现代数学基础丛书 166

交换代数与同调代数

（第二版）

李克正 著

科学出版社

I 环与模

1. 环与代数

一个 (结合) 环是一个具有两种运算 (加法和乘法) 的集合 R, 按加法为阿贝尔群, 满足如下条件 (其中 r, r', r'' 为 R 的任意元):

i) $(r'+r'')r = r'r + r''r$, $r(r'+r'') = rr' + rr''$ (分配律);

ii) $(rr')r'' = r(r'r'')$ (乘法结合律)。

环 R 称作交换的, 如果它还满足交换律

iii) $rr' = r'r$。

称为有单位元的, 如果存在单位元 $1 \in R$, 使得

iv) $|r = r| = r$。

(显然此时单位元是唯一的。)

例如, 体都是有单位元的环, 域都是交换环。有理数域 $\mathbb{Q}$, 实数域 $\mathbb{R}$ 和复数域 $\mathbb{C}$ 之间有包含关系 $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$。一般地, 若环 R 的非空子集 R' 在减法和乘法下封闭, 则 R' 称为 R 的一个子环, 而称 R 为 R' 的扩环; 此时对任意子集 $S \subset R'$ 可以定义 S 在 R 上生成的扩环 $R[S] \subset R'$, 即 R (在 R' 中) 的包含 S 的最小扩环 (参看习题 I.4)。

例 1.1. i) 整数环 $\mathbb{Z}$ 的子环 $2\mathbb{Z}$ 没有单位元。

ii) 任一集合 S 上的所有实值函数全体按加法和乘法组成一个有单位元的交换环。

iii) 对两个环 R 与 R' 可以定义直积 $R \times R'$ (加法和乘法按分量)。

iv) 对任一正整数 n, $R = \mathbb{Z}/n\mathbb{Z}$ 是一个有限的有单位元的交换环。特别地, 对任意素数 p, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 为一个有限域。若 n 非素数, 例如 $n = 18$, 则在 R 中有两个非零元 $\bar{2}$ 和 $\bar{9}$ 的积是 0, 此外有 $\bar{6}^2 = 0$。

两个环之间的一个映射 $f : R \to R'$ 称作 (环) 同态, 如果它与加法和乘法交换, 即 $f(r+r') = f(r) + f(r')$, $f(rr') = f(r)f(r')$ (若我们讨论有单位元的环, 则我们还要求 $f(1) = 1$)。此时 R' 连同 f 称作一个 R-代数。若 f 还是一一映射, 则说 f

是 (环) 同构。与群论类似, 我们可以定义自同态、自同构、单同态、满同态等。设 $g: R \to R''$ 是另一个环同态 (因而 R'' 也是 R-代数), 一个环同态 $\phi: R' \to R''$ 称作一个 R-代数同态, 如果 $\phi \circ f = g$。

例 1.2. i) 对任一环 R 可以定义 R 上的 $n \times n$ 矩阵代数 $M_n(R)$, 当 $R = \mathbb{R}$, $n > 1$ 时这是一个典型的非交换环。

ii) 对任一环 R 可以定义 R 上的多项式代数 $R[x]$, 它由所有以 R 的元为系数的多项式组成。若 R 是交换的, 则 $R[x]$ 也是交换的。还可以定义多个变元的多项式环。次数、常数项、首一多项式、不可约多项式、零点等术语都可以用于 $R[x]$。用归纳法我们可以在 R 上建立多个变元的多项式代数。

iii) 定义一个 (非交换) $\mathbb{R}$-代数 Q 如下: 作为 $\mathbb{R}$-线性空间, Q 具有基 $\{1, i, j, k\}$, 且 $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$。Q 称作 $\mathbb{R}$ 上的四元数代数。不难验证 Q 是一个体 (习题 2.i))。

对任一 R-代数 R' 及任一元 $a \in R'$, 存在唯一的 R-代数同态 $f: R[x] \to R'$ 使得 $f(x) = a$。这称作多项式代数的泛性。

例 1.3. 在交换环 R 上可以 (用拉普拉斯展开式) 定义行列式。设 $A = (a_{ij})$ 为 R 上的 $n \times n$-矩阵 ($n > 1$), A_{ij} 为 A 的 (i, j)-代数余子式, 则 $\det(A_{ij}) = (\det A)^{n-1}$。证明很简单: 若 $R = \mathbb{Z}$ 而 $a_{ij} = x_{ij}$ 为独立变元, 这是线性代数中熟知的恒等式; 任意 R 都是 $\mathbb{Z}$-代数, 由多元多项式代数的泛性, 存在 $\mathbb{Z}$-代数同态 $f: \mathbb{Z}[x_{ij} | 1 \leqslant i, j \leqslant n] \to R$ 使得 $f(x_{ij}) = a_{ij}$ $(1 \leqslant i, j \leqslant n)$, 这就给出 R 中的等式

$$\det(A_{ij}) = (\det A)^{n-1}$$

设 R 为有单位元的交换环, $a \in R$。若存在 $b \in R$ 使得 $ab = 1$, 则称 a 为 R 的单位; 若 $a \neq 0$ 且存在非零元 $b \in R$ 使 $ab = 0$, 则称 a 为 R 的零因子; 特别地, 若 $a \neq 0$ 但存在正整数 n 使 $a^n = 0$, 则称 a 是幂零的 (参看例 1.1.iv)。若 R 中没有零因子且 $1 \neq 0$, 则称 R 为整环。此时我们可以把 R 按如下方法嵌入一个域 K。在集合 $R \times (R - \{0\})$ 中定义一个关系 $\sim$: $(r, s) \sim (r', s')$ 当且仅当 $rs' = sr'$, 易见 $\sim$ 是一个等价关系。令 $K = R \times (R - \{0\}) / \sim$, 则不难验证 R 的环结构诱导 K 的一个域结构, 而 $r \mapsto (r, 1)$ 将 R 等同于 K 的一个子环, 使得 K 的元都是 R 中元的商。我们称 K 为 R 的商域, 记为 $K = \text{q.f.}(R)$。

2. 理想

设 $f: R \to R'$ 为环同态, 则 f 的核 $I = \ker(f) = \{a \in R | f(a) = 0\}$ 为 R 的加法子群, 且满足

(*) 对任意 $r \in R, a \in I$ 都有 $ar, ra \in I$。

满足 $(*)$ 的加法子群 $I \subset R$ 称为 R 的**理想**。(更一般地, 若对任意 $r \in R, a \in I$ 都有 $ra \in I$, 则称 I 为**左理想**, 类似地可以定义**右理想**。)

设 I 为环 R 的理想, 则易见加法商群 R/I 具有诱导的环结构 ($a+I$ 与 $b+I$ 的积为 $ab+I$), 称作 R 模 I 的**剩余类环**。投射 $p: R \to R/I$ ($p(r) = r+I$) 是环的满同态 (从而可以将 R/I 看作一个 R-代数), 且显然 $\ker(p) = I$。若 I 是同态 $f: R \to R'$ 的核, 则 f 诱导一个单同态 $R/I \hookrightarrow R'$。

以下设 R 为有单位元的交换环。若 I, J 为 R 的理想, 则 $I+J, IJ, I \cap J$ 和 $(I:J) = \{a \in R | aJ \subset I\}$ 都是 R 的理想。包含一个子集 $S \subset R$ 的所有理想的交是一个理想, 称作 S **生成的理想**, 记作 (S)。作为一个加法群, (S) 由所有 rs ($r \in R, s \in S$) 生成。

一个理想 $P \subsetneq R$ 称作**素理想**, 如果 R/P 是整环; 称作**极大理想**, 如果 R 中除 R 和 P 外没有包含 P 的理想。易见一个理想 I 是极大的当且仅当 R/I 只有两个理想 R/I 与 0, 换言之 R/I 是域。故极大理想都是素理想。记 $\mathrm{Spec}(R)$ 为 R 中素理想全体的集合, 称为 R 的**谱**。若 A 也是有单位元的交换环且 $f: R \to A$ 为同态, 则对任意理想 $I \subset A$, $f^{-1}(I)$ 为 R 的理想, 且 f 诱导单射同态 $R/f^{-1}(I) \hookrightarrow A/I$; 特别地, 若 I 为素理想, 则 $R/f^{-1}(I)$ 是整环 (因为它同构于整环 A/I 的子环), 即 $f^{-1}(I)$ 为素理想, 故 f 诱导映射

$$\hat{f}: \mathrm{Spec}(A) \to \mathrm{Spec}(R)$$

$$P \mapsto f^{-1}(P)$$

若 $a \in R$ 不是单位, 则由佐恩引理存在极大理想包含 a。

一个元 $a \in R$ 称为**素的**, 如果 (a) 是素理想。若 R 为整环且每个非零非单位元都能分解成素元素的积, 则称 R 为**唯一因子分解整环** (简称 UFD)。若 R 是整环且每个理想都是由一个元素生成的, 则称 R 为**主理想环** (简称 PID), 例如 $\mathbb{Z}$ 和任一域 K 上的多项式环 $K[x]$ 都是主理想环。任一 PID 都是 UFD (见习题 III.1)。

以下引理的一个直接推论是 $\mathbb{Z}$ 或任意域上任意多个变元的多项式代数为 UFD。

引理 2.1. (高斯定理) 若 R 为 UFD, 则 $R[x]$ 亦然。

证. 令 $K = \mathrm{q.f.}(R)$, 则 $R[x]$ 可以看作 $K[x]$ 的子环。我们先来证明, $R[x]$ 中的素元为所有 R 中的素元及所有在 $K[x]$ 中不可约的多项式, 其系数的最大公因子为 1。

若 $a \in R$, 则 $R[x]/aR[x] \cong R/aR[x]$, 故 a 在 $R[x]$ 中是素的当且仅当它在 R 中是素的。设 $f \in R[x]$ 是素的且次数 > 0。易见 f 的系数不能有公共素因子; 若 f 在 $K[x]$ 中可分解, $f = gh$ ($g, h \in K[x]$, 且次数小于 f 的次数), 可取 $a, b \in R - \{0\}$ 使得 $ag, bh \in R[x]$, 从而在 $R[x]$ 中有 $abf = ag \cdot bh$, 而因 f 是素的, ag 或 bh 在 (f)

中, 这是不可能的。反之, 若 f 在 $K[x]$ 中不可约且其系数的最大公因子为 1, 则对任意 $g,h\in R[x]$ 使得 $gh\in(f)$, g,h 中必有一个在 $K[x]$ 中能被 f 整除, 不妨设 (在 $K[x]$ 中) $f|g$。于是存在 $a\in R-\{0\}$ 及 $g_1\in R[x]$ 使得 $ag=fg_1$。由于 f 的系数的最大公因子为 1, a 的任一素因子必为 g_1 的系数的公因子, 故由归纳法可将 a 约化为 1, 即 $g\in(f)$。因而 f 是素的。

对于 $R[x]$ 中的任一元 f, 先将它在 $K[x]$ 中分解成不可约多项式的积, 从而有 $af=bf_1\cdots f_r$, 其中 $a,b\in R-\{0\}$ 而 $f_1,\cdots,f_r\in R[x]$ 为次数 >0 的素元。不难得到 $a|b$, 从而 f 可以分解成素因子的积。证毕。

3. 模

一个环 R 上的模 (或称为一个 R-模) 是一个阿贝尔加群 M, 带有一个 R 的作用, 即一个映射

$$\begin{aligned} R\times M&\to M\\ (r,m)&\mapsto rm \end{aligned}$$

满足下述条件:

i) $(r+r')m=rm+r'm$, $r(m+m')=rm+rm'$ (分配律);

ii) $(rr')m=r(r'm)$;

若讨论有单位元的环, 则我们还要求

iii) $1m=m$。

可以将 R-模 M 看作一个带有算子区 R 的阿贝尔加法群*, 由此就不难定义 R-子模 (在没有疑问时简称子模) 和商模、R-模的 R-同态 (在没有疑问时简称同态) 与同构、R-模的直和与直积等, 并可应用群论的同构定理等。任意多个 R (作为 R-模) 的拷贝的一个直和称为一个**自由** R-模, n 个 R 的拷贝的直和记为 $R^{\oplus n}$, n 称为它的**秩**。

注 3.1. 若 R 不是交换环, 我们常把上面定义的模称为 R-**左模**, 而若在定义中将 ii) 改为 $(rr')m=r'(rm)$, 则所定义的模称为 R-**右模** (此时常将 rm 改记为 mr)。例如 R 中的左理想为左模而右理想为右模。

例 3.1. i) 任一理想 $I\subset R$ 可以看作 R-模。

ii) 任意 R-代数 A 具有 R-模结构, 而且任意 A-模也可以看作 R-模。特别地, 对任意理想 $I\subset R$, R/I 为 R-模。

iii) 设 M,N 为 R-模, 记 $Hom_R(M,N)$ 为所有从 M 到 N 的 R-同态的集合, 则 $Hom_R(M,N)$ 具有阿贝尔加群结构; 而当 R 为交换环时 $Hom_R(M,N)$ 具有 R-模

* 不了解带算子的群的读者可参看附录 A。

结构 (对 $r \in R$, $f \in Hom_R(M,N)$, $m \in M$, 令 $(rf)(m) = rf(m)$), $End_R(M) = Hom_R(M,M)$ 具有 R-代数结构 (这是例 1.2.i) 的推广)。

注意有限多个 R-模的直和与直积是同构的, 但无穷多个 R-模则不然, 例如可数多个 R-模 $M_1, M_2, \cdots$ 的直积为序列的集合 $M = \prod_i M_i = \{(a_1, a_2, \cdots) | a_i \in M_i \ \forall i\}$, 而它们的直和 $\bigoplus_i M_i$ 为 M 中所有只有有限多个非零分量的序列组成的子集。像这样给出结构的定义称作 "内在的" 定义。我们可以给直和与直积以 "外在的" (即通过与其他 R-模的关系) 定义如下。设 $\mathfrak{M} = \{M_i | i \in I\}$ 为一族 R-模, 其中 I 为指标集, 则 $\mathfrak{M}$ 中模的直和是一个 R-模 M, 带有同态 $f_i : M_i \to M$ $(i \in I)$, 使得对任一 R-模 M' 及任意同态 $f_i' : M_i \to M'$ $(i \in I)$, 存在唯一的同态 $\phi : M \to M'$ 使得 $f_i' = \phi \circ f_i$ $(i \in I)$; 而 $\mathfrak{M}$ 中模的直积是一个 R-模 N, 带有同态 $g_i : N \to M_i$ $(i \in I)$, 使得对任一 R-模 N' 及任意同态 $g_i' : N' \to M_i$ $(i \in I)$, 存在唯一的同态 $\psi : N' \to N$ 使得 $g_i' = g_i \circ \psi$ $(i \in I)$。这些分别是直和与直积的 "泛性"。

设 $f : M \to N$ 为 R-模同态, 则其核 $K = \ker(f) = \{m \in M | f(m) = 0\}$ 也具有泛性: 令 $i : K \to M$ 为包含映射, 对任意 R-模 K' 及任意同态 $g : K' \to M$, 若 $f \circ g = 0$, 则存在唯一同态 $\phi : K' \to K$ 使得 $g = i \circ \phi$。这也给出核的外在定义。我们有一串同态

$$0 \to K \xrightarrow{i} M \xrightarrow{f} N$$

其中 i 是单射且 $\ker(f) = \mathrm{im}(i)$, 这样的一串同态称作一个*左正合列*。类似地, 称 $C = N/f(M)$ 为 f 的*余核*, 我们有*右正合列* $M \to N \to C \to 0$, 且余核也有泛性, 可用作外在定义。

更一般地, 一串 R-模同态

$$\cdots \xrightarrow{f_{n-2}} M_{n-1} \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \xrightarrow{f_{n+1}} \cdots$$

称作一个*复形*, 如果对所有 n 都有 $f_n \circ f_{n-1} = 0$; 称作一个*正合列*, 如果对所有 n 都有 $\ker(f_n) = \mathrm{im}(f_{n-1})$。一个正合列 $0 \to M' \to M \to M'' \to 0$ 称作一个*短正合列*, 它相当于 M' 是 M 的子模且 $M'' \cong M/M'$。

若

$$0 \to N' \xrightarrow{f} N \xrightarrow{g} N'' \tag{1}$$

是一个左正合列, 则对任一 R-模 M 有 (阿贝尔群的) 左正合列

$$0 \to Hom_R(M,N') \xrightarrow{f_*} Hom_R(M,N) \xrightarrow{g_*} Hom_R(M,N'') \tag{2}$$

其中 f_* 的定义为 $f_*(\phi) = f \circ \phi$, g_* 的定义类似。理由很简单: 因为 f (或者说 N') 是 g 的核, 由核的泛性, 对任一 $\psi \in Hom_R(M,N)$, 若 $g \circ \psi = g_*(\psi) = 0$, 则存在唯

一的 $\phi \in Hom_R(M, N')$ 使得 $\psi = f \circ \phi = f_*(\phi)$, 这 (由内在定义) 正好说明 f_* 是 g_* 的核, 或者说 (2) 是左正合的。实际上我们说明了, (1) 是左正合当且仅当对任意 R-模 M, (2) 是 (阿贝尔加群的) 左正合列。

像这样的论证几乎是同义反复, 它只是把定义换个说法而已。我们把这样的论证称作**抽象废话**。最典型的抽象废话是外在定义的唯一性, 例如对 R-模的一个 R-同态 $f: M \to N$, 若 $i: K \to M$ 和 $i': K' \to M$ 都是 f 的外在意义下的核 (即满足泛性), 则存在唯一的 R-同构 $\phi: K' \to K$ 使得 $i' = i \circ \phi$。

类似地, 若

$$N' \xrightarrow{f} N \xrightarrow{g} N'' \to 0 \tag{3}$$

是一列 R-模同态, 则由抽象废话, (3) 是右正合当且仅当对任一 R-模 M, 下列 (阿贝尔群的) 同态列为左正合

$$0 \to Hom_R(N'', M) \xrightarrow{g^*} Hom_R(N, M) \xrightarrow{f^*} Hom_R(N', M) \tag{4}$$

其中 $f^*(\phi) = \phi \circ f$, 等等。总而言之有如下结论.

引理 3.1. 一个 R-模同态列 (1) 是左正合的当且仅当对任意 R-模 M, (2) 是 (阿贝尔群的) 左正合列。类似地, 一个 R-模同态列 (3) 是右正合的当且仅当对任意 R-模 M, (4) 是 (阿贝尔群的) 左正合列。

注意即使在 (1) 中 g 是满射, (2) 中的 g_* 也未必是满射。具体地说, 一个 R-同态 $\phi: M \to N''$ 未必能提升成 M 到 N 的同态。例如当 $R = \mathbb{Z}$, g 为投射 $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ 时, $\phi = \mathrm{id}: \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ 就不能提升成 $\mathbb{Z}/2\mathbb{Z}$ 到 $\mathbb{Z}$ 的同态。但如果 M 是自由模 (例如 $M = R^{\oplus n}$), 则当 g 为满射时 g_* 必为满射 (注意 $Hom_R(M, N) \cong N^{\oplus n}$, 在一般情形 g_* 等于一些 g 的拷贝的直积)。更一般地, 一个 R-模 M 称为**投射的**, 如果对任意满同态 $g: N \to N''$, 诱导的 (阿贝尔群) 同态 $g_*: Hom_R(M, N) \to Hom_R(M, N'')$ 都是满射。不难验证一个 R-模 M 是投射模当且仅当存在 R-模 M' 使得 $M \oplus M'$ 同构于一个自由模: 若 $F = M \oplus M'$ 是自由模, 则对任一满同态 $g: N \to N''$ 有 $Hom_R(F, N) \twoheadrightarrow Hom_R(F, N'')$, 故由

$$Hom_R(F, N) \cong Hom_R(M, N) \oplus Hom_R(M', N)$$

易见 $Hom_R(M, N) \twoheadrightarrow Hom_R(M, N'')$; 反之, 若 M 是投射模, 取自由模 F 使得存在满同态 $g: F \twoheadrightarrow M$, 则由投射模的定义存在同态 $h: M \to F$ 使得 $g \circ h = \mathrm{id}_M$, 由此可见 $F = h(M) + \ker(g) \cong M \oplus \ker(g)$。我们将看到投射模不一定是自由的 (见例 VII.1.2)。

类似地, 即使在 (3) 中 f 是单射, (4) 中的 f^* 也未必是满射。具体地说, 一个 R-同态 $\phi: M' \to N$ 未必能扩张成 M 到 N 的同态。例如当 $R = \mathbb{Z}$, $f = 2\cdot:$

$\mathbb{Z} \to \mathbb{Z}$, ϕ 为投射 $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ 时, 不存在 $\psi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ 使得 $\phi = \psi \circ f$。一个 R-模 M 称为**内射的**, 如果对任意单同态 $f : N' \hookrightarrow N$, 诱导的 (阿贝尔群) 同态 $f^* : Hom_R(N, M) \to Hom_R(N', M)$ 都是满射。若 $R = \mathbb{Z}$, 不难验证 M 是单射模当且仅当 M 作为阿贝尔加群是可除的 (对充分性的证明需要用超限归纳法)。我们将看到对一般的 R 如何构造内射 R-模 (见例 VI.1.3)。

一个 R-模同态的图 (箭头图)

$$\begin{array}{ccc} A & \xrightarrow{e} & B \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ C & \xrightarrow{h} & D \end{array} \tag{5}$$

称为**交换的**, 如果 $g \circ e = h \circ f$。更一般地, 一个箭头图称为交换的, 如果其中每个形如 (5) 的圈都是交换的。

引理 3.2. (**蛇形引理**) 设有 R-模的交换图

$$\begin{array}{ccccccc} 0 \to & M' & \xrightarrow{g_1} & M & \xrightarrow{h_1} & M'' & \to 0 \\ & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & \\ 0 \to & N' & \xrightarrow{g_2} & N & \xrightarrow{h_2} & N'' & \to 0 \end{array} \tag{6}$$

其中的行都是正合的, 则有长正合列

$$\begin{aligned} 0 \to \ker(f') \to \ker(f) \to \ker(f'') &\xrightarrow{\delta} \operatorname{coker}(f') \\ \to \operatorname{coker}(f) \to \operatorname{coker}(f'') &\to 0 \end{aligned} \tag{7}$$

证. 将 (6) 扩大成下面的交换图

$$\begin{array}{ccccccc} 0 \to & \ker(f') & \xrightarrow{g_0} & \ker(f) & \xrightarrow{h_0} & \ker(f'') & \\ & \downarrow{\scriptstyle i'} & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i''} & \\ 0 \to & M' & \xrightarrow{g_1} & M & \xrightarrow{h_1} & M'' & \to 0 \\ & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & \\ 0 \to & N' & \xrightarrow{g_2} & N & \xrightarrow{h_2} & N'' & \to 0 \\ & \downarrow{\scriptstyle j'} & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle j''} & \\ & \operatorname{coker}(f') & \xrightarrow{g_3} & \operatorname{coker}(f) & \xrightarrow{h_3} & \operatorname{coker}(f'') & \to 0 \end{array} \tag{8}$$

其中 g_0 是这样定义的: 对任意 $m \in \ker(f')$, $f(g_1(m)) = g_2(f'(m)) = 0$, 故 $g_1(m) \in \ker(f)$, 这样 g_1 在 $\ker(f')$ 上的限制就诱导 $g_0 : \ker(f') \to \ker(f)$。$h_0, g_3$ 和 h_3 的定义类似。

设 L 为任一 R-模而 $\phi : L \to \ker(f)$ 为 R-同态使得 $h_0 \circ \phi = 0$, 则有 $h_1 \circ i \circ \phi = 0$。由于 $M' = \ker(h_1)$, 存在唯一的 $\psi' : L \to M'$ 使得 $g_1 \circ \psi' = i \circ \phi$。因为 $g_2 \circ f' \circ \psi' = f \circ g_1 \circ \psi' = f \circ i \circ \phi = 0$ 而 g_2 是单射, 有 $f' \circ \psi' = 0$, 故存在唯一的 $\psi : L \to \ker(f')$ 使得 $i' \circ \psi = \psi'$。于是

$$i \circ g_0 \circ \psi = g_1 \circ i' \circ \psi = g_1 \circ \psi' = i \circ \phi$$

由于 i 是单射, 我们有 $g_0 \circ \psi = \phi$。由核的外在定义我们有 $\ker(f') \cong \ker(h_0)$, 或者说 $0 \to \ker(f') \to \ker(f) \to \ker(f'')$ 是左正合的。类似地可以证明 $\operatorname{coker}(f') \to \operatorname{coker}(f) \to \operatorname{coker}(f'') \to 0$ 是右正合的。

现在来定义 (7) 中的 δ。设 $m \in \ker(f'')$, 则因 h_1 是满射, 存在 $m' \in M$ 使得 $h_1(m') = m$。我们有 $h_2(f(m')) = f''(h_1(m')) = f''(m) = 0$, 故 $f(m') \in N'$。令 $\delta(m) = j'(f(m'))$。我们首先验证这样定义的 $\delta(m)$ 与 m' 的选择无关: 若 $m'' \in M$ 使得 $h_1(m'') = m$, 则 $n = m' - m'' \in M'$, 故 $j'(f(n)) = 0$, $j'(f(m'')) = j'(f(m'))$。不难验证 δ 是 R-同态。此外显然 $\delta \circ h_0 = 0$。另一方面, 若 $\delta(m) = 0$, 则存在 $n \in M'$ 使得 $f'(n) = f(m')$。令 $m'' = m' - n$, 则 $h_1(m'') = m$ 且 $f(m'') = 0$, 即 $m'' \in \ker(f)$。这说明 (7) 在 $\ker(f'')$ 处是正合的。类似地可以证明 (7) 在 $\operatorname{coker}(f')$ 处正合, 因而是正合列。证毕。

上面最后一段中的论证方法称为**图跟踪** (*diagram chase*)。

习 题 I

I.1 设 $T = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$。证明存在 $\mathbb{R}$-代数同构 $T \cong \mathbb{C}$。

I.2 设 Q 为 $\mathbb{R}$ 上的四元数代数。

i) 对任一元 $\alpha = a_1 + a_2 i + a_3 j + a_4 k \in Q$ $(a_1, a_2, a_3, a_4 \in \mathbb{R})$, 令 $\bar{\alpha} = a_1 - a_2 i - a_3 j - a_4 k$ (称为 α 的**共轭元**), $|\alpha|^2 = \alpha\bar{\alpha} = \bar{\alpha}\alpha = a_1^2 + a_2^2 + a_3^2 + a_4^2$。验证对任意 $\alpha, \beta \in Q$ 有 $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$, 从而 $|\alpha\beta|^2 = |\alpha|^2 |\beta|^2$。

ii) 证明 Q 是可除环 (即体)。

iii) 设 $T = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \middle| a, b \in \mathbb{C} \right\}$, 其中 $\bar{a}$ 为 a 的复共轭。证明 T 同构于四元数环。

I.3 设 $\mathbb{R}$-代数 A 为有限秩的 (即 A 作为 $\mathbb{R}$-线性空间是有限维的)。假设对任意 $r \in \mathbb{R}$ 及 $\alpha \in A$ 有 $r\alpha = \alpha r$。若 A 无零因子, 则 A 同构于 $\mathbb{R}$, $\mathbb{C}$ 或四元数代数。按下列步骤证明这一事实。

i) 若 $\alpha \in A-\mathbb{R}$, 则 $\mathbb{R}[\alpha] \cong \mathbb{C}$。(提示: 若 $\dim_{\mathbb{R}}(\mathbb{R}[\alpha])=n$, 则 $1,\alpha,\alpha^2,\cdots,\alpha^n$ 在 $\mathbb{R}$ 上线性相关。)

ii) 若 $\alpha \in A-\mathbb{R}$ 而 $\beta \in A-\mathbb{R}[\alpha]$, 则 $\mathbb{R}[\alpha,\beta]$ 同构于四元数代数。(提示: 取 $i \in \mathbb{R}[\alpha]$ 与 $j \in \mathbb{R}[\beta]$ 使得 $i^2=j^2=-1$。证明 $ij+ji \in \mathbb{R}$, 且 $|ij+ji|<2$。设 $j'=ai+bj$, $a,b \in \mathbb{R}$. 取 a,b 使得 $j'^2=-1$ 且 $ij'=-j'i$。)

iii) 若存在 $\alpha \in A-\mathbb{R}$ 及 $\beta \in A-\mathbb{R}[\alpha]$, 则 $\mathbb{R}[\alpha,\beta]=A$。(参看 ii) 的提示。)

I.4 证明: 一个 (有单位元的) 环中的任意多个子环的交仍是子环。设 R' 为 R 的扩环, 则对任意子集 $S \subset R'$ 可以定义 S 在 R 上生成的扩环 $R[S]$ 为 R' 中包含 R 和 S 的所有环的交, 若它由所有元 $rs_1\cdots s_n$ ($r \in R, s_1,\cdots,s_n \in S$) 的有限和组成。

I.5 设 R 为有单位元的交换环, A 为 R 上的 n 阶方阵, I 为 R 上的 n 阶单位阵。令 $\chi_A(x)=\det(xI-A) \in R[x]$。证明 $\chi_A(A)=0$。(提示: 参看例 1.3。)

I.6 证明有限的整环必为域 (故其元素个数为素数的幂)。

I.7 设 I 为 $\mathbb{Z}[x]$ 中由 5 和 x^2+2 生成的理想, 证明 I 是极大的。

I.8 设 $R=\{a+bi|a,b \in \mathbb{Z}\}$, 其中 $i^2=-1$.

i) 证明对任意 $\alpha,\beta \in R$, $\beta \neq 0$, 存在 $\gamma \in R$ 使得 $|\alpha-\gamma\beta|<|\beta|$。(提示: 对于 $\alpha,\beta \in R$, $\beta \neq 0$, 令 $\dfrac{\alpha}{\beta}=a+bi$, $a,b \in \mathbb{Q}$。取 $m,n \in \mathbb{Z}$ 使得 $|a-m| \leqslant \dfrac{1}{2}$, $|b-n| \leqslant \dfrac{1}{2}$, 且令 $\gamma=m+ni$。)

ii) 证明 R 是 PID。

I.9* 设 R 为整环。一个非单位非零元 $a \in R$ 称作**不可约的** (或**不可分解的**), 如果它不等于两个非单位的积。一个非零元 $r \in R$ 称作**可唯一分解的**, 如果它可以分解为不可约元的积, 且若 $r=a_1\cdots a_m=b_1\cdots b_n$ 为这样两个分解, 则有 $m=n$, 且在适当改变 $b_1,\cdots,b_n$ 的次序后有 $a_i=b_ic_i$ ($1 \leqslant i \leqslant n$), 其中 c_i 为单位。

证明 R 为 UFD 当且仅当 R 的每个非零元都是可唯一分解的, 且此时一个元是素的当且仅当它是不可约的。

I.10 设 k 为特征 $\neq 3$ 的域。证明 $(x^2+xy+y^2+z^2)$ 是多项式环 $k[x,y,z]$ 中的素理想。

I.11 设 $0=M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} \cdots \xrightarrow{f_{n-1}} M_n=0$ 为 R-模正合列。证明:

i) 存在短正合列 $0 \to \ker(f_i) \to M_i \to \ker(f_{i+1}) \to 0$ ($0<i<n-1$)。

ii) 若 R 为体而 M_i 为 R 上的 d_i 维线性空间 ($0 \leqslant i \leqslant n$), 则 $d_0+d_2+\cdots=d_1+d_3+\cdots$。

I.12 设

$$(*)\quad 0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

为 R-模短正合列。我们说 $(*)$ **分裂**, 如果存在同构 $h: M \cong M' \oplus M''$ 使得在此等价之下 f 为到第一个因子的包含映射而 g 为到第二个因子的投射。一个 f 的**分拆**指的是一个 R-模同态 $\phi: M \to M'$ 使得 $\phi \circ f=\mathrm{id}_{M'}$; 一个 g 的**分拆**指的是一个 R-模同态 $\psi: M'' \to M$ 使得 $g \circ \psi=\mathrm{id}_{M''}$。证明

$$(*) \text{ 分裂} \Leftrightarrow f \text{ 具有分拆} \Leftrightarrow g \text{ 具有分拆}$$

I.13 证明 "5- 引理": 设 R 为环。假设有一个 R-模交换图

$$\begin{array}{ccccccccc}
M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\
\downarrow{\scriptstyle f_1} & & \cong\downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \cong\downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} \\
N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5
\end{array}$$

其中 f_2 与 f_4 为同构, f_1 为满射, 而 f_5 为单射，则 f_3 为同构。(提示: 这是蛇形引理的一个推论, 但也可直接证明。)

I.14 证明 "9-引理": 设 R 为环。假设有一个 R-模交换图

$$\begin{array}{ccccccc}
 & & & & 0 & & \\
 & & & & \downarrow & & \\
 & & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle f} \\
0 & \longrightarrow & M_4 & \longrightarrow & M_5 & \longrightarrow & M_6 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & M_7 & \xrightarrow{g} & M_8 & \longrightarrow & M_9 \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
\end{array}$$

其中的行和列都是正合的，则 f 为单射当且仅当 g 为单射。

I.15* 证明 (加强的) Schanuel 引理: 设 P, P' 为投射 R-模, $K \subset P$, $K' \subset P'$ 为子模。若有 $P/K \cong P'/K'$, 则存在 $P \oplus P'$ 的自同构 ϕ 使得 $\phi(K \oplus P') = P \oplus K'$, 特别地有 $K \oplus P' \cong P \oplus K'$。

I.16 设 k 为域, $f \in k[x, y]$ 为不可约多项式使得 $R = k[x, y]/(f)$ 是有理的, 即 q.f.$(R) \cong k(t)$(k 的纯超越扩张), 则存在 $\phi, \psi \in k(t)$ 使得 $R \cong k[\phi, \psi] \subset k(t)$。若 f 为下列多项式之一, 具体给出 ϕ, ψ:

i) $x^2 + y^2 - 1$;

ii) $y^2 - x^3 + x^2$;

iii) $x^3y - y - 1$ (或 $x^4 + x^3y - y$);

iv) $y^2 + x^2(x^2 + 1)$。

II 整 性

本章中讨论的环都是有单位元的交换环。

1. 整元与整扩张

定义 1.1. 设环 A 为环 R 的一个扩环。对任一 $a \in A$, 若存在首一多项式 $f(x) \in R[x]$ 使得 $f(a) = 0$, 则称 a 在 R 上是整的。对 A 的任一子集 S, 若 S 的所有元在 R 上都是整的, 则称 S 在 R 上是整的。

注意当 A 为整环时, 若 $a \in A$ 在 R 上是整的, 则 a 在 R 上是代数的 (即 a 在 $K = \text{q.f.}(R)$ 上是代数的)。

例 1.1. 下列事实是显然的:

i) 若 R 为域, 则 $a \in A$ 在 R 上是整的当且仅当 a 在 R 上是代数的;

ii) $R \subset A$ 在 R 上是整的;

iii) 若 R 为整环且 $a \in A$ 在 R 上是代数的, 则存在 R 中的非零元素 r 使得 ra 在 R 上是整的。

例 1.2. 设 $R = \mathbb{Z}$, $f(x) \in \mathbb{Z}[x]$ 为首一多项式, 而 $\alpha \in \mathbb{C}$ 为 $f(x)$ 的一个根, 则 α 在 $\mathbb{Z}$ 上是整的 (称作一个代数整数)。例如 $\sqrt{2}$ 和 $\dfrac{-1+\sqrt{-3}}{2}$ 是代数整数。

整性的一个判别准则是引理 1.1.

引理 1.1. 一个元素 $a \in A$ 在 R 上是整的当且仅当 A 中存在一个有限生成的 R-子模 $M \supset R$, 使得 $aM \subset M$。

证. 若 $a \in A$ 在 R 上是整的, 不妨设 $a^n + r_1 a^{n-1} + \cdots + r_n = 0$, 可令 M 为由 $1, a, a^2, \cdots, a^{n-1}$ 生成的 R-子模。显然 $aM \subset M$。

反之, 若 $M \supset R$ 为 A 中有限生成的非零 R-子模使得 $aM \subset M$, 取 M 的一组 R-生成元 $m_1, \cdots, m_n$, 则存在 $r_{ij} \in R$ $(1 \leqslant i, j \leqslant n)$ 使得

$$am_i = r_{i1}m_1 + r_{i2}m_2 + \cdots + r_{in}m_n \qquad (1 \leqslant i \leqslant n)$$

令

$$f(x)=\begin{vmatrix} x-r_{11} & -r_{12} & \cdots & -r_{1n} \\ -r_{21} & x-r_{22} & \cdots & -r_{2n} \\ \vdots & \vdots & & \vdots \\ -r_{n1} & -r_{n2} & \cdots & x-r_{nn} \end{vmatrix}$$

由线性代数 (参看例 I.1.3) 可知 $f(a)m_i=0$ $(1\leqslant i\leqslant n)$, 故 $f(a)M=0$, 特别地有 $f(a)\cdot 1=f(a)=0$。由于 f 是首一多项式, 这说明 a 在 R 上是整的。证毕。

命题 1.1. 若 $a,b\in A$ 在 R 上都是整的, 则 $a+b,ab\in A$ 在 R 上也是整的。

证. 不妨设 $f(a)=g(b)=0$, 其中 $f,g\in R[x]$ 分别为 m,n 次首一多项式。令 M 为由所有 a^ib^j $(0\leqslant i<m,0\leqslant j<n)$ 生成的 R-子模, 则显然 $aM\subset M$, $bM\subset M$。于是 $(a+b)M\subset M$, $abM\subset M$, 故由引理 1.1 知 $a+b$ 和 ab 在 R 上是整的。证毕。

推论 1.1. 设 $B=\{a\in A|a$ 在 R 上是整的 $\}$, 则 B 是 A 的子环。

我们将称 B 为 R 在 A 中的**整闭包**。若 R 是域, 则 B 是 R 在 A 中的代数闭包, 即 A 中所有在 R 上代数的元组成的子环。

推论 1.2. 若 $a\in A$ 在 R 上是整的, 则 $R[a]$ 在 R 上是整的。

命题 1.2. 设 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n\in A[x]$, 而 $a\in A$ 满足 $f(a)=0$。若 $a_1,\cdots,a_n$ 在 R 上是整的, 则 a 在 R 上是整的。

证. 令 M 为由所有 $a,a_1,\cdots,a_n$ 的单项式生成的 R-子模, 则易见 M 是有限生成的且 $aM\subset M$。故由引理 1.1 知 a 在 R 上是整的。证毕。

推论 1.3. 设 $B\supset A\supset R$ 为环扩张, 其中 A 在 R 上是整的, 则任一元 $a\in B$ 在 R 上是整的当且仅当它在 A 上是整的。特别地, 若 B 在 A 上是整的, 则它在 R 上是整的 (这称作 "整性的传递性")。

2. 整闭性

定义 2.1. 设 R 是整环, $K=\text{q.f.}(R)$。若 R 在 K 中的整闭包为 R 本身, 则称 R 是**整闭的**。

例 2.1. $\mathbb{Z}[\sqrt{-3}]$ 不是整闭的, 因为 $\dfrac{-1+\sqrt{-3}}{2}\notin\mathbb{Z}[\sqrt{-3}]$ 在 $\mathbb{Z}$ 上是整的。我们来证明 $R=\mathbb{Z}\left[\dfrac{-1+\sqrt{-3}}{2}\right]$ 是 UFD, 从而由命题 2.1 可知 R 是整闭的。

对任意 $\alpha=a+b\sqrt{-3}\in\mathbb{Q}[\sqrt{-3}]$ $(a,b\in\mathbb{Q})$, 取 $a_0,b_0\in\mathbb{Z}$ 使得 $|a-a_0|,|b-b_0|\leqslant\dfrac{1}{2}$, 则有 $|\alpha-a_0-b_0\sqrt{-3}|\leqslant 1$, 且等号仅当 $|a-a_0|=|b-b_0|=\dfrac{1}{2}$ 时成立, 而此时 $\alpha\in R$。由此可见在任何情况下都存在 $\gamma\in R$ 使得 $|\alpha-\gamma|<1$。

若 $\alpha,\beta\in R$ 且 $0<|\beta|<|\alpha|$, 则可取 $\gamma\in R$ 使得 $\left|\frac{\alpha}{\beta}-\gamma\right|<1$, 即 $|\alpha-\beta\gamma|<|\beta|$。故在 R 中可以作辗转相除法, 因而 R 中任意两个元有最大公因子, 这说明 R 是 UFD (参看习题 I.9)。

例 2.2. 设 R 为整环, $K=\text{q.f.}(R)$, R^0 为 R 在 K 中的整闭包, 则 R^0 是整闭的。更一般地, 若 $L\supset K$ 为任意域扩张, 则 R 在 L 中的整闭包 A 是整闭的 (因为任一元 $a\in L$ 在 A 上是整的当且仅当它在 R 上是整的, 即 $\in A$)。

命题 2.1. 任一 UFD 是整闭的。

证. 设 R 为 UFD, $K=\text{q.f.}(R)$。设 $a\in K$ 在 R 上是整的, 明确地说

$$a^n+c_1a^{n-1}+\cdots+c_n=0\quad(c_1,\cdots,c_n\in R)\tag{1}$$

取互素的元 $r,s\in R$ 使得 $a=\frac{r}{s}$。代入 (1) 式得

$$r^n=s(-c_1r^{n-1}-c_2r^{n-2}s-\cdots-c_ns^{n-1})\tag{2}$$

若 t 是 s 的素因子, 则由 (2) 式 $t|r^n$, 故 $t|r$, 与 r,s 互素的假设矛盾。这说明 s 是单位, 故 $a\in R$。证毕。

由此可知 PID 都是整闭的 (参看习题 III.1)。

以下我们考虑伽罗瓦理论与整性的关系。

引理 2.1. 设 R 为整环, $K=\text{q.f.}(R)$。设 L 为 K 的有限扩域, A 为 R 在 L 中的整闭包, 则

i) 对任意 $\sigma\in\text{Gal}(L/K)$, 有 $\sigma(R)=R$, $\sigma(A)=A$;

ii) 若 R 整闭, 则 A 中任一元 α 在 K 上的定义多项式 (即满足 $\phi(\alpha)=0$ 的不可约首一多项式 $\phi\in K[x]$) 在 $R[x]$ 中。

证. i) 因 σ 保持 K 的元素不变, 故 $\sigma(R)=R$。设 $\alpha\in A$, 则存在首一多项式 $f(x)\in R[x]$ 使得 $f(\alpha)=0$。由于 $\sigma f(x)=f(x)$, 有 $f(\sigma(\alpha))=0$, 故 $\sigma(\alpha)\in A$。

ii) 任取有限扩域 $L'\supset L$ 使得 $L'\supset K$ 为正规扩张。令 $G=\text{Gal}(L'/K)$, $\{\alpha_1,\cdots,\alpha_n\}$ 为 α 的 G-轨迹 (即所有 $g(\alpha)$ $(g\in G)$)。令

$$\psi(x)=\prod_{i=1}^{n}(x-\alpha_n)$$

则由伽罗瓦理论可知 $\phi(x)$ 是 $\psi(x)$ 的一个幂 (若 $\phi(x)$ 是可分的, 则 $\phi(x)=\psi(x)$, 否则 $\phi(x)=\psi(x)^{p^r}$, 其中 $p=\text{char}(K)$, $r\geqslant 0$)。由 i) 每个 α_i 在 R 上是整的, 故由命题 1.1., $\phi(x)$ 的系数都是在 R 上整的。但 $\phi(x)\in K[x]$ 且 R 在 K 中整闭, 故 $\phi(x)\in R[x]$。证毕。

推论 2.1.　设 R 为整闭整环, $K=\text{q.f.}(R)$, $f\in R[x]$ 为首一多项式, 则 f 在 $K[x]$ 中的首一因子都在 $R[x]$ 中。

证.　设 g 为 f 在 $K[x]$ 中的不可约首一因子。令 $L\supset K$ 为 f 的分裂域, α 为 g 在 L 中的一个根, 则 $f(\alpha)=0$ 说明 α 在 R 上是整的, 而 g 为 α 在 K 上的定义多项式, 故由引理 2.1.ii) 得 $g\in R[x]$。证毕。

命题 2.2.　设 $R[x]$ 为整环 R 上的多项式环, $K=\text{q.f.}(R)$, 则 $a\in K(x)$ 在 $R[x]$ 上是整的当且仅当 $a\in K[x]$ 且 a 的每个系数在 R 上是整的。特别地, 若环 R 是整闭的, 则 $R[x]$ 也是整闭的。

证.(Bourbaki)　充分性是显然的, 我们来证必要性。

设 $a\in K(x)$ 在 $R[x]$ 上是整的, 则它在 $K[x]$ 上是整的。由于 $K[x]$ 是整闭的, 我们有 $a\in K[x]$, 故可令 $a=c_0x^m+\cdots+c_m$ $(c_0,\cdots,c_m\in K)$。存在多项式 $f(y)=y^n+f_1(x)y^{n-1}+\cdots+f_n(x)\in R[x][y]$ 使得 $f(a)=0$, 取一个大于所有 $\deg(f_i)$ 的整数 N 并令 $g(y)=f(y-x^N)=y^n+g_1(x)y^{n-1}+\cdots+g_n(x)\in R[x][y]$, 则易见 $(-1)^ng_n(x)$ 为 x 的首一多项式, 而 $g(a+x^N)=0$, 由此可得一个首一多项式 $h(x)\in K[x]$ 使得 $(-1)^ng_n(x)=(a+x^N)h(x)$。令 $R'\subset K$ 为 R 的整闭包, 则由推论 2.1 可见 $a+x^N\in R'[x]$, 这说明 $c_0,\cdots,c_m$ 都是在 R 上整的。证毕。

推论 2.2.　设 $k\subset K$ 为域扩张且 k 在 K 中代数闭, 则 $k(t)$ (纯超越扩张) 在 $K(t)$ 中代数闭。

证.　设 $f(t)\in K(t)$ 在 $k(t)$ 上是代数的, 则可取 $g(t)\in k[t]$ 使得 $g(t)f(t)$ 在 $k[t]$ 上是整的, 由命题 2.2 可知 $g(t)f(t)\in K[t]$ 且系数都是在 k 上整的, 而由 k 在 K 中代数闭可见这些系数都在 k 中, 即 $g(t)f(t)\in k[t]$, 从而 $f(t)\in k(t)$。证毕。

例 2.3.　我们来证明 $R=\mathbb{Z}\left[\dfrac{1+\sqrt{5}}{2}\right]$ 是整闭的。设 $\alpha=r+s\sqrt{5}\in\mathbb{Q}[\sqrt{5}]=\text{q.f.}(R)$ $(r,s\in\mathbb{Q},s\neq0)$, 则 α 在 $\mathbb{Q}$ 上的定义多项式为

$$\begin{aligned}\phi(x)&=(x-r-s\sqrt{5})(x-r+s\sqrt{5})\\&=(x-r)^2-5s^2\\&=x^2-2rx+r^2-5s^2\end{aligned}$$

若 α 在 R 上是整的, 则 α 在 $\mathbb{Z}$ 上是整的 $\left(\text{因为 }\dfrac{1+\sqrt{5}}{2}\text{ 在 }\mathbb{Z}\text{ 上是整的}\right)$, 故 $\phi(x)\in\mathbb{Z}[x]$。由此可得 $2r\in\mathbb{Z}$, $r^2-5s^2\in\mathbb{Z}$。若 $r\in\mathbb{Z}$, 则 $5s^2\in\mathbb{Z}$, 故 $s\in\mathbb{Z}$, $\alpha\in\mathbb{Z}[\sqrt{5}]\subset R$; 若 $r\notin\mathbb{Z}$, 则 $\beta=\alpha-\dfrac{1+\sqrt{5}}{2}$ 是在 R 上整的, 由上所述 $\beta\in\mathbb{Z}[\sqrt{5}]$, 故 $\alpha\in R$。

例 2.4.　设 $f(x_1,\cdots,x_n)$ 为环 R 上 (n 个变量) 的对称多项式 (即对 $x_1,\cdots,x_n$

的任意置换 τ 都有 $\tau f = f$)。我们知道 $f \in R[\sigma_1, \cdots, \sigma_n]$, 其中 $\sigma_1, \cdots, \sigma_n$ 为 $x_1, \cdots, x_n$ 的初等对称多项式。我们用整性理论给这个事实一个证明, 这个方法的优点是不需要复杂的计算, 故可用于处理更复杂的类似问题。

先考虑 $R = \mathbb{Z}$ 的情形。令 $K = \mathbb{Q}(\sigma_1, \cdots, \sigma_n)$, $L = \mathbb{Q}(x_1, \cdots, x_n)$, 则易见 $[L : K] \leqslant n!$。任一 $x_1, \cdots, x_n$ 的置换诱导 L 的一个自同构且保持 K 的元素不变, 故 $|\mathrm{Gal}(L/K)| \geqslant n!$。由伽罗瓦理论, 可知 $[L : K] = |\mathrm{Gal}(L/K)| = n!$ 且 K 是 $\mathrm{Gal}(L/K)$ 的不变子域。于是 $f \in K$。另一方面, 这说明 $\sigma_1, \cdots, \sigma_n$ 在 $\mathbb{Q}$ 上代数无关, 故 $\mathbb{Z}[\sigma_1, \cdots, \sigma_n]$ 同构于 $\mathbb{Z}$ 上的多项式环, 因而是整闭的 (命题 2.2)。由于 $x_1, \cdots, x_n$ 都是多项式 $\phi(x) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n \in \mathbb{Z}[\sigma_1, \cdots, \sigma_n, x]$ 的零点, 故都是在 $\mathbb{Z}[\sigma_1, \cdots, \sigma_n]$ 上整的。因而 f 在 $\mathbb{Z}[\sigma_1, \cdots, \sigma_n]$ 上是整的 (命题 1.1), 故属于 $\mathbb{Z}[\sigma_1, \cdots, \sigma_n]$。

对一般的 R, 考虑 $x_1, \cdots, x_n$ 的所有单项式 $x_1^{i_1} \cdots x_n^{i_n}$ 的集合 S。对任意 $\alpha \in S$, 所有元素 $\tau\alpha$ (其中 τ 为 $x_1, \cdots, x_n$ 的一个置换) 组成 S 的一个有限子集, 称作一个**置换轨迹**。由 $R = \mathbb{Z}$ 的情形可知, 一个置换轨迹中所有元素的和等于 $\sigma_1, \cdots, \sigma_n$ 的一个整系数多项式, 称为一个**轨迹和**。若 $\alpha \in S$ 在 f 中出现 (即系数不为 0), 则 f 的对称性说明对 $x_1, \cdots, x_n$ 的任一置换 τ, $\tau\alpha$ 也在 f 中出现, 且 $\tau\alpha$ 的系数等于 α 的系数。所以 f 等于一些轨迹和在 R 上的线性组合, 故属于 $R[\sigma_1, \cdots, \sigma_n]$。

3. 理想与整扩张

一个环 R 的一个子集 S 称作**乘性子集**, 如果 S 中任两个元的积都在 S 中, 且 $1 \in S$, $0 \notin S$。利用乘性子集我们可以将商域的构造方法推广。首先在集合 $R \times S$ 中定义一个关系 $\sim$:

$(a, r) \sim (b, s)$ 当且仅当存在 $t \in S$ 使得 $t(as - br) = 0$。

不难验证 $\sim$ 是一个等价关系。记 $S^{-1}R = R \times S/\sim$, 一个元 $(a, r) \in R \times S$ 在 $S^{-1}R$ 中的象记为 $\overline{(a, r)}$。不难验证 $S^{-1}R$ 具有一个环结构, 其加法和乘法分别由 $\overline{(a, r)} + \overline{(b, s)} = \overline{(as + br, rs)}$ 及 $\overline{(a, r)} \cdot \overline{(b, s)} = \overline{(ab, rs)}$ 给出。我们称 $S^{-1}R$ 为环 R (被 S) 的**局部化**。此外, 映射

$$R \to S^{-1}R$$
$$r \mapsto \overline{(r, 1)}$$

是一个 "典范" 同态, 在这个意义上我们将 $S^{-1}R$ 看作一个 R-代数。注意 S 的元在典范同态下映到 $S^{-1}R$ 的单位。

上述定义不难推广到模, 以建立一个 R-模 M 被 S 的局部化 $S^{-1}M$, 它是一个 $S^{-1}R$-模, 也可以 (通过典范同态 $R \to S^{-1}R$) 看作一个 R-模。若 $0 \to M' \to M \to$

$M'' \to 0$ 是一个 R-模的正合列, 则不难验证其局部化 $0 \to S^{-1}M' \to S^{-1}M \to S^{-1}M'' \to 0$ 也是正合的。

例 3.1. 若 P 是 R 的一个素理想, 则 $S = R - P$ 是一个乘性子集。记 $R_P = S^{-1}R$。易见 R_P 只有一个极大理想 PR_P。具有唯一极大理想的环称作**局部环**。

设 S 是 R 的乘性子集, I 是 R 的理想, 则当 $I \cap S \neq \varnothing$ 时 $I \cdot S^{-1}R = S^{-1}R$, 而当 $I \cap S = \varnothing$ 时 $I \cdot S^{-1}R$ 是 $S^{-1}R$ 的理想。不难验证 $S^{-1}R$ 的理想都可以这样得到, 因此我们有满映射

$$\{R \text{ 中与 } S \text{ 不相交的理想 }\} \to \{S^{-1}R \text{ 中的理想 }\}$$

一般说来这个映射不一定是单射, 但不难验证它在 $\{P \in \mathrm{Spec}(R) |\ P \cap S = \varnothing\}$ 上的限制是一一对应 (其逆为典范同态诱导的映射 $\mathrm{Spec}(S^{-1}R) \to \mathrm{Spec}(R)$)。

定理 3.1. 设 R 是环 A 的子环且 A 在 R 上是整的, 则

i) (**卧上定理**, 简记为 LO) 对 R 的任一素理想 p, 存在 A 的素理想 P 卧于其上, 即 $P \cap R = p$。

ii) 若 A 的两个素理想 P, P' 均卧于 $p \subset R$ 上, 则 $P \not\subset P'$。特别地, 若 R 为局部环且 p 为 R 的极大理想, 则 A 中卧于 p 上的素理想恰为 A 的全部极大理想。

iii) (**上行定理**, 简记为 GU) 设 P 为 A 的素理想, $p \subset q$ 为 R 的素理想且 $P \cap R = p$, 则存在 A 的素理想 $Q \supset P$ 使得 $Q \cap R = q$。

iv) (**下行定理**, 简记为 GD) 设 R 为整闭整环且 R 的非零元在 A 中都不是零因子。若 P 为 A 的素理想, $p \supset q$ 为 R 的素理想且 $P \cap R = p$, 则存在 A 的素理想 $Q \subset P$ 使得 $Q \cap R = q$。

v) 若 R, A 为整闭整环且 $L = \mathrm{q.f.}(A)$ 为 $K = \mathrm{q.f.}(R)$ 的正规扩域, 则对任两个卧于 $p \subset R$ 上的素理想 P, P', 存在 $\sigma \in \mathrm{Gal}(L/K)$ 使得 $\sigma P = P'$。

证. i) 设 m 为 $A_p = (R-p)^{-1}A$ 的一个极大理想, 则 $p' = m \cap R_p \subset pR_p$。由于 A_p/m 是域且 R_p/p' 是 A_p/m 的子环, R_p/p' 的任一非零元 a 在 A_p/m 中有逆。因为 A 在 R 上是整的, 易见 A_p/m 在 R_p/p' 上是整的, 故 a^{-1} 满足一个等式 $(a^{-1})^n + c_1(a^{-1})^{n-1} + \cdots + c_n = 0$ $(c_1, \cdots, c_n \in R_p/p')$。因而 $a^{-1} = -c_1 - c_2 a - \cdots - c_n a^{n-1} \in R_p/p'$, 即 R_p/p' 是域。由此 p' 为 R_p 的极大理想, 故 $p' = pR_p$。令 P 为 m 在典范同态 $A \to A_p$ 下的原象, 则有 $P \cap R = p' \cap R = p$。

ii) 用反证法, 设 $P \subset P'$。由于 R_p/pR_p 是域而 A_p/PA_p 是 R_p/pR_p 的扩环且在 R_p/pR_p 上是整的, 对 A_p/PA_p 的任一非零元 b 存在等式 $b^n + c_1 b^{n-1} + \cdots + c_n = 0$ $(c_1, \cdots, c_n \in R_p/pR_p, c_n \neq 0)$, 故 $b^{-1} = -c_n^{-1}(b^{n-1} + c_1 b^{n-2} + \cdots + c_{n-1}) \in A_p/PA_p$。这说明 PA_p 是极大理想, 因此 $PA_p = P'A_p$, 从而 $P = P'$, 矛盾。

若 R 为局部环而 $p \subset R$ 为极大理想, 则由此可得卧于 p 上的素理想 $P \subset A$ 必