〔德〕E·阿　丁著

伽罗华理论

李同孚译

上海科学技术出版社

伽罗华理论

E. 阿丁 著
李同孚 译

上海科学技术出版社

Galoissche Theorie
E. Artin
B. G. Teubner Verlagesellschaft.

伽罗华理论

E·阿丁 著
李同孚 译
上海科学技术出版社出版
（上海瑞金二路450号）
新华书店上海发行所发行　上海商务印刷厂印刷
开本787×1092 1/32　印张3.125　字数66,000
1979年10月第1版　1984年7月第2次印刷
印数18,001—23,200

书号：13119·803　　定价：0.32元

序

此书的英文版原是我过去在 Notre Dame 大学一个夏季学期里所作讲义的整理. 当时是为了使代数初步知识较少的大学生在较短时间内了解 Galois 理论的方法及问题的提出. A. N. Milgram 先生为此整理工作写了一个涉及这理论应用的附录.

当出版社建议我出德文译本时,提出问题,可否同时写出近世代数抽象基础的导论. 但经仔细考虑后, 我想保持本书的原来计划,还是针对同样的读者. 现在已有足够的教科书,其中详述了代数的基础.

但是,在 Ziegler 先生的译文初稿完成之后, 发现最后两部分需要修改. 第二部分里较大的更变仅如下述: 简化了 Galois 理论基本定理的证明. 述及单位根的那节里, 采用了分圆多项式不可约性的证明,它不用整多项式分解的性质,而是凭借 Landau 的证法. 最后,第三部分完全重写.

改写上得到 Hel Braun 小姐的大力支持. 我感谢 H. Reichardt 先生在校对上的许多有价值的建议和协助.

E. Artin

汉堡, 1959 年 8 月

目　录

I. 线性代数

II. 体　论

III. 应　用

A. N. Milgram

I

线性代数

A. 体

体是一个集，对它的元定义了叫做加法和乘法的两种运算. 这运算同实数系(它本身就是体的一个例子)里的加法和乘法相类似. 在每个体 K 之中总有两个唯一确定了的叫做0和1的元，它们与 K 的另一些元相加或相乘的作用恰如实数系中相应的元所示. 这种类似不足之处有二：1. 并未假设每个体中的乘法都是可交换的；2. 体还可能只由有限多个元所组成.

说得更确切些，体是一个集，它的元对于加法组成 Abel 群，而且不把零算在里面的元组成乘法群，还有这两个群的运算是用分配律来连系着的. 容易看到，零与任意元之积仍为零.

一个体中的乘法如果是可交换的，就把它叫做**交换体**. 如果要特地强调乘法非交换的这种可能性，那就称之为**斜体**.

B. 向量空间

设 V 是以 $A, B, \cdots$ 为元的 Abel 加法群，K 是以 $a, b, \cdots$ 为元的体. 对于 K 的每个元 a 与 V 的每个元 A 还假设定义了积 aA 作为 V 的一元. 如果下列的假设成立，集 V 就叫做 K 上的(左)**向量空间**：

1. $a(A+B)=aA+aB$,

2. $(a+b)A=aA+bA$,

3. $a(bA)=(ab)A$,

4. $1A=A$.

如果V是K上的向量空间，读者就容易证实，$oA=0$与$a0=0$成立，其中o与0分别是K与V中的零元．例如前一个关系式从下列方程推出：

$$aA=(a+o)A=aA+oA.$$

如果把积aA换成适合类似规律而定义的积Aa，V就叫做K上的右向量空间．如果左与右向量空间在讨论中不同时出现，就简称之为"向量空间"．

C. 齐次线性方程

如果在体K中给定$n\cdot m$个元a_{ij}，$i=1, 2, \cdots, m$，$j=1, 2, \cdots, n$．要求下列方程组在K中的解x_i：

$$\begin{aligned} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n&=0,\\ \vdots\qquad\quad &\vdots\qquad\quad\ \vdots\quad\ \vdots\\ a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n&=0. \end{aligned}\tag{1}$$

(1)叫做以$x_1, x_2, \cdots, x_n$为未知元的齐次线性方程组．如果(K中有满足这组方程的)元$x_1, x_2, \cdots, x_n$不都是o，就叫非平凡解，否则叫平凡解．

命题1 线性齐次方程组有非平凡解，如果未知元的个数多于方程的个数．

证明所根据的方法是读者还在中学时就学过的，即用未知元的逐次消去法．如果$n(>0)$个变量的方程一个也没有(即$m=0$)，那么未知元就不受任何限制，可把它们全部取作$=1$．

按完全归纳法来进行证明. 假设未知元的个数多于 k 个而方程只有 k 个的那种方程组当 $k<m$ 时总有非平凡解. 在方程组(1)中设 $n>m$ 而且把表式 $a_{i1}x_1+a_{i2}x_2+\cdots+a_{in}x_n$ 记作 L_i, $i=1, 2, \cdots, m$. 我们来找那些不全为 o 的、使得 $L_1=L_2=\cdots=L_m=o$ 的 $x_1, x_2, \cdots, x_n$. 如果对于每个 i 和 j 都有 $a_{ij}=o$, 那么(在 K 中)任意选取的 $x_1, x_2, \cdots, x_n$ 就总是解. 如果这些 a_{ij} 不全为 o, 因为变更这些方程的次序或未知元的编码并不影响联立解的存在与否, 所以可设 $a_{11}\neq 0$. 要对给定的方程组能求得非平凡解, 必须而且只须对于下列方程组能求得非平凡解:

$$L_1=o$$
$$L_2-a_{21}a_{11}^{-1}L_1=o$$
$$\cdots\cdots\cdots\cdots$$
$$L_m-a_{m1}a_{11}^{-1}L_1=o.$$

这是因为: 如果 $x_1, x_2, \cdots, x_n$ 是刚才列出的方程组的解, 由 $L_1=o$ 就使得其余所有方程中的第二项都消失, 因此有 $L_2=L_3=\cdots=L_m=o$. 反之, 如果(1)成立, 这组新的方程就显然成立. 读者注意到新方程组是由后 $m-1$ 个方程"消去" x_1 而建立的. 把后 $m-1$ 个方程当作 $x_2, \cdots, x_n$ 的方程组来看, 如果它有非平凡解, 那么取 $x_1=-a_{11}^{-1}(a_{12}x_2+a_{13}x_3+\cdots+a_{1n}x_n)$ 就得到整个方程组的解. 然而按归纳假设, 这后 $m-1$ 个方程是有非平凡解的, 由此得到本命题.

注 方程组(1)中所有系数 a_{ij} 是 x_j 左方的因子. 对于其中所有系数是右方因子的方程组, 于是各个项换写成 x_ja_{ij}, 用类似的证明使同样的命题成立. 如果既有左方系数又有右方系数出现, 那么在非交换的情形就作不出这样的命题.

D. 向量的相关性与无关性

体 K 上的向量空间 V 中向量 $A_1, A_2, \cdots, A_n$ 叫做**相关的**，如果 K 中有不全为 o 的元 $x_1, x_2, \cdots, x_n$ 存在，使得 $x_1A_1+x_2A_2+\cdots+x_nA_n=0$ 成立. 否则把向量 $A_1, A_2, \cdots, A_n$ 叫做**无关的**.

体 K 上的向量空间 V 的**维数**了解为 V 中无关向量的最大个数. 确切地说，向量空间的维数是无穷的，如果 V 中有任意多个无关的向量存在；如果 V 中有一组 n 个无关向量存在，而每组超过 n 个的向量总是相关的，V 就是 n 维的.

V 中一组元 $A_1, A_2, \cdots, A_m$ 叫做 V 的**生成系**，如果 V 的每个元 A 总能通过在 K 中适当地选取元 a_i, $i=1, \cdots, m$ 由 $A_1, A_2, \cdots, A_m$ 线性地表示出来，即

$$A=\sum_{i=1}^{m} a_iA_i.$$

命题 2 如果 V 有生成系 $A_1, A_2, \cdots, A_m$，那么这个生成系中无关向量的最大数就是 V 的维数.

证 如果所有的 $A_i=0$, V 就只由零向量组成. 如关系 $1\cdot 0=0$ 所示，零向量是相关的，因此 V 的维数为 o.

否则，设 r 为生成系 $A_1, A_2, \cdots, A_m$ 的无关向量最大数，通过重新编码就能实现 $A_1, A_2, \cdots, A_r$ 是无关的. 因为已设 r 是 A_i 中无关最大数，$r+1$ 个向量 $A_1, A_2, \cdots, A_r, A_i$ 就相关，因此有关系

$$a_1A_1+a_2A_2+\cdots+a_rA_r+b\cdot A_i=o,$$

其中系数不全为 0. 如果 $b=0$, $A_1, A_2, \cdots, A_r$ 就相关了. 因此 $b\neq 0$, 上式可写成

$$A_i=-b^{-1}(a_1A_1+a_2A_2+\cdots+a_rA_r).$$

从此得到，A_1, A_2, …, A_r 也是生成系；因为 V 中任一向量的线性表式中的 A_i 总可代以 A_1, A_2, …, A_r 的线性组合.

设 B_1, B_2, …, B_t 是 V 中某一组向量，$t>r$. 于是有 a_{ij} 使得 $B_j=\sum_{i=1}^{r} a_{ij}A_i$. 要证明这些向量 B_1, B_2, …, B_t 相关，就要证 K 中有不全为 0 的 x_i 存在，使得

$$x_1B_1+x_2B_2+\cdots+x_tB_t=0$$

成立. 在这方程中用 $\sum_{i=1}^{r} a_{ij}A_i$ 代 B_j，就得到 A_i 的一个线性组合，其中 $\sum_{j=1}^{t} x_ja_{ij}$ 为 A_i 的系数. 因此只须求得使方程组 $\sum_{j=1}^{t} x_ja_{ij}=0$, $i=1, 2, \cdots, r$ 成立的非平凡解 x_j. 由于 $t>r$ 和命题 1，这样的 x_j 是存在的.

既然个数比 r 多的向量组都相关，而向量 A_1, A_2, …, A_r 又无关，所以 r 就是 V 的维数.

注 n 维向量空间的任意 n 个无关向量 A_1, A_2, …, A_n 构成生成系. 因为任一向量 A 总与向量 A_1, A_2, …, A_n 相关，从而相关式中 A 的系数不能为零. 由 A 的解就证明了 A_1, A_2, …, A_n 构成生成系.

向量空间 V 的一个子集叫做**子空间**，如果它是这向量空间的子群而且这子集的任一元与体元相乘仍不出此子集. 如果 A_1, A_2, …, A_s 是向量空间 V 的元，所有形如 $a_1A_1+a_2A_2+\cdots+a_sA_s$ 的元就显然构成 V 的子空间. 由维数的定义得知，子空间的维数不超过全向量空间的维数.

设 V 是有限维 n 的向量空间，W 是具有同一维数 n 的 V 的子空间. 于是 $W=V$. 这子空间含有 n 个无关向量，它们其实构成 V 的生成系.

体 K 中 s 个元的序列 $(a_1, a_2, \cdots, a_s)$ 叫做**行向量**. 所

有这些 s 个元的序列由下列定义构成向量空间：

α) $(a_1, a_2, \cdots, a_s)=(b_1, b_2, \cdots, b_s)$当且仅当 $a_i=b_i$, $i=1, 2, \cdots, s$;

β) $(a_1, a_2, \cdots, a_s)+(b_1, b_2, \cdots, b_s)=(a_1+b_1, a_2+b_2, \cdots, a_s+b_s)$;

γ) $b(a_1, a_2, \cdots, a_s)=(ba_1, ba_2, \cdots, ba_s)$对于 K 中的元 b.

把 s 个元的序列写成纵列

$$\begin{pmatrix} a_1 \\ \vdots \\ a_s \end{pmatrix}$$

就叫做列向量.

命题 3 体 K 中所有 n 个元的序列构成的行(列)向量空间 K^n 是 K 上的 n 维向量空间.

证 n 个元(所谓单位向量)

$$\begin{aligned} \varepsilon_1&=(1, o, o, \cdots, o)\\ \varepsilon_2&=(o, 1, o, \cdots, o)\\ &\vdots\\ \varepsilon_n&=(o, o, o, \cdots, 1) \end{aligned}$$

是无关的而且生成 K^n. 此二者都由关系

$$(a_1, a_2, \cdots, a_n)=\sum_{i=1}^{n} a_i\varepsilon_i$$

得以证明.

体 K 中的元作成的长方形阵列

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

叫做**矩阵**. 矩阵的**右行秩**是指由体元右乘矩阵的行 $(a_{i1}, a_{i2}, \cdots, a_{in})$时，各行之间得到的无关行向量的最大数. 相应地定义左行秩，右列秩与左列秩.

命题 4 矩阵的右列秩等于左行秩，而且左列秩等于右行秩. 如果体是可交换的，这四个数就相等，而且叫做矩阵的秩.

证 用 $C_1, C_2, \cdots, C_n$ 来记矩阵的列向量，$R_1, R_2, \cdots, P_m$ 记其行向量. 列向量 0 是

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

因此相关性 $C_1x_1+C_2x_2+\cdots+C_nx_n=0$ 就等价于方程组

$$\begin{aligned} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n&=0, \\ \vdots \qquad\qquad &\quad \vdots \\ a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n&=0 \end{aligned} \tag{1}$$

的解. 矩阵中行的次序变更引出同一方程组，因此并不改变矩阵的列秩. 行秩也不变，因为改变了的矩阵有同样的行向量. 以 s 记矩阵的右列秩，z 记左行秩. 根据上述考虑可以假定矩阵的前 z 个行是无关的行向量. 由矩阵中所有行生成的行向量的向量空间按命题 2 就有维数 z，而且已由前 z 个向量生成. 于是每一行可由前 z 个行线性地表出. 因此(1)中前 z 个方程的任一解就是整个方程组的解；因为每个方程可作成前 z 个方程的线性组合. 反之，(1)的每个解也是前 z 个方程的解. 这就是说，由原来的矩阵中前 z 个行组成的矩阵

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots\cdots & & & \\ a_{z1} & a_{z2} & \cdots & a_{zn} \end{pmatrix}$$

与原矩阵有相同的右列秩. 它们也有相同的左行秩, 因为这 z 个行是选为无关的. 然而由命题 3, 新矩阵的列秩不能超过 z. 因此 $s \leqslant z$. 仿此得到, 如以 s' 记左列秩, z' 记右行秩, 就有 $s' \leqslant z'$. 把原矩阵转置, 即行列互换, 于是转置矩阵的左行秩就等于原矩阵的左列秩. 上述讨论应用于转置矩阵就得到 $z \leqslant s$ 与 $z' \leqslant s'$.

E. 非齐次线性方程

现在来讨论非齐次线性方程组

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2, \\ \vdots \qquad\qquad & \vdots \quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned} \tag{2}$$

的可解性问题. 有两个矩阵 M 与 N 与这组方程对应. M 为系数 a_{ij} 的矩阵; N 由 M 的第 i 行多加元 b_i 所组成. N 的列向量记作 $A_1, A_2, \cdots, A_n, B$. 组(2)能简写为式子:

$$A_1x_1 + A_2x_2 + \cdots + A_nx_n = B.$$

设 K^m 是所有 m 项列向量的右向量空间. K^m 中向量 $A_1, A_2, \cdots, A_n$ 生成 K^m 的一个子空间 T. 方程组的可解性得以简单地说明为 B 属于 T. T 的维数是矩阵 M 的右列秩. 因此方程的可解性就是说, M 与 N 有同样的右列秩. 所有这些只不过是对可解性的另一种说法而已. 引用命题 4 就看到, 方程(2)恰好在 M 和 N 有相同的左行秩时有解, 而且这

种说法在有的情况下可能有用.

如果 $m=n$, 方程个数就等于未知元个数, 这样还要考虑与(2)相连系的**伴随齐次方程组**

$$A_1x_1+A_2x_2+\cdots+A_nx_n=0.$$

下列问题的提法是最常见的:

给定系数 a_{ij} 的方程组(2)对于 K 中任意的 b_i 有解吗? 如果有, 就是说每个列向量 B 属于 T, 因此 T 就是整个空间 K^n. 既然 K^n 具有维数 n, 当这些向量 A_1, A_2, $\cdots$, A_n 无关时, 正好就是如此. 而这就是说, 伴随齐次方程组只有平凡解. 而且每个向量 B 只能用一种方式表成向量 A_1, A_2, $\cdots$, A_n 的线性组合. 于是就证明了

命题 5 如果方程组 (2) 中的 $m=n$, 那么对于方程右方是体中任意元的情形, 方程有解当且仅当伴随齐次方程组只有平凡解. 如果是这种情形, 那么这个解并且是唯一的.

F. 行 列 式

这儿所发挥的行列式论, 在 Galois 理论中并不需要. 因此, 读者可随意去留.

假设体是可交换的, 从而来考虑具有 n 行与 n 列的正方形矩阵

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}. \tag{1}$$

现在来定义这矩阵的某一函数, 它的值是体的元, 把这函数叫做行列式并记作

$$\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots\cdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix} \tag{2}$$

或 $D(A_1, A_2, \cdots, A_n)$，如果把它看成(1)中列向量 $A_1, A_2, \cdots, A_n$ 的函数. 如果除 A_k 外的其它列都固定了，因而把行列式看成 A_k 的函数，就写成 $D_k(A_k)$，或者有时只写成 D.

定义 列向量的函数叫做行列式，如果它适合三条公理：

1. 作为任一列 A_k 的函数来看，它是线性的而且是齐次的，即

$$D_k(A_k+A_k')=D_k(A_k)+D_k(A_k'), \tag{3}$$

$$D_k(cA_k)=c\cdot D_k(A_k). \tag{4}$$

2. 它的值$=0$，当两个相邻的列 A_k 与 A_{k+1} 相等时.

3. 它的值$=1$，如果每个 A_k 是单位向量 U_k，

$$U_1=\begin{pmatrix}1\\0\\0\\\vdots\\0\end{pmatrix},\quad U_2=\begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix},\quad \cdots,\quad U_n=\begin{pmatrix}0\\0\\0\\\vdots\\1\end{pmatrix}. \tag{5}$$

一般来说，行列式是否存在这个问题暂先把它挂起来. 然而由公理得到一些推论：

a) 在(4)中取 $c=0$ 得到：行列式为 0，如果它有一个列为 0.

b) $D_k(A_k)=D_k(A_k+cA_{k\pm1})$，或者：行列式不变，如果把一个列的倍数加到与它相邻的列. 其实，根据公理 2 和方程(3)与(4)就得到

$$D_k(A_k+cA_{k\pm1})=D_k(A_k)+cD_k(A_{k\pm1})=D_k(A_k).$$

c) 考虑 A_k 与 A_{k+1} 这两列. 这是能用 A_k 与 $A_{k+1}+A_k$ 来代替的. 从前列减去后列就有新列 $-A_{k+1}$ 与 $A_{k+1}+A_k$. 把前列加到次列就得到 $-A_{k+1}$ 与 A_k. 最后把 -1 括出来. 由此得出结论: 行列式变号, 如果将两相邻列互换.

d) 行列式等于零, 如果其某两列相等. 其实, 在累次互换了充分的相邻列之后, 任意两列可取成相邻的. 至此就只需应用公理 2 了.

与 b) 及 c) 中相同的方法能证明下列较一般的规则:

e) 把一列的倍数加到另一列上, 行列式之值不变.

f) 任意两列互换只变行列式的符号.

g) 设 $(\nu_1, \nu_2, \cdots, \nu_n)$ 为下标 $(1, 2, \cdots, n)$ 的一置换. 把 $D(A_{\nu_1}, A_{\nu_2}, \cdots, A_{\nu_n})$ 中之列重排直到恢复原来的次序就得到

$$D(A_{\nu_1}, A_{\nu_2}, \cdots, A_{\nu_n}) = \pm D(A_1, A_2, \cdots, A_n).$$

其中 $\pm$ 为适当确定了的符号, 它与 A_k 的特殊值是毫无关系的. 代 A_k 以 U_k 就变成 $D(U_{\nu_1}, U_{\nu_2}, \cdots, U_{\nu_n}) = \pm 1$, 从而这个符号就只与单位向量的置换有关[1].

现在把每个向量 A_k 代以 $A_1, A_2, \cdots, A_n$ 的线性组合 A'_k 如下:

$$A'_k = b_{1k}A_1 + b_{2k}A_2 + \cdots + b_{nk}A_n. \tag{6}$$

在计算 $D(A'_1, A'_2, \cdots, A'_n)$ 时先把公理 1 应用于 A'_1, 于是把这行列式分解成一个和; 然后对每一项的 A'_2 应用同样的方法, 等等, 如此进行. 结果得到

$$\begin{aligned} &D(A'_1, A'_2, \cdots, A'_n) \\ &= \sum_{\nu_1, \nu_2, \cdots, \nu_n} D(b_{\nu_1 1}A_{\nu_1}, b_{\nu_2 2}A_{\nu_2}, \cdots, b_{\nu_n n}A_{\nu_n}) \\ &= \sum_{\nu_1, \nu_2, \cdots \nu_n,} b_{\nu_1 1}b_{\nu_2 2}, \cdots, b_{\nu_n n}D(A_{\nu_1}, A_{\nu_2}, \cdots, A_{\nu_n}), \end{aligned} \tag{7}$$

1) 按照它的推导, $\pm$ 号也与所选择的行列式无关.