代数数论初步

熊锐

2018 年 9 月 17 日

本书的目的在于介绍代数数论最基本的内容, 首先是重要的, 有启发性的例子, 同时为了避免干扰, 在理论建立中, 凡是有扰于理论展示的部分皆诉诸附录. 另外希望本书能够成为学习交换代数的一个动机.

本书分为两个部分, 第一部分是 Dedekind 整环的理论, 这部分最典型的例子无疑是 Gauss 整环; 第二部分是赋值的理论, 这部分最典型的例子无疑是 p 进数.

读者在阅读本书前应当有初等数论和抽象代数有关群环域的基本知识, 数论需要知道唯一分解, 还有二次剩余, 一个简约的介绍可见 [11] 的 §I.3. 关于代数的大体的介绍可见 [1] 第三部分, 详细的介绍例如 [5] 和 [2], 只需大致了解群环域的基本概念, 稍微超出 “概念” 的对应的内容附录中均有所补充.

Contents

Part I

第一部分
Dedekind 整环

Chapter 1

例子 — Gauss 整环

在本章 $i = \sqrt{-1} \in \mathbb{C}$

1.1 Gauss 整数环的唯一分解

定义 1.1 (Gauss 整数环) 如下的环被称为 **Gauss 整数环**

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

显然, 她关于复数的通常加法和乘法封闭, 且是一个整环, 其中的元素被称为 **Gauss 整数**. 在 *Gauss* 整环上可以定义如下 **范数 (norm)**

$$\mathcal{N}(a + bi) = a^2 + b^2 \in \mathbb{Z}_{\geq 0}$$

容易知道 $\mathcal{N} : \mathbb{Z}[i] \to \mathbb{Z}$ 保持乘法, 且 $\mathcal{N}(x) = 0 \iff x = 0$. 并且我们沿袭 *(B.9)* 的整除和相伴的记号和 *(B.10)* 的定义.

回忆 §A.1, 对整数分解的操作, 其关键在于建立带余除法, 不过在此之前我们先把单位计算出来, 注意到 $\mathbb{Z}$ 的单位是 $\{\pm 1\}$.

命题 1.2 *Gauss* 整环 $\mathbb{Z}[i]$ 上的单位正是那些范数为单位的元素. 即

$$\operatorname{unit} \mathbb{Z}[i] = \{1, -1, i, -i\}$$

证明 所谓单位无非是 $xy = 1$ 的其中一个解, 两边同时取范数知 $\mathcal{N}x\mathcal{N}y = \mathcal{N}1 = 1$, 这迫使 $\mathcal{N}x = \pm 1$, 而容易通过范数的定义直接知道满足条件的 x 只有 $\pm 1, \pm i$. 而反过来也容易知道他们是单位. □

定理 1.3 (带余除法) *在 Gauss 整环 $\mathbb{Z}[i]$ 上有带余除法. 具体来说任何 $a, b \in \mathbb{Z}[i]$, 其中 $b \neq 0$, 都存在 $d, r \in \mathbb{Z}[i]$ 使得*

$$a = db + r \qquad \mathcal{N}r < \mathcal{N}b$$

证明 这里采取几何化的证明[1], 如下图, 选择 $d \in \mathbb{Z}[i]$ 使得 db 距离 a 最近,

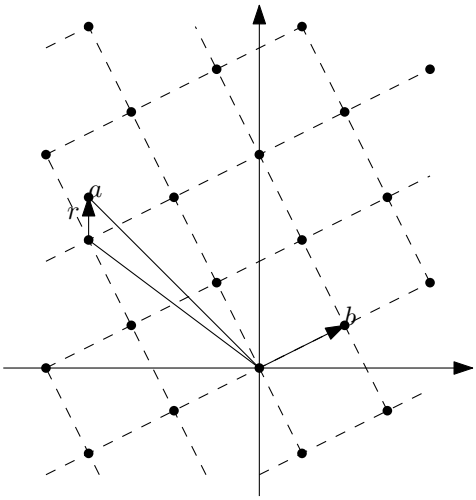


Figure 1.1: 带余除法

即 $\mathcal{N}(db - a)$ 最小, 从图中可以断言

$$\mathcal{N}(db - a) \leq \frac{\sqrt{2}}{2}\mathcal{N}b < \mathcal{N}b$$

这样 $r = db - a$ 为所求的 r. □

推论 1.4 *Gauss 整数环 $\mathbb{Z}[i]$ 是主理想整环, 进而是唯一分解整环.*

[1] 读者还可以自行补出严格的证明, 或参见 [2]§5.7 例 4.7.7

证明 任意选取理想 $\mathfrak{a} \subseteq \mathbb{Z}[i]$, 若 $\mathfrak{a} = (0)$ 则休矣. 若 $\mathfrak{a} \neq 0$, 因为范数 $\mathcal{N}$ 的值域是 $\mathbb{Z}_{\geq 0}$ 可以挑选其中非零的最小者 a, 显然 $a \neq 0$. 任意取 $x \in \mathfrak{a}$, 作 x 对 a 的带余除法得到 $d, r \in \mathbb{Z}[i]$ 使得

$$x = da + r \qquad \mathcal{N}r < \mathcal{N}a$$

因为 $r = x - da \in \mathfrak{a}$, 从而迫使 $r = 0$, 从而 $x = da$, 换言之 $\mathfrak{a} = (a)$. 关于是唯一分解整环的论证见 (B.11). □

1.2 Gauss 整环上素元

下面的一个问题是怎样的元在 Gauss 整环上是素元? 当然, 寄希望于给出所有唯一分解整环上的素元的刻画是不现实的, 我们的描绘当然要依托于 $\mathbb{Z}$ 上的素数.

定理 1.5 *Gauss 整环 $\mathbb{Z}[i]$ 上的素元有如下刻画*

(1) *正实数 $p \in \mathbb{Z}[i]$ 是素元*

$$\Longleftrightarrow\ p \in \mathbb{Z} \text{ 是素数, 且不存在 } a, b \in \mathbb{Z}, \text{s. t. } a^2 + b^2 = p$$

$$\Longleftrightarrow\ p \in \mathbb{Z} \text{ 是素数, 且 } p \equiv 3 \mod 4.$$

(2) *虚数 $(b \neq 0)$, $a + bi \in \mathbb{Z}[i]$ 是素元*

$$\Longleftrightarrow\ \text{范数 } \mathcal{N}(a+bi) = a^2+b^2 \text{ 是素数 } p, \text{ 且存在 } a, b \in \mathbb{Z}, \text{s. t. } a^2+b^2 = p.$$

$$\Longleftrightarrow\ \text{范数 } \mathcal{N}(a+bi) = a^2+b^2 \text{ 是素数 } p, \text{ 并且 } p \equiv 1 \mod 4 \text{ 或 } p = 2.$$

证明 首先, 我们先证明第一个等价, 若 p 不是素元, 则有非单位素元 $q|p$, 但 q 与 p 不相办. 从而在 $\mathbb{Z}$ 上, $\mathcal{N}q|\mathcal{N}p = p^2$. 容易得到[2] $\mathcal{N} = p$, 设 $q = a + bi$, 则 $p = \mathcal{N}q = a^2 + b^2$. 反之, 如果 $p = a^2 + b^2$, 则 $p = a^2 + b^2 = (a+bi)(a-bi)$.

下面再证明第二个等价, 首先, p 是素元直接蕴含 p 是素数, 并且在 p 是素数时,

$$p \text{ 是素元} \Longleftrightarrow \mathbb{Z}[i]/(p) \text{ 是整环}$$

[2] 若 $\mathcal{N}q = p^2$, 则 $\mathcal{N}(p/q) = 1$, 这样 $q \sim p$, 矛盾.

而

$$\frac{\mathbb{Z}[i]}{(p)} = \frac{\mathbb{Z}[X]/(X^2+1)}{(p)} = \frac{\mathbb{Z}/(p)[X]}{(X^2+1)} = \frac{\mathbb{F}_p[X]}{X^2+1}$$

故上式是整环当且仅当 X^2+1 在 $\mathbb{F}_p[X]$ 没有根, 换言之, $\left(\frac{-1}{p}\right) = -1$, 其中 $\left(\frac{*}{*}\right)$ 是 Legendre 符号 (A.4). 根据 (A.5) 这等价于 $p \equiv 3 \mod 4$.

若素元具有形式 $a+bi$, 则 $a+bi | \mathcal{N}(a+bi) = a^2+b^2$, 于是 $a+bi$ 势必整除 a^2+b^2 在 $\mathbb{Z}$ 的某个素因子, 设之为 p, 即

$$a+bi | p \quad \Rightarrow \quad \mathcal{N}(a+bi) | \mathcal{N}p \quad \Rightarrow \quad a^2+b^2 | p^2$$

此时 $p | a^2+b^2 | p^2$, 则 $a^2+b^2 = p$ 或 $a^2+b^2 = p^2$. 容易知道, $a+bi$ 是素元, 则 $a-bi$ 也是素元, 加之 $b \neq 0$, 这迫使[3] $a^2+b^2 = p$. 根据 $a^2+b^2 = p$ 是否有解, 我们知道, $p \equiv 1 \mod 4$ 或 $p = 2$. □

推论 1.6 *对于素数 $p \in \mathbb{Z}$, 其在 $\mathbb{Z}[i]$ 中的分解有三种情况*

(1) $p = 2$, 则 $2 = (1+i)(1-i) = -i(1+i)^2$. **(分歧的)**

(2) $p \equiv 3 \mod 4$, 则 $p = p$. **(惰性的)**

(3) $p \equiv 1 \mod 4$, 则 $p = (a+bi)(a-bi)$. *对某个 $a, b \in \mathbb{Z}$.* **(分裂的)**

1.3 Gauss 整环上的同余

引理 1.7 *对于素数 p, 选取一个 $\mathbb{Z}[i]$ 素元 $q | p$, 则 $(q) \cap \mathbb{Z} = (p)$.* [4]

证明 因为 $q | p$ 即 $p \in (q)$, 故 $(p) \subseteq (q) \cap \mathbb{Z}$. 但是 $(q) \cap \mathbb{Z}$ 是一个理想, 设为 (a), $(p) \subseteq (a)$ 意味着 $a | p$, 若 $a \sim p$ 即 $|a| = p$, 则已经得证. 若 $a = \pm 1$, 这意味着 $1 \in \mathbb{Z} \subseteq (q)$, 从而矛盾. □

引理 1.8 *对于 $a+bi \in \mathbb{Z}[i]$, 有*

$$\mathcal{N}a = a^2+b^2 = |\mathbb{Z}[i]/(a+bi)|$$

[3] 因为若 $(a+bi)(a-bi) = a^2+b^2 = p^2$ 给出了 p^2 的两种分解 (如果 p 继续分解下去的话).
[4] 前一组括号是在 $\mathbb{Z}[i]$ 中生成的一组理想, 后一组括号是在 $\mathbb{Z}$ 中生成的理想.

证明 这需要考虑 $(a+bi)[\mathbb{Z}\oplus i\mathbb{Z}]$ 在 $\mathbb{Z}\oplus i\mathbb{Z}$ 中的指数, 根据 (B.2), 我们要计算指数只需要计算如下映射在各自基 $\{a+bi,(a+bi)i\}$ 和 $\{1,i\}$ 下的矩阵的行列式

$$\det\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2+b^2 = \mathcal{N}(a+bi)$$

命题得证. □

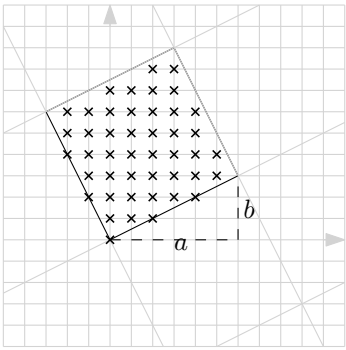


Figure 1.2: Gauss 整环上的范数

约定 1.9 对于素数 p, 选取一个 $\mathbb{Z}[i]$ 素元 $q|p$, 实际上, 我们可以得到一个自然同态

$$\mathbb{Z}/(p)\to\mathbb{Z}[i]/(q) \qquad (*)$$

这由 $\mathbb{Z}$ 到 $\mathbb{Z}[i]$ 的包含映射诱导 [5], 且这是单射. 而因为有限整环总是域[6], 根据上面的引理我们知道, 所以上面的 $(*)$ 实际上可以看成域扩张. 方便起见, 下面直接认为是包含关系 $\mathbb{Z}/(p)\subseteq\mathbb{Z}[i]/(q)$.

定义 1.10 (分歧指数, 惰性指数) 对于素数 p, $\mathbb{Z}[i]$ 的素元 $q|p$,

- 定义 **分歧 (ramification) 指数 (index)**

$$\mathsf{e}(q|p)=\operatorname{ord}_q p = p \text{ 分解为 } q \text{ 的指数}$$

[5] 具体来说, $\iota:\mathbb{Z}/(p)\longrightarrow\mathbb{Z}[i]/(q)\qquad x \bmod p\longmapsto x \bmod q$.
[6] 考虑左乘诱发的平移作用会得到域的论断.

即 p 可以写成

$$p = q^{\mathsf{e}(q|p)}(\dots) \qquad (\dots) = (\text{不相伴于 } q \text{ 的素元})$$

- 定义 **惰性 (inertia) 指数**

$$\mathsf{f}(q|p) = [\,\mathbb{Z}[i]/(q) \,:\, \mathbb{Z}/(p)\,] = \text{域扩张 } \mathbb{Z}/(p) \subseteq \mathbb{Z}[i]/(q) \text{ 的次数}$$

- 定义 **纤维数**

$$\mathsf{r}(p) = \#\{\text{“素元”}q \in \mathbb{Z}[i] : q|p\} = \#\{\text{“素元”}q \in \mathbb{Z}[i] : (p) \subseteq (q)\}$$

以上 “素元” 均在相伴意义下计数.

定理 1.11 对于素数 p, $\mathbb{Z}[i]$ 的素元 $q|p$,

(1) $p = 2$ 时, 唯一的选择是 $q = 1 + i$, 则

$$\mathsf{e}(q|p) = 2 \qquad \mathsf{f}(q|p) = 1 \qquad \mathsf{r}(p) = 1$$

(2) $p \equiv 3 \mod 4$ 时, 唯一的选择是 $q = p$, 则

$$\mathsf{e}(q|p) = 1 \qquad \mathsf{f}(q|p) = 2 \qquad \mathsf{r}(p) = 1$$

(3) $p \equiv 1 \mod 4$ 时, 唯一的选择是 $q = a + bi$ 或 $q = a - bi$, 则

$$\mathsf{e}(q|p) = 1 \qquad \mathsf{f}(q|p) = 1 \qquad \mathsf{r}(p) = 2$$

证明 根据 (1.6), 以及 (1.8) 容易计算得到. □

1.4 应用—勾股方程

命题 1.12 勾股方程

$$X^2 + Y^2 = Z^2$$

在相差一个顺序下的通解为

$$X = u^2 + v^2 \qquad Y = 2uv \qquad Z = u^2 - v^2$$

其中 $u, v \in \mathbb{Z}$.

证明 先不放假设 X,Y 互素, 将方程变形为

$$(X+Yi)(X-Yi)=Z^2$$

因为 $2X=(X+Yi)+(X-Yi), 2iY=(X+Yi)-(X-Yi)$, 故二者公因子为 2 的因子, 若不是 1, 则 $2|\mathcal{N}(X+Yi)=Z^2$, 于是 $2|Z$, 这迫使 X,Y 都是奇数, 但是 $X^2+Y^2\equiv 1+1\neq 0\equiv Z^2 \mod 4$ 意义下, 矛盾. 从而根据唯一分解,

$$X+Yi=u(a+bi)^2 \qquad X-Yi=u'(a'+b'i)^2$$

其中 $u,u'\in \text{unit}\,\mathbb{Z}[i]$, 但是二者互为共轭, 故 $X-Yi=\overline{u}(a-bi)^2$, 不妨假设 $u=1$, 则

$$X=u^2+v^2 \qquad Y=2uv \qquad Z=u^2-v^2$$

问题得以解决. □

1.5 应用 — 平方和问题

命题 1.13 *对于 $n\in\mathbb{Z}$, 关于 (X,Y) 的不定方程*

$$X^2+Y^2=n$$

有解当且仅当任意奇素数 $p|n$ 若 $p\equiv 3 \mod 4$, 则 $\operatorname{ord}_p n$ 是偶数.

证明 必要性. 置于 $\mathbb{Z}[i]$ 中考虑, 则化为 $(X+Yi)(X-Y_i)=n$. 若 n 有实不可约因子, 即 $p\equiv 3 \mod 4$, 设 $\operatorname{ord}_p n=k$, 设 $p^i|(X+Yi)$ 以及 $p^{k-i}|(X-Yi)$. 则通过取范数有 $p^{2(k-i)}|X^2+Y^2=n, p^{2i}|X^2+Y^2=n$, 由于 $\operatorname{ord}_p n=k$, 为了防止次数超过, 这迫使 $i=k-i$ 使得 k 为偶数.

充分性. 将 n 唯一分解,

$$n=p_1^{a_1}\dots p_k^{a_k}q_1^{2b_1}\dots q_h^{2b_h} \qquad p_i\equiv 1 \bmod 4 \text{或} p_i=2, \quad q_i\equiv 3 \mod 4$$

其中 p_i,q_j 两两不同. 有 (x_i,y_i) 使得 $p_i=x_i^2+y_i^2$, 则在 $\mathbb{Z}[i]$ 中的唯一分解是

$$n=\prod_{i=1}^{k}(x_i+y_ii)^{a_i}\prod_{i=1}^{k}(x_i-y_ii)^{a_i}\prod_{j=1}^{h}q_i^{2b_i}$$

则设

$$\prod_{i=1}^{k}(x_i+y_i i)^{a_i}\prod_{j=1}^{h}q_i^{b_i}=X+Yi \qquad \prod_{i=1}^{k}(x_i-y_i i)^{a_i}\prod_{j=1}^{h}q_i^{b_i}=X-Yi$$

则 $n=(X+Yi)(X-Yi)=X^2+Y^2$. 故有解. □

命题 1.14 条件承上, 解的个数为

$$4\prod_{\substack{p|n\\ \text{是 } 4k+1 \text{ 型素数或 } 2}}\operatorname{ord}_p n=4\sum_{d|n}\begin{cases}0 & 2|d\\ 1 & d\equiv 1 \mod 4\\ -1 & d\equiv 3 \mod 4\end{cases}$$

证明 其解数应当是范数为 n 的 Gauss 整数个数为了数清解数, 对于

$$n=2^m p_1^{a_1}\dots p_k^{a_k}q_1^{b_1}\dots q_h^{b_h} \qquad p_i\equiv 1 \mod 4 \qquad q_j\equiv 3 \mod 4$$

其中 p_i,q_j 两两不同. 显然, 各素因子在相差一个单位的意义下各司其职, 可使用乘法原理.

- 对于 $n=2^m=i^m(1-i)^{2m}$ 时, 在相差单位的意义下, 解数为 1.
- 对于 $n=p^a=(x-yi)^a(x+yi)^a$ 时, 在相差单位的意义下, 解数为 a.
- 对于 $n=q^b$ 时, 在相差单位的意义下, 解数为 1.

考虑到单位有四个, 故解数为 $4a_1\dots a_k$. 考虑多项式

$$f(X,Y,Z)=(1+\dots+X^m)\prod_{i=1}^{k}(1+\dots+Y^{a_i})\prod_{j=1}^{h}(1+\dots+Z^{b_j})$$

则 n 的 $4k+1$ 型因数的数量为上多项式展开后所有 X 的次数为 0, Z 的次数为偶数的单项式的系数和; $4k+3$ 型则是 X 的次数为 0, Z 的次数为奇数的单项式的系数和. 故当 b_i 是偶数时,

$$\sum_{d|n}\begin{cases}0 & 2|d\\ 1 & d\equiv 1 \mod 4\\ -1 & d\equiv 3 \mod 4\end{cases}=f(0,1,-1)=\prod a_i$$

计数完毕. □

1.6 另例—$\mathbb{Z}[\sqrt{2}]$

定义 1.15 我们下面记

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$$

这显然是一个整环. 可以也在上面定义范数

$$\mathcal{N}(a + b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Z}$$

容易知道 $\mathcal{N} : \mathbb{Z}[i] \to \mathbb{Z}$ 保持乘法, 且 $\mathcal{N}(x) = 0 \iff x = 0$. 并且我们继续沿袭 *(B.9)* 的整除和相伴的记号和 *(B.10)* 的定义.

下面, 沿着 Gauss 整环的理论建立过程, 我们对 $\mathbb{Z}[\sqrt{2}]$ 作同样的事儿.

命题 1.16 $\mathbb{Z}[\sqrt{2}]$ 上的单位正是那些范数为单位的元素. 即

$$\operatorname{unit} \mathbb{Z}[\sqrt{2}] = \mathcal{N}^{-1}(\{\pm 1\})$$

定理 1.17 在 $\mathbb{Z}[\sqrt{2}]$ 上有带余除法. 具体来说任何 $a, b \in \mathbb{Z}[\sqrt{2}]$, 其中 $b \neq 0$, 都存在 $d, r \in \mathbb{Z}[i]$ 使得

$$a = db + r \qquad |\mathcal{N}r| < |\mathcal{N}b|$$

证明 设

$$\frac{a}{b} = u + v\sqrt{2} \qquad u, v \in \mathbb{Q}$$

选择与 u, v 最接近的整数 x, y, 并取 $d = x + y\sqrt{2}$, $r = a - db$, 且

$$\begin{aligned}
|\mathcal{N}r| &= |\mathcal{N}(b(a/b - d))| && \because \mathcal{N} \text{ 可延拓到 } \mathbb{Q}[\sqrt{2}] \\
&= |\mathcal{N}b||\mathcal{N}((u - x) + (v - y)\sqrt{2})| \\
&= |\mathcal{N}b|\left|(u - x)^2 - 2(v - y)^2\right| && \because |u - x|, |v - y| < \tfrac{1}{2} \\
&\leq |\mathcal{N}b|\left(\tfrac{1}{4} + 2\tfrac{1}{4}\right) \\
&< |\mathcal{N}b|
\end{aligned}$$

命题得证. □

推论 1.18 $\mathbb{Z}[\sqrt{2}]$ 是是主理想整环, 进而是唯一分解整环.

定理 1.19 $\mathbb{Z}[\sqrt{2}]$ 上的素元有如下刻画

(1) 有理数 $p \in \mathbb{Z}[\sqrt{2}]$ 是素元

$$\iff p \in \mathbb{Z} \text{ 是素数, 且不存在 } a, b \in \mathbb{Z}, \text{s.t.} |a^2 - 2b^2| = p$$

$$\iff p \in \mathbb{Z} \text{ 是素数, 且 } p \equiv \pm 3 \bmod 8.$$

(2) 无理数 $(b \neq 0)$, $a + bi \in \mathbb{Z}[\sqrt{2}]$ 是素元

$$\iff |\mathcal{N}(a+bi)| = |a^2-2b^2| \text{ 是素数 } p, \text{ 且存在 } a, b \in \mathbb{Z}, \text{s.t.} |a^2-2b^2| = p.$$

$$\iff |\mathcal{N}(a+bi)| = |a^2 - 2b^2| \text{ 是素数 } p, \text{ 并且 } p \equiv \pm 1 \bmod 8 \text{ 或 } p = 2.$$

证明 证明与 (1.5) 相似, 同时需要 (A.6) 对 $\left(\frac{2}{p}\right)$ 的计算. □

推论 1.20 对于素数 $p \in \mathbb{Z}$, 其在 $\mathbb{Z}[i]$ 中的分解有三种情况

(1) $p = 2$, 则 $2 = \sqrt{2}^2$. (分歧的)

(2) $p \equiv \pm 3 \mod 8$, 则 $p = p$. (惰性的)

(3) $p \equiv \pm 1 \mod 8$, 则 $p = \pm(a + b\sqrt{2})(a - b\sqrt{2})$, 其中 $a, b \in \mathbb{Z}$. (分裂的)

前面的部分大抵与 Gauss 整环 $\mathbb{Z}[i]$ 类似, 但是关于单位, 似乎不尽相同.

定理 1.21 整环 $\mathbb{Z}[\sqrt{2}]$ 的全部单位是

$$\pm(1 + \sqrt{2})^n \qquad n \in \mathbb{Z}$$

证明 我们已经知道 (1.16) 单位就是那些范数是 ± 1 的元. 换句话说我们要解方程

$$X^2 - 2Y^2 = \pm 1$$

我们证明所有的解 $X + \sqrt{2}Y$ 都是 $\pm(1 + \sqrt{2})^n$. 首先, 通过不断除以 $1 + \sqrt{2}$, 即乘以 $1 - \sqrt{2}$, 以及调整正负号, 可以假设

$$1 \leq X + \sqrt{2}Y < 1 + \sqrt{2}$$

可得到

$$\sqrt{2}-1<\pm(X-\sqrt{2}Y)\leq 1\leq X+\sqrt{2}Y<1+\sqrt{2}$$

对于 $\pm=-$ 的情形,

$$X=\frac{(X+\sqrt{2}Y)-(\sqrt{2}Y-X)}{2}<\frac{(1+\sqrt{2})-(\sqrt{2}-1)}{2}=1$$

这迫使 $X=0$, 此时无解. 对于 $\pm=+$ 的情形,

$$Y=\frac{(X+\sqrt{2}Y)-(X-\sqrt{2}Y)}{2\sqrt{2}}<\frac{(1+\sqrt{2})-(\sqrt{2}-1)}{2\sqrt{2}}=\frac{1}{\sqrt{2}}<1$$

这迫使 $Y=0$, 此时唯一的解是 $X=1$, 命题得证. □

以上证明是 Pell 方程的标准证明, 一个一般 Pell 方程的简单的证明参见 [12]P260 Chapter 34.

1.7 应用 — Fermat-Wiles 大定理的伪证

如果伪证也算应用的话...

定理 1.22 (Fermat-Wiles 大定理) 对于 $n\geq 3$, 如下方程没有非零整数解

$$X^n+Y^n=Z^n$$

伪证 (Lamé) 由于 "写不下", 我们只给出证明的框架. 首先, 注意到, 只需要证明对所有奇素数 p 证明即可. 将 $X^p+Y^p=Z^p$ 改写为

$$X^p+Y^p=(X+Y)(\zeta X+\zeta^{-1}Y)\dots(\zeta^{-1}X+\zeta Y)=Z^p$$

其中 $\zeta=\mathrm{e}^{2\pi i/p}$ 是 p 次本原单位根. 而根据唯一分解性,

$$\zeta^i X+\zeta^{-i}Y=u_i a_i^p \qquad u_i\text{是单位}$$

不妨调整 $u_i=1$. 注意到如下恒等式

$$(\zeta^i X+\zeta^{-i}Y)+(\zeta^j X+\zeta^{-j}Y)=(\zeta^{\frac{i-j}{2}}+\zeta^{-\frac{i-j}{2}})(\zeta^{-\frac{i+j}{2}}X+\zeta^{-\frac{i+j}{2}}Y)$$

其中 $x/2$ 是 mod$p$ 意义下的除法. 注意到 $(\zeta^{\frac{i-j}{2}}+\zeta^{-\frac{i-j}{2}})$ 不是一个 p 次幂. 将其改写为

$$a_i^p+a_j^p=z_{\frac{i-j}{2}}a_{\frac{i+j}{2}}^p$$

当 $i=1,j=3$ 时, $a_1^p+a_3^p=z_1a_2^p$, 这迫使 $z_1|a_1^p+a_3^p$. 这是不可能的[7]. □

以上伪证采自 [7], 其第一个错误[8] 在于假设 $\mathbb{Z}[\zeta]$ 是唯一分解整环. 倘若想要延续这一思路给出一个像样的证明, 则需要更多的知识, 参见 [8]P101 Chapter 6.

例 1.23 实际上, 很多环都不是唯一分解整环, 例如

$$\mathbb{Z}[\sqrt{-5}]=\{n+m\sqrt{-5}:n,m\in\mathbb{Z}\}\subseteq\mathbb{C}$$

容易验证这是一个整环, 但是.

- 2 不是素元. 由于

  $$6=2\times3=(1+\sqrt{-5})(1-\sqrt{-5})$$

  而 $\frac{2}{1\pm\sqrt{-5}}=\frac{1\mp\sqrt{-5}}{3}\notin\mathbb{Z}[\sqrt{-5}]$ 从而 2 不整除 $1\pm\sqrt{-5}$, 但是 $2|6$.

- 2 是不可约元. 若

  $$2=(a+b\sqrt{-5})(c+d\sqrt{-5})$$

  则取作为复数的模长的平方可知

  $$4=(a^2+5b^2)(c^2+5d^2)$$

  这迫使 $b=d=0$, 从而 $ac=2$ 可得 $a=\pm2$ 或 $b=\pm2$.

[7]这一步是最扯的.
[8]虽然之后错误不计其数.

Chapter 2

Dedekind 整环

2.1 Dedekind 整环的性质

I. Dedekind 整环的唯一分解

定义 2.1 (Dedekind 整环) 一个整环 A, 如果是 *Nother* 的 *(C.3)*, 整闭的 *(C.17)*, 以及所有理想都是有限生成的[1], 则称 A 是 **Dedekind 整环**.

我们建立唯一分解的一个重要步骤是消去律的存在, 但是在理想上这件事并不容易, 为此我们定义分式理想.

定义 2.2 (分式理想) 对于整环 A, 所有形如

$$\frac{\mathfrak{a}}{x} \qquad \mathfrak{a} \subseteq A \text{ 是理想}, x \in R \setminus 0$$

的集合被称为 A 的 **分式 (fractional) 理想**. 对应地, 称原本的那些理想为 A 的 **整 (integral) 理想**. 对于分式理想, 也有自然的加法, 交以及乘法.

对于 $\frac{x}{y} \in \mathrm{Frac}A$, 记 $\left(\frac{x}{y}\right) = \frac{(x)}{y}$ 就是一个分式理想, 这被称为 **主分式理想**.

这等价于说 $\mathfrak{f}$ 是分式理想指的是满足 $x\mathfrak{f} \subseteq A$ 对某个 $x \in A \setminus 0$ 的 $\mathrm{Frac}A$ 中的某个 A-子模 $\mathfrak{f}$. 对于 *Noether* 整环, 这等价于说分式理想是一个 $\mathrm{Frac}A$ 中

[1] 这在代数几何中对应为 "维数为 1".

的有限生成 A-子模 [2].

定义 2.3 (可逆) 对于整环 A 的分式理想 $\mathfrak{f}$, 若存在分式理想 $\mathfrak{g}$ 使得 $\mathfrak{fg} = A$, 则称 $\mathfrak{f}$ 是 可逆的, 并记 $\mathfrak{g} = \mathfrak{f}^{-1}$.

显然, 在可逆时下, 逆是唯一的, 记号承上, $\mathfrak{g} = \{x \in \mathrm{Frac}A : x\mathfrak{f} \subseteq A\}$. 显然, 在 $\mathfrak{f}$ 是非零主分式理想 (x) 时, $(x)^{-1} = (x^{-1})$.

定理 2.4 对于 *Dedekind* 整环 A, 任何 A 的理想 $\mathfrak{a}$ 可以唯一地写成一些素理想的乘积

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_n = \{ \textstyle\sum p_1 \dots p_n : p_i \in \mathfrak{p}_i \}$$

且, 全体非零分式理想都可逆, 且关于分式理想的乘法构成一个 *Abel* 群, 单位元是理想 A 本身, $\mathfrak{f}$ 的逆元是 $\mathfrak{f}^{-1}$. 且这个群是自由的, 全体素理想是一组基.

证明 实际上, 为了证明了全体非零分时理想构成 Abel 群的论断, 我们只要证明全体非零理想都可逆. 因为任何非零分式理想 $\frac{\mathfrak{a}}{x}$, 其逆就是 $x\mathfrak{a}^{-1}$. 这还可以得到任何非零分式理想即两个非零整理想的商[3]. 而假如证明了唯一分解的性质, 容易得到全体素理想是一组基.

这个证明来自 Van der Waerden. 这个证明的首尾两段可以类比 (B.11).

先证明任何 A 的理想 $\mathfrak{a}$ 包含一些非零素理想的乘积. 假如不对, 则可以挑选极大的不满足条件的理想 $\mathfrak{a}$, 注意此时 $\mathfrak{a}$ 不是素理想, 从而存在两个理想 $\mathfrak{a}_1, \mathfrak{a}_2$ 使得

$$\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a} \qquad \mathfrak{a}_1 \nsubseteq \mathfrak{a} \qquad \mathfrak{a}_2 \nsubseteq \mathfrak{a}$$

用 $\mathfrak{a} + \mathfrak{a}_i$ 替代 $\mathfrak{a}_i$, 则条件还可以强化为

$$\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a} \qquad \mathfrak{a} \subsetneq \mathfrak{a}_1 \qquad \mathfrak{a} \subsetneq \mathfrak{a}_2$$

但是这样根据 $\mathfrak{a}$ 的极大性, $\mathfrak{a}_1, \mathfrak{a}_2$ 就是一些素理想的乘积, 矛盾.

[2]因为, 对于 Noether 整环, 任何理想都是有限生成的, 除以一个分母也是有限生成的; 反之, 将那些生成元的分母乘起来就可以作为一致的分母, 可得其某个非零倍数是 A 中的有限生成 A-模, 即 A 的理想.

[3]一边是因为构成群, 另一边是因为 $\frac{\mathfrak{a}}{x} = \mathfrak{a}(x)^{-1}$.

再证明非零素理想都是可逆的. 对于非零素理想 $\mathfrak{p}$, 考虑

$$[A:\mathfrak{p}] := \{x \in \mathrm{Frac}A : x\mathfrak{p} \subseteq A\} \supseteq A$$

现在,

$$\mathfrak{p} \subseteq \mathfrak{p} \cdot [A:\mathfrak{p}] \subseteq A$$

这迫使左右两边的包含取到一个等号, 我们希望右边取到等号, 这样本段就证明结束了. 如果左边取到等号, 任意 $x \in [A:\mathfrak{p}]$, 有 $x\mathfrak{p} \subseteq \mathfrak{p}$, 因为 $\mathfrak{p}$ 是 $\mathrm{Frac}A$ 中有限生成的 A-模, 根据 (C.11), 这说明 x 在 A 上整, 根据整闭性, $x \in A$, 这意味着 $A = [A:\mathfrak{p}]$.

但这是不可能的, 取 $a \in \mathfrak{p} \setminus 0$, 则根据第一段

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq aA \subseteq \mathfrak{p}$$

则存在某个素理想 $\mathfrak{p}_i \subseteq \mathfrak{p}$, 因为维数为 1 的假设, $\mathfrak{p} = \mathfrak{p}_i$, 不妨设 $\mathfrak{p}_1 = \mathfrak{p}$, 这样

$$\mathfrak{p}\frac{\mathfrak{p}_2 \dots \mathfrak{p}_r}{a} \subseteq A \quad \Rightarrow \quad \frac{\mathfrak{p}_2 \dots \mathfrak{p}_r}{a} \subseteq [A:\mathfrak{p}] \quad \Rightarrow \quad \frac{\mathfrak{p}_2 \dots \mathfrak{p}_r}{a} \subseteq A$$

即

$$\mathfrak{p}_2 \dots \mathfrak{p}_r \subseteq aA \subseteq \mathfrak{p}$$

假如我们一开始假设取 r 是最小的, 就产生了矛盾.

接着证明非零理想都是可逆的. 假如不对, 则可以挑选极大的不满足条件的理想 $\mathfrak{a}$, 注意此时 $\mathfrak{a}$ 不是素理想, 从而存在素理想 $\mathfrak{p}$ 使得 $\mathfrak{a} \subsetneq \mathfrak{p}$, 则

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a} \cdot [A:\mathfrak{a}] \subseteq A$$

第一个包含关系的等号不能取到, 假如取到则任意 $x \in \mathfrak{p}^{-1}$, 有 $x\mathfrak{a} \subseteq \mathfrak{a}$, 因为 $\mathfrak{a}$ 是 $\mathrm{Frac}A$ 中有限生成的 A-模, 根据 (C.11), $x \in A$, 我们第二段已经证明过 $A \neq \mathfrak{p}^{-1}$ 了. 根据极大性, $\mathfrak{a}\mathfrak{p}^{-1}$ 是可逆的, 则 $(\mathfrak{a}\mathfrak{p}^{-1})^{-1}\mathfrak{p}^{-1}$ 是 $\mathfrak{a}$ 的逆.

最后证明唯一分解性. 假如不对, 则可以挑选极大的不满足条件的理想 $\mathfrak{a}$, 注意此时 $\mathfrak{a}$ 不是素理想, 从而存在素理想 $\mathfrak{p}$ 使得 $\mathfrak{a} \subsetneq \mathfrak{p}$, 则

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a} \cdot [A:\mathfrak{a}] \subseteq A$$

第一个包含关系的等号同样不能取到, 那么根据极大性, $\mathfrak{a}\mathfrak{p}^{-1}$ 可以写成一些素理想的乘积, 则

$$\mathfrak{a} = (\mathfrak{a}\mathfrak{p}^{-1})\mathfrak{p}$$

也是一些素理想的乘积. 而如果一个理想

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_n = \mathfrak{q}_1 \dots \mathfrak{q}_m$$

那么

$$\mathfrak{q}_1 \dots \mathfrak{q}_m = \mathfrak{p}_1 \dots \mathfrak{p}_n \subseteq \mathfrak{p}_1$$

根据素理想的条件, 必定有一个 $\mathfrak{q}_i \subseteq \mathfrak{p}_1$, 根据维数为 1, $\mathfrak{q}_i = \mathfrak{p}_1$, 两边同时乘以 $\mathfrak{p}^{-1}$ 消去 $\mathfrak{p}$, 可以持续下去得到 $n = m$ 和置换 $\sigma \in \mathfrak{S}_n$, 使得 $\mathfrak{p}_{\sigma(i)} = \mathfrak{q}_i$, 命题得证. □

定义 2.5 (类群) 对于 *Dedekind* 整环 A, 记

$$\mathcal{I}(A) = \text{全体非零分式理想} \quad \supseteq \quad \mathcal{P}(A) = \text{全体非零分式主理想}$$

他们都构成 *Abel* 群, A 的 **类 (class) 群** 和 **类数** 被定义为

$$\textsc{Class}(A) = \mathcal{I}(A)/\mathcal{P}(A) \qquad \textsc{class}(A) = |\textsc{Class}(A)|$$

显然, $\textsc{Class}(A)$ 是平凡群 $\iff \textsc{class}(A) = 1 \iff A$ 是主理想整环.

例 2.6 实际上, *(C.16)* 介绍的二次扩张都是 *Dedekind* 整环. 关于维数为 1 是根据 *(C.22)*, 整闭和 *Noether* 不难验证.

例 2.7 当 $A = \mathbb{Z}[i]$ 或 $A = \mathbb{Z}[\sqrt{2}]$ 时, 根据第一章, 他们都是主理想整环, 故 $\textsc{class}(A) = 1$. 除此之外, 还有很多可以验证有带余除法的环如 $A = \mathbb{Z}\left[\frac{1-\sqrt{-3}}{2}\right]$, $A = \mathbb{Z}\left[\frac{\sqrt{5}-1}{2}\right]$.

例 2.8 回忆 *(1.23)*, 当 $A = \mathbb{Z}[\sqrt{-5}]$ 时, 在后面 *(2.27)* 我们会知道她是 *Dedekind* 整环, 不过目前我们知道其不是主理想整环, 故 $\textsc{class}(A) > 1$. 实际上可以将 6 的分解改写为主理想的乘法

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

依托于此, 可以给出 (6) 的唯一分解.

- 考虑理想 $(2,1+\sqrt{-5})$, 不难验证, [4] 当中的元素形如 $x+y\sqrt{-5}$, 其中 x,y 同奇偶. 若

$$(a+b\sqrt{-5})(c+d\sqrt{-5})=ac-5bd+(ad+bc)\sqrt{-5}\in(2,1+\sqrt{-5})$$

  则 $ac-5bd$ 与 $ad+bc$ 同奇偶. 这迫使 a,b 同奇偶, 或 c,d 同奇偶[5]. 这可以得到 $(2,1+\sqrt{-5})$ 是素理想.

- 类似可以得到 $(2,1-\sqrt{-5})=(2,1+\sqrt{-5})$ 也是素理想.

- 再考虑 $(3,1+\sqrt{-5})$, 其形式容易验证为 $x+y\sqrt{-5}$, 满足 $x-y$ 是 3 的倍数, 这样若

$$(a+b\sqrt{-5})(c+d\sqrt{-5})=ac-5bd+(ad+bc)\sqrt{-5}\in(3,1+\sqrt{-5})$$

  有 $ac-5bd-ad-bc\equiv 0 \mod 3$ 即

$$ac-5bd-ad-bc\equiv ac+bd-ad-bc=(a-b)(c-d)\equiv 0 \mod 3$$

  因为 $\mathbb{Z}/3\mathbb{Z}$ 是整环, 故 $a-b\equiv 0 \bmod 3$ 或 $c-d\equiv 0 \bmod 3$, 这证明了 $(3,1+\sqrt{-5})$ 是素理想.

- 类似地考虑 $(3,1-\sqrt{-5})$, 其形式容易验证为 $x+y\sqrt{-5}$, 满足 $x+y$ 是 3 的倍数, 故 $(3,1+\sqrt{-5})\neq(3,1-\sqrt{-5})$, 同样可以验证其是素理想.

- 从而我们得到了不可约元的分解

$$(2,1\pm\sqrt{5})(3,1\pm\sqrt{5})=(6,1\pm\sqrt{5})=(1\pm\sqrt{5})$$

$$(2)=(2,1+\sqrt{-5})^2 \qquad (3)=(3,1+\sqrt{-5})(3,1-\sqrt{-5})$$

故实际上 "理想的唯一分解" 是这样的

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

Dedekind 所创造的 "理想" 这一概念, 就源起于本仅存于意识和虚妄或者说理想之中的那个 2 和 $1+\sqrt{-5}$ 的最大公约数.

[4] 因为形如 $2(a+b\sqrt{-5})+(1+\sqrt{-5})(c+d\sqrt{-5})=2a+c-5d+(2b+c+d)\sqrt{5}$, 端详其形式可知.

[5] 假如 a,b 不同奇偶, c,d 不同奇偶, 这样,

$$ac-5bd\equiv ac+(a+1)(c+1)\equiv a+c+1 \qquad ad+bc\equiv a(c+1)+(a+1)c\equiv a+c$$

不可能同奇偶.

II. Dedekind 整环的算术

记号 2.9 (整除) 源自数论的记号, 我们约定, 对于整理想 $\mathfrak{a},\mathfrak{b}$, 整除

$$\mathfrak{a}|\mathfrak{b} \iff \mathfrak{b}\subseteq\mathfrak{a}$$

定义 2.10 (阶) 对于 *Dedekind* 整环 A 的非零素理想 $\mathfrak{p}$, 分式理想 $\mathfrak{f}$, 假如

$$\mathfrak{f}=\mathfrak{p}_1^{f_1}\dots\mathfrak{p}_r^{f_r}$$

是 $\mathfrak{f}$ 的唯一分解, 且 $\mathfrak{p}_i$ 是两两不同的非零素理想, 定义 阶 **(order)**

$$\operatorname{ord}_{\mathfrak{p}}\mathfrak{f}=\begin{cases}a_i & \mathfrak{p}=\mathfrak{p}_i\text{对某个 }i\\ 0 & \text{其他情况}\end{cases}$$

此即 $\mathfrak{f}$ 的唯一分解中 $\mathfrak{p}$ 的指数. 约定 $\operatorname{ord}_{\mathfrak{p}}0=\infty$. 同时记 $\operatorname{ord}_{\mathfrak{p}}a$ 是 $\operatorname{ord}_{\mathfrak{p}}(a)$ 的简写.

评注 2.11 实际上, 按照 *(2.5)* 的记号, 若记 A 的全体素理想是 $\operatorname{spec}A$, 则

$$\varphi:\mathcal{I}(A)\xrightarrow{\sim}\mathbb{Z}^{\oplus\operatorname{spec}A}\qquad \mathfrak{f}\longmapsto(\operatorname{ord}_{\mathfrak{p}}\mathfrak{f})_{\mathfrak{p}\in\operatorname{spec}A}$$

给出一个同构, 其逆映射是

$$\psi:\mathbb{Z}^{\oplus\operatorname{spec}A}\xrightarrow{\sim}\mathcal{I}(A)\qquad (a_{\mathfrak{p}})_{\mathfrak{p}\in\operatorname{spec}A}\longmapsto\prod\mathfrak{p}^{a_{\mathfrak{p}}}$$

定理 2.12 对于 *Dedekind* 整环 A, 两个理想 $\mathfrak{a},\mathfrak{b}$, 假设其唯一分解为

$$\mathfrak{a}=\mathfrak{p}_1^{a_1}\dots\mathfrak{p}_r^{a_r}\qquad \mathfrak{b}=\mathfrak{p}_1^{b_1}\dots\mathfrak{p}_r^{b_r}$$

其中 $\{\mathfrak{p}_i\}$ 是两两不同的素理想[6]. 则

(1) $\mathfrak{a}|\mathfrak{b}\iff a_i\le b_i$ 即对于任何非零素理想 $\mathfrak{p}$, $\operatorname{ord}_{\mathfrak{p}}\mathfrak{a}\le\operatorname{ord}_{\mathfrak{p}}\mathfrak{b}$.

(2) $\mathfrak{a}+\mathfrak{b}=\mathfrak{p}_1^{c_1}\dots\mathfrak{p}_r^{c_r}$, 其中 $c_i=\min(a_i,b_i)$. 即 $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}+\mathfrak{b})=\min(\operatorname{ord}_{\mathfrak{p}}\mathfrak{a},\operatorname{ord}_{\mathfrak{p}}\mathfrak{b})$.

(3) $\mathfrak{a}\cap\mathfrak{b}=\mathfrak{p}_1^{d_1}\dots\mathfrak{p}_r^{d_r}$, 其中 $d_i=\max(a_i,b_i)$. 即 $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}+\mathfrak{b})=\max(\operatorname{ord}_{\mathfrak{p}}\mathfrak{a},\operatorname{ord}_{\mathfrak{p}}\mathfrak{b})$.

[6] 总可以这样假设, 如果允许某些 a_i,b_i 为零.

(4) 特别地, $\mathfrak{a},\mathfrak{b}$ 互素当且仅当对每个 i, $a_i = 0$ 或 $b_i = 0$.

(5) 特别地, $\mathfrak{p}$ 出现在 $\mathfrak{a}$ 的分解中当且仅当 $\mathfrak{a} \subseteq \mathfrak{p}$.

证明 (1) 充分性显然. 反之, 若 $\mathfrak{b} \subseteq \mathfrak{a}$, 可以作 $\mathfrak{a}^{-1} \cdot \mathfrak{b} \subseteq A$ 的唯一分解, 立刻会得到 $a_i \le b_i$. (2) 是因为 $\mathfrak{a}+\mathfrak{b}$ 是包含 $\mathfrak{a},\mathfrak{b}$ 的最小的理想. (3) 是因为 $\mathfrak{a}\cap\mathfrak{b}$ 是包含于 $\mathfrak{a},\mathfrak{b}$ 的最大的理想. (4)(5) 显然. □

推论 2.13 关于阶, 有如下不难验证的事实,

(1) $\operatorname{ord}_{\mathfrak{p}} \mathfrak{a} = a \iff \mathfrak{p}^a \mid \mathfrak{a}$但$\mathfrak{p}^{a+1} \nmid \mathfrak{a}$

(2) $\operatorname{ord}_{\mathfrak{p}} a = n \iff a \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$

(3) $\operatorname{ord}_{\mathfrak{p}} \mathfrak{fg} = \operatorname{ord}_{\mathfrak{p}} \mathfrak{f} + \operatorname{ord}_{\mathfrak{f}} \mathfrak{g}$

(4) $\operatorname{ord}_{\mathfrak{p}}(x+y) \ge \min(\operatorname{ord}_{\mathfrak{p}} x, \operatorname{ord}_{\mathfrak{p}} y)$

其中 $\mathfrak{a}$ 是整理想, $\mathfrak{f},\mathfrak{g}$ 是分式理想, $a,x,y \in A$.

回忆互素的定义 (B.4).

命题 2.14 对于 *Dedekind* 整环 A 的有限个非零素理想 $\mathfrak{p}_1,\dots,\mathfrak{p}_r$, 任意非负整数 $n_1,\dots,n_r$, 必存在 $x \in A$ 使得

$$\operatorname{ord}_{\mathfrak{p}_i} x = n_i \qquad \forall i = 1,\dots,r$$

证明 根据 (2.13) 之 (2), 因为唯一分解性 $\mathfrak{p}^{n_i} \supsetneq \mathfrak{p}^{n_i+1}$, 故可以挑选 $x_i \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$, 这样再根据 (2.12), 以及中国剩余定理 (B.8) 存在

$$x \equiv x_i \mod \mathfrak{p}_i^{n_i+1} \qquad \forall i = 1,\dots,r$$

此时 $\operatorname{ord}_{\mathfrak{p}_i} x = n_i$. □

推论 2.15 如果 *Dedekind* 整环只有有限个素理想, 则是主理想整环.

证明 根据 (2.14), 因为只有有限个素理想, 任何理想 $\mathfrak{a}$ 都存在 a 使得 $\operatorname{ord}_{\mathfrak{p}} \mathfrak{a} = \operatorname{ord}_{\mathfrak{p}} a$. 这就说明 $\mathfrak{a} = (a)$. □

命题 2.16 对于 *Dedekind* 整环的理想 $\mathfrak{b}$, 任意非零理想 $\mathfrak{a} \subseteq \mathfrak{b}$, 都存在主理想 (a) 使得 $\mathfrak{b} = \mathfrak{a} + (a)$.

证明 考虑那些出现在 $\mathfrak{a}$ 和 $\mathfrak{b}$ 分解之中的素理想 $\mathfrak{p}_1, \dots, \mathfrak{p}_r$, 根据 (2.14), 取 $a \in A$ 使得

$$\operatorname{ord}_{\mathfrak{p}_i} a = \operatorname{ord}_{\mathfrak{p}_i} \mathfrak{b} \leq \operatorname{ord}_{\mathfrak{p}_i} \mathfrak{a}$$

则

$$\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a} + (a)) = \min(\operatorname{ord}_{\mathfrak{p}} \mathfrak{a}, \operatorname{ord}_{\mathfrak{p}} a) = \begin{cases} \operatorname{ord}_{\mathfrak{p}_i} \mathfrak{b} & \mathfrak{p} = \mathfrak{p}_i \\ 0 & \text{其他情况} \end{cases} = \operatorname{ord}_{\mathfrak{p}} \mathfrak{b}$$

命题得证. □

推论 2.17 (一又二分之一定理) 对于 *Dedekind* 整环的理想 $\mathfrak{a}$, 任意 $a \in \mathfrak{a} \setminus 0$, 都存在 $b \in \mathfrak{a}$ 使得 $(a, b) = \mathfrak{a}$.

特别地, *Dedekind* 整环的任何理想都可以由两个元生成.

命题 2.18 对于 *Dedekind* 整环的理想 $\mathfrak{a}$, $\mathfrak{c}$, 存在理想 $\mathfrak{b}$ 使得

$$\mathfrak{a}\mathfrak{b}\text{是主理想} \qquad \mathfrak{c} + \mathfrak{b} = (1)$$

即是说任何理想在类群中的逆都可以取得不出现预先给点的一些素理想.

证明 考虑 $\mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}$, 则存在 a 使得 $\mathfrak{a}\mathfrak{c} + (a) = \mathfrak{a}$, 两边同时除以 $\mathfrak{a}$, 得到

$$\mathfrak{c} + (a) \cdot \mathfrak{a}^{-1} = (1)$$

取 $\mathfrak{b} = (a) \cdot \mathfrak{a}^{-1}$ 即满足条件. □

III. Dedekind 整环的局部化 回忆局部化 §C.3.

命题 2.19 对于 *Dedekind* 整环的局部化还是 *Dedekind* 整环. 具体来说, 对于 *Dedekind* 整环 A, 乘性子集 S, 则局部化 $S^{-1}A$ 还是 *Dedekind* 整环[7].

[7]排除平凡的情况, 如 $0 \in S$ 以及 $S = A \setminus 0$.

并且, $\mathfrak{a}$ 的唯一分解将给出 $S^{-1}\mathfrak{a}$ 的唯一分解

$$\mathfrak{a}=\prod_{i=1}^{r}\mathfrak{p}_i^{a_i}\quad\Rightarrow\quad S^{-1}\mathfrak{a}=\prod_{i\in I}(S^{-1}\mathfrak{p}_i)^{a_i}$$

其中 $\mathfrak{p}_i$ 是不同的素理想, $S^{-1}\mathfrak{p}_i$ 也是不同的素理想, $I=\{i:S\cap\mathfrak{p}_i=\varnothing\}$.

证明 前一个论断只需要验证定义的三条, 根据 (C.8) 理想的对应, 是 Noether 的. 根据 (C.8) 素理想的对应, 维数至多为 1, 因为排除了平凡的情况, 故维数为 1. 再根据 (C.14), $S^{-1}A$ 在 $S^{-1}\mathrm{Frac}A=\mathrm{Frac}A$ 的整闭包为 $S^{-1}A$ 本身, 故整闭.

第二个论断需要注意到

$$S^{-1}\mathfrak{a}S^{-1}\mathfrak{b}=\left\{\sum\frac{ab}{s}:\begin{array}{c}\{a\}\subseteq A\\ \{b\}\subseteq B\\ \{s\}\subseteq S\end{array}\right\}\overset{\text{通分}}{=}\left\{\frac{\sum ab}{s}:\begin{array}{c}\{a\}\subseteq A\\ \{b\}\subseteq B\\ s\in S\end{array}\right\}=S^{-1}\mathfrak{a}\mathfrak{b}$$

根据 (C.8), 经过局部化只有那些 $S\cap\mathfrak{p}=\varnothing$ 的素理想幸存, 且 $S^{-1}\mathfrak{p}$ 是 $S^{-1}A$ 的素理想. 否则 $S^{-1}\mathfrak{p}=S^{-1}A$, 故命题得证. □

推论 2.20 对于 *Dedekind* 整环 A, 非零素理想 $\mathfrak{p}$, 则

$$\mathfrak{a}A_{\mathfrak{p}}=(\mathfrak{p}A_{\mathfrak{p}})^{v}\qquad v=\mathrm{ord}_{\mathfrak{p}}\,\mathfrak{a}$$

而我们关心对一个非零素理想的局部化, 回忆对一个素理想的局部化 (C.9). 为了准确表述其性质, 我们先回忆离散赋值整环 §C.5.

命题 2.21 对于 *Dedekind* 整环 A, 非零素理想 $\mathfrak{p}$, 则 $A_{\mathfrak{p}}$ 是离散赋值环, 赋值就是 $\mathrm{ord}_{\mathfrak{p}}$.

证明 根据 (2.13), $\mathrm{ord}_{\mathfrak{p}}$ 确实满足赋值的条件. 我们验证

$$A_{\mathfrak{p}}=\{x\in\mathrm{Frac}A:\mathrm{ord}_{\mathfrak{p}}\,x\geq 0\}$$

任意取 $\frac{x}{y}\in A_{\mathfrak{p}}$, 其中 $x\in A, y\notin\mathfrak{p}$, 那么

$$\mathrm{ord}_{\mathfrak{p}}\,x\geq 0,\mathrm{ord}_{\mathfrak{p}}\,y=0\quad\Rightarrow\quad\mathrm{ord}\,\frac{x}{y}\geq 0$$

反之, 若 $\operatorname{ord}_{\mathfrak{p}} x \geq 0$, 我们要取 $a \notin \mathfrak{p}$ 使得 $ax \in A$, 根据 (2.14) 取 a 满足

$$\forall \operatorname{ord}_{\mathfrak{p}} x < 0, \quad \operatorname{ord}_{\mathfrak{p}} a = |\operatorname{ord}_{\mathfrak{p}} x| \qquad \operatorname{ord}_{\mathfrak{p}} x = 0$$

这样任意 $\mathfrak{q}$ 都有 $\operatorname{ord}_{\mathfrak{q}} ax \geq 0$, 这就意味着 $ax \in A$. □

命题 2.22 对于 *Dedekind* 整环 A, 非零素理想 $\mathfrak{p}$, 有 $A/\mathfrak{p}$-线性空间的同构

$$A/\mathfrak{p} \cong \mathfrak{p}/\mathfrak{p}^2 \cong \ldots \cong \mathfrak{p}^i/\mathfrak{p}^{i+1}$$

换言之, A 的伴随分次代数 $\operatorname{gr} A = \sum_{i=0}^{\infty} \mathfrak{p}^i/\mathfrak{p}^{i+1} \cong (A/\mathfrak{p})[X]$.

证明 我们知道[8] $\mathfrak{p}^i/\mathfrak{p}^{i+1} = \mathfrak{p}^i A_{\mathfrak{p}}/\mathfrak{p}^{i+1}A_{\mathfrak{p}}$, 故不妨假设 $A = A_{\mathfrak{p}}$ 是离散赋值环, 这已经在 (C.28) 证明过. 或者可以这样证明, 构造

$$\varphi : A/\mathfrak{p} \longrightarrow \mathfrak{p}^i/\mathfrak{p}^{i+1} \qquad x \bmod \mathfrak{p} \longmapsto ax \bmod \mathfrak{p}^{i+1}$$

其中 $a \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$, 容易验证这是良定义的. 计算阶知是单射. 为了看到是满射, 任意取 $b \in \mathfrak{p}^i$, 因为 (a) 和 $\mathfrak{p}^i$ 互质, 根据互质的定义存在 $ax \equiv 1 \mod \mathfrak{p}^i$, 命题得证. □

2.2 Dedekind 整环的扩张

I. 扩张的基本性质

回忆 2.23 (迹配合) 回忆对于有限可分域扩张 $K \subseteq L$, *(B.28)* 定义了 "**迹 (trace) 配合 (pairing)**"

$$\langle -, - \rangle : L \times L \longrightarrow K \qquad (\alpha, \beta) \longmapsto \operatorname{tr}\downarrow_K^L (\alpha\beta)$$

并断言其是非退化的. 这一记号将贯穿本节.

定理 2.24 对于 *Dedekind* 整环 A, 以及其商域的有限可分扩张 $K \subseteq L$, 设 A 在 L 中的整闭包是 B, 则 B 也是 *Dedekind* 整环.

[8] 利用局部化的正合性.

事实上 B 作为 A-模是有限生成的. 当 A 是主理想整环时, B 还是自由 A-模, 其秩为 $[L:K]$.

而且 $\mathrm{tr}{\downarrow_K^L}$ 和 $\mathrm{Nm}{\downarrow_K^L}$ 将 B 映入 A.

且根据 *(C.21)*, 还有 $K\cdot B=L, B\cap K=A$, 特别地 $\mathrm{Frac}B=L$.

证明 关于后者是显然的, 因为他们的共轭也在 A 上整, 故 $\mathrm{tr}{\downarrow_K^L}$ 和 $\mathrm{Nm}{\downarrow_K^L}$ 分别是一些整元的加和乘, 故也在 A 上整, 但同时 $\mathrm{tr}{\downarrow_K^L}$ 和 $\mathrm{Nm}{\downarrow_K^L}$ 落在 K 中, 由于 A 是整闭的, 故实际上落在 A 中.

假设 $L=K\alpha_1+\ldots+K\alpha_n$.

接着, B 是整闭的 根据 (C.21) 或者根据定义显然.

接着, B 维数为 1. 如果 $\mathfrak{b}$ 是 B 的非零素理想但不是极大理想, 则 $\mathfrak{a}=\mathfrak{b}\cap A$ 是素理想故是极大理想或 0, 但根据 (C.22), $\mathfrak{a}$ 处于两难境地, 矛盾.

首先, B 是 Noether 的. 实际上, 我们可以证明 B 作为 A-模是有限生成的. 根据 (C.21), $B\cdot K=L$, 故不妨假设 $\alpha_i\in B$. 根据 (B.28), 考虑非退化的"迹配合"$\langle -,-\rangle$, 选取 $\beta_i\in B$ 使得

$$\langle\alpha_i,\beta_j\rangle=\delta_{ij}=\begin{cases}1 & i=j\\ 0 & i\neq j\end{cases}$$

因为有限性, β_i 也构成一组基. 我们要证明

$$\sum A\alpha_i\subseteq B\subseteq\sum A\beta_i$$

第一个是显然的, 第二个是因为任意 $x\in B\subseteq L$, 假设 $x=\sum c_i\beta_i$, 其中 $c_i\in K$, 那么

$$c_i=\langle x,\alpha_i\rangle=\mathrm{tr}{\downarrow_K^L}(x\alpha_i)\in A$$

这就证明了结果.

此时容易得到 B 是有限生成 A-模的子模, 因为 A 是 Noether 模从而也是有限生成的. 容易由此得到 B 是 Noether 的[9].

[9]根据 (C.6), 此时 B 的理想实际上都是有限生成 A-模, 故满足降链条件.

且当 A 是主理想整环时, B 还是自由 A-模, 其秩为 $[L:K]$. □

实际上, 如果对于 Dedekind 整环 A, $K=\mathrm{Frac}A$, L 是 K 的有限代数扩张, B 是 A 在 L 中的整闭包, 那么 B 依旧是 Dedekind 整环, 即使 $K\subseteq L$ 不可分, 参见 [3]P161 (26.18).

定义 2.25 为了行为流畅, 在本节, 约定称号 "**Dedekind 扩张**" 是一对扩张

$$(A\subseteq B, K\subseteq L):\quad \begin{bmatrix} & & L & \\ & B & & \\ & & & K \\ A & & & \end{bmatrix}$$

- A 是 *Dedekind* 整环, $\mathrm{Frac}A=K$.
- $K\subseteq L$ 是有限可分扩张.
- B 是 A 在 L 中的整闭包.

则结合我们已经知道的结论, 有 *(1)*A,B 都是 *Dedekind* 整环; *(2)*$A\subseteq B$ 是整扩张, $K\subseteq L$ 是有限可分扩张; *(3)*$\mathrm{Frac}A=K, \mathrm{Frac}B=L$; *(4)*$K\cdot B=L, B\cap K=A$.

例 2.26 显然 $(\mathbb{Z}\subseteq\mathbb{Z}[i], \mathbb{Q}\subseteq\mathbb{Q}[i])$ 是 *Dedekind* 扩张.

例 2.27 根据 *(2.24)*, 任何 $\mathbb{Q}$ 的有限扩张 L, $\mathbb{Z}$ 在 L 中的整闭包都是 *Dedekind* 整环.

II. 素理想扩张

引理 2.28 (上行定理) 对于 *Dedekind* 扩张 $A\subseteq B$, A 的非零素理想 $\mathfrak{p}$, 则存在 B 的非零素理想 $\mathfrak{P}$ 使得

$$\mathfrak{P}\cap A=\mathfrak{p}$$

证明 先证明 A 是局部环的情况. 取 B 的极大理想 $\mathfrak{P}$, 根据 (C.22) $\mathfrak{P}\cap A=\mathfrak{p}$.

一般地, 考虑乘性子集 $S=A\setminus\mathfrak{p}\subseteq B$, 考虑局部化 $A_{\mathfrak{p}}=S^{-1}A\subseteq S^{-1}B$, 根据第一段, 存在 $S^{-1}B$ 的极大理想 $\mathfrak{M}$ 使得 $\mathfrak{M}\cap A_{\mathfrak{p}}=\mathfrak{p}A_{\mathfrak{p}}$, 那么

$$\mathfrak{p}A_{\mathfrak{p}}\cap A=\{x\in A:\exists a\in\mathfrak{p},b\in A\setminus\mathfrak{p},\text{s. t. }xb=a\}=\mathfrak{p}$$

且 $\mathfrak{P}=\mathfrak{M}\cap B$ 是素理想, 因为 $\mathfrak{P}\cap A=\mathfrak{p}$, 故 $\mathfrak{P}\neq 0$, 命题得证. □

定理 2.29 *对于 Dedekind 扩张 $A\subseteq B$, 非零素理想 $\mathfrak{p}$, 则*

$$\mathfrak{p}B\cap A=\mathfrak{p}$$

证明 因为 $\mathfrak{p}\subseteq\mathfrak{p}B\cap A$, 由 $\mathfrak{p}$ 是极大理想, 有 $\mathfrak{p}B\cap A=\mathfrak{p}$, $\mathfrak{p}B\cap A=A$, 前者即所要求的. 后者意味着 $1\in A\subseteq\mathfrak{p}B$, 即 $B=\mathfrak{p}B$. 但是这与上行定理 (2.28) 矛盾. □

推论 2.30 *对于 Dedekind 扩张 $A\subseteq B$, $\mathfrak{p},\mathfrak{P}$ 分别是 A,B 的非零素理想, 则*

$$\mathfrak{p}\subseteq\mathfrak{P}\iff\mathfrak{P}\cap A=\mathfrak{p}$$

且这样的素理想只有有限个.

证明 关于有限的论证是因为那些满足条件的 $\mathfrak{P}$ 正是那些出现在 $\mathfrak{p}B$ 分解中的素理想. □

我们的目标是为了计算分解

$$\mathfrak{p}B=\mathfrak{P}_1^{e_1}\dots\mathfrak{P}_r^{e_r}$$

为此我们定义如下的概念. 同样类似, 仿照 (1.9), 有上面的定理保证, 约定

$$A/\mathfrak{p}\subseteq B/\mathfrak{P}$$

称 $A/\mathfrak{p}$ 为 $\mathfrak{p}$ 的**剩余类域**.

定义 2.31 (分歧指数, 惰性指数, 纤维数) *对于 n 次 Dedekind 扩张 $A\subseteq B$, 称 $\mathfrak{p}\subseteq\mathfrak{P}$ 是素理想的*扩张*如果 $\mathfrak{p},\mathfrak{P}$ 分别是是 A,B 的素理想. 记*

- **分歧指数**

$$\mathsf{e}(\mathfrak{P}|\mathfrak{p}) = \mathrm{ord}_{\mathfrak{P}}\,\mathfrak{p} = \mathfrak{p} \text{ 唯一分解中 } \mathfrak{P} \text{ 的指数}$$

- **惰性指数**

$$\mathsf{f}(\mathfrak{P}|\mathfrak{p}) = [B/\mathfrak{P} : A/\mathfrak{p}] = \text{域扩张 } A/\mathfrak{p} \subseteq B/\mathfrak{P} \text{ 的扩张次数}$$

- **纤维数**

$$\mathsf{r}(\mathfrak{p}) = \#\{B \text{ 的素理想} \mathfrak{P} : \mathfrak{p} \subseteq \mathfrak{P}\}$$

容易验证分歧指数和惰性指数的塔性质, 对素理想的扩张 $\mathfrak{p} \subseteq \mathfrak{P} \subseteq \mathcal{P}$ 有**塔性质**

$$\mathsf{e}(\mathcal{P}|\mathfrak{P})\mathsf{e}(\mathfrak{P}|\mathfrak{p}) = \mathsf{e}(\mathcal{P}|\mathfrak{p}) \qquad \mathsf{f}(\mathcal{P}|\mathfrak{P})\mathsf{f}(\mathfrak{P}|\mathfrak{p}) = \mathsf{f}(\mathcal{P}|\mathfrak{p})$$

如上定义和 (1.10) 所定义的如出一辙, 例子也在例子之后.

定理 2.32 (基本恒等式) 对于 n 次 *Dedekind* 扩张 $A \subseteq B$, $\mathfrak{p} \subseteq \mathfrak{P}$ 是素理想的扩张, 则

$$n = \sum_{\mathfrak{P} \supseteq \mathfrak{p}} \mathsf{e}(\mathfrak{P}|\mathfrak{p})\mathsf{f}(\mathfrak{P}|\mathfrak{p})$$

证明 对于右边, 根据中国剩余定理

$$B/\mathfrak{p}B = B/\mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r} \cong \bigoplus_{i=1}^{r} B/\mathfrak{P}_i^{e_i}$$

作为 $B/\mathfrak{P}_i$-线性空间 (2.22) [10],

$$B/\mathfrak{P}_i^{e_i} \cong (B/\mathfrak{P}_i)^{e_i}$$

故右边作为 $A/\mathfrak{p}$-线性空间的维数为 $\sum_{i=1}^{r} e_i f_i$.

对于左边, 如果 A 是主理想整环, 那么 B 是秩为 n 的自由 A-模. 故作为线性空间,

$$B/\mathfrak{p}B \cong A^n/\mathfrak{p}A^n \cong (A/\mathfrak{p})^n$$

[10] 具体来说, 构造 $B \supseteq \mathfrak{P}_i \supseteq \dots \supseteq \mathfrak{P}_i^{e_i}$

故作为 $A/\mathfrak{p}$-线性空间的维数为 n. 对于一般情况, 类似地, 取 $S = A \setminus \mathfrak{p}$, 根据 (2.19) 于是 $S^{-1}(\mathfrak{p}B)$ 的分解依旧保留, 各 e_i 对应相等, 且商和局部化可以交换, 各 f_i 对应相等. 但 n 不随着局部化而变, 命题得证. □

定义 2.33 对于 n 次 *Dedekind* 扩张 $A \subseteq B$, $\mathfrak{p} \subseteq \mathfrak{P}$ 是素理想的扩张,

- 称 $\mathfrak{P}$ 是**不分歧的 (unramified)** 如果

$$\mathsf{e}(\mathfrak{P}|\mathfrak{p}) = 1$$

否则称 $\mathfrak{P}$ 是**分歧的 (ramified)**. 称 $\mathfrak{p}$ 是**不分歧的**如果对所有 $\mathfrak{P} \supseteq \mathfrak{p}$,$\mathfrak{P}$ 不分歧, 否则称 $\mathfrak{p}$ 是**分歧的**. 即 $\mathfrak{p}B$ 在 B 中分解为不同素理想的乘积.

- 称 $\mathfrak{P}$ 是**完全不惰性的**如果

$$\mathsf{f}(\mathfrak{P}|\mathfrak{p}) = 1$$

- 称 $\mathfrak{p}$ 是**不分裂的 (nonsplit, indecomposed)** 如果

$$\mathsf{r}(\mathfrak{p}) = 1$$

即 $\mathfrak{p}B$ 在 B 中分解为一个素理想的幂次.

除此之外, 定义

- 称 $\mathfrak{p}$ 是**完全分歧的 (completely ramified)** 如果对所有 $\mathfrak{P} \supseteq \mathfrak{p}$,

$$\mathsf{e}(\mathfrak{P}|\mathfrak{p}) = n \qquad \mathsf{f}(\mathfrak{P}|\mathfrak{p}) = 1 \qquad \mathsf{r}(\mathfrak{p}) = 1$$

- 称 $\mathfrak{p}$ 是**完全分裂的 (split completely, totally split)** 如果对所有 $\mathfrak{P} \supseteq \mathfrak{p}$,

$$\mathsf{e}(\mathfrak{P}|\mathfrak{p}) = 1 \qquad \mathsf{f}(\mathfrak{P}|\mathfrak{p}) = 1 \qquad \mathsf{r}(\mathfrak{p}) = n$$

即 $\mathfrak{p}B$ 在 B 中分解为 n 个不同素理想的乘积.

- 称 $\mathfrak{p}$ 是**惰性的 (inert)** 如果对所有 $\mathfrak{P} \supseteq \mathfrak{p}$,

$$\mathsf{e}(\mathfrak{P}|\mathfrak{p}) = 1 \qquad \mathsf{f}(\mathfrak{P}|\mathfrak{p}) = n \qquad \mathsf{r}(\mathfrak{p}) = 1$$

即 $\mathfrak{p}B$ 在 $\mathfrak{B}$ 中还是素理想.

定理 2.34 (Dedekind) 对于 *Dedekind* 扩张 $A \subseteq B$, A 的非零素理想 $\mathfrak{p}$. 如果 $B = A[\alpha]$, 令 $f(X)$ 是 α 的最小多项式, 设首一 $f_1(X), \dots, f_r(X) \in A[X]$ 使得

$$f \equiv f_1^{e_1} \dots f_r^{e_r} \mod \mathfrak{p}$$

是 f 在 $A/\mathfrak{p}[X]$ 中的唯一分解. 那么

$$\mathfrak{p}B = \prod_{i=1}^{r} \left[\mathfrak{p} + (f_i(\alpha))\right]^{e_i}$$

是 $\mathfrak{p}B$ 在 B 中的唯一分解. 且对应的惰性指数 $f_i = \deg f_i$.

证明 注意到

$$\frac{B}{\mathfrak{p}B} = \frac{A[X]/(f)}{\mathfrak{p}B} = \frac{A/\mathfrak{p}[X]}{(f \bmod \mathfrak{p})} = \frac{A/\mathfrak{p}[X]}{(f_1^{e_1} \dots f_r^{e_r} \bmod \mathfrak{p})} = \bigoplus_{i=1}^{r} \frac{A/\mathfrak{p}[X]}{(f_i^{e_i} \bmod \mathfrak{p})} \quad (*)$$

不难得到[11] 其极大理想就是 $(f_i^{e_i} \bmod \mathfrak{p})$, 根据商环的理想对应, B 中包含 $\mathfrak{p}B$ 的素理想就是 $\mathfrak{p} + (f_i(\alpha))$, 记 $\mathfrak{P}_i = \mathfrak{p} + (f_i(\alpha))$. 且 $(*)$ 还说明[12] $\mathrm{ord}_{\mathfrak{P}_i} \mathfrak{a} = e_i$, 故命题中关于分解的部分得证. 然后

$$\frac{B}{\mathfrak{P}_i} = \frac{A[\alpha]}{\mathfrak{p} + (f_i(\alpha))} = \frac{A[X]}{\mathfrak{p} + (f_i)} = \frac{A/\mathfrak{p}[X]}{(f_i \bmod \mathfrak{p})}$$

故 $\frac{B}{\mathfrak{P}_i}$ 是 $A/\mathfrak{p}$ 添加上 f_i 的某个根的单扩张, 故 $\deg f_i$ 就是惰性指数. □

实际上上述的证明过程是 (1.5) 的深入, 在原本的证明中我们只给出了不可约的判据, 但是上述证明实际上还决定了可约的情况.

评注 2.35 对于 *Dedekind* 整环 $A \subseteq B, K \subseteq L$, A 的非零素理想 $\mathfrak{p}$. 如果某个 $\alpha \in B$ 使得 $L = K[\alpha]$, 一般没有 $B = A[\alpha]$, 但可以取 “分母集 ”

$$\mathfrak{F} = \{b \in B : bB \subseteq A[\alpha]\}$$

这是一个理想, 如果 $\mathfrak{p}$ 与 $\mathfrak{F}$ 互素, 那么上面的结论依旧成立, 因为若记 $B' = A[\alpha]$, 不难[13]得到 $\frac{B}{\mathfrak{p}B} \cong \frac{B'}{\mathfrak{p}B'}$, 后续的证明是一样的.

[11] 注意到一个环论的事实, $A \times B$ 的理想都形如 $\mathfrak{a} \times \mathfrak{b}$, 故 $A \times B$ 的极大理想都形如 $\mathfrak{m} \times B$ 或 $A \times \mathfrak{m}'$.

[12] 因为 $\mathfrak{P}_i^{e_i} \mid \mathfrak{p}$, 且 $\mathfrak{P}_i^{e_i+1} \nmid \mathfrak{p}$.

[13] 因为 $\mathfrak{p}B + \mathfrak{F} = B$, 故 $B = \mathfrak{p}B + \mathfrak{F} \subseteq \mathfrak{p}B + B' \subseteq B$, 故 $B' = B \mod \mathfrak{p}B$.

例 2.36 考虑 *Gauss* 整环 $\mathbb{Z}[i]$, i 的最小多项式是 X^2+1, 由二次互反律 *(A.5)* 知,

- 当 $p=2$ 时, $\mathbb{Z}/2\mathbb{Z}$ 上的完全分解

$$X^2+1 \equiv (X+1)^2 \mod 2$$

则根据上面的定理 *(2.34)*,

$$(2) = ((2)+(i+1))^2 = ((i+1))^2$$

- 在 $p \equiv 3 \mod 4$ 时, 在 $\mathbb{Z}/p\mathbb{Z}[X]$ 上的 X^2+1 不可约, 则根据上面的定理 *(2.34)*,

$$(p) = ((p)+(i^2+1)) = (p)$$

给出唯一分解.

- 在 $p \equiv 1 \mod 4$ 时, 在 $\mathbb{Z}/p\mathbb{Z}[X]$ 上的完全分解

$$X^2+1 \equiv (X+\iota)(X-\iota) \mod p \qquad \iota^2 \equiv -1 \mod p$$

则根据上面的定理 *(2.34)*,

$$(p) = ((p)+(i+\iota)) \cdot ((p)+(i-\iota))$$

给出唯一分解. $((p)+(i+\iota))$ 的前者的形式[14] 是 $x+yi$, 其中 $y \equiv x\iota \bmod p$, 如果期望将其配成一个主理想, 应当取其中范数最小者, 即使得 x^2+y^2 最小者, 且这个最小值必须为 p.

例 2.37 考虑 $\mathbb{Z}[\phi]$, 其中 $\phi = \frac{\sqrt{5}-1}{2}$ 为黄金分割, 其最小多项式为 X^2+X-1,

- 在奇素数 p 时, 因为 2 可逆, 施以配方得到

$$X^2+X-1 = \left(X+\frac{1}{2}\right)^2 - \frac{5}{4}$$

因为是否可约完全取决于 5 是否是二次剩余, 根据二次互反律 *(A.7)*,

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} 1 & p \equiv \pm 1 \mod 5 \\ -1 & p \equiv \pm 2 \mod 5 \end{cases}$$

[14] 因为 $(a+bi)(i+\iota)+(c+di)p = (a+b\iota+cp)+(a\iota-b+dp)i = (a+b\iota+cp)+(a+b\iota-d\iota p)\iota i$.

当 $p \equiv \pm 1 \mod 5$ 时, 设

$$\kappa^2 \equiv 5 \mod p \qquad 2\lambda \equiv 1 \mod p$$

那么根据上面的定理 *(2.34)*,

$$\begin{aligned}(p) &= ((p) + (\phi + \lambda + \lambda\kappa)) \cdot ((p) + (\phi + \lambda - \lambda\kappa)) \\ &= ((p) + (2\phi + 2\lambda + 2\lambda\kappa)) \cdot ((p) + (2\phi + 2\lambda - 2\lambda\kappa)) \\ &= ((p) + (\sqrt{5} + \kappa)) \cdot ((p) + (\sqrt{5} - \kappa))\end{aligned}$$

- 而如果用 *(2.35)*, 我们不妨直接使用 $\mathbb{Z}[\sqrt{5}]$, 其 "分母集" 为

$$\mathfrak{F} = \{x \in \mathbb{Z}[\phi] : x\sqrt{5} \in \mathbb{Z}[\phi]\} \supseteq (2)$$

故只要和 (2) 互素就可以使用. 交给读者去验证得到的结果是一样的.

- 若想要得到 (2) 的分解, 因为 $X^2 + X - 1 = 0$ 在 $\mathbb{Z}/2\mathbb{Z}$ 没有根, 故 $(2) = (2)$ 是完全分解.

例 2.38 考虑 $\mathbb{Z}[\sqrt{-5}]$, 这是 $\mathbb{Z}$ 的 *Dedekind* 扩张. 生成元 $\sqrt{-5}$ 是最小多项式是 $X^2 + 5$, 其在 $\mathbb{Z}/p\mathbb{Z}[X]$ 上是否可约取决于 -5 是否是二次剩余, 根据二次互反律 *(A.7)*,

$$\left(\frac{-5}{p}\right) = \begin{cases} 1 & p \equiv 1, 3, 7, 9 \mod 20 \\ -1 & p \equiv -1, -3, -7, -9 \mod 20 \end{cases}$$

特别地, $p = 3$ 时, 容易计算 $1^2 \equiv -5 \mod 3$, 故根据上面的定理 *(2.34)*,

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

$p = 2$ 时, $X^2 + 5 \equiv (X + 1)^2 \mod 2$, 故根据定理 *(2.34)*

$$(2) = ((2) + (1 + \sqrt{-5}))^2$$

这和 *(2.8)* 给出的分解是一样的, 但是显然这种方法更有效.

更多这样的计算, 可见 [8]P63.

III. Galois 扩张 下面我们要考虑 Dedekind 扩张 $(A \subseteq B, K \subseteq L)$ 在 $K \subseteq L$ 是 Galois 扩张的情况. 此时我们称之为**Galois-Dedekind-扩张**.

定理 2.39 *对于 Galois-Dedekind-扩张 $(A \subseteq B, K \subseteq L)$, 其 Galois 群是 G. 则 $G \cdot B = B$. 且对于 A 的任意非零素理想 $\mathfrak{p}$, 则 G 在 $\mathfrak{p}$ 在 B 的素理想扩张上的作用是可迁的. 即*

$$\forall \mathfrak{P}_1, \mathfrak{P}_2 \supseteq \mathfrak{p}, \exists \sigma \in G, \text{s.t.} \quad \sigma\mathfrak{P}_1 = \mathfrak{P}_2$$

证明 第一个论断是只需考虑整性方程[15]. 关于第二个论断, 显然, G 中的元素把素理想变成素理想. 否则, 可以使用中国剩余定理[16], 找 $x \in B$ 使得

$$x \equiv 0 \mod \sigma^{-1}\mathfrak{P}_1 \qquad x \equiv 1 \mod \sigma^{-1}\mathfrak{P}_2 \qquad \forall \sigma \in G$$

而 $\mathrm{Nm}{\downarrow_K^L} x = \prod \sigma x \in K \cap B = A$, 根据左边 $\mathrm{Nm}{\downarrow_K^L} x \in \mathfrak{P}_1 \cap A = \mathfrak{p}$, 根据右边 $\mathrm{Nm}{\downarrow_K^L} x \equiv 1 \mod \mathfrak{P}_2$, 故 $\mathrm{Nm}{\downarrow_K^L} x - 1 \in \mathfrak{p}$, 矛盾. □

评注 2.40 *上述定理说明实际上 Galois 群还顺便描述了素理想扩张的对称性, 所有素理想的扩张的特性都是一样的[17], 这样定义 (2.31) 和 (2.33) 中的各种质数和对素理想的描述都可以直接加在素理想上而不管其扩张的选择, 换句话说, 我们定义*

$$\mathsf{e}(\mathfrak{p}) = \mathsf{e}(\mathfrak{P}|\mathfrak{p}) \qquad \mathsf{f}(\mathfrak{p}) = \mathsf{f}(\mathfrak{P}|\mathfrak{p}) \qquad \forall \mathfrak{P} \supseteq \mathfrak{p}$$

这样素理想的分解应该是

$$\mathfrak{p} = \mathfrak{a}^m \qquad \mathfrak{a} = \mathfrak{P}_1 \dots \mathfrak{P}_{\mathsf{r}(\mathfrak{p})} \quad \text{即, “无平方因子”}$$

这样基本恒等式 (2.32) 变成了 $n = \mathsf{e}(\mathfrak{p})\mathsf{f}(\mathfrak{p})\mathsf{r}(\mathfrak{p})$.

定义 2.41 *对于 Galois-Dedekind-扩张 $(A \subseteq B, K \subseteq L)$, 其 Galois 群是 G. 对于素理想扩张 $\mathfrak{p} \subseteq \mathfrak{P}$,*

[15] 如果 $\beta \in B$ 满足 $\beta^n + a_{n-1}\beta^{n-1} + \dots + a_0 = 0$, 则 $(\sigma\beta)^n + \dots = \sigma((\beta)^n + \dots) = 0$, 故 $\sigma\beta \in L$ 在 A 上整, 故 $\sigma\beta \in B$.

[16] 因为 $\sigma^{-1}\mathfrak{Q} \neq \tau^{-1}\mathfrak{P}$ 对任何 $\sigma, \tau \in G$, 且都是有限个

[17] 具体而言, $\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$, $\mathfrak{p} = \sigma\mathfrak{p} = \sigma\mathfrak{P}_1^{e_1} \dots \sigma\mathfrak{P}_r^{e_r}$, 故 $e_1 = \dots = e_r$. 而 $B/\sigma\mathfrak{P} = \sigma B/\sigma\mathfrak{P} = \sigma(B/\mathfrak{P}) \cong B/\mathfrak{P}$, 故扩张次数相同.

- 记 **分解 (decompostion) 群**, **分解域** 和 **分解环**

$$G_{\mathsf{dec}\mathfrak{P}} = \{\sigma \in G : \sigma\mathfrak{P} = \mathfrak{P}\}$$

$$L_{\mathsf{dec}\mathfrak{P}} = \{x \in L : \sigma x = x \quad \forall \sigma \in G_{\mathsf{dec}\mathfrak{P}}\}$$

$$B_{\mathsf{dec}\mathfrak{P}} = \{x \in L_{\mathsf{dec}\mathfrak{P}} : x \text{ 在 } A \text{ 上整}\}$$

- 记 **惰性 (inertia) 群**, **惰性域** 和 **惰性环**

$$G_{\mathsf{ine}\mathfrak{P}} = \{\sigma \in G : \forall x \in B, \quad \sigma x \equiv x \bmod \mathfrak{P}\}$$

$$L_{\mathsf{ine}\mathfrak{P}} = \{x \in L : \sigma x = x \quad \forall \sigma \in G_{\mathsf{ine}\mathfrak{P}}\}$$

$$B_{\mathsf{ine}\mathfrak{P}} = \{x \in L_{\mathsf{ine}\mathfrak{P}} : x \text{ 在 } A \text{ 上整}\}$$

故 $G_{\mathsf{ine}\mathfrak{P}} \subseteq G_{\mathsf{dec}\mathfrak{P}} \subseteq G$, 根据 *Galois* 理论 *(B.23)* $K \subseteq L_{\mathsf{ine}\mathfrak{P}} \subseteq L_{\mathsf{dec}\mathfrak{P}} \subseteq L$. 有 *Dedekind* 扩张 $A \subseteq A_{\mathsf{ine}\mathfrak{P}} \subseteq A_{\mathsf{dec}\mathfrak{P}} \subseteq B$.

记号 2.42 方便起见, 下面我们固定如下记号, 对于 *Galois-Dedekind*-扩张 $(A \subseteq B, K \subseteq L)$, 其 *Galois* 群是 G. 对于素理想扩张 $\mathfrak{p} \subseteq \mathfrak{P}$. 径直以下标 d, i 代替 $\mathsf{dec}\mathfrak{P}, \mathsf{ine}\mathfrak{P}$. 并且记

$$\mathfrak{P}_d = B_d \cap \mathfrak{P} \qquad \mathfrak{P}_i = B_i \cap \mathfrak{P}$$

他们分别是 B_d, B_i 的素理想, 且 $\mathfrak{p} \subseteq \mathfrak{P}_d \subseteq \mathfrak{P}_i \subseteq \mathfrak{P}$. 以及

$$e = \mathsf{e}(\mathfrak{p}) \qquad f = \mathsf{f}(\mathfrak{p}) \qquad r = \mathsf{r}(\mathfrak{p})$$

并且, 为了得到漂亮的结论, 我们约定 $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ 是可分的[18].

以下四个定理被称为 **Hilbert 分歧理论**.

定理 2.43 (Hilbert 分歧理论) 记号承上, 有

[18] 例如 $A/\mathfrak{p}$ 是有限域, 这是一个完美域, 即任何代数扩张都可分.

(1) 对于 *Galois-Dedekind* 扩张 $A \subseteq B$, $\mathfrak{p}B$ 在 B 中的分解[19]为 $\mathfrak{p} = \prod_{\sigma \in G/G_d} \sigma\mathfrak{P}^e$. 且 *(以下符号指的是在扩张 $A \subseteq B$ 下的各指标)*

$$\mathsf{e}(\mathfrak{p}) = e \qquad \mathsf{f}(\mathfrak{p}) = f \qquad \mathsf{r}(\mathfrak{p}) = r$$

(2) 对于 *Galois-Dedekind* 扩张 $B_d \subseteq B$, $\mathfrak{P}_d$ 在 B_d 中的分解为 $\mathfrak{P}_d B = \mathfrak{P}^e$. 且 *(以下符号指的是在扩张 $B_d \subseteq B$ 下的各指标)*

$$\mathsf{e}(\mathfrak{P}_d) = e \qquad \mathsf{f}(\mathfrak{P}_d) = f \qquad \mathsf{r}(\mathfrak{P}_d) = 1$$

(3) 对于 *Galois-Dedekind* 扩张 $B_i \subseteq B$, $\mathfrak{P}_i$ 在 B_i 中的分解为 $\mathfrak{P}_i B = \mathfrak{P}^e$. 且 *(以下符号指的是在扩张 $B_i \subseteq B$ 下的各指标)*

$$\mathsf{e}(\mathfrak{P}_i) = e \qquad \mathsf{f}(\mathfrak{P}_i) = 1 \qquad \mathsf{r}(\mathfrak{P}_i) = 1$$

证明 (1) 因为 G/G_d 同构于 $\mathfrak{P}$ 所在的轨道, 故 G/G_d 表出所有互异的 $\mathfrak{P}$.

(2) 根据 Galois 定理, $\mathrm{Gal}(L : L_d) = G_d$, 而 $\mathfrak{P}$ 是 $\mathfrak{P}_d$ 的素理想扩张, 故

$$\{\sigma\mathfrak{P} : \sigma \in G\}$$

是全部 $\mathfrak{P}_d$ 在 B 中的素理想扩张, 但是 $\sigma\mathfrak{P} = \mathfrak{P}$, 故实际上上述集合只有 $\mathfrak{P}$ 一个元素. 故 $\mathsf{r}(\mathfrak{p}) = 1$. 由于基本恒等式 $n = efr$, 以及塔性质, 这迫使 $\mathsf{e}(\mathfrak{P}_d) = e, \mathsf{f}(\mathfrak{P}_d) = f$.

(3) 假如我们用 $B_i \subseteq B$ 代替 $A \subseteq B$, 那么 $G = G_i$, $K = L_d = L_i$, 此时用下面的引理 (2.44) 得到 $B/\mathfrak{P} = B_i/\mathfrak{P}_i$, 从而 $\mathsf{f}(\mathfrak{P}_i) = 1$, 根据基本恒等式得到 $\mathsf{e}(\mathfrak{P}_i) = e, \mathsf{r}(\mathfrak{P}_i) = 1$. □

引理 2.44 *记号承上, $A/\mathfrak{P} \subseteq B/\mathfrak{P}$ 是 Galois 扩张. 且任何一个 $\sigma \in G_d$, 都诱导了在 $B/\mathfrak{P}$ 在 $A/\mathfrak{p}$ 上的自同构[20], 换言之, 存在*

$$\varphi : G_d \to \mathrm{Gal}(B/\mathfrak{P} : A/\mathfrak{p})$$

且 $\ker\varphi = G_i$, φ 是满射[21] , 根据 Galois 定理有

$$\mathrm{Gal}(B/\mathfrak{P} : A/\mathfrak{p}) = \mathrm{Gal}(L_i : L_d)$$

[19] 其中 G/G_d 是左陪集, 代表同一个左陪集的代表元在 $\mathfrak{P}$ 的作用是一样的.

[20] 即 $\sigma \cdot (a \bmod \mathfrak{P}) = (\sigma a) \bmod \mathfrak{P}$, 若 $a - b \in \mathfrak{P}$, 则 $\sigma(a) - \sigma(b) \in \mathfrak{P}$, 所以是良定义的.

[21] 换言之有正合列 $0 \to G_i \to G_d \xrightarrow{\varphi} \mathrm{Gal}(B/\mathfrak{P} : A/\mathfrak{p}) \to 0$.

证明 对于 $x \in B$, 我们要证明 $x \bmod \mathfrak{P}$ 的最小多项式在 $B/\mathfrak{P}$ 上分解为一次式. 假设 x 满足整性方程 $f(X) = 0$, 假设其在 $A/\mathfrak{p}[X]$ 上的完全分解为

$$f(X) \equiv f_1(X)^{\cdots} \dots f_n(X)^{\cdots} \mod \mathfrak{p}$$

此时, $x \bmod \mathfrak{P}$ 必然是某个 f_i 的根, 故是 $x \bmod \mathfrak{P}$ 的最小多项式, 因为 $K \subseteq L$ 为 Galois 扩张, 故 $f(X)$ 在 $B[X]$ 上分解为一次式[22], 这迫使 f_i 在 $B/\mathfrak{P}$ 上也分解为一次式. 事实上, 这还证明了 f_i 根必然形如 $x' \bmod \mathfrak{P}$, 其中 x 是某个 f 的根.

根据定义, $\ker \varphi = G_i$ 为显然. 比较困难的是满射的结论. 想法是将 Galois 群理解为根的置换.

因为我们已经知道[23] 对于 $A \subseteq B_d$ 有 $\mathsf{f}(\mathfrak{p}) = 1$, 即剩余域相同, 故可以替换 $A = B_d$, 这样 $G = G_d$.

根据本原元存在定理 (B.22), 假设第一段所取的 x 是 $A/\mathfrak{p} \subseteq B/\mathfrak{P}$ 的本原元 $x \in B$ 即

$$B/\mathfrak{P} = A/\mathfrak{p}\,[\,x \bmod \mathfrak{P}\,]$$

任意取 $\tau \in \mathrm{Gal}(B/\mathfrak{P} : A/\mathfrak{p})$, $\tau\, x \bmod \mathfrak{P}$ 还是 f_i 的根. 根据第一段末尾, 存在 f 的根 x' 使得

$$x' \bmod \mathfrak{P} = \tau\, x \bmod \mathfrak{P}$$

因为 Galois 群对根的作用是可迁的, 故可以找 $\sigma \in G$ 使得 $\sigma x = x'$, 而按照诱导的规则[24], σ 诱导的自同构就是 τ. □

推论 2.45 *作为推论, 我们分拆看扩张*

(1) *Dedekind 扩张 $A \subseteq B_d$ 上*

$$\mathsf{e}(\mathfrak{P}_d|\mathfrak{p}) = 1 \qquad \mathsf{f}(\mathfrak{P}_d|\mathfrak{P}_d) = 1 \qquad \mathsf{r}(\mathfrak{P}_d) = r$$

(2) *Dedekind 扩张 $B_d \subseteq B_i$ 也是 Galois 的, 且*

$$\mathsf{e}(\mathfrak{P}_d) = 1 \qquad \mathsf{f}(\mathfrak{P}_d) = f \qquad \mathsf{r}(\mathfrak{P}_d) = 1$$

且 $\mathrm{Gal}(B_i/\mathfrak{P}_i : B_d/\mathfrak{P}_d) \cong \mathrm{Gal}(L_i : L_d)$.

[22] 首先 $f(X)$ 在 $L[X]$ 上分解为一次式, 但是其根都是代数整数, 故在 $B[X]$ 上分解为一次式.
[23] 利用 (2.43) 的 (1) 以及塔性质.
[24] 因为取的是本原元, 所以本原元如何映就决定了整个域如何映.

(3) *Dedekind* 扩张 $B_i \subseteq B$ 是 *Galois* 的, 且

$$\mathsf{e}(\mathfrak{P}_i) = e \qquad \mathsf{f}(\mathfrak{P}_i) = 1 \qquad \mathsf{r}(\mathfrak{P}_i) = 1$$

证明 (1)(2)(3) 根据塔性质显然. 而 (2)Galois 的论断来自于 G_i 是 G_d 的正规子群. 根据下面的引理 (2.44),

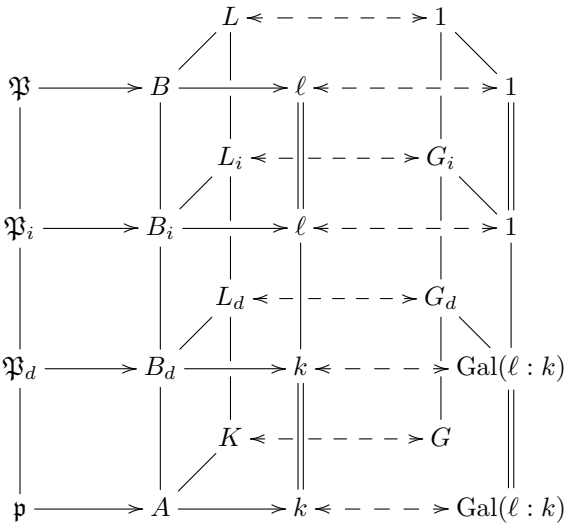
$$\mathrm{Gal}(B/\mathfrak{P} : A/\mathfrak{p}) \cong \mathrm{Gal}(L_i : L_d)$$

因为 $B/\mathfrak{P} = B_i/\mathfrak{P}_i, A/\mathfrak{p} = B_d/\mathfrak{P}_d$. □

评注 2.46 最后让我们以图作结, 记

$$k = A/\mathfrak{p} = B_d/\mathfrak{P}_d \qquad \ell = B_i/\mathfrak{P}_i = B/\mathfrak{P}$$

可以画出下图, 其中虚线是 *Galois* 对应



现在再回看 *Hilbert* 分歧理论的意义在于将一个扩张分解为一个完全分裂的, 惰性的和完全分歧的三个扩张的复合 *(2.33)*.

2.3 代数整数环

对于 $\mathbb{C}$ 中在 $\mathbb{Z}$ 上整的元素, 我们通常称为**代数整数**. 对于 Dedekind 扩张 $\mathbb{Z} \subseteq A$, 称 A 是**代数整数环**.

I. 整基与判别式

定义 2.47 对于 *Dedekind* 扩张 $A \subseteq B$, 如果 B 作为 A-模是自由的, 换言之存在 $\beta_1, \dots, \beta_n$ 使得

$$B = A\beta_1 \oplus \dots \oplus A\beta_n$$

作为 A-模, 则称其基, 即这里的 $\beta_1, \dots, \beta_n$ 是一组**整基**.

显然, *(2.24)* 的一部分断言了 A 是主理想整环时必定存在整基.

回忆迹配合 (B.28). 我们曾在 (2.24) 看到其威力, 下面的判别式则在 A 是主理想整环时可以某种程度上代替其作用.

定义 2.48 (判别式) 对于 n 次 *Dedekind* 扩张 $(A \subseteq B, K \subseteq L)$, 对于 $\beta_1, \dots, \beta_n \in B$, 定义**判别式 (discriminant)**

$$\mathrm{Disc}(\beta_1, \dots, \beta_n) = \det(\langle \beta_i, \beta_j \rangle) = \det(\mathrm{tr}{\downarrow_K^L}(\beta_i \beta_j)) \in A$$

因为 *(B.28)* 断言其非退化, 故 β_i 线性无关时, $\mathrm{Disc}(\dots) \neq 0$.

线性代数的技巧告诉我们[25]

$$\mathrm{Disc}(\beta_1, \dots, \beta_n) = \det(\sigma_j \beta_i)^2$$

其中 σ_j 取遍所有 K 同态 $L \to \overline{\mathrm{alg}}\, K$.

根据线性代数, 如果 $\gamma_i = \sum a_{ij}\beta_i$, 那么

$$\mathrm{Disc}(\gamma_1, \dots, \gamma_n) = \det(a_{ij})^2 \,\mathrm{Disc}(\beta_1, \dots, \beta_n)$$

特别地如果存在整基 $\beta_1, \dots, \beta_n$, 此时定义

$$\mathrm{Disc}(B|A) = \mathrm{Disc}(\beta_1, \dots, \beta_n)$$

显然, 若用另一组整基定义只相差 A 的一个单位的平方, 这被称为 B 的**判别式**. 特别地, $A = \mathbb{Z}$ 时则始终是同一个数.

[25] 这不意味着 $\mathrm{Disc}(\dots) \in A^2$, 因为 $\det(\sigma_j \beta_i)$ 可能不在 A 中.

命题 2.49 对 *Dedekind* 扩张 $\mathbb{Z} \subseteq A$, 设 $\alpha_1, \ldots, \alpha_n$ 是一组整基, 如果有线性无关的 $\gamma_1, \ldots, \gamma_n \in A$, 假设 $\gamma_i = \sum c_{ij}\alpha_j$, 根据 *(B.2)*, $\det(c_{ij}) = [A : \mathbb{Z}\gamma_1 + \ldots + \mathbb{Z}\gamma_n]$, 故

$$\mathrm{Disc}(A|\mathbb{Z})[A : \mathbb{Z}\gamma_1 + \ldots + \mathbb{Z}\gamma_n]^2 = \mathrm{Disc}(\gamma_1, \ldots, \gamma_n)$$

特别地, $\mathrm{Disc}(A|\mathbb{Z}) \mid \mathrm{Disc}(\gamma_1, \ldots, \gamma_n)$.

命题 2.50 对于 n 次 *Dedekind* 扩张 $A \subseteq B$, 若 $\beta_1, \ldots, \beta_n \in B$ 线性无关, 则

$$\sum A\beta_1 \subseteq B \subseteq \frac{1}{d}\sum A\beta_1$$

其中 $d = \mathrm{Disc}(\beta_1, \ldots, \beta_n)$.

证明 第一个包含为显然. 下面证明第二个包含, 任意 $x \in B$, 设 $x = \sum c_i\beta_i$, 其中 $c_i \in \mathrm{Frac}A$, 那么

$$\beta_j x = \sum c_i\beta_i\beta_j \quad \Rightarrow \quad \mathrm{tr}\beta_j x = \sum c_i \,\mathrm{tr}(\beta_i\beta_j)$$

这样根据 Cramer 法则, $c_i = \frac{a_i}{d}$, 对某个 [26]$a_i \in A$, 故 $x \in \frac{1}{d}\sum A\beta_1$. □

例 2.51 根据 *(C.16)*,

$$\mathbb{Z}[\delta] = \{a + b\delta : a, b \in \mathbb{Z}\} \qquad \delta = \begin{cases} \frac{1+\sqrt{d}}{2} & d \equiv 1 \mod 4 \\ \sqrt{d} & d \equiv 2, 3 \mod 4 \end{cases}$$

换言之 $\mathbb{Z}[\delta] = \mathbb{Z} + \mathbb{Z}\delta$, 可以根据定义直接计算

$$\mathrm{Disc}(1, \delta) = \begin{cases} d & d \equiv 1 \mod 4 \\ 4d & d \equiv 2, 3 \mod 4 \end{cases}$$

例 2.52 一般地, 设 $\mathbb{Z} \subseteq \mathbb{Z}[\alpha]$ 是 *Dedekind* 扩张, 如果 $\mathbb{Q} \subseteq \mathbb{Q}[\alpha]$ 可分, α 的首一最小多项式是 $f(X)$, 则

$$\mathrm{Disc}(\mathbb{Z}[\alpha]|\mathbb{Z}) = \mathrm{Disc}(1, \alpha, \ldots, \alpha^{n-1}) = \det(\sigma_j\alpha^i)^2 = \prod_{i<j}(\sigma_i\alpha - \sigma_j\alpha)^2$$

[26] 因为 $\mathrm{tr}(B) \subseteq A$.

其中 σ_j 取遍所有 K 同态 $L\to\overline{\mathrm{alg}}\,K$. 而 $\sigma_j x$ 取遍 $f(X)$ 的所有根, 故上述判别式即 f 的判别式 [27].

例 2.53 若 $\alpha_1,\dots,\alpha_n$ 满足 $\mathrm{Disc}(\alpha_1,\dots,\alpha_n)$ 无平方因子, 那么 $\alpha_1,\dots,\alpha_n$ 是一组整基. 根据 *(2.48)*, 假设有整基 $\beta_1,\dots,\beta_n$, 设 $\alpha_i=\sum a_{ij}\beta_j$, 那么

$$\mathrm{Disc}(\alpha_1,\dots,\alpha_n)=\det(a_{ij})^2\,\mathrm{Disc}(\beta_1,\dots,\beta_n)$$

因为无平方因子, 故 $\det(a_{ij})^2=1$, 这使得 (a_{ij}) 可逆, 故 $\beta_1,\dots,\beta_n$ 是一组整基.

实际上判别式给出一种可计算性的途径, 一旦计算出判别式, 那么 B 必然被控制在两个之差常数的子群之间, 而之间的子群只有有限个 [28], 故总可以在有限时间内计算出整基. 然而事实上, 判别式的用途远不止于此.

命题 2.54 对于两个 *Dedekind* 扩张 $(\mathbb{Z}\subseteq B_1,\mathbb{Q}\subseteq L_1),(\mathbb{Z}\subseteq B_2,\mathbb{Q}\subseteq L_2)$, 那么对应于 L_1L_2, 取 $\mathbb{Z}$ 的整闭包 C, 有 *Dedekind* 扩张 $(\mathbb{Z}\subseteq C,\mathbb{Q}\subseteq L_1L_2)$. 若

$$[L_1L_2:\mathbb{Q}]=[L_1:\mathbb{Q}][L_2:\mathbb{Q}]\qquad \mathrm{Disc}(B_1|\mathbb{Z})\text{ 和 }\mathrm{Disc}(B_1|\mathbb{Z})\text{ 互质}$$

那么

$$C=B_1B_2\qquad \mathrm{Disc}(C|\mathbb{Z})=\mathrm{Disc}(B_1|\mathbb{Z})^{[L_2:\mathbb{Q}]}\,\mathrm{Disc}(B_2|\mathbb{Z})^{[L_1:\mathbb{Q}]}$$

前者即是说若 B_1 有整基 $\beta_1,\dots,\beta_n$, B_2 有整数基 $\gamma_1,\dots,\gamma_m$, 那么 $\{\beta_i\gamma_j\}_{\substack{1\le i\le n\\1\le j\le m}}$ 是 C 的整基.

证明 如果 $\sigma_1,\dots,\sigma_n$ 给出所有 $L_1\to\overline{\mathrm{alg}}\,\mathbb{Q}$ 的同态, 如果 $\tau_1,\dots,\tau_n$ 给出所有 $L_2\to\overline{\mathrm{alg}}\,\mathbb{Q}$ 的同态, 因为 $[L_1L_2:\mathbb{Q}]=[L_1:\mathbb{Q}][L_2:\mathbb{Q}]$, 那么 $\{\sigma_i\tau_j\}_{\substack{1\le i\le n\\1\le j\le m}}$ 给出所有 $L_1L_2\to\overline{\mathrm{alg}}\,\mathbb{Q}$ 的同态.

[27] 一个多项式 f 的判别式是 $a_0^{2n-2}\prod_{i<j}(x_i-x_j)^2$, 其中 x_i 取遍 f 所有根, a_0 是首项系数, 例如对于二次多项式 aX^2+bX+c, 判别式为 b^2-4ac.

[28] 因为对于有限自由 Abel 群 G, G/dG 是有限群.

关于判别式的论断在证明前面的结论后将是完全是线性代数的 [29]. 取 $x \in C$, 假设 $x = \sum c_{ij}\beta_i\gamma_j$ 其中 $c_{ij} \in \mathbb{Q}$, 这样 [30]

$$\operatorname{tr}{\downarrow_{L_2}^{L_1L_2}}(\beta_k x) = \sum c_{ij} \operatorname{tr}{\downarrow_{L_2}^{L_1L_2}}(\beta_k\beta_i)\gamma_j = \sum_i \left(\operatorname{tr}{\downarrow_{\mathbb{Q}}^{L_1}}(\beta_k\beta_i) \sum_j c_{ij}\gamma_j \right)$$

同样根据 Cramer 法则, 若记 $\operatorname{Disc}(B_1|\mathbb{Z}) \sum c_{ij} = D_1$,

$$D_1\gamma_j = \sum (D_1 c_{ij})\, \gamma_j \in B_2$$

这迫使 $D_1 c_{ij} \in \mathbb{Z}$. 即 $c_{ij} \in \frac{1}{D_1}\mathbb{Z}$, 同理, 若记 $\operatorname{Disc}(B_2|\mathbb{Z}) = D_2$, 则 $c_{ij} \in \frac{1}{D_2}\mathbb{Z}$, 由于 D_1, D_2 互质, 故 $\frac{1}{D_1}\mathbb{Z} \cap \frac{1}{D_2}\mathbb{Z} = \mathbb{Z}$, 命题得证. □

II. 范数 下面, 我们将范数推广. 我们已经知道, 对于 Dedekind 扩张 $(A \subseteq B, K \subseteq L)$, $\operatorname{Nm}{\downarrow_K^L}$ 将 B 引入 A, 下面我们直接记范数为 $\mathcal{N}$. 我们下面要做的是将 $\mathcal{N}$ 延拓到所有理想上, 使得在所有主理想 (x) 上都有 $\mathcal{N}(x) = (\mathcal{N}x)$.

定义 2.55 (理想的范数) 对于 *Dedekind* 扩张 $(A \subseteq B, K \subseteq L)$, B 的非零素理想 $\mathfrak{P}$, 定义其 范数

$$\mathcal{N}\mathfrak{P} = \mathfrak{p}^{\mathrm{f}(\mathfrak{P}|\mathfrak{p})}$$

其中 $\mathfrak{p} = \mathfrak{P} \cap A$, 这是 A 中的理想. 因为唯一分解, 这一定义延拓到 B 的所有分式理想上.

显然, 如果有多层扩张 $(A \subseteq B \subseteq C, K \subseteq L \subseteq F)$, 那么有 塔性质

$$\mathcal{N}_K^L \mathcal{N}_L^F \mathfrak{a} = \mathcal{N}_K^F \mathfrak{a}$$

命题 2.56 对 n 次 *Dedekind* 扩张 $(A \subseteq B, K \subseteq L)$,

(1) 对于 A 的理想 $\mathfrak{a}$, $\mathcal{N}\mathfrak{a} = \mathfrak{a}^n$.

[29] 根据 (2.48), 故作为矩阵 $(\sigma_i\tau_{i'}\alpha_j\beta_{j'}) = (\sigma_i\alpha_j) \otimes (\tau_i\beta_j)$, 从而 $\det(\sigma_i\tau_{i'}\alpha_j\beta_{j'}) = \det(\sigma_i\alpha_j)^m \det(\tau_i\beta_j)^n$.

[30] 因为 $\operatorname{tr}{\downarrow_{L_2}^{L_1L_2}}(-) = \sum \sigma_i(-)$, 故限制在 L_1 上即 $\operatorname{tr}{\downarrow_{\mathbb{Q}}^{L_1}}(-)$.

(2) 如果 $K \subseteq L$ 是 *Galois* 扩张, *Galois* 群是 G, 那么对于任何 B 的理想 $\mathfrak{b}$,

$$\mathcal{N}\mathfrak{b} \cdot B = \prod_{\sigma \in G} \sigma\mathfrak{b}$$

(3) 任意 $x \in L$, 有

$$\mathcal{N}(x) = (\mathcal{N}x)$$

证明 (1) 只需要验证素理想即可, 则

$$\mathcal{N}\mathfrak{p} = \mathcal{N}(\mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}) = \mathfrak{p}^{e_1 f_1} \dots \mathfrak{p}^{e_r f_r} = \mathfrak{p}^n$$

(2) 同样只需要验证素理想, 设 $\mathfrak{P} \cap A = \mathfrak{p}$, 则 $\mathcal{N}\mathfrak{P} = \mathfrak{p}^f$,

$$\mathfrak{p}^f \cdot B = (\mathfrak{P}_1^e \dots \mathfrak{P}_r^e)^f$$

容易计算 $\sigma\mathfrak{P}$ 恰好按照 $n/r = ef$ 的重数取每个 $\mathfrak{P}$.

(3) 挑选一个含 (B, L) 的有限 Galois-Dedekind 扩张 $(A \subseteq C, K \subseteq E)$, 假设 $[E : L] = m$, 任意取 $x \in L$, 那么根据塔性质和 (1)

$$\begin{cases} \mathcal{N}_K^E(x) = \mathcal{N}_K^L \mathcal{N}_L^E(x) = \left[\mathcal{N}_K^L(x)\right]^m \\ \left(\mathcal{N}_K^E x\right) = \left(\mathcal{N}_K^L \mathcal{N}_L^E x\right) = \left[\left(\mathcal{N}_K^L x\right)\right]^m \end{cases}$$

如果能够证明上述两式左边相等, 那么根据 Dedekind 整环的唯一分解就有 $\left(\mathcal{N}_K^L x\right) = \mathcal{N}_K^L(x)$. 但是根据 (2)

$$\mathcal{N}_K^E(x) \cdot C = \prod_{\sigma \in G} \sigma\left(x\right) = \left(\prod_{\sigma \in G} \sigma(x)\right) = \left(\mathcal{N}_K^E x\right)$$

命题得证. □

记号 2.57 对于 *Dedekind* 扩张 $(\mathbb{Z} \subseteq A, \mathbb{Q} \subseteq K)$, 如果按照定义 $\mathcal{N}\mathfrak{a} = (a)$, 那么我们还约定 $\mathcal{N}\mathfrak{a} = |a| \in \mathbb{Z}$.

命题 2.58 对于 *Dedekind* 扩张 $(\mathbb{Z} \subseteq A, \mathbb{Q} \subseteq K)$, A 的理想 $\mathfrak{a}$, 则

$$\mathcal{N}\mathfrak{a} = |A/\mathfrak{a}|$$

证明 根据中国剩余定理, 只需要验证 $\mathfrak{a}$ 是素数方幂的情况, 而这个情况早在 (2.32) 的证明中就出现了. 具体来说

$$|A/\mathfrak{P}^e| = |A/\mathfrak{P}|^e = |\mathbb{Z}/p\mathbb{Z}|^{fe} = p^{fe} = \mathcal{N}\mathfrak{P}^e$$

命题得证. □

III. 类数有限 回忆 Minkowski 理论 (D.4).

记号 2.59 对于 n 次 *Dedekind* 扩张 $(\mathbb{Z} \subseteq A, \mathbb{Q} \subseteq K)$, 假如 K 有 r 个实嵌入[31] $\sigma_1, \dots, \sigma_n$, $2s$ 个复嵌入 $\sigma_{r+1}, \overline{\sigma_{r+1}}, \dots, \sigma_{r+s}, \overline{\sigma_{r+s}}$, 那么 $n = r + 2s$, 考虑如下的嵌入

$$\varsigma : K \longrightarrow \mathbb{R}^r \times \mathbb{C}^s \qquad x \longmapsto (\sigma_1 x, \dots, \sigma_{r+s} x)$$

为了行文方便, 记 $\mathbb{R}^r \times \mathbb{C}^s = V$, 通过视 $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$, 视作 $\mathbb{R}^{r+2s} = \mathbb{R}^n$. 换句话说

$$\varsigma : K \longrightarrow \mathbb{R}^n \qquad x \longmapsto (\sigma_1 x, \dots, \sigma_s x, \Re\sigma_{r+1} x, \Im\sigma_{r+1} x, \dots, \Re\sigma_{r+s} x, \Im\sigma_{r+s} x)$$

固定以上记号.

命题 2.60 对于 A 的非零理想 $\mathfrak{a}$, $\varsigma\mathfrak{a}$ 是 V 中的全格, 且基本区域的体积为

$$2^{-s}\,\mathcal{N}\mathfrak{a}\,\sqrt{|\operatorname{Disc}(A|\mathbb{Z})|}$$

证明 因为 $|A/\mathfrak{a}| < \infty$, 故 $\mathfrak{a}$ 是秩为 n 的自由 Abel 群, 取 $\mathfrak{a}$ 的一组基 $\alpha_1, \dots, \alpha_n$, 考虑 $\det(\tau_j \alpha_i)$. 其中 τ_j 取遍所有实复嵌入, 其值为[32]

$$\det(\tau_j \alpha_i) = \sqrt{\operatorname{Disc}(\alpha_1, \dots, \alpha_n)} = |A/\mathfrak{a}|\sqrt{\operatorname{Disc}(A|\mathbb{Z})} = \mathcal{N}\mathfrak{a}\,\sqrt{|\operatorname{Disc}(A|\mathbb{Z})|}$$

但是实际上基本区域的体积为 $\det(\varsigma_j \alpha_i)$, 通过行列变换知,

$$\det(\varsigma_j \alpha_i) = 2^{-s}\det(\tau_j \alpha_i) = 2^{-s}\,\mathcal{N}\mathfrak{a}\,\sqrt{|\operatorname{Disc}(A|\mathbb{Z})|}$$

命题得证. □

[31] 此时, 实嵌入指的是 $\sigma = \overline{\sigma}$ 的嵌入 $K \to \mathbb{C}$, 其中 $\overline{*}$ 表示共轭.

[32] 取 A 的整基 $\beta_1, \dots, \beta_n$, $\alpha_i = \sum c_{ij}\beta_j$, $\det(c_{ij})$ 就是其指数, 见 (B.2).

引理 2.61 对于 A 的非零理想 $\mathfrak{a}$, 存在 $a \in \mathfrak{a}$,

$$\mathcal{N}a \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\, \mathcal{N}\mathfrak{a}\, \sqrt{|\operatorname{Disc}(A|\mathbb{Z})|}$$

证明 作如下 V 中的形状

$$X(t) = \{(x_i)_{i=1}^r \times (z_j)_{j=r+1}^{r+s} \in \mathbb{R}^r \times \mathbb{C}^s : |x_1| + \ldots + |x_r| + 2|z_1| + \ldots + 2|z_s| \leq t\}$$

经过计算[33], 其体积为 $2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}$. 而如果取 t 使得

$$2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!} \geq 2^n \cdot 2^{-s}\, \mathcal{N}\mathfrak{a}\, \sqrt{|\operatorname{Disc}(A|\mathbb{Z})|}$$

选择最小的 t, 满足

$$t^n = n!\, \frac{2^{n-r}}{\pi^s}\, \mathcal{N}\mathfrak{a} \sqrt{|\operatorname{Disc}(A|\mathbb{Z})|} \tag{$*$}$$

根据 Minkowski 定理 (D.4), 有 $a \in \mathfrak{a}$ 使得

$$\begin{aligned}
\mathcal{N}a &= |\sigma_1 a| \ldots |\sigma_r a||\sigma_{r+1} a|^2 \ldots |\sigma_{r+s} x|^2 && \because \text{均值不等式} \\
&\leq \tfrac{1}{n^n} \left(\textstyle\sum |\sigma_i a| + \sum 2|\sigma_j a|\right)^n && \because a \in X(t) \\
&\leq \tfrac{t^n}{n^n} && \because (*), n - r = 2s \\
&\leq \left(\tfrac{4}{\pi}\right)^s \tfrac{n!}{n^n}\, \mathcal{N}\mathfrak{a}\, \sqrt{|\operatorname{Disc}(A|\mathbb{Z})|}
\end{aligned}$$

命题得证. □

---

[33] 作换元 $z_j = x_j + iy_i = \frac{1}{2} r_j(\cos\theta_j + \sin\theta_j)$, 则 $\frac{\partial(x_j, y_j)}{\partial(r_j, \theta_j)} = \frac{1}{4} r_j$, 此时 θ_j 自由了, 得到

$$\mu(X(t)) = \int_{X(t)} 1 \mathrm{d}x_i \mathrm{d}x_j \mathrm{d}y_j = \frac{1}{4^s} \int_{\ldots} \rho_{r+1} \ldots \rho_{r+s} \mathrm{d}x_i \mathrm{d}\rho_j \mathrm{d}\theta_j = \frac{(2\pi)^s}{4^s} \int_{\ldots} \rho_{r+1} \ldots \rho_{r+s} \mathrm{d}x_i \mathrm{d}\rho_j$$

将积分区域缩小为 $x_i \geq 0$,

$$\mu(X(t)) = \frac{2^r (2\pi)^s}{4^s} \int_{\substack{x_i \geq 0, \rho_j \geq 0 \\ \sum x_i + \sum \rho_j \leq t}} \rho_{r+1} \ldots \rho_{r+s} \mathrm{d}x_i \mathrm{d}\rho_j =: \frac{2^r (2\pi)^s}{4^s} I(r, s, t)$$

注意到

$$I(r, s, t) = t^{r+2s} I(r, s, 1) \qquad I(r, s, 1) = \frac{I(r, s-1, 1)}{(r+2s)(r+2s-1)} \qquad I(r, s, 1) = \frac{I(r-1, s)}{r+2s}$$

归纳得

$$I(r, s, t) = \frac{1}{(r+2s)!} = \frac{t^n}{n!}$$

定理 2.62 (Minkowski 界) 任意 A 的非零分式理想 $\mathfrak{a}$, 存在整理想 $\mathfrak{c}$ 使得

$$\mathcal{N}\mathfrak{c} \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\operatorname{Disc}(A|\mathbb{Z})|}$$

且 $\mathfrak{c}$ 和 $\mathfrak{a}$ 只相差主理想. 右边的界被称为 **Minkowski 界**.

证明 取 $d \in K$ 使得 $d\mathfrak{a}^{-1} = \mathfrak{b}$ 是整理想, 用 (2.61) 可以找 $b \in \mathfrak{b}$ 使得

$$\mathcal{N}b \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \mathcal{N}\mathfrak{b} \sqrt{|\operatorname{Disc}(A|\mathbb{Z})|}$$

取 $\mathfrak{c} = b\mathfrak{b}^{-1}$ 这是整理想[34] 则 $\mathfrak{c}$ 和 $\mathfrak{a}$ 只相差主理想, 且

$$\mathcal{N}c \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\operatorname{Disc}(A|\mathbb{Z})|}$$

命题得证. □

推论 2.63 (类数有限定理) 特别地, A 的类数是有限的.

证明 因为取特定范数的分式理想是有限的, 因为根据范数的定义, 其素因子必须是一些有限素数的扩张, 而后者是有限的, 而根据定义, 其指数又不会无限大, 故只要证明这个命题的前半部分. □

评注 2.64 读者会发现如果我们只为了证明类数有限, 其实不必大费周章地在 *(2.61)* 那样取 $X(t)$ 并计算, 取得粗一些例如

$$X(t) = \{(x_i)_{i=1}^n \in \mathbb{R}^r \times \mathbb{C}^s : |x_i| \leq t\}$$

在 $\mathcal{N}x$ 的粗略估计之后也足以得到一个界, 只是这个界未必如 *Minkowski* 界有效, 因为 $\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}$ 非常迅速地趋向于 0.

例 2.65 对于 $\mathbb{Q}[i]$, $n = 2, r = 0, s = 1$, 于是根据 *(2.51)* 其 *Minkowski* 界为 $\frac{4}{\pi}\frac{2!}{2^2}\sqrt{4} < 2$, 但是哪里有真理想范数满足这个条件呢? 说明在类群中, 所有理想都和 (1) 差一个主理想, 故 $\mathbb{Z}[i]$ 是主理想整环.

[34] 因为 $b \in \mathfrak{b} \iff \mathfrak{b}|(b) \iff 1|b\mathfrak{b}^{-1}$.

例 2.66 对于 $\mathbb{Q}[\sqrt{-5}]$, $n=2, r=2, s=0$, 于是根据 *(2.51)* 其 *Minkowski* 界为 $\frac{2!}{2^2}\sqrt{20}<3$, 唯一有可能的理想 $\mathfrak{a}$ 使得 $\mathcal{N}\mathfrak{a}<3$ 的是 $\mathcal{N}\mathfrak{a}=2$, 这迫使 $\mathfrak{a}$ 是素理想, 且 $\mathfrak{a}\cap\mathbb{Z}=(2)$, 且 $\mathfrak{f}(\mathfrak{a}|\mathfrak{p})=1$, 而通过 *(2.38)* 的计算我们知道 $\mathfrak{a}=(2,1+\sqrt{-5})$ 是唯一满足条件的理想, 而我们有知道 $\mathbb{Z}[\sqrt{-5}]$ 不是主理想整环, 故 $\mathrm{CLASS}\mathbb{Z}[\sqrt{-5}]=2$.

本节说明对于 $\mathbb{Z}$ 的 Dedekind 扩张的类群是有限的, 但是一般的 Dedekind 整环不是有限的.

IV. Dirichlet 单位定理 同样, 下面我们固定 Dedekind 扩张

$$(\mathbb{Z}\subseteq A, \mathbb{Q}\subseteq K)$$

下面我们关心 A 的单位的情况, 回忆 (1.2) 和 (1.21), 这似乎表明 "实扩张" 和 "复扩张" 情况大不相同.

引理 2.67 对于 $x\in A$, x 是单位根 $\iff$ 对任何[35]σ, $|\sigma x|=1$,

证明 只要证明 $\{1,x,x^2,\dots\}$ 是有限集合. 实际上, 每个 x^i 的次数都不超过 n, 其共轭 $\sigma(x^i)=(\sigma x)^i$ 也具有范数 1, 容易根据三角不等式得到 x^i 的最小多项式是次数不超过 n, 各项系数绝对值不超过 n 的整系数多项式, 这样的多项式只有有限个. 故 $\{1,x,x^2,\dots\}$ 是有限集合. □

引理 2.68 对于 $x\in A$, x 是单位 $\iff |\mathcal{N}x|=1$,

证明 回忆 (1.2) 和 (1.21), 不难直接验证. □

我们处理的工具仍然是 Minkowski 理论 (D.4), 不过此时为乘性. 为此作以下记号的约定.

记号 2.69 对于 n 次 *Dedekind* 扩张 $(\mathbb{Z}\subseteq A,\mathbb{Q}\subseteq K)$, 假如 K 有 r 个实嵌入[36] $\sigma_1,\dots,\sigma_n$, $2s$ 个复嵌入 $\sigma_{r+1},\overline{\sigma_{r+1}},\dots,\sigma_{r+s},\overline{\sigma_{r+s}}$, 那么 $n=r+2s$, 考虑如下的同态

$$\ell: K\setminus 0\longrightarrow \mathbb{R}^{r+s}\qquad x\longmapsto(\log|\sigma_1 x|,\dots,\log|\sigma_{r+s}x|)$$

[35]其中 σ 取遍 $K\to\overline{\mathrm{alg}}\,\mathbb{Q}$ 的所有同态.

[36]此时, 实嵌入指的是 $\sigma=\overline{\sigma}$ 的嵌入 $K\to\mathbb{C}$, 其中 $\overline{*}$ 表示共轭.

容易验证, $\ker \ell = A$ 的单位根, 且根据如上两个引理, 单位群 $\operatorname{unit} A$ 在 ℓ 下的像就是如下超平面和 $A \setminus 0$ 的像的交

$$X_1 + \ldots + X_r + 2X_{r+1} + \ldots + 2X_{r+s} = 0$$

记这个超平面为 H. 换言之目前记号如图

$$\begin{array}{ccccc} A \setminus 0 & \xrightarrow{\ell} & \ell(A \setminus 0) & \longrightarrow & V \\ \uparrow & & \uparrow & & \uparrow \\ \operatorname{unit} A & \xrightarrow[\ell]{} & \ell(\operatorname{unit} A) & \longrightarrow & H \end{array}$$

定理 2.70 单位群在 ℓ 下的像 $\ell(\operatorname{unit} A)$ 是 H 中的全格.

证明 下面施展 (D.2) 和 (D.3), 我们还会借用 (2.59) 的记号.

首先, 先展开回忆. 在 (2.60), ςA 是 V 的全格.

接着, $\ell(\operatorname{unit} A)$ 是格. 利用 (D.2), 只要说明任意 $d > 0$, 满足 $\log|\sigma_i x| \leq d$ 对所有 i 的 x 只有有限个即可. 这等价于

$$\mathrm{e}^{-d} \leq |\sigma x| \leq \mathrm{e}^{d}$$

转化为加性, 因为 ςA 是全格, 所以有限性得证.

最后, $\ell(\operatorname{unit} A)$ 是全格. 利用 (D.3), 只要找有界集合 M 使得 $H = M + \ell(\operatorname{unit} A)$. 通过取原像即找 M' 使得

$$M' \subseteq \{x \in K : |\mathcal{N} x| = 1\} = \bigcup_{u \in \operatorname{unit} A} M'u$$

且 $\ell(T)$ 有界. 对于 $(x_i) \in V = \mathbb{R}^n$, 再定义

$$\mathcal{N}(x_i) = |x_1| \ldots |x_r| \cdot \sqrt{x_{r+1}^2 + x_{r+2}^2} \cdots \sqrt{x_{n-1}^2 + x_n^2}$$

容易知道, 对于 $x \in K$, $\mathcal{N} x = \mathcal{N} \sigma x$. 即是找 M'' 使得

$$M'' \subseteq \{(x_i) \in V : \mathcal{N}(x_i) = 1\} = \bigcup_{u \in \operatorname{unit} A} M''\varsigma u$$

通过取 $M'' = M''' \cap \{(x_i) \in V : \mathcal{N}(x_i) = 1\}$, 实际上只需要找 M''' 使得 [37]

$$\{(x_i) \in V : \mathcal{N}(x_i) = 1\} \subseteq \bigcup_{u \in \operatorname{unit} A} M'' \varsigma u$$

且关于有界性的条件只需要 M'' 在 V 中有界即可, 因为 $\varsigma(T)$ 有界, 故 $\log|\sigma_i x|$ 有上界, 加之 $|\sigma_1 x| \dots |\sigma_{r+s} x| = 1$, 故有下界.

取 V 充分大的有界中心对称凸集

$$C = [-c_1, c_1] \times \dots \times [-c_n, c_n] \qquad c := c_1 \dots c_n$$

对于任意 $y \in \{(x_i) \in V : \mathcal{N}(x_i) = 1\}$, 诸位相乘 Cy 体积不变, 此时 Minkowski 定理 (D.4) 断言必有 $a \in A \setminus 0$ 使得 $\varsigma a \in Cy^{-1}$, 即 $y \in C(\varsigma a)^{-1}$. 对这样的 a, 有

$$\mathcal{N}a = \mathcal{N}(\varsigma a) \leq c_1 \dots c_n \mathcal{N}y = c$$

在相差单位的意义下, 这样的 a 是有限的[38], 选择这样有限的 a_i, 取 $M'' = \bigcup_i C(\varsigma a_i)^{-1}$ 还是有界集合, 这样

$$\bigcup_{u \in \operatorname{unit} A} M'' \varsigma u^{-1} = \bigcup_{i,u} C(\varsigma a_i u)^{-1} = \bigcup_{\mathcal{N}a \leq c} C(\varsigma a)^{-1} \supseteq \{(x_i) \in V : \mathcal{N}(x_i) = 1\}$$

命题得证. □

推论 2.71 (Dirichlet 单位定理) *记号承上, 特别地,*

$$A\text{的单位群} \,/\, A\text{的单位根群} \cong \mathbb{Z}^{r+s-1}$$

特别地,

$$\operatorname{unit} A \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}^{r+s-1}$$

注意到左边都是乘法群, 右边都是加法群.

证明 第一个论断根据 (2.69) 关于 ℓ 核的断言. 第二个论断是因为 A 只含有限个单位根, 以及如下两个简单的代数结论. (1) 单位根群的有限子群必是循环群. (2) 如果 Abel 群的商群 A/B 是自由的, 那么 $A \cong B \oplus A/B$. □

[37] 因为 $\sigma u \in \{(x_i) \in V : \mathcal{N}(x_i) = 1\}$.

[38] 因为取特定范数值的理想是有限的.

例 2.72 事实上不是所有单位圆上且在 $\mathbb{Z}$ 整的元都是单位根, 例如考虑如下方程

$$X^4 + X^3 - X^2 + X + 1 = 0$$

化为 $\left(X + \frac{1}{X}\right)^2 + \left(X + \frac{1}{X}\right) - 3 = 0$, 这样

$$X + \frac{1}{X} = \frac{-1 \pm \sqrt{13}}{2}$$

考虑 $\pm = +$ 时, 上方程有两个实根, $\pm = -$ 时, 上方程有两个虚根. 这两个虚根必定共轭, 且乘起来为 1, 这迫使其落在单位圆上. 但是最开始给定的方程不可约. 事实上, 这样的代数整数从 4 次才开始有[39].

例 2.73 对于 *Gauss* 整数环 $\mathbb{Z}[i]$, $n = 2, r = 0, s = 1$, 这样其单位群只有单位根部分. 这和 *(1.2)* 一致.

例 2.74 对于 $\mathbb{Z}[\sqrt{2}]$, $n = 2, r = 2, s = 0$, 这样其单位群是 $\{\pm 1\}$ 和 $\mathbb{Z}$ 的直和. 这和 *(1.21)* 一致.

2.4 分歧性

定理 2.75 (分歧定理) 对于任何 $\mathbb{Z}$ 的 *Dedekind* 扩张 A, 素数 $p \in \mathbb{Z}$, 则

$$(p) \text{ 分歧} \iff p \mid \mathrm{Disc}(A|\mathbb{Z})$$

证明 设 $\mathrm{Frac}A = K$, 选出 A 的整基 $\alpha_1, \dots, \alpha_n$. 注意到根据中国剩余定理

$$\frac{B}{pB} = \bigoplus_{\mathfrak{P} \ni p} \frac{B}{\mathfrak{P}^{\mathsf{e}(\mathfrak{P}|p)}}$$

此时 A/pA 是一个 $\mathbb{Z}/p\mathbb{Z}$-代数. 所谓 (p) 分歧就是某个 $\mathsf{e}(\mathfrak{P}|p) \geq 2$, 即 A/pA 有幂零元. 所谓 (p) 不分歧就是所有 $\mathsf{e}(\mathfrak{P}|p) = 1$, 即 A/pA 是一些域的乘积.

显然, 根据基本恒等式的证明过程 (2.32), $\alpha_1, \dots, \alpha_n$ 在 A/pA 中构成一组基. 且

$$\det(\mathrm{tr}(\alpha_i \alpha_j)) \equiv \det(\mathrm{tr}(\alpha_i \alpha_j \cdot *)) \mod p$$

[39]因为二次我们可以把所有代数数整数都算出来, 而三次都具有实根, 可能产生单位圆上元素的二次方程常数项必须为 1, 但是这就迫使实根是实数, 矛盾.

其中, 对于 $x \in A/pA$, $x \cdot *$ 表示 $y \mapsto xy$, 即左乘 x 产生的 A/pA 的线性映射. 但是容易验证, 后者是不依赖于基的选取的.

假如有 $x \in A$ 使得其在 A/pA 中是幂零元, 那么任意 $y \in A$, 左乘 xy 作为 A/pA 上的 $\mathbb{Z}/p\mathbb{Z}$-线性变换也是幂零的, 故 $\mathrm{tr}(xy \cdot *) = 0$, 故将 x 扩充为一组基, 根据判别式的定义, 判别式必须为 0. 换言之 $p | \mathrm{Disc}(A|\mathbb{Z})$.

反之, 假如 A/pA 是一些域的乘积, 对于某个直和项域 F 中的元素 x, 由于这些域互不影响, $x \cdot *$ 无论是表示在 A/pA 上还是 F 上的线性映射, $\mathrm{tr}(x \cdot *)$ 是一致的. 那么将基分别选在这些域上. 只需要证明对于 $\mathbb{Z}/p\mathbb{Z}$ 的扩域 F 的一组基 $x_1, \dots, x_n$, 都有

$$\det(\mathrm{tr}(x_i x_j \cdot *)) \neq 0$$

这根据迹配合的非平凡性 (B.28) 是显然的. □

定理 2.76 *对于任何 $\mathbb{Z}$ 的 Dedekind 扩张 A, 总有 $\mathbb{Z}$ 的素理想分歧.*

证明 在 (2.61) 中取 $\mathfrak{a} = A$, 那么有 $a \in A$ 使得

$$1 \leq \mathcal{N}a \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \mathcal{N}\mathfrak{a} \sqrt{|\mathrm{Disc}(A|\mathbb{Z})|}$$

这样

$$\sqrt{|\mathrm{Disc}(A|\mathbb{Z})|} \geq \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!} \geq \left(\frac{\pi}{4}\right)^n \frac{n^n}{n!} \quad (\text{归纳}) \quad > 1$$

根据 (2.75), 总有素理想是分歧的. □

2.5 应用—计算 Galois 群

本部分采自 [5]. 回看 Hilbert 分歧理论 (2.45), 当中有对 Galois 群的断言, 我们想要做的是通过剩余域的 Galois 群来反应原本域的 Galois 群, 再加以分析得到 Galois 群.

下面限定代数扩张 $\mathbb{Q} \subseteq K$, 假设 K 是 n 次不可约整系数多项式 f 的分裂域, 设对应的 Galois 群为 G. 由于 Galois 群理解为根的置换, 故可以视 $G \subseteq \mathfrak{S}_n$. 假设对应的 Dedekind 扩张为 $\mathbb{Z} \subseteq A$.

定理 2.77 对于素数 p, 假设 f 在 $\mathbb{Z}/p\mathbb{Z}[X]$ 的完全分解为

$$f \equiv f_1 \dots f_r \mod p \qquad \deg f_i = d_i$$

假如 f_i 各不相同, 即分解为不同的不可约式乘积, 那么 G 中含有一个不相交 d_i-轮换的乘积.

证明 任何素理想扩张 $(p) \subseteq \mathfrak{p}$, 首先根据 (2.34) 分解为不同的不可约式乘积说明 [40] 分歧指数为 1, 所以根据 Hilbert 分歧理论 (2.45), 可以认为

$$G_0 := \mathrm{Gal}(A/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}) \subseteq G$$

下面的问题是如何计算 G_0, 显然任何 $\sigma \in G_0$ 只能将 f_i 的根映为 f_i 的根, 根据上述 $\subseteq$ 的构造 (2.44), 并且视 $G \subseteq \mathfrak{S}_n$, 有

$$G_0 \subseteq \mathfrak{S}_{d_1} \times \dots \mathfrak{S}_{d_r} \subseteq \mathfrak{S}_n$$

其中后一个 $\subseteq$ 是不相交轮换的乘积. 于是只说明每个都是轮换即可, 这根据 f_i 不可约显然[41]. □

例 2.78 考虑 $f(X) = X^5 - X + 1$, 下面计算其分裂域的 *Galois* 群 G. 此时 $f(X)$ 在 $\mathbb{Z}/3\mathbb{Z}$ 上不可约 [42], 而

$$X^5 - X + 1 \equiv (X^2 + X + 1)(X^3 + X^2 + 1) \mod 2$$

于是 G 含有写成不相交轮换形如 $(a_1a_2a_3a_4a_5)$ 和 $(b_1b_2)(c_1c_2c_3)$ 的元素, 他们生成了整个 $\mathfrak{S}_5$.

2.6 例子—二次扩张

下面我们考虑 $\mathbb{Q}[\sqrt{d}]$ 对应的二次 Dedekind 扩张

$$\mathbb{Z} \subseteq \mathbb{Z}[\delta] \qquad \delta = \begin{cases} \frac{1+\sqrt{d}}{2} & d \equiv 1 \mod 4 \\ \sqrt{d} & d \equiv 2, 3 \mod 4 \end{cases}$$

[40] 具体来说, 任意添加 f 的一个根不分歧, 接着再添加也不分歧, 因为分解成为不同的不可约式乘积就是说 $f \bmod \mathfrak{p}$ 没有重根.

[41] 这是因为如果有两条以上的轨道那么根据 Galois 理论 (B.23) $\prod(X-a), \prod(X-b)$ 都是 $\mathbb{Z}/p\mathbb{Z}[X]$ 上的多项式, 与 f_i 不可约矛盾.

[42] 因为二次多项式是有限的, 不可约的则更少

我们已经在 (2.51) 计算过

$$\mathrm{Disc}(\mathbb{Z}[\delta]|\mathbb{Z}) = \mathrm{Disc}(1,\delta) = \begin{cases} d & d \equiv 1 \mod 4 \\ 4d & d \equiv 2,3 \mod 4 \end{cases}$$

下面记

$$A = \mathbb{Z}[\delta] \qquad \Delta = \mathrm{Disc}(\mathbb{Z}[\delta]|\mathbb{Z})$$

定理 2.79 *对于素数 p 如何分解, 有*

- *$p|\Delta$, 则素理想分解为 $pA = \mathfrak{p}^2$, 其中*

$$\mathsf{e}(\mathfrak{p}|p) = 2 \qquad \mathsf{f}(\mathfrak{p}|p) = 1 \qquad \mathsf{r}(p) = 1 \qquad \mathcal{N}\mathfrak{p} = p$$

- *对于奇素数 $p \nmid \Delta$, 且 $\left(\frac{d}{p}\right) = -1$, 或当 $p = 2 \nmid \Delta$ 且 $d \equiv 5 \mod 8$, 则 $pA = \mathfrak{p}$, 其中,*

$$\mathsf{e}(\mathfrak{p}|p) = 1 \qquad \mathsf{f}(\mathfrak{p}|p) = 2 \qquad \mathsf{r}(p) = 1 \qquad \mathcal{N}\mathfrak{p} = p^2$$

- *对于奇素数 $p \nmid \Delta$ 且 $\left(\frac{d}{p}\right) = 1$, 或当 $p = 2 \nmid \Delta$ 且 $d \equiv 1 \mod 8$, 则 $pA = \mathfrak{p}_1\mathfrak{p}_2$, 其中, 对于 $i = 1, 2$*

$$\mathsf{e}(\mathfrak{p}_i|p) = 1 \qquad \mathsf{f}(\mathfrak{p}_1|p) = 1 \qquad \mathsf{r}(p) = 2 \qquad \mathcal{N}\mathfrak{p} = p$$

证明 第一则论断是显然. 得益于 (2.34) 和 (2.35), 对于 $p \neq 2$ 时, 我们只需要考虑 $X^2 - d$ 在 $\mathbb{Z}/p\mathbb{Z}[X]$ 中如何分解, 这就是二次互反律所断言的内容 Legandre 符号的含义所在.

问题是 $p = 2$ 时的情况. $d \equiv 2, 3 \bmod 4$ 时, $2|\Delta$, 或者直接计算知 $X^2 - d \equiv (X + d)^2$ 始终分歧. $d \equiv 1 \bmod 4$ 时, 此时 $\delta = \frac{1+\sqrt{d}}{2}$, 最小多项式是 $X^2 - X - \frac{d-1}{4}$, 在 $\frac{d-1}{4} \equiv 0 \bmod 2$ 时, 即 $d \equiv 1 \bmod 8$ 时, 可以分解成两个不同的不可约式的乘积, 在 $\frac{d-1}{4} \equiv 1 \bmod 2$ 时, 即 $d \equiv 5 \bmod 8$ 时, 是不可约的. 这样命题得证. □

2.7 例子 — 分圆扩张

回忆分圆扩张 (B.34). 我们的目的是计算其整基. 为此我们先计算第素数方幂个分圆扩张. 对于素数的方幂 p^n, 考虑第 p^n 个分圆扩张 $\mathbb{Q} \subseteq K$, 其次数是 $\varphi(p^n) = p^n - p^{n-1}$. 注意到 p^n 次本原单位根 ζ 是代数整数, 其最小多项式是

$$f(X) = \Phi_{p^n}(X) = 1 + X^{p^{n-1}} + \ldots + \left(X^{p^{n-1}}\right)^{p-1}$$

计算判别式[43]

$$\mathrm{Disc}(1, \zeta, \ldots, \zeta^{p^n - p^{n-1} - 1}) = \pm p^c$$

其中

$$\pm = (-1)^{\frac{p^n - p^{n-1}}{2}} \qquad c = p^{n-1}(pn - n - 1)$$

定理 2.80 *记号承上, 假设对应的 Dedekind 扩张是 $\mathbb{Z} \subseteq A$. 则 $A = \mathbb{Z}[\zeta]$, 其中 ζ 是任意一个 p^n 次本原单位根. 且*

证明 需要注意到, $1, \zeta, \zeta^2, \ldots, \zeta^{p^n - p^{n-1} - 1}$ 都是代数整数, 故 $\mathbb{Z}[\zeta] \subseteq A$. 根据前面的计算, 根据 (2.49), $\mathrm{Disc}(A|\mathbb{Z}) | p^c$.

另一方面, 我们可以计算 pA 的分解. 注意到 $f'(1) = p$, 这样

$$pA = f'(1)A = \prod (1 - \zeta_i)A = \prod \frac{1 - \zeta_i}{1 - \zeta}(1 - \zeta)A = \left((1 - \zeta)A\right)^{p^n - p^{n-1}}$$

[43] 具体来说, 根据 (2.52), 需要计算

$$\prod_{i \neq j} (\zeta_i - \zeta_j) = \prod_i f'(\zeta_i) = \prod_i f'(\zeta_i) = \prod_\sigma f'(\sigma\zeta) = \mathrm{Nm}_{\mathbb{Q}}^{K\downarrow} f'(\zeta)$$

其中 $\{\zeta_i\}$ 是所有 p^n 次本原单位根. 因为 $f(X)(X^{p^{n-1}} - 1) = X^{p^n} - 1$, 两边同时微分带入 ζ 得到

$$f'(\zeta) = \frac{p^r \zeta^{p^n - 1}}{\zeta^{p^{n-1}} - 1}$$

这样

$$\mathrm{Nm} f'(\zeta) = \frac{\mathrm{Nm} p^n \cdot \mathrm{Nm} \zeta^{p^n - 1}}{\mathrm{Nm}(\zeta^{p^{n-1}} - 1)} = \frac{p^{n(p^n - p^{n-1})} \cdot 1}{p^{p^{n-1}}} = p^c$$

其中 $\zeta^{p^{n-1}}$ 是 p 次本原单位根, 其范数的计算需要先在 p 次分圆扩张上计算. 而

$$\mathrm{Disc}(\ldots) = \prod_{i \neq j} (\zeta_i - \zeta_j) = (-1)^{\frac{p^n - p^{n-1}}{2}} \prod_{i < j} (\zeta_i - \zeta_j)^2$$

其中 ζ_i 取遍所有 n 次本原单位根, ζ 是其中任意一个固定的 n 次本原单位根, 最后的等号是因为 $\frac{1-\zeta^i}{1-\zeta}$ 是单位 [44]. 这说明 $(1-\zeta)A$ 是素理想, 且根据基本恒等式 (2.32)f$(1-\zeta|p)=1$, 即

$$A/(1-\zeta)A = \mathbb{Z}/p\mathbb{Z}$$

换句话说

$$A = \mathbb{Z} + (1-\zeta)A \quad \Rightarrow \quad A = \mathbb{Z}[\zeta] + (1-\zeta)A$$

运用循环归纳法, 将 A 不断带入自己得到

$$A = \mathbb{Z}[\zeta] + (1-\zeta)\Big(\mathbb{Z}[\zeta] + (1-\zeta)A\Big) = \mathbb{Z}[\zeta] + (1-\zeta)^2 A$$

以此类推

$$\forall s>0, A = \mathbb{Z}[\zeta] + (1-\zeta)^s A \quad \Rightarrow \quad \forall t>0, A = \mathbb{Z}[\zeta] + p^t A$$

而根据 (2.50), 我们知道 $A \subseteq \frac{\mathbb{Z}[\zeta]}{\mathrm{Disc}(1,\zeta,\dots)} = \frac{\mathbb{Z}[\zeta]}{\pm p^c}$, 故

$$A = \mathbb{Z}[\zeta] + p^c A \subseteq \mathbb{Z}[\zeta] + \mathbb{Z}[\zeta] = \mathbb{Z}[\zeta]$$

命题得证. □

定理 2.81 *对于第 n 个分圆扩张 K, 对应的 Dedekind 扩张是 $\mathbb{Z} \subseteq A$, 则 $A = \mathbb{Z}[\zeta]$, 其中 ζ 是任意一个 n 次本原单位根.*

证明 将 n 拆解成素数的方幂, 然后利用 (B.35) 和 (2.54). □

[44] 因为 ζ 是本原单位根, ζ_i 是 ζ 的方幂, 从而 $\frac{1-\zeta_i}{1-\zeta}$ 是 ζ 的多项式是代数整数, 反之亦然.

Part II

第二部分
赋值理论

Chapter 3

例子—p 进数域

下面固定素数 p.

3.1 p 进数域的算数

定义 3.1 (p 进整数) 对于一串数 $\{a_i\}_{i=0}^{\infty} \subseteq \{0, \ldots, p-1\}$, 形式地记

$$a_0 + a_1 p + \ldots = \sum_{i=0}^{\infty} a_i p^i$$

称之为一个**形式 p 进整数**. 将全体这样的形式记为 $\mathbb{Z}_p$, 称为 **p 进整数环**. 所谓 "形式", 就是二者相等当且仅当每一位都相同, 注意, 此时的加号和连加号也都是形式的.

命题 3.2 对于两个形式 p 进数 $\alpha = \sum_{i=0}^{\infty} a_i p^i, \beta = \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_p$, 记前 n 项的部分和 $\alpha^{(n)} = \sum_{i=0}^{n} a_i p^i, \beta^{(n)} = \sum_{i=0}^{n} b_i p^i \in \mathbb{Z}$. 假设 $\alpha^{(n)}$ 和 $\beta^{(n)}$ 的和与积展成 p 进制为

$$\alpha^{(n)} + \beta^{(n)} = \sum_{i=0}^{\infty} c_i^{(n)} p^i \qquad \alpha^{(n)} \beta^{(n)} = \sum_{i=0}^{\infty} d_i^{(n)} p^i$$

注意到中间的 $\sum$ 是有限和. 则

$$\forall i \leq k, \quad n \geq k, \quad c_i^{(n)} = c_i^{(k)}, \quad d_i^{(n)} = d_i^{(k)}$$

即, α,β 的部分和项数充分大时, γ,δ 的部分和也逐步变为常数, 不再变动.

证明 显然, 对于任何 $n \geq k$,

$$\alpha^{(n)} \equiv \alpha^{(k)} \mod p^{k+1} \qquad \beta^{(n)} \equiv \beta^{(k)} \mod p^{k+1}$$

则

$$\alpha^{(n)} \equiv a_k p^k + \ldots + a_0 \mod p^{k+1} \qquad \beta^{(n)} \equiv b_k p^k + \ldots + b_0 \mod p^k$$

故

$$\alpha^{(n)} + \beta^{(n)} \equiv \alpha^{(k)} + \beta^{(k)} \mod p^{k+1} \qquad \alpha^{(n)}\beta^{(n)} \equiv \alpha^{(k)}\beta^{(k)} \mod p^{k+1}$$

而在 $\mod p^{k+1}$ 意义下, p 进制展开是唯一的, 这就意味着不再变化. □

定义 3.3 ($\mathbb{Z}_p$ 上的运算) 沿袭 *(3.2)* 的记号, 对于两个形式 p 进数 $\alpha = \sum_{i=0}^{\infty} a_i p^i, \beta = \sum_{i=0}^{\infty} b_i p^i \in \mathbb{Z}_p$. 假设 c_i 是 $c_i^{(n)}$ 最终固定下来的数, d_i 是 $d_i^{(n)}$ 最终固定下来的数, 定义

$$\alpha + \beta = \sum_{i=0}^{\infty} c_i p^i \qquad \alpha\beta = \sum_{i=0}^{\infty} d_i p^i$$

这可以类比实数的加法和乘法可以用有限小数的加法和乘法逼近. 后续工作还有验证运算律.

命题 3.4 在 $\mathbb{Z}_p$ 中, 加法是结合的, 且具有零元 $0 = \sum_{i=0}^{\infty} 0p^i$, 乘法是交换且结合的, 乘法对加法是分配的, 且具有单位元 $1 = 1 + \sum_{i=1}^{\infty} 0p^i$. 且 $\mathbb{Z} \to \mathbb{Z}_p$, 即将 n 映射为 n 的 p 进制展开, 是单射. 且

$$xy = 0 \quad \Rightarrow \quad x = 0 \text{ 或 } y = 0$$

一言以蔽之, $\mathbb{Z}_p$ 是一个特征为 0 的整环.

证明 关于构成一个环的论证是因为总可以截断前 n 位验证, 这样无非是说 $\mathbb{Z}/p^{n+1}\mathbb{Z}$ 是一个环. 为了看到这是一个整环, 只需要考虑 x,y 非零的最低位即可. □

例 3.5 $p \cdot \sum_{i=0}^{\infty} a_i p^i = \sum_{i=1}^{\infty} a_{i-1} p^i$.

例 3.6 若我们记

$$\sum_{i=0}^{\infty} a_i p^i = \ldots a_2\, a_1\, a_0$$

上面的定义确保我们可以列竖式计算加法减法和乘法, 如同进位借位等问题和小学所学的如出一辙. 例如在 $p = 2$ 时,

$$\begin{array}{cccccccc} & \ldots & 1 & 1 & 1 & 1 & 1 & 1 \\ + & \ldots & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline & \ldots & 0 & 1 & 0 & 1 & 0 & 0 \end{array} \qquad \begin{array}{cccccccc} & \ldots & 1 & 1 & 1 & 1 & 1 & 1 \\ \times & \ldots & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline & \ldots & 1 & 1 & 1 & 1 & 1 & 1 \\ & \ldots & 1 & 1 & 1 & 1 & & \\ & \ldots & \ldots & \ldots & & & & \\ \hline & \ldots & 1 & 0 & 1 & 0 & 1 & 1 \end{array}$$

定义 3.7 记 $\mathbb{Z}_p$ 的商域为 $\mathbb{Q}_p$, 这被称为 p **进数域**.

3.2 p 进数的代数

命题 3.8 (单位) $\mathbb{Z}_p$ 上所有可逆元为常数项不为 0 的元. 精确地说, 对于形式 p 进整数 $x = \sum_{i=0}^{\infty} a_i p^i$,

$$x \text{ 可逆} \iff a_0 \neq 0$$

证明 不难验证 $\Rightarrow$ 方向. 反之, 我们总可以将 x 的逆给解出来, 设 $y = \sum_{i=0}^{\infty} b_i p^i$, 则

$$1 = a_0 b_0 \mod p \qquad 0 = a_1 b_0 p + a_0 b_1 p + a_0 b_0 \mod p^2 \qquad \ldots$$

解总是存在的, 因为 a_0 总是可逆. □

命题 3.9 (元素形式) $\mathbb{Z}_p$ 所有非零元素都可以唯一地写成 $p^n u$ 的形式, 其中 $n \in \mathbb{Z}_{\geq 0}$, 而 u 可逆. 从而 $\mathbb{Z}_p$ 是唯一分解整环.

证明 取 $x = \sum_{i=0}^{\infty} a_i p^i$, 取最小的 n 使得 $a_n \neq 0$, 则

$$x = \sum_{i=n}^{\infty} a_i p^i = p^n \underbrace{\left(\sum_{i=0}^{\infty} a_{i+n} p^i \right)}_{\in \text{unit } \mathbb{Z}_p}$$

于是存在性已经完成. 唯一性是一样的. □

推论 3.10 (元素形式) $\mathbb{Q}_p$ 所有非零元素都可以唯一地写成 $p^n u$ 的形式, 其中 $n \in \mathbb{Z}$, 而 u 在 $\mathbb{Z}_p$ 中可逆.

推论 3.11 从而, 每一个 $x \in \mathbb{Q}_p$ 都可以写成 $x = \sum_{i=-m}^{\infty} a_i p^i$, 即有有限负项的形式 p 进数.

回忆离散赋值环的定义 (C.23).

定义 3.12 (p-进赋值) 在 $\mathbb{Q}_p$ 上存在 p 进赋值,

$$\operatorname{ord}_p : \mathbb{Q}_p \setminus 0 \longrightarrow \mathbb{Z} \qquad \sum_{i=k}^{\infty} a_i p^i \longmapsto k \qquad k \in \mathbb{Z}, a_k \neq 0$$

根据上面的刻画,

- 对应的离散赋值环显然就是 $\mathbb{Z}_p$.
- 对应唯一的极大理想就是 $\{x \in \mathbb{Z}_p : \operatorname{ord}_p x \geq 1\} = p\mathbb{Z}_p$.
- 对应的单位就是 $\mathbb{Z}_p \setminus p\mathbb{Z}_p$.

命题 3.13 有如下同构

$$\varphi : \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}_p/p^n\mathbb{Z}_p \qquad x \bmod p^n \longmapsto x \bmod p^n$$

其逆为

$$\psi : \mathbb{Z}_p/p\mathbb{Z}_p^n \xrightarrow{\sim} \mathbb{Z}/p^n\mathbb{Z} \qquad \sum_{i=0}^{\infty} a_i p^i \bmod p \longmapsto \sum_{i=0}^{n-1} a_i p^i \bmod p$$

3.3 p 进数的初等分析

定义 3.14 回忆 p 进赋值 ord_p*(3.12)*, 可以在 $\mathbb{Q}_p$ 中定义一个绝对值, 进而诱导了一个度量

$$|x| = \frac{1}{p^{\mathrm{ord}_p(x)}} \qquad \rho(x,y) = |x-y| = \frac{1}{p^{\mathrm{ord}_p(x-y)}}$$

容易验证作为绝对值有

(1) $|a| \geq 0$, 且 $|a| = 0 \iff a = 0$. *(正定性)*

(2) $|ab| = |a| \cdot |b|$. *(乘法同态)*

(3) $|a+b| \leq \max(|a|, |b|) \leq |a| + |b|$. *(强三角不等式)*

作为度量有

(1) $\rho(x,y) \geq 0$, 且 $\rho(x,y) = 0 \iff x = y$. *(正定性)*

(2) $\rho(x,y) = \rho(y,x)$. *(对称性)*

(3) $\rho(x,z) \leq \max(\rho(x,y), \rho(y,z)) \leq \rho(x,y) + \rho(y,z)$. *(强三角不等式)*

例 3.15 在 2 进绝对值下, $|6| = \frac{1}{2}, |24| = \frac{1}{8}, |1/24| = 8$.

定义 3.16 (收敛, Cauchy) 在 $\mathbb{Q}_p$ 中, 对于一个序列 $\{x_n\}_{n=1}^{\infty} \subseteq \mathbb{Q}_p$, $x \in \mathbb{Q}_p$,

- 若
$$\forall \epsilon > 0, \exists N > 0, \forall n > N, \rho(x_n, x) < \epsilon$$
则称 x_n **收敛** 于 x, 记为 $x_n \to x$.
- 如果
$$\forall \epsilon > 0, \exists N > 0, \forall m, n > N, \rho(x_n, x_m) < \epsilon$$
则称 x_n **Cauchy**.

直观地说, 在 $\mathbb{Q}_p$ 来看, 两个数 x, y 接近指的是 $\rho(x,y)$ 小, $\mathrm{ord}_p(x-y)$ 大, 指的是 x, y 的截断相同的多. 而收敛实际上说明部分和逐步变为常数.

例 3.17 例如, $p^n \to 0$. 更一般地, 对于任何 p 进整数 x_n, $p^n x_n \to 0$.

命题 3.18 (Hausdorff 性质) 在 $\mathbb{Q}_p$ 中, 对于一个序列 $\{x_n\}_{n=1}^{\infty} \subseteq \mathbb{Q}_p$, 若 $x_n \to x, x_n \to y$, 则 $x = y$.

证明 这是因为假如 $x \neq y$, 则取 $\epsilon = \rho(x, y) > 0$, 此时 $n \gg 0$ 时,

$$\rho(x_n, x) < \epsilon \qquad \rho(x_n, y) < \epsilon$$

从而 $\rho(x, y) \leq \max(\rho(x_n, x), \rho(x_n, y)) < \epsilon$, 矛盾. □

命题 3.19 (完备性) 在 $\mathbb{Q}_p$ 中, 对于一个序列 $\{x_n\}_{n=1}^{\infty} \subseteq \mathbb{Q}_p$, 则

$$\{x_n\} Cauchy \iff \text{存在 } x \in \mathbb{Q}_p, \text{使得 } x_n \to x$$

证明 首先, 充分性, 对于 $\epsilon > 0$, 当 $n \gg 0$ 时, $\rho(x_n, x) < \epsilon$, 从而

$$\rho(x_n, x_m) \leq \max(\rho(x_n, x), \rho(x_m, x)) < \epsilon$$

从而 Cauchy. 反之, 假设

$$x_n = \sum_{i=-\infty}^{\infty} a_i^{(n)} p^i$$

其中所有负项均有限. 这时, 注意到 $\rho(x_n, x_m)$ 充分小指的是 $\nu(x_n - x_m)$ 充分大, 即 $x_n - x_m$ 重合的项目越多. 具体来说, Cauchy 指的是

$$\forall k > -\infty, \exists N > 0, \forall m, n > N, i \leq k, \qquad a_i^{(n)} = a_i^{(m)}$$

这也就意味着对每个 k, $n \gg 0$ 时, $a_k^{(n)}$ 为一个常数, 设这个常数为 a_k, 容易知道 $k \ll 0$ 时 $a_k = 0$, 故这定义了一个 p 进数 $x = \sum_{i=-\infty}^{\infty} a_i p^i$. 容易根据 Cauchy 验证, $x_n \to x$. □

命题 3.20 (局部列紧性) 在 $\mathbb{Q}_p$ 中, 任何一个有界[1] 无限子集 X 都有收敛的序列.

[1] 即存在 M, 使得这个集合中的元素 x 都满足 $|x| < M$

证明 将 X 中所有元素都写成形式 p 进数. 首先, 根据有界性, 我们存在 k 使得

$$\forall \sum_{i=-\infty}^{\infty} a_i p^i \in X, \qquad i \leq k, \qquad a_i = 0$$

此时 p^k 前系数因为只有 p 种选择, 从而至少有一 $b_k \in \{0, \dots, p-1\}$ 使得

$$\underbrace{\#\left\{ \sum_{i=-\infty}^{\infty} a_i p^i \in A : a_k = b_k \right\}}_{:=B_k} = \infty$$

此时 p^{k+1} 前系数因为也只有 p 种选择, 从而至少有一 $b_{k+1} \in \{0, \dots, p-1\}$ 使得

$$\underbrace{\#\left\{ \sum_{i=-\infty}^{\infty} a_i p^i \in A : a_{k+1} = b_{k+1} \right\}}_{:=B_{k+1}} = \infty$$

以此类推, 得到 $\{a_i\}_{i=k}^{\infty}$, 以及 $B_k \supseteq B_{k+1} \supseteq \dots$. 任意从 B_{k+n} 中选元素 x_n, 则

$$x_n \to \sum_{i=k}^{\infty} a_i p^i$$

这样便证明了列紧性. □

命题 3.21 $\mathbb{Z}$ 在 $\mathbb{Z}_p$ 中是稠密的. $\mathbb{Q}$ 在 $\mathbb{Q}_p$ 中是稠密的.

证明 任意 $x \in \mathbb{Z}_p$, 部分和就收敛到 x. $\mathbb{Q}_p$ 是同理的. □

命题 3.22 在 $\mathbb{Q}_p$ 中,

$$x_n \to x, y_n \to y \qquad x_n + y_n \to x + y, x_n y_n \to xy$$

从而加法和乘法是连续的.

证明 这是分析的惯常

$$|(x_n + y_n) - (x + y)| \leq \max(|x_n - x|, |y_n - y|)$$

以及

$$|x_n y_n - xy| \leq \max(|(x_n - x)(y_n - y)|, |x_n - x| \cdot |y|, |x| \cdot |y_n - y|)$$

容易得证. □

以上都是和实数 $\mathbb{R}$ 上分析的相似之处. 下面我们会看到强三角不等式的非 Archimedes 性和 Archimedes 性的本质不同. 在实数中存在 $\sum a_n \to \infty$ 但是 $a_n \to 0$ 的序列, 例如 $\frac{1}{n}$, 而强三角不等式保证了在 $\mathbb{Q}_p$ 中不会发生这样的事.

命题 3.23 (级数收敛准则) *对于一个序列 $\{x_n\}_{n=1}^{\infty} \subseteq \mathbb{Q}_p$, 若*

$$\sum_{i=1}^{n} x_i \text{ 收敛到某一个元} \iff x_n \to 0$$

证明 若 $\sum_{i=1}^{n} x_i \to x$, 则

$$x_n = \sum_{i=1}^{n} x_i - \sum_{i=1}^{n-1} x_i \to x - x \to 0$$

反之, 利用完备性论证, 对于 $\epsilon > 0$, 取 N 使得 $n > N$ 时 $\rho(x_n, 0) < \epsilon$, 则对于 $n > m > N$,

$$\left| \sum_{i=m}^{n} x_i \right| < \max(|x_m|, \ldots, |x_n|) < \epsilon$$

故 $\sum_{i=1}^{n} x_i$ 是 Cauchy 列. □

推论 3.24 *序列 $\{x_n\}_{n=1}^{\infty} \subseteq \mathbb{Q}_p$, 其是 Cauchy 的当且仅当 $x_n - x_{n-1} \to 0$.*

至此, p 进数不再是形式的, 其连加号是有收敛含义的.

3.4 整体 -局部原理

命题 3.25 *对于素数 p, 整系数多项式 f, 则*

$$f(x) \equiv 0 \mod p^n$$

对任意 n 都有解的充分必要条件是

$$f(x) = 0$$

在 p 进整数中有解.

证明 首先, 充分性是显然的. 下面证明必要性. 设解集

$$E_n = \{x \in \mathbb{Z} : f(x) \equiv 0 \mod p^n\}$$

则显然 E_n 是无限集, 我们的目标是要说明存在抽出一列数组能够使得其成为 p 进数. 具体来说, 由于 E_1 是无穷的, 必然有 y_1 使得有无穷个

$$x \in E_1, x \equiv y_1 \mod p$$

同样, 在这无穷个解当中, 必然还有 y_2 使得有无穷个

$$x \in E_2, x \equiv y_2 \mod p^2$$

根据解的来源, $y_2 \equiv y_1 \mod p$. 以此类推得到 Cauchy 列 $\{y_n\}$. □

引理 3.26 (Hensel 引理) 对于素数 p, 整系数多项式 f, 如果有整数 x_1 使得

$$f(x_1) \equiv 0 \mod p \qquad f'(x_1) \not\equiv 0 \mod p$$

其中 f' 是 f 的形式导数. 则有 p 进数 x 满足 $f(x) = 0$.

证明 换句话说, 即存在 $\{x_k\}_{k=1}^{\infty}$ 使得

$$f(x_k) \equiv 0 \mod p^k$$

对 f 施加以 Taylor 展开有

$$f(x_1 + a_1 p) = f(x_1) + f'(x_1)a_1 p + rp^2 \equiv f(x_1) + f'(x_1)a_1 p \mod p^2$$

即解 $f(x_1)/p + f'(x_1)a_1 \equiv 0 \mod p$, 可以解出 a_1, 从而

$$x_2 = x_1 + a_1 p \text{使得} f(x_2) \equiv 0 \mod p^2 \qquad f'(x_2) \equiv f'(x_1) \not\equiv 0 \mod p$$

下面, 假设 x_k 已经构造好, 同样运用 Taylor 展开有

$$f(x_k + a_k p^k) = f(x_k) + f'(x_k)a_k p^k + rp^{2k} \equiv f(x_k) + f'(x_k)a_k p^k \mod p^{k+1}$$

即解 $f(x_k)/p^k + f'(x_k)a_k \equiv 0 \mod p$, 可以解出 a_k, 从而

$$x_{k+1} = x_k + a_k p^k \text{使得} f(x_{k+1}) \equiv 0 \mod p^{k+1} \qquad f'(x_{k+1}) \equiv f'(x_k) \not\equiv 0 \mod p$$

命题得证. □

评注 3.27 倘若和欧式空间类比, 上述即著名的牛顿切线法, 如下图

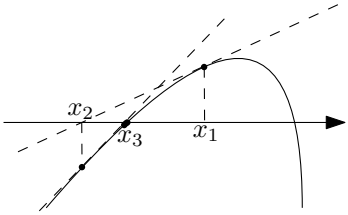


Figure 3.1: 牛顿切线法

注意到, 在 x_1 处的 "切线" 为

$$y - f(x_1) = f'(x_1)(x - x_1)$$

与 "x 轴" 的交点为 $x_2 = x_1 - \frac{f(x_1)}{f'(x_1)} = x_1 - \frac{f(x_1)/p}{f'(x_1)}p$, 其中 $-\frac{f(x_1)/p}{f'(x_1)}$ 正是证明中待定的 a_1. 以此类推.

引理 3.28 (Hensel 引理) 对于素数 p, n 元整系数多项式 f, 如果有整数 $x_1, \ldots, x_n$ 使得

$$f(x_1, \ldots, x_n) \equiv 0 \mod p \qquad \frac{\partial f}{\partial X_i}(x_1, \ldots, x_n) \not\equiv 0 \mod p$$

则有 p 进数 $x_1, \ldots, x_n$ 满足 $f(x_1, \ldots, x_n) = 0$.

证明 归纳易得. □

以上定理可以加强为如下. 对于素数 p, p 进整系数多项式 f, 正整数 n, 如果有整数 x_n 使得

$$f(x_n) \equiv 0 \mod p^n \qquad \mathrm{ord}_p(f'(x_1)) < n/2$$

其中 ν 是 p 进赋值, f' 是 f 的形式导数. 则有 p 进数 x 满足 $f(x) = 0$. 参见 [11] P14 Lemma.

3.5 应用 — Fermat 大定理的失败尝试

回顾 Fermat 大定理 (1.22), 如果我们证明了 Fermat 大定理的方程 $f(X,Y,Z) = X^n + Y^n - Z^n = 0$ 在 $n \geq 2$ 时在 $\mathbb{Z}_p$ 上无解, 那么自动得到 $\mathbb{Z}$ 上无解. 但是相比读者能够理解 —如此经典的故事没有被付诸尝试只能说明数学的研究不过流于灵机一动的脑筋急转弯.

引理 3.29 (Schur) *对于任意的 $n \in \mathbb{N}$, 总存在 $m \in \mathbb{N}$ 使得素数 $p \geq m$ 时,*

$$X^n + X^n \equiv Z^n \mod p$$

总有非平凡解, 即 x, y, z 都不为同余为 0 的解.

证明 Schur 利用了一个他自己证明的引理如下. 对于 $n \geq \mathrm{e}r!$, 函数

$$\varphi : \{1, \ldots, n\} \to \{1, \ldots, r\}$$

都存在 $x, y, z \in \{1, \ldots, n\}$ 使得 $x + y = z$ 且 $\varphi(x) = \varphi(y) = \varphi(z)$. 即被染色的数足够, 总会选出同一种颜色的数填进 $\square + \square = \square$"空格" 使得等号成立.

否则, 任何满足 $\varphi(x) = \varphi(y)$ 的 x, y 都有 $\varphi(x) \neq \varphi(x + y)$.

考虑 $B = \{1, \ldots, r\}$ 中原像元素最多的元素, 设为 r_1, 设原像为 $x_{11} < x_{12} < \ldots < x_{1n_1}$, 则根据鸽笼原理

$$n \leq rn_1$$

再考虑集合 $A_1 = \{x_{12} - x_{11}, \ldots, x_{1n_1} - x_{11}\}$, 则根据假设, $\forall y \in A_1, \varphi(y) \neq r_1$, 再设 $B \setminus \{r_1\}$ 中在 A_1 中原像最多的元素为 r_2, 设原像为 $x_{21} < x_{22} < \ldots < x_{2n_2}$, 则根据鸽笼原理

$$n_1 - 1 \leq (r-1)n_2$$

再考虑集合 $A_2 = \{x_{22} - x_{21}, \ldots, x_{2n_1} - x_{21}\}$ 这样持续下去会得到

$$n \leq \sum_{i=0}^{r-1} r(r-1)\ldots(r-i) = \sum_{i=0}^{r-1} \frac{r!}{i!} < \mathrm{e}r!$$

与假设矛盾!

而这个定理的证明, 需要取原根 $g \in \mathbb{F}_p^*$, 则 $\mathbb{F}_p \setminus \{0\} = \{g, \ldots, g^{p-1}\}$, 固定一种表法, 定义

$$\varphi : \mathbb{F}_p \setminus \{0\} \longrightarrow \mathbb{Z}_n \qquad g^i \longmapsto i \mod n$$

则根据引理, 当 p 充分大时, 有

$$g^{i_1+j_1 n} + g^{i_1+j_2 n} = g^{i_1+j_3 n} \iff (g^{j_1})^n + (g^{j_2})^n = (g^{j_3})^n$$

$x = g^{j_1}, y = g^{j_2}, z = g^{j_3}$ 就是一组非平凡解. □

以上证明选自 [6] P63, 原始论文是 [10].

命题 3.30 *对于任意的 $n \in \mathbb{N}$, 总存在 $m \in \mathbb{N}$ 使得素数 $p \geq m$ 时, 方程*

$$X^n + X^n \equiv Z^n \mod p$$

总在 $\mathbb{Z}_p$ 上有解.

证明 利用 (3.28) 以及上面的引理 (3.29). □

以上结果并未将从这个角度杀死 Fermat 大定理的所有可能性杀死, 但是说明对于固定的指数 n, 仅仅只有有限的素数可供检验.

Chapter 4

赋值理论

4.1 赋值域的性质

I. 赋值与绝对值

定义 4.1 (绝对值) 对于域 K, 称 $|\cdot|: K \to \mathbb{R}$ 为 **绝对值**, 如果

- $\forall x \in K, |x| \geq 0$, 且取到等号当且仅当 $x = 0$. *(正定性)*
- $\forall x, y \in K, |xy| = |x| \cdot |y|$. *(乘法同态)*
- $\forall x, y \in K, |x + y| \leq |x| + |y|$. *(三角不等式)*

称为 **非 Archimedes 绝对值**, 如果三角不等式可以被加强为

- $\forall x, y \in K, |x + y| \leq \max\{|x|, |y|\}$. *(强三角不等式)*

显然, 通过定义距离 $\rho(x, y) = |x - y|$, 这构成一个距离空间.

命题 4.2 对于域 K 上的绝对值 $|\cdot|, |\cdot|$ 是非 *Archimedes* 绝对值的当且仅当 $\{|n1| : n \in \mathbb{Z}\}$ 是有界的.

证明 首先, 如果非 Archimedes, 则

$$|n1| = |1 + 1 + \ldots + 1| \leq \max |1|, |1|, \ldots, |1| = |1|$$

反之, 假设 $|n1| < N$, 则

$$|x+y|^n = \left|\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}\right| \le \sum N|x|^i|y|^{n-i} \le Nn\big[\max(|x|,|y|)\big]^n$$

故 $|x+y| \le N^{1/n} n^{1/n} \max(|x|,|y|)$, 因为 n 是任意的, 取极限即得. □

回忆 (C.23) 对离散赋值的定义.

评注 4.3 (赋值) 对于域 K, 如果存在一个映射 $\nu : K \longrightarrow \mathbb{R} \sqcup \{\infty\}$, 满足

(1) $\nu(0) = \infty$

(2) $\nu(xy) = \nu(x) + \nu(y)$

(3) $\nu(x+y) \ge \min(\nu(x), \nu(y))$

其中关于 ∞ 的运算约定俗成. 此时称 ν 为一个**赋值 (valuation)**.

当然赋值可以定义得更为抽象, 这被称为 Krull 赋值, 参见 [2]§10.2.

约定 4.4 以后我们不再要求离散赋值的值域是 $\mathbb{Z} \sqcup \{\infty\}$, 而是改为是 $\mathbb{R}$ 的离散子群 $\sqcup\{\infty\}$, 他们一定形如 $\frac{1}{r}\mathbb{Z} \sqcup \{\infty\}$.

推论 4.5 容易验证, *(C.23)* 的性质依旧成立, $\nu(-1) = 0$, $\nu(x) = \nu(-x)$, $\nu(x) \ne \nu(y)$, 则 *(3)* 取到等号, 这被俗称为 "**木桶原理**"[1]. 更一般地, $x + y + \ldots + z = 0$, 则必有两个元素 $\in \{x, y, \ldots, z\}$ 取到 ν 在其上的最小值. 以及

- $A = \{x \in K : \nu(x) \ge 0\}$ 是一个环. 这被称为**赋值环**.
- $\mathfrak{m} = \{x \in K : \nu(x) > 0\}$ 是 A 的极大理想.
- $A \setminus \mathfrak{m} = \{x \in K : \nu(x) = 0\}$ 是 A 的单位.

从而 A 是以 $\mathfrak{m}$ 为极大理想的局部环, 即只有一个极大理想的环, 参见 *(C.9)*.

[1]其实 (3) 意味着任何 "三角形" 都是等腰的, 具体来说, 否则, 例如 $\nu(x) < \nu(y)$, 考虑 $\nu(y) = \nu(x+y-x) \ge \min(\nu(x+y), \nu(x)) = \nu(x)$, 矛盾.

例 4.6 回忆 *(3.14)*, 当中对 $\mathbb{Z}_p$ 定义的 $|\cdot|$ 是一个绝对值.

一般地, 任何一个域上的赋值都可以对应到一个范数

$$|x| := \frac{1}{e^{\nu(x)}}$$

其中 e 是任意预先选择好的大于 1 的常数. 反之, 任何非 *Archimedes* 绝对值 $|\cdot|$ 都对应一个赋值通过 $\nu(x) := -\log|x|$.

显然, 上述 e 的选取本质上不影响拓扑结构, 下面我们来说明这是唯一可能发生的情况.

命题 4.7 令 K 是一个域, 其上有两个绝对值 $|\cdot|_1, |\cdot|_2$, 则下列命题是等价的,

(1) $|\cdot|_1, |\cdot|_2$ 诱导了相同拓扑.

(2) $|x|_1 < 1 \iff |x|_2 < 1$.

(3) 存在 $a > 0$ 使得 $|x|_2 = |x|_1^a$.

证明 (1)⇒(2) 只需要注意到 $|x|_{1,2} < 1 \iff x^n \to 0$.

(2)⇒(3), 我们希望证明 $\frac{\log|x|_2}{\log|x|_1}$ 是与 x 无关的常数. 显然, 如果 $|\cdot|_1$ 在 $K \setminus 0$ 上恒取 1, 则 $|\cdot|_2$ 根据条件亦然, 自然 (3) 满足. 否则, 存在 $y \in K$ 使得 $|y|_1 > 1$, 令 $a = \frac{\log|y|_2}{\log|y|_1}$. 任意 $x \in K \setminus 0$, 取 $b > 0$ 使得 $|x|_1 = |y|_1^b$, 我们希望证明 $|x|_2 = |y|_2^b$. 考虑用有理数逼近 b, 选取有理数 $m/n > b$, 则

$$|x|_1 < |y|_1^{m/n} \iff |x|_1^n < |y|_1^m \iff |x^n/y^m|_1 < 1$$

逆向再推回去得到 $|x|_2 < |y|_2^{m/n}$, 因为有理数稠密, 所以 $|x|_2 \le |y|_2^b$. 再取 $p/q < b$, 类似可以得到 $|y|_2^b \le |x|_2$, 这样就完成了证明.

(3)⇒(1), 显然. □

推论 4.8 令 K 是一个域, 其上有两个赋值 μ, ν, 其诱导相同的拓扑当且仅当存在 $a > 0$ 使得 $\mu = a\nu$.

II. 置放 我们的一大目标是将下面定义的置放类比之前 Dedekind 整环的素理想.

定义 4.9 (置放) 令 K 是一个域, 称 **置放 (place)** 是绝对值的等价类.

我们总是排除 $K \setminus 0 \mapsto 0$ 的绝对值.

定理 4.10 (Artin-Whaples 逼近定理) 令 K 是一个域, $|\cdot|_1, \ldots, |\cdot|_n$ 是互不同构的绝对值, 令 $x_1, \ldots, x_n \in K$, $\epsilon > 0$, 存在 $x \in K$ 使得

$$|x - x_i| < \epsilon \qquad i = 1, \ldots, n$$

证明 我们寄希望于找 $z \in K$ 使得 $|z|_1 > 1$, 而 $2 \leq i \leq n$ 时 $|z|_i < 1$. 从 $n = 2$ 时开始归纳, 存在 $x, y \in K$ 使得

$$|x|_1 < 1 \quad |x|_2 \geq 1 \qquad |y|_2 < 1 \quad |y|_1 \geq 1$$

则 $z = y/x$ 使得 $|z|_1 > 1, |z|_2 < 1$. 根据归纳以及 $n = 2$ 的情况, 存在 x, y 使得

$$\begin{array}{llllll} |x|_1 > 1 & |x|_2 < 1 & \ldots & |x|_{n-1} < 1 & * \\ |y|_1 > 1 & & & & |y|_n < 1 \end{array}$$

如果 $|x|_n \leq 1$, 则 $x^m y$ 在 m 充分大时即可满足, 否则 $|x|_n > 1$, $\frac{x^m}{1+x^m}$ 在 $|\cdot|_{1,n}$ 意义下趋向于 1, 在 $|\cdot|_{2,\ldots,n-1}$ 意义下趋向于 0, 故 $\frac{x^m}{1+x^m} y$ 在 m 充分大时满足条件.

如果找到了这样的 z, 此时 $\frac{z^m}{1+z^m}$ 在 $|\cdot|_1$ 意义下趋向于 1, 在 $|\cdot|_{2,\ldots,n}$ 意义下趋向于 0, 如法炮制 z_i, 使得

$$z_i(m) \xrightarrow{|\cdot|_j} \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

这样, $x = z_1(m)x_1 + \ldots + z_n(m)x_n$ 在 m 充分大时就满足条件. □

实际上这可以类比中国剩余定理 (2.14).

定理 4.11 (Ostrowski) 有理数域 $\mathbb{Q}$ 上的所有放置就是通常的绝对值和 p 进赋值.

证明 如果是非 Archimedes 的, 那么对应一个赋值 ν, 对应赋值环 A 与 $\mathbb{Z}$ 的交必是一个非零素理想 (因为非平凡), 设对应的素数是 p, 此时任何和 p 互质的 n, 则 n 必定 A 中单位, 即 $\nu(n)=0$, 通过调整一个常数倍, 实际上这就是 p 进赋值.

如果是 Archimedes 的, 假设绝对值是 $|\cdot|$, 对于任意 m,n, 假设将 m 展成 n 进制是 $m=a_kn^k+\dots a_0$, 那么

$$k\leq\frac{\log m}{\log n}\qquad |a_i|\leq|a_i\cdot 1|=a_i<n$$

而三角不等式蕴含

$$|m|\leq\sum_{i=0}^{k}|a_i|\cdot|n|^i\leq\sum_{i=0}^{k}n|n|^i$$

这说明 $|n|\geq 1$, 否则, $|m|\leq\frac{n}{1-|n|}$ 恒有界 (4.2), 与 Archimedes 矛盾. 从而

$$|m|\leq(1+k)n|n|^k\leq\left(1+\frac{\log m}{\log n}\right)\cdot n\cdot|n|^{\frac{\log m}{\log n}}$$

改 $m=m^t$, 其中 $t\in\mathbb{Z}_{\geq 1}$, 则

$$|m|\leq\sqrt[t]{\left(1+t\frac{\log m}{\log n}\right)\cdot n\cdot|n|^{t\frac{\log m}{\log n}}}\to|n|^{\frac{\log m}{\log n}}$$

故 $|m|^{\frac{1}{\log m}}\leq|n|^{\frac{1}{\log n}}$, 对称地, 他们是相等的. 令常数 $\mathrm{e}^s=|n|^{\frac{1}{\log n}}$, 这样 $|n|=\mathrm{e}^{s\log n}=|n|^s$. □

III. 完备化 任何一个度量空间都可以进行完备化, 参见 [1]P135 习题 6.33. 这样如果一个域 K 上有绝对值 $|\cdot|$, 可以按该绝对值诱导的度量空间进行完备化 $\hat{K}$, 不难验证的是此时 $\hat{K}$ 还是一个域, 且 $|\cdot|$ 得以自然地延拓. 对于赋值也是类似的.

我们希望证明, $\mathbb{Q}$ 关于 p 进赋值 ord_p 的完备化就是 p 进数域 $\mathbb{Q}_p$.

一般地我们考虑离散赋值.

引理 4.12 对于域 K, 赋值 ν, 其完备化记为 $\hat{K}$, 则其赋值仍然为离散赋值, 继续记为 ν, 假如对应的离散赋值环和极大理想分别为

$$A = \{x \in K : \nu(x) \geq 0\} \quad \mathfrak{m} = \{x \in K : \nu(x) \geq 1\}$$
$$\hat{A} = \{x \in \hat{K} : \nu(x) \geq 0\} \quad \hat{\mathfrak{m}} = \{x \in \hat{K} : \nu(x) \geq 1\}$$

则有同构

$$\varphi : A/\mathfrak{m}^n \xrightarrow{\sim} \hat{A}/\hat{\mathfrak{m}}^n \qquad a \bmod \mathfrak{m}^n \longmapsto a \bmod \mathfrak{m}^n$$

证明 注意到 $\hat{K}$ 是一些 Cauchy 组成的, 从而 μ 的值域应该是原本值域的闭包, 但是离散时取闭包是不变的. 对于同构的论断, 首先, 显然 $\mathfrak{m}^n = A \cap \hat{\mathfrak{m}}^n$, 故是单射. 而 $A \subseteq \hat{A}$ 是稠密的, $\hat{\mathfrak{m}}^n$ 是一个开集, 从而任何 $x \in \hat{A}$, $x + \hat{\mathfrak{m}}^n$ 总能交到一个 A 中的元素. □

命题 4.13 记号承上, 假如 $S \subseteq A$ 是 $A/\mathfrak{m}$ 的代表元, π 生成了 $\mathfrak{m}$, 则任何 $x \in \hat{K} \setminus 0$ 都可以唯一地写成

$$\sum_{i=m}^{\infty} a_i \pi^i \qquad a_i \in S \quad a_m \not\equiv 0 \mod \mathfrak{m}$$

且 $\nu(x) = m$.

证明 显然, 上述级数的部分和是 Cauchy 列. 首先, 根据 (C.25), 我们只需要说明单位具有此特性. 取一个单位 $u \in A$, 根据引理 (4.12) 存在 s_0 使得 $\nu(u - s_0) \geq 1$, 这样, 考虑单位 $\frac{y - s_0}{\pi}$, 一直继续下去会得到

$$\nu\left(\frac{y - s_0 - s_1\pi - \ldots - s_n\pi^n}{\pi^{n+1}}\right) \geq 1$$

故

$$|y - s_0 - s_1\pi - \ldots - s_n\pi^n| \to 0$$

从而 y 可以写成命题中的级数. 关于唯一性只需要说明 0 的表法是唯一的, 根据赋值这是一定的. □

也就是说这和我们构造的 p 进数域不谋而合, 故 $\mathbb{Q}$ 对 ord_p 的完备化就是 $\mathbb{Q}_p$.

如果一个域的绝对值不是非 Archimedes 的, 则称为 Archimedes 域. 下面这个惊人的事实是完备的 Archimedes 域都 (代数和拓扑意义下) 同构于 $\mathbb{R}$ 和 $\mathbb{C}$. 这就意味着我们讨论完备域时, 总可以单独在 $\mathbb{R},\mathbb{C}$ 上验证完毕, 进而假设绝对值来自赋值.

定理 4.14 (Ostrowski) *完备的 Archimedes 域只有 $\mathbb{R}$ 和 $\mathbb{C}$.*

证明 令域 K, 显然, Archimedes 蕴含特征为 0, 从而 $\mathbb{Q}\subseteq K$, 根据 K 完备, $\mathbb{R}\subseteq K$. 我们要证明任何 $x\in K$ 都是二次多项式 $Q_x\in\mathbb{R}[X]$ 的根. 这样就足以说明 $K=\mathbb{R}$ 或 $\mathbb{C}$. 固定 $x\in K$, 考虑连续函数

$$f:\mathbb{C}\longrightarrow\mathbb{R}_{\geq 0}\qquad z\longmapsto|x^2-(z+\overline{z})x+z\overline{z}|$$

仅需证明 f 有零点. 注意到 f 取得极小值 m, 取 $w=f^{-1}(m)$ 使得 $|w|$ 最大. 我们只需要说明 $m=0$. 假如 $m>0$, 选择充分小的 $\epsilon>0$, 此时计算判别式 $g(X)=X^2-(w+\overline{w})X+w\overline{w}+\epsilon$ 会发现具有一对复根 $\alpha,\overline{\alpha}$, 此时 $\alpha+\overline{\alpha}=w\overline{w}+\epsilon$, 故 $|\alpha|>|w|$, 故 $f(\alpha)>m$. 考虑

$$G(X)=(g(X)-\epsilon)^n-(-\epsilon)^n\in\mathbb{R}[X]$$

令其根为 $\alpha=\alpha_1,\ldots,\alpha_{2n}\in\mathbb{C}$, 则

$$\begin{aligned}|G(x)|^2&=|G(x)^2|=\left|\prod_{i=1}^{2n}(x-\alpha_i)(x-\overline{\alpha_i})\right|\\&=\left|\prod_{i=1}^{2n}(x^2-(\alpha_i+\overline{\alpha_i})x-\alpha_i\overline{\alpha_i})\right|\\&=\prod_{i=1}^{2n}f(\alpha_i)\geq f(\alpha)m^{2n-1}\end{aligned}$$

另一方面

$$\begin{aligned}|G(x)|&\leq|x^2-(w+\overline{w})+w\overline{w}|+|\epsilon|^n\\&=f(w)^n+\epsilon^n=m^n+\epsilon^n\end{aligned}$$

故

$$\sqrt{\frac{f(\alpha)}{m}}\leq 1+\left(\frac{\epsilon}{m}\right)^n$$

令 $n\to\infty$, 得到 $f(\alpha)\leq m$, 矛盾! □

4.2 赋值域的方程

I. Hensel 引理

命题 4.15 (Hensel 引理) 对于完备的离散赋值环[2] A, 假设 $\mathfrak{m}$ 是唯一的极大理想, 如果多项式 $f \in A[X]$ 在 $A/\mathfrak{m}$ 上有单根, 则 f 在 A 上有根.

证明 取 $\mathfrak{m}$ 的生成元 π, 证明同 (3.26). □

命题 4.16 (Hensel 引理) 对于完备的离散赋值环 A, 假设 $\mathfrak{m}$ 是唯一的极大理想, 假如本原多项式[3] $f(X) \in A[X]$ 在 $A/\mathfrak{m}[X]$ 上有分解

$$f(X) \equiv g_0(X)h_0(X) \mod \mathfrak{m}$$

假如 g_0, h_0 在 $k[X]$ 中互素, 且 g_0 首一, 则存在 $g, h \in A[X]$ 使得

$$f(X) = g(X)h(X) \qquad g(X) \equiv g_0(X) \mod \mathfrak{m} \quad h(X) \equiv h_0(X) \mod \mathfrak{m}$$

且 g 首一, $\deg g = \deg(g \bmod \mathfrak{m})$.

证明 取 $\mathfrak{m}$ 的生成元 π, 不放假设 g_0 首一,

$$\deg g_0 = \deg(g_0 \bmod \mathfrak{m}) \qquad \deg h_0 = \deg(h_0 \bmod \mathfrak{m})$$

我们实际上要找多项式

$$\begin{aligned} g(X) &= g_0(X) + p_1(X)\pi + p_2(X)\pi^2 + \dots \\ h(X) &= h_0(X) + q_1(X)\pi + q_2(X)\pi^2 + \dots \end{aligned}$$

我们记部分和

$$g_n(X) = g_0(X) + \sum_{i=1}^{n} p_i(X) \qquad h_n(X) = h_0(X) + \sum_{i=1}^{n} q_i(X)$$

为了使得上面的构造真的是一个多项式, 需要对次数提一些要求, 再加上命题要求的条件, 需要

[2] 即, 完备离散赋值域对应的离散赋值环, 因为对应的离散赋值环是闭集, 所以还是完备的.
[3] 即系数的最大公约数是 1, 这里就是说系数赋值的最小值是 0.

- $\deg g_n \le \deg g_0$, 这样才能保证 g 是一个多项式.
- $p_n < \deg g_0$, 这样才能保证 g 首一.
- $\deg h_n \le \deg h_0 = \deg f - \deg g_0$, 这样才能保证 $f = gh$.
- $q_n \le \deg h_0 = \deg f - \deg g_0$.

我们希望做到

$$f \equiv g_n h_n \mod \mathfrak{m}^{n+1}$$

假设已经构造好了 g_{n-1}, h_{n-1} 使得 $f \equiv g_{n-1}h_{n-1} \bmod \mathfrak{m}^n$. 假如已经有 $f \equiv g_{n-1}h_{n-1} \bmod \mathfrak{m}^{n+1}$, 取 $g_n = g_{n-1}, h_n = h_{n-1}$ 即可. 如若不然, 为了满足

$$f \equiv g_n h_n \equiv (g_{n-1} + p_n\pi^n)(h_{n-1} + q_n\pi^n) \mod \mathfrak{m}^{n+1}$$

的要求, 则

$$\frac{f - g_{n-1}h_{n-1}}{\pi^n} \equiv g_{n-1}q_n + h_{n-1}p_n \equiv g_0q_n + h_0p_n \mod \mathfrak{m}$$

因为 p_n, q_n 在 mod$\mathfrak{m}$ 下互质, 故总可以找到 $a, b \in A[X]$ 使得 $bg_0 + ah_0 \equiv 1 \bmod \mathfrak{m}$, 我们希望取 $p_n = a\frac{f-g_{n-1}h_{n-1}}{\pi^n}, q_n = b\frac{f-g_{n-1}h_{n-1}}{\pi^n}$, 不过此时次数无法控制, 注意到

$$g_0q_n + h_0p_n \equiv g_0(q_n + rg_0) + h_0(p_n - rg_0) \mod \mathfrak{m}$$

因为 g_0 首一, 可以挑选恰当的 r, 就可以用 $p_n - rg_0$ 代替 p_n 使得 $\deg p_n < \deg g_0$. 而注意到

$$\underbrace{\frac{f - g_{n-1}h_{n-1}}{\pi^n}}_{\deg * \le \deg f} \equiv g_0q_n + \underbrace{h_0p_n}_{\deg * < \deg h_0 + \deg g_0} \mod \mathfrak{m}$$

从而 $\deg q_n \le \deg h_0 = \deg f - \deg g_0$. □

推论 4.17 *对于完备的离散赋值环 A, 假设 $\mathfrak{m}$ 是唯一的极大理想, 首一的 $f \in A[X]$ 是不可约的, 则在 $A/\mathfrak{m}[X]$ 之中 f 是不可约多项式的方幂.*

推论 4.18 对于完备的离散赋值域 K, 若 $f(X)=\sum_{i=0}^{n}a_iX^i\in K[X]$ 是不可约的, 那么赋值的最小值在首项和常数项上取到, 换言之,

$$\min\{\nu(a_0),\dots,\nu(a_n)\}=\min\{\nu(a_0),\nu(a_n)\}$$

特别地, 如果 $a_0,a_n\in A$, 则 $f(X)\in A[X]$.

证明 假设对应的离散赋值环是 A, 唯一的极大理想是 $\mathfrak{m}$. 通过乘以一个恰当的数, 可以假定 $f(X)\in A[X]$, 且各系数赋值的最小值为 0, 即本原多项式. 假设 $\nu(a_r)=0$, 且 r 被选得尽可能小, 此时

$$f(X)=X^r(a_nX^{n-r}+\dots+a_r)\mod\mathfrak{m}$$

为了不破坏 $f(X)$ 的不可约性, 要求 X^r 或 $(a_nX^{n-r}+\dots+a_r)$ 是常数, 那么要么 $r=0$, 要么 $n=r$, 要么至少 $a_n\equiv 0\bmod\mathfrak{m}$, 这都说明 $\min\{\nu(a_0),\nu(a_n)\}=0$. □

II. Newton 折线

定义 4.19 (Newton 折线) 考虑赋值域 K, 记其赋值为 ν, 考虑多项式 $f(X)=\sum_{i=0}^{n}a_iX^i\in K[X]$, 定义其 **Newton 折线** 为点集

$$\Big\{\big(i,\nu(a_i)\big):i=0,\dots,n\Big\}\subseteq\mathbb{Z}\times(\mathbb{R}\sqcup\{\infty\})$$

的下凸包[4].

注意到 Newton 折线的斜率总是递增的.

定理 4.20 考虑赋值域 K, 记其赋值为 ν, 如果多项式 $f(X)\in K[X]$ 在 K 上有所有根 [5], 那么

$$\#\left\{\begin{array}{l}\nu(x)=s:\\ x\text{ 是 }f(X)\text{ 的根}\end{array}\right\}=\begin{array}{l}\textit{Newton 折线中斜率}\\ \textit{为 } s \textit{ 线段的横向长度}\end{array}\qquad(\textit{按重数计算})$$

[4]即选择一些点从左向右用线段连接起来, 使得所有点都在这些线的上方.

[5]后面我们会看到, 如果在完备域上, 赋值可以唯一地延拓, 那么总可以在更大的域上考虑, 而不必顾忌所有跟在 K 上的要求, 见 (4.22).

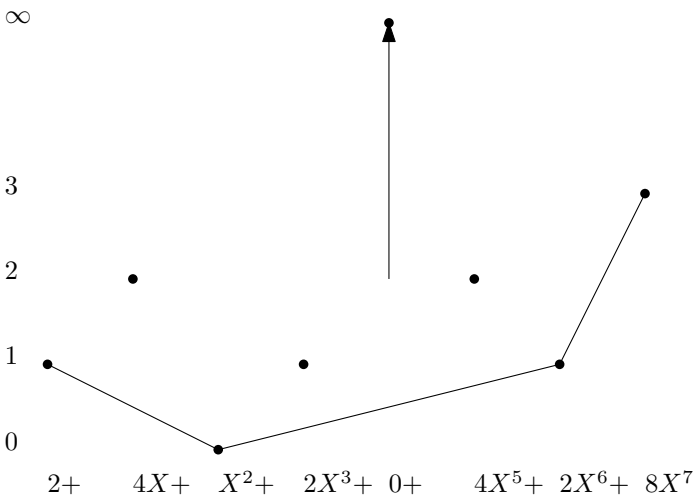


Figure 4.1: Newton 折线

证明 实际上这本质上是 Vieta 定理的计算, 首先不放调整 f 的首项系数为 1, 这对应 Newton 折线的下移, 不影响结果, 假设所有根是 $x_1, \ldots, x_n$, 那么

$$f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \qquad a_k = \pm \sum_{\substack{S \subseteq \{1,\ldots,n\} \\ |S|=k}} \prod_{s \in S} x_s$$

不妨假设 $x_1, \ldots, x_n$ 满足

$$\begin{aligned} \nu(x_1) = \ldots = \nu(x_{t_1}) &:= \quad v_1 \\ &\quad \wedge \\ \nu(x_{t_1+1}) = \ldots = \nu(x_{t_1+t_2}) &:= \quad v_2 \\ &\quad \wedge \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots &\quad \vdots \end{aligned}$$

我们要证明如下 P_k 的连线就是 Newton 折线, 且 P_k-P_{k+1} 的斜率就是 v_k.

$$T_k = t_1 + \ldots + t_k \qquad P_k = (T_k, \nu(a_{T_k}))$$

- 先求出 $\nu(a_{T_k})$, 这样就验证了 P_k-P_{k+1} 的斜率就是 v_k. 注意到取遍所有基数为 T_k 的子集 $S \subseteq \{1, \ldots, n\}$, $\nu\left(\prod_{s \in S} x_s\right)$ 仅在 $\{1, \ldots, T_k\}$ 时取到

最小值. 故根据 “木桶原理”,

$$\nu(a_{T_k}) = \nu\left(\prod_{s=1}^{T_k} x_s\right) = t_1v_1 + \ldots + t_kv_k$$

- 我们证明 $(i, \nu(a_i))$ 都在 P_k-P_{k+1} 连线的上方, 如果 $T_k \leq i \leq T_{k+1}$. 注意到取遍所有基数为 i 的子集 $S \subseteq \{1, \ldots, n\}$, 考虑 $\nu\left(\prod_{s\in S} x_s\right)$ 的最小值, 可得

  $$\nu(a_i) \geq t_1v_1 + \ldots + t_kv_k + (i - T_k)v_{k+1}$$

  实际上, $Y = t_1v_1 + \ldots + t_kv_k + (X - T_k)v_{k+1}$ 就是经过 P_k-P_{k+1} 的直线.

这样命题得证. □

例 4.21 *我们后面会看到, 任意一个完备赋值完美域都可以扩充到其代数闭域上 (4.24)*

4.3 赋值域的扩张

I. 完备赋值域的扩张

定理 4.22 *令 K 是一个完备的离散赋值域, 设其赋值是 ν, L 是一个 n 次有限可分扩张, 那么 L 上有唯一的完备离散赋值[6] μ 使得*

$$\mu|_K = \nu \qquad \mu(x) = \frac{1}{n}\nu(\mathrm{Nm}(x))$$

且假设对应赋值环和极大理想是 $\mathfrak{p} \subseteq A \subseteq K, \mathfrak{P} \subseteq B \subseteq L$, 则 $A \subseteq B$ 是 Dedekind 扩张, $\mathfrak{P} \cap A = \mathfrak{p}$.

证明 完备性是来自积拓扑的自然性质.

令 A 是 K 对应的离散赋值环, B 为 A 在 L 中的整闭包, 考虑 A 唯一的素理想 $\mathfrak{p}$, 根据 Dedekind 整环的定理 (2.28), 存在 B 的素理想 $\mathfrak{P}$ 使得

[6] 此时值域可能不再是 $\mathbb{Z} \sqcup \{\infty\}$ 而是 $\frac{1}{n}\mathbb{Z}$ 的子群 $\sqcup\{\infty\}$.

$\mathfrak{P}\cap A=\mathfrak{p}$. 我们将要说明 B 是以 $\mathfrak{P}$ 为唯一极大理想的离散赋值环. 根据 Dedekind 整环的理论, 只需要说明 B 是局部环, 我们证明 $B\setminus\mathfrak{P}$ 都是单位. 假设 $y\in B\setminus\mathfrak{P}$ 满足方程

$$f(y)=y^m+a_{m-1}y^{m-1}+\ldots+a_0=0$$

通过除以 y^m, 只要证明 a_0 是单位即可. 否则, $f(X)$ 在 $A/\mathfrak{p}$ 上有重根, 根据 Hensel 引理的推论 (4.17), 有 $f(X)\equiv X^m \bmod \mathfrak{p}$, 这样,

$$\underbrace{y^m}_{\in B\setminus\mathfrak{P}}+\underbrace{\overbrace{a_{m-1}}^{\in\mathfrak{p}}y^{m-1}+\ldots+\overbrace{a_0}^{\in\mathfrak{p}}}_{\in\mathfrak{P}}=0$$

导致矛盾! 这样实际上 B 的赋值已经完全决定了 L 上的赋值, 不难验证这样的赋值满足 $\mu|_K=\nu$,

唯一性, 假设另有赋值 μ', 那么对应不同的赋值环 B', 令 $x\in B$, 假设 x 的最小多项式是

$$f(X)=X^d+a_{d-1}X^{d-1}+\ldots+a_0\qquad a_i\in A$$

假如 $\mu'(x)<0$, 那么 x^n 无疑是上式各项中赋值最小的, 从而矛盾! 故 $x\in B'$. 这说明在 K 上, $\mu(x)\geq 0$ 能推出 $\mu'(x)\geq 0$, 根据 (4.7) 可得唯一性.

下面论证后者, 先假定 $K\subseteq L$ 是 Galois 扩张, 运用前段得到唯一的 μ, 此时任意 $\sigma\in\mathrm{Gal}(L:K)$, $\mu\circ\sigma$ 也是一个赋值, 根据唯一性有 $\mu\circ\sigma=\mu$, 这意味着

$$\mu(\mathrm{Nm}x)=\mu\left(\prod_\sigma\sigma x\right)=\sum_\sigma\mu(\sigma x)=n\mu(x)$$

这样命题得证. 一般的情况只需要考虑包含 L 的扩张 L', 使得 $K\subseteq L'$ 是 Galois 的, 此时 $L\subseteq L'$ 也是 Galois 的, 再利用塔性质即可. □

实际上, 更一般的情况也可以扩张, 不过一般不是唯一的, 参见 [2]§10.6. 而代数的情形也无需可分, 参见 [2]§10.7.

推论 4.23 *令 K 是一个带完备绝对值的域, 设其绝对值是 $|\cdot|$, L 是一个 n 次有限可分扩张, 那么 L 上有唯一的完备绝对值 $||\cdot||$ 使得*

$$\forall x\in K,||x||=|x|\qquad ||x||=\sqrt[n]{|\mathrm{Nm}x|}$$

证明 无非是验证 Archimedes 域的情形, 根据 (4.14), 无非是验证 $\mathbb{R}$ 和 $\mathbb{C}$, 这是显然的. □

推论 4.24 *令 K 是一个完备的赋值域的离散赋值, $K \subseteq L$ 是可分代数扩张, 则赋值可以唯一延拓到 L 上.*

证明 考虑每一个有限扩张. □

记号 4.25 *假设 $K \subseteq L$ 是有限可分扩张, K, L 上分别有离散赋值 ν, μ, 记 $\mu|\nu$ 如果 $\mu|_K = \nu$. 在此情况下, 我们直接称 $(K \subseteq L, \nu \subseteq \mu)$ 是* **离散赋值域的有限可分扩张**.

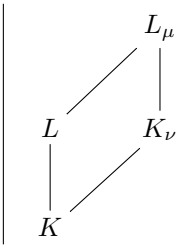
II. 非完备情况 下面我们要研究和非完备情形的联系. 下面假设特征为 0, 此时可分性得以无条件的保障.

命题 4.26 *令 K 是一个离散赋值域, 设其赋值是 ν, L 是一个 n 次有限扩张, L 上存在离散赋值 μ 使得 $\mu|_K = \nu$.*

证明 考虑 K 关于 ν 的完备化 K_ν, 上面自然继承了离散赋值 ν, 再考虑其代数闭包 $\overline{\mathrm{alg}}\, K_\nu$, 根据 (4.24), ν 总是能唯一地延拓到 $\overline{\mathrm{alg}}\, K_\nu$, 总存在嵌入 $L \to \overline{\mathrm{alg}}\, K_\nu$, 这时, 只需要限制在上面即可, 取稍大的 L, 利用 Newton 折线 (4.20) 会发现新加入的斜率是有限的, 从而不难证明其是离散的. □

命题 4.27 *条件承上, 有*

$$L_\mu = LK_\nu$$



其中 K_ν 是沿着 ν 的完备化, L_μ 是沿着 μ 的完备化. 形式地, 假如选定了嵌入 $\tau : L \to \overline{\mathrm{alg}}\, K_\nu$, 那么 $L_\mu = \overline{\tau L} = \tau L \cdot K$. 特别地, $[L_\mu, K_\nu] \leq [L : K]$.

证明 实际上 L_μ 即在之前证明过程中的 $\overline{\mathrm{alg}}\, K_\nu$ 中取闭包, 从而 $L \subseteq LK_\nu \subseteq L_\mu$, 故只要证明 LK_ν 闭即可. 因为 L 是有限维 K-线性空间, 故 LK_ν 是有限维 K_ν 线性空间, 必定完备从而是闭的. □

定理 4.28 (扩张定理) 条件上承, 关于 L 上的赋值有

- 任何 L 上的赋值 μ 都来自某个嵌入 $\tau : L \to \overline{\mathrm{alg}}\, K_\nu$, 使得 $\mu = \tau \circ \nu$.
- 两个赋值 $\mu = \tau \circ \nu, \mu' = \tau \circ \nu'$ 是相同的当且仅当存在共轭 $\sigma \in \mathrm{Hom}_{K_\nu}(\overline{\mathrm{alg}}\, K_\nu, \overline{\mathrm{alg}}\, K_\nu)$ 使得 $\nu \circ \sigma = \nu'$.

证明 第一条是显然的, 因为同时完备化后 L_μ 还在 K_ν 上有限, 故 $\overline{\mathrm{alg}}\, L_\mu = \overline{\mathrm{alg}}\, K_\nu$, 且延拓出的赋值也是相等的. 对于第二条, 考虑 $\sigma : \tau'\tau^{-1} : \tau L \to \tau' L$, 这自动延拓到 $\sigma : L_\mu \to L_{\mu'}$, 这就是所求的 σ. □

定理 4.29 条件和记号承上, 令 K 是一个离散赋值域, 设其赋值是 ν, $L = K(\alpha)$ 是代数扩张. 假设 α 的最小多项式是 f, 令

$$f = f_1 \dots f_n$$

是 f 在 K_ν 上的分解[7], 则 f_i 和所有 L 上 $\mu|\nu$ 的赋值一一对应. 具体来说, 取 f_i 的根 α_i, 对应的赋值是 μ, 那么 $L_\mu = K_\nu(\alpha)$.

证明 因为 L 到 $\overline{\mathrm{alg}}\, K_\nu$ 的嵌入完全由 α 映为 $f(X)$ 在 $\overline{\mathrm{alg}}\, K_\nu$ 中的哪个根决定, 而是否共轭取决于两个根是否是同一个 f_i 的根. 而 $L_\mu = K_\nu(\alpha)$ 的论断来自 (4.27). □

推论 4.30 令 K 是一个离散赋值域, 设其赋值是 ν, $K \subseteq L$ 是有限扩张. 则

$$[L : K] = \sum_{\mu|\nu} [L_\mu : K_\nu]$$

且

$$\mathrm{Nm}{\downarrow}_K^L\, x = \prod_{\mu|\nu} \mathrm{Nm}{\downarrow}_{K_\nu}^{L_\mu}\, x \qquad \mathrm{tr}{\downarrow}_K^L\, x = \sum_{\mu|\nu} \mathrm{tr}{\downarrow}_{K_\nu}^{L_\mu}\, x$$

[7] f_i 各不相同, 否则与可分矛盾.

证明 取原根 x, 上述三点都是如下性质的推论.

$$x \text{ 在 } K \text{ 上的特征多项式} = \prod_{\mu|\nu} x \text{ 嵌入 } L_\mu \text{ 在 } K_\nu \text{ 上特征多项式}$$

命题得证. □

下面我们类比定义 (2.31).

定义 4.31 (分歧指数, 惰性指数) 对于离散赋值域的有限可分扩张 ($K \subseteq L, \nu \subseteq \mu$), 可以定义

- **分歧指数**

$$\mathsf{e}(\mu|\nu) = [\mu(L \setminus 0) : \nu(K \setminus 0)] = \nu \text{ 值域在 } \mu \text{ 值域的指数}$$

- **惰性指数**

$$\mathsf{f}(\mu|\nu) = [B/\mathfrak{P} : A/\mathfrak{p}] = \text{域扩张 } A/\mathfrak{p} \subseteq B/\mathfrak{P} \text{ 的扩张次数}$$

其中 $A, B, \mathfrak{p}, \mathfrak{P}$ 对应于 K, L 的离散赋值环和其中的极大理想.

评注 4.32 实际上他们和定义 *(2.31)* 是相协调的, 如果 K 是完备的, 不妨假设 ν 的值域是 $\mathbb{Z}$, 如果 $\mathfrak{p}B = \mathfrak{P}^e$, 那么

$$\frac{\mathbb{N}_{\geq e}}{\mathsf{e}(\mu|\nu)} = \mu(\mathfrak{P}^e) = \mu(\mathfrak{p}B) = 1 + \frac{\mathbb{N}_{\geq 0}}{\mathsf{e}(\mu|\nu)}$$

立得 $e = \mathsf{e}(\mu|\nu)$.

下面是 (2.32) 的类比.

定理 4.33 (基本恒等式) 令 K 是一个离散赋值域, 设其赋值是 ν, $K \subseteq L$ 是 n 次有限扩张, 则

$$n = \sum_{\mu|\nu} \mathsf{e}(\mu|\nu)\mathsf{f}(\mu|\nu)$$

证明 根据 (4.30), 以及完备的情况 (4.32), 而我们知道离散的情况完备化不改变赋值值域, 完备化不改变剩余域 (4.12). 命题得证. □

对于一般的赋值 (不必完备) 可以证明对任意 $\mu|\nu$ 都有 $\mathsf{e}(\mu|\nu)\mathsf{f}(\mu|\nu) \leq n$, 这个证明是直接的, 参见 [2] §10.6 命题 10.6.8.

4.4 Krasner 引理

下面依旧假定特征 0.

引理 4.34 (Krasner) 令 K 是一个完备的离散赋值域. α, β 在 K 上代数, 如果 α 与 β 之间的距离短于 α 各共轭之间的距离, 即

$$\forall \sigma \in \mathrm{Hom}_K(\overline{\mathrm{alg}}\, K, \overline{\mathrm{alg}}\, K), \quad \alpha \neq \sigma\alpha \Rightarrow |\alpha - \beta| < |\alpha - \sigma\alpha|$$

那么 $K[\alpha] \subseteq K[\beta]$.

证明 根据 Galois 理论 (B.23), 无非是证明

$$\forall \sigma \in \mathrm{Hom}_{K[\alpha]}(K[\alpha, \beta], \overline{K}), \quad \sigma\alpha = \alpha$$

此时, 因为赋值的延拓是唯一的 (4.22), 从而 $|\sigma *| = |*|$,

$$|\sigma\alpha - \beta| = |\sigma\alpha - \sigma\beta| = |\alpha - \beta|$$

那么

$$|\sigma\alpha - \alpha| = |\sigma\alpha - \beta + \beta - \alpha| \leq |\alpha - \beta|$$

这迫使 $\alpha = \sigma\alpha$. □

定理 4.35 令 K 是一个完备的离散赋值域, $f \in K[X]$ 是一个首一不可约多项式, 那么和 f 充分接近[8]且次数相同的 $g \in K[X]$ 依旧不可约, 且

$$\forall \beta \,\mathrm{s.t.}\, g(\beta) = 0, \quad \exists \alpha \,\mathrm{s.t.}\, f(\alpha) = 0 \qquad K[\alpha] = K[\beta]$$

证明 令 $h = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K[X]$, 定义 $||h|| = \max |a_i|$. 首先, 注意到如下两个事实[9]

$$f \in K[X], f(\alpha) = 0 \qquad ||f|| \leq M \Rightarrow |\alpha| \leq \max(M, 1)$$

[8]即所有系数一致地充分接近

[9]具体来说, 因为 $|\alpha^n| \leq |a_i\alpha^i|$, 对某个 f 的系数 a_i, 从而 $|\alpha|^{n-i} \leq M$, 这样 $|\alpha| > 1$ 时, $|\alpha| \leq |\alpha|^{n-i} \leq M$. 第二个事实显然.

以及

$$f \in K[X], \beta, \qquad ||f|| \leq M, \deg f = n, |\beta| \leq N \Rightarrow |f(\beta)| < MN^n$$

假设 $f(X) = \prod(X - \alpha_i)$, 那么任意和 f 不太远的 g 则任何 g 根 β,

$$|(f-g)(\beta)| = |f(\beta)| = \prod |\beta - \alpha_i|$$

令 g 充分接近 f, 因为 β 的界有一致的控制, 从而上式充分小, 使得 $|\beta - \alpha_i| \leq |a_i - a_j|$, 根据 (4.34), $K[\alpha] \subseteq K[\beta]$, 再根据次数的要求即得 $K[\alpha] = K[\beta]$ 以及 g 不可约. □

定理 4.36 令 K 是一个离散赋值域, K_ν 是其完备化, 那么 K_ν 的任何有限扩张 L', 都存在 K 的扩张 L, 使得

$$L' = LK_\nu \qquad [L:K] = [L':K_\nu]$$

证明 因为 K 在 K_ν 稠密, 故通过选取与原根的最小多项式充分接近的 K 中多项式即可. □

4.5 完全分歧扩张

定义 4.37 (Eisenstein) 令 K 是一个离散赋值域, 赋值是 ν, 称 $f(X) = a_n X^n + \ldots + a_0$ 是 **Eisenstein 的**如果

$$\nu(a_n) = 0 \qquad \nu(a_i) > 0 \qquad \nu(a_0) = 1$$

其中 ν 的值域是 $\mathbb{Z} \sqcup \{\infty\}$. 通过放在剩余域中考虑, 或者说直接根据 *Eisenstein* 判据, f 是不可约的.

定理 4.38 令 $(K \subseteq L, \nu \subseteq \mu)$ 是 n 次完备离散赋值域的有限可分扩张, 这个扩张是完全分歧的, 即

$$\mathsf{e}(\mu|\nu) = n \qquad \mathsf{f}(\mu|\nu) = 1$$

当且仅当 $L = K(\alpha)$, 其中 α 是某个 *Eisenstein* 多项式的根.

证明 不妨假设 ν 的值域是 $\mathbb{Z} \sqcup \{\infty\}$.

先证明充分性. 根据 Newton 折线 (4.20), Eisenstein 多项式的 Newton 折线只有一种斜率, 是 $\frac{1}{n}$, 故 $\mu(\alpha) = \frac{1}{n}$, 这就已经说明 $\mathsf{e}(\mu|\nu) \geq n$, 但根据基本恒等式 (4.33), 只有可能 $\mathsf{e}(\mu|\nu) = n$.

再证明必要性. 取 L 离散赋值环极大理想的生成元 α, 于是 $\mu(\alpha) = \frac{1}{n}$, 我们断言 α 的次数是 n, 从而 $L = K(\alpha)$. 否则如果有次数更小的关系

$$a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0 \qquad \mu(a_i) \in \mathbb{Z}$$

产生矛盾, 故 α 的次数超过 n, 这说明 α 一定是 n 次的. 此时设方程

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 \qquad \mu(a_i) \in \mathbb{Z}$$

根据木桶原理, 一定有两项取到赋值的最小值, 唯一的可能是

$$\nu(a_0) = \nu(\alpha^n) = 1 \qquad \nu(a_i) > 0$$

从而 α 的最小多项式是 Eisenstein 的, 这就完成了证明. □

4.6 局部域

引理 4.39 *一个完备赋值域 K, 令 A 是离散赋值环以及极大理想 $\mathfrak{m}$, 下列条件是等价的*

- *K 局部紧致.*
- *A 紧致.*
- *$A/\mathfrak{m}$ 有限.*

证明 显然, 通过调整一个 $\mathfrak{m}$ 的生成元的方幂前两点是等价的. 因为 $\mathfrak{m}$ 是开集, 因为紧致性的要求 $A/\mathfrak{m}$ 必定是有限的. 反之, 根据 (4.13), 类似 (3.20) 论证[10]. □

[10] 因为对于度量空间列紧和紧致是等价的.

定义 4.40 (局部域) 一个域被称为 **局部域 (local field)** 如果配有一个完备的离散赋值, 满足 *(4.39)* 中的等价性质.

命题 4.41 局部域一定是如下两种情况, 其中 p 是素数,

- p 进数域 $\mathbb{Q}_p$ 的有限扩.
- 有限域上 *Laurant* 级数域 *(C.27)*$\mathbb{F}_p((X))$ 的有限扩张.

证明 显然, 上述两种情况都是局部域的典型. 反之, 假设 K 是局部域, 如果特征为 0, 那么 $\mathbb{Q} \subseteq K$, 此时根据 (4.11), 必有某个素数 p 使得 $\mathbb{Q}_p \subseteq K$, 这必须是有限维, 否则与局部紧致性 (4.39) 矛盾. 如果特征为 p, 那么 $\mathbb{F}_p \subseteq K$, 挑选极大理想的生成元 t, 此元必定不在 $\mathbb{F}_p$ 上代数, 否则 $\mathbb{F}_p(t) = \mathbb{F}_p[t]$, 此时 t 是单位与生成极大理想矛盾, 故 $\mathbb{F}_p(t) \subseteq K$, 不难验证, 其完备化是 $\mathbb{F}_p((t))$, 从而替换不定元为 X, 有 $\mathbb{F}_p((X)) \subseteq K$, 同样的理由, 这必须是有限维, 否则与局部紧致性 (4.39) 矛盾. □

命题 4.42 特征为 0 的局部域上只有有限的给定次数的完全分歧扩张.

证明 假设极大理想是 $\mathfrak{m}$, 全体 n 次 Eisenstein 多项式同胚于

$$\mathfrak{m} \times \ldots \times \mathfrak{m} \times (\mathfrak{m} \setminus \mathfrak{m}^2)$$

每一个都是离散赋值环中即开又闭的子集, 从而紧致, 故是紧致的, 而根据 (4.35), 任何一点都存在邻域, 使得领域内导出的扩张是相同的, 根据紧致性的定义即得有限性. □

这可以看做 (2.75) 的类比.

Part III

第三部分
附录

Appendix A

初等数论背景

A.1 整数的唯一分解

定理 A.1 (带余除法) *对于任意整数 $a, b \in \mathbb{Z}$, 如果 $b \neq 0$, 则存在 $q, r \in \mathbb{Z}$ 使得*

$$a = qb + r \qquad 0 \leq r < |b|$$

证明 不妨假设 a, b 都是非负正整数. 对 a 归纳, 如果 $b > a$, 那么取 $q = 0, r = a$ 即可, 否则对 $a - b$ 用归纳假设即可. 再说明唯一性. 假如 $a = q_1 b + r_1 = q_2 b + r_2$, 此时 $(q_1 - q_2)b = r_2 - r_1$, 右侧绝对值小于 b, 这迫使 $q_1 - q_2 = 0$, 进而 $q_1 = q_2, r_1 = r_2$. □

推论 A.2 *整数环 $\mathbb{Z}$ 是主理想整环, 进而是唯一分解整环.*

证明 任意选取理想 $\mathfrak{a} \subseteq \mathbb{Z}[i]$, 若 $\mathfrak{a} = (0)$ 则休矣. 若 $\mathfrak{a} \neq 0$, 可以挑选其中非零的最小者 a, 显然 $a \neq 0$. 任意取 $x \in \mathfrak{a}$, 作 x 对 a 的带余除法得到 $d, r \in \mathbb{Z}$ 使得

$$x = da + r \qquad r < a$$

因为 $r = x - da \in \mathfrak{a}$, 从而迫使 $r = 0$, 从而 $x = da$, 换言之 $\mathfrak{a} = (a) = a\mathbb{Z}$. 关于是唯一分解整环的论证见 (B.11). □

记号 A.3 注意到对于素数 p, $\mathbb{Z}/p\mathbb{Z}$ 是一个域, 记为 $\mathbb{F}_p$.

A.2 二次剩余

定义 A.4 (Legendre 符号) 对于 $x \in \mathbb{F}_p \setminus 0$, 记

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & x = 0 \\ 1 & x \neq 0, \exists y \in \mathbb{F}_p, \text{s. t. } y^2 = x \\ -1 & x \neq 0, \nexists\, y \in \mathbb{F}_p, \text{s. t. } y^2 = x \end{cases}$$

利用原根可以证明乘性以及 *Euler* 判别法

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \qquad \left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \mod p$$

其中关于原根的存在性证明可见 ([11])§1.1. 关键的是如下的三个定理, 他们给出 Legendre 符号的一种计算方法.

定理 A.5 $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv 3 \mod 4 \end{cases}$.

定理 A.6 $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \mod 8 \\ -1 & p \equiv \pm 3 \mod 8 \end{cases}$.

定理 A.7 (二次互反律) $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \begin{cases} 1 & p\text{或}q \equiv 1 \mod 4 \\ -1 & \text{其他情况.} \end{cases}$.

本部分的证明对理解本书内容并无大的作用, 其证明可见任何初等数论的教材, 简单清晰的证明可见 [11]§1.3, 更为代数的证明可见 [9] P51 §1.8, 8.6.

Appendix B

抽象代数回顾

B.1 Abel 群

引理 B.1 *有限生成的自由 Abel 群 G 的子群 H 还是自由的, 且 $\operatorname{rank} H \leq \operatorname{rank} G$.*

证明 不妨假设 $G = \mathbb{Z}^n$, 考虑如下 H 上的旗

$$F: \quad \mathbb{Z} \cap H \subseteq \mathbb{Z}^2 \cap H \subseteq \ldots \subseteq \mathbb{Z}^n \cap H$$

其中 $\mathbb{Z}^i$ 表示只有前 i 位不为 0 的子群, 考虑投影

$$\pi(F): \quad \pi_1(\mathbb{Z} \cap H) \quad \pi_2(\mathbb{Z}^2 \cap H) \quad \ldots \quad \pi_n(\mathbb{Z}^n \cap H)$$

其中 $\pi_i : \mathbb{Z}^n \to \mathbb{Z}$ 为第 i 位的投影. 设 $\pi_i(\mathbb{Z} \cap H) = r_i\mathbb{Z}$, $x_i \in \mathbb{Z}^i \cap H$ 使得 $\pi_i(x_i) = r_i$, 且约定当 $r_i = 0$ 时, 取 $x_i = 0$. 我们证明 x_i 中那些非零元构成一组基. 先证明线性无关, 假如有线性方程 (假设其中 $x_i = 0$ 时有 $a_i = 0$)

$$\underbrace{\underbrace{\underbrace{a_1x_1}_{\mathbb{Z}\cap H} + \ldots + a_nx_n}_{\cdots}}_{\mathbb{Z}^n\cap H} = 0$$

则部分和落在旗中 $\sum_{i=1}^{k} a_i x_i \in \mathbb{Z}^k \cap H$, 找下标最大的 $a_i \neq 0$, 通过 π_i 得到 $a_i r_i = 0$, 则 $a_n = 0$, 矛盾. 下面再说明其生成了 H, 实际上 H 上有旗

$$\langle x_1 \rangle \subseteq \langle x_1, x_2 \rangle \subseteq \ldots \subseteq \langle x_1, \ldots, x_n \rangle$$

我们证明上述旗就是 F, 特别地, $H = \mathbb{Z}^n \cap H = \langle x_1, \ldots, x_n \rangle$, 命题便得证. 假设 $h \in \mathbb{Z}^i \cap H$, $\pi_i(h) \in r_i\mathbb{Z}$, 则不难得到[1] $h - \frac{\pi_i(h)}{r_i} x_i \in S \cap \mathbb{Z}^{n-1}$, 实现递降到 $i = 1$, 此时显然. □

定理 B.2 *有限生成的自由 Abel 群 G 的子群 H 还是自由的, 并且还有*

存在 A 的一组基 $a_1, \ldots, a_n$, 使得 $d_1 a_1, \ldots, d_r a_r$ 是 B 的一组基

其中 $d_1 | d_2 | \ldots | d_r$. 特别地, $[G : H] = d_1 \ldots d_r$.

证明 首先, 先选取 G 的标准基 $\{e_i\}_{i=1}^n$, 再取 H 的一组基 $\{h_i\}_{i=1}^k$, 设 $h_i = \sum_{j=1}^n m_{ij} e_j$, 用矩阵写即

$$\begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_k \end{pmatrix} = \begin{pmatrix} m_{11} & m_{12} & \ldots & m_{1n} \\ m_{21} & m_{22} & \ldots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{k1} & m_{k2} & \ldots & m_{kn} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} \quad \text{记为: } \boldsymbol{h} = \boldsymbol{M}\boldsymbol{e}$$

我们断言, 存在 $\mathbb{Z}$ 组成的可逆矩阵 $\boldsymbol{P}, \boldsymbol{Q}$, 使得

$$\boldsymbol{P}\boldsymbol{M}\boldsymbol{Q} = \begin{pmatrix} d_1 & & & & \\ & d_2 & & & \\ & & \ddots & & \\ & & & d_k & \\ & & & & \boldsymbol{O}_{n-k} \end{pmatrix} := \boldsymbol{D} \quad d_1 | d_2 | \ldots | d_k \qquad (*)$$

此时 $\boldsymbol{x} = \boldsymbol{Q}^{-1}\boldsymbol{e}$ 仍然是 G 的一组基, $\boldsymbol{D}\boldsymbol{x} = \boldsymbol{P}\boldsymbol{h}$ 仍然是 H 的一组基 (因为 $\boldsymbol{P}, \boldsymbol{Q}$ 可逆), 此时回看命题的结果, 就是矩阵语言的转述而已. 下面我们开始证明我们的断言. 记 $\boldsymbol{E}_{ij}$ 为第 i 行第 j 列为 1, 其余都为 0 的矩阵, 下面对 n 和 m_{11} 归纳, 显然的是, $n = 0$ 时总成立.

[1] 因为 $\pi_i\left(h - \frac{\pi_i(h)}{r_i} x_i\right) = 0$, 以及 $\frac{\pi_i(h)}{r_i} \in \mathbb{Z}$.

- 首先第一行不全为 0, 不妨假设 $m_{11} \neq 0$, 因为交换两列即右乘以可逆矩阵 $\boldsymbol{I} - \boldsymbol{E}_{11} - \boldsymbol{E}_{ii} + \boldsymbol{E}_{1i} + \boldsymbol{E}_{i1}$.
- 若存在 i 使得 $m_{11} \nmid m_{1i}$, 则利用带余除法设 $m_{1i} = qm_{11} + r$, 施加初等列变换将第 1 列乘以 $-q$ 加到第 i 列即右乘以可逆矩阵 $(\boldsymbol{I} - q\boldsymbol{E}_{i1})$, 再交换第 1 列和第 i. 这样得到新矩阵 $\boldsymbol{M}'$, 其第一行第一列元素为 r 严格小于 m_{11}, 将用归纳假设得证. 故还可以不妨假设 $m_{11} | m_{1i}$.
- 同理, 对列做同样的工作, 可以不妨假设 $m_{11} | m_{i1}$.
- 若 $m_{11} | m_{1i}$, 则施加初等列变换将 m_{1i} 都消为 0, 再施加以初等行变换将 m_{i1} 都消为 0. 故可以不妨假设 $m_{11} \neq 0, m_{12} = \ldots = m_{1n} = 0, m_{21} = \ldots = m_{k1} = 0$.
- 若有 $2 \leq i \leq k, 2 \leq j \leq n$ 使得 $m_{11} \nmid m_{ij}$, 利用带余除法 $m_{ij} = qm_{11} + r$, 将第 1 列加到第 j 列, 再将第一行乘以 $-q$ 加到第 i 行, 再交换第 1 列和第 j 列, 再交换第 1 行和第 i 行, 这样得到新矩阵 $\boldsymbol{M}'$, 其第一行第一列元素为 r 严格小于 m_{11}, 将用归纳假设得证. 故还可以不妨假设 $\forall 2 \leq i \leq k, 2 \leq j \leq n, m_{11} | m_{ij}$.

经过上面一番约化, 可以假设 $\boldsymbol{M} = \begin{pmatrix} d_1 & \\ & d_1\boldsymbol{N} \end{pmatrix}$, 根据归纳假设, 设 $\boldsymbol{P}'\boldsymbol{N}\boldsymbol{Q}'$ 成 $(*)$ 形式, 作 $\boldsymbol{P} = \begin{pmatrix} 1 & \\ & \boldsymbol{P}' \end{pmatrix}$, $\boldsymbol{Q} = \begin{pmatrix} 1 & \\ & \boldsymbol{Q}' \end{pmatrix}$, 则 $\boldsymbol{P}\boldsymbol{M}\boldsymbol{Q}$ 化成 $(*)$ 形式. 得证. □

定理 B.3 (Abel 群结构定理) *对于有限生成的 Abel 群 G,*

(1) *都存在正整数 d 和有限正整数序列 $\{d_i > 1\}_{i=1}^{s}$ 满足 $d_{i-1} | d_i$ 对任何 $2 \leq i \leq k$, 使得*

$$G \cong \mathbb{Z}^d \oplus \bigoplus_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$$

(2) *都存在正整数 d 和由素数的方幂组成的有限多重集 $\{p_i^{n_i}\}_{i=1}^{t}$, 使得*

$$G \cong \mathbb{Z}^d \oplus \bigoplus_{i=1}^{t} \mathbb{Z}/p_i^{n_i}\mathbb{Z}$$

证明 (1) 设 $\langle g_i\rangle_{i=1}^n = G$, 作同态

$$\varphi : \mathbb{Z}^n \longrightarrow G \qquad e_i \longmapsto g_i$$

其中 $\{e_i\}_{i=1}^n$ 是标准基, 考虑 $\ker\varphi$ 是 $\mathbb{Z}^n$ 的子群, 按 (B.2), 则

$$\mathbb{Z}^n = \mathbb{Z}x_1 \oplus \ldots \oplus \mathbb{Z}x_n \quad \ker\varphi = \mathbb{Z}d_1x_1 \oplus \ldots \oplus \mathbb{Z}d_rx_r$$

于是

$$G \cong \frac{\mathbb{Z}^n}{\ker\varphi} = \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \ldots \oplus \frac{\mathbb{Z}}{d_k\mathbb{Z}} \oplus \mathbb{Z}x_{k+1} \oplus \ldots \mathbb{Z}x_n \cong \mathbb{Z}^{n-k} \oplus \bigoplus_{i=1}^{k} \mathbb{Z}/d_i\mathbb{Z}$$

而当 $d_i = 1$ 时, 将 $\frac{\mathbb{Z}}{d_i\mathbb{Z}}$ 被约为平凡群, 当 $d_i = 0$ 时, $\frac{\mathbb{Z}}{d_i\mathbb{Z}}$ 为 $\mathbb{Z}$.

(2) 因为根据中国剩余定理 $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$. □

B.2 局部化

B.3 中国剩余定理

定义 B.4 (互素) 对于交换环 R, 理想 $\mathfrak{a}, \mathfrak{b}$, 若 $\mathfrak{a} + \mathfrak{b} = R$, 则称 $\mathfrak{a}$ 和 $\mathfrak{b}$ **互素 (coprime, relative prime)**.

推论 B.5 如果 $\mathfrak{a}, \mathfrak{b}$ 互素, 则 $\mathfrak{a}^n + \mathfrak{b}^m = (1)$.

证明 因为已经有 $\mathfrak{a} + \mathfrak{b} = (1)$, 故存在 $a \in \mathfrak{a}, b \in \mathfrak{b}$ 使得 $a + b = 1$, 那么

$$1 = (a+b)^{2n} = \sum \cdots a^\bullet b^\bullet \qquad \text{每项要么} \in \mathfrak{a}, \text{要么} \in \mathfrak{b}$$

故 $\mathfrak{a}^n + \mathfrak{b}^m = (1)$, 命题得证. □

命题 B.6 若 $\mathfrak{a} + \mathfrak{c} = \mathfrak{b} + \mathfrak{c} = A$, 则 $\mathfrak{ab} + \mathfrak{c} = A$.

证明 $A = (\mathfrak{a} + \mathfrak{c})(\mathfrak{b} + \mathfrak{c}) \subseteq \mathfrak{ab} + \mathfrak{c}(\mathfrak{a} + \mathfrak{b} + \mathfrak{c}) \subseteq \mathfrak{ab} + \mathfrak{c} \subseteq A$. □

命题 B.7 对于两个互素的理想 $\mathfrak{a}, \mathfrak{b}$, $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.

证明 $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b} = (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) = \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{ab} + \mathfrak{ab} = \mathfrak{ab}.$ □

定理 B.8 (中国剩余定理) *对于交换环 R, 有限个两两互素的理想 $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, 则有*

$$\frac{R}{\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n} \cong \frac{R}{\mathfrak{a}_1} \times \ldots \times \frac{R}{\mathfrak{a}_n}$$

证明 首先

$$\varphi : R \longrightarrow \frac{R}{\mathfrak{a}_1} \times \ldots \times \frac{R}{\mathfrak{a}_n} \qquad r \longmapsto (r \bmod \mathfrak{a}_i)_i$$

的核就是 $\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$, 故是单射. 为了看到是满射, 只需要证明右手边的标准基

$$e_i = (\underbrace{\ldots}_{\text{都}=0}, \underbrace{1}_{\text{第 } i \text{ 位}}, \underbrace{\ldots}_{\text{都}=0})$$

不妨只证明 $i = 1$ 的情况, 因为两两互素, 所以 $\mathfrak{a}_1$ 和 $\mathfrak{a}_2 \ldots \mathfrak{a}_n$ 互素, 设 $a \in \mathfrak{a}_1, b \in \mathfrak{a}_2 \ldots \mathfrak{a}_n$ 使得 $a + b = 1$, 则

$$b = 1 - a \equiv \begin{cases} 0 & \bmod \mathfrak{a}_i \\ 1 & \bmod \mathfrak{a}_1 \end{cases}$$

故 $\varphi(b) = e_i$, 命题得证. □

B.4 整环

定义 B.9 *对于整环 R, $a, b \in R \setminus \{0\}$,*

- *若 $c \in R$ 使得 $b = ac$, 则称 a 整除 b, 记为 $a|b$. 并且约定 $a|0$ 对任何 $a \in R$. 容易验证, 这 $a|b \iff (b) \subseteq (a)$.*
- *定义等价关系, 方便起见$\sim$符号将贯穿本节*

$$a \sim b \iff \exists u \in U(R), \text{s.t. } a = bu$$

称之为 相伴. 容易验证, $x \sim y \iff x|y, y|x$.

定义 B.10 (素元, 不可约元) 在整环 R 上, $a,b\in R\setminus\{0\}$. 非零元 p,q 不是单位.

- 若 $p|ab \iff p|a$或$p|b$, 则称 R 为 **素元**. 注意, 其中 $\Leftarrow$ 对任何都成立.
- 若 $q=ab\Rightarrow a\sim 1$或$b\sim 1$, 则称 q 为 **不可约元**.

显然, 与素元相伴的元还是素元, 与不可约元相伴的元还是不可约元. 故我们可以在相伴的意义下谈论素元与不可约元.

定理 B.11 主理想整环是唯一分解整环.

证明 首先, 主理想整环都是 Noether 的 (参见 (C.4)), 因为任何理想升链

$$\mathfrak{a}_\bullet:\mathfrak{a}_1\subseteq\mathfrak{a}_2\subseteq\dots$$

的并 $\bigcup_{i=1}^{\infty}\mathfrak{a}_i$ 还是理想, 因此是主理想, 设为 (a), 但是 a 必定落在某一个 $\mathfrak{a}_i$ 里, 从而从 $\mathfrak{a}_i$ 开始, $\mathfrak{a}_\bullet$ 就相同了. 有了 Noether 性, 可以将任何一个元 x 分解成不可约元的乘积 [2],

$$x=p_1\dots p_n\qquad p_1,\dots,p_n \text{ 是不可约元}$$

其次, 主理想整环中不可约元[3] 一定是素元[4]. 因为若 $p|ab$ 但 $p\nmid a,p\nmid b$, 假设 $(p)+(a)=(c)$, 则 $c|p$ 故 $c\sim 1$ 或 $c\sim p$, 但后者意味着 $p|a$ 矛盾, 故 $c\sim 1$. 这意味着 $px_1+ay_1=1$ 对某个 x_1,y_1. 同理可得 $px_2+by_2=1$ 对某个 x_2,y_2, 故

$$1=1^2=(px_1+ay_1)(px_2+by_2)=p(px_1x_2+x_2by_2+1y_1x_2)+ab(y_1y_2)$$

但此时 $p|ab$, 这意味着 $p|1$, 矛盾! 这可以导出分解是唯一的, 若 x 有两种分解

$$x=p_1\dots p_n=q_1\dots q_m$$

则 $p_1|x=q_1\dots q_m$, 根据素元的定义, $p_1|q_i$, 根据不可约性知 $p_1\sim q_i$, 两边同时约去 p_1 只相差单位, 可以持续下去得到 $n=m$ 和置换 $\sigma\in\mathfrak{S}_n$, 使得 $p_{\sigma(i)}=q_i$, 命题得证. □

[2]因为如果 x 本身不可约, 则已经分解完, 否则可以拆成两部分, 然后再继续分析.
[3]即满足如下条件的不是单位或零元的 p, $ab=p\iff a\sim p$ 或$b\sim p$
[4]即满足如下条件的不是单位或零元的 p, $p|ab\iff p|a$ 或$p|b$.

定理 B.12 (Gauss) *若 R 是唯一分解整环, 则 $R[X]$ 也是唯一分解整环. 且 $R[X]$ 中的不可约元是 R 中的不可约元或是系数最大公约元[5] 为 1 的 $\mathrm{Frac}R[X]$ 中不可约多项式.*

证明 首先, 对于多项式 $f \in R[X]$, 我们引入 **容度** $c(f)$ 为系数的最大公约元. 这延展到整个 $\mathrm{Frac}R[X]$ 上通过 $c\left(\frac{f}{a}\right) = \frac{c(f)}{a}$. 我们证明 $c(fg)\sim c(f)c(g)$. 通过用 $f/c(f)$ 替代 f, $g/c(g)$ 替代 g, 不妨假设 $c(f)\sim 1, c(g)\sim 1$, 我们证明 $c(fg)\sim 1$. 否则有素元 $p|c(fg)$, 这样

$$fg \equiv 0 \mod p$$

但是 $R/pR[X]$ 是整环, 故 $f \equiv 0 \mod p$ 或 $g \equiv 0 \mod p$, 这与容度为 1 矛盾.

对于一个多项式 $f \in R[X]$, 假如 f 在 $\mathrm{Frac}R[X]$ 中的完全分解[6]为

$$f = cf_1 \dots f_n$$

可以取 $c = c(f)$, $c(f_i)\sim 1$. 这就是我们期望的唯一分解. 剩余的关于不可约性和唯一性的部分交给读者自行验证. □

B.5 域扩张

对于域 L 的子域 K, 称 $K \subseteq L$ 为 **域扩张 (extension)**. 有时记为 $L|K$.

定义 B.13 *对于域扩张 $K \subseteq L$, $x \in L$, 则*

$$\mathfrak{f} = \{f \in K[X] : f(x) = 0\}$$

*是一个理想, 如果 $\mathfrak{f} = 0$, 则称 x 在 K 上 **超越 (transcendental)**, 即任何非零多项式都不能杀死 x. 如果 $\mathfrak{f} = \langle f \rangle$, 则称 x 在 K 上 **代数 (algebraic)**, 并称 f 为 x 的 **极小多项式 (irreducible polynomial)**. 显然, 最小多项式都是不可约的.*

如果 L 所有元都在 K 上代数, 则称 $K \subseteq L$ 为代数扩张.

[5] 即整除他们最大的元, 因为唯一分解, 对应素数的方幂是每个元对应素数方幂的最小值. 这在相伴意义下是唯一的.

[6] 因为 $\mathrm{Frac}[X]$ 是主理想整环, 因为上面也有欧式除法.

记号 B.14 对于域扩张 $K \subseteq L$, $x \in K$, 记

$$K(x) = \left\{ \frac{f(x)}{g(x)} : f, g \in K[X], g(x) \neq 0 \right\}$$

为 K 包含 x 的最小域扩张, 即 x 和 K 生成的域, 这被称为 **单 (simple) 扩张**. 记

$$K[x] = \{f(x) : f \in K[X]\}$$

为包含 x 和 K 的最小的环, 即 x 和 K 生成的环. 更多元的记号以此类推.

定理 B.15 (单扩张) 对于域扩张 $K \subseteq L$, $x \in K$,

- 当 x 代数时,

$$K(x) = K[x] \cong \frac{K[X]}{\langle f \rangle} \qquad f \text{ 是 } x \text{ 的最小多项式}$$

- 当 x 超越时,

$$K(x) \cong K(X) \qquad \text{即 } K \text{ 上的 1 元有理函数域}$$

证明 先证明 $K[X] \cong \frac{K[X]}{\langle f \rangle}$. 可以作

$$\varphi : K[X] \longrightarrow K[x] \qquad f \longmapsto f(x)$$

其核正是 $\langle f \rangle$, 故已经得到 $K[X]/\langle f \rangle \to K[x]$ 的单射, 其是满射是显然的. 然后, 因为 $K[X]$ 是主理想整环, $\langle f \rangle$ 是极大理想, 故 $K[x]$ 已经是域[7], 故 $K(x) = K[x]$. 超越的情况根据定义显然. □

定义 B.16 对于域扩张 $K \subseteq L$, 显然 L 成为 K-线性空间, 记 $[L : K] = \dim_K L$. 如果 $[L : K] < \infty$, 则称为 **有限扩张**.

不难验证 **塔性质** 对于域扩张 $K \subseteq L \subseteq F$ 有 $[F : L][L : K] = [F : K]$.

如果 $K \subseteq L$ 是有限扩张, 则也是代数扩张[8]. 从而代数扩张的代数扩张还是代数扩张[9].

[7] 当然, 也可以使用分母有理化的手法

[8] 因为 $x \in L$, $1, x, x^2, \ldots$ 必定线性相关, 便得方程.

[9] 因为 $K \subseteq L \subseteq F$, 当都是有限扩张的时候非常容易, 而一般情况, 对于任意 $x \in F$, 将 x 在 L 上的方程的系数 a_i 拿出来, 这样实际上 x 在 $K[a_1, \ldots, a_n]$ 上代数, 约化为有限情形.

B.6 代数闭包

定义 B.17 (代数闭包) 对于域 K, 若代数扩张 $K \subseteq L$ 使得任何 $f \in K[X]$ 都在 L 上有 $\deg f$ 个根, 换言之 f 都分解为一次式, 则称 L 是 K 的**代数闭包 (algebraic closure)**, 记为 $\overline{\mathrm{alg}}\, K$.

定理 B.18 (代数闭包存在) 对于域 K, 代数闭包总是存在的.

证明 设其上的全体不可约多项式 $\{f_i\}_{i\in I}$, 考虑有理函数域 $K[X_i]_{i\in I}$, 并挑选 [10] 包含 $\langle f_i(X_i)\rangle$ 的极大理想 $\mathfrak{M}$. 则 $K[X_i]/\mathfrak{M} \supseteq K$ 且 f_i 在上面有根 X_i. 但是这样操作可能不是 f_i 的所有根, 于是可以继续作下去得到链

$$K \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n \subseteq \ldots$$

取 $L = \bigcup_{i=1}^{\infty} K_i$, 这时, 任何 $f \in K[X]$ 都在 L 上有根. □

定理 B.19 (延拓定理) 对于域 K, 其代数闭包 L, 对于任何代数扩张 $K \subseteq E$, 则任何同态 $K \to L$, 可以延拓为同态 $E \to L$.

证明 在 $E = K[x]$ 时, 设 f 是 x 的最小多项式, 那么 f 在 L 上有某个根 x', 那么直接映射

$$\varphi : K[X] \longrightarrow L \qquad f(X) \longmapsto x'$$

容易验证, $\ker\varphi = \langle f\rangle$, 其诱导了同态. 然后, 对于一般情形, 则是 Zorn 引理的惯常运用. □

关于 Zorn 引理, 读者如果想要快速把握其使用要诀, 可移步 [1]§5.4.

推论 B.20 对于域 K, 任意两个代数闭包都同构.

证明 对于两个代数闭包 L, F, 根据延拓定理 (B.19), 有嵌入 $L \to F$, 但是任何 F 中的元素 x 都在 K 上代数, 而落在 L 中, 故是满射. □

[10] 显然, 因为 $\langle f_i(X_i)\rangle$ 是真理想, 这总是存在的 (C.2).

定义 B.21 (可分扩张, 正规扩张) 对于任何代数扩张 $K \subseteq E$ 记

$$\mathrm{Hom}_K(E, \overline{\mathrm{alg}}\, K) = \{f : E \to \overline{\mathrm{alg}}\, K \mid f|_K = \mathrm{id}\}$$

称当中元素为 E 到 $\overline{\mathrm{alg}}\, K$ 的 K 同态, 并记 $\#\mathrm{Hom}_K(E : \overline{\mathrm{alg}}\, K) = [E : K]_s$, 称为 **可分次数**.

称 K-同态的作用为 K-**共轭 (conjugate)**, 例如对于 $x \in E$, 对于 $f \in \mathrm{Hom}_K(E, \overline{\mathrm{alg}}\, K)$, $f(x)$ 就被称为 x 在 K 上的共轭. 显然, x 的 K-共轭取遍 x 在 K 上最小多项式的所有根[11].

- 对于有限代数扩张 $K \subseteq E$, 称其为 **可分 (separable) 扩张**, 如果 *(B.19)* 的扩张方法数等于扩张次数, 即 $[E : K]_s = [E : K]$.

  不难验证对于域扩张 $K \subseteq L \subseteq F$ 有 $[F : L]_s[L : K]_s = [F : K]_s$. 单扩张 $K[x]$ 是可分的当且仅当 x 的最小多项式没有重根 [12], 作为推论, 特征为 0 时, 所有代数扩张都是可分的[13].

  对于一般的代数扩张 $K \subseteq E$, 称 $x \in E$ 为可分元如果单扩张 $K \subseteq K[x]$ 可分, 称 $K \subseteq E$ 可分, 如果所有元都可分, 容易验证两个定义是相容的.

- 如果代数扩张 $K \subseteq E$, 如果任意 $f \in \mathrm{Hom}_K(E, \overline{\mathrm{alg}}\, K)$ 使得 $f(E) = E$, 则称为 **正规 (normal) 扩张**.

  等价地, 任何不可约 $f \in K[X]$ 要么在 E 上没有根, 要么有所有根. .

  容易验证, 对于有限扩张 $K \subseteq E$, 总存在一个包含 E 的有限正规扩张 $K \subseteq N$, 因为只需要把那些生成元的最小多项式的其他根一并添加进去即可.

- 如果代数扩张 $K \subseteq E$ 既是可分的, 又是正规的, 则称之为 **Galois 扩张**. 如果挑选选定某个 $E \to \overline{\mathrm{alg}}\, K$, 从而视作子域, 还可以看成

$$\mathrm{Hom}_K(E, \overline{\mathrm{alg}}\, K) = \mathrm{Hom}_K(E, E)$$

[11] 因为对任何根 x', $K[x'] \cong \frac{K[X]}{\langle f \rangle}$, 故总存在 $x \mapsto x'$ 的 $K[X] \to \overline{\mathrm{alg}}\, K$ 的同态, 再延拓.

[12] 因为满足 $f : K[x] \to \overline{\mathrm{alg}}\, K$ 且 $f|_K = \mathrm{id}_K$ 的 f 只由 x 的取值决定, 而 f 只能将 x 映为 f 的根, 且映成任何根都可以形成同态.

[13] 因为 f 和 $f' \neq 0$ 都是互质的, 而特征 p 时会出现 $f' = 0$ 的情况.

此时, $\mathrm{Hom}_K(E, \overline{\mathrm{alg}}\, K)$ 构成一个群 [14]. 这被称之为 **Galois 群**, 通常记为 $\mathrm{Gal}(E : K)$.

关于可分性有一系列更为深入的刻画, 参见 [5]§IV.5, IV.6.

B.7 Galois 理论

定理 B.22 (本原元存在定理) *对于有限可分扩张 $K \subseteq L$, 总存在 $x \in L$ 使得 $L = K[x]$.*

证明 在 K 是有限域的情况, L 也是有限域, 而有限域的乘法群都是循环群 (B.36), 直接取这个循环群的生成元即可. 下面我们关注无穷的情况. 考虑递归论证, 只需证明二元情况, 设 $L = K[a_1, a_2]$, 考虑 $a_1 + xa_2$, 考虑 $F = K[a_1 + xa_2]$, 我们只要存在某个 x 使得 $a_2 \in F$ 即可. 设 a_1, a_2 的最小多项式为 f_1, f_2, 那么

$$f_1(a_1 + xa_2 - Xa_2) \qquad f_2(X)$$

有公共根, 故有公因式 $R \in F[X]$, 我们希望取 x 使得 $\deg R = 1$, 这样 $x_2 \in F$. 否则, 根据可分性, R 还有 a_2 以外的其他根, 这些根还和 a_2 共轭, 这也是 $f_1(a_1 + xa_2 - Xa_2)$ 的根, 而 f_1 的根有限, a_2 的共轭亦有限, 这可以解出此时 x 的取值, 但这样的取值只有限多, 只需取 x 避开这些取值即可. □

定理 B.23 (Galois 对应) *对于 Galois 扩张 $K \subseteq L$, 对应的 Galois 群是 G. 那么关于中间域 F 和子群 $H \leq G$ 有如下对应*

$$H = \mathrm{Gal}(L : F) \iff F = \{x \in L : \forall \sigma \in H, \sigma x = x\}$$

证明 先证明 $\Rightarrow$, 根据 Galois 群的定义有

$$F \subseteq \{x \in L : \forall \sigma \in H, \sigma x = x\}$$

[14] 因为实际上任何 $f \in \mathrm{Hom}_K(E, E)$ 都是同构, 单射不必说, 那么 E 是有限维的时候就得证了, 满射只需考虑某个单扩张.

反之, 对于 $y \in \{x \in L : \forall \sigma \in H, \sigma x = x\}$, 考虑 y 在 F 上的某个共轭 y', 找共轭 σ 使得 $y \mapsto y'$, 此时 $\sigma \in H$, 从而 $y' = y$, 根据可分性, $y \in F$.

再证明 $\Leftarrow$, 首先, 根据 Galois 群的定义有

$$H \subseteq \mathrm{Gal}(L : F)$$

我们要证明 $|\mathrm{Gal}(L : F)| \leq |H|$, 根据可分性即 $[L : F] \leq |H|$. 根据 (B.22), 找本原元[15] x 使得 $L = F(x)$, 那么考虑 $f = \prod_{h \in H}(X - h(x))$, 这个多项式的系数被 h 作用是不变的, 故 x 的最小多项式 f_0 整除 f, 故

$$\deg f_0 = [L : F] \leq |H| = \deg f$$

命题得证. □

定理 B.24 *对于 Galois 扩张 $K \subseteq L$, 对应的 Galois 群是 G. 如果关于中间域 F 是 K 的正规扩张, 则 $\mathrm{Gal}(L : F)$ 是 $\mathrm{Gal}(L : K)$ 的正规子群, 且*

$$\mathrm{Gal}(F : K) = \frac{\mathrm{Gal}(L : K)}{\mathrm{Gal}(L : F)}$$

证明 所谓正规指的就是 $\forall \sigma \in \mathrm{Gal}(L : K)$, $\sigma(F) = F$, 故

$$\sigma(\mathrm{Gal}(L : F))\sigma^{-1} = \{\sigma f \sigma^{-1} : f|_F = \mathrm{id}_F\} \subseteq \mathrm{Gal}(L : F)$$

是正规子群. 而考虑

$$\varphi : \mathrm{Gal}(L : K) \longrightarrow \mathrm{Gal}(F : K) \qquad f \longmapsto f|_F$$

这个映射的核就是 $\mathrm{Gal}(L : F)$. □

B.8 迹与范数

定义 B.25 (迹与范数) *对于域扩张 $K \subseteq L$, $x \in L$, 用 $x \cdot *$ 表示 L 上的左乘 x 的线性变换 $[y \mapsto xy]$, 定义 x 的 迹 与 范数*

$$\mathrm{tr}\downarrow_K^L x = \mathrm{tr}(x \cdot *) \qquad \mathrm{Nm}\downarrow_K^L x = \det(x \cdot *)$$

[15] 显然, 可分扩张的子扩张还是可分的.

容易验证这是良定义的, 实际上 $\mathrm{tr}{\downarrow_K^L}$ 和 $\mathrm{Nm}{\downarrow_K^L}$ 分别是 L 到 K 的加法和乘法同态.

容易验证的是如果 $x \in K$, 则

$$\mathrm{tr}{\downarrow_K^L}\, x = [L:K]x \qquad \mathrm{Nm}{\downarrow_K^L}\, x = x^{[L:K]}$$

且利用线性代数, 对于域扩张 $K \subseteq L \subseteq F$, 不难知道对任何 $x \in F$, 有 塔性质

$$\mathrm{tr}{\downarrow_K^F}\, x = \mathrm{tr}{\downarrow_K^L}\, (\mathrm{tr}{\downarrow_L^F}\, x) \qquad \mathrm{Nm}{\downarrow_K^F}\, x = \mathrm{Nm}{\downarrow_K^L}\, (\mathrm{Nm}{\downarrow_L^F}\, x)$$

还可以验证单扩张 $K \subseteq K[x]$, 设 $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ 是 x 的极小多项式, 则取基 $1, x, \ldots, x^{n-1}$ 计算知道

$$\mathrm{tr}{\downarrow_K^{K[x]}}\, x = -a_{n-1} \qquad \mathrm{Nm}{\downarrow_K^{K[x]}}\, x = (-1)^n a_0$$

命题 B.26 对于可分域扩张 $K \subseteq L$, $x \in L$, 有

$$\mathrm{tr}{\downarrow_K^L}\, x = \sum_{\sigma \in \mathrm{Hom}_K(L, \overline{\mathrm{alg}}\, K)} \sigma x \qquad \mathrm{Nm}{\downarrow_K^L}\, x = \prod_{\sigma \in \mathrm{Hom}_K(L, \overline{\mathrm{alg}}\, K)} \sigma x$$

证明 首先, 当 $L = K[X]$ 时这是正确的, 因为 $\{\sigma x : \sigma \in \mathrm{Hom}_K(L, \overline{\mathrm{alg}}\, K)\}$ 恰好取遍所有 x 的极小多项式的根各 1 次. 其次, 当 $x \in L$ 时利用可分性可以直接算出这是正确的. 最后, 利用塔性质, 拆分成 $K \subseteq K[x] \subseteq L$ 得证. □

命题 B.27 (Dedekind-Artin 引理) 设 Γ 为乘法幺半群 E 是整环, 令 $\mathcal{X}$ 是一族幺半群的互异同态 $\Gamma \to E$, 则 $\mathcal{X}$ 在 E 上线性无关. 具体来说, 对于 $a_\chi \in E$, 方程

$$\sum_{\chi \in \mathcal{X}} a_\chi \chi(-) = 0 \iff a_\chi = 0$$

证明 挑选 $(a_\chi) \neq 0$ 满足条件, 首先, 因为 $\chi(1) = 1$, 所以至少有两个 $a_\chi \neq 0$. 那么任意选择这样两个 $\xi, \eta \in \mathcal{X}$, 即 $0 \neq a_\xi \neq a_\eta \neq 0$, 因为互异, 所以存在 $g \in \Gamma$ 使得 $\xi(g) \neq \eta(g)$, 这样

$$\sum_{\chi \in \mathcal{X}} a_\chi \chi(g)\chi(-) = \sum_{\chi \in \mathcal{X}} a_\chi \chi(g-) = 0 \qquad \sum_{\chi \in \mathcal{X}} a_\chi \xi(g)\chi(-) = 0$$

两式相减将 $\xi(-)$ 前系数约去, 但没有约去 η 前的系数, 得到了一个规模更小的线性方程, 实现了递降, 导出矛盾. □

命题 B.28 对于有限可分域扩张 $K \subseteq L$, “**迹 (trace) 配合 (pairing)**”

$$\langle -,- \rangle : L \times L \longrightarrow K \qquad (\alpha, \beta) \longmapsto \operatorname{tr}\downarrow_K^L (\alpha\beta)$$

是非退化的, 即任意 $\alpha \neq 0$ 都存在 β 使得 $\langle \alpha, \beta \rangle \neq 0$.

证明 记 $\operatorname{tr}\downarrow_K^L = \operatorname{tr}$. 即证明存在 $\alpha \in L$ 使得 $\operatorname{tr}\alpha \neq 0$. 若任意 $\alpha \in L$ 都有 $\operatorname{tr}\alpha = 0$, 因为可分, 实际上

$$\operatorname{tr}\alpha = \sum_\sigma \sigma\alpha$$

其中 σ 取遍所有 K 同态 $L \to \overline{\operatorname{alg}}\, K$. 若 $\operatorname{tr} = 0$, 而根据 (B.27), σ 是线性无关的, 故矛盾. □

B.9 分圆扩张

定义 B.29 (本原单位根) 称一个单位根 ζ 是 n 次**本原 (primitive) 单位根**如果 $\zeta^n = 1$ 且 $\zeta^d \neq 1$ 对任何 $d < n$. 换言之, 使得

$$\zeta^n = 1 \qquad \zeta^m = 1 \iff n | m$$

容易验证所有 n 次本原单位根都形如

$$\zeta_n = \mathrm{e}^{\frac{2\pi i}{n}} \qquad (n, i) = 1$$

共有 $\varphi(n)$ 个. 其中 φ 是 *Euler* 函数. 容易验证, 任意给 n 次本原单位根 ζ, 对于所有和 n 互质的 m, ζ^m 取遍所有本原单位根.

定义 B.30 对于 $n \geq 1$, 定义第 n 个**分圆 (cyclotomic) 多项式**

$$\Phi_n(X) = \prod_{\substack{i=1,\dots,n \\ (n,i)=1}} (X - \zeta_n^i) \qquad \zeta_n = \mathrm{e}^{\frac{2\pi}{n}}$$

注意到 $\prod_{d|n} \Phi_n(X)$ 的所有零点取遍全部 n 次单位根, 故

$$\prod_{d|n} \Phi_n(X) = X^n - 1$$

从而归纳得到 $\Phi_n(X)$ 是首一的整系数系数多项式 [16].

命题 B.31 *$\Phi_n(X)$ 是 $\mathbb{Z}$ 上的不可约多项式.*

证明 任意取 ζ 为 n 次本原单位根, 其最小多项式 $f|\Phi_n$, 假设 $fg = \Phi_n$. 下面证明 ζ^p 也是 f 的根, 当 $p \nmid n$. 这就足够说明 f 有所有本原 n 次单位根了 [17]. 首先, 不难验证 ζ^p 也是本原单位根[18]. 若不是 f 的根, 则是 g 的根. 此时 $f(X)$ 和 $g(X^p)$ 有公共根 ζ^p, 这使得有非常数整系数多项式

$$h(X)|f(X) \qquad h(X)|g(X^p)$$

再 mod$p$ 考虑, 此时 $g(X^p) = g(X)^p$, 因此有非常数整系数多项式 $k(X)$ 在 $\mathbb{Z}/p\mathbb{Z}$ 中有 $k|h$, 且 $k|g$, 这样

$$k(X)|f(X) \qquad k(X)|g(X)$$

这迫使 $fg = \Phi_n$ 有重根, 但是 $\Phi_n(X)|X^n - 1$, $(X^n - 1)' = nX^{n-1} \neq 0$, 故没有重根, 矛盾. □

推论 B.32 *任何 n 次本原单位根 ζ_n 其最小多项式都是 $\Phi_n(X)$. 且 $\mathbb{Q} \subseteq \mathbb{Q}[\zeta_n]$ 是 Galois 扩张. 其 Galois 群同构于 $\mathbb{Z}_n$ 的单位群 $\mathbb{Z}_n^\times$.*

证明 因为 $\mathbb{Q}[\zeta_n]$ 含有所有的 $\Phi_n(X)$ 的根. 故是正规扩张. 因为特征为 0, 故是可分的. 而 Galois 群可以理解为置换, 具体来说

$$\varphi : \mathbb{Z}_n^\times \longrightarrow \mathrm{Gal}(\mathbb{Q}[\zeta_n] : \mathbb{Q}) \qquad m \bmod n \longmapsto [\zeta \mapsto \zeta^m]$$

容易验证这是同构. □

推论 B.33 *仔细端详 (B.24) 和上面给出的同构. 对于 $n|m$, $K_n \subseteq K_m$, 且*

$$\mathrm{Gal}(\mathbb{Q}[\zeta_n] : \mathbb{Q}[\zeta_m]) = \{k \bmod m \in \mathbb{Z}_m^\times : k \equiv 1 \mod n\}$$

[16] 是因为 "整除" 是不依赖于数域的, 具体来说若 $f = gh$, 如果 $f, h \in k[X]$, 那么自动能得到 g 的系数落在 k 里, 故 $\Phi_n(X)$ 是有理系数多项式, 通过计算容度知道还是整系数多项式.

[17] 因为这样任何和 n 互质的 m 都有 ζ^m 是 f 的根, 假设 $\zeta = \mathrm{e}^{\frac{2\pi i}{n}}$, $ia + nb = 1$, 那么 a 和 n 互素, 那么 $\zeta^a = \mathrm{e}^{\frac{2\pi}{n}}$, 反之亦然.

[18] 因为任何 d, $\zeta^{pd} = 1$ 意味着 $n|pd$, 矛盾.

定义 B.34 记号承上, 称 $\mathbb{Q}[\zeta_n]$ 为第 n 个 **分圆扩张**.

命题 B.35 暂记 $\mathbb{Q}[\zeta_n]=K_n$, 关于分圆扩张有如下性质,

(1) $K_n\cap K_m=K_{(m,n)}$.

(2) 包含 K_n,K_m 的最小域 $K_nK_m=K_{[m,n]}$.

(3) $K_n=K_m$ 对 $n<m$ 当且仅当 n 是奇数, $2n=m$.

证明 (2) 包含 K_n,K_m 的最小域就是包含 ζ_n,ζ_m 的最小域, 显然, $\zeta_n\zeta_m$ 是 $[m,n]$ 次本原单位根, 其生成了所有的 $[m,n]$ 次单位根, 当然生成了 ζ_n,ζ_n, 故 $K_nK_m=K_{[m,n]}$.

(2) 都置于 $K_{[m,n]}$ 中考虑, 利用 Galois 理论,

$$K_n\cap K_m=\left\{x\in K_{[m,n]}:\begin{array}{l}\forall\sigma\in\mathrm{Gal}(K_{[m,n]}:K_m)\cup\mathrm{Gal}(K_{[m,n]}:K_n)\\ \sigma x=x\end{array}\right\}$$

根据 (B.33)

$$\begin{cases}\mathrm{Gal}(K_{[m,n]}:K_m)=\{k \bmod [m,n]:k\equiv 1 \mod m\}\\ \mathrm{Gal}(K_{[m,n]}:K_n)=\{k \bmod [m,n]:k\equiv 1 \mod n\}\end{cases}$$

故 $\mathrm{Gal}(K_{[m,n]}:K_m)$ 和 $\mathrm{Gal}(K_{[m,n]}:K_n)$ 生成的子群是 [19]

$$\{k \bmod [m,n]:k\equiv 1 \mod (m,n)\}$$

故根据 (B.33) 和 Galois 理论 $K_nK_m=K_{[m,n]}$.

(3) 通过复合分圆域, 只需要证明 $n|m$ 的情况, 通过取中间域还可以不妨假设 m/n 是素数. 根据 (B.33), 即

$$\{k \bmod m\in\mathbb{Z}_m^\times:k\equiv 1 \mod n\}=\{1 \bmod m\}$$

[19] 因为对于 ℓ, 存在 $\ell\equiv kh \mod [m,n]$, 使得 $k\equiv 1 \mod n, h\equiv 1 \mod m$ 即
$\begin{cases}k\equiv 1 \mod n/(m,n)\\ k,h\equiv 1 \mod (m,n)\\ h\equiv 1 \mod m/(m,n)\end{cases}$ 根据中国剩余定理只需要存在 $k,h\equiv 1 \mod (m,n)$, 则就是 $n\equiv 1 \mod (m,n)$.

换言之, 所有可疑的元素

$$1+n \bmod m \qquad 1+2n \bmod m \qquad \dots \qquad 1+(p-1)\,n \bmod m$$

均不是单位, 但是 $1+2n$ 和 n 互质, 这迫使 $p|1+n, 1+2n, \dots, 1+(p-1)$. 这迫使 $p=2$, 且 n 是奇数. 命题得证. □

B.10 有限域

有限域根据其特征可以将 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 嵌入其中. 因为任何扩域都视为基域的向量空间, 故有限域的阶必为素数的方幂.

命题 B.36 *有限域的乘法群都是循环群.*

证明 在有限域的乘法群 G 上 $X^n = 1$ 的解至多只有 n 个, 找 G 中阶最大的元素 x, 不妨设之为 n, 不难得到[20]任何元素的阶都整除 n, 换言之所有元素都满足方程 $X^n = 1$, 这迫使 $n = |G|$. □

命题 B.37 *对于固定的素数方幂 p^n, 在同构意义下有唯一的 p^n 阶有限域.*

证明 因为乘法群都是循环群, 即所有非零元都满足 $X^{p^n-1} = 1$. 那么实际上 p^n 阶有限域一定是 $X^{p^n} - X$ 的所有根组成的集合. 在 $\mathbb{F}_p$ 的代数闭包中选出 $X^{p^n} - X$ 的所有根, 不难验证, 他们就构成了 p^n 阶有限域. □

定义 B.38 *记阶为 p^n 的有限域为 $\mathbb{F}_{p^n}$.*

定义 B.39 (Frobenius 自同态) *对于有限域的扩张 $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$, 可以定义* **Frobenius 自同态**

$$\mathrm{Fr}_{p^n} : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m} \qquad x \longmapsto x^{p^n}$$

因为特征 p 之故, 这是乘法同态, 又因为是单射, 故实际上是满射. 因为 $x \in \mathbb{F}_{p^n} \iff x^{p^n} = x$, 故 Fr_{p^n} 是 $\mathbb{F}_{p^n}$-同态.

[20] 对于 y, 设其阶为 m, 根据算术基本定理取互质 p, q 满足 $pq = [m, n]$, $p|m, q|n$, 则 $x^{m/p}$ 的阶为 p, $y^{n/q}$ 的阶为 q, 从而 $x^{m/p}y^{n/q}$ 的阶为 pq.

命题 B.40 *有限域的扩张 $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ 必是 Galois 扩张, 且 Galois 群是由 Frobenius 自同态 Fr_{p^n} 生成的 m/n 阶循环群.*

证明 先说明其是 Galois 扩张, 这只需要约化到 $n = 1$ 的情况. 此时 $\mathbb{F}_{p^m}$ 就是 $X^{p^m} - X$ 的所有根, 故是正规的. 可分是因为 $X^{p^m} - X$ 没有重根. 为了计算 Galois 群, 注意到

$$\mathrm{Fr}_{p^n}^i \qquad i = 1, \ldots, m/n$$

两两不同, 即 Fr_{p^n} 的阶是 m/n, 根据定义其阶是对 $x \in \mathbb{F}_{p^m}$ 有 $x^{nd} = x$ 的最小之 d, 容易知道 $d = m/n$. 而他们就已经有 $[\mathbb{F}_{p^m} : \mathbb{F}_{p^n}]$ 个了, 已经将 Galois 群填满. □

Appendix C

交换代数简介

C.1 素理想和极大理想

定义 C.1 对于交换环 R, 称一个理想 $\mathfrak{p}$ 是 **素理想 (prime)** 如果是一个真理想, 且

$$xy \in \mathfrak{p} \iff x \in \mathfrak{p} \text{或} y \in \mathfrak{p}$$

称 $\mathfrak{m}$ 是 **极大 (maximal) 理想** 如果是一个真理想, 且没有比之更大的真理想.

不难验证 $\mathfrak{p}$ 是素理想 $\iff R/\mathfrak{p}$ 是整环, $\mathfrak{p}$ 是极大理想 $\iff R/\mathfrak{p}$ 是域, 从而极大理想必是素理想.

如果有环同态 $R \xrightarrow{\varphi} R'$, R' 有素理想 $\mathfrak{p}'$, 则 $\varphi^{-1}(\mathfrak{p}')$ 也是素理想.

定理 C.2 (极大理想存在) 对于交换环 R, 任意真理想 $\mathfrak{a}$ 都存在极大理想 $\mathfrak{m} \supseteq \mathfrak{a}$.

证明 考虑全体包含 $\mathfrak{a}$ 的真理想 Σ, 因为 $\Sigma \neq \varnothing$, 且任何链 $\mathfrak{b}_\bullet$ 都有上界 [1] $\bigcup \mathfrak{b}_\bullet \in \Sigma$, 于是根据 Zorn 引理, 有极大元, 这就是极大理想. □

关于 Zorn 引理, 读者如果想要快速把握其使用要诀, 可移步 [1]§5.4.

[1] 具体来说因为 $1 \notin \bigcup \mathfrak{b}_\bullet$, 故还是真理想.

C.2 降链条件

定义 C.3 (Noether 环) 一个交换环 R 被称为 **Noether** 的, 如果任意理想升链

$$\mathfrak{a}_\bullet : \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \subseteq \mathfrak{a}_n \subseteq \ldots$$

都静止, 即存在 $n > 0$ 使得 $N > n$ 时总有 $\mathfrak{a}_N = \mathfrak{a}_n$. 等价地, 任何由 R 的理想组成的非空集合必有极大元, 因为不然的话, 可以得到严格递增的理想升链.

类似地, 对于 R-模 M 被称为 **Noether** 的, 如果任意子模升链

$$N_\bullet : N_1 \subseteq N_2 \subseteq \ldots \subseteq N_n \subseteq \ldots$$

都静止.

命题 C.4 一个交换环 R 是 *Noether* 的当且仅当其理想都是有限生成的.

证明 首先, 先证明 "当". 如果有理想链

$$\mathfrak{a}_\bullet : \mathfrak{a}_1 \subseteq \ldots \subseteq \mathfrak{a}_n \subseteq \ldots$$

则 $\bigcup \mathfrak{a}_\bullet$ 也是一个理想, 其生成元散落在有限个被并项中, 从而存在 n 使得 $\mathfrak{a}_n = \bigcup \mathfrak{a}_\bullet$, 换言之, $\mathfrak{a}_\bullet$ 从 $\mathfrak{a}_n$ 开始不变.

反之, 对于理想 $\mathfrak{a}$, 可以取她包含的极大的有限生成理想 $\mathfrak{b} \subseteq \mathfrak{a}$, 那么 $\mathfrak{b} = \mathfrak{a}$, 否则任意 $x \in \mathfrak{a} \setminus \mathfrak{b}$ 使得 $\mathfrak{b} + xR \subseteq \mathfrak{a}$ 有限生成而更大. □

利用类似的方法可以证明模的版本.

命题 C.5 一个模是 *Noether* 模当且仅当所有子模都是有限生成的.

命题 C.6 对于 *Noether* 环 R 的模 M, M 是有限生成模, 当且仅当所有子模都是有限生成的.

证明 不妨只验证自由模的情形. 假设 Noether 环 R, 考虑 $M = R^n$. 只需要证明 R^n 是 Noether 的, 对于一条子模升链 $M_\bullet$, 考虑 $R \cap M_\bullet$, 其中 R 是 M 的第一个分量, 根据环的 Noether 性, 不妨假设 $R \cap M_\bullet = A$, 那么

$$\frac{M_\bullet}{A} = \frac{M_\bullet}{R \cap M_\bullet} = \frac{R + M_\bullet}{R} \subseteq \frac{R^n}{R} = R^{n-1}$$

实现递降. 假设 $\frac{M_\bullet}{M_1}$ 静止于 B, 这就可以断言 $M_\bullet$ 静止了 [2]. □

关于 Noether 性的讨论远不止于此, 这里只是为了本书内容而做的最基本的讨论. 深入的讨论详见 [4]6, 7 两章或 [3]16 章.

C.3 局部化

定义 C.7 (局部化) *对于整环 R, 若 R 的不含 0 但含 1 的对乘法封闭的子集 S, 此时称 S 为* **乘性子集**, *定义*

$$S^{-1}R = \left\{ \frac{r}{s} \in \mathrm{Frac}R : r \in R, s \in S \right\}$$

这还是一个环, 称为 R 对 S 的 **局部化**.

一般的局部化不一定在整环上处理, 详见 [4]3 章或 [3]11, 12 章, 下面的定理实际上依旧成立, 不过验证时, 需要再小心一些, 因为一般情况 $\frac{x}{s} = \frac{y}{t}$ 并不直接等价于 $xt = ys$.

命题 C.8 (局部化的理想对应) *对于整环 R,*

- *R 的理想 $\mathfrak{a}$ 在 $S^{-1}R$ 中生成的理想, 记*

$$\alpha(\mathfrak{a}) := \quad \mathfrak{a}S^{-1}R = S^{-1}\mathfrak{a} := \left\{ \frac{a}{s} : a \in \mathfrak{a}, s \in S \right\}$$

- *$S^{-1}R$ 的理想 $\mathfrak{b}$, 记*

$$\beta(\mathfrak{b}) := \quad \mathfrak{b} \cap R = \left\{ x \in R : \exists s \in S, \mathrm{s.t.}\ \frac{x}{s} \in \mathfrak{b} \right\}$$

- *对 R 的理想 $\mathfrak{a}$, $S^{-1}R$ 的理想 $\mathfrak{b}$,*

$$\beta(\alpha(\mathfrak{a})) = \mathfrak{a}^S := \{x \in A : \exists s \in S, \mathrm{s.t.}\ sx \in \mathfrak{a}\} \qquad \alpha(\beta(\mathfrak{b})) = \mathfrak{b}$$

[2] 具体来说, 对于 $M \subseteq M'$, 如果 $M/A = M'/A = B$, 那么任意 $x' \in M'$ 都对应一个 $x \in M$ 使得 $x \equiv x' \bmod A$, 那么 $x - x' \in A \subseteq M$, 换句话说 $x' \in M$, 或者根据五引理或蛇形引理均可得证.

- 特别地, α, β 限制在如下集合上是一一对应

$$\alpha : \{R \text{ 的素理想 } \mathfrak{p} : \mathfrak{p} \cap S = \varnothing\} \longleftrightarrow \{S^{-1}R \text{ 的素理想 } \mathfrak{q}\} : \beta$$

证明 前者是因为任意 $\frac{x}{s}a = \frac{xa}{s}$, 不难验证互相包含. 后者是因为若 $\frac{x}{1} \in \mathfrak{b}$, 则 $\frac{x}{s} \in \mathfrak{b}$, 因为 $\frac{1}{s} \in S^{-1}R$. 关于 $\beta \circ \alpha$ 的论断, 即

$$\beta(\alpha(\mathfrak{a})) = \left\{x \in R : \exists a \in \mathfrak{a}, s, t \in S, \text{s.t.} \frac{x}{s} = \frac{a}{t}\right\}$$

而不难验证存在 t, s, a 使得 $xt = as$ 等价于存在 $t \in S$ 使得 $tx \in \mathfrak{a}$. 关于 $\alpha \circ \beta$ 的论断根据前两者的刻画不难. 关于素理想的论断是因为任何素理想 $\mathfrak{p}$, 不难验证 [3]

$$S^{-1}\mathfrak{p} \begin{cases} = S^{-1}R & S \cap \mathfrak{p} \neq \varnothing \\ \text{是素理想} & S \cap \mathfrak{p} = \varnothing \end{cases}$$

然后需要注意在 $S \cap \mathfrak{p} = \varnothing$ 时, $\mathfrak{p}^S = \mathfrak{p}$. □

定义 C.9 特别地, 对于素理想 $\mathfrak{p}$, $S \setminus \mathfrak{p}$ 根据素理想的定义是一个乘性子集, 记此时的局部化为 $R_{\mathfrak{p}}$. 此时根据 *(C.8)*, $R_{\mathfrak{p}}$ 只有唯一的极大理想 $\mathfrak{p}R_{\mathfrak{p}}$. 一般地, 如果一个环只有一个极大理想则称之为 **局部 (local) 环**.

C.4 整性

定义 C.10 (整) 对于两个整环 $A \subseteq B$, $x \in B$, 如果 $f \in A[X]$ 是首一的, 且 $f(x) = 0$, 则称 x 在 A 上 **整 (integral)**. $f(X) = 0$ 被称为一个适合 x 的 **整性方程**. 将所有 B 中所有在 A 上整的元素收集起来, 称为 A 在 B 中的 **整闭包**. 显然, A 包含在整闭包当中.

命题 C.11 对于两个整环 $A \subseteq B$, $x \in B$, 如下命题是等价的

(1) x 在 A 上整.

(2) 存在有限生成 A-模 $M \subseteq \mathrm{Frac}B$ 使得 $xM \subseteq M$. 其中 Frac 表示分式域.

[3] 第一行是因为 $1 \in S^{-1}\mathfrak{p}$, 第二行是因为 $1 \notin S^{-1}\mathfrak{p}$, 否则 $1 = \frac{p}{s}$, 这迫使 $p = s \in S \cap \mathfrak{p}$, 然后验证其真的是素理想.

证明 假设 (1), 找首一的 $f = X^n + a_{n-1}X + \ldots + a_0 \in A[X]$ 使得 $f(x) = 0$. 则 $M = A[x] = \sum_{i=0}^{n-1} Ax^i$, 是有限生成的, 且显然 $xM \subseteq M$, 从而 (2) 获证.

反之, 取 M 的生成元 $e_1, \ldots, e_n$, 根据 $xM \subseteq M$, "左乘 x" 是一个 "线性映射", 换言之, 存在 $\{a_{ij}\} \subseteq A$, 使得

$$\begin{cases} xe_1 = a_{11}e_1 + \ldots a_{1n}e_n \\ \quad \ldots \quad \ldots \quad \ldots \\ xe_n = a_{n1}e_1 + \ldots a_{nn}e_n \end{cases}$$

根据 Hamilton-Cayley 定理, 矩阵 $\{a_{ij}\}$ 的特征多项式将 "乘 x" 这个线性映射杀死, 因为 $M \subseteq \mathrm{Frac}B$, 所以特征多项式直接杀死了 x, 这就是一个所求的首一多项式. □

实际上, 对于一般的交换环如果之间连接以同态, 就可以定义整性, 也有类似如上的刻画, 证明大抵相似, 最后的 $\subseteq \mathrm{Frac}B$ 这一条件被换为 "忠实模", 参见 [3]P60 Chapter 10 或 [4]P59 Chapter 5.

推论 C.12 *对于两个整环 $A \subseteq B$, A 在 B 中的整闭包是还是一个环.*

证明 无非是验证对加法和乘法封闭. 注意到若 $x, y \in B$ 在 A 上整, 则 $M = A[x, y] \subseteq \mathrm{Frac}B$ 是有限生成 A-模, 此时 $xyM \subseteq M, (x+y)M \subseteq M$, 根据 (C.11) 便得到对加法和乘法封闭, 得证. □

命题 C.13 *对于三个整环 $A \subseteq B \subseteq C$, A 在 B 中的整闭包在 C 中的整闭包是 A 在 C 中的整闭包.*

证明 约定临时的记号 $X^Y = X$ 在 Y 中的整闭包. 对于 $x \in C$, 首先, x 在 A 上整必定在 A^B 上整, 故 $A^C \subseteq (A^B)^C$. 而若 x 在 A^B 上整, 假设

$$x^n + b_{n-1}x^{n-1} + \ldots + b_0 = 0$$

则实际上 x 在 $A' = A[b_1, \ldots, b_n]$ 上整. 需要注意到 A' 还是一个有限生成 A-模, 因为 b_i 在 A 上整.

则根据 (C.11), 存在有限生成 A'-模 $M \subseteq \mathrm{Frac}C$ 使得 $xM \subseteq M$. 我们断言这也是有限生成 A-模. 因为注意到

$$M = \sum A'x_i = \sum\sum Ay_jx_i$$

其中 $A'=\sum Ay_j$ 是有限生成 A-模. □

命题 C.14 对于整环 $A\subseteq B$, A 的乘性子集 S, 则

$$A \text{ 在 } B \text{ 中的整闭包设为 } C \quad \Rightarrow \quad S^{-1}A \text{ 在 } S^{-1}B \text{ 中的整闭包设为 } S^{-1}C$$

证明 因为若 $x\in S^{-1}C$ 在 $S^{-1}A$ 上整, 假设是

$$x^n+\frac{a_{n-1}}{s_{n-1}}x^{n-1}+\ldots+\frac{a_0}{s_0}=0 \qquad a_i\in A, s_i\in S$$

通过通分知道存在 $t\in S$ 使得 xt 在 A 上整, 从而 $xt\in C$, 从而 $x\in S^{-1}C$. □

命题 C.15 对于两个整环 $A\subseteq B$, 若 A 是唯一分解整环, $x\in B$ 在 A 上整, 则 x 的首一最小多项式 $\in A[X]$.

证明 若 $F(X)\in A[X]$ 是首一的且 $F(x)=0$ 的多项式. 根据 Gauss 的定理 (B.12),

$$F=af_1\ldots f_n \qquad f_i\in \mathrm{Frac}A[X] \text{ 是容度为 1 的不可约多项式}$$

通过查看首项系数, 以及通过调整一个单位, 这些多项式还可以被假设是首一的. 因为 $f_1(x)\ldots f_n(x)=0$, 那么必定有某个 f_i 是 x 的最小多项式. □

例 C.16 (二次扩张) 下面来决定 $\mathbb{Z}$ 在 $\mathbb{Q}[\sqrt{d}]=\left\{a+b\sqrt{d}:a,b\in\mathbb{Q}\right\}$ 上的整闭包. 其中 d 不含平方因子.

若 $a+b\sqrt{d}$ 整, 则 $X^2-2aX+a^2-b^2d$ 是 $a+b\sqrt{d}$ 在 $\mathbb{Q}$ 上的最小多项式, 好在有 *(C.15)*, 只要 $2a, a^2-b^2d\in\mathbb{Z}$. 设 $2a=n$, 则 $n^2-(2b)^2d\in 4\mathbb{Z}\subseteq\mathbb{Z}$, 因为 d 无平方因子, 则 $(2b)^2$ 的分母总有 "多余", 故 $2b=m\in\mathbb{Z}$, 故

$$2a=n\in\mathbb{Z} \qquad 2b=m\in\mathbb{Z} \qquad n^2-m^2d\equiv 0 \mod 4$$

注意到

$$n^2\equiv\begin{cases}0 & n \text{ 是偶数}\\ 1 & n \text{ 是奇数}\end{cases}\mod 4$$

- 若 $d\equiv 1 \mod 4$, $n^2-m^2d\equiv 0 \mod 4$ 当且仅当 m,n 同奇偶.

- 若 $d \equiv 2,3 \mod 4$, $n^2 - m^2 d \equiv 0 \mod 4$ 当且仅当 m, n 都是偶数.

故, 我们得到 $\mathbb{Q}[\sqrt{d}]$ 上全体整元为

$$\mathbb{Z}[\delta] = \{a + b\delta : a, b \in \mathbb{Z}\} \qquad \delta = \begin{cases} \frac{1+\sqrt{d}}{2} & d \equiv 1 \mod 4 \\ \sqrt{d} & d \equiv 2,3 \mod 4 \end{cases}$$

特别地, $d = -1$ 时, 就是第一章的 *Gauss* 整数环, $d = 2$ 时, 就是第一章的 $\mathbb{Z}[\sqrt{2}]$. 而 $d = 5$ 时, 整闭包为 $\mathbb{Z}[\psi]$, 其中 $\phi = \frac{\sqrt{5}-1}{2}$ 是著名的黄金分割, 满足 $\phi^2 + \phi - 1 = 0$, 当然是整的.

有了上面的介绍, 我们要将目光放在性质较好的环扩张上.

定义 C.17 (整闭) 如果对于两个整环 $A \subseteq B$, B 的所有元都在 A 上是整的, 则称扩张 $A \subseteq B$ 是整的. 换句话说 A 在 B 中的整闭包是 B 全体.

如果 A 在 $\mathrm{Frac}A$ 中的整闭包是 A 本身, 就称 A 是**整闭的**或**正规的**. 换句话说 A 在 $\mathrm{Frac}A$ 中的整闭包是 A 本身.

命题 C.18 (塔性质) 对于三个整环 $A \subseteq B \subseteq C$, 如果 $A \subseteq B$ 是整的, $B \subseteq C$ 是整的, 则 $A \subseteq C$ 是整的.

证明 根据 (C.13) 显然. □

命题 C.19 (Gauss) 主理想整环是整闭的.

证明 设主理想整环 A, $\frac{a}{b} \in \mathrm{Frac}A$, 可以假设 a, b 互质, 若其满足

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \ldots + a_0 = 0$$

通分变形成

$$a^n = -b(a_{n-1}a^{n-1} + \ldots a_0 b^{n-1})$$

与互质矛盾. □

命题 C.20 对于两个整环 $A \subseteq B$, 若 A 是整闭的, $x \in B$ 在 A 上整, 则 x 的首一最小多项式 $\in A[X]$.

证明 取 $x \in B$, 若 x 的最小多项式是

$$F(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \qquad a_0 \in \mathrm{Frac}A$$

取 F 的所有根 $x_1, \ldots, x_n$, 且 $x_1 = x$, 根据域论, 存在自同构 $\sigma_n : x_1 \mapsto x_n$. 因为 $F(x) = 0$, 则

$$F(x_n) = F(\sigma_n x) = \sigma F(x) = 0$$

故 x_n 在 A 上整, 从而根据 Vieta 定理, $a_{n-1}, \ldots, a_0$ 也在 A 上整, 因为 A 是整闭的, $a_{n-1}, \ldots, a_n \in A$. □

定理 C.21 对于整环的整扩张 $A \subseteq B$, 域的代数扩张 $K \subseteq L$. 若

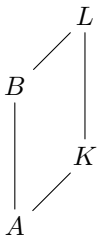
$$A \text{ 是整闭的} \qquad A \text{ 的分式域是 } K$$

B 是 A 在 L 中的整闭包, 则

$$B \text{ 是整闭的} \qquad B \text{ 的分式域是 } L$$

且

$$\begin{array}{l} K \cdot B = L \\ B \cap K = A \\ \mathrm{tr}(B) \subseteq A \\ \mathrm{Nm}(B) \subseteq A \end{array}$$



特别地, $\mathrm{Frac}B = L$.

证明 根据定义, B 是整闭的以及 $B \cap K = A$ 是显然的. 而 $\mathrm{tr}(B) \subseteq A$ 和 $\mathrm{Nm}(B) \subseteq A$ 的论断是因为整元的共轭还是整元, 整元相加还是整元, 而 $B \cap K = A$.

对于 $x \in L$ 则 x 满足方程

$$x^n + \frac{a'_{n-1}}{a_{n-1}}x^{n-1} + \ldots + \frac{a'_0}{a_0} = 0 \qquad a'_i, a_i \in A$$

则两边同时乘以 a^n, 其中 $a = a_{n-1} \dots a_0 \in A$, 可以得到 ax 的整性方程, 根据 B 是 A 在 L 中的整闭包, 有 $ax \in B$. 故

$$L \subseteq \left\{ \frac{y}{x} : y \in B, x \in A \right\} = K \cdot B \subseteq L$$

这要求 $L = K \cdot B$. □

定理 C.22 对于整环的整扩张 $A \subseteq B$, 对于素理想 $\mathfrak{b} \subseteq B$, 记 $\mathfrak{a} = \mathfrak{b} \cap A$, 则

$$\mathfrak{a} = 0 \iff 0 = \mathfrak{b}$$

$$\mathfrak{a}\text{是极大理想} \iff \text{极大理想有}\mathfrak{b}$$

证明 (1)$\Leftarrow$ 是显然的. 反之, 若有 $b \in \mathfrak{b} \setminus 0$, 则 $b \in B$ 适合整性方程

$$b^n + a_{n-1} b^{n-1} + \ldots + a_0 = 0$$

不妨假设 n 取得最小, 故 $a_0 \neq 0$, 这样 $a_0 = b(\ldots) \in \mathfrak{b} \cap \mathbb{Z}$ 产生矛盾.

(2) 需要证明 $A/\mathfrak{a}$ 是一个域 $\iff$ $B/\mathfrak{b}$ 是一个域. 首先容易验证 $\mathfrak{a}$ 是素理想, 故他们都是整环. 实际上有典范的嵌入 $A/\mathfrak{a} \to B/\mathfrak{b}$, 因为 B 在 A 上整, 故 $B/\mathfrak{b}$ 在 $A/\mathfrak{a}$ 上整. 换句话说, 我们只要证明两个整环的整扩张 $R \subseteq R'$, 只要其中一者为域则另一者为域.

假如 R' 是一个域, 对于 $x \in R \setminus 0$, 考虑 $1/x \in R'$, 因为 R' 在 R 上整, 所以

$$\frac{1}{x^n} + a_{n-1} \frac{1}{x^{n-1}} + \ldots + a_0 = 0 \qquad a_i \in R$$

通分以 x^{n-1}, 可以得到

$$\frac{1}{x} = -(a_{n-1} + \ldots + a_n x^{n-1}) \in R$$

这就证明了 R 是一个域.

而假如 R 是一个域, 对于 $y \in R' \setminus 0$, 假设

$$y^n + a_{n-1} y^{n-1} + \ldots + a_0 = 0 \qquad a_i \in A$$

不妨假设取得 n 最小, 这样 $a_0 \neq 0$, 同时除以 y,

$$\frac{1}{y} = -\frac{1}{a_0}(y^{n-1} + a_{n-1} y^{n-2} + \ldots) \in R'$$

这就证明了 R' 是一个域. □

以上命题说明对于整扩张而言, 最 "矮" 的素理想是对应的, 最 "高" 的素理想也是对应的. 关于两个整扩张之间的素理想如何对应交换代数有更加深入的研究, 参见 [3]P84 Chapter 14 或 [4]P59 Chapter 5.

C.5 离散赋值环

定义 C.23 对于域 K, 如果存在一个**满**射 $\nu : K \longrightarrow \mathbb{Z} \cup \{\infty\}$, 满足

(1) $\nu(0) = \infty$

(2) $\nu(xy) = \nu(x) + \nu(y)$

(3) $\nu(x + y) \geq \min(\nu(x), \nu(y))$

其中关于 ∞ 的运算约定俗成. 此时称 ν 为一个**离散赋值 (valuation)**.

容易验证, $\nu(-1) = 0$, $\nu(x) = \nu(-x)$, $\nu(x) \neq \nu(y)$, 则 *(3)* 取到等号, 这被俗称为 "**木桶原理**"[4]. 更一般地, $x + y + \ldots + z = 0$, 则必有两个元素 $\in \{x, y, \ldots, z\}$ 取到 ν 在其上的最小值.

容易验证,

- $A = \{x \in K : \nu(x) \geq 0\}$ 是一个环.
- $\mathfrak{m} = \{x \in K : \nu(x) > 0\}$ 是 A 的理想.
- $A \setminus \mathfrak{m} = \{x \in K : \nu(x) = 0\}$ 是 A 的单位.

从而 A 是以 $\mathfrak{m}$ 为极大理想的局部环, 即只有一个极大理想的环, 参见 *(C.9)*. 称这样得到的 A 为**离散赋值环 (discrete valuation ring)**, 这时常被简写作 **DVR**.

显然, 若 ν 是 A 到 $\mathbb{Z}_{\geq 0} \cup \{\infty\}$ 的满射, 且满足 *(1),(2),(3)* 的条件, 就可以自然延拓到整个 K 上. 但是对应的离散赋值环可能比 A 更大.

所谓离散, 指的是 "值群" 离散, 更一般地赋值环参见 [2]§10.2.

[4]其实 (3) 意味着任何 "三角形" 都是等腰的, 具体来说, 否则, 例如 $\nu(x) < \nu(y)$, 考虑 $\nu(y) = \nu(x + y - x) \geq \min(\nu(x + y), \nu(x)) = \nu(x)$, 矛盾.

命题 C.24 实际上, 离散赋值环 A 有 *Euclid* 除法, 具体来说, 对于任意 $a \in A, b \in A \setminus 0$, 都存在 $d, r \in A$ 使得

$$a = db + r \qquad r = 0 \text{或} \nu(r) < \nu(b)$$

从而是主理想整环, 是唯一分解整环.

更具体地, 任何理想都形如 $\mathfrak{m}^n$. 其中 $\mathfrak{m} = \{x \in K : \nu(x) > 0\}$; 任意的 $x \in A$ 使得 $\nu(x) = 1$ 都生成了极大理想 $\mathfrak{m} = \{x \in K : \nu(x) > 0\}$.

证明 如果 $\nu(a) \geq \nu(b)$, 那么取 $d = a/b, r = 0$, 因为 $\nu(d) = \nu(a) - \nu(b) \geq 0$, 故 $d \in A$. 否则 $\nu(a) < \nu(b)$, 则取 $d = 0, r = a$. 关于主理想的断言是日常的[5].

而注意到, 如果一个理想 $\mathfrak{a}$ 取到某一个 n 阶元, 则取到所有的 n 阶元, 因为任意两个 n 阶元之间只相差单位[6], "具体" 的断言得证. □

评注 C.25 换言之, 假如选定了 x 使得 $\nu(x) = 1$, 离散赋值环任何一个非零元素都可以写成 $x^n u$, 其中 u 是单位, $n \in \mathbb{Z}_{\geq 0}$. 从而离散赋值环的分式域任何一个非零元素也都可以写成 $x^n u$, 其中 u 是单位, $n \in \mathbb{Z}$.

现在我们可以画出如下的包含关系图[7]

$$\mathsf{DVR} \subseteq \mathsf{ED} \subseteq \mathsf{PID} \subseteq \mathsf{UFD} \cap \mathsf{DedekindD}$$

例 C.26 对于素数 p, 记 p 进赋值 ord_p 是满足 *(C.23)* 定义的赋值, 其对应的离散赋值环正是局部化

$$\mathbb{Z}_{(p)} = \left\{ \frac{x}{y} : x, y \text{ 互质}, p \nmid y \right\} \subseteq \mathbb{Q}$$

---

[5] 任何理想 $\mathfrak{a}$ 中都可以选择 ν 取值最小的元素 a, 则 $(a) \subseteq \mathfrak{a}$, 任意 $x \in \mathfrak{a}$, 根据条件 $\nu(x) \geq \nu(a)$, 则 $\nu(x/a) \geq 0$ 迫使 $x/a \in A$, 从而 $x \in (a)$.

[6] 对于 n 阶元 x, y, $\nu(x/y) = 0$.

[7] 最后一个包含关系实际上是相等关系. 假设 A 是 Dedekind 整环, 唯一分解整环, 因为理想的唯一分解, 我们只需要证明非零素理想都是主理想. 对于任意非零素理想 $\mathfrak{p}$, 当中的某个非零元素 x 经过元素的唯一分解, 由于 $\mathfrak{p}$ 是素理想, 那么必有一个素元 $p \in \mathfrak{p}$, 但是素元生成的主理想是素理想, 维数为 1 的条件导致了 $(p) = \mathfrak{p}$.

例 C.27 对于域上的幂级数环 $K[\![X]\!]$, 上面有次数

$$\deg \sum_{i=0}^{\infty} a_i X^i = \max\{i : a_i = 0\}$$

于是 $f = X^i f_0$, 其中 $\deg f_0 = 0$, 因为公式

$$\frac{1}{1-Xf} = 1 + (Xf) + (Xf)^2 + \dots$$

各项系数逐步被确定, 故次数为 0 的幂级数通过调整常数项为 1 都可以验证可逆. 于是其商域是 *Laurant* 级数环

$$K(\!(X)\!) = \left\{ \sum_{i=-n}^{\infty} a_i X^i : a_i \in K \right\}$$

容易验证 "次数" 在 $K(\!(X)\!)$ 上满足定义 *(C.23)*, 对应的离散赋值环就是幂级数环 $K[\![X]\!]$.

命题 C.28 对于离散赋值 A, 极大理想 $\mathfrak{m}$, 有 $A/\mathfrak{m}$-线性空间的同构

$$A/\mathfrak{m} \cong \mathfrak{m}/\mathfrak{m}^2 \cong \dots \cong \mathfrak{m}^i/\mathfrak{m}^{i+1}$$

换言之, A 的伴随分次代数 $\operatorname{gr} A = \sum_{i=0}^{\infty} \mathfrak{m}^i/\mathfrak{m}^{i+1} \cong (A/\mathfrak{m})[X]$.

证明 可以作同态

$$\varphi : A/\mathfrak{m} \longrightarrow \mathfrak{m}^i/\mathfrak{m}^{i+1} \qquad x \bmod \mathfrak{m} \longmapsto ax \bmod \mathfrak{m}^{i+1}$$

其中 $\nu(a) = i$. 因为

$$x \in \mathfrak{m} \iff \nu(x) \geq 1 \iff \nu(ax) \geq 1 + i \iff ax \in \mathfrak{m}^{i+1}$$

这意味着这是良定义的单射, 而任何 $x \in \mathfrak{m}^i$, 即 $\nu(x) = i$, $\nu(x/a) \geq 0$ 故 $x/a \in A$ 满足 $\varphi(x/a \bmod \mathfrak{m}) = x \bmod \mathfrak{m}^{i+1}$. 这证明了是满射. □

Appendix D

Minkowski 理论

定义 D.1 (格) 令 V 是一个 n 维 $\mathbb{R}$ 线性空间, 若 V 作为加法群的子群 Γ 满足

$$\Gamma = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m \qquad v_1, \ldots, v_m \text{ 线性无关}$$

则称 Γ 是一个秩为 m 的**格 (Lattice)**. 如果 $m = n$, 称 Γ 是一个**全 (full) 格**. 选定 Γ 的一组基, 称 $\{x_1v_1 + \ldots + x_mv_m : 0 \leq x_i \leq 1\} \subseteq V$ 为**基本区域 (fundamental mesh)**.

利用实分析容易验证对于全格, 基本区域的体积[1]是 $|\det(v_1, \ldots, v_n)|$, 和基的选取是无关的.

引理 D.2 令 V 是一个 n 维 $\mathbb{R}$ 线性空间, 若 V 作为加法群的子群 Γ, 对于 Γ 下列命题是等价的 *(1)*Γ 是格. *(2)*Γ 是离散的[2]. *(3)* 任意 $d > 0$ 以 d 为半径原点为中心的球总是交 Γ 于有限个元素.

证明 (1)⇒(2) 利用可逆线性变换是同胚容易转化到 $\mathbb{R}^n$ 中的标准格 $\mathbb{Z}^n$ 上.

(2)⇒(3) 若含无穷个点, 根据离散性这些不相交开集将挤爆这个球. [3]

[1] 具体来说是 V 上标准的 Lebesgue 测度.

[2] 即拓扑地, 任意一个点 $x \in \Gamma$, 存在开集 $U \subseteq V$ 分开 x 和 $\Gamma \setminus x$, 即使得 $U \cap \Gamma = \{x\}$.

[3] 具体来说, 对原点找 δ 使得以 2δ 为半径的球分离原点与其他 Γ 中的点, 取 U 为以 δ 为半径的球, 这样 $\{U + \gamma\}_{\gamma \in \Gamma}$ 实际上两两不交, 假如以 d 为半径原点为中心的球交 Γ 于无穷个元素, 那么以 $d + \delta$ 为半径原点为中心的球被 "挤爆", 产生矛盾.

(3)⇒(1) 首先, 考虑 Γ 生成的线性空间, 不妨直接假设就是 V, 从而可以从 Γ 中选基 $u_1,\dots,u_n$, 考虑 $\Gamma_0=\mathbb{Z}u_1+\dots+\mathbb{Z}u_n\subseteq\Gamma$, 显然[4] 根据 (3), Γ_0 是有限指数的, 设指数为 r, 那么 $\Gamma_0\subseteq\Gamma\subseteq\frac{1}{r}\Gamma_0$, 这就说明了 Γ 是格[5]. □

引理 D.3 *令 V 是一个 n 维 $\mathbb{R}$ 线性空间, 格 Γ 是完备的当且仅当存在有界集 $U\subseteq V$ 使得 $\Gamma+U$ 覆盖了整个 V.*

证明 必要性显然, 因为基本区域就满足条件. 关于必要性, 任意取 $x\in V$, 因为 $V=\Gamma+U$, $nx=\gamma_n+u_n$ 其中 $\gamma_n\in\Gamma,u_n\in U$. 这样因为 U 有界,

$$x=\frac{\gamma_n}{n}+\underbrace{\frac{u_n}{n}}_{\to 0}$$

这意味着 x 在 Γ 生成的线性空间中. □

定理 D.4 (Minkowski 定理) *令 V 是一个 n 维 $\mathbb{R}$ 线性空间, 完备格 Γ, 若 U 是中心对称的凸集[6]若*

$$\mu(X)>2^n\,\mu(\,\Gamma\text{的基本区域}\,)$$

则 $X\cap\Gamma$ 含某个非零元.

证明 我们的目标是证明 $\{\frac{1}{2}X+\gamma\}_{\gamma\in\Gamma}$ 不能两两不交, 这样的话有 $x\neq y$ 使得 $\frac{1}{2}x\equiv\frac{1}{2}y \mod\Gamma$, 那么 $0\neq\frac{x+(-y)}{2}\in X\cap\Gamma$, 因为 Γ 中心对称且是凸集.

假如 $\{\frac{1}{2}X+\gamma\}_{\gamma\in\Gamma}$ 两两不交, 那么考虑基本区域 F,

$$\mu(F)\geq\sum_{\gamma\in\Gamma}\mu\left[F\cap\left(\frac{1}{2}X+\gamma\right)\right]=\sum_{\gamma\in\Gamma}\mu\left[(F-\gamma)\cap\frac{1}{2}X\right]=\mu\left(\frac{1}{2}X\right)$$

其中 $\{F-\gamma\}_{\gamma\in\Gamma}$ 正好覆盖了 V, 上述不等式与条件矛盾. □

[4]因为任何 Γ 中的元素都可以平移到 Γ_0 的基本区域内, 而基本区域显然是有界的.
[5] 因为 Γ 的一组基可以写成 $\frac{1}{r}\Gamma_0$ 的基整数组合, 但是 $\frac{1}{r}\Gamma_0$ 是格.
[6]即 $-U=U$, 且 $\forall x,y\in U,tx+(1-t)y\in U$ 对任意 $0\leq t\leq 1$.

Bibliography

[1] 刘守民 and 熊锐. 数学入门, volume 1 of 本科数学讲义. 2018. www.cnblogs.com/XiongRuiMath/articles/8992691.html.

[2] 李文威. 代数学方法, 卷一. 北京, 高等教育出版社 (尚未出版), 2016. 在http://www.wwli.url.tw可以下载.

[3] Steven Kleniman Allen Altman. *a term of commutative algebra*. Worldwide Center of Mathematics, LLC, 2013. Available at http://www.centerofmathematics.com/wwcomstore/index.php/commalg.html.

[4] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[5] Pierre Antoine Grillet. *Abstract algebra*, volume 242 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2007.

[6] Stasys Jukna. *Extremal combinatorics: with applications in computer science*. Springer Science & Business Media, 2011.

[7] G. Lamé. Démonstration générale du théorème de fermat sur l'impossibilité en nombres entiers de l'équation $x^n + y^n = z^n$. *C. R. Acad. Sci. Paris*, 24:310–314, 1847. Available at https://gallica.bnf.fr/ark:/12148/bpt6k29812/f310.image.

[8] James S. Milne. Algebraic number theory (v3.07), 2017. Available at `https://www.jmilne.org/math/`.

[9] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[10] Issai Schur. Über die kongruenz $x^m + y^m \equiv z^m (\mathrm{mod}.p.)$.. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 25:114–116, 1917.

[11] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[12] Joseph H Silverman. *A friendly introduction to number theory*. Pearson Prentice Hall Upper Saddle River, NJ, 2006.

Index