必须证明如果(t, x)是 X 的点，则(t, u)是 Y 的点. 因为在 K 里 $g(t, \gamma)=0$，且 u 是 $F[x]$里代表 γ 的元素，故 $g(t, u)$属于理想(f). 存在 $F[x]$的元素 h 使得

$$g(t,u) = fh$$

如果(t, x)是 X 的点，则 $f(t, x)=0$，从而 $g(t, u)=0$. 所以，(t, u)的确是 Y 里的点. 然而，因为 u 与 h 是 $F[x]$的元素，所以它们的系数是 t 的可能有分母的有理函数. 于是，η 在一个有限点集上可能没有定义.

η 的逆函数通过互换 K 和 L 的作用得到. ■

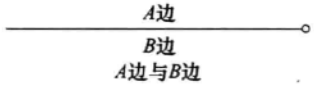
剪切和粘贴

“剪切和粘贴”是构造或拆分分支覆盖的过程.

我们回到多项式 x^2-t 的黎曼曲面 X 的例子，且同以前一样写 $x=x_0+x_1\mathrm{i}$. 如果沿着图 11.9.15 的重合轨迹(即负实 t 轴)剪切开 X，则它分解为两部分 $x_0>0$ 与 $x_0<0$. 倘若我们忽略切口上发生了什么，这两部分的每一个都以双射的方式投射到 T 上.

把这个过程反转过来，我们可以下列方式构造一个与 X 同构的分支覆盖：将 T 上两个复平面的副本 S_1，S_2 堆叠起来并将它们沿负实轴剪切开. T 的这些副本称为叶. 然后，把
465 S_1 上切口的 A 边与 S_2 上切口的 B 边粘起来，反之亦然.（这在 3 维空间不能完成.）

【15.9.6】图



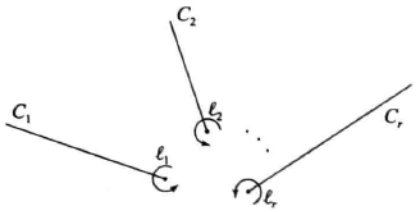
假设给定 n-叶分支覆盖 $X\to T$，且设 $\Delta=\{p_1, \cdots, p_k\}$是 T 中它的分支的点集. 对 $v=1, \cdots, k$，我们选取互不相交的从 p_v 到无穷远的半直线 C_v. 沿着这些半直线剪切开 T，在所有这些位于半直线上的点处也剪切开 X.

我们应该明确剪切指的是什么. 剪切开 T 意味着移去了半直线 C_v 上的所有点，包括点 p_v；剪切开 X 意味着移去了位于这些半直线上的所有点.

【15.9.7】引理 *当在半直线 C_v 之上剪切开 X 时，它分解成 n 个“叶”$S_1, \cdots, S_n$ 的并，这些叶可任意地标号排序. 每个叶以双射的方式投影到剪切面 T 上.*

这是真的，因为剪切曲面 X 是剪切面 T 的非分支覆盖空间，这是一个单连通集：剪切面上的任一个圈可连续收缩成一个点. 直观上是有道理的：单连通空间的每个非分支覆盖完全分解. 含有 X 的点 p 的叶由所有通过不跨越剪切口的路连接到 p 的点组成.（这是[Munkres]里的练习，p. 342.）

【15.9.8】图



剪切面 T

现在重新构造曲面 X，取剪切面 T 的 n 个副本，我们称其为“叶”，且将其标记为 S_1，…，S_n. 将它们放在 T 上堆叠起来. 除剪切口外，这些叶的并是分支覆盖. 我们必须描述沿着剪切口把这些叶粘回在一起的规则. 在 T 上，我们围绕分支点 p_v 以反时针方向转一个圈 ℓ_v，对于 C_v 的边，在我们跨过 C_v 前称为“边 A”，在跨过 C_v 后称为“边 B”. 我们把叶 S_i 的对应边分别标记为边 A_i 与边 B_i. 这样，粘贴 X 的规则等于边 A_i 与边 B_j(对某个 j)粘贴起来的规则. 这个规则由映 $i \rightsquigarrow j$ 的指标 $\mathbf{1}$，…，$\boldsymbol{n}$ 的置换 σ 所描述. 466

看起来显然可以用置换 σ_v 的任意集合来构造覆盖，但在分支点附近发生了什么似乎不清楚. 为避免模糊不清，我们去掉所有分支点和所有在它们上面的点.

- 分支数据：对 $v=1$，…，r，指标 $\mathbf{1}$，…，$\boldsymbol{n}$ 的置换 σ_v.
- 粘贴规则：如果 $\sigma_v(i)=j$，则沿着剪切口 C_v 把边 A_i 与边 B_j 粘贴在一起.

当粘贴完成而没有剪切口剩下时，叶的并就是我们的覆盖. 就像图 11.9.15 所描绘的黎曼曲面一样，粘贴而不跨越剪切口需要四维空间.

如果 σ_v 是平凡置换，则每个叶在 C_v 上与自己粘贴在一起. 这样，这个剪切口就不需要了，我们说 p_v 不是真的剪切点.

下一个推论重述了上面的讨论.

【15.9.9】引理 每个 n-叶分支覆盖 $X \to T$ 同构于通过剪切和粘贴过程得到的覆盖.

注意 叶的标号是任意的，且“顶叶”的概念对黎曼曲面没有本质意义. 如果存在顶叶，则可以通过选择在该叶的值而定义 x 为一个单值函数. 只有在黎曼曲面被剪切开时才能这样做. 在曲面 X 上漫步将使我们从一叶走到另一叶.

除了叶的任意标号外，置换 σ_v 是由分支覆盖 C_v 唯一确定的. 由置换 ρ 所确定的标号的变换把某个 σ_v 变为共轭 $\rho^{-1}\sigma_v\rho$.

【15.9.10】引理 令 X 与 Y 是用同一点 p_v 与半直线 C_v 通过剪切和粘贴构造的分支覆盖. 设定义它们粘贴数据的置换分别是 σ_v 与 τ_v，则 X 与 Y 是同构的分支覆盖当且仅当存在置换 ρ 使得对每个 v 有 $\tau_v=\rho^{-1}\sigma_v\rho$.

【15.9.11】引理 通过剪切和粘贴构造的分支覆盖 X 是路连通的当且仅当置换 σ_1，…，σ_r 生成对称群的子群 H，且它可迁地作用在指标 $\mathbf{1}$，…，$\boldsymbol{n}$ 上.

证明 每个叶是路连通的. 如果置换 σ_v 映指标 $\boldsymbol{i}$ 到 $\boldsymbol{j}$，则叶 S_i 与 S_j 沿着剪切口 C_v 粘在一起. 这样，将有一条从 S_i 的点到 S_j 的点的跨越剪切口的短路，且因为叶本身是路连通的，故 $S_i \cup S_j$ 的所有点可用路连接. 所以，X 是路连通的当且仅当对每对指标 $\boldsymbol{i}$，$\boldsymbol{j}$，存在一系列置换 σ_v 使得 $i=i_0 \rightsquigarrow i_1 \rightsquigarrow \cdots \rightsquigarrow i_d=j$. 这是真的当且仅当 H 可迁地作用. ■ 467

【15.9.12】例 T 的最简单的 k-叶路连通分支覆盖是在单个点分支的. 令 Y 是这样的覆盖，仅在原点 $t=0$ 处分支. Y 的分支数据由单个置换 σ 组成，这个置换对应于绕原点的圈. 先前的引理告诉我们，因为 Y 是路连通的，所以 σ 一定可迁地作用在 k 指标上，且可迁作用的仅有置换是 k 阶循环置换. 所以，对叶适当地标号，得 $\sigma=(\mathbf{1}\ \mathbf{2}\ \cdots\ \boldsymbol{k})$. 在同构意义下，恰存在一个在原点分支的 k-叶分支覆盖. 黎曼存在定理告诉我们，在同构意义下，恰存在

一个带有这个黎曼曲面的域扩张. 不难猜测这个域扩张：它是由多项式 y^k-t 所定义的域，亦即$K=F(y)$，其中 $y=\sqrt[k]{t}$. 黎曼曲面 Y 有 k 个叶. 它仅在原点分支，因为每个不同于零的 t 有 k 个 k 次复根.

这里还有两点要说明. 首先，定理断言这是仅有的在单个点 $t=0$ 处分支的 k 次扩域. 这不是显然的. 其次，相同的域扩张 $K=F(y)$可由许多元素生成. 对绝大多数生成元的选取而言，仅存在一个真分支点将不是显然的. ■

计算置换

给定多项式 $f(t, x)$，希望确定定义它的黎曼曲面的粘贴数据的置换 σ_v. 出现两个问题. 首先，“局部问题”：在每个分支点 p 处，必须确定当圈这个点时出现的叶的置换 σ. 就像我们已经看到的，σ 依赖于叶的标号. 其次，必须谨慎地使用每个分支点的同一标号. 这是更困难的问题. 计算机处理它没有问题，但除了很简单的情形外，手工处理是困难的.

要计算置换，计算机选取剪切面 T 里的“基点”b，且以适当的精度数值地计算多项式 $f(b, x)$的 n 个根. 对这些根任意地标号，比如说，γ_1，…，γ_n，且把叶标号，称含有根 γ_i 的叶为 S_i. 这样，它到达分支点 p_v 附近的点 b_v，小心不要跨过任一剪切口. 诸根 γ_i 连续变化，计算机可通过每次取一小步重算根来跟随这个变化. 这给出了在点 b_v 如何给叶进行标号. 这样，要确定置换 σ_v，计算机跟随反时针方向绕 p_v 的圈 ℓ_v，随着往下进行，它重新计算根. 因为圈跨越剪切口 C_v，故当路回到点 b_v 时诸根将由 σ_v 进行置换. 以这种方式，计算机确定了 σ_v. 因为标号在基点 b 已经建立，所以对所有分支点来说标号都是相同的.

不用说，手工处理是非常令人厌烦的. 在下面给出的例子里我们寻找方法绕开这个问题.

局部问题可通过分析方法解决，在这里我们给出不完备的分析. 方法是将黎曼曲面与
468 熟悉的曲面(即多项式 y^k-t 的黎曼曲面 Y)联系起来. 令 t_0 是黎曼曲面 $X:\{f(t, x)=0\}$的分支点，其中 f 是形如(15.9.1)的多项式. 替换 $t=t_0$，我们得到单变量多项式$f^0(x)=f(t_0, x)$.

【15.9.13】引理 *令 x_0 是 $f^0(x)$的根. 假设*

- *x_0 是 $f^0(x)$的 k-重根，且*
- *偏导数$\dfrac{\partial f}{\partial t}$在点$(t_0, x_0)$处不为零.*

则叶的置换在点 t_0 处含有 k-循环.

证明 我们做变量替换，将点(t_0, x_0)移到原点$(0, 0)$，所以 $f^0(x)=f(0, x)$，且写 $f(t, x)=f^0(x)-tv(t, x)$. 这样，$\dfrac{\partial f}{\partial t}(0, 0)=-v(0, 0)$. 由假设可得 $v(0, 0)\neq 0$. 而且，因为 $x=0$ 是 $f^0(x)$的 k-重根，故多项式有形式 $x^k u(x)$，其中 $u(x)$是 x 的多项式且 $u(0)\neq 0$. 这样，$f(t, x)=x^k u(x)-tv(t, x)$. 设 $c=u(0)/v(0, 0)$. 用 $c^{-1}t$ 替换 t. 现在的结果是 $u(0)/v(0, 0)=1$.

我们把注意力限制在(t, x)-空间中原点$(0, 0)$的小邻域U上，且写方程$f=0$为

$$x^k u/v = t$$

对U里的(t, x)，u/v接近于1. 在u/v的k次根中，有一个接近1，且称这个根为w，它连续依赖于U里的点(t, x). 其他k次根是$\zeta^v w$，其中$\zeta=e^{2\pi i/k}$.

令$y=xw$. 这样，在我们的邻域U里，方程$f(t, x)=0$等价于$y^k=t$. 所以，存在黎曼曲面X的k个叶交于U，且当绕点$t=0$做个圈时，与黎曼曲面Y的诸叶一样，我们将循环地置换这k个叶. ■

现在，对于一些简单多项式描述分支数据. 我们取x的首一多项式. 分支点是在$f(t_0, x)$有重根的点t_0——$f(t_0, x)$与$\dfrac{\partial f}{\partial x}(t_0, x)$有公共根的点. 命题15.9.13将是我们的主要工具.

【15.9.14】例

(a) $f(t, x)=x^2-t^3+t$，$\dfrac{\partial f}{\partial x}=2x$，$\dfrac{\partial f}{\partial t}=-3t^2+1$.

这里X是T的2-叶覆盖. 有3个分支点$t=0$，$t=1$与$t=-1$，且在所有这些点处$\dfrac{\partial f}{\partial t}\neq 0$. 所以，叶的置换在所有这些点处含有2-循环. 因为有两个叶，故每个置换是对换**(1 2)**. 当有两个叶时我们可随意标号.

(b) 我们寻找T在两个点p_1与p_2处分支的路连通的3-叶分支覆盖X，并使得置换σ_i在点p_i处是对换.

我们可对叶标号使得$\sigma_1=$**(1 2)**. 这样，因为X是路连通的，所以置换σ_2一定或是**(2 3)**或是**(1 3)**(15.9.11). 互换称为S_1与S_2的叶不影响σ_1，但它互换两个其他的对换， 469
所以，在叶的适当标号下，$\sigma_1=$**(1 2)**，$\sigma_2=$**(2 3)**. 恰有一个这样覆盖的同构类.

黎曼存在定理告诉我们，在同构意义下，存在F的唯一域扩张K具有这个覆盖作为它的黎曼曲面. 当然，K依赖于两个分支点的位置，但通过变量t的线性变换它们可移到任意位置.

我们如何求得多项式$f(t, x)$使其黎曼曲面具有这个形式？没有一般的方法，所以，必须猜测，这个情形很简单以致很容易猜到. 因为有极小分支，所以我们寻找很简单的多项式即x的三次多项式. 开始寻找需要些勇气，但第一个尝试也许是形如x^3+x+t的多项式. 这将会成功，但我们取$f(t, x)=x^3-3x+t$. 这样，$\dfrac{\partial f}{\partial x}=3x^2-3$与$\dfrac{\partial f}{\partial t}=1$. 将$\dfrac{\partial f}{\partial x}$的根$x=\pm 1$代入$f$中，会发现分支点是点$t=\pm 2$. 因为$\dfrac{\partial f}{\partial t}$处处不为零，所以可以应用命题15.9.13.

在点$p_1=(2, -1)$处存在二重根. 于是，σ_1含有2-循环，它是一个对换. 类似地，σ_2是一个对换. 所以，除了两个分支点的位置外，多项式$f=x^3-3x+t$的黎曼曲面有所要的

性质，且 $F[x]/(f)$定义了具有那样分支的域扩张.

(c) $f(t,\ x)=x^3-t^3+t^2$，$\dfrac{\partial f}{\partial x}=3x^2$，$\dfrac{\partial f}{\partial t}=-3t^2+t$.

这里 X 是 T 的 3-叶覆盖. 分支点在 $t=0$ 与 $t=1$ 处，且 $f(0,\ x)$与 $f(1,\ x)$都有 3 重根. 令 σ_0 与 σ_1 表示叶在分支点的置换. 偏导数$\dfrac{\partial f}{\partial t}$在 $t=1$ 处不为零，于是，3 个叶在那里被循环地置换. 在适当的标号下，σ_1 将是**(1 2 3)**.

点 $t=0$ 出现问题. 首先，$\dfrac{\partial f}{\partial t}$在那里消失了. 第二，我们如何确信在两个点处使用叶的同一个标号？在前面的例子里，知道黎曼曲面必是路连通的就足够确定分支. 这个事实在此处没有给出任何信息，因为 σ_1 通过自身可迁地作用在诸叶上.

我们用一个仅在最简单情形里使用的技巧，就是计算我们绕大圆 Γ 行走所得的置换. 大的回路将跨越每个剪切口一次(见图 15.9.8)，所以，根据我们开始的假设，这些叶由积置换 $\sigma_0\sigma_1$ 或 $\sigma_1\sigma_0$ 进行置换. 如果能确定这个置换，则因为知道 σ_1，故我们将能够恢复 σ_0.

替换 $t=u^{-1}$双射地映 T 到复 u-平面 U，除了在点 $t=0$ 与 $u=0$ 处无定义外. 因为当 $t\to\infty$时$u\to 0$，故 U 的点 $u=0$ 称为 T 的*在无穷远的点*. 在 T 里大的圆 Γ 对应到小的圆，称之为 U 里围绕原点的 L. 然而，绕 Γ 反时针方向行走对应于绕 L 的顺时针方向的行走：如果 $t=re^{i\theta}$，则 $u=r^{-1}e^{-i\theta}$.

我们将替换 $t=u^{-1}$代入多项式 $f=x^3-t^3+t^2$ 并去分母，得 x^3u^3-1+u. 当分析这个替换时，通常也必须替换 x. 似乎显然应置 $y=ux$. 这给出

470
$$y^3-1+u$$

称这个多项式为 $g(u,\ y)$. 黎曼曲面 X 与 $Y:\{g=0\}$通过替换$(x,\ t)\leftrightarrow(y,\ u)$对应，这个对应除了在平面 T 与 U 里原点附近外均有定义且是可逆的. 所以，通过绕 Γ 按反时针方向行走所定义的 X 的诸叶的置换与通过绕 L 的顺时针方向行走所定义的 Y 的诸叶的置换是相同的. 这个置换是平凡的，因为黎曼曲面 Y 在 $u=0$ 处是不分支的. 所以，$\sigma_0\sigma_1=1$，且因为$\sigma_1=$**(1 2 3)**，故 $\sigma_0=$**(3 2 1)**. ∎

第十节　代数基本定理

一个域 F 是*代数封闭的*，如果每个系数属于 F 的正次数多项式在 F 上有根. 代数基本定理断言复数域是代数闭域.

【15.10.1】定理(代数基本定理)　每个复系数的非常数多项式有一个复根.

这个定理有许多种证明方法，其中有一个证明特别引人注目，在此提供证明的梗概. 我们必须证明一个复系数的非常数多项式

【15.10.2】
$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

有一个复根. 如果 $a_0=0$，则 0 是一个根. 故假设 $a_0\neq 0$.

规则 $y=f(x)$定义了从 x-复平面到 y-复平面的一个函数. 令 C_r 表示 x-复平面上圆心在原点且半径为 r 的圆，写成参数的形式为 $x=re^{i\theta}$，其中 $0\leqslant\theta<2\pi$. 我们研究 C_r 的像 $f(C_r)$.

先做些准备工作，我们考虑由多项式 $y=x^n=r^ne^{in\theta}$ 定义的函数. 当 θ 取遍从 0 到 2π 的所有值，点 x 取遍半径为 r 的圆上的每个点一次. 同时，$n\theta$ 从 0 到 $2n\pi$. 点 y 绕半径为 r^n 的圆周 n 次.

令 f 是多项式(15.10.2). 对于充分大的 r，x^n 是 $f(x)$的起主要作用的项. 为了准确起见，令 M 是 f 的系数 a_i 的绝对值的最大值. 则如果 $|x|=r\geqslant 10nM$，

$$|f(x)-x^n| = |a_{n-1}x^{n-1}+\cdots+a_1x+a_0| \leqslant nM|x|^{n-1} \leqslant \frac{1}{10}r^n$$

从这个不等式可知，当 θ 取遍从 0 到 2π 的每个值且 x^n 绕半径为 r^n 的圆转 n 圈时，$f(x)$也绕着原点转 n 圈. 直观理解这个结论的一个好办法就是用狗拴在链上的模型. 如果一个人沿着一个大圆路径遛狗 n 圈，则狗也转 n 圈，也许可能是反方向. 假设狗链长度比路的半径小，这也是成立的. 这里 x^n 表示人在 θ 时刻的位置，而 $f(x)$代表狗的位置. 路的半径是 r^n，狗链的长度是$\frac{1}{10}r^n$.

我们改变半径 r. 由于 f 是连续函数，故像 $f(C_r)$会随着 r 连续变化. 当 r 很小时，$f(C_r)$在 f 的常数项 a_0 附近形成一个小圈. 这个小圈不包围原点. 但是正如我们看到的， 471
如果 r 足够大，则 $f(C_r)$绕原点转 n 圈. 对此的唯一的解释是对于某个较小的半径 r'，$f(C_{r'})$通过原点. 这意味着对于圆 $C_{r'}$上的一个点 α，有 $f(\alpha)=0$. 则 α 是 f 的一个根.

我不认为证是代数，
但证并不是现代数学家不能做.

——Garrett Birkhoff

练　习

第一节　域的例子

1.1　令 R 是包含一个域 F 作为子环的一个整环，且作为 F 上向量空间是有限维的，证明 R 是一个域.

1.2　令 F 是一个域，其特征不是 2，令 $x^2+bx+c=0$ 是系数在 F 上的二次方程. 证明如果 δ 是 F 中的元素且满足 $\delta^2=b^2-4c$，则 $x=(-b+\delta)/2a$ 是二次方程在 F 上的解. 并证明如果判别式 b^2-4c 不是 F 上某个元素的平方，则多项式在 F 上没有根.

1.3　$\mathbf{C}$ 的哪个子域是 $\mathbf{C}$ 的稠密子集？

第二节　代数元与超越元

2.1　令 α 是多项式 x^3-3x+4 的一个复根. 求 $\alpha^2+\alpha+1$ 的形如 $a+b\alpha+c\alpha^2$ 的逆，其中 a，b，$c\in\mathbf{Q}$.

2.2　令 $f(x)=x^n-a_{n-1}x^{n-1}+\cdots\pm a_0$ 是 F 上的既约多项式，并令 α 是 f 在扩域 K 上的根. 用 α 和多项式的系数 a_i 把 α^{-1} 明确地表示出来.

2.3　令 $\beta=\omega\sqrt[3]{2}$，其中 $\omega=e^{\frac{2\pi i}{3}}$，且令 $K=\mathbf{Q}(\beta)$. 证明方程 $x_1^2+\cdots+x_k^2=-1$ 在 K 上没有解.

第三节 扩域的次数

3.1 令 F 是一个域，令 α 是 F 的 5 次扩域的一个生成元. 证明 α^2 也是同一个 5 次扩域的生成元.

3.2 证明多项式 x^4+3x+3 是域 $\mathbf{Q}[\sqrt[3]{2}]$ 上的既约多项式.

3.3 令 $\zeta_n=e^{2\pi i/n}$. 证明 $\zeta_5\notin\mathbf{Q}(\zeta_7)$.

3.4 令 $\zeta_n=e^{2\pi i/n}$. 确定下列元素在 $\mathbf{Q}$ 上和 $\mathbf{Q}(\zeta_3)$ 上的既约多项式：

(a)ζ_4 (b)ζ_6 (c)ζ_8 (d)ζ_9 (e)ζ_{10} (f)ζ_{12}

472 3.5 确定 n 的值使得 ζ_n 在 $\mathbf{Q}$ 上的次数至多为 3.

3.6 令 a 是一个正有理数但不是 $\mathbf{Q}$ 上的平方数. 证明 $\sqrt[4]{a}$ 在 $\mathbf{Q}$ 上的次数为 4.

3.7 (a) i 属于域 $\mathbf{Q}(\sqrt[4]{-2})$ 吗？(b) $\sqrt[3]{5}$ 属于 $\mathbf{Q}(\sqrt[3]{2})$ 吗？

3.8 令 α 和 β 是复数. 证明如果 $\alpha+\beta$ 和 $\alpha\beta$ 是代数数，则 α 和 β 也是代数数.

3.9 令 α 和 β 是 $\mathbf{Q}[x]$ 上既约多项式 $f(x)$ 和 $g(x)$ 的复根. 令 $K=\mathbf{Q}(\alpha)$ 和 $L=\mathbf{Q}(\beta)$. 证明 $f(x)$ 在 $L[x]$ 上是既约的当且仅当 $g(x)$ 在 $K[x]$ 上是既约的.

3.10 一个扩域 K/F 是代数扩域如果 K 中每个元素都是 F 上的代数元. 令 K/F 和 L/K 是代数扩域. 证明 L/F 也是代数扩域.

第四节 求既约多项式

4.1 令 $K=\mathbf{Q}(\alpha)$，其中 α 是 x^3-x-1 的根. 确定 $\gamma=1+\alpha^2$ 在 $\mathbf{Q}$ 上的既约多项式.

4.2 确定 $\alpha=\sqrt{3}+\sqrt{5}$ 在下列域上的既约多项式：

(a)$\mathbf{Q}$ (b)$\mathbf{Q}(\sqrt{5})$ (c)$\mathbf{Q}(\sqrt{10})$ (d)$\mathbf{Q}(\sqrt{15})$

4.3 参考例 15.4.4(b)，确定 $\gamma=\alpha_1+\alpha_2$ 在域 $\mathbf{Q}$ 上的既约多项式.

第五节 尺规作图

5.1 用实数的平方根表示 $\cos 15°$.

5.2 证明正五边形可由尺规作图：(a)利用域的理论 (b)通过找出明确的构造.

5.3 确定正 9 边形是否可以用尺规作图.

5.4 能否用尺规作出一个正方形，使它的面积正好是给定的三角形的面积？

5.5 参考命题 15.5.5 的证明，假设判别式 D 是负数. 确定几何证明的最后一步出现的直线.

5.6 把平面想象为复平面，刻画作为复数的可构造点的集合.

第六节 添加根

6.1 令 F 是一个特征为零的域，令 f' 表示多项式 $f\in F[x]$ 的导数，并设 g 是一个既约多项式且为 f 和 f' 的一个公因子. 证明 g^2 整除 f.

6.2 (a) 令 F 是一个特征为零的域. 确定所有形如 $F(\sqrt{a})$ 的二次扩域所包含的 F 的元素的平方根.

473 (b) 对 $\mathbf{Q}$ 的二次扩域分类.

6.3 确定一个二次数域 $\mathbf{Q}[\sqrt{d}]$，使得对某个整数 n，它包含一个本原 n 次单位根.

第七节 有限域

7.1 确定群 $\mathbf{F}_4^+$.

7.2 确定在 15.7.8 中列出的 $\mathbf{F}_8$ 的每个元素的既约多项式.

7.3 求域 $\mathbf{F}_{13}$ 中 2 的 13 次方根.

7.4 确定在 $\mathbf{F}_3$ 和 $\mathbf{F}_5$ 上 3 次既约多项式的个数.

7.5 在域 $\mathbf{F}_3$ 上分解多项式 x^9-x 和 $x^{27}-x$.

7.6 在域 $\mathbf{F}_4$ 和 $\mathbf{F}_8$ 上分解多项式 $x^{16}-x$.

7.7 设 K 是一个有限域. 证明 K 的非零元素的积为 -1.

7.8 多项式 $f(x)=x^3+x+1$ 和 $g(x)=x^3+x^2+1$ 在 $\mathbf{F}_2$ 上都是既约多项式. 令 K 是通过添加 f 的根得到的扩域，令 L 是通过添加 g 的根得到的扩域. 具体刻画由 K 到 L 的同构，并确定这样的同构的个数.

7.9 不借助定理 15.7.3 解决下列问题. 令 $F=\mathbf{F}_p$.

(a) 确定 $F[x]$上次数为 2 的首一的既约多项式的个数.

(b)令 $f(x)$是 $F[x]$上次数为 2 的首一的既约多项式. 证明 $K=F[x]/(f)$是一个阶为 p^2 的域，且它的元素具有形式 $a+b\alpha$，其中 a，$b\in F$，α 是 f 在 K 上的一个根. 而且，每个形如这样的元素(当 $b\neq 0$ 时)是 $F[x]$上一个二次既约多项式的根.

(c) 证明 $F[x]$上每个二次多项式在 K 上有一个根.

(d) 证明对于给定素数 p，上述构造出来的所有域 K 是同构的.

7.10 令 F 是一个有限域，令 $f(x)$是一个非常数的多项式，它的导数为零多项式. 证明 $f(x)$在 F 上不是既约的.

7.11 令 $f(x)=ax^2+bx+c$，其中 a，b，c 属于环 R. 证明由 f 和 f'生成的多项式环 $R[x]$的理想包含判别式，即常数多项式 b^2-4ac.

7.12 令 p 是一个素整数，令 $q=p^r$ 和 $q'=p^k$. 对怎样的 r 和 k 的值，在 $\mathbf{Z}[x]$上 $x^{q'}-x$ 整除 x^q-x?

7.13 证明任何域 F 的乘法群的一个有限子群是循环群.

7.14 求把域 $\mathbf{F}_p$ 上 n 次既约多项式的个数用欧拉函数 ϕ 表示的公式.

第八节 本原元

8.1 证明一个有限域的每个有限扩域都有本原元.

8.2 确定 $\mathbf{Q}$ 的扩域 $K=\mathbf{Q}(\sqrt{2},\sqrt{3})$的所有本原元. 474

第九节 函数域

9.1 令 $f(x)$是系数属于域 F 的一个多项式. 证明如果存在一个有理函数 $r(x)$使得 $r^2=f$，则 $r(x)$是多项式.

9.2 确定下列多项式的黎曼曲面的分支点和粘贴数据：

(a) x^2-t^2+1 (b) x^4-t-1 (c) $x^3-3tx-4t$ (d) x^3-3x^2-t

(e) $x^3-t(t-1)$ (f) x^3-3tx^2+t (g) x^4+4x+t (h) $x^3-3tx-t-t^2$

9.3 (a) 确定域 $F=\mathbf{C}(t)$上只在点 1 和 -1 分叉的次数为 3 的函数域 K 的同构类的个数.

(b) 刻画对应于每一个作为置换对的域的同构类的黎曼曲面的粘贴数据.

(c) 对于每一个同构类，求多项式 $f(t,x)$使得 $K=F[t]/(f)$代表这个同构类.

*9.4 证明对于二次扩域的黎曼存在定理.

提示：证明对于同构，F 的二次扩域由它的真的分支点的有限集合$\{p_1,\cdots,p_k\}$刻画.

*9.5 写出一个计算机程序确定分支点 p_v 和给定的多项式的黎曼曲面的置换 σ_v.

第十节 代数基本定理

10.1 证明 $\mathbf{C}$ 的由所有代数数构成的子集是代数闭域.

10.2 构造一个包含素域 $\mathbf{F}_p$ 的代数闭域.

*10.3 用这一节最后的记号，对不同半径下像 $f(C_r)$ 的比较证明另一个有趣的几何性质：对于充分大的半径 r，曲线 $f(C_r)$ 围绕原点转 n 圈. 它的总曲率为 $2\pi n$. 假设系数 $a_1 \neq 0$，则线性项 $a_1 z + a_0$ 对于充分小的 z 起主要作用. 则对于小的 r，$f(C_r)$ 围绕 a_0 只转一圈. 它的总曲率仅为 2π. 当 r 变化时，圈会变化. 解释原因.

*10.4 写出一个计算机程序描述 $f(C_r)$ 随着半径 r 变化而变化.

杂题

M.1 令 $K = F(\alpha)$ 是由超越元 α 生成的扩域，令 $\beta \in K$ 但 $\beta \notin F$. 证明 α 在域 $F(\beta)$ 上是代数元.

M.2 在 $\mathbf{F}_7[x]$ 上分解 $x^7 + x + 1$.

*M.3 令 $f(x)$ 是域 F 上的 6 次既约多项式，令 K 是 F 的二次扩域. 关于 $f(x)$ 在 $K[x]$ 上的既约因子的次数有何结论？

475

M.4 (a) 令 p 是奇素数. 证明 $\mathbf{F}_p^\times$ 中恰有一半元素是平方数，且如果 α 和 β 不是平方数，则 $\alpha\beta$ 是平方数.

(b) 证明对于奇数阶的有限域有同样的断言.

(c) 证明对于偶数阶的有限域，其每个元素都是平方数.

(d) 证明 $\mathbf{Q}$ 上关于 $\gamma = \sqrt{2} + \sqrt{3}$ 的既约多项式模任何素数 p 都是可约的.

*M.5 证明有限阶的一般线性群 $GL_2(\mathbf{Z})$ 的任何元素的阶为 1，2，3，4 或 6

(a) 用域的理论.

(b) 应用晶体局限定理.

*M.6 (a) 证明能够生成所有有理函数域 $\mathbf{C}(t)$ 的有理函数 $f(t)$ 定义一个双射 $T' \to T'$.

(b) 证明一个有理函数 $f(x)$ 生成有理函数域 $\mathbf{C}(x)$ 当且仅当 $f(x)$ 具有形式 $(ax+b)/(cx+d)$，其中 $ad - bc \neq 0$.

(c) 确定在 $\mathbf{C}$ 上恒等的 $\mathbf{C}(x)$ 的自同构群.

476 *M.7 证明同态 $SL_2(\mathbf{Z}) \to SL_2(\mathbf{F}_p)$ 通过将矩阵的元素模 p 化简是一个满射.

第十六章　伽罗瓦理论

总之计算是做不到的.

——Evariste Galois

我们已经看到，由单个代数元 α 生成的扩域里的计算可以简单地通过将它等同于形式地构造的域 $F[x]/(f)$来进行，其中 f 是 α 在 F 上的既约多项式. 假设 f 在扩域 K 中分解成线性因子的乘积，但我们并不清楚如何同时用这些根来进行计算. 为此，需要知道这些根是如何联系起来的，而且这也依赖于特殊的情形. 通过许多人，特别是拉格朗日和伽罗瓦的工作，一个基本的发现是根之间的关系可以用对称的观点来理解. 对称是本章的主题.

从本章第四节开始，我们假设所讨论的域是特征为零的. 这个假设的最重要结论是：

- 域 F 上的既约多项式的根是不同的(15.6.8).
- 有限扩域 K/F 有本原根(15.8.1).

第一节　对称函数

令 $R[u]$表示环 R 上 n 个变量的多项式环 $R[u_1, \cdots, u_n]$. 指标$\{\mathbf{1}, \cdots, \boldsymbol{n}\}$的置换 σ 通过置换变量作用多项式：

【16.1.1】
$$f = f(u_1, \cdots, u_n) \rightsquigarrow f(u_{\sigma 1}, \cdots, u_{\sigma n}) = \sigma(f)$$

以这种方式，σ 定义了 $R[u]$的自同构，我们也将其记为 σ. 因为 σ 在常数多项式上作用是恒等的，我们称其为 R-自同构. 对称群 S_n 通过 R-自同构作用在多项式环上. 对称多项式是在每个置换作用下固定不变的多项式. 对称多项式构成多项式环 $R[u]$的子环.

多项式 g 是对称的，如果属于同一轨道的两个单项式(诸如 $u_1u_2^2$ 与 $u_2u_3^2$)在 g 中有相同的系数. 称一个轨道中单项式的和为轨道和. 轨道和构成对称多项式空间的基. 三个变量次数至多为 3 的轨道和是 477

$$1, \boldsymbol{u_1 + u_2 + u_3}, u_1^2 + u_2^2 + u_3^2, \boldsymbol{u_1u_2 + u_1u_3 + u_2u_3},$$
$$u_1^3 + u_3^3 + u_3^3, u_1u_2^2 + u_2u_1^2 + u_1u_3^2 + u_3u_1^2 + u_2u_3^2 + u_3u_2^2, \boldsymbol{u_1u_2u_3}$$

初等对称函数是一些特殊对称多项式. 当有 n 个变量时，它们是：

$$\begin{aligned}
s_1 &= \sum_i u_i &&= u_1 + u_2 + \cdots + u_n \\
s_2 &= \sum_{i<j} u_iu_j &&= u_1u_2 + u_1u_3 + \cdots \\
s_3 &= \sum_{i<j<k} u_iu_ju_k &&= u_1u_2u_3 + \cdots \\
&\vdots \qquad \vdots && \qquad\quad \vdots \\
s_n &= u_1u_2\cdots u_n &&= u_1u_2\cdots u_n
\end{aligned}$$

选取指标使得 s_i 是多项式 $u_1u_2\cdots u_i$ 的轨道和. 三个变量的初等对称函数在上面用黑斜体表出.

初等对称函数是具有变量根 u_1，…，u_n 的多项式的系数：

【16.1.2】
$$P(x)=(x-u_1)(x-u_2)\cdots(x-u_n)$$
$$=x^n-s_1x^{n-1}+s_2x^{n-2}-\cdots\pm s_n$$

当 $n=2$ 时，

$$P(x)=(x-u_1)(x-u_2)=x^2-(u_1+u_2)x+(u_1u_2)$$

当 $n=3$ 时，

$$P(x)=x^3-(u_1+u_2+u_3)x^2+(u_1u_2+u_1u_3+u_2u_3)x-(u_1u_2u_3)$$

在(16.1.2)里指标的顺序是我们从前多项式系数指标的反转，并且符号交错. 因为指标和符号以这种方式出现，我们在本章以类似形式给一个多项式未定系数标号：

【16.1.3】
$$f(x)=x^n-a_1x^{n-1}+a_2x^{n-2}-\cdots\pm a_n$$

同以前一样，我们说一个多项式在域 K 里完全分裂，如果它分解成线性因子之积，比如说

【16.1.4】
$$f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$$

478 其中 $\alpha_i\in K$. 如果这样，则替换 $u_i=\alpha_i$ 表明 f 的系数由计算对称函数得到.

【16.1.5】引理 *如果(16.1.4)是多项式(16.1.3)的分解，则* $a_i=s_i(\alpha_1,\cdots,\alpha_n)$.

【16.1.6】定理(对称函数定理) *系数属于环 R 的每个对称多项式 $g(u_1,\cdots,u_n)$ 可以用唯一的方式写成初等对称函数 $s_1,\cdots,s_n$ 的多项式.*

更确切地：如果 $g(u)$ 是对称多项式，存在系数属于 R 的另一组变量 $z_1,\cdots,z_n$ 的唯一多项式 $G(z_1,\cdots,z_n)$，使得 $g(u)$ 由替换 $z_i\rightsquigarrow s_i$：$g(u_1,\cdots,u_n)=G(s_1,\cdots,s_n)$ 得到.

我们下面证明定理，但首先给出一些例子：

【16.1.7】例

(a) 对称多项式 $u_1^2+\cdots+u_n^2$ 是线性组合 $c_1s_1^2+c_2s_2$，因为它有次数 2. 可用变量的特殊值来确定系数. 替换 $u=(1,0,\cdots,0)$ 表明 $c_1=1$，替换 $u=(1,-1,0,\cdots,0)$ 表明 $c_2=-2$：

【16.1.8】
$$u_1^2+\cdots+u_n^2=s_1^2-2s_2$$

(b) 对三个变量 u_1，u_2，u_3 的对称多项式

【16.1.9】
$$g(u)=u_1u_2^2+u_2u_1^2+u_1u_3^2+u_3u_1^2+u_2u_3^2+u_3u_2^2$$

我们使用不同的方法. 第一步是置 $u_3=0$. 得到剩余变量的对称多项式 $g^\circ=u_1^2u_2+u_2^2u_1$. 令 s_i° 表示 u_1，u_2 的初等对称函数：$s_1^\circ=u_1+u_2$ 与 $s_2^\circ=u_1u_2$. 我们注意到 $g^\circ=s_1^\circ s_2^\circ$.

第二步是将多项式 g 与三个变量对称多项式 s_1s_2 比较：

$$s_1s_2=(u_1+u_2+u_3)(u_1u_2+u_1u_3+u_2u_3)$$

我们将不具体展开右边，而我们注意到展开式有 9 项，其中之一是 $u_1^2u_2$. 因为 s_1s_2 是对称的，故 $u_1^2u_2$ 的轨道和 g 有 6 项. 剩余 3 项等于 $u_1u_2u_3=s_3$：

【16.1.10】
$$g=s_1s_2-3s_3$$

这个计算是系统方法的例子，下面给出的对称函数定理的证明就基于这个方法. ■

对称函数定理的证明 当 $n=1$ 时，没有什么要证明的，因为在这个情形里 $u_1=s_1$. 用归纳法进行证明. 假设定理对于对称函数在 $n-1$ 时成立. 已给 u_1，…，u_n 的对称多项式 g，我们考虑通过把最后一个变量替换为零得到的多项式 $g^\circ: g^\circ(u_1, \cdots, u_{n-1})=g(u_1, \cdots, u_{n-1}, 0)$. 注意 g° 是 u_1，…，u_{n-1} 的对称多项式. 所以，由归纳假设，g° 可写为 u_1，…，u_{n-1} 的初等对称函数的多项式，这些初等对称函数标记为 s_1°，…，s_{n-1}°：

$$s_1^\circ = u_1 + u_2 + \cdots + u_{n-1}, \text{等等}$$

479

存在对称多项式 $Q(z_1, \cdots, z_{n-1})$ 使得 $g^\circ=Q(s_1^\circ, \cdots, s_{n-1}^\circ)$.

【16.1.11】引理 令 g 是变量 u_1，…，u_n 的 d 次对称多项式，且设 $g^\circ=Q(s_1^\circ, \cdots, s_{n-1}^\circ)$，则 $g=Q(s_1, \cdots, s_{n-1})+s_n h$，其中 h 是 u_1，…，u_n 的 $d-n$ 次对称多项式.

证明 令 $p(u_1, \cdots, u_n)=g(u_1, \cdots, u_n)-Q(s_1, \cdots, s_{n-1})$. 这是对称多项式的差，从而它是对称的. 如果置 $u_n=0$，我们得到 $p(u_1, \cdots, u_{n-1}, 0)=g^\circ-Q(s^\circ)=0$. 所以，$u_n$ 整除 p. 由于 p 是对称的，每个 u_i 整除 p，所以 s_n 整除 p. 写 $p=s_n h$，多项式 h 是对称的. 这给了我们一个由引理断言的型的方程. ■

我们回到对称函数定理的证明. 上面引理告诉我们 $g=Q(s)+s_n h$，其中 h 是对称的. 对对称多项式的次数再使用归纳法，可得 h 是对称函数的多项式. 因此，g 也是.

通过仔细检查这个证明可证得 G 是唯一确定的. ■

我们给出系统方法的另一个例子. 令 g 是单项式 $u_1 u_2^2$ 的轨道和，但这次是关于 4 个变量 u_1，…，u_4 的. 设 s_1，…，s_4 表示 4 个变量的初等对称函数. 我们置 $u_4=0$，得到公式(16.1.10)，现在写为 $g^\circ=s_1^\circ s_2^\circ-3s_3^\circ$. 这样，如同上面公式里的，

$$g = s_1 s_2 - 3s_3 + s_4 h$$

因为 g 有次数 3，故 $h=0$. 当 g 是 $u_1^2 u_2$ 在变量个数 $n\geqslant 3$ 的轨道和时，公式(16.1.10)是正确的.

下面是对称函数定理的重要结果：

【16.1.12】推论 假设多项式 $f(x)=x^n-a_1 x^{n-1}+\cdots\pm a_n$ 的系数属于域 F，且设它在扩域 K 里完全分裂，并有根 α_1，…，α_n. 令 $g(u_1, \cdots, u_n)$ 是 u_1，…，u_n 且系数在 F 里的对称多项式，则 $g(\alpha_1, \cdots, \alpha_n)$ 是 F 的元素.

例如，$\alpha_1^k+\alpha_2^k+\cdots+\alpha_n^k$ 是 F 的元素.

证明 对称函数定理告诉我们 g 是初等对称函数的多项式. 比如说 $g(u_1, \cdots, u_n)=G(s_1, \cdots, s_n)$，其中 $G(z)$ 是系数在 F 里的多项式. 当计算 $u=\alpha$ 处的值时，我们得到 $s_i(\alpha)=a_i$(16.1.5). 于是，

【16.1.13】
$$g(\alpha_1, \cdots, \alpha_n) = G(a_1, \cdots, a_n)$$

因为 a_1，…，a_n 属于 F 且 G 的系数在 F 里，故 $G(a)$ 属于 F. ■

480

下一个命题提供了从任一个多项式开始构造对称多项式的方法.

【16.1.14】命题 令 $p_1=p_1(u_1, \cdots, u_n)$ 是多项式，设 $\{p_1, \cdots, p_k\}$ 是它的关于对称群在变量上作用的轨道，且设 $w=w_1, \cdots, w_k$ 是另一个变量集，其中 k 是在 p_1 的轨道里多项

式的个数.（于是，k 整除对称群的阶 $n!$.）如果 $h(w_1, \cdots, w_k)$ 是 w 的对称多项式，则 $h(p_1, \cdots, p_k)$ 是 u 的对称多项式.

证明 除了稍许混乱，这几乎是平凡的. 变量 $u_1, \cdots, u_n$ 的置换置换集合 $\{p_1, \cdots, p_k\}$，因为这个集合是轨道. 又因为 h 是对称多项式，所以 $p_1, \cdots, p_k$ 的置换把 $h(p_1, \cdots, p_k)$ 变为自身. ■

【16.1.15】例 有三个变量 u_1，u_2，u_3 与 $p_1 = u_1^2 + u_2u_3$. p_1 的轨道由三个多项式组成：

$$p_1 = u_1^2 + u_2u_3, p_2 = u_2^2 + u_3u_1, p_3 = u_3^2 + u_1u_2$$

我们用 $w = p$ 替换对称多项式 $w_1w_2 + w_1w_3 + w_2w_3$，得到 u 的对称多项式：

$$p_1p_2 + p_2p_3 + p_3p_1 = (\overset{3\text{项}}{u_1^2u_2^2} + \cdots) + (\overset{6\text{项}}{u_1^3u_3} + \cdots) + (\overset{3\text{项}}{u_1u_2u_3^2} + \cdots)$$ ■

第二节 判 别 式

除了初等对称函数外，最重要的对称多项式为带有变量根 $u_1, \cdots, u_n$ 的多项式

$$P(x) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots \pm s_n$$

的判别式. 判别式定义为

【16.2.1】
$$D(u) = (u_1 - u_2)^2(u_1 - u_3)^2 \cdots (u_{n-1} - u_n)^2 = \prod_{i<j}(u_i - u_j)^2$$

它的主要性质是：

- $D(u)$ 是整系数对称多项式.
- 如果 $\alpha_1, \cdots, \alpha_n$ 是域的元素，则 $D(u) = 0$ 当且仅当诸元素 α_i 中有两个是相等的.

对称函数定理告诉我们判别式 D 可唯一地写成初等对称函数的整多项式. 令

【16.2.2】
$$\Delta(z) = \Delta(z_1, \cdots, z_n)$$

是这个多项式，所以，$D(u) = \Delta(s)$. 当 $n = 2$ 时，

【16.2.3】
$$D = (u_1 - u_2)^2 = s_1^2 - 4s_2, \quad \Delta(z) = z_1^2 - 4z_2$$

这是熟悉的二次多项式 $x^2 - s_1x + s_2$ 的判别式，尽管 D 是根的差的平方的事实在我们上学
481 时没有强调.

不幸的是，当 n 较大时，D 与 Δ 是很复杂的. 当 $n > 3$ 时，我不知道它们是什么. 一般来说，三次多项式

【16.2.4】
$$P(x) = x^3 - s_1x^2 + s_2x - s_3$$

的判别式已经是太复杂以致记不住：

【16.2.5】
$$\begin{aligned} D &= (u_1 - u_2)^2(u_1 - u_3)^2(u_2 - u_3)^2 \\ &= -4s_1^3s_3 + s_1^2s_2^2 + 18s_1s_2s_3 - 4s_2^3 - 27s_3^2 \\ \Delta &= -4z_1^3z_3 + z_1^2z_2^2 + 18z_1z_2z_3 - 4z_2^3 - 27z_3^2 \end{aligned}$$

当对变量 u_i 做替换时这些公式仍成立. 如果给出环 R 中特殊元素 $\alpha_1, \cdots, \alpha_n$，且如果

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = x^n - a_1x^{n-1} + a_2x^{n-2} - \cdots \pm a_n$$

则用 α_i 替换 u_i，有

$$D(\alpha_1,\cdots,\alpha_n)=\prod_{i<j}(\alpha_i-\alpha_j)^2=\Delta(a_1,\cdots,a_n)$$

无论多项式 $f(x)=x^n-a_1x^{n-1}+a_2x^{n-2}-\cdots\pm a_n$ 是否为线性因子之积，它的判别式都定义为元素 $\Delta(a_1,\cdots,a_n)$，其中 $\Delta(z)$是多项式(16.2.2). 如果 f 的系数属于域 F，则 $\Delta(z)$的系数在域 F 里，且 $\Delta(a)$是 F 的元素.

当 $f(x)$中 x^2 的系数为零时，三次多项式的判别式变得较简单. 倘若特征不是 3，一般多项式(16.2.4)里的二次项可以通过类似完全平方法的替换消去，称为 Tschirnhausen 变换，

【16.2.6】 $$x=y+s_1/3$$

如果把二次项消失的三次多项式写为

【16.2.7】 $$f(x)=x^3+px+q$$

则判别式由(16.2.5)的替换得到：

【16.2.8】 $$\Delta(0,p,-q)=-4p^3-27q^2$$

因为初等对称函数 s_i 的变量 u 的次数为 i，所以分派给变量 z_i 权 i，并且定义单项式 $z_1^{e_1}z_2^{e_2}\cdots z_n^{e_n}$ 的加权次数为 $e_1+2e_2+\cdots+ne_n$ 是很方便的. 在 z 的加权次数为 d 的单项式里用 s_i 替换 z_i 产生 u_1，…，u_n 的通常次数为 d 的多项式. 例如，z_1z_2 有加权次数 3，且 $s_1s_2=(u_1+\cdots)(u_1u_2+\cdots)$有次数 3. 如果 $g(u)$是次数为 d 的对称多项式，且 $G(z)$是使得 $g(u)=G(s)$的多项式，则 G 关于 z 有加权次数 d. 482

三次多项式(16.2.4)的判别式是 u 的次数为 6 的齐次多项式. 有 7 个 z_1，z_2，z_3 的加权次数为 6 的单项式：

【16.2.9】 $$z_1^6,z_1^4z_2,z_1^2z_2^2,z_2^3,z_1^3z_3,z_1z_2z_3,z_3^2$$

且 Δ 为这些单项式的整线性组合. 我们将用系统方法确定前 4 个单项式的系数：在 $D=(u_1-u_2)^2(u_1-u_3)^2(u_2-u_3)^2$ 中置 $u_3=0$，得到 u_1，u_2 的对称多项式$(u_1-u_2)^2u_1^2u_2^2=(s_1^{\circ 2}-4s_2^{\circ})s_2^{\circ 2}$. 所以，$D=s_1^2s_2^2-4s_2^3+s_3h$，其中 h 是对称三次多项式. s_1^6 与 $s_1^4s_2$的系数是零. 我不知道确定余下的 Δ 的三个系数的容易方法，但一个方法是给变量 u_1，u_2，u_3 分派某个特殊值.

第三节 分 裂 域

令 f 是系数在域 F 里的多项式，不一定是既约的. F 上 f 的分裂域是扩域 K/F，使得

- f 在 K 里完全分裂，比如说 $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$，其中 $\alpha_i\in K$，且
- K 是由根生成的：$K=F(\alpha_1,\cdots,\alpha_n)$.

第二个条件蕴含着，对 K 的每个元素 β，存在系数在 F 中的多项式 $p(u_1,\cdots,u_n)$，使得 $p(\alpha_1,\cdots,\alpha_n)=\beta$. 事实上，存在许多这样的多项式：因为根在 F 上是代数的，所以一些多项式等于零.

如果我们的域 F 是复数域 $\mathbf{C}$ 的子域，分裂域 K 可简单地通过添加 f 的复数根到 F 得到，我们可把 K 说成是 f 的分裂域. 但如果 F 不是 $\mathbf{C}$ 的子域，我们必须抽象地构造分裂域，就像上一章解释的(第十五章第六节).

【16.3.1】引理

(a) 如果 $F \subset L \subset K$ 是域，且 K 是多项式 f 在 F 上的分裂域，则 K 也是同一个多项式在 L 上的分裂域.

(b) $F[x]$中的每个多项式 $f(x)$有分裂域.

(c) 分裂域是 F 的有限扩张，且每个有限扩张包含在分裂域里.

证明

(a) 显然.

(b) 已给系数在 F 里的多项式 f，存在 F 的域扩张 K'，f 在其中完全分裂(15.6.3). 由 f 的根生成的 K'的子域是分裂域.

(c) 分裂域是由有限多个在 F 上为代数的元素生成的，所以，它是 F 的有限扩张. 反之，有限扩张 L/F 是由有限多个元素生成的，比如说 γ_1，…，γ_k，每个元素在 F 上是代数的. 令 g_i 是 γ_i 在 F 上的既约多项式，且令 f 是积 $g_1 \cdots g_k$. 我们可将域 L 扩张为 f 在 L 上
483 的分裂域，从而 K 也是 F 上的分裂域. ■

我们现在用对称函数证明一个令人惊讶的事实：

【16.3.2】定理(分裂定理) 令 K 是域 F 的扩域，且它是系数在 F 里的多项式 $f(x)$的分裂域. 如果系数在 F 里的既约多项式 $g(x)$有一个根属于 K，则它在 K 里完全分裂.

这个定理提供了分裂域的一个性质. F 上分裂域 K 是具有这个性质的有限域扩张：

$$F \text{上有一个根在} K \text{里的既约多项式在} K \text{里完全分裂}$$

哪个多项式用来定义 K 为分裂域是不重要的.

分裂定理的证明 令 f 与 g 如同定理所叙述的. 已给 g 在 K 里的一个根 β_1，我们必须证明 g 在 K 里完全分裂. 由于 g 是既约的，它是 β_1 在 F 上的既约多项式.

分裂域 K 是由 f 的根 α_1，…，α_n 在 F 上生成的. K 的每个元素可写成 α 的多项式，且系数在 F 里. 选取多项式 $p_1(u_1, \cdots, u_n)$使得 $p_1(\alpha)=\beta_1$.

令$\{p_1, \cdots, p_k\}$是 $p_1(u)$关于对称群 S_n 在多项式环 $F[u_1, \cdots, u_n]$上作用的轨道，且设 $\beta_j = p_j(\alpha)$. 所以，β_1，…，β_k 是 K 的元素. 我们将通过证明多项式

$$h(x) = (x-\beta_1)\cdots(x-\beta_k)$$

的系数属于 F 来证明分裂定理. 假设这个结论已经证明，则因为 β_1 是 h 的根，故可得 β_1 在 F 上的既约多项式 g 整除 h. 且因为 h 在 K 里完全分裂，所以 g 也完全分裂.

比如说，$h(x)=x^k-b_1x^{k-1}+b_2x^{k-2}-\cdots\pm b_k$. 系数 b_1，…，b_k 由初等对称函数在 $\beta=\beta_1$，…，β_k 处取值得到. 但这些是 k 个变量的初等对称函数. 我们引进新的变量 w_1，…，w_k，并且把这些变量的初等对称函数标记为 $s'_1(w)$，…，$s'_k(w)$(用斜撇提醒我们变量是新的)，这样，$b_j=s'_j(\beta)$.

我们分两步计算 s'_j：首先，做替换 $w=p$，亦即 $w_j=p_j(u)$. 因为 $s'_j(w)$关于 w 是对称的，所以 $s'_j(p)$是 u 的对称多项式(16.1.4). 其次，做替换 $u_i=\alpha_i$. 因为 $s'_j(p(u))$关于 u 是对称的，所以 $s'_j(p(\alpha))$属于域 F(16.1.2). 另一方面，$s'_j(p(\alpha))=s'_j(\beta)=b_j$. 系数 b_j 属于 F. ■

第四节 域扩张的同构

对于本章余下的部分，假设域的特征为零. 我们将不再提及这个假设. 所考虑的域扩张是有限扩张. 我们需要一些新的定义：

- 令 K 与 K' 是 F 的域扩张. F-同构 $\sigma: K \to K'$ 的概念是在前面引进的(见(15.2.9)). 它是限制在子域 F 上且为恒等映射的同构. 扩域 K 的 F-自同构是从 K 到自身的 F-同构. K 的 F-自同构是域扩张的对称.
- 有限扩张 K 的 F-自同构构成一个群，称为 K 在 F 上的伽罗瓦群，常记为 $G(K/F)$. 484
- 有限扩张 K/F 是伽罗瓦扩张，如果它的伽罗瓦群 $G(K/F)$ 的阶等于扩张次数：$|G(K/F)| = [K:F]$.

下面我们将看到伽罗瓦群的阶总是整除扩张的次数(16.6.2).

【16.4.1】例 复数域 $\mathbf{C}$ 是实数域 $\mathbf{R}$ 的伽罗瓦扩张. 伽罗瓦群 $G(\mathbf{C}/\mathbf{R})$ 是 2 阶循环群，由复共轭的自同构生成. 对任意二次扩张 K/F 有类似叙述. 二次扩张由附加一个平方根得到，比如说 $K = F(\alpha)$，其中 $\alpha^2 = a$ 属于 F. K/F 的伽罗瓦群 G 有阶 2，且 G 不同于恒等元的元素 τ 互换两个平方根 α 与 $-\alpha$. 例如，如果 $F = \mathbf{Q}$，且 $K = \mathbf{Q}(\sqrt{2})$，则有 K 的 F-自同构 τ 映 $a + b\sqrt{2} \rightsquigarrow a - b\sqrt{2}$. 以前我们见到过这个自同构. ■

【16.4.2】引理 令 K 与 K' 是域 F 的扩张.

(a) 令 $f(x)$ 是系数属于 F 的多项式，且设 σ 是从 K 到 K' 的 F-自同构. 如果 α 是 f 的属于 K 的根，则 $\sigma(\alpha)$ 是 f 的属于 K' 的根.

(b) 假设 K 是由一些元素 $\alpha_1, \cdots, \alpha_n$ 在 F 上生成的. 令 σ 与 σ' 是 F-同构 $K \to K'$. 如果对 $i = 1, \cdots, n$，$\sigma(\alpha_i) = \sigma'(\alpha_i)$，则 $\sigma = \sigma'$. 如果 K 的 F-自同构 σ 固定所有生成元不动，则它是恒等映射.

(c) 令 f 是系数属于 F 的既约多项式，且设 α 与 α' 是 f 的分别属于 K 与 K' 的根，则存在唯一的 F-同构 $\sigma: F(\alpha) \to F(\alpha')$ 将 α 映射为 α'. 如果 $F(\alpha) = F(\alpha')$，则 σ 是 F-自同构.

证明 (a)在上一章已证(15.2.10). 我们略去(b)的证明. 在(c)中，σ 的存在在上一章已证(15.2.8)，而(b)表明 σ 是唯一的. ■

【16.4.3】命题

(a) 令 f 是系数属于 F 的多项式. 扩域 L/F 至多含有 f 在 F 上的一个分裂域.

(b) 令 f 是系数属于 F 的多项式. f 在 F 上的任意两个分裂域是同构扩域.

证明

(a) 若 L 含有 f 的分裂域，则 f 在 L 里完全分裂，比如说，$f = (x - \alpha_1)\cdots(x - \alpha_n)$，其中 $\alpha_i \in L$. 如果 β 是 f 在 L 里的任意根，代入这个乘积里，对某个 i，有 $\beta = \alpha_i$. 于是，f 在 L 里没有其他根，从而含在 L 里的 f 的仅有分裂域是 $F(\alpha_1, \cdots, \alpha_n)$.

(b) 令 K_1 与 K_2 是 f 在 F 上的两个分裂域. 第一个分裂域 K_1 是 F 的有限扩张，因

此，它有本原元 γ. 设 g 是 γ 在 F 上的既约多项式. 我们选取第二个域 K_2 的扩张 L，且 g
485 在其中有根 γ'，令 K' 表示由 γ' 生成的 L 的子域 $F(\gamma')$. 存在 F-同构 $\varphi: K_1 \to K'$ 映射 γ 为 γ'. 因为 K' 与分裂域 K_1 是 F-同构的，故它也是 f 的分裂域. 这样，K' 与 K_2 是包含在域 L 里的分裂域，由(a)知它们是相等的. 所以，φ 是从 K_1 到 K_2 的 F-同构. ■

第五节 固 定 域

令 H 是域 K 的自同构群. H 的固定域(常记为 K^H)是 K 的由每个群元素固定不动的元素集合：

【16.5.1】 $$K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha, \quad \text{对于所有 } \sigma \in H\}$$

容易证明 K^H 是 K 的子域，且 H 是伽罗瓦群 $G(K/K^H)$ 的子群. 事实上，下面的固定域定理表明 H 等于 $G(K/K^H)$.

【16.5.2】定理 令 H 是域 K 的有限自同构群，且设 F 表示固定域 K^H. 令 β_1 是 K 的元素，且 $\{\beta_1, \cdots, \beta_r\}$ 是 β_1 的 H-轨道.

(a) β_1 在 F 上的既约多项式是 $g(x) = (x-\beta_1)\cdots(x-\beta_r)$.

(b) β_1 在 F 上是代数的，且它在 F 上的次数等于它的轨道的阶. 所以，β_1 在 F 上次数整除 H 的阶.

证明 定理(b)部分的结论可由(a)部分的结论证得. 我们证明(a). 比如说

$$g(x) = (x-\beta_1)\cdots(x-\beta_r) = x^r - b_1 x^{r-1} + \cdots \pm b_r$$

g 的系数是轨道 $\{\beta_1, \cdots, \beta_r\}$ 的对称函数(16.1.5). 因为 H 的元素置换轨道，故它们固定系数不动. 所以，g 的系数属于固定域.

令 h 是系数属于 F 的多项式，并以 β_1 为其一个根. 对 $i=1, \cdots, r$，存在 H 的一个元素 σ 使得 $\sigma(\beta_1) = \beta_i$. 因为 H 的元素是 K 的 F-自同构，且又因为 h 的系数属于 F，所以，β_i 也是 h 的根(16.4.2)(a). 于是，$x-\beta_i$ 整除 f. 因为这对每个 i 都是成立的，故在 $K[x]$ 与 $F[x]$ 里，g 整除 f(15.6.4)(b). 这表明 g 生成了 $F[x]$ 中以 β_1 为根的多项式的主理想，且 g 是 β_1 在 F 上的既约多项式(15.2.3). ■

扩域 K/F 称为代数的，如果 K 的每个元素在 F 上是代数的.

【16.5.3】引理 令 K 是域 F 的代数扩张，且不是 F 的有限扩张，则在 K 里存在其在 F 上的次数是任意大的元素.

证明 构造中间域链 $F < F_1 < F_2 < \cdots$ 如下：在 K 中选取不属于 F 的元素 α_1，并令 $F_1 = F(\alpha_1)$. 这样，α_1 在 F 上是代数的，所以，$[F_1:F] < \infty$，从而 $F_1 < K$. 其次，在 K 中选取不属于 F_1 的元素 α_2，并令 $F_2 = F(\alpha_1, \alpha_2)$. 于是，$[F_2:F] < \infty$ 且 $F_1 < F_2 < K$. 在
486 K 中选取不属于 F_2 的 α_3，等等. 这个域链是 F 的有限扩张的严格递增链. 次数 $[F_i:F]$ 变得任意大，但仍是有限的. 每个扩张 F_i/F 有本原元 γ_i，且 γ_i 在 F 上的次数也变得任易大. ■

【16.5.4】定理(固定域定理) 令 H 是域 K 的有限自同构群，且设 $F = K^H$ 是它的固定域，

则 K 是 F 的有限扩张，且它的次数$[K:F]$等于群的阶$|H|$.

证明 令 $F=K^H$，且设 n 是 H 的阶. 定理 16.5.2 表明扩张 K/F 是代数的，K 的任意元素 β 在 F 上的次数整除 n. 所以，次数$[K:F]$是有限的(16.5.3). 令 γ 是这个扩张的本原元. H 的每个元素 σ 是 F 上的恒等元，于是，如果 σ 也固定 γ，则它将是恒等映射——H 的恒等元. 所以，γ 的稳定子是 H 的平凡子群$\{1\}$，且 γ 的轨道有阶 n. 定理 16.5.2 表明 γ 在 F 上的次数为 n. 因为 $K=F(\gamma)$，故次数$[K:F]$也等于 n. ■

一个变量的有理函数域 $\mathbf{C}(t)$的自同构提供了说明固定域定理与定理 16.5.2 的例子.

【16.5.5】例 令 $K=\mathbf{C}(t)$，且设 σ 与 τ 是 K 的在 $\mathbf{C}$ 上为恒等的自同构，并使得 $\sigma(t)=\mathrm{i}t$ 与 $\tau(t)=t^{-1}$. 这样，$\sigma^4=1$，$\tau^2=1$，$\tau\sigma=\sigma^{-1}\tau$. 所以，$\sigma$ 与 τ 生成了与二面体群 D_4 同构的自同构群 H.

【16.5.6】引理 有理函数 $u=t^4+t^{-4}$ 在 $\mathbf{C}$ 上是超越的.

证明 令 $g(x)=x^d+c_{d-1}x^{d-1}+\cdots+c_0$ 是复系数的首项系数为 1 的 d 次多项式. 这样，$t^{4d}g(u)$是 t 的首项系数为 1 的 $8d$ 次多项式. 因为 t 是超越的，故 $t^{4d}g(u)\neq 0$，且 $g(u)\neq 0$. ■

由此引理可得域 $\mathbf{C}(u)$同构于一个变量的有理函数域. 我们证明它是固定域 K^H. 我们注意到 u 是由 σ 和 τ 固定不动的. 因此 u 属于固定域 K^H，所以，$\mathbf{C}(u)\subset K^H$. 定理 16.5.2 告诉我们 K^H 上 t 的既约多项式是其根构成它的轨道的多项式. t 的轨道是

$$\{t,\mathrm{i}t,-t,-\mathrm{i}t,t^{-1},-\mathrm{i}t^{-1},-t^{-1},\mathrm{i}t^{-1}\}$$

且其根是这个轨道元素的多项式是

$$(x^4-t^4)(x^4-t^{-4})=x^8-ux^4+1$$

于是，t 是系数属于 $\mathbf{C}(u)$的 8 次多项式的根，所以，次数$[K:\mathbf{C}(u)]$至多是 8. 固定域定理断言$[K:K^H]=8$. 因为 $\mathbf{C}(u)\subset K^H$，故可得 $\mathbf{C}(u)=K^H$. ■ 487

这个例子说明了一个著名定理：

【16.5.7】定理(Lüroth 定理) 令 F 是包含 $\mathbf{C}$ 但不是 $\mathbf{C}$ 自身的有理函数域 $\mathbf{C}(t)$的子域，则 F 同构于有理函数域 $\mathbf{C}(u)$.

第六节 伽罗瓦扩张

我们现在来到了本章的主题：伽罗瓦理论.

注 如果 K 是 F 的扩域，则中间域 L 是一个使得 $F\subset L\subset K$ 的域. 一个中间域是真的，如果它既不是 F 也不是 K.

如果 L 是中间域，则 K 的每个 L-自同构将是 F-自同构，所以，

【16.6.1】
$$G(K/L)\subset G(K/F)$$

【16.6.2】引理

(a) 有限扩域 K/F 的伽罗瓦群 G 是其阶整除扩张次数$[K:F]$的有限群.

(b) 令 H 是域 K 的有限自同构群，则 K 是它的固定域 K^H 的伽罗瓦扩张，且 H 是

K/K^H的伽罗瓦群.

证明

(a) 由 F-自同构的定义，G 的元素平凡作用在 F 上，于是，F 包含在固定域 K^G 里. 这样，$F\subset K^G\subset K$. 于是，$[K:K^G]$整除$[K:F]$. 由固定域定理，$|G|=[K:K^G]$.

(b) 由 K^H 的定义，H 的元素是 K^H-自同构. 所以，H 是伽罗瓦群 $G(K/K^H)$的子群. 因为$|G(K/K^H)|$整除$[K:K^H]$，且$|H|=[K:K^H]$，故这两个群是相等的，且 K 是 K^H 的伽罗瓦扩张. ■

【16.6.3】引理 令 γ_1 是域 F 的有限扩域 K 的本原元，且设 $f(x)$是 γ_1 在 F 上的既约多项式. 令 γ_1，…，γ_r 是 f 的属于 K 的根，则存在 K 的唯一 F-自同构 σ_i 使得 $\sigma_i(\gamma_1)=\gamma_i$. 这些是 K 的所有 F-自同构，所以，$G(K/F)$的阶为 r.

证明 存在唯一 F-同构 $\sigma_i:F(\gamma_1)\to F(\gamma_i)$映 $\gamma_1\rightsquigarrow\gamma_r$(16.4.2)(c). 给定 $K=F(\gamma_1)$，且因为 $F(\gamma_i)$在 F 上有同一次数，故也有 $K=F(\gamma_i)$. 所以，σ_i 是 K 的 F-自同构. K 的每个 F-自同构映 γ_1 到 f 的一个根. 于是，它是诸自同构 σ_i 之一. ■

【16.6.4】定理(伽罗瓦扩张的特征性质) 令 K/F 是有限扩张，且设 G 是它的伽罗瓦群. 下列论述是等价的：

(a) K/F 是伽罗瓦扩张，亦即$|G|=[K:F]$.

(b) 固定域 K^G 等于 F.

(c) K 是 F 上的分裂域.

定理的(b)部分可用来证明伽罗瓦扩张 K 的元素实际上属于 F，(c)可用来证明扩张是
488 伽罗瓦的.

定理的证明 (a)⇔(b)：由固定域定理，$|G|=[K:K^G]$. 因为 $F\subset K^G\subset K$，故$|G|=[K:F]$当且仅当 $F=K^G$.

(a)⇔(c)：令 $n=[K:F]$. 选取 K 在 F 上的一个本原元 γ_1. 设 f 是 F 上的既约多项式. 因为 γ_1 是本原元，故 f 的次数是 n. 令 γ_1，…，γ_r 是 f 的属于 K 的根. 引理 16.6.3 告诉我们$|G|=r$. 于是，$|G|=[K:F]$，即扩张是伽罗瓦的，当且仅当 f 在 K 里完全分裂. 因为 K 是 γ_1 在 F 上生成的，故它也是由 f 的所有根的集合生成的. 所以，K 是 F 上的分裂域当且仅当 f 在 K 里完全分裂. ■

如果 K 是多项式 f 在 F 上的分裂域，我们也可将扩张 K/F 的伽罗瓦群说成是 f 的伽罗瓦群.

【16.6.5】推论

(a) 每个有限扩张 K/F 包含在一个伽罗瓦扩张里.

(b) 如果 K/F 是伽罗瓦扩张，且如果 L 是中间域，则 K 也是 L 的伽罗瓦扩张，且伽罗瓦群 $G(K/L)$是伽罗瓦群 $G(K/F)$的子群.

证明 定理 16.6.4 允许我们将短语“伽罗瓦扩张”替换为“分裂域”，这样，推论由引理 16.3.1 和 16.6.2 可得到. ■

【16.6.6】**定理** 令 K/F 是带有伽罗瓦群 G 的伽罗瓦扩张，且设 g 是系数属于 F 的且在 K 中完全分裂的多项式. 令它在 K 中的根为 $\beta_1, \cdots, \beta_r$.

(a) 群 G 作用在根的集合 $\{\beta_i\}$ 上.

(b) 如果 K 是 g 在 F 上的分裂域，则在根上的作用是忠实的，且由其在根上的作用，G 嵌入对称群 S_r 作为其子群.

(c) 如果 g 在 F 上是既约的，则在根上的作用是可迁的.

(d) 如果 K 是 g 在 F 上的分裂域，且 g 在 F 上是既约的，则 G 嵌入 S_r 作为其可迁子群.

证明 (a)是(16.4.2)(a)而(b)是(16.4.2)(b). 如果 g 是既约的，则它是 β_1 在 F 上的既约多项式. 因为 F 是 G 的固定域，故定理 16.5.2 告诉我们 g 的诸根 β_i 构成 β_1 的 G-轨道. 所以，作用是可迁的，如同(c)所断言的. 最后，(d)是条件(b)与(c)的组合. ■

这个定理是有用的，尽管它不足以确定伽罗瓦群. 整数 r 与到 S_r 的嵌入不仅依赖于伽罗瓦扩张 K，还依赖于 f. 再有，当 $r>2$ 时，对称群 S_r 有若干个可迁子群.

第七节 主要定理

伽罗瓦理论最重要的部分之一是中间域的确定. 伽罗瓦理论的主要定理断言，当 K/F 是伽罗瓦扩张时，中间域和伽罗瓦群的子群是一一对应的. 这个事实的重要性不是马上就 489
看出来的；我们将在使用中理解它.

【16.7.1】**定理**(主要定理) 令 K 是域 F 的伽罗瓦扩张，且设 G 是它的伽罗瓦群，则在 G 的子群与中间域之间存在一一对应：

$$\{\text{子群}\} \leftrightarrow \{\text{中间域}\}$$

这个对应把子群 H 与它的固定域以及中间域 L 与 K 在 L 上的伽罗瓦群结合起来. 映射

$$H \rightsquigarrow K^H \quad \text{与} \quad L \rightsquigarrow G(K/L)$$

是逆函数.

证明 我们必须证明两个映射任意顺序的合成都是恒等映射，这样证明工作就完成了. 令 H 是 G 的子群，且设 L 是它的固定域. 固定域定理告诉我们 $G(K/L)=H$. 另一方面，令 L 是中间域，且设 H 是 K 在 L 上的伽罗瓦群. 这样，K 是 L 的伽罗瓦扩张(推论 16.6.5(b)). 定理 16.6.4 告诉我们 H 的固定域是 L. ■

【16.7.2】**推论**

(a) 由主要定理给出的对应是反向包含：如果 L 与 L' 是中间域，且如果 H 与 H' 是对应子群，则 $L \subset L'$ 当且仅当 $H \supset H'$.

(b) 对应于域 F 的子群是整个群 $G(K/F)$，而对应于 K 的子群是平凡子群 $\{1\}$.

(c) 如果 L 对应于 H，则 $[K:L]=|H|$，$[L:F]=[G:H]$.

在(c)中，第一个等式可由 K 是 L 的伽罗瓦扩张与 $H=G(K/L)$ 的事实得到. 这样就得到了第二个等式，这是因为

$$|G| = [K:F] = [K:L][L:F] \text{ 与 } |G| = |H|[G:H]$$

【16.7.3】推论 有限域扩张 K/F 有有限多个中间域 $F\subset L\subset K$.

证明 当 K/F 是伽罗瓦扩张时，这可由主要定理得到，这是因为有限群有有限多个子群. 这是因为可把任意有限扩张嵌入伽罗瓦扩张，故对任意有限扩张这都是成立的. ■

【16.7.4】例 令 F 是有理数域，且设 $\alpha=\sqrt{3}$ 与 $\beta=\sqrt{5}$，所以，$\alpha\beta=\sqrt{15}$. 多项式 $(x^2-3)\times(x^2-5)$ 的分裂域 $K=F(\alpha,\beta)$ 是 F 的 4 次伽罗瓦扩张. 它的伽罗瓦群 G 的阶为 4，于是，它或是克莱因四元群，或是循环群. 容易求出 F 上三个 2 次中间域，亦即 $F(\alpha)$，$F(\beta)$ 与 $F(\alpha\beta)$. 这三个中间域对应于 G 的三个真子群. 所以，G 是克莱因四元群，它有三个 2 阶
490 元，从而有三个 2 阶子群. 4 阶循环群仅有一个 2 阶子群.

2 阶子群是 G 仅有的真子群，所以，主要定理告诉我们除我们发现的三个中间域外，没有别的真中间域. 因此，K 的元素 $\gamma=a+b\alpha+c\beta+d\alpha\beta$（其中 a，b，c，$d\in F$）在 F 上次数为 4，除非它在三个真中间域之一里. 这种情形仅当系数 b，c，d 中至少有两个为零时出现. ■

假设给定域链 $F\subset L\subset K$，且 K 是 F 的伽罗瓦扩张. 这样，K 也是 L 的伽罗瓦扩张. 然而，L 不一定是 F 的伽罗瓦扩张. 为了得到完整描述，我们证明作为 F 的伽罗瓦扩张的中间域 L 对应于 G 的正规子群.

【16.7.5】定理 *令 K/F 是带有伽罗瓦群 G 的伽罗瓦扩张，且设 L 是 G 的子群 H 的固定域. 扩张 L/F 是伽罗瓦扩张当且仅当 H 是 G 的正规子群. 如果是这样，则伽罗瓦群 $G(L/F)$ 同构于商群 G/H.*

$$G=G(K/F)\ \text{在}\ K\ \text{上作用，使}\ F\ \text{不变}\begin{cases}K\\L\\F\end{cases}\begin{cases}H=G(K/L)\ \text{在}\ K\ \text{上作用，使}\ L\ \text{不变}\\ \text{如果}\ H\ \text{正规，则}\ G/H=G(L/F)\ \text{在此作用}\end{cases}$$

证明 令 ε_1 是扩张 L/F 的本原元，且设 g 是 ε_1 在 F 上的既约多项式. 这个多项式在分裂域 K 中完全分裂；设它的根为 ε_1，…，ε_r. 我们用下列事实进行证明：

- L/F 是伽罗瓦扩张当且仅当它是分裂域，这种情形当所有根 ε_i 属于 L 时发生.
- 如果根 ε_i 属于 L，则 $L=F(\varepsilon_i)$，这是因为 ε_i 与 ε_1 在 F 上有相同次数且 $L=F(\varepsilon_1)$.
- G 的元素 σ 在 L 上是恒等的当且仅当它固定 ε_1 不动. 所以，ε_1 的稳定子等于 H.
- G 在集合 $\{\varepsilon_1,\cdots,\varepsilon_r\}$ 上的作用是可迁的：对任意 $i=1,\cdots,r$，存在 G 的元素 σ 使得 $\sigma(\varepsilon_1)=\varepsilon_i$（16.4.2）(c).

令 σ 是 G 的元素，比如说 $\sigma(\varepsilon_1)=\varepsilon_i$. 这样，$F(\varepsilon_i)=L$ 当且仅当 ε_i 属于 L，且如果是这样，则 ε_i 的稳定子等于 H. 另一方面，$\sigma(\varepsilon_1)$ 的稳定子是共轭群 $\sigma H\sigma^{-1}$. 所以，K/F 是伽罗瓦扩张当且仅当 $\sigma H\sigma^{-1}=H$ 对所有 σ 成立，亦即当且仅当 H 是正规子群.

假设 L 是 F 的伽罗瓦扩张. 这样，诸根 ε_i 属于 L. 伽罗瓦群 G 的元素 σ 映 ε_1 到另一个
491 根 ε_i，所以，它映 $L=F(\varepsilon_1)$ 到 $F(\varepsilon_i)=L$. 因此，限制 σ 到 L 定义了 L 的一个 F-自同构. 这个限制给出同态 $\varphi:G\to G(L/F)$. φ 的核是限制到 L 上的恒等元的 σ 的集合，它是 H. 而

且，$|G/H|=[G:H]=|G(L/F)|$. 第一同构定理告诉我们 G/H 同构于 $G(L/F)$. ■

在下一节里，我们考察伽罗瓦理论应用的最重要情形.

第八节 三次方程

令 $f(x)=x^3-a_1x^2+a_2x-a_3$ 是 F 上的既约多项式，且设 K 是 f 在 F 上的分裂域. 比如说，f 在 K 中的根是 α_1，α_2，α_3. 这样，在 $K[x]$ 中，

【16.8.1】 $$f(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

因为 a_1 属于 F 且 $a_1=\alpha_1+\alpha_2+\alpha_3$，故第三个根 α_3 属于由前两个根生成的域. 所以，我们有扩域链

$$F\subset F(\alpha_1)\subset F(\alpha_1,\alpha_2) \quad 与 \quad F(\alpha_1,\alpha_2)=F(\alpha_1,\alpha_2,\alpha_3)=K$$

令 L 表示域 $F(\alpha_1)$. 因为 f 在 F 上是既约的，故 $[L:F]=3$. 由于 α_1 属于 L，故多项式 f 在 $L[x]$ 中分解：

【16.8.2】 $$f(x)=(x-\alpha_1)q(x)$$

其中 q 是其根为 α_2 与 α_3 的二次多项式. 所以，K 由 L 通过添加二次多项式的根得到. 有两种情形：如果 q 在 L 上是既约的，则 $[K;L]=2$ 与 $[K:F]=6$. 如果 q 在 L 上是可约的，则 α_2 与 α_3 属于 L，$L=K$ 与 $[K:F]=3$.

【16.8.3】例

(a) $f(x)=x^3+3x+1$ 在 $\mathbf{Q}$ 上是既约的，且它的导数在实直线上永不为零. 所以，f 定义了实变量 x 的递增函数，且它仅取零值一次：f 有一个实根. 这个根不生成分裂域 K，它含有两个复数根. 于是，$[K:\mathbf{Q}]=6$.

(b) $f(x)=x^3-3x+1$ 在 $\mathbf{Q}$ 上也是既约的. 在这种情形下，如果 α_1 是 f 的根，则 $\alpha_2=\alpha_1^2-2$ 是另一个根. 这可通过代入 f 中检验. 所以，分裂域 K 等于 $\mathbf{Q}(\alpha_1)$ 且 $[K:\mathbf{Q}]=3$. ■

我们回到任意既约三次方程. 由它在根上的作用，K/F 的伽罗瓦群 G 成为对称群 S_3 的可迁子群(16.4.2)(c). 可迁子群为 S_3 与 A_3——3 阶循环群. 如果 $[K:F]=3$，则 $G=A_3$，且如果 $[K:F]=6$，则 $G=S_3$. 为区别这两种情形，我们需要确定出现在(16.8.2)里的二次多项式 $q(x)$ 在域 $L=F(\alpha_1)$ 上是否为既约的. 在域 L 里讨论是痛苦的，我们宁可在域 F 里做计算. 幸运的是，存在元素使得确定 f 的判别式(16.2.5)的平方根 δ 成为可能：

【16.8.4】 $$\delta=(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)$$ 492

它的主要性质是：

- δ 是 K 的元素.
- $\delta\neq 0$(因为诸根 α_i 是不同的).
- 根的置换使得 δ 乘上一个置换的符号.

【16.8.5】定理(三次方程的伽罗瓦理论) *令 K 是既约三次多项式 f 在域 F 上的分裂域，设 D 是 f 的判别式，设 G 是 K/F 的伽罗瓦群.*

- *如果 D 是 F 里的平方，则 $[K:F]=3$ 与 G 是交错群 A_3.*

• 如果 D 不是 F 里的平方，则 $[K:F]=6$ 与 G 是对称群 S_3.

x^3+3x+1 的判别式是 $-5\cdot 3^3$，不是一个平方，而 x^3-3x+1 的判别式是 3^4，是一个平方数(见 16.2.8). 这与上面例子讨论的一致.

定理 16.8.5 的证明 根的置换使 δ 乘上一个置换的符号. 如果 δ 属于 F，则它由 G 的每个元素所固定不动. 在这种情形里，奇置换不属于 G，所以，$G=A_3$，$[K:F]=3$. 如果 δ 不属于 F，则它不为 G 所固定不动，所以，G 含有奇置换. 在这种情形里，$G=S_3$，$[K:F]=6$. ■

交错群没有真子群. 所以，如果 $G=A_3$，则不存在真中间域. 这是显然的，因为 $[K:F]=3$ 是素数. 对称群 S_3 有 4 个真子群. 用通常的记号，它们是 3 个 2 阶群 $\langle y\rangle$，$\langle xy\rangle$，$\langle x^2y\rangle$ 与 3 阶群 $\langle x\rangle$，即为 A_3. 主要定理告诉我们当 $G=S_3$ 时，存在 4 个真中间域. 它们是 $F(\alpha_3)$，$F(\alpha_2)$，$F(\alpha_1)$ 与 $F(\delta)$.

第九节 四次方程

令 $f(x)$ 是系数属于 F 的既约 4 次多项式，且设 f 在 F 上的分裂域 K 里的根为 α_1，α_2，α_3，α_4. 由它在诸根上的作用，伽罗瓦群 $G=G(K/F)$ 可表示为 S_4 的一个可迁子群(16.6.6). 可迁子群容易确定，因为 S_4 同构于八面体群，该八面体群是一个旋转群. 任意子群也都是旋转群，所以，它将是定理 6.12.1 列出的群之一. S_4 的可迁子群为

【16.9.1】 $$S_4, A_4, D_4, C_4, D_2$$

有 3 个共轭子群同构于 D_4，而有 3 个共轭子群同构于 C_4. 子群 D_2 是克莱因四元群，由恒等元与不相交对换的 3 个积组成. 它是 S_4 的正规子群，以前我们见过这个群(2.5.15). (S_4 的一些其他子群同构于 D_2，但它们不是可迁的.)注意到 G 的阶等于次数 $[K:F]$，除最后两个外，它区分所有的群. 不幸的是，不容易确定次数.

我们从容易具体分析的 4 次多项式开始. 我是从 Suan Landau[Landau]那里学到这些
493 知识的.

【16.9.2】例 这里 F 表示有理数域 $\mathbf{Q}$.

(a) 令 α 是"嵌套"平方根 $\alpha=\sqrt{4+\sqrt{5}}$. 为确定 α 在 F 上的既约多项式，我们猜测它的根可能是 $\pm\alpha$ 与 $\pm\alpha'$，其中 $\alpha'=\sqrt{4-\sqrt{5}}$. 有了这个猜测，我们展开多项式

$$f(x)=(x-\alpha)(x+\alpha)(x-\alpha')(x+\alpha')=x^4-8x^2+11$$

不是很难证明这个多项式在 F 上是既约的. 我们将证明留作练习. 所以，它是 α 在 F 上的既约多项式. 令 K 是 f 的分裂域. 这样，

$$F\subset F(\alpha)\subset F(\alpha,\alpha'),\quad F(\alpha,\alpha')=K$$

因为 f 是既约的，故 $[F(\alpha):F]=4$，又因为 $\sqrt{5}$ 属于 $F(\alpha)$，故 $\alpha'=\sqrt{4-\sqrt{5}}$ 在 $F(\alpha)$ 上的次数至多为 2. 我们还不知道 α' 是否属于域 $F(\alpha)$. 在任一情形里，$[K:F]$ 是 4 或 8. K/F 的伽罗瓦群 G 也有阶 4 或 8，所以，它是 D_4，C_4 或 D_2.

D_4 的哪个共轭子群可作用依赖于如何对诸根排序. 让我们这样对它们排序:

$$\alpha_1 = \alpha, \quad \alpha_2 = \alpha', \quad \alpha_3 = -\alpha, \quad \alpha_4 = -\alpha'$$

在这样的排序下，映 $\alpha_1 \rightsquigarrow \alpha_i$ 的自同构也映 $\alpha_3 \rightsquigarrow -\alpha_i$. 具有这个性质的置换构成由

【16.9.3】 $$\sigma = (1\ 2\ 3\ 4) \quad 与 \quad \tau = (2\ 4)$$

生成的二面体群 D_4. 我们的伽罗瓦群是这个群的子群. 它可以是整个群 D_4，即由 σ 生成的循环群 C_4，或由 σ^2 与 τ 生成的二面体群 D_2.

注意 必须小心：这个群 D_4 的每个元素置换诸根，但我们还不知道这些置换里的哪一个来自 K 的自同构. 不是来自 K 的自同构的置换没有为我们提供关于 K 的任何信息.

有一个置换 $\rho=\sigma^2=(1\ 3)(2\ 4)$ 属于所有 3 个群 D_4, C_4 与 D_2. 于是，它扩展为 K 的 F-自同构，仍记为 ρ. 这个自同构生成 G 的 2 阶子群 N.

为计算固定域 K^N，我们寻找由 ρ 固定不动的根的表达式. 不难发现一些：$\alpha^2=4+\sqrt{5}$ 与 $\alpha\alpha'=\sqrt{11}$. 所以，K^N 含有域 $L=F(\sqrt{5}, \sqrt{11})$. 检查域链 $F\subset L\subset K^N\subset K$. 我们有 $[K:F]\leqslant 8$，$[L:F]=4$ 与 $[K:K^N]=2$(固定域定理). 于是得 $L=K^N$，$[K:F]=8$ 以及 G 是二面体群 D_4.

(b) 令 $\alpha=\sqrt{2+\sqrt{2}}$. α 在 F 上的既约多项式是 x^4-4x^2+2. 同以前一样，它的根是 α，$\alpha'=\sqrt{2-\sqrt{2}}$，$-\alpha$，$-\alpha'$. 这里 $\alpha\alpha'=\sqrt{2}$，属于域 $F(\alpha)$. 所以，α' 也属于这个域. 次数 $[K:F]$ 为 4，且 G 或为 C_4，或为 D_2.

因为 G 在诸根上的作用是可迁的，故存在 G 的元素 σ' 映 $\alpha \rightsquigarrow \alpha'$. 因为 $\alpha^2=2+\sqrt{2}$ 与 $\alpha'^2=2-\sqrt{2}$，故 σ' 映 $\sqrt{2}\rightsquigarrow -\sqrt{2}$ 以及 $\alpha\alpha' \rightsquigarrow -\alpha\alpha'$. 这蕴含着 $\alpha' \rightsquigarrow -\alpha$. 所以，$\sigma'=\sigma$. 伽罗瓦群 494
是循环群 C_4.

(c) 令 $\alpha=\sqrt{4+\sqrt{7}}$. 它在 F 上的既约多项式是 x^4-8x^2+9. 这里 $\alpha\alpha'=3$. 而且，α' 属于域 $F(\alpha)$，且次数 $[K:F]$ 为 4. 如果自同构 σ' 映 $\alpha \rightsquigarrow \alpha'$，则因为 $\alpha\alpha'=3$，故它一定映 $\alpha' \rightsquigarrow \alpha$. 伽罗瓦群是 D_2.

可用这种方法分析形如 x^4+bx^2+c 的任一个 4 次多项式. ■

分析一般多项式

【16.9.4】 $$f(x) = x^4 - a_1x^3 + a_2x^2 - a_3x + a_4$$

是比较困难的，因为它的根 α_1，…，α_4 很难用通常方法具体写出来. 主要方法是寻找由 S_4 里的一些置换(不是全部置换)所固定不动的根的表示式. 判别式 D 的平方根首先是这样的表示式:

$$\delta = \prod_{i<j}(\alpha_i - \alpha_j) = (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_1-\alpha_4)(\alpha_2-\alpha_3)(\alpha_2-\alpha_4)(\alpha_3-\alpha_4)$$

因为诸根是不同的，故 δ 不为零. 如同三次方程一样(16.8.4)，根的置换 σ 使 δ 乘上一个置换的符号. 偶置换固定 δ 不动，而奇置换不固定 δ 不动.

【16.9.5】命题 令 G 是既约 4 次多项式 f 的伽罗瓦群. f 的判别式 D 是 F 里的一个平方

数当且仅当 G 不含有奇置换. 所以,

- 如果 D 是 F 里的一个平方数, 则 G 是 A_4 或 D_2.
- 如果不 D 是 F 里的一个平方数, 则 G 是 S_4, D_4 或 C_4.

证明 D 是 F 里的一个平方数当且仅当 δ 属于 F, 当 G 的每个元素固定 δ 不动时这种情形发生. 固定 δ 不动的置换是偶置换. 后面的叙述可通过查看 S_4 的可迁子群列表(16.9.1)得证. ■

对任意次数多项式的分裂域有类似叙述.

【16.9.6】命题 *令 K 是 $F[x]$ 里 n 次既约多项式 f 在 F 上的分裂域, 且设 D 是 f 的判别式. 伽罗瓦群 $G(K/F)$ 是交错群 A_n 的子群当且仅当 D 是 F 里的一个平方数.*

拉格朗日发现诸根 α_i 的另一个有用的表示式, 它是相对于 4 次多项式的一个特殊表示式. 令

【16.9.7】
$$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \quad \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \quad \beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$$

且设

495
$$g(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3)$$

这个多项式称为 f 的三次预解式. 诸根 α_i 的每个置换置换元素 β_j, 所以 g 的系数是根里的对称函数. 它们是 F 的元素, 需要时可以计算出来.

幸运的是, 既约 4 次多项式的根互不相同的事实蕴含着诸元素 β_i 互不相同. 例如,

$$\beta_1 - \beta_2 = \alpha_1\alpha_2 + \alpha_3\alpha_4 - \alpha_1\alpha_3 - \alpha_2\alpha_4 = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)$$

因为诸 α_v 是不同的, 故 $\beta_1 - \beta_2$ 不为零. 多项式 f 与 g 的判别式实际上是相等的.

三次预解式在 F 中是否有根给出了有关伽罗瓦群 G 的许多信息.

【16.9.8】命题 *令 G 是既约 4 次多项式 f 在 F 上的伽罗瓦群, 且设 g 是 f 的三次预解式. 则 g 是既约的当且仅当 G 的阶为 3 整除. 而且,*

- *如果 g 在 F 里完全分裂, 则 $G=D_2$.*
- *如果 g 在 F 里有一个根, 则 $G=D_4$ 或 C_4.*
- *如果 g 在 F 上是既约的, 则 $G=S_4$ 或 A_4.*

证明 命题的证明是简单的, 但三个元素 β_i 是不同的事实为容易忽略的关键点. 令 B 表示集合 $\{\beta_1, \beta_2, \beta_3\}$. 它的阶为 3. 对称群 S_4 在诸根 α_v 上的作用定义了在 B 上的可迁作用, 且伴随置换表示是同态 $\varphi: S_4 \to S_3$, 这我们在前面已经见过(2.5.13). 它的核是子群 D_2. 如果 g 在 F 里完全分裂, 则伽罗瓦群平凡地作用在 B 上, 所以, $G=D_2$.

如果 g 在 F 上是既约的, 则 G 可迁地作用在 B 上(16.6.6), 于是, 它的阶为 3 整除. 反过来, 如果 $|G|$ 为 3 所整除, 则 G 含有 3 阶元素, 比如说, ρ. 因为 φ 的核是 D_2, 故 ρ 不是平凡地作用在 B 上. 它循环地置换三个元素. 所以, G 可迁地作用在 B 上, 且 g 是既约的.

命题的剩下部分可通过回看列表(16.9.1)得证. ■

因此, 多项式 $x^2 - D$(这里 D 是判别式)与三次预解式 $g(x)$ 就差不多足以描述伽罗瓦群了. 结果总结在下表中:

【16.9.9】

	D是平方数	D非平方数
g 可约	$G=D_2$	$G=D_4$ 或 C_4
g 既约	$G=A_4$	$G=S_4$

不幸的是，没有根的简单表示式去除余下的歧义性(见练习 M.11).

注意 命题 16.9.8 的证明根据诸根 α_v 的置换利用特别公式(16.9.7)定义集合 B 的置换. 如果诸根的置换来自 F-自同构，则 B 的置换由这个自同构给出. 然而，如果置换不是来自 F-自同构，则用这个公式所定义的 B 的置换对域没有意义. 496

例如，令 K 是多项式 X^4-2 在 $\mathbf{Q}$ 上的分裂域. 从 1 到 4 把诸根排序为 $\alpha_1=\alpha$，$\alpha_2=i\alpha$，$\alpha_3=-\alpha$，$\alpha_4=-i\alpha$，其中 α 是 2 的 4 次正实根. 这样，$\beta_1=2i\sqrt{2}$，$\beta_2=0$，$\beta_3=-2i\sqrt{2}$. 对换 $\epsilon=(1\ 2)$不是伽罗瓦群的元素. 当我们使用公式 16.9.7 定义 ϵ 如何置换集合 B 时，所得的作用使 β_2 与 β_3 互换. 因为 $\beta_2=0$ 且 $\beta_3\neq 0$，所以这个置换在代数上没有意义.

第十节 单 位 根

在本节中，F 表示有理数域 $\mathbf{Q}$. 在 F 上由 n 次单位根 $\zeta_n=e^{2\pi i/n}$ 生成的复数子域叫做分圆域. 假设 n 是素整数 p. $\zeta=e^{2\pi i/p}$在有理数域上的既约多项式是

【16.10.1】
$$f(x)=x^{p-1}+\cdots+x+1$$

(定理 12.4.9). 它的根是幂 ζ，ζ^2，…，ζ^{p-1}，于是，ζ 生成 f 的分裂域. 所以，$K=F(\zeta)$ 是次数为 $p-1$ 的 F 的伽罗瓦扩张.

【16.10.2】命题

(a) 令 p 是素数，且设 $\zeta=e^{2\pi i/p}$. 则 $\mathbf{Q}(\zeta)$在 $\mathbf{Q}$ 上的伽罗瓦群是 $p-1$ 阶循环群. 它同构于素域 $\mathbf{F}_p$ 的非零元素的乘法群 $\mathbf{F}_p^\times$.

(b) 对于 $\mathbf{C}$ 的任意子域 F'，$F'(\zeta)$在 F'上的伽罗瓦群是循环群.

证明

(a) 设 $F=\mathbf{Q}$，令 G 是 $F(\zeta)$在 F 上的伽罗瓦群. G 的元素 σ 由像 $\delta(\zeta)$确定，而$\delta(\zeta)$可以是 f 的 $p-1$ 个根里的任一个. 称 σ_i 为使得 $\sigma(\zeta)=\zeta^i$的元素. 幂指数 i 确定为模 p 的非零剩余类，这是因为 $\zeta^p=1$. 于是，映射 $\sigma_i\rightsquigarrow i$ 定义了双射 $\epsilon:G\to\mathbf{F}_p^\times$. 计算

$$\sigma_i\sigma_j(\zeta)=\sigma_i(\zeta^j)=\sigma_i(\zeta)^j=\zeta^{ij}$$

表明 ϵ 是同态，所以，它是同构. $\mathbf{F}_p^\times$ 是循环的事实是定理 15.7.3 的一部分.

映 $\zeta\rightsquigarrow\zeta^v$ 的元素 σ_v 生成 G 当且仅当 v 是模 p 本原根，它是循环群 $\mathbf{F}_p^\times$ 的生成元.

(b) 伽罗瓦群 $G'=G(F'(\zeta)/F')$的元素 σ 也映 ζ 到幂 ζ^v. 上面的证明表明 G'同构于循环群 $\mathbf{F}_p^\times$ 的子群. 所以，它也是循环群. ■

【16.10.3】例 $p=17$ 与 $\zeta=e^{i\theta}$，其中 $\theta=2\pi/17$.

3 的剩余是模 17 本原根，于是，伽罗瓦群 $G=G(K/F)$是 16 阶循环群，由映$\zeta\rightsquigarrow\zeta^3$的自同构 σ 生成. 有 5 个分别由 σ，σ^2，σ^4，σ^8 与 1 生成的阶为 16，8，4，2 与 1 的子群. 令 497 这些子群的固定域为 $F=L_0=K^{(\sigma)}$，$L_1=K^{(\sigma^2)}$，$L_2=K^{(\sigma^4)}$，$L_3=K^{(\sigma^8)}$，$L_4=K$. 它们构成

域链 $L_0\subset L_1\subset L_2\subset L_3\subset L_4$，其中每个扩张 L_i/l_{i-1} 的次数是 2. 主要定理告诉我们这些是仅有的中间域. ■

【16.10.4】引理 上面定义的域 L_3 由 $\cos\theta$ 生成，它在 F 上的次数是 8.

证明 令 $L'=F(\cos\theta)$. 因为 $\zeta+\zeta^{-1}=2\cos\theta$，故 $\cos\theta$ 属于 $K=F(\zeta)$. 而且，ζ 是系数属于 L' 的二次多项式 $(x-\zeta)(x-\zeta^{-1})=x^2-2(\cos\theta)x+1$ 的根，于是，$[K:L']\leqslant 2$，$[L':F]\geqslant 8$. 所以，L' 或是 L_3，或是 K. 又因为 L' 是 $\mathbf{R}$ 的子域，而 K 不是，故 $L'=L_3$. ■

【16.10.5】推论 正 17 边形可用直尺和圆规作图.

证明 链 $F\subset L_1\subset L_2\subset L_3$ 表明我们可通过一系列添加 3 个连续平方根到达含有 $\cos\theta$ 的域 L_3，又因为 L_3 是 $\mathbf{R}$ 的子域，故这些平方根是实的. (见(15.5.10).) ■

下面的引理对于描述 F 的二次扩张 L_1 是有用的：

【16.10.6】引理 令 $\alpha=c_1\zeta+c_2\zeta^2+\cdots+c_{p-2}\zeta^{p-2}+c_{p-1}\zeta^{p-1}$ 是具有有理系数 c_i 的线性组合，其中 $\zeta=e^{2\pi i/p}$ 且 p 是素数. 如果 α 是有理数，则 $c_1=c_2=\cdots=c_{p-1}$，且 $\alpha=-c_1$.

证明 因为 ζ 是 f 的根(16.10.1)，故我们可解出 ζ^{p-1}，且重新把给定的线性组合写为 $\alpha=(-c_{p-1})1+(c_1-c_{p-1})\zeta+\cdots+(c_{p-2}-c_{p-1})\zeta^{p-2}$. 因为幂 1，$\zeta$，…，$\zeta^{p-2}$ 构成 K 在 F 上的一组基，故这个组合是有理数仅当除 $-c_{p-1}$ 外所有系数等于零. 如果是这样，则 $c_i=c_{p-1}$ 对每个 i 成立，且 $\alpha=-c_1$，如所断言的. ■

【16.10.7】例 继续 $p=17$ 的情形.

本原根 3 模 17 的幂和取自 -8 和 8 之间的同余类的代表元按序列出如下：

【16.10.8】 $$1,3,-8,-7,-4,5,-2,-6,-1,-3,8,7,4,-5,2,6$$

$K=F(\zeta)$ 的映 ζ 到 ζ^3 的自同构 σ 生成伽罗瓦群 G，且它在对应的顺序中遍历 ζ 的幂：

【16.10.9】 $$\zeta\rightsquigarrow\zeta^3\rightsquigarrow\zeta^{-8}\rightsquigarrow\zeta^{-7}\rightsquigarrow\cdots$$

ζ 的 G-轨道由不同于 1 的 ζ 的 16 个幂组成.

令 H 表示 8 阶子群 $\langle\sigma^2\rangle$. ζ 的 G-轨道分裂成两个 H-轨道，这是通过在幂序列中隔一项取一项得到的(16.10.9)：

$$\{\zeta,\zeta^{-8},\zeta^{-4},\cdots\}\quad 与\quad \{\zeta^3,\zeta^{-7},\zeta^5,\cdots\}$$

令 α_1 与 α_2 分别表示这两个轨道上的和：$\alpha_1=\zeta+\zeta^{-8}+\cdots$. 集合 $\{\alpha_1,\alpha_2\}$ 是 G-轨道. 定理 498 16.5.2 告诉我们元素 α_i 在 G 的固定域 F 上有次数 2，且 α_i 在 F 上的既约多项式为 $(x-\alpha_1)(x-\alpha_2)$. 要确定这个多项式，我们需要计算两个对称函数 $s_1(\alpha)=\alpha_1+\alpha_2$ 与 $s_2(\alpha)=\alpha_1\alpha_2$.

首先，我们注意到 $s_1(\alpha)$ 是不同于 1 的 ζ 的所有幂的和，所以，$s_1(\alpha)=-1$(16.10.6). 其次，

$$s_2(\alpha)=\alpha_1\alpha_2=(\zeta+\zeta^{-8}+\cdots)(\zeta^3+\zeta^{-7}+\cdots)$$

写 α_i 需要多次写 ζ，所以，我们用速记符号. 我们写

【16.10.10】 $\alpha_1=[1,-8,-4,-2,-1,8,4,2],\alpha_2=[3,-7,5,-6,-3,7,-5,6]$

这个记号表示 α_1 是 ζ 的幂的和，而幂指数在第一个括号的数字串里. 为计算 $s_2(\alpha)$，我们必须把第一个括号里八个数的每一个加到第二个括号里的每个数字上，再模 p，得到 64 个

幂指数. 这样，$s_2(\alpha)$是ζ对应幂的和. 我们不具体这样做. 因为$s_2(\alpha)$是有理数，故不同于$\zeta^0=1$的所有幂一定出现同样多次(16.10.6). 我们注意到当做加法时得不到任何零值，因为剩余和它的负值在同一括号的数字序列里. 所以，64项一定包含16个非零项里每一项4次. 所以，$s_2(\alpha)=-4$. α_i在F上的既约多项式是

【16.10.11】 $$(x-\alpha_1)(x-\alpha_2)=x^2+x-4$$

它的判别式是17，所以，$L_1=F(\sqrt{17})$. ■

对任意奇素数p以同样方法可确定F上次数为2且包含在分圆域$F(\zeta_p)$里的扩域.

【16.10.12】**定理** *令p是不同于2的素数，且设L是$\mathbf{Q}$的包含于分圆域$\mathbf{Q}(\zeta_p)$里的唯一二次扩域. 如果$p\equiv1(\mathrm{mod}\ 4)$，则$L=\mathbf{Q}(\sqrt{p})$；如果$p\equiv3(\mathrm{mod}\ 4)$，则$L=\mathbf{Q}(\sqrt{-p})$.*

这似乎是“用例子证明”的情形. 情形$p\equiv1(\mathrm{mod}\ 4)$由素数17例证了，而计算对于任一个这样的素数都是类似的. 我们通过素数11来说明情形$p\equiv3(\mathrm{mod}\ 4)$. 2的剩余是模11本原根. 它的幂把模11的非零剩余类以如下顺序列出：

$$1,2,4,-3,5,-1,-2,-4,3,-5$$

令$\zeta=\zeta_{11}$，且设σ是映$\zeta\rightsquigarrow\zeta^2$的自同构. 用像上面那样的速记符号，$\sigma^2$的轨道和是

$$\alpha_1=[1,4,5,-2,3],\quad \alpha_2=[2,-k,-1,-4,-5]$$

这里如果k属于和α_1的幂指数列，则$-k$属于α_2幂指数列. 所以，零在$\alpha_1\alpha_2$的幂指数列的25项里出现5次，这为$\alpha_1\alpha_2$的值贡献数5. 因为$\alpha_1\alpha_2$属于$\mathbf{Q}$，故20个余项一定由10个模11非零同余类中每项重复两次所构成. 这些项的和是-2. 所以，$\alpha_1\alpha_2=3$. α_i的既约多项式是x^2+x+3. 它的判别式为-11. 499

定理16.10.12是代数数论漂亮定理的一个特殊情形.

【16.10.13】**定理**(Kronecker-Weber定理) *每个有理数域$\mathbf{Q}$上伽罗瓦群是阿贝尔的伽罗瓦扩张包含于某个分圆域$\mathbf{Q}(\zeta_n)$中.*

第十一节 库默尔扩张

本节讨论下面的定理.

【16.11.1】**定理** *令F是$\mathbf{C}$的含有p次单位根$\zeta=e^{2\pi i/p}$的子域，其中p为素数，且设K/F是p次伽罗瓦扩张，则K由添加一个p次根得到. 换句话说，K是由F上的元素β生成的，其中$\beta^p\in F$.*

这种类型的扩张常称为库默尔扩张. 库默尔扩张的伽罗瓦群是素数阶循环群.

定理对$p=2$是熟悉的：每个2次扩张可由添加一个平方根得到. 假设$p=3$，且设F含有3次单位根$\omega=e^{2\pi i/3}$. 如果既约3次多项式f的判别式(16.2.7)是F里的一个平方项，则f的分裂域的次数为3(16.8.5). 定理断言分裂域有形式$F(\sqrt[3]{b})$，其中某个$b\in F$. 这不是显然的. 如果判别式不是平方项，则诸根不能由添加一个立方根得到(这是练习11.1).

下一个命题完善了叙述. 假设β是F的非零元素b在扩域K里的p次根. 这样，它是

多项式 $g(x)=x^p-b$ 的根，且如果 $f\in F$，则 f 在 K 里的根是 $\zeta^v\beta$，$v=0,1,\cdots,p-1$. 所以，β 生成 g 在 F 上的分裂域.

【16.11.2】命题 令 p 是素数，设 F 是含有 p 次单位根 $\zeta=e^{2\pi i/p}$ 的域，且设 b 是 F 的非零元素，则多项式 $g(x)=x^p-b$ 或者在 F 上是既约的，或者它完全分裂.

证明 令 K 是 g 在 F 上的分裂域，假设 g 的某个根 β 不属于 F. 则次数 $[K:F]$ 将比 1 大，于是，伽罗瓦群 $G=G(K/F)$ 将含有不同于恒等元的元素. 因为 β 在 F 上生成 K，故 $\sigma(\beta)$ 不能等于 β. 于是，$\sigma(\beta)=\zeta^v\beta$ 对某个 v，$0<v<p$ 成立. 我们还有 $\sigma(\zeta)=\zeta$. 所以，$\sigma^2(\beta)=\zeta^v(\zeta^v\beta)=\zeta^{2v}\beta$，且一般地，有 $\sigma^k(\beta)=\zeta^{kv}\beta$. 因为 $0<v<p$ 且 p 是素数，故 v 的倍数遍历所有模 p 剩余. 这表明 G 可迁地作用在 g 的 p 个根上. 所以，g 在 F 上是既约的. ■

定理 16.11.1 的证明 证明很漂亮. 将 K 视为 F 上的向量空间，我们证明伽罗瓦群 G 的元素 σ 是 K 上的线性算子. 如果 α 与 β 属于 K 且 c 属于 F，则 $\sigma(c)=c$. 因为 σ 是自同构，故

$$\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta),\quad \sigma(c\alpha)=\sigma(c)\sigma(\alpha)=c\sigma(\alpha)$$

选取循环伽罗瓦群 G 的生成元 σ. 这样，$\sigma^p=1$，于是，σ 的任一特征值 λ 满足关系 $\lambda^p=1$，这意味着 λ 是 ζ 的幂. 由假设，这些特征值属于域 F. 而且，p 阶线性算子至少有一个不同于 1 的特征值. 这是因为在复数域上 σ 的矩阵是可对角化的(见定理 4.7.1 或推论 (10.3.9)). 它的特征值是对应于对角矩阵 Λ 的元素. 如果 σ 不是恒等元，则 $\Lambda\neq I$，所以，某个对角元一定不同于 1.

500

令 β 是 σ 的伴随于特征值 $\lambda\neq1$ 的特征向量，且设 $b=\beta^p$. 则 $\sigma(\beta)=\lambda\beta$. 因此，$\sigma(b)=(\lambda\beta)^p=b$. 因为 σ 生成 G，故 b 属于固定域 F，而 β 不属于 F. 因为 $[K:F]$ 是素数，故 $F(\beta)=K$. ■

利用如同定理 16.11.1 中的记号，比如说，K 是 p 次既约多项式 f 在 F 上的分裂域. f 的根有简单表示式，这个表示式常给出算子 σ 的特征向量. 由 σ 定义的 f 诸根 $\alpha_1,\cdots,\alpha_p$ 的置换是循环的，所以，如果我们适当给诸根标号，σ 将是置换 $(\mathbf{12}\cdots\boldsymbol{p})$. 令 λ 是 σ 的特征值，且设

【16.11.3】
$$\beta=\alpha_1+\lambda\alpha_2+\cdots+\lambda^{p-1}\alpha_p$$

这样，$\sigma(\beta)=\alpha_2+\lambda\alpha_3\cdots+\lambda^{p-2}\alpha_{p-1}+\lambda^{p-1}\alpha_1=\lambda^{-1}\beta$. 所以，除非 β 恰好是零，否则它是伴随于特征值 λ^{-1} 的特征向量.

【16.11.4】例 库默尔定理引出三次多项式的一个求根公式，该公式于 16 世纪为卡尔达诺(Cardano)与塔尔塔利亚(Tartaglia)所发现. 我们这里给出的大概推证不像卡尔达诺给出的那样短，但容易记住，因为它是系统的. 假设三次多项式的二次项系数为零，为避免解里出现分母，将其写为

$$f(x)=x^3+3px+2q$$

这样，$s_1=0$，$s_2=3p$，$s_3=-2q$，且判别式为 $D=-2^2\,3^3(q^2+p^3)$.

令诸根为 u_1，u_2，u_3，任意排序. 设 $\omega=e^{2\pi i/3}$，元素

$$z = u_1 + \omega u_2 + \omega^2 u_3 \text{ 与 } z' = u_1 + \omega^2 u_2 + \omega u_3$$

是循环置换 $\sigma=(1\ 2\ 3)$的特征向量. 因为 $1+\omega+\omega^2=0$，故

$$z + z' = s_1 + z + z' = u_1$$

立方 z^3 与 z'^3 为 σ 所固定不动，于是，根据库默尔定理与定理 16.8.5，它们可用 p，q，$\delta=\sqrt{D}$与 ω 写出来. 当以这种方式写出立方时，$u_1=z+z'$将表示为立方根的和.

做下列计算. 令

$$A = u_1^2 u_2 + u_2^2 u_3 + u_3^2 u_1$$
$$B = u_2^2 u_1 + u_3^2 u_2 + u_1^2 u_3$$

则

$$A - B = (u_1 - u_2)(u_1 - u_3)(u_2 - u_3) = \delta,$$
$$A + B = s_1 s_2 - 3s_3 = 6q$$

还有，$u_1^3+u_2^3+u_3^3=u_1^3+3s_1s_2+3s_3=-6q$.

求解 A，B，展开 z^3 与 z'^3. 这个计算的结果是卡尔达诺公式：

【16.11.5】
$$u_1 = \sqrt[3]{-q+\sqrt{q^2+p^3}} + \sqrt[3]{-q-\sqrt{q^2+p^3}}$$

例如，如果 $f(x)=x^3+3x+2$，则 $x=\sqrt[3]{-1+\sqrt{2}}-\sqrt[3]{-1-\sqrt{2}}$. 501

然而，公式是模棱两可的. 在项$\sqrt[3]{-q+\sqrt{q^2+p^3}}$中，平方根可取两个值，且当平方根被选取时，立方根有 3 个可能的值，这样就给出 6 个值. 另一项也有 6 个值. 但 f 仅有 3 个根. ■

第十二节 五次方程

伽罗瓦工作背后的主要动机是解五次方程. 稍早些时候，阿贝尔已经证明具有变量系数 a_i 的五次方程

【16.12.1】
$$x^5 - a_1 x^4 + a_2 x^3 - a_3 x^2 + a_4 x - a_5 = 0$$

不能用根式求解，但不知道不能求解这整系数方程. 无论如何，这个问题已有 200 年的历史，它一直令人感兴趣. 同时，伽罗瓦的思想实际上比激发出这些思想的问题要重要得多. 令人惊讶的是，伽罗瓦能够在发展群理论之前做了他所做的.

【16.12.2】命题 *令 F 是复数域的子域. 关于复数 α 的下列两个条件是等价的，且 α 称为在 F 上是可解的，如果它满足这两个条件之一：*

(a) *存在 $\mathbf{C}$ 的子域链 $F=F_0\subset F_1\subset\cdots\subset F_r=K$ 使得 α 属于 K，且*

- *对于 $j=1$，…，r，$F_j=F_{j-1}(\beta_j)$，其中 β_j 的幂属于 F_{j-1}.*

(b) *存在 $\mathbf{C}$ 的子域链 $F=F_0\subset F_1\subset\cdots\subset F_r=K$ 使得 α 属于 K，且*

- *对于 $j=1$，…，r，F_{j+1}是 F_j 的素数次的伽罗瓦扩张.*

命题的证明是不困难的，但它没有多少内在的意思，所以，我们把它推迟到了本节末. 为能够使用伽罗瓦理论，我们需要条件(b). 它是非常重要的可解性刻画，且通过接

受它作为定义可避免命题的技巧性.

条件(a)意味着 F_j 是由对某个整数 n(依赖于 j)的 n 次根在 F_{j-1} 上生成的. 这类似于由尺规作出的实数的描述. 在那个描述里，仅允许正实数的平方根. 理论上，用一系列嵌套根拆解扩张可以写出可解元素 α. 但就像三次方程的卡尔达诺公式一样，在涉及根式的公式里有大量模棱两可的情形，因为 n 次根有 n 个选择. 在复杂的根式表示式里具体写出一个根是没有用的. 的确，卡尔达诺公式是无用的.

【16.12.3】命题 *如果 α 是系数在域 F 里次数至多为 4 的多项式的根，则 α 在 F 上是可解的.*

证明 对于二次多项式，二次公式证明了这个结论. 对于三次多项式，卡尔达诺公式 16.11.7 给出了解答. 如果 $f(x)$是四次的，我们从添加 D 的平方根 δ 开始. 这样，我
502 们用卡尔达诺公式求解三次预解式 $g(x)$的根，并且添加它. 在这一点上，表 16.9.9 表明 f 在我们所得的域上的伽罗瓦群是克莱因四元群的子群. 所以，f 可由至多两个平方根扩张解出. ■

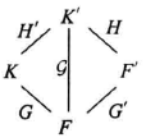
【16.12.4】定理 *令 f 是复数域的子域 F 上的 5 次既约多项式，其伽罗瓦群 G 或是交错群 A_5，或是对称群 S_5，则 f 的根在 F 上是不可解的.*

证明 如果 $G=S_5$，我们用二次扩域 $F(\delta)$替换 F，其中 δ 是判别式的平方根. 如果在 F 上能够求解，则在较大域 $F(\delta)$上也能求解. 所以，可假设 G 是交错群 A_5，它是一个单群(7.5.4).

策略如下：考虑素数次数 p 的伽罗瓦扩张 F'/F，带有伽罗瓦群，该群是 p 阶循环群，我们证明当用 F'替换 F 时，对于求解方程 $f=0$ 没有进展. 我们通过证明 f 在 F' 上的伽罗瓦群仍是交错群 A_5 来求解. 因为 A_5 含有 5 阶元素，故它不可能是 5 次可约多项式的伽罗瓦群. 所以，f 在 F' 上仍是既约的. 因此，没有(16.12.2)(b)类型的链，且 f 的根是不可解的.

我们选取这样的扩域 F'，于是，我们有两个伽罗瓦扩张. 首先，K/F 是 5 次多项式 f 在 F 上的分裂域. 它的伽罗瓦群是 $G=A_5$. 其次，F'/F 有 p 阶循环伽罗瓦群 G'. 因为它是伽罗瓦扩张，故它是某个既约多项式 g 在 F 上的分裂域.

令 K'是多项式积 fg 在 F 上的分裂域. 它分别由 f 与 g 的复根α_1，…，α_5 与 β_1，…，β_p 所生成. 诸根 α_i 生成 f 的分裂域 K，而诸根 β_j 生成 g 的分裂域 F'. 四个域间的包含关系在下面的图里显示出来. 每个扩域都是伽罗瓦扩张，且伽罗瓦群在图里也标了出来.



因为 K 是 F 的伽罗瓦扩张，故 G 同构于商群$\mathcal{G}/H'$. 因为 F'是 F 的伽罗瓦扩张，故 G' 同构于商群$\mathcal{G}/H$(16.7.5). 我们要证明 H 同构于G，亦即 H 是交错群 A_5.

群 H'由 K'的固定诸根 α_i 不动的 F-自同构组成，且 H 由固定诸根 β_j 不动的 F-自同构组成. 如果 K'的 F-自同构固定诸根 α_i 与 β_j 不动，则因为这些根生成 K'，故它是恒等的.

所以，$H\cap H'$是平凡群.

我们限制典型映射$\mathcal{G}\to\mathcal{G}/H\approx G'$到子群 H'. 这个限制的核是平凡群 $H\cap H'$，所以，限制是单射. 它同构地映射 H'到 G'的子群. 由假设，G'是阶为素数 p 的循环群. 所以，仅存在两种可能性：或者 H'是平凡群，或者 H'是 p 阶循环群.

503

情形 1：H'是平凡群. 则从$\mathcal{G}$到商群$\mathcal{G}/H'\approx G$ 的满射是同构，且$\mathcal{G}$同构于单群 $G=A_5$. 这使得从$\mathcal{G}$到循环商群$\mathcal{G}/H'\approx G$ 的满射的存在成为可能. 所以，将这个情形排除掉.

情形 2：H'是 p 阶循环群. 则$|\mathcal{G}|=|G|\,|H'|=p|G|$，且还有$|\mathcal{G}|=|G'|\,|H|=p|H|$. 所以，$G$ 与 H 有相同的阶 60. 我们限制典范映射$\mathcal{G}\to\mathcal{G}/H'\approx G$ 到子群 H. 这个限制的核是平凡群 $H\cap H'$，所以，限制是单射. 它同构地映射 H 到 G 的子群. 因为两个群的阶均为 60，故限制是同构，且 $H\approx G=A_5$. ■

我们现在展示 $\mathbf{Q}$ 上 5 次既约多项式，其伽罗瓦群是 S_5. 5 为素整数和伽罗瓦群 G 可迁地作用在诸根 α_1，…，α_5 上的事实限制了可能的伽罗瓦群. 因为作用是可迁的，故 $|G|$ 为 5 所整除. 因此，G 含有 5 阶元素. S_5 中唯一的 5 阶元素是 5-循环. 我们把下一个引理留作练习.

【16.12.5】引理 *如果 S_5 的子群 G 含有 5-循环与对换，则 $G=S_5$.*

【16.12.6】推论 *令 $f(x)$是 $\mathbf{Q}$ 上 5 次既约多项式. 如果 f 恰有 3 个实根，则它的伽罗瓦群 G 是对称群，从而它的根是不可解的.*

证明 令诸根为 α_1，…，α_5，其中 α_1，α_2，α_3 是实根，α_4，α_5 是虚根，且设 K 是 f 的分裂域. 固定前 3 个根不动的根的唯一置换是恒等与对换(**4 5**). 因为 $F(\alpha_1,\alpha_2,\alpha_3)\neq K$，故对换一定属于 G. 因为 G 可迁地作用在诸根上，故它含有一个 5 阶元素，即 5-循环. 所以，$G=S_5$. ■

【16.12.7】例 多项式 $x^5-16x=x(x^2-4)(x^2+4)$有 3 个实根. 当然，它是既约的，但我们可添加一个小的常数而不改变实根的个数. 这可通过观察多项式的图形看到. 例如，$x^5-16x+2$也有 3 个实根，且它在 $\mathbf{Q}$ 上是既约的. 它的根在 $\mathbf{Q}$ 上是不可解的. ■

我们现在证明命题 16.12.2.

【16.12.8】引理 *令 K/F 是伽罗瓦扩张，其伽罗瓦群 G 是阿贝尔的，则存在中间域链 $F=F_0\subset F_1\subset\cdots F_m=K$ 使得 F_i/F_{i-1} 对每个 i 是素数次的伽罗瓦扩张.*

证明 阿贝尔群 G 含有素数阶子群 H. 这个子群对应于一个中间域 L，且 K 是 L 的带有群 H 的伽罗瓦扩张. 因为 G 是阿贝尔的，故 H 是正规子群，所以，L 是 F 的带有阿贝尔伽罗瓦群$\widetilde{G}=G/H$ 的伽罗瓦扩张. 因为$\widetilde{G}$的阶比 G 的小，故归纳法完成证明. ■

命题 16.12.2 的证明 (a)⇒(b) 从域链(a)开始，我们添加更多的扩张和域到这个链以得到具有性质(b)的链. 首先，因为$\sqrt[n]{a}=\sqrt[r]{\sqrt[t]{a}}$，故我们以添加中间域的代价假设出现在链里的根是 p 次根，其中 p 为不同素数. 注意出现的素数 p_1，…，p_k，我们把这个链先暂时放在一旁.

504

回到域 F，首先，一个接着一个地添加 p_v 次单位根，$v=1$，…，k. 每个这样的扩张是伽罗瓦扩张，带有循环伽罗瓦群(命题 16.10.2(b))．引理 16.12.8 表明它们均含有链，其层是素数次的伽罗瓦扩张.

令 F' 是我们得到的域. 继续添加根到 F'. 由库默尔理论，每添加一个这样的根将得到一个带有素数阶循环伽罗瓦群的伽罗瓦扩张，除非它是平凡扩张. 我们得到的在新链末端的域 K' 包含有开始时所给的链中最后一个域 K，所以，α 将是 K' 的元素. 因此，这个新链是形如(b)的链.

(b)⇒(a) 假设给定(b)链，考虑这个链里的一个扩张，比如说，$F_{i-1}\subset F_i$. 它是素数次 p 的伽罗瓦扩张. 定理 16.11.1 表明倘若 p 次单位根属于 F_{i-1}，那么这个扩张由添加一个 p 次根得到. 所以，从添加所需要的 p 次单位根到 F 开始，我们扩大链. 扩大的链满足条件(a). ■

我们提出的解后来没有推出任何结果.

——Evariste Galois

练　习

第一节　对称函数

1.1 确定下列多项式的轨道. 如果多项式是对称的，则用初等对称函数把它写出来.

(a) $u_1^2u_2+u_2^2u_3+u_3^2u_1$　$(n=3)$

(b) $(u_1+u_2)(u_2+u_3)(u_1+u_3)$　$(n=3)$

(c) $(u_1-u_2)(u_2-u_3)(u_1-u_3)$　$(n=3)$

(d) $u_1^3u_2+u_2^3u_3+u_3^3u_1-u_1u_2^3-u_2u_3^3-u_3u_1^3$　$(n=3)$

(e) $u_1^3+u_2^3+\cdots+u_n^3$

1.2 求对称多项式环作为环 R 上模的两个基.

*1.3 令 $w_k=u_1^k+\cdots+u_n^k$.

(a) 证明牛顿恒等式：$w_k-s_1w_{k-1}+\cdots\pm s_{k-1}w_1\mp ks_k=0$.

505 (b) w_1，…，w_n 生成对称函数环吗？

第二节　判别式

2.1 证明判别式是对称函数.

2.2 (a) 证明实三次多项式的判别式是非负的当且仅当三次多项式有三个实根.

(b) 假设实四次多项式有正判别式. 关于实根个数有什么结论？

2.3 (a) 证明 Tschirnhausen 替换(16.2.6)不改变三次多项式的判别式.

(b) 确定(16.2.7)中从一般三次多项式(16.2.4)通过 Tschirnhausen 替换得到的系数 p 与 q.

2.4 用待定系数确定多项式的判别式.

(a) x^3+px+q　(b) x^4+px+q　(c) x^5+px+q

2.5 在四个变量的判别式上用系统方法确定 $\Delta(s_1,\cdots,s_4)$ 里所有不能为 s_4 所整除的单项式的系数.

2.6 令 $u_i'=u_i+t$，$i=1,2,3$. 计算导数 $\frac{d}{dt}s_i(u')$ 与 $\frac{d}{dt}\Delta(u')$，并用你的结果对三次多项式的判别式证明公式(16.2.5).

2.7 有 n 个变量. 令 $m=u_1u_2^2u_3^3\cdots u_n^{n-1}$，且设 $p(u)=\sum_{\sigma\in A_n}\sigma(m)$. $p(u)$ 的 s_n-轨道含有两个元素 p 与另一

个多项式 q. 证明 $(p-q)^2=D(u)$.

第三节 分裂域

3.1 令 f 是系数属于 F 的 n 次多项式，且设 K 是 f 在 F 上的分裂域. 证明 $[K:F]$ 整除 $n!$.

3.2 确定下列多项式在 $\mathbf{Q}$ 上分裂域的次数：

(a) x^3-2 (b) x^4-1 (c) x^4+1

3.3 令 $F=\mathbf{F}_2(u)$ 是素域 $\mathbf{F}_2$ 上的有理函数域. 证明多项式 x^2-u 在 F 上是既约的，且它在分裂域里有二重根.

第四节 域扩张的同构

4.1 (a) 确定域 $\mathbf{Q}(\sqrt[3]{2})$ 与域 $\mathbf{Q}(\sqrt[3]{2},\ \omega)$ 的所有自同构，其中 $\omega=e^{2\pi i/3}$.

(b) 令 K 是 $f(x)=(x^2-2x-1)(x^2-2x-7)$ 在 $\mathbf{Q}$ 上的分裂域. 确定 K 的所有自同构.

第五节 固定域

5.1 对下列有理函数域 $\mathbf{C}(t)$ 的自同构集，确定它们生成的自同构群，并具体确定固定域：

(a) $\sigma(t)=t^{-1}$ (b) $\sigma(t)=it$ (c) $\sigma(t)=-t$，$\tau(t)=t^{-1}$

(d) $\sigma(t)=\omega t$，$\tau(t)=t^{-1}$，其中 $\omega=e^{2\pi i/3}$

506

5.2 证明 $\mathbf{C}(t)$ 的自同构 $\sigma(t)=\dfrac{t+i}{t-i}$ 与 $\tau(t)=\dfrac{it-i}{t+1}$ 生成同构于交错群 A_4 的群，并确定这个群的固定域.

5.3 令 $F=\mathbf{C}(t)$ 是 t 的有理函数域. 证明 F 的每个不属于 $\mathbf{C}$ 的元素在 $\mathbf{C}$ 上是超越的.

第六节 伽罗瓦扩张

6.1 令 α 是多项式 x^3+x+1 在 $\mathbf{Q}$ 上的复根，且设 K 是这个多项式在 $\mathbf{Q}$ 上的分裂域. $\sqrt{-31}$ 属于域 $\mathbf{Q}(\alpha)$ 吗？它属于 K 吗？

6.2 令 $K=\mathbf{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$. 确定 $[K:\mathbf{Q}]$，证明 K 是 $\mathbf{Q}$ 的伽罗瓦扩张，并确定它的伽罗瓦群.

6.3 令 $K\supset L\supset F$ 是 2 次扩域链. 证明 K 可由形如 x^4+bx^2+c 的 4 次既约多项式的根在 F 上生成.

第七节 主要定理

7.1 不使用主要定理确定形如 $F(\sqrt{a},\sqrt{b})$ 的扩域的中间域.

7.2 令 K/F 是伽罗瓦扩张使得 $G(K/F)\approx C_2\times C_{12}$. 有多少个中间域 L 使得下列各式成立？

(a) $[L:F]=4$ (b) $[L:F]=9$ (c) $G(K/L)\approx C_4$

7.3 当 K/F 是伽罗瓦扩张使得其伽罗瓦群为(a)交错群 A_4，(b)二面体群 D_4 时有多少个中间域 L 使得 $[L:F]=2$？

7.4 令 $F=\mathbf{Q}$ 与 $K=\mathbf{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$. 确定所有中间域.

7.5 令 $f(x)$ 是 $\mathbf{Q}$ 上既约三次多项式，其伽罗瓦群为 S_3. 确定多项式 $(x^3-1)f(x)$ 的可能的伽罗瓦群.

7.6 令 K/F 是伽罗瓦扩张，其伽罗瓦群为对称群 S_3. K 是三次既约多项式在 F 上的分裂域吗？

7.7 (a)确定 $i+\sqrt{2}$ 在 $\mathbf{Q}$ 上的既约多项式.

(b)证明集合 $(1,\ i,\ \sqrt{2},\ i\sqrt{2})$ 是 $\mathbf{Q}(i,\sqrt{2})$ 在 $\mathbf{Q}$ 上的基.

7.8 令 α 表示 2 的 4 次正实根. 在每个域 $\mathbf{Q}$，$\mathbf{Q}(\sqrt{2})$，$\mathbf{Q}(\sqrt{2},\ i)$，$\mathbf{Q}(\alpha)$，$\mathbf{Q}(\alpha,\ i)$ 上分解多项式 x^4-2 为既约因子.

7.9 令 $\zeta=e^{2\pi i/5}$. 证明 $K=\mathbf{Q}(\zeta)$ 是多项式 x^5-1 在 $\mathbf{Q}$ 上的分裂域，并确定次数 $[K:\mathbf{Q}]$. 不用定理 16.7.1 证明 K 是 $\mathbf{Q}$ 的伽罗瓦扩张，并确定它的伽罗瓦群.

7.10 令 K/F 是带有伽罗瓦群 G 的伽罗瓦扩张，且设 H 是 G 的子群. 证明存在元素 $\beta\in K$，其稳定子等于 H.

7.11 令 $\alpha=\sqrt[3]{2}$，$\beta=\sqrt{3}$ 和 $\gamma=\alpha+\beta$. 令 L 是域 $\mathbf{Q}(\alpha,\beta)$，且设 K 是多项式 $(x^3-2)(x^2-3)$ 在 $\mathbf{Q}$ 上的分裂域.

(a) 确定 γ 在 $\mathbf{Q}$ 上的既约多项式 f 和它在 $\mathbf{C}$ 中的根.

(b) 确定 $K/\mathbf{Q}$ 的伽罗瓦群.

第八节 三次方程

8.1 令 K/F 是伽罗瓦扩张，其伽罗瓦群 G 为克莱因四元群 D_2. 证明 K 可由添加两个平方根到 F 得到，
507 并解释 G 如何作用在 K 上.

8.2 在 $\mathbf{Q}$ 上确定下列多项式的伽罗瓦群：

(a) x^3-2 (b) $x^3+3x+14$ (c) x^3-3x^2+1 (d) $x^3-21x+7$

(e) x^3+x^2-2x-1 (f) x^3+x^2-2x+1

8.3 利用 α_1 和 f 的系数具体确定在(16.8.2)中出现的二次多项式 $q(x)$.

8.4 令 $K=\mathbf{Q}(\alpha)$，其中 α 是多项式 x^3+2x+1 的根，且设 $g(x)=x^3+x+1$. $g(x)$ 在 K 中有根吗？

8.5 令 α_i 是三次多项式 $f(x)=x^3+px+q$ 的根，用元素 α_1，δ 与 f 的系数求第二个根 α_2 的公式.

第九节 四次方程

9.1 令 K 是 F 的伽罗瓦扩张，其伽罗瓦群是对称群 S_4. 哪个整数作为 K 的元素在 F 上的次数出现？

9.2 借助例 16.9.2(a)，把元素 $\alpha+\alpha'$ 写为嵌套平方根. K 含有的其他嵌套平方根是什么？

9.3 $\sqrt{4+\sqrt{7}}$ 可以用有理数 a 与 b 写成形式 $\sqrt{a}+\sqrt{b}$ 吗？

9.4 (a) 用两种方法证明多项式 x^4-8x^2+11 在 $\mathbf{Q}$ 上是既约的：用第十二章的方法与用它的根计算的方法.

(b) 对多项式 x^4-8x^2+9 做相同的证明.

(c) 当 K 是 x^4-8x^2+11 在 $\mathbf{Q}$ 上的分裂域时确定所有中间域.

9.5 考虑嵌套平方根 $\alpha=\sqrt{r+\sqrt{t}}$，其中 r 与 t 属于域 F. 假设 α 在 F 上次数为 4，设 f 是 α 在 F 上的既约多项式，并设 K 是 f 在 F 上的分裂域.

(a) 计算 α 在 F 上的既约多项式 $f(x)$. 证明 $G(K/F)$ 是群 D_4，C_4 或 D_2 之一.

(b) 解释如何用元素 r^2-t 确定伽罗瓦群.

(c) 假设 K/F 的伽罗瓦群是二面体群 D_4. 确定所有中间域 $F\subset L\subset K$ 的生成元.

9.6 计算四次多项式 x^4+1 的判别式，并确定它在 $\mathbf{Q}$ 上的伽罗瓦群.

9.7 假设扩域 K/F 有形式 $K=F(\sqrt{a},\sqrt{b})$. 确定属于 K 的所有嵌套平方根，其中 r 与 t 属于域 F.

9.8 确定下列嵌套根式是否能用非嵌套平方根写出来，如果能，求出表示式.

(a) $\sqrt{2+\sqrt{11}}$ (b) $\sqrt{10+5\sqrt{2}}$ (c) $\sqrt{11+6\sqrt{2}}$ (d) $\sqrt{6+\sqrt{11}}$ (e) $\sqrt{11+\sqrt{6}}$

9.9 (a) 确定形如 $f(x)=x^4+rx+s$ 的多项式的判别式与三次预解式.

(b) 确定 $x^4+8x+12$ 与 $x^4+8x-12$ 在 $\mathbf{Q}$ 上的伽罗瓦群.

508 (c) 多项式 x^4+x-5 的根能够用直尺和圆规作出来吗？

9.10 (a) 恰有两个实根的四次既约多项式在 $\mathbf{Q}$ 上的可能伽罗瓦群是什么？

(b) 判别式为负的四次既约多项式在 $\mathbf{Q}$ 上的可能伽罗瓦群是什么？

9.11 令 $F=\mathbf{Q}$，且设 K 是多项式 $f(x)=x^4-2$ 在 F 上的分裂域. 根是 α，$-\alpha$，$i\alpha$，$-i\alpha$，其中 $\alpha=\sqrt[4]{2}$.

(a) 确定伽罗瓦群 $G=G(K/F)$ 与子群 $H=G(K/F(i))$.

(b) 说明 H 的每个元素如何置换 f 的诸根.

(c) 求所有中间域.

9.12 确定下列多项式在 $\mathbf{Q}$ 上的伽罗瓦群.

(a) x^4+4x^2+2 (b) x^4+2x^2+4 (c) x^4+1

(d) x^4+x+1 (e) $x^4+x^3+x^2+x+1$ (f) x^4+x^2+1

9.13 令 K 是多项式 x^4-2x^2-1 在 $\mathbf{Q}$ 上的分裂域. 确定 $K/\mathbf{Q}$ 的伽罗瓦群 G，求所有中间域，并将它们与 G 的子群匹配起来.

*9.14 令 $F=\mathbf{Q}(\omega)$，其中 $\omega=e^{2\pi i/3}$. 确定(a) $\sqrt[3]{2+\sqrt{2}}$，(b) $\sqrt{2+\sqrt[3]{2}}$的分裂域在 F 上的伽罗瓦群.

*9.15 令 K 是既约四次多项式 $f(x)$在 F 上的分裂域，且设 $f(x)$在 K 中的根是 α_1，α_2，α_3，α_4. 假设三次预解式 $g(x)$在 F 里有根 $\beta_1=\alpha_1\alpha_2+\alpha_3\alpha_4$. 用嵌套平方根把根 α_1 具体表示出来.

9.16 确定一般的四次多项式(16.9.4)的三次预解式.

9.17 利用 $\mathbf{Q}$ 上的 4 次实数 α 的既约多项式的伽罗瓦群确定可用直尺和圆规作出的 $\mathbf{Q}$ 上的 4 次实数 α.

9.18 证明其伽罗瓦群是二面体群 D_4 的任意伽罗瓦扩张是形如 x^4+bx^2+c 的多项式的分裂域.

第十节 单位根

10.1 确定 ζ_7 在域 $\mathbf{Q}(\zeta_3)$上的次数.

10.2 令 $\zeta=\zeta_{17}$. 求在例 16.10.3 中描述的中间域 L_2 的生成元.

10.3 令 $\zeta=\zeta_7$. 确定下列元素在 $\mathbf{Q}$ 上的次数：

(a) $\zeta+\zeta^6$ (b) $\zeta^3+\zeta^4$ (c) $\zeta^3+\zeta^5+\zeta^6$

10.4 令 $\zeta=\zeta_{13}$. 确定下列元素在 $\mathbf{Q}$ 上的次数：

(a) $\zeta+\zeta^{12}$ (b) $\zeta+\zeta^2$ (c) $\zeta+\zeta^5+\zeta^8$ (d) $\zeta^2+\zeta^5+\zeta^6$ (e) $\zeta+\zeta^5+\zeta^8+\zeta^{12}$

(f) $\zeta+\zeta^2+\zeta^5+\zeta^{12}$ (g) $\zeta+\zeta^3+\zeta^4+\zeta^9+\zeta^{10}+\zeta^{12}$

10.5 令 $K=\mathbf{Q}(\zeta_p)$. 当 p 为下列各值时具体确定所有中间域.

(a) $p=5$ (b) $p=7$ (c) $p=11$ (d) $p=13$

10.6 (a) 给出定理 16.10.12 的证明.

(b) 对二次扩张证明 Kronecker-Weber 定理. 509

10.7 令 $\zeta_n=e^{2\pi i/n}$，且设 $K=\mathbf{Q}(\zeta_n)$.

(a) 证明 K 是 $\mathbf{Q}$ 的伽罗瓦扩张.

(b) 在环 $\mathbf{Z}/(n)$中定义单同态 $G(K/\mathbf{Q})\to U$ 到单位群 U.

(c) 当 $n=6$，8，12，证明这个同态是双射的. (事实上，这个映射永远是双射.)

10.8 确定诸多项式 x^8-1，$x^{12}-1$，x^9-1 的伽罗瓦群.

10.9 令 $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$.

(a) 证明 f 的判别式是 $\pm f'(\alpha_1)\cdots f'(\alpha_n)$，其中 f'是 f 的导数，并确定符号.

(b) 用公式计算多项式 x^p-1 的判别式，并用它给出定理 16.10.12 的另一个证明.

10.10 关于在第十六章第十一节末描述的特征向量 γ，证明诸元素 $\gamma_i=\alpha_1+\zeta^i\alpha_2+\cdots+\zeta^{i(p-1)}\alpha_p$ 至少有一个不是零.

第十一节 库默尔扩张

11.1 证明如果 $F[x]$中三次既约多项式的判别式不是 F 里的平方项，则诸根不能通过添加立方根到 F 得到.

11.2 (a) 不用伽罗瓦理论证明命题 16.11.2.

(b) F 是任意的，证明如果 x^p-a 是 $F[x]$ 里的既约多项式，则它在 F 里有根.

*11.3 令 F 是 $\mathbf{C}$ 的含有 i 的子域，且设 K 是 F 的伽罗瓦扩张，其伽罗瓦群为 C_4. K 是否有形式 $F(\alpha)$? 其中 α^4 在 F 里.

11.4 进行计算得出卡尔达诺公式(16.13.3).

11.5 (a) 如何用卡尔达诺公式(16.13.3)表示多项式 x^3+3x，x^3+2，x^3-3x+2 与 x^3+3x+2 的根?

(b) 什么是卡尔达诺公式里根的正确选择?

第十二节 五次方程

12.1 每个 10 次伽罗瓦扩张都是可解的吗?

12.2 确定 S_5 的可迁子群.

12.3 令 G 是五次既约多项式的伽罗瓦群. 证明如果 G 含有 3 阶元素，则 G 是 S_5 或 A_5.

12.4 令 s_1，…，s_n 是变量 u_1，…，u_n 的初等对称函数，且设 F 是域.

(a) 证明 u_1，…，u_n 的有理函数域 $F(u)$是域 $F(s_1,\cdots,s_n)$的伽罗瓦扩张，且它的伽罗瓦群是对称群 S_n.

(b) 假设 $n=5$，且设 $w=u_1u_2+u_2u_3+u_3u_4+u_4u_5+u_5u_1$. 确定 $F(u)$在域 $F(s,w)$上的伽罗瓦群.

510 (c) 令 G 是有限群. 证明存在其伽罗瓦群是 G 的域 F 和 F 的伽罗瓦扩张 K.

12.5 令 K 是 $\mathbf{Q}$ 的伽罗瓦扩张，其次数为 2 的幂，使得 $K\subset\mathbf{R}$. 证明 K 的元素可用直尺和圆规作出.

12.6 证明：如果多项式 f 的伽罗瓦群是非阿贝尔单群，则根是不可解的.

12.7 求 $\mathbf{Q}$ 上其伽罗瓦群是 S_7 的 7 次多项式.

12.8 令 p 是素数. 证明对称群 S_p 是由 p-循环与任一个对换生成的.

杂题

M.1 令 $F_1\subset F_2$ 是域扩张，且设 f 是系数属于 F_1 的多项式. f 在 F_2 上的分裂域 K_2 将含有 f 在 F_1 上的分裂域 K_1. 伽罗瓦群 $G(K_1/F_1)$与 $G(K_2/F_2)$之间的关系是什么?

M.2 令 L/F 与 K/L 是伽罗瓦扩张. K/F 一定是伽罗瓦扩张吗?

M.3 (范德蒙德行列式)

(a) 证明矩阵的行列式

$$\begin{bmatrix} 1 & u_1 & u_1^2 & \cdots & u_1^{n-1} \\ 1 & u_2 & & & u_2^{n-1} \\ \vdots & \vdots & & & \vdots \\ 1 & u_n & \cdots & \cdots & u_n^{n-1} \end{bmatrix}$$

是判别式 $\delta(u)=\prod_{i<j}(u_i-u_j)$ 的平方根的常数倍.

(b) 确定这个常数.

M.4 (a) 非负实数是有实平方根的那些数. 用这个事实证明域 $\mathbf{R}$ 除恒等同构外没有别的自同构.

*(b) 证明 $\mathbf{C}$ 除了复共轭与恒等同构外没有连续自同构.

M.5 令 $K=\mathbf{F}_q$，其中 $q=p^r$.

(a) 证明由 $\varphi(x)=x^p$ 定义的弗洛贝尼乌斯映射 φ 是 $F=\mathbf{F}_p$ 的自同构.

(b) 证明伽罗瓦群 $G(K/F)$是由弗洛贝尼乌斯映射 φ 生成的 r 阶循环群.

(c) 证明伽罗瓦理论的主要定理对扩张 K/F 也是成立的.

⊖M.6 令 K 是 $\mathbf{C}$ 的子域，且设 G 是自同构群. 可将 G 视为作用在复平面的点集 K 上. 这个作用也许是不

⊖ 为纪念 Bruce Renshaw.

连续的，但无论如何，我们通过定义 $g[\alpha, \beta]=[g\alpha, g\beta]$定义了线段$[\alpha, \beta]$上其端点属于 K 的作用. 这样，G 也作用于其顶点属于 K 的多边形上.

(a) 令 $K=\mathbf{Q}(\zeta)$，其中 ζ 是 1 的五次本原根. 求其顶点为 $1, \zeta, \zeta^2, \zeta^3, \zeta^4$ 的正五边形的 G-轨道.

(b) 令 α 是(a)的五边形的边长. 证明 α^2 属于 K，并求 α 在 $\mathbf{Q}$ 上的既约多项式. 511

*M. 7 $F(u_1, \cdots, u_n)$中的多项式 f 是$\frac{1}{2}$对称的，如果 $f(u_{\sigma 1}, \cdots, u_{\sigma n})=f(u_1, \cdots, u_n)$对每个偶置换 σ 成立；是斜对称的，如果 $f(u_{\sigma 1}, \cdots, u_{\sigma n})=(\operatorname{sign}\sigma) f(u_1, \cdots, u_n)$对每个置换 σ 成立.

(a) 证明判别式 $\delta=\prod_{i<j}(u_i-u_j)$的平方根是斜对称的.

(b) 证明每个$\frac{1}{2}$对称多项式有形式 $f+g\delta$，其中 f，g 是对称多项式.

㊀*M. 8 设有变量 u_0，u_1，u_2，u_3，令 $p_i=(u_i-u_{i+1})(u_i-u_{i+2})(u_{i+1}-u_{i+2})$，指标模 4. 确定

(a) $\sum_{i=0}^{3}\frac{u_i}{p_{i+1}}$　　(b) $\sum_{i=0}^{3}\frac{u_i^3}{p_{i+1}}$

*M. 9 令 $f(t, x)$是 $\mathbf{C}[t, x]$中的既约多项式，当视为 x 的多项式时为首项系数是 1 的三次多项式. 假设对某个 t_0，多项式 $f(t_0, x)$有一单根和一个二重根. 证明 $f(x)$在 $\mathbf{C}[t]$上的分裂域 K 的次数为 6.

*M. 10 令 K 是域 F 的有限扩张，且设 $f(x)$属于 $K[x]$. 证明在 $K[x]$中存在非零多项式 $g(x)$使得积 $f(x)g(x)$属于 $F[x]$.

*M. 11 令 $f(x)$是 $F[x]$里的既约四次多项式，且设 α_1，α_2，α_3，α_4 是它在分裂域 K 中的根. 假设三次预解式在 F 里有根 $\beta=\alpha_1\alpha_2+\alpha_3\alpha_4$，但判别式 D 不是 F 里的平方项. 根据(16.9.9)，K/F 的伽罗瓦群是 C_4 或 D_4.

(a) 具体确定稳定 β 的诸根 α_i 的置换群 S_4 的子群 H. 不要忘记证明除了你所列出的置换外，其他置换都不能使 β 固定不动.

(b) 令 $\gamma=\alpha_1\alpha_2-\alpha_3\alpha_4$ 与 $\epsilon=\alpha_1+\alpha_2-\alpha_3-\alpha_4$. 证明 γ^2 与 ϵ^2 属于 F.

(c) 令 δ 是判别式的平方根. 证明如果 $\gamma\neq 0$，则 $\delta\gamma$ 是 F 里的平方项当且仅当 $G=C_4$. 类似地，证明如果 $\epsilon\neq 0$，则 $\delta\epsilon$ 是 F 里的平方项当且仅当 $G=C_4$.

(d) 证明 γ 与 ϵ 不可能都为零.

*M. 12 有限群 G 是可解的，如果它含有子群链 $G=H_0\subset H_1\subset\cdots\subset H_k=\{1\}$使得对每个 $i=1, \cdots, k$，H_i 是 H_{i-1}的正规子群，且商群 H_i/H_{i+1}是循环群. 令 f 是域 F 上的既约多项式，且设 G 是它的伽罗瓦群. 证明 f 的根在 F 上是可解的当且仅当 G 是可解群.

㊁*M. 13 令 K/F 是带有伽罗瓦群 G 的伽罗瓦扩张. 如果我们把 K 看成 F-向量空间，则得到 G 在 K 上的一个表示. 设 χ 表示这个表示的特征标. 证明如果 F 包含有足够多的单位根，则 χ 是正则表示的特征标.

这种方法能做些什么，
只有将来才知道.

——Emmy Noether 512

㊀ 由 Harold Stark 建议.

㊁ 由 Galyna Dobrovolska 建议.

附录　背景材料

当然从历史上讲，没有矛盾的数学是和当不真实的；
没有矛盾是一个想要达到的目标，
而不是上帝赋予我们的一劳永逸的质量.

——Nicolas Bourbaki

第一节　关于证明

数学家所认为的给出证明的适当方法是没有明确定义的. 通常并不是给出一个每一步都由对上一步应用逻辑法则而得到在这样的意义下的完整的证明. 写出这样一个证明会太长而且要点不够突出. 另一方面，证明中所有困难的步骤都认为应该包含在其中. 阅读证明的人应该能够补充理解它所需的细节. 如何写出证明是一种只有通过实践才能学会的技能.

用于构造证明的三个一般方法是二分法、归纳法和反证法.

二分一词是指分成两部分，它用于把一个问题分解为更小、更易于处理的部分. 这个过程的其他名称有案例分析和分而治之.

这里是一个二分法的例子：二项式系数$\binom{n}{k}$(读作 n 选 k)是在下标集合$\{1, 2, \cdots, n\}$中 k 阶子集的个数. 例如，$\binom{4}{2}=6$. 集合$\{1, 2, 3, 4\}$有六个 2 阶子集，它们是$\{1, 2\}$，$\{1, 3\}$，$\{1, 4\}$，$\{2, 3\}$，$\{2, 4\}$，$\{3, 4\}$.

【A. 1. 1】命题　对每个整数 r 及每个 $k \leqslant r$，有$\binom{r}{k}=\binom{r-1}{k}+\binom{r-1}{k-1}$.

证明　设 S 是$\{1, 2, \cdots, n\}$的一个 k 阶子集. 则或者 $n \in S$，或者 $n \notin S$. 这是我们的二分法.

情形 1：$n \notin S$. 在这一情形中，S 实际上是$\{1, 2, \cdots, n-1\}$的一个子集. 由定义，有$\binom{n-1}{k}$个这样的子集.

513

情形 2：$n \in S$. 设 $S'=S-\{n\}$是由从集合 S 删去指标 n 得到的子集. 于是，S'是$\{1, 2, \cdots, n-1\}$的一个 $k-1$ 阶子集. 有$\binom{n-1}{k-1}$个这样的子集. 因此有$\binom{n-1}{k-1}$个 k 阶子集包含 n. 这总共给出$\binom{n-1}{k}+\binom{n-1}{k-1}$个 k 阶子集. ■

这里显示了二分法的巨大威力：这两种情形的每一种，即 $n\in S$ 和 $n\notin S$，我们都有一个关于集合 S 的另外的事实. 这一另外的事实可以在证明中使用.

一个证明常常会需要整理出若干可能性，并逐个检查. 这就是二分法或案例分析. 例如要确定一个植物的种属，格雷的《植物学手册》提出一系列的二分法. 一个典型例子是“叶子在茎上相对”，或“叶子在茎上交错”. 数学结构的分类也要通过一系列的二分法来进行. 在简单的情形中这不必正式地指出，但当处理复杂的可能性的范围时，就需要仔细地分类.

*归纳法*是证明一系列由正整数 n 作指标的命题 P_n 的主要方法. 为了对所有 n 证明命题 P_n，归纳法原理要求我们做两件事：

【A. 1. 2】

(i) 证明 P_1 成立；

(ii) 证明如果对某个整数 $k>1$ 有 P_k 成立，则 P_{k+1} 也成立. 这不过是指标变换.

下面是一些归纳法的例子. 如果 n 是正整数，则 $n!$（“n 的阶乘”）是从 1 到 n 的整数的积$1\cdot 2\cdots\cdot n$. 而且，0! 定义为 1.

【A. 1. 3】**命题** $\dbinom{n}{k}=\dfrac{n!}{k!\ (n-k)!}$.

证明 令 P_r 为命题$\dbinom{r}{\ell}=\dfrac{r!}{\ell!\ (r-\ell)!}$对所有 $\ell=1,\cdots,r$ 成立. 先检验 P_1 成立. 假设 P_{r-1} 成立. 则当用 $n=r-1$ 和 $\ell=k$ 代入时公式成立，当用 $n=r-1$ 和 $\ell=k-1$ 代入时也成立：

$$\binom{r-1}{k}=\frac{(r-1)!}{k!(r-1-k)!},\quad \binom{r-1}{k-1}=\frac{(r-1)!}{(k-1)!(r-k)!}$$

根据命题(A. 1. 1)，

$$\binom{r}{k}=\binom{r-1}{k}+\binom{r-1}{k-1}=\frac{(r-1)!}{k!(r-k-1)!}+\frac{(r-1)!}{(k-1)!(r-k)!}$$

$$=\frac{(r-k)(r-1)!}{k!(r-k)!}+\frac{k(r-1)!}{k!(r-k)!}=\frac{r!}{k!(r-k)!}$$

这表明 P_r 成立. ■ 514

作为另一个例子，我们证明“鸽笼原理”. 此处$|S|$表示集合 S 的元素个数.

【A. 1. 4】**命题** *如果有限集合间的一个映射 φ：$S\to T$ 是单射，则 T 至少包含与 S 中一样多的元素：$|S|\leqslant|T|$.*

证明 我们对 $n=|S|$ 用归纳法. 如果 $n=0$，即如果 S 是空集合，则断言是成立的，因为到空集合有映射的集合只能是空集合.

假设定理对 $n=k-1$ 已经得证，我们着手验证 $n=k$ 的情形，其中 $k>0$. 假设$|S|=k$，我们选取一个元素 $s\in S$. 令 $t=\varphi(s)$是 s 在 T 中的像. 由于 φ 是单射，故 s 是唯一以 t 为像

的元素. 因此 φ 是集合 $S'=S-\{s\}$ 到集合 $T'=T-\{t\}$ 的单射. 显然 $|S'|=|S|-1=k-1$, $|T'|=|T|-1$. 由归纳假设, $|S'|\leqslant|T'|$, 故 $|S|\leqslant|T|$. ■

归纳法原理有一个另外的表达形式, 称为*完全归纳法*. 同样, 我们还是希望证明命题 P_n 对每个正整数 n 成立. 完全归纳法原理断言只需证明下面的命题:

如果 n 是一个正整数, 且 P_k 对于每个正整数 $k<n$ 成立, 则 P_n 成立.

当 $n=1$ 时, 没有满足 $k<n$ 的正整数. 因而对 $n=1$, 命题中的假设自动地成立. 因此使用完全归纳法的证明必包括 P_1 的证明.

当对某个较小的整数 k, 有一个把 P_n 化为 P_k 而不一定是 P_{n-1} 的过程时, 便使用完全归纳法原理. 下面是一个例子:

【A. 1. 5】定理 *每个 $n>1$ 的整数 n 是素整数的乘积.*

证明 令 P_n 为 n 是素数的乘积这一命题. 假设对所有 $k<n$ 有 P_k 成立, 我们必须证明 P_n 是成立的, 即 n 是素数的乘积. 如果 n 本身是素数, 则它是一个素数的积. 否则, n 可以写成两个正整数的乘积 $n=ab$, 且 a, b 都不是 1. 则 a, b 是小于 n 的正整数, 故由归纳假设, P_a 和 P_b 都为真, 即 a 和 b 都是素整数之积. 把这两个积放在一起, 就得到 n 的因子分解, 即 n 是素整数的乘积. ■

*反证法*通过假设希望的结论是错的并由这个假设导出矛盾来证明. 因而结论必是正确的. 这样的证明经常是假的, 因为反证法容易变成直接证明. 下面就是一个例子:

【A. 1. 6】命题 *令 φ: $S\to T$ 是有限集合间的一个单射. 如果 φ 是双射, 则 $|S|=|T|$.*

证明 既然已知 φ 是单射, 则 φ 是双射当且仅当 φ 为满射. 我们假设 $|S|=|T|$, 但 φ
515 不是满射. 则存在元素 $t\in T$, 但它不是 S 的像. 这样的话, φ 实际上单射地映射 S 到集合 $T'=T-\{t\}$. 则命题 A. 1. 4 告诉我们 $|S|\leqslant|T'|=|T|-1$, 此与 $|S|=|T|$ 矛盾. ■

不要这样安排证明. 在证明中假设 $|S|=|T|$ 是没有用的. 直接表述, 论证表明如果 φ 是单射而不是双射, 则 $|S|<|T|$.

如果 X 代表某个命题, 则令非 X 代表 X 不真, 则断言"若非 B, 则非 A"是断言"若 A, 则 B"的*逆否命题*, 这两种表述在逻辑上是等价的. 上面提供的论证证明了命题所述的断言的逆否命题.

要找到用反证法证明的一个简单的例子不太容易, 但在课本中确实存在.

第二节 整 数

在小学我们学过整数的加法和乘法的初等性质, 但为了证明某些性质, 我们再回顾一下所需要的诸如结合律和分配律这样的性质. 完全证明需要相当大的篇幅, 我们只做个抛砖引玉的工作. 通常从正整数的加法和乘法的定义开始. 负数之后才引入. 这意味着随着研究的深入, 必须处理几种情况, 这很令人厌烦, 否则就要找到一个聪明的记号来避免这种案例分析. 我们将满足于对正整数的运算的描述. 正整数又叫做*自然数*.

自然数集合 **N** 用下面这些性质来刻画.

佩亚诺公理

- 自然数集合 **N** 包含一个特殊的元素 1.
- *后继元函数*：存在一个映射 σ：$\mathbf{N}\to\mathbf{N}$ 把一个整数映射到另一个整数，称为*后继元*或下一个整数. 这个映射是单射，且对于每一个 $n\in\mathbf{N}$，$\sigma(n)\neq 1$.
- *归纳公理*：假设 **N** 的一个子集 S 有下列性质：
  (i) $1\in S$，且
  (ii) 如果 $n\in S$，则 $\sigma(n)\in S$.
  则 S 包含每一个自然数：$S=\mathbf{N}$.

当定义了加法后，后继元 $\sigma(n)$ 变成 $n+1$. 在这个阶段记号 $n+1$ 容易令人费解. 最好用一个中性的记号，记后继元 $\sigma(n)$ 为 n'. 后继元函数使得我们能用自然数计数，这是算术的基础.

归纳性质可以直观地描述为自然数可以从 1 反复取后继元得到：

$$\mathbf{N}=\{1,1',1'',\cdots\}\quad(=\{1,2,3,\cdots\})$$

516

换句话说，计数取遍所有自然数. 这个性质是归纳法证明的基础.

佩亚诺公理也可用于递归定义. 短语*递归定义*或*归纳定义*是指用自然数索引的一个对象序列 C_n 的定义，其中一个对象用它前一个对象来定义. 例如，函数 x^n 的递归定义是

$$x^1=x\quad\text{且}\quad x^{n'}=x^n x$$

要点是：

【A. 2. 1】 C_1 已经定义好了，由 C_n 确定 $C_{n'}(=C_{n+1})$ 的规则已知.

虽然用佩亚诺公理给出快捷的证明并不容易，但是这些性质确定唯一序列 C_n 这一点在直观上是显然的. 我们并不给出证明.

给定一个正整数集合以及做递归定义的能力，我们可以如下定义正整数的加法和乘法：

【A. 2. 2】

$$\text{加法：}\ m+1=m',\ m+n'=(m+n)'.$$

$$\text{乘法：}\ m\cdot 1=m,\ m\cdot n'=m\cdot n+m.$$

在这些定义中，我们取任意整数 m 并对这个整数 m 及每个 n 递归地定义加法和乘法. 这样，$m+n$ 和 $m\cdot n$ 对于所有 m 和 n 都定义好了.

整数的结合律、交换律和分配律的证明是称为“佩亚诺游戏”的使用归纳法的练习. 在此作为例子我们给出其中一个的证明.

加法结合律的证明 我们要证明对所有 a，b，$n\in\mathbf{N}$，$(a+b)+n=a+(b+n)$. 首先检验在 $n=1$ 的情形对所有 a，b 成立. 上面定义的三个应用给出

$$(a+b)+1=(a+b)'=a+b'=a+(b+1)$$

其次，假设结合律对特别的 n 值以及所有 a，b 成立. 则我们验证结合律对于 n' 成立：

$$\begin{aligned}(a+b)+n'&=(a+b)+(n+1)\quad(\text{定义})\\&=((a+b)+n)+1\quad(n=1\text{ 的情形})\end{aligned}$$

$$
\begin{aligned}
&= (a+(b+n))+1 && \text{（归纳假设）}\\
&= a+((b+n)+1) && (n=1\text{ 的情形})\\
&= a+(b+(n+1)) && (n=1\text{ 的情形})\\
&= a+(b+n') && \text{（定义）}
\end{aligned}
$$

■

517 加法和乘法性质的证明遵循同样的思路.

第三节 佐恩引理

在本书的几个地方，我们会借助于佐恩引理这样一个处理无穷集合的工具. 我们现在描述它.

注 集合 S 上的偏序是一个关系 $s\leqslant s'$，这个关系对某些特定元成立，且对于所有 S 中的元素 s，s'，s'' 满足下面的公理：

【A. 3. 1】

(i) $s\leqslant s$；

(ii) 如果 $s\leqslant s'$ 且 $s'\leqslant s''$，则 $s\leqslant s''$；

(iii) 如果 $s\leqslant s'$ 且 $s'\leqslant s$，则 $s=s'$.

一个偏序集称为全序集，如果除了上面的条件外，还满足

(iv) 对于所有 S 中的元素 s，s'，或者 $s\leqslant s'$ 或者 $s'\leqslant s$.

例如，令 $\mathcal{S}$ 是以集合作为元素的集合. 如果 A，$B\in\mathcal{S}$，则定义 $A\leqslant B$ 如果 A 是 B 的子集：$A\subset B$. 这是 $\mathcal{S}$ 上的一个偏序，称为按包含排序. 它是否为全序取决于特殊情况.

一个偏序集 S 的元素 m 是极大元如果在 S 中不存在异于 m 的元素 $s\in S$ 满足 $m\leqslant s$. 一个偏序集 S 可以含有多个不同的极大元. 例如，一个集合 U 的子集 V 称为真子集，如果 V 不是空集也不是整个集合 U. 集合 $\{\mathbf{1},\mathbf{2},\cdots,\boldsymbol{n}\}$ 的所有真子集的集合按照集合的包含关系构成偏序集，这个偏序集含有 n 个极大元，$\{\mathbf{2},\cdots,\boldsymbol{n}\}$ 就是极大元之一.

一个非空有限偏序集 S 至少含有一个极大元，但是一个无限偏序集（例如整数集合）可能根本没有极大元. 一个全序集包含至多一个极大元.

注 若 A 是偏序集 S 的一个子集，则 $b\in S$ 叫做集合 A 的一个上界，使得对于任意 $a\in A$，有 $a\leqslant b$. 一个偏序集 S 是归纳的，如果 S 的每个全序子集 T 有上界.

一个有限的全序集包含唯一的极大元，因此是归纳的.

【A. 3. 2】引理（佐恩引理） 一个归纳的偏序集 S 有至少一个极大元.

佐恩引理和选择公理是等价的，它独立于集合论的基本公理. 我们不进一步讨论这个等价性，但会表明佐恩引理如何用于证明每个向量空间都有一组基.

【A. 3. 3】命题 域 F 上每个向量空间 V 有一组基.

证明 令 $\mathcal{S}$ 是一个集合，它的元素是 V 的线性无关的子集，按照集合的包含关系构成
518 偏序集. 我们证明 $\mathcal{S}$ 是归纳的：令 $\mathcal{T}$ 是 $\mathcal{S}$ 的一个全序子集. 则我们断言这些集合的并构成 $\mathcal{T}$ 也是线性无关的，这表明 $\mathcal{T}$ 属于 $\mathcal{S}$. 为证明这一点，令

$$B=\bigcup_{A\in\mathcal{T}}A$$

是集合的并. 由定义，B 上线性无关的关系是有限的，故可以写成下面的形式：

【A. 3. 4】 $$c_1v_1+\cdots+c_nv_n=0$$

其中 $v_i\in B$. 由于 B 是$\mathcal{T}$中集合的并，故每个 v_i 属于这些子集之一，比如 A_i. 这些子集的集合$\{A_1,\cdots,A_n\}$是一个有限集，它是$\mathcal{T}$的全序子集. 它有唯一的极大元 A. 则 $v_i\in A$ 对所有$i=1,\cdots,n$成立. 由于 A 属于$\mathcal{S}$，故它是线性无关的集合，因此(A. 3. 4)是平凡关系. 这表明 B 是线性无关的，因此是$\mathcal{S}$中的元素.

我们已经证明了佐恩引理的假设. 故$\mathcal{S}$包含一个极大元 M，我们断言 M 是一组基. 由$\mathcal{S}$的定义，M 是线性无关的. 令 $W=\mathrm{Span}(M)$. 如果 $W<V$，则选取元素 $v\in V$，$v\notin W$. 集合 $M\cup\{v\}$是线性无关的. 此与 M 的极大性矛盾，这表明 $W=V$，因此 M 是一组基. ■

类似的论证可以证明第十一章的定理 11. 9. 2：

【A. 3. 5】命题 令 R 是一个环. 每个理想 $I\neq R$ 都包含在一个极大理想中.

第四节 隐函数定理

在本书中多次用到复多项式函数的隐函数定理，由于缺乏参考材料，我们把关于实值函数的隐函数定理叙述在这里作为参考. 关于实值函数的定理可参考在“进一步阅读建议”中所列的卢丁(Rudin)的书中的定理 9. 27.

【A. 4. 1】定理(隐函数定理) 设 $f_1(x,y),\cdots,f_r(x,y)$是 $n+r$ 个实变量 $x_1,\cdots,x_m,y_1,\cdots,y_r$ 的函数，它在 $\mathbf{R}^{n+r}$ 中包含点(a,b)的一个开集上有连续偏导数. 假设雅可比行列式

$$\det\begin{bmatrix}\dfrac{\partial f_1}{\partial y_1} & \cdots & \dfrac{\partial f_1}{\partial y_r}\\ \cdots & & \cdots\\ \dfrac{\partial f_r}{\partial y_1} & \cdots & \dfrac{\partial f_r}{\partial y_r}\end{bmatrix}$$

在点(a,b)不为零. 在 $\mathbf{R}^n$ 中存在点 a 的一个邻域 U，使得 U 上存在唯一的连续可微函数 $Y_1(x),\cdots,Y_r(x)$满足条件

$$\text{对 } i=1,\cdots,r\quad f_i(x,Y(x))=0 \text{ 且 } Y(a)=b$$

519

复多项式 $f(x,y)$的偏导数由微积分的求导法则定义. 但我仍用实部和虚部表示，比如 $x=x_0+x_1\mathrm{i}$，$y=y_0+y_1\mathrm{i}$，其中 x_0，x_1，y_0，y_1 是实变量，且 $f=f_0+f_1\mathrm{i}$，其中 $f_i=f_i(x_0,x_1,y_0,y_1)$是四个实变量的实值函数. 由于 f 是关于 x 和 y 的多项式，故实函数 f_i 是实变量 x_i 和 y_i 的多项式. 因此它们有连续的偏导数.

【A. 4. 2】引理 设 $f(x,y)$为一个两个变量的复系数多项式. 用上面的记号，有

(a) $\dfrac{\partial f}{\partial y}=\dfrac{\partial f_0}{\partial y_0}+\dfrac{\partial f_1}{\partial y_0}\mathrm{i}$.

(b)(柯西-黎曼方程)$\dfrac{\partial f_0}{\partial y_0}=\dfrac{\partial f_1}{\partial y_1}$，$\dfrac{\partial f_1}{\partial y_0}=-\dfrac{\partial f_0}{\partial y_1}$.

证明 可以利用乘法法则来验证这些公式. 设 $f=gh$. 则 $f_0=g_0h_0-g_1h_1$，$f_1=g_0h_1+g_1h_0$. 如果公式对于 g，h 成立，则对 f 成立. 故只需验证引理对函数 $f=y$ 和 $f=x$ 成立即可，而这是显然的. ■

【A.4.3】定理(复多项式的隐函数定理) 设 $f(x, y)$为一个复多项式. 假设对某个$(a, b)\in \mathbf{C}^2$，我们有 $f(a, b)=0$ 且$\dfrac{\partial f}{\partial y}(a, b)\neq 0$. 存在 x 在 $\mathbf{C}$ 中的一个邻域 U，在这个邻域上面存在一个唯一的连续函数 $Y(x)$，它具有下列性质：

$$f(x,Y(x))=0,\quad Y(a)=b$$

证明 我们化简这个定理为实隐函数定理 A.4.1. 对多个变量的情形，论证同样适用.

用上面的记号，我们要对作为 x_0，x_1 的函数 y_0，y_1 解一对方程 $f_0=f_1=0$. 为此，我们要证明在(a, b)上雅可比行列式

$$\det\begin{bmatrix}\dfrac{\partial f_0}{\partial y_0} & \dfrac{\partial f_0}{\partial y_1}\\ \dfrac{\partial f_1}{\partial y_0} & \dfrac{\partial f_1}{\partial y_1}\end{bmatrix}$$

不为零. 由假设，$f_i(a_0, a_1, b_0, b_1)=0$. 同样，由于$\dfrac{\partial f}{\partial y}(a, b)\neq 0$，由引理 A.4.2(a)得 $\dfrac{\partial f_0}{\partial y_0}=d_0$ 和$\dfrac{\partial f_1}{\partial y_0}=d_1$ 不同时为零. 引理的(b)部分表明，雅可比行列式为

$$\det\begin{bmatrix}d_0 & -d_1\\ d_1 & d_0\end{bmatrix}=d_0^2+d_1^2>0$$

520 这表明满足隐函数定理 A.4.1 的假设. ■

练　习

第一节　关于证明

1.1 用归纳法求下列表达式的一个紧凑型形式.

(a) $1+3+5+\cdots+(2n+1)$

(b) $1^2+2^2+\cdots+n^2$

1.2 证明 $1^3+2^3+\cdots+n^3=(n(n+1))^2/4$.

1.3 证明 $1/(1\cdot 2)+1/(2\cdot 3)+\cdots+1/(n(n+1))=n/(n+1)$.

1.4 令 φ：$S\to T$ 是有限集合间的满射. 用归纳法证明 $|S|\geqslant|T|$ 且如果 $|S|=|T|$，则 φ 是双射.

1.5 令 n 是正整数. 证明如果 2^n-1 是素数，则 n 是素数.

1.6 令 $a_n=2^{2^n}+1$. 证明 $a_n=a_0a_1\cdots a_{n-1}+2$.

1.7 有理系数的非常数多项式称为既约的，如果它不是两个非常数有理系数多项式的乘积. 证明每个有理系数多项式可以写为既约多项式的乘积.

第二节 整数

2.1 证明每个不为 1 的自然数有形式 m'，其中 m'为某个自然数 m 的后继元.

2.2 证明下面的自然数运算律.

(a) 加法交换律.

(b) 乘法结合律.

(c) 分配律.

(d) 加法消去律：如果 $a+b=a+c$，则 $b=c$.

2.3 自然数集合 $\mathbf{N}$ 上的关系$<$由下列规则定义：如果 $b=a+n$ 对于某个 $n\in\mathbf{N}$ 成立，则 $a<b$. 假设加法性质已经证明.

(a) 证明：如果 $a<b$，则 $a+n<b+n$ 对于所有 $n\in\mathbf{N}$ 成立.

(b) 证明关系$<$是传递的.

(c) 证明：如果 a，b 是自然数，则 $a<b$，或 $a=b$，或 $b<a$.

2.4 假设自然数集合 $\mathbf{N}$ 上的关系$<$的基本性质已知(练习 2.3). 证明完全归纳法原则：$\mathbf{N}$ 的一个子集 S 如果具有下面的性质，则 $S=\mathbf{N}$：如果 $n\in\mathbf{N}$ 使得对于 S 中任何元素 m 均有 $m<n$，则 $n\in S$. 521

第三节 佐恩引理

3.1 令 S 是一个偏序集.

(a) 证明：如果 S 包含一个上界 b，则 b 是唯一的，且 b 也是一个极大元.

(b) 证明：如果 S 是全序的，则极大元 m 是 S 的一个上界.

3.2 用佐恩引理证明环 R 的每个异于 R 的理想 I 都包含在一个极大理想中.

第四节 隐函数定理

4.1 证明引理 A.4.2.

4.2 设 $f(x, y)$是复多项式，假设方程

$$f=0,\quad \frac{\partial f}{\partial x}=0,\quad \frac{\partial f}{\partial y}=0$$

在 $\mathbf{C}^2$ 中没有公共解. 证明轨迹 $f=0$ 是一个 2 维流形. 522

参考文献

一般代数

- G. Birkhoff and S. MacLane, *A Survey of Modern Algebra*, 3rd ed., Macmillan, New York, 1965.
- I. N. Herstein, *Topics in Algebra*, 2nd ed., Wiley, New York, 1975.
- N. Jacobson, *Basic Algebra I, II*, Freeman, San Francisco, 1974, 1980.
- S. Lang, *Algebra*, 2nd ed., Addison Wesley, Reading, MA, 1965.
- B. L. van der Waerden, *Modern Algebra*, Ungar, New York, 1970.

线性代数

- P. D. Lax, *Linear Algebra and Its Applications*, 2nd ed., Wiley, Hoboken, NJ, 2007.
- G. Strang, *Linear Algebra and Its Applications*, 3rd ed., Harcourt Brace Jovanovich, San Diego, 1988.

分析和拓扑学

- A. P. Mattuck, *Introduction to Analysis*, Prentice-Hall, Upper Saddle, River, N.J., 1999.
- J. R. Munkres, Topology; *A First Course*, 2nd ed., Prentice Hall, Englewood Cliffs, N. J. , 2000.
- W. Rudin, *Principles of Mathematical Analysis*, 3rd ed., McGraw-Hill, New York, 1976.

数论

- H. Cohn, *A Second Course in Number Theory*, John Wiley & Sons, New York-London, 1962.
- K. F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, 1801.
- H. Edwards, *Galois Theory*, Springer-Verlag, New York, 1984.
- H. Hasse, *Number Theory*, Springer-Verlag, New York, 1980.
- J.-P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973.
- J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1992.
- H. Stark, *An Introduction to Number Theory*, M.I.T. Press, Cambridge, MA, 1978.

群

- M. R. Sepanski, *Compact Lie Groups*, Springer-Verlag, New York, 2009.
- J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, New York, 1977.
- H. Weyl, *The Classical Groups*, Princeton University Press, Princeton, N.J., 1946.

几何学

- G. A. Bliss, *Algebraic Functions*, AMS Colloquium Publications XVI, New York, 1933.

- H. S. M. Coxeter, *Introduction to Geometry*, Wiley, New York, 1961.
- D. Schwarzenbach, *Crystallography*, Wiley, Chichester, U.K., 1993.
- M. Senechal, *Quasicrystals*, Cambridge University Press, Cambridge, U.K., 1996.

数学历史

- N. Bourbaki, *Elements d'histoire des mathematiques*, Hermann, Paris, 1974.
- M. Kline, *Mathematical Thought from Ancient to Modern Times*, Oxford, New York, 1972.
- E. Landau, *Foundations of Analysis*, AMS Chelsea, New York, 2001.
- B. L. van der Waerden, *A History of Algebra*, Springer-Verlag, Berlin, New York, 1985.

期刊论文

- A. F. Filippov, *A short proof of the theorem on reduction of a matrix to jordan form*, Vestnik Mosk. Univ. Ser. I Mat. Meh. 26 (1971) 18–19.
- R. Howe, *Very Basic Lie Theory*, Math Monthly 90 (1983) 600–623.
- S. Landau, *How to tangle with a nested radical*, Math. Intelligencer 16 (1994) 49–55.
- A.K. Lenstra, H. W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients* Math. Annalen 261 (1982) 515–534.
- J. Milnor, *Analytic proofs of the "hairy ball theorem" and the Brouwer fixed-point theorem*, Amer. Math. Monthly (1978) 521–524.
- J. Stillwell, *The word problem and the isomorphism problem for groups*, Bull. Amer. Math. Soc. 6 (1982) 33–56.
- J. A. Todd and H. S. M. Coxeter, *A practical method for enumerating cosets of a finite abstract group*, Proc. Edinburg Math. Soc, II Ser. 5 (1936) 26–34.

索　引

索引中的页码为英文原书页码，与书中页边标注的页码一致.

E

N

S

W

Z