抽象代数

作者： Autin

目录

第一部分

环论

第 1 章 环

1.1 定义和例子

定义 1.1 (环)

(含幺) 环是一组资料 $(R,+,\cdot)$，其中

1. $(R,+)$ 是交换群。
2. 乘法运算 $\cdot : R\times R\to R$ 简记为 $a\cdot b=ab$，满足下述性质：对于所有的 $a,b,c\in R$
   - $a(b+c)=ab+ac,\quad (b+c)a=ba+ca$，(分配率，或曰双线性)，
   - $a(bc)=(ab)c$ (乘法结合律)；
3. 存在元素 $1\in R$，使得对于所有的 $a\in R$，皆有 $a\cdot 1=a=1\cdot a$，称为 R 的幺元。

♣

Remark

1. 除去和幺元相关的性质，得到 $(R,+,\cdot)$ 称作无幺环。
2. 定义蕴含了 $R,\cdot$ 构成幺半群，故幺元 1 唯一。
3. 练习 1.

1.2 一些特殊的环

定义 1.2 (交换环)

称环 R 是交换的，若

$$\forall a,b\in\mathbb{R},\quad ab=ba$$

♣

Remark 类似地可以定义交换的无幺环。

定义 1.3 (零因子)

设 R 是环 (或无幺环)。称 $a\in R$ 是一个零因子，若存在非零元 $b\in R$，使得 $ab=0$ 或 $ba=0$。

♣

Remark 0 总是非平凡环中的零因子 ($0\cdot 1=0, 1\neq 0$)。

定义 1.4 (整环)

无非零零因子的非平凡交换环被称为是一个整环。 ♣

命题 1.1 (消去律)

若 R 是环，$a \in R$。若 a 不是零因子，则乘法消去律对 a 成立，即

$$\forall b, c \in R \quad , \quad ab = ac \implies b = c \text{且} ba = ca \implies b = c$$

特别地，若 R 是整环，则消去律对于 R 中任一非零元成立。 ♠

Proof 当 a 不是零因子，

$$ab = ac \implies a(b - c) = 0 \implies b = c$$

□

定义 1.5 (可逆元（单位）)

设 R 是环，$a, b \in R$。称 b 是 a 的一个乘法逆，若 $ab = ba = 1_R$。

若 $a \in R$ 是（在 R 中）是乘法可逆的，则称 a 是一个可逆元（或单位）。R 中单位的全体记作 R^*。 ♣

定义 1.6 (除环和域)

若非零环 R 中的每个元素皆可逆，则称 R 为除环。交换除环称为域。 ♣

命题 1.2

若 R 是一个有限整环，则 R 是一个域。 ♠

Proof 设 R 是有限整环，$a \in R$ 是非零元（由整环的定义存在）。为了说明 a 是可逆元，令

$$r_1, \cdots, r_m$$

是 R 的所有元素，且无充分。断言

$$ar_1, \cdots, ar_m$$

也无重复地组成 R 的全体元素。事实上，由于 a 不是零因子，故 $ar_i = ar_j$ 蕴含 $r_i = r_j$。这表明上列元素无重复。又 R 最多只有 m 个元素，因此 $ar_1, \cdots, ar_m$ 就是 R 的所有元素。立即有 $ar_i = 1$ 对某个 r_i 成立，R 的交换性立即给出 $r_i a = 1$，于是 a 是可逆元。

□

Remark

- 若 R 是域，则 $R^* = R \setminus \{0\}$

第 1 章 练习

1. 设 $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$，其中 $i^2 = -1$ 。证明集合 $\mathbb{Z}[i]$ 在复数加法和乘法下构成一个无幺环。(Gauss 整环)

   Proof

   (a). 加法子群:

   任取 $a + bi, c + di \in \mathbb{Z}[i]$，其中 $a, b, c, d \in \mathbb{Z}$，我们有

   $$(a + bi) - (c + di) = (a - c) + (b - d)\, i \in \mathbb{Z}[i]$$

   因此 $(\mathbb{Z}[i], +)$ 是 $\mathbb{C}$ 的一个加法子群。

   (b). 乘法封闭:

   $$(a + bi)(c + di) = (ac - bd) + (ad + bc)\, i \in \mathbb{Z}[i]$$

   故对复数乘法封闭。

   (c). 双线性、结合律:

   继承自 $\mathbb{C}$

   综上 $\mathbb{Z}[i]$ 是一个无幺环。

   □

2. 设 R 是无幺环，若对于任意的 $a, b, c \in R$，$a \neq 0, ab = ca$ 蕴含 $b = c$。则 R 是交换的。

   Proof 任取 $a, b \in R$，注意到

   $$a(ba) = (ab)\, a$$

   由条件 $ab = ba$

   □

3. 设 R 是非平凡的有限无幺环，若 R 无非零零因子，则 R 是除环。

   Proof

   (a). 任取 $0 \neq a \in R$，由 a 不是零因子，$ax = ay \implies x = y$，因此左乘 a 是 R 上的单同态，又 R 有限，故 $aR = R$，同理 $Ra = a$。故存在 r_1, r_2，使得

   $$ar_1 = a = r_2 a$$

   我们有

   $$a(r_1 - r_2)\, a = ar_1 a - ar_2 a = a \cdot a - a \cdot a = 0$$

于是再一次由 a 不是零因子

$$a\left(r_1-r_2\right)=0,$$

进而 $r_1=r_2=:r$。

(b). 再任取 $b\in R$，由上面的讨论，存在 r'，使得

$$br'=b=r'b$$

。再由 $aR=R$ 知，存在 c，使得 $ac=b$ 。于是

$$r'b=b=ac=rac=rb$$

由 b 不是零因子 $r=r\pi$。这表明 r 是 R 中的幺元，记作 1 。

(c). 最后，根据 $aR=R=Ra$，可得存在 $d,d'\in R$，使得

$$ad=1=d'a$$

由

$$a\left(d-d'\right)a=ada-ad'a=a-a=0$$

可得 $d=d'$，因此 $ad=da=1$，这表明 a 是可逆元。

4. 设 R 是（含幺）环，a,b 是 R 中的元素。证明 $1-ab$ 可逆当且仅当 $1-ba$ 可逆。

Proof 有对称性，只证一边即可，设 $1-ab$ 可逆，则

$$\begin{aligned}\left(1-ba\right)\left(b\left(1-ab\right)^{-1}a\right)&=b\left(1-ab\right)^{-1}a-bab\left(1-ab\right)^{-1}a\\&=b\left(1-ab\right)\left(1-ab\right)^{-1}a\\&=ba\\&=1-\left(1-ba\right)\end{aligned}$$

因此

$$\left(1-ba\right)\left(1+b\left(1-ab\right)^{-1}a\right)=1$$

这表明 $1-ba$ 可逆。

□

第 2 章　环范畴

2.1　子环

定义 2.1 (子环)

设 R 是环，S 是 R 的子集。设 $0_R \in S, 1_R \in S$，并且 S 在 R 中的运算 $+$ 和运算 $\cdot$ 下封闭。称 S 是 R 一个子环，若 S 满足所有环公理，并且 $0_S = 0_R, 1_S = 1_R$。 ♣

Remark

- 对于无幺环，则无需 $1_R \in S$ 以及 $1_S = 1_R$ 。

命题 2.1 (子环判据)

设 R 是一个环，$S \subseteq R$ 是包含了 0_R 和 1_R 的子集。则 S 是 R 的子环，当且仅当它在 $+$ 和 $\cdot$ 下封闭，并且包含 S 的加法逆。 ♠

Remark 对于无幺环，不需要 $1_R \in S$。

第 2 章 练习

1. 设 $R = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$ 是环 $\mathbb{Z}_{10}$ 的子无幺环。问 R 是否有幺元？

   Remark R 在（含幺）环范畴下不是 $\mathbb{Z}_{10}$ 的子环；在无幺环范畴下是 $\mathbb{Z}_{10}$ 的子无幺环。

   Proof 注意到

   $$\overline{6} \cdot \overline{2} = \overline{12} = \overline{2}, \quad \overline{6} \cdot \overline{4} = \overline{24} = \overline{4}, \quad \overline{6} \cdot \overline{6} = \overline{36} = \overline{6}, \quad \overline{6} \cdot \overline{8} = \overline{48} = \overline{8}$$

   因此 R 有单位元 $\overline{6}$。

   □

第 3 章　标准分解，商环，同构定理

3.1　像与核

命题 3.1

设 $f:R\to S$ 是环同态。则像 $S'=\operatorname{im} f:=f(R)$ 是 S 的子环。 ♠

Remark

- 使用与下面相似的讨论可得：当 R' 是 R 的子环时，$f(R')$ 是 S 的一个子环。

Proof

因为环同态映 1 为 1，映 0 为 0，所以 $f(R)$ 同时包含 0 和 1。

为了说明 $f(R)$ 在运算下封闭，令 $s_1,s_2\in f(R)$；则 $\exists r_1,r_2\in R$，使得 $s_1=f(r_1),s_2=f(r_2)$。由于 f 保持运算，我们有

$$s_1+s_2=f(r_1)+f(r_2)=f(r_1+r_2),\quad s_1\cdot s_2=f(r_1)\cdot f(r_2)=f(r_1\cdot r_2)$$

因此 s_1+s_2 和 $s_1\cdot s_2$ 位于 $f(R)$ 中。

最后，为了说明 $f(R)$ 包含加法逆，令 $s\in f(R)$，则 $\exists r\in R$，使得 $s=f(r)$，并且

$$-s=-f(r)=f(-r)$$

因此 $-s\in f(R)$。

由命题2.1即得。

□

定义 3.1 (理想)

称环 (或无幺环) R 的一个子集 I 是一个理想，若 $(I,+)$ 是 R 的 (正规) 子群，且满足以下被称为是“吸收性”的性质

$$(\forall a\in I)(\forall r\in R),\quad ar\in I\text{且}ra\in I$$

♣

Remark

- 上面的定义也称 I 是一个双边理想；若只满足 $ar\in I$ 则称为右理想，左理想同理。

命题 3.2

环 R 的非空子集 I 是一个理想，当且仅当它在加法下封闭且满足吸收性。

Remark 对于无幺环，无法利用下面的 $-a=(-1)\cdot a\in I$

Proof 只需说明充分性。

由 I 非空，它至少存在一个元 $a\in I$，由吸收性 $0=0\cdot a\in I$。

此外，对于任意的 $a\in I$，由吸收性 $-a=(-1)\cdot a\in I$。

以下表明 I 是 R 的一个加法子群，又它满足吸收性，故 I 是 R 的一个理想。

□

命题 3.3

设 $f:R\to S$ 是一个环同态。则 $(\ker f)$ 是 R 的一个理想。

Proof 首先 $f(0)=0,0\in\ker f$，故 $\ker f$ 非空。

任取 $a,b\in\ker f$,

$$f(a+b)=f(a)+f(b)=0+0=0$$

因此 $a+b\in\ker f$, $\ker f$ 对加法封闭。

再任取 $r\in R$,

$$f(ra)=f(r)f(a)=f(r)\cdot 0=0=0\cdot f(r)=f(ar)$$

因此 $ra,ar\in\ker f$，这表明 $\ker f$ 具有吸收性，故由命题3.2, $\ker f$ 是 R 的一个理想。

□

命题 3.4

若 R 是交换环 (或无幺环)，$a\in R$，则子集

$$(a):\{ra:r\in R\}$$

是 R 的一个理想。

Remark

- 类似地有 $(a_1,\cdots,a_n)$ 是 R 的一个理想。

Proof $a\in(a)$，故 (a) 非空。取 $r_1,r_2\in R$, 则

$$r_1a-r_2a=(r_1-r_2)a\in(a)$$

故 (a) 是加法子群。

此外，任取 $b=ca$，其中 $c\in R$，我们有

$$rb=r(ca)=(rc)a\in(a)$$

这表明 R 有左吸收性。此外右 R 交换，R 也有右吸收性。

由命题3.2, (a) 是 R 的一个理想。

□

定义 3.2

设 R 是交换环，$a \in R$。则 (a) 被称为是由 a 生成的主理想。此外，对于 $a_1, \cdots, a_n \in R$, 理想 $(a_1, \cdots, a_n)$ 被称为是由 $a_1, \cdots, a_n$ 生成的理想。 ♣

3.2 商环

引理 3.1

设 I 是环 R 的理想，$a, a', b, b' \in R$, 若 $a' - a \in I, b' - b \in I$ 则

$$a' \cdot b' - a \cdot b \in I$$

♡

Proof 设 $a' - a = i, b' - b = j$，则

$$\begin{aligned} a' \cdot b' - a \cdot b &= (a + i)(b + i) - ab \\ &= ai + ib + i^2 \in I \end{aligned}$$

□

定义 3.3

设 I 是环 R 的理想，$a + I, b + I$ 是 R/I 中的元素，定义

$$(a + I) \cdot (b + I) := (a \cdot b) + I$$

♣

Remark 该定义由上述引理是良定义的。

定理 3.1

设 I 是环 R 的理想，$(R/I, +, \cdot)$ 是一个环，使得 $0_{R/I} = 0 + I = I, 1_{R/I} = 1 + I$ ♡

Proof trivial 的验证，只取一项举例：

任取陪集 $a + I$, 考虑 $(-a) + I$,

$$(a + I) + ((-a) + I) = (a - a) + I = 0 + I, \quad ((-a) + I) + (a + I) = (-a + a) + I = 0 + I$$

故加法逆存在。

□

Example 3.1 设 $R = \mathbb{Z}[x]$ 是整系数多项式环。考察 $\mathbb{Z}[x]/(x)$。

每个 $\mathbb{Z}[x]$ 中的元素写作 $f(x)=a_0+a_1x+\cdots+a_nx^n$。注意到 $a_0=f(0)$，且

$$(a_0+a_1x+\cdots+a_nx^n)-a_0=\left(a_1+a_2x+\cdots+a_nx^{n-1}\right)\cdot x\in(x)$$

因此 $f(x)-f(0)\in(x)$，有陪集的等式

$$f(x)+(x)=f(0)+(x)$$

商环 $\mathbb{Z}[x]/(x)$ 中任意的元素都有形式 $a+(x)$，其中 a 是一个整数。

另外，定义

$$\varphi:\mathbb{Z}\to\mathbb{Z}[x]/(x)$$
$$a\mapsto a+(x)$$

上面的讨论告诉我们 φ 是满射。另一方面，若 $\varphi(a)=\varphi(b)$，其中 $a,b\in\mathbb{Z}$，则

$$b+(x)=a+(x)$$

这表明 $b-a$ 写作 x 与某个元的乘积，但是 $b-a$ 是整数，只能有 $b-a=0$，故 φ 是单射。此外 φ 是环同态，首先 $\varphi(1)=1+(x)$ 是单位元，且

$$\varphi(a+b)=(a+b)+(x)=[a+(x)]+[b+(x)]=\varphi(a)+\varphi(b)$$

也可以直接证明对乘法的保持。

因此 $\mathbb{Z}[x]/(x)\simeq\mathbb{Z}$。

上面的讨论没有用到 $\mathbb{Z}$ 的特殊性质，相同的讨论完全可以得到

$$R[x]/(x)\simeq R$$

对任意的环[1] R 成立。

Example 3.2 设 R 是交换环，$r\in R$，考虑 $R[x]$ 的理想 $(x-r)$，考虑 $R[x]/(x-r)$。

令 $x=t+r$，则 $g(t):=f(t+r)$ 是 t 的多项式，则上面的例子告诉我们 $g(t)-g(0)$ 是 t 的乘积。于是

$$f(x)-f(r)\in(x-r)$$

给出陪集的等式

$$f(x)+(x-r)=f(r)+(x-r)$$

我们知道 $R[x]/(x-r)$ 中任意元素都写作 $a+(x-r),a\in R$。类似地，定义 $\varphi:R\to R[x]/(x-r)$，可以类似地验证 φ 是环同构。

因此我们有结论 $R[x]/(x-r)\simeq R$ 都与任意的交换环 R 和 $r\in R$ 成立。

Example 3.3 考虑 $\mathbb{R}[x]/(x^2+1)$，证明 $\mathbb{C}\simeq\mathbb{R}[x]/(x^2+1)$。

使用与上面两个例子类似的技巧，可以得到 $\mathbb{R}[x]/(x^2+1)$ 中的每个元素唯一地写

[1] 由于 x 与 $\mathbb{R}[x]$ 中任意元素交换，因此甚至无需假设 R 是交换的，$(x):=\{rx:r\in R\}$ 自动就是一个理想。

作

$$a+bx+\left(x^2+1\right)$$

进而由一对实数 (a,b) 决定。我们规定实数对有着与 $\mathbb{R}[x]/\left(x^2+1\right)$ 上相同的加法和乘法，那么

$$\begin{aligned}(a_1,b_1)+(a_2,b_2) &\sim \left(a_1+b_1x+\left(x^2+1\right)\right)+\left(a_2+b_2x+\left(x^2+1\right)\right)\\ &=(a_1+a_2)+(b_1+b_2)\,x+\left(x^2+1\right)\\ &\sim (a_1+a_2,b_1+b_2)\end{aligned}$$

对于乘法

$$\begin{aligned}(a_1,b_1)\cdot(a_2,b_2) &\sim \left(a_1+b_1x+\left(x^2+1\right)\right)\cdot\left(a_2+b_2x+\left(x^2+1\right)\right)\\ &=(a_1+b_1x)\cdot(a_2+b_2x)+\left(x^2+1\right)\\ &=a_1a_2+(a_1b_2+a_2b_1)\,x+b_1b_2x^2+\left(x^2+1\right)\\ &=(a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)\,x+\left(x^2+1\right)\\ &\sim (a_1a_2-b_1b_2,a_1b_2+a_2b_1)\end{aligned}$$

定义 $a+bi\mapsto a+bx+\left(x^2+1\right)$，得到 $\mathbb{C}\simeq\mathbb{R}[x]/\left(x^2+1\right)$

第 3 章 练习

1. 设 U 是环（或无么环）R 的理想，令 $r(U)=\{x\in R:\forall u\in U,xu=0\}$。证明：$r(U)$ 也是 R 的理想。

   Proof

   (a). 显然 $0\in r(U)$，故 $r(U)$ 非空。任取 $x,y\in r(U)$，

   $$(x-y)\,u=xu-y_0=0$$

   故 $x-y\in r(U)$，这表明 $r(U)$ 是加法子群。

   (b). 任取 $x\in r(U),a\in R$。由 U 是理想，对于每个 $u\in U$，$au\in U$，于是

   $$(ax)\,u=a\,(xu)=0,\quad (xa)\,u=x\,(au)=0$$

   这表明 $ax,xa\in r(U)$，故 $r(U)$ 满足吸收性。

   综上可得 $r(U)$ 是 R 的一个理想。

   □

2. 设 R 是环(或无么环)，I,J 是 R 的理想。令 $IJ=\{\sum_{k=1}^{n}a_ib_i:a_i\in I,b_i\in J,n\in\mathbb{N}\}$
   - 证明 IJ 也是环 R 的理想，且 $IJ\subseteq I\cap J$；
   - 给出 I,J，使得 $IJ\neq I\cap J$

Proof

任取 $\sum_{i=1}^{n} a_i b_i, \sum_{i=1}^{m} c_i d_i \in IJ$，则

$$\sum_{i=1}^{n} a_i b_i - \sum_{i=1}^{m} c_i d_i = \sum_{i=1}^{n} a_i b_i + \sum_{i=1}^{m} (-c_i)\, d_i \in IJ$$

故 IJ 是 R 的加法子群。

任取 $r \in R$，

$$r\left(\sum_{i=1}^{n} a_i b_i\right) = \sum_{i=1}^{n} (r a_i)\, b_i \in IJ, \qquad \left(\sum_{i=1}^{n} a_i b_i\right) \cdot r = \sum_{i=1}^{n} a_i\, (b_i r) \in IJ$$

因此 IJ 是 R 的理想。

由 I, J 是 R 的理想 $IJ \subseteq I$，$JI \subseteq J$ 由，因此 $IJ \subseteq I \cap J$ 。这就证明了第一个结论。

对于第二个结论，考虑 $R = \mathbb{Z}$，$I = (2)$，$J = (4)$ ，则 $IJ = (8)$，$I \cap J = (4)$。

□

3. 设 R 是交换环，I, J 是 R 的理想。若 $I + J = R$，证明 $IJ = I \cap J$。

Proof

由上面的练习 $IJ \subseteq I \cap J$ 。由 $I + J = R$，存在 $i \in I, j \in J$，使得 $i + j = 1_R$。于是任取 $x \in I \cap J$，

$$x = x\,(i + j) = xi + xj = ix + xj \in IJ$$

因此，$I \cap J \subseteq IJ$。

□

第 4 章　整环

4.1　素理想和极大理想

定义 4.1 (素理想和极大理想)

1. 设 R 是交换环，令 I 是 R 的理想。若商环 R/I 是整环，则称 I 是素理想。
2. 设 R 是交换环，令 I 是 R 的理想。若商环 R/I 是一个域，则称 I 是极大理想。

♣

Remark

1. 极大理想是素理想。

   Proof　域是整环。

定理 4.1 (素理想的一个等价刻画)

设 R 是交换环，令 I 是 R 的素理想。那么 I 是素理想当且仅当 $I \neq (1)$，且以下成立：

$$\forall a, b \in R \quad ab \in I \iff (a \in I) \vee (b \in I)$$

♡

Proof

1. 设 I 是素理想，则 R/I 是整环，特别地在 R/I 中 $0 \neq 1$。进而 R/I 是非平凡的环，从而 $I \neq (1)$。设 $a, b \in R$ 使得 $ab \in I$，那么 $ab+I=0$。又 $ab+I=(a+I)(b+I)$，根据整环的定义，$a+I=0$，或 $b+I=0$。这表明 $a \in I$ 或 $b \in I$。
2. 若上述条件对 I 成立。由 R 交换可得 R/I 交换。又 $I \neq (1)$，故 R/I 非平凡，因此在其中 $0 \neq 1$。设 $(a+I), (b+I)$ 是 R/I 中的元素，使得 $(a+I)(b+I)=0$，这表明 $ab+I=0$，即 $ab \in I$。有条件知 $a \in I$ 或 $b \in I$，即 $a+I=0$ 或 $b+I=0$，这说明 R/I 无非零的零因子，即 R/I 是整环。

定理 4.2 (极大理想的一个等价刻画)

设 R 是交换环，I 是 R 的理想。那么 I 是极大理想当且仅当 $I \neq (1)$ 并且不存在理想 J，使得 $I \subsetneq J \subsetneq R$。

♡

Proof

1. 设 I 是极大理想，那么 R/I 是一个域，特别地 R/I 是非平凡的环，从而 $I \neq (1)$。反证：若存在理想 J，使得 $I \subsetneq J \subsetneq R$，那么 J/I 是 R/I 的理想，并且 $(0) \subsetneq J/I \subsetneq (1)$

在 R/I 中成立。但是域中的理想只有 (0) 和 (1)（域 F 的非零理想包含可逆元，进而包含单位元，故为 (1)），故 J/I 不是一个域。

2. 反之，若条件成立。首先由于 $I \neq (1)$，R/I 不是平凡环，进而 $0 \neq 1$ 在 R/I 中成立。若 R/I 不是一个域，那么存在非平凡的理想 $\bar{J}$（若不然，任意 $a \in \bar{J}$ 成立 $1 \in (a)$，进而 a 可逆，R/I 为域），由对应定理，$\bar{J}$ 对应到（真）包含了 I 的 R 的（真）理想，故矛盾。

4.2 素元和不可约元

定义 4.2 (整除和最大公因子)

1. 设 R 是交换环，令 $a, b \in R$。称 b 整除 a，记作 $b|a$，若 $a \in (b)$，即存在 $c \in R$，使得 $a = bc$。
2. 设 R 是整环，$a, b \in R$。称 $d \in R$ 是 a 和 b 的一个最大公因子（gcd），若 (d) 是包含了 a 和 b 的最小的 R 的主理想。

♣

Remark

1. 最大公因子不一定存在。最大公因子为 1 时，1 也不一定写成 a, b 的线性组合。

定义 4.3 (不可约元)

设 R 是整环，$q \in R$。称 q 是不可约元，若 q 不是可逆元，并且

$$\forall a, b \in R \quad q = ab \implies a \text{ 是可逆元或} b \text{ 是可逆元}.$$

♣

Remark

1. $q \neq 0$。
2. 等价刻画：条件等价于 $\forall a, b \in R, \quad q = ab \implies (q) = (a)$ or $(q) = (b)$。

   Proof 若 a 是可逆元，则存在 $d \in R$，使得 $b = dq$，故 $(q) = (b)$。反之，若 $(q) = (b)$，则存在 $d \in R$，使得 $b = dq$，故 $q = adq \implies ad = 1$，从而 a 是可逆元。这表明当 $q = ab$ 时，a 可逆当且仅当 $(q) = (b)$。

定理 4.3 (不可约元的一个等价刻画)

设 R 是整环，$q \in R, q \neq 0$，且 q 不是可逆元。那么 q 是不可约的，当且仅当理想 (q) 在所有 R 的真主理想中是极大的：即 $(q) \subset (a)$ 蕴含 $(a) = (1)$ 或 $(a) = (q)$。

♡

Proof 若 q 不可约，令 $a \in R$，$(q) \subset (a)$。那么 $q = ab$ 对某个 $b \in R$ 成立。又 q 不可约，故 a 是可逆元或 b 是可逆元，对于前者 $(a) = 1$，对于后者 $(a) = (ab) = (q)$。这表

明 (q) 确实在真主理想中极大。

反之，若 $q \neq 0$，q 不是可逆元，并且具有上面的极大性条件。是 $q = ab$，那么 $(q) \subset (a)$，要么 $(a) = (1)$，要么 $(a) = (q)$，对于前者 a 是可逆元。对于后者我们有 $a = qu$ 对某个可逆元 u 成立，故 $q = qub$，得到 $ub = 1$，从而 bu 是可逆元。

命题 4.1 (非零素元不可约)

设 R 是整环，$p \in R$ 是非零素元。那么 p 不可约。 ♠

Proof 设 $p \in R$ 是非零素元，设 $(p) \subset (a)$。我们说明 $(a) = 1$ 或 $(a) = (p)$，进而 p 不可约。由 $(p) \subset (a)$，存在 $b \in R$，使得 $p = ab$。由于 p 是素元，故 $a \in (p)$ 或 $b \in (p)$。对于前者，$(a) \subset (p)$，我们有 $(a) = (p)$。对于后者，存在 $c \in R$ 使得 $b = cp$，于是 $p = acp$，得到 $ac = 1$。故 a 是可逆元，从而 $(a) = (1)$。

4.3 欧氏整环、PIDs

定义 4.4 (欧氏整环)

设 R 是整环。称 R 是一个欧氏整环，若存在函数 $\nu : R\backslash\{0\} \to \mathbb{Z}^{\geqslant 0}$，具有如下性质：对于所有 $a \in R$ 和所有非零的 $b \in R$，存在 $q, r \in R$ 使得

$$a = bq + r$$

其中要么 $r = 0$，要么 $\nu(r) < \nu(q)$，函数 ν 称为欧式赋值。 ♣

定义 4.5 (PID)

设 R 是整环。称 R 是一个主理想环（PID），若 R 的每个理想都是主理想，即对于 R 的每个理想 I，存在 $a \in R$，使得 $I = (a)$。 ♣

定理 4.4 (欧氏整环 $\Longrightarrow$ PIDs)

欧氏整环都是 PID。 ♡

Idea 理想皆由赋值最小的元素生成，具体地 I 中元素对赋值最小元 b 的余数为 0（最小性），故为 b 整除，即 $I \subset (b)$。

Proof 设 R 是欧式整环，I 是 R 的理想。不妨 $I \neq (0)$，那么令

$$S := \{\nu(s) \in \mathbb{Z}^{\geqslant 0} : s \in I, s \neq 0\}$$

于是 S 有最小元 $\nu(b)$。首先，显然有 $(b) \subset I$，接下来说明另一边。任取 $a \in I$，存在

$q, r \in R$，使得 $a = bq + r$，使得 $r = 0$ 或 $\nu(r) < \nu(b)$，我们有

$$r = a - bq \in I$$

若 $\nu(r) < \nu(b)$，则与 $\nu(b)$ 的最小性矛盾，故 $r = 0$。这表明 $a \in (b)$，a 选取的任意性给出 $I \subset (b)$。综上 $I = (b)$ 是主理想。

命题 4.2 (PID 和最大公因子)

若 R 是 PID，$a, b \in R$。> 理想 $(a, b) = (d)$ 对某个 $d \in R$ 成立，因此 (a, b) 本身就是包含了 a 和 b 的最小的主理想，即 a, b 的最大公因子。> 此外，d 是 a 和 b 的线性组合，因为 $d \in (a, b)$，而 (a, b) 就是 a, b 线性组合的全体。 ♠

Remark

1. 特别地，a, b 互素（即最大公因子为 1），当且仅当 $(a, b) = (1)$。这是 PID 中的特殊性质。

命题 4.3 (PID 中非零素理想的极大性)

设 R 是一个 PID，I 是非零素理想。那么 I 是极大理想。 ♠

Proof 设 I 是 R 的非零素理想。由于 R 是 PID，故 $I = (p)$ 对某个 $p \in R, p \neq 0$ 成立。I 是素理想，那么 p 是不可约的，进而 (p) 在 R 的所有真主理想中极大，而 R 的任意真理想都是主理想，故 (p) 在 R 的真理想中极大，即 I 是 R 的极大理想。

定理 4.5 (PID 的升链条件)

设 R 是 PID，那么 R 的任意理想升链皆稳定。即若

$$I_1 \subset I_2 \subset \cdots$$

是 R 的一个理想升链，则存在 m，使得 $I_m = I_{m+1} = \cdots$。 ♡

Proof 令 $I_1 \subset I_2 \subset \cdots$ 是一个理想升链，那么

$$I := \bigcup_{j \geqslant 1} I_j = \{r \in R : \exists j, r \in I_j\}$$

是 R 的一个理想。由 R 是 PID 知，存在 $r \in R$，使得 $I = (r)$。根据 I 的定义，存在 m，使得 $r \in I_m$，于是 $(r) \subset I_m$，这就有

$$I = (r) \subset I_m \subset I_{m+1} \subset \cdots \subset I$$

于是 $I_m = I_{m+1} = \cdots = I$。

4.4 PIDs、UFDs

命题 4.4

设 R 是 PID，$q \in R$ 是不可约元。那么 (q) 是极大理想，特别地 q 是素元。♠

Proof (q) 在所有真主理想中极大，而 PID 上任意理想皆为主理想，故 (q) 是极大理想。立即有 (q) 是素理想，即 q 是素元。

定理 4.6 (PID 上的算数学基本定理)

设 R 是 PID，$a \in R$；设 $a \neq 0$，且 a 不是可逆元。那么存在有限多个不可约元 $q_1, \cdots, q_r$，使得

$$a = q_1 \cdots q_r$$

此外，分解在相伴的意义下唯一，即若

$$a = q_1 \cdots q_r = p_1 \cdots p_s$$

是两个不可约分解，那么 $s = r$，且在一个指标重排后，$(p_1) = (q_1), \cdots, (p_r) = (q_r)$。♡

Remark PID $\Longrightarrow$ UFD

Idea

1. 利用 PID 上的升链条件，将分解翻译成主理想的包含关系。在不可约分解不存在的前提下，构造无穷严格升链。
2. 若存在元素分解不唯一，那么可以找到具有最少因子个数 r 的非唯一分解元，其中 $r \geq 2$，由此造出有 $r-1$ 个不可约因子的元，导出矛盾。主要利用 PID 上不可约元的素性。

Proof

1. 存在性：设存在 $a \in R$，$a \neq 0$，a 不可逆，且不存在不可约分解。那么特别地，a 本身是可约元。从而由定义，存在不可逆元 $a_1, b_1 \in R$ 使得 $a = a_1 b_1$。注意到 $(a) \subsetneq (a_1)$ 且 $(a) \subsetneq (b_1)$。断言 a_1, b_1 中存在可约元，否则 a 有不可约分解，矛盾，不妨设 a_1 是不可约的。对 a_1 重复上述讨论，依次类推，我们得到无穷升链

   $$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$$

   与 PID 的升链条件矛盾。
2. 唯一性：若分解不唯一，存在最小的 $r \in \mathbb{N}^+$，使得存在不可约因子，$q_1, q_2, \cdots, q_r, p_1, p_2, \cdots, p_s$ 使得

   $$a := q_1 q_2 \cdots q_r = p_1 p_2 \cdots p_s$$

是两个不同的不可约分解。断言 $r>1$，若不然 $q_1=p_1p_2\cdots p_s$，q_1 不可约迫使 $s=1$，与分解的不唯一性矛盾。接下来假设 $r\geq 2$，我们有

$$q_1q_2\cdots q_r\in(p_1)$$

而由 (p_1) 是素理想，存在某个 q_i，通过一个重排不妨设 $i=1$，使得 $(q_1)\subseteq(p_1)$，由 (q_1) 的极大性，我们得到 $(q_1)=(p_1)$，因此不妨设 $p_1=q_1$(通过乘以一个可逆元)。于是此时

$$q_1q_2\cdots q_r=q_1p_2\cdots p_s$$

又 R 是整环，由消去律可得

$$q_2\cdots q_r=p_2\cdots p_s$$

由对 r 的假设知，只能有 $s=r$，

$$(q_2)=(p_2),\cdots,(q_r)=(p_r)$$

从而 a 的分解是唯一的，矛盾。

定义 4.6

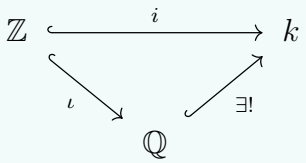
称整环 R 是一个“唯一分解整环”(UFD)，若定理 4.6 中的结论对 R 成立。即每个非零、非单位元都有在相伴意义下唯一的不可约分解 ♣

4.5 整环的分式域

先来看分式域概念提出的一个原型

命题 4.5

可以笼统地说 $\mathbb{Q}$ 是包含了 $\mathbb{Z}$ 的最小的域。意思是若 k 是包含了 $\mathbb{Z}$ 的一个域，那么 k 中存在唯一的包含了 $\mathbb{Z}$ 的 $\mathbb{Q}$ 的同构复制。可以用以下交换图表述：



♠

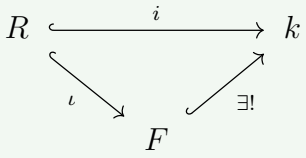
Proof 给定含入同态 $\iota:\mathbb{Z}\hookrightarrow\mathbb{Q}$，和 $i:\mathbb{Z}\to k$，任取 $\frac{p}{q}\in\mathbb{Q}$，其中 $q,p\in\mathbb{Z}$。现在考虑 $\mathbb{Q}\to k$ 的同态 φ，要是交换图成立，必然有 $\varphi(p)=i(p)$，$\varphi(q)=i(q)$，且 $\varphi\left(\frac{1}{q}\right)=(\varphi(q))^{-1}=(i(q))^{-1}$。那么 $\varphi\left(\frac{p}{q}\right)=\varphi(p)\,\varphi\left(\frac{1}{q}\right)=i(p)\,(i(q))^{-1}$ 由 p,q 唯一确定。此外，容易验证 φ 是单同态，从而 $\varphi(\mathbb{Q})\simeq\mathbb{Q}$。

4.5.1 分式域的泛性质

仿照上例，对一般的整环刻画它的分式域

定义 4.7 (分式域的泛性质)

设 R 是整环，k 是包含了 R 的一个域，若 F 使得下图成立，则称 F 为 R 的一个分式域。



Remark

1. 唯一性：上述 F 若存在，则在同构意义下唯一。

   Proof 设 F' 是另一个满足条件的域，置 $k = F'$，得到 $F \subseteq F'$，互换位置得到 $F' \subseteq F$。又存在 $F \to F'$ 的单同态，上述讨论表明此同态为同构。

4.5.2 分式域的具体构造

$\mathbb{Q}$ 的构造无非就是 $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ 上模去一个等价关系

$$(r_1, s_1) \sim (r_2, s_2) : \iff \frac{r_1}{s_1} = \frac{r_2}{s_2} \iff r_1 s_2 = r_2 s_1$$

类似地推广到 R 上

定义 4.8

令 $\hat{F}$ 是如下集合

$$\hat{F} := \{(r, s) \in R \times R : s \neq 0\}$$

定义 $\hat{F}$ 上的关系

$$(r_1, s_1) \sim (r_2, s_2) : \iff r_1 s_2 = r_2 s_1$$

Remark

1. $\sim$ 是一个等价关系

   Proof

   (a). $rs = rs \implies (r, s) \sim (r, s)$

   (b). $(r_1, s_1) \sim (r_2, s_2) \iff r_1 s_2 = r_2 s_1 \iff r_2 s_1 = r_1 s_2 \iff (r_2, s_2) \sim (r_1, s_1)$

(c). 若 $(r_1,s_1)\sim(r_2,s_2),(r_2,s_2)\sim(r_3,s_3)$ 那么

$$r_1s_2=r_2s_1,\quad r_2s_3=r_3s_2$$

从而

$$(r_1s_3)\,s_2=(r_1s_2)\,s_3=(r_2s_1)\,s_3=s_1\,(r_2s_3)=s_1\,(r_3s_2)=(s_1r_3)\,s_2$$

(注意到这里用到了 R 的交换性) 利用 R 上的消去律，可得 $r_1s_3=s_1r_3$，即 $(r_1,s_1)\sim(r_3,s_3)$ 。

接下来利用此等价关系，构造 R 上的分式域。

定义 4.9

设 R 是（交换）整环。定义 R 的分式域，为配有以下加法 $+$ 和乘法 $\cdot$ 的商环 $F=\tilde{F}\backslash\sim$

$$[(r_1,s_1)]+[(r_2,s_2)]:=[(r_1s_2+r_2s_1,s_1s_2)]$$

$$[(r_1,s_1)]\cdot[(r_2,s_2)]:=[(r_1r_2,s_1s_2)]$$

♣

Remark

1. 上述的加法和乘法是良定义的:

   Proof 若 $(r_1,s_1)\sim(r_1',s_1')$，即 $r_1s_1'=r_1's_1$。需要说明

   (a). $(r_1s_2+r_2s_1)\,(s_1's_2)=(r_1's_2+r_2s_1')\,(s_1s_2)$

   (b). $r_1r_2s_1's_2=r_1'r_2s_1s_2$

   第二个式子对 $r_1s_1'=r_1's_1$ 两边乘 r_2s_2 后由交换性立即得到。第一个式子可以通过第二个式子化为 $r_2s_1s_1's_2=r_2s_1's_1s_2$，而这由交换性立即得到。
2. $(F,+,\cdot)$ 满足环公理。
3. $[(0,1)]$ 为零元，$[(1,1)]$ 为幺元。
4. 在 F 中，零元和幺元不相等。

   Proof 在 R 中，$0\neq1$，从而 $0\cdot1\neq1\cdot1$ 在 R 中成立，进而 $[(0,1)]\neq[(1,1)]$。
5. F 是域。

   Proof 由乘法的定义和 R 的交换性，显然 F 是交换环。只需要证明 F 上的非零元皆可逆。为此，任取 $[(r,s)]\neq[(0,1)]$，则 $r\neq0$。那么 $(s,r)\in\hat{F}$ ，我们有 $[(s,r)]\in F$，并且

   $$[(r,s)]\cdot[(s,r)]=[(rs,sr)]$$

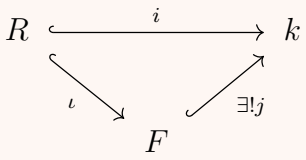
   因为 $rs\cdot1=sr\cdot1$，故 $[(rs,sr)]=[(1,1)]$，这就说明了 $[(r,s)]$ 可逆，且逆元为 $[(s,r)]$。
6. 通常记 $[(r,s)]$ 为 $\frac{r}{s}$。

接下来说明上述的构造确实满足我们一开始提出的泛性质。首先注意到 R 到 F 有自然的嵌入 $r \mapsto [(r,1)]$，记作 $\iota : R \hookrightarrow F$，这相当于将 r 与 $\frac{r}{1}$ 做等同。

定理 4.7

上述构造的 F 满足泛性质4.7。

具体地，设 R 是（交换）整环，F 和 $\iota : R \hookrightarrow F$ 分别设是 R 的分式域和上述的单的环同态。令 k 是一个域，$i : R \hookrightarrow k$ 是单（环）同态。那么存在唯一的单同态 $j : F \hookrightarrow k$，使得下图交换



即使得 $i = j \circ \iota$。 ♡

Proof

1. 唯一性：若这样的单同态 $j : F \hookrightarrow k$ 存在，接下来说明这样的 j 是唯一的。为此，任取 $\frac{r}{s} \in F$，其中 $r, s \in R$。由图表的交换性，$j\left(\frac{r}{1}\right) = j(\iota(r)) = i(r)$，$j\left(\frac{s}{1}\right) = j(\iota(s)) = i(s)$，再由 j 是环同态，
$$j\left(\frac{r}{s}\right) = j\left(\frac{r}{1}\right) j\left(\frac{1}{s}\right) = j\left(\frac{r}{1}\right)\left(j\left(\frac{s}{1}\right)\right)^{-1} = i(r)\,(i(s))^{-1}$$
由 r, s 唯一确定，故 j 若存在则唯一。
2. 存在性：上面的讨论给出了 j 的唯一表示，接下来仅需要说明
$$j\left(\frac{r}{s}\right) := i(r)\,(i(s))^{-1}$$
确实给出了满足条件的环同态。
   (a). 良定义：若 $\frac{r_1}{s_1} = \frac{r_2}{s_2}$，那么 $r_1 s_2 = r_2 s_1$，因此
   $$i(r_1)\, i(s_2) = i(r_2)\, i(s_1)$$
   由 i 是环同态可得
   $$i(r_1)\,(i(s_1))^{-1} = i(r_2)\, i(s_2)^{-1}$$

(b). 环同态：

$$\begin{aligned} j\left(\frac{r_1}{s_1}\right)+j\left(\frac{r_2}{s_2}\right) &= i(r_1)i(s_1)^{-1}+i(r_2)i(s_2)^{-1}=i(r_1s_2)i(s_1s_2)^{-1}+i(r_2s_1)i(s_1s_2)^{-1} \\ &= (i(r_1s_2)+i(r_2s_1))i(s_1s_2)^{-1}=i(r_1s_2+r_2s_1)i(s_1s_2)^{-1} \\ &= j\left(\frac{r_1s_2+r_2s_1}{s_1s_2}\right) \\ &= j\left(\frac{r_1}{s_1}+\frac{r_2}{s_2}\right), \end{aligned}$$

$$\begin{aligned} j\left(\frac{r_1}{s_1}\right)\cdot j\left(\frac{r_2}{s_2}\right) &= i(r_1)i(s_1)^{-1}\cdot i(r_2)i(s_2)^{-1}=i(r_1)i(r_2)i(s_1)^{-1}i(s_2)^{-1} \\ &= i(r_1r_2)i(s_1s_2)^{-1}=j\left(\frac{r_1r_2}{s_1s_2}\right) \\ &= j\left(\frac{r_1}{s_1}\cdot\frac{r_2}{s_2}\right), \end{aligned}$$

此外 $j\left(\frac{1}{1}\right)=i\left(1\right)i\left(1\right)^{-1}=1$ 明所欲证。

(c). 单同态：事实上，域到环的同态皆为单同态。

(d). 图的交换性：任取 $r\in R$，

$$j\circ\iota\left(r\right)=j\left(\frac{r}{1}\right)=i\left(r\right)i\left(r\right)^{-1}=i\left(r\right)$$

表明 $j\circ\iota=i$ 。

结论 整环 R 上的分式域构造，可以看成是强制让 R 上的所有非零元可逆。F 的构造让非零元 $s\in R$ 在 F 中有了逆元 $\frac{1}{s}$。这种构造是交换环的“局部化”的特殊情况。

第 5 章　多项式环

5.1　域上的多项式环

即将说明若 k 是一个域，$k[x]$ 是一个欧式整环。在此之前，需要对首项系数可逆的多项式的“长除法”。

引理 5.1 (“长除法”)

设 R 是一个环，$f(x), g(x) \in R[x]$ 是多项式，其中 $f(x) \neq 0$。若 $f(x)$ 的首项系数可逆，那么存在多项式 $q(x), r(x) \in R[x]$，使得

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

使得 $r(x) = 0$ 或 $\deg r(x) < \deg f(x)$ 成立。 ♡

Proof　当 $\deg g(x) < \deg f(x)$ 时，容易看出结论成立。

接下来，固定 $f(x) \in R[x]$，若命题不成立，我们取 g 是使得结论不成立的，次数最小的多项式，设 $n = \deg g(x)$，$m = \deg f(x)$，那么 $n \geq m$。设

$$f(x) = a_0 + a_1 x^1 + a_2 x^2 + \cdots + a_m x^m, \quad g(x) = b_0 + b_1 x^1 + b_2 x^2 + \cdots + b_n x^n$$

由假设 a_m 是可逆元，故存在 $u = a_m^{-1} \in R$，使得 $u a_m = 1$。令

$$g_1(x) := g(x) - b_n u f(x) x^{n-m} = (b_0 + \cdots + b_n x^n) - \left(b_n u a_0 x^{n-m} + \cdots + b_n u a_m x^n\right)$$

则 g_1 的 n 次项系数为 0，故 $\deg g_1(x) \leq n-1$，那么根据假设，$g_1(x)$ 对 $f(x)$ 的“长除法”存在，设

$$g_1(x) = q_1(x) f(x) + r_1(x)$$

其中 $r_1(x) = 0$ 或 $\deg r_1(x) < \deg f(x)$。紧接着有

$$g(x) = b_n u f(x) x^{n-m} + q_1(x) f(x) + r_1(x) = \left(b_n u x^{n-m} + q_1(x)\right) f(x) + r_1(x)$$

从而 $g(x)$ 对 $f(x)$ 的“长除法”存在，与对 g 的假设矛盾。

方便起见，引入根的概念

定义 5.1 (根)

设 R 是一个环，$g(x) \in R[x]$ 是一个多项式。若 $a \in R$ 使得 $g(a) = 0$，则称 a 是 $g(x)$ 的一个根。 ♣

Remark

1. $(x-a)$ 是 g 的一个因子，当且仅当 a 是 $g(x)$ 的一个根。

定理 5.1

设 k 是一个域，那么 $k[x]$ 是一个欧式整环。 ♡

Proof k 是一个域，特别地它是一个（交换）整环，从而 $k[x]$ 是一个（交换）整环。定义一个赋值 $\nu:(k[x]\setminus 0)\to\mathbb{Z}^{\geq 0}$，$\nu(f(x):=\deg f(x))$。由于 k 是域，每个非零多项式 $f(x)$ 的首项系数总是可逆元。因此对于所有的 $f(x),g(x)\in k[x]$，其中 $f(x)\neq 0$，都存在 $q(x)$ 和 $r(x)$，使得

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

使得 $r(x)=0$ 或 $\nu(r(x))<\nu(f(x))$。根据定义4.4，$k(x)$ 是一个欧式整环。

推论 5.1

若 k 是一个域。那么 $k[x]$ 是一个 PID，进而 $k[x]$ 中有唯一分解性（UFD）。 ♡

Proof 由定理4.4，每个欧氏整环都是一 PID，由定理4.6，每个 PID 都是一个 UFD。

命题 5.1 (带余除法的唯一性)

设 R 是整环，令 $f(x),g(x)\in R[x]$，其中 $f(x)\neq 0$。设 $f(x)$ 的首项系数是可逆元，那么 $g(x)$ 对 $f(x)$ 的带余除法是唯一的。 ♠

Proof 设

$$g(x)=q_1(x)f(x)+r_1(x)=q_2(x)f(x)+r_2(x)$$

始终 r_1,r_2 均要么为 0，要么次数小于 $f(x)$，则

$$(q_1(x)-q_2(x)f(x))+(r_1(x)-r_2(x))=g(x)-g(x)=0$$

因此 $(q_1(x)-q_2(x))f(x)=r_1(x)-r_2(x)$。若 $r_2(x)-r_1(x)\neq 0$，由整环的性质，左侧式子的次数一定不低于 $f(x)$ 的次数，但是等式右侧的式子次数严格小于 $f(x)$ 的次数。因此

$$(q_1(x)-q_2(x))f(x)=r_2(x)-r_1(x)=0$$

立即有 $r_1(x)=r_2(x),q_1(x)=q_2(x)$（因为 R 是整环）。

□

推论 5.2

设 R 是整环，$f(x)\neq 0$。设 $f(x)$ 的首项系数是单位。则 $R[x]/(f(x))$ 中的每个陪集都有唯一的表示 $r(x)+(f(x))$，使得要么 $r(x)=0$，要么 $\deg r(x)<\deg f(x)$ ♡

Idea 商环 $R[x]/(f(x))$ 由此可视作带余除法的余数环。

Proof 设 $g(x)+(f(x))$ 是 $R[x]/(f(x))$ 中的元素。由命题5.1和引理5.1，存在唯一的 $q(x)$ 和 $r(x)$，使得

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

满足 $r(x)=0$ 或 $\deg r(x)<\deg f(x)$。此时

$$g(x)+(f(x))=r(x)+(f(x))$$

这就说明了存在性。若 $r'(x)+(f(x))=g(x)+(f(x))$，则存在 $q'(x)$，使得 $g(x)=q'(x)f(x)+r'(x)$，带余除法的唯一性给出 $r'(x)=r(x)$。 □

定理 5.2

设 k 是域，$f(x)\in k[x]$ 是次数为 d 的非零多项式。则 $k[x]/(f(x))$ 是 d-维线性空间。 ♡

Remark 回忆 $\mathbb{C}\simeq\mathbb{R}[x]/(x^2+1)$，由此可知，在线性空间的意义下，$\mathbb{C}\simeq\mathbb{R}^2$

Proof $k[x]/(f(x))$ 中每一个元素唯一地写作

$$r(x)+(f(x))$$

其中 $r(x)=a_0+a_1x+\cdots+a_{d-1}x^{d-1}$ 是次数小于 $\deg f(x)$ 的多项式。将系数 $(a_0,\cdots,a_{d-1})$ 与陪集 $g(x)+(f(x))$ 建立映射。。又该映射保持加法和 k-标量乘法，且是单射（带余除法的唯一性）故为线性空间的同构。

□

Example 5.1 环 $(\mathbb{Z}/5\mathbb{Z})[x]/(x^3+1)$ 的元素个数为 125 个。

Proof 由于 5 是素数，故 $\mathbb{Z}/5\mathbb{Z}$ 是有限的交换整环，进而是一个域。由上面的命题，环 $(\mathbb{Z}/5\mathbb{Z})[x]/(x^3+1)$ 域同构于 $\mathbb{Z}/5\mathbb{Z}$ 上的 3 维线性空间，该线性空间上的元素个数为 $5^3=125$ 个。

□

5.2 多项式环上的不可约元

命题 5.2

设 k 是一个域，$f(x)\in k[x]$ 是次数不低于 2 的多项式。若 $f(x)$ 有根，则 $f(x)$ 是可约的。 ♠

Proof 若 a 是 $f(x)$ 的根，那么 $(x-a)$ 是 $f(x)$ 的因子。若 $\deg f(x)\geq 2$，我们有

$f(x)=(x-a)g(x)$，其中 $\deg g(x)\geq 1$。特别地 $g(x)$ 不是 $R[x]$ 中的可逆元，故 $f(x)$ 是可约的。

命题 5.3

若 k 是一个域，令 $f(x)\in k[x]$ 是次数为 2 或 3 的多项式。那么 $f(x)$ 不可约，当且仅当 $f(x)$ 在 k 中无根。

♠

Proof ($\Longrightarrow$) 是命题5.2的一个特殊情况。

($\Longleftarrow$) 反证法：若 $f(x)$ 可约，设 $f(x)=q_1(x)q_2(x)$，对于某两个不可逆的多项式 $q_1(x)$，$q_2(x)$ 成立。由于 k 是域，我们有 $q_1(x)$ 和 $q_2(x)$ 不为常系数多项式（否则它们可逆）。因为 $\deg f(x)=2$ 或 3，q_1,q_2 其中一个次数为次数为 1，它等于某个 $ax+b$，使得 $a,b\in k,a\neq 0$。但是根据条件假设 $-ba^{-1}$ 不是 $f(x)$ 的根矛盾。

第二部分

模论

第 6 章　模和 Aleb 群

定义 6.1 (模)

设 R 为环，左 R -模意谓以下资料

- 加法群 $(M,+)$;
- 映射 $R\times M\to M$, 记作 $(r,m)\mapsto r\cdot m=rm$, 满足以下条件
  1. $r\left(m_1+m_2\right)=rm_1+rm_2,\quad r\in R,m_1,m_2\in M$,
  2. $\left(r_1+r_2\right)m=r_1m+r_2m,\quad r_1,r_2\in R,m\in M$,
  3. $\left(r_1r_2m\right)=r_1\left(r_2m\right)$,
  4. $1_R\cdot m=m$

♣

Example 6.1 设 R 为含幺环，$M:=(R,+)$，取映射 $R\times M\to M$ 为 R 上的左乘映射，构成一个左 R -模。

Example 6.2 设 R 为含幺环，$V:=\left\{\begin{pmatrix}v_1\\v_2\\\vdots\\v_n\end{pmatrix}:v_i\in R,1\leq i\leq n\right\}=:R^n$。取左作用为逐项的左乘作用，则 V 是 R -模，称为环 R 的自由模。

Example 6.3 加法群都是 $\mathbb{Z}$-模。

Example 6.4 若 R 为域，则 R-模就是域 R 上的向量空间，也是 R 上的自由模。

6.1　R -模范畴

定义 6.2 (模同态)

设 R 是环，M,N 是 R -模。称函数 $f:M\to N$ 是一个 R -模同态，若 $\forall r\in R,\forall a,b\in M$,

$$f\left(a+b\right)=f\left(a\right)+f\left(b\right)$$

$$f\left(r\cdot a\right)=r\cdot f\left(a\right)$$

也称 f 是 R-线性的。

♣

Example 6.5 考虑环同态 $f : R \to S$，定义 R 在 S 上的作用，通过

$$r \cdot s := f(r)\, s, \quad \forall r \in R, \forall s \in S$$

则 S 在此作用下称为一个 R-模。

定义 6.3 (子模)

设 R 是一个环，M 是 R-模，N 是 M 的子集，且 N 也是 R-模。称 N 是 M 的一个子模，若含入映射 $\iota : N \hookrightarrow M$ 是 R-模同态。

♣

命题 6.1 (像与核)

设 $f : M \to N$ 是 R-模同态，那么:

1. 若 M' 是 M 的子模，则 $f(M')$ 是 M 的子模;
2. 若 N' 是 M 的子模，则 $f^{-1}(N')$ 是 M 的子模;

♠

定义 6.4 (生成模)

令 M 是 R-模，$m_1, \cdots, m_n$ 是 M 中的元素。称 $m_1, \cdots, m_n$ 的全体 R-线性组合，记作 $\langle m_1, m_2, \cdots, m_n \rangle$，为 M 的由 $1_1, 1_2, \cdots, 1_n$ 生成的子模。

♣

定义 6.5 (有限生成与循环)

称 R-模 M 是有限生成的，若存在 $m_1, m_2, \cdots, m_n \in M$，使得 $M = \langle m_1, m_2, \cdots, m_n \rangle$。

称 M 是循环的，若 $M = \langle m \rangle$ 对某个 $m \in M$ 成立。

♣

定义 6.6 (直和)

设 R 是环，M, N 是 R-模。称 R-模 $(M \times N, +, \cdot)$ 为 M 和 N 的直和，记作 $M \oplus N$，其中 $+, \cdot$ 按以下方式定义

$$(m_1, n_1) + (m_2, n_2) := (m_1 + m_2, n_1 + n_2)$$

$$r \cdot (m, n) := (rm, rn)\,.$$

♣

6.2 标准分解和商

定理 6.1 (标准分解)

令 $f : M \to N$ 是 R-模同态，以下交换图成立

$$M \xrightarrow{\pi} M/\ker f \xrightarrow[\tilde{f}]{\sim} f(M) \xrightarrow{\iota} N, \qquad M \xrightarrow{f} N$$

其中 π 是投影映射，ι 是含入映射，$\tilde{f}$ 是诱导同态。此外 $\tilde{f}$ 是同构。 ♡

6.3 整环上的模

第三部分

域论

第 7 章 域扩张

7.1 域和域同态

定义 7.1

设 k 是域。k 的一个域扩张是指，配备了同态 $k \hookrightarrow F$ 的一个域 F，使得 k 等同于 F 的一个子域。 ♣

Remark

1. 域同态无非是域之间的环同态，它一定是单射。

Example 7.1 设 $f(t) \in \mathbb{Q}[t]$ 是非零不可约多项式。则 $\mathbb{Q}[t]/(f(t))$ 是一个域，$Q \subseteq \mathbb{Q}[t](f(t))$ 是一个域扩张。

Example 7.2 设 $\mathbb{Q}(t)$ 是多项式环 $\mathbb{Q}[t]$ 的分式域；即 $\mathbb{Q}[t]$ 由商 $f(t)/g(t)$，其中 $f(t), g(t) \in \mathbb{Q}[t]$，且 $g(t) \neq 0$。则 $\mathbb{Q} \subseteq \mathbb{Q}[t]$ 是一个域扩张。

Example 7.3 $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$，其中 $\overline{\mathbb{Q}}$ 是“代数数”，即可以写作有理系数多项式根的复数的全体。

定义 7.2

设 k 是域。定义 k 的特征，为 $\mathbb{Z} \to k$ 的唯一环同态的核的非负生成元。即最小的正整数 n，使得 $n \cdot 1_k = 0_k$，或者当正整数不存在时取 0。 ♣

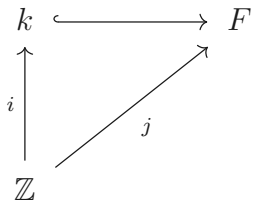
Remark

- $\mathbb{Z} \to k$ 的唯一性是因为 $\mathbb{Z}$ 是环范畴的始对象。

引理 7.1

设 $k \subseteq F$ 是一个域扩张。则 $\operatorname{char} k = \operatorname{char} F$ ♡

Proof 由于 $\mathbb{Z}$ 到任意环的环同态唯一，故图



交换。由于 $k \hookrightarrow F$ 是单射，故 $\ker i = \ker j$，进而有相同的生成元，即 $\operatorname{char} k = \operatorname{char} F$

。 □

引理 7.2

设 F 是域，则 F 包含了唯一的 $\mathbb{Q}$ 的复制或 $\mathbb{Z}/p\mathbb{Z}$ 的复制，其中 $p>0$ 是素数。 ♡

Proof 若 $\operatorname{char} F=n$，则要么 $n=p$ 对某个素数成立（整环的特征是素数），要么 $n=0$。对于后者，$\mathbb{Z}\to F$ 是单射，由定理??，存在唯一的单同态 $\mathbb{Q}\hookrightarrow F$。

若 $n=p>0$，则由同构定理，$\mathbb{Z}/p\mathbb{Z}\simeq i(\mathbb{Z})\subseteq F$，唯一性由 $\mathbb{Z}\to F$ 像集的唯一性可得。

□

定义 7.3

对于每个素数 p，记域 $\mathbb{Z}/p\mathbb{Z}$ 为 $\mathbb{F}_p$ ♣

上面的引理表明，特征为 k 的域的范畴有始对象 $\mathbb{F}_p$，特征为 0 的域的范畴有始对象 $\mathbb{Q}$；即存在唯一的域同态 $\mathbb{F}_p\to k$(其中 $\operatorname{char} k=p$)或存在唯一的域同态 $\mathbb{Q}\to k$(其中 $\operatorname{char} k=0$)。

因此，可以在每个单独的范畴中研究域扩张问题。

事实上，对于给定的域 k，我们考虑域 k 的扩张的范畴：对象是域扩张 $k\hookrightarrow F$，态射是（环）同态 $j:F'\hookrightarrow F''$，使得下图交换

$$\begin{array}{ccc} F' & \xhookrightarrow{j} & F'' \\ \uparrow & & \uparrow \\ k & \xrightarrow{\mathrm{id}_k} & k \end{array}$$

称 j 延拓了 id_k。可以视同态为一列扩张 $k\subseteq F'\subseteq F''$。

始对象是平凡扩张 $\mathrm{id}_k:k\to k$。分别令 $k=\mathbb{Q}$,$k=\mathbb{F}_p$，可以将上面的讨论统一起来。

7.2 有限扩张和扩张的次数

回忆每个环同态 $R\to S$ 都能使得 S 称为一个 R-模；特别地，若 $k\subseteq F$ 是一个域扩张，则 F 视为 k 上的线性空间。

定义 7.4 (扩张的次数)

域扩张 $k\subseteq F$ 的次数，记作 $[F:k]$，被定义为 F 作为 k-线性空间的维数。 ♣

定义 7.5

称域扩张 $k \subseteq F$ 是“有限”的，若 F 是有限维 k-线性空间。 ♣

引理 7.3

设 k 是域，$f(t) \in k[t]$ 是不可约多项式。则 $k[t]/f(t)$ 是一个域，且将 a 映到陪集 $a+(f(t))$ 的同态 $k \to k[t]/(f(t))$ 定义出域扩张 $k \subseteq k[t]/(f(t))$。则扩张是有限扩张，且

$$[k(t)/(f(t)) : k] = \deg f$$

♡

Proof $k[t]$ 是欧氏整环进而是 PID(定理4.4)，PIDs 中的不可约元生成极大理想 (命题4.4)，故 $k[t]/(f(t))$ 是一个域。且 $k[t]/(f(t))$ 由定理5.2是一个 $\deg f$ 维线性空间，陪集 $1+(f(t),\cdots,t^{d-1}+(f(t)))$ 构成一组基。

□

命题 7.1

设 $k \subseteq E \subseteq F$ 是域扩张。若 $k \subseteq E$ 和 $E \subseteq F$ 都是有限扩张，则 $k \subseteq F$ 是有限扩张，且

$$[F : k] = [F : E][E : k]$$

♠

Proof 令 $[E : k] = m, [F : E] = n$。设 $\varepsilon_1, \cdots, \varepsilon_m$ 是 E 在 k 上的一组基，$\varphi_1, \cdots, \varphi_n$ 是 F 在 E 上的一组基。断言 $\varepsilon_i\varphi_j, i = 1, \cdots, m, j = 1, \cdots, n$ 构成 F 在 k 上的一组基。为了说明 F 可以由这组基线性表出，任取 $f \in F$，设 $e_1, \cdots, e_n \in E$，使得

$$f = e_1\varphi_1 + \cdots + e_n\varphi_n = \sum_{i=1}^{n} e_i\varphi_i$$

而每个对于每个 e_i，都存在 $k_{i1}, \cdots, k_{im} \in k$，使得

$$e_i = \sum_{j=1}^{m} k_{ij}\varepsilon_j$$

于是

$$f = \sum_{i=1}^{n}\sum_{j=1}^{m} k_{ij}\varepsilon_j\varphi_i$$

这就说明了 $(\varepsilon_j\varphi_i)$ 在 k 上张成了 F。

为了说明线性无关性，考虑 $\varepsilon_j\varphi_i$ 在 k 上的线性组合

$$\sum_{i,j} k_{ij}\varepsilon_j\varphi_i = 0$$

由 φ_i 的线性无关性，对于每个 $i=1,2,\cdots,n$,

$$\sum_{j=1}^{m} k_{ij}\varepsilon_j = 0, \quad i=1,\cdots,n$$

再由 (ε_j) 的线性无关性，

$$k_{i1}=\cdots=k_{im}=0, \quad i=1,\cdots,n$$

□

定义 7.6

若 $k\subseteq E\subseteq F$ 是域扩张，称 E 为扩张 $k\subseteq F$ 的中间域。 ♣

Remark

- 容易看到若 E 是有限扩张 $k\subseteq F$ 的中间域，则 $k\subseteq E$ 和 $E\subseteq F$ 都是有限扩张。

Example 7.4 扩张 $\mathbb{Q}\subseteq\mathbb{Q}[t]/\left(t^7+2t^2+2\right)$ 没有非平凡的中间域。

Proof 若 $\mathbb{Q}\subseteq E\subseteq\mathbb{Q}[t]/\left(t^7+2t^2+2\right)$，则

$$[\mathbb{Q}[t]/\left(t^7+2t^2+2\right):E][E:\mathbb{Q}]=7$$

要么 $[E:Q]=1$，要么 $[\mathbb{Q}[t]/\left(t^7+2t^2+2\right):E]=1$

□

7.3 单扩张

定义 7.7

设 $k\subseteq F$ 是域扩张，$\alpha_1,\cdots,\alpha_r\in F$。记 $k\left(\alpha_1,\cdots,\alpha_r\right)$ 为 F 中最小的包含了 k 和所有 α_i 的子域。

若 $F=k\left(\alpha_1,\cdots,\alpha_r\right)$，则称 $k\subseteq F$ 是通过 $\alpha_1,\cdots,\alpha_r$ 有限生成的。 ♣

定义 7.8 (单扩张)

称扩张 $k\subseteq F$ 是一个单扩张，若 $F=k\left(\alpha\right)$ 对某个 $\alpha\in F$ 成立。 ♣

命题 7.2

设 $k\subseteq k\left(\alpha\right)=F$ 是单扩张。则以下其一成立

- $F\simeq k[t]/\left(p\left(t\right)\right)$ 对某个满足 $p\left(\alpha\right)=0$ 的不可约首一多项式 $p\left(t\right)\in k[t]$ 成立；
- F 同构于 $k[t]$ 的分式域 $k\left(t\right)$。

对于第一种情况，$[F:k]=\deg p(t)$，对于第二种情况，$[F:k]=\infty$。 ♠

Proof 定义一个同态 φ

$$\varphi: k[x] \to F$$
$$f(t) \mapsto f(\alpha)$$

若 $\ker \varphi \neq 0$，则由于 $k[t]$ 是 PID，对于某个多项式 $p(t) \in k[t]$，我们有 $\ker \varphi = (p(t))$。根据构造，$p(\alpha)=0$，通过乘以首项系数的逆，不妨设 $p(t)$ 是首一的。由第一同构定理，φ 诱导出单同态

$$\tilde{\varphi}: k[t]/(p(t)) \hookrightarrow F$$

特别地，$k[t]/(p(t))$ 视作 F 的子环是一个整环，从而 $(p(t))$ 是素理想，进而是极大理想（命题4.3），因此 $k[t]/(p(t))$ 是一个域。$\operatorname{im}\tilde{\varphi} \subseteq F$ 是包含了 $\varphi(t)=\alpha$ 和 $\varphi(k)=k$ 的 F 的子域，又 F 是包含了 k 和 α 的最小的子域，故 $\operatorname{im}\tilde{\varphi}=F$。因此 $\tilde{\varphi}$ 也是满射，进而是同构。此时由定理5.2，$[F:k]=[(k[t]/(p(t))):k]=\deg p$。这就说明了第一种情况。

若 $\ker \varphi=(0)$，则 $\varphi: k[t] \to F$ 是单射。又 $k[t]$ 是整环，它有分式域 $k(t)$。由泛性质4.7，存在单同态

$$k(t) \hookrightarrow F$$

，同态像是包含了 $\varphi(t)=\alpha$ 和 $\varphi(k)=k$ 的域，从而 $k(t) \simeq F$

□

定义 7.9

设 $k \subseteq F$ 是域扩张，$\alpha \in F$。称 α 是 k 上的 d 次代数元，若 $[k(\alpha):k]=d$ 是有限的。称 α 是超越的，若它不是代数的。 ♣

引理 7.4

设 $k \subseteq F$ 是域扩张，$\alpha \in F$。则 α 在 k 上是代数的，当且仅当 α 是某个非零多项式 $f(t) \in k[t]$ 的根。此时 α 是多项式 $p(t) \in k[t]$ 的根，其中 $p(t)$ 是唯一的使得 $p(t) \mid f(t)$ 且 $k(\alpha) \simeq k[t]/(p(t))$ 的不可约首一多项式。 ♡

Proof 若 α 是 k 上的代数元，则 $k \subseteq k(\alpha)$ 是命题7.2中满足第一条的扩张，特别地 $p(\alpha)=0$ 对某个非零不可约首一多项式成立。

反之，若 $f(\alpha)=0$ 对某个非零 $f(t) \in k[t]$ 成立。考虑“赋值”同态

$$\varphi: k[t] \to F$$

映 $g(t)$ 为 $g(\alpha)$。由假设 $f(t) \in \ker \varphi$，特别地 $\ker \varphi \neq (0)$。由命题7.2 的证明过程，$k(\alpha) \simeq k[t]/\ker \varphi$ 是 k 的有限扩张，从而 α 是代数元。

此外，$\ker \varphi$ 由一个不可约的首一多项式 $p(t)$ 生成。由于 $f(t) \in \ker \varphi = (p(t))$，故 $f(t)$ 是 $p(t)$ 的一个倍数。

最后，$k[t]$ 的首一生成元是唯一的：若 $(p_1(t)) = (p_2(t))$，则 $p_1(t), p_2(t)$ 相差一个单位，故当它们首一时相等。

□

定义 7.10 (极小多项式)

设 α 在 k 上是代数的，α 在 k 上的极小多项式是指使得 $p(\alpha) = 0$ 的唯一的不可约首一多项式 $p(t) \in k[x]$ 。

♣

Remark

- α 的次数就是 α 的极小多项式的次数。

命题 7.3

若 α 是 k 上的代数元，则 $k(\alpha)$ 中的每个元素都写成 k-系数的 α 多项式。

♠

Proof 由命题7.2的证明过程，

$$\begin{aligned} \varphi : k[x] &\to F = k(\alpha) \\ f(t) &\mapsto f(\alpha) \end{aligned}$$

是满射。

□

Example 7.5 “代数数”是复数在 $\mathbb{Q}$ 上的代数元，用 $\overline{\mathbb{Q}}$ 表示代数数的全体。

对于 $i \in \overline{\mathbb{Q}}$，$i$ 在 $\mathbb{Q}$ 上的极小多项式是 $t^2 + 1$ 。

命题 7.4

令 $k \subseteq E \subseteq F$ 是域扩张，$\alpha \in F$，设 α 在 k 上是代数的，有极小多项式 $p_k(t)$。则 α 在 E 上也是代数的，它的极小多项式 $p_E(t)$ 是 $p_k(t)$ 的一个因子。

♠

Remark $p_k(t)$ 在域 k 上是不可约的，但在更大的域（例如 E）上可能有非平凡的因子。比如 $t - \alpha$ 就是 $p_k(t)$ 在 $F[t]$ 上的因子。

Proof $k \subseteq E$，$p_k(t)$ 可以看做是 $E[t]$ 上的多项式。因为 $p_k(\alpha) = 0$，于是 α 在 E 上是代数的，由引理7.4，它的极小多项式 $p_E(t) \in E[t]$ 整除 $p_k(t)$ 。

□

Example 7.6

$$\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)=\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$$

是一个单扩张

Proof 显然 $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)\subseteq\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ 。

令 $\alpha=\sqrt{2}+\sqrt{3}$，则

$$\begin{cases}\alpha=\sqrt{2}+\sqrt{3},\\ \alpha^3=11\sqrt{2}+9\sqrt{3}\end{cases}$$

易见 $\sqrt{2},\sqrt{3}$ 都写作 α 的 $\mathbb{Q}$- 多项式。

□

命题 7.5

有限域的有限扩张是单扩张。 ♠

Proof 设 $k\subseteq F$ 是域扩张，其中 k 是有限域。若扩张是有限的，则 F 也是有限域，故而乘法群 F^* 是循环群（有限域的乘法群是循环的）。设 $F^*=\langle\alpha\rangle$，则 F 中的任一元素写作 α 的次幂，进而位于 $k(\alpha)$ 中。故 $k\subseteq k(\alpha)=F$ 是单扩张。

□

命题 7.6

设 $k\subseteq F=k(\alpha)$ 是单扩张，α 是 k 上的代数元。则 $k\subseteq F$ 只容许有限个中间域。 ♠

Remark

- 若 t 是 k 上的超越元，

Proof 设 $p(t)\in k[t]$ 是 α 在 k 上的极小多项式，令 E 是扩张 $k\subseteq k(\alpha)$ 的中间域。视 $p(t)$ 为 $E[t]$ 上的多项式，则由命题7.4，α 在 E 上的极小多项式 $p_E(t)$ 是 $p(t)$ 在 $E[t]$ 中的因子。令 $p_E(t)=e_0+e_1t+\cdots+e_{d-1}^{d-1}+t^d\in E[t]$，故 $[k(\alpha):E]=d$ 。

断言 $E=k(e_0,\cdots,e_{d-1})$，事实上，一方面我们有

$$E'\subseteq E\subseteq k(\alpha)$$

另一方面 E' 包含了 $p_E(t)$ 的所有系数，故 p_E 也是 E' 上的多项式。又因为 $p_E(t)$ 在 E 上不可约，从而也在 E' 上不可约，进而 $p_E(t)$ 一定是 α 在 E' 上的极小多项式。因此 $[k(\alpha):E']=d=[k(\alpha):E]$ ，于是由命题7.1

$$d=[k(\alpha):E']=[k(\alpha):E][E:E']=d[E:E']$$

从而 $[E:E']=0$，$E:E'$，断言成立。

断言表明 E 由 $p(t)$ 的因子 $p_E(t)$ 唯一确定，而 $p(t)$ 在 $k(\alpha)[t]$ 中只有有限个首一的因子，故中间域的选取是有限的。

□

定理 7.1 (*)

设 $k \subseteq F$ 是域扩张。则 $F = k(\alpha)$ 对某个 k 上的代数元 α 成立，当且仅当扩张只容许有限个中间域。

♡

Proof “仅当”的方向就是上面的命题，接下来说明“当”的方向。

首先断言 $k \subseteq F$ 是有限生成的，若不然：可以构造无限长的递增扩域链

$$k \subsetneq k(u_1) \subsetneq k(u_1, u_2) \subsetneq k(u_1, u_2, u_3) \subsetneq \cdots \subseteq F,$$

给出了无限多个中间域。由此不妨设 F 是有 n 个元素 $u_1, \cdots, u_n$ 生成的：$F = k(u_1, \cdots, u_n)$。再断言 u_i 是代数元，事实上，若 u_i 是超越元，则 $k(u_1, \cdots, u_{i-1})$ 和 $k(u_1, \cdots, u_i)$ 之间存在无穷多个中间域，进而 k 和 F 中间域也有无穷多个。特别地，$k \subseteq F$ 是有限扩张。

可以通过归纳化简为 $n = 2$ 的情况，具体地，若对于 $n \geq 3$ 是命题成立（可化为单扩张），则

$$F = k(u_1, \cdots, u_n) = k(u_1, \cdots, u_{n-1})(u_n) = k(u)(u_n) = k(u, v)$$

对于某个 u 成立，其中置 $v = u_n$。因此只需要证明 $n = 2$ 的情况。

因此，不妨设 $F = k(u, v)$。若 k 是有限域，则由于 $k \subseteq F$ 是有限扩张，命题7.5 给出 $k \subseteq F$ 是单扩张。

□

7.4 代数扩张

定义 7.11

称域扩张 $k \subseteq F$ 是代数扩张，若 F 上的每一个元素都是 k 上的代数元。

♣

命题 7.7

有限扩张都是代数扩张。事实上，若 $k \subseteq F$ 是有限扩张，且 $[F : k] = d$，则每个 $\alpha \in F$ 都是 k 上的代数元，且它的次数整除 d。

♠