# #BNS_NOTE 013

Xiaorui YIN

小孩子不懂事写着玩的

Septembre 2023

# 准备工作

在本文中我们约定,$K$ 总是指 $\mathbb{Q}$ 的有限次扩域,$\mathcal{O}_K$ 指 $K$ 的整数环, 而 $R$ 总是一个诺特整闭整环,$\mathrm{Quot}(R)$ 指 $R$ 的分式域.
尽管我们可以通过一些例子尝到甜头直接把整数的情况搬运到代数数里面来, 但众所周知很多代数体的整数环并不是 UFD, 因此我们不能期望再现这些令人愉快的结果. 然而当我们退而求其次改为讨论理想的算术时, 它就总是可以唯一分解了. 因此本次的话题是理想的算术以及素数的分解.

# 准备工作

**Lemma**

$\alpha \in \mathcal{O}_K^\times$ iff $|\mathrm{N}_{K|\mathbb{Q}}(\alpha)| = 1$.

**Corollary**

$|\mathrm{N}_{K|\mathbb{Q}}(\alpha)|$ 是有理素数, 那么 $\alpha$ 不可约.

**Lemma**

$\alpha \in \mathcal{O}_K \backslash 0$. 那么 $\frac{\mathrm{N}_{K|\mathbb{Q}}(\alpha)}{\alpha} \in \mathcal{O}_K$.

上面两个引理证明只需要处理那个范数. 写成 $\alpha$ 的最小多项式的根的乘积就结束了.

# 准备工作

**Lemma**

$\mathcal{O}_K$ is a factorisation domain. 也就是说每个元素都可以写成不可约元的乘积.

证明可以直接对番薯归纳.

**Lemma**

$\mathcal{O}_K$ contains infinitely many irreducible elements.

这个可以借助于有理素数无穷多导出. 对每一个有理素数根据上个引理取一个它的不可约因子; 看一下番薯就知道它们不能相同.

# Fractional Ideal

**Definition**

$R$ 的分式理想是指 $\mathrm{Quot}(R)$ 的 $R$-子模 $I$ 满足存在 $\alpha \in R\backslash\{0\},\ \alpha I \subset R$.

**Definition**

$I$ 和 $J$ 是两个分式理想, 如果 $IJ = R$, 就说 $J$ 是 $I$ 的逆, 记作 $I^{-1}$.

这个记号的合理性来源于可逆理想具有唯一的逆.

**Lemma**

下面三条等价

i) $I$ is invertible;

ii)$IJ = R$ for $J = \{\alpha \in \mathrm{Quot}(R) : \alpha I \subset R\}$;

iii)$I$ is a projective $R$-module.

# Fractional Ideal

## Lemma

i) $I$ is invertible;
ii)$IJ = R$ for $J = \{\alpha \in \mathrm{Quot}(R) : \alpha I \subset R\}$.

这个事情书上都说显然但我没觉得很显然, 不过也就是跟着定义慢慢验证.

## Proof

i)⇒(ii) 只需要验证 $J$ 的确是一个分式理想. 这玩意当然是一个 $\mathrm{Quot}(R)$ 的子模. 然后随便取 $I \cap R$ 当中的一个非零元就可以是一个公分母.
ii)⇒(i) 我们任取 $I$ 的逆 $I'$, 有 $I' \subset J$. 又按 $J$ 的定义会有 $J = JR$, 所以 $J = JII' \subset RI' \subset I'$, 从而 $I' = J$.

# $\mathcal{O}_K$

Recall: $\mathcal{O}_K$ is a free abelian group of rank $n$.

**Theorem**

$[K : \mathbb{Q}] = n$. Then any non-zero ideal $I$ of $\mathcal{O}_K$ is a free abelian group of rank $n$ as an addictive group.

$I$ 当然是 rank 不超过 $n$ 的自由 Abel 群了. 需要证明的是它的 rank 恰好是 $n$. 这样的事情当然是考虑基 (不如说对于随便一个环这种事情当然是不对的, 我们当然要彰显一下 $\mathcal{O}_K$ 的特别之处.
取 $\mathcal{O}_K$ 的 integral basis $(w_i)_{1\leq i\leq n}$, 任何 $\alpha \in I\backslash\{0\}$ 应当有 $(\alpha w_i)_{1\leq i\leq n} \subset I$ 在 $\mathbb{Z}$ 线性独立, 所以它的 rank 至少是 $n$.

**Corollary**

$\mathcal{O}_K$ is Noetherian.

**Theorem**

$\mathcal{O}_K$ 的非零素理想都极大.

和上面说的一样这个事情显然对于一般的环是不对的, 我们要充分发挥 $\mathcal{O}_K$ 的独特之处. 顺便这玩意儿似乎有好几个版本的证明, 下面的证明我个人觉得比较有感觉.

**Proof**

设 $\mathfrak{p}$ 是非零素理想,$\mathfrak{m}$ 是真包含它的理想. 选取 $\delta \in \mathfrak{m}\backslash\mathfrak{p}$.
任意选取 $a \in \mathfrak{p} \cap \mathbb{Z}\backslash\{0\}$(非空是因为随便一个人的番薯落在这里面). 然后因为我们有 integral basis, 把 $\mathcal{O}_K$ 的元素按照分量对 $a$ 进行带余除法, 变成 $\mathcal{O}_K = a\mathcal{O}_K + S$, 这里 $S$ 是一个有限集. 现在我们设 $\delta = a\beta_j + \gamma_j$, 其中 $\gamma_j \in S$, 那么就存在 $j > k$,$\gamma_j = \gamma_k$. 于是 $a(\beta_j - \beta_k) = \delta^k(\delta^{j-k} - 1)$. 左边落在 $\mathfrak{p}$ 里面, 右边 $\delta$ 不在里面, 只能是后面那个在 $\mathfrak{p}$ 里面, 这就导致 1 在 $\mathfrak{m}$ 里面了.

# Dedekind Domain

## Definition

诺特整闭整环被称为 Dedekind 整环如果它的非零素理想都极大.

正是 $\mathcal{O}_K$ 作为 Dedekind 整环的性质确保了它的理想的算术. 为了建立这些性质依旧需要准备工作. 例如这个技巧 (注意它只是 Noether):

## Lemma

诺特整环 $R$, 真理想 $I$, 那么存在一些素理想 $(\mathfrak{p}_i)_{1\leq i\leq r}$ 使得 $\prod_{i=1}^{r}\mathfrak{p}_i \subset I \subset \bigcap_{i=1}^{r}\mathfrak{p}_i$.

## Proof

把不满足这个引理性质的理想都放在一起, 假如真的有, 那么根据诺特就会有一个极大元 $J$. 它当然不能是素理想, 所以我们选择 $a, b \in R\backslash J$ 满足 $ab \in J$.$J$ 分别添上这两个元素之后的两个理想都是真理想, 根据极大性都会成立上面的性质, 于是把它们交一下 $I$ 就也满足这个了, 矛盾.

# Dedekind Domain

## Lemma

Dedekind domain $R$ 的非零素理想都可逆.

## Proof

对于素理想 $\mathfrak{p}$ 记 $\mathfrak{p}'$ 是之前提到的它的逆该有的样子. 要证明 $\mathfrak{p}\mathfrak{p}' = R$. 因为 $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}' \subset R$, $\mathfrak{p}\mathfrak{p}'$ 是一个整理想, 而且含有极大理想 $\mathfrak{p}$, 所以它只能是 $\mathfrak{p}$ 或 $R$. 如果它是 $\mathfrak{p}$, 取 $x \in \mathfrak{p}$, $y \in \mathfrak{p}'$, 那么 $xR[y] \subset \mathfrak{p} \subset R$ 是 $R$ 理想, 所以它是有限生成的, 因此 $R[y]$ 作为 $R$-module 也有限生成, 这就是说 $y \in \mathrm{Quot}(R)$ 在 $R$ 上整, 从而 $y \in R$ 即 $R = \mathfrak{p}'$, 矛盾!

# Dedekind Domain

## Lemma

Dedekind Domain $R$ 的每一个真理想都可以唯一地写成一些素理想的乘积.

## Proof

设 $I$ 是个真理想, 并且设素理想 $\prod_{i=1}^{r} \mathfrak{p}_i \subset I$. 我们对这样写所需的最少的素理想个数进行归纳. 只需 1 个素理想的情况因为它极大就对了. 如果只需少于 r 个的情况都对了, 在恰好需要 r 个时, 设 $\mathfrak{m}$ 是含有 $I$ 的极大理想. 无妨假设 $\mathfrak{p}_1 \subset \mathfrak{m}$, 所以据极大性 $\mathfrak{p}_1 = \mathfrak{m}$. 于是据上个引理同时乘以 $\mathfrak{p}_1^{-1}$ 得到 $\prod_{i=2}^{r} \mathfrak{p}_i \subset \mathfrak{p}_1^{-1} I \subset R$. 所以我们对 $\mathfrak{p}_1^{-1} I$ 使用归纳假设, 它被唯一地写成严格少于 r 个素理想的乘积, 这就差不多做完了.

# Dedekind Domain

从上面两个引理我们总结出

**Theorem**

Dedekind domain 的分式理想都可逆;
Dedekind domain 的真理想可以唯一地写成素理想的乘积.

这两个人都是充分必要的, 但是必要性用不到, 所以暂且略过.
理想的算术.

**Proposition**

$A, B, C$ 是 Dedekind 环 $R$ 的理想, 那么
i)$A \subset B \Leftrightarrow B \mid A$;
ii)$\gcd(A, B) = A + B$; $\operatorname{lcm}(A, B) = A \cap B$.

# Dedekind Domain

## Proposition

一个 Dedekind domain 是 UFD, 那么它是 PID.

## Proposition

给定 Dedekind domain $R$ 的两个非零理想 $I, J$. 那么存在 $R$ 理想 $A$, $A$ 与 $IJ$ 互素,$AI$ 是主理想.

## Proof

设包含 $I, J$ 的全部素理想是 $(\mathfrak{p}_i)_{1\leq i\leq r}$, 并且 $I=\prod_{i=1}^{r}\mathfrak{p}_i^{\alpha_i}$. 据 CRT, 选取 $x$ 满足 $x\equiv x_i \bmod \mathfrak{p}_i^{\alpha_i+1}$, 其中 $x_i\in\mathfrak{p}_i^{\alpha_i}\backslash\mathfrak{p}_i^{\alpha_i+1}$. 那么 $x\in I$ 即 $I\mid(x)$. 设 $AI=(x)$. 因为 $(x)$ 只有 $\alpha_i$ 个 $\mathfrak{p}_i$, 所以 $A$ 不能含有这些素因子, 从而与 $IJ$ 互素.

# Dedekind Domain

## Corollary

设 $I$ 是 Dedekind domain $R$ 理想, 那么任给 $x \in I \backslash \{0\}$, 存在 $y \in I$, $x, y$ 生成 $I$.

## Proposition

Dedekind domain $R$ 只有有限多个素理想, 那么它是 *PID*.

## Lemma

Dedekind domain $R$, prime ideal $\mathfrak{p}$. Then for any $n \in \mathbb{N}$ we have the isomorphism between addictive groups $R/\mathfrak{p} \simeq \mathfrak{p}^n/\mathfrak{p}^{n+1}$.

任取 $a \in \mathfrak{p}^n \backslash \mathfrak{p}^{n+1}$, 考虑 $R \to \mathfrak{p}^n/\mathfrak{p}^{n+1}$, $x \mapsto ax + \mathfrak{p}^{n+1}$ 即可.

# Norm

## Definition

对 Dedekind domain $R$ 及其理想 $I$, 定义 $I$ 的番薯 $\mathrm{N}(I) := \#R/I$.
Finite Norm Property: $\mathrm{N}(I) < \infty$ for all $I$.

## Lemma

$\mathcal{O}_K$ 具有 FNP.

Recall: $\mathcal{O}_K \simeq \mathbb{Z}^{\oplus n}$, $I$ 是它的 rank $n$ 子群.

## Proposition

$R$ 是具有 FNP 的 Dedekind 环. 那么对它的非零理想 $I, J$, 有 $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

$I, J$ 互素时从 CRT 直接得到; 上一页的引理解决素理想的幂的情形.
通过这个我们可以把番薯延拓成同态:$\{$分式理想群$\} \to \mathbb{Q}_{>0}^{\times}$.

# Norm

注意到 $R/\mathfrak{p}$ 是个 $\mathrm{N}(\mathfrak{p})$ 元有限域, 我们可以叙述一个 Fermat 小定理的平行版本.

**Proposition**

$R$ 是具有 FNP 的 Dedekind 环,$\mathfrak{p}$ 是素理想. 那么任何 $x \in R$ 有 $x^{\mathrm{N}(\mathfrak{p})} \equiv x \bmod \mathfrak{p}$, 而且 $\mathrm{N}(\mathfrak{p})$ 是使得这个性质成立的最小正整数.

一个有限性.

**Proposition**

$R$ 是具有 FNP 的 Dedekind 环. 给定实数 $t$. 满足 $\mathrm{N}(I) \leq t$ 的理想 $I$ 只有有限多个.

$R$ 有限的情况没什么可说的. 我们直接取 $R$ 中超过 t 个元素, 这些元素在 $R/I$ 的典范像一定有相同的, 也就是有 $a_i - a_j \in I$, 从而番薯小于 $t$ 的理想只能是它生成的主理想的因子 (注意我们选的这些元素和 $I$ 没有关系), 只能有有限多个.

# Norm

## Proposition

对 $\alpha \in \mathcal{O}_K$: $\mathrm{N}((\alpha)) = |\mathrm{N}_{K|\mathbb{Q}}(\alpha)|$.

这个可以用来判断一个理想是否极大 (通过取它当中的特殊元素得到番薯的整除性质).

## Proof

有 $\mathrm{N}((\alpha)) = [\mathcal{O}_K : \alpha\mathcal{O}_K]$. 取 integral basis $(w_i)_{1\leq i\leq n}$, 那么 $(\alpha w_i)_{1\leq i\leq n}$ 在 $\mathbb{Q}$ 的 Span 还是 $K$, 在 $\mathbb{Z}$ 的 Span 是 $\alpha\mathcal{O}_K$. 所以 $[\mathcal{O}_K : \alpha\mathcal{O}_K]^2 = \mathrm{D}_{K|\mathbb{Q}}(\alpha w_i)_{1\leq i\leq n}/d_K = \mathrm{D}_{K|\mathbb{Q}}(\alpha w_i)_{1\leq i\leq n}/\mathrm{D}_{K|\mathbb{Q}}(w_i)_{1\leq i\leq n} = (\det(\text{transition matrix from } w_i \text{ to } \alpha w_i))^2 = (\det(\text{matrix of } \alpha))^2 = \mathrm{N}_{K|\mathbb{Q}}(\alpha)^2$.

## Corollary

$|\mathrm{N}_{K|\mathbb{Q}}(\alpha)|$ 是有理素数, 那么 $\alpha$ prime.

# 使用例

## 使用例

$I = (1+\sqrt{-5}, 1-\sqrt{-5})$ is a maximal but not principal ideal of $\mathbb{Z}[\sqrt{-5}]$.

## Proof

首先容易验证 $1 \notin I$. 下面我们计算 $I$ 的番薯.
因为 $1+\sqrt{-5} \in I$, 所以 $\mathrm{N}(I) | \mathrm{N}_{K|\mathbb{Q}}(1+\sqrt{-5}) = 6$.
因为 $2 \in I$, 所以 $\mathrm{N}(I) | \mathrm{N}_{K|\mathbb{Q}}(2) = 4$. 所以 $\mathrm{N}(I) = 2$ prime. 这就说明 $I$ 极大. 另外如果 $I$ 是主理想, 那么生成它的元素的番薯是 2, 这不可能.

## Proposition

K 是 imaginary quadratic field, 其整数环 $\mathcal{O}_K$ 是 Euclidean domain 当且仅当 $d_K \in \{-3, -4, -7, -8, -11\}$

证明有一个番薯不超过 3 的代数整数, 直接写出番薯的显式表达控制大小然后逐个验证即可 (它们的番薯本身就可以作为 Euclidean map).

# Splitting of rational primes

从现在起 $p$ 总是指一个有理素数.

**Definition**

$\mathfrak{a}$ 是含 $p$ 的素理想.$p$ 在 $\mathfrak{a}$ 中的 ramification index 是指 $e \in \mathbb{N}$ s.t. $p \in \mathfrak{a}^e \backslash \mathfrak{a}^{e+1}$(也就是 $\mathfrak{a}$ 出现在主理想 $p$ 的分解里的次数);$\mathrm{N}(\mathfrak{a}) = p^f$ 就说 residual degree 是 $f$.

比较分解式两端的番薯有:

**Proposition**

$K|\mathbb{Q}$ 是 $n$ 次扩张,$(p) = \prod_{i=1}^{t} \mathfrak{a}_i^{e_i}$. 那么 $n = \sum_{i=1}^{t} e_i f_i$.

# Splitting of rational primes

## Proposition

$K|\mathbb{Q}$ finite Galois,$(p) = \prod_{i=1}^{t} \mathfrak{a}_i^{e_i}$. 那么任给 $1 \leq i, j \leq t$, 存在 $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ 使得 $\sigma\mathfrak{a}_i = \mathfrak{a}_j$.

## Proof

记 $\mathfrak{a}_i = \mathfrak{p}, \mathfrak{a}_j = \mathfrak{q}$. 反设任何 $\sigma, \tau \in \mathrm{Gal}(K|\mathbb{Q})$, $\sigma\mathfrak{p} \neq \tau\mathfrak{q}$. 因为这些都是极大理想, 作用完之后还是极大理想, 所以它们两两互素. 根据 CRT 我们选取 $x \in \mathcal{O}_K$ 满足 $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ 有 $x \equiv 0 \bmod \sigma\mathfrak{p}$, $x \equiv 1 \bmod \sigma\mathfrak{q}$.
知道 $\mathrm{N}_{K|\mathbb{Q}}(x) \in \mathfrak{p} \cap \mathbb{Z} = (p) = \mathfrak{q} \cap \mathbb{Z}$, 所以存在 $\rho \in \mathrm{Gal}(K|\mathbb{Q}), \rho x \in (p) \subset \mathfrak{q}$. 但是又知道 $x - 1 \in \rho^{-1}\mathfrak{q}$, 矛盾.

## Corollary

$K|\mathbb{Q}$ finite Galois,$(p) = \prod_{i=1}^{t} \mathfrak{a}_i^{e_i}$. 那么 $e_i = e_1; f_i = f_1$.

# Splitting of rational primes

设 $K=\mathbb{Q}(\theta)$,$\theta$ 整,$p\nmid[\mathcal{O}_K:\mathbb{Z}[\theta]]$.

## Lemma

在上面条件下,$\mathcal{O}_K/(p)$ 作为 $\mathbb{Z}/p\mathbb{Z}-$v.s. 有 basis $(\theta^i)_{0\leq i\leq n-1}$.

## Proof

因为 $\mathcal{O}_K/(p)$ 含 $p^n$ 个元素所以是 $n$ 维, 只需验证那些东西线性无关. 选取 integral basis $(w_i)_{1\leq i\leq n}$ 并且设 (作为 $\mathbb{Q}$-v.s.) 它到 $(\theta^i)_{0\leq i\leq n-1}$ 的转移矩阵是 $A$, 那么 $[\mathcal{O}_K:\mathbb{Z}[\theta]]=|\det A|$. 现在设 $a=\begin{pmatrix}a_0 & a_1 & \dots & a_{n-1}\end{pmatrix}$ 满足 $a_0+a_1\theta+\dots+a_{n-1}\theta^{n-1}\in(p)$. 那么

$$a\begin{pmatrix}1\\ \dots\\ \theta^{n-1}\end{pmatrix}=aA\begin{pmatrix}w_1\\ \dots\\ w_n\end{pmatrix}\equiv 0 \bmod (p).$$

所以 $aA\equiv 0_{1\times n} \bmod (p)$. 两边乘以 $A$ 的伴随就做完了.

# Splitting of rational primes

## Lemma

设 $G(X) \in \mathbb{Z}[X]$ 的典范像 $\widetilde{G}(X) \in \mathbb{Z}/p\mathbb{Z}[X]$ 不可约. 那么由 $p, G(\theta)$ 生成的理想极大或者是 $\mathcal{O}_K$.

## Proof

记这个理想为 $\mathfrak{a}$. 对 $\alpha, \beta \in \mathcal{O}_K$ s.t. $\alpha\beta \in \mathfrak{a}$, 如果 $\alpha \notin \mathfrak{a}$, 我们证明 $\beta \in \mathfrak{a}$. 根据上个引理, 存在 $\widetilde{H} \in \mathbb{Z}/p\mathbb{Z}[X]$, $\alpha = H(\theta) \bmod (p)$. 断言 $\widetilde{G}$, $\widetilde{H}$ 互素. 事实上若不然我们设 $\widetilde{H} = \widetilde{G}\widetilde{L}$, 提升到 $\mathbb{Z}[X]$ 中 $H(X) = G(X)L(X) + pQ(x)$, 代一个 $\theta$ 就导致 $H(\theta) \in \mathfrak{a}$ 矛盾. 于是我们可以设 $\widetilde{G}\widetilde{U} + \widetilde{H}\widetilde{V} = 1$. 提升到 $\mathbb{Z}[X]$ 中 $G(X)U(X) + H(X)V(X) = 1 + pR(X)$. 所以 $\beta(1 - H(\theta)V(\theta)) = \beta(G(\theta)U(\theta) - pR(\theta)) \in \mathfrak{a}$. 又有 $\beta(\alpha - H(\theta)) \in (p) \subset \mathfrak{a}$, 所以 $\beta H(\theta) \in \mathfrak{a}$, 从而 $\beta \in \mathfrak{a}$.

# Splitting of rational primes

**Theorem**

$\theta$ 的最小多项式是 $F(X)$, 它在 $\mathbb{Z}/p\mathbb{Z}$ 的典范像分解成不可约多项式 $\widetilde{F} = \prod_{k=1}^{h} \widetilde{F_k}^{e_k}$. 那么 $(p)$ 在 $\mathcal{O}_K$ 的素理想分解是 $(p) = \prod_{k=1}^{h} (p, F_k(\theta))^{e_k}$.