证明 R 的极大理想对应着 $\mathbf{C}[x_1, \cdots, x_n]$ 中一个包含 I 的极大理想(对应定理). $\mathbf{C}[x_1, \cdots, x_n]$ 的一个理想包含 I 当且仅当它包含 I 的所有生成元 $f_1, \cdots, f_r$. 环 $\mathbf{C}[x_1, \cdots, x_n]$ 的每个极大理想是对 $\mathbf{C}^n$ 中某个点 $a=(a_1, \cdots, a_n)$ 的代入映射 $x_i \rightsquigarrow a_i$ 的核 M_a,
347 且 $f_1, \cdots, f_r \in M_a$ 当且仅当 $f_1(a)=\cdots=f_r(a)=0$, 也就是说, 当且仅当 a 是 V 的点. ■

正如这个定理所示, 环 $R=\mathbf{C}[x]/I$ 的代数性质与簇 V 的几何性质紧密联系. 对两者关系的分析属于一个叫做代数几何的数学领域.

关于集合人们常问的一个问题是其是否为空集. 对于一个环, 是否可能没有极大理想? 这种情况只发生在零环上.

【11.9.2】定理 *令 R 是一个环. R 的每个不等于 R 本身的理想 I 都包含在一个极大理想中.*

要找到一个极大理想, 可以试试这个程序: 如果 I 不是极大理想, 则选取比 I 大的一个真理想 I'. 用 I' 代替 I, 重复上述过程. 证明遵循这样的推理思路, 但可能会多次重复这个程序, 甚至可能重复无数多次此程序. 鉴于此, 证明需要选择公理或佐恩引理(见附录). 希尔伯特基定理(后面将证明(14.6.7))表明, 对我们研究的多数环, 证明只需要一个弱可数版本的选择公理. 此处我们不讨论选择公理, 并将证明的进一步讨论推迟到第十四章.

【11.9.3】推论 *没有极大理想的唯一的环是零环.*

因为每个非零环 R 包含一个异于 R 的极大理想(零理想), 因此没有极大理想的环只有零环.

将定理 11.9.1 和 11.9.2 合并得到另一个推论:

【11.9.4】推论 *如果 n 个变量的多项式方程组 $f_1=\cdots=f_r=0$ 在 $\mathbf{C}^n$ 中没有解, 则 $1=\sum g_i f_i$, 其中 g_i 是多项式系数.*

证明 如果方程组没解, 则不存在包含理想 $I=(f_1, \cdots, f_r)$ 的极大理想. 故 I 是单位理想, 且 $1 \in I$. ■

【11.9.5】例 两个变量的三个多项式 f_1, f_2, f_3 多数情况下没有公共解. 例如, 由

【11.9.6】
$$f_1 = t^2 + x^2 - 2, \quad f_2 = tx - 1, \quad f_3 = t^3 + 5tx^2 + 1$$

生成的 $\mathbf{C}[t, x]$ 的理想是一个单位理想. 这可以通过验证方程组 $f_1=f_2=f_3=0$ 在 $\mathbf{C}^2$ 上无解来证明. ■

对于 $\mathbf{C}^n$ 的代数簇想要有一个清晰的几何图像是不容易的, 但是对于 $\mathbf{C}^2$ 中的簇的一般形状可以有一个相当简单的刻画, 在此我们从两个变量 t 和 x 的多项式环开始对 $\mathbf{C}^2$ 上代数簇的一般形状给予刻画.

348 **【11.9.7】引理** *令 $f(t, x)$ 是一个多项式, 令 a 是一个复数. 下列条件是等价的:*

(a) $f(t, x)$ 在 $\mathbf{C}^2$ 上轨迹为 $\{t=a\}$ 的每个点消失.

(b) 一个变量的多项式 $f(a, x)$ 为零多项式.

(c) 在 $\mathbf{C}[t, x]$ 上 $t-a$ 整除 f.

证明 如果 f 在轨迹 $t=a$ 上的每个点消失, 则多项式 $f(a, x)$ 对每个 x 而言为 0. 又

由于一个变量的非零多项式有有限多个根，故 $f(\alpha, x)$是零多项式. 这证明了(a)蕴含(b).

变换 $t=t'+\alpha$ 将(b)蕴含(c)的证明简化为 $\alpha=0$ 的情形. 如果 $f(0, x)$是零多项式，则 t 整除 f 中出现的每一个单项式，且 t 整除 f. 最后显然有(c)蕴含(a). ■

令$\mathcal{F}$表示关于 t 的有理函数域 $\mathbf{C}(t)$，即环 $\mathbf{C}[t]$的分式域. 环 $\mathbf{C}[t, x]$是单变量多项式环$\mathcal{F}(x)$的子环；它的元素是关于 x 的多项式，

【11.9.8】
$$f(t,x) = a_n(t)x^n + \cdots + a_1(t)x + a_0(t)$$

系数 $a_i(t)$为关于 t 的有理函数. 在环$\mathcal{F}(x)$上研究 $\mathbf{C}[t, x]$上的问题会很有帮助. 因为$\mathcal{F}(x)$上的代数更简单. 也可用带余除法，且$\mathcal{F}(x)$上的每个理想都是主理想.

【11.9.9】命题 *令 $h(t, x)$和 $f(t, x)$是 $\mathbf{C}[t, x]$的非零元. 假设 h 不能被任何形如 $t-\alpha$ 的多项式整除. 如果 h 在$\mathcal{F}(x)$中整除 f，则 h 在 $\mathbf{C}[t, x]$中整除 f.*

证明 h 在$\mathcal{F}[x]$中整除 f，比如 $f=hq$，我们证明 q 是 $\mathbf{C}[t, x]$中的元素. 由于 $q\in\mathcal{F}[x]$，故它是关于 t 的有理函数为系数的关于 x 的多项式. 将方程 $f=hq$ 两边均乘以关于 t 的首一多项式，以去掉系数中的分母. 这给出形如下面的方程：$u(t)f(t, x)=h(t, x)q_1(t, x)$，其中 $u(t)$是一个首一的关于 t 的多项式，且 $q_1\in\mathbf{C}[t, x]$. 我们对 u 的次数使用数学归纳法. 如果 u 有正的次数，则它必有一个复根 α. 于是 $t-\alpha$ 整除方程的左边，因而也整除方程的右边. 这意味着 $h(\alpha, x)q_1(\alpha, x)$是关于 x 的零多项式. 由假设，$t-\alpha$ 不整除 h，故 $h(\alpha, x)\neq 0$. 由于多项式环 $\mathbf{C}[x]$为整环，故$q_1(\alpha, x)=0$，且此引理表明 $t-\alpha$ 整除 $q_1(t, x)$. 从 u 和 q_1 中消去 $t-\alpha$. 归纳法完成证明. ■

【11.9.10】定理 *两个变量的两个非零多项式 $f(t, x)$和 $g(t, x)$在 $\mathbf{C}^2$ 上只有有限个共同的零点，除非它们在 $\mathbf{C}[t, x]$上有共同的非常数的因子.*

如果多项式 f 和 g 的次数分别为 m 和 n，则共同零点的个数至多为 mn 个. 这被称为贝祖界. 例如，两个二次多项式至多有 4 个共同的零点. (对于实多项式的类似命题是两条 349
圆锥曲线至多有 4 个交点.)除了有限性之外要证明贝祖界是困难的. 我们不需要贝祖界，因此也不证明它.

定理 11.9.10 的证明 假设 f 和 g 没有公因子. 令 I 表示$\mathcal{F}[x]$中由 f 和 g 生成的理想，此处$\mathcal{F}=\mathbf{C}(t)$，如上. 这是一个主理想，其生成元 h 是 f 和 g 在$\mathcal{F}[x]$上(首一)的最大公因子.

如果 $h\neq 1$，它将是一个多项式，其系数含有关于 t 的多项式的分母. 我们乘以一个关于 t 的多项式以去掉 h 中的分母，得到一个多项式 $h_1\in\mathbf{C}[t, x]$. 我们可以假设 h_1 不能被任何形如 $t-\alpha$ 的多项式整除. 由于分母在$\mathcal{F}$中是单位，且 h 在$\mathcal{F}[x]$中整除 f 和 g，故 h_1 在$\mathcal{F}[x]$中也整除 f 和 g. 命题 11.9.9 表明 h_1 在 $\mathbf{C}[t, x]$中整除 f 和 g. 则 f 和 g 在 $\mathbf{C}[t, x]$中有一个共同的非常数因子. 此与假设矛盾.

故 f 和 g 在$\mathcal{F}[x]$中的最大公因子为 1，且 $1=rf+sg$，此处 $r, s\in\mathcal{F}[x]$. 我们去掉 r 和 s 的分母，方程 $1=rf+sg$ 两边同乘以一个合适的多项式 $u(t)$. 得到如下形式的方程：

$$u(t) = r_1(t,x)f(t,x) + s_1(t,x)g(t,x)$$

此处右边所有的项都是 $\mathbf{C}[t, x]$中的多项式. 这个方程表明如果(t_0, x_0)是 f 和 g 的一个

共同零点，则 t_0 为 u 的一个根. 但 u 是关于 t 的多项式，且一个仅有一个变量的非零多项式有有限多个根. 故在 f 和 g 的共同零点上，变量 t 只取有限多个值. 类似的推理可证 x 也只取有限多个值. 对于共同零点只给了有限多种可能. ■

定理 11.9.10 表明 $\mathbf{C}^2$ 中最有趣的代数簇是那些定义在多项式 $f(t, x)$的零点的轨迹上的簇.

注 一个多项式 $f(t, x)$在 $\mathbf{C}^2$ 中的零点的轨迹 X 称为 f 的黎曼曲面.

黎曼曲面也称为平面代数曲线——一个令人费解的短语. 作为一个拓扑空间，轨迹 X 是二维的. 把它称为一条代数曲线指的是 X 中的点仅依赖于一个复参数. 这里我们对黎曼曲面给出一个粗略的描述. 假设 f 是既约的——即它不是任何两个非常数的多项式的积，且 f 关于变量 x 有正的次数. 令

【11.9.11】
$$X = \{(t,x) \in \mathbf{C}^2 \mid f(t,x) = 0\}$$

是它的黎曼曲面，且令 T 表示复 t-平面. 映射$(t, x)\rightsquigarrow t$ 定义一个连续映射，我们称之为投影

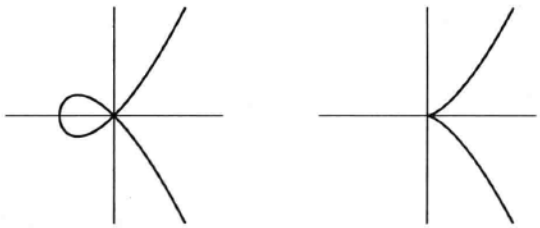
【11.9.12】
$$\pi : X \to T$$

我们将用这个投影来刻画 X. 然而，我们的描述需要从 X 中去掉“坏点”的一个有限集. 事实上，通常所说的黎曼曲面只在除去适当的有限子集后才与我们的定义一致. 轨迹$\{f=0\}$在某些点可能是“奇异的”，而 X 的其他点可能是“无穷远”点. 在无穷远的点解释如下(参见 11.9.17).

350

最简单的奇异点的例子是结点，在结点处曲面自交或出现尖点. $x^2 = t^3 - t^2$ 的轨迹在原点有一个结点，而 $x^2 = t^3$ 的轨迹在原点有一个尖点. 这些黎曼曲面的实点展示如下.

【11.9.13】图



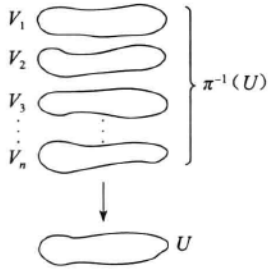
一些奇异曲线

为了避免重复说“除去一个有限子集”，我们用 X'记 X 的没有特别指定的有限子集的补，而这个有限子集允许变动. 只要结构在某点遇到麻烦，我们就简单地去掉这个点. 从本质上讲这里做的一切以及我们何时回到第十五章黎曼曲面时将仅对 X'成立. 我们手头保留 X 作为参考.

黎曼曲面的描述将作为复 t-平面 T 的分支覆盖. 这里给出的覆盖空间的定义假设空间是豪斯道夫空间([Munkres]p. 98). 如果你不知道它是什么意思，可以忽略这一点. 我们感兴趣的集合是豪斯道夫空间，因为它们是 $\mathbf{C}^2$ 的子集.

【11.9.14】定义 令 X 与 T 是豪斯道夫空间. 一个连续映射 $\pi: X \to T$ 是 n-叶覆盖空间，如果每个纤维由 n 个点组成，并且它有如下性质：令 x_0 是 X 的一个点，且设 $\pi(x_0)=t_0$，则 π 将 X 中点 x_0 的开邻域 U 同胚地映射到 T 中点 t_0 的开邻域 V.

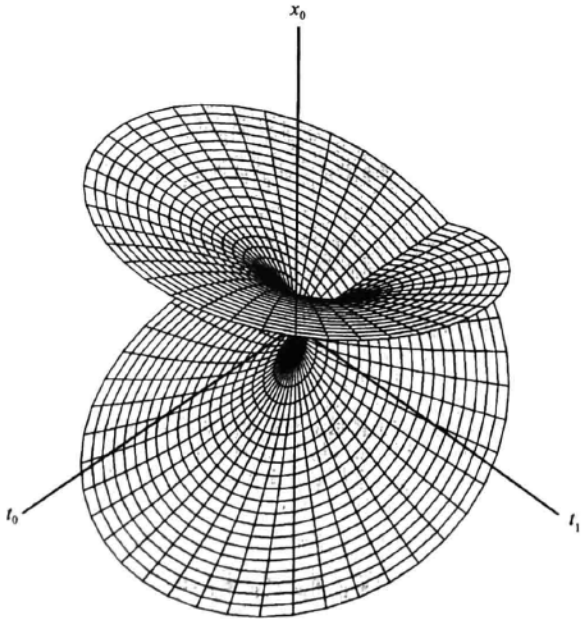
从 X 到复平面 T 的映射 π 是 n-叶分支覆盖，如果 X 不含有孤立点且 π 的纤维是有限的，并且如果存在 T 的有限点集 Δ(称为分支点)，使得映射 $(X-\pi^{-1}\Delta)\to(T-\Delta)$ 是 n-叶覆盖空间. 为了强调，覆盖空间有时也叫无分支覆盖.



无分支覆盖的一部分

图 11.9.15 描绘了多项式 x^2-t 的黎曼曲面，它是 T 在点 $t=0$ 处分叉的 2-叶覆盖. 图形通过用实部和虚部写出 t 和 x 得到，这里 $t=t_0+t_1\mathrm{i}$，$x=x_0+x_1\mathrm{i}$，去掉 x 的虚部 x_1 得到了一维空间的曲面. 它到平面的进一步投影用标准绘图学描绘.

【11.9.15】图



黎曼曲面 $x^2=t$

351
≀
352

投影曲面沿负 t_0 轴与自身相交，尽管黎曼曲面自身不相交. 每个负实数 t 有两个纯虚平方根，这些平方根的实部为 0，并且这在投影曲面里产生了自相交.

已知一个分支覆盖 $X\to T$，在集合 Δ 中的点作为分支点，尽管这样描述并不精确：当我们添加任意有限点集到 Δ 时，定义性质仍然成立. 故我们允许 Δ 的某些点不必包含在里面——它们不是"真的"分支点.

【11.9.16】定理 令 $f(t,x)$ 是 $\mathbf{C}[t,x]$ 中变量 x 的次数 $n>0$ 的既约多项式. 则 $f(t,x)$ 的黎曼曲面是复平面 T 的一个 n-叶覆盖.

证明 主要步骤是验证(11.9.14)的第一个条件，即纤维 $\pi^{-1}(t_0)$ 恰好由除去一个有限子集 Δ 外的 n 个点构成.

纤维 $\pi^{-1}(t_0)$ 中的点 (t_0,x_0) 是那些使 x_0 是单变量多项式 $f(t_0,x)$ 的根的点. 我们必须证明，除去 $t=t_0$ 的一个有限集外，这个多项式有 n 个不同的根. 把 $f(t,x)$ 写成 x 的多项式，其系数是 t 的多项式，比如说，$f(x)=a_n(t)x^n+\cdots+a_0(t)$，并且用 a_i^0 记 $a_i(t_0)$. 多项式 $f(t_0,x)=a_n^0x^n+\cdots+a_1^0x+a_0^0$ 次数至多为 n，于是，它至多有 n 个根. 所以，纤维 $\pi^{-1}(p)$ 至多含有 n 个点. 如果要么

【11.9.17】

(a) $f(t_0,x)$ 的次数小于 n，要么

(b) $f(t_0,x)$ 有重根，

则它将有少于 n 个的点.

当 t_0 是 $a_n(t)$ 的根时，第一种情形出现. (如果 t_0 是 $a_n(t)$ 的根，则当 $t_1\to t_0$，$f(t_1,x)$ 有一个根趋于无穷.)因为 $a_n(t)$ 是多项式，故存在有限多个这样的值.

考虑第二种情形. 对于复数 x_0，如果 $(x-x_0)^2$ 整除 $h(x)$，则 x_0 是多项式 $h(x)$ 的重根，并且这样的情况发生当且仅当 x_0 是 $h(x)$ 与它的导数 $h'(x)$ 的公共根(见练习 3.5). 这里 $h(x)=f(t_0,x)$. 第一个变量是固定的，所以，导数是偏导数 $\dfrac{\partial f}{\partial x}$. 回到两个变量的多项式 $f(t,x)$，我们看到第二种情形在点 (t_0,x_0) 出现，而这个点是 f 与 $\dfrac{\partial f}{\partial x}$ 的公共零点. 现在，f 不能整除它的偏导数，其 x 有较低的次数. 因为假设 f 是既约的，故 f 与 $\dfrac{\partial f}{\partial x}$ 没有公共非常数因子. 定理 11.9.10 告诉我们有有限多个零点.

我们现在检验(11.9.14)的第二个条件. 令 t_0 是 T 的点使得纤维 $\pi^{-1}(t_0)$ 由 n 个点组成，且设 (t_0,x_0) 是 X 在纤维里的点. 这样，x_0 是 $f(t_0,x)$ 的单根，所以，$\dfrac{\partial f}{\partial x}$ 在这一点不为零. 隐函数定理 A.4.3 蕴含着可在 t_0 的一个邻域里解出 x 作为 t 的函数 $x(t)$，使得 $x(t_0)=x_0$. 涉及覆盖空间定义里的邻域 U 是这个函数的图. ■

代数几何对于我来说是令人激动的代数.

——Solomon Lefschetz

练　习

第一节　环的定义

1.1　证明 $7+\sqrt[3]{2}$ 和 $\sqrt{3}+\sqrt{-5}$ 是代数数.

1.2　证明：对 $n\neq 0$，$\cos(2\pi/n)$ 是一个代数数.

1.3　令 $\mathbf{Q}[\alpha,\beta]$ 表示复数 $\mathbf{C}$ 的包含有理数 $\mathbf{Q}$ 和元素 $\alpha=\sqrt{2}$ 与 $\beta=\sqrt{3}$ 的最小子环. 令 $\gamma=\alpha+\beta$. 问 $\mathbf{Q}[\alpha,\beta]=\mathbf{Q}[\gamma]$ 成立吗？$\mathbf{Z}[\alpha,\beta]=\mathbf{Z}[\gamma]$ 成立吗？

1.4　令 $\alpha=\frac{1}{2}\mathrm{i}$. 证明 $\mathbf{Z}[\alpha]$ 的元素在复平面上是稠密的.

1.5　确定 $\mathbf{R}$ 的所有为离散集合的子环.

1.6　在下列两种情况下确定 S 是否为 R 的一个子环：

(a) S 是所有形如 a/b 的有理数集合，其中 b 不能被 3 整除，且 $R=\mathbf{Q}$.

(b) S 是函数集 $\{1,\cos nt,\sin nt\}(n\in\mathbf{Z})$ 的任意整系数线性组合的全体，且 R 是 t 的所有实值函数的集合.

1.7　确定所给结构是否构成环. 如果不是环，确定哪条环公理成立，哪条环公理不成立：

(a) U 是一个任意集合，且 R 是 U 的子集的集合. R 中元素的加法与乘法按规则 $A+B=(A\cup B)-(A\cap B)$ 和 $A\cdot B=A\cap B$ 定义.

(b) R 是 $\mathbf{R}\to\mathbf{R}$ 的连续函数的集合. 加法和乘法按规则 $[f+g](x)=f(x)+g(x)$ 和 $[f\circ g](x)=f(g(x))$ 定义.

1.8　确定下列环中的单位：(a)$\mathbf{Z}/12\mathbf{Z}$　(b)$\mathbf{Z}/8\mathbf{Z}$　(c)$\mathbf{Z}/n\mathbf{Z}$

1.9　令 R 是一个带有两个合成法则的满足除了加法的交换律之外的所有环公理的集合. 用分配律证明加法交换律成立，故 R 是一个环.

第二节　多项式环

2.1　对怎样的正整数 n，x^2+x+1 在 $[\mathbf{Z}/(n)][x]$ 上整除 $x^4+3x^3+x^2+7x+5$？

2.2　令 F 是一个域，所有形式幂级数 $p(t)=a_0+a_1t+a_2t^2+\cdots$ 的集合构成一个环，其中 $a_i\in F$，常记作 $F[[t]]$. 形式幂级数指的是其系数在 F 中构成任意一个元素数列. 并不要求级数收敛. 证明 $F[[t]]$ 是一个环，并确定其单位.

第三节　同态与理想

3.1　证明环 R 的一个理想是加群 R^+ 的一个子群.

3.2　证明高斯整数环的任意非零理想包含一个非零整数.

3.3　求出下列映射的核的生成元：

(a) $\mathbf{R}[x,y]\to\mathbf{R}$ 由 $f(x,y)\rightsquigarrow f(0,0)$ 定义.

(b) $\mathbf{R}[x]\to\mathbf{C}$ 由 $f(x)\rightsquigarrow f(2+\mathrm{i})$ 定义.

(c) $\mathbf{Z}[x]\to\mathbf{R}$ 由 $f(x)\rightsquigarrow f(1+\sqrt{2})$ 定义.

(d) $\mathbf{Z}[x]\to\mathbf{C}$ 由 $x\rightsquigarrow\sqrt{2}+\sqrt{3}$ 定义.

(e) $\mathbf{C}[x,y,z]\to\mathbf{C}[t]$ 由 $x\rightsquigarrow t$，$y\rightsquigarrow t^2$，$z\rightsquigarrow t^3$ 定义.

3.4　令 $\varphi:\mathbf{C}[x,y]\to\mathbf{C}[t]$ 是一个同态，且映 $x\rightsquigarrow t+1$，$y\rightsquigarrow t^3-1$. 确定 $K=\ker\varphi$，并证明 $\mathbf{C}[x,y]$ 的每个包含 K 的理想 I 可由两个元素生成.

3.5　系数属于一个域 F 的多项式 f 的导数由微积分公式 $(a_nx^n+\cdots+a_1x+a_0)'=na_nx^{n-1}+\cdots+1a_1$ 定义.

354

整系数理解为用唯一同态 $\mathbf{Z}\to F$ 定义的 F 中的元.

(a) 证明乘法法则$(fg)'=f'g+fg'$和链式求导法则$(f\circ g)'=(f'\circ g)g'$.

(b) 令 a 是 F 中一个元素. 证明 a 是一个多项式 f 的重根当且仅当它是 f 与其导数 f'的公共根.

3.6 环 R 的一个自同构是 R 到 R 自身的一个同构. 令 R 是一个环，且令 $f(y)$是系数在 R 中的一个变量 y 的一个多项式. 证明由 $x\rightsquigarrow x+f(y)$，$y\rightsquigarrow y$ 定义的映射 $R[x,y]\to R[x,y]$是 $R[x,y]$的一个自同构.

3.7 确定多项式环 $\mathbf{Z}[x]$的自同构(参见练习 3.6).

3.8 令 R 是具有素数特征 p 的环. 证明由 $x\rightsquigarrow x^p$ 定义的映射 $R\to R$ 是一个环同态. (称为弗洛贝尼乌斯映射.)

3.9 (a) 环 R 的一个元素 x 称为幂零的，如果它的某个幂为 0. 证明如果 x 是幂零的，则 $1+x$ 为单位.

(b) 假设 R 有素数特征 $p\neq 0$. 证明如果 a 是一个幂零元，则 $1+a$ 是幂单位元，即 $1+a$ 的某个幂等于 1.

3.10 确定系数在一个域 F 上的形式幂级数环 $F[[t]]$的所有理想(参见练习 2.2).

3.11 令 R 是一个环，且令 I 是多项式环 $R[x]$的一个理想. 令 n 为 I 中非零元的最低次数.

证明或举反例：I 包含一个次数为 n 的首一多项式当且仅当 I 是一个主理想.

3.12 令 I 和 J 是环 R 的理想，证明由形如 $x+y$，$x\in I$，$y\in J$ 的元素构成的集合 $I+J$ 是一个理想. 这个理想称为理想 I 和 J 的和.

3.13 令 I 和 J 是环 R 的理想. 证明交 $I\cap J$ 是一个理想. 举例说明积的集合$\{xy\mid x\in I,\ y\in J\}$未必是一个理想，但有限和$\sum x_v y_v$，$x_v\in I$，$y_v\in J$ 的集合是一个理想. 这个理想被称为积理想，记作 IJ. IJ 和$I\cap J$之间有什么关系?

第四节 商环

4.1 考虑由映射 $x\rightsquigarrow 1$ 定义的同态 $\mathbf{Z}[x]\to\mathbf{Z}$. 解释将对应定理应用于此同态映射时，对于$\mathbf{Z}[x]$的理想有何结论.

4.2 由对应定理，$\mathbf{Z}[x]$的包含 x^2+1 的理想是什么?

4.3 识别下列环：(a) $\mathbf{Z}[x]/(x^2-3,\ 2x+4)$ (b) $\mathbf{Z}[\mathrm{i}]/(2+\mathrm{i})$ (c) $\mathbf{Z}[x]/(6,\ 2x-1)$ (d) $\mathbf{Z}[x]/(2x^2-4,\ 4x-5)$ (e) $\mathbf{Z}[x]/(x^2+3,\ 5)$.

355 4.4 环 $\mathbf{Z}[x]/(x^2+7)$与 $\mathbf{Z}[x]/(2x^2+7)$同构吗?

第五节 元素的添加

5.1 令 $f=x^4+x^3+x^2+x+1$ 且令 α 表示 x 在环 $R=\mathbf{Z}[x]/(f)$中的剩余. 将$(\alpha^3+\alpha^2+\alpha)(\alpha^5+1)$用 R 的基$(1,\alpha,\alpha^2,\alpha^3)$表示.

5.2 令 $a\in R$，R 为一个环. 如果添加具有关系 $\alpha=a$ 的元素 α 我们希望得到一个与 R 同构的环. 证明此结论成立.

5.3 刻画从 $\mathbf{Z}/12\mathbf{Z}$ 中通过添加 2 的逆元所得到的环.

5.4 确定由 $\mathbf{Z}$ 添加满足下列关系集的元素 α 后得到的环 R'的结构：

(a) $2\alpha=b$，$6\alpha=15$ (b) $2\alpha-6=0$，$\alpha-10=0$ (c) $\alpha^3+\alpha^2+1=0$，$\alpha^2+\alpha=0$

5.5 是否存在域 F 使得环 $F[x]/(x^2)$与 $F[x]/(x^2-1)$同构?

5.6 令 a 是环 R 中的一个元素，令 R'是通过添加 a 的逆元到 R 上得到的环 $R[x]/(ax-1)$. 令 α 表示 x 的剩余(a 在 R'中的逆).

(a) 证明 R'中每个元素 β 可写成形式 $\beta=a^k b$，$b\in R$.

(b) 证明映射 $R\to R'$的核是 R 中满足 $a^n b=0$ 对某个 $n>0$ 成立的元素 b 的集合.

(c) 证明 R' 为零环当且仅当 a 是幂零的(参见练习 3.9).

5.7 令 F 是一个域，且令 $R=F[t]$是一个多项式环. 令 R'是通过添加 t 的逆元到 R 得到的环扩张 $R[x]/(tx-1)$. 证明这个环可看做劳伦多项式环，它是 t 的幂(包括负方幂)的有限线性组合.

第六节 积环

6.1 令 $\varphi:\mathbf{R}[x]\to\mathbf{C}\times\mathbf{C}$ 是由 $\varphi(x)=(1, i)$和 $\varphi(r)=(r, r)$，$r\in\mathbf{R}$ 定义的同态，确定 φ 的核与像.

6.2 $\mathbf{Z}/(6)$与积环 $\mathbf{Z}/(2)\times\mathbf{Z}/(3)$同构吗？$\mathbf{Z}/(8)$与 $\mathbf{Z}/(2)\times\mathbf{Z}/(4)$同构吗？

6.3 对阶为 10 的环分类.

6.4 在每一种情形，刻画在域 $\mathbf{F}_2$ 上通过添加满足给定关系的元素 α 后得到的环：

(a) $\alpha^2+\alpha+1=0$ (b) $\alpha^2+1=0$ (c) $\alpha^2+\alpha=0$

6.5 假设添加满足关系 $\alpha^2=1$ 的元素 α 到实数集合 $\mathbf{R}$ 上，证明所得到的环同构于积 $\mathbf{R}\times\mathbf{R}$.

6.6 刻画由积环 $\mathbf{R}\times\mathbf{R}$ 添加元素(2, 0)的逆元后得到的环.

6.7 证明在环 $\mathbf{Z}[x]$中，主理想(2)与(x)的交$(2)\cap(x)$是主理想$(2x)$，且商环 $R=\mathbf{Z}[x]/(2x)$同构于由满足 $f(0)\equiv n(\mathrm{mod}2)$的元素对$(f(x), n)$所构成的积环 $\mathbf{F}_2[x]\times\mathbf{Z}$ 的子环.

6.8 令 I 和 J 是环 R 的理想且满足 $I+J=R$.

(a) 证明 $IJ=I\cap J$(参见练习 3.13).

(b) 证明中国剩余定理：对 R 的元素对 a，b，存在一个元素 x 满足 $x\equiv a(\mathrm{mod}I)$和 $x\equiv b(\mathrm{mod}J)$(记号 $x\equiv a(\mathrm{mod}I)$意思是 $x-a\in I$). 356

(c) 证明如果 $IJ=0$，则 $R\approx(R/I)\times(R/J)$.

(d) 刻画对应于(c)中积的分解中的幂等元.

第七节 分式

7.1 证明有限阶的整环是一个域.

7.2 令 R 是一个整环. 证明多项式环 $R[x]$也是一个整环，并确定 $R[x]$中的单位.

7.3 存在恰好含有 15 个元素的整环吗？

7.4 证明域 F 上的形式幂级数环 $F[[x]]$的分式域可通过添加 x 的逆元(即添加 α，使得 $\alpha x=1$)得到，找到这个域中元素的一个简洁的描述(参见练习 11.2.1).

7.5 整环 R 的一个不包含零且在乘法下封闭的子集 S 称为一个**乘法集**. 给定一个乘法集 S，定义 S-分式为形如 a/b 的元素，其中 $b\in S$. 证明 S-分式的等价类构成一个环.

第八节 极大理想

8.1 在 $\mathbf{Z}[x]$中哪个主理想是极大理想？

8.2 确定下列环的极大理想：

(a) $\mathbf{R}\times\mathbf{R}$ (b) $\mathbf{R}[x]/(x^2)$ (c) $\mathbf{R}[x]/(x^2-3x+2)$ (d) $\mathbf{R}[x]/(x^2+x+1)$

8.3 证明环 $\mathbf{F}_2[x]/(x^3+x+1)$是一个域，但 $\mathbf{F}_3[x]/(x^3+x+1)$不是域.

8.4 建立 $\mathbf{R}[x]$的极大理想与上半平面上点之间的一一对应.

第九节 代数几何

9.1 令 I 是由 $\mathbf{C}[x, y]$中多项式 y^2+x^3-17 生成的主理想. 下列哪个集合生成商环 $R=\mathbf{C}[x, y]/I$ 中的极大理想：$(x-1, y-4)$，$(x+1, y+4)$，(x^3-17, y^2)？

9.2 令 f_1，…，f_r 是以 x_1，…，x_n 为变量的复多项式，令 V 是它们的公共零点所形成的簇，且令 I 是由 f_1，…，f_r 生成的多项式环 $R=\mathbf{C}[x_1, \cdots, x_n]$的理想. 定义商环 $\overline{R}=R/I$ 到 V 中连续的复值函数环 $\mathcal{R}$ 上的一个同态.

9.3 令 $U=\{f_i(x_1,\cdots,x_m)=0\}$，$V=\{g_j(y_1,\cdots,y_n)=0\}$ 分别是 $\mathbf{C}^m$ 和 $\mathbf{C}^n$ 上的簇．证明由方程组 $\{f_i(x)=0,\ g_j(y)=0\}$ 在 x，y 一空间 $\mathbf{C}^{m+n}$ 上定义的簇是集合的积 $U\times V$.

9.4 令 U 和 V 是 $\mathbf{C}^n$ 中的簇．证明其并 $U\cup V$ 和交 $U\cap V$ 是簇．$U\cap V=\varnothing$ 的代数意义是什么？$U\cup V=\mathbf{C}^n$ 的代数意义是什么？

9.5 证明由一个多项式集合 $\{f_1,\cdots,f_r\}$ 的零元定义的簇仅与它们生成的理想有关.

9.6 证明 $\mathbf{C}^2$ 的每一个簇是有限多个点和代数曲线的并.

9.7 在下面的每一种情形确定两个轨迹在 $\mathbf{C}^2$ 中的交点.

(a) $y^2-x^3+x^2=1$，$x+y=1$　(b) $x^2+xy+y^2=1$，$x^2+2y^2=1$

357 (c) $y^2=x^3$，$xy=1$　(d) $x+y^2=0$，$y+x^2+2xy^2+y^4=0$

9.8 多项式环 $\mathbf{C}[x,y]$ 中哪个理想包含 x^2+y^2-5 和 $xy-2$?

9.9 一条既约平面代数曲线 C 是既约多项式 $f(x,y)$ 在 $\mathbf{C}^2$ 中的零点的轨迹．C 的一个点 p 叫做曲线的奇异点，如果在 p 点有 $f=\partial f/\partial x=\partial f/\partial y=0$．否则 p 叫做非奇异点．证明既约曲线只有有限个奇异点.

9.10 令 L 是 $\mathbf{C}^2$ 中的(复)直线 $\{ax+by+c=0\}$，且令 C 是代数曲线 $\{f(x,y)=0\}$，其中 f 是次数为 d 的不可约多项式．证明除非 $C=L$，否则 $C\cap L$ 至多含有 d 个点.

9.11 令 C_1 和 C_2 分别是没有公共线性因子的两个二次多项式 f_1 和 f_2 的零点.

(a) 令 p 和 q 是 C_1 和 C_2 的不同的交点，且令 L 是通过 p 和 q 的(复)直线．证明存在不全为零的常数 c_1 和 c_2 使得 $g=c_1f_1+c_2f_2$ 同样在 L 上消失．并证明 g 是线性多项式之积．(提示：使 g 在 L 上的第三个点上消失.)

(b) 证明 C_1 和 C_2 至多有 4 个公共点.

9.12 以两种方式证明三个多项式 $f_1=t^2+x^2-2$，$f_2=tx-1$，$f_3=t^3+5tx^2+1$ 在 $\mathbf{C}[x,y]$ 上生成单位理想：通过证明它们没有公共的零点，且可以通过将 1 写成带有多项式系数的 f_1，f_2，f_3 的线性组合来证明.

*9.13 令 $\varphi:\mathbf{C}[x,y]\to\mathbf{C}[t]$ 在 $\mathbf{C}$ 上为恒等映射的同态，映 $x\rightsquigarrow x(t)$，$y\rightsquigarrow y(t)$，且 $x(t)$，$y(t)$ 不都是常数．证明 $\ker\varphi$ 是一个主理想.

杂题

M.1 证明或举反例：如果对非零环 R 中每个元素 a 有 $a^2=a$，则 R 有特征 2.

M.2 一个半群 S 是一个合成法则满足结合律且有单位元的集合．令 S 是一个交换半群且满足消去律：若 $ab=ac$，则 $b=c$．证明 S 可以嵌入到一个群中.

M.3 令 R 表示实数列 $a=(a_1,a_2,a_3,\cdots)$ 的集合，其中 a 具有性质：对某个充分大的 n，$a_n=a_{n+1}=\cdots$ 加法与乘法按照分量进行，即加法是向量的加法，乘法定义为 $ab=(a_1b_1,a_2b_2,\cdots)$．证明 R 是一个环，并确定其极大理想.

M.4 (a)对包含 $\mathbf{C}$ 且在 $\mathbf{C}$ 上向量空间的维数为 2 的环 R 进行分类.

(b) 对 3 维的情况做与(a)同样的分类.

M.5 定义 $\varphi:\mathbf{C}[x,y]\to\mathbf{C}[x]\times\mathbf{C}[y]\times\mathbf{C}[t]$，使得 $f(x,y)\rightsquigarrow(f(x,0)),f(0,y),f(t,t))$．确定此映射的像，并求其核的生成元.

M.6 证明 $y=\sin x$ 在 $\mathbf{R}^2$ 上的轨迹不位于 $\mathbf{C}^2$ 上的任何代数曲线上.

*M.7 令 X 表示闭单位区间 $[0,1]$，令 R 表示连续函数 $X\to\mathbf{R}$ 的环.

(a) 令 $f_1,\cdots,f_n$ 是在 X 上没有公共零点的函数．证明由这些函数生成的理想是单位理想．提示：考虑 $f_1^2+\cdots+f_n^2$.

358 (b) 建立 R 的极大理想与区间中的点之间的一一对应.

第十二章　因子分解

你也许认为人们知道多项式的一切.

——*Serge Lang*

第一节　整数的因子分解

本章学习环中的除法，由于它以整数环的性质为模型，因此我们将先复习这些性质，其中一些在本书前几章就已不加说明地使用了，有些已被证明.

由一个性质可得出所有其他性质，这就是带余除法：若 a，b 是整数且 $a>0$，则存在整数 q，r 使得

【12.1.1】　　$$b = aq + r, 0 \leqslant r < a$$

我们已经看到了带余除法的一些重要的结果：

【12.1.2】**定理**

(a) 整数环 $\mathbf{Z}$ 的每个理想都是主理想.

(b) 一对不全为零的整数 a，b 的最大公约数是 d，d 为正整数且具有下列性质：

(i) $\mathbf{Z}d=\mathbf{Z}a+\mathbf{Z}b$，

(ii) d 整除 a 且 d 整除 b，

(iii) 如果整数 e 整除 a 和 b，则 e 整除 d，

(iv) 存在整数 r，s 使得 $d=ra+sb$.

(c) 若素整数 p 整除两个整数的积 ab，则 p 整除 a 或 p 整除 b.

(d) 算术基本定理：每个正整数 $a\neq 1$ 可以写成积 $a=p_1\cdots p_k$ 的形式，其中 p_i 是正的素整数，且 $k>0$. 除了素因子的次序外，这个表达式是唯一的.

这些事实的证明将在下一节更广泛的背景下给予回顾.

第二节　唯一分解整环

看到整数环的因子分解，自然会问其他环是否也有类似的性质，在此便研究这个问题. 定理 12.1.2 的所有结论都能推广，相对来讲这样的环不多，但对域上的多项式环来说，这一定理的各个部分均可以拓广.

当研究因子分解时，自然会假定所给的环 R 是整环，因而可以使用消去律 11.7.1，而且我们不考虑元素零. 下面是一些要用到的术语：

【12.2.1】

u 是一个单位　如果 u 在环 R 中有乘法逆元.

a 整除 b　如果 $b = aq$ 对于某个 $q \in R$ 成立.

a 是 b 的真因子　如果 $b = aq$，且 a 和 q 都不是单位.

a 和 b 称为相伴的　如果它们互相整除，或如果 $b = ua$，且 u 为单位.

a 为既约的　如果它不是单位且没有真因子 —— 其仅有的因子为单位且是相伴的.

p 是素元　如果 p 不是单位，且当 p 整除积 ab，则 p 整除 a 或 p 整除 b.

这些概念可用由元素生成的主理想的语言来解释. 回忆由元素 a 生成的主理想 (a) 由 R 的所有能被 a 整除的元素组成. 于是

【12.2.2】

$$\begin{aligned}
u \text{ 是一个单位} &\Leftrightarrow (u) = (1)\\
a \text{ 整除 } b &\Leftrightarrow (b) \subset (a)\\
a \text{ 是 } b \text{ 的真因子} &\Leftrightarrow (b) < (a) < (1)\\
a \text{ 和 } b \text{ 称为相伴的} &\Leftrightarrow (a) = (b)\\
a \text{ 为既约的} &\Leftrightarrow (a) < (1), \text{且没有主理想 } (c) \text{ 使得 } (a) < (c) < (1)\\
p \text{ 是素元} &\Leftrightarrow ab \in (p) \text{ 蕴含 } a \in (p) \text{ 或 } b \in (p)
\end{aligned}$$

在继续讨论之前，我们看一个最简单的环中元素有多于一种分解的例子. 环 $R = \mathbf{Z}[\sqrt{-5}]$，它由所有形如 $a+b\sqrt{-5}$ 的复数组成，其中 a，b 为整数. 我们将在本章和下一章用这个环做例子. 在 R 中，整数 6 有两种分解方法：

【12.2.3】

$$2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$$

不难证明 2，3，$1+\sqrt{-5}$，$1-\sqrt{-5}$ 这些项不能继续分解，它们是环中的既约元.

首先，我们将带余除法抽象为一个程序. 为了使带余除法有意义，我们需要度量一个
360 元素大小. 一个整环 R 上的**尺度函数**可以是任何定义域为 R 上非零元集合且值域为非负整数集的函数 σ. 一个整环 R 是**欧几里得整环**，如果存在 R 上一个尺度函数 σ 使得带余除法在下面的意义下成为可能：

【12.2.4】　令 $a, b \in R, a \neq 0$. 存在元素 $q \in R$ 和 $r \in R$ 使得 $b = aq + r$，且或者 $r = 0$ 或者 $\sigma(r) < \sigma(a)$

关于带余除法最重要的事实是 r 为零当且仅当 a 整除 b.

【12.2.5】**命题**

(a) 整数环 $\mathbf{Z}$ 在尺度函数 $\sigma(a) = |a|$ 下是欧几里得整环.

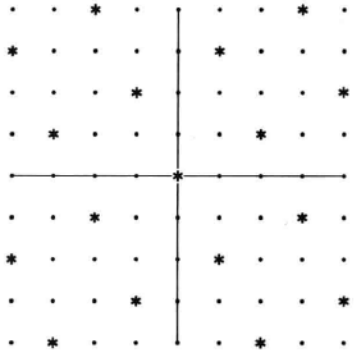
(b) 域 F 上单变量多项式环 $F[x]$ 在尺度函数 $\sigma(f) = f$ 的次数下是欧几里得整环.

(c) 高斯整数环 $\mathbf{Z}[\mathrm{i}]$ 在尺度函数 $\sigma(a) = |a|^2$ 下是欧几里得整环.

整数环和多项式环在第十一章已经讨论过. 在此我们证明高斯整数环是欧几里得整环. $\mathbf{Z}[\mathrm{i}]$ 的元素形成了复平面上的格点，给定非零元 α 的所有倍数构成主理想 (α)，它是相似的几何图形. 如果记 $\alpha = re^{i\theta}$，则 (α) 是 $\mathbf{Z}[\mathrm{i}]$ 的格点通过旋转 θ 度角并伸长 r 倍得到，正如

当 $\alpha=2+\mathrm{i}$ 时下图所示：

【12.2.6】图



高斯整数环的一个主理想

对于任何复数 β，存在格点 (α) 到 β 的平方距离小于 $|\alpha|^2$. 我们选取一个这样的点，比如 $\gamma=\alpha q$，且令 $r=\beta-\gamma$. 则 $\beta=\alpha q+r$，且 $|r|^2<|\alpha|^2$. 这里 $q\in\mathbf{Z}[\mathrm{i}]$，且如果 $\beta\in\mathbf{Z}[\mathrm{i}]$，则 $r\in\mathbf{Z}[\mathrm{i}]$.

带余除法不是唯一的：存在至多 4 种 γ 的选取.

注 一个整环如果其每一个理想都是主理想就称为主理想整环. 361

【12.2.7】**命题** 欧几里得整环是主理想整环.

证明 我们再一次模仿整数环是主理想整环的证明. 令 R 是带有尺度函数 σ 的欧几里得整环，且令 A 是 R 的理想. 我们必须证明 A 是主理想. 零理想是主理想，故假设 A 是非零理想. 则 A 包含非零元. 选取一个非零元 $a\in A$ 使得 $\sigma(a)$ 尽可能小，我们证明 A 是由元素 a 的倍数生成的主理想 (a).

因为 A 是一个理想，且 $a\in A$，故任何倍数 $aq\in A$，$q\in R$. 因此 $(a)\subset A$. 为了证明 $A\subset(a)$，任取元素 $b\in A$. 用带余除法写成 $b=aq+r$，其中 $r=0$ 或者 $\sigma(r)<\sigma(a)$. 则 $b\in A$，$aq\in A$，因此 $r=b-aq\in A$. 由于 $\sigma(a)$ 是最小值，故 $\sigma(r)<\sigma(a)$ 不成立，因此只有 $r=0$. 这就证明了 a 整除 b，因此 $b\in(a)$. 由 b 的任意性，$A\subset(a)$，因此 $A=(a)$. ■

令 a，b 是整环 R 上一对不全为零的元素，a，b 的最大公因子 d 是满足下列性质的元素：

(a) d 整除 a，d 整除 b，

(b) 如果 e 整除 a 和 b，则 e 整除 d.

任意两个最大公因子 d 和 d' 是相伴的元素. 第一个条件告诉我们 d 和 d' 整除 a 和 b，而第二个条件告诉我们 d 和 d' 相互整除.

然而，最大公因子可能不存在. 经常有这样的极大公因子 m，意思是 a/m 和 b/m 没有公共的真因子. 但这个元素不满足条件(b). 例如，在(12.2.3)的环 $\mathbf{Z}[\sqrt{-5}]$ 中，元素 $a=6$ 和 $b=2+2\sqrt{-5}$ 都能被 2 和 $1+\sqrt{-5}$ 整除. 这些是公因子的极大元，但是这两个元素彼此不整除.

最大公因子存在的一种情形是 a 和 b 没有除了单位元以外的公因子. 则 1 就是最大公

因子. 此时，a 和 b 称为是互素的.

在主理想整环上最大公因子总是存在的.

【12.2.8】命题 令 R 是主理想整环，令 a，b 是 R 上一对不全为零的元素. 理想 $(a, b)=Ra+Rb$ 的生成元 d 是 a，b 的最大公因子. 它有下面的性质：

(a) $Rd=Ra+Rb$.

(b) d 整除 a，d 整除 b.

(c) 如果 e 整除 a 和 b，则 e 整除 d.

(d) 存在 r，$s\in R$ 使得 $d=ra+sb$.

证明

证明实际上和整数环的情形是一样的. (a)重述为 d 生成理想 (a, b). (b)表示 a，$b\in Rd$. (d)表示 $d\in Ra+Rb$. 对于(c)，如果 e 整除 a 和 b，则 a 和 b 属于 Re. 在此情形，Re 包含 $Ra+Rb=Rd$，故 e 整除 d. ■

362

【12.2.9】推论 令 R 是主理想整环.

(a) 如果 a 和 b 是 R 中的互素元，则 1 是线性组合 $ra+sb$.

(b) R 中的元素是既约元当且仅当该元素是素元.

(c) R 的极大理想是既约元生成的主理想.

证明

(a) 由命题 12.2.8(d)可得.

(b) 在任何整环中，素元是既约元. 我们在下面的引理 12.2.10 中给出证明. 假设 R 是主理想整环且 q 是 R 中的既约元，q 整除积 ab. 必须证明：若 q 不整除 a，则 q 整除 b. 令 d 是 q 和 a 的最大公因子. 由于 q 是既约的，故其因子或为单位元或者与 q 相伴. 由于 q 不整除 a，故 d 不与 q 相伴. 因此 d 是单位元，q 和 a 互素，且 $1=ra+sq$，其中 r，$s\in R$. 两边乘以 b：$b=rab+sqb$. 方程右边两项都能被 q 整除，故 q 整除 b.

(c) 令 q 是既约元. 它的因子只有单位元和相伴元. 因此包含 (q) 的唯一主理想是 (q) 本身和单位理想 (1)(参见(12.2.2)). 由于 R 的理想是主理想，故这些是包含 (q) 的唯一理想. 因此 (q) 是极大理想. 反之，如果元素 b 有真因子 a，则 $(b)<(a)<(1)$，所以 (b) 本身不是极大理想. ■

【12.2.10】引理 在整环 R 中，素元是既约元.

证明 假设素元 p 是两个元素的积，比如 $p=ab$. 则 p 整除 a 和 b 其中之一，比如 a. 但是方程 $p=ab$ 也表明 a 整除 p. 故 a 和 p 是相伴的，且 b 是一个单位. 分解不是真分解. ■

对于一个整环，希望有什么与算术基本定理 12.1.2(d)类似的结果？我们可将分解唯一性所需要的叙述分成两部分. 第一，一个给定的元素可以写成既约元的乘积；第二，这个积实质上是唯一的.

环中的单位使得唯一性的叙述变得复杂. 单位因子必须忽略且相伴因子必须看成是等价的. 整数环的单位为 ±1，在这个环里，对正整数讨论是自然的. 类似地，在域上的多项式环 $F(x)$ 里，用首一多项式去讨论是自然的. 但是我们没有一种合理的方式把整环中的

元素正规化，最好别试.

我们说整环 R 上的分解是唯一的，如果整环 R 中的元素 a 有两种写为积的既约分解方式，比如，

【12.2.11】 $$p_1\cdots p_m = a = q_1\cdots q_n$$

则 $m=n$，且如果右边适当排序的话，可使得对于每个 i，p_i 和 q_i 相伴. 故在分解的唯一性的叙述中，相伴分解认为是等价的.

例如，在高斯整数环中，

$$(2+\mathrm{i})(2-\mathrm{i}) = 5 = (1+2\mathrm{i})(1-2\mathrm{i})$$

元素 5 的这两种分解是等价的，因为左右两边元素是相伴的：$-\mathrm{i}(2+\mathrm{i})=1-2\mathrm{i}$ 且 $\mathrm{i}(2-\mathrm{i})=1+2\mathrm{i}$. 363

讨论主理想比讨论元素要简洁，因为相伴元的主理想是相同的. 然而，讨论元素也不是很繁琐，我们在此还是讨论元素. 在下一章，理想的重要性就清楚了.

在我们尝试把一个元素 a 表示为既约元之积时，总是假设这个元素是非零的且不是单位. 这样，我们试图用下述方法分解 a：如果 a 本身是既约的，则已得到分解. 如果 a 不是既约的，则 a 有一个真因子，因而它以某种方式分解为乘积 $a=a_1b_1$，其中 a_1 和 b_1 都不是单位. 如果可能，继续分解 a_1 和 b_1，而且希望这一过程会停下来；换言之，希望在有限步后所有因子为既约的. 我们说在 R 中分解终止，就是指有限步后所有因子为既约的. 我们把分解成既约元的分解叫做既约分解.

一个整环 R 是唯一分解整环，如果它有下述性质：

【12.2.12】

- 分解终止.
- 元素的既约分解在上面的意义下是唯一的.

分解终止的条件用主理想有一个实用的描述：

【12.2.13】**命题** *设 R 是整环. 下列条件等价：*

- *因子分解过程在有限步后终止.*
- *R 中不包含主理想的无限的严格升链 $(a_1)<(a_2)<(a_3)<\cdots$.*

证明 假设分解过程不能终止，则有一个元素 a_1 有真分解使得这个分解过程至少对一个因子不能终止. 设真分解为 $a_1=a_2b_2$，且这个过程对 a_2 的分解不能终止. 由于 a_2 是 a_1 的真因子，故 $(a_1)<(a_2)$（参见(12.2.2)）. 用 a_2 替换 a_1 并重复上面的过程，我们得到一个无限升链.

反之，如果存在一个严格的升链 $(a_1)<(a_2)<(a_3)<\cdots$，则每个 (a_n) 都不是单位理想，因此，a_2 是 a_1 的真因子，a_3 是 a_2 的真因子，等等(12.2.2). 这表明分解过程不能终止. ■

我们很少遇到分解不能终止的环，后面我们会证明一个定理来解释原因（见推论 14.6.9），所以不必太担心. 实际上，分解的唯一性是导致大部分麻烦的所在. 因子分解为既约元通常是可能的，但即使是把相伴因子看成等价的，分解也未必是唯一的.

回到环 $R=\mathbf{Z}[\sqrt{-5}]$，不难证明 2，3，$1+\sqrt{-5}$，$1-\sqrt{-5}$ 都是既约的，而 R 的单位是 1 和 -1，所以 2 不是 $1+\sqrt{-5}$ 与 $1-\sqrt{-5}$ 的相伴元. 因此 $2\cdot 3=6=(1+\sqrt{-5})(1-\sqrt{-5})$ 是两种不同的分解方法；R 不是唯一分解整环. 364

【12.2.14】命题

(a) 令 R 是整环. 假设在 R 中分解可以终止. 则 R 是唯一分解整环当且仅当每个既约元是素元.

(b) 主理想整环是唯一分解整环.

(c) 整数环 $\mathbf{Z}$、高斯整数环 $\mathbf{Z}[\mathrm{i}]$和域 F 上的单变量多项式环 $F[x]$是唯一分解整环.

因此，在唯一分解整环中短语既约分解与素分解是同义词，但是多数环包含非素的既约元. 在环 $\mathbf{Z}[\sqrt{-5}]$中，元素 2 是既约元，但不是素元，因为 2 能整除积$(1+\sqrt{-5})(1-\sqrt{-5})$,但不整除其中任何一个因子.

(b) 的逆不真. 我们在下一节将看到整多项式环 $\mathbf{Z}[x]$是唯一分解整环，但不是主理想整环.

命题 12.2.14 的证明 首先，因为(c)里的环是欧几里得整环，因此是主理想整环. 由(b)知，(c)中的环均为唯一分解整环.

(a) 令 R 是一个环，其上每个既约元都是素元，且假设其中一个元素 a 采用两种方式分解为既约元的乘积，比如 $p_1\cdots p_m=a=q_1\cdots q_n$，其中 $m\leqslant n$. 如果 $n=1$，则 $m=1$ 且 $p_1=q_1$. 假设 $n>1$. 由于 p_1 是素元，故它整除 q_1，…，q_n 之一，比如 q_1. 由于 q_1 是既约元且 p_1 不是单位，故 q_1 和 p_1 是相伴的，不妨设 $p_1=uq_1$，此处 u 为单位. 我们移动单位因子到 q_2 上，用 uq_1 代替 q_1，用 $u^{-1}q_2$ 代替 q_2. 现在的结果是 $p_1=q_1$. 然后消去 p_1，并对 n 使用归纳法.

反过来，假设存在非素的既约元 p. 这样，存在元素 a 和 b 使得 p 整除它们的积 $r=ab$，比如说 $r=pc$，但 p 不整除 a 和 b. 通过将 a，b 和 c 分解为既约元的乘积，得到 r 的两个不等价的分解.

(b) 令 R 是一个主理想整环. 由于 R 的每个既约元都是素元(12.2.8)，只需证明分解可以终止(12.2.14). 我们利用证明 R 不含有无限的主理想的严格升链来证明. 假设给定了一个无限弱升链

$$(a_1)\subset(a_2)\subset(a_3)\subset\cdots$$

我们证明它不可能是严格升的.

【12.2.15】引理 令 $I_1\subset I_2\subset I_3\subset\cdots$ 是环 R 的理想的升链. 则 $I_1\subset I_2\subset I_3\subset\cdots$ 的并 $J=\bigcup I_n$ 是 R 的一个理想.

证明 如果 u，$v\in J$，则对某个 n，u，$v\in I_n$，从而 $u+v$ 及 ru 亦属于 I_n，其中 $r\in R$. 因此，它们也属于 J. 这就证明了 J 是一个理想. ■

将此引理应用于主理想链，且 $I_v=(a_v)$，并用 R 是主理想整环的假设得到并 J 是主理
365 想，比如说 $J=(b)$. 由于 b 属于理想(a_n)的并，因此它也属于其中一个理想. 但如果 $b\in(a_n)$，则$(b)\subset(a_n)$. 而另一方面，$(a_n)\subset(a_{n+1})\subset(b)$，因而$(b)=(a_n)=(a_{n+1})$. 这个链不是严格升的. ■

在唯一分解整环中可以利用元素的既约分解来确定元素 a 是否整除元素 b.

【12.2.16】命题 令 R 是一个唯一分解整环.

(a) 令 $a=p_1\cdots p_m$ 和 $b=q_1\cdots q_n$ 是 R 中两个元素的既约分解. 则 a 整除 b 当且仅当 $m\leqslant n$ 且适当调整 q_j 的次序，使得对于 $i=1$，…，m，p_i 是 q_i 的相伴元.

(b) 任何不全为零的元素对 a 和 b 都有最大公因子.

证明

(a) 的证明与命题 12.2.14(a)非常相似. a 的既约因子是素元. 如果 a 整除 b，则 p_1 整除 b，因此 p_1 整除某个 q_i，比如 q_1. 则 p_1 和 q_1 是相伴的. 从 a 中消去 p_1，从 b 中消去 q_1 后，断言由归纳法得证. 我们省去(b)的证明. ■

注意 任意两个数 a 和 b 的最大公因子是相伴的. 但是只有在唯一分解整环是主理想整环时，最大公因子(尽管存在)才不必具有形式 $ra+sb$. 2 和 x 在唯一分解整环 $\mathbf{Z}[x]$ 上的最大公因子为 1，但是我们不能将 1 写成这些整系数多项式的线性组合.

我们回顾一下对域上的多项式环 $F[x]$ 的这个重要情形已得出的结论. 多项式环 $F[x]$ 的单位是非零常数. 我们可以把非零多项式的首项系数提取出来得到首一多项式，而首一多项式 f 仅有的首一相伴元是 f 自身. 通过使用首一多项式，可以避免相伴分解造成的模糊认识. 考虑到这一点，下面的定理由命题 12.2.14 可得.

【12.2.17】定理 令 $F[x]$ 是域 F 上单变量的多项式环.

(a) 两个不全为零的多项式 f 和 g 有唯一的首一最大公因子 d，且存在多项式 r，s 使得 $rf+sg=d$.

(b) 如果两个多项式 f 和 g 没有非常数的公因子；则存在多项式 r，s 使得 $rf+sg=1$.

(c) 每个 $F[x]$ 上的既约多项式 p 是 $F[x]$ 上的素元：如果 p 整除积 fg，则 p 整除 f 或者 p 整除 g.

(d) 唯一分解：$F[x]$ 上每个首一多项式可以写成 $F(x)$ 上首一既约多项式的乘积 $p_1\cdots p_k$ 且 $k\geqslant 0$. 这个分解除了项的顺序之外是唯一的.

在今后，我们提到系数在一个域上的两个多项式的最大公因子时，指的是具有上面性质(a)的唯一的首一多项式. 最大公因子有时记作 $\gcd(f, g)$.

系数在域 F 上的两个不全为零的多项式 f 和 g 的最大公因子 $\gcd(f, g)$ 可以通过反复使用带余除法得到，这个过程称为欧几里得算法，在第二章第三节整数环中提到过：假设 g 的 366
次数至少等于 f 的次数. 将 g 写成 $g=fq+r$，此处 r 是余式，如果 r 非零，则次数低于 f 的次数. 于是 $\gcd(f, g)=\gcd(f, r)$. 如果 $r=0$，则 $\gcd(f, g)=f$. 如果 $r\neq 0$，则用 r 和 f 代替 f 和 g，重复上面的过程. 由于多项式的次数变低，因此这个过程止于有限步. 可用类似方法确定欧几里得整环上的最大公因子.

在复数域上任何正次数多项式都有根 α，因此有形如 $x-\alpha$ 的因子. 既约多项式是线性的，首一多项式的既约分解有下面的形式：

【12.2.18】
$$f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$$

其中 α_i 是 $f(x)$ 的根，重根重复计算. 分解的唯一性是显然的.

当 $F=\mathbf{R}$ 时，有两类既约多项式：线性的和二次的. 一个实二次多项式 x^2+bx+c 是既约的当且仅当判别式 $b^2-4c<0$，此时多项式有一对共轭的复根. 事实上，每个复数域上的既约多项式是线性的蕴含了没有次数大于 2 的实多项式.

【12.2.19】命题 令 α 是实多项式 f 的一个非实数的复根. 则其复共轭 $\bar{\alpha}$ 也是 f 的一个根. 二次多项式 $q=(x-\alpha)(x-\bar{\alpha})$ 有实系数，且整除 f. □

有理系数的多项式环 $\mathbf{Q}[x]$ 上的多项式的分解更有趣，因为在 $\mathbf{Q}[x]$ 上存在任意次数的既约多项式. 这在下两节解释. 在这种情形下既约分解的形式和唯一性都不是显然的.

为供以后参考，注意下面的基本事实：

【12.2.20】命题 系数在域 F 上的 n 次多项式 f 在 F 中至多有 n 个根.

证明 一个元素 α 是 f 的根当且仅当 $x-\alpha$ 整除 f(11.2.11). 若如此，则 $f(x)=(x-\alpha)q(x)$，其中 $q(x)$ 是 $n-1$ 次多项式. 令 β 是 f 的异于 α 的根，令 $x=\beta$，有 $0=(\beta-\alpha)q(\beta)$. 由于 $\beta\neq\alpha$，故 β 必是 $q(x)$ 的根. 对多项式次数应用归纳法，在域 F 上 $q(x)$ 至多有 $n-1$ 个根，加上根 α，则 f 至多有 n 个根. ■

第三节 高斯引理

每个首一的有理系数多项式 $f(x)$ 可以唯一表示为形式 $p_1\cdots p_k$，其中 p_i 是环 $\mathbf{Q}[x]$ 上首一既约的多项式. 但是，假设多项式 $f(x)$ 有整数系数，且其在 $\mathbf{Q}[x]$ 里分解. 这些因子是 367 整系数的多项式吗？我们将看到回答是肯定的，而且 $\mathbf{Q}[x]$ 是唯一分解整环.

下面是整系数多项式的既约分解的一个例子：

$$6x^3+9x^2+9x+3=3(2x+1)(x^2+x+1)$$

正如我们所看到的，$\mathbf{Z}[x]$ 上的既约分解较 $\mathbf{Q}[x]$ 上的要稍微复杂一些. 素整数是 $\mathbf{Z}[x]$ 上的既约元，它们也可能出现在一个多项式的分解中. 而且如果我们要保留整数系数，就不能要求是首一的因子.

研究 $\mathbf{Z}[x]$ 上的因子分解有两个主要工具. 第一个工具是将整系数多项式环看成是有理系数的多项式的环：

$$\mathbf{Z}[x]\subset\mathbf{Q}[x]$$

这样做会很有用，因为环 $\mathbf{Q}[x]$ 上的代数更简单.

第二个工具利用模素数 p 约简，同态

【12.3.1】 $$\psi_p:\mathbf{Z}[x]\to\mathbf{F}_p[x]$$

映 $x\rightsquigarrow x$(11.3.6). 我们经常把整系数多项式的像 $\psi_p(f)$ 记作 $\overline{f}$，虽然这个记号有点儿模棱两可，因为没有提到 p.

下面的引理应该是清楚的.

【12.3.2】引理 令 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 是整系数多项式，且令 p 是整素数. 下列叙述是等价的：

- p 整除 f 的每一个系数 $a_i\in\mathbf{Z}$.
- p 整除 $f\in\mathbf{Z}[x]$.
- $f\in\ker\psi_p$.

这个引理表明 ψ_p 的核可以很容易理解而不必提及这个映射. 但 ψ_p 是同态且它的像

$\mathbf{F}_p[x]$是整环的事实使得作为核的解释很有用.

注意 一个有理系数多项式 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 被称为是本原的，如果它是正次数的整系数多项式，且整数系数 a_0，a_1，…，a_n 的最大公因子是 1，多项式的首项系数 a_n 是正的.

【12.3.3】引理 令 f 是正次数的整多项式，其首相系数为正数. 下列条件是等价的：

- f 是本原的.
- f 不能被任何素数 p 整除.
- 对每一个整素数 p，$\psi_p(f)\neq 0$. ■

【12.3.4】命题

(a) 一个整数是 $\mathbf{Z}[x]$的素元当且仅当它是素整数. 故一个素整数 p 整除整多项式的积 fg 当且仅当 p 整除 f 或 p 整除 g.

(b) (高斯引理)本原多项式的积是本原的. 368

证明

(a) 显然，一个整数是素数如果它是 $\mathbf{Z}[x]$的既约元. 令 p 是素整数. 我们用横杠记号 $\overline{f}=\psi_p(f)$. 则 p 整除 fg 当且仅当$\overline{fg}=0$，且由于 $\mathbf{F}_p[x]$是一个整环，故 p 整除 fg 当且仅当$\overline{f}=0$ 或$\overline{g}=0$，即当且仅当 p 整除 f 或 p 整除 g.

(b) 假设 f 和 g 是本原多项式. 由于它们的首项系数均为正数，故积 fg 的首项系数也是正数. 而且，没有素数 p 整除 f 或 g，且由(a)，没有素数整除 fg. 故 fg 是本原的. ■

【12.3.5】引理 每个有理系数的正次数的多项式 $f(x)$可唯一地写成 $f(x)=cf_0(x)$，其中 c 是有理数，且 $f_0(x)$是本原多项式. 而且，c 是整数当且仅当 f 是整多项式. 如果 f 是整多项式，则 f 的系数的最大公因子是$\pm c$.

证明 要求 $f_0(x)$，首先用一个整数 d 乘 f 以去掉系数中的分母. 这样得到一个整系数多项式 $df=f_1$. 然后将 f_1 的系数的最大公约数提取出来，并调整首项系数的正负号. 得到的多项式 $f_0(x)$是本原的，且 $f=cf_0$ 对某个有理数 c 成立. 这证明了存在性.

如果 f 是整多项式，就不需要去分母了. 则 c 是整数，且加上符号，如前所述，正是系数的最大公约数.

积的唯一性是重要的，所以，我们仔细地检验. 假设给定有理数 c 和 c'以及本原多项式 f_0 和 f_0'使得 $cf_0=c'f_0'$. 我们将证明 $f_0=f_0'$. 由于 $\mathbf{Q}[x]$是整环，故有 $c=c'$.

方程 $cf_0=c'f_0'$两边同乘以一个整数，如果必要，调整一下正负号，从而化简为 c 和 c'为正整数. 如果 $c\neq 1$，则选取素整数 p 整除 c. 则 p 整除 $c'f_0'$. 命题 12.3.4(a)证明了 p 整除因子c'或因子 f_0'. 由于 f_0'是本原的，故它不能被 p 整除，所以 p 整除c'. 方程两边消去 p. 归纳化简得到 $c=1$ 的情形. 同样的推理可证明 $c'=1$. 故 $f_0=f_0'$. ■

【12.3.6】定理

(a) 令 f_0 是一个本原多项式，且令 g 是整多项式. 如果 f_0 在 $\mathbf{Q}[x]$中整除 g，则 f_0 在

$\mathbf{Z}[x]$中整除 g.

(b) 如果两个整多项式 f 和 g 在 $\mathbf{Q}[x]$上有非常数的公因子，则它们在 $\mathbf{Z}[x]$上有非常数的公因子.

证明

(a) 比如 $g=f_0q$，其中 q 有有理系数. 我们证明 q 有整系数. 记 $g=cg_0$ 且 $q=c'q_0$，g_0 和 q_0 是本原的. 则 $cg_0=c'f_0q_0$. 高斯引理告诉我们 f_0q_0 是本原的. 因此由引理 12.3.5 的唯一性的断言可知，$c=c'$且 $g_0=f_0q_0$. 由于 g 是整多项式，故 c 是整数. 因此 $q=cq_0$ 是整多项式.

(b) 如果整多项式 f 和 g 在 $\mathbf{Q}[x]$上有非常数的公因子 h，我们记 $h=ch_0$，其中 h_0 是
369 本原的，则 h_0 也在 $\mathbf{Q}[x]$上整除 f 和 g，且由(a)，h_0 在 $\mathbf{Z}[x]$上整除 f 和 g. ■

【12.3.7】命题

(a) 令 f 是首项系数是正数的整多项式. 则 f 是 $\mathbf{Z}[x]$上的既约元当且仅当它或为素整数或为 $\mathbf{Q}(x)$上既约的本原多项式.

(b) $\mathbf{Z}[x]$上的每个既约元是素元.

证明 命题 12.3.4(a)证明了对常数多项式(a)和(b)成立. 如果 f 是既约的且不为常数，则没有异于±1的整数因子，所以如果首项系数是正的，则它就是本原的. 假设 f 是本原多项式且在 $\mathbf{Q}[x]$上有真因子，比如 $f=gh$. 记 $g=cg_0$ 和 $h=c'h_0$，其中 g_0 和 h_0 是本原的. 则 g_0h_0 是本原的. 由于 f 也是本原的，故 $f=g_0h_0$. 因此 f 在 $\mathbf{Z}[x]$上有真因子. 故若 f 是 $\mathbf{Q}[x]$上的既约元，则也是 $\mathbf{Z}[x]$上的既约元. 显然，本原多项式在 $\mathbf{Z}[x]$上可约则在$\mathbf{Q}[x]$上也可约. 这就证明了(a).

令 f 是一个本原的既约多项式且整除两个整多项式的积 gh. 则 f 在 $\mathbf{Q}[x]$上是既约的. 由于 $\mathbf{Q}[x]$是主理想整环，故 f 是 $\mathbf{Q}[x]$上的素元(12.2.8)，所以 f 在 $\mathbf{Q}[x]$上整除 g 或 h. 由(12.3.6)，f 在 $\mathbf{Z}[x]$上整除 g 或 h. 这就证明了 f 是素元，即证明了(b). ■

【12.3.8】定理 多项式环 $\mathbf{Z}[x]$是唯一分解整环. 每个不是±1的非零多项式 $f(x)\in\mathbf{Z}[x]$可以写成积的形式：

$$f(x)=\pm\, p_1\cdots p_mq_1(x)\cdots q_n(x)$$

其中 p_i 是整素数，且 $q_j(x)$是一个本原的既约多项式. 这个表达式除了因子的次序外是唯一的.

证明 容易看出在 $\mathbf{Z}[x]$中分解是能终止的，故这个定理可以由命题 12.3.7 和 12.2.14 得到. ■

对于域 F 上两个变量的多项式环 $F[t,\ x]$，本节的结果有相似之处. 为建立这种相似，把 $F[t,\ x]$看成是系数为 t 的多项式的关于 x 的多项式环 $F[t][x]$. 与有理数域 $\mathbf{Q}$ 类似的是关于 t 的有理函数域 $F(t)$，即 $F[t]$的分式域. 记这个域为$\mathcal{F}$. 则 $F[t,\ x]$是多项式环 $\mathcal{F}[x]$的子环：

$$f=a_n(t)x^n+\cdots+a_1(t)x+a_0(t)$$

它的系数 $a_i(t)$是关于 t 的有理函数. 这一结论非常有用，因为$\mathcal{F}[x]$的每个理想都是主理想.

一个多项式 f 被称为是本原的，如果它是正次数的，其系数 $a_i(t)$ 是 $F[t]$ 中的多项式，这些系数的最大公因子是 1，而首项系数 $a_n(t)$ 是首一的. 一个本原多项式是多项式环 $F[t, x]$ 中的元素.

本原多项式的积仍是本原的，而且 $\mathcal{F}[x]$ 的每个元素 $f(t, x)$ 可以写成形式 $c(t)f_0(t, x)$，其中 f_0 是 $F[t, x]$ 上的本原多项式，c 是 t 的有理函数，二者在差一个常数因子的情形下是唯一确定的. 370

下面断言的证明与命题 12.3.4、定理 12.3.6 及 12.3.8 的证明几乎相同.

【12.3.9】定理 令 $F[t]$ 是域 F 带有一个变量的多项式环，且令 $\mathcal{F}=F(t)$ 是它的分式域.

(a) $F[t, x]$ 中的本原多项式的积是本原的.

(b) 令 f_0 是本原多项式，且令 g 是 $F[t, x]$ 中的多项式. 如果 f_0 在 $\mathcal{F}(x)$ 上整除 g，则 f_0 在 $F[t, x]$ 上整除 g.

(c) 如果 $F[t, x]$ 中两个多项式 f 和 g 在 $\mathcal{F}(x)$ 上有非常数的公因子，则它们在 $F[t, x]$ 中也有非常数的公因子.

(d) 令 f 是 $F[t, x]$ 中首相系数为首一多项式. 则 f 是 $F[t, x]$ 中的既约元当且仅当它或者为仅关于 t 的既约多项式或者为在 $\mathcal{F}(x)$ 上既约的本原多项式.

(e) 环 $F[t, x]$ 是唯一分解整环.

$\mathbf{Z}[x]$ 上的分解的结果还与系数在唯一分解整环 R 上的多项式的分解类似.

【12.3.10】定理 如果 R 是唯一分解整环，则有任意有限个变量的多项式环 $R[x_1, \cdots, x_n]$ 是唯一分解整环.

注意 与一个变量的多项式环相比，这里每个复多项式是线性多项式的积，而两个变量的复多项式在 $\mathbf{C}[t, x]$ 中经常是既约的，因此是素元.

第四节 整多项式的分解

现在提出一个给定的整多项式的因子分解的问题：

【12.4.1】
$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

其中 $a_n \neq 0$. 其线性因子很容易找到.

【12.4.2】引理

(a) 如果整多项式 $b_1 x + b_0$ 在 $\mathbf{Z}[x]$ 中整除 f，则 b_1 整除 a_n，且 b_0 整除 a_0.

(b) 一个本原多项式 $b_1 x + b_0$ 在 $\mathbf{Z}[x]$ 中整除 f 当且仅当有理数 $-\dfrac{b_0}{b_1}$ 是 f 的根.

(c) 首一的整多项式 f 的有理根是整数.

证明

(a) 乘积 $(b_1 x + b_0)(q_{n-1} x^{n-1} + \cdots + q_0)$ 的常数系数是 $b_0 q_0$，且若 $q_{n-1} \neq 0$，则首项系数为 $b_1 q_{n-1}$.

(b) 根据定理 12.3.10(c)，$b_1 x + b_0$ 在 $\mathbf{Z}[x]$ 中整除 f 当且仅当它在 $\mathbf{Q}[x]$ 上整除 f，并

371 且该结论成立当且仅当 $x+b_0/b_1$ 整除 f，即 $-b_0/b_1$ 是 f 的一个根.

(c) 如果 $\alpha=a/b$ 是一个根，且 $b>0$，如果 $\gcd(a,b)=1$，则 $bx-a$ 是一个整除首一多项式 f 的本原多项式，故 $b=1$ 且 α 是一个整数. ■

同态 ψ_p：$\mathbf{Z}[x]\to\mathbf{F}_p[x]$(12.3.1)对于具体的分解是有用的，原因之一就是在 $\mathbf{F}_p[x]$ 中每个次数的多项式只有有限多个.

【12.4.3】命题 令 $f(x)=a_nx^n+\cdots+a_0$ 是一个整多项式，且令 p 是一个不能整除首项系数 a_n 的素整数. 如果 f 模 p 的剩余 $\overline{f}$ 是 $\mathbf{F}_p[x]$ 中的既约元，则 f 是 $\mathbf{Q}[x]$ 上的既约元.

证明 我们证明其逆否命题，即如果 f 可约的，则 $\overline{f}$ 是可约的. 假设 $f=gh$ 是 f 在 $\mathbf{Q}[x]$ 上的真分解. 我们可假设 $g,h\in\mathbf{Z}[x]$(12.3.6). 由于在 $\mathbf{Q}[x]$ 中有真分解，故 g 和 h 的次数都是正的，且如果 f 的次数记作 $\deg f$，则 $\deg f=\deg g+\deg h$.

由于 ψ_p 是同态，$\overline{f}=\overline{g}\,\overline{h}$，故 $\deg\overline{f}=\deg\overline{g}+\deg\overline{h}$. 对于任何一个整多项式 p，$\deg\overline{p}\leqslant\deg p$. 关于 f 的首项系数的假设告诉我们 $\deg\overline{f}=\deg f$. 情形如此，必有 $\deg\overline{g}=\deg g$ 和 $\deg\overline{h}=\deg h$. 因此分解 $\overline{f}=\overline{g}\,\overline{h}$ 是真分解. ■

如果 p 整除 f 的首项系数，则 $\overline{f}$ 有较低的次数，用模 p 约化就更困难.

如果怀疑一个整多项式是既约的，则可试着对一些小素数模 p 进行约化，例如 $p=2$ 或 3，这时希望 $\overline{f}$ 是既约的且与 f 有相同的次数. 如果是这样，就证明了 f 也是既约的. 遗憾的是，存在这样的既约整多项式，对所有素数 p 它们是模 p 可分解的，多项式 x^4-10x^2+1 就是这样的一个例子. 因而模 p 约化的方法不总是可行的，但它常常是有效的.

$\mathbf{F}_p[x]$ 中的既约多项式可用“筛法”找到. 埃拉托色尼筛法是确定小于给定的数 n 的素数的方法. 列出从 2 到 n 的整数. 第一个整数 2 是素数，因为 2 的真因数必小于 2，而所列的数中没有比 2 小的数. 我们标注 2 是素数，然后在所列的数中划去 2 的倍数. 除去 2 本身，它们都不是素数. 剩下的第一个整数 3 是素数，因为它不能被比它小的任何素数整除. 我们认定 3 是素数，然后从所列的数中划去 3 的倍数. 剩下的下一个最小整数 5 也是个素数，等等.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ...

这一方法亦可确定 $\mathbf{F}_p[x]$ 中的既约多项式. 我们按次数依次列出首一多项式，然后划
372 去乘积. 例如，$\mathbf{F}_2[x]$ 中的线性多项式为 x 与 $x+1$. 它们是既约的. 二次多项式为 x^2，x^2+x，x^2+1 和 x^2+x+1，前面三个被 x 或 $x+1$ 整除，因而最后一个 x^2+x+1 是 $\mathbf{F}_2[x]$ 上仅有的二次既约多项式.

【12.4.4】 $\mathbf{F}_2[x]$ 中次数小于等于 4 的既约多项式如下：

$$x,x+1;\quad x^2+x+1;\quad x^3+x^2+1,\quad x^3+x+1;$$
$$x^4+x^3+1,\quad x^4+x+1,\quad x^4+x^3+x^2+x+1$$

列出的多项式来试除，我们可以在 $\mathbf{F}_2[x]$ 上分解所有 9 次以下的多项式. 例如，在 $\mathbf{F}_2[x]$ 上分解 $f(x)=x^5+x^3+1$. 如果能分解，则必有一个次数最多为 2 的既约因子. 0 和

1 都不是根，因此 f 没有线性因子. 只有一个既约二次多项式，即 $p=x^2+x+1$. 做带余除法：$f(x)=p(x)(x^3+x^2+x)+(x+1)$. 故 p 不能整除 f，因此 f 是既约的.

所以，整多项式 $f=x^5-64x^4+127x^3-200x+99$ 在 $\mathbf{Q}[x]$ 上是既约的，因为它在 $\mathbf{F}_2[x]$ 上的剩余是既约多项式 x^5+x^3+1.

【12.4.5】 $\mathbf{F}_3[x]$ 上二次的首一既约多项式有：

$$x^2+1,\quad x^2+x-1,\quad x^2-x-1$$

即使当模 p 的剩余可约时，它对刻画多项式的因式分解也是有帮助的. 作为例子，考虑多项式 $f(x)=x^3+3x^2+9x+6$. 模 3 约化，我们得到 x^3. 这看起来起不了什么作用. 然而，假设 $f(x)$ 在 $\mathbf{Z}[x]$ 上是可约的，比如设 $f(x)=(x+a)(x^2+bx+c)$. 则 $x+a$ 的剩余在 $\mathbf{F}_3[x]$ 中整除 x^3. 这表明 $a\equiv 0(\mathrm{mod}3)$. 类似地，我们得到 $c\equiv 0(\mathrm{mod}3)$. 因为常数项的乘积 $ac=6$，故这两个条件不可能同时得到满足. 因而没有这样的因式分解存在，从而 $f(x)$ 是既约的.

这个例子中起作用的原理称为艾森斯坦准则.

【12.4.6】**命题**(艾森斯坦准则) 设 $f(x)=a_nx^n+\cdots+a_0$ 是一个整多项式，并设 p 是一个素整数. 假设 f 的系数满足下列条件：

- p 不能整除 a_n；
- p 整除所有其余系数 $a_{n-1},\cdots a_0$；
- p^2 不能整除 a_0.

则 f 在 $\mathbf{Q}[x]$ 中是既约的.

例如，多项式 $x^4+25x^2+30x+20$ 在 $\mathbf{Q}[x]$ 中是既约的.

艾森斯坦准则的证明 假设 f 满足条件，并设 $\overline{f}$ 表示 f 模 p 的剩余. 假设蕴含了 $\overline{f}=\overline{a}_nx^n$ 和 $\overline{a}_n\neq 0$. 如果 f 在 $\mathbf{Q}[x]$ 上可约，则它将在 $\mathbf{Z}[x]$ 中分解成正次数因子的积，比如 $f=gh$，其中 $g(x)=b_rx^r+\cdots+b_0$ 和 $h(x)=c_sx^s+\cdots+c_0$. 则 $\overline{g}$ 整除 $\overline{a}_nx^n$，故 $\overline{g}$ 有如下形式：$\overline{b}_rx^r$. g 和 h 的所有系数(除去首项系数)都被 p 整除. f 的常系数 $a_0=b_0c_0$. 由于 p 整除 b_0 和 c_0，由此得到 p^2 必整除 a_0，这与假设的第三个条件矛盾. 因此，f 在 $\mathbf{Q}[x]$ 中是既约的. ■ 373

艾森斯坦准则的应用之一是证明分圆多项式 $\Phi(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ 的不可约性，其中 p 是素数. 其根为异于 1 的 p 次单位根，即 $\zeta=\mathrm{e}^{2\pi i/p}$ 的幂：

【12.4.7】
$$(x-1)\Phi(x)=x^p-1$$

【12.4.8】**引理** 令 p 为素整数. 对于任意整数 r，$1<r<p$，二项式系数 $\binom{p}{r}$ 是一个只有一个因子 p 的整数.

证明 二项式系数 $\binom{p}{r}$ 是

$$\binom{p}{r}=\frac{p(p-1)\cdots(p-r+1)}{r(r-1)\cdots 1}$$

当 $r<p$ 时，分母中的项均小于 p，因此不能和分子中的 p 约分. 因此 $\binom{p}{r}$ 只有一个因子 p. ■

【12.4.9】定理 令 p 为素数. 分圆多项式 $\Phi(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ 在 $\mathbf{Q}$ 中是既约的.

证明 用 $x=y+1$ 代入(12.4.7)中，并展开得到

$$y\Phi(y+1)=(y+1)^p-1=y^p+\binom{p}{1}y^{p-1}+\cdots+\binom{p}{p-1}y+1-1$$

消去 y. 这个引理表明艾森斯坦准则适用，且 $\Phi(y+1)$ 是既约的. 故 $\Phi(x)$ 也既约. ■

系数的估计

计算机通过编程借助分解模素数的幂来分解整多项式，通常素数取 $p=2$. 有一个快速算法为 Berlekamp 算法，它可以实现整多项式的分解. 最简单的情形是当 f 是首一的整多项式，其模 p 的剩余是互素的首一多项式之积，比如在 $\mathbf{F}_p[x]$ 中，$\overline{f}=\overline{g}\,\overline{h}$. 这样，有唯一一种方式分解 f 为模 p 的幂.（在此我们不花时间证明了）. 假设这个结论为真，且假设我们(或计算机)已经模方幂 p，p^2，p^3，…进行了分解. 如果 f 在 $\mathbf{Z}[x]$ 上分解，则因子模 p^k 的系数用介于 $-p^k/2$ 和 $p^k/2$ 间的整数表示时将是稳定的，且将产生整数分解. 如果 f 在 $\mathbf{Z}[x]$ 上既约，则因子的系数是不稳定的. 当这些系数太大时，可以得出多项式是既约的结论.

下面的柯西定理可以用来估计整因子的系数有多大.

【12.4.10】定理 令 $f(x)=x^n+\cdots+a_1+a_0$ 是首一的复数系数的多项式，且令 r 是所有系
374 数绝对值 $|a_i|$ 的最大值. f 的根的绝对值小于 $r+1$.

定理 12.4.10 的证明 技巧是改写 f 成下面的形式：

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

应用三角不等式：

【12.4.11】
$$\begin{aligned}|x|^n&\leqslant|f(x)|+|a_{n-1}||x|^{n-1}+\cdots+|a_1||x|+|a_0|\\&\leqslant|f(x)|+r(|x|^{n-1}+\cdots+|x|+1)=|f(x)|+r\frac{|x|^n-1}{|x|-1}\end{aligned}$$

令 α 是满足 $|\alpha|\geqslant r+1$ 的复数，则 $\frac{r}{|\alpha|-1}\leqslant 1$. 将 $x=\alpha$ 代入(12.4.11)：

$$|\alpha|^n\leqslant|f(\alpha)|+r\frac{|\alpha|^n-1}{|\alpha|-1}\leqslant|f(\alpha)|+|\alpha|^n-1$$

因此 $|f(\alpha)|\geqslant 1$，且 α 不是 f 的根. ■

我们给出两个 $r=1$ 时的例子.

【12.4.12】例

(a) 令 $f(x)=x^6+x^4+x^3+x^2+1$. 模 2 的既约分解是

$$x^5+x^4+x^3+x^2+1=(x^2+x+1)(x^4+x^3+x^2+x+1)$$

由于因子互不相同，故只存在一种模 2^2 的 f 的分解，即

$$x^6+x^4+x^3+x^2+1=(x^2-x+1)(x^4+x^3+x^2+x+1),\ \mod 4$$

模 2^3 和模 2^4 的分解是一样的. 如果已经做了这些计算，我们会猜测这是一个整数分解，事实上的确如此.

(b) 令 $f(x)=x^6-x^4+x^3+x^2+1$. 这个多项式做与模 2 同样的分解. 如果 f 在 $\mathbf{Z}[x]$ 上是可约的，则将有一个二次因子 x^2+ax+b，且 b 将是 f 的两个根的积. 柯西定理告诉我们根的绝对值小于 2，故 $|b|<4$. 计算模 2^4，

$$x^6-x^4+x^3+x^2+1=(x^2+x-5)(x^4-x^3+5x^2+7x+3),\ \mod 16$$

二次因子的常数项为 -5. 这太大了，故 f 是既约的. ■

注意 这里不必用柯西定理. 既然 f 的常数系数是 1，则 $-5\not\equiv\pm1\pmod{16}$ 的事实也证明了 f 是既约的.

用计算机实现分解很有趣，但若手工分解就难了. 用手工确定如上的模 16 的分解很不爽，虽然利用线性代数可以做. 对计算机分解方法我们不做进一步讨论. 如果你想探究这个话题，参看[LL&L]. 375

第五节 高斯素数

我们已知道高斯整数环 $\mathbf{Z}[i]$ 是欧几里得整环，并且每一个非零非单位的元素是素元的乘积，本节将研究这些称为高斯素数的素元以及它们与素整数的关系.

在 $\mathbf{Z}[i]$ 中，$5=(2+i)(2-i)$，且因子 $2+i$ 和 $2-i$ 是高斯素数. 而 3 在 $\mathbf{Z}[i]$ 中没有真因子. 它本身就是高斯素数. 这些例子展示了在高斯整数环中素整数可以通过两种方式进行因子分解.

下面的引理由高斯整数的定义直接可得：

【12.5.1】引理

- 作为实数的高斯整数是一个整数.
- 一个整数 d 在环 $\mathbf{Z}[i]$ 中整除高斯整数 $a+bi$ 当且仅当 d 在 $\mathbf{Z}$ 中整除 a 和 b.

【12.5.2】定理

(a) 设 π 是一个高斯素数，且令 $\overline{\pi}$ 是其共轭复数. 则 $\pi\overline{\pi}$ 或者是一个整素数或者是一个整素数的平方.

(b) 令 p 是一个整素数，则 p 或者是高斯素数或是一个高斯素数与其复共轭的积 $\pi\overline{\pi}$.

(c) 作为高斯素数的整素数 p 是模 4 与模 3 同余的那些整素数，即 $p=3, 7, 11, 19, \cdots$.

(d) 设 p 是整素数，下列结论等价：

(i) p 是两个复共轭高斯素数的乘积.

(ii) $p\equiv1\pmod 4$ 或 $p=2$，即 $p=2, 5, 13, 17, \cdots$.

(iii) p 是两个整数的平方和：$p=a^2+b^2$.

(iv) -1 的剩余是一个模 p 的平方.

定理 12.5.2 的证明

(a) 令 π 是一个高斯素数，比如 $\pi=a+bi$. 我们在整数环上分解正整数 $\bar{\pi}\pi=a^2+b^2$：$\bar{\pi}\pi=p_1\cdots p_k$. 这个分解在高斯整数上也是成立的，尽管该环上的分解可能不是素分解. 可能的话我们继续分解每一个 p_i，直到成为 $\mathbf{Z}[\mathrm{i}]$ 上的素分解. 因为高斯整数有唯一分解，所得到的 π 和 $\bar{\pi}$ 的素因子一定是两两相伴的. 因此 k 至多为 2. 或者 $\bar{\pi}\pi$ 是整素数，或者是两个整素数的积. 假设 $\bar{\pi}\pi=p_1p_2$，且比如说 π 是与整素数 p_1 相伴的，即 $\pi=\pm p_1$ 或者 $\pi=\pm \mathrm{i}p_1$. 则 $\bar{\pi}$ 也和 p_1 相伴，故 $p_1=p_2$，且 $\bar{\pi}\pi=p_1^2$.

(b) 设 p 是一个整素数，但不是环 $\mathbf{Z}[\mathrm{i}]$ 中的单位(单位为 ±1，$\pm\mathrm{i}$)，因此 p 被高斯素数 π 整除. 则 $\bar{\pi}$ 整除 $\bar{p}$，且 $\bar{p}=p$. 于是整数 $\bar{\pi}\pi$ 在 $\mathbf{Z}[\mathrm{i}]$ 中整除 p^2，且在 $\mathbf{Z}$ 中整除 p^2. 因此 $\bar{\pi}\pi$ 等于 p 或 p^2. 若 $\bar{\pi}\pi=p^2$，则 π 和 p 相伴. 故 p 是高斯素数.

定理的(c)部分由(b)和(d)可得，不必做进一步考虑，我们转而证明(d). 容易看出
376 (d)(i)与(d)(iii)是等价的：如果 $p=\bar{\pi}\pi$ 对某个高斯素数成立，比如 $\pi=a+bi$，则 $p=a^2+b^2$ 是两个整数的平方和. 反之，如果 $p=a^2+b^2$，则 p 分解为高斯整数：$p=(a-bi)(a+bi)$，(a)证明了两个因子是高斯素数.

下面的引理 12.5.3 表明(d)(i)和(d)(iv)是等价的，因为(12.5.3)(a)是(d)(i)的否定，(12.5.3)(c)是(d)(iv)的否定.

【12.5.3】引理 令 p 是一个整素数. 下列论断等价：

(a) p 是高斯素数；

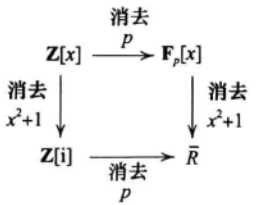
(b) 商环 $\bar{R}=\mathbf{Z}[\mathrm{i}]/(p)$ 是一个域；

(c) x^2+1 是 $\mathbf{F}_p[x]$ 的既约元(12.2.8)(c).

证明 前两个断言的等价性由事实 $\mathbf{Z}[\mathrm{i}]/(p)$ 是一个域当且仅当 $\mathbf{Z}[\mathrm{i}]$ 中的主理想 (p) 是一个极大理想，而这为真当且仅当 p 是高斯素数(参见(12.2.9)).

我们真正要证的是(a)与(c)等价，第一眼看上去两个断言似乎是根本没有联系的，就是为了得到这个等价关系我们才引入辅助的环 $\bar{R}=\mathbf{Z}[\mathrm{i}]/(p)$. 这个环可以由多项式环 $\mathbf{Z}[x]$ 经过两步得到：第一步消去 x^2+1，得到一个与 $\mathbf{Z}[\mathrm{i}]$ 同构的环；第二步，再消去 p 便得到 $\bar{R}=\mathbf{Z}[\mathrm{i}]/(p)$. 我们也可以以相反的顺序引进这个关系：消去 p 得到多项式环 $\mathbf{F}_p[x]$，再消去 x^2+1 得到 $\bar{R}=\mathbf{Z}[\mathrm{i}]/(p)$，如下图所总结的：

【12.5.4】图



我们现在有两种方法确定 $\bar{R}$ 是否是一个域. 首先，$\bar{R}$ 是域当且仅当 $\mathbf{Z}[\mathrm{i}]$ 中的主理想 (p)

是一个极大理想，这为真当且仅当 p 是高斯素数. 其次，$\overline{R}$是域当且仅当理想(x^2+1)在环 $\mathbf{F}_p[x]$中是极大理想，这为真当且仅当 x^2+1 是环(12.2.9)的既约元. 这证明了定理 12.5.2 的(a)和(c)是等价的. ■

为了证明定理 12.5.2(d)的(i)～(iv)等价只需证明(ii)与(iv)等价. -1 是模 2 的平方，考虑异于 2 的素数. 下面的引理完成这个工作.

【12.5.5】引理 *设 p 是奇素数.*

(a) *乘法群 $\mathbf{F}_p^\times$ 含有一个 4 阶元素当且仅当 $p\equiv 1(\mathrm{mod}\ 4)$.*

(b) *整数 a 是 $x^2\equiv -1(\mathrm{mod}\ p)$的解当且仅当其剩余$\overline{a}$是乘法群 $\mathbf{F}_p^\times$ 的一个 4 阶元素.* 377

证明

(a) 从以前提到的一个事实可得：乘法群 $\mathbf{F}_p^\times$ 是循环群(参见(15.7.3)). 在此给出一个特设的证明. 元素的阶整除群的阶. 故如果 $\mathbf{F}_p^\times$ 中$\overline{a}$的阶是 4，则群 $\mathbf{F}_p^\times$ 的阶(即 $p-1$)被 4 整除. 反之，假设 $p-1$ 被 4 整除. 考虑同态 φ: $\mathbf{F}_p^\times\to\mathbf{F}_p^\times$ 映 $x\rightsquigarrow x^2$. $\mathbf{F}_p^\times$ 中平方为 1 的元素只有± 1(参见(12.2.20)). 所以 φ 的核是$\{\pm 1\}$. 因此它的像(记为 H)有偶数阶$(p-1)/2$. 第一西罗定理表明 H 包含阶为 2 的元素. 那个元素就是阶为 4 的某个元素 x 的平方.

(b) 剩余$\overline{a}$阶为 4 当且仅当$\overline{a}^2$ 阶为 2. 在 $\mathbf{F}_p$ 中只有一个阶为 2 的元素，即 -1. 故$\overline{a}$阶为 4 当且仅当$\overline{a}^2=-\overline{1}$.

这完成了定理 12.5.2 的证明. ■

练　习

第一节　整数的因子分解

1.1　证明一个不是整数的平方的正整数 n 不是一个有理数的平方.

1.2　(部分分式)

(a) 将分式 7/24 写成 $a/8+b/3$ 的形式.

(b) 证明：如果 $n=uv$，其中 u 和 v 互素，则任意分式 $q=m/n$ 均可以写成 $q=a/u+b/v$ 的形式.

1.3　(中国剩余定理)

(a) 设 n，m 为互素的整数，并设 a，b 是任意整数. 证明存在整数 x 同时是同余式 $x\equiv a(\mathrm{mod}\ m)$及 $x\equiv b(\mathrm{mod}\ n)$的解.

(b) 求这两个同余式所有的解.

1.4　求下列同余式的公共解.

(a) $x\equiv 3(\mathrm{mod}8)$，$x\equiv 2(\mathrm{mod}5)$

(b) $x\equiv 3(\mathrm{mod}15)$，$x\equiv 5(\mathrm{mod}8)$，$x\equiv 2(\mathrm{mod}7)$

(c) $x\equiv 13(\mathrm{mod}43)$，$x\equiv 7(\mathrm{mod}71)$

1.5　令 a，b 是互素整数. 证明存在整数 m 和 n 使得 $a^m+b^n\equiv 1(\mathrm{mod}ab)$. 378

第二节　唯一分解整环

2.1　在 $\mathbf{F}_p[x]$上分解下列多项式为既约因子之积.

(a) x^3+x^2+x+1，$p=2$　(b)x^2-3x-3，$p=5$　(c)x^2+1，$p=7$

2.2 求多项式 $x^6+x^4+x^3+x^2+x+1$ 和 $x^5+2x^3+x^2+x+1$ 在 $\mathbf{Q}[x]$上的最大公因子.

2.3 多项式 x^2-2 模 8 有多少个根?

2.4 欧几里得用下面的方法证明了有无限多个素整数：如果 p_1，…，p_k 是素数，则$(p_1\cdots p_k)+1$ 的素因子一定不同于任何 p_i. 改写这个断言为证明对任何域 F，多项式环 $F[x]$中存在无限多个首一的既约多项式.

2.5 (多项式的部分分式)

(a) 证明 $\mathbf{C}(x)$中每个元素均可以写成多项式与形如 $1/(x-a)^i$ 的函数的线性组合的和；

(b) 列出有理函数域 $\mathbf{C}(x)$作为 $\mathbf{C}$ 上向量空间的一组基.

2.6 证明下面的环是欧几里得整环.

(a) $\mathbf{Z}[\omega]$，$\omega=e^{2\pi i/3}$　(b)$\mathbf{Z}[\sqrt{-2}]$.

2.7 令 a，b 是整数. 证明它们在整数环上的最大公因子就是在高斯整数环上的最大公因子.

2.8 描述在 $\mathbf{Z}[i]$中做带余除法的一种系统的方法. 用这种方法做除法 $4+36i$ 被 $5+i$ 除.

2.9 令 F 是域. 证明劳伦多项式环 $F[x, x^{-1}]$(第十一章练习 5.7)是一个主理想整环.

2.10 证明形式幂级数环 $\mathbf{R}[[t]]$(第十一章练习 2.2)是唯一分解整环.

第三节 高斯引理

3.1 令 φ 表示同态 $\mathbf{Z}[x]\to\mathbf{R}$，定义如下：

(a) $\varphi(x)=1+\sqrt{2}$　(b) $\varphi(x)=\frac{1}{2}+\sqrt{2}$

φ 的核是主理想吗? 如果是，找出生成元.

3.2 证明两个整多项式在 $\mathbf{Q}[x]$中互素当且仅当它们在 $\mathbf{Z}[x]$中生成的理想包含一个整数.

3.3 叙述并证明欧几里得整环的高斯引理.

3.4 令 x，y，z，w 是变量. 证明一个 2×2 矩阵 $\begin{bmatrix} x & z \\ w & y \end{bmatrix}$ 的行列式 $xy-zw$ 是多项式环 $\mathbf{C}[x, y, z, w]$上的一个既约元.

3.5 (a) 考虑映射 ψ：$\mathbf{C}[x, y]\to\mathbf{C}[t]$定义为 $f(x, y)\rightsquigarrow f(t^2, t^3)$. 证明它的像是满足 $\frac{dp}{dt}(0)=0$ 的多项式 $p(t)$的集合.

(b) 考虑由 $f(x, y)\rightsquigarrow f(t^2-t, t^3-t^2)$定义的映射 φ：$\mathbf{C}[x, y]\to\mathbf{C}[t]$. 证明它的核 $\ker\varphi$ 是一个主理想，并求这个主理想的生成元 $g(x, y)$. 证明 φ 的像是满足 $p(0)=p(1)$的多项式 $p(t)$的集合. 给出在 $\mathbf{C}^2$ 中簇$\{g=0\}$的直观几何解释.

379

3.6 令 a 是一个复数. 证明代入映射 $\mathbf{Z}[x]\to\mathbf{C}$ 映 $x\rightsquigarrow a$ 的核是一个主理想，并求此主理想的生成元.

第四节 整多项式的分解

4.1 (a)在 $\mathbf{F}_3[x]$中分解 x^9-x 和 x^9-1.　(b)在 $\mathbf{F}_2[x]$中分解 $x^{16}-x$.

4.2 证明下列多项式是既约的：

(a) 在 $\mathbf{F}_7[x]$中，x^2+1　(b)在 $\mathbf{F}_{31}[x]$中，x^3-9

4.3 确定多项式 x^4+6x^3+9x+3 是否生成 $\mathbf{Q}[x]$上的一个极大理想.

4.4 在模 2、模 3 和有理数域 $\mathbf{Q}$ 上分解整多项式 $x^5+2x^4+3x^3+3x+5$.

4.5 确定下列哪个多项式在 $\mathbf{Q}[x]$上是既约的：

(a) $x^2+27x+213$ (b) $8x^3-6x+1$ (c) x^3+6x^2+1 (d) x^5-3x^4+3

4.6 在 $\mathbf{Q}[x]$和 $\mathbf{F}_2[x]$上分解 x^5+5x+5 为既约多项式之积.

4.7 在 $\mathbf{F}_2[x]$，$\mathbf{F}_3[x]$和 $\mathbf{F}_5[x]$上分解多项式 x^3+x+1.

4.8 系数在域 F 上的多项式 $f(x)=x^4+bx^2+c$ 怎样才能在 $F[x]$上可分解？借助于特定多项式 x^4+4x^2+4 和 x^4+3x^2+4 给予解释.

4.9 对于怎样的素数 p 和怎样的整数 n，多项式 x^n-p 在 $\mathbf{Q}[x]$上既约？

4.10 在 $\mathbf{Q}[x]$上分解下列多项式.

(a) $x^2+2351x+125$ (b) x^3+2x^2+3x+1

(c) $x^4+2x^3+2x^2+2x+2$ (d) $x^4+2x^3+3x^2+2x+1$

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

(g) $x^8+x^6+x^4+x^2+1$ (h) $x^6-2x^5-3x^2+9x-3$

(i) x^4+x^2+1 (j) $3x^5+6x^4+9x^3+3x^2-1$

(k) $x^5+x^4+x^2+x+2$

4.11 用筛法确定所有小于 100 的素数，并讨论筛法的效率：非素数多快能被滤出？

4.12 确定：

(a) $\mathbf{F}_3$ 上首一的 3 次既约多项式，

(b) $\mathbf{F}_5$ 上首一的 2 次既约多项式，

(c) 域 $\mathbf{F}_5$ 上首一的 3 次既约多项式的个数.

4.13 拉格朗日插值公式：

(a) 令 a_0，…，a_d 是不同的复数. 求一个 n 次多项式 $p(x)$，它具有 n 个根 a_1，…，a_n 且 $p(a_0)=1$.

(b) 令 a_0，…，a_d 和 b_0，…，b_d 是复数，假设 a_i 不同. 存在唯一一个次数$\leqslant d$ 的多项式 g 使得 $g(a_i)=b_i$对于 $i=0$，…，d 成立. 用 a_i 和 b_i 明确表示多项式 g.

4.14 通过分析轨迹 $x^2+y^2=1$，证明多项式 x^2+y^2-1 在 $\mathbf{C}[x,y]$上是既约的.

4.15 参考艾森斯坦准则，在以下两种情况有何结论？

(a) $\overline{f}$是常数 (b)$\overline{f}=x^n+\overline{b}x^{n-1}$

4.16 在 $\mathbf{Q}[x]$上分解 $x^{14}+8x^{13}+3$，用模 3 进行约化.

4.17 借助模 4 同余，在 $\mathbf{Q}[x]$上分解 $x^4+6x^3+7x^2+8x+9$. 380

4.18 令 $q=p^r$，其中 p 为素数，且令 $r=p^{r-1}$. 证明分圆多项式$(x^q-1)/(x^r-1)$是既约的.

4.19 在模 2、模 16 和 $\mathbf{Q}$ 上分解 $x^5-x^4-x^2-1$.

第五节 高斯素数

5.1 在 $\mathbf{Z}[\mathrm{i}]$上分解下列各数为素数的积：(a)$1-3\mathrm{i}$ (b)10 (c)$6+9\mathrm{i}$ (d)$7+\mathrm{i}$

5.2 在 $\mathbf{Z}[\mathrm{i}]$上求每组数的最大公约数：(a)$11+7\mathrm{i}$，$4+7\mathrm{i}$ (b)$11+7\mathrm{i}$，$8+\mathrm{i}$ (c)$3+4\mathrm{i}$，$18-\mathrm{i}$

5.3 在 $\mathbf{Z}[\mathrm{i}]$上求由 $3+4\mathrm{i}$ 和 $4+7\mathrm{i}$ 生成的理想的生成元.

5.4 绘制一个清楚的图，表示出在适当大小范围内的高斯整数环的素数.

5.5 设 π 为高斯素数. 证明 π 与$\overline{\pi}$相伴当且仅当 π 和一个整素数相伴或者 $\pi\overline{\pi}=2$.

5.6 令 R 是环 $\mathbf{Z}[\sqrt{-3}]$. 证明整素数 p 是 R 中的素元当且仅当多项式 x^2+3 在 $\mathbf{F}_p[x]$中是不可约的.

5.7 对于每个素数 p 描述剩余环 $\mathbf{Z}[\mathrm{i}]/(p)$.

5.8 令 $R=\mathbf{Z}(\omega)$，其中 $\omega=\mathrm{e}^{2\pi\mathrm{i}/3}$. 作图表出 R 中绝对值$\leqslant 10$ 的素数.

*5.9 令 $R=\mathbf{Z}(\omega)$，其中 $\omega=e^{2\pi i/3}$. 令 p 是不等于 3 的整素数，修改定理 12.5.2 的证明过程来证明下列断言：

(a) 多项式 x^2+x+1 在 $\mathbf{F}_p$ 中有一个根当且仅当 $p\equiv 1(\mathrm{mod}\ 3)$.

(b) (p)是 R 的极大理想当且仅当 $p\equiv -1(\mathrm{mod}\ 3)$.

(c) p 在 R 中可以分解当且仅当存在整数 a，b 使得 p 可写为 $p=a^2+ab+b^2$ 的形式.

⊖5.10 (a) 令 α 是高斯整数. 假设 α 没有整数因子，且$\bar{\alpha}\alpha$ 是平方整数. 证明 α 在 $\mathbf{Z}[i]$上是一个平方.

(b) 令 a，b，c 是整数，且 a 和 b 互素，满足 $a^2+b^2=c^2$. 证明存在整数 m，n 使得 $a=m^2-n^2$，$b=2mn$，且 $c=m^2+n^2$.

杂题

M.1 令 S 是交换半群——一个合成法则满足交换律和结合律的有单位元的集合(第二章练习 M.4). 假设消去律在 S 中成立：如果 $ab=ac$，则 $b=c$. 给出适当的定义并把命题 12.2.14(a)推广到此情形.

M.2 令 v_1，…，v_n 是 $\mathbf{Z}^2$ 中的元素，令 S 是所有 $a_1v_1+\cdots+a_nv_n$(其中 a_i 为非负整系数)所组成的半群，合成法则是加法(第二章练习 M.4). 确定这些半群中那个具有唯一分解(a)当向量 v_i 的坐标非负，(b)一般情况.

381 提示：从把(12.2.1)的术语翻译为加法记号开始.

M.3 令 p 是一个整素数，且令 A 是一个 $n\times n$ 整数矩阵满足 $A^p=I$ 但是 $A\neq I$. 证明 $n\geqslant p-1$. 给出 $n=p-1$时的例子.

*M.4 (a) 令 R 是由关于 $\cos t$，$\sin t$ 的实系数多项式构成的函数环. 证明 R 同构于 $\mathbf{R}[x,y]/(x^2+y^2-1)$.

(b) 证明 R 不是唯一分解整环.

(c) 证明 $S=\mathbf{C}[x,y]/(x^2+y^2-1)$是主理想整环，因此是唯一分解整环.

(d) 确定环 S 和 R 的单位.

提示：证明 S 同构于劳伦多项式环 $\mathbf{C}[u,u^{-1}]$.

M.5 对于怎样的整数 n 圆 $x^2+y^2=n$ 包含具有整数坐标的点？

M.6 令 R 是一个整环，且令 I 是一个理想，这个理想可以以两种方式表示为不同的极大理想的积，比如 $I=P_1\cdots P_r=Q_1\cdots Q_s$. 证明这两个分解除了顺序之外是相同的.

M.7 令 $R=\mathbf{Z}[x]$.

(a) 证明 R 中每个极大理想具有形式(p,f)，其中 p 是一个整素数，f 是模 p 的既约的本原整多项式.

(b) 令 I 是 R 的由两个除了± 1 之外没有其他公因子的多项式 f 和 g 生成的理想. 证明 R/I 是有限的.

M.8 令 u 和 v 是互素整数，且令 R' 是由 $\mathbf{Z}$ 添加具有关系 $v\alpha=u$ 的元素 α 得到的环. 证明 R' 同构于 $\mathbf{Z}\left[\frac{u}{v}\right]$，也同构于 $\mathbf{Z}\left[\frac{1}{v}\right]$.

M.9 令 R 是高斯整数环，且令 W 是由系数在 R 上的 2×2 矩阵的列生成的 $V=R^2$ 的 R-子模.

解释如何求指标$[V:W]$.

M.10 令 f 和 g 是 $\mathbf{C}[x,y]$上没有公因子的多项式. 证明环 $R=\mathbf{C}[x,y]/(f,g)$是 $\mathbf{C}$ 上有限维向量

⊖ 由 Nathaniel Kuhn 建议.

空间.

M. 11 (Berlekamp 方法)此处谈到的问题是在 $\mathbf{F}_2[x]$ 上有效地分解. 解线性方程和求最大公因子用比较因子法很简单. 多项式 f 的导数 f' 利用微积分法则求出，但是注意要模 2. 证明：

(a)(平方因子)导数 f' 是一个平方，且 $f'=0$ 当且仅当 f 是一个平方. 而且，$\gcd(f, f')$ 是 f 的平方因子的幂的积.

(b)(互素因子) 令 n 是 f 的次数. 如果 $f=uv$，其中 u 和 v 是互素的，则中国剩余定理表明存在一个次数至多为 n 的多项式 g，满足 $g^2-g\equiv 0(\mathrm{mod} f)$，且 g 可以由解线性方程组求得. 或者 $\gcd(f, g)$ 或者 $\gcd(f, g-1)$ 是 f 的真因子.

(c) 用这个方法分解 $x^9+x^6+x^4+1$.

382

第十三章　二次数域

唯真最美.

Hermann Minkowski

在这一章，我们将看到在一些有趣的环上如何用理想代替元素．我们将用到各种关于平面格点的事实，为了不中断讨论，我们在本章的最后(第十节)把这些事实总结在一起.

第一节　代数整数

作为某个有理系数多项式的根的一个复数 α 叫做代数数．代入同态 φ：$\mathbf{Q}[x]\to\mathbf{C}$ 把 x 映射为代数数 α，代入同态的核是一个主理想，如同 $\mathbf{Q}[x]$ 的所有理想一样．它由一个以 α 为根的 $\mathbf{Q}[x]$ 上次数最低的首一多项式生成．如果 α 是多项式的积 gh 的根，则 α 是其中一个因子的根．故以 α 为根的首一的次数最低的多项式是既约的．我们称这个多项式是 α 在 $\mathbf{Q}$ 上的既约多项式.

注　一个代数数是代数整数，如果它在 $\mathbf{Q}$ 上的(首一的)既约多项式是整系数的.

单位立方根 $\omega=e^{2\pi i/3}=\frac{1}{2}(-1+\sqrt{-3})$ 是一个代数整数，因为它在 $\mathbf{Q}$ 上的既约多项式为 x^2+x+1，而 $\alpha=\frac{1}{2}(-1+\sqrt{3})$ 是既约多项式 $x^2-x-\frac{1}{2}$ 的根，它不是代数整数.

【13.1.1】引理　一个有理数是代数整数当且仅当它是一个通常的整数.

引理成立是因为一个有理数 a 在 $\mathbf{Q}$ 上的既约多项式为 $x-a$.

二次数域是一个形如 $\mathbf{Q}[\sqrt{d}]$ 的域，其中 d 是一个固定的正整数或负整数，它不是 $\mathbf{Q}$ 中数的平方．二次数域的元素是有如下形式的复数：

【13.1.2】
$$a+b\sqrt{d},\quad \text{其中 } a,b\in\mathbf{Q}$$

记号 $\sqrt{d}$ 代表正的实平方根，如果 $d>0$；如果 $d<0$，则代表正的虚平方根．如果 $d>0$，则
383 域 $\mathbf{Q}[\sqrt{d}]$ 是一个实二次数域；如果 $d<0$，则域 $\mathbf{Q}[\sqrt{d}]$ 是一个虚二次数域.

如果 d 有一个平方整数因子，则可以将其开方而不改变这个域．故我们假设 d 是无平方的．这样，d 可以是下列整数之一：

$$d=-1,\pm2,\pm3,\pm5,\pm6,\pm7,\pm10,\cdots$$

我们现在确定二次数域 $\mathbf{Q}[\sqrt{d}]$ 中的代数整数．令 δ 表示 $\sqrt{d}$．设 $\alpha=a+b\delta$ 是属于 $\mathbf{Q}[\delta]$ 但不属于 $\mathbf{Q}$ 的元素，即 $b\neq0$，且令 $\alpha'=a-b\delta$．则 α 和 α' 是下面多项式的根：

【13.1.3】
$$(x-\alpha')(x-\alpha)=x^2-2ax+(a^2-b^2d)$$

这个多项式具有有理系数．由于 α 不是有理数，故它不是线性多项式的根．因此这个二次

多项式在 $\mathbf{Q}$ 上是既约的. 因此，它就是 α 在 $\mathbf{Q}$ 上的既约多项式.

【13.1.4】推论 复数 $\alpha=a+b\delta$(其中 a，$b\in\mathbf{Q}$)是代数整数当且仅当 $2a$ 和 a^2-b^2d 是通常整数.

这个推论对于 $b=0$ 和 $\alpha=a$ 也成立.

a 和 b 的可能性取决于模 4 同余. 由于假设 d 是无平方的，故没有 $d\equiv0(\mathrm{mod}4)$，从而 $d\equiv1(\mathrm{mod}4)$，$d\equiv2(\mathrm{mod}4)$或 $d\equiv3(\mathrm{mod}4)$.

【13.1.5】引理 令 d 是无平方因子的整数，且令 r 是有理数. 如果 r^2d 是整数，则 r 是整数.

证明 d 是无平方因子的整数，故不能消去 r^2 的分母中的平方. ■

半整数是一个具有形式 $m+\frac{1}{2}$的有理数，其中 m 为整数.

【13.1.6】命题 二次数域 $\mathbf{Q}[\delta]$中的代数整数(其中 $\delta^2=d$ 且 d 是无平方的)具有形式 $\alpha=a+b\delta$，其中：

- 如果 $d\equiv2(\mathrm{mod}4)$或者 $d\equiv3(\mathrm{mod}4)$，则 a，b 是整数.
- 如果 $d\equiv1(\mathrm{mod}4)$，则 a，b 或者都是整数，或者都是半整数.

代数整数形成一个环 R，即域 F 的整数环.

证明 假设 $2a$ 和 a^2-b^2d 是整数，我们分析 a 和 b 取值的可能性有两种情形：a 要么是整数，要么是半整数.

情形 1：a 是整数. 则 b^2d 必为整数. 引理表明 b 为整数.

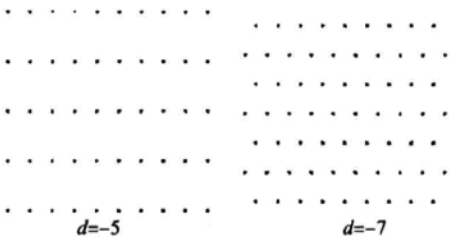
情形 2：$a=m+\frac{1}{2}$为半整数. 则 $a^2=m^2+m+\frac{1}{4}$属于集合 $\mathbf{Z}+\frac{1}{4}$. 由于 a^2-b^2d 是整数，故 b^2d 也属于 $\mathbf{Z}+\frac{1}{4}$. 则 $4b^2d$ 为整数，引理表明 $2b$ 是整数. 故 b 是半整数，于是，b^2d属于集合 $\mathbf{Z}+\frac{1}{4}$当且仅当 $d\equiv1(\mathrm{mod}4)$.

代数整数形成一个环的事实由计算可证明. ■ 384

虚二次情形 $d<0$ 比其他情形容易处理，故下一节集中阐述. 当 $d<0$ 时，代数整数形成复平面上一个格. 如果 $d\equiv2(\mathrm{mod}4)$或者 $d\equiv3(\mathrm{mod}4)$，则这个格是长方形；如果 $d\equiv1(\mathrm{mod}4)$，则这个格是“等腰三角形”.

当 $d=-1$ 时，R 是高斯整数环，且格是正方形. 当 $d=-3$ 时，格是等边三角形. 两个另外的例子如下图所示.

【13.1.7】图



在一些虚二次域中的整数

作为一个格是我们考虑环的一个非常特殊的性质，格的几何性质有助于分析这些环.

当 $d\equiv 2(\mathrm{mod}4)$ 或者 $d\equiv 3(\mathrm{mod}4)$ 时，在 $\mathbf{Q}[\delta]$ 中的整数是复数 $a+b\delta$，其中 a，b 是整数. 它们形成一个环，记作 $\mathbf{Z}[\delta]$. 当 $d\equiv 1(\mathrm{mod}4)$ 时，书写所有整数的便捷的方法是引入代数整数

【13.1.8】
$$\eta=\frac{1}{2}(1+\delta)$$

它是一个首一的整多项式

【13.1.9】
$$x^2-x+h$$

的根，其中 $h=(1-d)/4$. 在 $\mathbf{Q}[\delta]$ 中的代数整数是复数 $a+b\eta$，其中 a，b 是整数. 整数的环为 $\mathbf{Z}[\eta]$.

第二节 分解代数整数

符号 R 表示虚二次数域 $\mathbf{Q}[\delta]$ 上的整数所构成的环. 为集中精力，我们最好先考虑 $d\equiv 2(\mathrm{mod}4)$ 或者 $d\equiv 3(\mathrm{mod}4)$ 的情形，故代数整数具有形式 $a+b\delta$，其中 a，b 是整数. 385

可能的情况下，通常的整数用拉丁字母 a，b，…表示，R 的元素用希腊字母 α，β，…表示. 理想用大写字母 A，B，…表示. 我们只讨论非零理想.

如果 $\alpha=a+b\delta\in\mathbf{R}$，则其共轭复数 $\bar{\alpha}=a-b\delta$ 也属于 R. 这些是在本章第一节中引入的多项式 $x^2-2ax+(a^2-b^2d)$ 的根.

注 $\alpha=a+b\delta$ 的范数是 $N(\alpha)=\bar{\alpha}\alpha$.

范数等于 $|\alpha|^2$，也等于 a^2-b^2d. 对所有 $\alpha\neq 0$，其范数是个正整数，且有乘法性质：

【13.2.1】
$$N(\beta\gamma)=N(\beta)N(\gamma)$$

这个性质提供给我们一个元素的因子的掌控方法. 如果 $\alpha=\beta\gamma$，则(13.2.1)右边两项都是正整数. 为检验 α 的因子，只需检验元素 β 的范数是否整除 α 的范数. 当 $N(\alpha)$ 很小时，这是可以操作的. 例如，这使我们能够确定 R 的单位.

【13.2.2】命题 *令 R 为虚二次数域上的整数所构成的环.*

- *R 的元素 α 为一个单位当且仅当 $N(\alpha)=1$. 如果 α 为一个单位，则 $\alpha^{-1}=\bar{\alpha}$.*
- *R 的单位是 $\{\pm 1\}$，除非 $d=-1$ 或 -3.*
- *当 $d=-1$ 时，R 是高斯整数环，单位是 i 的四个方幂.*
- *当 $d=-3$ 时，单位是 $e^{2\pi i/6}=\frac{1}{2}(1+\sqrt{-3})$ 的六个方幂.*

证明 如果 α 是一个单位，则 $N(\alpha)N(\alpha^{-1})=N(1)=1$. 由于 $N(\alpha)$ 和 $N(\alpha^{-1})$ 是正整数，故它们都等于 1. 反之，如果 $N(\alpha)=\bar{\alpha}\alpha=1$，则 $\bar{\alpha}$ 是 α 的逆，故 α 是一个单位. 其余的断言通过研究格 R 得到. ■

【13.2.3】推论 *虚二次数域上的整数所构成的环上的分解终止.*

这由整数的分解可以终止的事实得到. 如果 $\alpha=\beta\gamma$ 是 R 上的真分解，则

$N(\alpha)=N(\beta)N(\gamma)$是 $\mathbf{Z}$ 上的真分解.

【13.2.4】命题 令 R 为虚二次数域上的整数所构成的环. 假设 $d\equiv 3(\mathrm{mod}4)$，则除去 $d=-1$(此时 R 是高斯整数环)的情形之外，R 不是单一分解整环.

证明 这和证明 $d=-5$ 的情况类似. 假设 $d\equiv 3(\mathrm{mod}4)$且 $d<-1$. R 中的整数有形式 $a+b\delta$，其中 a，$b\in\mathbf{Z}$，单位为 ± 1. 令 $e=(1-d)/2$. 则

$$2e = 1-d = (1+\delta)(1-\delta)$$

元素 $1-d$ 在 R 中有两种分解方式. 由于 $d<-1$，故没有元素 $a+b\delta$ 的范数等于 2. 因此，2 的范数为 4，它是 R 中的既约元. 如果 R 是单一分解整环，则 2 会被 R 中元素 $1+\delta$ 或 $1-\delta$整除，而这办不到：当 $d\equiv 3(\mathrm{mod}4)$时，$\frac{1}{2}(1\pm\delta)$不是 R 中的元素. ■ 386

当 $d\equiv 2(\mathrm{mod}4)$时有类似的论证(这是练习 2.2). 但是注意当 $d\equiv 1(\mathrm{mod}4)$时，推理就不成立了. 在这种情形，$\frac{1}{2}(1+\delta)\in\mathbf{R}$，事实上当 $d\equiv 1(\mathrm{mod}4)$时存在单一分解的多种情形. 一个著名的定理列举了这些情形：

【13.2.5】定理 虚二次数域 $\mathbf{Q}[\sqrt{d}]$上的整数所构成的环 R 是单一分解整环当且仅当 d 是下列整数之一：-1，-2，-3，-7，-11，-19，-43，-67，-163.

高斯证明了对于 d 的这些值，R 有唯一分解. 我们要学习如何分解. 他还猜想不存在别的整数. 这个定理更困难的部分在人们对此进行了 150 多年的研究之后，在 20 世纪中叶被 Baker、Heegner 和 Stark 证明了. 我们不能证明他们的定理.

第三节 $\mathbf{Z}[\sqrt{-5}]$中的理想

在讨论一般理论之前，我们用一种特设的方法把环 $R=\mathbf{Z}[\sqrt{-5}]$的理想描述为复平面上的格.

【13.3.1】命题 令 R 是虚二次数域上的整数所构成的环. R 的每个非零理想是格 R 的子格. 而且，

- 如果 $d\equiv 2(\mathrm{mod}4)$或者 $d\equiv 3(\mathrm{mod}4)$，则子格 A 是理想当且仅当 $\delta A\subset A$.
- 如果 $d\equiv 1(\mathrm{mod}4)$，则子格 A 是理想当且仅当 $\eta A\subset A$(见(13.1.8)).

证明 非零理想 A 包含非零元素 α，且$(\alpha,\ \alpha\delta)$是 $\mathbf{R}$ 上无关的集合. 而且，A 是离散的因为它是格 R 的子格. 因此 A 是一个格(定理 6.5.5).

要成为一个理想，R 的子集必须在 R 的加法和乘法下封闭. 每个子格 A 在整数的加法和乘法下是封闭的. 如果 A 被 δ 乘是封闭的，则被任何形如 $a+b\delta$(a，b 为整数)的元素乘也是封闭的. 如果 $d\equiv 2(\mathrm{mod}4)$或者 $d\equiv 3(\mathrm{mod}4)$，那么这包含了 R 的所有元素. 故 A 是一个理想. $d\equiv\tilde{1}(\mathrm{mod}4)$情形的证明类似. ■

我们刻画环 $R=\mathbf{Z}[\delta]$的理想，其中 $\delta^2=-5$.

【13.3.2】引理 令 $\mathbf{Q}=\mathbf{Z}[\delta]$，其中 $\delta^2=-5$. 则 2 和 $1+\delta$ 的整数组合的格 A 是一个理想.

证明 格 A 在被 δ 乘时是封闭的，因为 $\delta\cdot 2$ 和 $\delta\cdot(1+\delta)$ 是 2 和 $1+\delta$ 的整数组合. ■

图 13.3.4 展示了这个理想.

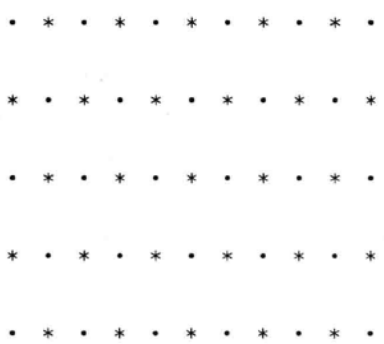
【13.3.3】定理 令 $R=\mathbf{Z}[\delta]$，其中 $\delta=\sqrt{-5}$，令 A 是 R 的一个非零理想. 令 α 是 A 中具有最小范数(或最小绝对值)的一个非零元. 则或者

- 集合$(\alpha,\ \alpha\delta)$是 A 的一组格基，且 A 是主理想(α)，或者
- 集合$\left(\alpha,\ \frac{1}{2}(\alpha+\alpha\delta)\right)$是 A 的一组格基，且 A 不是主理想.

387

这个定理有下面的几何解释：主理想(α)的格基$(\alpha,\ \alpha\delta)$由单位理想 R 的格基$(1,\ \delta)$乘 α 得到. 如果 α 用极坐标表示为 $\alpha=re^{i\theta}$，则用 α 乘就是在复平面上旋转 θ 角，并伸长 r 倍. 故所有主理想都是相似的几何图形. 而且，以$\left(\alpha,\ \frac{1}{2}(\alpha+\alpha\delta)\right)$为基的格由格$(2,\ 1+\delta)$乘 $\frac{1}{2}\alpha$得到. 所有第二种类型的理想是类似下图的几何图形(也可见图 13.7.4).

【13.3.4】图



环 $\mathbf{Z}[\sqrt{-5}]$中的理想$(2,\ 1+\delta)$

理想的相似类称为理想类，理想类的数量是 R 的类数. 此定理表明 $\mathbf{Z}[\sqrt{-5}]$的类数是 2. 其他虚二次数域的理想类将在本章第七节中讨论.

定理 13.3.3 基于下面关于格的简单引理：

【13.3.5】引理 令 A 是复平面上的一个格，设 r 是 A 中具有最小绝对值的非零元，且设 γ 是 A 的元素. 令 n 是一个正整数. 关于点 $\frac{1}{n}\gamma$ 的半径为 $\frac{1}{n}r$ 的圆盘内部不含有异于中心 $\frac{1}{n}\gamma$ 的 A 中的元素. 中心可以在 A 内，也可以在 A 外.

证明 如果 β 是 A 的元素且位于圆盘内，则 $\left|\beta-\frac{1}{n}\gamma\right|<\frac{1}{n}r$，也就是说，$|n\beta-\gamma|<r$. 而且，$n\beta-\gamma\in A$. 由于这个元素的绝对值小于最小值，故 $n\beta-\gamma=0$. 则 $\beta=\frac{1}{n}\gamma$ 是圆盘的中心. ■

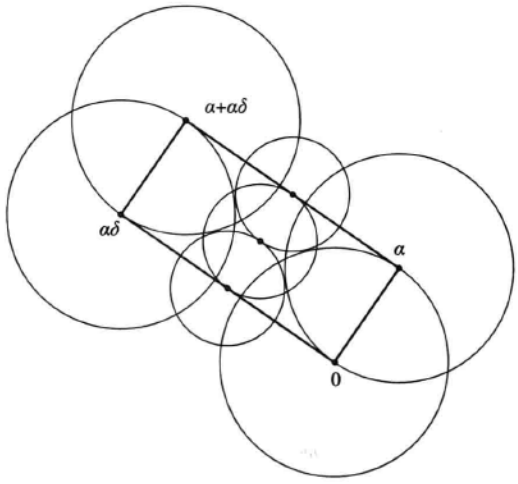
定理 13.3.3 的证明 令 α 是理想 A 中具有最小绝对值 r 的非零元. 由于 A 包含 α，故它包含主理想(α)，而 $A=(\alpha)$则是第一种情形.

假设 A 包含一个元素 $\beta\notin(\alpha)$. 理想(α)有格基 $\boldsymbol{B}=(\alpha,\ \alpha\delta)$，故我们可以选取 β 位于线性组合 $r\alpha+s\alpha\delta$(其中 $0\leqslant r,\ s\leqslant 1$)所成的平行四边形 $\Pi(\boldsymbol{B})$. (事实上，可以选取 β 使得 $0\leqslant r,\ s<1$，参见引理 13.10.2.)因为 δ 是纯虚数，故平行四边形是一个矩形. 这个矩形的大 388
小以及这个矩形在平面上的位置取决于 α，但边长的比总是 $1:\sqrt{5}$. 如果我们证明了 β 是矩形的中心 $\frac{1}{2}(\alpha+\alpha\delta)$，证明就完成了.

图 13.3.6 表明以矩形的四个顶点为圆心半径为 r 的四个圆盘和以三个半格点 $\frac{1}{2}\alpha\delta$，$\frac{1}{2}(\alpha+\alpha\delta)$和 $\alpha+\frac{1}{2}\alpha\delta$ 为圆心半径为 $\frac{1}{2}r$ 的圆盘. 注意这七个圆盘的内部覆盖了整个矩形. (要用代数的方法检验这一点是很难说清楚的，无需赘述. 几何上一眼就能看出.)

根据引理 13.3.5，圆盘内部属于 A 的元素只可能是这些圆的圆心. 由于 β 不属于主理想(α)，故它不是矩形的顶点. 因此 β 一定是三个半格点之一. 如果 $\beta=\alpha+\frac{1}{2}\alpha\delta$，则由于 $\alpha\in A$，故 $\frac{1}{2}\alpha\delta$ 也属于 A. 因此仅有两种情形要考虑：$\beta=\frac{1}{2}\alpha\delta$ 和 $\beta=\frac{1}{2}(\alpha+\alpha\delta)$.

【13.3.6】图



这就用尽了从 A 是格这个事实得到的所有信息. 现在我们要用 A 是一个理想的事实. 假设 $\frac{1}{2}\alpha\delta$ 属于 A. 用 δ 乘表明 $\frac{1}{2}\alpha\delta^2=-\frac{5}{2}\alpha$ 也属于 A. 故由于 $\alpha\in A$，故 $\frac{1}{2}\alpha\in A$. 此与 α 是 A 中绝对值最小的非零元相矛盾. 故 $\beta\neq\frac{1}{2}\alpha\delta$. 余下的可能性是 β 是矩形的中心 $\frac{1}{2}(\alpha+\alpha\delta)$. 如果这样，就是定理的第二种情形. ■

第四节　理想的乘法

令 R 为虚二次数域上的整数所构成的环. 和通常一样，记号 $A=(\alpha,\ \beta,\ \cdots,\ \gamma)$表示

A 是 R 上由 α，β，…，γ 生成的理想．它由所有系数属于环 R 的这些元素的线性组合
389 构成．

由于一个非零理想 A 是一个格，故它有包含两个元素的格基(α, β)．A 的每个元素是 α 和 β 的整数组合．我们必须仔细区分格基的概念和理想的生成元集的概念．任何格基生成一个理想，但是反过来不真．例如，主理想是由单个元素生成的理想，而格基却有两个元素．

戴德金用下面的理想乘法的定义将可除性概念推广到理想：

注 令 A 和 B 是环 R 的理想．积理想 AB 由积的所有有限和构成：

【13.4.1】 $$\sum_i \alpha_i\beta_i \quad \text{其中} \quad \alpha_i \in A, \quad \beta_i \in B.$$

这是包含所有乘积 $\alpha\beta$ 的 R 的最小理想．

理想乘法的定义可能不像人们希望的那样简单，但它很好用．注意到理想乘积满足交换律和结合律，还有单位元 R．（这是 R 被称为单位理想的原因之一．）

【13.4.2】 $$AB = BA, \quad A(BC) = (AB)C, \quad AR = RA = A.$$

我们省略下面命题的证明，这个命题对任意环成立．

【13.4.3】命题 令 A 和 B 是环 $\mathcal{R}$ 的理想．

(a) 令$\{\alpha_1, \cdots, \alpha_m\}$和$\{\beta_1, \cdots, \beta_n\}$分别是理想 A 和 B 的生成元．积理想 AB 是由 mn 个积 $\alpha_i\beta_j$ 生成的理想：AB 的每个元素是系数属于环的这些积 $\alpha_i\beta_j$ 的线性组合．

(b) 主理想的积是主理想：如果 $A=(\alpha)$，$B=(\beta)$，则 AB 是由积 $\alpha\beta$ 生成的主理想 $(\alpha\beta)$．

(c) 假设 $A=(\alpha)$是主理想，B 是任意理想．则 AB 是由积 $\alpha\beta$(其中 $\beta\in B$)所成的集合：$AB=\alpha B$.

我们回到环 $R=\mathbf{Z}[\delta]$，其中 $\delta^2=-5$，在这个环上，

【13.4.4】 $$2 \cdot 3 = 6 = (1+\delta)(1-\delta)$$

如果在 R 上的分解是唯一的，则存在 R 上的元素 γ，它整除 2 和 $1+\delta$，则 2 和 $1+\delta$ 都是主理想(γ)中的元素．不存在这样的元素．然而，存在包含 2 和 $1+\delta$ 的理想，即由这两个元素生成的理想$(2, 1+\delta)$，这个理想在图 13.3.4 中描述．

我们可用 6 的因子构造四个理想：

【13.4.5】 $$A=(2,1+\delta), \quad \overline{A}=(2,1-\delta), \quad B=(3,1+\delta), \quad \overline{B}=(3,1-\delta)$$

在每一个理想中，生成元恰好构成格基．我们记最后一个理想为$\overline{B}$，因为它是 B 的复共轭：

390 【13.4.6】 $$\overline{B} = \{\overline{\beta} | \beta \in B\}$$

它由 B 沿着实数轴做反射得到．$\overline{R}=R$ 意味着理想的复共轭还是理想．理想$\overline{A}$是理想 A 的复共轭，等于 A．格 A 恰好是对称的这种情况不常见．

我们现在计算一些积理想．由命题 13.4.3(a)可知理想$\overline{A}A$ 是由$\overline{A}$和 A 的生成元$(2, 1-\delta)$和$(2, 1+\delta)$的四个乘积生成的：

$$\overline{A}A = (4, 2+2\delta, 2-2\delta, 6)$$

这四个生成元的每一个都能被 2 整除，故$\overline{A}A$ 包含在主理想(2)中.（此处记号(2)代表理想 $2R$.）另一方面，2 是$\overline{A}A$ 中的元素，因为 $2=6-4$. 因此$(2)\subset\overline{A}A$. 这表明$\overline{A}A=(2)$.

其次，积理想 AB 由四个积生成：

$$AB = (6, 2+2\delta, 3+3\delta, (1+\delta)^2)$$

这四个生成元中每一个都被 $1+\delta$ 整除，且 $1+\delta$ 是其中两个生成元之差，故 $1+\delta\in AB$. 因此 AB 等于主理想$(1+\delta)$. 同样可以看到$\overline{A}\,\overline{B}=(1-\delta)$和$\overline{B}B=(3)$.

主理想(6)是四个理想的积：

【13.4.7】 $$(6) = (2)(3) = (\overline{A}A)(\overline{B}B) = (\overline{A}\,\overline{B})(AB) = (1-\delta)(1+\delta)$$

这不是很漂亮吗？理想的分解提供了两个分解的公共加细(13.4.4).

在下一节我们将证明任何虚二次数域上的整数环上的理想的分解的唯一性. 下面的引理是要用到的一个工具.

【13.4.8】引理（主引理） *令 R 为虚二次数域上的整数所构成的环. R 的非零理想 A 与其共轭$\overline{A}$的积是一个由普通正整数 n 生成的主理想：$\overline{A}A=(n)=nR$.*

这个引理在任何比 R 小的环上不成立，比如，当 $d\equiv 1 \pmod 4$时，如果这个环不含有以半整数为系数的元素.

证明 令(α, β)是理想 A 的格基. 则$(\bar{\alpha}, \bar{\beta})$是$\overline{A}$的格基. 而且，$\overline{A}$和 A 是由这些基生成的理想，故四个积$\bar{\alpha}\alpha$，$\bar{\alpha}\beta$，$\bar{\beta}\alpha$，$\bar{\beta}\beta$ 生成积理想$\overline{A}A$. 三个元素$\bar{\alpha}\alpha$，$\bar{\beta}\beta$ 和$\bar{\beta}\alpha+\bar{\alpha}\beta$ 属于$\overline{A}A$，是代数整数，等于自身的复共轭，故它们是有理数，因此是通常的整数(13.1.1). 令 n 是它们在整数环上的最大公约数. 它是那些元素的整线性组合，故也是$\overline{A}A$ 中的元素. 因此$(n)\subset\overline{A}A$. 如果我们能证明 n 整除 R 中$\overline{A}A$ 的四个生成元，则可得$(n)=\overline{A}A$，这就证明了引理.

由 n 的构造，n 整除$\bar{\alpha}\alpha$，$\bar{\beta}\beta\in\mathbf{Z}$，因此属于 R. 我们必须证明 n 整除$\bar{\alpha}\beta$ 和$\bar{\beta}\alpha$. 怎么做呢？这里需要美妙的洞察力. 我们用代数整数的定义. 如果我们证明了商 $\gamma=\bar{\alpha}\beta/n$ 和$\bar{\gamma}=\bar{\beta}\alpha/n$ 是代数整数，就知道它们是属于 R 的整数环的元素. 这就意味着在 R 中 n 整除$\bar{\alpha}\beta$ 和$\bar{\beta}\alpha$. 391

元素 γ 和$\bar{\gamma}$是多项式 $p(x)=x^2-(\gamma+\bar{\gamma})x+(\bar{\gamma}\gamma)$的根：

$$\bar{\gamma}+\gamma = \frac{\bar{\beta}\alpha+\bar{\alpha}\beta}{n}, \quad \bar{\gamma}\gamma = \frac{\bar{\beta}\alpha}{n}\frac{\bar{\alpha}\beta}{n} = \frac{\bar{\alpha}\alpha}{n}\frac{\bar{\beta}\beta}{n}$$

由其定义，n 整除三个整数$\bar{\beta}\alpha+\bar{\alpha}\beta$，$\bar{\alpha}\alpha$ 和$\bar{\beta}\beta$ 中的每一个. $p(x)$的系数是整数，故正如我们所希望的，γ 和$\bar{\gamma}$是代数整数.（对于 γ 恰好是有理数的情形参见引理 12.4.2.） ■

主引理的第一个应用是理想的可除性. 类似于环上元素的可除性，我们称一个理想 A 整除另一个理想 B，如果存在一个理想 C 使得 B 是积理想 AC.

【13.4.9】推论 *令 R 为虚二次数域上的整数所构成的环.*

(a) *消去律：令 A，B，C 是 R 的非零理想. 则 $AB=AC$ 当且仅当 $B=C$. 同理，$AB\subset AC$，当且仅当 $B\subset C$，且 $AB<AC$ 当且仅当 $B<C$.*

(b) *令 A，B 是 R 的非零理想. 则 $A\supset B$ 当且仅当 A 整除 B，即当且仅当存在一个理*

想 C 使得 $B=AC$.

证明

(a) 显然，如果 $B=C$，则 $AB=AC$. 如果 $AB=AC$，则 $\overline{A}AB=\overline{A}AC$. 由主引理，$\overline{A}A=(n)$，故 $nB=nC$. 两边除以 n，得证 $B=C$. 其他断言同理可证.

(b) 我们首先考虑由通常的整数 n 生成的主理想 (n) 包含理想 B 的情形. 则在 R 中 n 整除 B 的每一个元素. 令 $C=n^{-1}B$ 是商集，它是元素 $n^{-1}\beta$(其中 $\beta\in B$)的集合. 可以检验 C 是一个理想且 $nC=B$. 则 B 是积理想 $(n)C$，故 (n) 整除 B.

现在假设理想 $A\supset B$. 再一次应用主引理：$\overline{A}A=(n)$. 则 $(n)=\overline{A}A\supset\overline{A}B$. 由已经证明的结果，存在一个理想 C 使得 $\overline{A}B=(n)C=\overline{A}AC$. 由消去律，$B=AC$.

反之，如果 A 整除 B，比如 $B=AC$，则 $B=AC\subset AR=A$. ■

第五节 分解理想

这一节我们证明虚二次数域上的整数所构成的环上的非零理想唯一分解. 这从主引理 13.4.8 和它的推论 13.4.9 易得，但在推导这个定理以前，我们定义素理想的概念. 这样做是为了和标准术语保持一致：出现的素理想就是极大理想.

【13.5.1】命题 *令 $\mathcal{R}$ 是一个环. 下列关于 $\mathcal{R}$ 的理想 $\mathcal{P}$ 的条件是等价的. 一个满足这些条件的理想是素理想.*

(a) *商环 $\mathcal{R}/\mathcal{P}$ 是整环.*

(b) *$\mathcal{P}\neq\mathcal{R}$，如果 a，$b\in\mathcal{R}$ 满足 $ab\in\mathcal{P}$，则或者 $a\in\mathcal{P}$，或者 $b\in\mathcal{P}$.*

(c) *$\mathcal{P}\neq\mathcal{R}$，如果 A 和 B 是 $\mathcal{R}$ 的理想，满足 $AB\subset\mathcal{P}$，则 $A\subset\mathcal{P}$ 或者 $B\subset\mathcal{P}$.*

条件(b)解释了术语“素”. 它模仿了素整数的重要性质，即如果 p 整除整数的积 ab，
392 则或者 p 整除 a，或者 p 整除 b.

证明 (a)⇔(b)：条件“商环 $\mathcal{R}/\mathcal{P}$ 是整环”是 $\mathcal{R}/\mathcal{P}\neq\{0\}$，且 $\overline{ab}=0$ 蕴含 $\overline{a}=0$ 或 $\overline{b}=0$. 这些条件翻译为 $\mathcal{P}\neq\mathcal{R}$ 和 $ab\in\mathcal{P}$ 蕴含 $a\in\mathcal{P}$，或者 $b\in\mathcal{P}$.

(b)⇒(c)：假设 $ab\in\mathcal{P}$ 蕴含 $a\in\mathcal{P}$ 或者 $b\in\mathcal{P}$，且令 A 和 B 是 $\mathcal{R}$ 的理想，满足 $AB\subset\mathcal{P}$. 如果 $A\not\subset\mathcal{P}$，则存在 A 中元素 $a\notin\mathcal{P}$. 令 b 为 B 的任意元素. 则 $ab\in AB$，因此也属于 $\mathcal{P}$. 但 $a\notin\mathcal{P}$，故 $b\in\mathcal{P}$. 由 b 的任意性，故 $B\subset\mathcal{P}$.

(c)⇒(b)：假设 $\mathcal{P}$ 具有性质(c)，令 a，$b\in\mathcal{R}$ 满足 $ab\in\mathcal{P}$，主理想 (ab) 是积理想 $(a)(b)$. 如果 $ab\in\mathcal{P}$，则 $(ab)\subset\mathcal{P}$，故(a)$\subset\mathcal{P}$ 或者(b)$\subset\mathcal{P}$. 由此可得 $a\in\mathcal{P}$ 或者 $b\in\mathcal{P}$. ■

【13.5.2】推论 *令 $\mathcal{R}$ 是一个环.*

(a) *$\mathcal{R}$ 的零理想是一个素理想当且仅当 $\mathcal{R}$ 是一个整环.*

(b) *$\mathcal{R}$ 的极大理想是一个素理想.*

(c) *主理想 (a) 是 $\mathcal{R}$ 的一个素理想当且仅当 a 是 $\mathcal{R}$ 的一个素元.*

证明 (a) 由(13.5.1)(a)可直接推出，因为商环 $\mathcal{R}/(0)$ 同构于 $\mathcal{R}$.

(b) 也可以由(13.5.1)(a)推出，因此$\mathcal{M}$是极大理想，$\mathcal{R}/\mathcal{M}$是域. 域是整环，所以$\mathcal{M}$是素理想.

(c) 这是(13.5.1)(b)的主理想情形. ■

这完成了任意环上的素理想的讨论，我们回到虚二次数域上的整数所构成的环上.

【13.5.3】推论 *令R为虚二次数域上的整数所构成的环，令A，B是R的理想，令P是R的非零素理想. 如果P整除积理想AB，则P整除A或者P整除B.*

当把(13.4.9)(b)中的包含关系翻译成可除性时，从(13.5.1)(c)可得证.

【13.5.4】引理 *令R为虚二次数域上的整数所构成的环，令B是R的非零理想. 则*

(a) B在R中有有限指标，

(b) R中存在有限多个包含B的理想，

(c) B包含在一个极大理想中，

(d) B是素理想当且仅当它是极大理想.

证明

(a) 是引理 13.10.3(d)，(b)由推论 13.10.5 可得.

(c) 在包含B的有限多个理想中必有至少一个是极大理想.

(d) 令P是R的非零素理想. 则由(a)，P在R中有有限指标. 故R/P是有限整环. 有限整环是一个域(这是第十一章练习 7.1). 因此P是一个极大理想. 逆命题是(13.5.2)(b). ■ 393

【13.5.5】定理 *令R为虚二次数域F上的整数所构成的环. R的每个真理想是素理想的积. 一个理想除去因子的次序之外唯一地分解为素理想的积.*

证明 如果理想B是一个极大理想，则它本身就是素理想. 否则，存在一个理想A真包含B. 则A整除B，比如$B=AC$. 消去律表明C也真包含B. 继续分解A和C. 既然仅有有限多个理想包含B，这个分解过程便会终止. 当终止时，所以因子都是极大理想，因而是素理想.

如果$P_1\cdots P_r=Q_1\cdots Q_s$，其中$P_i$和$Q_j$是素理想，则$P_1$整除$Q_1\cdots Q_s$，因此$P_1$整除$Q_1\cdots Q_s$的因子之一，比如$Q_1$，则$P_1$包含$Q_1$，由于$Q_1$是极大理想，故$P_1=Q_1$. 当把方程两边消去$P_1$后，由归纳法可证分解的唯一性. ■

注意 *这个定理可以推广到其他数域上的代数整数环，但这是一个很特殊的性质. 多数环没有理想分解的唯一性这个性质，理由是在多数环中，$P\supset B$并不蕴含着P整除B，于是素理想和素元的相似程度就弱些.*

【13.5.6】定理 *虚二次数域的整数所构成的环R是唯一分解整环当且仅当它是主理想整环，且这个结论成立当且仅当R的类群C(见(13.7.3))是平凡群.*

证明 一个主理想整环是唯一分解整环(12.2.14). 反之，假设R是唯一分解整环. 我们必须证明每个理想都是主理想. 由于主理想的积还是主理想，且每个非零理想是素理

想的乘积，因此只要证明每个非零素理想是主理想即可.

令 P 是 R 的非零素理想，且令 α 是 P 中非零元素. 则 α 是既约元之积，且由于 R 是唯一分解的，因此这些既约元是素元(12.2.14). 由于 P 是素理想，故 P 包含 α 的一个素因子，比如 π，则 P 包含主理想(π). 但由于 π 是素元，故(π)是非零素理想，因此是一个极大理想. 由于 P 包含(π)，因此 $P=(\pi)$. 故 P 是主理想. ■

第六节 素理想与素整数

在第十二章第五节中，我们看到高斯素数与整素数有关. 对于虚二次数域的整数所构成的环 R 可以做类似的分析，但我们要谈素理想而不是素元. 这使定理 12.5.2 的一些部分的类似变得复杂了. 我们只考虑直接推广的部分.

【13.6.1】定理 令 R 为虚二次数域 F 上的整数所构成的环.

(a) 令 P 是 R 的非零素理想，比如说 $\overline{P}P=(n)$，其中 n 是正整数，则 n 或是一个整素数或是一个整素数的平方.

(b) 令 p 是一个整素数，则主理想$(p)=pR$ 或者是素理想，或者是一个素理想与这个
394 素理想的共轭的乘积 $\overline{P}P$.

(c) 假设 $d\equiv 2(\mathrm{mod}4)$或 $d\equiv 3(\mathrm{mod}4)$，则一个整素数 p 生成 R 的一个素理想(p)当且仅当 d 不是一个模 p 的平方，这个结论成立当且仅当多项式 x^2-d 在 $\mathbf{F}_p[x]$上是既约的.

(d) 假设 $d\equiv 1(\mathrm{mod}4)$，令 $h=\frac{1}{4}(1-d)$，则一个整素数 p 生成素理想(p)当且仅当多项式 x^2-x+h 在 $\mathbf{F}_p[x]$上是既约的.

【13.6.2】推论 用定理中的记号，任何严格大于(p)的真理想是素理想，因此是极大理想.

注 一个整素数 p 称为持素的，如果主理想$(p)=pR$ 是一个素理想. 否则主理想(p)是一个素理想与该素理想的共轭的积 $\overline{P}P$. 在此情形，素数 p 称为分裂的. 如果还满足条件 $\overline{P}=P$，则素数 p 称为可分叉的.

回到 $d=-5$ 的情形，素数 2 在 $\mathbf{Z}[\sqrt{-5}]$中可分叉，因为$(2)=\overline{A}A$ 且 $\overline{A}=A$. 素数 3 是分裂的. 它不是可分叉的，因为$(3)=\overline{B}B$ 但是 $\overline{B}\neq B$(参见(13.4.5)).

定理 13.6.1 的证明 证明从定理 12.5.2 的证明而来，故我们省略(a)和(b)的证明. 为了回顾推理过程，我们讨论(c). 设 $d\equiv 2(\mathrm{mod}4)$或 $d\equiv 3(\mathrm{mod}4)$. 则 $R=\mathbf{Z}[\delta]$与商环 $\mathbf{Z}[x]/(x^2-d)$同构. 一个素整数 p 在 R 上持素当且仅当 $\widetilde{R}=R/(p)$是一个域. (我们使用一个波浪号以避免与复共轭混淆.)这导出下面的图：

【13.6.3】图

$$\begin{array}{ccc} \mathbf{Z}[x] & \xrightarrow{\text{核}(p)} & \mathbf{F}_p[x] \\ \Big\downarrow{\scriptstyle \text{核}(x^2-d)} & & \Big\downarrow{\scriptstyle \text{核}(x^2-d)} \\ \mathbf{Z}[\delta] & \xrightarrow[\text{核}(p)]{} & \widetilde{R} \end{array}$$

这个图表明$\tilde{R}=R/(p)$是一个域当且仅当核x^2-d在$\mathbf{F}_p[x]$上是既约的.

(d)的证明类似. ■

【13.6.4】**命题** 令A，B，C是非零理想且$B\supset C$. C在B中的指标等于指标$[AB:AC]$.

证明 由于A是素理想的积，因此只要证明当P是非零素理想时，$[B:C]=[PB:PC]$即可. 对于任意理想A的引理只要一次乘以一个素理想即可得证.

存在一个素整数p使得或者$P=(p)$或者$\overline{P}P=(p)$(13.6.1). 如果$P=(p)$，则要证明的公式就是$[B:C]=[pB:pC]$，这是显然的(参见(13.10.3)(c)).

假设$(p)=\overline{P}P$. 我们研究理想链$B\supset PB\supset\overline{P}PB\supset pB$. 消去律表明包含关系是严格的，且$[B:pB]=p^2$. 因此$[B:PB]=p$. 同理，$[C:PC]=p$(13.10.3)(b). 下图以及指标的乘法性质表明$[B:C]=[PB:PC]$. 395

$$\begin{array}{ccc} B & \supset & C \\ \cup & & \cup \\ PB & \supset & PC \end{array}$$

■

第七节 理 想 类

和前面一样，R为虚二次数域上的整数所构成的环. 我们已经看到R是主理想整环当且仅当它是唯一分解整环(13.5.6). 我们定义一个与理想的乘法相容的非零理想间的等价关系，使得主理想形成一个等价类.

注 R的两个非零理想A和A'是相似的，如果对于某个复数λ，

【13.7.1】
$$A'=\lambda A$$

理想的相似性是一个等价关系，它的几何解释在前面已经提到过：A和A'相似当且仅当看成复平面上的格时，它们是相似的几何图形，相似是指保持同向. 要看清这一点，我们注意到一个格在各个点上看起来是相同的. 故几何相似性可以假设为把A的元素0与A'的元素0联系起来. 然后就可以描述成一个旋转之后紧跟着伸缩，即用复数λ去乘.

注 相似性理想类称为理想类. 一个理想A的类记作$\langle A\rangle$.

【13.7.2】**引理** 单位理想类$\langle R\rangle$由所有主理想构成.

证明 如果$\langle A\rangle=\langle R\rangle$，则存在某个复数$\lambda$，使得$A=\lambda R$. 由于1属于$R$，故$\lambda$属于$A$，因此它也是$R$中的元素. 则$A$是主理想$(\lambda)$. ■

我们在(13.3.3)中看到在环$R=\mathbf{Z}[\delta]$(其中$\delta^2=-5$)上有两个理想类. 理想$A=(2,\ 1+\delta)$和$B=(3,\ 1+\delta)$两个都代表非主理想类，如下图13.7.4中所示. 在图中放入一个矩形是为了从几何上直观地帮助理解两个格是相似的几何图形这个事实.

下面(定理13.7.10)我们会看到存在有限多个理想类. R中理想类的数量称为R的类数.

【13.7.3】**命题** 理想类构成阿贝尔群C，它是R的类群，由理想的乘法定义合成法则：

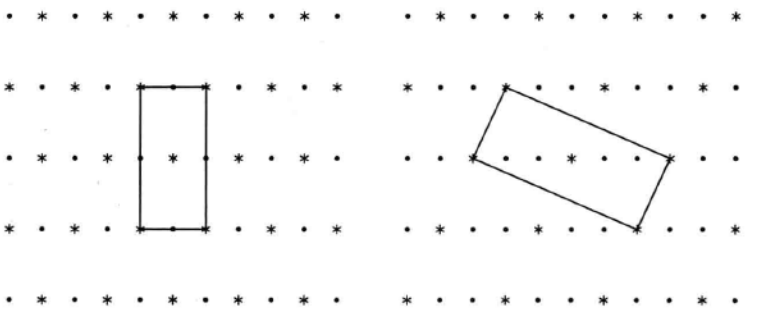
$\langle A\rangle\langle B\rangle=\langle AB\rangle$：

$$(A\text{ 的类})(B\text{ 的类})=(AB\text{ 的类})$$

证明 设$\langle A\rangle=\langle A'\rangle$，$\langle B\rangle=\langle B'\rangle$，即 $A'=\lambda A$ 和 $B'=\gamma B$ 对某些复数 λ，γ 成立. 则
396 $A'B'=\lambda\gamma AB$，因此$\langle AB\rangle=\langle A'B'\rangle$. 这表明合成法则是定义良好的. 合成法则是交换的和结合的是因为理想的乘法是交换的和结合的，单位理想类$\langle R\rangle$是单位元，和通常一样，还用 1 表示. 唯一不太明显的群的公理就是每个类$\langle A\rangle$有逆元. 但这由主引理可得，因为主引理断言 $\overline{A}A$是主理想(n). 由于主理想类是 1，因此$\langle\overline{A}\rangle\langle A\rangle=1$，且$\langle\overline{A}\rangle=\langle A\rangle^{-1}$. ■

类数被认为是量化元素不能唯一分解的恶劣程度的一个指标. 更精确的信息用类群的结构定理给出. 正如我们看到的，环 $R=\mathbf{Z}[\sqrt{-5}]$的类数为 2. R 的类群的阶为 2. 这个类群的结果之一是 R 的任意两个非主理想的积是一个主理想. 在(13.4.7)中我们看到了几个例子.

【13.7.4】图



理想 $A=(2,\ 1+\delta)$和 $B=(3,\ 1+\delta)$，$\delta^2=-5$

理想的度量

主引理告诉我们如果 A 是非零理想，则$\overline{A}A=(n)$是由一个正整数生成的主理想. 这个正整数定义为 A 的范数，记作 $N(A)$：

【13.7.5】 $N(A)=n$，如果 n 是正整数使得$\overline{A}A=(n)$

一个理想的范数类似于一个元素的范数. 对于元素的范数成立的乘法性质对于理想的范数也是成立的.

【13.7.6】**引理** *如果 A 和 B 是非零理想，则 $N(AB)=N(A)N(B)$. 而且，主理想(α)的范数等于元素 α 的范数 $N(\alpha)$.*

证明 设 $N(A)=m$，$N(B)=n$. 这意味着$\overline{A}A=(m)$，$\overline{B}B=(n)$. 则$(\overline{AB})(AB)=(\overline{A}A)(\overline{B}B)=(m)(n)=(mn)$. 因此 $N(AB)=mn$.

其次，假设 A 是主理想(α)，令 $n=N(\alpha)(=\bar{\alpha}\alpha)$. 则$\overline{A}A=(\bar{\alpha})(\alpha)=(\bar{\alpha}\alpha)=(n)$，故
397 $N(A)=n$. ■

我们现在有 4 种方式度量一个理想 A 的大小：

- 范数 $N(A)$.
- A 在 R 中的指标 $[R:A]$.
- A 的格基张成的平行四边形的面积 $\Delta(A)$.
- A 的非零元的范数 $N(\alpha)$ 的最小值.

这些度量之间的关系在下面的定理 13.7.8 中给出. 为表述这个定理，我们需要一个特殊的数：

【13.7.7】
$$\mu=\begin{cases}2\sqrt{\dfrac{|d|}{3}} & \text{如果 } d\equiv 2(\mathrm{mod}4) \text{ 或 } d\equiv 3(\mathrm{mod}4)\\ \sqrt{\dfrac{|d|}{3}} & \text{如果 } d\equiv 1(\mathrm{mod}4)\end{cases}$$

【13.7.8】定理 *令 R 为虚二次数域 F 上的整数所构成的环，且 A 是 R 的一个非零理想. 则*

(a) $N(A)=[R:A]=\dfrac{\Delta(A)}{\Delta(R)}$.

(b) *如果 α 是 A 中具有最小范数的非零元，则 $N(\alpha)\leqslant N(A)\mu$.*

关于(b)的最重要的一点是系数 μ 不依赖于理想.

证明

(a) 参考命题 13.10.6 关于 $[R:A]=\dfrac{\Delta(A)}{\Delta(R)}$ 的证明. $N(A)=[R:A]$ 的证明大致如下. 在等号上放上了参考字母. 令 $n=N(A)$. 则

$$n^2 \overset{1}{=} [R:nR] \overset{2}{=} [R:\overline{A}A] \overset{3}{=} [R:A][A:\overline{A}A] \overset{4}{=} [R:A][R:\overline{A}] \overset{5}{=} [R:A]^2.$$

等号上标注的 1 是引理 13.10.3(b)，标注的 2 是主引理，即 $nR=\overline{A}A$，标注的 3 是指标的乘法性质. 第四个等号从命题 13.6.4 得出：$[A:\overline{A}A]=[RA:\overline{A}A]=[R:\overline{A}]$. 最后，环 R 等于其复共轭 $\overline{R}$，第五个等号由 $[\overline{R}:\overline{A}]=[R:A]$ 得到.

(b) 当 $d\equiv 2(\mathrm{mod}4)$ 或 $d\equiv 3(\mathrm{mod}4)$ 时，R 有格基 $(1,\delta)$，而当 $d\equiv 1(\mathrm{mod}4)$ 时，R 有格基 $(1,\eta)$. 这个基张成的平行四边形的面积 $\Delta(R)$ 是

【13.7.9】
$$\Delta(R)=\begin{cases}\sqrt{|d|} & \text{如果 } d\equiv 2(\mathrm{mod}4) \text{ 或 } d\equiv 3(\mathrm{mod}4)\\ \dfrac{1}{2}\sqrt{|d|} & \text{如果 } d\equiv 1(\mathrm{mod}4)\end{cases}$$

故 $\mu=\dfrac{2}{\sqrt{3}}\Delta(R)$. 在引理 13.10.8 中，格中最短向量的长度估计为：$N(\alpha)\leqslant\dfrac{2}{\sqrt{3}}\Delta(A)$. 将从(a)得到的 $\Delta(A)=N(A)\Delta(R)$ 代入这个不等式，得到 $N(\alpha)\leqslant N(A)\mu$. ■ 398

【13.7.10】定理

(a) *每个理想类包含具有范数 $N(A)\leqslant\mu$ 的理想 A.*

(b) *类群 C 由素理想 P 的类生成，且素理想 P 的范数是小于 μ 的素整数 p.*

(c) *类群 C 是有限的.*

定理 13.7.10 的证明

(a) 令 A 是一个理想. 我们必须在类$\langle A\rangle$中找到一个范数至多为 μ 的理想 C. 选取 A 中非零元α，满足 $N(\alpha)\leqslant N(A)\mu$. 则 A 包含主理想(α)，故 A 整除(α)，即$(\alpha)=AC$ 对于某个理想 C 成立，且 $N(A)N(C)=N(\alpha)\leqslant N(A)\mu$. 因此 $N(C)\leqslant\mu$. 现在，既然 AC 是主理想，那么$\langle C\rangle=\langle A\rangle^{-1}=\langle\overline{A}\rangle$. 这表明类$\langle\overline{A}\rangle$包含一个理想，即 C，它的范数至多为 μ. 则类$\langle A\rangle$包含$\overline{C}$，且 $N(\overline{C})=N(C)\leqslant\mu$.

(b) 每个类包含范数小于等于 μ 的一个理想 A. 我们分解 A 为素理想：$A=P_1\cdots P_k$. 则$N(A)=N(P_1)\cdots N(P_k)$，故 $N(P_i)\leqslant\mu$ 对于每个 i 成立. 范数小于等于 μ 的素理想类生成C. 素理想 P 的范数或者是素整数 p 或者是素整数的平方 p^2. 如果 $N(P)=p^2$，则 $P=(p)$(13.6.1). 这是主理想，它的类是平凡的. 我们可以忽略那些素理想.

(c) 我们证明存在有限多个理想 A，其范数 $N(A)\leqslant\mu$. 如果把这样的理想写成素理想之积：$A=P_1\cdots P_k$ 且如果 $m_i=N(P_i)$，则 $m_1\cdots m_k\leqslant\mu$. 存在有限多个整数 m_i 的集合，每个 m_i 是素数或者是素数的平方且满足这个不等式. 存在至多两个素理想，它们的范数等于给定整数 m_i. 故存在有限多个素理想的集合使得 $N(P_1\cdots P_k)\leqslant\mu$. ■

第八节 计算类群

下表列出了几个类群. 在表中，$\lfloor\mu\rfloor$表示 μ 向下取整，它是不超过 μ 的最大整数. 如果 n 是一个整数，且 $n\leqslant\mu$，则 $n\leqslant\lfloor\mu\rfloor$.

【13.8.1】

d	$\lfloor\mu\rfloor$	类群
-2	1	C_1
-5	2	C_2
-7	1	C_1
-14	4	C_4
-21	5	$C_2\times C_2$
-23	2	C_3
-47	3	C_5
-71	4	C_7

一些类群

399 为了应用定理 13.7.10，我们检验素整数 $p\leqslant\lfloor\mu\rfloor$. 如果 p 在 R 中分裂(或分叉)，我们便将其两个素理想因子之一的类加入类群的生成元集合中. 另一个素因子的类是其逆元. 如果 p 持素，则它的类是平凡的，我们舍掉它.

【13.8.2】例 $d=-163$. 由于$-163\equiv1(\mathrm{mod}4)$，故整数环 R 是 $\mathbf{Z}[\eta]$，其中 $\eta=\frac{1}{2}(1+\delta)$，且$\lfloor\mu\rfloor=8$. 我们必须检查素数 $p=2$，3，5 和 7. 如果 p 分裂，则把它的素因子之一作为类群的一个生成元. 据定理 13.6.1，一个整素数 p 在 R 上持素当且仅当多项式 x^2-x+41 是

模 p 既约的. 这个多项式恰好是模每一个素数 $p=2$，3，5 和 7 既约的. 故类群是平凡的，R 是唯一分解整环. ■

这一节的余下的部分，我们考虑 $d\equiv 2(\mathrm{mod}4)$ 或 $d\equiv 3(\mathrm{mod}4)$ 的情形. 在这些情形，一个素数 p 分裂当且仅当 x^2-d 在 $\mathbf{F}_p$ 上有一个根. 下表告诉我们哪个素数需要检验.

【13.8.3】

	$p\leqslant\mu$
$-d\leqslant 2$	
$-d\leqslant 6$	2
$-d\leqslant 17$	2，3
$-d\leqslant 35$	2，3，5
$-d\leqslant 89$	2，3，5，7
$-d\leqslant 123$	2，3，5，7，11

当 $d\equiv 2(\mathrm{mod}4)$ 或 $d\equiv 3(\mathrm{mod}4)$ 时小于 μ 的素数

如果 $d=-1$ 或 $d=-2$，则不存在小于 μ 的素数，故类群是平凡的，R 是唯一分解整环.

我们假设已经确定了哪个素数需要检验其是分裂的，则得到类群的生成元集合. 但要确定类群的结构，我们还需要确定这些生成元之间的关系. 最好直接分析素数 2.

【13.8.4】**引理** *假设 $d\equiv 2(\mathrm{mod}4)$ 或 $d\equiv 3(\mathrm{mod}4)$. 素数 2 在 R 上分叉. 主理想(2)的素因子 P 是*

- $P=(2,\ 1+\delta)$，*如果* $d\equiv 3(\mathrm{mod}4)$，
- $P=(2,\ \delta)$，*如果* $d\equiv 2(\mathrm{mod}4)$.

类$\langle P\rangle$在类群中的阶为 2，除非 $d=-1$ 或 $d=-2$. 在 $d=-1$ 或 $d=-2$ 时，P 是主理想. 在所有情形，给定的生成元形成理想 P 的格基.

证明 令 P 如引理中所述. 我们计算积理想 $\overline{P}P$. 如果 $d\equiv 3(\mathrm{mod}4)$，则 $\overline{P}P=(2,\ 1-\delta)(2,\ 1+\delta)=(4,\ 2+2\delta,\ 2-2\delta,\ 1-d)$，而如果 $d\equiv 2(\mathrm{mod}4)$，则 $\overline{P}P=(2,\ -\delta)(2,\ \delta)=(4,\ 2\delta,\ -d)$. 在这两种情形，$\overline{P}P=(2)$. 定理 15.10.1 告诉我们理想(2)或者是素理想或者是素理想与该素理想的共轭的积，故 P 一定是素理想. 400

我们还注意到 $\overline{P}=P$，故 2 分叉，$\langle P\rangle=\langle P\rangle^{-1}$，$\langle P\rangle$在类群中的阶为 1 或 2. $\langle P\rangle$在类群中的阶为 1 当且仅当它是一个主理想. 这发生在 $d=-1$ 或 $d=-2$ 时. 如果 $d=-1$，则 $P=(1+\delta)$，而如果 $d=-2$，则 $P=(\delta)$. 当 $d<-2$ 时，整数 2 在 R 上没有真因子，则 P 不是主理想. ■

【13.8.5】**推论** *如果 $d\equiv 2(\mathrm{mod}4)$ 或 $d\equiv 3(\mathrm{mod}4)$ 且 $d<-2$，则类数是偶数.*

【13.8.6】**例** $d=-26$. 表 13.8 告诉我们检查素数 $p=2$，3，5. 多项式 x^2+26 是模 2，3，5 既约的，故所有素数 2，3，5 都分裂. 不妨设

$$(2)=\overline{P}P,\quad (3)=\overline{Q}Q,\quad (5)=\overline{S}S$$

关于类群我们有 3 个生成元：$\langle P\rangle$，$\langle Q\rangle$，$\langle S\rangle$，且$\langle P\rangle$阶为 2. 我们怎样确定这些生成元之间的关系？秘诀是计算几个元素的范数，希望从中获得一些信息. 我们并不需要看得

太远：$N(1+\delta)=27=3^3$，$N(2+\delta)=30=2\cdot 3\cdot 5$.

令 $\alpha=1+\delta$. 则$\bar{\alpha}\alpha=3^3$. 由于$(3)=\bar{Q}Q$，我们有理想间的关系

$$(\bar{\alpha})(\alpha)=(\bar{Q}Q)^3$$

因为理想因子唯一，故主理想(α)是上式右边一半项的乘积，$(\bar{\alpha})$是这些项的共轭. 我们注意到 3 在 R 上不整除α. 因此$\bar{Q}Q=(3)$不整除(α). 从而(α)或者是 Q^3 或者是$\bar{Q}^3$. $(\alpha)=Q^3$ 还是$(\alpha)=\bar{Q}^3$ 取决于我们把(3)的哪一个素因子标记为 Q.

无论在哪种情形，$\langle Q\rangle^3=1$，$\langle Q\rangle$在类群中的阶为 1 或 3. 我们验证了 3 在 R 中没有真因子. 由于 Q 整除(3)，故它不是主理想. 故$\langle Q\rangle$的阶为 3.

其次，令 $\beta=2+\delta$. 则$\bar{\beta}\beta=2\cdot 3\cdot 5$，这给出理想关系

$$(\bar{\beta})(\beta)=\bar{P}P\bar{Q}Q\bar{S}S$$

因此主理想(β)是上式右边一半理想之积，$(\bar{\beta})$是那些理想的共轭之积. 我们知道$\bar{P}=P$. 如果我们不在乎(3)和(5)的哪个素因子标注为 Q 和 S，则可以假定$(\beta)=PQS$. 这给出关系$\langle P\rangle\langle Q\rangle\langle S\rangle=1$.

我们已经发现三个关系：

$$\langle P\rangle^2=1,\quad \langle Q\rangle^3=1,\quad \langle P\rangle\langle Q\rangle\langle S\rangle=1$$

这些关系表明$\langle Q\rangle=\langle S\rangle^2$，$\langle P\rangle=\langle S\rangle^3$，$\langle S\rangle$的阶为 6. 类群是 6 阶循环群，由 5 的素理想因子生成. ■

下一个引理解释了为什么计算范数的方法有效.

401 **【13.8.7】引理** *令 P，Q，S 是虚二次整数环 R 的素理想，它们的范数分别为 p，q，s. 假设关系 $\langle P\rangle^i\langle Q\rangle^j\langle S\rangle^k=1$ 在类群 C 中成立. 则 R 中存在元素 α，它的范数为 $p^iq^js^k$.*

证明 由定义，$\langle P\rangle^i\langle Q\rangle^j\langle S\rangle^k=\langle P^iQ^jS^k\rangle$. 如果$\langle P^iQ^jS^k\rangle=1$，则理想 $P^iQ^jS^k$ 是主理想，比如，$P^iQ^jS^k=(\alpha)$. 则

$$(\bar{\alpha})(\alpha)=(\bar{P}P)^i(\bar{Q}Q)^j(\bar{S}S)^k=(p)^i(q)^j(s)^k=(p^iq^js^k)$$

因此 $N(\alpha)=\bar{\alpha}\alpha=p^iq^js^k$. ■

我们计算更多的类群.

【13.8.8】例 $d=-74$. 要检查的素数是 2，3，5 和 7. 此处，2 分叉，3 和 5 分裂，7 持素. 比如$(2)=\bar{P}P$，$(3)=\bar{Q}Q$，$(5)=\bar{S}S$. 则$\langle P\rangle$，$\langle Q\rangle$，$\langle S\rangle$生成类群，$\langle P\rangle$的阶为 2 (13.8.4). 我们注意到

$$\begin{aligned}N(1+\delta)&=75=3\cdot 5^2\\ N(4+\delta)&=90=2\cdot 3^2\cdot 5\\ N(13+\delta)&=243=3^5\\ N(14+\delta)&=270=2\cdot 3^3\cdot 5\end{aligned}$$

范数 $N(13+\delta)$表明$\langle Q\rangle^5=1$，故$\langle Q\rangle$的阶为 1 或 5. 由于 3 在 R 中没有真因子，故 Q 不是主理想. 因此$\langle Q\rangle$的阶为 5. 其次，$N(1+\delta)$表明$\langle S\rangle^2=\langle Q\rangle$或$\langle\bar{Q}\rangle$，因此$\langle S\rangle$的阶为 10. 我们从生成元集消去$\langle Q\rangle$. 最后，$N(4+\delta)$给出了关系$\langle P\rangle\langle Q\rangle^2\langle S\rangle=1$ 或$\langle P\rangle\langle Q\rangle^2\langle\bar{S}\rangle=1$. 每一个

允许我们从生成元集合中消去$\langle P\rangle$. 类群是 10 阶循环群，由(5)的素理想因子生成. ■

第九节 实二次域

我们简短地看一下实二次数域，即形如 $\mathbf{Q}[\sqrt{d}]$的域，其中 d 为非平方的正整数，我们以域 $\mathbf{Q}[\sqrt{2}]$为例. 在这个域上的整数环是唯一分解整环：

【13.9.1】 $$\boldsymbol{R}=\mathbf{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbf{Z}\}$$

可以证明对任何实二次数域上的整数环，它的理想唯一分解为素理想是成立的，且类数是有限的([Cohn]，[Hasse]). 猜测有无限多个 d 的值使得其二次数域上的整数环有唯一分解.

当 d 是正数时，$\mathbf{Q}[\sqrt{d}]$是实数域的子域. 它的整数环不能作为一个格嵌入复平面. 然而，我们可以通过把代数整数 $a+b\sqrt{d}$和平面 $\mathbf{R}^2$ 上的点(u,v)联系起来将 R 表示为在 $\mathbf{R}^2$ 上的一个格，其中

【13.9.2】 $$u=a+b\sqrt{d},\quad v=a-b\sqrt{d}$$

对于 $d=2$ 的情形所得到的格描述如下. 现在就解释双曲线被放入图中的原因. 402

回顾域 $\mathbf{Q}[\sqrt{d}]$同构于抽象地构造的域

【13.9.3】 $$F=\mathbf{Q}[x]/(x^2-d)$$

如果我们用 F 代替 $\mathbf{Q}[\sqrt{d}]$，且将 x 在 F 上的剩余记作 δ，则 δ 是 d 的一个抽象的平方根而不是正的实平方根，F 是元素 $a+b\delta$ 的集合，其中 a，$b\in\mathbf{Q}$. 坐标 u，v 提供了把抽象定义的域 F 嵌入实数平面的两种方法，即 u 映射 $\delta\rightsquigarrow\sqrt{d}$，$v$ 映射 $\delta\rightsquigarrow-\sqrt{d}$.

对于 $\alpha=a+b\delta\in\mathbf{Q}[\delta]$，我们记 α'为“共轭”元 $a-b\delta$. α 的范数是

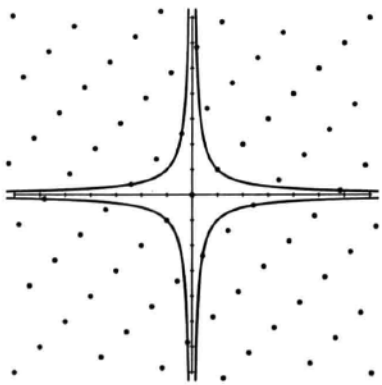
【13.9.4】 $$N(\alpha)=\alpha'\alpha=a^2-b^2d$$

如果 α 是一个代数整数，则 $N(\alpha)$是一个通常的整数. 范数是保持乘法的：

【13.9.5】 $$N(\alpha\beta)=N(\alpha)N(\beta)$$

但 $N(\alpha)$未必是正数. 它不等于$|\alpha|^2$.

【13.9.6】图



格 $\mathbf{Z}[\sqrt{2}]$

实和虚二次域的一个显著差别是实二次域的整数环总含有无限多个单位. 由于代数整数的范数是通常的整数，因此一个单位的范数一定为± 1，且如果$N(\alpha)=\pm 1$，则α的逆为$\pm\alpha'$，故α是一个单位. 例如，

【13.9.7】 $$\alpha = 1+\sqrt{2},\quad \alpha^2 = 3+2\sqrt{2},\quad \alpha^3 = 7+5\sqrt{2},\cdots$$

是在环$R=\mathbf{Z}[\sqrt{2}]$中的单位. 元素α在单位所成的群中是无限阶的.

对于单位的条件$N(\alpha)=a^2-2b^2=\pm 1$转换成(u, v)坐标的形式为

403 【13.9.8】 $$uv = \pm 1$$

故单位是位于两条双曲线$uv=1$和$uv=-1$之一上的格点，即图13.9.6中描述的点. 值得注意的是实二次域的整数环有无穷多个单位，换句话说，无穷多个格中的点位于这些双曲线上. 无论从代数的还是从几何的角度看，这一点都不是显然的，但从图上可以看到几个这样的点.

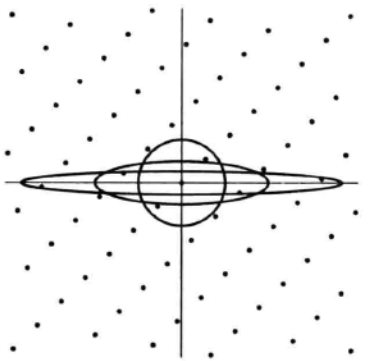
【13.9.9】定理 *令R是一个实二次数域上的整数环. R中的单位的群是一个无限群.*

我们把证明安排为一个引理序列. 第一个引理来自下一节的引理13.10.8.

【13.9.10】引理 *对于每个$\Delta_0>0$，存在具有下列性质的$r>0$：令L是(u, v)平面P上的一个格，令$\Delta(L)$表示由一个格基张成的平行四边形的面积，假设$\Delta(L)\leqslant\Delta_0$. 则$L$包含一个非零元$\gamma$使得$|\gamma|<r$.*

令Δ_0和r如上. 对于$s>0$，令D_s表示(u, v)平面P上由不等式$s^{-2}u^2+s^2v^2\leqslant r^2$定义的椭圆盘. 故$D_1$是半径为$r$的圆盘. 下图展示了三个$D_s$盘.

【13.9.11】图



包含格点的椭圆盘

【13.9.12】引理 *用上面的记号，令L是不包含除去原点外的坐标轴上的点的一个格，满足$\Delta(L)\leqslant\Delta_0$.*

(a) 对任意$s>0$，椭圆盘D_s包含L的一个非零元.

(b) 对于椭圆盘D_s的任意点$\alpha=(u, v)$，$|uv|\leqslant\frac{r^2}{2}$.

证明

(a) 映射 $\varphi:\mathbf{R}^2\to\mathbf{R}^2$ 定义为 $\varphi(x,\ y)=(sx,\ s^{-1}y)$映射 D_1 到 D_s. L 的逆像 $L'=\varphi^{-1}L$ 不含有除去原点外的轴上的点. 我们注意到 φ 是保持面积不变的一个映射，因为它把一个坐标乘 s，把另一个坐标乘 s^{-1}. 因此 $\Delta(L')\leqslant\Delta_0$. 引理 13.9.10 表明圆盘 D_1 包含 L'的一个非零元，比如 γ. 则 $\alpha=\varphi(\gamma)$是在椭圆盘 D_s 中 L 的一个元素. 404

(b) 不等式对于圆盘 D_1 成立. 令 φ 是上面定义的映射. 如果 $\alpha=(u,\ v)\in D_s$，则 $\varphi^{-1}(\alpha)=(s^{-1}u,\ sv)\in D_1$，故 $|uv|=|(s^{-1}u)(sv)|\leqslant\frac{r^2}{2}$. ■

【13.9.13】引理 用与上面引理相同的假设，则格 L 包含无限多个点$(u,\ v)$满足 $|uv|\leqslant\frac{r^2}{2}$.

证明 我们应用上一个引理. 对于充分大的 s，椭圆盘 D_s 非常狭窄，它包含 L 的一个非零元，比如 α_s. 元素 α_s 不能位于横轴 e_1 上，但是它随着 s 的无限增大越来越贴近横轴. 因此其中有无限多个点，如果 $\alpha_s=(u_s,\ v_s)$，则 $|u_sv_s|\leqslant\frac{r^2}{2}$. ■

令 R 是实二次域的整数环，令 n 是一个整数，我们称 R 的两个元素 β_i 模 n 同余如果 n 在 R 上整除 $\beta_1-\beta_2$. 当 $d\equiv2(\mathrm{mod}4)$或 $d\equiv3(\mathrm{mod}4)$时，$\beta_i=m_i+n_i\delta$，这就意味着 $m_1\equiv m_2(\mathrm{mod}n)$，$n_1\equiv n_2(\mathrm{mod}n)$. 当 $d\equiv1(\mathrm{mod}4)$时，把 β_i 记成 $\beta_i=m_i+n_i\eta$，则 β_i 模 n 同余意味着 $m_1\equiv m_2(\mathrm{mod}n)$，$n_1\equiv n_2(\mathrm{mod}n)$. 无论哪种情形，都有 n^2 个模 n 的同余类.

定理 13.9.9 由下面的引理可得.

【13.9.14】引理 令 R 是实二次数域的整数环.

(a) 存在一个正整数 n 使得 R 中范数为 n 的元素的集合 S 是无限集. 而且，S 中存在无限多个模 n 同余的元素对.

(b) 如果 R 中范数为 n 的两个元素 β_1 和 β_2 模 n 同余，则 β_2/β_1 是 R 中的单位.

证明

(a) 格 R 不包含异于原点的坐标轴上的点，因为 u 和 v 不是零除非 a 和 b 都是零. 如果 α 是 R 的元素，它在平面上的像是点$(u,\ v)$，则 $|N(\alpha)|=uv$. 引理 13.9.13 证明了 R 包含无限多个范数在一个有界区间上的点. 由于存在有限多个整数 n 在这个区间，故至少有一个整数 n 使得以此 n 为范数的 R 中元素的集合是有限的. 存在有限多个模 n 的同余类的事实证明了第二个断言.

(b) 我们证明 β_2/β_1 是 R 中的单位. 同理 β_1/β_2 也是 R 中的单位. 由于 β_1 和 β_2 是同余的，我们可以记 $\beta_2=\beta_1+n\gamma$，其中 $\gamma\in R$. 令 β_1' 为 β_1 的共轭. 故 $\beta_1\beta_1'=n$. 则 $\beta_2/\beta_1=(\beta_1+n\gamma)/\beta_1=1+\beta_1'\gamma$. 这是 R 的元素. ■

第十节 关 于 格

平面 $\mathbf{R}^2$ 的一个格 L 是由集合 S 生成的或张成的，如果 L 的每个元素可以写成 S 中元素的整数线性组合. 每个格 L 有一个由两个元素组成的格基 $\boldsymbol{B}=(v_1,\ v_2)$. L 的元素都可以

405 以唯一的方式写成格基向量的整数线性组合(参看(6.5.5)).

一些记号:

【13.10.1】

$\Pi(\boldsymbol{B})$:线性组合 $r_1v_1+r_2v_2(0\leqslant r_i\leqslant 1)$所围成的平行四边形.

它的顶点是 0, v_1, v_2, v_1+v_2.

$\Pi'(\boldsymbol{B})$:线性组合 $r_1v_1+r_2v_2(0\leqslant r_i<1)$的集合. 它由删除平行四边形 $\Pi(\boldsymbol{B})$的两条边 $[v_1, v_1+v_2]$和$[v_2, v_1+v_2]$得到.

$\Delta(L)$:$\Pi(\boldsymbol{B})$的面积.

$[M:L]$:格 M 的子格 L 的指标,即 L 在 M 中的加法陪集的个数.

我们将看到$\Delta(L)$是与格基无关的,这样所有记号没有歧义. 其他的记号以前已经介绍过。作为参考,我们回忆一下引理 6.5.8:

【13.10.2】**引理** 令 $\boldsymbol{B}=(v_1, v_1)$是 $\mathbf{R}^2$ 的一个基,令 L 是 $\boldsymbol{B}$ 的整数组合所成的格. $\mathbf{R}^2$ 中每个向量 v 可唯一写成形式 $v=w+v_0$,其中 $w\in L$, $v_0\in\Pi'(\boldsymbol{B})$.

【13.10.3】**引理** 令 $K\subset L\subset M$ 是平面上的格,令 $\boldsymbol{B}$ 是 L 的格基. 则

(a) $[M:K]=[M:L][L:K]$.

(b) 对任何正整数 n, $[L:nL]=n^2$.

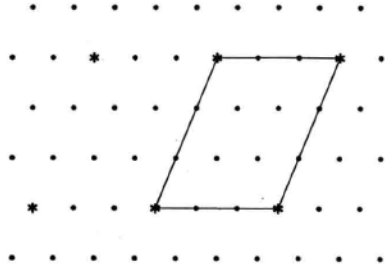
(c) 对任何正实数 r, $[M:L]=[rM:rL]$.

(d) $[M:L]$是有限的,且等于 M 在区域$\Pi'(\boldsymbol{B})$的点的数量.

(e) 格 M 是由 L 和有限集合 $M\cap\Pi'(\boldsymbol{B})$生成的.

证明 (d), (e) 我们可以把 M 中元素 x 唯一地写成形式 $v+y$,其中 $v\in L$, $y\in\Pi'(\boldsymbol{B})$. 则 $v\in M$,故 $y\in M$. 因此 x 属于陪集 $y+L$. 这表明 $M\cap\Pi'(\boldsymbol{B})$的元素是 L 在 M 中的陪集的代表元. 由于只有一种方式将 x 写成 $x=v+y$,因此这些陪集是不同的. 由于 M 是离散的,且 $\Pi'(\boldsymbol{B})$是有界集,因此 $M\cap\Pi'(\boldsymbol{B})$是有限集.

【13.10.4】图



406 $L=\{\cdot\}$ $3L=\{*\}$

公式(a)是指标的乘法性质(2.8.14). (b)由(a)得,因为格 nL 是由格 L 延伸 n 倍得到的,如上图 $n=3$ 的情形. (c)成立是因为被 r 乘把两个格伸长相同的倍数. ■

【13.10.5】**推论** 令 $L\subset M$ 是平面 $\mathbf{R}^2$ 上的格,存在有限多个格介于 L 和 M 之间.

证明 令 $\boldsymbol{B}$ 是格 L 的一个格基,且令格 N 满足 $L\subset N\subset M$. 引理 13.10.3(e)表明 N

是由 L 和集合 $N\cap\Pi'(\boldsymbol{B})$ 生成的，其中 $N\cap\Pi'(\boldsymbol{B})$ 是有限集合 $M\cap\Pi'(\boldsymbol{B})$ 的一个子集. 一个有限集合有有限多个子集. ■

【13.10.6】命题 *如果 $L\subset M$ 是平面上的格，则* $[M:L]=\dfrac{\Delta(L)}{\Delta(M)}$.

证明 令 $\boldsymbol{C}$ 是 M 的格基 (u_1, u_2). 令 n 是一个大的正整数，且令 M_n 表示以 $\boldsymbol{C}_n=\left(\dfrac{1}{n}u_1, \dfrac{1}{n}u_2\right)$ 为基的格. 令 Γ' 表示小区域 $\Pi'(\boldsymbol{C}_n)$. 它的面积为 $\dfrac{1}{n^2}\Delta(M)$. Γ' 的所有平移 $x+\Gamma'$，$x\in M_n$ 无重叠地覆盖了平面，且在每个平移 $x+\Gamma'$ 中恰好有唯一一个 M_n 中的元素，即 x. (这是引理 13.10.2.)

令 $\boldsymbol{B}$ 是 L 的格基. 我们用估计二重积分的方法估计 $\Pi(\boldsymbol{B})$ 的面积，这里用到了 Γ' 的平移. 令 $r=[M:L]$. 则 $[M_n:L]=[M_n:M][M:L]=n^2r$. 引理 13.10.3(d) 告诉我们区域 $\Pi'(\boldsymbol{B})$ 包含 n^2r 个格 M_n 中的点. 由于 Γ' 的平移覆盖了平面，因此这 n^2r 个点的平移近似覆盖 $\Pi(\boldsymbol{B})$.

$$\Delta(L)\approx n^2r\Delta(M_n)=r\Delta(M)=[M:L]\Delta(M)$$

这个近似的误差源自 $\Pi'(\boldsymbol{B})$ 的边界并没有精确覆盖. 我们可以用 $\Pi(\boldsymbol{B})$ 的边界长度以及 Γ' 的直径(最大直线距离)界定误差. 当 $n\to\infty$ 时，直径趋于零，故误差也趋于零. ■

【13.10.7】推论 *平行四边形 $\Pi(\boldsymbol{B})$ 的面积 $\Delta(L)$ 与格 L 的格基 $\boldsymbol{B}$ 无关.*

前面命题中令 $M=L$ 即可得证.

【13.10.8】引理 *令 v 是格 L 的最小长度的非零元. 则* $|v|^2\leqslant\dfrac{2}{\sqrt{3}}\Delta(L)$.

当格为一个等边三角形格时，不等号变为等号.

证明 我们选取 L 中具有最小长度的一个元素 v_1. 则 v_1 生成一个子群 $L\cap\ell$，此处 ℓ 是由 v_1 张成的直线，且存在元素 v_2 使得 (v_1, v_2) 是 L 的格基(参看定理 6.5.5 的证明). 407
刻度的变化使 $|v_1|^2$ 和 $\Delta(L)$ 改变同样的倍数，故可以假定 $|v_1|=1$. 我们定位坐标使得 $v_1=(1, 0)^t$.

比如 $v_2=(b_1, b_2)^t$. 我们可以假设 b_2 是正的. 则 $\Delta(L)=b_2$. 我们也可以通过加上 v_1 的倍数来调整 v_2，使 $-\dfrac{1}{2}\leqslant b_1\leqslant\dfrac{1}{2}$，使得 $b_1^2\leqslant\dfrac{1}{4}$. 由于 v_1 是 L 中有最小长度的非零元，因此 $|v_2|^2=b_1^2+b_2^2\geqslant|v_1|^2=1$. 因此 $b_2^2\geqslant\dfrac{3}{4}$. 这样 $\Delta(L)=b_2\geqslant\dfrac{\sqrt{3}}{2}$，且 $|v_1|^2=1\leqslant\dfrac{2}{\sqrt{3}}\Delta(L)$.

■

对于经过努力仍未解决的问题，
如果没有大量卓有成效的创造，
我们就看不到问题的本质所在.

——Carl Friedrich Gauss

练　习

第一节　代数整数

1.1 $\frac{1}{2}(1+\sqrt{5})$是代数整数吗？

1.2 证明 $\mathbf{Q}[\sqrt{d}]$中的整数形成一个环.

1.3 (a) 令 α 是一个复数，它是一个首一的整多项式的根，这个多项式不必是既约的. 证明 α 是代数整数.

(b) 令 α 是代数数，它是一个整多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$ 的根. 证明 $a_n\alpha$ 是代数整数.

(c) 令 α 是代数整数，它是多项式 $x^n+a_{n-1}x^{n-1}+\cdots+a_0$ 的根. 证明 α^{-1} 是代数整数当且仅当 $a_0=\pm1$.

1.4 令 d 和 d' 是整数. 何时域 $\mathbf{Q}(\sqrt{d})$ 和 $\mathbf{Q}(\sqrt{d'})$ 是不同的？

第二节　分解代数整数

2.1 证明 2，3 和 $1\pm\sqrt{-5}$ 是环 $R=\mathbf{Z}[\sqrt{-5}]$ 的既约元且这个环的单位为 ±1.

2.2 对哪个负整数 $d\equiv2(\mathrm{mod}4)$ 是环 $\mathbf{Q}[\sqrt{d}]$ 中整数环的唯一分解？

第三节　$\mathbf{Z}[\sqrt{-5}]$中的理想

3.1 令 α 是环 $R=\mathbf{Z}[\delta]$，$\delta=\sqrt{-5}$ 中的一个元素，且令 $\gamma=\frac{1}{2}(\alpha+\alpha\delta)$. 在什么情况下以 $(\alpha,\ \gamma)$ 作为基的格是一个理想？

3.2 令 $\delta=\sqrt{-5}$. 确定给定向量的任意整数组合的格是否是一个理想：

408 (a) $(5,\ 1+\delta)$　(b) $(7,\ 1+\delta)$　(c) $(4-2\delta,\ 2+2\delta,\ 6+4\delta)$

3.3 令 A 是虚二次域的整数环 R 的一个理想. 证明存在 A 的一组格基，其中一个元素是通常的正整数.

3.4 对下面所列的每个环 R，用命题 13.3.3 的方法刻画在 R 中的理想. 作图展示每种情况下格可能的形状.

(a) $R=\mathbf{Z}[\sqrt{-3}]$　(b) $R=\mathbf{Z}\left[\frac{1}{2}(1+\sqrt{-3})\right]$　(c) $R=\mathbf{Z}[\sqrt{-6}]$

(d) $R=\mathbf{Z}\left[\frac{1}{2}(1+\sqrt{-7})\right]$　(e) $R=\mathbf{Z}[\sqrt{-10}]$

第四节　理想的乘法

4.1 令 $R=\mathbf{Z}[\sqrt{-6}]$. 求积理想 AB 的格基，其中 $A=(2,\ \delta)$，$B=(3,\ \delta)$.

4.2 令 R 是环 $\mathbf{Z}[\delta]$，其中 $\delta=\sqrt{-5}$，令 A 表示由下面的元素生成的理想：

(a) $3+5\delta$，$2+2\delta$；(b) $4+\delta$，$1+2\delta$. 确定给定的生成元是否形成 A 的格基，并确定理想 $\overline{A}A$.

4.3 令 R 是环 $\mathbf{Z}[\delta]$，其中 $\delta=\sqrt{-5}$，令 A 与 B 是形如 $A=\left(\alpha,\ \frac{1}{2}(\alpha+\alpha\delta)\right)$，$B=\left(\beta,\ \frac{1}{2}(\beta+\beta\delta)\right)$ 的理想. 通过求生成元证明 AB 是主理想.

第五节　分解理想

5.1 令 $R=\mathbf{Z}[\sqrt{-5}]$.

(a) 确定 11 是否为 R 的一个既约元，(11) 是否为 R 的一个素理想.

(b) 在 $\mathbf{Z}[\delta]$中分解主理想(14)为素理想.

5.2 令 $\delta=\sqrt{-3}$且 $R=\mathbf{Z}[\delta]$. 这不是虚二次域 $\mathbf{Q}[\delta]$上的整数环. 令 A 是理想$(2, 1+\delta)$.

(a) 证明 A 是一个极大理想，并确定商环 R/A.

(b) 证明$\overline{A}A$ 不是主理想，主引理对于这个环不成立.

(c) 证明 A 包含主理想(2)，但是 A 不整除(2).

5.3 令 $f=y^2-x^3-x$. 环 $\mathbf{C}[x, y]/(f)$是一个整环吗?

第六节 素理想与素整数

6.1 令 $d=-14$. 对于下面每一个素数 $p=2$，3，5，7，11 和 13，确定 p 在 R 中是否分裂或分叉. 如果是的话，求(p)的素理想因子的格基.

6.2 假设 d 是一个负整数，且 $d\equiv 1(\mathrm{mod}4)$. 分析 2 在模 8 同余的条件下是否是持素的.

6.3 令 R 是虚二次域的整数环.

(a) 假设一个整素数 p 在 R 上是持素的. 证明 $R/(p)$是具有 n^2 个元素的域.

(b) 证明如果 p 分裂但不分叉，则 $R/(p)$同构于积环 $\mathbf{F}_p\times\mathbf{F}_p$. 409

6.4 当 $d\equiv 2(\mathrm{mod}4)$或 $d\equiv 3(\mathrm{mod}4)$时，一个整素数 p 在环 $\mathbf{Q}[\sqrt{d}]$的整数环上是持素的如果多项式 x^2-d 是模 p 既约的.

(a) 证明这对 $d\equiv 1(\mathrm{mod}4)$，$p\neq 2$ 也是成立的.

(b) 当 $d\equiv 1(\mathrm{mod}4)$，$p=2$ 时情况会怎样?

6.5 假设 $d\equiv 2(\mathrm{mod}4)$或 $d\equiv 3(\mathrm{mod}4)$.

(a) 证明素整数 p 在 R 上分叉当且仅当 $p=2$ 或 p 整除 d.

(b) 令 p 是分叉的整素数，且设$(p)=P^2$. 求 P 的一个具体的格基. 在什么情况下 P 是一个主理想?

6.6 令 $d\equiv 2(\mathrm{mod}4)$或 $d\equiv 3(\mathrm{mod}4)$. 一个整素数具有形式 a^2-b^2d，其中 a，$b\in\mathbf{Z}$. 这与整数环 R 上(p)的素理想分解有什么联系?

6.7 假设 $d\equiv 2(\mathrm{mod}4)$或 $d\equiv 3(\mathrm{mod}4)$，且一个素数 $p\neq 2$ 在 R 上是持素的. 令 a 是一个整数满足 $a^2\equiv d(\mathrm{mod}p)$. 证明$(p, a+\delta)$是整除$(p)$的一个素理想的格基.

第七节 理想类

7.1 令 $R=\mathbf{Z}[\sqrt{-5}]$，且令 $B=(3, 1+\delta)$. 求主理想 B^2 的生成元.

7.2 证明虚二次域上的整数环上的两个非零理想 A 和 A'相似的充分必要条件是存在非零理想 C 使得 AC 和 $A'C$ 是主理想.

7.3 令 $d=-26$. 对于下列整数 n，确定 n 是否是 R 中元素 α 的范数. 如果是，求 α:n=75 250 375 5^6.

7.4 令 $R=\mathbf{Z}[\delta]$，其中 $\delta^2=-6$.

(a) 证明格 $P=(2, \delta)$和 $Q=(3, \delta)$是 R 的素理想.

(b) 在 R 上明确地分解主理想(6)为素理想.

(c) 确定 R 的类群.

第八节 计算类群

8.1 参考例 13.8.6，由于$\langle P\rangle=\langle S\rangle^3$ 和$\langle Q\rangle=\langle S\rangle^2$，因此引理 13.8.7 预言存在范数为 $2\cdot 5^3$ 和 $3^2\cdot 5^2$ 的元素. 求这些元素.

8.2 参考例 13.8.8，解释为什么 $N(4+\delta)$和 $N(14+\delta)$不能导致矛盾的结论.

8.3 令 $R=\mathbf{Z}[\delta]$，$\delta=\sqrt{-29}$. 在每一种情形，计算范数，解释为什么能够从对 R 中理想的范数的计算得出结论，并确定 R 的类群：$N(1+\delta)$，$N(4+\delta)$，$N(5+\delta)$，$N(9+2\delta)$，$N(11+2\delta)$.

8.4 证明定理 13.2.5 中所列的 d 的值有唯一分解.

8.5 对每一种情形，确定类群并画出可能的格的形状：

(a) $d=-10$ (b) $d=-13$ (c) $d=-14$ (d) $d=-21$

8.6 对每一种情形，确定类群：

410 (a) $d=-41$ (b) $d=-57$ (c) $d=-61$ (d) $d=-77$ (e) $d=-89$

第九节 实二次域

9.1 证明 $1+\sqrt{2}$ 在 $\mathbf{Z}[\sqrt{2}]$ 的单位的群中是无限阶的元素.

9.2 确定方程 $x^2-y^2d=1$ 的解，其中 d 是一个正整数.

9.3 (a) 证明度量函数 $\sigma(\alpha)=|N(\alpha)|$ 把环 $\mathbf{Z}[\sqrt{2}]$ 变成欧几里得整环，且这个环有唯一分解.

(b) 在图 13.9.6 嵌入的描述中，做一个简图展示 $R=\mathbf{Z}[\sqrt{2}]$ 的主理想 $(\sqrt{2})$.

9.4 令 R 是实二次数域的整数环. R 的单位群的可能结构是什么？

9.5 令 R 是实二次数域的整数环，令 U_0 表示嵌入(13.9.2)中位于第一象限的 R 的单位的集合.

(a) 证明 U_0 是单位群的一个无限循环子群.

(b) 当 $d=3$ 和 $d=5$ 时，求 U_0 的一个生成元.

(c) 对 $d=3$，在合理的尺寸范围画一个图表示这个双曲线和这些单位.

第十节 关于格

10.1 令 M 是 $\mathbf{R}^2$ 上的整数格，令 L 为以 $((2,3)^t,(3,6)^t)$ 为基的格. 确定指标 $[M:L]$.

10.2 令 $L\subset M$ 是分别以 $\boldsymbol{B}$ 和 $\boldsymbol{C}$ 为基的格，令 A 是使得 $\boldsymbol{B}A=\boldsymbol{C}$ 的整数矩阵. 证明 $[M:L]=|\det A|$.

杂题

M.1 描述 $\mathbf{C}$ 的子环 S，这个子环是复平面上的格.

*M.2 令 $R=\mathbf{Z}[\delta]$，其中 $\delta=\sqrt{-5}$，且令 p 是一个素整数.

(a) 证明如果 p 在 R 上分裂，比如 $(p)=\overline{P}P$，则恰有椭圆 $x^2+5y^2=p$ 或 $x^2+5y^2=2p$ 包含一个整数点.

(b) 求一个性质使其能确定哪一个椭圆有整数点.

M.3 描述在下列两种情形下的素理想：(a)两个变量的多项式环 $\mathbf{Z}[x,y]$；(b)整多项式环 $\mathbf{Z}[x]$.

M.4 令 L 表示平面 $\mathbf{R}^2$ 上的整数格 $\mathbf{Z}^2$，令 P 是一个顶点在平面上的格 L 上的多边形. Pick 定理断言面积 $\Delta(P)$ 等于 $a+b/2-1$，其中 a 是 P 的内部的格 L 的点的数目，b 是 P 的边界上的格 L 的点的数目.

(a) 证明 Pick 定理.

411 (b) 从 Pick 定理推导出命题 13.10.6.

第十四章　环中的线性代数

发聩明点！做雅广！

——*Picayune Sentinel*

线性代数的一个基本问题是解线性方程组．我们考虑方程组 $AX=B$，其中 A 与 B 中的元素都属于环 R，且要求其解 $X=(x_1, \cdots, x_n)^t$，满足 $x_i \in \mathbf{R}$，当 R 是环时，解方程组是复杂的，但我们将看到当环 R 是整数环或者是一个域上的多项式环时，这样的方程组有解．

第一节　模

与域上的向量空间类似，环上的向量空间叫做模．

令 R 是一个环．R-模 V 是一个带有记作＋的合成法则的阿贝尔群与一个标量积 $R\times V \to V$，写成 $r, v \rightsquigarrow rv$，且满足下面公理：

【14.1.1】　$1v=v$，　$(rs)v=r(sv)$，　$(r+s)v=rv+sv$，　$r(v+v')=rv+rv'$

对所有 $r, s\in R$ 和 $v, v'\in V$ 都成立．

注意到这几条恰好是向量空间(3.1.2)的公理．但环的元素不必可逆这一事实使得模更为复杂．

我们的第一个例子是 R-向量的模 R^n，即 R 中元素的列向量的模．这些模称为自由模．R-向量的合成法则与元素在一个域中的向量的合成法则是一样的：

$$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1+b_1 \\ \vdots \\ a_n+b_n \end{bmatrix}, \quad r\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} ra_1 \\ \vdots \\ ra_n \end{bmatrix}$$

但当 R 不是域时，这些模不再是仅有的模．存在不同构于任意自由模的模，即使它们是由有限集合张成的．

一个合成法则记为加法的任意阿贝尔群 V 有唯一的方法构成 $\mathbf{Z}$ 上的一个模．分配律使得我们可以令 $2v=(1+1)v=v+v$，等等：

$$nv = v+\cdots+v = \text{“}n\text{ 倍 }v\text{”}$$

412

且 $(-n)v=-(nv)$ 对于任意正整数 n 成立．我们的确把 V 做成一个 $\mathbf{Z}$-模，直观上这是非常容易接受的．这是把 V 做成一个 $\mathbf{Z}$-模的唯一一种方式．这里我们不给出正式证明了．

反之，任意 $\mathbf{Z}$-模具有一个由忘却其标量乘法只保持其加法运算律的阿贝尔群结构．

【14.1.2】　阿贝尔群和 $\mathbf{Z}$-模是等价的概念．

我们需要在阿贝尔群上用加法记号而使这个对应看起来是自然的，而整章我们都这样做．

阿贝尔群提供了环上的模不必是自由模的例子．由于当 n 为正数时，$\mathbf{Z}^n$ 是无限的，因此除了零群以外的有限阿贝尔群不同构于一个自由模．

R-模 V 的子模 W 是一个在加法和标量乘法下封闭的子集. V 上的合成法则使子模 W 成为模. 当环 R 看作自由 R-模 R^1 时，我们已经见过了前面情形的子模，即环 R 的子模.

【14.1.3】命题 R-模 R 的子模是 R 的理想.

由定义，理想是 R 的关于加法和乘法封闭的非空子集.

R-模同态 $\varphi: V \to W$ 的定义类似于向量空间的线性变换，这个映射关于合成法则是相容的：

【14.1.4】
$$\varphi(v+v') = \varphi(v) + \varphi(v'), \quad \varphi(rv) = r\varphi(v)$$

对于所有 v，$v' \in V$ 和 $r \in \mathbf{R}$ 成立. 同构是一个双射同态. 同态 $\varphi: V \to W$ 的核是满足 $\varphi(v)=0$ 的 $v \in V$ 的元素的集合，是定义域 V 的一个子模，同态的像是值域 W 的一个子模.

我们可以把商结构推广到模上. 令 W 是 R-模 V 的一个子模. 商模 $\overline{V}=V/W$ 是加法陪集 $\overline{v}=[v+W]$ 所成的群. 它由下面的规则成为一个 R-模：

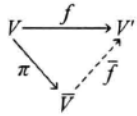
【14.1.5】
$$r\overline{v} = \overline{rv}$$

关于商模的主要结论列举如下.

【14.1.6】定理 令 W 是 R-模 V 的一个子模.

(a) W 在 V 中的加法陪集的集合 $\overline{V}$ 是一个 R-模，且典范映射 $\pi: V \to \overline{V}$ 映 $v \rightsquigarrow \overline{v}=[v+W]$ 是 R-模的满同态，其核为 W.

(b) 映射性质：令 $f: V \to V'$ 是 R-模同态，且同态核 K 包含 W. 则存在唯一的同态：$\overline{f}: \overline{V} \to V'$ 使得 $f=\overline{f} \circ \pi$.



413

(c) 第一同构定理：令 $f: V \to V'$ 是 R-模满同态，其核等于 W. 则(b)中定义的映射 $\overline{f}: \overline{V} \to V'$ 是一个同构.

(d) 对应定理：令 f：$V \to \mathcal{V}$ 是核为 W 的 R-模满同态. 则存在 $\mathcal{V}$ 的子模与 V 的包含 W 的子模之间的一个一一对应. 这个对应定义如下：如果 $\mathcal{S}$ 是 $\mathcal{V}$ 的子模，对应于 V 的子模为 $S=f^{-1}(\mathcal{S})$ 且如果 S 是 V 的包含 W 的子模，则对应的 W 的子模为 $\mathcal{S}=f(S)$. 如果 S 和 $\mathcal{S}$ 是对应的子模，则 V/S 同构于 $\mathcal{V}/\mathcal{S}$.

我们已经看到了环与理想以及群与正规子群间的类似的结果. 证明和以前的证明类似，在此省略.

第二节 自 由 模

自由模构成一个重要的代数类，在此予以讨论. 从本章第五节开始，我们讨论其他模.

注 R 是一个环. 一个 R-矩阵是元素在环 R 中的矩阵. 一个 R-可逆矩阵是其逆矩阵也是 R-矩阵的 R-矩阵. $n \times n$ 可逆 R-矩阵形成的群叫做 R 上的一般线性群：

【14.2.1】
$$GL_n(R) = \{n \times n \text{ 可逆 } R\text{- 矩阵}\}.$$

R-矩阵 $A=(a_i a_j)$的行列式可由第一章描述的规则计算，例如，完全展开式(1.6.4)将行列式 $\det A$ 表示为带有 n^2 个矩阵元素的系数为± 1 的多项式.

【14.2.2】
$$\det A = \sum_p \pm a_{1,p1},\cdots,a_{n,pn}$$

和前面一样，这个和取遍指标集合$\{1, \cdots, n\}$的所有置换，符号± 1 代表置换的符号. 将这个公式在一个 R-矩阵上取值，得到 R 的一个元素. 通常的行列式规则仍然成立，例如

$$(\det A)(\det B) = \det(AB)$$

当矩阵元素属于一个域时我们已经证明这一规则(1.4.10)，下一节将讨论这样的性质能搬到 R-矩阵的原因，我们假定它们可搬到 R-矩阵上.

【14.2.3】**引理** *令 R 是一个非零环.*

(a) 一个方 R-矩阵 A 是可逆的当且仅当它有左逆或右逆，或当且仅当它的行列式是环的一个单位.

(b) 一个可逆 R-矩阵是方阵.

证明

(a) 如果 A 有左逆 L，则$(\det L)(\det A)=\det I=1$ 表明 $\det A$ 在 R 中有逆元，故 $\det A$ 是 R 的一个单位. 类似的推理表明如果 A 有右逆，则 $\det A$ 是一个单位. 414

如果 A 是 R-矩阵且其行列式 δ 为 R 上的单位，则克莱姆法则 $A^{-1}=\delta^{-1}\mathrm{cof}(A)$(其中 $\mathrm{cof}(A)$是(1.6.7)中的伴随矩阵)表明存在系数在 R 上的逆矩阵.

(b) 假设一个 $m\times n$ 的 R-矩阵 P 是可逆的，即存在一个 $n\times m$ 的 R-矩阵 Q，使得 $PQ=I_m$，$QP=I_n$. 如果有必要，可交换 P 和 Q，我们无妨假设 $m\geqslant n$. 如果 $m\neq n$，则通过添加 0 使 P 和 Q 为方阵：

$$\left[P \;\middle|\; 0\right]\begin{bmatrix}Q\\0\end{bmatrix}=I_m$$

这并不改变 P 和 Q 的乘积，但是这些方阵的行列式都是 0，故它们不可逆. 因此 $m=n$. ■

当环 R 中单位不多时，可逆矩阵的行列式必须是单位这一事实对于矩阵是一个很强的条件. 例如，如果 R 是整数环，则行列式必为± 1. 大多数整数矩阵是可逆的实矩阵，因而它们属于 $GL_n(\mathbf{R})$. 但除非行列式为± 1，否则逆矩阵的元素不会是整数：它们不是 $GL_n(\mathbf{Z})$的元素. 而如果 $n>1$，则仍有相当多的可逆 $n\times n$ R-矩阵. 初等矩阵 $E=I+ae_{i,j}$(其中 $i\neq j$，$a\in\mathbf{R}$)是可逆的，因此它们生成一个相当大的群.

我们现在回到环 R 上的模的讨论，基与无关性的概念(第三章第四节)可以不做改动地由向量空间搬到模上. 称模 V 的一个有序元素集$(v_1, \cdots, v_k)$生成或张成 V，如果每个 $v\in V$是一个线性组合：

【14.2.4】
$$v = r_1 v_1 + \cdots + r_k v_k$$

其中系数 $r_i\in R$. 像这种情形，元素 v_i 称为生成元. 如果模 V 有一个有限的生成元集，则称为有限生成的，我们研究的大多数模都将是有限生成的.

模 V 的一个元素集合$(v_1, \cdots, v_n)$是无关的，如果线性组合 $r_1 v_1+\cdots+r_n v_n$ 是零，其

中$r_i \in R$，且所有系数$r_i = 0$. 若元素集合$(v_1, \cdots, v_n)$生成V，且$(v_1, \cdots, v_n)$是无关的，则称为一组基. 和向量空间一样，集合$(v_1, \cdots, v_n)$是一组基如果V中每个元素v可以唯一方式表示为线性组合(14.2.4). 标准基$\boldsymbol{E} = (e_1, \cdots, e_k)$是$R^n$的一组基.

我们也会谈到无限集合的线性组合和线性无关，这会用到第三章第七节的术语. 即使S是无限集合，它的线性组合也只涉及有限多项.

如果V的元素的一个有序集合$(v_1, \cdots, v_n)$用$\boldsymbol{B}$来表示，如第三章所述，则用$\boldsymbol{B}$乘，得

415

$$\boldsymbol{BX} = (v_1, \cdots, v_n)\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = v_1 x_1 + \cdots + v_n x_n$$

这定义了一个模同态，仍然记为$\boldsymbol{B}$：

【14.2.5】
$$R^n \xrightarrow{\boldsymbol{B}} V$$

和前面一样，标量移到了右边. 这个同态是满射，当且仅当$\boldsymbol{B}$生成V；同态是单射，当且仅当$\boldsymbol{B}$是无关的；同态是双射，当且仅当$\boldsymbol{B}$是一组基. 因此一个模V有基当且仅当它同构于某个自由模R^k，如果这样，该模也称为自由模. 一个模是自由的当且仅当它有基.

多数模没有基

一个自由$\mathbf{Z}$-模也叫做自由阿贝尔群. $\mathbf{R}^2$上的格是自由阿贝尔群，当有限时，非零阿贝尔群不是自由的.

自由模的基的运算和向量空间的基运算类似. 如果$\boldsymbol{B}$是自由模V的一组基，则一个元素$v \in V$在这组基$\boldsymbol{B}$下的坐标向量是使得$v = \boldsymbol{B}X$成立的唯一的列向量X. 如果$\boldsymbol{B} = (v_1, \cdots, v_m)$和$\boldsymbol{B}' = (v'_1, \cdots, v'_n)$是同一个自由模$V$的两组基，则如第三章那样可得基变换矩阵，同构把新的基的元素用旧的基的线性组合来表示$\boldsymbol{B}' = \boldsymbol{B}P$.

【14.2.6】命题 *令R是一个非零环.*

(a) 一个自由模的基变换矩阵P是一个可逆的R-矩阵.

(b) R上同一个自由模的两个基具有同样的元素个数.

(a)的证明和命题3.5.9的证明相同；(b)的证明由(a)和14.2.3可得.

一个自由模V的基的元素个数叫做V的秩. V的秩和向量空间的维数类似.（许多概念在环上的模中有不同的名称.）

正如在向量空间中一样，任意两个自由模R^n和R^m之间的模同态可以由左乘一个R-矩阵A给出：

【14.2.7】
$$R^n \xrightarrow{A} R^m$$

A的第j列是$f(e_j)$. 同样，如果$\varphi: V \to W$是分别以$\boldsymbol{B} = (v_1, \cdots, v_n)$和$\boldsymbol{C} = (w_1, \cdots, w_m)$为基的两个自由$R$-模的同态，则关于$\boldsymbol{B} = (v_1, \cdots, v_n)$的同态矩阵是$A = (a_{ij})$，其中

【14.2.8】
$$\varphi(v_j) = \sum_i w_i a_{ij}$$

如果 X 是向量 v 的坐标向量，即如果 $v=\boldsymbol{B}X$，则 $Y=AX$ 是其像的坐标向量，即 $\varphi(v)=\boldsymbol{C}Y$.

【14.2.9】

$$\begin{array}{ccc} R^n & \xrightarrow{A} & R^m \\ \boldsymbol{B}\downarrow & & \downarrow\boldsymbol{C} \\ V & \xrightarrow{\varphi} & W \end{array} \qquad \begin{array}{ccc} X & \rightsquigarrow & Y \\ \downarrow & & \downarrow \\ v & \rightsquigarrow & \varphi(v) \end{array}$$

416

正如在线性变换中一样，借助一个可逆 R-矩阵 P 和 Q 变换基 $\boldsymbol{B}$ 和基 $\boldsymbol{C}$，这个变换把 φ 的矩阵变为 $A'=Q^{-1}AP$.

第三节 恒 等 式

本节我们着重考虑下面的问题：为什么元素属于一个域的矩阵的性质对于元素属于一个任意环的矩阵仍然成立？简单地说，如果它们是恒等式，也就是说当把矩阵元素换为变量时它们仍然成立. 更准确地说，假设想要证明像行列式的乘法性质这样的恒等式，$(\det A)(\det B)=\det(AB)$，或克莱姆法则等. 假如已对复元素矩阵验证了恒等式，我们不想再重复一次，然而可能用到 $\mathbf{C}$ 的特殊性质，例如域的公理来验证恒等式，我们的确用到了域的性质来证明得到的恒等式，因而给出的证明对环不起作用，我们现在指出如何关于复数的恒等式对所有环推导出同样的恒等式.

原理是非常一般的，但为集中注意力，我们利用行列式的完全展开(即定义)来考虑乘法性质：$(\det A)(\det B)=\det(AB)$. 首先将矩阵元素用变量代替. 用 X 和 Y 表示待定的 $n\times n$矩阵，则恒等式为$(\det X)(\det Y)=\det(XY)$. 写为

【14.3.1】 $$f(X,Y)=(\det X)(\det Y)-\det(XY)$$

这是一个有 $2n^2$ 个变量矩阵元素 x_{ij} 和 y_{kl} 的多项式，是关于这些变量的整多项式环 $\mathbf{Z}[\{x_{ij}\},\{y_{kl}\}]$中的一个元素.

给定系数在环 R 上的两个矩阵 $A=(a_{ij})$和 $B=(b_{kl})$，存在唯一一个同态

【14.3.2】 $$\varphi:\mathbf{Z}[\{x_{ij}\},\{x_{kl}\}]\to R$$

代入作替换，使得 $x_{ij}\rightsquigarrow a_{ij}$，$y_{kl}\rightsquigarrow b_{kl}$.

参看行列式的定义，我们看到，因为 φ 是同态，所以有

$$f(X,Y)\rightsquigarrow f(A,B)=(\det A)(\det B)-\det(AB)$$

要证明行列式的乘法性质对任意环成立，只需证明 f 是多项式环 $\mathbf{Z}[\{x_{ij}\},\{y_{kl}\}]$中的零元即可. 这就是证明$(\det X)(\det Y)=\det(XY)$是个恒等式. 如果是这样，则由于 $\varphi(0)=0$，故$f(A,B)=0$对于任意环上的矩阵 A，B 成立.

现在，如果我们展开 f 并合并同类项，并将 f 写成单项式的线性组合，则这些单项式的系数均为 0. 然而，我们不会也不想这么做. 为解释清楚这一点，我们以 2×2 矩阵为例. 在此情形下，

$$\begin{aligned} f(X,Y)=&((x_{11}x_{22}-x_{12}x_{21})(y_{11}y_{22}-y_{12}y_{21}))-(x_{11}y_{11}+x_{12}y_{21})(x_{21}y_{12}+x_{22}y_{22}) \\ &+(x_{11}y_{12}+x_{12}y_{22})(x_{21}y_{11}+x_{22}y_{22}) \end{aligned}$$

417

这是零多项式，但它并不显然为零，我们也不想用更大的矩阵验算了.

换一种方式，我们做如下推理：多项式确定了 $2n^2$ 个复变量$\{x_{ij}, y_{kl}\}$空间上的函数：如果 A，B 是复矩阵，且如果计算 f 在$\{a_{ij}, b_{kl}\}$的值，我们得到 $f(A, B)=(\det A)(\det B)-\det(AB)$. 我们知道 $f(A, B)=0$ 是因为恒等式当 A，B 是复矩阵时成立. 故函数 f 恒等于 0. 定义为零函数的多项式只有零多项式. 故 $f=0$.

在任意环上进行下面的讨论并证明关于恒等式成立的一般定理是可能的. 然而，即使是数学家有时也感到不必做出精确的表述——当遇到每一具体情形再考虑有时会更容易些，这里就是一个这样的情形.

第四节 整数矩阵的对角化

本节讨论本章开始提到的问题：给定一个 $m\times n$ 整数矩阵 A(矩阵中的元素均为整数)和一个整数列向量 B，求线性方程组的整数解

【14.4.1】
$$AX = B$$

用整数矩阵 A 左乘就定义了一个映射 $\mathbf{Z}^n \xrightarrow{A} \mathbf{Z}^m$. 它的核是齐次方程组 $AX=0$ 的整数解的集合，它的像是使得方程组 $AX=B$ 有整数解的那些整数向量 B 的集合. 和以往一样，非齐次方程组 $AX=B$ 的全部解由其一个特解和相应的齐次方程组的通解相加得到.

当系数在一个域上时，行约简是解线性方程组的常用方法. 这里，这些运算受到了很多限制：只有当给定的整数矩阵是*可逆的整数矩阵*时，即有一个整数矩阵为其逆矩阵时，这个行约简的方法才能使用. 可逆的整数矩阵形成*整数一般线性群* $GL_n(\mathbf{Z})$.

当用行或列变换简化矩阵时，能得到最好的结果. 故我们允许做下列运算：

【14.4.2】

- 一行(列)的整数倍加到另一行(列)上去；
- 互换两行或两列；
- 用-1乘以某行或某列.

任何上面的运算都可以用一个*初等整数矩阵*左乘或右乘 A 来得到. *初等整数矩阵*是可逆的整数矩阵. 通过一系列这样的运算将得到形如

【14.4.3】
$$A' = Q^{-1}AP$$

418. 的矩阵，其中 Q 和 P 是适当大小的可逆整数矩阵.

在一个域上，任何矩阵都可通过行或列运算(4.2.10)简化为下面的矩阵块的形式：

$$A' = \begin{bmatrix} I & \\ & 0 \end{bmatrix}$$

但对于整数环上的矩阵我们不能指望其化简成上面的形式：对 1×1 矩阵就不能化简成上述形式. 但我们可以对角化整数矩阵.

例如：

【14.4.4】
$$A=\begin{bmatrix}1&2&3\\4&6&6\end{bmatrix}\xrightarrow{\text{行运算}}\begin{bmatrix}1&2&3\\0&-2&-6\end{bmatrix}\xrightarrow{\text{列运算}}\begin{bmatrix}1&0&0\\0&-2&-6\end{bmatrix}$$
$$=\begin{bmatrix}1&0&0\\0&-2&-6\end{bmatrix}\xrightarrow{\text{行运算}}\begin{bmatrix}1&0&0\\0&2&6\end{bmatrix}\xrightarrow{\text{列运算}}\begin{bmatrix}1&0&0\\0&2&0\end{bmatrix}=A'$$

所得矩阵具有形式 $A'=Q^{-1}AP$，其中 Q 和 P 是可逆整数矩阵：

【14.4.5】
$$Q^{-1}=\begin{bmatrix}1&\\4&-1\end{bmatrix},\quad P=\begin{bmatrix}1&-2&3\\&1&-3\\&&1\end{bmatrix}$$

（计算这些矩阵时很容易出错．为了计算 Q^{-1}，行运算所产生的初等矩阵以逆序相乘，而计算矩阵 P 时是按照初等矩阵的运算顺序相乘的．）

【14.4.6】定理 *令 A 是一个整数矩阵．存在适当大小的初等整数矩阵 Q 和 P 使得 $A'=Q^{-1}AP$ 是对角矩阵，比如*

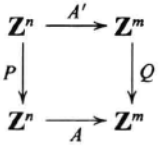
$$A'=\begin{bmatrix}\begin{bmatrix}d_1&&\\&\ddots&\\&&d_k\end{bmatrix}&\\&0\end{bmatrix}$$

此处对角线元素 d_i 是正整数，且一个整除另一个：$d_1\mid d_2\mid\cdots\mid d_k$.

注意对角线不一定到右下角，除非矩阵 A 为方阵．如果 $k<m$，$k<n$，则对角线元素在下面会有一些零．

我们可以把上述定理中出现的四个矩阵的内在联系用下图总结起来：

【14.4.7】图



此处映射用定义这个映射的矩阵来表示．

419

证明 设 $A\neq 0$．方法是实施一系列行或列变换得到如下形式的矩阵

【14.4.8】
$$\begin{bmatrix}d_1&0&\cdots&0\\0&&&\\\vdots&&M&\\0&&&\end{bmatrix}$$

其中 d_1 整除 M 中的每一个元素．当这步完成后，再对 M 做同样的变换．我们给出一个系统的方法，虽然这个方法可能不是把矩阵化为对角形的最快的方法．这个方法基于反复使用带余除法．

第一步：通过行或列置换，把绝对值最小的非零元素移到矩阵的左上角．如果必要，

用-1乘以第一行使得左上角元素a_{11}是正数.

接下来，我们尝试把第一列其他位置的元素消为零. 每当遇到一个运算产生了绝对值比a_{11}小的非零元素，就回到第一步再开始整个过程. 虽然这会把我们前面的工作搞砸，但是也有进步，因为a_{11}变小了. 通常经有限步就能使a_{11}最小.

第二步：如果第一列含有非零元素a_{i1}，$i>1$，则用a_{11}除a_{i1}：

$$a_{i1} = a_{11}q + r$$

其中q，r是整数，且余数r满足$0 \leqslant r < a_{11}$. 我们将第i行减去第1行的q倍. 将a_{i1}用r代替. 如果$r \neq 0$，则回到第一步. 如果$r=0$，我们就把第一列某个元素消成零.

第一步和第二步施行有限步之后所有a_{i1}都为零，其中$i>1$. 同理，用列变换把第一行的其他位置元素消为零，最终得到了只有第一行第一列元素a_{11}不是零，而第一行和第一列其他位置元素全为零的矩阵.

第三步：假设a_{11}是第一行和第一列仅有的非零元素，但M中有某个元素b不能被a_{11}整除，则我们把A的含有b的那一列加到第一列上去，这就在第一列生成元素b. 回到第二步. 带余除法产生一个更小的非零的元素，又回到第一步. ■

我们现在准备好了解整数线性方程组$AX=B$.

【14.4.9】命题 令A是一个$m \times n$矩阵，令P和Q是可逆的整数矩阵使得$A'=Q^{-1}AP$为定理14.4.6中描述的对角形矩阵.

(a) 齐次方程组$A'X'=0$的整数解是整数向量X'，它的前k个坐标均为零.

(b) 齐次方程组$AX=0$的整数解是所有形如$X=PX'$的整数解，其中$A'X'=0$.

420 (c) 用A'乘得到的像W'由所有向量d_1e_1，…，d_ke_k的任意整系数组合构成.

(d) 用A乘得到的像W由所有向量$Y=QY'$构成，其中Y'属于W'.

证明

(a) 因为A'是对角形的，故方程组$A'X'=0$可写成

$$d_1x_1' = 0, \quad d_2x_2' = 0, \cdots, d_kx_k' = 0$$

为得到方程组$A'X'=0$的解，必须对于所有$i=1$，…，k，有$x_i'=0$而对于$i>k$，x_i'可以为任意整数.

(c) 映射A'的像由A'的列生成，因为A'是对角形的，其列非常简单：当$j \leqslant k$，$A_j' = d_je_j$；当$j>k$，$A_j'=0$.

(b)和(d) 将P和Q分别看成$\mathbf{Z}^n$和$\mathbf{Z}^m$的基变换矩阵. 图14.4.7中竖直向下的箭头是双射，故P把A'的核双射地映射为A的核，Q把A'的像双射地映射为A的像. ■

我们回到例(14.4.4). 观察矩阵A'，看到方程组$A'X'=0$的解是e_3的整数倍. 所有方程组$AX=0$的解是Pe_3的整数倍，它是P的第三列$(3, -3, 1)^t$. A'的像由向量e_1和$2e_2$的整数组合构成. A的像由用Q乘这些向量得到. 在这个例子中恰巧$Q=Q^{-1}$. 故它的像由矩阵列向量的整数组合构成.

$$QA' = \begin{bmatrix} 1 & 0 \\ 4 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 4 & -2 \end{bmatrix}$$

当然，A 的像也由 A 的列的整数组合的集合表示，但是那些列不能构成 **Z**-基.

自由模的子模

整矩阵的对角化的定理可用于刻画自由阿贝尔群间的同态.

【14.4.10】推论 *令 $\varphi: V \to W$ 是自由阿贝尔群的同态. 存在 V 和 W 的基使得同态矩阵为对角形矩阵(14.4.6).*

【14.4.11】定理 *令 W 是秩为 m 的自由阿贝尔群，且令 U 是 W 的子群. 则 U 是一个自由阿贝尔群，且它的秩小于等于 m.*

证明 首先我们选取 W 的一组基 $\boldsymbol{C}=(w_1, \cdots, w_m)$ 和 U 的一组生成元集 $\boldsymbol{B}=(u_1, \cdots, u_n)$. 记 $u_j=\sum_i w_i a_{ij}$，令 $A=(a_{ij})$. 当以 W 的基 $\boldsymbol{C}$ 来计算，矩阵 A 的列是生成元 u_j 的坐标向量. 我们得到了阿贝尔群的同态交换图 421

【14.4.12】图

$$\begin{array}{ccc} \mathbf{Z}^n & \xrightarrow{A} & \mathbf{Z}^m \\ {\scriptstyle B}\downarrow & & \downarrow{\scriptstyle C} \\ U & \xrightarrow{i} & W \end{array}$$

其中 i 表示 U 到 W 的包含关系. 因为 $\boldsymbol{C}$ 是基，故右边向下的箭头是双射，且因为 $\boldsymbol{B}$ 生成 U，故左边的向下的箭头是满射.

我们对角化矩阵 A. 用通常的记号 $A'=Q^{-1}AP$，我们把矩阵 P 看成是 $\mathbf{Z}^n$ 的基变换矩阵，把 Q 看作是 $\mathbf{Z}^m$ 的基变换矩阵. 令 $\boldsymbol{C}'$ 和 $\boldsymbol{B}'$ 是新的基. 由于当初的基 $\boldsymbol{C}$ 的选取和生成元集 $\boldsymbol{B}$ 的选取是任意的，因而可以把上图中的 $\boldsymbol{C}$，$\boldsymbol{B}$ 和 A 替换成 $\boldsymbol{C}'$，$\boldsymbol{B}'$ 和 A'. 故我们可以假设矩阵 A 有(14.4.6)中给定的对角形. 则对于 $j=1, \cdots, k$，$u_j=d_j w_j$.

粗略地说，这就是证明，但是还有几点需要考虑. 首先，对角矩阵 A 可以包含零列. 一个零列对应着一个生成元 u_j，u_j 关于 W 的基 $\boldsymbol{C}$ 下的坐标向量为零向量. 故 u_j 也是零. 这个向量作为生成元是没用的，因而将其去掉. 当去掉了零生成元之后，所有的对角元素都是正的，且有 $k=n$ 和 $n \leqslant m$.

如果 W 是零子群，那么最后将舍弃所有生成元. 与向量空间一样，我们必须采用空集合作为零模的一个基；或在定理的叙述中要特别提到这一例外情形.

我们假定 $m \times n$ 矩阵是对角形的，对角线上元素 $d_1, \cdots, d_n$ 均为正的，且 $n \leqslant m$，我们证明集合 $(u_1, \cdots, u_n)$ 是 U 的基. 由于这个集合生成 U，故只需证明这个集合是无关的。我们将线性关系 $a_1u_1 + \cdots + a_nu_n = 0$ 写成形式 $a_1d_1w_1 + \cdots + a_nd_nw_n = 0$. 由于 $(w_1, \cdots, w_n)$ 是基，故对于每个 i，有 $a_id_i=0$，由于 $d_i>0$，因此 $a_i=0$.

最后一点更为严重：需要从 U 的一个生成元的有限集合开始. 怎么知道存在这样一个集合？有限生成的阿尔贝群的子集都是有限生成的，这是一个事实. 我们将在本章第六节证明这一点. 目前定理只能是在 U 是有限生成的子集的附加假设之下得证. ■

假设 $\mathbf{R}^2$ 上的一个带有基 $\boldsymbol{B}=(v_1, v_2)$ 的格 L 是带有基 $\boldsymbol{C}=(u_1, u_2)$ 的格 M 的子格，令

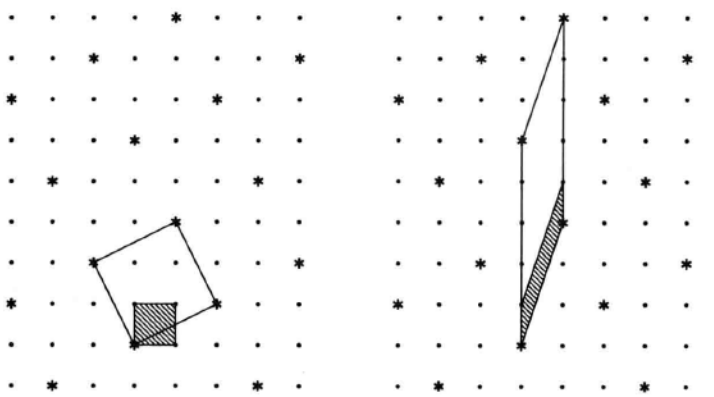
A 是整数矩阵满足 $\boldsymbol{B}=\boldsymbol{C}A$. 如果我们改变 L 和 M 的基，矩阵 A 将变为矩阵 $A'=Q^{-1}AP$，其中 Q 和 P 是可逆整数矩阵. 根据定理 14.4.6，可以适当选择基使得 A 为对角形的矩阵，对角元素为正整数 d_1，d_2. 假设已经做到这样了. 则如果 $\boldsymbol{B}=(v_1, v_2)$ 和 $\boldsymbol{C}=(u_1, u_2)$，则由方程 $\boldsymbol{B}=\boldsymbol{C}A$ 可得到 $v_1=d_1u_1$ 和 $v_2=d_2u_2$.

【14.4.13】例 令 $\mathrm{Q}=\begin{bmatrix}1 & \\ 3 & 1\end{bmatrix}$，$\mathrm{A}=\begin{bmatrix}2 & -1\\ 1 & 2\end{bmatrix}$，$\mathrm{P}=\begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}$，$\mathrm{A}'=\mathrm{Q}^{-1}\mathrm{AP}=\begin{bmatrix}1 & \\ & 5\end{bmatrix}$.

令 M 是具有标准基 $\boldsymbol{C}=(e_1, e_2)$ 的整数格，令 L 是以 $\boldsymbol{B}=(v_1, v_2)=((2, 1)^t,$ 422 $(-1, 2)^t)$为基的格. 它的坐标向量是 A 的列向量. 我们把 P 理解为 L 的基的变换矩阵，把 Q 理解为 M 的基的变换矩阵. 用坐标向量表示，新的基是 $\boldsymbol{C}'=(e_1, e_2)Q=((1, 3)^t, (0, 1)^t)$且 $\boldsymbol{B}'=(v_1, v_2)P=((1, 3)^t, (0, 5)^t)$.

下面左边的图表示由两个原来的基张成的正方形，右边的图表示由两个新的基张成的平行四边形. 由 L 的新的基张成的平行四边形由将阴影部分的平行四边形平移 5 次填充得到，而阴影部分的平行四边形由 M 的新基张成. 指标是 5. 注意在区域 $\Pi'(v_1, v_2)$ 中有 5 个格点，这与命题 13.10.3(d)一致. 右图也清楚地表明比值 $\Delta(L)/\Delta(M)$ 是 5.

【14.4.14】图



对角化，应用于一个子格 ■

第五节 生成元和关系

本节将注意力转到非自由的模，我们将指出如何用称为表现矩阵的矩阵来刻画一大类模.

用一个 $m\times n$ 的 R-矩阵 A 左乘定义一个 R-模同态 $R^n \xrightarrow{A} R^m$. 同态的像由系数属于环 R 的矩阵 A 的列的线性组合构成，记作 AR^n. 我们称商模 $V=R^m/AR^n$ 由矩阵 A 表现. 更一般地，我们称任何同构 $\sigma: R^m/AR^n \to V$ 是模 V 的一个表现. 如果存在这样的同构的话，则矩阵 A 称为模 V 的一个表现矩阵.

例如，5 阶循环群 C_5 用一个 1×1 整数矩阵[5]表现为一个 $\mathbf{Z}$-模，因为 C_5 同构于 $\mathbf{Z}/5\mathbf{Z}$.

423 我们用典范映射 $\pi: R^m \to V=R^m/AR^n$(14.1.6)解释商模 R^m/AR^n 如下：

【14.5.1】命题

(a) V 是由元素 $\boldsymbol{B}=(v_1, \cdots, v_m)$ 的集合生成，其中 $\boldsymbol{B}=(v_1, \cdots, v_m)$ 是 R^m 的标准基元素的像.

(b) 如果 $Y=(y_1, \cdots, y_m)^t$ 是 R^m 的一个列向量，则 V 的元素 $\boldsymbol{B}Y=v_1y_1+\cdots+v_my_m$ 为零当且仅当 Y 是 A 的列的线性组合，元素属于环 R——当且仅当存在元素属于 R 的列向量 X，使得 $Y=AX$.

证明 因为映射 π 是满射，故 R^m 的标准基元素的像生成 V. 它的核是 AR^n 的子模. 这个子模恰好由 A 的列的线性组合构成. ■

注 如果一个模 V 由集合 $\boldsymbol{B}=(v_1, \cdots, v_m)$ 生成，我们称使得 $\boldsymbol{B}Y=0$ 的 R^m 的元素 Y 为关系向量，或简称为生成元的一个关系. 我们也称方程 $v_1y_1+\cdots+v_my_m=0$ 为一个关系，意味着当在 V 中计算时，左边是 0. 一个关系的集合 S 是一个完全集当且仅当每个关系都是系数在环上的 S 的线性组合.

【14.5.2】**例** 带有关系的完全集

【14.5.3】
$$\begin{aligned} 3v_1+2v_2+v_3&=0\\ 8v_1+4v_2+2v_3&=0\\ 7v_1+6v_2+2v_3&=0\\ 9v_1+6v_2+v_3&=0 \end{aligned}$$

的三个元素 v_1，v_2，v_3 生成的 $\mathbf{Z}$-模或阿贝尔群 V 可用矩阵

【14.5.4】
$$A=\begin{bmatrix} 3 & 8 & 7 & 9\\ 2 & 4 & 6 & 6\\ 1 & 2 & 2 & 1 \end{bmatrix}$$

表示. 它的列是关系(14.5.3)的系数：

$$(v_1, v_2, v_3)A=(0,0,0,0)$$ ■

我们现在描述一种求 R-模 V 的表示的理论性的方法，这个方法很简单：选取 V 的生成元集合 $\boldsymbol{B}=(v_1, \cdots, v_m)$. 这些生成元态我们提供了一个满同态 $R^m \to V$，把列向量 Y 映射为线性组合 $\boldsymbol{B}Y=v_1y_1+\cdots+v_my_m$. 映射的核记为 W. 它是关系的模，它的元素是关系向量.

我们重复这个过程，选取 W 的生成元集合 $\boldsymbol{C}=(w_1, \cdots, w_n)$，且用这个生成元集合定义一个满射 $R^n \to W$. 但这里生成元 w_j 是 R^m 的元素. 它们是列向量. 我们把 w_j 的坐标向量 A_j 组成一个 $m \times n$ 矩阵

【14.5.5】
$$A=\begin{bmatrix} | & & | \\ A_1 & \cdots & A_m \\ | & & | \end{bmatrix}$$

424

则用 A 乘定义了一个映射

$$R^n \xrightarrow{A} R^m$$

映 $e_j \rightsquigarrow A_j = w_j$. 它是映射 $R^n \to W$ 与包含关系 $W \subset R^m$ 的合成. 根据其结构，W 是映射的像，用 AR^n 表示.

由于映射 $R^n \to V$ 是满射，因此第一同构定理告诉我们 V 同构于 $R^m/W = R^m/AR^n$. 因此模 V 由矩阵 A 表示. 这样模 V 的表现矩阵 A 如下确定：

【14.5.6】

- V 的一个生成元集；
- 关系的模的生成元集合 W.

除非生成元集构成 V 的一组基，此时 A 是空的，否则生成元的个数等于 A 的行数.

这个构造基于两个假设：一是模 V 具有有限生成元集. 这足够公平：我们不指望以这样的方式刻画太大的模，比如无限维向量空间. 二是假设关系的模 W 具有有限生成元集. 因为 W 是在构造过程中得到的一个辅助模，所以这样的假设有些出乎意料. 在下一节我们会仔细检验这一点(参见(14.6.5)). 除去这一点，我们可以讨论有限生成 R-模 V 的生成元和关系.

由于表现矩阵依赖于(14.5.6)的选取，因此许多矩阵表示同一个模，或同构的模. 下面是一些处理表现矩阵 A 的规则，这些规则并不改变它表示的模的同构类.

【14.5.7】**命题** 令 A 是模 V 的 $m \times n$ 表现矩阵. 下面的矩阵 A' 表示同一个模 V：

(i) $A' = Q^{-1}A$，$Q \in GL_m(R)$；

(ii) $A' = AP$，$P \in GL_n(R)$；

(iii) A' 通过删除一些零列得到；

(iv) A 的第 j 列为 e_i，A' 是 A 删除第 i 行第 j 列得到.

运算(iii)和(iv)也可以倒过来. 可以添加一个零列或者添加一个新行和列使 1 为其公共元素而其余元素为零.

证明 借助用矩阵 A 定义的映射 $R^n \xrightarrow{A} R^m$.

(i) A 到 $Q^{-1}A$ 的变换对应着 R^m 一个基的变换.

(ii) A 到 AP 的变换对应着 R^n 一个基的变换.

(iii) 一个零列对应着一个平凡关系，可以省略.

(iv) A 的等于 e_i 的列对应着关系 $v_i = 0$. 零元作为生成元是没用的，它的出现在任何关系中是无关的. 故我们可以从生成元集合和关系中删除 v_i. 这样做就把矩阵 A 中的第 i 行第 j 列删掉了. ■

425

用这些规则可以把矩阵 A 简化很多. 例如，我们原来的整数矩阵 A 的例子(14.5.4)可简化如下：

$$A = \begin{bmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{bmatrix} \to \begin{bmatrix} 0 & 2 & 1 & 6 \\ 0 & 0 & 2 & 4 \\ 1 & 2 & 2 & 1 \end{bmatrix} \to \begin{bmatrix} 2 & 1 & 6 \\ 0 & 2 & 4 \end{bmatrix} \to \begin{bmatrix} 2 & 1 & 6 \\ -4 & 0 & -8 \end{bmatrix}$$

$$\to[-4 \quad -8]\to[4 \quad 8]\to[4 \quad 0]\to[4].$$

因此 A 表示阿贝尔群 $\mathbf{Z}/4\mathbf{Z}$.

由定义，一个 $m\times n$ 矩阵表示一个由 m 个生成元和 n 个关系生成的模. 但是正如我们在前面的例子中看到的，数 m 和 n 依赖于生成元和关系的选取，它们不是由模唯一确定的.

另一个例子：2×1 矩阵 $\begin{bmatrix}4\\0\end{bmatrix}$ 表示由两个生成元 (v_1, v_2) 和一个关系 $4v_1=0$ 生成的阿贝尔群。我们不能化简这个矩阵. 它表示的阿贝尔群是一个 4 阶循环群和一个无限循环群的直和 $\mathbf{Z}/4\mathbf{Z}\oplus\mathbf{Z}$（参看本章第七节）. 另一方面，正如我们在前面的例子中看到的，矩阵 $[4 \quad 0]$ 表示具有一个生成元 v_1 和两个关系的阿贝尔群，第二个关系是平凡关系. 它是 4 阶循环群.

第六节 诺 特 环

这一节我们讨论关系的模的有限生成. 对于一个令人讨厌的环上的模，关系的模不必是有限生成的，虽然 V 是有限生成的. 幸运的是，在我们正在研究的环上并不出现这种情形，正如这里所证明的.

【14.6.1】命题 *在 R-模 V 上，下列条件是等价的：*

(i) V 的每个子模是有限生成的；

(ii) 升链条件：不存在 V 的子模的无限的严格升链：$W_1<W_2<\cdots$.

证明 假设 R-模 V 满足升链条件，令 W 是模 V 的子模. 我们用下面的方式选取 W 的生成元集合：如果 $W=0$，则 W 由空集合生成，否则，就从一个非零元 $w_1\in W$ 开始，并设 W_1 是 (w_1) 的张成. 如果 $W_1=W$，证毕. 否则，选取 w_2 是 W 中一个不属于 W_1 的元素，并令 W_2 是 (w_1, w_2) 的张成，则有 $W_1<W_2$. 如果 $W_2<W$，则选取 W 中不属于 W_2 的元素 w_3，等等. 用这种方式我们得到 W 的子模的一个严格升链 $W_1<W_2<\cdots$. 由于 V 满足升链条件，故子模链不会无限制地继续下去，因此某个 $W_k=W$，$(w_1, \cdots, w_k)$ 生成 W.

反过来的证明与命题 12.2.13（这个命题指出整环分解能终止当且仅当不存在主理想的严格升链）的证明类似. 假设 V 的每个子模是有限生成的，且设 $W_1\subset W_2\subset\cdots$ 是 V 的子模的一个无限弱升链，我们证明这个链不是严格增的. 令 U 是这些子模的并，则 U 是一个 V 的子模. 证明跟理想的证明是一样的(12.2.15). 故 U 是有限生成的. 令 $(u_1, \cdots, u_r)$ 是 U 元素的生成元集合，每个 u_v 属于某个子模 W_i，由于 $W_1\subset W_2\subset\cdots$ 是升链，故存在 W_i 包含 426
所有元素 $u_1, \cdots, u_r$. 则 W_i 包含由 $(u_1, \cdots, u_k)$ 生成的模 U：$U\subset W_i\subset W_{i+1}\subset U$. 这表明 $U=W_i=W_{i+1}=U$，故链不是严格升链. ■

【14.6.2】定义 *一个环 R 是诺特环如果它的每个理想都是有限生成的.*

【14.6.3】推论 *一个环 R 是诺特环当且仅当它满足升链条件：不存在环 R 的理想的无限严格升链 $I_1<I_2<\cdots$.*

主理想整环是诺特环是因为它的每个理想都是由一个生成元生成的. 故环 $\mathbf{Z}$, $\mathbf{Z}[i]$和域 F 上的多项式环 $F[x]$是诺特环.

【14.6.4】推论 令 R 是诺特环. R 的每个真理想 I 都包含在一个极大理想中.

证明 如果 I 不是极大理想，则它真包含在一个真理想 I_2 中，且如果 I_2 不是极大理想，则它包含在一个真理想 I_3 中，如此进行下去. 由升链条件(14.6.1)，链 $I<I_2<I_3<\cdots$一定是有限的. 因此某个 I_k 是极大理想. ■

诺特环的概念与子模的有限生成问题的关系由下面的定理表明.

【14.6.5】定理 令 R 是诺特环. 有限生成 R-模 V 的每个子模是有限生成的.

证明 情形 1：$V=R^m$. 我们对 m 用归纳法. R^1 的子模是 R 的理想(14.1.3). 由于 R 是诺特环，故定理对 $m=1$ 成立. 假设 $m>1$. 我们考虑投影映射：

$$\pi:R^m \to R^{m-1}$$

满足 $\pi(a_1, \cdots, a_m)=(a_1, \cdots, a_{m-1})$. 它的核为前 $m-1$ 个坐标为 0 的 R^m 中的向量的集合. 令 W 为 R^m 的子模，令 $\varphi:W\to R^{m-1}$ 是 π 在 W 上的限制. 像 $\varphi(W)$ 是 R^{m-1} 的子模. 由归纳法知像是有限生成的. 而且，$\ker\varphi=(W\cap\ker\pi)$ 是 $\ker\pi$ 的子模，$\ker\pi$ 同构于 R^1. 所以 $\ker\varphi$ 是有限生成的. 引理 14.6.6 表明 W 是有限生成的.

情形 2：一般情形. 令 V 是有限生成 R-模. 存在一个从自由模到 V 的满射 $\varphi:R^m\to V$. 给定 V 的子模 W，对应定理告诉我们 $U=\varphi^{-1}(W)$ 是模 R^m 的子模，故是有限生成的，且 $W=\varphi(U)$. 因此，W 是有限生成的(14.6.6(a)). ■

【14.6.6】引理 令 $\varphi:V\to V'$ 是一个 R-模的同态.

(a) 如果 V 是有限生成的且 φ 是满射，则 V' 是有限生成的.

427 (b) 如果 φ 的核和像是有限生成的，则 V 是有限生成的.

(c) 令 W 是 R-模 V 的子模. 如果 W 和 $\overline{V}=V/W$ 都是有限生成的，则 V 是有限生成的. 如果 V 是有限生成的，则 $\overline{V}$ 也是有限生成的.

证明

(a) 假设 φ 是满射，$(v_1, \cdots, v_n)$ 是 V 的生成元集，则集合 $(v_1', \cdots, v_n')$ 生成 V'，其中 $v_i'=\varphi(v_i)$.

(b) 我们按照线性变换(4.1.5)的维数公式的证明思路. 选取核的生成元集合 $(u_1, \cdots, u_k)$ 与像的生成元集合 $(v_1', \cdots, v_m')$. 再选取元素 $v_i\in V$ 使得 $\varphi(u_i)=v_i'$，我们证明集合 $(u_1, \cdots, u_k; v_1, \cdots, v_m)$ 是 V 的生成元. 令 v 是 V 的元素，则 $\varphi(v)$ 是 $(v_1', \cdots, v_m')$ 的线性组合，比如，$\varphi(v)=a_1v'_1+\cdots+a_mv'_m$. 令 $x=a_1v_1+\cdots+a_mv_m$. 则 $\varphi(x)=\varphi(v)$，因此 $v-x\in\ker\varphi$. 故 $v-x$ 是 $(u_1, \cdots, u_k)$ 的线性组合，比如 $v-x=b_1u_1+\cdots+b_ku_k$，且

$$v=a_1v_1+\cdots+a_mv_m+b_1u_1+\cdots+b_ku_k$$

由于 v 是任意的，故 $(u_1, \cdots, u_k; v_1, \cdots, v_m)$ 生成 V.

(c) 当 φ 换成典范映射 $\pi: V\to\overline{V}$，由(b)和(a)可得(c). ■

这就完成了定理 14.4.11 的证明.

由于主理想整环是诺特的，因此这些环上的有限生成模的子模也是有限生成的. 事实上，我们研究的大部分环是诺特的，这从希尔伯特的另一个定理得到.

【14.6.7】**定理**(希尔伯特基本定理) 假设 R 是诺特环，则多项式环 $R[x]$ 是诺特环.

这个定理的证明如下. 由归纳法可证明一个诺特环 R 上的多变量多项式环 $R[x_1, \cdots, x_n]$ 是诺特的. 因此环 $\mathbf{Z}[x_1, \cdots, x_n]$ 和域 F 上的多项式环 $F[x_1, \cdots, x_n]$ 是诺特环. 而且，诺特环的商环还是诺特的：

【14.6.8】**命题** 令 R 是诺特环，且 I 是 R 的理想. 则任何同构于商环 $\overline{R}=R/I$ 的环都是诺特的.

证明 令 $\overline{J}$ 是 $\overline{R}$ 的一个理想，令 $\pi: R\to\overline{R}$ 是典范映射. 令 $J=\pi^{-1}(\overline{J})$ 是相应的 R 中的理想. 由于 R 是诺特的，故 J 是有限生成的，由(14.6.6(a))得到 $\overline{J}$ 是有限生成的. ■

【14.6.9】**推论** 令 P 是整数或域上的有限个变量的多项式环. 任何同构于商环 P/I 的环 R 是诺特的.

现在我们回到希尔伯特基本定理的证明.

【14.6.10】**引理** 令 R 是一个环，令 I 是多项式环 $R[x]$ 的一个理想. 集合 A 是 I 中以非零多项式的首项系数和 R 的零元所成的集合，是 R 的一个理想，即首项系数的理想. 428

证明 我们必须证明如果 α，$\beta\in A$，则 $\alpha+\beta\in A$，$r\alpha\in A$. 如果 α，β，$\alpha+\beta$ 之一为 0，则 $\alpha+\beta\in A$，故我们假设这三者均不为零. 则 α 是 I 中某个多项式 f 的首项系数，β 是 I 中某个多项式 g 的首项系数. 用 x 的适当方幂乘以 f 或 g，使它们的次数相等，我们得到的多项式仍属于 I. 这两个多项式相加得到首相系数为 $\alpha+\beta$. 因为 I 是理想，故这两个多项式的和 $f+g$ 属于 I，因此 $\alpha+\beta\in A$. $r\alpha\in A$ 的证明类似. ■

希尔伯特基本定理的证明 设 R 是一个诺特环，I 是多项式环 $R[x]$ 的一个理想. 我们必须证明存在 I 的有限子集 S 生成 I，其中的子集为使得 I 的每个元素可以表示为其元素与多项式系数的线性组合.

令 A 是 I 的首项系数的理想. 由于 R 是一个诺特环，故 A 有有限生成元集合，例如，$(\alpha_1, \cdots, \alpha_k)$. 我们在 I 中选取多项式 f_i，其中 $i=1, \cdots, k$，其首项系数为 α_i. 必要时用 x 的适当方幂乘以 f_i，使得它们的次数相同，比如次数都是 n.

其次，令 P 表示由次数小于 n 的 $R[x]$ 的多项式再加上 0 所成的集合. 这是一个以 $(1, x, \cdots, x^{n-1})$ 为基的自由 R-模. 则子集 $P\cap I$ 是 P 的 R-子模，它是由 I 中次数小于 n 的多项式和零所组成的. 我们称这为子模 W. 由于 P 是有限生成 R-模且 R 是诺特的，故 W 是有限生成 R-模. 我们选取 W 的生成元为 $(h_1, \cdots, h_\ell)$. I 中每个次数小于 n 的多项式是系数属于 R 的 $(h_1, \cdots, h_\ell)$ 的线性组合.

我们证明集合 $(f_1, \cdots, f_k; h_1, \cdots, h_\ell)$ 生成理想 I. 我们对 g 的次数 d 使用数学归纳法.

情形 1：$d<n$. 在此情形，g 是 W 中的元素，它是系数属于 R 的 $(h_1, \cdots, h_\ell)$ 的线性组合. 在此不需要考虑多项式的系数.

情形 2：$d \geqslant n$. 令 β 是 g 的首项系数，故 $g=\beta x^d+$(次数较低的项). 则 β 是首项系数的理想 A 的一个元素，故 β 是 f_i 的首项系数 α_i 的线性组合：$\beta=r_1\alpha_1+\cdots+r_k\alpha_k$，$r_i \in R$. 多项式

$$q=\sum r_i x^{d-n} f_i$$

是属于由$(f_1, \cdots, f_k)$生成的理想. 如果 q 的次数为 d，首项系数为 β. 因此 $g-q$ 的次数小于 d. 由归纳法，$g-q$ 是$(f_1, \cdots, f_k; h_1, \cdots, h_\ell)$的多项式组合. 则 $g=q+(g-q)$也是这样的组合. ■

第七节 阿贝尔群的结构

阿贝尔群的结构定理(下面将给出)断言一个有限阿贝尔群 V 是循环群的直和. 证明工作已经完成. 我们知道存在一个 V 的对角表现矩阵，剩下要做的是对于群解释这个对角矩阵的意义.

429 模的直和的定义和向量空间的直和的定义是一样的.

注 令 $W_1, \cdots, W_k$ 是 R-模 V 的子模. 它们的和是它们生成的子模. 这个子模是由下面所示的和表示的：

【14.7.1】 $$W_1+\cdots+W_k=\{v \in V \mid v=w_1+\cdots+w_k, w_i \in W_i\}$$

我们说 V 是子模 $W_1, \cdots, W_k$ 的直和，记作 $V=W_1 \oplus \cdots \oplus W_k$，如果

【14.7.2】

- 它们生成：$V=W_1+\cdots+W_k$，且
- 它们是无关的，即如果 $w_1+\cdots+w_k=0$，$w_i \in W_i$，则对于所有 i，有 $w_i=0$.

因此，$V=W_1 \oplus \cdots \oplus W_k$，如果对于任何 $v \in V$，v 可以唯一地表示为 $v=w_1+\cdots+w_k$，其中 $w_i \in W_i$. 和向量空间的直和一样，一个模 V 是两个子模 W_1 和 W_2 的直和 $V=W_1 \oplus W_2$ 当且仅当 $V=W_1+W_2$ 且 $W_1 \cap W_2=0$(参见(3.6.6)).

同样的定义适用于阿贝尔群. 一个阿贝尔群 V 是其子群 $W_1, \cdots, W_k$ 的直和，即 $V=W_1 \oplus \cdots \oplus W_k$，如果：

- V 的每个元素可以写为和 $v=w_1+\cdots+w_k$，$w_i \in W_i$，即 $V=W_1+\cdots+W_k$，且
- 如果 $w_1+\cdots+w_k=0$，$w_i \in W_i$，则对于所有 i，有 $w_i=0$.

【14.7.3】定理(阿贝尔群的结构定理) 有限生成阿贝尔群 V 是循环子群 $C_{d_1}, \cdots, C_{d_k}$ 和一个自由阿贝尔群 L 的直和：

$$V=C_{d_1} \oplus \cdots \oplus C_{d_k} \oplus L$$

其中 d_i 是循环群 C_{d_i} 的阶，$d_i>1$，且 $d_i \mid d_{i+1}$，$i=1, \cdots, k-1$.

结构定理的证明 选取 V 的由一个生成元集合和一个关系的完全集确定的表现矩阵 A. 我们可以这样做是因为 V 是有限生成的并且 $\mathbf{Z}$ 是诺特环. 适当变换生成元和关系之后，可使矩阵 A 具有定理 14.4.6 中的对角矩阵形式. 我们可以消去对角线元素为 1 的元素和零列(参见(14.5.7))，矩阵 A 将有下面的形式：

【14.7.4】
$$A=\begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_k \\ \hline & 0 & \end{bmatrix}$$

其中 $d_1>1$，且 $d_1\mid d_2\mid\cdots\mid d_k$. 它是一个 $m\times k$ 矩阵，$0\leqslant k\leqslant m$. 对阿贝尔群而言，其意义是 V 由 m 个元素 $\boldsymbol{B}=(v_1,\cdots,v_m)$ 生成，而且

【14.7.5】
$$d_1v_1=0,\cdots,d_kv_k=0$$

构成这些生成元之间关系的完全集. 430

对于 $j=1,\cdots,m$，用 C_j 表示由 v_j 生成的循环子群. 对于 $j\leqslant k$，C_j 是阶为 d_j 的循环群，且对于 $j>k$，C_j 是无限循环群. 我们证明 V 是这些循环群的直和. 由于 $\boldsymbol{B}$ 生成 $V=C_1+\cdots+C_m$. 假设给定关系 $w_1+\cdots+w_m=0$，$w_j\in C_j$. 由于 v_j 生成 C_j，故对于某个整数 y_j，有 $w_j=v_jy_j$. 关系为 $\boldsymbol{B}Y=v_1y_1+\cdots+v_my_m=0$. 由于 A 的列形成关系的一个完全集，故对某个整向量 X，有 $Y=AX$，这意味着当 $j\leqslant k$ 时，y_j 是 d_j 的倍数；当 $j>k$ 时，$y_j=0$. 由于当 $j\leqslant k$ 时，$v_jd_j=0$，因此当 $j\leqslant k$ 时，$w_j=0$. 关系是平凡的，所以循环群 C_j 是独立的. 无限循环群 C_j，$j>k$ 的直和是一个自由阿贝尔群. ■

一个有限阿贝尔群是有限生成的，因而如上所述，结构定理将一个有限阿贝尔群分解为有限循环群的直和，其中一个直和分量的阶整除下一个的阶. 这时自由阿贝尔群的直和项为零.

有时将循环群进一步分解为素数幂阶循环群的直和更为方便. 这一分解基于命题 2.11.3：如果 a 和 b 是互素整数，则 ab 阶的循环群 C_{ab} 是 a 阶和 b 阶循环子群的直和 $C_a\oplus C_b$. 把这个命题和结构定理结合起来，就得到下面的结果：

【14.7.6】推论（结构定理的另一形式） *每一个有限生成阿贝尔群是素数幂阶循环群的直和.*

有限阿贝尔群分解的循环子群的阶是由群唯一确定的. 如果 V 的阶是不同素数的积，这没有问题. 例如，如果阶为 30，则 V 必同构于 $C_2\oplus C_3\oplus C_5$ 和 C_{30}. 但 $C_2\oplus C_2\oplus C_4$ 同构于 $C_4\oplus C_4$ 吗？通过比较 1 阶和 2 阶元素的个数不难证明这是不可能的. 群 $C_4\oplus C_4$ 含有 4 个这样的元素，而 $C_2\oplus C_2\oplus C_4$ 含有 8 个. 这种比较元素个数的方法总是很有效的.

【14.7.7】定理（结构定理的唯一性） *假设一个有限阿贝尔群 V 是素数幂阶 $d_j=p_j^{r_j}$ 循环群的直和，整数 d_j 由群 V 唯一确定.*

证明 令 p 是在 V 的直和分解中出现的素数之一，令 c_i 表示在 V 的直和分解中阶为 p^i 的循环群的个数，阶能整除 p^i 的元素集合形成 V 的一个子群，这个子群的阶为素数 p 的方幂，比如 p^{ℓ_i}. 令 k 是使得 $c_k>0$ 的最大指标. 则

$$\ell_1=c_1+c_2+c_3+\cdots+c_k$$
$$\ell_2=c_1+2c_2+2c_3+\cdots+2c_k,$$

$$\ell_3 = c_1 + 2c_2 + 3c_3 + \cdots + 3c_k$$
$$\cdots$$
$$\ell_k = c_1 + 2c_2 + 3c_3 + \cdots + kc_k.$$

431 指数 ℓ_i 确定整数 c_i. ■

整数 d_i 也是唯一确定的，如在定理 14.7.3 中所选取的，使得 $d_1 \mid \cdots \mid d_k$.

第八节 对线性算子的应用

阿贝尔群的分类和域 F 上单变量多项式环 $R=F[t]$ 的分类类似. 关于对角化整数矩阵的定理 14.4.6 进行下去，因为定理 14.4.6 的证明的关键成分(即除法算法)在 $F[t]$ 上也可用. 因为多项式环是诺特的，故任何有限生成 R-模 V 有一个表现矩阵(14.2.7).

【14.8.1】定理 令 $R=F[t]$ 是域 F 上单变量多项式环，且令 A 是一个 $m\times n$ R-矩阵. 存在初等 R-矩阵的积 Q 和 P. 使得 $A'=Q^{-1}AP$ 是对角的，A' 的每个非零对角线元素 d_i 是首一多项式，且 $d_1 \mid d_2 \mid \cdots \mid d_k$.

【14.8.2】例 多项式矩阵的对角化：

$$A=\begin{bmatrix} t^2-3t+1 & t-2 \\ (t-1)^3 & t^2-3t+2 \end{bmatrix} \xrightarrow{\text{row}} \begin{bmatrix} t^2-3t+1 & t-2 \\ t^2-t & 0 \end{bmatrix}$$
$$\xrightarrow{\text{col}} \begin{bmatrix} -1 & t-2 \\ t^2-t & 0 \end{bmatrix} \xrightarrow{\text{col}} \begin{bmatrix} -1 & 0 \\ t^2-t & t^3-3t^2+2t \end{bmatrix} \xrightarrow{\text{row}} \begin{bmatrix} 1 & 0 \\ 0 & t^3-3t^2+2t \end{bmatrix}$$

注意 对角形矩阵的左上角元素是 1 并不奇怪. 当矩阵元素的最大公约数为 1 时，这种情况就会发生. ■

与整数环上的一样，定理 14.8.1 提供给我们求方程组 $AX=B$ 的多项式解的方法，其中 A，B 的元素都是多项式矩阵(参看命题 14.4.9).

下面我们把结构定理推广到多项式环上. 为了把阿贝尔群的结构定理搬到多项式环上，我们定义循环 R-模 C(其中 R 是任一个环)是由一个元素 v 生成的模. 则存在一个满同态 $\varphi: R\to C$ 映 $r \rightsquigarrow rv$. φ 的核为关系的模，它是 R 的子模，是一个理想 I. 由第一同构定理，C 同构于 R-模 R/I.

当 $R=F[t]$ 时，理想 I 是主理想，且 C 同构于 $R/(d)$，系数 d 是某个多项式. 关系的模由单个元素生成.

【14.8.3】定理(多项式环上模的结构定理) 令 $R=F[t]$ 是系数属于域 F 的单变量多项式环.

(a) 令 V 是 R 上有限生成模. 则 V 是循环模 C_1，…，C_k 和一个自由模 L 的直和，其中 C_i 同构于 $R/(d_i)$，d_1，…，d_k 是正次数的首一多项式，且 $d_1 \mid \cdots \mid d_k$.

432 (b) 如(a)的断言，只是条件 $d_i \mid d_{i+1}$ 换成每个 d_i 是一个首一的既约多项式的幂.

(b)中的素数幂是唯一的，但此处不费时间证明了.

例如，令 $R=\mathbf{R}[t]$，例 14.8.2 中 R-模 V 用矩阵 A 表示．这个模也可以由对角矩阵

$$A'=\begin{bmatrix}1 & 0\\ 0 & t^3-3t^2+2t\end{bmatrix}$$

表示，且我们可以去掉矩阵(14.5.7)的第一行和第一列．故 V 由一个 1×1 矩阵$[g]$表示，其中 $g(t)=t^3-3t^2+2t=t(t-1)(t-2)$．这意味着 V 是一个循环模，它同构于 $C=R/(g)$．由于 g 有三个互素因子，因此 V 可进一步分解．它同构于循环 R-模的直和：

【14.8.4】 $$R/(g)\approx(R/(t))\oplus(R/(t-1))\oplus(R/(t-2))$$

现在来应用在域上向量空间上发展起来的线性算子理论．这个应用提供了如何从抽象到一个新视野的典范．由阿贝尔群发展的方法形式地推广到多项式环上的模上，然后应用到具体的新情况中．历史进程并不是这样的．阿贝尔群和线性算子的理论是各自独立发展起来的，后来才联系起来．但令人惊讶的是这两种情形(阿贝尔群和线性算子)可以在形式上相似而当同样的理论在它们之上应用时最终产生看起来是如此不同的结果．

我们能够着手进行讨论的一个关键事实是如果给定域 F 上向量空间的一个线性算子

【14.8.5】 $$T:V\to V$$

则可以用这个算子将 V 构造成多项式环 $F[t]$上的一个模．为此，需要定义一个多项式 $f(t)=a_nt^n+\cdots+a_1t+a_0$ 与向量 v 的乘法．令

【14.8.6】 $$f(t)v=a_nT^n(v)+a_{n-1}T^{n-1}(v)+\cdots+a_1T(v)+a_0v$$

右边可以记为$[f(T)](v)$，其中 $f(T)$表示线性算子 $a_nT^n+\cdots+a_1T+a_0I$．(加上括号只是为了清楚说明算子 $f(T)$作用在 v 上.)用这个记号得到公式

【14.8.7】 $$tv=T(v),\quad f(t)v=[f(T)](v)$$

规则(14.8.6)使 V 成为一个 $F[t]$-模这个事实是容易验证的．公式(14.8.7)看起来没有什么特别的地方．它们产生了为什么需要一个新符号 t 的问题．但要记住 $f(t)$是多项式而 $f(T)$表示的是某个线性算子．

反之，如果 V 是一个 $F[t]$-模，则 V 的元素由多项式 $f(t)$来作标量乘法是有定义的．特别是我们得到一个常数多项式 $f(T)$(即 F 中元素)的乘法的法则．如果保持常数乘法法则而暂时忘 433
掉非常数多项式的乘法 $f(T)$，则关于模的公理表明 V 成为 F 上的一个向量空间(14.1.1)．其次，可以用多项式 t 乘 V 的元素．将 t 在 V 上的乘法作用表示为 T．则 T 是映射

【14.8.8】 $$V\xrightarrow{T}V,\quad \text{定义为}\quad T(v)=tv$$

当将 V 视为 F 上的向量空间时，这个映射是一个线性算子．因为由分配律，$t(v+v')=tv+tv'$，因此 $T(v+v')=T(v)+T(v')$．如果 c 是一个标量，则 $tcv=ctv$；因此 $T(cv)=cT(v)$．因而一个 $F[t]$-模 V 给出向量空间上的一个线性算子．我们所描述的规则(从线性算子到模及其反过来)是互逆的：

【14.8.9】 F- 向量空间上的线性算子与 $F[t]$- 模是等价概念

我们将把这个事实应用于有限维向量空间，但顺便注意一下对应于秩为 1 的自由 $F[t]$-模的线性算子. 当 $F[t]$作为 F 上向量空间时，单项式$(1, t, t^2, \cdots)$形成一组基，我们用这组基把 $F[t]$等同于无限维 F-向量空间 Z：

$$Z = \{(a_0, a_1, \cdots,) \mid a_i \in F \text{ 并且仅有有限个 } a_i \text{ 非零}\} \quad (3.7.2)$$

在 $F[t]$上用 t 乘对应于移位算子 T：

$$(a_0, a_1, a_2, \cdots) \rightsquigarrow (0, a_0, a_1, a_2, \cdots)$$

空间 Z 上的移位算子对应于秩为 1 的自由 $F[t]$-模.

现在我们开始应用于线性算子. 给定 F 上向量空间 V 的线性算子 T，可以将 V 也视为 $F[t]$-模. 假设 V 作为向量空间是有限维的，比如设为 n 维. 则它作为模是有限生成的，因此它有表现矩阵. 因为有两个矩阵可用，这里有搞混淆的危险：两个矩阵为模 V 的表现矩阵和线性算子 T 的矩阵. 表现矩阵是元素为多项式的 $r \times s$ 矩阵，其中 r 是模的选定的生成元的个数，而 s 是关系的个数. 另一方面，线性算子的矩阵是 $n \times n$ 标量矩阵，其中 n 是 V 作为向量空间的维数. 两个矩阵都含有描述模和线性算子所必需的信息.

视 V 为 $F[t]$-模，可以应用定理 14.8.3 得到 V 是循环子模的直和的结论，设

$$V = W_1 \oplus \cdots \oplus W_k$$

其中 W_i 同构于 $F[t]/(f_i)$，f_i 是 $F[t]$中首一多项式. 当 V 是有限维时，自由直和项为零.

要对线性算子 T 解释直和分解的意义，我们选取空间 W_i 的一组基 $\boldsymbol{B}_i$. 则关于这组基 $\boldsymbol{B}=(\boldsymbol{B}_1, \cdots, \boldsymbol{B}_k)$，$T$ 的矩阵是一个分块矩阵(4.4.4)，其中矩阵块是 T 限制在不变子空间 W_i 上的矩阵. 或许只需检验算子对应着循环模即可.

434

令 W 是一个循环 $F[t]$-模，设由单个元素 w_0 生成. 由于 $F[t]$的每个理想都是主理想，故 W 同构于 $F[t]/(f)$，其中 $f(t)=t^n+a_{n-1}t^{n-1}+\cdots+a_1t+a_0$ 是 $F[t]$中首一多项式. 同构 $F[t]/(f) \to W$ 把 1 映射为 w_0. 集合$(1, t, \cdots, t^{n-1})$是 $F[t]/(f)$的一组基(11.5.5)，故集合$(w_0, tw_0, \cdots, t^{n-1}w_0)$是 W 作为向量空间的一组基.

对应的线性算子 $T: W \to W$ 的作用是用 t 乘. 用 T 来表示 W 的一组基为$(w_0, w_1, \cdots, w_{n-1})$，其中 $w_j = T^j w_0$. 则

$$\begin{aligned} T(w_0) &= w_1, T(w_1) = w_2, \cdots, T(w_{n-2}) = w_{n-1} \\ [f(T)]w_0 &= T^n w_0 + a_{n-1}T^{n-1}w_0 + \cdots + a_1 T w_0 + a_0 w_0 = 0 \\ &= T w_{n-1} + a_{n-1}w_{n-1} + \cdots + a_1 w_1 + a_0 w_0 = 0 \end{aligned}$$

这确定了 T 的矩阵. 对不同的 n 值的表示如下：

【14.8.10】
$$[-a_0], \begin{bmatrix} 0 & -a_0 \\ 1 & -a_1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{bmatrix}, \cdots$$

这个矩阵的特征多项式是 $f(t)$.

【14.8.11】定理 令 T 是域 F 上有限维向量空间 V 上的一个线性算子. 则存在 V 的一组基

使得在这组基下 T 的矩阵为上面形式的矩阵块.

线性算子矩阵的这样一个形式称为一个有理典范型. 这是对任何域都可以得到的最好的形式.

【14.8.12】例 令 $F=\mathbf{R}$. 下面所示矩阵 A 是有理典范型的. 它的特征多项式是 t^3-1. 由于这是互素多项式之积: $t^3-1=(t-1)(t^2+t+1)$, 因此它所表示的循环 $\mathbf{R}[t]$-模是循环模的直和. 矩阵 A' 是另一个有理典范型矩阵, 它刻画了同一个模. 在复数域上, A 是可以对角化的. 它的对角形矩阵为 A'', 其中 $\omega=e^{2\pi i/3}$.

【14.8.13】
$$A=\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix},\quad A'=\left[\begin{array}{c|cc}1&&\\\hline &0&-1\\&1&-1\end{array}\right],\quad A''=\begin{bmatrix}1&&\\&\omega&\\&&\omega^2\end{bmatrix}$$ ■

$F[t]$-模与对应的线性算子的性质之间的各种联系总结如下表:

【14.8.14】

$F[t]$-模	线性算子 T
用 t 乘	T 的作用
秩为 1 的自由模	移位算子
子模	T-不变子空间
子模的直和	T-不变子空间的直和
由 w 生成的循环模	由 w, Tw, T^2w, …张成的子空间

435

第九节 多变量多项式环

随着环变得越来越复杂, 环上的模也越来越复杂了, 确定一个明确表示出来的模是否是自由的就困难了. 本节我们不加证明地描述刻画多变量多项式环上自由模的定理. 这个定理是在 1976 年由奎伦(Quillen)和苏斯林(Suslin)证明的.

设 $R=\mathbf{C}[x_1, \cdots, x_k]$ 是 k 个变量的多项式环, 并设 V 是有限生成的 R-模. 我们选定模 V 的一个表现矩阵 A, A 的元素是多项式 $a_{ij}(x)$, 且如果 A 是 $m\times n$ 矩阵, 则 V 同构于 A 在 R-向量上乘法变换的余核 R^m/AR^n.

当计算矩阵元素 $a_{ij}(x)$ 在 $\mathbf{C}^k$ 上任意点 $(c_1, \cdots, c_k)$ 的值后, 我们得到了一个复矩阵 $A(c)$, 其第 i 行第 j 列元素为 $a_{ij}(c)$.

【14.9.1】定理 *设 V 是多项式环 $\mathbf{C}[x_1, \cdots, x_k]$ 上的有限生成模, 并设 A 是 V 的一个 $m\times n$ 表现矩阵. 用 $A(c)$ 表示 A 在点 $c\in\mathbf{C}^k$ 的取值. 则 V 是秩为 r 的自由模当且仅当矩阵 $A(c)$ 在每一点 c 的秩为 $m-r$.*

定理的证明所需要的太多背景要在这里给出. 然而, 可以用它来确定一个给定的模是否自由. 例如, 设 V 是由 4×2 矩阵

【14.9.2】
$$A=\begin{bmatrix}1&x\\y&x+3\\x&y\\x^2&y^2\end{bmatrix}$$

表示的 $\mathbf{C}[x, y]$上的模，故 V 有四个生成元(比如 v_1，v_2，v_3，v_4)和两个关系：

$$v_1 + yv_2 + xv_3 + x^2v_4 = 0, \quad xv_1 + (x+3)v_2 + yv_3 + y^2v_4 = 0$$

不难证明在每个点 $c \in \mathbf{C}^2$ 上 $A(c)$的秩为 2，定理 14.9.1 告诉我们 V 是秩为 2 的自由模.

考虑由矩阵 $A(c)$的列张成的向量空间 $W(c)$可以得到对这个定理的一个直观的理解. 它是 $\mathbf{C}^m$ 的子空间. 当 c 在空间 $\mathbf{C}^k$ 中变化时，矩阵 $A(c)$连续变换. 因此假若子空间 $W(c)$的维数不跳跃的话，$W(c)$的点也将连续变化. 由一个拓扑空间 $\mathbf{C}^k$ 参数化的固定维数的向量空间的连续簇称为向量丛. 模 V 是自由的当且仅当向量空间簇 $W(c)$形成一个向量丛.

我认为对数学家来说通常的变形过于保守.

436

——Jean-Louis Verdier

练　习

第一节　模

1.1 设 R 是一个环，令 V 表示 R-模 R，确定所有模同态 $\varphi: V \to V$.

1.2 令 V 是一个阿贝尔群. 证明如果 V 有一个带有加法合成法则的 $\mathbf{Q}$-模结构，则这个结构是唯一确定的.

1.3 令 $R = \mathbf{Z}[\alpha]$是由代数整数 α 在 $\mathbf{Z}$ 上生成的环. 证明对于任意整数 m，R/mR 是有限的，并确定其阶.

1.4 一个模叫做单模如果它不是零模且不含有真子模.

(a) 证明任意单 R-模同构于形如 R/M 的 R-模，其中 M 是 R 的一个极大理想.

(b) 证明舒尔引理：令 $\varphi: S \to S'$是单模同态. 则 φ 或是零同态或是同构.

第二节　自由模

2.1 令 $R = \mathbf{C}[x, y]$，且令 M 是 R 的由两个元素 x，y 生成的理想. 问 M 是自由 R-模吗?

2.2 证明一个环 R 如果具有性质：每个有限生成 R-模都是自由的. 则这个环 R 是零环或是域.

2.3 令 A 是自由 $\mathbf{Z}$-模同态 $\varphi: \mathbf{Z}^n \to \mathbf{Z}^m$ 的矩阵.

(a) 证明 φ 是单射当且仅当 A 作为实矩阵其秩为 n.

(b) 证明 φ 是满射当且仅当 A 的 $m \times m$ 子式的最大公约数是 1.

2.4 令 I 是环 R 的一个理想.

(a) 在什么情况下 I 是自由 R-模?

(b) 在什么情况下商环 R/I 是自由 R-模?

第三节　恒等式

3.1 令 $\tilde{f}$表示 $\mathbf{C}^n$ 上的函数，其定义为(形式)复多项式 $f(x_1, \cdots, x_n)$的值，证明若 $\tilde{f}$是零函数，则 f 是零多项式.

3.2 在某种情况下，只对实数验证恒等式成立会是方便的，这样足够吗?

3.3 令 A 和 B 分别是 $m \times m$ 和 $n \times n$ 的 R-矩阵. 用恒等式的不变性原理证明 $R^{m \times n}$ 空间上的线性算子 $f(M) = AMB$的迹等于 $\operatorname{trace}(A) \cdot \operatorname{trace}(B)$.

3.4 在每一种情形，确定恒等式的不变性是否能从复数推广到任意的交换环上.

(a) 矩阵乘法的结合律

(b) 凯莱-哈密顿定理 437

(c) 克莱姆法则

(d) 多项式的乘法法则、除法法则和链式求导法则

(e) n 次多项式至多有 n 个根

(f) 多项式的泰勒展开式

第四节 整数矩阵的对角化

4.1 (a) 通过整数行和列变换化简下列每个矩阵为对角形矩阵.

$$\begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix}, \quad \begin{bmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \end{bmatrix}, \quad \begin{bmatrix} 3 & 1 & -4 \\ 2 & -3 & 1 \\ -4 & 6 & -2 \end{bmatrix}$$

(b) 对于第一个矩阵，令 $V=\mathbf{Z}^2$，且 $L=AV$，画出子格 L，并求 V 和 L 的展示对角化的基.

(c) 确定对角化第二个矩阵的整数矩阵 Q^{-1} 和 P.

4.2 令 d_1，d_2，…是定理 14.4.6 中的整数. 证明 d_1 是矩阵 A 的元素 a_{ij} 的最大公约数.

4.3 当 $A=\begin{bmatrix} 4 & 7 & 2 \\ 2 & 4 & 6 \end{bmatrix}$ 时，确定方程组 $AX=0$ 的全部整数解. 求使得方程组 $AX=B$ 有解的整列向量 B 所成的空间的一组基.

4.4 求方程组 $x+2y+3z=0$，$x+4y+9z=0$ 的整数解的 $\mathbf{Z}$-模的一组基.

4.5 令 α，β，γ 是复数. 在什么条件下整数的线性组合的集合 $\{\ell\alpha+m\beta+n\gamma \mid \ell, m, n\in\mathbf{Z}\}$ 是复平面的一个格?

4.6 令 $\varphi:\mathbf{Z}^k\to\mathbf{Z}^k$ 是用整数矩阵 A 乘给定的同态. 证明 φ 的像的指标是有限的当且仅当 A 是非奇异的，且如果这样的话，φ 的像的指标等于 $|\det A|$.

4.7 令 $A=(a_1, \cdots, a_n)^t$ 是整的列向量，且 d 是 a_1，…，a_n 的最大公约数. 证明存在矩阵 $P\in GL_n(\mathbf{Z})$ 使得 $PA=(d, 0, \cdots, 0)^t$.

4.8 用高斯整数环 $\mathbf{Z}[i]$ 上的行和列的可逆变换将矩阵 $\begin{bmatrix} 3 & 2+i \\ 2-i & 9 \end{bmatrix}$ 对角化.

4.9 用对角化证明如果 $L\subset M$ 是格，则 $[M:L]=\dfrac{\Delta(L)}{\Delta(M)}$.

第五节 生成元和关系

5.1 令 $R=\mathbf{Z}[\delta]$，其中 $\delta=\sqrt{-5}$，确定理想 $(2, 1+\delta)$ 作为 R-模的一个表现矩阵.

5.2 确定表现矩阵 $\begin{bmatrix} 3 & 1 & 2 \\ 1 & 1 & 1 \\ 2 & 3 & 6 \end{bmatrix}$ 的阿贝尔群. 438

第六节 诺特环

6.1 令 $V\subset\mathbf{C}^n$ 是多项式 f_1，f_2，f_3，…的无限集合的共同零点的轨迹. 证明存在多项式的一个有限子集使得它们的零点是同样的轨迹.

6.2 找一个环 R 的例子，R 的理想 I 不是有限生成的.

第七节 阿贝尔群的结构

7.1 求循环群的一个直和使得它同构于表现矩阵 $\begin{bmatrix}2&2&2\\2&2&0\\2&0&2\end{bmatrix}$ 所确定的阿贝尔群.

7.2 将具有关系 $3x+4y=0$ 的 x，y 生成的阿贝尔群表示为循环群的直和.

7.3 当 V 是由 x，y，z 生成的阿贝尔群且分别满足下列关系时，求出其同构的循环群的直积.

(a) $3x+2y+8z=0$，$2x+4z=0$

(b) $x+y=0$，$2x=0$，$4x+2z=0$，$4x+2y+2z=0$

(c) $2x+y=0$，$x-y+3z=0$

(d) $7x+5y+2z=0$，$3x+3y=0$，$13x+11y+2z=0$

7.4 在每一种情形，确定给定的表现矩阵的阿贝尔群：

$$\begin{bmatrix}2\\1\end{bmatrix},\begin{bmatrix}0\\5\end{bmatrix},\begin{bmatrix}2&0&0\end{bmatrix},\begin{bmatrix}1&0\\0&1\\0&0\end{bmatrix},\begin{bmatrix}2&3\\1&2\end{bmatrix},\begin{bmatrix}2&4\\1&4\end{bmatrix},\begin{bmatrix}2&4\\6&4\end{bmatrix},\begin{bmatrix}4&6\\2&3\end{bmatrix}$$

7.5 确定 400 阶阿贝尔群的同构类的个数.

7.6 (a) 令 a 和 b 为互素的正整数. 通过对对角线元素为 a，b 的对角矩阵的运算，证明循环群 C_{ab} 同构于积 $C_a \oplus C_b$.

(b) 如果去掉 a，b 是互素的这个假设，会得到什么结论?

7.7 令 $R=\mathbf{Z}[\mathrm{i}]$ 且 V 是具有关系 $(1+\mathrm{i})v_1+(2-\mathrm{i})v_2=0$，$3v_1+5\mathrm{i}v_2=0$ 的元素 v_1，v_2 生成的 R-模. 将这个模表示为循环模的直和.

7.8 令 $F=\mathbf{F}_p$. 对怎样的素整数 p，加群 F^1 有 $\mathbf{Z}[\mathrm{i}]$-模的结构? 对于 F^2 结果怎样?

7.9 证明下列概念是等价的：

- R-模，其中 $R=\mathbf{Z}[\mathrm{i}]$；
- 阿贝尔群 V，具有同态 $\varphi: V\to V$ 使得 $\varphi\circ\varphi=-$恒等式.

第八节 对线性算子的应用

439 8.1 令 T 是 $\mathbf{C}^2$ 上的线性算子，其矩阵为 $\begin{bmatrix}2&1\\0&1\end{bmatrix}$. 其对应的 $\mathbf{C}[t]$-模是循环模吗?

8.2 令 M 是一个形如 $\mathbf{C}[t]/(t-a)^n$ 的 $\mathbf{C}[t]$-模. 证明对 M 存在 $\mathbf{C}$-基，使得对应于线性算子的矩阵是一个若尔当块.

8.3 令 $R=F[x]$ 是域 F 上单变量多项式环，令 V 是由满足关系 $(t^3+3t+2)v=0$ 的元素 v 生成的 R-模. 选取 V 的作为 F-向量空间的一组基，确定关于这组基用 t 乘的算子的矩阵.

8.4 令 V 是一个 $F[t]$-模，令 $\boldsymbol{B}=(v_1,\cdots,v_n)$ 是 F-向量空间的 V 的一组基，令 B 是在这组基下的 T 的矩阵. 证明 $A=tI-B$ 是此模的表现矩阵.

8.5 证明矩阵(14.8.10)的特征多项式是 $f(t)$.

8.6 对环 $\mathbf{C}[\varepsilon]$(其中 $\varepsilon^2=0$)上的有限生成模进行分类.

第九节 多变量多项式环

9.1 确定在 $\mathbf{C}[x,y]$ 上由下列矩阵表现的模是否是自由的.

(a) $\begin{bmatrix} x^2+1 & x \\ x^2y+x+y & xy+1 \end{bmatrix}$ (b) $\begin{bmatrix} xy-1 \\ x^2-y^2 \\ y \end{bmatrix}$ (c) $\begin{bmatrix} x-1 & x \\ y & y+1 \\ x & y \\ x^2 & 2y \end{bmatrix}$

9.2 通过写出一个基证明由(14.9.2)表现的模是自由的.

9.3 按单变量多项式环的模型，用带有附加结构的复向量空间的语言描述环 $\mathbf{C}[x, y]$上的模.

9.4 证明奎伦-苏斯林定理较容易的那一半：如果 V 自由，则 $A(c)$的秩为常数.

9.5 令 $R=\mathbf{Z}[\sqrt{-5}]$，令 V 是由矩阵 $A=\begin{bmatrix} 2 \\ 1+\delta \end{bmatrix}$表现的模. 证明对于每个 R 的素理想 P，A 在 R/P 上的剩余的秩为 1，但 V 不是自由模.

杂题

M.1 有多少种方法把 $\mathbf{Z}/5\mathbf{Z}$ 看成是高斯整数上的模结构?

M.2 对环 $\mathbf{Z}/(6)$上的有限生成模进行分类.

M.3 令 A 是一个有限阿贝尔群，且令 $\varphi: A \to \mathbf{C}^\times$ 是一个非平凡同态. 证明 $\sum_{a\in A}\varphi(a)=0$.

M.4 当一个 2×2 整矩阵 A 被 $Q^{-1}AP$ 对角化时，矩阵 P 和 Q 怎样才是唯一的?

M.5 在 $GL_2(\mathbf{R})$中那个矩阵 A 使得 $\mathbf{R}^2$ 上的格 L 是稳定的? 440

M.6 (a) 刻画在 2×2 整矩阵空间上用 $G=GL_2(\mathbf{Z})$右乘的轨道.

(b) 证明对于任意整矩阵 A，存在一个可逆整矩阵 P 使得 AP 有下面的哈密顿正规型：

$$\begin{bmatrix} d_1 & 0 & 0 & 0 & \cdots \\ a_2 & d_2 & 0 & 0 & \\ a_3 & b_3 & d_3 & 0 & \\ \vdots & & & & \ddots \end{bmatrix}$$

其中矩阵元素是非负的，$a_2<d_2$，a_3，$b_3<d_3$，等等.

M.7 令 S 是多项式环 $R=\mathbf{C}[t]$的包含 $\mathbf{C}$ 但不等于 $\mathbf{C}$ 的一个子环. 证明 R 是有限生成 S-模.

*M.8 (a) 令 α 是一个复数，令 $\mathbf{Z}[\alpha]$是由 α 生成的 $\mathbf{C}$ 的子环. 证明 α 是代数整数当且仅当 $\mathbf{Z}[\alpha]$是有限生成阿贝尔群.

(b) 证明：如果 α 和 β 是代数整数，则由 α 和 β 生成的 $\mathbf{C}$ 的子环 $\mathbf{Z}[\alpha, \beta]$是有限生成阿贝尔群.

(c) 证明代数整数形成 $\mathbf{C}$ 的子环.

*M.9 考虑欧几里得空间 $\mathbf{R}^k$，带有点积$(v\cdot w)$. L 是 V 中一个格，定义为包含 k 个无关向量的 V^+ 的离散子群. 如果 L 是一个格，定义 $L^*=\{w \mid (v\cdot w)\in\mathbf{Z},\ v\in L\}$.

(a) 证明 L 有一个格基为 $\boldsymbol{B}=(v_1, \cdots, v_k)$，$k$ 个向量张成 L 作为 $\mathbf{Z}$-模.

(b) 证明 L^* 是一个格. 刻画如何用 $\boldsymbol{B}=(v_1, \cdots, v_k)$来确定 L^* 的格基.

(c) 在什么条件下 L 是 L^* 的子格?

(d) 假设 $L\subset L^*$. 求指标$[L^*:L]$的公式.

*M.10 (a) 证明有理数的乘法群 $\mathbf{Q}^\times$ 同构于一个 2 阶循环群和一个有可数多个生成元的自由阿贝尔群的直和.

(b) 证明有理数的加群 $\mathbf{Q}^+$ 不是两个真子群的直和.

(c) 证明商群 $\mathbf{Q}^+/\mathbf{Z}^+$ 不是循环群的直和. 441

第十五章　域

我们的困难不在于证明，
而在于学习证明什么.

——*Emil Artin*

第一节　域的例子

大部分域理论与其中一个包含在另一个之中的一对域 $F \subset K$ 有关. 对于给定的这一对域，将 K 称为 F 的域扩张，或一个扩域. 记号 K/F 表示 K 是 F 的扩域.

下面是三个最重要的域类.

数域

数域 K 是 $\mathbf{C}$ 的一个子域.

$\mathbf{C}$ 的任意子域包含有理数域 $\mathbf{Q}$，因而一个数域是 $\mathbf{Q}$ 的扩域. 最常用到的数域是其所有元素都是代数数的代数数域. 我们在第十三章学习了二次数域.

有限域

有有限多个元素的域称为一个有限域.

一个有限域包含一个素域 $\mathbf{F}_p$，因此一个有限域是某个素域的扩张. 有限域将在本章第七节讨论.

函数域

有理函数域 $F=\mathbf{C}(t)$ 的扩张称为函数域.

函数域可以由一个方程 $f(t, x)=0$ 来定义，其中 $f(t, x)$ 是两个变量 t 和 x 的既约复多项式，例如 $f(t, x)=x^2-t^3+t$. 我们可以用方程 $f(t, x)=0$ 来定义 x 为关于 t 的“隐”函数 $x(t)$，就像在微积分中学过的一样. 在我们的例子中，函数是 $x=\sqrt{t^3-t}$. 相应的函数域 K 由组合 $p+q\sqrt{t^3-t}$ 构成，其中 p 和 q 是关于 t 的有理函数. 在这个域上的做法就和在域 $\mathbf{Q}(\sqrt{-5})$ 上一样. 对于多数多项式 $f(t, x)$，没有对于隐函数 $x(t)$ 的明显的表达式但由定义，它满足方程 $f(t, x(t))=0$. 在本章第九节我们将看到 $x(t)$ 定义了 F 的一个扩域.

442

第二节　代数元与超越元

设 K 是域 F 的一个扩域，并设 α 是 K 的元素. 与代数数的定义(第十一章第一节)类似，

元素 α 称为在 F 上的代数元，如果 α 是一个系数属于 F 的某个首一多项式的根，比如

【15.2.1】 $$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\text{其中 } a_i\in F$$

且 $f(\alpha)=0$. 一个元素在 F 上是超越的，如果它不是 F 上的代数元，即它不是任意这样的多项式的根.

代数的和超越的这两个性质依赖于给定的域 F. 复数 $2\pi i$ 在实数域上是代数的，但在有理数域上是超越的. 而且一个域 K 中的每个元素 α 在 K 上是代数的，因为它是多项式 $(x-\alpha)$ 的根，其系数属于 K.

元素 α 的这两种可能性可以用代入同态

【15.2.2】 $$\varphi:F[x]\to K,\quad \text{由 } x\rightsquigarrow\alpha \text{ 定义}$$

描述. 如果 φ 是单射，则元素 α 在 F 上是超越的，而在其他情形，即如果 φ 的核不等于零，则它在 F 上是代数的. 对于 α 在 F 上是超越的情形没有太多的要说.

假设 α 在 F 上是代数的. 由于 $F[x]$ 是主理想整环，因此 $\ker\varphi$ 是一个主理想，它由一个首一的系数属于 F 的多项式 $f(x)$ 生成. 有多种方式来描述这个多项式.

【15.2.3】**命题** 令 α 是域 F 的扩域 K 中的元素，且为 F 上的代数元. 关于系数属于 F 的首一多项式 f 的下列条件是等价的. 满足这些条件的唯一的首一多项式叫做 α 在 F 上的既约多项式.

- f 是 $F[x]$ 上首一的次数最低的以 α 为根的多项式.
- f 是 $F[x]$ 上的既约多项式，α 为多项式 f 的根.
- f 的系数属于 F，α 为多项式 f 的根，f 生成的 $F[x]$ 的主理想是一个极大理想.
- α 为多项式 f 的根，如果 g 是任何以 α 为根的 $F[x]$ 中的多项式，则 f 整除 g.

F 上关于 α 的既约多项式 f 的次数叫做 α 在 F 上的次数.

重要的是要注意这个既约(即不可约)多项式 f 既依赖于 F 也依赖于 α，因为一个多项式的 443
既约性依赖于域. 例如，$\sqrt{i}$ 在有理数域 $\mathbf{Q}$ 上的既约多项式为 x^4+1，但这个多项式在域 $\mathbf{Q}(i)$ 上能因子分解. $\sqrt{i}$ 在有理数域 $\mathbf{Q}(i)$ 上的既约多项式为 x^2-i. 当有几个域的时候，必须仔细搞清楚所说的是哪个域，说一个多项式既约是模糊的. 最好说 f 在 F 既约，或它是 $F[x]$ 的既约元.

设 K 是域 F 的一个扩域，并设 α 是 K 的元素. 由 α 生成的 K 的子域用 $F(\alpha)$ 表示：

【15.2.4】 $$F(\alpha)\text{ 是 } K \text{ 的包含 } F \text{ 和 } \alpha \text{ 的最小的域}$$

类似地，如果 $\alpha_1,\cdots,\alpha_k$ 是 F 的一个扩域 K 中的元素，则记号 $F(\alpha_1,\cdots,\alpha_k)$ 将表示 K 中包含这些元素和 F 的最小的子域.

如在第十一章里一样，我们把由 α 在 F 上生成的环记作 $F(\alpha)$. 如上面所定义的，它是映射 $\varphi:F[x]\to K$ 的像，它由 K 中所有可以写成系数属于 F 的 α 的多项式的元素 β 组成：

【15.2.5】 $$\beta=b_n\alpha^n+\cdots+b_1\alpha+b_0,\text{其中 } b_i\in F$$

域 $F(\alpha)$ 与 $F[\alpha]$ 的分式域同构. 其元素是形如(15.2.5)的元素的比(见第十一章第七节).

类似地，如果 $\alpha_1,\cdots,\alpha_k$ 是 F 的一个扩域 K 中的元素，则包含元素 $\alpha_1,\cdots,\alpha_n$ 和 F

的 K 的最小子环记为 $F[\alpha_1, \cdots, \alpha_k]$. 它是由 K 的系数属于 F 的关于 $\alpha_1, \cdots, \alpha_k$ 的多项式 β 组成. 域 $F(\alpha_1, \cdots, \alpha_k)$ 是环 $F[\alpha_1, \cdots, \alpha_k]$ 的分式域.

如果元素 α 在 F 上是超越的，则映射 $F[x] \to F[\alpha]$ 是一个同构，在此情形下，$F(\alpha)$ 同构于有理函数域 $F(x)$. 对所有超越元 α，扩域 $F(\alpha)$ 是同构的.

如果 α 是代数元，则情况大不一样：

【15.2.6】命题 *令 α 是扩域 K/F 中的元素，α 是 F 上的代数元，且令 f 是 α 在 F 上的既约多项式.*

(a) 典范映射 $F[x]/(f) \to F[\alpha]$ 是一个同构，并且 $F[\alpha]$ 是一个域. 因此 $F[\alpha] = F(\alpha)$.

(b) 更一般地，如果 $\alpha_1, \cdots, \alpha_k$ 是 F 的一个扩域 K/F 中的元素，它们都是 F 上的代数元，则环 $F[\alpha_1, \cdots, a_k]$ = 域 $F(\alpha_1, \cdots, a_k)$.

证明

(a) 设 $\varphi: F[x] \to K$ 为映射(15.2.2). 由于 (f) 是极大理想，故 $f(x)$ 生成 $\ker f$，且 $F[x]/(f)$ 同构于 φ 的象，也就是 $F[\alpha]$. 而且 $F[x]/(f)$ 是一个域，这证明了 $F[\alpha]$ 是域. 由于 $F(\alpha)$ 与 $F[\alpha]$ 的分式域，因此它等于 $F[\alpha]$.

(b) 由归纳法得：

$$F[\alpha_1, \cdots, \alpha_k] = F[\alpha_1 \cdots, \alpha_{k-1}][\alpha_k] = F(\alpha_1, \cdots, \alpha_{k-1})[\alpha_k] = F(\alpha_1, \cdots, \alpha_n) \qquad \blacksquare$$

下一个命题是命题 11.5.5 的特殊情形.

【15.2.7】命题 *设 α 为 F 上的代数元，并设 $f(x)$ 是 α 在 F 上的既约多项式. 假设 $f(x)$ 的次数为 n，即 α 在 F 上次数为 n，则 $(1, \alpha, \alpha^2, \cdots, \alpha^{n-1})$ 是 $F(\alpha)$ 作为 F 上向量空间的基.*

444 例如，$\omega = e^{2\pi i/3}$ 在 $\mathbf{Q}$ 上的既约多项式为 $x^2 + x + 1$. ω 在 $\mathbf{Q}$ 上的次数为 2，且 $(1, \omega)$ 是 $\mathbf{Q}(\omega)$ 在 $\mathbf{Q}$ 上的一组基.

说清楚两个代数元 α, β 是否生成同构的域扩张可能不太容易，虽然命题(15.2.7)给出了一个必要条件：它们在 F 上的既约多项式要有相同的次数，因为 α 在 F 上的次数是扩域 $F(\alpha)$ 作为 F-向量空间的维数. 这显然不是一个充分条件. 例如，第十三章学习的所有虚二次域都是由添加 $\mathbf{Q}$ 上次数为 2 的元素得到的，但它们不都是同构的.

另一方面，如果 α 是 $x^3 - x + 1$ 的根，则 $\beta = \alpha + 1$ 是 $x^3 - 3x^2 + 2x + 1$ 的根. 两个域 $\mathbf{Q}(\alpha)$ 和 $\mathbf{Q}(\beta)$ 相等. 如果只是给出两个多项式，那么我们要花点时间才能看出它们是如何联系的.

容易描述这样的情形：存在一个使 F 不变而将 α 映到 β 的同构 $F(\alpha) \to F(\beta)$. 下面的命题虽然简单，但对于我们理解扩域却是基本命题：

【15.2.8】命题 *设 F 是一个域，设 $\alpha \in K/F$ 和 $\beta \in L/F$ 是 F 的两个扩域中的代数元，存在域的同构 $\sigma: F(\alpha) \to F(\beta)$，其在 F 上是恒等的，且映 $\alpha \rightsquigarrow \beta$，当且仅当 α 和 β 在 F 上的既约多项式是相同的.*

证明 由于 α 是 F 上的代数元，故 $F[\alpha] = F(\alpha)$. 同理 $F[\beta] = F(\beta)$. 假定 α 和 β 在 F 上的既约多项式都是 $f(x)$. 应用命题(15.2.6)，得到两个同构

$$F[x]/(f)\xrightarrow{\varphi}F[\alpha] \quad \text{和} \quad F[x]/(f)\xrightarrow{\psi}F[\beta]$$

合成映射 $\sigma=\psi\varphi^{-1}$ 是所需要的同构 $F(\alpha)\to F(\beta)$. 反之，如果存在将 α 映到 β 且在 F 上是恒等映射的同构 σ，且如果 $f(x)$ 是系数属于 F 的使得 $f(\alpha)=0$ 的多项式，则也有 $f(\beta)=0$ (见下面命题(15.2.10)). 因此两个元素有同一个既约多项式. ■

例如，令 α_1 表示 2 的实立方根，令 $\omega=e^{2\pi i/3}$ 为 1 的复立方根. x^3-2 的三个复根为 α_1，$\alpha_2=\omega\alpha_1$，$\alpha_3=\omega^2\alpha_1$. 因此存在一个同构 $\mathbf{Q}(\alpha_1)\xrightarrow{\sim}\mathbf{Q}(\alpha_2)$ 将 α_1 映射为 α_2. 在此情形 $\mathbf{Q}(\alpha_1)$ 中的元素是实数，但 α_2 不是实数. 为了理解这个同构，我们必须看一下域的内部代数结构.

【15.2.9】定义 *设 K 和 K' 是同一个域 F 的两个扩域. 一个在子域 F 上的限制为恒等映射的同构 $\varphi:K\to K'$ 称为 F-同构或扩域的同构. 如果存在一个 F-同构 $\varphi:K\to K'$，则域 F 的两个扩域 K 和 K' 称为同构的扩域.*

下面的命题在(12.2.19)之前对于复共轭的情形已经证明.

【15.2.10】命题 *设 $\varphi:K\to K'$ 是 F 的扩域的一个同构，并设 $f(x)$ 是系数属于 F 的多项式. 设 α 是 $f(x)$ 在 K 中的一个根，并设 $\alpha'=\varphi(\alpha)$ 是它在 K' 中的像. 则 α' 亦是 $f(x)$ 的根.* 445

证明 设 $f(x)=a_nx^n+\cdots+a_1x+a_0$. 则由于 φ 是 F-同构，$a_i\in F$，故 $\varphi(a_i)=a_i$. 由于 φ 是一个同态，故

$$\begin{aligned}0=\varphi(0)&=\varphi(f(\alpha))=\varphi(a_n\alpha^n+\cdots+a_1\alpha+a_0)\\&=\varphi(a_n)\varphi(\alpha)^n+\cdots+\varphi(a_1)\varphi(\alpha)+\varphi(a_0)=a_n\alpha'^n+\cdots+a_1\alpha'+a_0\end{aligned}$$

因此 α' 是 $f(x)$ 的根. ■

第三节 扩域的次数

域 F 的一个扩域 K 总是可以视为一个 F-向量空间. 加法是 K 中的加法法则，K 中元素 a 用 F 的元素 c 的标量乘法定义为由这两个元素在 K 中相乘构成的积 ca. K 作为 F-向量空间的维数称为扩域的次数. 这个次数记作 $[K:F]$，是扩域的一个最基本的属性.

【15.3.1】 $[K:F]$ 是扩域 K 作为 F- 向量空间的维数

例如，$\mathbf{C}$ 有 $\mathbf{R}$-基(1，i)，因而次数 $[\mathbf{C}:\mathbf{R}]=2$.

如果次数 $[K:F]$ 是有限的，则扩域 K/F 称为一个有限扩域. 次数为 2 的扩域称为二次扩域. 次数为 3 的扩域为三次扩域，等等.

【15.3.2】引理

(a) 扩域 K/F 的次数为 1 当且仅当 $F=K$.

(b) 扩域 K 中元素 α 在 F 上的次数为 1 当且仅当 $\alpha\in F$.

证明

(a) 如果 K 作为 F 上的向量空间的维数为 1，则 K 上任何非零元(包括 1)都是 F 的基. 如果 1 是基，则 K 上任何元素都属于 F.

(b) 由定义，α 在 F 上的次数为 α 在 F 上的(首一的)既约多项式的次数. 若 α 在 F 上

的次数为 1，则此多项式必为 $x-\alpha$，且若多项式 $x-\alpha$ 的系数均属于 F，则 $\alpha\in F$. ■

【15.3.3】命题 假设域 F 的特征不为 2，即在 F 中 $1+1\neq 0$. 则 F 上任意二次扩域 K 可由添加一个平方根得到：$K=F(\delta)$，其中 $\delta^2=d\in F$. 反之，如果 δ 是 F 的扩域的元素，且如果 $\delta^2\in F$ 但 $\delta\notin F$，则 $F(\delta)$ 是 F 的一个二次扩域.

并不是所有的三次扩域都由添加一个三次方根得到. 这一点在下一章(参见第十六章第十一节)会了解更多.

证明 我们先证明每个二次扩域 K 由添加一个系数属于 F 的二次多项式 $f(x)$ 的根得到. 为此，选择 K 中不属于 F 的元素 α. 则 $(1,\alpha)$ 是 F 上的线性无关的集合. 由于 K 作为
446 F 上的向量空间的维数为 2，因此 $(1,\alpha)$ 是 K 的基. 由此得到 α^2 是 $(1,\alpha)$ 的线性组合，系数属于 F. 将该线性组合记为 $\alpha^2=-b\alpha-c$，其中 $b,c\in F$. 则 α 是 $f(x)=x^2+bx+c$ 的根. 由于 $\alpha\notin F$，故此多项式在 F 上是既约的. 当域 F 的特征是 2 时，这个结论也是对的.

二次多项式 $f(x)=x^2+bx+c$ 的判别式 $D=b^2-4c$. 在特征不是 2 的域里，我们可用二次求根公式 $\frac{1}{2}(-b+\sqrt{D})$ 来解方程 $x^2+bx+c=0$，这可由代入多项式来验证. 对平方根有两种选择，令 δ 表示这两个平方根之一. 则 $\delta\in K$，$\delta^2\in F$，且由于 $\alpha\in F(\delta)$，故 δ 在 F 上生成 K. 反之，如果 $\delta^2\in F$，$\delta\notin F$，则 $(1,\delta)$ 是 $F(\delta)$ 在 F 上的一组基，故 $[F(\delta):F]=2$. ■

次数的术语来自于由代数元 α 生成的域 $K=F(\alpha)$. 这是次数的第一个重要性质.

【15.3.4】命题

(a) 若扩域的一个元素 α 是 F 上的代数元，则 $F(\alpha)$ 在 F 上的次数 $[F(\alpha):F]$ 等于 α 在 F 上的次数.

(b) 扩域的一个元素 α 是 F 上的代数元当且仅当次数 $[F(\alpha):F]$ 是有限的.

证明 (a) 若 α 是 F 上的代数元，则由定义，其在 F 上的次数为其在 F 上某个既约多项式 f 的次数. 如果 f 的次数是 n，则 $F(\alpha)$ 有 F-基 $(1,\alpha,\cdots,\alpha^{n-1})$(命题 15.2.7)，故 $[F(\alpha):F]=n$. 若 α 不是 F 上的代数元，则 $F[\alpha]$ 和 $F(\alpha)$ 在 F 上是无限维的. ■

第二个重要性质是关于扩域的链的.

【15.3.5】定理(次数的乘法性质) 令 $F\subset K\subset L$ 是域. 则 $[L:F]=[L:K][K:F]$. 因此 $[L:K]$ 和 $[K:F]$ 都整除 $[L:F]$.

证明 设 $\boldsymbol{B}=(\beta_1,\beta_2,\cdots,\beta_n)$ 是 L 作为 K-向量空间的基，并设 $\boldsymbol{A}=(\alpha_1,\cdots,\alpha_m)$ 是 K 作为 F-向量空间的基. 因而 $[L:K]=n$ 而 $[K:F]=m$. 我们证明 mn 个积 $\boldsymbol{P}=\{\alpha_i\beta_j\}$ 的集合是 L 作为 F-向量空间的基，由此就证明了此定理. 同样的推理在 $\boldsymbol{B}$ 或 $\boldsymbol{A}$ 有一个是无限时也是可行的.

设 γ 是 L 的元素. 由于 $\boldsymbol{B}$ 是 L 在 K 上的基，故 γ 可以唯一表示为线性组合 $b_1\beta_1+\cdots+b_n\beta_n$，其中系数 $b_j\in K$. 由于 $\boldsymbol{A}$ 是 K 在 F 上的基，故每个 b_j 可以唯一地表示为线性组合 $a_{1j}\alpha_1+\cdots+a_{mj}\alpha_m$，其中系数 $a_{ij}\in F$. 则 $\gamma=\sum_{i,j}a_{ij}\alpha_i\beta_j$. 这表明 $\boldsymbol{P}$ 张成 F-向量空间 L. 如果线性组合 $\sum_{i,j}a_{ij}\alpha_i\beta_j=0$，则因为 $\boldsymbol{B}$ 是 L 作为 K-向量空间的基，故对每个 j，β_j 的系数 $\sum_i a_{ij}\alpha_i=0$. 又由

于 $\boldsymbol{A}$ 是 K 在 F 上的基，故系数 $a_{ij}=0$ 对于所有 i，j 成立. 因此 $\boldsymbol{P}=\{\alpha_i\beta_j\}$ 是线性无关的，因此它是 L 在 F 上的基. ■

【15.3.6】推论

(a) 设 $F\subset K$ 是一个 n 次有限扩域，并设 α 是 K 的一个元素. 则 α 在 F 上是代数的，且其在 F 上的次数整除 n.

(b) 令 $F\subset F'\subset L$ 是域. 如果 L 中元素 α 是 F 上的代数元，则它也是 F' 上的代数元. 如果 α 在 F 上的次数为 d，则它在 F' 上的次数至多为 d.

(c) 由 F 上的有限多个代数元生成的扩域 K 是有限扩域. 一个有限扩域由有限多个元素生成.

(d) 如果 K 是 F 的扩域，则 K 中所有 F 上的代数元的集合构成 K 的子域.

证明

(a) 元素 α 生成一个中间域 $F\subset F(\alpha)\subset K$，乘法性质指出：$[K:F]=[K:F(\alpha)][F(\alpha):F]$. 因此 $[F(\alpha):F]$ 是有限的，且它整除 $[K:F]$.

(b) 令 f 表示 α 在 F 上的既约多项式. 由于 $F\subset F'$，故 f 也是 $F'[x]$ 上的元素. 由于 α 是 f 的一个根，故 α 在 F' 上的既约多项式 g 整除 f. 故 g 的次数至多是 f 的次数.

(c) 令 a_1，…，a_k 生成 K，且它们是 F 上的代数元，令 F_i 表示由前 i 个元素生成的域 $F(a_1,\cdots,a_i)$. 这些域形成一个链 $F=F_0\subset F_1\subset\cdots\subset F_k=K$. 由于 α_i 在 F 上是代数元，故它也是更大的域 F_{i-1} 上的代数元. 因此次数 $[F_i:F_{i-1}]$ 对于任意 i 为有限的. 由乘法性质，$[K:F]$ 是有限的. 第二个断言是显然的.

(d) 我们必须证明如果 α 和 β 是 K 中元素，且为 F 上的代数元，则 $\alpha+\beta$，$\alpha\cdot\beta$ 等在 F 上也是代数元. 这从(a)和(c)可得，因为它们是域 $F(\alpha,\beta)$ 中的元素. ■

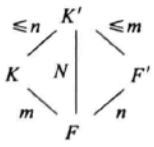
【15.3.7】推论 设 K 是 F 上的素数 p 次的扩域，并设 α 是 K 中不属于 F 的元素. 则 α 在 F 上次数为 p 且 $K=F(\alpha)$.

【15.3.8】推论 令 κ 是域 F 的扩域，令 K 和 F' 是 κ 的子域，且是 F 的有限扩域，令 K' 是由两个域 K 和 F' 生成的 κ 的子域. 令 $[K':F]=N$，$[K:F]=m$，$[F':F]=n$. 则 m 和 n 整除 N，且 $N\leqslant mn$.

证明 乘法性质表明 m 和 n 整除 N. 其次，假设 F' 是由一个元素在 F 上生成的域：对于某个元素 β 有 $F'=F[\beta]$. 则 $K'=K(\beta)$. 推论 15.3.6(b)表明 β 在 K 上的次数(等于 $[K':K]$)至多为 n. 乘法性质表明 $N\leqslant mn$. F 由几个元素生成的情形通过一次添加一个元素，再用归纳法可得. ■

下图是上面推论的总结：

【15.3.9】图



从推论可知$[K':F]=N$被m和n的最小公倍数整除，且如果m和n互素，则$N=mn$.

可能会试图猜测N整除mn，但这一点不总是成立.

【15.3.10】例

(a) x^3-2的三个复根是$\alpha_1=\alpha$，$\alpha_2=\omega\alpha$，$\alpha_3=\omega^2\alpha$，其中$\alpha=\sqrt[3]{2}$且$\omega=e^{2\pi i/3}$. 每个根α_i在$\mathbf{Q}$上的次数都是3，但是$\mathbf{Q}(\alpha_1,\alpha_2)=\mathbf{Q}(\alpha,\omega)$，且由于$\omega$在$\mathbf{Q}$上的次数是2，故$[\mathbf{Q}(\alpha_1,\alpha_2):\mathbf{Q}]=6$.

(b) 令$\alpha=\sqrt[3]{2}$且β是$\mathbf{Q}$上既约多项式x^4+x+1的一个根. 因为3和4是互素的，故$\mathbf{Q}(\alpha,\beta)$在$\mathbf{Q}$上的次数为12. 因此α不属于域$\mathbf{Q}(\beta)$. 另一方面，由于i在$\mathbf{Q}$上的次数为2，因此确定i是否属于$\mathbf{Q}(\beta)$不太容易. (i不属于$\mathbf{Q}(\beta)$.)

(c) 令$K=\mathbf{Q}(\sqrt{2},\mathrm{i})$是在$\mathbf{Q}$上添加$\sqrt{2}$和i生成的域. $\sqrt{2}$和i在$\mathbf{Q}$上的次数都是2，且因为i是复数，故它不属于$\mathbf{Q}(\sqrt{2})$. 所以$[\mathbf{Q}(\sqrt{2},\mathrm{i}):\mathbf{Q}]=4$. 因此i在$\mathbf{Q}(\sqrt{2})$上的次数为2. 由于$\sqrt{-2}$和i也生成$K$，因此i不属于域$\mathbf{Q}[\sqrt{-2}]$. ■

第四节 求既约多项式

令γ是F的扩域K中的元素，且为F上的代数元. 有两种求γ在F上的既约多项式$f(x)$的方法. 一种方法是计算γ的幂并寻找这些幂之间的线性关系. 虽然不太常用，但有时我们可以猜测f的其余的根，比如$\gamma_1,\cdots,\gamma_k$，其中$\gamma=\gamma_1$. 然后展开积$(x-\gamma_1)\cdots(x-\gamma_k)$将产生一个多项式. 我们后面将给出例子来说明这两种方法，其中的F是有理数域$\mathbf{Q}$.

【15.4.1】例 令$\gamma=\sqrt{2}+\sqrt{3}$. 计算γ的幂，当可能时进行简化：$\gamma^2=5+2\sqrt{6}$，$\gamma^4=49+20\sqrt{6}$. 我们不需要其他的幂，因为从这两个方程消去$\sqrt{6}$，得到关系$\gamma^4-10\gamma^2+1=0$. 因此，γ是多项式$g(x)=x^4-10x^2+1$的根. ■

下面是两个重要的初等结论：

【15.4.2】引理

(a) *元素γ的幂之间的一个线性相关关系$c_n\gamma^n+\cdots+c_1\gamma+c_0=0$意味着$\gamma$是多项式$c_nx^n+\cdots+c_1x+c_0$的根.*

(b) *令α和β是F的扩域中的代数元，且令它们在F上的次数分别为d_1和d_2. 则d_1d_2个单项式$\alpha^i\beta^j$(其中$0\leqslant i<d_1$，$0\leqslant j<d_2$)张成$F(\alpha,\beta)$为F上的向量空间.*

证明 虽然(a)很重要，但却是平凡的. 为了证明(b)，我们注意到α和β在F上是代
449 数元. $F(\alpha,\beta)=F[\alpha,\beta]$(15.2.6). 所列出的单项式张成$F[\alpha,\beta]$. ■

【15.4.3】例 例15.4.1的另一种方法是猜测g的根为$\gamma_1=\sqrt{2}+\sqrt{3}$，$\gamma_2=-\sqrt{2}-\sqrt{3}$，$\gamma_3=-\sqrt{2}+\sqrt{3}$和$\gamma_4=\sqrt{2}-\sqrt{3}$. 展开以这些为根的多项式，得到

$$\begin{aligned}&(x-\gamma_1)(x-\gamma_2)(x-\gamma_3)(x-\gamma_4)\\&=(x^2-(\sqrt{2}+\sqrt{3})^2)(x^2-(\sqrt{2}-\sqrt{3})^2)=x^4-10x^2+1.\end{aligned}$$

这就是我们前面得到的多项式. ■

这个引理表明假设关于 α 和 β 的既约多项式已知，我们总可以产生一个多项式以 $\gamma=\alpha+\beta$ 为根. 比如设 α 和 β 在 F 上的次数分别为 d_1 和 d_2. 给定 $F(\alpha,\beta)$ 上的任一元素 γ，它的幂记为 $1,\gamma,\cdots,\gamma^n$ 为单项式 $\alpha^i\beta^j$（其中 $0\leqslant i<d_1$，$0\leqslant j<d_2$）的线性组合. 当 $n=d_1d_2$，我们得到 $n+1$ 个方幂 γ^v 都是 n 个单项式的线性组合，故这些方幂是线性相关的. 一个线性相关关系确定了系数属于 F 的多项式以 γ 为一个根. 然而，有一点把问题复杂化了. 那就是以这种方法得到的以 γ 为根的多项式可能是可约的. 关于 γ 的在 F 上的既约多项式是以 γ 为一个根的次数最低的多项式. 要用这种方法确定这个既约多项式，我们需要找到 K 在 F 上的一组基.

【15.4.4】例

(a) 在例 15.4.1 中，其中 $\alpha=\sqrt{2}$，$\beta=\sqrt{3}$，且 $d_1=d_2=2$，元素 $\alpha^i\beta^j$（其中 $i,j<2$）为 $1,\sqrt{2},\sqrt{3},\sqrt{6}$. 这些元素确实构成了 K 在 $\mathbf{Q}$ 上的一组基. 多项式 x^4-10x^2+1 是既约多项式.

(b) 我们回到例 15.3.10(a)，其中多项式 x^3-2 的 3 个根标记为 α_i，$i=1,2,3$. 令 $F=\mathbf{Q}$，$L=\mathbf{Q}(\alpha)$ 和 $K=\mathbf{Q}(\alpha_1,\alpha_2)$. 每个根在 F 上的次数都是 3. 由引理，9 个单项式 $\alpha_1^i\alpha_2^j$（其中 $0\leqslant i,j<3$）在 F 上张成 K. 然而，这些单项式不是线性无关的. 由于 f 在域 $L=\mathbf{Q}(\alpha)$ 上有根 α_1，故它在 $L[x]$ 上分解，比如分解为 $f(x)=(x-\alpha_1)q(x)$. 则 α_2 是 $q(x)$ 的根，故 α_2 在 L 上的次数至多为 2. 集合 $(1,\alpha_2)$ 是 K 在域 L 上的一组基，故 6 个单项式 $\alpha_1^i\alpha_2^j$（其中 $0\leqslant i<3$，$0\leqslant j<2$）形成 K 在域 F 上的一组基. 如果我们要得到单项式的一组基，则应该用这个方法. ■

第五节 尺规作图

著名的定理断言：某些几何构造不能用直尺和圆规作出. 为了证明这些定理，我们现在用扩域次数的概念证明三等分任意角是不可能用尺规作图的.

下面是直尺和圆规作图的基本法则：

【15.5.1】

- 以给定平面上的两点作为开始. 这两个点认为是作出的.
- 如果作了两个点 p_0，p_1，则可过它们作一条直线，或者作一个以 p_0 为圆心并过另一点 p_1 的圆. 这样的直线和圆被认为是作出的.
- 已作出的直线和圆的交点被认为是作出的.

点、直线和圆称为是可构造的，如果可以通过应用上述规则有限步骤得到.

注意我们的直尺只能用于过作出的点作直线，不能用它来度量长度. 有时将其称为“直边”来明确这一点.

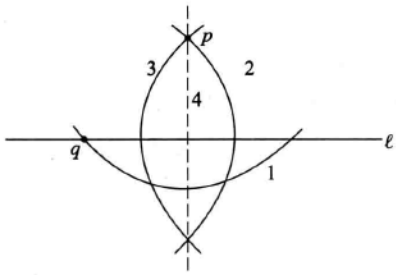
我们将从一些熟知的作图开始来描述所有可能的作图. 在每个图中，直线和圆按标出的顺序作出. 前两个构造用到了直线 ℓ 上的点 q，唯一的限制是这个点不在垂线上. 每当

450

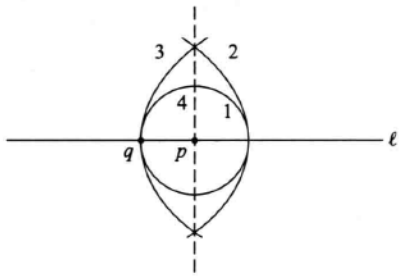
需要任意点时，我们将作出一个特别的点来用. 因为一个作出的直线 ℓ 包含无数多个可作出的点.

【15.5.2】作图 过一个作出的点 p 作一条与作出的直线 ℓ 垂直的直线.

情形 1：$p \notin \ell$



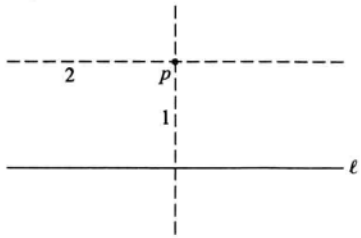
情形 2：$p \in \ell$



451

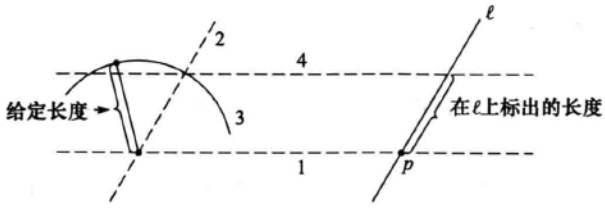
【15.5.3】作图 过一个作出的点 p 作一条与作出的直线 ℓ 平行的直线.

应用上面的情形 1 和 2：



【15.5.4】作图 从一个点 $p \in \ell$ 开始，在作出的直线 ℓ 上标出由两个点定义的长度.

利用平行线的做法：



我们在平面上引入笛卡儿坐标系使得开始时给定的两个点的坐标为(0，0)和(1，0).

【15.5.5】命题

(a) 令 $p_0=(a_0, b_0)$和点 $p_1=(a_1, b_1)$是坐标 a_i 和 b_i 在实数域的子域 F 上的点. 通过 p_0 和 p_1 的直线用系数属于 F 的线性方程来定义. 圆心在 p_0 且通过 p_1 的圆用系数属于 F 的二次方程来定义.

(b) 令 A 和 B 分别为由系数属于实数域的子域 F 的线性方程或二次方程所定义的直线和圆. 则 A 和 B 的交点的坐标属于 F, 或者属于 F 的实二次扩域 F'.

证明

(a) 过(a_0, b_0)和(a_1, b_1)的直线是线性方程

$$(a_1-a_0)(y-b_0)=(b_1-b_0)(x-a_0)$$

的轨迹.

452

以(a_0, b_0)为中心、过(a_1, b_1)的圆是二次方程

$$(x-a_0)^2+(y-b_0)^2=(a_1-a_0)^2+(b_1-b_0)^2$$

的轨迹. 这些方程的系数在域 F 中.

(b) 两条直线的交点通过解系数属于 F 的两个线性方程得到, 因此它的坐标属于 F. 要求直线和圆的交点, 我们用直线方程去消去圆的方程中的一个变量, 得到一个未知变量的二次方程. 这个二次方程在域 $F'=F[\sqrt{D}]$中有解, 其中 D 为二次方程的判别式. 这个判别式是 F 中的元素. 如果 $F'\neq F$, 则 F'在 F 上的次数为 2. 如果 $D<0$, 则方程没有实数解. 于是直线和圆不相交.

考虑两个圆的交, 比如

$$(x-a_1)^2+(y-b_1)^2=c_1 \text{ 和} (x-a_2)^2+(y-b_2)^2=c_2$$

其中 a_i, b_i, $c_i\in F$. 一般来说, 求一对二元二次方程的解需要解四次方程. 在这里很幸运: 两个二次方程的差是线性方程. 我们可以像前面一样, 用这个线性方程来消去一个变量. 这个令人庆幸的事实反映了这样的事实: 当一对圆锥曲线可能有四个交点时, 两个圆的交点至多为两个. ■

【15.5.6】定理 令 p 是一个可构造的点. 对某个整数 n, 存在一个域的链

$$\mathbf{Q}=F_0\subset F_1\subset F_2\subset\cdots\subset F_n=K, \text{使得}$$

- K 是实数域的一个子域;
- 点 p 的坐标属于 K;
- 对于每个 $i=0, \cdots, n-1$, 次数$[F_{i+1}:F_i]$等于 2.

因此次数$[K:\mathbf{Q}]$是 2 的幂.

证明 我们引入坐标使得原来给定的点为(0, 0)和(1, 0). 这些点的坐标在 $\mathbf{Q}$ 中. 构造点 p 的过程涉及一个步骤序列, 每一步骤都是作圆或直线.

假设我们到第 k 步时所有作出的点的坐标均属于域 F. 下一步作出通过这些点中的两点的直线或圆, 且根据命题 15.5.5(a), 直线和圆的方程的系数均在 F 中. 域没有变. 则由命题 15.5.5(b), 所作出的直线和直线、圆和圆、直线和圆的交点的坐标或者属于

F，或者属于 F 的一个二次扩域．本断言利用归纳法由命题 15.5.5 和次数的乘法性质可得证． ■

注 我们称一个实数是可构造的如果点$(a, 0)$是可构造的．既然我们能作出垂线，这相当于说 a 是一个可构造点的横坐标．而由于我们可以标出长度，因此一个正实数 a 是可
453 构造的当且仅当存在一对可构造的点 p 和 q，它们之间的距离为 a．

【15.5.7】推论 令 a 是一个可构造的实数．则 a 是一个代数数，且它在 $\mathbf{Q}$ 上的次数是 2 的幂．

由于 a 是域 K 中的元素，而域 K 是上述定理中域链的最后一个域，且$[K:\mathbf{Q}]$是 2 的幂，所以 a 的次数也是 2 的幂(15.3.6)．

此推论的逆不真．存在 $\mathbf{Q}$ 上次数为 4 的实数，这个实数是不可构造的．伽罗瓦理论提供了理解这一点的方法．(这是第十六章的练习 9.17.)

我们现在能证明一些几何构造的不可能性．这个方法是通过证明如果一个特定的结构是可构造的，那么就可以构造一个在 $\mathbf{Q}$ 上的次数不是 2 的幂的代数数．这就与推论矛盾．我们的例子是证明三等分任意角是不可能的，这要求我们在角 θ 已知的情况下，去作出角 $\frac{1}{3}\theta$．现在许多角(例如 45°)可以用尺规三等分．三等分任意角要求我们给出一个一般的作出方法．

既然 60°角很容易作出，我们便把 60°角当成已知的，用尺规作出来．如果三等分这个角能够作出来，也就是我们可以作出 20°角．我们将证明这个特殊角是不可能作出来的，因此没有作出三等分任意角的一般方法．

我们说一个角 θ 是可构造的如果可以作出一对直线，它们相交成 θ 角．如果在直线上标出单位长度并垂直投影到另一条直线上，我们将作出实数 $\cos\theta$．反之，如果 $\cos\theta$ 是一个可构造的实数，则可以把这个过程逆回去作出一对相交成 θ 角的直线．

下一个引理证明 $20°=\pi/9$ 是不可能作出的．

【15.5.8】引理 实数 $\cos 20°$ 是 $\mathbf{Q}$ 上的代数元，它在 $\mathbf{Q}$ 上的次数为 3．因此 $\cos 20°$ 是不可能构造的数．

证明 令 $\alpha=2\cos\theta=e^{i\theta}+e^{-i\theta}$，其中 $\theta=\pi/9$．则 $e^{3i\theta}+e^{-3i\theta}=2\cos(\pi/3)=1$，且

$$\alpha^3=(e^{i\theta}+e^{-i\theta})^3=e^{3i\theta}+3e^{i\theta}+3e^{-i\theta}+e^{-3i\theta}=1+3\alpha$$

故 α 是多项式 x^3-3x-1 的一个根．多项式在 $\mathbf{Q}$ 上是既约的，因为它没有整数根．因此这个多项式是 α 在 $\mathbf{Q}$ 上的既约多项式．故 α 在 $\mathbf{Q}$ 上的次数为 3，故 $\cos\theta$ 在 $\mathbf{Q}$ 上的次数也为 3． ■

另一个例子：正 7 边形不可作出．这和上面的问题类似，因为作出 20°角等价于作出正 18 边形．我们稍稍改变一下解题方法．令 $\theta=2\pi/7$ 且令 $\zeta=e^{i\theta}$．则 ζ 是 7 次单位根，它是既约多项式 $x^6+x^5+\cdots+x+1$ 的一个根(定理 12.4.9)，故 ζ 在 $\mathbf{Q}$ 上的次数为 6．如果正 7 边形可以构造，则 $\cos\theta$ 和 $\sin\theta$ 都是可构造的数．它们将属于在 $\mathbf{Q}$ 上次数为 2 的幂的实扩域

K，比如$[K:\mathbf{Q}]=2^k$. 称这个域为 K，并考虑其扩域 $K(\mathrm{i})$. 这个扩域的次数为 2，故$[K(\mathrm{i}):\mathbf{Q}]=2^{k+1}$. 但 $\zeta=\cos\theta+\mathrm{i}\sin\theta\in K(\mathrm{i})$. 这与 ζ 在 $\mathbf{Q}$ 上的次数为 6 矛盾. 454

我们所用的论证方法对于数 7 不是特殊的. 它适用于任意素数 p，如果 $p-1$ 是既约多项式 $x^{p-1}+x^{p-2}+\cdots+x+1$ 的次数，但不是 2 的方幂.

【15.5.9】推论 令 p 是一个素数. 如果正 p 边形可以用尺规作出，则 $p=2^r+1$，其中 r 是某个正整数.

高斯证明了其逆命题：如果一个素数具有形式 2^r+1，则正 p 边形可以用尺规作出. 例如，正 17 边形可以用尺规作出. 在下一章(参见推论 16.10.5)我们将学习如何证明这个结论.

为完成讨论，我们证明定理 15.5.6 的逆命题.

【15.5.10】定理 令 $\mathbf{Q}=F_0\subset F_1\subset\cdots\subset F_n=K$ 是实数域 $\mathbf{R}$ 的子域链，且具有性质$[F_{i+1}:F_i]=2$，其中 $i=0,\cdots,n-1$. 则 K 的每个元素是可构造的.

由于任何一个 2 次扩域可以由添加一个平方根得到，因此这个定理可从下面的引理得到.

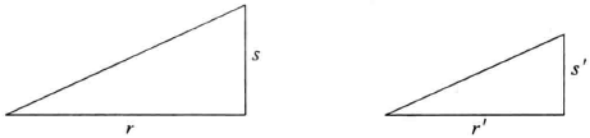
【15.5.11】引理

(a) 可构造数形成实数域 $\mathbf{R}$ 的一个子域.

(b) 如果 a 是一个正的可构造数，则$\sqrt{a}$也是可构造的.

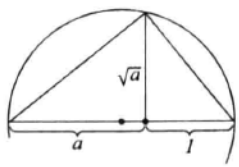
证明

(a) 我们必须证明如果 a 和 b 是正的可构造数，则 $a+b$，$-a$，ab 和 $a^{-1}(a\neq0)$也是可构造的. a 和 b 为负数的情形容易得到. 加法和减法通过在直线上标出长度作出. 对乘法和除法，我们用相似直角三角形.



给定一个三角形及另一个三角形的一条边，第二个三角形可以用平行线作出. 要构造积 ab，我们取 $r=1$，$s=a$ 和 $r'=b$，则 $s'=ab$. 要作出 a^{-1}，我们取 $r=a$，$s=1$ 和 $r'=1$. 则 $s'=a^{-1}$.

(b) 再一次应用相似直角三角形. 我们必须构造它们使得 $r=a$，$r'=s$ 且 $s'=1$. 则 $s=\sqrt{a}$. 这次要如何作图并不是太明显，但可以用圆的内接三角形. 以直径为其斜边的圆的内接三角形是直角三角形. 这是高中几何的一个定理，可用圆的方程和毕达哥拉斯定理验证. 这样我们作出一个直径为 $1+a$ 的圆，然后如下图继续. 注意大三角形被分为两个相似三角形. 455



■

第六节 添 加 根

到目前为止，我们一直用复数的子域作为我们的例子. 创建这些域不需要抽象的构造(除了从 **R** 到 **C** 的构造是抽象的以外). 根据需要，可以简单地在有理数上添加复数并使用它们生成的子域. 但有限域和函数域不是类似于 **C** 这样的我们熟悉的、包含一切的域的子域，因而必须构造这些域. 构造它们的基本工具是在第十一章中所学的在环上添加元素. 在这里把它应用到开始时环是一个域 F 的情形.

我们复习这一构造过程. 给定系数属于 F 的多项式 $f(x)$，可以添加 $f(x)$的一个根到 F. 抽象过程是构造多项式环 $F[x]$的商环

【15.6.1】 $$K = F[x]/(f)$$

这个构造总是产生环 K 及同态 $F\to K$，使得 x 的剩余$\bar{x}$满足关系 $f(\bar{x})=0$(11.5.2). 然而我们要构造的不仅是环，而且是域，在这里域上多项式的理论起了作用. 这个理论告诉我们多项式环 $F[x]$上的主理想(f)是极大理想当且仅当 f 是既约多项式(见(12.2.8)). 因而环 K 是一个域当且仅当 f 是一个既约多项式(11.8.2).

【15.6.2】引理 *设 F 是一个域，并设 f 是 $F[x]$中的既约多项式. 则环 $K=F[x]/(f)$是 F 的扩域，x 的剩余$\bar{x}$是 $f(x)$在 K 中的根.*

证明 因为(f)是一个极大理想，所以环 K 是一个域，而且，因为 F 是域，所以将 F 中的元素映到常多项式的剩余的同态 $F\to K$ 是一个单射. 因而可将 F 等同于其像，也就是等同于 K 的一个子域. 在这一等同的意义下，域 K 成为 F 的一个扩域. 最后，$\bar{x}$ 满足方程$f(\bar{x})=0$，这表明它是 f 的一个根(见(11.5.2)). ■

注 一个多项式 f 在域 K 上是完全分裂的如果它在 K 上的因子全是线性因子.

【15.6.3】命题 *设 F 是域，并设 $f(x)$是 $F[x]$中正次数的首一多项式. 存在 F 的扩域 K 使得 $f(x)$在 K 上完全分裂.*

证明 对 f 的次数用归纳法. 第一种情形是 f 在 F 中的有一个根 α，使得 $f(x)=(x-\alpha)q(x)$对于某个多项式 q 成立. 如果这样，则用 q 代替 f，而且对于 q 用归纳法可知 456 是完全分裂. 否则，我们选取 f 的一个既约多项式因子 g. 由引理 15.6.2，存在 F 的一个扩域 F_1，F_1 中 g 有一个根 α. 则 α 也是 f 的一个根. 我们用 F_1 代替 F 就将其化为第一种情形. ■

正如我们所见，多项式环 $F[x]$是研究域 F 的扩域的一个重要工具. 当涉及扩域时，域的多项式环之间相互关联. 这种相互关联并不会带来严重的困难，我们将需要指出的要点都集中在这里而不是分散在书中各处来加以叙述，将这些要点收集整理成下面的命题.

【15.6.4】命题 *设 f 和 g 是系数属于域 F 的多项式，且 $f\neq 0$，并设 K 是 F 的扩域.*

(a) *多项式环 $K[x]$包含 $F[x]$作为其子环，故在环 $F[x]$上的运算在 $K[x]$上也成立.*

(b) *不论在 $F[x]$中还是在 $K[x]$中，由 f 对 g 作的带余除法得到相同的答案.*

(c) *在 $K[x]$中 f 整除 g 当且仅当在 $F[x]$中 f 整除 g.*

(d) 不论在 $F[x]$ 中还是在 $K[x]$ 中，f 和 g 的(首一的)最大公因子 d 都是相同的.

(e) 如果 f 和 g 在 K 上有公共根，则它们在 $F[x]$ 中不是互素的. 反之，如果 f 和 g 在 $K[x]$ 中不是互素的，则存在一个扩域 L，它们在其中有公共根.

(f) 如果 f 在 $F[x]$ 中是既约的且 f 和 g 在 K 中有公共根，则 f 在 $F[x]$ 中整除 g.

证明

(a) 是显然的.

(b) 在 $F[x]$ 中作除法：$g=fq+r$. 这个等式在更大的环 $K[x]$ 中也是成立的，而且由于在 $K[x]$ 带余除法是唯一的，故结果是一样的.

(c) 这是(b)中余数为零的情况.

(d) 令 d 和 d' 分别是 f 和 g 在 $F[x]$ 和 $K[x]$ 中的最大公因子，则 d 是 $K[x]$ 中的一个公因子，且由于 d' 是 f 和 g 在 $K[x]$ 中的最大公因子，故 d 整除 d'. 此外，我们知道对于某个 p 和 q 属于 $F[x]$，d 具有形式 $d=pf+qg$. 由于 d' 整除 f 和 g，故 d' 整除 d. 因此 d 和 d' 在 $K[x]$ 中是相伴元，且由于它们是首一多项式，因此它们相等.

(e) 如果 α 是 f 和 g 在 K 中的公共根. 则 $x-\alpha$ 是 f 和 g 在 $K[x]$ 中的公因子，因而它们在 $K[x]$ 中的最大公因子不为 1. 由(d)，它们在 $F[x]$ 中的最大公因子也不为 1. 反之，如果 f 和 g 在 $F[x]$ 中有一个次数>0 的公因子 d，则存在 F 的一个扩域 L 使得 d 在 L 中有一个根. 这个根就是 f 和 g 的一个公共根.

(f) 如果 f 是既约的，则它在 $F[x]$ 中仅有的首一的因子为 1 和 f. (e)告诉我们 f 和 g 在 $F[x]$ 中的最大公因子不是 1. 因而它是 f. ■

本节最后一个主题涉及多项式 $f(x)$ 的导数 $f'(x)$. 导数是用微积分中求多项式函数的 457
微分的规则计算的. 换句话说，如果 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，则

【15.6.5】
$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1$$

公式中的整数系数理解为 F 的元素 $1+1+\cdots+1$. 故如果 $f(x)$ 的系数在域 F 中，则其导数的系数也在域 F 中. 可以证明像微分的乘法法则那样的法则成立(这是练习 3.5).

导数可以被用来识别多项式的重根.

【15.6.6】**引理** *令 f 是一个系数属于一个域 F 的多项式. 域 F 的扩域 K 上的一个元素 α 是重根，也就是说 $(x-\alpha)^2$ 整除 f 当且仅当它同时是 f 和 f' 的根.*

证明 如果 α 是 f 的一个根，则 $x-\alpha$ 整除 f，比如 $f(x)=(x-\alpha)g(x)$. 于是 α 是 f 的重根当且仅当它是 g 的一个根. 由微分的乘法法则，

$$f'(x)=(x-\alpha)g'(x)+g(x)$$

代入 $x=\alpha$，可知 $f'(\alpha)=0$ 当且仅当 $g(\alpha)=0$. ■

【15.6.7】**命题** *令 $f(x)$ 是一个系数属于一个域 F 的多项式. 存在域 F 的扩域 K，在其上 $f(x)$ 有重根当且仅当 f 和 f' 不是互素的.*

证明 如果 f 在 K 中有一个重根，则 f 和 f' 在 K 中有公共根，因而它们在 K 中不互素，因此它们在 F 上也不互素. 反之，如果 f 和 f' 不互素，则它们在某个扩域 K 中有公

共根，因此 f 在这个域中有一个重根. ■

下面是导数在域论中最重要的应用之一：

【15.6.8】命题 设 f 是 $F[x]$ 中的一个既约多项式.

(a) 除非导数 f' 是零多项式，否则 f 在 F 的任何扩域中均没有重根.

(b) 如果域 F 的特征为零，则 f 在 F 的任意扩域中没有重根.

证明

(a) 由前面的命题，必须证明除非 f' 是零多项式，否则 f 与 f' 是互素的. 由于 f 是既约的，因此它与另一个多项式 g 有非常数公因子仅有的可能情形是 f 整除 g. 而如果 f 整除 g，则 $\deg g \geqslant \deg f$，或者 $g=0$. 如果 $f' \neq 0$，则 f' 的次数小于 f 的次数，那么 f 与 f' 没有非常数公因子，这正是所要证的.

(b) 在特征为零的域中非常数多项式的导数不等于零. ■

当域 F 的特征为素数 p 时，非常数多项式 f 的导数可以为零. 当在 f 中出现的每个单项式的指数都被 p 整除时就会发生这种情形. 在特征为 5 时导数为零的多项式的一个典型例子是

458

$$f(x) = x^{15} + ax^{10} + bx^5 + c$$

其中 a，b，c 是 F 中的任意元素. 由于这个多项式的导数恒等于零，因此它在任意扩域中的根都是重根.

第七节 有 限 域

本节描述有有限多个元素的域. 一个有限域 K 的特征不为零，故其特征为一个素整数 (3.2.10)，因此 K 必含有素域 $F=\mathbf{F}_p$ 中的一个. 由于 K 是有限的，因此它作为这个域上的向量空间当然是有限维的.

我们用 r 表示次数 $[K:F]$. 作为 F-向量空间，K 与列空间 F^r 同构，而这个空间包含 p^r 个元素. 因而一个有限域的阶(即域的元素个数)总是一个素数的幂. 习惯上用字母 q 表示这个阶：

【15.7.1】

$$|K| = p^r = q$$

在这一节，q 表示素整数 p 的正的幂. q 个元素的域常常记为 $\mathbf{F}_q$. 我们将证明所有 q 阶有限域都是同构的，因而这个记号并不太含糊，虽然当 $r>1$ 时，两个 q 阶有限域间的同构不是唯一的.

除了素域外，最简单的有限域是 4 阶域 $\mathbf{F}_4$. 令 $K=\mathbf{F}_4$，且令 $F=\mathbf{F}_2$. 在 $F[x]$ 中存在唯一的 2 次既约多项式 $f(x)$，即 x^2+x+1(12.4.4)，且域 K 由添加 $f(x)$ 的一个根 α 到 F 上得到：

$$K \approx F[x]/(x^2+x+1)$$

因为 α(即 x 的剩余)的次数为 2，故集合(1，α)形成 K 在 F 上的一组基(15.2.7). 所有域 K 的元素是这组基的 4 个线性组合，系数模 2：

【15.7.2】 $$K=\{0,1,\alpha,1+\alpha\}$$

元素 $1+\alpha$ 是多项式 $f(x)$ 在 K 中的另一个根. 在 $\mathbf{F}_4$ 的计算要用到关系 $1+1=0$ 及 $\alpha^2+\alpha+1=0$.

不要将域 $\mathbf{F}_4$ 与环 $\mathbf{Z}/(4)$ 混淆起来，$\mathbf{Z}/(4)$ 不是一个域.

下面是关于有限域的主要事实：

【15.7.3】**定理** 设 p 是一个素整数，并设 $q=p^r$ 是 p 的正的方幂.

(a) 设 K 是一个 q 阶域. K 的元素是多项式 x^q-x 的根.

(b) 在素域 $F=\mathbf{F}_p$ 上的多项式 x^q-x 的既约因子是次数整除 r 的 $F[x]$ 上的既约多项式.

(c) 令 K 是一个 q 阶域. K 的非零元素的乘法群 $K^\times$ 是一个 $q-1$ 阶循环群.

(d) 存在一个 q 阶域，且所有 q 阶域是同构的.

(e) p^r 阶域 K 含有 p^k 阶子域当且仅当 k 整除 r. 459

【15.7.4】**推论** 对于任何正整数 r，存在素域 $\mathbf{F}_p$ 上的一个次数为 r 的既约多项式.

证明 由(d)，存在一个阶为 $q=p^r$ 的域 K. 它在 $F=\mathbf{F}_p$ 上的次数 $[K:F]$ 是 r. 由(c)，乘法群 $K^\times$ 是循环群. 显然循环群的生成元 α 将生成扩域 K，即 $K=F(\alpha)$. 由于 $[K:F]=r$，因此 α 在 F 上的次数为 r. 故 α 是一个次数为 r 的既约多项式的根. ■

作为例子，我们看一些 q 是 2 的幂的例子. $\mathbf{F}_2$ 上次数至多为 4 的既约多项式在(12.4.4)中已经列出.

【15.7.5】**例**

(i) 域 $\mathbf{F}_4$ 在 $\mathbf{F}_2$ 上的次数是 2. 它的元素是多项式

【15.7.6】 $$x^4-x=x(x-1)(x^2+x+1)$$

的根. 注意 x^2-x 的因子出现，因为 $\mathbf{F}_4$ 包含 $\mathbf{F}_2$.

既然我们在特征为 2 的域上讨论问题，符号就没有关系了：$x-1=x+1$.

(ii) 阶为 8 的域 $\mathbf{F}_8$ 在素域 $\mathbf{F}_2$ 上的次数为 3. 它的元素是多项式 x^8-x 的 8 个根. 此多项式在 $\mathbf{F}_2$ 上的分解为

【15.7.7】 $$x^8-x=x(x-1)(x^3+x+1)(x^3+x^2+1)$$

立方因子是在 $\mathbf{F}_2[x]$ 上两个 3 次既约多项式.

要在域 $\mathbf{F}_8$ 中计算，可选择域上的既约立方因子之一的一个根 β，比如 x^3+x+1 的根. 它在 $\mathbf{F}_2$ 上的次数为 3. 则 $(1,\beta,\beta^2)$ 是 $\mathbf{F}_8$ 在 $\mathbf{F}_2$ 上作为向量空间的一个基. $\mathbf{F}_8$ 的元素是系数为 0，1 的这组基的 8 个线性组合：

【15.7.8】 $$\mathbf{F}_8=\{0,1,\beta,1+\beta,\beta^2,1+\beta^2,\beta+\beta^2,1+\beta+\beta^2\}$$

在 $\mathbf{F}_8$ 中利用关系 $1+1=0$ 和 $\beta^3+\beta+1=0$ 进行计算.

注意到 x^2+x+1 不是 x^8-x 的因子，因此 $\mathbf{F}_8$ 不包含 $\mathbf{F}_4$. 因为 $[\mathbf{F}_8:\mathbf{F}_2]=3$，$[\mathbf{F}_4:\mathbf{F}_2]=2$，故 2 不整除 3，因而包含关系是不可能的.

(iii) 域 $\mathbf{F}_{16}$ 在 $\mathbf{F}_2$ 上的次数为 4，它的元素是多项式 $x^{16}-x$ 的根. 这个多项式在 $\mathbf{F}_2[x]$ 上分解为：

【15.7.9】

$$x^{16}-x=x(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1)$$

在 $\mathbf{F}_2[x]$ 上出现了 3 个 4 次既约多项式. x^4-x 的因子也在其中，因为 $\mathbf{F}_{16}$ 包含 $\mathbf{F}_4$. ■

现在开始定理 15.7.3 的证明. 令 F 表示素域 $\mathbf{F}_p$.

定理 15.7.3(a)的证明(K 的元素是多项式 x^q-x 的根) 令 K 是阶为 q 的域. 乘法群 460 $K^\times$ 的阶为 $q-1$. 因此 $K^\times$ 的任何一个元素的阶整除 $q-1$，故 $\alpha^{(q-1)}-1=0$，这意味着 α 是多项式 $x^{(q-1)}-1$ 的根. K 的其余元素都是零，是多项式 x 的根. 故 K 的每个元素是多项式 $x(x^{(q-1)}-1)=x^q-x$ 的根. ■

定理 15.7.3(c)的证明(乘法群是循环群) 证明基于阿贝尔群的结构定理 14.7.3，该定理告诉我们 $K^\times$ 是循环群的直和.

结构定理用加法符号叙述为：一个有限阿贝尔群 V 是阶为 d_1，…，d_k 的循环子群的直和 $C_1\oplus\cdots\oplus C_k$，其中每个 d_i 整除下一个：$d_1\mid d_2\mid\cdots\mid d_k$. 令 $d=d_k$. 如果 w_i 是 C_i 的生成元，则 $d_iw_i=0$，且由于 d_i 整除 d，故 $dw_i=0$. 因此 $dv=0$ 对于 V 中任何元素 v 成立. 因此 V 中任何元素 v 的阶整除 d.

回到乘法记号，$K^\times$ 是循环子群的直和，比如 $H_1\oplus\cdots\oplus H_k$，其中 H_i 的阶为 d_i，且 $d_1\mid d_2\mid\cdots\mid d_k$. 记 $d=d_k$，$K^\times$ 的每个元素 α 的阶整除 d，这意味着 $\alpha^d=1$. 因此 $K^\times$ 的每个元素 α 是多项式 x^d-1 的根. 这个多项式在 K 上至多有 d 个根(12.2.20)，因此 $|K^\times|=q-1\leqslant d$. 另一方面，$|K^\times|=|H_1\oplus\cdots\oplus H_k|=d_1\cdots d_k$. 故 $d_1\cdots d_k=|K^\times|=q-1\leqslant d$. 由于 $d=d_k$，故仅有一种可能就是 $k=1$ 和 $q-1=d$. 因此 $K^\times=H_1$，且 $K^\times$ 是循环群. ■

定理 15.7.3(d)的证明(q 阶域的存在性) 既然已经证明了(a)，我们知道 q 个元素的域中的元素是多项式 x^q-x 的根. 存在 F 的扩域 L 使多项式完全分裂(15.6.3). 我们自然要尝试取这样的域 L 且希望最好多项式 x^q-x 在 L 上的根形成我们要求的一个子域 K. 这将在引理 15.7.11 中证明. ■

【15.7.10】**引理** *令 F 是特征为素数 p 的域，且令 $q=p^r$ 是 p 的正的方幂.*

(a) 多项式 x^q-x 在 F 的任何扩域上没有重根.

(b) 在多项式环 $F[x,y]$ 中，$(x+y)^q=x^q+y^q$.

证明

(a) x^q-x 的导数为 $qx^{q-1}-1$. 在特征为 p 的情形，系数 q 等于 0，而导数等于 -1. 由于常数多项式 -1 没有根，因此 x^q-x 与它的导数没有公共根，因此 x^q-x 没有重根(引理 15.6.6).

(b) 我们在 $\mathbf{Z}[x,y]$ 上展开 $(x+y)^q$：

$$(x+y)^p=x^p+\binom{p}{1}x^{p-1}y+\binom{p}{2}x^{p-2}y^2+\cdots+\binom{p}{p-1}xy^{p-1}+y^p$$

引理 12.4.8 告诉我们二项式系数 $\binom{p}{r}$ 被 p 整除，其中 $1<r<p$. 由于 F 的特征为 p，故映

射 $\mathbf{Z}[x, y]\to F[x, y]$将这些系数映射为零，且在 $F[x, y]$中有$(x+y)^p=x^p+y^p$. 当 $q=p^r$ 时，$(x+y)^q=x^q+y^q$ 的事实由归纳法得证. ■ 461

【15.7.11】引理 设 p 是一个素数，并设 $q=p^r$ 是 p 的正的方幂. 令 L 是特征为 p 的域，令 K 是多项式 x^q-x 在 L 上所有根的集合. 则 K 是 L 的子域.

证明 令 α 和 β 是多项式 x^q-x 在 L 上的两个根. 我们必须证明 $\alpha+\beta$，$-\alpha$，$\alpha\beta$，α^{-1}(如果 $\alpha\neq 0$)和 1 是同一个多项式的根. 故假设 $\alpha^q=\alpha$ 和 $\beta^q=\beta$. 证明 $\alpha\beta$，α^{-1}和 1 是根是显然的，我们在此省略. 代入引理 15.7.10(b)表明$(\alpha+\beta)^q=\alpha^q+\beta^q=\alpha+\beta$.

最后，我们验证 -1 是 x^q-x 的根：由于根的积是根，故可得 $-\alpha$ 是一个根. 如果 $p\neq 2$，则 q 是一个奇整数，且$(-1)^q=-1$ 成立. 如果 $p=2$，则 q 是偶数，且$(-1)^q=1$. 但此时 L 的特征为 2，故 $1=-1$ 在 L 上成立. ■

我们仍必须证明两个阶均为 $q=p^r$ 的域 K 和 K'同构. 令 α 是循环群 $K^\times$ 的生成元. 则 $K=F(\alpha)$，故 α 在 F 上的既约多项式 f 的次数为$[K:F]=r$. 则 f 生成一个以 α 为根的 $F[x]$的多项式的理想，且由于 α 也是 x^q-x 的根，故 f 整除 x^q-x. 由于 x^q-x 在 K'上是完全分裂的，故 f 也有一个根 α'在 K'上. 则 $F(\alpha)$和 $F(\alpha')$都同构于 $F[x]/(f)$，因此，$F(\alpha)$和 $F(\alpha')$彼此同构. 计算次数可证明 $F(\alpha')=K'$，故 K 和 K'同构.

定理 15.7.3(e)的证明($\mathbf{F}_q$ 的子域) 令 $q=p^r$ 和 $q'=p^k$. 则$[\mathbf{F}_q:\mathbf{F}_p]=r$ 且$[\mathbf{F}_{q'}:\mathbf{F}_p]=k$. 只有 k 整除 r 才有 $\mathbf{F}_p\subset\mathbf{F}_{q'}\subset\mathbf{F}_q$. 假设 k 整除 r，比如 $r=ks$. 将 $y=p^k$ 代入方程$y^s-1=(y-1)(y^{s-1}+\cdots+y+1)$表明 $q'-1$ 整除 $q-1$. 由于乘法群 $K^\times$ 是 $q-1$ 阶循环群且 $q'-1$ 整除 $q-1$，故 $K^\times$ 包含一个阶为 $q'-1$ 的元素 β. 这个元素的 $q'-1$ 次方幂是 $x^{(q'-1)}-1$ 在 K 中的根. 因此 $x^{q'}-x$ 在 K 上完全分裂. 引理 15.7.11 表明这些根形成阶为 q'的域. ■

定理 15.7.3(b)的证明(x^q-x 的既约因子) 令 g 是 F 上的 k 次既约多项式. 多项式 x^q-x 在 K 上分解为线性因子是因为该多项式在 K 上有 q 个根. 如果 g 整除 x^q-x，则 g 也分解为线性因子，故在 K 上有一个根 β. β 在 F 上的次数整除$[K:F]=r$，且等于 k. 故 k 整除 r. 反之，假设 k 整除 r. 令 β 是 g 在 F 的扩域上的一个根. 则$[F(\beta):F]=k$，且由(e)，K 包含一个同构于 $F(\beta)$的子域. 因此 g 在 K 上有一个根，故 g 整除 x^q-x.

这就完成了定理 15.7.3 的证明. ■

第八节 本 原 元

令 K 是域 F 的一个扩域. 一个元素 α 如果它生成扩域 K/F，即 $K=F(\alpha)$，则称该元素为该扩域的本原元. 本原元很有用，因为如果 α 在 F 上的既约多项式已知，那么在 $F(\alpha)$上的运算会很容易进行.

【15.8.1】定理(本原元定理) 特征为零的域 F 的任何有限扩域 K 包含本原元. 462

这个命题当 F 是有限域的时候也是成立的，只是证明不同. 对于特征 $p\neq 0$ 的无限域，定理需要更多的假设条件. 由于我们不研究这样的域，因此不考虑这种情况.

本原元定理的证明 由于扩域 K/F 是有限扩域，故 K 由有限集合生成. 例如，K 作为

F-向量空间的一组基就在 F 上生成 K. 设 $K=F(\alpha_1, \cdots, \alpha_k)$. 我们对于 k 应用归纳法. 当 $k=1$时, 无需证明. 假设 $k>1$, 归纳假设定理对于域 $K_1=F(\alpha_1, \cdots, \alpha_{k-1})$成立, 该域 K_1 由前 $k-1$ 个元素 α_i 生成. 故我们可以假设 K_1 由单个元素 β 生成. 所以 K 由两个元素 α_k 和 β 生成. 定理的证明于是简化为 K 由两个元素生成的情形. 下面的引理解决这种情形. ■

【15.8.2】引理 令 F 是特征为零的域, 令 K 是由两个元素 α 和 β 在 F 上生成的扩域. 除去 F 中有限多个 c 之外, $\gamma=\beta+c\alpha$ 是 K 在 F 上的本原元.

证明 令 $f(x)$和 $g(x)$分别是 α 和 β 在 F 上的既约多项式, 且令$\mathcal{K}$是使得 $f(x)$和 $g(x)$完全分裂的 K 的扩域. 记它们的根分别为 $\alpha_1, \cdots, \alpha_m$ 和 $\beta_1, \cdots, \beta_n$, 其中 $\alpha=\alpha_1$, $\beta=\beta_1$.

由于特征为零, 故根 α_i 互不相同, β_j 也互不相同(15.6.8)(b). 令 $\gamma_{ij}=\beta_j+c\alpha_i$, 其中 $i=1, \cdots, m$, $j=1, \cdots, n$. 当$(i, j)\neq(k, \ell)$时, 方程 $\gamma_{ij}=\gamma_{k\ell}$至多对于某一个 c 成立. 所以除去 F 中有限多个 c 之外, γ_{ij}是不同的. 我们将证明如果 c 绕过这些"坏"值, 则 $\gamma_{11}=\beta_1+c\alpha_1$ 将是本原元. 我们省略下标, 记作 $\gamma=\beta_1+c\alpha_1$.

令 $L=F(\gamma)$. 为了证明 γ 是本原元, 只要证明 $\alpha_1\in L$ 即可. 这样, $\beta_1=\gamma-c\alpha_1$ 也属于 L. 因此, $L=K$. 首先, α_1 是 $f(x)$的根. 技巧是用 g 构造出一个以 α_1 为根的另一个多项式, 即 $h(x)=g(\gamma-cx)$. 这个多项式的系数不属于 F, 但由于 $g\in F[x]$, 故 $c\in F$ 和 $\gamma\in L$, g 的系数属于 L.

我们考察 f 和 h 的最大公因子 d. 它们的公因子无论在 $L[x]$还是在扩域$\mathcal{K}[x]$(15.6.4)上都是一样的. 由于在$\mathcal{K}$上 $f(x)=(x-\alpha_1)\cdots(x-\alpha_m)$, 故 d 是整除 h 的那些因子$(x-\alpha_i)$之积, 即 α_i 是 h 和 f 的公共根. 一个公共根为 α_1. 如果我们证明了这是唯一的公共根, 那么将得到 $d=x-\alpha_1$, 且因为最大公因子是 $L[x]$中的一个元素(15.6.4)(d), 故 $\alpha_1\in L$.

所以我们必须做的就是检验 α_i 在 $i>1$ 时不是 h 的根. 作替换: $h(\alpha_i)=g(\gamma-c\alpha_i)$. g 的根为 $\beta_1, \cdots, \beta_n$, 故必须检验 $\gamma-c\alpha_i\neq\beta_j$ 对于任意 j 成立, 或者 $\beta_1+c\alpha_1\neq\beta_j+c\alpha_i$. 这是成立的因为 c 已经被选取使得所有 γ_{ij}互不相同. ■

第九节 函 数 域

本节我们看一下函数域, 即本章开始提到的第三类扩域. 将关于变量 t 的有理函数域 463 $\mathbf{C}(t)$记为 F. 它的元素是复多项式的分式 p/q, 其中 $p, q\in\mathbf{C}(t)$, $q\neq0$. 函数域是 F 的有限扩域.

令 α 是次数为 n 的 F 的有限扩域 K 的本原元, 且令 f 是 α 在 F 上的既约多项式, 使得 $K=F(\alpha)$同构于域 $F[x]/(f)$, 其中 α 对应着 x 的剩余. 通过去分母, 我们把 f 变成本原多项式, 写成关于 x 的多项式:

【15.9.1】
$$f(t,x)=a_n(t)x^n+\cdots+a_1(t)x+a_0(t)$$

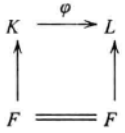
假设 f 是本原多项式意味着系数 $a_i(t)$是关于 t 的多项式, 其最大公因子是 1, 且 $a_n(t)$是首一的(12.3.9). 这样的多项式的黎曼曲面 X 在第十一章第九节中给出了定义, 作为零点$\{f=0\}$在复(t, x)-空间 $\mathbf{C}^2$ 中的轨迹. 已经证明 X 是复 t-平面 T 的一个 n-叶分支覆盖

(11.9.16). 分支点是 T 的点 $t=t_0$，在该点单变量多项式 $f(t_0, x)$ 有少于 n 个的根，这种情况发生在 $f(t_0, x)$ 有重根的情形，或当 t_0 是 f 的首项系数 $a_n(t)$ 的根(11.9.17)的情形.

和以前一样，用 X' 表示从 X 中删掉一个未指定的有限子集得到的集合，我们不说除去 X 的某个有限子集外某个论断是成立的，而是说这个论断在集合 X' 上是成立的.

F 的两个扩域 K 和 L 的同构在(15.2.9)中已经定义. 它是一个在 F 上恒等的域的同构 $\varphi: K \to L$：

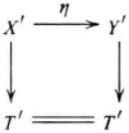
【15.9.2】图



图中竖直箭头表示 F 作为 K 和 L 的子域的包含映射，长的等号代表恒等映射.

注 T 的分支覆盖 X 和 Y 的同构是一个连续的双射 $\eta: X' \to Y'$，它与这些曲面到 T 的投射是相容的：

【15.9.3】图



斜撇表示我们希望在 X 和 Y 中去掉点的有限子集以便映射 η 被定义且为双射.

说得更宽泛一点，我们称一个分支覆盖 $\pi: X \to T$ 是路连通的，如果 X' 是路连通的，即对于 X 的任何有限子集 Δ，集合 $X-\Delta$ 是路连通的.

本节的目的是解释下面的定理，该定理用它们的黎曼曲面描述了函数域. 464

【15.9.4】**定理**(黎曼存在定理) 在 F 上 n 次函数域的同构类和 T 的连通 n-叶分支覆盖之间存在双射对应，使得由既约多项式 $f(t, x)$ 定义的扩域 K 的类对应着黎曼曲面 X 的类.

这个定理给我们提供了确定两个关于 x 的同次数的多项式定义同构的扩域的方法. 常用的一个简单的判别法就是它们的黎曼曲面的分支点必须匹配. 然而，这个定理并没有告诉我们如何求具有作为黎曼曲面的给定的分支覆盖的多项式. 这个定理做不到这一点. 许多多项式定义了同构的扩域，当有多种选择时，求这些多项式是困难的.

定理的证明太长因而在此省略，但有一部分是很容易验证的：

【15.9.5】**命题** 令 $f(t, x)$ 和 $g(t, y)$ 分别是 $\mathbf{C}[t, x]$ 和 $\mathbf{C}[t, y]$ 中的既约多项式. 令 $K=F[x]/(f)$ 和 $L=F[y]/(g)$ 是它们定义的扩域，令 X 和 Y 是黎曼曲面 $\{f=0\}$ 和 $\{g=0\}$. 如果 K/F 和 L/F 是同构的扩域，则 X 和 Y 是 T 的同构的分支覆盖.

证明 y 在 $L=F[y]/(g)$ 中的剩余类(记作 β)是 g 的根，亦即 $g(t, \beta)=0$，且一个 F-同构 $\varphi: K \to L$ 给出了 g 在 K 中的一个根，即 $\gamma=\varphi^{-1}(\beta)$. 故 $g(t, \gamma)=0$. 就像 $K=F[x]/(f)$ 里的元素一样，γ 可表示为 $F[x]$ 里的元素模 (f) 的剩余. 令 u 是这样的元素，我们用 $\eta(t, x)=(t, u(t, x))$ 定义同构 $\eta: X \to Y$.