$$\text{设 } \alpha = \sum_{j=0}^{m-1} a_j \theta^j, \beta = \sum_{j=0}^{m-1} b_j \theta^j, \text{ 则 } \alpha^{\tau_i} = \sum_{j=0}^{m-1} a_j \theta_i^j,$$

$$\beta^{\tau_i} = \sum_{j=0}^{m-1} b_j \theta_i^j. \text{ 若 } \alpha^{\tau_i} = \beta^{\tau_i}, \text{ 就有 } \sum_{j=0}^{m-1} (a_j - b_j) \theta_i^j = 0,$$

也就是说 θ_i 是 F 上的一个多项式

$$(1) \quad (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{m-1} - b_{m-1})x^{m-1}$$

的根. 而 θ_i 是 F 上 m 次不可约多项式 $g(x)$ 的根, 因而 $g(x)$ 与 θ_i 在 F 上的极小多项式至多相差一个 F^* 中的元, 所以 $g(x)$ 必整除 (1), 故 (1) 必须是零多项式, 从而

$$a_i - b_i = 0, \quad i = 0, 1, \dots, m-1,$$

或

$$a_i = b_i, \quad i = 0, 1, \dots, m-1,$$

于是 $\alpha = \beta$, 故 τ_i 是 N 到自身的单射, 因之 τ_i 是 N 到自身的双射. 容易验证 τ_i 是同构映射, 并且对于任意 $a \in F$, 有 $a^{\tau_i} = a$, 即 τ_i 是 N 在 F 上的自同构.

因为当 $i \neq j$ 时, $\theta_i \neq \theta_j$, 故 $\tau_i \neq \tau_j$, 因之 $|\text{Gal}N/F| \geq m$.

以下证明 $\text{Gal}N/F$ 除 τ_i 外不含其它 N 在 F 上的自同构. 设 $\sigma \in \text{Gal}N/F$, 因为对于 F 中任意元 a 都有 $a^\sigma = a$,

$$\text{所以对于 } N \text{ 中任意元 } \alpha = \sum_{j=0}^{m-1} a_j \theta^j, \text{ 都有 } \alpha^\sigma = \sum_{j=0}^{m-1} a_j (\theta^\sigma)^j,$$

换言之, σ 由 θ 的象 θ^σ 唯一确定, 但由 3·2·5, 若 $g(\theta) = 0$, 则 $g(\theta^\sigma) = 0$, 即 θ^σ 是 $g(x)$ 的根, 因之 $\theta^\sigma = \theta_i$, 故 $\sigma = \tau_i$. 于是

$$|\text{Gal}N/F| = m = [N : F].$$

例 4 例 3 中 $\mathbb{Q}(\theta)$ 是 \mathbb{Q} 的正规域, $|\text{Gal}\mathbb{Q}(\theta)/\mathbb{Q}| = 4$.

例 5 $\mathbb{Q}(\sqrt[3]{2})$ 不是 \mathbb{Q} 的正规域, 由实际验证可知 $\mathbb{Q}(\sqrt[3]{2})$ 在 \mathbb{Q} 上的自同构群的阶为 1, 而 $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

我们说, 3·2·6 的逆命题也是正确的, 即

3·2·7 定理 设 N 是域 F 上的有限扩域, $[N : F] = m$. 如果 N 在 F 上的自同构群的阶为 m , 则 N 是 F 的正规域.

证明 由于 $[N : F] = m$, 根据 2·4·4, $N = F(\alpha)$, α 在 F 上的极小多项式 $p(x)$ 为 m 次的. 令 N 在 F 上的自同构群为 G , 因 $|G| = m$, 故可设

$$G = \{\tau_1 = \varepsilon, \tau_2, \dots, \tau_m\}.$$

因为 $p(\alpha) = 0$, 根据 3·2·5, $p(\alpha^{\tau_i}) = 0$, $i = 1, 2, \dots, m$.

显然, $\alpha^{\tau_i} \in N$, 且当 $i \neq j$ 时, $\alpha^{\tau_i} \neq \alpha^{\tau_j}$, 因而 $\alpha^{\tau_1} = \alpha$,

$\alpha^{\tau_2}, \dots, \alpha^{\tau_m}$ 恰为 $p(x)$ 的 m 个不同的根, 于是 $N \supseteq F(\alpha^{\tau_1},$

$\dots, \alpha^{\tau_m})$, 而 $N = F(\alpha)$, 故 N 是 $p(x)$ 在 F 上的分裂域. 由 3·1·4, N 是 F 的正规域.

习 题

1. 设 N 是 F 的正规域, τ 是 N 到自身的一个映射, 并且对于 F 中的任意元 a 都有 $a^\tau = a$. 求证, 如果 $(a+b)^\tau = a^\tau + b^\tau$, $(ab)^\tau = a^\tau b^\tau$, $\forall a, b \in N$, 则 $\tau \in \text{Gal}N/F$.

2. 设 $N = Q(\sqrt{5}, \omega)$, $\omega = \frac{-1 + \sqrt{3}i}{2}$, 找出 N 的自同构群

$\text{Aut} N$ 及 N 在 $Q(\sqrt{5})$ 上的自同构群(要求列出乘法表).

3. 证明, $N = Q(\sqrt[3]{2}, \omega)$ 是 Q 的正规域, 找出 N 在 Q 上的伽罗华群.

§ 3.3 方程的伽罗华群

我们的目标是研究方程的根号解, 为此, 我们需要讨论方程的伽罗华群.

3.3.1 定义 设 $f(x)$ 是域 F 的一个多项式, 而 N 是它在 F 上的分裂域, 则 N 在 F 上的伽罗华群称为方程 $f(x) = 0$ 在 F 上的伽罗华群.

由 3.3.1 可以看出, F 上方程 $f(x) = 0$ 的伽罗华群就是它的根域在 F 上的伽罗华群. 在确定方程的伽罗华群时, 3.2.5 起着很重要的作用, 利用 3.2.5, 再考虑到 3.2.6, 可以求出一些形式比较简单的方程的伽罗华群. 这里值得提出的有以下两个问题:

1° 设 $f(x) \in F[x]$, 且 $\partial^\circ(f(x)) \geq 1$, 根据域上多项式因式分解定理, 我们有

$$f(x) = p_1^{r_1}(x) p_2^{r_2}(x) \cdots p_s^{r_s}(x)$$

这里 $p_1(x), \dots, p_s(x)$ 为 $F[x]$ 中互不相同的不可约多项式, $r_i \geq 1, i = 1, 2, \dots, s$. $f(x)$ 与 $p_1(x)p_2(x)\cdots p_s(x)$ 在 F 上的分裂域是相同的. 因为 $\text{char } F = \infty$, 所以 $p_i(x)$ 无重根, 从而 $p_1(x)p_2(x)\cdots p_s(x)$ 也无重根. 这样, 研究方程的伽罗华群时可以只研究没有重根的方程的伽罗华群.

2° 设 $f(x) \in F[x]$, 不妨设 $f(x)$ 的首项系数为 1,

$f(x)$ 在 F 上的分裂域为 N . 若 $f(x)$ 在 $F[x]$ 可以分解为互不相同的不可约多项式的乘积:

$$f(x) = p_1(x)p_2(x)\cdots p_r(x),$$

设 α 是 $p_i(x)$ 的根, 对某个 i , 则 $p_i(x)$ 是 α 在 F 上的极小多项式. 任取 $\tau \in \text{Gal}N/F$, 由 3.2.5, α 与 α^τ 的极小多项式相同, 因此 $p_i(\alpha^\tau) = 0$. 而 α 与 α^τ 在 F 上的极小多项式是唯一的, 所以 α^τ 只能是 $p_i(x)$ 的根. 这也就是说, 设 α, β 分别为 $p_i(x)$ 和 $p_j(x)$ 的根 ($i \neq j$), 若一变换 σ , 使得 $\alpha^\sigma = \beta$, 则 $\sigma \notin \text{Gal}N/F$.

现在我们研究几个例子.

例 1 设 $f(x) = (x^2 - 2)(x^2 - 3)$ 是 $\mathbb{Q}[x]$ 中一个多项式, $f(x)$ 在 \mathbb{Q} 上的分裂域为 $N = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. $f(x)$ 在 N 中有根 $\pm\sqrt{2}, \pm\sqrt{3}$. 任取 $\tau \in \text{Gal}N/\mathbb{Q}$, 由于 $x^2 - 2$ 在 \mathbb{Q} 上不可约, 则 τ 必须把 $x^2 - 2$ 的根变为它的根, 同样, τ 必须把 $x^2 - 3$ 的根变为它的根. 又因为 $[N : \mathbb{Q}] = 4$, 所以 $\text{Gal}N/\mathbb{Q}$ 恰由 4 个元素组成, 列表说明为下:

	τ_1	τ_2	τ_3	τ_4
$\sqrt{2} \mapsto$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$-\sqrt{2} \mapsto$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$
$\sqrt{3} \mapsto$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$
$-\sqrt{3} \mapsto$	$-\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$

$\text{Gal}N/\mathbb{Q} = \{\tau_1 = \varepsilon, \tau_2, \tau_3, \tau_4\}$ 即为方程 $f(x) = 0$ 的伽罗华群. 如果把方程的四个根 $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$ 依次标为 1, 2, 3, 4, 则 $\tau_1, \tau_2, \tau_3, \tau_4$ 分别对应于 (1), (12), (34), (12)(34). 于是 $\text{Gal}N/\mathbb{Q}$ 与 S_4 的子群

克莱因四元群 B_4 同构, 即

$$\text{Gal}N/\mathbb{Q} \cong B_4 = \{(1), (12), (34), (12)(34)\}.$$

例 2 在 § 3.2 的例 3 中 $\text{Gal}N/\mathbb{Q} = \{\tau_1, \tau_2, \tau_3, \tau_4\}$, 这里 $\tau_1: \theta \mapsto \theta$; $\tau_2: \theta \mapsto \theta^2$; $\tau_3: \theta \mapsto \theta^3$; $\tau_4: \theta \mapsto \theta^4$, 注意到 $\theta^5 = 1$, 我们可以列表如下:

	τ_1	τ_2	τ_3	τ_4
$\theta \mapsto$	θ	θ^2	θ^3	θ^4
$\theta^2 \mapsto$	θ^2	θ^4	θ	θ^3
$\theta^3 \mapsto$	θ^3	θ	θ^4	θ^2
$\theta^4 \mapsto$	θ^4	θ^3	θ^2	θ

$\text{Gal}N/\mathbb{Q}$ 即为方程 $x^4 + x^3 + x^2 + x + 1 = 0$ 的伽罗华群. 如果把 $\theta, \theta^2, \theta^3, \theta^4$ 依次标为 1, 2, 3, 4, 那么 $\tau_1, \tau_2, \tau_3, \tau_4$ 分别对应于 $(1), (1243), (1342), (14)(23)$. 易知

$$H = \{(1), (1243), (14)(23), (1342)\}$$

是由 (1243) 生成的循环群. 显然 $\text{Gal}N/\mathbb{Q} \cong H$, H 是 S_4 的一个子群.

例 3 求方程 $x^3 - 2 = 0$ 在 \mathbb{Q} 上的伽罗华群 G . 我们知道 $f(x) = x^3 - 2$ 在 \mathbb{Q} 上的分裂域是 $N = \mathbb{Q}(\sqrt[3]{2}, \omega)$, 这里 $\omega = \frac{-1 + \sqrt{3}i}{2}$, 由 3.3.1, $G = \text{Gal}N/\mathbb{Q}$.

因为 $N = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2} + \omega)$, $[N : \mathbb{Q}] = 6$, 所以 $\sqrt[3]{2} + \omega$ 在 \mathbb{Q} 上极小多项式必为 6 次, 因而 N 中每个元可唯一表成

$$a_0 + a_1\alpha + \cdots + a_5\alpha^5$$

这里 $\alpha = \sqrt[3]{2} + \omega$, $a_i \in \mathbb{Q}$, $i = 0, 1, \dots, 5$. 任取 $\tau \in G$, 则

$$(a_0 + a_1\alpha + \dots + a_5\alpha^5)^\tau = a_0 + a_1\alpha^\tau + \dots + a_5(\alpha^\tau)^5.$$

因此只需确定 α^τ , 而 $\alpha^\tau = (\sqrt[3]{2} + \omega)^\tau = (\sqrt[3]{2})^\tau + \omega^\tau$. 由于 $\sqrt[3]{2}$ 在 τ 元下只有 3 种可能: $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$; ω 的象只有两种可能: ω , ω^2 . 因此共有 6 种可能的组合. 又因为 $|G| = [N : \mathbb{Q}] = 6$, 所以 G 恰含 6 个元, 现将这 6 个自同构列表如下:

	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6
$\sqrt[3]{2} \mapsto$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
$\omega \mapsto$	ω	ω	ω	ω^2	ω^2	ω^2

这 6 个自同构作用在 $x^3 - 2 = 0$ 的三个根上的结果如下表所示:

	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6
$\sqrt[3]{2} \mapsto$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
$\sqrt[3]{2}\omega \mapsto$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$
$\sqrt[3]{2}\omega^2 \mapsto$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$

于是 $G = \{\tau_1 = \varepsilon, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6\}$, 如果把 $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ 依次标为 1, 2, 3, 则 $\tau_1, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6$ 分别对应于 (1), (123), (132), (23), (12), (13). 故 $G \cong S_3$.

例 4 求 $x^4 - 2 = 0$ 在 \mathbb{Q} 上的伽罗华群 G . 这个方程在

\mathbb{Q} 上的根域为 $N = \mathbb{Q}(\sqrt[4]{2}, i)$, 这里 $i^2 = -1$. 仿例 3 的讨论可知 G 由 8 个元素组成. 设 $\sqrt[4]{2} = \alpha$, G 的 8 个元列表如下

	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
$\alpha \mapsto$	α	$-\alpha$	αi	$-\alpha i$	α	$-\alpha$	αi	$-\alpha i$
$-\alpha \mapsto$	$-\alpha$	α	$-\alpha i$	αi	$-\alpha$	α	$-\alpha i$	αi
$\alpha i \mapsto$	αi	$-\alpha i$	$-\alpha$	α	$-\alpha i$	αi	α	$-\alpha$
$-\alpha i \mapsto$	$-\alpha i$	αi	α	$-\alpha$	αi	$-\alpha i$	$-\alpha$	α

这里 $\alpha, -\alpha, \alpha i, -\alpha i$ 为方程 $x^4 - 2 = 0$ 的 4 个根, 若把它们依次标为 1, 2, 3, 4, 则

$$\tau_1 \mapsto (1), \tau_2 \mapsto (12)(34), \tau_3 \mapsto (1324),$$

$$\tau_4 \mapsto (1423), \tau_5 \mapsto (34), \tau_6 \mapsto (12),$$

$$\tau_7 \mapsto (13)(24), \tau_8 \mapsto (14)(23)$$

这 8 个置换构成 S_4 的子群, 记为 H , 且 $G \cong H$.

从这四个例子可以看出, 尽管各例中方程 $f(x) = 0$ 的伽罗华群的阶数和结构各有不同, 但它们都与 $f(x) = 0$ 的根集上某个置换群同构. 不难证明, 这个结果对于一般情形也是正确的.

3.3.2 定理 域 F 上一个没有重根的 n 次方程 $f(x) = 0$ 的伽罗华群 G 与 n 次对称群的一个子群同构.

证明 令 N 是 $f(x) = 0$ 在 F 上的根域, $N = F(\alpha_1, \dots, \alpha_n)$, $\alpha_1, \dots, \alpha_n$ 是 $f(x) = 0$ 的根. 在 N 中

$$f(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

任取 $\tau \in G$, 则 $\alpha_1^\tau, \alpha_2^\tau, \dots, \alpha_n^\tau$ 仍为方程 $f(x) = 0$ 的 n 个根, 而且当 $i \neq j$ 时 $\alpha_i^\tau \neq \alpha_j^\tau$. 因此给定 τ , 就可以唯一确

定

$$P_\tau = \begin{pmatrix} a_1 & a_2 \cdots a_n \\ a_1^\tau & a_2^\tau \cdots a_n^\tau \end{pmatrix}$$

令

$$G_0 = \left\{ P_\tau \mid P_\tau = \begin{pmatrix} a_1 & a_2 \cdots a_n \\ a_1^\tau & a_2^\tau \cdots a_n^\tau \end{pmatrix}, \tau \in G \right\}$$

我们断言 $G \cong G_0$. 事实上, 定义

$$\varphi: \tau \mapsto P_\tau,$$

则 φ 是 G 到 G_0 的满射. 为证 φ 是单射, 先注意到 $N = F(a_1, a_2, \dots, a_n) = F(a_1)(a_2) \cdots (a_n)$, 由单代数扩域的结构可知, N 中任意元都可以表示为系数属于 F 的关于 a_1, a_2, \dots, a_n 的一个多项式

$$g(a_1, a_2, \dots, a_n).$$

假定 $P_\tau = P_\lambda$, $\tau, \lambda \in G$, 就是说

$$(1) \quad a_i^\tau = a_i^\lambda, \quad i = 1, 2, \dots, n,$$

对于任意 $a \in N$, a 可以表示为

$$(2) \quad a = g(a_1, a_2, \dots, a_n)$$

这里 $g(a_1, a_2, \dots, a_n)$ 是系数属于 F 的关于 a_1, a_2, \dots, a_n 的多项式. 则

$$(3) \quad a^\tau = (g(a_1, a_2, \dots, a_n))^\tau = g(a_1^\tau, a_2^\tau, \dots, a_n^\tau),$$

$$(4) \quad a^\lambda = (g(a_1, a_2, \dots, a_n))^\lambda = g(a_1^\lambda, a_2^\lambda, \dots, a_n^\lambda),$$

由(1), (3), (4), $a^\lambda = a^\tau$, 从而 $\tau = \lambda$. 因此 φ 是单射, 故 φ 是 G 到 G_0 的双射.

我们可以把 P_λ 写成如下形式

$$(5) \quad P_\lambda = \begin{pmatrix} a_1^\tau & a_2^\tau \cdots a_n^\tau \\ a_1^{\tau\lambda} & a_2^{\tau\lambda} \cdots a_n^{\tau\lambda} \end{pmatrix}$$

那么

$$P_{\tau} P_{\lambda} = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1^{\tau \lambda} & a_2^{\tau \lambda} & \cdots & a_n^{\tau \lambda} \end{pmatrix} = P_{\tau \lambda}$$

因此 $G \cong G_0$, G_0 是 n 次对称群的一个子群。

这样,我们就可以把任意伽罗华群都理解为某方程的根的置换群,置换群是具体的而且容易计算,因而使我们的讨论更加方便。

一般说, n 次方程 $f(x)=0$ 的伽罗华群 G 与 S_n 的子群同构。我们要问:什么样的 n 次方程的伽罗华群恰与 S_n 同构呢?为此我们研究 n 次一般方程的伽罗华群。

3.3.3 定义 令 u_1, u_2, \dots, u_n 是某一域 K 上的 n 个无关未定元, 方程

$$x^n - u_1 x^{n-1} + u_2 x^{n-2} - \cdots + (-1)^n u_n = 0$$

称为 K 上 n 次一般方程。

由此定义我们看出方程的系数 u_i 不在 K 内,而在 $K(u_1, u_2, \dots, u_n)$ 内,这个定义与我们一般了解的意义是一样的。比如我们解二次方程 $x^2 + ax + b = 0$, 在解的过程中只把 a, b 看成符号,它们是没有关系的,实际上 a, b 就是无关未定元,在解方程时,当然不能从有理数域 \mathbb{Q} 出发,而从 $F = \mathbb{Q}(a, b)$ 出发,至于式子中出现的正负号,只是为我们计算方便罢了。

3.3.4 引理 令

$$f(x) = x^n - u_1 x^{n-1} + \cdots + (-1)^n u_n = 0$$

是域 K 上的 n 次一般方程,而 a_1, a_2, \dots, a_n 是方程的 n 个根,则 a_1, a_2, \dots, a_n 是 K 上无关未定元。

证明 设 N 是 $f(x)=0$ 在 $F = K(u_1, u_2, \dots, u_n)$ 上的根域,在 N 中

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_n),$$

$$u_1 = \sum a_i, u_2 = \sum_{i \neq j} a_i a_j, \dots, u_n = a_1 a_2 \cdots a_n,$$

令 $\bar{N} = K(x_1, x_2, \dots, x_n)$, x_i 是 K 上无关未定元 (这里 $K(x_1, x_2, \dots, x_n)$ 可以理解为 n 元多项式环 $K[x_1, x_2, \dots, x_n]$ 的商域). 作 $\bar{f}(x) = (x - x_1)(x - x_2) \cdots (x - x_n) = x^n - \theta_1 x^{n-1} + \cdots + (-1)^n \theta_n$, 这里 $\theta_1 = \sum x_i, \theta_2 = \sum_{i \neq j} x_i x_j, \dots, \theta_n = x_1 x_2 \cdots x_n$. 比较

$$K \subseteq \bar{F} = K(\theta_1, \theta_2, \dots, \theta_n) \subseteq \bar{N} = K(x_1, x_2, \dots, x_n)$$

$$K \subseteq F = K(u_1, u_2, \dots, u_n) \subseteq N = K(a_1, a_2, \dots, a_n)$$

首先证明 $\theta_1, \theta_2, \dots, \theta_n$ 是 K 上无关未定元. 若

$$g(\theta_1, \theta_2, \dots, \theta_n) = 0,$$

g 是以 K 的元为系数的 n 元多项式. 于是

$$g(\sum x_i, \sum_{i \neq j} x_i x_j, \dots, x_1 x_2 \cdots x_n) = 0$$

$$g(\sum a_i, \sum_{i \neq j} a_i a_j, \dots, a_1 a_2 \cdots a_n) = 0$$

$$g(u_1, u_2, \dots, u_n) = 0$$

由于 u_1, u_2, \dots, u_n 是 K 上无关未定元, 所以 g 的所有系数皆为零, 故 $\theta_1, \theta_2, \dots, \theta_n$ 是 K 上无关未定元. 所以 $K[\theta_1, \dots, \theta_n] \cong K[u_1, u_2, \dots, u_n]$, 因而

$$F \cong \bar{F}$$

在此同构映射之下, K 的元不动, $\theta_i \mapsto u_i, f(x) \mapsto \bar{f}(x)$, 但 N 是 $f(x)$ 在 F 上的分裂域, \bar{N} 是 $\bar{f}(x)$ 在 \bar{F} 上的分裂域, 因而

$$N \cong \bar{N}$$

在此同构映射之下, K 的元不动, $x_i \mapsto a_i, i = 1, \dots, n$, 故 a_1, a_2, \dots, a_n 是 K 上无关未定元.

3.3.5 定理 域 K 上 n 次一般方程

$$f(x) = x^n - u_1 x^{n-1} + \cdots + (-1)^n u_n = 0$$

在 $F = K(u_1, u_2, \cdots, u_n)$ 上的伽罗华群与 S_n 同构。

证明 设 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是 $f(x)$ 的 n 个根, N 为 $f(x)$ 在 F 上的分裂域, 则 $N = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$, 由 $3 \cdot 3 \cdot 2$, $\text{Gal}N/F \cong S_n$ 的一个子群。看

$$\tau = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_{i_1} & \alpha_{i_2} & \cdots & \alpha_{i_n} \end{pmatrix},$$

$\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_n}$ 是 $f(x) = 0$ 的 n 个根 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 的任一排列。定义

$$r(\alpha_1, \alpha_2, \cdots, \alpha_n) \mapsto r(\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_n}),$$

r 是系数在 K 里的有理分式, 由 $3 \cdot 3 \cdot 4$, $\alpha_1, \alpha_2, \cdots, \alpha_n$ 和 $\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_n}$ 是 K 上无关未定元, 因此这个映射是 N 的一个自同构映射, 在这个同构映射之下, K 的元不动, 又由于 α_i 调动次序不影响 $f(x) = 0$ 的系数, 因之在这个同构映射之下, F 的元亦不动, 故这个映射是 N 在 F 上的自同构映射, 因而它属于 $\text{Gal}N/F$, 但形如 τ 的置换共有 $n!$ 个, 所以 $|\text{Gal}N/F| \geq n!$, 故 $\text{Gal}N/F \cong S_n$ 。

习 题

1. 令 G 是 n 个数码的任一置换群, 证明, 存在一个域 F 以及 F 上的一个方程 $f(x) = 0$, 这个方程在 F 上的伽罗华群与 G 同构。
2. 设域 F 上的 n 次多项式 $f(x)$ 在 F 上可约, 则 $f(x) = 0$ 在 F 上的伽罗华群不与 S_n 同构。

§ 3·4 伽罗华理论的基本定理

有了前面的准备工作, 我们就可以讨论伽罗华理论的核心

心内容——伽罗华理论的基本定理。

设 N 是域 F 的正规域，令 \tilde{L} 表示由 N 与 F 的所有中间域作成的集合：

$$(1) \quad \tilde{L} = \{L \mid L \text{ 是 } N \text{ 的包含 } F \text{ 的子域}\}.$$

对于 \tilde{L} 中任意元 L 都有 N 是 L 的正规域。我们把由 $\text{Gal}N/F$ 的所有子群作成的集合记成 \tilde{H} ：

$$(2) \quad \tilde{H} = \{H \mid H \text{ 是 } \text{Gal}N/F \text{ 的子群}\},$$

显然， \tilde{L} 与 \tilde{H} 都是非空的。伽罗华把这两个集合联系起来，很巧妙地在这两个集合之间建立了某种一一映射关系，这就是伽罗华理论基本定理所阐述的重要内容。

通过具体验证，很容易得到

3.4.1 引理 设 N 是 F 的正规域， $\text{Gal}N/F$ 是 N 在 F 上的伽罗华群，那么

1) 设 H 是 $\text{Gal}N/F$ 的一个子群，则由 H 所确定的 N 的子集

$$\text{Inv}H = \{a \in N \mid a^\tau = a, \forall \tau \in H\},$$

是 N 的一个包含 F 的子域，称 $\text{Inv}H$ 为 H 的不变子域。

2) 设 L 是 N 的包含 F 的一个子域，则 N 在 L 上的伽罗华群

$$\text{Gal}N/L = \{\sigma \in \text{Gal}N/F \mid a^\sigma = a, \forall a \in L\}$$

是 $\text{Gal}N/F$ 的一个子群。

根据 3.4.1 可得映射

$$\Phi: \begin{array}{ccc} \tilde{H} & \longrightarrow & \tilde{L} \\ H & \longmapsto & \text{Inv}H, \forall H \in \tilde{H}. \end{array}$$

这个映射可用下面的图来表示：

$$\begin{array}{c}
 \text{Gal}N/F \supseteq H \\
 \downarrow \Phi \\
 N \supseteq \text{Inv}H \\
 \\
 \Psi: \quad \tilde{L} \longrightarrow \tilde{H} \\
 \\
 L \longmapsto \text{Gal}N/L, \quad \forall L \in \tilde{L}.
 \end{array}$$

这也可用图来表示:

$$\begin{array}{c}
 \text{Gal}N/F \supseteq \text{Gal}N/L \\
 \uparrow \Psi \\
 N \supseteq L
 \end{array}$$

我们把 Φ 与 Ψ 称为两个伽罗华映射。

由于 $\text{Inv}H$ 是 N 包含 F 的子域, 则 N 是 $\text{Inv}H$ 的正规域(根据 § 3.1 的习题 3)。这样, 自然可以提出这样的问题, $\text{Gal}N/\text{Inv}H$ 与 H , $\text{Inv}(\text{Gal}N/L)$ 与 L 各有什么关系。我们有

3.4.2 引理 伽罗华映射具有如下性质:

- 1) $\text{Gal}(N/\text{Inv}H) = H$;
- 2) $\text{Inv}(\text{Gal}N/L) = L$.

证明

1) 为书写方便, 设 $\text{Gal}(N/\text{Inv}H) = H_1$.

首先由于 H 的元是 N 在 F 上的自同构, 并且使 $\text{Inv}H$ 的元保持不动, 故 H 的元是 N 在 $\text{Inv}H$ 上的自同构, 因之

$$(3) \quad H \subseteq H_1$$

其次, 由 3.2.6, $|\text{Gal}(N/\text{Inv}H)| = [N : \text{Inv}H]$. 设 $[N : \text{Inv}H] = k$, $\text{Inv}H = L$, 则存在一个 k 次不可约多项式 $g(x) \in L[x]$, 且有 $g(\theta) = 0$, $N = L(\theta)$. 令

$$H = \{\tau_1 = \varepsilon, \tau_2, \dots, \tau_m\}$$

考虑多项式

$$h(x) = (x - \theta^{\tau_1})(x - \theta^{\tau_2}) \cdots (x - \theta^{\tau_m})$$

$h(x)$ 的 m 个根为

$$(4) \quad \theta^{\tau_1}, \quad \theta^{\tau_2}, \quad \dots, \quad \theta^{\tau_m}$$

对于任意 $\tau \in H$, 显然有

$$H = \{\tau_1\tau, \tau_2\tau, \dots, \tau_m\tau\}$$

故

$$(5) \quad \theta^{\tau_1\tau}, \theta^{\tau_2\tau}, \dots, \theta^{\tau_m\tau}$$

与(4)只有次序不同. 因之, $h(x)$ 的系数经 H 的任意元 τ 作用后仍保持不动, 这就是说 $h(x) \in L[x]$, 从而 θ 在 L 上的极小多项式 $g(x)$ 是 $h(x)$ 的因式. 于是 $[L(\theta) : L] \leq m$, 但 $L(\theta) = N$, 而 $[N : L] = k$, 因此, $k \leq m$, 即

$$(6) \quad |H_1| \leq |H|$$

由(3)和(6)即得, $H_1 = H$, 即

$$\text{Gal}(N/\text{Inv}H) = H.$$

2) 令 $\text{Inv}(\text{Gal}N/L) = L_1$, 则

$$L_1 = \{a \in N \mid a^\tau = a, \forall \tau \in \text{Gal}N/L\}$$

由1)知, $\text{Gal}N/L_1 = \text{Gal}(N/\text{Inv}(\text{Gal}N/L)) = \text{Gal}N/L$, 即 $\text{Gal}N/L$ 恰为 N 在 L_1 上的伽罗华群 $\text{Gal}N/L_1$, 于是

$$(7) \quad |\text{Gal}N/L| = |\text{Gal}N/L_1|$$

根据3.2.6, 我们有

$$(8) \quad |\text{Gal}N/L| = [N : L]$$

$$(9) \quad |\text{Gal}N/L_1| = [N : L_1]$$

由(7), (8), (9)得

$$[N : L] = [N : L_1]$$

而根据 $\text{Gal}N/L$ 的定义知, $L \subseteq L_1$, 故 $L_1 = L$, 即

$$\text{Inv}(\text{Gal}N/L) = L.$$

根据3·4·2的结论, 我们可得

$$\begin{aligned} H &\xrightarrow{\Phi} \text{Inv} H \xrightarrow{\Psi} \text{Gal}(N/\text{Inv} H) = H, \quad \forall H \in \tilde{H} \\ L &\xrightarrow{\Psi} \text{Gal} N/L \xrightarrow{\Phi} \text{Inv}(\text{Gal} N/L) = L, \quad \forall L \in \tilde{L} \end{aligned}$$

即

$$\Phi \circ \Psi = I_{\tilde{H}}, \quad \Psi \circ \Phi = I_{\tilde{L}}$$

这里“ \circ ”表示映射的乘法, $I_{\tilde{H}}$ 表示 \tilde{H} 到 \tilde{H} 的恒等映射, $I_{\tilde{L}}$ 表示 \tilde{L} 到 \tilde{L} 的恒等映射. 因此, Φ 与 Ψ 都是双射, 并且, $\Psi = \Phi^{-1}$

综合以上讨论, 我们得到

3·4·3 基本定理 I 设 N 是域 F 的正规域, \tilde{H} 和 \tilde{L} 分别由(2)和(1)定义, 则伽罗华映射 Φ 和 Ψ 均为双射, 而且互为逆映射.

由伽罗华映射定义易得

3·4·4 定理 \tilde{H} 与 \tilde{L} 之间的伽罗华映射具有性质: $H_1 \geq H_2 \iff \text{Inv} H_1 \subseteq \text{Inv} H_2$

3·4·3和3·4·4的结论可以用图示意如下:

$$\begin{array}{ccc} \text{Gal} N/F \geq H = \text{Gal} N/L \geq \{\varepsilon\} \\ \downarrow \Phi \quad \uparrow \Psi \\ F \subseteq \text{Inv} H = L \subseteq N \end{array}$$

此图称为伽罗华对应图.

下面给出如何求伽罗华映射的方法.

假定中间域 L 已知, 我们来求 $H = \text{Gal} N/L$.

设 $L = F(\beta_1, \beta_2, \dots, \beta_m)$, 因为 $N = F(\alpha)$, 所以 β_i 是 α 的多项式. 假定 $\text{Gal} N/F$ 中元 τ 把 α 变为 α_1 , 如果我们

在表示 β_i 的 α 的多项式中, 把 α 换成 α_i , 仍然是这个多项式, 那么 τ 就不使 β_i 变动. $\text{Gal}N/F$ 中不使 $\beta_1, \beta_2, \dots, \beta_n$ 变动的元也不使 L 中任意元变动, 因此所有这些元构成的子群就是 $H = \text{Gal}N/L$.

假定 $\text{Gal}N/F$ 的子群 H 已知, 我们来求中间域 $L = \text{Inv}H$.

设 $H = \{\tau_1 = \varepsilon, \tau_2, \dots, \tau_m\}$. 由 3.4.2 的证明中可知多项式

$$g(x) = (x - \alpha^{\tau_1})(x - \alpha^{\tau_2}) \cdots (x - \alpha^{\tau_m})$$

的系数都在 L 中, 因此把这些系数添加于 F 得到的扩域 $L' \subseteq L$, 并且 $[N : L'] \leq m$, 于是由次数定理推出 $[L : L'] = 1$, 因此 $L' = L$. 这就是说, 把 $\alpha^{\tau_1}, \alpha^{\tau_2}, \dots, \alpha^{\tau_m}$ 的初等对称多项式添加于 F 所得的扩域就是所求的 $L = \text{Inv}H$.

例 1 § 3.2 的例 3 中 $Q(\theta)$ 是 Q 的正规域, 这里 θ 是 $x^4 + x^3 + x^2 + x + 1 = 0$ 的一个根, $[Q(\theta) : Q] = 4$, 设

$$\text{Gal}Q(\theta)/Q = \{\tau_1 = \varepsilon, \tau_2, \tau_3, \tau_4\}$$

而 $\text{Gal}Q(\theta)/Q \cong Z_4^*$. Z_4^* 是循环群, 它只有一个真子群, 即 $H = \{\tau_1, \tau_4\}$, 因之 $\text{Gal}Q(\theta)/Q$ 共有三个子群, 于是 $Q(\theta)$ 与 Q 的中间域也有三个. 于是有

$$\Phi: \quad \{\varepsilon\} \mapsto Q(\theta)$$

$$H \mapsto Q(\theta^{\tau_1} + \theta^{\tau_4}, \theta^{\tau_1}\theta^{\tau_4}) = Q(\theta + \theta^4)$$

$$\text{Gal}Q(\theta)/Q \mapsto Q$$

例 2 § 3.3 中的例 3 给出方程 $x^3 - 2 = 0$ 的伽罗华群 $G = \text{Gal}N/Q$, 这里 $N = Q(\sqrt[3]{2}, \omega)$. 又知

$$G = \{\tau_1 = \varepsilon, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6\}$$

	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6
(10) $\sqrt[3]{2} \mapsto$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
$\omega \mapsto$	ω	ω	ω	ω^2	ω^2	ω^2

由 § 3.3 的(1)可知 $G \cong S_3$, 由此可得 G 共有 6 个子群:

$$\{\tau_1\}, H_1 = \{\tau_1, \tau_2, \tau_3\}, H_2 = \{\tau_1, \tau_4\},$$

$$H_3 = \{\tau_1, \tau_5\}, H_4 = \{\tau_1, \tau_6\}, G.$$

由(10)直接看出 $\{\tau_1\}, H_1, H_2, G$ 在 Φ 之下的象分别为 $N, L_1 = Q(\omega), L_2 = Q(\sqrt[3]{2}), Q$. 因为 $(\sqrt[3]{2}\omega^2)^{\tau_5} = \sqrt[3]{2}\omega^2, (\sqrt[3]{2}\omega)^{\tau_6} = \sqrt[3]{2}\omega$, 再利用 3.2.6 可知 H_3 和 H_4 在 Φ 之下的象分别为 $L_3 = Q(\sqrt[3]{2}\omega^2), L_4 = Q(\sqrt[3]{2}\omega)$. 于是, 我们有

$$\Phi: \{\tau_1\} \mapsto N$$

$$H_1 \mapsto L_1$$

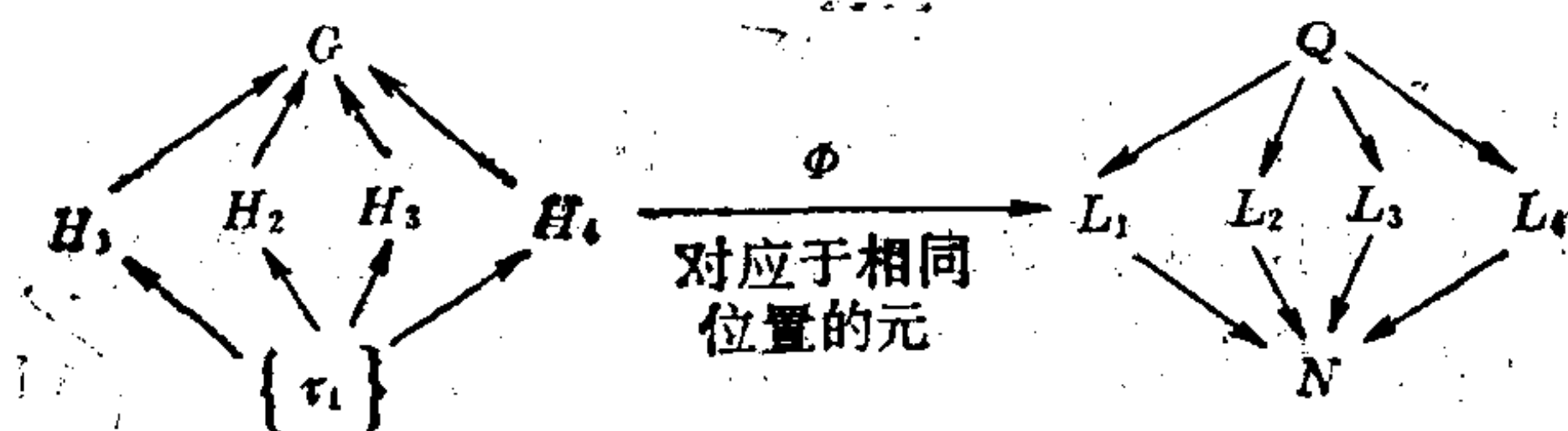
$$H_2 \mapsto L_2$$

$$H_3 \mapsto L_3$$

$$H_4 \mapsto L_4$$

$$G \mapsto Q$$

这种对应关系可以用图 3-1 来表示:



$H \rightarrow K$ 表示 H 是 K 的子群

$M \rightarrow P$ 表示域 $M \subseteq P$

图 3-1

在这个例子中, 由于 $\sqrt[3]{2}$ 在 \mathbb{Q} 上的共轭元 $\sqrt[3]{2}\omega$ 不属于 $\mathbb{Q}(\sqrt[3]{2})$, 所以 $L_2 = \mathbb{Q}(\sqrt[3]{2})$ 不是 \mathbb{Q} 的正规域, 可以验证相应于 G 的子群 H_2 不是 G 的不变子群. 然而 $L_1 = \mathbb{Q}(\omega)$ 是 \mathbb{Q} 的正规域, 相应的子群 H_1 是 G 的不变子群. 这个结果可以推广到一般情形.

3.4.5 基本定理 II 设 Φ 是伽罗华映射, 如果 $H \triangleleft \text{Gal} N/F$, 则 $H^\Phi = \text{Inv} H$ 是 F 的正规域, 反之亦然, 并且

$$\text{Gal} N/F / \text{Gal} N/L \cong \text{Gal} L/F$$

证明 设 $H \triangleleft \text{Gal} N/F$, $L = \text{Inv} H$. 我们要证明, 对于任意的 $a \in L$, a 在 F 上的共轭元属于 L . 为此, 先来证明 a 在 F 上的共轭元一定具有 a^τ 的形式, $\tau \in \text{Gal} N/F$. 令

$$\text{Gal} N/F = \{\tau_1 = \varepsilon, \tau_2, \dots, \tau_n\}$$

对于任意 $\tau \in \text{Gal} N/F$, 仍然有,

$$\text{Gal} N/F = \{\tau_1 \tau, \tau_2 \tau, \dots, \tau_n \tau\}$$

现考虑多项式

$$f(x) = \prod_{i=1}^n (x - a^{\tau_i})$$

显然有

$$f(x) = \prod_{i=1}^n (x - a^{\tau_i \tau})$$

故 $f(x)$ 的系数在任意 τ 的作用下不变, 即 $f(x) \in F[x]$. 由 $f(a) = 0$, 因之 a 在 F 上的极小多项式 $g(x)$ 整除 $f(x)$. 如果 b 与 a 在 F 上共轭, 则 $g(b) = 0$, 故存在 $\tau \in \text{Gal} N/F$ 使得 $b = a^\tau$.

由此, 只要证明, 对于任意 $\tau \in \text{Gal} N/F$, 任意 $a \in L$, 均有 $a^\tau \in L$, 则 L 即为 F 的正规域.

因为 $H \triangleleft \text{Gal}N/F$, 所以, 对于任意 $\tau \in \text{Gal}N/F$, 任意 $\sigma \in H$, 都有 $\tau\sigma\tau^{-1} \in H$. 设 $a \in L = \text{Inv}H$, 则 $a^{\tau\sigma\tau^{-1}} = a$, 从而 $a^{\tau\sigma} = a^{\tau}$, 即 a^{τ} 在 σ 之下不变. 故 $a^{\tau} \in L$, 即 L 是 F 的正规域.

反之, 设 L 是 F 的正规域, $a \in L$, $\sigma \in \text{Gal}N/F$, 由 3·2·5 知 a^{σ} 与 a 共轭, 因而 $a^{\sigma} \in L$, 故 $\text{Gal}N/F$ 的元 σ 可诱导出 L 的一个自同构 σ' :

$$a^{\sigma'} = a^{\sigma}, \quad \forall a \in L$$

因为对于任意 $a \in F$, 都有 $a^{\sigma} = a$, 故 $a^{\sigma'} = a$, 即 σ' 是 L 在 F 上的自同构, L 是 F 的正规域, $\sigma' \in \text{Gal}L/F$. 作 $\text{Gal}N/F$ 到 $\text{Gal}L/F$ 内的一个映射 ρ :

$$\rho: \sigma \mapsto \sigma'$$

容易验证 ρ 是一个同态映射.

我们来看 ρ 的核. 由 $\rho: \sigma \mapsto \varepsilon$ 可得对于任意的 $a \in L$ 都有 $a^{\sigma} = a$, 因而 ρ 的核是 H , 所以 $H \triangleleft \text{Gal}N/F$. 又 $H = \text{Gal}N/L$, 由同态基本定理可知

$$\text{Gal}N/F / \text{Gal}N/L \cong \text{Gal}L/F \text{ 的一个子群}$$

设 $[N:L] = r$, $[L:F] = s$, 则 $[N:F] = rs$, 因之

$$|\text{Gal}N/F / \text{Gal}N/L| = rs/r = s$$

而 $|\text{Gal}L/F| = s$, 所以

$$\text{Gal}N/F / \text{Gal}N/L \cong \text{Gal}L/F.$$

习 题

1. 设 $N = Q(\sqrt[4]{3}, i)$, 找出 $\text{Gal}N/Q$ 的所有子群, 并找出与这些子群对应的 N 与 Q 的中间域.

2. 设 $N = Q(\sqrt[4]{2}, i)$, 找出 $\text{Gal}N/Q$ 的所有子群, 何者是不变子群; 找出这些子群对应的 N 与 Q 的中间域, 何者是 Q 的正规域.

3. 如果 $\text{Gal}N/F$ 的子群 $H \cong \text{Gal}N/F$, 则 N 中存在一元 $a \notin F$, a 在 H 的任何元作用下不变.

4. 设 N 是 F 上的有限扩域, G 是 N 在 F 上的自同构群, $L = \{x \in N \mid x^\tau = x, \tau \in G\}$, 证明, N 是 F 上正规域的充分必要条件是 $F = L$.

5. 令 E 是 F 的一个扩域, 而 I_1 及 I_2 是两个中间域, 若 I_1 与 I_2 之间存在一个使 F 不动的同构映射, 我们就说 I_1 与 I_2 是 F 上的共轭域. 令 G 是一个群, 而 H_1 及 H_2 是 G 的两个子群, 若是存在 G 的元 a , 使 $H_2 = aH_1a^{-1}$, 我们就说 H_1 与 H_2 是共轭子群.

令 N 是域 F 的一个正规域, G 是 N 在 F 上的伽罗华群, 而 I_1 与 I_2 是两个中间域. 证明, 在伽罗华映射之下, I_1 与 I_2 共轭的充分必要条件是: 与它们对应的 G 的子群 H_1 与 H_2 共轭.

第四章 伽罗华理论的应用

本章是应用伽罗华理论的基本定理来讨论方程的根号解，给出方程可用根号解的充要条件，并且得出五次和五次以上一般方程不能用根号解；进一步给出方程不能用根号解的具体例子；最后讨论了圆规和直尺作图问题。

§ 4.1 单位根和循环扩域

在讨论方程的根号解时，域 F 上二项方程 $x^n - a = 0$ 占有突出的地位。由于 $\sqrt[n]{a}$ 是方程 $x^n - a = 0$ 的一个根，所以我们称 $F(\sqrt[n]{a})$ 为 F 的根次数是 n 的根号扩域。

以下我们就研究域 F 上根号扩域 $F(\sqrt[n]{a})$ ，主要研究方程 $x^n - a = 0$ 的伽罗华群。先从最简单的方程 $x^n - 1 = 0$ 研究开始。

在 F 上作方程 $x^n - 1 = 0$ 的根域 N ，这个方程的根叫做 n 次单位根。若 n 是使 $\varepsilon^n = 1$ 的最小正整数，称 ε 是 n 次本原单位根，简称 n 次本原根。我们知道 n 次本原根一共有 $\varphi(n)$ 个，这里 $\varphi(n)$ 表示一切小于 n 且与 n 互素的正整数的个数。称 $\varphi(n)$ 为欧拉函数。

4.1.1 引理 一切 n 次单位根对乘法来说作成循环群 G 。

证明 任取 $\varepsilon_1, \varepsilon_2 \in G \Rightarrow (\varepsilon_1 \varepsilon_2)^n = \varepsilon_1^n \varepsilon_2^n = 1 \Rightarrow \varepsilon_1 \varepsilon_2 \in G$ ，又 $\varepsilon \in G$ ， $\varepsilon \cdot \varepsilon^{n-1} = 1 \Rightarrow \varepsilon^{n-1}$ 是 ε 的逆元。 $(\varepsilon^{n-1})^n = (\varepsilon^n)^{n-1}$

$= 1 \Rightarrow \varepsilon^{-1} \in G$, 即它是方程 $x^n - 1 = 0$ 的根域 N 的乘群的子群, 所以 G 是一个有限可换群.

令 m 是 G 的元的阶中最大者, 那么有

$$\varepsilon_i^m = 1 \text{ 对于任意 } \varepsilon_i \in G,$$

这就是说, 多项式 $x^m - 1$ 至少有 n 个根, 由此推出 $m \geq n$, 但 $m \leq n$, 于是推出 $m = n$. 这就是说, G 有一元 ε , 它的阶为 n , 因而 G 是一个循环群.

4.1.2 定理 方程 $x^n - 1 = 0$ 在 F 上的伽罗华群是交换群.

证明 设 ε 是任一 n 次本原根, G 是方程 $x^n - 1 = 0$ 的伽罗华群.

任 $\tau \in G$, $\tau: \varepsilon \mapsto \varepsilon^i$, 这里 i 是小于 n 的正整数, 则 ε^i 也是 n 次本原根. 于是 $(i, n) = 1$. 设 G' 是整数模 n 的既约剩余类的乘法群, 知 G' 是可换群. 令

$$\varphi: \tau \mapsto \overline{i} \text{ 若 } \varepsilon^\tau = \varepsilon^i.$$

因为 ε^i 是本原根, 所以 $(i, n) = 1$, 因之 $\overline{i} \in G'$. 即 φ 是 G 到 G' 的一个映射. 又令

$$\sigma: \varepsilon \mapsto \varepsilon^j$$

若 $\tau \neq \sigma \Rightarrow \varepsilon^\tau \neq \varepsilon^\sigma \Rightarrow \varepsilon^i \neq \varepsilon^j \Rightarrow i \neq j \Rightarrow \overline{i} \neq \overline{j}$, 所以 φ 是 G 到 G' 的一个单射. 令

$$\varphi: \tau \mapsto \overline{i}, \quad \sigma \mapsto \overline{j}$$

由于 $\varepsilon^{\tau\sigma} = (\varepsilon^\tau)^\sigma = (\varepsilon^i)^\sigma = (\varepsilon^\sigma)^i = \varepsilon^{ji} = \varepsilon^{ij}$. 所以

$$\varphi: \tau\sigma \mapsto \overline{ij} = \overline{i} \overline{j}$$

因而 φ 是 G 到 G' 内的一个同构映射. 即 G 和 G' 的一个子群同构. 由于 G' 是可换群, 所以 G' 的子群也是可换群, 故 G 是可换群.

4.1.3 推论 设 p 为素数, 方程 $x^p - 1 = 0$ 在 F 上的伽罗华群 G 是循环群.

证明 因 p 为素数, 所以由 4.1.2 知 $G' = \{\overline{1}, \overline{2}, \dots, \overline{p-1}\}$, 但 G' 对剩余类的乘法做成一个循环群, 又由于循环群的子群还是循环群, 所以 G 为循环群.

现在研究方程 $x^n - a = 0$ 的伽罗华群.

4.1.4 定理 设域 F 含有一切 n 次单位根, 则方程 $x^n - a = 0 (a \neq 0)$ 在 F 上的伽罗华群是循环群.

证明 设 $\varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}, \varepsilon^n = 1$, 是方程 $x^n - 1 = 0$ 的 n 个根, G 是方程 $x^n - a = 0$ 的伽罗华群.

若 α 是方程 $x^n - a = 0$ 的一个根, 则每一 $\varepsilon^i \alpha$ 都是 $x^n - a = 0$ 的根. $\alpha \neq 0 \Rightarrow \varepsilon^i \alpha \neq \varepsilon^j \alpha, i \neq j (i, j = 1, 2, \dots, n)$. 故 $\varepsilon^i \alpha (i = 1, 2, \dots, n)$ 是 $x^n - a = 0$ 的 n 个不同的根.

任 $\tau \in G, \tau: \alpha \mapsto \varepsilon^i \alpha$, 我们规定

$$\varphi: \tau \mapsto \varepsilon^i$$

则 φ 是 G 到出现 ε^i 所成的集合上的满单射.

若 $\varphi: \tau \mapsto \varepsilon^i, \lambda \mapsto \varepsilon^j$, 则 $a^{\tau\lambda} = (\varepsilon^i \alpha)^\lambda = \varepsilon^i \alpha^\lambda = \varepsilon^i (\varepsilon^j \alpha) = (\varepsilon^i \varepsilon^j) \alpha$, 故

$$\varphi: \tau\lambda \mapsto \varepsilon^i \varepsilon^j.$$

所以 G 与一切 n 次单位根所成之循环群的一个子群同构, 因而 G 是群循环.

4.1.5 推论 在 $F[x]$ 中, $x^p - a$ (p 为素数) 或是不可约, 或是完全分解.

证明 阶为素数 p 的群子群或是它本身, 或是单位元群. 设 N 是方程 $x^p - a = 0$ 在 F 上的根域, G 是它的伽罗华群, 由 4.1.4 知 G 的阶等于 p 或 1 . 若 G 的阶 $= p$, $[N : F] = p$, $N = F(\alpha)$, 即是说 α 在 F 上的次数 $= p$. 但 α 又是

$x^p - a$ 的根, 故 $x^p - a$ 是 a 在 F 上的极小多项式, 因之 $x^p - a$ 在 F 上不可约.

若 G 的阶为 1, $[N : F] = 1 \Rightarrow N = F$, $x^p - a$ 在 F 上完全分解.

为了讨论方便, 我们给出如下

4.1.6 定义 设 N 是 F 的正规域, 若 $\text{Gal} N/F$ 是循环群, 则称 N 是 F 的循环扩域.

由此定义和 4.1.4 知, 域 F 上方程 $x^n - a = 0$ 的根域 N 是 F 的循环扩域.

4.1.4 的逆定理也是成立的, 我们只讨论 n 为素数的情况, 为此, 我们先证明一个引理.

4.1.7 引理 若 $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$ 是一切 n 次单位根, 则

$$\varepsilon_1^k + \varepsilon_2^k + \dots + \varepsilon_n^k = 0 \quad k = 1, 2, \dots, n-1.$$

证明 不妨假定 $\varepsilon_i = \varepsilon^i$, ε 是 n 次本原根.

$$\begin{aligned} \varepsilon_1^k + \varepsilon_2^k + \dots + \varepsilon_n^k &= \varepsilon^k + (\varepsilon^k)^2 + \dots + (\varepsilon^k)^n \\ &= \varepsilon^k + \varepsilon_k^2 + \dots + \varepsilon_k^n = \varepsilon_k(1 - \varepsilon_k^n)/(1 - \varepsilon_k) = 0 \\ &\quad (\varepsilon_k = \varepsilon^k \neq 1). \end{aligned}$$

4.1.8 定理 设域 F 包含一切 p (p 为素数) 次单位根, 若 N 是 F 的一个 p 次循环扩域, 则 $N = F(\alpha)$, 其中 α 是方程 $x^p - a = 0$ ($a \in F$) 的一个根.

证明 令 $\varepsilon, \varepsilon^2, \dots, \varepsilon^{p-1}, \varepsilon^p = 1$ 表示一切 p 次单位根, $\text{Gal} N/F = \{\tau, \tau^2, \dots, \tau^{p-1}, \tau^p = \varepsilon\}$, N 是域 F 的 p 次循环扩域, $N = F(\theta)$. 令

$$\alpha_j = \theta + \varepsilon_j \theta^\tau + \dots + \varepsilon_j^{p-1} \theta^{\tau^{p-1}}, \quad j = 1, 2, \dots, p.$$

(这个式子称为 Lagrange 预解式). 由 4.1.7

$$\sum_{j=1}^p a_j = p\theta \quad \text{故} \quad \theta = \frac{\sum_{j=1}^p a_j}{p}$$

其中至少有一 $a_i \notin F$, 否则 $\theta \in F$, 矛盾.

$$\begin{aligned} \alpha_i^p &= \theta^p + \varepsilon_i \theta^{\tau^2} + \varepsilon_i^2 \theta^{\tau^3} + \cdots + \varepsilon_i^{p-2} \theta^{\tau^{p-1}} + \varepsilon_i^{p-1} \theta^{\tau^p} \\ &= \varepsilon_i^{p-1} (\theta + \varepsilon_i \theta^{\tau} + \cdots + \varepsilon_i^{p-1} \theta^{\tau^{p-1}}) = \varepsilon_i^{p-1} a_i \end{aligned}$$

又 $(\alpha_i^p)^\tau = (\alpha_i^p)^p = (\varepsilon_i^{p-1})^p a_i^p = a_i^p$, 故 α_i^p 在 $\text{Gal} N/F$ 作用下不变, 所以 $\alpha_i^p = a \in F$. 即 a_i 是方程 $x^p - a = 0$ 的一个根, 由 4.1.5 $x^p - a$ 在 F 上不可约, 因之, $N = F(a_i)$. 取 $a = a_i$, 则 $N = F(a)$, 而 a 是 $x^p - a = 0$ 的一个根.

习 题

1. 令 n 是任意给定的一个正整数, 方程 $x^n - 1 = 0$ 在 F 上的伽罗华群是不是一个循环群?

2. 如果基域 F 不含 n 次单位根, 那么方程 $x^n - a = 0$ 的伽罗华群是不是交换群?

§ 4.2 方程可用根号解的充要条件

有了以上的准备, 我们就可以讨论用根号解方程. 本节我们给出方程可用根号解的充要条件, 并且得到 Abel-Ruffini 定理.

让我们先看一下, 能用根号解的方程的求根公式有什么特点.

我们看 \mathbb{Q} 上二次一般方程

$$x^2 - ax + b = 0$$

可看成 $F = \mathbb{Q}(a, b)$ 上的方程。把 $\sqrt{D} = \sqrt{a^2 - 4b}$ 添加到 F 上得到的扩域 $F(\sqrt{D})$ 中包含了 $f(x)$ 的所有根。 $x = (a \pm \sqrt{D})/2$ 。对于高于二次的方程能用根号解也是这个意思，此时的添加元不一定是平方根，而是一般的 n 次方根，而且可能是多次添加才能得到一个扩域使方程的所有根含于这个扩域内。为了叙述简洁，我们形象地采用根塔这个术语：即扩域 K/F 的如下子域塔

$$F = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_i \subseteq F_{i+1} \subseteq \cdots \subseteq F_r \subseteq F_{r+1} = K$$

其中每个 $F_{i+1} = F_i(a_i)$, $a_i^{n_i} = a_i \in F_i$, $i = 1, 2, \dots, r$ 。称为 K/F 的根塔。下面我们就精确地给出方程可用根号解的定义。

4.2.1 定义 设 $f(x)$ 是域 F 上某一首项系数是 1 的多项式，称方程 $f(x) = 0$ 在 F 上可用根号解，如果存在 F 的某个扩域 K 满足以下条件：

1) K 包含了 $f(x)$ 在 F 上的分裂域 E ，即

$$F \subseteq E \subseteq K$$

2) 扩域 K/F 有如下根塔

$$F = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r \subseteq F_{r+1} = K$$

其中每个 $F_{i+1} = F_i(a_i)$, $a_i^{n_i} = a_i \in F_i$, $i = 1, 2, \dots, r$ 。对应的自然数集 $\{n_1, n_2, \dots, n_r\}$ 称为此根塔的根次数集。并称 K 为 F 的根次数集是 $\{n_1, n_2, \dots, n_r\}$ 的根号扩域。简称 K/F 为根号扩域。

用这种条件定义的方程可用根号解是否合理？因为每个 F_{i+1} 是把 $F_i[x]$ 中某个 n_i 次方程 $x^{n_i} - a_i = 0$ 的一个根 $a_i = \sqrt[n_i]{a_i}$ 添加到 F_i 上而得的单代数扩域，所以 F_{i+1} 中每个元都可表为 a_i 的多项式，系数属于 F_i ，即 F_{i+1} 中的

每个元都可由 P_i 中的元经过有限次加减乘除和开 n_i 次方运算得出, 因为 $f(x)=0$ 的所有根都在 $f(x)$ 的分裂域 E 中, 因而也在 K 中, 所以 $f(x)=0$ 的每一个根都可利用 $f(x)$ 的系数, 经过有限次加减乘除和开 n_i 次方运算表示, 这恰好是通常所说的方程可用根号解的含义, 因此定义是合理的.

例 有理数域 \mathbb{Q} 上二项方程

$$x^5 - p = 0 \quad (p \text{ 为素数})$$

可用根号解.

因为 $x^5 - p = 0$ 的五个根为 $\sqrt[5]{p}$, $\varepsilon\sqrt[5]{p}$, $\varepsilon^2\sqrt[5]{p}$, $\varepsilon^3\sqrt[5]{p}$, $\varepsilon^4\sqrt[5]{p}$, 这里 $\varepsilon = \cos 72^\circ + i\sin 72^\circ$ 是五次本原根.

取 $\alpha = 18^\circ$, 则由 $\sin 3\alpha = 3\sin\alpha - 4\sin^3\alpha$, $\cos 2\alpha = 1 - 2\sin^2\alpha$ 得 $4\sin^2\alpha + 2\sin\alpha - 1 = 0$, 故有

$$\sin 18^\circ = \frac{\sqrt{5} - 1}{4} = \cos 72^\circ$$

$$\sin 72^\circ = \frac{1}{4} \sqrt{10 + 2\sqrt{5}} = \cos 18^\circ$$

于是

$$\varepsilon = \frac{1}{4} \left(-1 + \sqrt{5} + \sqrt{-10 - 2\sqrt{5}} \right)$$

我们构造一个根塔

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[5]{p}) \subset \mathbb{Q}(\sqrt[5]{p}, \sqrt{5}) \subset \mathbb{Q}(\sqrt[5]{p}, \sqrt{5}, \sqrt{-10 - 2\sqrt{5}}) = K,$$

其中相邻两域次数依次为 5, 2, 2, 而且都是添加一个根号所得的扩域. K 中包含了 $x^5 - p = 0$ 的所有根, 所以方程 $x^5 - p = 0$ 可用根号解.

下面我们讨论方程可用根号解的充要条件，为此需要用到伽罗华的基本定理，但是伽罗华基本定理仅讨论正规域，而且有根塔的扩域 K/F 未必为正规域。因此首先解决以下重要定理。

4.2.2 定理 设 K 是 F 的根号扩域，则存在 F 的正规根号扩域 N ，使 $F \subseteq K \subseteq N$ 。

证明：设 K/F 的根塔为

$$(1) \quad F = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r \subseteq F_{r+1} = K$$

$$F_{i+1} = F_i(\alpha_i), \quad \alpha_i^{n_i} = a_i \in F_i$$

我们对 r 用数学归纳法

当 $r=1$ 时， $K = F_2 = F_1(\alpha_1) = F(\alpha_1)$ ，其中 $\alpha_1^{n_1} = a_1 \in F$ ，取 ε_1 是 n_1 次本原根，令 $N = F(\varepsilon_1, \alpha_1)$ ，则 $N \supseteq K$ ，而 N 显然是 F 的根号扩域。由于 N 是 $x^{n_1} - a_1 = 0$ 的根域，故 N 是 F 的正规域。

假定对 $r-1$ 定理成立，即是说存在 F 的正规根号扩域 N' ，而 $N' \supseteq F_r$ 。

$K = F_{r+1} = F_r(\alpha_r)$ ， α_r 是 $x^{n_r} - a_r = 0$ 的根，而 $a_r \in F_r \subseteq N'$ 。令 G 是 N' 在 F 上的伽罗华群，考虑

$$\prod_{\tau \in G} (x^{n_r} - a_r^\tau) = f(x) \in F[x].$$

在 N' 上作 $f(x)$ 的分裂域 N ，因 $N' \supseteq F_r \Rightarrow N \supseteq K = F_{r+1}$ 。由于 N' 是根号扩域，而 $f(x)$ 的每个根都可用开 n_r 次根号表示，故 N 是 F 的根号扩域。

又 $N = N'(a^{(1)}, \dots, a^{(s)})$ ，某一 $a^{(i)} = a_r$ ，这里 $a^{(1)}, \dots, a^{(s)}$ 是 $f(x)$ 的全部根，而 N' 又是 F 上某个多项式 $g(x)$ 的分裂域。所以 N 是 F 上 $g(x)f(x)$ 的分裂域，所以 N 是 F 的正规扩域。即有 F 的正规根号扩域 N ，使 $F \subseteq K$

$\subseteq N$.

在证明方程可用根号解的充要条件之前, 我们再来证明一个引理.

4.2.3 引理 令 $N = F(\alpha)$ 是 F 的一个正规扩域, 而域 $K \supseteq F$, 又假定 N 与 K 同属于一域 Ω , 则 $K(\alpha)$ 是 K 的正规扩域, 并且 $K(\alpha)$ 在 K 上的伽罗华群 G' 与 N 在 F 上的伽罗华群 G 的一个子群同构.

证明 设 $f(x)$ 是 α 在 F 上的极小多项式, $g(x)$ 是 α 在 K 上的极小多项式, 于是 $g(x) \mid f(x)$, 由于 N 是 F 的正规域, 所以在 N 中 $f(x)$ 完成分解:

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

又 $K(\alpha) \supseteq N$, 所以 $f(x)$ 在 $K(\alpha)$ 中完全分解, 因之 $g(x)$ 在 $K(\alpha)$ 中也完全分解, 不妨假设:

$$g(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r)$$

于是 $K(\alpha)$ 是 K 上 $g(x)$ 的分裂域. 故 $K(\alpha)$ 是 K 的正规域.

$$\text{设 } G = \{\tau_1, \tau_2, \dots, \tau_n\} \quad \tau_i: F(\alpha) \rightarrow F(\alpha_i) \\ i = 1, 2, \dots, n,$$

$$G' = \{\tau'_1, \tau'_2, \dots, \tau'_r\} \quad \tau'_i: K(\alpha) \rightarrow K(\alpha_i) \\ i = 1, 2, \dots, r.$$

$$\text{令 } \tau'_i \mapsto \tau_i$$

这显然是 G' 到 G 的一个单射, 对应的 τ 对于 $N = F(\alpha)$ 来说作用一样, 即:

$$\tau'_i \tau'_j = \tau'_h \Rightarrow \tau_i \tau_j = \tau_h$$

因此 G' 与 G 的一个子群同构.

4.2.4 定理 域 F 上的一个方程 $f(x) = 0$ 在 F 上可用根号解的充要条件是: 这个方程在 F 上的伽罗华群是可解群.

证明 (i) 先证条件是必要的.

假定方程 $f(x)=0$ 在 F 上可用根号解, 根据 4·2·1 和 4·2·2 知必存在 F 的某个正规扩域 K , 它有根塔

$$(2) \quad F = F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r \subseteq F_{r+1} = K$$

$$F_{i+1} = F_i(a_i), \quad a_i^{n_i} = a_i \in F_i \quad i = 1, 2, \cdots, r.$$

且 K 包含 $f(x)$ 在 F 上的分裂域 E .

设根塔(2)中所有根次数 n_1, n_2, \cdots, n_r 的最小公倍数是 n , 任意取定一个 n 次本原根 ε , 我们先把 ε 添加到(2)中每个域上去, 即令

$$K_i = F_i(\varepsilon), \quad i = 1, 2, \cdots, r, r+1.$$

那么从根塔(2)又可得到 $K(\varepsilon)/F$ 的一个根塔

$$(3) \quad F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_r \subseteq K(\varepsilon) = K_{r+1}.$$

这里

$$K_1 = F(\varepsilon) = K_0(\varepsilon)$$

$$K_{i+1} = F_{i+1}(\varepsilon) = F_i(\varepsilon, a_i) = K_i(a_i)$$

$$a_i^{n_i} = a_i \in F_i \subseteq K_i, \quad i = 1, 2, \cdots, r$$

因为 K 是 F 的正规域, 所以 K 必是某个 $g(x) \in F[x]$ 在 F 上的分裂域, 因为 ε 是 n 次本原根, $x^n - 1 = 0$ 的根都是 ε 的方幂, 所以 $K(\varepsilon)$ 就是 $g(x)(x^n - 1) \in F[x]$ 在 F 上的分裂域, 因而 $K(\varepsilon)$ 必是 F 的正规域, $K(\varepsilon)$ 也是每个 K_i 的正规域, $i = 0, 1, 2, \cdots, r$. 记

$$H_i = \text{Gal} K(\varepsilon)/K_i$$

则 $K_i = \text{Inv} H_i, \quad i = 0, 1, \cdots, r$. 现在考虑伽罗华对应图

$$F = K_0 \subseteq \cdots \subseteq K_i \subseteq K_{i+1} \subseteq \cdots \subseteq K_r \subseteq K_{r+1} = K(\varepsilon)$$

$$H_0 \supseteq \cdots \supseteq H_i \supseteq H_{i+1} \supseteq \cdots \supseteq H_r \supseteq H_{r+1} = \{e\}$$

因为 $K_1 = F(\varepsilon)$ 是 $x^n - 1$ 在 F 上的分裂域, 由 4·1·2 知

$\text{Gal}K_i/F$ 是交换群, 对于任一 $i(1 \leq i \leq r)$, 由于 K_i 中包含了 n_i 次本原根 $\varepsilon^{\frac{n}{n_i}}$, 而 $K_{i+1} = K_i(\alpha_i)$ 是 $x^{n_i} - a_i \in K_i[x]$ 在 K_i 上的分裂域, 由 4.1.4 知 $\text{Gal}K_{i+1}/K_i$ 也是交换群. 于是应用伽罗华基本定理 II, 由 K_{i+1}/K_i 是正规域知 H_{i+1} 是 H_i 的不变子群, 且每个因子群

$$H_i/H_{i+1} \cong \text{Gal}K_{i+1}/K_i$$

都是交换群, 所以 $H_0 = \text{Gal}K(\varepsilon)/F$ 是可解群. 再考虑另一张伽罗华对应图:

$$\begin{array}{ccccc} F & \subseteq & E & \subseteq & K(\varepsilon) \\ \downarrow & & \downarrow & & \downarrow \\ H_0 & \geq & \bar{H} & \geq & \{e\} \end{array}$$

其中 E 是 $f(x)$ 在 F 上的分裂域, $\bar{H} = \text{Gal}K(\varepsilon)/E$, 因为 E 是 F 的正规域, 所以 \bar{H} 是 H_0 的不变子群, 且 $f(x)$ 的伽罗华群

$$G = \text{Gal}E/F \cong H_0/\bar{H}$$

因为 H_0 是可解群, 所以与其商群同构的群 G 也是可解群.

(ii) 证明条件也是充分的.

假定方程 $f(x) = 0$ 的伽罗华群 G 是可解群. 由 1.5.1 知 G 有合成列

$$G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_i \triangleright G_{i+1} \triangleright \cdots \triangleright G_{r+1} = \{e\}$$

且 G_i/G_{i+1} 的阶为素数 p_i , $i = 1, 2, \dots, r$. 设 E 为 $f(x)$ 在 F 上的分裂域, 考虑伽罗华对应图:

$$\begin{array}{ccccccc} G = G_1 & \triangleright & G_2 & \triangleright & \cdots & \triangleright & G_i & \triangleright & G_{i+1} & \triangleright & \cdots & \triangleright & G_{r+1} = \{e\} \\ \updownarrow & & \updownarrow & & & & \updownarrow & & \updownarrow & & & & \updownarrow \\ F = F'_1 & \subset & F'_2 & \subset & \cdots & \subset & F'_i & \subset & F'_{i+1} & \subset & \cdots & \subset & F'_{r+1} = E \end{array}$$

由于 $|G_i/G_{i+1}| = p_i$, 所以 $F'_{i+1} = F'_i(a_i)$ 是 p_i 次循环扩域, 且 $a_i^{p_i} = a_i \in F'_i$. 于是

$$E = F(a_1, a_2, \dots, a_r),$$

作

$$K = F(\varepsilon_1, \dots, \varepsilon_r, a_1, \dots, a_r),$$

这里 ε_i 是 p_i 次本原根. 于是有子域塔

$$(4) \quad F = L_1 \subseteq L_2 \subseteq \dots \subseteq L_{r+1} = F_1 \subseteq F_2 \subseteq \dots \subseteq F_{r+1} = K$$

其中 $L_{i+1} = L_i(\varepsilon_i)$, $\varepsilon_i^{p_i} = 1$, $i = 1, 2, \dots, r$

$$F_{i+1} = F_i(a_i),$$

由 4.2.3 知 F_{i+1} 是 F_i 的正规域, 且其伽罗华群与 F'_{i+1} 在 F'_i 上的伽罗华群的子群同构. 因而得到或是 $F_{i+1} = F_i$ 或是 F_{i+1} 是 F_i 的 p_i 次循环扩域, 由 4.1.8 知,

$$F_{i+1} = F_i(\beta_i), \quad \beta_i^{p_i} = b_i \in F_i,$$

所以 (4) 是 K/F 的根塔, 而且 $K \supseteq E$. 故方程 $f(x) = 0$ 可用根号解.

由 3.3.5 已知 n 次一般方程 $f(x) = 0$ 的伽罗华群是 n 次对称群 S_n , 且由 1.5.5 知当 $n > 4$ 时 S_n 不是可解群, 这样就导出有名的

4.2.5 Abel-Ruffini 定理 当 $n > 4$ 时, 特征为 ∞ 的域上 n 次一般方程不能用根号解.

这个定理只是对 n 次一般方程来说, 对于特殊的 n 次方程, 当 $n > 4$ 时是不是能用根号解? 这个定理不能保证, 我们将在下一节讨论.

习 题

1. 设 $f(x)$ 是 F 上一个不可约多项式, 证明若 $f(x) = 0$ 的一个根可用根号表示 (即此根含在 F 的一个根号扩域中), 则 $f(x) = 0$ 在 F 上

可用根号解.

2. 证明: 域 F 上二项方程 $x^n - a = 0$ 在 F 上的伽罗华群是可解群. 因而 F 上二项方程 $x^n - a = 0$ 可用根号解.

§ 4.3 不能用根号解的方程的例子

上一节我们证明了, 当 $n > 4$ 时, 特征为 ∞ 的一个域上的 n 次一般方程不能用根号解, 但对特殊的 n 次方程来说, 当 $n > 4$ 时是不是能用根号解, 这个定理不能保证. 在某一数域内有些特殊的五次或五次以上方程可以用根号解出, 但是在有理数域内, 总存在五次或五次以上方程它的伽罗华群是 S_n , 因而它不能用根号解, 这一节我们就来解决这个问题.

首先证明以下:

4.3.1 定理 设 $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ 是实系数 n 次多项式, n 是素数, $f(x)$ 在 $F = \mathbb{Q}(a_1, \cdots, a_n)$ 上不可约, 并且 $f(x)$ 有 $n-2$ 个实根, 则 $f(x)$ 在 F 上的伽罗华群 G 与 S_n 同构.

证明 设 $f(x)$ 在 F 上的分裂域为 N , 即 $N = F(a_1, a_2, \cdots, a_n)$, 此处 a_1, a_2, \cdots, a_n 是 $f(x)$ 的全部根, 令 $G = \text{Gal} N/F = \{\tau_1, \tau_2, \cdots, \tau_r\}$, 则由 3.3.2 知

$$G \cong S_n \text{ 的一个子群 } G'$$

今证明 $G' = S_n$.

首先证明 G' 为可迁群, 为此需要证明对于任意 a_k , $1 \leq k \leq n$, 存在 $\sigma \in G$, 使得 $a_1^\sigma = a_k$

令
$$h(x) = \prod_{i=1}^r (x - a_i^{\tau_i})$$

则对任意 $\tau \in G$, 用 τ 作用在 $h(x)$ 的系数上有

$$(h(x))^{\tau} = \prod_{i=1}^r (x - a_i^{\tau}) = \prod_{i=1}^r (x - a_i) = h(x)$$

所以 $h(x) \in F[x]$.

又 $f(a_1) = 0$, 而 $f(x)$ 在 F 上不可约, 所以

$$f(x) \mid h(x)$$

而 $f(x)$ 的任一根有 a_i^{σ} 形, 即对任一根 a_k , 有 $\sigma \in G$, 使 $a_1^{\sigma} = a_k$. 即

$$\varphi: \sigma \mapsto P_{\sigma} = \begin{pmatrix} a_1 & \cdots \\ & \ddots \\ a_k & \cdots \end{pmatrix} \in G'$$

所以 G' 为可迁群.

其次, 我们证明 G' 含有一个对换.

由题设 $f(x)$ 有 $n-2$ 个实根, 故 $f(x)$ 有一对共轭复根, 不妨假定 a_1, a_2 是共轭复数, 而 a_3, a_4, \dots, a_n 是实数, 因 $N = F(a_1, a_2, \dots, a_n)$. 故 $\alpha \in N \Rightarrow \alpha = g(a_1, a_2, \dots, a_n)$, 此处 g 是 F 上 a_1, a_2, \dots, a_n 的多项式. 又

$$\tau: \alpha \mapsto \overline{\alpha} = g(\overline{a_1}, \overline{a_2}, \dots, \overline{a_n}) = g(a_2, a_1, a_3, \dots, a_n)$$

则 $\overline{\alpha} \in N$. 易证 τ 是 N 的一个自同构, 且 τ 使 F 不动, 故 $\tau \in G$. 由 τ 的定义可知

$$a_1^{\tau} = a_2, a_2^{\tau} = a_1, a_i^{\tau} = a_i, i = 3, 4, \dots, n.$$

所以,
$$\tau \mapsto P_{\tau} = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_2 & a_1 & a_3 & \cdots & a_n \end{pmatrix} = (a_1 a_2) \in G'$$

这样我们证明了 G' 含有一个对换.

由于 n 是素数, G' 为可迁群, 且 G' 含有一个对换, 由 1.6.4 定理得 $G' = S_n$.

例 设

$$f(x) = x^5 - p^2x + p$$

p 是任意正的素数.

由于 $f(x)$ 的最高项系数不能被 p 整除, 而其余各项的系数均能被 p 整除, 并且常数项 p 不能被 p^2 整除, 利用艾森施坦因判别法, 知 $f(x)$ 在有理数域 \mathbb{Q} 上不可约.

我们说 $f(x)$ 恰有三个实根, 为此我们需要用到数学分析的以下两个简单事实:

1°. 设 $f(x)$ 是实系数多项式, 且对实数 $a < b$ 来说有 $f(a) > 0$, $f(b) < 0$, 则存在实数 c , 而 $a < c < b$ 使 $f(c) = 0$.

2°. 对 $f(x)$ 的导数 $f'(x)$ 来说, $a < b$ 有 $f(a) = 0$, $f(b) = 0$, 则至少有一实数 c , 而 $a \leq c \leq b$ 使 $f'(c) = 0$.

$$f(x) = x^5 - p^2x + p$$

x	$+\infty$	1	0	$-\infty$
$f(x)$	$+\infty$	< 0	> 0	$-\infty$

由1°知 $f(x)$ 至少有三个实根, 但 $f(x)$ 的实根不能多于三个, 否则 $f(x)$ 有五个实根, 设为

$$a_1 < a_2 < a_3 < a_4 < a_5$$

由2°知 $f'(x)$ 至少有四个实根, 但 $f'(x) = 5x^4 - p^2$ 只有二个实根, 矛盾, 所以 $f(x)$ 恰有三个实根. 于是 $f(x)$ 适合定理条件, $f(x)$ 的伽罗华群 G 与 S_5 同构, 但 S_5 不是可解群, 因之 $f(x)$ 不能用根号解.

习 题

1. 再举一个不能用根号解的五次方程的例子.

§ 4.4 三次方程和它的不可约情形

本节我们给出三次一般方程求根公式，并讨论一下实系数三次方程不可约情形。

为了方便起见，我们在复数域范围内进行讨论。

三次一般方程

$$(1) \quad y^3 + ay^2 + by + c = 0$$

首先经过代换

$$(2) \quad y = x - \frac{a}{3}$$

可以变成

$$(3) \quad x^3 + px + q = 0$$

的形式。

如果求得方程(3)的根，那么由(2)我们就得出所给方程(1)的根。因此，我们只需解方程(3)。

由代数基本定理，方程(3)有三个复数根。设 x_0 为它的任何一个根，引进辅助未知量 u 来讨论多项式

$$f(u) = u^2 - x_0 u - \frac{p}{3}$$

设它的两个根为 α 和 β ，由根与系数关系得

$$(4) \quad \alpha + \beta = x_0$$

$$(5) \quad \alpha\beta = -\frac{p}{3}$$

用根 x_0 的表示式(4)代进(3)中去，我们得出：

$$(\alpha + \beta)^3 + p(\alpha + \beta) + q = 0$$

或

$$\alpha^3 + \beta^3 + (3\alpha\beta + p)(\alpha + \beta) + q = 0$$

但由(5)得 $3\alpha\beta + p = 0$, 故有

$$(6) \quad \alpha^3 + \beta^3 = -q$$

另一方面由(5)推得

$$(7) \quad \alpha^3 \beta^3 = -\frac{p^3}{27}$$

等式(6)和(7)说明了数 α^3 和 β^3 为系数是复数的二次方程

$$(8) \quad z^2 + qz - \frac{p^3}{27} = 0$$

的根。

解方程(8), 我们得出

$$z = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

故

$$(9) \quad \alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

$$\beta = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

我们得到下面的卡当公式, 把方程(3)的根经它的系数用平方根和立方根来表示:

$$x_0 = \alpha + \beta = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

因立方根在复数域中有三个值, 所以(9)式给出 α 的三个值和 β 的三个值。

设 α_1 和 β_1 分别为 α 和 β 的三个值中的任何一个, 则知

α 和 β 的三个值分别为

$$\alpha_1, \alpha_1\omega, \alpha_1\omega^2$$

和

$$\beta_1, \beta_1\omega, \beta_1\omega^2$$

这里 $\omega = \frac{-1 + \sqrt{3}i}{2}$ 为 1 的立方根。

若取 β_1 , 使 $\alpha_1\beta_1 = -\frac{p}{3}$, 则有

$$\alpha_1\omega \cdot \beta_1\omega^2 = \alpha_1\beta_1 = -\frac{p}{3}$$

$$\alpha_1\omega^2 \cdot \beta_1\omega = \alpha_1\beta_1 = -\frac{p}{3}$$

于是方程(3)的三个根可以写成如下形式:

$$(10) \quad \begin{cases} x_1 = \alpha_1 + \beta_1 \\ x_2 = \alpha_1\omega + \beta_1\omega^2 \\ x_3 = \alpha_1\omega^2 + \beta_1\omega \end{cases}$$

关于四次一般方程也有求根公式, 我们不在此来介绍。

下面我们来研究一下实系数不完全三次方程

$$(11) \quad x^3 + px + q = 0$$

的根。在这一情形下, 我们发现卡当公式中平方根下面的表

示式 $\frac{q^2}{4} + \frac{p^3}{27}$ 有重要的作用。

通常我们称

$$D = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$$

为三次方程(11)的判别式。

事实上, 由根与系数的关系, 有

$$(12) \quad \begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1 x_2 + x_2 x_3 + x_1 x_3 = p \\ x_1 x_2 x_3 = -q \end{cases}$$

利用(12)的前两个关系式, 我们得

$$x_1 x_2 - x_3^2 = p$$

$$x_1 x_3 - x_2^2 = p$$

$$x_2 x_3 - x_1^2 = p$$

$$(x_1 - x_2)^2 = -4p - 3x_3^2$$

$$(x_1 - x_3)^2 = -4p - 3x_2^2$$

$$(x_2 - x_3)^2 = -4p - 3x_1^2$$

$$x_1^2 + x_2^2 + x_3^2 = -2p$$

$$x_1^2 x_2^2 + x_2^2 x_3^2 + x_1^2 x_3^2 = p^2$$

于是

$$\begin{aligned} D &= (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 \\ &= (-4p - 3x_3^2)(-4p - 3x_2^2)(-4p - 3x_1^2) \\ &= -64p^3 - 48p^2(x_1^2 + x_2^2 + x_3^2) - 36p(x_1^2 x_2^2 \\ &\quad + x_1^2 x_3^2 + x_2^2 x_3^2) - 27x_1^2 x_2^2 x_3^2 \\ &= -64p^3 - 48p^2(-2p) - 36p \cdot p^2 - 27q^2 \\ &= -4p^3 - 27q^2 \end{aligned}$$

所以 $D = -4p^3 - 27q^2 = -108\left(\frac{q^2}{4} + \frac{p^3}{27}\right)$

于是卡当公式可以写成

$$x_0 = \sqrt[3]{-\frac{q}{2} + \frac{1}{18}\sqrt{-3D}} + \sqrt[3]{-\frac{q}{2} - \frac{1}{18}\sqrt{-3D}}$$

(i) 若方程(11)有一个实根和两个共轭的复根, 于是 $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \sqrt{D}$ 显然是纯虚数, 从而 $D < 0$.

(ii) 若方程 (11) 有三个实根, 这时, \sqrt{D} 是实的, 因之 $D \geq 0$. 在 $D = 0$ 时, 方程 (11) 有两个相等的实根; 当 $D > 0$ 时, 方程 (11) 有三个不相等的实根, 但在 α, β 的表示式中有虚数出现, 我们问这个时候是否能使在它的表示式中没有虚数出现呢? 这是不可能的. 我们管这种情形称三次方程不可约情形. 这一点, 我们用伽罗华理论来证明.

为此我们先证两个引理.

4.4.1 引理 令 $x^p - a$ (p 为素数) 是域 F 上的多项式, 那么, 或者 $x^p - a$ 在 F 上不可约, 或者 a 是 F 中一个元的 p 次方幂.

证明 假定 $x^p - a = h(x)g(x)$, 在复数域内, $x^p - a = \prod_{i=1}^p (x - \varepsilon^i \theta)$, ε 是 p 次本原根, $\theta^p = a$, $h(x)$ 的常数项 $b = \varepsilon' \theta^m$, m 是 $h(x)$ 的次数, ε' 是 p 次单位根. 我们可以推得

$$b^p = (\varepsilon' \theta^m)^p = (\varepsilon')^p (\theta^p)^m = a^m, \quad 0 < m < p,$$

$(m, p) = 1$, 存在整数 s, t , 使得 $sm + tp = 1$, 所以,
 $a = a^{sm} \cdot a^{tp} = b^{sp} \cdot a^{tp} = (b^s \cdot a^t)^p$

令 $b^s \cdot a^t = c$, 则 $a = c^p$, $c \in F$.

4.4.2 引理 若多项式 $f(x) = x^3 + px + q$ 在域 F 上不可约, 且 F 含 \sqrt{D} , 则方程 $f(x) = 0$ 在 F 上的伽罗华群的阶是 3.

证明 令 N 是 $f(x)$ 在 F 上的分裂域, G 为 N 在 F 上的伽罗华群, $f(x)$ 的三个根为 x_1, x_2, x_3 . 因 F 含 \sqrt{D} , 即 F 含 $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$.

设 $\tau \in G$

$$\tau \mapsto \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1^{\tau} & x_2^{\tau} & x_3^{\tau} \end{pmatrix}$$

由 $3 \cdot 3 \cdot 2$ 知 $G \cong S_3$ 的一个子群.

假定某一 $\tau \mapsto (x_1, x_2)$

$$\begin{aligned}\tau: (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) &\mapsto \\ &(x_2 - x_1)(x_1 - x_3)(x_2 - x_3) \\ &= -(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\end{aligned}$$

与 $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \in F$ 不合, 因之在这个映射下 (x_1, x_2) 不出现.

同样地, $(x_1, x_3), (x_2, x_3)$ 也不出现.

所以 $G \cong \{(1), (132), (123)\}$ 的一个子群. 但 $\{(1), (123), (132)\}$ 只有两个子群: 它本身和单位元群 $\{(1)\}$, 显然, $G \cong \{(1)\}$, 故

$$G \cong \{(1), (132), (123)\}.$$

所以 G 的阶为 3.

4.4.3 定理 令 F 是实数域的子域, 假定 F 上的方程

$$f(x) = x^3 + px + q = 0$$

的判别式 $D > 0$, 但 $f(x)$ 在 F 上不可约, 那么方程的根域不可能被包含在 F 的一个实根号扩域中.

证明 假定方程 $f(x) = 0$ 的根域 N 被包含在 $F(r_1, r_2, \dots, r_r)$, 其中 $r_i^{p_i} = a_i \in F(r_1, \dots, r_{i-1})$, r_i 是实数, p_i 为素数. 所以 $N \subseteq F(\sqrt{D}, r_1, \dots, r_r)$ 实根号扩域中, 在 $F(\sqrt{D}, r_1, \dots, r_r)$ 中 $f(x)$ 完全分解, 且在 $F(D)$ 上 $f(x)$ 亦不可约, 因此可找到 r_i 使 $f(x)$ 在 $K = F(\sqrt{D}, r_1, \dots, r_{i-1})$ 上不可约, 但在 $K(r_i)$ 中开始分解. r_i 是方程 $x^{p_i} - a_i = 0$ 的根, $a_i \in F(\sqrt{D}, r_1, \dots, r_{i-1})$.

(i) 证明 $x^{p_i} - a_i = 0$ 在 K 上不可约. 假定 $x^{p_i} - a_i$ 在 K 上可约, 由 4.4.1 知 $a_i = c^{p_i}$, $c \in K$, $\Rightarrow c = \sqrt[p_i]{a_i}$, c 为实数, 当 p_i 是单数时, a_i 有一个实根, 当 p_i 是双数时,

a_i 有两个实根, 所以 $r_i = c$ 或 $r_i = -c$, 因之 $r_i \in K$ 矛盾.

所以, $x^{p_i} - a_i$ 在 K 上不可约.

(ii) 证明 $K(r_i)$ 是 K 的正规扩域. 由 (i) 知 $x^{p_i} - a_i$ 在 K 上不可约, 所以 $[K(r_i) : K] = p_i$. 设 x_1, x_2, x_3 是 $f(x)$ 的三个根, 由于 $f(x)$ 在 $K(r_i)$ 中开始分解, 所以至少 $f(x)$ 的一个根属于 $K(r_i)$, 不妨设, $x_1 \in K(r_i)$, 于是, $K(x_1) \subseteq K(r_i)$, 因而 $3 | p_i$. 但因 p_i 是素数, 所以 $3 = p_i$. 故 $K(r_i) = K(x_1)$. 由 $4 \cdot 4 \cdot 2$ 又知 $[K(x_1, x_2, x_3) : K] = 3$, 所以, $K(r_i) = K(x_1) = K(x_1, x_2, x_3)$, 所以 $K(r_i)$ 是 K 的正规扩域.

(iii) 证明 $K(r_i)$ 不是全由实数构成的域. 因 $K(r_i)$ 是 K 的正规扩域, 因之 r_i 的极小多项式 $x^3 - a_i = 0$ 在 $K(r_i)$ 中完全分解, 即 $K(r_i)$ 包含它的三个根 $r_i, \omega r_i, \omega^2 r_i \Rightarrow \omega \in K(r_i)$, 但 ω 是虚数, 与 $K(r_i)$ 都是实数相矛盾.

注: 若 p_i 不为素数, 设 $p_i = rs$, 则 $\sqrt[p_i]{a} = \sqrt[r]{\sqrt[s]{a}}$, 所以可假定 p_i 为素数.

习 题

1. 用卡当公式解 \mathbb{Q} 上方程: $x^3 - 2x + 4 = 0$
2. 试求有理数域 \mathbb{Q} 上多项式

$$f(x) = x^3 - 3x + 1$$

在 \mathbb{Q} 上的分裂域 N , 并证明: N 是 \mathbb{Q} 上的三次正规域.

3. 证明: 有理数域 \mathbb{Q} 上三次方程

$$g(x) = x^3 + x + 1 = 0$$

的伽罗华群与 S_3 同构.

§ 4·5 尺 规 作 图

用圆规和直尺作图是中学几何的内容之一，几何作图三大问题也是许多数学爱好者很感兴趣的问题。本节我们就来研究尺规作图问题。并证明几何三大问题不可能用圆规和直尺作出。

我们知道，尺规作图所使用的直尺不带刻度，但可延伸。直尺的功能过两点可以画一条直线。圆规两脚可以任意张开，它的功能是以一点为圆心，以定长为半径画圆或截取定长。

所谓尺规作图，是在平面上给定了一些初等几何图形，点、线、圆，利用这些图形，来作一些满足某些要求的几何图形，但在作图的过程中，仅限用圆规和直尺。

讨论尺规作图，先来分析一下，用尺规作图到底能做些什么？归纳起来，用尺规能作以下六件事情：

- 1° 在平面上的某一区域内，选择一个任意点；
- 2° 通过二点画一直线；
- 3° 用给定的圆心及半径(两点的距离)画一圆；
- 4° 使二直线相交；
- 5° 使一直线与一圆相交；
- 6° 使两圆相交。

由此我们看出，用尺规只能作出点、直线和圆来。事实上，我们只能用步骤1°、4°、5°、6°来作点，用步骤2°来作直线，用步骤3°来作圆。

所谓一个有某些性质的图形可以用尺规作出指的是：能够给出由有限个上述步骤组成一个确定的程序(方案)，通过

这个程序,必然地会得到一个所要的图形。

现在我们用代数的方法来研究图形什么时候可以用圆规和直尺作出的问题。

我们在平面上任意取定一个笛卡儿坐标系。那么,每一个点有一对确定的坐标 (a, b) ; 每一条直线有一个确定的方程:

$$x + cy + d = 0 \quad \text{或} \quad y + d = 0;$$

每个圆有一个确定的方程:

$$x^2 + y^2 + ex + fy + g = 0$$

注意,我们限定直线和圆的方程取以上的形式,因此它们是由它们所代表的图形唯一确定的。

我们把一个直线或圆的方程的系数叫做直线或圆的坐标。

这样,取定坐标系后,对于平面上每一初等几何图形有一组确定的实数(图形的坐标)与它对应。

我们把两个坐标都是有理数的点叫做有理点。由有理数的稠密性,这样的点在平面的任何区域内都存在。

4.5.1 定理 假定某一图形,可从给定的图形用尺规作出,那么任意取定平面的一个笛卡尔坐标系后,都可以作出一个所要图形,它有以下性质:对于给定图形的任意取定了的坐标 a, b, c, \dots 来说,都可以这样选取所作的图形的坐标,使它们属于一个域 K , 而 K 是 $F = \mathbb{Q}(a, b, c, \dots)$ 的一个 2^m (m 为非负整数)次扩域。此处 \mathbb{Q} 是有理数域。

证明 按照假设,所要的图形可以用圆规和直尺作出,这就是说,它可以通过有限次施行步骤 $1^\circ \sim 6^\circ$ 中的某些个而必然地得到。这样,当我们每次需要施行步骤 1° 时,都取一个有理点,我们也将得到一个所要的图形。

对于给定的图形，任意取定它的坐标 $a, b, c \dots$ ，先看施行头一步后所得图形的坐标是什么？头一步只能是六个步骤中的一个。

假定第一步是 1° ，在某一区域内任取一点，按照我们的约定取定的是有理点，所得的坐标根本就在 $Q(a, b, c, \dots)$ 内。

假定第一步是 2° ，通过两点画一直线。两个点在图形中早已给定，直线的方程可以用给定的点有理表示，在这种情况下，可选直线的坐标属于 $Q(a, b, c, \dots)$ 内。

假定第一步是 3° ，用给定的圆心及半径画圆。圆的方程是： $(x - x_1)^2 + (y - y_1)^2 = r^2$ ，这里 (x_1, y_1) 是圆心的坐标， r 是给定的半径， r 可由给定两点的距离表示，这样圆的坐标是给定三点坐标的有理函数，于是圆的坐标属于 $Q(a, b, c, \dots)$ 内。

假定第一步是 4° ，使两直线相交，这时两条直线是给定的，解这两直线的方程就得出交点来，其交点是系数的有理式，所得的点的坐标属于 $Q(a, b, c, \dots)$ 内。

假定第一步是 5° ，使一直线与一圆相交，圆和直线是给定的，求圆方程及直线方程的交点，其解最多有系数开平方式子出现，所得点的坐标属于一个域，这个域对于 $Q(a, b, c, \dots)$ 来说，其次数是 $2^{\mu_1} (\mu_1 = 0, 1)$ 。

假定第一步是 6° ，两圆相交，解两圆方程相当于解一个直线和一个圆的方程，和 5° 一样，其解最多是系数开平方的表示式，所得点属于一个域。这个域对于 $Q(a, b, c, \dots)$ 来说，其次数是 $2^{\mu_2} (\mu_2 = 0, 1)$ 。

总的来说，完成第一步，得出一个新的图形，使新的图形的坐标属于域 K_1 ，而

$$[K_1 : Q(a, b, c, \dots)] = 2^{m_1}.$$

做完第一步，做第二步，这时给定的图形就多了第一步所作出的一个新的图形，给定的图形属于域 K_1 内，这时用 K_1 代替 $Q(a, b, c, \dots)$ 继续讨论。与第一步一样，完成第二步使所得新的图形的坐标属于域 K_2 内，而 $[K_2 : K_1] = 2^{m_2}$ 。

这样一直做下去，由于只用有限次 $1^\circ \sim 6^\circ$ 步骤所确定的程序就得出所要的图形，最后得到所要的图形属于域 K 内，而 $[K : K_{n-1}] = 2^{m_n}$ ，这样

$$[K : Q(a, b, c, \dots)] = [K_1 : Q(a, b, c, \dots)]$$

$$[K_2 : K_1] \cdots [K : K_{n-1}]$$

$$= 2^{m_1} \cdot 2^{m_2} \cdots 2^{m_n}$$

$$= 2^{m_1 + m_2 + \cdots + m_n}$$

$$= 2^m.$$

4.5.2 推论 4.5.1定理中的域 $K \subseteq \bar{K}$ ，而 \bar{K} 是 $F = Q(a, b, c, \dots)$ 的正规域，并且 $[\bar{K} : F] = 2^s$ 。

证明 由4.5.1定理的证明知

$$F = F_1 \subset F_2 \subset \cdots \subset F_i \subset F_{i+1} \subset \cdots \subset F_{m+1} = K$$

其中 $F_{i+1} = F_i(a_i)$ 而 $a_i^2 = a_i \in F_i$ 。即 $[F_{i+1} : F_i] = 2$ ，而 $[K : F] = 2^m$ 。我们称这样的扩域 K/F 有平方根塔。

仿4.2.2定理的证明对 m 应用数学归纳法可知存在一个正规扩域 \bar{K} ，而 $\bar{K} \supseteq K$ ，且 \bar{K} 亦具有平方根塔，因之 $[\bar{K} : F] = 2^s$ ，而 s 为非负整数。

有了4.5.2我们就可以假定4.5.1定理中的 K/F 为正规域，而 K/F 有平方根塔，或说 $[K : F] = 2^m$ 。

下面在假定 K/F 为正规域的前提下，来证明4.5.1定理

的逆定理。为此我们做一些说明，我们知道，初等几何图形都是由点、线、圆弧和角度构成的。两点可定一直线，三点可定一圆，角的顶点和角的两边上的两点可定一角，给定的图形和所要做的图形都可以用平面上的点来表示。但平面上直角坐标为 (a, b) 的点又可用复数 $a + bi$ 来表示。这样一个几何图形是否可作，要看确定这个图形的点即复数是否可作。下面我们把给定的复数的运算，用几何作图来实现。实现的方法按照：

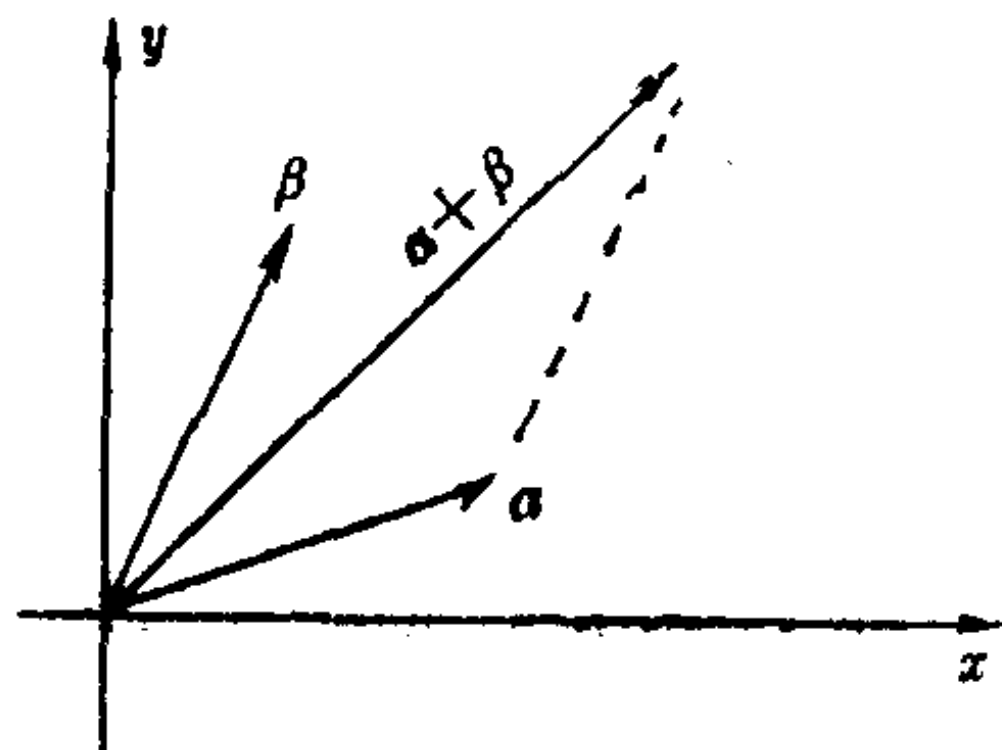


图 4-1

加法是向量的加法(如图 4-1 示)。减法是它的逆运算。

乘法就是辐角相加而模相乘，如果相乘的两个数的辐角是 φ_1, φ_2 ，模是 r_1, r_2 ，那么乘积的辐角 φ 与模 r ，即按方程

$\varphi = \varphi_1 + \varphi_2$ 与 $r = r_1 r_2$ 或 $1 : r_1 = r_2 : r$ 来构造(如图4-2示)。除法又是它的逆运算。

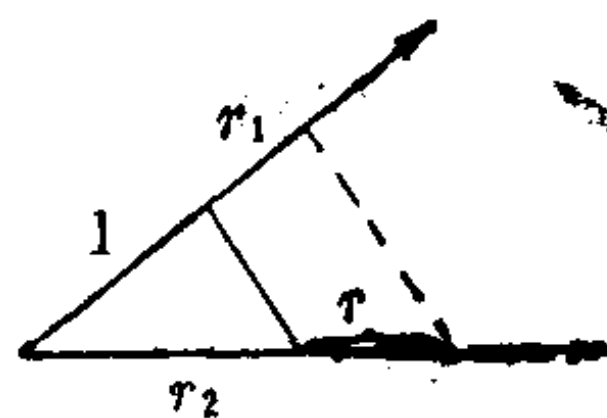
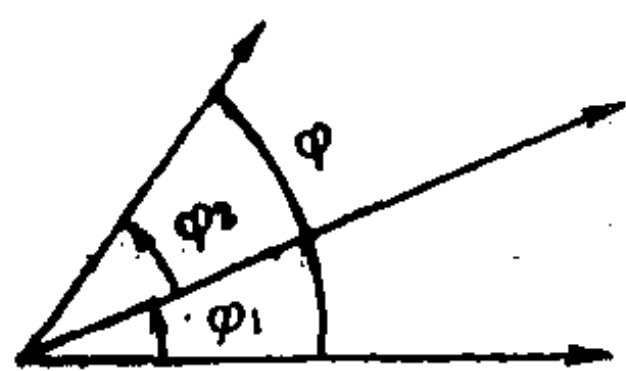


图 4-2

复数的开平方。对于一个模为 r ，辐角为 φ 的复数的平方根，由方程

$$\varphi = 2\varphi_1 \quad \text{或} \quad \varphi_1 = \frac{1}{2}\varphi$$

与 $r = r_1^2$ 或 $1 : r_1 = r_1 : r$
来构造(如图 4-3 示).



图 4-3

对于已知的实数或复数可以用圆规和直尺进行加、减、乘、除和开平方五种运算.

4.5.3 定理 任意取定平面上的一个笛卡尔坐标系, 对于给定图形的任意取定了的坐标 a, b, c, \dots 来说, 只要能够选取所作图形的坐标, 使它们属于 $F = Q(a, b, c, \dots)$ 的一个正规扩域 K , 而 $[K : F] = 2^m$, m 为非负整数. 则这个图形就可以用圆规和直尺作出.

证明 只需在 $F = Q(a, b, c, \dots)$ 的每一个数可作的假定下, 来证明 K 的每个数都是可作的.

因 K 是 F 上的 2^m 次正规域, 故 $G = \text{Gal}(K/F)$ 的阶为 2^m . 因之, G 为 $p(=2)$ 群, 由 1.5.9 知 G 为可解群. 于是 G 有合成列:

$$G = G_1 \triangleright G_2 \triangleright \dots \triangleright G_i \triangleright G_{i+1} \triangleright \dots \triangleright G_{m+1} = \{e\}$$

而 G_i/G_{i+1} ($i = 1, 2, \dots, m$) 是阶为 2 的循环群. 因之由伽罗华基本定理 I 知 K/F 有如下平方根塔:

$$F = K_1 \subset K_2 \subset \dots \subset K_i \subset K_{i+1} \subset \dots \subset K_{m+1} = K$$

而 $[K_{i+1} : K_i] = 2$

令对 m 应用数学归纳法来证明 K 的每一元可用圆规与直尺作出.

当 $m = 0$ 时, 定理显然成立.

假定 $m=i$ 时定理成立, 即 K_i 中每一元可作, 在这个假定下, 我们证明 K_{i+1} 的每一元也可作.

因 $[K_{i+1} : K_i] = 2$, 即 $K_{i+1} = K_i(a_i)$. 而 $a_i^2 = a_i \in K_i$, 又 $K_{i+1} = \{a + ba_i, a, b \in K_i\}$. 因 $a_i \in K_i$, 所以 a_i 可作, 因之, a_i 的平方根 a_i 可作. 又 $a, b \in K_i$, 所以 a, b 可作. 于是 ba_i 可作, 因而 $a + ba_i$ 可作. 这样 K_{i+1} 的每一元都可作, 归纳法完成.

下面我们利用 4.5.1 的结果, 来证明几何三大问题不可能用尺规作出.

1. 三等分任一角, 假定能够用圆规和直尺三等分任意角, 那么给定了夹角是 60° 的两条直线 OA 与 OB (如图 4-4) 以及直线 OB 上任一点 D (D 不与 O 重合) 以后, 我们可以用圆规和直尺作出直线 OC 使 $\angle COD = 20^\circ$, 并且作出以 O 为圆心, OD 为半径的圆, 这样我们也可以作出 OC 与这个圆的交点 E (如图 4.4).

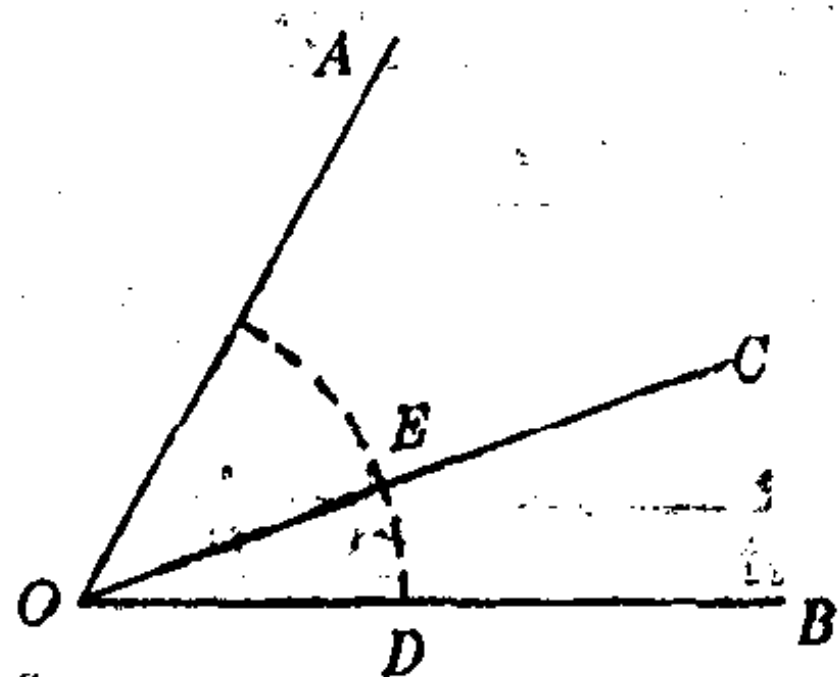


图 4-4

取以 O 为原点, OB 为 x 轴, OD 长为单位的笛卡尔坐标系, 那么, D 点的坐标是 $(1, 0)$, 直线 OB 与 OA 的方程分别是:

$$y = 0 \quad \text{和} \quad y = \operatorname{tg} 60^\circ x = \sqrt{3} x \quad \text{即} \quad x - \frac{1}{\sqrt{3}} y = 0$$

取 $Q(a, b, c, \dots) = Q\left(\frac{1}{\sqrt{3}}\right) = Q(\sqrt{3})$. 假如用尺规能

三等分 60° 角就得出点 $E = (\cos 20^\circ, \sin 20^\circ)$ 在 $Q(\sqrt{3})$ 的

2^m (m 非负整数) 次扩域内, 即在 \mathbb{Q} 的 2^{m+1} 次扩域内.

另一方面, 由三角公式

$$\cos 3(20^\circ) = 4\cos^3 20^\circ - 3\cos 20^\circ,$$

我们知道 $\cos 20^\circ$ 满足 $4x^3 - 3x = \frac{1}{2}$, 即 $8x^3 - 6x - 1 = 0$,

但 $8x^3 - 6x - 1$ 在有理数域上不可约, $\cos 20^\circ$ 包含在 \mathbb{Q} 的三次扩域内, 这与前者是矛盾的. 故三等分任意角不能用尺规作出.

2. 立方倍积. 给了立方体, 求作一个立方体, 使它的体积是前者的二倍. 这个问题归结为: 给了一个线段 AB , (换一句话说, 给了 A 和 B 两点) 求作一线段, 使这个线段的长等于 $\sqrt[3]{2} AB$.

取以 A 为原点, AB 为 x 轴, AB 长为单位的笛卡尔坐标系, 那么 A 点的坐标是 $(0,0)$, B 点的坐标是 $(1,0)$. (如



图 4-5

图4-5).

这样 $\mathbb{Q}(a, b, c \dots) = \mathbb{Q}$.

假定合乎要求的线段可以用尺规作出, 那么可以在 x 轴上得出一点 E , 使 E 点的横坐标 $a = \sqrt[3]{2}$. 于是由定理应有 $[\mathbb{Q}(a) : \mathbb{Q}] = 2^m$, 但 a 是有理数域 \mathbb{Q} 上不可约多项式 $x^3 - 2$ 的一个根, 所以, $[\mathbb{Q}(a) : \mathbb{Q}] = 3$. 这样我们得到一个矛盾. 因此, 立方倍积问题也不能通过尺规作图来解决.

3. 化圆为方. 设给定一个圆, 求作一线段, 使得以这个线段为边的正方形的面积等于所给圆的面积.

取以圆心 O 为原点, 半径长为单位的笛卡尔坐标系. (如

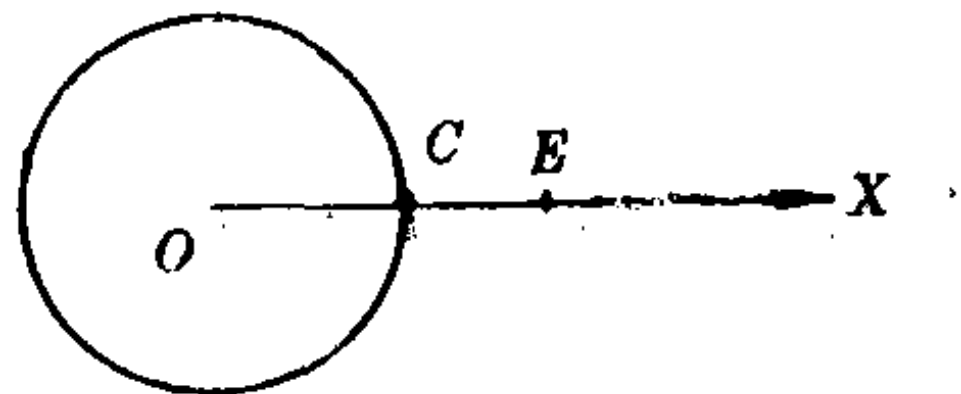


图 4-6

图4-6).

那么圆的方程是

$$x^2 + y^2 - 1 = 0$$

这时 $Q(a, b, c, \dots) = Q$

假定合乎要求的线段可以用尺规作出, 那么在 x 轴上可以得出一一点 E , E 的横坐标 $\alpha = \sqrt{\pi}$, 于是由定理 $[Q(\alpha) : Q] = 2^s$, 但 $1, \pi = \alpha^2, \pi^2, \dots, \pi^{2^s}$ 这 $2^s + 1$ 个数属于 $Q(\alpha)$, 所以根据扩域次数的定义, 这 $2^s + 1$ 个数在 Q 上线性相关. 这就是说, 存在不全为零的有理数 a_0, a_1, \dots, a_{2^s} , 能使

$$a_0 + a_1\pi + \dots + a_{2^s}\pi^{2^s} = 0$$

但我们知道 π 是一个超越数, 因而以上等式不可能成立. 这样, 化圆为方问题也不能够通过尺规作图来解决.

习 题

1. 利用4.5.1定理证明正七边形不可能用圆规和直尺作出.

§ 4.6 分圆多项式和正 n 边形作图

正 n 边形的作图是一个有趣的问题, 自古以来就吸引着数学家的注意. 在古希腊时代, 人们就会用尺规作出 3, 4, 5, 6, 8, 10, 12, 15, 16 等边数的正多边形. 但是企图用尺规作出正七边形或正九边形却是失败的. 一直到十八世纪, 高斯才给出正十七边形的作图法, 并且知道并非任何一个正多边形都能用尺规来作出. 然而怎样判断一个正多边形能不能用尺规来作图呢? 下面我们利用 § 4.5 得到的结果来讨论这个问题.

由上节我们知道, 一个图形可以用圆规和直尺作出当且

仅当对于给定图形的任意取定的坐标 a, b, c, \dots 来说, 只要能够选取所作图形的坐标, 使它们属于 $F = \mathbb{Q}(a, b, c, \dots)$ 的一个正规域 K , 而 $[K : F] = 2^m (m \geq 0)$.

一般说来, 图形的坐标 a, b, c, \dots 是实数, 因而 F 是实数域的子域, 但上节我们说过, 一个图形可以用平面上的有限个点或复数来刻划. 一个图形可作, 就是这些点或者说这些复数可作. 由于 K 为正规域, 故若 $z \in K$, 因而其共轭复数 $\bar{z} \in K$. 显然, $z = re^{i\theta}$ 可作, 则其 $\bar{z} = re^{i(-\theta)}$ 亦可作. 这样上述尺规作图判别准则可以改述如下:

4.6.1 定理(尺规作图判别准则) 设 z_1, z_2, \dots, z_n 是给定的复数, 令 $F = \mathbb{Q}(z_1, z_2, \dots, z_n, \bar{z}_1, \dots, \bar{z}_n)$, 则某数 z 可由 z_1, z_2, \dots, z_n 作出 $\Leftrightarrow z$ 是 F 上代数元, 且有 F 的正规域 K , 使 $F \subseteq F(z) \subseteq K$, 而 $[K : F] = 2^m$, m 是非负整数.

运用这个判别准则可以彻底解决正 n 边形作图问题.

首先讨论分圆多项式的不可约性.

看有理系数多项式 $x^n - 1$, 我们知道 n 次本原根一共有 $\varphi(n)$ 个, 设为

$$\xi_1, \xi_2, \dots, \xi_{\varphi(n)}$$

4.6.2 定义 称

$$(1) \quad \Phi_n(x) = (x - \xi_1)(x - \xi_2) \cdots (x - \xi_{\varphi(n)})$$

为分圆多项式, 由 4.1.1 知 \mathbb{Q} 上一切 n 次单位根作成 n 阶循环群 (ξ) , 因之, $\mathbb{Q}(\xi)$ 为 \mathbb{Q} 上正规域, 称它为分圆域.

4.6.3 引理

$$(2) \quad x^n - 1 = \prod_{d|n} \Phi_d(x)$$

证明 首先证明 $\Phi_n(x) \in \mathbb{Q}[x]$. 任取 $\eta \in \text{Gal} \mathbb{Q}(\xi)/\mathbb{Q}$,

因 ξ 是本原根, 所以 ξ^n 亦为本原根, 于是

$$(\Phi_n(x))^n = \Phi_n(x)$$

从而 $\Phi_n(x) \in \mathbb{Q}[x]$, 显然 $\Phi_n(x) \mid x^n - 1$.

因为任意一个 n 次单位根的阶 d 是 n 的因数, 故这个单位根是 d 次本原根, 反之当 d 为 n 的因数时, d 次本原根也是一个 n 次单位根, 所以

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

4.6.4 引理 $\Phi_n(x)$ 为整系数多项式.

证明 对 n 用数学归纳法.

当 $n=1$ 时, 命题显然成立.

假设对 $\Phi_d(x)$ $1 \leq d < n$ 此命题成立, 现在来证明对 $\Phi_n(x)$ 命题亦成立.

由(2)知, $x^n - 1 = \Phi_n(x)g(x)$, 其中 $g(x) = \prod_{\substack{d \mid n \\ d < n}} \Phi_d(x)$.

由归纳假设知 $g(x)$ 为首项系数为 1 的整系数多项式, 由带余除法知

$$x^n - 1 = q(x)g(x) + r(x)$$

且 $\partial^\circ(r(x)) < \partial^\circ(g(x))$, $g(x)$ 是整系数多项式.

因 $g(x)$ 和 $r(x)$ 在 $\mathbb{Q}[x]$ 中是唯一的, 且在 $\mathbb{Q}[x]$ 中, $x^n - 1 = \Phi_n(x)g(x)$, 所以 $\Phi_n(x) = q(x)$ 是整系数多项式.

4.6.5 定理 $\Phi_n(x)$ 是 \mathbb{Q} 上不可约多项式.

证明 设 ξ 是任意一个 n 次本原根, $p(x)$ 是 ξ 在 \mathbb{Q} 上的极小多项式, 则 $p(x) \mid \Phi_n(x)$, 从而 $p(x)$ 为整系数多项式, 下面我们证明 $\Phi_n(x) = p(x)$, 从而 $\Phi_n(x)$ 为 \mathbb{Q} 上不可约多项式.

首先证明, 如果素数 $p \nmid n$, 则 ξ^p 也是 $p(x)$ 的根.

令 $\psi(x)$ 为 ξ^p 在 \mathbb{Q} 上的极小多项式, 仿上知 $\psi(x)$ 为

整系数多项式。我们断言 $\psi(x) = p(x)$ 。假设 $\psi(x) \neq p(x)$ ，则在 $\mathbb{Q}[x]$ 内应有

$$(3) \quad x^n - 1 = P(x)\psi(x)f(x)$$

其中 $f(x)$ 是首项系数为 1 的整系数多项式，由 $P(x)$ 与 $\psi(x^p)$ 有公根 ξ ，故有

$$(4) \quad \psi(x^p) = P(x)g(x)$$

其中 $g(x)$ 为首项系数为 1 的整系数多项式。如果把 (3) 与 (4) 都看成 $\mathbb{Z}_p[x]$ 中的等式，其中 $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$ 为素域，则由于在 \mathbb{Z}_p 中总有 $a^p = a (a \in \mathbb{Z}_p)$ ，故 $\psi(x^p) = [\psi(x)]^p$ ，而 (4) 成为

$$(5) \quad [\psi(x)]^p = p(x)q(x)$$

令 $\varphi(x)$ 为 $p(x)$ 在 $\mathbb{Z}_p[x]$ 中的一个不可约因式，则由 (5) 知， $\varphi(x) | [\psi(x)]^p$ ，从而 $\varphi(x) | \psi(x)$ ，故由 (3) 知 $[\varphi(x)]^2 | x^n - 1$ 。但 $p \nmid n$ ， $x^n - 1$ 在 $\mathbb{Z}_p[x]$ 中无重因式，此为矛盾。因此必有 $p(x) = \psi(x)$ ，即 ξ^p 也是 $p(x)$ 的根。

其次证明，任意 n 次本原根 ε 都是 $p(x)$ 的根。

设 $\varepsilon = \xi^m$ ， $(m, n) = 1$ ，于是

$$m = p_1 p_2 \cdots p_s \quad (p_i \text{ 均为素数})$$

且诸 p_i 均非 n 的因数。故逐次用上段已得到的结论即知 ξ^{p_1} ，从而 $\xi^{p_1 p_2}$ ， \dots ， $\xi^{p_1 p_2 \cdots p_s} = \xi^m$ ，应为 $p(x)$ 的根，于是 n 次本原根都为 $p(x)$ 的根，故 $\Phi_n(x) | p(x)$ ，从而 $\Phi_n(x) = p(x)$ 。

所以， $\Phi_n(x)$ 是 \mathbb{Q} 上不可约多项式。

由此定理知 $\Phi_n(x)$ 显然是任意 n 次本原单位根 ξ 的极小多项式。于是 $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$ 。

若 p 为素数，则

$$x^p - 1 = (x - 1)\Phi_p(x)$$

所以 $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ 在 \mathbb{Q} 上不可约。

公式(2)提供给我们求分圆多项式 $\Phi_n(x)$ 的一个算法。首先有

$$\Phi_1(x) = x - 1.$$

再假设对 n 的真因子 d , 我们知道 $\Phi_d(x)$, 则(2)便给出 $\Phi_n(x)$ 。例如

$$\Phi_2(x) = (x^2 - 1)/\Phi_1(x) = x + 1.$$

$$\Phi_3(x) = (x^3 - 1)/\Phi_1(x) = x^2 + x + 1.$$

$$\begin{aligned}\Phi_6(x) &= (x^6 - 1)/\Phi_1(x)\Phi_2(x)\Phi_3(x) \\ &= x^2 - x + 1.\end{aligned}$$

有了上面的准备, 我们可以较容易解决正多边形的尺规作图问题。

我们首先指出: 若 s 是某个自然数使得 $2^s + 1$ 是素数, 则必存在非负整数 t 使 $s = 2^t$ 。

事实上, 如果 s 有奇数因子 u 使 $s = uv$ 则由

$$2^s + 1 = (2^v + 1)(2^{(u-1)v} - 2^{(u-2)v} + 2^{(u-3)v} - \cdots + 1)$$

知 $2^s + 1$ 不是素数。凡形如 $2^{2^t} + 1$ 的素数称为费尔马(Fermat)素数, 费尔马曾猜测它们都是素数。实则当 $t = 5$ 时, 欧拉(Euler)已发现它不是素数:

$$2^{2^5} + 1 = 641 \times 6700417$$

当 $t = 6, 7$ 时, $2^{2^t} + 1$ 也不是素数。所以很多数学家都猜测在 $t = 4$ 时, 是最后的费尔马素数。即 3, 5, 17, 257, 65537, 是仅有的全部费尔马素数。当然, 这一点目前也没有得到证明。

下面我们给出正 n 边形可用尺规作图的判别定理:

4·6·6 定理 正 n 边形可作 $\Leftrightarrow n = 2^s (s \geq 2)$ 或 $n = 2^l p_1 p_2 \cdots p_r$. 这里 $l \geq 0$, p_1, p_2, \dots, p_r 是两两不同的费尔马素数.

证明 设 ξ 是 n 次本原根, 由前面的证明已知 $\mathbb{Q}(\xi)/\mathbb{Q}$ 是 $\varphi(n)$ 次正规域. 由 4·6·1 可知,

正 n 边形可作 $\Leftrightarrow \xi$ 可作 $\Leftrightarrow \varphi(n)$ 是 2 的方幂.

设 $n = 2^l p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$, p_i 为两两不同的奇素数. 如果 $n = 2^l$, $l \geq 2$, 显然正 2^l 边形可作, 因此仅需要讨论 $l \geq 0$ 且所有 $l_i \geq 1$ 的情形.

根据欧拉函数定义, 对于任一素数方幂 p^k 有

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

且当 r 与 s 互素时, 必有

$$\varphi(rs) = \varphi(r)\varphi(s) \quad \text{所以得到}$$

$$\begin{aligned} \varphi(n) &= \varphi(2^l)\varphi(p_1^{l_1})\cdots\varphi(p_r^{l_r}) \\ &= 2^{l-1} p_1^{l_1-1} \cdots p_r^{l_r-1} (p_1-1)\cdots(p_r-1) \end{aligned}$$

易见 $\varphi(n)$ 是 2 的方幂 \Leftrightarrow 所有 $l_i = 1$ 且 $p_i - 1 = 2^{s_i}$, 且由 $p_i = 2^{s_i} + 1$ 为素数知 s_i 为 2 的方幂, 即 p_i 为费尔马素数.

有了高斯定理我们就彻底解决了正 n 边形作图问题.

当 $t = 2$ 时, $2^{2^2} + 1 = 17$ 是第三个费尔马素数, 正十七边形可作, 由高斯给出作法, 继高斯之后, 为西罗给出正 257 边形的完善作法, 盖尔美斯又给出了正 65537 边形的作图方法, 这里我们不再介绍. 最后我们给出:

4·6·7 正十七边形的作法

我们先推导出作法的依据. 令

$$\theta = 2\pi/17, \quad z = \cos\theta + i\sin\theta, \quad \text{则}$$

$$z^k = \cos k\theta + i\sin k\theta, \quad (1 \leq k \leq 17)$$

是17个17次单位根。由

$$x^{17} - 1 = (x - 1)(x^{16} + x^{15} + \cdots + x + 1)$$

和 z^k , $k = 1, 2, \dots, 16$, 是17次本原根的全体, 可知 z 在 \mathbb{Q} 上的极小多项式为

$$g(x) = \sum_{i=0}^{16} x^i = \prod_{k=1}^{16} (x - z^k)$$

$g(x)$ 在 \mathbb{Q} 上的分裂域是 $E = \mathbb{Q}[z]$, $[E : \mathbb{Q}] = 16$, 且

$$G = \text{Gal} E / \mathbb{Q} = (\sigma)$$

为16阶循环群, 这里

$$\sigma: z \mapsto z^k \quad \sigma \text{ 不变 } \mathbb{Q} \text{ 中数}, (k, 16) = 1$$

为讨论简单起见, 可取 $k = 3$, 即 $z^\sigma = z^3$. 设

$$3^i = 17q_i + l_i, \quad 1 \leq l_i \leq 16, \quad i = 1, 2, \dots, 16.$$

利用 $z^{\sigma^i} = z^{3^i}$ 和 $z^{17} = 1$ 可列出下表.

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
l_i	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

易见 $G = (\sigma)$ 有合成群列

$$\begin{aligned} G &= G_1 = (\sigma) \triangleright G_2 = (\sigma^2) \triangleright G_3 = (\sigma^4) \triangleright G_4 \\ &= (\sigma^8) \triangleright G_5 = \{e\}. \end{aligned}$$

其中 G_i / G_{i+1} 都是2阶群. 根据伽罗华映射可得平方根塔

$$\mathbb{Q} = F_1 \subset F_2 \subset F_3 \subset F_4 \subset F_5 = E$$

这里 $F_i = \text{Inv} G_i$, $[F_{i+1} : F_i] = 2$, $i = 1, 2, 3$. 现要依次定出 F_{i+1} / F_i ($i = 1, 2, 3$) 的添加元.

1) 设

$$(6) \quad \begin{cases} x_1 = \sum_{i=0}^7 z^{\sigma^{2i}} = \sum_{i=0}^7 z^{3^{2i}} \\ x_2 = x_1^{\sigma} = \sum_{i=0}^7 z^{\sigma^{2i+1}} = \sum_{i=0}^7 z^{3^{2i+1}} \end{cases}$$

由上表可知 $x_1 \neq x_2$, 但却有 $x_1^{\sigma^2} = x_1$, 所以 $x_1 \notin F_1$, 但 $x_1 \in F_2 = \text{Inv}(\sigma^2)$. 由 $[F_2 : F_1] = 2$, 所以

$$F_2 = F_1(x_1)$$

又由 $g(z) = 0$, 知

$$\sum_{k=1}^{16} z^k = -1$$

由 $z\bar{z} = 1$ 得 $\bar{z} = z^{-1}$, $(z^k)^{-1} = \bar{z}^k = \cos k\theta - i \sin k\theta$

因而

$$z^k + z^{-k} = 2 \cos k\theta, \quad 1 \leq k \leq 17.$$

利用上表可算出

$$\begin{aligned} x_1 &= (z^{3^0} + z^{3^8}) + (z^{3^2} + z^{3^{10}}) + (z^{3^4} + z^{3^{12}}) + (z^{3^6} + z^{3^{14}}) \\ &= (z + z^{-1}) + (z^8 + z^{-8}) + (z^4 + z^{-4}) + (z^2 + z^{-2}) \end{aligned}$$

从而

$$(7) \quad x_1 = 2(\cos \theta + \cos 8\theta + \cos 4\theta + \cos 2\theta)$$

同理可得

$$(8) \quad x_2 = 2(\cos 3\theta + \cos 7\theta + \cos 5\theta + \cos 6\theta)$$

故有

$$x_1 + x_2 = \sum_{k=1}^{16} z^k = -1$$

利用三角恒等式

$$2 \cos \alpha \cos \beta = \cos(\alpha + \beta) + \cos(\alpha - \beta)$$

直接将(7)、(8)两式相乘得

$$x_1 x_2 = 4(x_1 + x_2) = -4$$

所以 x_1, x_2 是 $(x - x_1)(x - x_2) = x^2 + x - 4 = 0$ 的二根, 它们是 $\frac{1}{2}(-1 \pm \sqrt{17})$. 由于 $\theta = \frac{2\pi}{17}$, $\cos 3\theta > 0, \cos 7\theta < 0, \cos 5\theta < 0, \cos 6\theta < 0$, 而且

$$|\cos 6\theta| = \cos(\pi - 6\theta) = \cos \frac{5\pi}{17} > \cos \frac{6\pi}{17} = \cos 3\theta$$

因此 $x_2 < 0$ 而

$$(9) \quad \begin{cases} x_1 = \frac{1}{2}(-1 + \sqrt{17}) \\ x_2 = \frac{1}{2}(-1 - \sqrt{17}) \end{cases}$$

2) 设

$$(10) \quad \begin{cases} y_1 = \sum_{i=0}^3 z^{\sigma^{4i}} = \sum_{i=0}^3 z^{3^{4i}} \\ y_2 = y_1^{\sigma^2} = \sum_{i=0}^3 z^{\sigma^{4i+2}} = \sum_{i=0}^3 z^{3^{4i+2}} \end{cases}$$

也有 $y_1 \neq y_2$, 由

$$y_1^{\sigma^4} = \sum_{i=0}^3 z^{\sigma^{4(i+1)}} = y_1$$

知 $y_1 \notin F_2$, $y_1 \in F_3 = \text{Inv}(\sigma^4)$. 所以

$$F_3 = F_2(y_1) = F_1(x_1, y_1)$$

和 x_1, x_2 类似地可算出

$$y_1 = z + z^{-1} + z^4 + z^{-4} = 2(\cos \theta + \cos 4\theta)$$

$$y_2 = z^8 + z^{-8} + z^2 + z^{-2} = 2(\cos 8\theta + \cos 2\theta)$$

再令

$$y_3 = z^3 + z^{-3} + z^5 + z^{-5} = 2(\cos 3\theta + \cos 5\theta)$$

$$y_4 = z^7 + z^{-7} + z^6 + z^{-6} = 2(\cos 7\theta + \cos 6\theta)$$

仍使用上述三角恒等式可得:

$$y_1 y_2 = 4(\cos \theta + \cos 4\theta)(\cos 8\theta + \cos 2\theta)$$

$$= 2 \sum_{k=1}^8 \cos k\theta = -1$$

同理

$$y_3 y_4 = -1$$

又因

$$y_1 + y_2 = x_1, \quad y_3 + y_4 = x_2$$

故

y_1, y_2 是 $x^2 - x_1 x - 1 = 0$ 的根, 而 y_3, y_4 是 $x^2 - x_2 x - 1 = 0$ 的根.

因 $\theta = \frac{2\pi}{17}$ 时, $\cos\theta > \cos 2\theta$, $\cos 4\theta > 0$, $\cos 8\theta < 0$.

故有 $y_1 > y_2$, 同理 $y_3 > y_4$. 因此

$$(11) \quad \begin{cases} y_1 = \frac{1}{2} (x_1 + \sqrt{x_1^2 + 4}) = \frac{1}{4} (\sqrt{17} - 1) \\ \quad \quad \quad + \frac{1}{4} \sqrt{34 - 2\sqrt{17}} \\ y_2 = \frac{1}{2} (x_1 - \sqrt{x_1^2 + 4}) \\ y_3 = \frac{1}{2} (x_2 + \sqrt{x_2^2 + 4}) = \frac{1}{4} (-\sqrt{17} - 1) \\ \quad \quad \quad + \frac{1}{4} \sqrt{34 + 2\sqrt{17}} \\ y_4 = \frac{1}{2} (x_2 - \sqrt{x_2^2 + 4}) \end{cases}$$

$$y_2 = \frac{1}{2} (x_1 - \sqrt{x_1^2 + 4})$$

$$y_3 = \frac{1}{2} (x_2 + \sqrt{x_2^2 + 4}) = \frac{1}{4} (-\sqrt{17} - 1)$$

$$+ \frac{1}{4}\sqrt{34} + 2\sqrt{17}$$

$$y_4 = \frac{1}{2} (x_2 - \sqrt{x_2^2 + 4})$$

3) 设

$$(12) \quad \begin{cases} z_1 = z + z^{3^8} \\ z_2 = z_1^{\sigma^4} = z^{3^4} + z^{3^{12}} \end{cases}$$

必有 $z_1 = z_2$, 由 $z_1^{\sigma^8} = z^{3^8} + z = z_1$, 知 $z_1 \in F_3$, 而 $z_1 \in F_4 = \text{Inv}(\sigma^4)$. 所以

$$F_4 = F_3(z_1) = F_1(x_1, y_1, z_1)$$

易见

$$z_1 = z + z^{-1} = 2\cos\theta$$

$$z_2 = z^4 + z^{-4} = 2\cos 4\theta$$

则 $z_1 > z_2$, $z_1 + z_2 = y_1$, $z_1 z_2 = 4\cos\theta \cos 4\theta = 2(\cos 5\theta + \cos 3\theta) = y_3$, 故

$$(13) \quad \begin{cases} z_1 = \frac{1}{2} (y_1 + \sqrt{y_1^2 - 4y_3}) \\ z_2 = \frac{1}{2} (y_1 - \sqrt{y_1^2 - 4y_3}) \end{cases}$$

最后可得

$$\cos\theta = \frac{1}{2} z_1 = \frac{1}{4} (y_1 + \sqrt{y_1^2 - 4y_3})$$

利用公式(11)可得 $\cos\theta$ 的显表示式, 再利用 $\sin\theta = \sqrt{1 - \cos^2\theta}$, 就可得到

$$z = \cos\theta + i\sin\theta$$

这表示 z 确是一个可作的复数, 即正十七边形是可用尺规作出的.

现在给出具体的作图步骤. 作直角坐标系 xOy . 在 x 轴上以 $OA = 4$ 为半径作圆 O 交 y 轴于 C . 取 $OE = |OA|/4 = 1$, 连结 CE . 作

$$EF = EF' = EC = \sqrt{OC^2 + OE^2} = \sqrt{17}.$$

在 x 轴上取

$$\begin{aligned} FG = FC &= \sqrt{OC^2 + OF^2} = \sqrt{16 + (1 + \sqrt{17})^2} \\ &= \sqrt{34 + 2\sqrt{17}} \end{aligned}$$

$$\begin{aligned} F'G' = F'C &= \sqrt{OC^2 + OF'^2} = \sqrt{16 + (\sqrt{17} - 1)^2} \\ &= \sqrt{34 - 2\sqrt{17}} \end{aligned}$$

以 AG 为直径作圆 O' ，与 y 轴交于 H ，作

$$\begin{aligned} IH = IJ &= \frac{1}{2} OG' = \frac{1}{2} (OF' + F'G') \\ &= \frac{1}{2} (\sqrt{34 - 2\sqrt{17}} + \sqrt{17} - 1) = 2y_1 \end{aligned}$$

作 OJ 的中垂线分别交圆 O 于 K 和 L 两点，则可证

$$\angle AOK = 2\pi/17,$$

于是 AK 就是所求的正十七边形的边长。事实上，

$$OG = FG - FO = \sqrt{34 + 2\sqrt{17}} - \sqrt{17} - 1 = 4y_3,$$

$$OH^2 = OG \cdot OA = 4y_3 \cdot 4 = 16y_3,$$

$$OI = \sqrt{IH^2 - OH^2} = \sqrt{4y_1^2 - 16y_3} = 2\sqrt{y_1^2 - 4y_3},$$

$$OJ = OI + IJ = 2y_1 + 2\sqrt{y_1^2 - 4y_3} = 4z_1,$$

$$OM = \frac{1}{2} OJ = 2z_1$$

$$\text{所以, } \cos \angle AOK = \frac{OM}{OK} = \frac{2}{4} z_1 = \frac{1}{2} z_1, \angle AOK = \frac{2\pi}{17}.$$

于是正十七边形作出来了(见图4-7)。

$a_1 = a_2 d$ 和 $b_2 = d b_1$.

3. 对任 $a \notin H$ 有 $aH = Ha$ 又 $eH = He$.

4. 对 $x \in A, y \in B \Rightarrow y^{-1}xy \in A, x^{-1}y^{-1}x \in B$
 $\Rightarrow x^{-1}y^{-1}(xy) = x^{-1}(y^{-1}xy) = (x^{-1}y^{-1}x)y \in A \cap B = \{e\}$

5. 因群 G 的中心 $Z \cong \{e\}$, 所以 $|G/Z| \leq p$ 为循环群.

§ 1.2 习 题

1. 设 $G = \{a_1, a_2, \dots, a_n\}$, 令

$\tau_{a_i}: a \mapsto aa_i = a^{\tau_{a_i}}$. 则

$\varphi: a_i \mapsto \tau_{a_i}$

是 G 和 S_n 的一个子群间的同构映射.

2. 设 $N \triangleleft S_4$, 且 $N \cong A_4, B_4, \{(1)\}$.

(i) N 不能包含 3-循环, 否则 $N = S_4$.

(ii) N 不能包含一个对换, 否则 $N = S_4$.

(iii) N 不能包含一个 4-循环, 否则 $N = S_4$.

(iv) N 不能包含两个对换之积, 否则 $N = S_4$.

3. 假定 $N \geq 3, N \cong 4$.

设 $N \leq S_n, \Rightarrow N \cap A_n \triangleleft A_n \Rightarrow N \cap A_n = A_n$ 或 $N \cap A_n = \{e\}$.

(i) 若 $N \cap A_n = A_n \Rightarrow N \supseteq A_n$, 若 $N \cong A_n \Rightarrow N$ 包有奇置换 $\alpha \Rightarrow N = S_n$.

(ii) 若 $N \cap A_n = \{(1)\} \Rightarrow N$ 的元除单位元外都是奇置换, 且其平方为单位元, 再这些奇置换用不同文字循环置换的乘积表示时又都是对换的乘积, 因为不如此, 它们的平方就不是单位元. 又 N 不含两个奇置换, 因为两个奇置换的乘积是单位元, 于是它们互逆, 因此它们就相等. 假如 $\beta =$

$(ij)\cdots$ 是 N 所含奇置换, 命 $r = (ik)$, $k \neq j$, 那末 $\tau = r\beta r^{-1} = (kj)\cdots \in N$, 这不可能. 所以 $N = \{(1)\}$.

§ 1.3 习 题

1. 令 $\bar{S}_3 = \{(1), (12), (13), (23), (123), (132)\} \subseteq S_4$, 且 $S_4 = \bar{S}_3 B_4$, 而 $\bar{S}_3 \cap B_4 = \{(1)\}$, 再利用第一同构定理即可证明之.

2. 设 G 是所给的置换群, 且 G 包有奇置换, 而 H 是由 G 中偶置换做成的群, 则 $S_n = GA_n$, $H = G \cap A_n$. 然后利用第一同构定理即可证明 $S_n/A_n \cong G/H$. 所以 $[G:H] = 2$.

3. 若 $H \cap N = K \cap N \Rightarrow KN \cap H = K$, 于是

$$HN/KN = H(KN)/KN \cong H/KN \cap H = H/K$$

§ 1.4 习 题

1. 设 $G = \langle a \rangle$, 则 G 的合成列有如下 3 个.

$$(i) G \triangleright H_1 \triangleright H_3 \triangleright \{e\}$$

$$(ii) G \triangleright H_1 \triangleright H_4 \triangleright \{e\}$$

$$(iii) G \triangleright H_2 \triangleright H_4 \triangleright \{e\}$$

这里 $H_1 = \langle a^2 \rangle$, $H_2 = \langle a^3 \rangle$, $H_3 = \langle a^4 \rangle$, $H_4 = \langle a^6 \rangle$.

2. 令 $G = \langle B_4, (12) \rangle$, 则 G 的合成列有如下 7 个.

$$(i) G \triangleright B_4 \triangleright C_1 \triangleright \{(1)\}$$

$$(ii) G \triangleright B_4 \triangleright C_2 \triangleright \{(1)\}$$

$$(iii) G \triangleright B_4 \triangleright C_3 \triangleright \{(1)\}$$

$$(iv) G \triangleright \bar{B}_4 \triangleright \bar{C}_1 \triangleright \{(1)\}$$

$$(v) G \triangleright \bar{B}_4 \triangleright \bar{C}_2 \triangleright \{(1)\}$$

$$(vi) G \triangleright \bar{B}_4 \triangleright \bar{C}_3 \triangleright \{(1)\}$$

$$(vii) G \triangleright H \triangleright C_2 \triangleright \{(1)\}$$

这里 $\overline{B_4} = \{(1), (12), (34), (12)(34)\} \cong B_4, H = ((1234)), C_i$ 和 $\overline{C_i}$ 自明.

3. 因 $G = \langle a \rangle$, 而 $|G| = 2^n$. G 除本身外有如下 n 个子群.

$H_1 = \langle a^2 \rangle, H_2 = \langle a^{2^2} \rangle, \dots, H_{n-1} = \langle a^{2^{n-1}} \rangle, H_n = \{e\}$
 设 H 为 G 的任一子群, 通过整数性质可以证明: $H = H_i = \langle a^{2^i} \rangle$. 故 G 只有如下一个合成列.

$$G \triangleright H_1 \triangleright H_2 \triangleright \dots \triangleright H_{n-1} \triangleright H_n = \{e\}$$

4. 设 G 是可换群, 且

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_{i-1} \triangleright G_i \triangleright \dots \triangleright G_r = \{e\}$$

为 G 的一个合成列, 于是知每一因子群 G_{i-1}/G_i 为单群, 且 G_{i-1}/G_i 亦为可换群. 因之 G_{i-1}/G_i 的阶为素数或 1, 即每一因子群皆为有限群.

§ 1.5 习 题

1. 由第一同构定理知

$$HK/K \cong H/H \cap K$$

利用 H 是可解群, 知 $H/H \cap K$ 是可解群, 利用 K 和 HK/K 是可解群, 可推出 HK 是可解群.

2. 设 $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_{i-1} \triangleright G_i \triangleright \dots \triangleright G_r = \{e\}$ 是 G 的一个可解列. 设 $H \leq G$, 则

$$\begin{aligned} H &= H \cap G_0 \supseteq H \cap G_1 \supseteq \dots \supseteq H \cap G_{i-1} \\ &\supseteq H \cap G_i \supseteq \dots \supseteq H \cap G_r = \{e\} \end{aligned}$$

因 $G_i \triangleright G_{i-1}$, 而 $H \cap G_i \leq G_{i-1}$. 由第一同构定理得 $(H \cap G_{i-1})G_i/G_i \cong H \cap G_{i-1}/(H \cap G_{i-1}) \cap G_i = H \cap G_{i-1}/H \cap G_i$ 但 $(H \cap G_{i-1})G_i \subseteq G_{i-1}$, 故

$(H \cap G_{i-1})G_i/G_i \leq G_{i-1}/G_i$ 又 G_{i-1}/G_i 可换 \Rightarrow
 $(H \cap G_{i-1})G_i/G_i$ 可换, 故 $H \cap G_{i-1}/H \cap G_i$ 可换, 所以
 H 是可解群.

3. 因 $G^{(1)} = [G, G] = G_1$, $G^{(2)} = [G^{(1)}, G^{(1)}] \subseteq$
 $[G_1, G] = G_2$. 一般有 $G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \subseteq [G,$
 $G^{(i-1)}] = G_i$ 又因 $G_m = [G, G_{m-1}] = \{e\}$, 所以 $G^{(m)} \subseteq$
 $G_m = \{e\}$.

§ 1.6 习 题

1. 设 $M = \{a_1, a_2, \dots, a_n\}$, 任取 $a_i, a_j \in M$, 知有
 $\alpha, \beta \in G$ 使 $a_i^\alpha = a_i, a_j^\beta = a_j$. 取 $\gamma = \alpha^{-1}\beta$ 则 $a_i^\gamma = a_j$.

2. 设 G_a 为 a 的稳定子群, 对任 $\tau \in G$, 令

$$\varphi: G_a \tau \rightarrow a^\tau$$

则 φ 显然是 G_a 的右陪集的集合到作用集合 M 的满单射,
 所以 $|G : G_a| = m$; 因之 $m | n$.

§ 2.1 习 题

1. 利用 2.1.6 直接验证.

2. 令 $F = \bigcap_{\alpha} F_{\alpha}$, F_{α} 为 F 的子域, F 中显然含非零元.

任取 $a, b \in F$, 则对一切 $\alpha, a, b \in F_{\alpha}$, 所以 $a - b \in F_{\alpha}$, 当
 $b \neq 0$ 时 $ab^{-1} \in F_{\alpha}$, 从而 $a - b \in F, ab^{-1} \in F (b \neq 0)$, 故 F 是
 E 的子域.

4. 列出 Z_{11} 的加法表和乘法表, 然后计算或利用同余法
 则进行计算.

5. 可直接利用 2.1.4 来验证, 或利用 2.1.6 验证它们是
 实数域 R 的子域.

§ 2.2 习 题

1. $[Q(\sqrt{2}) : Q] = 2$. $1, \sqrt{2}$ 是 $Q(\sqrt{2})$ 在 Q 上一个基.

$$[Q(\sqrt{2}, \sqrt{3}) : Q]$$

$$= [Q(\sqrt{2}, \sqrt{3}) : Q(\sqrt{2})][Q(\sqrt{2}) : Q] = 4$$

$1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ 是一个基.

2. 由于 Z_p 有 p 个元, $[K : Z_p] = n$, 所以 K 恰含有 p^n 个元.

3. $[Q(a) : Q] = 3$. $1, a, a^2$ 为 $Q(a)$ 在 Q 上的通常基, $a^4 = -18 - 57a + 27a^2$, $3a^5 - a^4 + 2 = -223 - 726a$

$+ 288a^2$, 由于 $\frac{1}{13}[(x+1)(x^2-7x+16)] - f(x) = 1$, 所以

$$(a+1)^{-1} = \frac{16}{13} - \frac{7}{13}a + \frac{1}{13}a^2.$$

4. 因 $[K : F] = [K : E][E : F] = [K : E]$, 所以 $[E : F] = 1$, 故 $E = F$.

5. 由于 $[E : F] = p$ (素数), 则 $p \geq 2$, 所以可取 $a \in E/F$, $[E : F] = [E : F(a)][F(a) : F]$, $[F(a) : F] > 1$, $[F(a) : F] | p$, 故 $[F(a) : F] = p$, 因而 E 是 F 的单代数扩域.

6. 若 $[F(a) : F] = 1$, 则显然有 $F(a) = F(a^2)$

若 $[F(a) : F] > 1$, 且 $[F(a) : F]$ 为奇数, 则由 $[F(a) : F(a^2)][F(a^2) : F] = [F(a) : F]$. 知道 $[F(a) : F(a^2)]$ 和 $[F(a^2) : F]$ 也都是奇数. 所以 a^2 是 F 上奇次代数元, 今证明 $[F(a) : F(a^2)] = 1$.

显然 a 是 $F(a^2)$ 上多项式 $x^2 - a^2 = 0$ 的根, 故 a 在 $F(a^2)$ 上的次数至多为 2, 又因为 $[F(a) : F(a^2)]$ 为奇数. 所以 $[F(a) : F(a^2)] = 1$.

7. (1) 设 α, β 在 F 上的极小多项式分别为 $f(x), g(x)$, 则 $\partial^\circ(f(x)) = m, \partial^\circ(g(x)) = n$. 若 β 在 $F(\alpha)$ 上的极小多项式为 $p(x)$, 则 $p(x) | g(x)$, 从而 $\partial^\circ(p(x)) \leq \partial^\circ(g(x))$. 故

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] \leq mn.$$

(2) 设 $[F(\alpha, \beta) : F] = s$, 由 (1) $s \leq mn$. 因为 $[F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] = [F(\alpha, \beta) : F(\beta)][F(\beta) : F(\alpha)] = [F(\alpha, \beta) : F]$, 所以 $m | s, n | s$, 又 $(m, n) = 1$, 故 $mn | s$, 于是 $mn = s$.

8. 充分性, 设 $E = F(\alpha)$, α 在 F 上的极小多项式是 $x^4 + ax^2 + b$. 令 $L = F(\alpha^2)$, 显然 $F \subset L \subset E$. 由于 $x^4 + ax^2 + b$ 在 F 上不可约, 所以 $x^2 + ax + b$ 在 F 上也不可约. 易验证 α^2 是 $x^2 + ax + b$ 的根, 因此 $x^2 + ax + b$ 是 α^2 在 F 上的极小多项式, L 是 F 的二次扩域.

必要性 设 $F \subset L \subset E$, $[L : F] = 2, [E : F] = 4$, 则 $[E : L] = 2$. 利用 $\text{char } F \neq 2$, 可以证明 $E = L(\theta)$ 而 θ 在 L 上极小多项式是 $x^2 - \lambda, \lambda \in L$.

(i) 若 $\lambda \notin F$, λ 在 F 上极小多项式为 $x^2 + ax + b$, 由于 $\theta^2 = \lambda$, 所以 $\theta^4 + a\theta^2 + b = 0$, 但

$$L = F(\lambda), E = L(\theta) = F(\lambda, \theta) = F(\theta)$$

而 $[E : F] = 4$, 所以 θ 在 F 上的极小多项式是 $x^4 + ax^2 + b$.

(ii) 若 $\lambda \in F$, 那么由 $[L : F] = 2$, 可找到 $\mu \in L, \mu \notin F$ 而 $\mu^2 \in F$. 取 $\theta' = \theta(1 + \mu)$, 则可证 $\theta'^2 = \lambda' \notin F$, 与 (i) 一样可证 $E = F(\theta')$, 而 θ' 在 F 上的极小多项式是 $x^4 + ax^2 + b$.

§ 2.3 习 题

$$1. L = \mathbb{Q}(\sqrt[3]{2}, \omega), \text{ 这里 } \omega = \frac{-1 + \sqrt{3}i}{2}, [L : \mathbb{Q}] = 6,$$

2. 设 a_1, a_2, \dots, a_n 为 $f(x)$ 的 n 个根, 则 a_1 在 F 上的极小多项式的次数 $m_1 \leq n$, 即 $[F(a_1) : F] = m_1 \leq n$, 在 $F(a_1)$ 上 $f(x)$ 可分解成

$$f(x) = (x - a_1) \cdot f_1(x)$$

$\partial^\circ(f_1(x)) = n - 1$, a_2, \dots, a_n 是 $f_1(x)$ 的根, 则 a_2 在 $F(a_1)$ 上的极小多项式的次数 $m_2 \leq n - 1$, 于是

$$\begin{aligned} [F(a_1)(a_2) : F] &= [F(a_1)(a_2) : F(a_1)][F(a_1) : F] \\ &\leq n(n-1) \end{aligned}$$

这样做下去可得

$$[F(a_1, a_2, \dots, a_n) : F] \leq n!$$

设 $N = F(a_1)(a_2)\cdots(a_n) = F(a_1, \dots, a_n)$, N 为 $f(x)$ 在 F 上的分裂域.

3. $f(x) = (x-1)(x^{p-1} + x^{p-2} + \cdots + 1)$, $x^{p-1} + x^{p-2} + \cdots + 1$ 是 \mathbb{Q} 上不可约多项式, 其分裂域为 $E = \mathbb{Q}(\theta)$, θ 为 p 次本原单位根, E 也是 $f(x)$ 在 \mathbb{Q} 上的分裂域, 而 $[E : \mathbb{Q}] = p - 1$.

4. 令 $f(x) = p_1(x)p_2(x)\cdots p_s(x)$, 作 $f(x)$ 在 F 上的分裂域 E , E 含有 $f(x)$ 的所有根, 因而含有 a_1, \dots, a_s , 其中 a_i 为 $p_i(x)$ 的根, $i = 1, 2, \dots, s$, 因此

$$F(a_1, \dots, a_s) \subseteq E$$

$F(a_1, \dots, a_s)$ 是 F 的有限扩域.

§ 2.4 习 题

1. $f(x)$ 的根为

$$\alpha_1 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, \quad \alpha_2 = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i,$$

$$\alpha_3 = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, \quad \alpha_4 = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$$

又因为 $\alpha_2 = \alpha_1^{-1}$, $\alpha_3 = -\alpha_1^{-1}$, $\alpha_4 = -\alpha_1$, 所以令 $\alpha = \alpha_1$

则 $\mathbf{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \mathbf{Q}(\alpha)$

为 $f(x) = x^4 + 1$ 在 \mathbf{Q} 上的分裂域.

2. (1) 取 $c = 1$ 即满足条件(4), 故 $\theta = \sqrt{3} + \sqrt[3]{2}$

(2) 令 $\alpha = \frac{-1 + \sqrt{3}i}{2}$, $\beta = 2i$, 取 $c = 1$, $\theta = \alpha + \beta$

即为所求.

3. 设 $\alpha = \sqrt{2} + \sqrt{3}$, $\alpha^3 = 11\sqrt{2} + 9\sqrt{3}$, 于是

$$11\alpha - \alpha^3 = 2\sqrt{3}, \quad \sqrt{3} = \frac{11}{2}\alpha - \frac{1}{2}\alpha^3. \quad \text{同理可知}$$

$$\sqrt{2} = \frac{1}{2}\alpha^3 - \frac{9}{2}\alpha.$$

4. 设 E 是 F 的代数扩域, K 是 E 的不可分扩域, $\alpha \in K$ 是 E 的不可分元素, 则有 E 上不可约多项式 $p(x)$ 以 α 为根. 但 K 也是 F 的扩域, 故是可分扩域, α 是 F 上可分元, 设 α 在 F 上极小多项式为 $g(x)$, $g(x)$ 无重根, 在 $E[x]$ 中 $p(x) | g(x)$, 故 $p(x)$ 也无重根, 矛盾.

§ 2.5 习 题

1. 设 Δ 是特征为 3 的素域, $\Delta = \{0, 1, 2\}$, 则 $f(x) = x^2 + 1$ 在 $\Delta[x]$ 中不可约. 作 Δ 上单式数扩域 $F = \Delta(\alpha)$, α 在 Δ 上的极小多项式为 $f(x)$, F 含有 9 个元, $|F^*| = 8$, 但 $\alpha^2 = -1$, $\alpha^4 = 1$, 所以 α 不是 F^* 的生成元.

2. 设 Δ 是特征为 3 的素域, $\Delta = \{0, 1, 2\}$, Δ 上 2 次不可约多项式必为 $x^{3^2-1} - 1 = x^8 - 1$ 的因式, 而

$$x^8 - 1 = (x+1)(x-1)(x^2+1)(x^2+x+2)(x^2+2x+2)$$

且 x^2+1 , x^2+x+2 , x^2+2x+2 皆为 $\Delta[x]$ 中不可约多项式. $\Delta[x]/(x^2+1)$, $\Delta[x]/(x^2+x+2)$, $\Delta[x]/(x^2+2x+2)$ 皆是特征为 3 的 9 元域, 仿例 1 可列出它们的加法表和乘法表, 只列出 $\Delta[x]/(x^2+1)$ 即可.

3. 令 E 所含素域为 Δ , 根据 2.5.3, E 是多项式 $x^{p^n} - x$ 在 Δ 上的分裂域, 若 $m|n$, 则 $p^m - 1 | p^n - 1$, 进一步有 $x^{p^{m-1}} - 1 | x^{p^n-1} - 1$, 即 $x^{p^m} - x | x^{p^n} - x$, 因此 E 含 $x^{p^m} - x$ 的所有根, 这些根作成有一个有 p^m 个元的 E 的子域, 若 L_1 也是含有 p^m 个元的 E 的子域, 由 2.5.3 知 L_1 也是由 $x^{p^m} - x$ 在 E 中所有根作成的, 因而 $L_1 = L$.

§ 3.1 习 题

1. 由 $[E : \mathbb{Q}] = 2$, 知 E 是 \mathbb{Q} 的单代数扩域, 因而存在 $\beta \in E/\mathbb{Q}$, 使得 $E = \mathbb{Q}(\beta)$, β 在 \mathbb{Q} 上的极小多项式是

$$f(x) = x^2 + ax + b. \quad a, b \in \mathbb{Q}$$

将 $f(x)$ 化为整系数多项式

$$g(x) = hx^2 + kx + l, \quad h, k, l \in \mathbb{Z}$$

$f(x)$ 与 $g(x)$ 有相同的根, 取

$$\beta = \frac{-k \pm \sqrt{k^2 - 4hl}}{2h}$$

$k^2 - 4hl$ 为整数, 则 $\sqrt{k^2 - 4hl} = n\sqrt{m}$. 这里 $n \in \mathbb{Z}$ $m = -1$ 或者 $m = \pm p_1 p_2 \cdots p_s$, p_1, p_2, \dots, p_s 为互不相同的素数.

令 $\alpha = \sqrt{m}$, 则有 $\beta = -\frac{k}{2h} + \frac{n}{2h}\alpha$, $-\frac{k}{2h}, \frac{n}{2h} \in \mathbb{Q}$

所以 $E = \mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$, 这里 $\alpha = \sqrt{m}$, $m = -1$ 或 $m = \pm p_1 \cdots p_s$, 当 $i \neq j$ 时 $p_i \neq p_j$.

2. 令 $F = \mathbb{Q}(\sqrt[3]{3})$, 显然 $[F : \mathbb{Q}] = 3$, 由于 $\sqrt[3]{3}$ 在 \mathbb{Q} 上的共轭元 $\sqrt[3]{3}\omega \notin \mathbb{Q}(\sqrt[3]{3})$, 这里 $\omega = \frac{-1 + \sqrt{3}i}{2}$, 所以

F 不是 \mathbb{Q} 的正规域. 令 $F = \mathbb{Q}(\sqrt[4]{2})$, 显然 $[F : \mathbb{Q}] = 4$, 同样讨论可知 F 不是 \mathbb{Q} 的正规域.

3. 因为 P_2 是 F 的正规域, 所以 P_2 是 F 上某个多项式 $f(x)$ 的分裂域. 但 $f(x)$ 也是 P_1 上的多项式, 所以 P_2 也是 $f(x)$ 在 P_1 上的分裂域, 故 P_2 也是 P_1 的正规域.

若 P_2 是 F 的正规域, 则 P_1 不一定是 F 的正规域. 例如 $\mathbb{Q}(\sqrt[3]{2}, i) \supseteq \mathbb{Q}(\sqrt[3]{2}) \supseteq \mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2}, i)$ 是 $\mathbb{Q}(\sqrt[3]{2})$ 的正规域, 但 $\mathbb{Q}(\sqrt[3]{2})$ 不是 \mathbb{Q} 的正规域.

§ 3.2 习 题

1. 只需证明 τ 是 N 到自身的双射. 因为 N 是 F 的正规域, 所以 $N = F(\theta)$, θ 在 F 上的极小多项式为 $g(x)$. 由 $g(\theta) = 0$ 可得 $g(\theta^\tau) = 0$. 则 $\theta^\tau \in N$, 从而 $N = F(\theta) = F(\theta^\tau)$. 这样 τ 是 N 到自身的双射.

2. 因为 N 的任一自同构都使 \mathbb{Q} 中的元不动, 所以找出 $\text{Aut } N$ 就是找出 N 的保持 \mathbb{Q} 的元不动的一切自同构.

由于 N 是 \mathbb{Q} 上有限可分扩域, $N = \mathbb{Q}(\sqrt{5}, \omega) = \mathbb{Q}(\sqrt{5} + \omega)$. 任取 $\tau \in \text{Aut } N$, 则

$$(\sqrt{5} + \omega)^\tau = (\sqrt{5})^\tau + \omega^\tau$$

显然 $\sqrt{5}^\tau = \begin{cases} \sqrt{5} \\ -\sqrt{5} \end{cases}$, $\omega^\tau = \begin{cases} \omega \\ \omega^2 \end{cases}$, 这样可得

$$\tau_1: \sqrt{5} + \omega \rightarrow \sqrt{5} + \omega$$

$$\tau_2: \sqrt{5} + \omega \rightarrow \sqrt{5} + \omega^2$$

$$\tau_3: \sqrt{5} + \omega \rightarrow -\sqrt{5} + \omega$$

$$\tau_4: \sqrt{5} + \omega \rightarrow -\sqrt{5} + \omega^2$$

于是 $\text{Aut}N = \{\tau_1 = \varepsilon, \tau_2, \tau_3, \tau_4\}$, 其乘法表如下:

	τ_1	τ_2	τ_3	τ_4
τ_1	τ_1	τ_2	τ_3	τ_4
τ_2	τ_2	τ_1	τ_4	τ_3
τ_3	τ_3	τ_4	τ_1	τ_2
τ_4	τ_4	τ_3	τ_2	τ_1

设 N 在 $\mathbb{Q}(\sqrt{5})$ 上的自同构群为 H , 则 $H = \{\tau_1, \tau_2\}$, 这是因为 $\sqrt{5}^{\tau_1} = \sqrt{5}$, $\sqrt{5}^{\tau_2} = \sqrt{5}$.

3. 因为 $N = \mathbb{Q}(\sqrt[3]{2}, \omega)$ 是 $(x^3 - 2)(x^2 + x + 1)$ 在 \mathbb{Q} 上的分裂域, 所以 N 是 \mathbb{Q} 的正规域, 且 $N = \mathbb{Q}(\sqrt[3]{2} + \omega)$, 任取 $\tau \in \text{Gal}N/\mathbb{Q}$, 则

$$(\sqrt[3]{2} + \omega)^\tau = (\sqrt[3]{2})^\tau + \omega^\tau$$

$$(\sqrt[3]{2})^\tau = \begin{cases} \sqrt[3]{2} \\ \sqrt[3]{2}\omega \\ \sqrt[3]{2}\omega^2 \end{cases}, \quad \omega^\tau = \begin{cases} \omega \\ \omega^2 \end{cases}$$

又 $|\text{Gal}N/\mathbb{Q}| = 6$, 所以 $\text{Gal}N/\mathbb{Q}$ 恰含 6 个元素:

$\text{Gal}N/Q = \{\tau_1 = \varepsilon, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6\}$. 且

	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6
$\sqrt[3]{2} \rightarrow$	$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}\omega^2$
$\omega \rightarrow$	ω	ω^2	ω	ω^2	ω	ω^2

由上表很容易引出 $\text{Gal}N/Q$ 的乘法表.

§ 3.3 习 题

1. 设 G_0 是域 K 上 n 次一般方程

$$x^n - u_1 x^{n-1} + \cdots + (-1)^n u_n = 0$$

在域 $F' = K(u_1, \cdots, u_n)$ 上的伽罗华群, 则由 3.3.4 知 $G_0 \cong S_n$. 因为 $G \subseteq S_n$, 在 G_0 存在一个子群 $G' \cong G$, 令

$$G' \rightarrow F = \text{Inv}G'$$

由伽罗华基本定理, $F' \subseteq F \subseteq N$, 这里 N 为所给一般方程的根域. F 唯一存在且 N 是 F 的正规域, $N = F(\alpha)$. 设 α 在 F 上的极小多项式为 $f(x)$, 则 $f(x) = 0$ 在 F 上的伽罗华群就是 G' .

2. 因为 $f(x)$ 在 F 上可约, 所以 $f(x)$ 在 F 上可分解为

$$f(x) = p_1^{r_1}(x) \cdots p_s^{r_s}(x)$$

这里 $p_1(x), \cdots, p_s(x)$ 为 $F[x]$ 中互不相同的不可约多项式, $r_i \geq 1, i = 1, 2, \cdots, s$.

设 $f(x)$ 在 F 上的分裂域为 N , 令

$$f_0(x) = p_1(x) \cdots p_s(x)$$

则 $f_0(x)$ 在 F 上的分裂域仍为 N . 因而 $f(x)$ 与 $f_0(x)$ 在 F 上伽罗华群相同, 记为 G . 设 $\partial^\circ(f_0(x)) = m$, 由 3.3.2 知 $G \cong S_m$ 的一个子群.

$$\varphi: \tau \rightarrow \begin{pmatrix} a_1 & a_2 & \cdots & a_m \\ a_1' & a_2' & \cdots & a_m' \end{pmatrix}, a_1, \cdots, a_m \text{ 为 } f_0(x)$$

的根。

i) 当 $m < n$ 时, G 不与 S_n 同构。

ii) 当 $m = n$ 时, $f(x) = f_0(x)$. 设 a_1 与 a_2 分别为 $p_1(x)$ 与 $p_2(x)$ 的根, 由于 $p_1(x)$ 与 $p_2(x)$ 无公根, 所以 $a_1' \neq a_2$. 因之在 $\varphi(G)$ 中不出现 $\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_2 & a_1 & a_3 & \cdots & a_n \end{pmatrix}$, 所以 G 不与 S_n 同构。

§ 3.4 习 题

1. $N = \mathbb{Q}(\sqrt{3}, i)$ 是方程 $(x^2 - 3)(x^2 + 1) = 0$ 在 \mathbb{Q} 上的根域. $|\text{Gal}N/\mathbb{Q}| = [N : \mathbb{Q}] = 4$. $\text{Gal}N/\mathbb{Q}$ 中四个元可列表说明如下:

	τ_1	τ_2	τ_3	τ_4
$\sqrt{3} \mapsto$	$\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$
$i \mapsto$	i	i	$-i$	$-i$

$\text{Gal}N/\mathbb{Q} = \{\tau_1 = \varepsilon, \tau_2, \tau_3, \tau_4\}$, 将 $\sqrt{3}, -\sqrt{3}, i, -i$ 分别标为 1, 2, 3, 4, 则

$$\text{Gal}N/\mathbb{Q} \cong \{(1), (12), (34), (12)(34)\} \cong B_4$$

于是 $\text{Gal}N/\mathbb{Q}$ 有 5 个子群: $\text{Gal}N/\mathbb{Q}, H_1 = \{\tau_1, \tau_2\}, H_2 = \{\tau_1, \tau_3\}, H_3 = \{\tau_1, \tau_4\}, \{\varepsilon\}$. 这 5 个子群在伽罗华映射 Φ 之下的象分别为 $\mathbb{Q}, L_1 = \mathbb{Q}(i), L_2 = \mathbb{Q}(\sqrt{3}), L_3 = \mathbb{Q}(\sqrt{3}i), N$. 即如图 A 所示.

2. $N = \mathbb{Q}(\sqrt[4]{2}, i)$ 为 $x^4 - 2 = 0$ 在 \mathbb{Q} 上的根域, 由 § 3.3 的例 4 知 $\text{Gal}N/\mathbb{Q}$ 恰含 8 个元, 设为 $\tau_1 = \varepsilon, \tau_2, \cdots, \tau_8$.

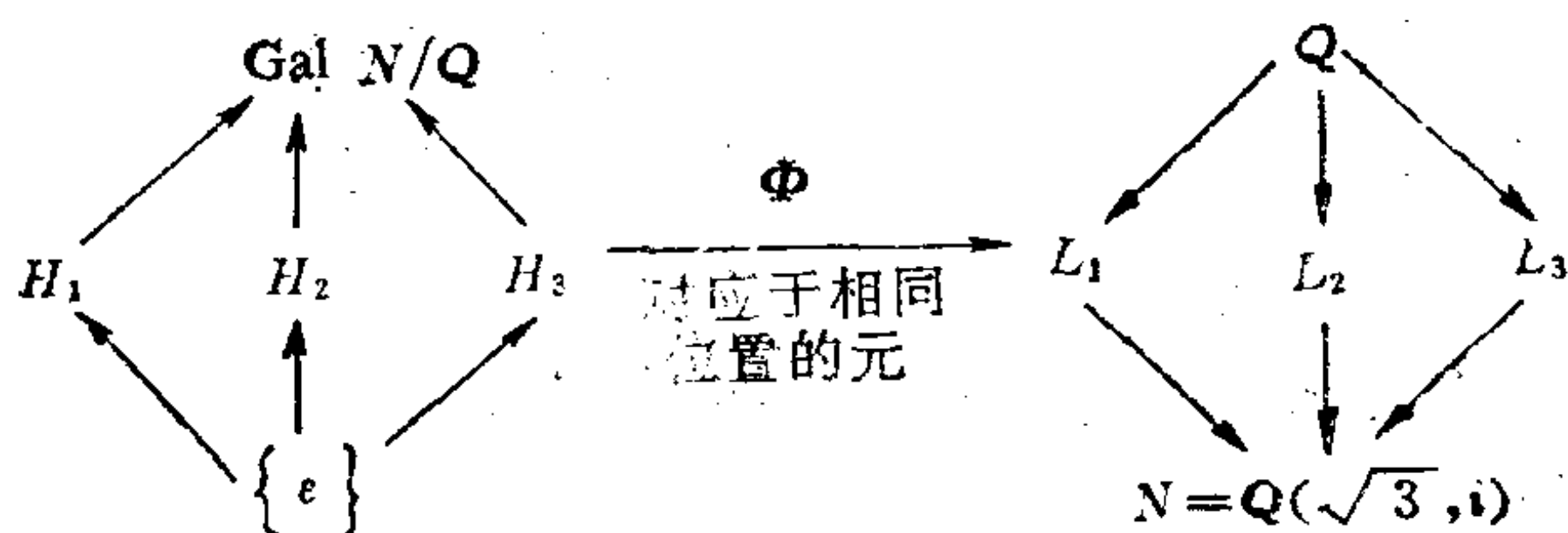


图 A

且 $\text{Gal } N/Q \cong H$, 这里

$$H = \{(1)(12)(34), (1324), (1423), (34), (12), (13)(24), (14)(23)\}$$

H 是 S_4 的一个子群。由此可知 $\text{Gal } N/Q$ 有 10 个子群:

$\text{Gal } N/Q$, $H_1 = \{\tau_1, \tau_6, \tau_5, \tau_2\}$, $H_2 = \{\tau_1, \tau_2, \tau_3, \tau_4\} = (\tau_3)$, $H_3 = \{\tau_1, \tau_2, \tau_7, \tau_8\}$, $H_4 = \{\tau_1, \tau_6\}$, $H_5 = \{\tau_1, \tau_5\}$, $H_6 = \{\tau_1, \tau_2\}$, $H_7 = \{\tau_1, \tau_7\}$, $H_8 = \{\tau_1, \tau_8\}$, $\{\tau_1\}$. 它们分别对应的子域是:

Q , $L_1 = Q(\alpha^2)$, $L_2 = Q(i)$, $L_3 = Q(\alpha^2 i)$, $L_4 = Q(\alpha i)$, $L_5 = Q(\alpha)$, $L_6 = Q(\alpha^2, i)$, $L_7 = Q((1+i)\alpha)$, $L_8 = Q((1-i)\alpha)$, $N = Q(\alpha, i)$. 这里 $\alpha = \sqrt[4]{2}$, 可以用图 B 表示这种对应关系:

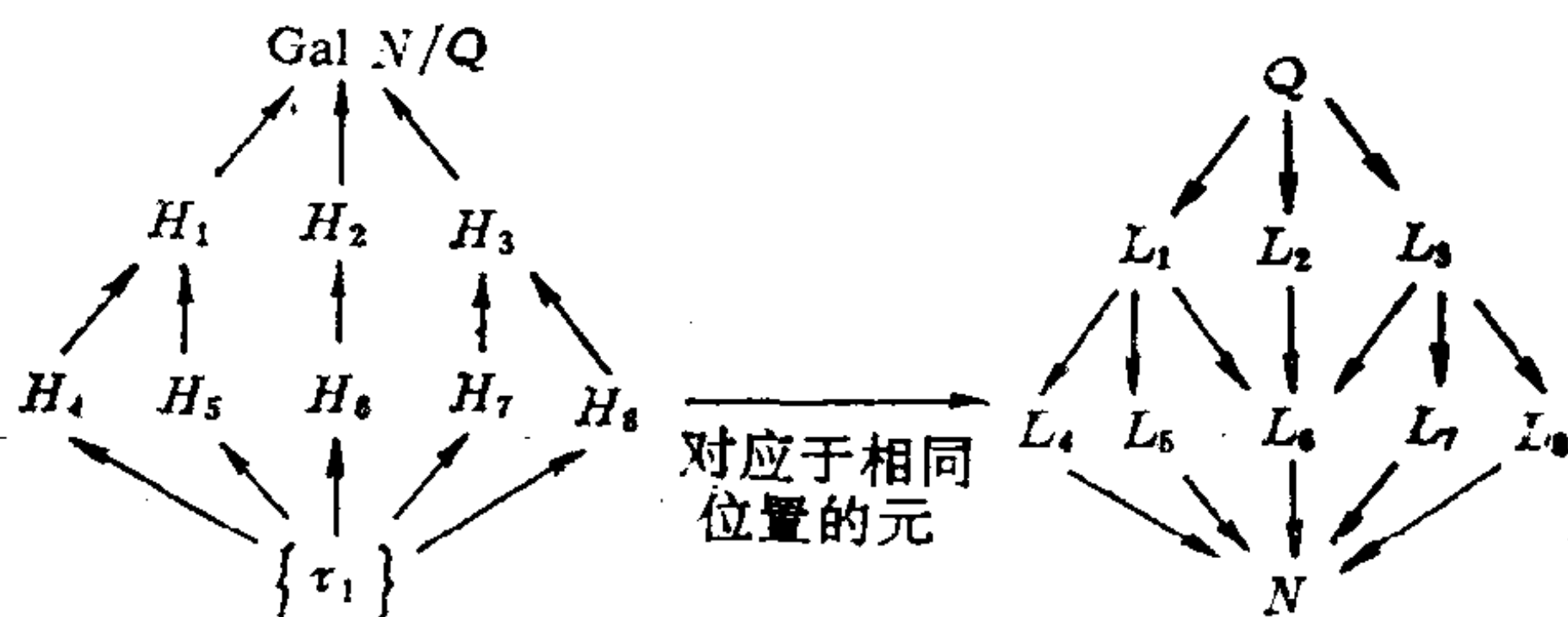


图 B

因为 $\{\tau_1\}$, H_1, H_2, H_3 , $\text{Gal}N/Q$ 是 $\text{Gal}N/Q$ 的不变子群, 所以 N, L_1, L_2, L_3, Q 是 Q 的正规域.

3. 因为 $H \cong \text{Gal}N/F$, 所以 $H \subseteq \text{Gal}N/F$

$$\varphi: H \rightarrow \text{Inv}H = L$$

则 $L \supseteq F$. 因为 L 的元在 H 元下均不变, 所以存在 $a \in L$ 而 $a \notin F$ 使得 a 在 H 元下不变.

4. 设 N 是 F 的正规域. 因为 G 是 N 在 F 上的自同构群, 所以对于任意 $a \in F$, $\tau \in G$ 都有 $a^\tau = a$, 因而 $F \subseteq L$. 由 $G = \text{Gal}N/F$ 恰为 N 在 L 上的伽罗华群, 利用 3.2.6 可得 $F = L$.

反之, 设 $F = L$, 由于 N 是 F 的有限扩域, 所以 $N = F(\theta)$. 由于 G 是 N 在 F 上的自同构群, 所以 G 的阶一定有限, 设

$$G = \{\tau_1 = \varepsilon, \tau_2, \dots, \tau_m\}$$

考虑

$$f(x) = (x - \theta^{\tau_1}) (x - \theta^{\tau_2}) \cdots (x - \theta^{\tau_m})$$

对任意 $\tau \in G$, 有

$f(x)^\tau = (x - \theta^{\tau_1\tau}) (x - \theta^{\tau_2\tau}) \cdots (x - \theta^{\tau_m\tau}) = f(x) \in L[x] = F[x]$. 于是 N 是 F 上多项式 $f(x)$ 的分裂域, 故 N 是 F 的正规域

5. 令 Ψ 是伽罗华映射

$$\Psi: I_1 \rightarrow H_1, I_2 \rightarrow H_2$$

假设 I_1 和 I_2 在 F 上共轭, 并设 $I_1 = F(\alpha)$. $\tau: I_1 \rightarrow I_2$ 是同构映射, 且 $a^\tau = a, \forall a \in F$. 设 $\alpha^\tau = \beta$, 则 $F(\beta) = I_2$, 进一步有 α 与 β 在 F 上共轭. 由 3.4.5 的证明知, 存在 $\sigma \in \text{Gal}N/F = G$ 使得 $\beta = \alpha^\sigma$, 于是 $F(\alpha^\sigma) = F(\beta) = I_2$. 这

样, $I_1 = F(\alpha) \cong F(\alpha^\sigma) = I_2$. 任取 $\tau_1 \in H_1$, 则 $(\alpha^\sigma)^{\sigma^{-1}\tau_1\sigma} = \alpha^{\tau_1\sigma} = \alpha^\sigma$, 即 $\sigma^{-1}H_1\sigma$ 的任意元不使 α^σ 变动, 因而 $\sigma^{-1}H_1\sigma$ 也不使 I_2 的元变动, 所以 $\sigma^{-1}H_1\sigma \subseteq H_2$. 同理, 我们可以把 I_1 写成 $I = F((\alpha^\sigma)^{\sigma^{-1}})$, 因此 $\sigma H_2 \sigma^{-1} \subseteq H_1$, 于是 $H_2 \subseteq \sigma^{-1}H\sigma$, 故 $H_2 = \sigma^{-1}H_1\sigma$.

反之, 假设 H_1 与 H_2 共轭, 令 $H_2 = \sigma^{-1}H\sigma$, $\sigma \in G$. 设 $I_1 = F(\alpha)$, 则 $I_1 = F(\alpha) \cong F(\alpha^\sigma) = I'_2$, 显然 I_1 与 I'_2 共轭. 由前面的证明知

$$\begin{aligned} \Psi: \quad I_1 &\rightarrow H_1 \\ I'_2 &\rightarrow \sigma^{-1}H_1\sigma \end{aligned}$$

但

$$\Psi: \quad I_2 \rightarrow H_2$$

又 $H_2 = \sigma^{-1}H_1\sigma$ 所以 $I'_2 = I_2$.

§ 4.1 习 题

1. 方程 $x^n - 1 = 0$ 在 F 上的伽罗华群不一定是循环群. 例如方程 $x^8 - 1 = 0$ 在 \mathbb{Q} 上的伽罗华群就不是一个循环群.

2. 方程 $x^n - a = 0$ 在 F 上的伽罗群不一定是交换群. 例如方程 $x^3 - 2 = 0$ 在 \mathbb{Q} 上的伽罗华群与 S_3 同构, 而 S_3 不是交换群.

§ 4.2 习 题

1. 设 α 是 $f(x)$ 的一个根, 且 $\alpha \in N$, 并且 N/F 具有根塔, 可假设 N 为 F 的正规域. 由于 $f(x)$ 不可约, 且 $f(\alpha) = 0$, 而 $\alpha \in N$. 由正规扩域的定义知 N 包含 $f(x) = 0$ 的根域, 即方程的所有根皆在 N 中, 所以 $f(x) = 0$ 在 F 上可用根号

解.

2. 设 ε 是 n 次本原根, α 是 $x^n - a = 0$ 的一个根, 则方程 $x^n - a = 0$ 在 F 上的根域 $N = F(\varepsilon, \alpha)$. 于是

$$N \subseteq F(\varepsilon) \subseteq F(\varepsilon)(\alpha) = N$$

考虑伽罗华映射图

$$\begin{array}{ccccc} F \subseteq F(\varepsilon) \subseteq F(\varepsilon)(\alpha) = N \\ \updownarrow \quad \updownarrow \quad \updownarrow \\ G \supseteq G_1 \supseteq G_2 = \{e\} \end{array}$$

则不难看出

$$G \supseteq G_1 \supseteq G_2 = \{e\}$$

为可解列.

§ 4.3 习 题

$$1. \quad f(x) = 3x^5 - 5x^3 - 30x + 30 = 0$$

是 \mathbb{Q} 上不能用根号解的 5 次方程又一个例子.

§ 4.4 习 题

2. $f(x) = x^3 - 3x - 1$ 在 \mathbb{Q} 上显然不可约. 又 $\mathbb{Q} \ni \sqrt{D}$, 所以 $f(x) = 0$ 在 \mathbb{Q} 上的伽罗群 G 的阶是 3, 设 N 是 $f(x)$ 在 \mathbb{Q} 上的分裂域, 则 $[N : \mathbb{Q}] = 3$. 设 α 是 $f(x) = 0$ 的一个根, 则 $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, 又 $\mathbb{Q}(\alpha) \subseteq N$. 所以 $N = \mathbb{Q}(\alpha)$.

3. 显然 $g(x) = x^3 + x + 1$ 在 \mathbb{Q} 上不可约, 不难算出 $\sqrt{D} \notin \mathbb{Q}$. 所以 $g(x)$ 在 \mathbb{Q} 上的伽罗华群不与 A_3 同构. 这样可证出 $G \cong S_3$.

§ 4.5 习 题

$$1. \quad x^7 - 1 = 0 \text{ 的本原根为}$$

$$\varepsilon = \cos \frac{2}{7}\pi + i \sin \frac{2}{7}\pi$$

$$\varepsilon^{-1} = \varepsilon^6 = \cos \frac{2}{7}\pi - i \sin \frac{2}{7}\pi$$

ε 是 $\varphi(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$ 的根。正七边形可作 $\Leftrightarrow \varepsilon + \varepsilon^6 = 2\cos \frac{2}{7}\pi$ 可作。

又 $\varepsilon + \varepsilon^6$ 是 $f(x) = x^3 + x^2 - 2x - 1 = 0$ 的根，且 $f(x)$ 不可约，所以 $[\mathbf{Q}(\varepsilon + \varepsilon^6) : \mathbf{Q}] = 3$ 。因之 $\varepsilon + \varepsilon^6 = 2\cos \frac{2}{7}\pi$ 不可作。

[G e n e r a l I n f o r m a t i o n]

书名 = 伽罗华理论基础

作者 = 刘长安 王春森

页数 = 1 6 3

S S 号 = 1 0 1 0 1 7 7 1

出版日期 = 1 9 8 9 年 0 9 月 第 1 版

前言
目录

第一章	群论的初步知识
	1 . 1 群的基本概念
	1 . 2 置换群
	1 . 3 同态和同构定理
	1 . 4 正规群列与合成群列
	1 . 5 可解群
	1 . 6 可迁群
第二章	域、扩域
	2 . 1 域的基本概念
	2 . 2 有限扩域、代数扩域
	2 . 3 多项式的分裂域
	2 . 4 有限可分扩域的单纯性
	2 . 5 有限域
第三章	伽罗华理论初步
	3 . 1 正规扩域
	3 . 2 伽罗华群
	3 . 3 方程的伽罗华群
	3 . 4 伽罗华理论的基本定理
第四章	伽罗华理论的应用
	4 . 1 单位根和循环扩域
	4 . 2 方程可用根号解的充要条件
	4 . 3 不能用根号解的方程的例子
	4 . 4 三次方程和它的不可约情形
	4 . 5 尺规作图
	4 . 6 分圆多项式和正 n 边形作图
附：习题答案	