学　　号：2017210481　　密　级：公开

合肥工業大學

Hefei University of Technology

本科毕业设计（论文）

UNDERGRADUATE THESIS

类　　型：	论文
题　　目：	二次域类群的结构以及算术应用
专业名称：	数学与应用数学
入学年份：	2017 级
学生姓名：	刘旭鸿
指导教师：	张神星
系 名 称：	应用数学系
完成时间：	2022 年 5 月

合　肥　工　业　大　学

本科毕业设计（论文）

二次域类群的结构以及算术应用

学生姓名：刘旭鸿

学生学号：2017210481

指导教师：张神星

专业名称：数学与应用数学

系 名 称：应用数学系

2022 年 5 月

A Dissertation Submitted for the Degree of Bachelor

The class groups of quadratic fields and their applications

By

Liu Xuhong

Hefei University of Technology

Hefei, Anhui, P.R.China

May, 2022

毕业设计（论文）独创性声明

本人郑重声明：所呈交的毕业设计（论文）是本人在指导教师指导下进行独立研究工作所取得的成果。据我所知，除了文中特别加以标注和致谢的内容外，设计（论文）中不包含其他人已经发表或撰写过的研究成果，也不包含为获得 合肥工业大学 或其他教育机构的学位或证书而使用过的材料。对本文成果做出贡献的个人和集体，本人已在设计（论文）中作了明确的说明，并表示谢意。

毕业设计（论文）中表达的观点纯属作者本人观点，与合肥工业大学无关。

毕业设计（论文）作者签名：刘旭鸿 签字日期：2022年 5 月 29 日

毕业设计（论文）版权使用授权书

本学位论文作者完全了解 合肥工业大学 有关保留、使用毕业设计（论文）的规定，即：除保密期内的涉密设计（论文）外，学校有权保存并向国家有关部门或机构送交设计（论文）的复印件和电子光盘，允许设计（论文）被查阅或借阅。本人授权 合肥工业大学 可以将本毕业设计（论文）的全部或部分内容编入有关数据库，允许采用影印、缩印或扫描等复制手段保存、汇编毕业设计（论文）。

（保密的毕业设计（论文）在解密后适用本授权书）

学位论文作者签名：刘旭鸿 指导教师签名：张神星

签名日期：2022年 5 月 29 日 签名日期：2022年 5 月 29 日

摘　要

数域的类群是代数数论的研究课题之一. 为了研究类群的结构, 我们需要它的初等因子中素数幂次的出现次数. 本文中我们将考虑二次域缩理想类群的 2-Sylow 子群的结构. 首先我们将回顾高斯型理论, 这包括高斯对于二次域 2 阶秩和 Rédei 对于二次域 4 阶秩的研究. 通过这些理论, 我们给出了一些情形下不同的二次域缩理想类群的 4 阶秩之间的关系, 并对 8 阶秩进行了一些探索研究.

关键词：类群；高斯型理论；Rédei 理论；希尔伯特符号；二次域

ABSTRACT

The ideal class groups of number fields play an important role in algebraic number theory. In order to study the structure of the class group, we need to know the multiplicities of prime powers as elementary divisors. In this paper, we want to study the 2-Sylow subgroups of the narrow class groups of quadratic fields. First we will review the Gauss genus theory, which includes Gauss's work on the 2-ranks and Rédei's work on the 4-ranks. Based on these theories, we will give a relation between the 4-ranks of different quadratic fields and some results on the 8-ranks.

KEYWORDS: Class groups; Gauss genus theory; Rédei theory; Hilbert symbols; Quadratic fields

目 录

符号说明

$\mathbb{Q}_v$	表示实数域 $\mathbb{R}$ 或 p 进数域 $\mathbb{Q}_p$, 见 § 2.1, § 2.5.
$(a,b)_v$	$\mathbb{Q}_v$ 上的希尔伯特符号, 见 § 2.2.
$[a,b]_v$	$\mathbb{Q}_v$ 上的加性希尔伯特符号, 见(3.2).
$\left(\frac{a}{b}\right)$	雅可比符号, 见 § 2.2.
$\left[\frac{a}{b}\right]$	加性雅可比符号, 见(3.3).
r_{2^a}	有限阿贝尔群的 2^a-秩, 见 § 2.7.
$h_{2^a}(m)$	数域 $\mathbb{Q}(\sqrt{m})$ 的缩理想类群的 2^a-秩, 见 § 2.7.
$\mathrm{Cl}(F)$	数域 F 的理想类群, 见 § 2.3.
$C(F)$	数域 F 的缩理想类群, 见 § 3.1.
$C(F)[2]$	表示 $C(F)$ 中阶不超过 2 的元素全体构成的子群.
$C(F)[4]$	表示 $C(F)$ 中阶整除 4 的元素全体构成的子群.
$\gcd(a,b)$	表示整数 a,b 的最大公因子.
$\mathbf{A}_{n'}$	表示一个与 n' 有关的矩阵, 见(3.4).
$\mathbf{D}_{\varepsilon}$	表示一个与 n' 和 ε 有关的矩阵, 见(3.5).
$\varepsilon(z),\omega(z)$	$U/U_3 \to \mathbb{Z}/2\mathbb{Z}$ 的同态, 具体定义见(2.1), (2.2).

1 简介

1.1 背景介绍

希尔伯特在著名的《数论报告》前言的一开始就写出:“数论是最古老的数学分支之一. 人们很早就注意到自然数具有一些相当深刻的性质. 但是数论作为一门完全独立系统的科学则是现代研究的成果. ”人类在文字产生之前便在日常的生产和生活实践中创建了整数的概念. 三千多年前, 四大文明古国（埃及、巴比伦、印度、中国）开始研究整数的各种性质以及方程的整数解和有理数解, 由此便产生了数论. 代数数论的发源可以追溯到丢番图方程的发现, 丢番图方程的命名是因为 3 世纪的古希腊数学家丢番图对它的研究. 一个典型的丢番图问题是去找两个整数 x, y 使得它们的和和它们的平方和等于给定的两个整数 A, B, 即

$$A = x + y,$$
$$B = x^2 + y^2.$$

丢番图方程已经被研究了上千年. 比如说由毕达哥拉斯给出的形如 $x^2 + y^2 = z^2$ 二次丢番图方程, 最初被古巴比伦人所解决. 形如 $26x + 65y = 13$ 的线性丢番图方程被发现可以利用欧几里得算法解决.

古代的中国对数论的研究有着众多杰出的贡献, 这涵盖了勾股定理、勾股数以及中国剩余定理等等. 古代中国的数论具有鲜明的实践、直觉和算法特点, 而古代希腊的数论则具有理性和思辨的特征, 例如唯一因子分解、素数的无限性、方程 $x^2 + y^2 = z^2$ 的整数解. 数论的近代发展是从十七世纪开始的. 而在十九世纪, 数论取得了重大进步, 集中体现为研究方法的创新, 在数论问题的研究中引入了深刻的代数工具和解析工具, 产生了两个重要的数论分支——代数数论和解析数论. 费马大定理首先由费马在 1637 年提出, 并且费马在一张纸上写下了：“我有个绝妙的证明方法, 但是这里太小我写不下. ”尽管有无数的数学家前仆后继, 可还是过了几百年, 直到 1995 年才被怀尔斯证明, 证明过程用到了大量的代数数论知识和模形式理论的内容.

代数数论中对于类群的研究是一个重要的方向, 数域的类群在代数数论和算术几何中有着重要的地位和应用. 类群本身是代数数域的重要算术性质, 它决定了数域中数域理想的差异. 而二次数域作为相对简单的数域, 其类群的结构也仍然没有被完全研究清楚.

1.2 本文的主要工作

首先由类群有限定理可以知道类群是一个有限阿贝尔群, 然后利用有限阿贝尔群结构定理可以把类群分解为 Sylow p-子群的直和. 本文的研究主要围绕 $C(F)[2]$ 这个群展开. 回顾高斯型理论, 高斯型理论给出了缩理想类群 $C(F)[2]$ 中元素的刻画以及缩理想类群的 2 阶秩, 再考虑 $C(F)[2] \cap C(F)^2$, 注意到 $r_4(C(F)) = \mathrm{rank}_{\mathbb{F}_2}\left(C(F)[2] \cap C(F)^2\right)$. 于是我们对二次域类群的 4 阶秩转为去研究群 $C(F)[2] \cap C(F)^2$ 的结构. 然后我们再利用 Rédei 理论的一套内容去给出二次域类群的 4 阶秩的刻画, 并利用二次域类群的 4 阶秩的计算公式给出一些特殊二次域类群的 4 阶秩之间的一些联系. 具体的联系参见3.3. 最后我们再对二次域类群的 8 阶秩进行一些探究.

2 代数数论基础知识

2.1 p 进数域

定义 2.1 (赋值) 如果域 K 上的函数 $|\cdot|: K \to \mathbb{R}_{\geqslant 0}$ 满足

(1) $|x| = 0$ 当且仅当 $x = 0$;

(2) $|xy| = |x| \cdot |y|, \forall x, y \in K$;

(3) (三角不等式)$|x + y| \leqslant |x| + |y|, \forall x, y \in K$;

我们称 $|\cdot|$ 为域 K 上的一个乘性赋值, 称 $(K, |\cdot|)$ 为赋值域. 如果称 $|\cdot|$ 还满足条件 $|x + y| \leqslant \max\{|x|, |y|\}, \forall x, y \in K$, 则称之为非阿赋值, 否则称之为阿基米德赋值.

定义 2.2 (加性赋值) 设 Γ 是全序加法交换群. 如果域 K 上的函数 $v : K \to \Gamma \cup \{\infty\}$ 满足

(1) $v(x) = 0$ 当且仅当 $x = 0$;

(2) $v(xy) = v(x) + v(y), \forall x, y \in K$;

(3) $v(x + y) \geqslant \min\{v(x), v(y)\}, \forall x, y \in K$.

则称之为加性赋值.

加性赋值和非阿赋值之间是一一对应的. 对于 $\Gamma = \mathbb{R}_{>0}$, 我们可以更直接的构造映射 $\log_a : \mathbb{R}_{>0} \to \mathbb{R}$ 来体现两者之间的对应, 这里 $0 < a < 1$.

定义 2.3 (等价赋值) 赋值将 K 变为一个度量空间, 于是定义出 K 上的一个拓扑, 其中

$$U(a, r) = \{x \in K : |x - a| < r\}, \quad a \in K, r > 0$$

构成一组拓扑基. 若两种赋值诱导出来的拓扑空间相同, 则称两种赋值为等价赋值.

定理 2.1 (Ostrowski 定理) 考虑有理数域 $\mathbb{Q}$ 上的赋值等价类, 只有两种. 分别是通常实数域上的赋值 $|\cdot|_\infty$ 和 p 进赋值 $|\cdot|_p$.

此定理具体证明参考[1]§ 2.1.2. 以下有关 p 进数域和希尔伯特符号的定义和性质参考了文献[2]§ 3.1.

2.1.1 p 进数域的代数构造

考虑模 p^n 的同余类环 $\mathbb{Z}/p^n\mathbb{Z}$, $\mathbb{Z}/p^n\mathbb{Z}$ 与 $\mathbb{Z}/p^{n-1}\mathbb{Z}$ 中存在环同态:

$$\begin{aligned} \varphi_n : \mathbb{Z}/p^n\mathbb{Z} &\longrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z}, \\ x \bmod p^n &\longmapsto x \bmod p^{n-1}. \end{aligned}$$

考虑一条逆向链

$$\cdots \xrightarrow{\varphi_{n+1}} \mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\varphi_n} \mathbb{Z}/p^{n-1}\mathbb{Z} \xrightarrow{\varphi_{n-1}} \cdots \xrightarrow{\varphi_3} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\varphi_2} \mathbb{Z}/p\mathbb{Z}.$$

定义 $\mathbb{Z}_p$ 为其逆向极限：$\mathbb{Z}_p = \varprojlim \left(\mathbb{Z}/p^n\mathbb{Z}, \varphi_n\right)$. 所以对于每一个 $\mathbb{Z}_p$ 中的元素 a, 都可以将 a 写成一个无穷序列的形式 $a = \left\{a_1, a_2, \cdots, a_n, \cdots\right\}$.

代数构造的 p 进数域有如下一些性质：

1. 对于 $\mathbb{Z}_p$ 中任一元素 a, a 可逆当且仅当 a 不被 p 整除.
2. 令 U 表示 $\mathbb{Z}_p$ 的乘法单位群, $\mathbb{Z}_p$ 中每一个非零元 a 都可以被唯一的表示为 $a = p^n u$, 其中 $u \in U$, 且 $n \geqslant 0$.
3. 定义 $\mathbb{Z}_p$ 上的赋值 ν_p. 对于 $\mathbb{Z}_p$ 中元素 $a = p^n u$, 定义 $\nu_p(a) = n$, 且 $\nu_p(0) = +\infty$. 利用 $\nu_p(xy) = \nu_p(x) + \nu_p(y)$ 很容易得到 $\mathbb{Z}_p$ 是一个整环.

在 $\mathbb{Z}_p$ 上可以定义度量 $d(x, y) = p^{-\nu_p(x-y)}$, 这是一个非阿基米德度量. 在这种度量诱导出来的拓扑空间下, $\mathbb{Z}_p$ 是一个完备的度量空间, 且 $\mathbb{Z}$ 在 $\mathbb{Z}_p$ 中是稠密的.

定义 $\mathbb{Q}_p$ 为 $\mathbb{Z}_p$ 的分式域. 容易看出 $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$, 对于 $\mathbb{Q}_p$ 中非零元素 a, a 可以被唯一的表示为 $a = p^n u$, 其中 $u \in U$, 且 $n \in \mathbb{Z}$. 通过这样定义出来的域 $\mathbb{Q}_p$, 是一个局部紧的域, 且 $\mathbb{Z}_p$ 是 $\mathbb{Q}_p$ 中的一个开子环, $\mathbb{Q}$ 在 $\mathbb{Q}_p$ 中稠密.

2.1.2 p 进数域的分析构造

给定一个素数 p, 将 $\mathbb{Q}$ 中元素 x 写为 $x = \frac{a}{b}$, 其中 a, b 为互素的整数. 考察 p 在 a, b 素因子分解中的次数, 记为 $\mathrm{ord}_p(a), \mathrm{ord}_p(b)$, 定义 p 进赋值

$$\nu_p(x) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b).$$

同时约定 $\nu_p(x) = +\infty$. 在此基础上, 可以很自然的诱导出 p 进数域的距离函数和范数

$$\mathrm{d}_p(x, y) = p^{-\nu_p(x-y)}, \quad |\, x \,|_p = p^{-\nu_p(x)}.$$

有了度量之后就可以建立柯西列的概念, 然后仿照实数那样将 p 进赋值下的 $\mathbb{Q}$ 完备化, 从而我们得到了 $\mathbb{Q}_p$.

以上两种构造方法实际上是等价的, 考虑分析定义下的 $\mathbb{Q}_p$, 定义 $\mathbb{Q}_p$ 下的 p 进整数环 $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \leqslant 1\}$(由强三角不等式很容易得到这是一个环). 构造环同态

$$\phi : \varprojlim \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p.$$

对 $(a_n) \in \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, 取定一个整数 x_n 使得 x_n 在 $\mathbb{Z}/p^n\mathbb{Z}$ 中像为 a_n, 由于当 $m, n > N$ 时, $\left|x_m - x_n\right|_p \leqslant \frac{1}{p^N}$, 故 $\left|\left(x_n\right)\right|_p \leqslant 1$; 反之, 对于 $a = \left(a_n\right) \in \mathbb{Z}_p$(不妨假定 a_n 都为整数), (a_n) 在环同态 $\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ 下的剩余类序列 $\left(\overline{a_n}\right)$ 会收敛于一个常数 $\sigma_n(a)$, 因为 $\left|\left(a_n\right)\right|_p \leqslant 1$. 很容易证明上述的映射是 1-1 的, 从而我们得到了这里两个定义是等价的.

2.1.3 $\mathbb{Q}_p$ 中平方数问题

令 U 表示 $\mathbb{Z}_p$ 的乘法单位群, 定义 $U_n = 1 + p^n\mathbb{Z}_p$. 容易看出 U_n 是同态 $\phi : U \to \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$ 的核. 特别的, 考虑商群 U/U_1, 这个商群同构于 $F_p^\times$.

对于 $p \neq 2$, 令 $x = p^n u$ 是 $\mathbb{Q}_p^\times$ 中的一个元素. 存在 $a \in \mathbb{Q}_p^\times$ 使得 $x = a^2$ 当且仅当 n 是偶数且 u 在 U/U_1 中的像 $\bar{u}$ 是一个元素的平方 (最后一个条件相当于勒让德符号 $\left(\frac{\bar{u}}{p}\right) = 1$).

当 $p \neq 2$ 时, 考虑商群 $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, 这个群同构于 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. 当 $p = 2$ 时, 考虑商群 $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$, 这个群同构于 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

对于 $p = 2$, 定义同态 $\varepsilon, \omega : U/U_3 \to \mathbb{Z}/2\mathbb{Z}$

$$\varepsilon(z) \equiv \frac{z-1}{2} (\mathrm{mod} 2), \tag{2.1}$$

$$\omega(z) \equiv \frac{z^2-1}{8} (\mathrm{mod} 2). \tag{2.2}$$

定义 2.4 (无穷素位)　设 K 为 n 次数域. 定义无穷素位为嵌入 $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, 容易看出 $\bar{\sigma} : K \xrightarrow{\sigma} \mathbb{C} \xrightarrow{\text{复共轭}} \mathbb{C}$ 也是一个嵌入. 如果$\sigma(K) \subseteq \mathbb{R}$, 即$\bar{\sigma} = \sigma$, 称$\sigma$ 为实嵌入或实素位, 否则称之复嵌入或者复素位. 如果 K 没有复素位, 则称 K 为全实域. 如果 K 没有实素位, 则称 K 为全虚域.

在本文后续的证明中, 需要讨论一些 $\mathbb{Q}_p$ 上的二次型, 因此我们引入下面这个定理, 具体证明参见[2]§ 3.2.

定理 2.2 (Hasse-Minkowski)　有理数域 $\mathbb{Q}$ 上的非退化二次型 f 能表示 0 的充要条件为对 $\mathbb{Q}$ 的所有素位 v, 二次型 f_v 在对应的 $\mathbb{Q}_v$ 上能表示 0.

2.2 希尔伯特符号

采用 $\mathbb{Q}_v$ 表示实数域 $\mathbb{R}$ 或者 p 进数域 $\mathbb{Q}_p$. 当 $v = \infty$ 时, $\mathbb{Q}_v = \mathbb{R}$; 当 $v = p$ 时, 用 $\mathbb{Q}_v$ 表示 p 进数域 $\mathbb{Q}_p$.

2.2.1 雅可比符号

定义 2.5 (雅可比符号) 对于任意整数 a 和正奇数 n, 考虑 n 的素因子分解 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. 将雅可比符号 $(\frac{a}{n})$ 定义为一些勒让德符号的乘积

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}.$$

这里勒让德符号的计算方法为

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ 若} a \equiv 0(\mathrm{mod}p), \\ 1 \text{ 若} a \neq 0(\mathrm{mod}p) \text{且存在整数 } x \text{ 使得} a \equiv x^2(\mathrm{mod}p), \\ -1 \text{ 若} a \neq 0(\mathrm{mod}p) \text{且不存在这样的} x. \end{cases}$$

勒让德符号具有如下的一些性质, 这些性质对于我们的计算过程具有极大的帮助:

- $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right), \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right).$
- $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}} = \begin{cases} 1 & \text{若} n \equiv 1(\mathrm{mod}4) \text{ 或} m \equiv 1(\mathrm{mod}4), \\ -1 & \text{若} n \equiv m \equiv 3(\mathrm{mod}4). \end{cases}$
- $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 & \text{若} n \equiv 1(\mathrm{mod}4), \\ -1 & \text{若} n \equiv 3(\mathrm{mod}4). \end{cases}$
- $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 & \text{若} n \equiv 1, 7(\mathrm{mod}8), \\ -1 & \text{若} n \equiv 3, 5(\mathrm{mod}8). \end{cases}$

2.2.2 希尔伯特符号的基本性质

希尔伯特符号定义：对于 $a, b \in \mathbb{Q}_v^\times$, 若方程 $z^2 = ax^2 + by^2$ 有非零解, 则记为 $(a, b)_v = 1$, 其他情况记为 $(a, b)_v = -1$. 容易看出, 希尔伯特符号给出了一个 $\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2} \times \mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2}$ 到 $\{\pm 1\}$ 的映射. 希尔伯特符号有如下几点性质：

- 对于 $a, b \in \mathbb{Q}_v^\times$, 令 $k_b = \mathbb{Q}_v\left(\sqrt{b}\right)$, 则 $(a, b)_v = 1$ 的充要条件是 $a \in \mathbf{N}k_b^\times$.
- $(a, b)_v = (b, a)_v, \left(a, c^2\right)_v = 1.$
- $(a, -a)_v = 1, (a, 1-a)_v = 1.$
- $(a, b)_v = 1 \Rightarrow \left(aa', b\right)_v = \left(a', b\right)_v.$
- $(a, b)_v = (a, -ab)_v = (a, (1-a)b)_v.$

希尔伯特符号还具有下面比较重要的性质, 具体证明参见[2].

定理 2.3 对于任意的 $a, b \in \mathbb{Q}^\times$ 我们有等式

$$\prod_v (a,b)_v = 1$$

成立, 其中 v 取遍 $\mathbb{Q}$ 的所有素位.

2.2.3 希尔伯特符号的计算

当 $v = \infty$ 的时候, $(a,b) = 1$ 当 $a > 0$ 或 $b > 0$; $(a,b) = -1$ 当 $a < 0$ 且 $b < 0$.

当 $v = p$ 时, 将 a, b 表示为 $p^\alpha u, p^\beta v$, 此时有

$$(a,b)_v = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha, \qquad p \neq 2. \tag{2.3}$$

$$(a,b)_v = (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)}, \qquad p = 2. \tag{2.4}$$

例 2.1 考虑希尔伯特符号 $(7,-21)_3$, 此时

$$7 = 3^0 \times 7, \quad -21 = 3^1 \times (-7).$$

从而 $(7,-21)_3 = (\frac{7}{3}) = 1$.

考虑希尔伯特符号 $(3,-21)_2$, 此时

$$3 = 2^0 \times 3, \quad -21 = 2^0 \times (-21).$$

从而 $(7,-21)_3 = (-1)^{\varepsilon(3)\varepsilon(-21)} = -1$.

2.3 类群与类数

由唯一分解定理可以知道 $\mathbb{Z}$ 中任意整数 n 都能分解为素元的乘积, 但是唯一分解定理并不是在任意环中成立. 比如考虑 $\mathbb{Z}[\sqrt{-5}]$, $6 = \left(1+\sqrt{-5}\right) \times \left(1-\sqrt{-5}\right) = 2 \times 3$, 此时分解并不唯一. 此时若引入类群这一概念, 就可以很好的刻画一个环同唯一分解整环之间的差距. 首先给出分式理想的定义:

定义 2.6 设 K 是一个数域, 称 K 的子集合 $\mathfrak{a}$ 是分式理想, 如果它满足如下的等价条件:

- 存在非零数 $c \in \mathcal{O}_K$ 使得 $c\mathfrak{a}$ 是 $\mathcal{O}_K$ 的非零理想;
- $\mathfrak{a}$ 是 K 的非零有限生成 $\mathcal{O}_K$-子模.

对于 K 中每个非零元, 很自然的可以定义出主分式理想 $(\alpha) = \alpha\mathcal{O}_K, \alpha \in K^\times$. 记 $\mathcal{P}_K$ 为全体主分式理想组成的集合. 很自然的我们可以定义分式理想的乘积为

$\mathfrak{ab} = \left\{\sum_{i=1}^{n} a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\right\}$. 而且不难验证所有的分式理想组成的集合构成了一个阿贝尔群 $\mathcal{I}_K$, 其中的单位元为 $(1) = \mathcal{O}_K$, 相关证明参考[3].

考虑群的正合列

$$1 \longrightarrow \mathcal{O}_K^{\times} \longrightarrow K^{\times} \xrightarrow{\alpha \mapsto (\alpha)} \mathcal{I}_K \longrightarrow \mathrm{Cl}_K \longrightarrow 1,$$

其中 $\mathcal{O}_K^{\times}$ 为 $\mathcal{O}_K$ 中的全体单位, 定义 K 的理想类群为 $\mathrm{Cl}(K) = \mathcal{I}_K/\mathcal{P}_K$.

为了方便下一章的叙述, 我们需要引入如下的定义:

定义 2.7　定义有限阿贝尔群 A 的 2^a-秩为

$$r_{2^a}(A) = \dim_{\mathbb{F}_2}\left(\frac{2^{a-1}A}{2^a A}\right).$$

令 $h_{2^a}(m)$ 表示二次域 $\mathbb{Q}(\sqrt{m})$ 的缩理想类群的 2^a-秩.

对于 $\mathrm{Cl}(F)$ 和 $\mathcal{O}_K^{\times}$, 有两个重要的定理, 它们分别是类数有限定理和狄利克雷单位定理.

定理 2.4 (类数有限定理)　类群为一个有限阿贝尔群, 类群的大小被记为 h_K.

定理 2.5 (狄利克雷单位定理)　$\mathcal{O}_K$ 的单位群 $\mathcal{O}_K^{\times}$ 同构于 $\mu_K \times \mathbb{Z}^{r+s-1}$, 其中 μ_K 为数域 K 中单位根全体, 是一个循环群; r, s 分别表示 K 的实素位和复素位的个数.

根据参考文献[3]§ 1.6 可知有许多类数为 1 的实二次域 $\mathbb{Q}(\sqrt{d})$, 比如

$$\begin{aligned} d =& 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, \\ & 31, 33, 37, 38, 41, 43, 46, 47, 53, 57, 59, 61, \\ & 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97. \end{aligned}$$

对应的有且仅有如下这些类数为 1 的虚二次域,

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163,$$

这由 Baker-Stark 证明. 类数为 1 预示着环 $\mathbb{Z}[\sqrt{d}]$ 为一个唯一分解整环. 从而 $\mathbb{Z}$ 中任意整数 n 在 $\mathbb{Z}[\sqrt{d}]$ 中都能唯一的分解为素元的乘积.

3 高斯型理论

3.1 高斯型理论

设 $m \neq 0,1$ 为一个无平方因子的整数. 令 $F = \mathbb{Q}(\sqrt{m})$, $\mathbf{N}F = \mathbf{N}_{F/\mathbb{Q}}\left(F^{\times}\right)$. 定义缩理想类群 $C(F) = \mathcal{I}_K/\mathcal{P}_K^+$, 其中 $\mathcal{P}_K^+$ 表示主分式理想 (x), 其中 x 满足 $\sigma(x) > 0$, 对于任意实嵌入 σ 成立. 考虑二次域 F 判别式 D 的素因子分解 $D = p_1^* \cdots p_t^*$, 其中

$$p^* = (-1)^{\frac{p-1}{2}} p, \quad 2^* = -4, 8, -8.$$

令集合 V 表示 D 的所有的无平方因子的正因子, $\omega_m = \frac{D+\sqrt{D}}{2}$. $C(F)[2]$ 表示 $C(F)$ 中阶不超过 2 的元素全体构成的子群, $C(F)[4]$ 表示 $C(F)$ 中阶整除 4 的元素全体构成的子群. 考虑分式理想 $\mathfrak{d} = \left(d, \omega_m\right)$, 由高斯型理论可以知道缩理想类群的 2-部分由 $\left[\left(d, \omega_m\right)\right]$ 组成. 高斯型理论的具体表述如下:

定理 3.1 $C(F)[2]$ 是一个阿贝尔群, 这个阿贝尔群的元素形为$\left[(d, \omega_m)\right]$, 其中 $d \in V$. 且

$$\operatorname{rank}_{\mathbb{F}_2} C(F)[2] = t - 1.$$

对于 $C(F)$ 中的元素 $[\mathfrak{d}]$, $[\mathfrak{d}] \in C(F)^2$ 当且仅当存在非零整数 z 和 $a \in \mathfrak{a}$ 使得

$$z^2 \cdot \mathbf{N}\mathfrak{a} = \mathbf{N}a.$$

引入缩理想类群的概念是为了更好地研究二次数域 F 的类群的结构. 而且它们有如下关系:

- 对于虚二次域而言, 有 $\mathrm{Cl}(F) = C(F)$.
- 对于实二次域而言, 若有基本单位的范数为 -1, 那么 $\mathrm{Cl}(F) = C(F)$.
- 对于实二次域而言, 若有基本单位的范数为 $+1$, 那么存在 $C(F)$ 到 $\mathrm{Cl}(F)$ 的一个 2-1 的满同态.

3.2 二次域类群的四阶秩

利用高斯型理论, 可以很好的研究二次域类群的四阶秩. 注意到

$$r_4(C(F)) = \operatorname{rank}_{\mathbb{F}_2}\left(C(F)[2] \cap C(F)^2\right).$$

于是我们对二次域类群的四阶秩转为去研究群 $C(F)[2] \cap C(F)^2$ 的结构.

定义一个映射

$$\theta : V \cap \mathbf{N}F \longrightarrow C(F)[2] \cap C(F)^2,$$

$$d \longmapsto [\mathfrak{d}].$$

并且在集合 $V \cap \mathbf{N}F$ 上定义乘法

$$d_1 \odot d_2 := \frac{d_1 d_2}{\gcd(d_1, d_2)^2}.$$

接下来验证映射 θ 是一个 2-1 的同态.

命题 3.2 映射

$$\theta : V \cap \mathbf{N}F \longrightarrow C(F)[2] \cap C(F)^2,$$

$$d \longmapsto [\mathfrak{d}].$$

为一个 2-1 的同态.

证明 本证明主要参考文献[4]§ 3.1. 首先, 验证 θ 是一个良定义的映射: 因为 $d \in V \cap \mathbf{N}F$, 由高斯型理论可以知道 $\left[\left(d, \omega_m\right)\right] \in C(F)[2]$. 从 $d \in \mathbf{N}F$ 可以知道存在 $\alpha \in F^\times$ 使得 $d = \mathbf{N}\alpha$, 选取适当的正整数 z, 使得 $z\alpha = xd + y\omega_m \in \left(d, \omega_m\right)$. 由 $\mathbf{N}\left(d, \omega_m\right) = d$ 可知 $\left[\left(d, \omega_m\right)\right] \in C(F)^2$.

接下来验证 θ 是一个同态映射: 对于互素的 d_1, d_2, 有

$$\left(d_1, \omega_m\right) \cdot \left(d_2, \omega_m\right) = \left(d_1 d_2, \omega_m^2, d_1 \cdot \omega_m, d_2 \cdot \omega_m\right) = \left(d_1 d_2, \omega_m\right).$$

对于一般的 d_1, d_2, 有 $d_i = \frac{d_i}{\gcd\left(d_1, d_2\right)} \cdot \gcd\left(d_1, d_2\right)$, 从而

$$\left(d_i, \omega_m\right) = \left(\frac{d_i}{\gcd\left(d_1, d_2\right)}, \omega_m\right) \cdot \left(\gcd\left(d_1, d_2\right), \omega_m\right).$$

利用上述等式可以得到对于任意的 d_1, d_2 有

$$\begin{aligned} \left(d_1, \omega_m\right) \cdot \left(d_2, \omega_m\right) &= \left(\gcd\left(d_1, d_2\right), \omega_m\right)^2 \cdot \prod_{i=1}^{2} \left(\frac{d_i}{\gcd\left(d_1, d_2\right)}, \omega_m\right) \\ &= \left(\gcd\left(d_1, d_2\right), \omega_m\right)^2 \cdot \left(d_1 \odot d_2, \omega_m\right). \end{aligned} \tag{3.1}$$

从而有

$$\theta\left(d_1\right) \cdot \theta\left(d_2\right) = \theta\left(d_1 \odot d_2\right).$$

由此可知 θ 是一个同态映射.

然后验证 θ 是一个满同态: 对于任意 $\left[\left(d, \omega_m\right)\right] \in C(F)[2] \cap C(F)^2$, 满足 d 为 D 的一个无平方因子的除数, $d \in V$, 且存在非零整数 z 和 $a \in \mathfrak{a}$ 使得 $z^2 \cdot \mathbf{N}\left(d, \omega_m\right) = \mathbf{N}a$, 即 $z^2 \cdot d = \mathbf{N}a$, 从而 $d \in \mathbf{N}F$. 所以 θ 是一个满同态.

验证 θ 是 2-1 的同态: 这一部分主要参考文献[5]§ 45. 此时我们希望找到一个数 α 和一种非平凡关系使得

$$\alpha = \mathfrak{q}_1^{a_1} \cdots \mathfrak{q}_t^{a_t}, \quad N(\alpha) > 0.$$

这里我们有 $(\alpha) = (\bar{\alpha}), \alpha = \eta\bar{\alpha}$, 这里 η 是一个单位元且满足 $N(\eta) = +1$, 现在我们分三种情况来讨论:

- 若 $m < 0$, 当 $m = -3$ 或者 -4 时, 缩理想类群的阶数为 1, 此时命题显然成立. 考虑当 $m < -4$ 时, 此时 F 中的单位元为 ± 1, 因此

  $$\alpha = \pm\alpha', \quad \alpha = r\left(\sqrt{d}\right)^n \quad (n = 0, 1),$$

  这里 r 为一个有理数. 当 $n = 0$ 时对应所有的指数 a_i 都为偶数. 当 $n = 1$ 时, 因为 d 不是一个平方数, 所以所有的指数 a_i 中必存在至少一个为奇数.
- 若 $m > 0$ 且数域 F 的基本单位 ε 的范数为 -1. 因为 $N(\alpha) > 0$, 所以 $N(\eta) > 0$. 从而 $\eta = \varepsilon^{2n}$, 因为

  $$\varepsilon^2 = -\frac{\varepsilon}{\varepsilon'} = \frac{\varepsilon\sqrt{d}}{-\varepsilon'\sqrt{d}}.$$

  从而我们得到

  $$\frac{\alpha}{(\varepsilon\sqrt{d})^n} = \frac{\alpha'}{\left(-\varepsilon'\sqrt{d}\right)^n}, \quad \alpha = r\left(\varepsilon\sqrt{d}\right)^n,$$

  这里 r 为一个有理数. 当 $n = 0$ 时对应所有的指数 a_i 都为偶数. 当 $n = 1$ 时, 因为 d 不是一个平方数, 所以所有的指数 a_i 中必存在至少一个为奇数.
- 若 $m > 0$ 且数域 F 的基本单位 ε 的范数为 $+1$. 这里

  $$\eta = \varepsilon^n, \quad \varepsilon = \frac{1+\varepsilon}{1+\varepsilon'}, \quad \eta = \frac{(1+\varepsilon)^n}{(1+\varepsilon')^n},$$

  $$\alpha = r(1+\varepsilon)^n.$$

  理想 $(1+\varepsilon)$ 等于它的共轭, 且不等于任何一个有理数生成的主理想. 若

  $$1 + \varepsilon = r_1\varepsilon^k$$

  对于有理数 r_1 成立, 那么我们有

  $$\varepsilon = \frac{1+\varepsilon}{1+\varepsilon'} = \varepsilon^{2k}, \quad \varepsilon^{2k-1} = 1.$$

  因此理想 $(1+\varepsilon)$ 有一个分解

  $$(1+\varepsilon) = \mathfrak{a} \times \mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_t^{b_t}.$$

  这里 $\mathfrak{a}$ 为一个有理理想, 且至少有一个 b_i 为奇数.

由上述三种情况可知都存在一种非平凡关系, 所以 θ 是 2-1 的同态, 命题得证. ∎

现在, 我们已经准备好来引入 F 上的 Rédei 矩阵 $\mathbf{R}_m$: 首先假定如果 $2 \mid D$, 那么令 $p_t = 2$. 定义加性希尔伯特符号

$$[a,b]_v = \begin{cases} 0 & 若(a,b)_v = 1, \\ 1 & 若(a,b)_v = -1. \end{cases} \tag{3.2}$$

加性雅可比符号 $[\frac{a}{b}]$ 也可以类似的定义出来

$$[\frac{a}{b}] = \begin{cases} 0 & 若\frac{a}{b} = 1, \\ 1 & 若\frac{a}{b} = -1. \end{cases} \tag{3.3}$$

然后定义 Rédei 矩阵为 $\mathbf{R}_m = (r_{ij})_{t\times t}$ 是一个 $\mathbb{F}_2$ 上的 $t \times t$ 阶矩阵:

$$\mathbf{R}_m = \left(\left[p_j, m \right]_{p_i} \right)_{t\times t}.$$

为了构造 Rédei 矩阵同四阶秩之间的联系, 我们需要引进如下的命题, 并给出它们的证明:

命题 3.3 以下四条命题是等价的:

(1) $d \in V \cap \mathbf{N}F$.

(2) $X^2 - mY^2 = dZ^2$ 在 $\mathbb{Z}$ 上有非平凡解.

(3) 对于 $p \mid D$, 希尔伯特符号 $(d,m)_p = 1$.

(4) $\mathbf{R}_m\mathbf{d} = \mathbf{0}$, 这里 $\mathbf{d} = \left(v_{p_1}(d), \cdots, v_{p_t}(d) \right)^T$.

证明 (1) $\Longleftrightarrow$ (2): 对于 $d \in V \cap \mathbf{N}F$, 可知存在 $\alpha \in F^\times$, 其中 $\alpha = x + y\sqrt{m}, x, y \in \mathbb{Q}$, 使得 $\mathbf{N}(\alpha) = d$, 即

$$x^2 - my^2 = d$$

取 x, y 分母的最大公倍数 a_0, 并在等式两边乘以 a_0^2, 从而可以得到 $X^2 - mY^2 = dZ^2$ 在 $\mathbb{Z}$ 上有非平凡解. 对于另外一个方向, 若 $X^2 - mY^2 = dZ^2$ 在 $\mathbb{Z}$ 上有非平凡解, 则 $(\frac{X}{Z})^2 - m(\frac{Y}{Z})^2 = d$, 从而可以知道 $d \in V \cap \mathbf{N}F$.

(2) $\Longleftrightarrow$ (3): 由 Hasse-Minkowski 定理可知

$$X^2 - mY^2 = dZ^2$$

在 $\mathbb{Z}$ 上有非平凡解等价于对于任意素数 p,

$$X^2 - mY^2 = dZ^2$$

在 $\mathbb{Z}_p$ 上有解, 这里 $\mathbb{Z}_p$ 表示 p 进整数. 从而充分性是显然的. 现在考虑必要性, 若 $p \nmid D$, 则显然有 $(d,m)_p = 1$. 再根据题设所给条件, 所以我们可以得到命题 2, 3 为等价的.

(1) $\Longleftrightarrow$ (4): 对于 $d \in V \cap \mathbf{N}F$, 由命题 (1) 和 (3) 等价可以得出

$$[d,m]_{p_i} = 0, 1 \leqslant i \leqslant t$$

又 $\mathbf{R}_m\mathbf{d} = \mathbf{0}$ 等价于 $\left([d,m]_{p_1}, \cdots, [d,m]_{p_t}\right)^T = \mathbf{0}$ 成立, 从而命题得证. ∎

利用上面定义的同态 θ, 可以给出命题刻画 Rédei 矩阵同四阶秩之间的联系.

命题 3.4 二次域类群的四阶秩满足如下关系式:

$$h_4(m) = t - 1 - \operatorname{rank}\left(\mathbf{R}_m\right).$$

证明 由 θ 是一个 2-1 的同态可以知道

$$|V \cap \mathbf{N}F| = 2|C(F)[2] \cap C(F)^2|$$

又由命题 4 可以得到 $|V \cap \mathbf{N}F| = 2^{t-\operatorname{rank}_{\mathbb{F}_2}\mathbf{R}_m}$. 从而有

$$|C(F)[2] \cap C(F)^2| = 2^{t-1-\operatorname{rank}_{\mathbb{F}_2}\mathbf{R}_m}.$$

从而可以知道 $h_4(m) = t - 1 - \operatorname{rank}_{\mathbb{F}_2}\mathbf{R}_m$. ∎

例 3.1 给定实二次域 $\mathbb{Q}(\sqrt{21})$, 这里 $m = 21 \equiv 1 (\mathrm{mod}\, 4)$. 从而二次域的判别式 $D = m = 21$. 此时 $D = 3 \times 7$, 有两个素因子, 从而对应的 Rédei 矩阵为 2×2 阶矩阵. 计算可得

$$\mathbf{R}_{21} = \begin{pmatrix} [3,21]_3 & [7,21]_3 \\ [3,21]_7 & [7,21]_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

此时有 $\operatorname{rank}_{\mathbb{F}_2}\mathbf{R}_{21} = 1$. 所以 $h_4(21) = 2 - 1 - \operatorname{rank}_{\mathbb{F}_2}\mathbf{R}_{21} = 0$. 即此时二次域 $\mathbb{Q}(\sqrt{21})$ 理想类群的四阶秩为 0.

例 3.2 给定虚二次域 $\mathbb{Q}(\sqrt{-21})$, 这里 $m = -21 \equiv 3 (\mathrm{mod}\, 4)$. 从而二次域的判别式 $D = 4m = -84$. 此时 $D = -3 \times 7 \times 4$, 有三个素因子, 从而对应的 Rédei 矩阵为 3×3 阶矩阵. 计算可得

$$\mathbf{R}_{-21} = \begin{pmatrix} [3,-21]_3 & [7,-21]_3 & [2,-21]_3 \\ [3,-21]_7 & [7,-2\,|]_7 & [2,-21]_7 \\ [3,-21]_2 & [7,-21]_2 & [2,-21]_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

此时有 $\operatorname{rank}_{\mathbb{F}_2}\mathbf{R}_{-21} = 2$. 所以 $h_4(-21) = 2 - \operatorname{rank}_{\mathbb{F}_2}\mathbf{R}_{-21} = 0$. 即此时二次域 $\mathbb{Q}(\sqrt{-21})$ 理想类群的四阶秩为 0.

例 3.3 给定虚二次域 $\mathbb{Q}(\sqrt{-1105})$, 这里 $m=-1105\equiv 3(\mathrm{mod}\,4)$. 从而二次域的判别式 $D=4m=-4\times 1105$. 此时 $D=-5\times 13\times 17\times 4$, 有四个素因子, 从而对应的 Rédei 矩阵为 4×4 阶矩阵. 计算可得

$$\begin{aligned}\mathbf{R}_{-1105}&=\begin{pmatrix}[5,-1105]_5 & [13,-1105]_5 & [17,-1105]_5 & [2,-1105]_5\\ [5,-1105]_{13} & [13,-1105]_{13} & [11,-1105]_{13} & [2,-1105]_{13}\\ [5,-1105]_{17} & [13,-1105]_{17} & [17,-1105]_{17} & [2,-1105]_{17}\\ [5,-1105]_2 & [13,-1105]_2 & [17,-1105]_2 & [2,-1105]_2\end{pmatrix}\\&=\begin{pmatrix}0&1&1&1\\1&1&0&1\\1&0&1&0\\0&0&0&0\end{pmatrix}.\end{aligned}$$

此时有 $\mathrm{rank}_{\mathbb{F}_2}\mathbf{R}_{-1105}=2$. 所以 $h_4(-1105)=4-1-\mathrm{rank}_{\mathbb{F}_2}\mathbf{R}_{21}=1$. 即此时二次域 $\mathbb{Q}(\sqrt{-1105})$ 理想类群的四阶秩为 1.

我们此时观察到对于上述例子中的 Rédei 矩阵的每一列和为 0, 由此猜测是否有 Rédei 矩阵的每一列和为 0, 此时我们得到了如下命题.

命题 3.5 我们有 $\mathbf{1}^{\mathrm{T}}\mathbf{R}_m=\mathbf{0}^{\mathrm{T}}$.

证明 由定理 2.3 可以得到 $\sum_{p\,\mathrm{prime}}\left[p_j,m\right]_p=0$, 又当 $p\nmid D$ 时, 显然有 $\left[p_j,m\right]_p=0$. 从而 $\sum_{p\,\mathrm{prime}}\left[p_j,m\right]_p=\sum_{i=1}^{t}\left[p_j,m\right]_{p_i}=0$. ∎

3.3 具体运用

为了接下来叙述方便, 我们约定一些记号. 给定一个正整数 n, 令 $n'=p_1\cdots p_t$ 表示 n' 的素分解, 其中 $n'=\dfrac{n}{\gcd(n,2)}$. 令

$$\mathbf{A}=\mathbf{A}_{n'}=\left(a_{ij}\right)_{k\times k},\quad \text{这里}\quad a_{ij}=\left[p_j,-n'\right]_{p_i}=\begin{cases}\left[\dfrac{p_j}{p_i}\right], & i\neq j\\ \left[\dfrac{n'/p_i}{p_i}\right], & i=j\end{cases},\tag{3.4}$$

$$\mathbf{D}_{\varepsilon}=\mathrm{diag}\left\{\left[\frac{\varepsilon}{p_1}\right],\cdots,\left[\frac{\varepsilon}{p_k}\right]\right\},\quad \mathbf{b}_{\varepsilon}=\mathbf{D}_{\varepsilon}\mathbf{1},\quad \text{其中}\mathbf{1}=(1,\cdots,1)^{\mathrm{T}}.\tag{3.5}$$

现在我们来证明一个命题, 这个命题可以给出 Rédei 矩阵更好的形式, 从而给出一些特殊二次域的四阶秩之间的一些关系.

命题 3.6 令 $n=p_1\cdots p_t$ 是一个无平方因子的正奇数. 当 $n\equiv 1(\mathrm{mod}\,4)$ 时, 我们

有

$$\mathbf{R}_n = \mathbf{A} + \mathbf{D}_{-1}, \qquad \mathbf{R}_{-n} = \begin{pmatrix} \mathbf{A} & \mathbf{b}_2 \\ \mathbf{b}_{-1}^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix},$$

$$\mathbf{R}_{2n} = \begin{pmatrix} \mathbf{A} + \mathbf{D}_{-2} & \mathbf{b}_2 \\ \mathbf{b}_2^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix}, \quad \mathbf{R}_{-2n} = \begin{pmatrix} \mathbf{A} + \mathbf{D}_2 & \mathbf{b}_2 \\ \mathbf{b}_{-2}^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix}.$$

证明 当 $n \equiv 1(\mathrm{mod}\,4)$ 时, 考虑 $\mathbf{R}_n = (r_{ij})_{t\times t}$, 当 $i \neq j$ 时, $r_{ij} = \left[p_j, n\right]_{p_i}$, 利用等式(2.1)计算可知 $\left[p_j, n\right]_{p_i} = \left[\frac{p_j}{p_i}\right]$. 当 $i = j$ 时, 利用等式(2.1)计算可知 $\left[p_i, n\right]_{p_i} = \left[\frac{-n/p_i}{p_i}\right] = \left[\frac{-1}{p_i}\right] + \left[\frac{n/p_i}{p_i}\right]$. 从而我们得到 $\mathbf{R}_n = \mathbf{A} + \mathbf{D}_{-1}$.

由 $n \equiv 1(\mathrm{mod}\,4)$ 可以得到 $-n \equiv 3(\mathrm{mod}\,4)$. 此时二次域 $\mathbb{Q}(\sqrt{-n})$ 的判别式 $D = -4n$, 所以此时二次域 $\mathbb{Q}(\sqrt{-n})$ 对应的 Rédei 矩阵为 $(t+1)\times(t+1)$ 阶. 当 $1 \leqslant i \neq j \leqslant t$ 时, $r_{ij} = \left[p_j, -n\right]_{p_i}$, 利用等式(2.1)计算可知 $\left[p_j, -n\right]_{p_i} = \left[\frac{p_j}{p_i}\right]$;

当 $1 \leqslant i = j \leqslant t$ 时, 利用等式(2.1)计算可知 $\left[p_i, -n\right]_{p_i} = \left[\frac{-n/p_i}{p_i}\right] = \left[\frac{-1}{p_i}\right] + \left[\frac{n/p_i}{p_i}\right]$;

当 $i = t+1, 1 \leqslant j \leqslant t$ 时, 利用等式(2.2)计算可知 $\left[p_j, -n\right]_{p_i} = \left[\frac{-1}{p_i}\right]$;

当 $i = j = t+1$ 时, 利用等式(2.2)计算可知 $\left[p_j, -n\right]_{p_i} = \left[\frac{2}{n}\right]$. 因此我们得到了

$$\mathbf{R}_{-n} = \begin{pmatrix} \mathbf{A} & \mathbf{b}_2 \\ \mathbf{b}_{-1}^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix}.$$

考虑 $\mathbf{R}_{2n} = (r_{ij})_{(t+1)\times(t+1)}$, 当 $1 \leqslant i \neq j \leqslant t$ 时, $r_{ij} = \left[p_j, 2n\right]_{p_i}$, 利用等式(2.1)计算可知 $\left[p_j, 2n\right]_{p_i} = \left[\frac{p_j}{p_i}\right]$. 当 $1 \leqslant i = j \leqslant t$ 时, 利用等式(2.1)计算可知 $\left[p_i, 2n\right]_{p_i} = \left[\frac{-2n/p_i}{p_i}\right] = \left[\frac{-2}{p_i}\right] + \left[\frac{n/p_i}{p_i}\right]$;

当 $i = t+1, 1 \leqslant j \leqslant t$ 时, $r_{ij} = \left[p_j, 2n\right]_{p_i}$, 利用等式(2.2)计算可知 $\left[p_j, n\right]_{p_i} = \left[\frac{2}{p_j}\right]$;

当 $j = t+1, 1 \leqslant i \leqslant t$ 时, $r_{ij} = \left[p_j, 2n\right]_{p_i}$, 利用等式(2.2)计算可知 $\left[p_j, n\right]_{p_i} = \left[\frac{2}{p_i}\right]$;

当 $i = j = t+1$ 时, 利用等式(2.2)计算可知 $\left[p_j, 2n\right]_{p_i} = \left[\frac{2}{n}\right]$.

从而我们得到 $\mathbf{R}_{2n} = \begin{pmatrix} \mathbf{A} + \mathbf{D}_{-2} & \mathbf{b}_2 \\ \mathbf{b}_2^{\mathrm{T}} & \left[\frac{2}{n}\right] \end{pmatrix}$.

考虑 $\mathbf{R}_{-2n} = (r_{ij})_{(t+1)\times(t+1)}$, 当 $1 \leqslant i \neq j \leqslant t$ 时, $r_{ij} = \left[p_j, -2n\right]_{p_i}$, 利用等式(2.1)计算可知 $\left[p_j, n\right]_{p_i} = \left[\frac{p_j}{p_i}\right]$. 当 $1 \leqslant i = j \leqslant t$ 时, 利用等式(2.1)计算可知 $\left[p_i, -2n\right]_{p_i} = \left[\frac{2n/p_i}{p_i}\right] = \left[\frac{2}{p_i}\right] + \left[\frac{n/p_i}{p_i}\right]$;

当 $i = t+1, 1 \leqslant j \leqslant t$ 时, $r_{ij} = \left[p_j, -2n\right]_{p_i}$, 利用等式(2.2)计算可知 $\left[p_j, n\right]_{p_i} = \left[\frac{-2}{p_j}\right]$;

当 $j=t+1, 1\leqslant i\leqslant t$ 时, $r_{ij}=\left[p_j,-2n\right]_{p_i}$, 利用等式(2.2)计算可知 $\left[p_j,n\right]_{p_i}=\left[\frac{2}{p_i}\right]$;

当 $i=j=t+1$ 时, 利用等式(2.2)计算可知 $\left[p_j,-2n\right]_{p_i}=\left[\frac{2}{n}\right]$.

从而我们得到 $\mathbf{R}_{-2n}=\begin{pmatrix}\mathbf{A}+\mathbf{D}_2 & \mathbf{b}_2\\ \mathbf{b}_{-2}^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix}$. ∎

命题 3.7 令 $n=p_1\cdots p_t$ 是一个无平方因子的正奇数. 当 $n\equiv -1(\mathrm{mod}\,4)$ 时, 我们有

$$\mathbf{R}_n=\begin{pmatrix}\mathbf{A}+\mathbf{D}_{-1} & \mathbf{b}_2\\ \mathbf{b}_{-1}^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix},\quad \mathbf{R}_{-n}=\mathbf{A},$$

$$\mathbf{R}_{2n}=\begin{pmatrix}\mathbf{A}+\mathbf{D}_{-2} & \mathbf{b}_2\\ \mathbf{b}_{-2}^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix},\quad \mathbf{R}_{-2n}=\begin{pmatrix}\mathbf{A}+\mathbf{D}_2 & \mathbf{b}_2\\ \mathbf{b}_2^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix}.$$

证明 由 $n\equiv 3(\mathrm{mod}\,4)$ 可以得到此时二次域 $\mathbb{Q}(\sqrt{n})$ 的判别式 $D=4n$, 所以此时二次域 $\mathbb{Q}(\sqrt{n})$ 对应的 Rédei 矩阵为 $(t+1)\times(t+1)$ 阶. 当 $1\leqslant i\neq j\leqslant t$ 时, $r_{ij}=\left[p_j,n\right]_{p_i}$, 利用等式(2.1)计算可知 $\left[p_j,n\right]_{p_i}=\left[\frac{p_j}{p_i}\right]$;

当 $1\leqslant i=j\leqslant t$ 时, 利用等式(2.1)计算可知 $\left[p_i,n\right]_{p_i}=\left[\frac{-n/p_i}{p_i}\right]=\left[\frac{-1}{p_i}\right]+\left[\frac{n/p_i}{p_i}\right]$;

当 $i=t+1, 1\leqslant j\leqslant t$ 时, 利用等式(2.2)计算可知 $\left[p_j,n\right]_{p_i}=\left[\frac{-1}{p_i}\right]$;

当 $j=t+1, 1\leqslant i\leqslant t$ 时, 利用等式(2.2)计算可知 $\left[p_j,n\right]_{p_i}=\left[\frac{2}{p_i}\right]$;

当 $i=j=t+1$ 时, 利用等式(2.2)计算可知 $\left[p_j,n\right]_{p_i}=\left[\frac{2}{n}\right]$. 因此我们得到了 $\mathbf{R}_n=\begin{pmatrix}\mathbf{A}+\mathbf{D}_{-1} & \mathbf{b}_2\\ \mathbf{b}_{-1}^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix}$.

由 $n\equiv 3(\mathrm{mod}\,4)$ 可以得到此时二次域 $\mathbb{Q}(\sqrt{-n})$ 的判别式 $D=-n$, 所以此时二次域 $\mathbb{Q}(\sqrt{-n})$ 对应的 Rédei 矩阵为 $t\times t$ 阶. 当 $1\leqslant i\neq j\leqslant t$ 时, $r_{ij}=\left[p_j,-n\right]_{p_i}$, 利用等式(2.1)计算可知 $\left[p_j,-n\right]_{p_i}=\left[\frac{p_j}{p_i}\right]$;

当 $1\leqslant i=j\leqslant t$ 时, 利用等式(2.1)计算可知 $\left[p_i,-n\right]_{p_i}=\left[\frac{n/p_i}{p_i}\right]$. 即 $\mathbf{R}_{-n}=\mathbf{A}$.

考虑 $\mathbf{R}_{2n}=(r_{ij})_{(t+1)\times(t+1)}$, 当 $1\leqslant i\neq j\leqslant t$ 时, $r_{ij}=\left[p_j,2n\right]_{p_i}$, 利用等式(2.1)计算可知 $\left[p_j,2n\right]_{p_i}=\left[\frac{p_j}{p_i}\right]$. 当 $1\leqslant i=j\leqslant t$ 时, 利用等式(2.1)计算可知 $\left[p_i,2n\right]_{p_i}=\left[\frac{-2n/p_i}{p_i}\right]=\left[\frac{-2}{p_i}\right]+\left[\frac{n/p_i}{p_i}\right]$;

当 $i=t+1, 1\leqslant j\leqslant t$ 时, $r_{ij}=\left[p_j,2n\right]_{p_i}$, 利用等式(2.2)计算可知 $\left[p_j,2n\right]_{p_i}=\left[\frac{-2}{p_j}\right]$;

当 $j=t+1, 1\leqslant i\leqslant t$ 时, $r_{ij}=\left[p_j,2n\right]_{p_i}$, 利用等式(2.2)计算可知 $\left[p_j,2n\right]_{p_i}=\left[\frac{2}{p_i}\right]$;

当 $i=j=t+1$ 时, 利用等式(2.2)计算可知 $\left[p_j,2n\right]_{p_i}=\left[\frac{2}{n}\right]$.

从而我们得到 $\mathbf{R}_{2n}=\begin{pmatrix}\mathbf{A}+\mathbf{D}_{-2} & \mathbf{b}_2\\ \mathbf{b}_2^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix}$.

考虑 $\mathbf{R}_{-2n}=(r_{ij})_{(t+1)\times(t+1)}$, 当 $1\leqslant i\neq j\leqslant t$ 时, $r_{ij}=\left[p_j,-2n\right]_{p_i}$, 利用等式(2.1)计算可知 $\left[p_j,-2n\right]_{p_i}=\left[\frac{p_j}{p_i}\right]$. 当 $1\leqslant i=j\leqslant t$ 时, 利用等式(2.1)计算可知 $\left[p_i,-2n\right]_{p_i}=\left[\frac{2n/p_i}{p_i}\right]=\left[\frac{2}{p_i}\right]+\left[\frac{n/p_i}{p_i}\right]$;

当 $i=t+1,1\leqslant j\leqslant t$ 时, $r_{ij}=\left[p_j,-2n\right]_{p_i}$, 利用等式(2.2)计算可知 $\left[p_j,-2n\right]_{p_i}=\left[\frac{2}{p_j}\right]$;

当 $j=t+1,1\leqslant i\leqslant t$ 时, $r_{ij}=\left[p_j,-2n\right]_{p_i}$, 利用等式(2.2)计算可知 $\left[p_j,n\right]_{p_i}=\left[\frac{2}{p_i}\right]$;

当 $i=j=t+1$ 时, 利用等式(2.2)计算可知 $\left[p_j,-2n\right]_{p_i}=\left[\frac{2}{n}\right]$.

从而我们得到 $\mathbf{R}_{-2n}=\begin{pmatrix}\mathbf{A}+\mathbf{D}_{2} & \mathbf{b}_2\\ \mathbf{b}_{-2}^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix}$. ∎

推论 3.8 给定正整数 n 满足 $n\equiv 1(\mathrm{mod}\,4)$, $n=p_1\cdots p_t$, 其中 $p_i\equiv 1(\mathrm{mod}\,4)(1\leqslant i\leqslant t)$. 那么 $h_4(2n)=h_4(-2n)$ 成立; 若正整数 n 还满足 $n\equiv 5(\mathrm{mod}\,8)$, 那么 $h_4(n)=h_4(-n)$ 成立.

证明 因为在这里 $n\equiv 1(\mathrm{mod}\,4)$, 且 $p_i\equiv 1(\mathrm{mod}\,4)$. 所以

$$\mathbf{b}_{-2}^{\mathrm{T}}=\left(\left[\frac{-2}{p_1}\right],\cdots,\left[\frac{-2}{p_k}\right]\right)=\left(\left[\frac{2}{p_1}\right],\cdots,\left[\frac{2}{p_k}\right]\right)=\mathbf{b}_2^{\mathrm{T}},$$

$$\mathbf{D}_{-2}=\mathrm{diag}\left\{\left[\frac{-2}{p_1}\right],\cdots,\left[\frac{-2}{p_k}\right]\right\}=\mathrm{diag}\left\{\left[\frac{2}{p_1}\right],\cdots,\left[\frac{2}{p_k}\right]\right\}=\mathbf{D}_2.$$

此时

$$\mathbf{R}_{2n}=\begin{pmatrix}\mathbf{A}+\mathbf{D}_{-2} & \mathbf{b}_2\\ \mathbf{b}_2^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix}=\mathbf{R}_{-2n}.$$

从而有 $\mathrm{rank}_{\mathbb{F}_2}\mathbf{R}_{2n}=\mathrm{rank}_{\mathbb{F}_2}\mathbf{R}_{-2n}$.

此时 $h_4(2n)=t-\mathrm{rank}_{\mathbb{F}_2}\mathbf{R}_{2n}$, $h_4(-2n)=t-\mathrm{rank}_{\mathbb{F}_2}\mathbf{R}_{-2n}$, $h_4(2n)=h_4(-2n)$.

当 $n\equiv 5(\mathrm{mod}\,8)$, 且 $p_i\equiv 1(\mathrm{mod}\,4)$. 有

$$\mathbf{b}_{-1}^{\mathrm{T}}=\left(\left[\frac{-1}{p_1}\right],\cdots,\left[\frac{-1}{p_k}\right]\right)=\mathbf{0},\mathbf{D}_{-1}=\mathrm{diag}\left\{\left[\frac{-1}{p_1}\right],\cdots,\left[\frac{-1}{p_k}\right]\right\}=\mathbf{0},\left[\frac{2}{n}\right]=1.$$

此时由命题 3.6 可以得到

$$\mathbf{R}_n=\mathbf{A}+\mathbf{D}_{-1}=\mathbf{A},\quad \mathbf{R}_{-n}=\begin{pmatrix}\mathbf{A} & \mathbf{b}_2\\ \mathbf{b}_{-1}^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix}=\begin{pmatrix}\mathbf{A} & \mathbf{b}_2\\ \mathbf{0}^T & 1\end{pmatrix}.$$

从而有 $\operatorname{rank}_{\mathbb{F}_2}\mathbf{R}_n=\operatorname{rank}_{\mathbb{F}_2}\mathbf{A},\operatorname{rank}_{\mathbb{F}_2}\mathbf{R}_{-n}=\operatorname{rank}_{\mathbb{F}_2}\mathbf{A}+1.$

此时 $h_4(n)=t-1-\operatorname{rank}_{\mathbb{F}_2}\mathbf{A},h_4(-n)=t-\operatorname{rank}_{\mathbb{F}_2}\mathbf{A}-1.$ 这表明 $h_4(n)=h_4(-n)$ 成立. ∎

推论 3.9 给定正整数 $n\equiv 1(\bmod 4)$, $n=p_1\cdots p_t$, 其中 $p_i\equiv 1,7(\bmod 8)(1\leqslant i\leqslant t)$. 那么有等式

$$h_4(n)+1=h_4(-n)=h_4(2n)=h_4(-2n)$$

成立.

证明 因为在这里 $n\equiv 1(\bmod 4)$, 且 $p_i\equiv 1,7(\bmod 8)$. 所以由命题 3.6 可以得到

$$\mathbf{R}_n=\mathbf{A}+\mathbf{D}_{-1},\qquad \mathbf{R}_{-n}=\begin{pmatrix}\mathbf{A} & \mathbf{0}\\ \mathbf{b}_{-1}^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix},$$

$$\mathbf{R}_{2n}=\begin{pmatrix}\mathbf{A}+\mathbf{D}_{-1} & \mathbf{0}\\ \mathbf{0}^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix},\quad \mathbf{R}_{-2n}=\begin{pmatrix}\mathbf{A} & \mathbf{0}\\ \mathbf{b}_{-2}^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix}.$$

利用命题 3.5 可知只需计算矩阵 $\mathbf{R}'_{-n}=(\mathbf{A},\mathbf{0})$ 和 $\mathbf{R}'_{2n}=\left(\mathbf{A}+\mathbf{D}_{-1},\mathbf{0}\right)$ 和 $\mathbf{R}'_{2n}=(\mathbf{A},\mathbf{0})$ 的秩. 由参考文献[6]p10 的引理 4.1 可知 $\operatorname{rank}_{\mathbb{F}_2}\mathbf{A}=\operatorname{rank}_{\mathbb{F}_2}\left(\mathbf{A}+\mathbf{D}_{-1}\right)$ 从而有 $\operatorname{rank}_{\mathbb{F}_2}\mathbf{R}_n=\operatorname{rank}_{\mathbb{F}_2}\mathbf{R}_{-n}=\operatorname{rank}_{\mathbb{F}_2}\mathbf{R}_{2n}=\operatorname{rank}_{\mathbb{F}_2}\mathbf{R}_{-2n}.$

此时有等式

$$h_4(n)+1=h_4(-n)=h_4(2n)=h_4(-2n)$$

成立. ∎

推论 3.10 给定正整数 $n\equiv 1(\bmod 4)$, $n=p_1\cdots p_t$, 其中 $p_i\equiv 1,3(\bmod 8)(1\leqslant i\leqslant t)$. 那么有等式

$$h_4(n)+1=h_4(-2n),\quad h_4(2n)=h_4(-n)$$

成立.

证明 因为在这里 $n\equiv 1(\bmod 4)$, 且 $p_i\equiv 1,3(\bmod 8)$. 所以由命题 3.6 可以得到

$$\mathbf{R}_n=\mathbf{A}+\mathbf{D}_2,\qquad \mathbf{R}_{-n}=\begin{pmatrix}\mathbf{A} & \mathbf{b}_2\\ \mathbf{b}_{-1}^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix},$$

$$\mathbf{R}_{2n}=\begin{pmatrix}\mathbf{A} & \mathbf{b}_2\\ \mathbf{b}_2^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix},\quad \mathbf{R}_{-2n}=\begin{pmatrix}\mathbf{A}+\mathbf{D}_2 & \mathbf{b}_2\\ \mathbf{0}^{\mathrm{T}} & \left[\frac{2}{n}\right]\end{pmatrix}.$$

利用命题 3.5 可知只需计算矩阵 $\mathbf{R}'_{-n} = \left(\mathbf{A}, \mathbf{b}_2\right)$ 和 $\mathbf{R}'_{2n} = \left(\mathbf{A}, \mathbf{b}_2\right)$ 和 $\mathbf{R}'_{-2n} = \left(\mathbf{A}+\mathbf{D}_2, \mathbf{b}_2\right)$ 的秩. 由 $\mathbf{R}'_{-2n}$ 的每一行和为 0 可知 $\operatorname{rank}_{\mathbb{F}_2} \mathbf{R}'_{-2n} = \operatorname{rank}_{\mathbb{F}_2} \mathbf{A}+\mathbf{D}_2$ 从而有 $\operatorname{rank}_{\mathbb{F}_2} \mathbf{R}_n = \operatorname{rank}_{\mathbb{F}_2} \mathbf{R}_{-2n}, \operatorname{rank}_{\mathbb{F}_2} \mathbf{R}_{2n} = \operatorname{rank}_{\mathbb{F}_2} \mathbf{R}_{-n}$.

此时有等式

$$h_4(n)+1 = h_4(-2n), \quad h_4(2n) = h_4(-n)$$

成立. ∎

推论 3.11 给定正整数 $n \equiv 3(\bmod 4)$, $n = p_1 \cdots p_t$, 其中 $p_i \equiv 1, 3(\bmod 8)(1 \leqslant i \leqslant t)$. 那么此时有等式

$$h_4(n) = h_4(-2n)$$

成立, 若正整数 n 还满足 $n \equiv 3(\bmod 8)$, 那么有 $h_4(-n) = h_4(2n)$.

证明 利用命题 3.5 和命题 3.7 可知只需计算矩阵 $\mathbf{R}'_n = \left(\mathbf{A}+\mathbf{D}_{-1}, \mathbf{b}_2\right)$ 和 $\mathbf{R}'_{-2n} = \left(\mathbf{A}+\mathbf{D}_2, \mathbf{b}_2\right)$ 的秩.

又 $p_i \equiv 1, 3(\bmod 8)(1 \leqslant i \leqslant t)$, 所以 $\mathbf{D}_{-1} = \mathbf{D}_2$. 从而 $\operatorname{rank}_{\mathbb{F}_2} \mathbf{R}'_{-2n} = \operatorname{rank}_{\mathbb{F}_2} \mathbf{R}'_n$, 即 $h_4(n) = h_4(-2n)$. 若更进一步有 $n \equiv 3(\bmod 8)$, 那么

$$\mathbf{R}_{-n} = A, \quad \mathbf{R}_{2n} = \begin{pmatrix} \mathbf{A} & \mathbf{b}_2 \\ \mathbf{0}^{\mathrm{T}} & 1 \end{pmatrix}.$$

那么 $\operatorname{rank}_{\mathbb{F}_2} \mathbf{R}_{-n} + 1 = \operatorname{rank}_{\mathbb{F}_2} \mathbf{R}_{2n}$. 此时有 $h_4(-n) = h_4(2n)$ 成立. ∎

推论 3.12 给定正整数 $n \equiv 3(\bmod 4)$, $n = p_1 \cdots p_t$, 其中 $p_i \equiv 1, 7(\bmod 8)(1 \leqslant i \leqslant t)$. 那么此时有等式

$$h_4(n) = h_4(2n) = h_4(-2n) = h_4(-n)+1$$

成立.

证明 利用命题 3.5, 命题 3.7 和 $p_i \equiv 1, 7(\bmod 8)(1 \leqslant i \leqslant t)$ 可知只需计算矩阵 $\mathbf{R}'_n = \left(\mathbf{A}+\mathbf{D}_{-1}, \mathbf{0}\right)$ 和 $\mathbf{R}'_{2n} = \left(\mathbf{A}+\mathbf{D}_{-1}, \mathbf{0}\right)$ 和 $\mathbf{R}'_{-2n} = (\mathbf{A}, \mathbf{0})$ 的秩.

此时由参考文献[6]p10 的引理 4.1 可知 $\operatorname{rank}_{\mathbb{F}_2} \mathbf{R}_n = \operatorname{rank}_{\mathbb{F}_2} \mathbf{R}_{-n} = \operatorname{rank}_{\mathbb{F}_2} \mathbf{R}_{2n} = \operatorname{rank}_{\mathbb{F}_2} \mathbf{R}_{-2n}$. 所以等式 $h_4(n) = h_4(2n) = h_4(-2n) = h_4(-n)+1$ 成立. ∎

将上述推论整理汇总成如下几条:

当正整数 $n \equiv 1(\bmod 4)$:

- 当 $p_i \equiv 1(\bmod 4)(1 \leqslant i \leqslant t)$ 时, 有 $h_4(2n) = h_4(-2n)$; 若正整数 n 还满足 $n \equiv 5(\bmod 8)$, 有 $h_4(n) = h_4(-n)$.

- 当 $p_i \equiv 1,7(\mathrm{mod}\,8)(1 \leqslant i \leqslant t)$ 时, 有 $h_4(n)+1 = h_4(-n) = h_4(2n) = h_4(-2n)$.
- 当 $p_i \equiv 1,3(\mathrm{mod}\,8)(1 \leqslant i \leqslant t)$ 时, 有 $h_4(n)+1 = h_4(-2n), h_4(2n) = h_4(-n)$.

当正整数 $n \equiv 3(\mathrm{mod}\,4)$ 时:

- 当 $p_i \equiv 1,3(\mathrm{mod}\,8)(1 \leqslant i \leqslant t)$ 时, 有 $h_4(n) = h_4(-2n)$; 若正整数 n 还满足 $n \equiv 3(\mathrm{mod}\,8)$, 有 $h_4(-n) = h_4(2n)$.
- 当 $p_i \equiv 1,7(\mathrm{mod}\,8)(1 \leqslant i \leqslant t)$ 时, 有 $h_4(n) = h_4(2n) = h_4(-2n) = h_4(-n)+1$.

4 二次域类群的八阶秩

现在我们着手开始研究二次域类群的八阶秩, 此时我们注意到

$$r_8(C(F)) = \mathrm{rank}_{\mathbb{F}_2}\left(C(F)[2] \cap C(F)^4\right).$$

于是我们对二次域类群的八阶秩转为去研究群 $C(F)[2] \cap C(F)^4$ 的结构. 下面的这个命题可以帮助我们得到 $C(F)[2] \cap C(F)^4$ 的结构性质.

命题 4.1 对于任意 $d \in V \cap \mathbf{N}F$, 令 $(\alpha, \beta, \gamma) \in \mathbb{Z}_{>0}^2$ 为等式

$$d\alpha^2 - \frac{m}{d}\beta^2 = 4\gamma^2$$

的一个非平凡本原解, 那么我们有

(1) $[\mathfrak{d}] \in C(F)^4$ 当且仅当 $\left([\gamma, D]_{p_1}, \cdots, [\gamma, D]_{p_t}\right)^{\mathrm{T}} \in \mathrm{Im}\,\mathbf{R}_m$;

(2) $\sum_{i=1}^{t} [\gamma, D]_{p_i} = 0$.

证明 此证明主要参考文章[7]§ 2.

(1) 令 σ 表示域 F 的非平凡自同构. 对于 γ 的每个奇素因子, p 不整除 m 且 m 是模 p 的二次剩余. 因此主理想 $(p) = \mathfrak{p}\mathfrak{p}^\sigma$ 在 F 上分裂且 $[\gamma, D]_p = 0$. 我们现在证明 $x = \frac{d\alpha + \beta\sqrt{m}}{2} \in \mathcal{O}_F$.

- 若 d 是奇数且 m 是偶数, 那么 α, β 都为偶数, 所以 $x \in \mathcal{O}_F$.
- 若 d 和 m 是奇数, 那么 α, β 奇偶性相同. 若 α, β 都为偶数, 则 $x \in \mathcal{O}_F$; 若 α, β 都为奇数, 则 $4 \mid (d - m/d)$, 因此 $m \equiv 1 \bmod 4$, 所以 $x \in \mathcal{O}_F$.
- 若 d 是偶数, 那么 β 也为偶数, 因此 $m \equiv 1 \bmod 4$, 所以 $x \in \mathcal{O}_F$.

我们有 $p \mid d\gamma^2 = \mathbf{N}(x)$. 若 $\mathfrak{p}, \mathfrak{p}^\sigma$ 都整除 (x), 那么 (p) 整除 (x), 因此 p 整除 α, β, γ. 这与 (α, β, γ) 是一个本原解相矛盾. 所以 $\mathfrak{p}, \mathfrak{p}^\sigma$ 中仅有一个整除 (x). 我们不妨假定 $\mathfrak{p}^\sigma \mid (x)$.

假定 d 是一个奇数. 若 γ 为奇数, 我们有

$$(x) = \mathfrak{d}\prod_{p \mid \gamma} (\mathfrak{p}^\sigma)^{2v_p(\gamma)} = \gamma^2 \mathfrak{d}\mathfrak{c}^{-2}, \quad \text{这里}\mathfrak{c} := \prod_{p \mid \gamma} \mathfrak{p}^{v_p(\gamma)} \text{ 其中} \mathbf{N}\mathfrak{c} = \gamma. \tag{4.1}$$

若 γ 为偶数, 那么 m 也为偶数, α, β 都为奇数. $8 \mid (d - m/d)$, 所以 $m \equiv 1 \bmod 8$. 因此 $(2) = \mathfrak{q}\mathfrak{q}^\sigma$ 在 F 上分裂. 相似的, $\mathfrak{q}, \mathfrak{q}^\sigma$ 中仅有一个整除 (x), 假定 $\mathfrak{q}^\sigma$ 整除 (x). 因此我们同样有(4.1), 这里当 $p = 2$ 时 $\mathfrak{p} = \mathfrak{q}$.

假定 d 是一个偶数. 那么 D 是一个偶数, $m \not\equiv 1 \bmod 4$ 和 $(2) = \mathfrak{q}^2$ 在 F 上分歧. 相似的, 我们有(4.1), 这里当 $p = 2$ 有 $\mathfrak{p} = \mathfrak{p}^\sigma = \mathfrak{q}$.

现在我们知道 $[\mathfrak{d}]=[\mathfrak{c}]^2\in C(F)^4$ 当且仅当存在 $a\in V$ 使得 $[\boldsymbol{c}]+\left[\left(a,\omega_m\right)\right]\in C(F)^2$. 通过高斯型定理可以知道这等价于 $a\mathbf{N}c=a\gamma\in\mathbf{N}F$. 因为对于任意奇素数 $p|\gamma$, 有 $[D,a\gamma]_p=1$. 这等价于 $\mathbf{R}_m\mathbf{a}=\mathbf{c}$, 这里

$$\mathbf{a}=\left(v_{p_1}(a),\cdots,v_{p_t}(a)\right)^{\mathrm{T}},\quad \mathbf{c}=\left([\gamma,D]_{p_1},\cdots,[\gamma,D]_{p_t}\right)^{\mathrm{T}}.$$

(2) 若 $m\not\equiv 1 \bmod 4$, 那么 D 是一个偶数且

$$\sum_{i=1}^{t}[\gamma,D]_{p_i}=\sum_{p|\gamma'}[\gamma,D]_p=0.$$

若 $m\equiv 1 \bmod 4$ 且 γ 为一个奇数, 那么 $[\gamma,m]_2=0$; 若 $m\equiv 1 \bmod 4$ 且 γ 为一个偶数, 那么 $m\equiv 1 \bmod 8$ 且 $[\gamma,m]_2=0$. 因此有

$$\sum_{i=1}^{t}[\gamma,m]_{p_i}=\sum_{p|\gamma'}\left[\gamma_0,m\right]_p+[\gamma,m]_2=0.$$

∎

参考文献

[1] 张神星. 代数数论讲义 (v2.3)[M]. 2021: vi+163.

[2] Serre J. Graduate texts in mathematics: A course in arithmetic[M]. Springer New York, 2012.

[3] Neukirch J., Schappacher N. Grundlehren der mathematischen wissenschaften: Algebraic number theory[M]. Springer Berlin Heidelberg, 2013.

[4] Wang Z. Congruent elliptic curves with non-trivial Shafarevich-Tate groups[J]. Science in China A: Mathematics, 2016, 59(11): 2145-2166.

[5] Hecke E., Brauer G., Goldman J., Kotzen R. Graduate texts in mathematics: Lectures on the theory of algebraic numbers[M]. Springer New York, 2013.

[6] Wang Z., Zhang S. On the quadratic twist of elliptic curves with full 2-torsion[J]. 2022.

[7] Zhang S. On non-congruent numbers with $8a \pm 1$ type odd prime factors and tame kernels[J]. arXiv e-prints, 2021: arXiv:2111.11618.

致谢

行文至此, 意味着我大学五年的故事写到这里就要宣告落幕了. 始于 2017 年的金秋, 终于 2022 年的盛夏, 逐梦合工大, 终于迎来了倒计时. 回首在学校的五年生活, 从机械专业转而投入数学的海洋, 不仅学到了许多知识, 还交到了许多朋友. 但即使再不舍, 也到了说再见的时候了, 是时候踏上新的旅途, 去追寻更高的理想.

桃李不言, 下自成蹊. 感谢给我帮助的张神星老师. 无论是毕业设计的指导, 还是专业课程的学习, 修改到最后定稿. 张老师总是会给予耐心专业的解答. 感谢大学四年遇到的所有老师, 你们丰富了我的专业知识, 开拓了我的视野, 让我的大学四年受益匪浅. 祝老师们工作顺利, 生活如意, 桃李满天下, 春晖遍四方.

平生感知己, 方寸岂悠悠. 感谢我遇到的好朋友们, 是你们的存在丰富了我的青春色彩. 愿我们都能保持热爱, 奔赴各自精彩的未来. 愿我们未来顺遂, 携手相伴, 喜乐有分享, 共度日月长.

哀哀父母, 生我劬劳. 感恩父母二十余载对我的教育和培养, 惟孝顺父母, 可以解忧. 毕业后即将踏入新的征程, 我将会更加努力, 为社会为家庭做出我自己的贡献. 感恩我的母校, 你见证了我五年的青春生涯, 我见证了你五年的落叶繁花. 最后, 由衷感谢各位指导老师在百忙之中对本文进行评审并提出宝贵意见.

作者：刘旭鸿

2022 年 05 月 15 日