剩余符号与Hilbert符号

Lh

2021 年 8 月 24 日

目录

1 数域中的剩余符号

该部分主要参考[6].

在初等数论中，我们知道整数环$\mathbb{Z}$中有二次剩余符号：设$p \in \mathbb{Z}$是奇素数，$a \in \mathbb{Z}$,若$p \nmid a$,则有

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow x^2 \equiv a \ mod \ p\text{有整数解}.$$

对于二次互反律，我们有Eular判别法:设p是素数，$(a,p)=1$,则有

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ mod \ p.$$

Gauss首先证明下面互反律：设p,q为不同的奇素数，则有

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

利用该互反律我们可以很容易计算一些二次剩余符号,例如：

$$\left(\frac{5}{17}\right) = \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

下面我们说明二次互反律存在统一的推广。

1.1 基本定义及性质

设k是一个数域，$\mathcal{O}_k$是k的代数整数环。$\mathfrak{p}$是一个$\mathcal{O}_k$中素理想，则$N_{k|\mathbb{Q}}(\mathfrak{p})=p^f$,其中$f$是剩余类域$(\mathcal{O}_k/\mathfrak{p})/(\mathbb{Z}/p\mathbb{Z})$的扩张次数。下令$q=p^f$。对于任意$\mathcal{O}_k$中元素$\alpha\notin\mathfrak{p}$(即$\alpha$与$\mathfrak{p}$互素),有

$$\alpha^{q-1}\equiv 1\ mod\ \mathfrak{p}.$$

Lemma 1.1. *若k中包含n次单位根ξ_n，且素理想$\mathfrak{p}$与n互素，则$\xi_n\ mod\ \mathfrak{p}$在$(\mathcal{O}_k/\mathfrak{p})^*$中生成的子群阶为$n$.*

证明. (1)若n是素数幂，因n与$\mathfrak{p}$互素，$n\notin\mathfrak{p}\cap\mathbb{Z}=(p)$.设$n=l^r$,其中$l$是素数，且$(l,p)=1$. K中包含分圆域$\mathbb{Q}(\xi_{l^r})$,若$1-\xi_{l^r}\in\mathfrak{p}$,则

$$l\in(1-\xi_{l^r})\mathcal{O}_k\subseteq\mathfrak{p}.$$

与$(l,p)=1$矛盾！类似的，对于任意$1\le a<l^r$,可证明若$1-\xi_{l^r}^a\in\mathfrak{p}$，则$l\in(1-\xi_{l^r}^a)\mathcal{O}_k\subseteq\mathfrak{p}$.矛盾！从而$1-\xi_{l^r}^a\notin\mathfrak{p}$,由此可知$l^r$次单位根模$\mathfrak{p}$两两不同余。 (2)若$n$不是素数幂，即$n$中至少包含两个不同的素因子，且$(p,n)=1$，则$1-\xi_n$是单位。对于$1\le a<n$,若$n=am$,其中$m$有两个不同的素因子，则$1-\xi_n^a$仍是单位，若$m$是素数幂，由(1)仍有$1-\xi_n^a\notin\mathfrak{p}$.

综上，当n与$\mathfrak{p}$互素时，对任意$1\le a<n$，总有$1-\xi_n^a\notin\mathfrak{p}$成立，从而$n$次单位根模$\mathfrak{p}$两两不同余 □

因此$n||(\mathcal{O}_k/\mathfrak{p})^*|=q-1$.于是$\alpha^{\frac{q-1}{n}}$是$(\mathcal{O}_k/\mathfrak{p})^*$中一个$n$次单位根:即存在唯一($(\mathcal{O}_k/\mathfrak{p})^*$是循环群,$n$次单位根模$\mathfrak{p}$两两不同余)的$n$次单位根,记为$(\frac{\alpha}{\mathfrak{p}})$，使得

$$\alpha^{\frac{q-1}{n}}\equiv\left(\frac{\alpha}{\mathfrak{p}}\right)\ mod\ \mathfrak{p}.$$

称符号$(\frac{\alpha}{\mathfrak{p}})$为$k$中$n-$次剩余符号。回顾$\mathbb{Z}$上二次剩余符号,当时我们称上述同余式为欧拉判别法。上述符号中可将$\mathfrak{p}$替换称任意与n互素的理想$\mathfrak{a}$:设$\mathfrak{a}=\prod\mathfrak{p}$为素理想分解，规定 $(\alpha/\mathfrak{a})=\prod(\alpha/\mathfrak{p})$。像整数环中二次剩余那样，对一般的$n$次剩余，有下面类似的性质

Proposition 1.1. *([6]Proposition 4.1)设k是包含n次本原单位根ξ_n的代数数域,$\mathfrak{p}$是$\mathcal{O}_k$的素理想，则有：*

i) 若$\alpha\equiv\beta\ mod\ \mathfrak{p}$,则$(\frac{\alpha}{\mathfrak{p}})=\left(\frac{\beta}{\mathfrak{p}}\right)$;

ii) $\frac{\alpha}{\mathfrak{p}}=1$当且仅当$\alpha$是模$\mathfrak{p}$ n次剩余，即当且仅当存在$\xi\in\mathcal{O}_k-\mathfrak{p}$使得$\alpha\equiv\xi^n\ mod\ \mathfrak{p}$;

iii) 设素数$p\equiv 1\ mod\ m$,$a\in\mathbb{Z}$是模p m-次剩余当且仅当对于$\mathbb{Q}(\xi_m)$中任何在p上的素理想$\mathfrak{p}$都有$(\frac{a}{\mathfrak{p}})$.

下面命题是考虑域扩张之间的剩余符号的关系。

Proposition 1.2. *([6]Prop4.2)设K/F是正规扩张，Galois群为G，k/F是其子扩张，且$\xi_n\in k$.则*

i) 对于每个$\sigma\in G$，任意的$\alpha\in K^*$,和与n互素的理想$\mathfrak{a}$，我们有$\left(\frac{\alpha}{\mathfrak{a}}\right)_K^\sigma=\left(\frac{\alpha^\sigma}{\mathfrak{a}^\sigma}\right)_K$.

ii) 若$\mathfrak{p}$在域扩张K/k上一个素理想为$\mathfrak{P}$,且$f(\mathfrak{P}/\mathfrak{p})=1$,则对任意 $\alpha\in\mathcal{O}_k$,有$\left(\frac{\alpha}{\mathfrak{P}}\right)_K=\left(\frac{\alpha}{\mathfrak{p}}\right)_k$.

iii) 若$K|k$是$Abel$扩张，$\mathfrak{p}$是$\mathcal{O}_K$中一个素理想，$N=N_{K|k}$表示相对范数，则对任意$\alpha\in\mathcal{O}_k$,有$\left(\frac{\alpha}{\mathfrak{p}}\right)_K=\left(\frac{N\alpha}{\mathfrak{p}}\right)_k$.

iv) 设$K|k$是次数为n的循环扩张，设存在$\mathcal{O}_k$中素理想$\mathfrak{p}$使得$\mathfrak{p}\nmid n\mathcal{O}_k$且$\mathfrak{p}$在$K|k$扩张下是完全分歧的，即$\mathfrak{p}\mathcal{O}_K=\mathfrak{P}^n$。则 $\left(\frac{N_{K|k}\alpha}{\mathfrak{p}}\right)_k=1$对任意$\alpha\in\mathcal{O}_K-\mathfrak{P}$成立。

证明. ii)设$\mathfrak{P}$是$\mathcal{O}_K$中一个在$\mathfrak{p}$上的素理想，$f(\mathfrak{P}/\mathfrak{p})=1$,则$N(\mathfrak{P})=N(\mathfrak{p})=q$.因此

$$\left(\frac{\alpha}{\mathfrak{P}}\right)_K\equiv\alpha^{\frac{q-1}{n}}\ mod\,\mathfrak{P}\ \ and\ \ \left(\frac{\alpha}{\mathfrak{p}}\right)_k\equiv\alpha^{\frac{q-1}{n}}\ mod\,\mathfrak{p}.$$

由此有

$$\left(\frac{\alpha}{\mathfrak{P}}\right)_K\equiv\left(\frac{\alpha}{\mathfrak{p}}\right)_k\ mod\,\mathfrak{P}.$$

前面已说明若n与$\mathfrak{P}$互素，则n次单位根模$\mathfrak{P}$两两不同余，从而由上面同余式知$\left(\frac{\alpha}{\mathfrak{P}}\right)_K=\left(\frac{\alpha}{\mathfrak{p}}\right)_k$. □

数域中n次剩余符号也可由$Artin$符号给出。

首先回顾赋值扩张的一些结论(见[1] Chapter II,section 8)：设$K|k$是数域的扩张，$\mathfrak{p}$表示$\mathcal{O}_k$中任意一个素理想，设$\mathfrak{p}$在k上决定的赋值为ν,k_ν是k关于ν的完备化。则v到K上的赋值延拓完全由$\mathfrak{p}$上$\mathcal{O}_K$中的素理想决定。事实上，设$\mathfrak{p}\mathcal{O}_K=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$,则$v$的所有延拓恰为 $\omega_i=\frac{1}{e_i}v_{\mathfrak{P}_i},i=1\cdots,g$. 且$[K_{\omega_i}:k_\nu]=e_if_i$,其中$e_i=e(\mathfrak{P}_i|\mathfrak{p})=e(\mathfrak{P}_{\omega_i}|\mathfrak{p}_v)$, $f_i=f(\mathfrak{P}_i/\mathfrak{p})=f(\mathfrak{P}_{\omega_i}|\mathfrak{p}_v)$。其中$\mathfrak{P}_{\omega_i},\mathfrak{p}_v$分别为局部域$K_{\omega_i},k_v$中唯一的素理想。若$K|k$是Galois扩张，则$k$中任意素理想$\mathfrak{p}$的分歧指数$e(\mathfrak{P}_i|\mathfrak{p})$相同。若想说明$\mathfrak{p}$在域扩张$K|k$下是非分歧的，只需证明任一局部域扩张$K_{\omega_i}|k_v$是非分歧扩张。

设k是包含$n-$次本原单位根ζ_n的数域。$\mathfrak{p}$表示$\mathcal{O}_k$中任意一个素理想，设$\mathfrak{p}$在k上决定的赋值为ν, k_ν是k关于ν的完备化。$\alpha\in k^*$,令$K=k(\sqrt[n]{\alpha})$, 用S表示k的所有阿基米德素除子和k中所有整除n的非阿基米德素除子组成的集合。若$a_1,\cdots,a_r\in k*$,用$S(a_1,\cdots,a_r)$表示S与

$$S'(a_1,\cdots,a_r)=\{\ v\ |\text{存在某个指标i,}1\le i\le r,v(a_i)\neq 0,v\text{是k的素除子}\}$$

的并集。对于$a\in k^*$,用$I^{S(a)}$表示k的所有与$S(a)$中有限素除子(即素理想)互素的k的分式理想的全体。显然若$\mathfrak{p}\in I^{S(a)}$,则$\mathfrak{p}\nmid n\alpha$.

下面就取定这样一个素理想$\mathfrak{p}$,则 $\mathfrak{p}$在$K|k$上非分歧：只需说明 $k_\nu(\sqrt[n]{\alpha})|k_\nu$是非分歧扩张，由于$\mathfrak{p}\nmid\alpha$, $\nu(\alpha)=0$,从而α是$\mathcal{O}_{k_\nu}$中单位，又因$\mathfrak{p}\nmid n$,设$N_{k|\mathbb{Q}}\mathfrak{p}=p^f$,则$(n,p)=1$,即 n与$\mathcal{O}_{k_\nu}$的剩余类域特征互素，由[1]中 ChapterV,section3中lemma 3.3知$k_\nu(\sqrt[n]{\alpha})|k_\nu$是非分歧扩张。

对于满足$\mathfrak{p}\nmid n\alpha$的素理想$\mathfrak{p}$，我们断言

$$\left(\frac{K|k}{\mathfrak{p}}\right)\sqrt[n]{\alpha}=\left(\frac{\alpha}{\mathfrak{p}}\right)_k\sqrt[n]{\alpha}.$$

证明. 取K中一个在$\mathfrak{p}$上的素理想$\mathfrak{P}$,$K|k$是循环扩张，由Artin符号定义

$$\left(\frac{K|k}{\mathfrak{p}}\right)\sqrt[n]{\alpha}\equiv(\sqrt[n]{\alpha})^{N\mathfrak{p}}\ mod\ \mathfrak{P},$$

而右侧$\left(\frac{\alpha}{\mathfrak{p}}\right)_k\sqrt[n]{\alpha}\equiv\alpha^{(N\mathfrak{p}-1)/n}\sqrt[n]{\alpha}\ mod\ \mathfrak{P}$.由此

$$\left(\frac{K|k}{\mathfrak{p}}\right)\sqrt[n]{\alpha}\equiv\left(\frac{\alpha}{\mathfrak{p}}\right)_k\sqrt[n]{\alpha}\ mod\ \mathfrak{P}.$$

设$\left(\frac{K|k}{\mathfrak{p}}\right)\sqrt[n]{\alpha}=\zeta\sqrt[n]{\alpha}$,其中$\zeta$是某个n次单位根。$\mathfrak{p}\nmid\alpha\Rightarrow\mathfrak{P}\nmid\sqrt[n]{\alpha}$,故上一同余式可导出，

$$\zeta\equiv\left(\frac{\alpha}{\mathfrak{p}}\right)_k\ mod\ \mathfrak{P}.$$

类似前文，该同余实为相等.由此得到断言成立。 □

1.2 例

Example 1.1. $\mathbb{Z}$中二次剩余符号.默认已被读者熟悉,这里不再赘述。

Example 1.2. *Gauss*整数环$\mathbb{Z}[i]$中二次剩余.2在域扩张$\mathbb{Q}(i)|\mathbb{Q}$下是分歧的，$2=(1+i)(1-i)=i^3(1+i)^2$,其中$1+i$是$\mathbb{Z}[i]$中素元。设$\pi=a+bi,\lambda=c+di$是两个不同的素元，且$\pi\equiv\lambda\equiv1\ mod\ 2$(从而与$1+i$互素)。用$\left[\frac{\cdot}{\cdot}\right]$表示$\mathbb{Z}[i]$中二次剩余符号，则有

$$\left[\frac{\pi}{\lambda}\right]=\left[\frac{\lambda}{\pi}\right].$$

作为补充律，有

$$\left[\frac{i}{a+bi}\right]=(-1)^{b/2},\left[\frac{1+i}{a+bi}\right]=\left(\frac{2}{a+b}\right).$$

其中$\left(\frac{\cdot}{\cdot}\right)$表示$\mathbb{Z}$中二次剩余符号(证明见[6]Chapter5,Proposition5.1).

Example 1.3. $\mathbb{Z}$中四次剩余.用$\left(\frac{\cdot}{\cdot}\right)_4$表示$\mathbb{Z}$中四次剩余符号。对于素数$p\equiv3\ mod\ 4$，因$\left(\frac{-1}{p}\right)=-1$,易证得对于与$p$互素的整数$a\in\mathbb{Z}$

$$\left(\frac{a}{p}\right)_4=1\Leftrightarrow\left(\frac{a}{p}\right)=1.$$

上面等价号右侧表示二次剩余，左侧表示四次剩余。故四次剩余一般是研究$\equiv1\ mod\ 4$的素数p。注意到若$\left(\frac{a}{p}\right)=1$,则$\left(\frac{a}{p}\right)_4$取值为$\pm1$.下设素数$p\equiv1\ mod\ 4$. 关于$\mathbb{Z}$上的四次剩余符号$\left(\frac{\cdot}{p}\right)_4$，有如下一些结果：

- ([6]Proposition5.3)设$p\equiv1\mod 4$是素数，令i是满足$i\equiv b/a\ mod\ p$的整数。则

$$\left(\frac{2}{p}\right)_4\equiv i^{\frac{ab}{2}}\ (mod\ p).$$

- ([6]Propositio 5.4)令$p=a^2+b^2=c^2+2d^2=e^2-2f^2=8n+1$是素数,假设$b$是偶数。则

$$\left(\frac{2}{p}\right)_4=(-1)^{b/4}=\left(\frac{2}{c}\right)=(-1)^{n+d/2}=\left(\frac{-2}{e}\right).$$

- ([6]Propositio 5.5)设$p=a^2+b^2,q$是两个素数，且$\left(\frac{q}{p}\right)=1$,假设$2|b$.令$\sigma$是同余式$\sigma^2\equiv p \mod q$的一个解，则

$$\left(\frac{q^*}{p}\right)_4=\left(\frac{\sigma(b+\sigma)}{q}\right).$$

这里$q^*=(-1)^{\frac{q-1}{2}}q$.

- 设$p=a^2+b^2$,$q=c^2+d^2$是素数，其中b,d是偶数且$\left(\frac{p}{q}\right)=1$,则

$$\left(\frac{q}{p}\right)_4\equiv\left(\frac{a/b-c/d}{a/b+c/d}\right)^{\frac{q-1}{4}} \mod q.$$

另有几个等价公式，请看[6]第五章。

Example 1.4. *Gauss*整数环中四次剩余。称$\mathbb{Z}[i]$中满足$\alpha\equiv 1 \mod (1+i)^3$的非单位元为准素元.用$\left[\frac{\cdot}{\cdot}\right]_4$表示$\mathbb{Z}[i]$中四次剩余符号($\mathbb{Z}[i]$中四次剩余符号在不同文献中写法不同，例如在[6]中第6.3节，仍用$\left[\frac{\cdot}{\cdot}\right]$表示$\mathbb{Z}[i]$中四次剩余符号。请读者注意区分)，则有性质

- 设π是$\mathbb{Z}[i]$中奇素数(即$N(\pi)$是$\mathbb{Z}$中奇素数),则

$$\left[\frac{\alpha\beta}{\pi}\right]_4=\left[\frac{\alpha}{\pi}\right]_4\left[\frac{\beta}{\pi}\right]_4,\forall\alpha,\beta\in\mathbb{Z}[i].$$

$$\left[\frac{\overline{\alpha}}{\overline{\pi}}\right]_4=\overline{\left[\frac{\alpha}{\pi}\right]_4}=\left[\frac{\alpha}{\pi}\right]_4^{-1},$$

这里上划线表示复共轭。

- 互反律: 如果π和λ是$\mathbb{Z}[i]$中两个不同的准素素数，则有

$$\left[\frac{\lambda}{\pi}\right]_4=\left[\frac{\pi}{\lambda}\right]_4(-1)^{(N(\lambda)-1)(N(\pi)-1)/16}.$$

作为补充律有:

$$\left[\frac{i}{\pi}\right]_4=i^{-(a-1)/2}$$

$$\left[\frac{1+i}{\pi}\right]_4=i^{(a-b-1-b^2)/4}.$$

这里a,b满足$\pi=a+bi$(证明见[6]6.3节或[7]9.9节).

关于进一步的性质，请看[6].

我们用一个例子说明$\mathbb{Z}$中四次剩余符号和$\mathbb{Z}[i]$中四次剩余符号是不同的。在$\mathbb{Z}$中，用欧拉判别法

$$\left(\frac{2}{17}\right)_4 \equiv 2^{\frac{17-1}{2}} = 16\ mod\ 17$$

故$\left(\frac{2}{17}\right)_4 = -1$. 而在$\mathbb{Z}[i]$中 $17 = (1+4i)(1-4i)$是准素分解($p \equiv 1\ mod\ 4$的素数都有准素分解)，故

$$\left[\frac{2}{17}\right]_4 = \left[\frac{2}{1+4i}\right]_4 \left[\frac{2}{1-4i}\right]_4 = \left[\frac{2}{1+4i}\right]_4 \left[\frac{2}{1+4i}\right]_4^{-1} = 1.$$

2 Hilbert符号

该部分的定理及命题主要参考[1].

2.1 定义

下设K是局部域，或$K=\mathbb{R}, K=\mathbb{C}$. 假设$K$中包含$n$次单位根群$\mu_n$,这里$n$与$K$的特征互素(若$char(K)=0$,对$n$没有要求). 是由Kummer理论$L=K(\sqrt[n]{K^*})$是$K$的指数为$n$的极大Abel扩张。且可证得([1]Chapter V,Proposition1.5)

$$N_{L|K}L^* = K^{*n},$$

由此，局部类域论给出同构

$$K^*/K^{*n} \cong G(L|K), \tag{1}$$

同构由$a \mapsto (a, L|K)$给出。这里我们简写$Gal(L|K)$为$G(L|K)$,下文亦是如此。

另一方面，通过Kummer配对，我们有同构

$$K^*/K^{*n} \cong Hom(G(L|K), \mu_n), \tag{2}$$

同构由

$$a \mapsto \varphi_a : \chi \mapsto \frac{\chi(\sqrt[n]{a})}{\sqrt[n]{a}}$$

给出。

我们想把上面两个同构联系起来。为此考虑双线性映射

$$G(L|K) \times Hom(G(L|K), \mu_n) \to \mu_n, \quad (\sigma, \chi) \mapsto \chi(\sigma), \tag{3}$$

该配对是非退化的:若对任意$\sigma \in G(L|K), \chi(\sigma)=1$,则自然有$\chi = 1$.反之，若对任意

$$\chi \in Hom(G(L|K), \mu_n), \quad \chi(\sigma) = 1.$$

若$\sigma \neq 1$,记σ生成的子群为$<\sigma>$,则$\chi \in Hom(G(L|K)/<\sigma>, \mu_n)$,考虑阶数

$$|G(L|K)| = |Hom(G(L|K), \mu_n)| < |Hom(G(L|K)/<\sigma>, \mu_n)| = |G(L|K)/<\sigma>|,$$

显然这是不可能的，矛盾！故$\sigma = 1$.

现在我们利用上面(1),(2)和(3)，便可得到一个双线性配对，

$$\left(\frac{\ ,\ }{\mathfrak{p}}\right): K^*/K^{*n} \times K^*/K^{*n} \longrightarrow \mu_n, \tag{$*$}$$

这里$\mathfrak{p}$是局部域K的唯一的素理想，上述映射元素对应为

$$\left(\frac{a,b}{\mathfrak{p}}\right) = \frac{(a, L|K)\sqrt[n]{b}}{\sqrt[n]{b}}.$$

这里注意到，我们取定$(*)$式中的第一个$K^*/K^{*n} \cong G(L|K)$,而第二个K^*/K^{*n}是同构于$Hom(G(L|K), \mu_n)$(一些文献可能会恰好相反)。上述符号$\left(\frac{\ ,\ }{\mathfrak{p}}\right)$称为*Hilbert*符号. 关于Hilbert符号，有如下性质.

Proposition 2.1. *([1]Chapter V,Proposition 3.1)对于$a, b \in K^*$,Hilbrt符号$\left(\frac{a,b}{\mathfrak{p}}\right) \in \mu_n$满足*

$$(a, K(\sqrt[n]{b})|K)\sqrt[n]{b} = \left(\frac{a,b}{\mathfrak{p}}\right)\sqrt[n]{b}.$$

Proposition 2.2. 记号如上，

(i) $\left(\frac{aa',b}{\mathfrak{p}}\right) = \left(\frac{a,b}{\mathfrak{p}}\right)\left(\frac{a',b}{\mathfrak{p}}\right)$,

(ii) $\left(\frac{a,bb'}{\mathfrak{p}}\right) = \left(\frac{a,b}{\mathfrak{p}}\right)\left(\frac{a,b'}{\mathfrak{p}}\right)$,

(iii) $\left(\frac{a,b}{\mathfrak{p}}\right) = 1 \Leftrightarrow a$是域扩张$K(\sqrt[n]{b})|K$的一个范,

(iv) $\left(\frac{a,b}{\mathfrak{p}}\right) = \left(\frac{b,a}{\mathfrak{p}}\right)^{-1}$,

(v) $\left(\frac{a,1-a}{\mathfrak{p}}\right) = \left(\frac{a,-1}{\mathfrak{p}}\right) = 1$,

(vi) 若对任意$b \in K^*$,有$\left(\frac{a,b}{\mathfrak{p}}\right) = 1$，则$a \in K^{*n}$.

2.2 例

下面给出Hilbert符号的一个应用。

Example 2.1. 令$F = \mathbb{Q}(\sqrt{2}, i), L = \mathbb{Q}(\sqrt{2}, \sqrt{p_1p_2}, i)$,其中$p_1, p_2$是奇素数，且$p_1 \equiv p_2 \equiv 5\ mod\ 8$.判断$F$的基本单位$\varepsilon_2 = 1+\sqrt{2}$和$\sqrt{i}$是否是$L$中元素的范.这里$i^2 = -1$.

注意到$L|F$是二次扩张，从而是循环扩张。对于循环扩张，我们有Hesse Norm定理([1]Chapter VI,Corollary4.5)

Theorem 2.1. *(Hesse Norm Theorem)设$L|K$是循环扩张，则$x \in K^*$是L中元素的范当且仅当它是每一个局部域扩张 $L_{\mathfrak{P}}|K_{\mathfrak{p}}(\mathfrak{P}|\mathfrak{p})$的一个元素的范.*

回到例子中，我们只需判断$\varepsilon_2,\sqrt{i}$是否是局部范. 注意到$L=F(\sqrt{p_1p_2})$,由上面第二个命题的(iii),我们需要对$\mathcal{O}_F$中每个素理想$\mathfrak{p}$,在F关于$\mathfrak{p}$的完备化$F_\mathfrak{p}$中计算$\left(\frac{\varepsilon_2,p_1p_2}{\mathfrak{p}}\right),\left(\frac{\sqrt{i},p_1p_2}{\mathfrak{p}}\right)$.

为此，设$\mathfrak{p}$是F中不在2(2在F上惯性)上的素理想，$\left(\frac{\cdot}{\mathfrak{p}}\right)$表示2−次Hiilbert符号，即定义中的$n$取2. 分下面几种情形进行计算:

(1) 若$\mathfrak{p}$不在p_1,p_2上，则$v_\mathfrak{p}(\varepsilon_2)=v_\mathfrak{p}(p_1p_2)=v_\mathfrak{p}(\sqrt{i})=0$,从而$\left(\frac{p_1p_2,\varepsilon_2}{\mathfrak{p}}\right)=\left(\frac{p_1p_2,\sqrt{i}}{\mathfrak{p}}\right)=1.$

(2) 若$\mathfrak{p}$为p_1上素理想,则$v_\mathfrak{p}(\varepsilon_2)=v_\mathfrak{p}(\sqrt{i})=0$,$F|\mathbb{Q}$有三个中间域，$p_1$在上面均非分歧，从而$p_1$在$F|\mathbb{Q}$上非分歧,故$v_\mathfrak{p}(p_1p_2)=v_\mathfrak{p}(p_1)=1$.因2-次Hilbert符号只取值$\pm1$,Hilbert符号是关于两个变量$a,b$对称的，为简记，对任意域$E$,用$\widehat{E}$表示$E(\sqrt{E^*})$. 下面推理需用下述命题

Proposition 2.3. *([1]Chapter IV,Proposition6.4)若$L|K,L'|K'$是有限Galois扩张，$K\subseteq K',L\subseteq L'$,令$\sigma\in G$,则有下述交换图*

$$\begin{array}{ccc} K'^* & \xrightarrow{(\ ,L'|K')} & G(L'|K')^{ab} \\ \downarrow{\scriptstyle N_{K'|K}} & & \downarrow{\scriptstyle res} \\ K^* & \xrightarrow{(\ ,L|K)} & G(L|K)^{ab} \end{array}$$

这里res表示限制映射.

下面开始计算Hilbert符号.

$$\left(\frac{p_1p_2,\varepsilon_2}{\mathfrak{p}_F}\right)=\left(\frac{p_1,\varepsilon_2}{\mathfrak{p}_F}\right)=\left(\frac{\varepsilon_2,p_1}{\mathfrak{p}_F}\right)=\frac{(\varepsilon_2,\widehat{F_\mathfrak{p}}|F_\mathfrak{p})\sqrt{p_1}}{\sqrt{p_1}}$$

$$=\frac{(N_{F_\mathfrak{p}|\mathbb{Q}_\mathfrak{p}(\sqrt{2})}(\varepsilon_2),\widehat{\mathbb{Q}_\mathfrak{p}(\sqrt{2})}|\mathbb{Q}_\mathfrak{p}(\sqrt{2}))\sqrt{p_1}}{\sqrt{p_1}}$$

p_1在$\mathbb{Q}(\sqrt{2})$中是惯性的，这里$\mathbb{Q}_\mathfrak{p}(\sqrt{2})$表示$\mathbb{Q}(\sqrt{2})$关于$p_1$上唯一素理想$\mathfrak{p}_{\mathbb{Q}(\sqrt{2})}$的完备化。因此

$$[\mathbb{Q}_\mathfrak{p}(\sqrt{2}):\mathbb{Q}_\mathfrak{p}]=e(\mathfrak{p}_{\mathbb{Q}(\sqrt{2})}/p_1)f(\mathfrak{p}_{\mathbb{Q}(\sqrt{2})}/p_1)=1,$$

故$F_\mathfrak{p}=\mathbb{Q}_\mathfrak{p}(\sqrt{2},i)=\mathbb{Q}_\mathfrak{p}(\sqrt{2})$.从而上式

$$=\frac{(\varepsilon_2,\widehat{\mathbb{Q}_\mathfrak{p}(\sqrt{2})}|\mathbb{Q}_\mathfrak{p}(\sqrt{2}))\sqrt{p_1}}{\sqrt{p_1}}=\frac{(-1,\widehat{\mathbb{Q}_{p_1}}|\mathbb{Q}_{p_1})\sqrt{p_1}}{\sqrt{p_1}}=\left(\frac{p_1,-1}{p_1}\right)$$

注意到Hilbert符号在一定条件下转化为n-次剩余符号: 一般地，设局部域K的剩余类域特征为p,且$(p,n)=1$,这里n是指最开始定义中K中包含n次单位根群。因$U_K=\mu_{q-1}\times U_K^{(1)}$，每个单位$u\in U_K$存在唯一分解

$$u=\omega(u)<u>$$

其中$\omega(u)\in\mu_{q-1},<u>\in U_K^{(1)}$.设$\pi$是$K$的任意一致化子，即$(\pi)=\mathfrak{p}$,则n-次Hilbert符号([1]Chapter V,Proposition 3.4)

$$\left(\frac{\pi,u}{\mathfrak{p}}\right)=\omega(u)^{(q-1)/n}, \tag{4}$$

这里q是K的剩余类域中的元素个数。简记

$$\left(\frac{u}{\mathfrak{p}}\right) := \left(\frac{\pi, u}{\mathfrak{p}}\right) \ for \ \ u \in U_K.$$

且有如下命题

Proposition 2.4. *([1]Chapter V,Proposition 3.5)*若$(n,p)=1$且$u \in U_K$.则有

$$\left(\frac{u}{\mathfrak{p}}\right) = 1 \Leftrightarrow u\text{是}mod\ \mathfrak{p}\text{的}n\text{次幂元}.$$

由此,在$\mathbb{Q}_{p_1}$中

$$\left(\frac{p_1,-1}{p_1}\right) = \begin{cases} 1 & \text{-1 是}\mathbb{Z}_\mathfrak{p}/p\mathbb{Z}_\mathfrak{p}\text{中平方元} \\ -1 & \text{-1 不是}\mathbb{Z}_\mathfrak{p}/p\mathbb{Z}_\mathfrak{p}\text{中平方元} \end{cases}$$

因$\mathbb{Z}_\mathfrak{p}/p\mathbb{Z}_\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$上述恰为二次剩余的性质。故最终有

$$\left(\frac{p_1p_2,\varepsilon_2}{\mathfrak{p}_F}\right) = \left(\frac{-1}{p_1}\right) = 1(p_1 \equiv 5\ mod\ 8).$$

同样地,

$$\left(\frac{p_1p_2,\sqrt{i}}{\mathfrak{p}_F}\right) = \left(\frac{p_1,\sqrt{i}}{\mathfrak{p}_F}\right) = \left(\frac{\sqrt{i},p_1}{\mathfrak{p}_F}\right) = \frac{(\sqrt{i},\widehat{F_\mathfrak{p}}|F_\mathfrak{p})\sqrt{p_1}}{\sqrt{p_1}}$$

$$= \frac{(N_{F_\mathfrak{p}|\mathbb{Q}_\mathfrak{p}(i)}(\sqrt{i}),\widehat{\mathbb{Q}_\mathfrak{p}(i)}|\mathbb{Q}_\mathfrak{p}(i))\sqrt{p_1}}{\sqrt{p_1}},$$

因$\sqrt{i} = \frac{1}{\sqrt{2}}(1+i)$,故$N_{F_\mathfrak{p}|\mathbb{Q}_\mathfrak{p}}(i) = \frac{1}{\sqrt{2}}(1+i)\frac{-1}{\sqrt{2}}(1+i) = -i$,而$-1 = i^2 \in (\mathbb{Q}_\mathfrak{p}(i))^2$,于是上面等式

$$= \frac{(i^2 \cdot i,\widehat{\mathbb{Q}_\mathfrak{p}(i)}|\mathbb{Q}_\mathfrak{p}(i))\sqrt{p_1}}{\sqrt{p_1}} = \frac{(i,\widehat{\mathbb{Q}_\mathfrak{p}(i)}|\mathbb{Q}_\mathfrak{p}(i))\sqrt{p_1}}{\sqrt{p_1}}$$

$$= \left(\frac{p_1,i}{p_1}\right) = i^{\frac{p_1-1}{2}} = -1(p_1 \equiv 5\ mod\ 8).$$

上面倒数第二个等号是利用(4)式。

(3) 若$\mathfrak{p}$是p_2上素理想,则类似于(2),有$v_\mathfrak{p}(\varepsilon_2) = v_\mathfrak{p}(p_1p_2) = 1$,因此$\left(\frac{p_1p_2,\varepsilon_2}{\mathfrak{p}}\right) = \left(\frac{-1}{p_2}\right) = 1(p_2 \equiv 5\ mod\ 8)$.

我们尚未考虑F中在2上的素理想，但由*Hilbert*乘积公式: 对于任意$a,b \in F^*$,有

$$\prod_\mathfrak{p}\left(\frac{a,b}{\mathfrak{p}}\right) = 1.$$

故对于F上的每个素理想$\mathfrak{p}$,均有$\left(\frac{p_1p_2,\varepsilon_2}{\mathfrak{p}}\right) = 1$. 从而由Haees Norm Theorem ,$\varepsilon_2 \in N_{L|K}(L^*)$,因在(2)的计算中有$\left(\frac{p_1p_2,\sqrt{i}}{\mathfrak{p}}\right) = -1$,故有$\sqrt{i} \notin N_{L|K}(L^*)$.至此，我们完成了判断.

参考文献

[1] Neukirch.*Algebraic Number Theory.*

[2] 李文威.代数学方法(第一卷）.Vol,67.1.现代数学基础丛书.北京：高等教育出版社，2019.

[3] 张贤科.代数数论导引.

[4] Serge lang.*Algebra.*

[5] 冯克勤.代数数论.哈尔滨：哈尔滨工业大学出版社,2018.

[6] Franz Lemmermeyer.*Reciprocity Laws:From Euler to Eisenstein.*Springer Monographs in Mathematics.Springer,Berlin,2000.

[7] Rosen.*A classical Introduction to Modern Number Theory.* Graduate Texts in Mathematica;84.