PRIME DECOMPOSITIONS IN DEDEKIND DOMAINS

YONG-QI LIANG

1. Extension of Dedekind Domains

Lemma 1.1. *Let R be a Noetherian one dimensional domain with fractional field K, S be the integral closure of R in K. Then for any nonzero ideal $\mathfrak{a}$ of R, $S/\mathfrak{a}S$ is a finitely generated R-module.*

Proof. See Prof. Y.Tian's lecture notes. □

Proposition 1.2. *Let R be a Dedekind domain with fractional field K, L/K be finite extension of fields, S be the integral closure of R in L, then S is Dedekind domain.*

Proof. See Prof. Y.Tian's lecture notes. □

Remark 1.3. In [2], another proof of this proposition is given by discussing purely inseparable extension. For example the integral closure of $\mathbb{F}_p[t]$ in $\mathbb{F}_p(\sqrt[p]{t})$ is $\mathbb{F}_p[\sqrt[p]{t}]$ which is Dedekind domain.

Corollary 1.4. *If L/K is separable, $\mathfrak{b}$ is an ideal of S, then $\mathfrak{b} \simeq R^{n-1} \oplus \mathfrak{a}$ as R-module with $\mathfrak{a}$ nonzero ideal of R. Moreover if $Cl(K)$ is trivial, then $\mathfrak{b} \simeq R^n$ (i.e. Integral basis theorem holds for L/K).*

Proof. We have shown that S is a finitely generated R-module, so is $\mathfrak{b}$ since R is Noetherian. By the structure theorem of finitely generated modules over Dedekind domain, we only need to show that $\mathfrak{b}$ is of "rank" $n = [L : K]$. Choose $0 \neq x_1 \in \mathfrak{b}$, and let $\{x_1, \cdots, x_n\}$ be basis of L over K. Then for $i \geq 2$, $x_i = l_i x_1 \in \mathfrak{b}$ with $l_i \in L$, there exists $a_i \in R$ such that $a_i l_i$ is integral over R, hence in S, then $a_i x_i = a_i l_i x_1 \in \mathfrak{b}$, $\{x_1, a_2 x_2, \cdots, \mathfrak{a}_n x_n\}$ is also a basis of L over K, hence $\mathfrak{b}$ is of "rank" n as R-module. (a much simpler proof: take $a \in I$ then $aS \subseteq I$, so I must be of "rank" n.) □

Example 1.5. We consider the quadratic number field $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ (with d square-free) and S be the ring of integers of $\mathbb{Q}(\sqrt{d})$, then $S = \mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha$ where $\alpha = \begin{cases} \sqrt{d} & , \text{ if } d \equiv 2, 3 (mod 4), \\ \frac{\sqrt{d}+1}{2} & , \text{ if } d \equiv 1 (mod 4) \end{cases}$ In fact, it is easy to see that $S \supseteq \mathbb{Z}[\alpha]$ since in each case α is integral over $\mathbb{Z}$. Conversely, let $\beta \in S$, then $\beta = u + v\sqrt{d}$ with $u, v \in \mathbb{Q}$. If $v = 0$, $\beta = u \in \mathbb{Q}$ is integral over $\mathbb{Z}$, which implies $u \in \mathbb{Z}$ and $\beta \in \mathbb{Z}[\alpha]$. If $v \neq 0$, the minimal polynomial of β over $\mathbb{Q}$ is $x^2 + ax + b$ with

Key words and phrases. prime decomposition , Dedekind domain.
This work was completed with the help of Prof. Y.Tian .

$a, b \in \mathbb{Z}$, then $u + v\sqrt{d} = \beta = -\frac{a}{2} \pm \frac{1}{2}\sqrt{a^2 - 4b}$, therefore (*) $a^2 - 4b = t^2 d$ with $t \in \mathbb{Z}$. If $d \equiv 1(mod4)$, $u, v \in \mathbb{Z}\frac{1}{2}$, $\beta \in \mathbb{Z}[\alpha]$, $S = \mathbb{Z}[\alpha]$. If $d \equiv 2, 3(mod4)$, we have $2 \mid a$ by (*), hence $u, v \in \mathbb{Z}$ and $S = \mathbb{Z}[\alpha]$.

Example 1.6. Cyclotomic field $\mathbb{Q}(\zeta_n)$ with $\zeta_n = e^{\frac{2\pi i}{n}}$

$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, the ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$, for details see [3].

2. Prime Decomposition

Theorem 2.1. *Let S/R be a finite extension of Dedekind domains with fractional fields L/K, $\mathfrak{p}$ be nonzero prime ideal of R, writing $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ with $e_i \geq 1$, $f_i = [S/\mathfrak{P}_i : R/\mathfrak{p}]$, then $\sum_{i=1}^{g} e_i f_i = [L : K]$.*

Proof. We have $S/\mathfrak{p}S = S/\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \simeq S/\mathfrak{P}_1^{e_1} \times \cdots \times S/\mathfrak{P}_g^{e_g}$. Consider $S/\mathfrak{P}^e$, $f = [S/\mathfrak{P} : R/\mathfrak{p}]$, $\mathfrak{P}^i/\mathfrak{P}^{i+1}$ is a $S/\mathfrak{P}$-vector space, there is no ideal between $\mathfrak{P}^i$ and $\mathfrak{P}^{i+1}$, so $\mathfrak{P}^i/\mathfrak{P}^{i+1}$ has no proper submodule, hence $dim_{S/\mathfrak{P}}\mathfrak{P}^i/\mathfrak{P}^{i+1} = 1$, $dim_{R/\mathfrak{p}}\mathfrak{P}^i/\mathfrak{P}^{i+1} = f$. $0 \subseteq \mathfrak{P}^{e-1}/\mathfrak{P}^e \subseteq \mathfrak{P}^{e-2}/\mathfrak{P}^e \subseteq \cdots \subseteq \mathfrak{P}/\mathfrak{P}^e \subseteq S/\mathfrak{P}^e$ is a chain of $R/\mathfrak{p}$-vector spaces with $\frac{\mathfrak{P}^i/\mathfrak{P}^e}{\mathfrak{P}^{i+1}/\mathfrak{P}^e} \simeq \mathfrak{P}^i/\mathfrak{P}^{i+1}$, therefore $dim_{R/\mathfrak{p}}S/\mathfrak{P}^e = ef$, $dim_{R/\mathfrak{p}}S/\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} = \sum e_i f_i$.

S is a finitely generated R-module and S is torsion-free for $S \subseteq L$, so by the structure theorem $S = Rx_1 \oplus \cdots \oplus Rx_{n-1} \oplus \mathfrak{a}x_n$, with $\mathfrak{a}$ an ideal of R, by tensor-ing with K we obtain $n = [L : K]$. Now $\mathfrak{p}S = \mathfrak{p}x_1 \oplus \cdots \oplus \mathfrak{p}x_{n-1} \oplus \mathfrak{p}\mathfrak{a}x_n$, $S/\mathfrak{p}S \simeq (R/\mathfrak{p})^{n-1} \oplus \mathfrak{a}/\mathfrak{p}\mathfrak{a} \simeq (R/\mathfrak{p})^n$ as $R/\mathfrak{p}$-vector space, $dim_{R/\mathfrak{p}}S/\mathfrak{p}S = n$. Therefore $[L : K] = n = \sum e_i f_i$.

$\square$

Remark 2.2. In deed, we just dealt with the fibre of the point $\mathfrak{p}$, hence the problem is local. We can treat it "near" $\mathfrak{p}$, that is localization at $\mathfrak{p}$, this process will not change e and f, and we can proof the theorem by using the structure theorem of finitely generated modules over P.I.D instead of that over Dedekind domain.

Theorem 2.3. *Let S/R be a finite extension of Dedekind domains with fractional fields L/K. If $L = K(\alpha)$ with $\alpha \in S$, whose minimal polynomial over K is $F(X) \in R[X]$, and $\mathfrak{p}$ is a nonzero prime ideal of R. Assume that $\mathfrak{p}S \cap R[\alpha] = \mathfrak{p}R[\alpha]$. $\bar{F}(X) = \bar{F}_1(X)^{e_1} \cdots \bar{F}_g(X)^{e_g}$ in $R/\mathfrak{p}[X]$ where $F_i(X) \in R[X]$ is monic such that $\bar{F}_i(X) \in R[X]$ is irreducible. Set $f_i = degF_i$ and $\mathfrak{P}_i = (\mathfrak{p}, F_i(\alpha))$, then $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ with $f_i = [S/\mathfrak{P}_i : R/\mathfrak{p}]$.*

Proof. Denote $R/\mathfrak{p}$ by k. Note that $R[X]/(F) \simeq R[\alpha]$, tensor with $k = R/\mathfrak{p}$, we obtain $k[X]/(\bar{F}) \simeq R/\mathfrak{p} \otimes_R R[\alpha] \simeq R[\alpha]/\mathfrak{p}[\alpha] = R[\alpha]/\mathfrak{p}S \cap R[\alpha]$.

We observe that the kernel of $R[\alpha] \to S/\mathfrak{p}S$ is $\mathfrak{p}S \cap R[\alpha] = \mathfrak{p}R[\alpha]$, hence induces an injection $R[\alpha]/\mathfrak{p}R[\alpha] \to S/\mathfrak{p}S$, we claim that it is an isomorphism. In deed, $dim_{R/\mathfrak{p}}S/\mathfrak{p}S = [L : K]$ by the previous theorem. Note that $R[\alpha] \subseteq L$ is a finitely generated torsion-free R-module, the structure theorem of finitely generated modules over Dedekind domain implies $R[\alpha] \simeq \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_n x_n$ with $\mathfrak{a}_i$ ideals of R, $n = [K(\alpha) : K] = [L : K]$. $R[\alpha]/\mathfrak{p}R[\alpha] \simeq \mathfrak{a}_1/\mathfrak{p}a_1 \oplus$

$\cdots \oplus \mathfrak{a}_n/\mathfrak{p}\mathfrak{a}_n \simeq R/\mathfrak{p} \oplus \cdots \oplus R/\mathfrak{p}$ hence is of dimension n as $R/\mathfrak{p}$-vector space. $R[\alpha]/\mathfrak{p}R[\alpha] \to S/\mathfrak{p}S$ must be surjective, hence isomorphic. So we obtain $\phi : k[X]/(\bar{F}) \to S/\mathfrak{p}S; G + (\bar{F}) \mapsto G(\alpha) + \mathfrak{p}S$ as ring isomorphism.

$\{$maximal ideal of S that divides $\mathfrak{p}S\}\xleftrightarrow{1:1}\{$maximal ideal of S containing $\mathfrak{p}S\}\xleftrightarrow{1:1}\{$maximal ideal of $S/\mathfrak{p}S\}\xleftrightarrow{1:1}\{$maximal ideal of $k[X]/(\bar{F})\}\xleftrightarrow{1:1}\{$maximal ideal of $k[X]$ containing $(\bar{F})\}\xleftrightarrow{1:1}\{$irreducible polynomial of $k[X]$ that divides $\bar{F}\}$, this is just $\bar{F}_i \xleftrightarrow{1:1} (F_i(\alpha), \mathfrak{p}) = \mathfrak{P}_i$ by the definition of ϕ. So we have $\mathfrak{p}S = \mathfrak{P}_1^{t_1} \cdots \mathfrak{P}_g^{t_g}$.

Note that $\bar{F} = \bar{F}_1^{e_1} \cdots \bar{F}_g^{e_g}$, $\bar{F}_1^{e_1} \cdots \bar{F}_g^{e_g} = 0$ in $k[X]/(\bar{F})$, so $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} = 0$ in $S/\mathfrak{p}S$, so $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \subseteq \mathfrak{p}S = \mathfrak{P}_1^{t_1} \cdots \mathfrak{P}_g^{t_g}$, hence $e_i \geq t_i$ by localizing S at $\mathfrak{P}_i$. Conversely, $\mathfrak{p}S = \mathfrak{P}_1^{t_1} \cdots \mathfrak{P}_g^{t_g}$, that is $\mathfrak{P}_1^{t_1} \cdots \mathfrak{P}_g^{t_g} = 0$ in $S/\mathfrak{p}S$ so $\bar{F}_1^{t_1} \cdots \bar{F}_g^{t_g} = 0$ in $k[X]/(\bar{F})$, $\bar{F} \mid \bar{F}_1^{t_1} \cdots \bar{F}_g^{t_g}$, hence $e_i \leq t_i$. Therefore $\mathfrak{p}S = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$.

At last, we have to show that $f_i = [S/\mathfrak{P}_i : R/\mathfrak{p}]$. Consider $\pi : R[X] \to S/\mathfrak{P}_i; G \mapsto G(\alpha) + \mathfrak{P}_i$, $(\mathfrak{p}, F_i) \subseteq ker\pi$ for $\mathfrak{P}_i = (F_i(\alpha), \mathfrak{p})$, this induces $\bar{\pi} : R[X]/(\mathfrak{p}, F_i) \to S/\mathfrak{P}_i$, and $R[X] \to k[X] \to k[X]/(\bar{F}_i)$ induces isomorphism $R[X]/(\mathfrak{p}, F_i) \xrightarrow{\simeq} k[X]/(\bar{F}_i)$, therefore $R/\mathfrak{p} = k \to k[X] \to k[X]/(\bar{F}_i) \to S/\mathfrak{P}_i$ is a field extension. $f_i' = [S/P_i : R/\mathfrak{p}] \geq [k[X]/(\bar{F}_i) : R/\mathfrak{p}] = deg\bar{F}_i = f_i$, but we always have $\sum f_i' e_i = [L : K] = degF = deg\bar{F} = \sum e_i f_i$, hence $f_i = f_i'$, $f_i = [S/\mathfrak{P}_i : R/\mathfrak{p}]$. (a much simpler proof: $\phi : k[X]/(\bar{F}) \to S/\mathfrak{p}S$ is a k-algebra isomorphism with $\bar{F}_i \xleftrightarrow{1:1} (F_i(\alpha), \mathfrak{p}) = \mathfrak{P}_i$, hence the degree of residue field at corresponding closed points are the same, i.e. $f_i = f_i'$.)

$\square$

Remark 2.4.

(1)We define $I = \{\beta \in S \mid \beta S \subseteq R[\alpha]\}$ to be the *conductor*, it is the maximum ideal of S contained in $R[\alpha]$. The geometric condition $I + \mathfrak{p}S = S$ implies $\mathfrak{p}S \cap R[\alpha] = \mathfrak{p}R[\alpha]$. In deed, $I + \mathfrak{p}S = S$ implies $I + \mathfrak{p}R[\alpha] = R[\alpha]$(otherwise $I + \mathfrak{p}R[\alpha] \subseteq \mathfrak{m}$ maximal ideal in $R[\alpha]$, then $I \subseteq \mathfrak{m}S$ and $\mathfrak{p}S \subseteq \mathfrak{m}S$ with $\mathfrak{m}S \neq S$ since S is integral over $R[\alpha]$ and going-up theorem, this leads to a contradiction), then $\mathfrak{p}S \cap R[\alpha] = (I + \mathfrak{p}R[\alpha])(\mathfrak{p}S \cap R[\alpha]) \subseteq I(\mathfrak{p}S \cap R[\alpha]) + \mathfrak{p}R[\alpha] \subseteq I\mathfrak{p}S + \mathfrak{p}R[\alpha] \subseteq \mathfrak{p}I + \mathfrak{p}R[\alpha] \subseteq \mathfrak{p}R[\alpha]$ (remember that $I \subseteq R[\alpha]$).

(2)In number theory, for $R = \mathbb{Z}$, $L/\mathbb{Q}$ number field, $S = O_L$ integral closure of $\mathbb{Z}$ in L and p prime number in $\mathbb{Z}$. If $p \nmid [S : \mathbb{Z}[\alpha]]$, then $pS \cap \mathbb{Z}[\alpha] = p\mathbb{Z}[\alpha]$. In general $pS \cap \mathbb{Z}[\alpha] \supseteq p\mathbb{Z}[\alpha]$, and $[pS \cap \mathbb{Z}[\alpha] : p\mathbb{Z}[\alpha]]$ divides $[pS : p\mathbb{Z}[\alpha]] = [S : \mathbb{Z}[\alpha]]$ and $[\mathbb{Z}[\alpha] : p\mathbb{Z}[\alpha]] =$ some power of p, hence $[pS \cap \mathbb{Z}[\alpha] : p\mathbb{Z}[\alpha]] = 1$.

(3)Dedekind showed that there exist some ring of integers O such that for some p one cannot find α satisfying $p \mid [O : \mathbb{Z}[\alpha]]$.

Example 2.5. Consider the prime decomposition of quadratic fields. For $\mathbb{Q}(\sqrt{d})$ with d square-free we know that $S = \begin{cases} \mathbb{Z}[\sqrt{d}] & , \text{ if } d \equiv 2, 3(mod4), \\ \mathbb{Z}[\frac{\sqrt{d}+1}{2}] & , \text{ if } d \equiv 1(mod4) \end{cases}$

(1)$d\equiv 2,3(mod 4)$, we choose $\alpha=\sqrt{d}$ with minimal polynomial x^2-d. Consider $x^2-d\equiv 0(mod p)$, if $(\frac{d}{p})=1$ then $pS=\begin{cases} (p,c+\sqrt{d})^2 & ,\ \text{if p=2} \\ (p,c+\sqrt{d})(p,c-\sqrt{d}) & ,\ \text{if } p\neq 2 \end{cases}$ with $d=c^2(mod p)$, if $(\frac{d}{p})=-1$, then pS is still a prime ideal, if $p\mid d$, then $pS=(p,\sqrt{d})^2$.

(2)$d\equiv 1(mod 4)$, we can also choose $\alpha=\sqrt{d}$, in this case $[S:\mathbb{Z}[\sqrt{d}]]=2$. If $p\neq 2$, $pS=\begin{cases} (\mathfrak{p},c+\sqrt{d})(\mathfrak{p},c-\sqrt{d}) & ,\ \text{if } (\frac{d}{p})=1 \\ \text{still prime} & ,\ \text{if } (\frac{d}{p})=-1 \end{cases}$ with $d=c^2(mod p)$.
If $p=2$, we should choose $\alpha=\frac{\sqrt{d}+1}{2}$, consider $x^2-x+\frac{1-d}{4}\equiv 0(mod 2)$ $d=1(mod 8)\iff x^2-x+\frac{1-d}{4}\equiv(x-1)x(mod 2)$; $d=5(mod 8)\iff x^2-x+\frac{1-d}{4}(mod 2)$ is irreducible. $pS=\begin{cases} (p,\sqrt{d})(p,\sqrt{d}-1) & ,\ \text{if } d\equiv 1(mod 8) \\ \text{still prime} & ,\ \text{if } d\equiv 5(mod 8) \end{cases}$

Example 2.6.

$\mathbb{Z}[\zeta_5]=\mathbb{Z}[\zeta_5-1]$ is the ring of integers of $\mathbb{Q}(\zeta_5)$, the minimal polynomial of ζ_5-1 is $x^4+5x^3+10x^2+10x+5$, hence $5\mathbb{Z}[\zeta_5]=(5,\zeta_5-1)^4$, in general, $p\mathbb{Z}[\zeta_p]=(p,\zeta_p-1)^{p-1}$ for prime number p.

Example 2.7 (Eisenstein extension).

Let R be a Dedekind domain, $\mathfrak{p}$ be a nonzero prime ideal of R, for $a\in R$ we define $ord_{\mathfrak{p}}(a)=ord_{\mathfrak{p}}(aR)$.

First we note that

(*) if $a_1+\cdots+a_t=0$ with $a_i\in R$ then the minimum value of $ord_{\mathfrak{p}}(a_i)$ must be attained for at least two i's.

Now assume that R is a Dedekind domain with fractional field K, $f=X^n+a_1X^{n-1}+\cdots+a_n\in R[X]$ is an Eisenstein polynomial for $\mathfrak{p}$ nonzero ideal of R(i.e. $ord_{\mathfrak{p}}(a_i)\geq 1$, $ord_{\mathfrak{p}}(a_n)=1$). Let α be a root of f, S be integral closure of R in $K(\alpha)$. Then $\alpha\in S$ and $\mathfrak{p}S=\mathfrak{P}^e\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_t^{e_t}$ with $e\leq[K(\alpha):K]=m\leq n$.

$$\begin{cases} 0 &= \alpha^n+a_1\alpha^{n-1}+\cdots+a_n \\ ord_{\mathfrak{P}}(\alpha^n) &= n ord_{\mathfrak{P}}(\alpha) \\ ord_{\mathfrak{P}}(a_i\alpha^{n-i}) &\geq (n-i)ord_{\mathfrak{P}}(\alpha)+e, (1\leq i<n) \\ ord_{\mathfrak{P}}(a_n) &= e \end{cases}$$

By (*), we have $ord_{\mathfrak{P}}(\alpha^n)\geq 1$, $ord_{\mathfrak{P}}(\alpha)\geq 1$. Again by (*), the minimum value must be e and $ord_{\mathfrak{P}}(\alpha^n)=e\leq m\leq n$. Hence $ord_{\mathfrak{P}}(\alpha)=1, n=m=e$, and $\mathfrak{p}S=\mathfrak{P}^e$ since $m=ef+e_1f_1+\cdots+e_tf_t$. $ord_{\mathfrak{P}}(\alpha)=1$ also implies that $(\mathfrak{p},\alpha)=\mathfrak{p}S+\alpha S=\mathfrak{P}^e+\mathfrak{P}^1\mathfrak{P}_1^{s_1}\cdots\mathfrak{P}_t^{s_t}=\mathfrak{P}$.

Conversely, assume $[K:L]=m$, S is the integral closure of R in L, $\mathfrak{p}$ is a nonzero ideal of R, $\mathfrak{p}S=\mathfrak{P}^m, \alpha\in S$ and $ord_{\mathfrak{P}}(\alpha)=1$. Let $f=X^n+a_1X^{n-1}+\cdots+a_n\in R[X]$ be the minimal polynomial of α over K, so $n\leq[L:K]=m$

$$\begin{cases} 0 & = \alpha^n + a_1\alpha^{n-1} + \cdots + a_n \\ ord_{\mathfrak{P}}(\alpha^n) & = nord_{\mathfrak{P}}(\alpha) = n \leq m \\ ord_{\mathfrak{P}}(a_i\alpha^{n-i}) & = n - i + ord_{\mathfrak{P}}(a_i) = n - i + mord_{\mathfrak{p}}(a_i), (1 \leq i < n) \\ ord_{\mathfrak{P}}(a_n) & = mord_{\mathfrak{p}}(a_n) \end{cases}$$

Note that $m \geq n, 1 \leq i < n, ord_{\mathfrak{P}}(a_i\alpha^{n-i})$ cannot equal to each other for different i (**). (*) implies $ord_{\mathfrak{P}}(a_n) > 0$, then $ord_{\mathfrak{p}}(a_n) \geq 1$, $ord_{\mathfrak{P}}(a_n) \geq m$. If $ord_{\mathfrak{p}}(a_n) > 1$ we obtain a contradiction by (*) and (**), so $ord_{\mathfrak{p}}(a_n) = 1$. Similarly, $m > n$ also implies contradiction, so $m = n$. Hence the minimum value must be m, $ord_{\mathfrak{p}}(a_i) > 0, (1 \leq i < n)$, f is Eisenstein polynomial, and $[K(\alpha) : K] = n = m = [L : K], L = K(\alpha)$.

Remark 2.8. In the example above, it is not necessary that $S = R[\alpha]$, if so the decomposition of $\mathfrak{p}$ follows directly from the previous theorem. For example, $\mathbb{Q}(\sqrt{5})/\mathbb{Q}, \mathbb{Z}[\frac{1+\sqrt{5}}{2}] \supsetneq \mathbb{Z}[\sqrt{5}] \supseteq \mathbb{Z}$ with $\alpha = \sqrt{5}$.

References

[1] J.S.Milne. *Algebraic Number Theory.*

[2] K.Q.Feng. *Basic Commutative Algebra*. publisher: forgotten, Chinese edition.

[3] L.C.Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, 1996.

Institute of Mathematics, Academy of Mathematics and System Sciences, Chinese Academy of Sciences

E-mail address: yongqi_liang@amss.ac.cn