university of groningen

faculty of science and engineering

On finding imaginary quadratic fields where the class group has higher p-rank

Master Project Mathematics

August 2018

Student: P.L. Los

First supervisor: Prof.dr. J. Top

Second supervisor: Dr.ir. F.W. Wubs

ON FINDING IMAGINARY QUADRATIC FIELDS WHERE THE CLASS GROUP HAS HIGHER p-RANK

P.L. LOS

Abstract. In this thesis, we derive an isomorphism between some subgroup of the multiplicative group of an algebraic number field modulo m-th powers and the elements of the class group that have order dividing m. Using p-adic techniques it can be tested whether elements in this subgroup are different or even independent, providing a way to find independent elements of order dividing m in the class group. This can be used to find lower bounds on the q-rank of the class group (for primes q dividing m).
In case of imaginary quadratic fields, a correspondence between cubic norm equations and ideal classes of order dividing 3 as used by D.A. Buell [Bue76] and D. Shanks and R. Serafin [SS73] is studied. After making this correspondence precise, it is generalised to arbitrary odd m, and it is interpreted in terms of the isomorphism above. Furthermore, results of J.J. Solderitsch [Sol92], M. Craig [Cra73] and Y. Yamamoto [Yam70] about independency of elements of specific order in the class group are interpreted as special cases of the independence-showing above.
Finally, the isomorphism above is used to consider a relation between rational points on elliptic curves and elements of order dividing 3 in class groups of quadratic fields as described by M. van Beek [Bee10].

Contents

1. Introduction 3
2. Prerequisites 3
2.1. Algebraic Number Fields and Quadratic Fields 3
2.2. Valuations 7
2.3. p-Adic Numbers 8
3. An isomorphism between a subgroup of K^*/K^{*m} and $\mathcal{O}_K^*/\mathcal{O}_K^{*m} \times Cl_K[m]$ 9
3.1. Valuations modulo three on K^*/K^{*3}. 9
3.2. A map g from $\ker(v)$ to the class group Cl_K 10
3.3. Examples illustrating §3.1 and §3.2 12
3.4. Proving independence in $Cl_K[m]$ using p-adic techniques. 18
4. A relation between norm equations and elements of a specific order in Cl_K 21
4.1. Introduction: the idea used by D.A. Buell and by D. Shanks & R. Serafin 21
4.2. Solutions of a cubic norm equation versus elements of $Cl_K[3]$ 23
4.3. Generalisation of §4.2 to arbitrary odd $m \geqslant 3$ 27
4.4. Comparing the correspondence in §4.3 with the isomorphism of Proposition 3.4 33
5. Independent elements in $Cl_K[m]$ 35
5.1. Solderitsch 35
5.2. Craig, Yamamoto 37
6. From rational points on certain elliptic curves to $Cl_K[3]$ 38
6.1. Van Beek: $E_{A,B}(\mathbb{Q}) \longrightarrow \mathbb{Q}(\sqrt{A})^*/\mathbb{Q}(\sqrt{A})^{*3}$ 38
6.2. From Van Beek's elliptic curves to the norm equation of §4.2 39
7. Conclusions and outlook 41
References 42
8. Appendix: Tables 43

1. Introduction

In algebraic number theory, a well known problem is the Gauss class number problem, which is to give for each positive integer h a complete list of all imaginary quadratic fields with class number h, i.e. having a class group consisting of precisely h ideal classes. In this thesis, we consider a closely related problem: how to find imaginary quadratic fields where the class group contains a specific subgroup? In particular, given a prime number p, we want to find class groups with a lot of independent elements of order p. The main reasons for doing this are: directly obtaining a better understanding of the class groups of quadratic fields, and providing examples of class groups with high p-rank which can be used when developing other theory about class groups of imaginary quadratic fields.
Already in 1970, Yoshihiko Yamamoto published an article [Yam70] which contains a large part of the theory considered in this thesis, as he described criteria to solutions of some equation to yield imaginary quadratic fields with a class group containing a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Maurice Craig used the same methods [Cra73] to obtain class groups containing a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. James J. Solderitsch [Sol92] describes another method to explicitely find imaginary quadratic fields with p-rank at least 2. In this thesis we also considered work of Duncan A. Buell [Bue76] who describes a method to find class groups of 3-rank $\geqslant 3$ using a correspondence between solutions of cubic norm equations and ideals in classes of order dividing 3.
In this thesis, we start with describing an isomorphism between some subgroup of an algebraic number field K modulo m-th powers and elements in the class group of order dividing m. Instead of proving independence of the classes of different ideals by considering their norms, we derive a method to prove independence by considering the corresponding elements in K^*/K^{*m} using p-adic techniques.
This theory is used to interpret the methods used in the articles described above, especially the relation between solutions of norm equations and ideals in classes of specific order, and the methods to prove that such solutions yield independent elements in the class group.
In the end, we notice the relation between this theory, and a relation between elliptic curves and class groups as occurs in the master's thesis of Monique van Beek [Bee10].

2. Prerequisites

2.1. Algebraic Number Fields and Quadratic Fields.

This thesis is mainly about the class groups of algebraic number fields, or, more specific, imaginary quadratic fields. In this section we recall some basic information about those fields and introduce some notation used throughout this paper.

An *algebraic number field* (or *number field*), in this thesis usually denoted by K, is a finite - and hence algebraic - field extension of the field of rational numbers $\mathbb{Q}$. A *quadratic field* is an algebraic number field where this extension has degree two, in other words: an extension of $\mathbb{Q}$ with some $\sqrt{d}$ (where d is a square-free integer unequal to 0 or 1, and $\sqrt{d}$ is a zero of the polynomial $X^2 - d$). If $d = -D$ is negative, such a quadratic field $K = \mathbb{Q}(\sqrt{-D})$ is called an *imaginary* quadratic field (as opposed to *real* quadratic fields), and it can be embedded in $\mathbb{C}$ by mapping $\sqrt{-D}$ to either $i\sqrt{D}$ or $-i\sqrt{D}$.

The *ring of integers* - denoted by $\mathcal{O}_K$ - of an algebraic number field K is the ring containing al elements of K that are a root of a monic polynomial with coefficients in $\mathbb{Z}$. We often use the fact that an algebraic number field K is the field of fractions of its ring of integers.
For $\mathbb{Q}$ the ring of integers is simply $\mathbb{Z}$. For other algebraic number fields, which are always extensions of $\mathbb{Q}$, this is always a finitely generated $\mathbb{Z}$-module.
For quadratic number fields we have the following: Let d be a square-free integer unequal to 0 or 1, and let $K = \mathbb{Q}(\sqrt{d})$, then the ring of integers $\mathcal{O}_K$ of K is given by:

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{d}\right] & \text{if} \quad d \equiv 1 \bmod 4 \\ \mathbb{Z}\left[\sqrt{d}\right] & \text{if} \quad d \not\equiv 1 \bmod 4 \end{cases}$$

The *discriminant* of an algebraic number field K we denote by Δ_K. For a quadratic field $K = \mathbb{Q}(\sqrt{d})$ as above, we have:

$$\Delta_K = \begin{cases} d & \text{if} \quad d \equiv 1 \bmod 4 \\ 4d & \text{if} \quad d \not\equiv 1 \bmod 4 \end{cases}$$

Although a norm can be defined on algebraic number fields in general, we only make use of the following norm map on quadratic fields:
Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field as above, then the norm of an element $b + c\sqrt{d} \in K$ is given by $N(b + c\sqrt{d}) = b^2 - c^2 d$. Note that for imaginary quadratic fields (with $d = -D < 0$) the norm $N(b + c\sqrt{-D}) = b^2 + c^2 D$ is positive for all nonzero elements in K, whereas for real quadratic fields it may be negative.

2.1.1. *Units and the unit group.*
In general, the *units* R^* of a ring R are the elements of R with a multiplicative inverse in R. Hence for a field K, the units K^* are all nonzero elements of K.
By the *unit group* of an algebraic number field K, we mean the units $\mathcal{O}_K^*$ of its ring of integers.
About the structure of the unit group of an algebraic number field, there is the following well known theorem:

Theorem 2.1. *(Dirichlet's unit theorem for the unit group of an algebraic number field) Let K be an algebraic number field with r real embeddings and s pairs of complex embeddings, and let U_K be the group of roots of unity in $\mathcal{O}_K$. Then U_K is finite, and $\mathcal{O}_K^* \cong U_K \times \mathbb{Z}^{r+s-1}$.*

For a more general version and proof of this theorem, we refer to [Ste17].

Consider as an example the field of rationals $\mathbb{Q}$. For $\mathbb{Q}$ we have $r = 1$, $s = 0$, which implies $\mathcal{O}_{\mathbb{Q}}^* \cong U_{\mathbb{Q}} \times \mathbb{Z}^0$. So $\mathbb{Z}^*$ consists of only the group of roots of unity $U_{\mathbb{Q}} = \{\pm 1\} \subset \mathbb{Z}$, which is obviously true.

For real quadratic fields $K = \mathbb{Q}(\sqrt{d})$, we have $r = 2$ (sending $\sqrt{d} \in K$ to either $\sqrt{d}$ or $-\sqrt{d}$ in $\mathbb{R}$), $s = 0$, which implies $\mathcal{O}_K^* \cong U_K \times \mathbb{Z} = \{\pm 1\} \times \mathbb{Z}$.
So for real quadratic fields, the unit group is generated by two elements: -1 and one *fundamental unit* $\eta \in \mathcal{O}_K^*$, all other units are of the form $\pm 1 \cdot \eta^k \quad (k \in \mathbb{Z})$.

For imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-D})$, we have $r = 0$ and $s = 1$. So $r + s - 1 = 0$, hence $\mathcal{O}_K^* = U_K$ and $\mathcal{O}_K$ contains no fundamental units.
For $D = 1$, $\mathcal{O}_K$ is the Gaussian integers and $\mathcal{O}_K^* = U_K = \{\pm 1, \pm i\}$.
For $D = 3$, $\mathcal{O}_K^* = U_K = \{\pm 1, \pm \frac{1+\sqrt{3}i}{2}, \pm \frac{1-\sqrt{3}i}{2}\}$.
For $D > 3$ square-free, $\mathcal{O}_K^* = U_K = \{\pm 1\}$.

2.1.2. *Ideals, Prime Ideals and Unique Ideal Factorisation.*
Let K be an algebraic number field with ring of integers $\mathcal{O}_K$.
In this thesis, whenever we speak of an *ideal*, we mean *integral $\mathcal{O}_K$-ideal*, i.e. a subgroup of the additive group of $\mathcal{O}_K$, closed under multiplication by elements of $\mathcal{O}_K$.
For *principal* ideals, which are generated by one single element $a \in \mathcal{O}_K$, we use the notation $(a) := a \cdot \mathcal{O}_K$.
In quadratic fields, all ideals can be written as generated by at most two elements in $\mathcal{O}_K$.
Sometimes we will use the notion of *fractional ($\mathcal{O}_K$-)ideal*, which is defined as a nonzero $\mathcal{O}_K$-module $I \subset K$ such that there exists a nonzero element $a \in \mathcal{O}_K$ for which $aI \subset \mathcal{O}_K$.

In $\mathcal{O}_K$, we don't have unique factorisation of elements, but we do have unique factorisation of ideals into prime ideals, a fact we frequently will use.

The prime ideals of $\mathcal{O}_K$ can be described using the Kummer-Dedekind theorem, of which a proof can be found in [Ste17].
We here present a slightly simpler version of the theorem.

Theorem 2.2. *(Kummer-Dedekind) Let $\mathcal{O}_K = \mathbb{Z}[\alpha]$ be the ring of integers of an algebraic number field K, and let $f \in \mathbb{Z}[x]$ be the minimal polynomial of α.*

Let p be a $\mathbb{Z}$-prime and write

$$f(x) \equiv \prod_{i=1}^{s} (f_i(x))^{e_i} \mod p$$

with the $f_i(x)$ monic irreducible polynomials in $Z[x]$ and different mod p. *Then we have*

$$(p) = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$$

where $\mathfrak{p}_i = p\mathcal{O}_K + f_i(\alpha)\mathcal{O}_K$ are the prime ideals above p.

A prime p is called:
inert if $s = e_1 = 1$, i.e. if (p) is a prime ideal itself,
splitting if $s > 1$, i.e. if there are different prime ideals above p,
and *ramifying* if there is a prime ideal $\mathfrak{p}_i$ above p with *ramification index* $e_i > 1$.

In the case of quadratic fields, the minimal polynomial is quadratic, and it is easy to show that for each prime p either:
$p|\Delta_K$, in which case p ramifies and (p) is the square of some prime ideal $(p) = \mathfrak{p}^2$,
or p splits into two different prime ideals $(p) = \mathfrak{pq}$,
or p is inert.

2.1.3. *Class Groups.*
On nonzero ideals and fractional ideals, we can define an equivalence relation: two (fractional) ideals I and J are equivalent if there are nonzero elements $a, b \in \mathcal{O}_K$ for which $(a)I = (b)J$. The equivalence classes are called *ideal classes*, and the ideal class of I we denote by $[I]$. On the set of ideal classes we can define addition by multiplication of the representing ideals. With this addition, the ideal classes form a group, the *ideal class group*, which we denote by Cl_K.

It is easy to see that all principal ideals belong to the same ideal class: the *trivial* ideal class, which is the zero-element of Cl_K.
The class group is trivial if and only if $\mathcal{O}_K$ is a unique factorisation domain.

Theorem 2.3. *(Minkowski's bound) Let K be an algebraic number field of degree n over $\mathbb{Q}$ with s pairs of complex embeddings. Then every ideal class in Cl_K contains an integral ideal of norm less than or equal to Minkowski's bound:*

$$M_K = \left(\frac{4}{\pi}\right)^s \cdot \frac{n!}{n^n} \cdot \sqrt{|\Delta_K|}$$

For a proof of this theorem, we refer to [Ste17].

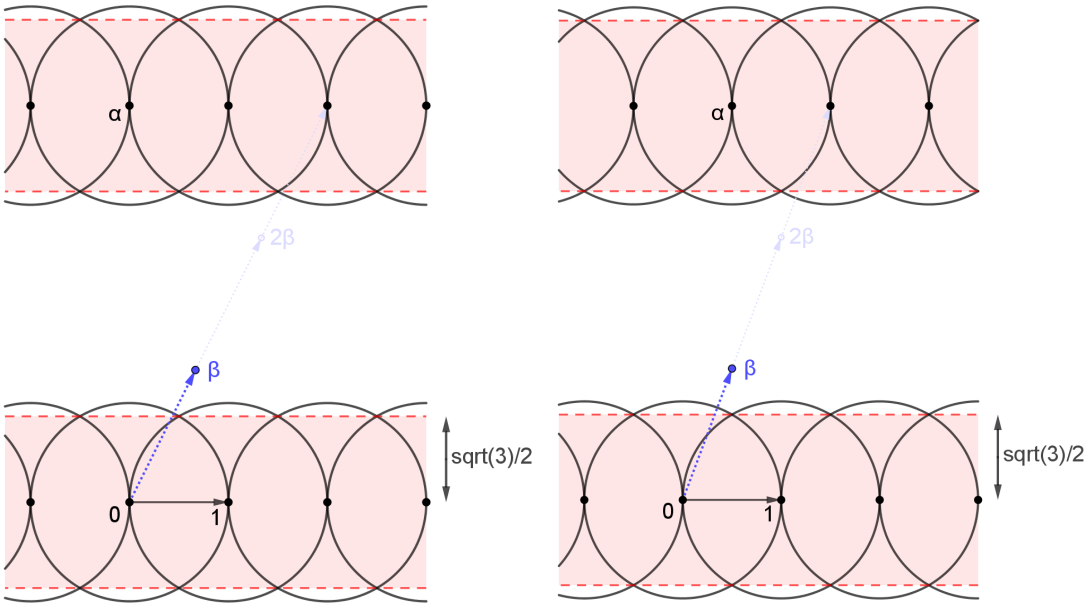
For real quadratic fields, this reduces to $M_K = \frac{1}{2}\sqrt{|\Delta_K|}$,
and for imaginary quadratic fields $M_K = \frac{2}{\pi}\sqrt{|\Delta_K|}$.

Let m be a positive integer, and p be a prime number.
The group of all ideal classes in Cl_K which have order divisible by m, we denote by $Cl_K[m]$.
With the p-rank of Cl_K, we mean the dimension of $Cl_K[p]$ seen as a vectorspace over $\mathbb{F}_p$.

2.1.4. *On the Norm of Ideals of Ideal Classes in the Class Group of an Imaginary Quadratic Field.*

Proposition 2.4. *Let K be an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$ with $D \in \mathbb{Z}$, $D > 3$ square-free. The discriminant of K is denoted Δ_K, the ring of integers $\mathcal{O}_K = \mathbb{Z}[\alpha]$ with $\alpha = \begin{cases} \frac{1}{2} + \frac{1}{2}\sqrt{-D} & \text{if } D \equiv 3 \mod 4 \\ \sqrt{-D} & \text{if } D \not\equiv 3 \mod 4 \end{cases}$, and the class group Cl_K.*
Every ideal class in Cl_K contains an integral $\mathcal{O}_K$-ideal of norm strictly less than $\sqrt{|\Delta_K|/3} = \begin{cases} \sqrt{D/3} & \text{if } D \equiv 3 \mod 4, \\ 2\sqrt{D/3} & \text{if } D \not\equiv 3 \mod 4. \end{cases}$

Proof. Suppose we have an ideal class in Cl_K. Let $\mathfrak{a}$ be an integral $\mathcal{O}_K$-ideal which represents this class. Let a be a nonzero element of minimal norm in $\mathfrak{a}$ and consider the fractional $\mathcal{O}_K$-ideal $I = \frac{1}{a}\mathfrak{a}$.
Because a is a nonzero element of minimal norm in $\mathfrak{a}$, we have that $1 = \frac{a}{a}$ is a nonzero element of minimal norm in I. Therefore either $I = (1)$ which implies $\mathfrak{a} \sim (1)$ which is an integral $\mathcal{O}_K$-ideal of norm $1 < \sqrt{|\Delta_K|/3}$ and we are done, or $I = (1, \beta)$ for some $\beta \in K$, $\beta \notin \mathcal{O}_K$. We write $\beta = b + c\alpha$ with $b, c \in \mathbb{Q}$ and choose β such that $c \geq 0$ is minimal. Because 1 has minimal norm in I, we have $N(\beta - \gamma) \geq N(1) = 1$ for all $\gamma \in I$.



(A) $D \not\equiv 3 \mod 4$, $\alpha = \sqrt{-D}$ (B) $D \equiv 3 \mod 4$, $\alpha = \frac{1}{2} + \frac{1}{2}\sqrt{-D}$

Therefore $\begin{cases} c\frac{\sqrt{D}}{2} & > & \frac{\sqrt{3}}{2} & \text{if } D \equiv 3 \mod 4 \\ c\sqrt{D} & > & \frac{\sqrt{3}}{2} & \text{if } D \not\equiv 3 \mod 4 \end{cases}$ (equality is not possible because $D \neq 3$) and $nc = 1$ for some integer $n \in \mathbb{N}$ (otherwise c was not minimal). But then also $n \cdot b \in \mathbb{Z}$, and $n \cdot I = (n, n\beta) = (n, nb + \alpha)$ is an integral $\mathcal{O}_K$-ideal of norm $n = \frac{1}{c} < \begin{cases} \sqrt{\frac{D}{3}} & \text{if } D \equiv 3 \mod 4 \\ 2\sqrt{\frac{D}{3}} & \text{if } D \not\equiv 3 \mod 4 \end{cases}$.
Because $a \cdot nI = n \cdot \mathfrak{a}$ we have that $[\mathfrak{a}] = [nI]$ and we are done. □

Proposition 2.5. *Let $K = \mathbb{Q}(\sqrt{-D})$ an imaginary quadratic field with $D \in \mathbb{Z}$ square-free and $D > 3$.*
Every ideal class in Cl_K contains at most one ideal $\mathfrak{a}$ which is not divisible by any $\mathbb{Z}$-prime p and which has norm $N(\mathfrak{a})$ less than $\sqrt{|\Delta_K|/4}$.

Proof. Suppose $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of norm smaller than $\sqrt{|\Delta_K|/4}$ in the same ideal class in Cl_K and both not divisible by any $\mathbb{Z}$-prime p.
Because $[\mathfrak{a}] = [\mathfrak{b}]$, we have that there exists some $\gamma \in K^*$ such that $\mathfrak{b} = \gamma\mathfrak{a}$. Hence we have $\mathfrak{a}\overline{\mathfrak{b}} = \mathfrak{a}\overline{\gamma}\overline{\mathfrak{a}} = \overline{\gamma} \cdot N(\mathfrak{a})$. By assumption, the norm of $\mathfrak{a}\overline{\mathfrak{b}}$ is smaller than $|\Delta_K|/4$, so $\overline{\gamma} \cdot N(\mathfrak{a})$ is an element of $\mathcal{O}_K$ of norm smaller than $|\Delta_K|/4$. Therefore $\overline{\gamma} \cdot N(\mathfrak{a}) \in \mathbb{Z}$, and hence $\gamma = \overline{\gamma} = \frac{b}{a}$ for some $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$. So we have that $b\mathfrak{a} = a\gamma\mathfrak{a} = a\mathfrak{b}$ is an integral ideal which is divisible by all $\mathbb{Z}$-primes dividing a or b. By unique ideal factorisation, this yields $a|\mathfrak{a}$ and $b|\mathfrak{b}$, which by assumption implies that $a = b = \pm 1$, and hence $\mathfrak{a} = \mathfrak{b}$. □

Theorem 2.6. *Let $K = \mathbb{Q}(\sqrt{-D})$ an imaginary quadratic field with $D \in \mathbb{Z}$ square-free and $D > 3$.*
Every ideal class in Cl_K of order $\neq 2$ contains a unique ideal of minimal norm, which is by Proposition 2.4 strictly less than $\sqrt{|\Delta_K|/3}$.

Proof. $\mathcal{O}_K = \mathbb{Z}[\alpha]$ with $\alpha = \begin{cases} \frac{1}{2} + \frac{1}{2}\sqrt{-D} & \text{if } D \equiv 3 \mod 4; \\ \sqrt{-D} & \text{if } D \not\equiv 3 \mod 4. \end{cases}$
Let $\mathfrak{a} \subset \mathcal{O}_K$ be an ideal, with ideal class $[\mathfrak{a}] \in Cl_K$ of order $\neq 2$. Write $\mathfrak{a} = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z}$ with α_1 an nonzero element of minimal norm in $\mathfrak{a}$, and subsequently α_2 an element of $\mathfrak{a}$ with minimal norm for which $\alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} = \mathfrak{a}$. We claim that $N(\alpha_1) \neq N(\alpha_2)$.

Indeed, suppose $N(\alpha_1) = N(\alpha_2)$. As fractional ideals, we then have

$$\frac{1}{\alpha_1}\mathfrak{a} = \mathbb{Z} + \frac{\alpha_2}{\alpha_1}\mathbb{Z} = \frac{\alpha_2}{\alpha_1} \cdot \left(\mathbb{Z} + \frac{\alpha_1}{\alpha_2}\mathbb{Z}\right) = \frac{1}{\overline{\alpha_2}}\overline{\mathfrak{a}},$$

since the assumption on the norms implies $\overline{\alpha_1/\alpha_2} = \alpha_2/\alpha_1$. As $[\mathfrak{a}]^{-1} = [\overline{\mathfrak{a}}]$ and the order of $[\mathfrak{a}]$ is not two, it follows that $\mathfrak{a} = (\beta)$ for some $\beta \in \mathcal{O}_K$. The minimal norm in this ideal is clearly $N(\beta)$, so it follows that $\alpha_j = u_j \cdot \beta$ with $u_j \in \mathcal{O}_K^*$. Because $D > 3$, $u_j = \pm 1$ and therefore α_1, α_2 are not independent over $\mathbb{Z}$. This contradiction shows that $N(\alpha_1) \neq N(\alpha_2)$.

Consider the fractional ideal $I = \frac{1}{\alpha_1}\mathfrak{a} = \mathbb{Z} + \frac{\alpha_2}{\alpha_1}\mathbb{Z}$.
Changing the sign of α_2 if necessary, we can assume $\mathrm{Im}(\frac{\alpha_2}{\alpha_1}) > 0$. Because the norm of α_2 is as small as possible, we have $-\frac{1}{2} \leqslant \mathrm{Re}(\frac{\alpha_2}{\alpha_1}) \leqslant \frac{1}{2}$, and moreover replacing α_2 by $\alpha_2 + \alpha_1$ if necessary, we have $-\frac{1}{2} < \mathrm{Re}(\frac{\alpha_2}{\alpha_1}) \leqslant \frac{1}{2}$.
Similar to the argument used in the proof of Proposition 2.4, we will now show that unique $n, m \in \mathbb{Z}$ exist with $n\frac{\alpha_2}{\alpha_1} = \alpha + m$. Moreover the constructed fraction $\frac{\alpha_2}{\alpha_1}$ is the same for every choice of the ideal $\mathfrak{a}$ representing the class $[\mathfrak{a}]$. In particular, n, m are uniquely determined by $[\mathfrak{a}]$.

Indeed, given any fractional ideal $\mathfrak{b}$ representing $[\mathfrak{a}]$, we have $\mathfrak{b} = \lambda\mathfrak{a} = \lambda(\alpha_1\mathbb{Z} + \alpha_2\mathbb{Z})$ for some $\lambda \in K^*$. From this, the unicity of $\tau = \alpha_2/\alpha_1$ with $|\tau| > 1$ and $-\frac{1}{2} < \mathrm{Im}(\tau) \leq \frac{1}{2}$ follows.
Since $\mathfrak{a} \subset \mathcal{O}_K$ is an ideal containing α_1, it also contains $\alpha \cdot \alpha_1$. As α_1, α_2 is a basis of $\mathfrak{a}$ as a module over $\mathbb{Z}$, there exist unique integers n, m with $\alpha \cdot \alpha_1 = -m\alpha_1 + n\alpha_2$.

We will now determine the integral $\mathcal{O}_K$-ideal of smallest norm in the class $[\mathfrak{a}]$. A fractional ideal in this class is $\frac{1}{\alpha_1}\mathfrak{a} = \mathbb{Z} + \frac{\alpha_2}{\alpha_1}\mathbb{Z} = \mathbb{Z} + \frac{\alpha+m}{n}\mathbb{Z}$. Choosing $a \in K^*$ of minimal positive norm such that $(a) \cdot (\mathbb{Z} + \frac{\alpha+m}{n}\mathbb{Z}) \subset \mathcal{O}_K$, we obtain the integral ideal $(a, a\frac{\alpha+m}{n})$ representing $[\mathfrak{a}]$, and this is an integral ideal of minimal norm in this class. In particular $a \in \mathcal{O}_K$.
If $a \in \mathbb{Z}$, then $a = \pm n$.
We claim that the case $a \notin \mathbb{Z}$ does not occur. So suppose $a \in \mathcal{O}_K \setminus \mathbb{Z}$. By minimality of a we have $N(a) \leq n^2$. Write $a = k\alpha + l$ for integers k, l; since $a \notin \mathbb{Z}$, we have $k \neq 0$. We may assume $k > 0$.
From $N(\alpha_1) \neq N(\alpha_2)$ and $-\frac{1}{2} < \mathrm{Re}(\frac{\alpha_1}{\alpha_2}) \leq \frac{1}{2}$ we obtain

$$|n| < |\alpha + m| = \sqrt{|\mathrm{Re}(\alpha) + m|^2 + |\mathrm{Im}(\alpha)|^2} \leqslant \sqrt{|\frac{n}{2}|^2 + |\mathrm{Im}(\alpha)|^2}.$$

Therefore $|\mathrm{Im}(\alpha)| > \frac{1}{2}\sqrt{3}|n|$ and hence $|a| = |k\alpha + l| > \frac{k}{2}\sqrt{3}|n|$. From $N(a) \leqslant n^2$ it follows that $k = 1$ and $a = \alpha + l$ and $(\alpha + l)\frac{\alpha+m}{n} \in \mathcal{O}_K$. Moreover $N(\alpha + m) > n^2 \geqslant N(a) = N(\alpha + l)$ implies that $|\mathrm{Re}(\alpha) + l| < |\mathrm{Re}(\alpha) + m|$.

We compute $(\alpha + l)\frac{\alpha+m}{n} = \frac{\alpha^2+(l+m)\alpha+lm}{n} = \frac{(l+m+2\cdot\mathrm{Re}(\alpha))\alpha+q}{n}$ for some $q \in \mathbb{Z}$. So n divides $l + m + 2 \cdot \mathrm{Re}(\alpha)$. But from $-\frac{1}{2} < \mathrm{Re}(\frac{\alpha_2}{\alpha_1}) \leqslant \frac{1}{2}$ it follows that $|\mathrm{Re}(\alpha + l)| < |\mathrm{Re}(\alpha + m)| \leqslant \frac{|n|}{2}$, therefore

$$|l + m + 2 \cdot \mathrm{Re}(\alpha)| \leqslant |\mathrm{Re}(\alpha + l)| + |\mathrm{Re}(\alpha + m)| < |n|.$$

The real part of $(\alpha + l) + (\alpha + m)$ is nonzero since we saw $|\mathrm{Re}(\alpha + l)| < |\mathrm{Re}(\alpha + m)|$.

Since n divides the nonzero integer $l + m + 2 \cdot \mathrm{Re}(\alpha)$ and also $|n| > |l + m + 2 \cdot \mathrm{Re}(\alpha)|$, we have a contradiction.
We conclude that the ideal of smallest norm in $[\mathfrak{a}]$ is given by $(n, \alpha + m)$ and that it is unique. □

2.2. **Valuations.**

Throughout this thesis, we often need to know things about how often an element of a field is divisible by some prime number or prime ideal. Valuations on a field provide some kind of measure of the size or the divisibility of elements.
In this subsection, first we give the general definition of a valuation, subsequently we describe the most basic examples of valuations: the p-adic valuations on $\mathbb{Q}$, and we conclude with a generalisation of those examles to the valuations on algebraic number fields used in this thesis.

2.2.1. *General definition.*
In general, let K be a field and let $(G, +, \geqslant)$ be a totally ordered abelian group (for example the integers or the rationals). Extend the set, the group law and the ordering by adding one element "∞" satisfying: $\infty \geqslant g$ and $g + \infty = \infty + g = \infty$ for all $g \in G$.
Now a *valuation* v on K is a map $v : K \to G \cup \{\infty\}$ satisfying the following conditions for all $a, b \in K$:
1) $v(a) = \infty$ if and only if $a = 0$,
2) $v(a) + v(b) = v(ab)$,
3) $v(a + b) \geqslant \min\{v(a), v(b)\}$ with equality if $v(a) \neq v(b)$.
Note that the first two conditions imply that the restriction of v to K^* defines a group homomorphism from K^* to the *valuation group* $v(K^*) \subset G$.

A valuation v is called *trivial* if $v(a) = 0$ for all $a \in K^*$.

Two valuations v and $\tilde{v}$ are *equivalent* if there exists an order-preserving isomorphism between $v_1(K^*)$ and $v_2(K^*)$.

2.2.2. *p-adic valuations.*
The most basic examples of nontrivial valuations are the p-adic valuations on $\mathbb{Q}$, which measure how often an element of $\mathbb{Q}$ is divisible by the prime p:
Let p be a prime in $\mathbb{Z}$, then the p-adic valuation $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is given by:

$$v_p(x) = \begin{cases} \infty & \text{for} \quad x = 0, \\ \max\{n \in \mathbb{Z}_{\geqslant 0} \text{ such that } p^n | x\} & \text{for} \quad x \in \mathbb{Z}_{\neq 0}, \\ v_p(m) - v_p(n) & \text{for} \quad x = \frac{m}{n} \text{ with } m, n \in \mathbb{Z}. \end{cases}$$

For example $v_3(45) = 2$ (the valuation *at* 3 *of* 45 is 2), and $v_5(\frac{10}{75}) = 1 - 2 = -1$.

2.2.3. *Generalisation to Algebraic Number Fields.*
The construction of p-adic valuations on $\mathbb{Q}$ uses the fact that $\mathbb{Z}$ is a unique factorisation domain. In a general algebraic number field K, we in general don't have unique prime factorisation anymore, but we do have unique ideal factorisation into prime ideals. Analogue to the p-adic valuations on $\mathbb{Q}$ we can for each prime ideal $\mathfrak{p}$ define a $\mathfrak{p}$-adic valuation on K:
Let K be an algebraic number field, and let $\mathfrak{p}$ be an $\mathcal{O}_K$-prime ideal. Then the $\mathfrak{p}$-adic valuation $v_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\}$ is defined by:

$$v_\mathfrak{p}(x) = \begin{cases} \infty & \text{for} \quad x = 0, \\ \max\{n \in \mathbb{Z}_{\geqslant 0} \text{ such that } x \in \mathfrak{p}^n, x \notin \mathfrak{p}^{n+1}\} & \text{for} \quad x \in \mathcal{O}_K,\ x \neq 0, \\ v_\mathfrak{p}(m) - v_\mathfrak{p}(n) & \text{for} \quad x = \frac{m}{n} \text{ with } m, n \in \mathcal{O}_K. \end{cases}$$

Note that for nonzero $x \in \mathcal{O}_K$ the number "$\max\{n \in \mathbb{Z}_{\geqslant 0}$ such that $x \in \mathfrak{p}^n, x \notin \mathfrak{p}^{n+1}\}$" is equal to "$\max\{n \in \mathbb{Z}_{\geqslant 0}$ such that $\mathfrak{p}$ occurs n times in the ideal factorisation of the ideal $x \cdot \mathcal{O}_K\}$".

2.3. p-Adic Numbers.

In Section 3.4 we need some basic p-adic theory to prove independence of certain elements in $Cl_K[m]$, so in this section we will provide a short explanation of p-adic numbers and state Hensel's lemma. For a more detailed explanation, see for example the book of N. Koblitz on p-adic numbers [Kob77].

The idea is to construct a "complete" field in which elements of $\mathbb{Q}$ are "smaller" when their p-adic valuation is higher (when they are more often divisible by p) - this instead of neglecting elements divisible by p completely as in modular arithmetic.

Let K be a field. A *norm* on K is a map $|| \ || : K \to \mathbb{R}_{\geqslant 0}$ such that for all $a, b \in K$:
1) $||a|| = 0$ if and only if $a = 0$,
2) $||a \cdot b|| = ||a|| \cdot ||b||$,
3) $||a + b|| \leqslant ||a|| + ||b||$ (the triangle inequality).
Such a norm is called *non-Archimedean* if $||a + b|| \leqslant \max(||a||, ||b||)$ (for all $a, b \in K$). Otherwise it is called *Archimedean*, like for example the usual absolute value.

Using the p-adic valuations on $\mathbb{Q}$ of the previous section, we can construct corresponding non-Archimedean norms on $\mathbb{Q}$: $|x|_p = \begin{cases} 0 & \text{for } x = 0, \\ p^{-v_p(x)} & \text{for } x \neq 0. \end{cases}$

Now we follow Koblitz [Kob77] in constructing the p-adic field $\mathbb{Q}_p$ for a given prime number p: Recall that a sequence $\{a_i\}$ is a Cauchy sequence with respect to the norm $|\ |_p$ if for all $\varepsilon > 0$ there exists some $N \in \mathbb{N}$ such that $|a_i - a_j| < \varepsilon$ whenever $i, j > N$.
Define an equivalence relation on such Cauchy sequences: $\{a_i\} \sim \{b_i\}$ if $\lim_{i\to\infty} |a_i - b_i|_p = 0$.
The field of the p-adic numbers $\mathbb{Q}_p$ is now defined as the set of all equivalence classes of Cauchy sequences (with respect to the norm $|\ |_p$ and the equivalence relation described above). Addition, subtraction and multiplication of those classes are defined by addition, subtraction and multiplication of (elements of) representants, for example $[\{a_i\}]\cdot[\{b_i\}] = [\{a_i \cdot b_i\}]$. To find the multiplicative inverse of a nonzero class $[\{a_i\}]$, note that it is possible to find a representative $\{a_i\} \in [\{a_i\}]$ where all a_i are nonzero, and $\{\frac{1}{a_i}\}$ represents the multiplicative inverse of $[\{a_i\}]$.

The field of rational numbers $\mathbb{Q}$ can be seen as the subfield of $\mathbb{Q}_p$ consisting of all classes represented by a constant Cauchy sequence.

On $\mathbb{Q}_p$ we have the norm $|[\{a_i\}]|_p = \lim_{i\to\infty} |a_i|_p$. The ring of *$p$-adic integers* denoted by $\mathbb{Z}_p$ is the subring of $\mathbb{Q}_p$ consisting of all classes of norm less than or equal to 1. Koblitz states the following theorem to provide a simpler way to look at the p-adic numbers:

Theorem 2.7. [Kob77] *Every equivalence class a in $\mathbb{Q}_p$ for which $|a|_p \leqslant 1$ has exactly one representative Cauchy sequence of the form $\{a_i\}$ for which:*
1) $0 \leqslant a_i < p^i$ for $i = 1, 2, 3, \ldots$,
2) $a_i \equiv a_{i+1} \mod p^i$ for $i = 1, 2, 3, \ldots$.

This implies that a class $a \in \mathbb{Z}_p$ can be seen as a number

$$a = b_0 + b_1 p + b_2 p^2 + \text{“higher order terms”} \text{ (with } b_i \in \{0, 1, \ldots, p-1\}),$$

and in general, that a class $a \in \mathbb{Q}_p$ can be seen as a number

$$a = \frac{1}{p^m}\left(b_0 + b_1 p + b_2 p^2 + \text{“higher order terms”}\right) \quad (\text{with } m \in \mathbb{Z}, \quad b_i \in \{0, 1, \ldots, p-1\}).$$

It follows that in $\mathbb{Z}_p$ the *p-adic units* $\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p | \frac{1}{a} \in \mathbb{Z}_p\}$ are those elements in $\mathbb{Z}_p$ for which the number b_0 in the expansion above is nonzero.

2.3.1. *Hensel's lemma.*
An often used theorem is Hensel's lemma. For the proof we refer again to Koblitz [Kob77].

Theorem 2.8. *(Hensel's lemma) Let $f(x)$ be a polynomial in $\mathbb{Z}_p[x]$, and $f'(x)$ its derivative. Let $a \in \mathbb{Z}_p$ such that $f(a) \equiv 0 \mod p$ and $f'(a) \not\equiv 0 \mod p$. Then there exists a unique $b \in \mathbb{Z}_p$ such that $f(b) = 0$ and $b \equiv a \mod p$.*

3. An isomorphism between a subgroup of K^*/K^{*m} and $\mathcal{O}_K^*/{\mathcal{O}_K^*}^m \times Cl_K[m]$

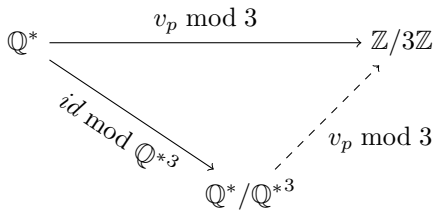
Let K be a number field. In this section we look at the relation between K^*/K^{*m} and $Cl_K[m]$, the part of the class group of K consisting of all elements of order dividing m. Our goal is to show that a specific subgroup “$\ker(v)$” of K^*/K^{*m} is isomorphic to $\mathcal{O}_K^*/{\mathcal{O}_K^*}^m \times Cl_K[m]$.
This gives us a way to describe $Cl_K[m]$ in terms of elements of K^*/K^{*m}, especially for imaginary quadratic fields where in general $\mathcal{O}_K^*/{\mathcal{O}_K^*}^m$ is trivial.

We first will look at the case where $m = 3$, but all steps hold for any natural number m, so in the end we will generalise and the results hold for all $m \in \mathbb{N}$.

3.1. Valuations modulo three on K^*/K^{*3}.

Suppose we have some algebraic number field K. The nonzero elements in K form the multiplicative group K^*, and the cubes in K^* form a subgroup K^{*3}. We will discuss the factor group K^*/K^{*3}.

Take for example $K = \mathbb{Q}$. Writing a nonzero element $r \in \mathbb{Q}$ as $r = n/d$ for coprime integers n, d, we have for each prime p that $v_p(r) = v_p(n) - v_p(d)$. In this way $v_p \bmod 3$ defines a homomorphism $\mathbb{Q}^* \to \mathbb{Z}/3\mathbb{Z}$ which clearly contains $\mathbb{Q}^{*3}$ in its kernel. Hence one obtains a corresponding homomorphism, which we also denote by $v_p \bmod 3$, from $\mathbb{Q}^*/\mathbb{Q}^{*3}$ to $\mathbb{Z}/3\mathbb{Z}$:



Example: $\frac{7}{18} \cdot \mathbb{Q}^{*3} = \frac{7}{2\cdot 3\cdot 3} \cdot \mathbb{Q}^{*3} = 2 \cdot 3 \cdot 3 \cdot 7 \cdot \mathbb{Q}^{*3}$, its valuation modulo 3 at 2 is 2 mod 3, its valuation modulo 3 at 3 is 1 mod 3, its valuation modulo 3 at 7 is 1 mod 3, and its valuation at all other primes is 0 mod 3.

So for each prime p we have a map

$$\begin{array}{ccc} \mathbb{Q}^*/\mathbb{Q}^{*3} & \xrightarrow{\quad v_p \bmod 3 \quad} & \mathbb{Z}/3\mathbb{Z} \\ \cup & & \cup \\ \alpha\mathbb{Q}^{*3} & \longmapsto & v_p(\alpha) \bmod 3 \end{array}$$

We can combine those maps for all primes p into one single map to a direct product of copies of $\mathbb{Z}/3\mathbb{Z}$, or to a direct sum because for each element all but finitely many valuations are 0 mod 3.

$$\begin{array}{ccc} \mathbb{Q}^*/\mathbb{Q}^{*3} & \xrightarrow{\quad v \ \text{(“all } v_p \bmod 3\text{”)} \quad} & \bigoplus_{\text{primes } p} \mathbb{Z}/3\mathbb{Z} \\ \cup & & \cup \\ \alpha\mathbb{Q}^{*3} & \longmapsto & (v_{p_1}(\alpha) \bmod 3,\ \ v_{p_2}(\alpha) \bmod 3,\ \ v_{p_3}(\alpha) \bmod 3,\ \ \dots) \end{array}$$

In this example where $K = \mathbb{Q}$, the kernel of this map v is zero and $\mathbb{Q}^*/\mathbb{Q}^{*3} \cong \bigoplus_{\text{primes } p} \mathbb{Z}/3\mathbb{Z}$. This is because $\mathbb{Q}$ is a principal ideal domain, but in general the kernel of this map could be nonzero and will tell us something about the nonprincipal ideals of K.

For a general number field K with ring of integers $\mathcal{O}_K$ we can construct the same map v:

$$\begin{array}{ccc} K^*/K^{*3} & \xrightarrow{\quad v \ \text{(“all } v_{\mathfrak{p}} \bmod 3\text{”)} \quad} & \bigoplus_{\text{all } \mathcal{O}_K\text{-prime ideals } \mathfrak{p}} \mathbb{Z}/3\mathbb{Z} \\ \cup & & \cup \\ \alpha K^{*3} & \longmapsto & (v_{\mathfrak{p}_1}(\alpha) \bmod 3,\ \ v_{\mathfrak{p}_2}(\alpha) \bmod 3,\ \ v_{\mathfrak{p}_3}(\alpha) \bmod 3,\ \ \dots) \end{array}$$

3.2. **A map g from $\ker(v)$ to the class group Cl_K.**

For any element $\alpha K^{*3} \in K^*/K^{*3}$, we can choose (by multiplying α by a suitable element of K^{*3}) the representative α such that $\alpha \in \mathcal{O}_K$.

Suppose we have $\alpha K^{*3} \in \ker v$ where we choose $\alpha \in \mathcal{O}_K$. The ideal $\alpha\mathcal{O}_K$ has a unique factorisation into prime ideals. The valuation $v_{\mathfrak{p}}(\alpha)$ of α at any prime ideal $\mathfrak{p}$ is divisible by 3 (because $\alpha \in \ker v$), therefore $\alpha\mathcal{O}_K = \mathfrak{p}_1^{3q_1}\mathfrak{p}_2^{3q_2} \cdot \ldots \cdot \mathfrak{p}_n^{3q_n}$ for certain prime ideals $\mathfrak{p}_j$, certain rational integers q_j and some unit $u \in \mathcal{O}_K^*$.

Lemma 3.1. *The decomposition into prime ideals described above induces a homomorphism g from $\ker(v)$ to Cl_K:*

$$\begin{array}{ccc} K^*/K^{*3} & \xrightarrow{v \text{ (“all } v_{\mathfrak{p}} \bmod 3\text{”)}} & \bigoplus_{\text{all } \mathcal{O}_K\text{-prime ideals } \mathfrak{p}} \mathbb{Z}/3\mathbb{Z} \\ \cup & & \\ \ker(v) & \xrightarrow{\quad g \quad} & Cl_K \\ \cup & & \cup \\ \alpha K^{*3} & \longmapsto & [\mathfrak{p}_1^{q_1}\mathfrak{p}_2^{q_2}\cdot\dots\cdot\mathfrak{p}_n^{q_3}], \\ \left(\alpha\mathcal{O}_K = \mathfrak{p}_1^{3q_1}\mathfrak{p}_2^{3q_2}\cdot\dots\cdot\mathfrak{p}_n^{3q_n}\right). & & \end{array}$$

Proof. First we show that g is well-defined. Suppose we have $\alpha, \beta \in \mathcal{O}_K$ representing the same class αK^{*3} in $\ker(v)$. Writing $\alpha\mathcal{O}_K = \prod \mathfrak{p}_j^{3q_j}$ and $\beta\mathcal{O}_K = \prod \mathfrak{q}_j^{3r_j}$ we have to show that $\prod \mathfrak{p}_j^{q_j}$ and $\prod \mathfrak{q}_j^{r_j}$ represent the same element in Cl_K.

By assumption $\beta K^{*3} = \alpha K^{*3}$, so nonzero $\zeta, \eta \in \mathcal{O}_K$ exist such that $\beta = \left(\frac{\zeta}{\eta}\right)^3 \alpha$, i.e., $\zeta^3\alpha = \eta^3\beta$. But then we have:

$$\begin{array}{rcll} [\mathfrak{p}_1^{q_1}\mathfrak{p}_2^{q_2}\cdot\dots\cdot\mathfrak{p}_n^{q_n}] & = & [(\zeta)] + [\mathfrak{p}_1^{q_1}\mathfrak{p}_2^{q_2}\cdot\dots\cdot\mathfrak{p}_n^{q_n}] & \text{(because } \zeta\mathcal{O}_K \text{ is a principal ideal)} \\ & = & [\zeta\cdot\mathfrak{p}_1^{q_1}\mathfrak{p}_2^{q_2}\cdot\dots\cdot\mathfrak{p}_n^{q_n}] & \\ & = & [\eta\cdot\mathfrak{q}_1^{r_1}\mathfrak{q}_2^{r_2}\cdot\dots\cdot\mathfrak{q}_m^{r_m}] & \text{(using } \zeta^3\alpha = \eta^3\beta \text{ and unique factorization of ideals)} \\ & = & [(\eta)] + [\mathfrak{q}_1^{r_1}\mathfrak{q}_2^{r_2}\cdot\dots\cdot\mathfrak{q}_m^{r_m}] & \\ & = & [\mathfrak{q}_1^{r_1}\mathfrak{q}_2^{r_2}\cdot\dots\cdot\mathfrak{q}_m^{r_m}], & \end{array}$$

showing that g is well-defined.

To complete the proof, we show that g is a group homomorphism:
For $\alpha K^{*3},\ \beta K^{*3} \in \ker(v)$ we have:

$$\begin{array}{rcl} g(\alpha K^{*3}) + g(\beta K^{*3}) & = & [\mathfrak{p}_1^{q_1}\mathfrak{p}_2^{q_2}\cdot\dots\cdot\mathfrak{p}_n^{q_n}] + [\mathfrak{q}_1^{r_1}\mathfrak{q}_2^{r_2}\cdot\dots\cdot\mathfrak{q}_m^{r_m}] \\ & = & [\mathfrak{p}_1^{q_1}\mathfrak{p}_2^{q_2}\cdot\dots\cdot\mathfrak{p}_n^{q_n}\cdot\mathfrak{q}_1^{r_1}\mathfrak{q}_2^{r_2}\cdot\dots\cdot\mathfrak{q}_m^{r_m}] \\ & = & g(\alpha\beta K^{*3}). \end{array}$$

□

Proposition 3.2. *The following sequence is exact:*

$$1 \longrightarrow \mathcal{O}_K^*/{\mathcal{O}_K^*}^3 \longrightarrow \ker(v) \xrightarrow{g} Cl_K[3] \longrightarrow 0.$$

Proof. The proof consists of showing that the image of g is $Cl_K[3]$ and that the kernel of g is a subgroup of $\ker(v)$ isomorphic to $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$.

The image of g
As g is a homomorphism from $\ker(v)$ to Cl_K, the image of g is some subgroup of Cl_K. We will now show that this subgroup is $Cl_K[3]$.
($\subset$) Suppose we have some $\alpha K^{*3} \in \ker(v)$. We can write $\alpha\cdot\mathcal{O}_K = \mathfrak{p}_1^{3q_1}\mathfrak{p}_2^{3q_2}\cdot\dots\cdot\mathfrak{p}_n^{3q_n}$ and we get

$$3\cdot g(\alpha K^{*3}) = g(\alpha^3 K^{*3}) = \left[\mathfrak{p}_1^{3q_1}\mathfrak{p}_2^{3q_2}\cdot\dots\cdot\mathfrak{p}_n^{3q_n}\right] = [(\alpha)] = 0.$$

($\supset$) On the other side, suppose we have some ideal class $[\mathfrak{p}_1^{q_1}\mathfrak{p}_2^{q_2}\cdot\dots\cdot\mathfrak{p}_n^{q_n}]$ for which $3\cdot[\mathfrak{p}_1^{q_1}\mathfrak{p}_2^{q_2}\cdot\dots\cdot\mathfrak{p}_n^{q_n}] = 0$. Then $\mathfrak{p}_1^{3\cdot q_1}\mathfrak{p}_2^{3\cdot q_2}\cdot\dots\cdot\mathfrak{p}_n^{3\cdot q_n} = (\mathfrak{p}_1^{q_1}\mathfrak{p}_2^{q_2}\cdot\dots\cdot\mathfrak{p}_n^{q_n})^3$ is principal, so $\exists\alpha \in \mathcal{O}_K$ with $(\alpha) = \mathfrak{p}_1^{3q_1}\mathfrak{p}_2^{3q_2}\cdot\dots\cdot\mathfrak{p}_n^{3q_n}$. We see that $v(\alpha K^{*3}) = 0$, i.e. $\alpha K^{*3} \in \ker(v)$, and $g(\alpha K^{*3}) = [\mathfrak{p}_1^{q_1}\mathfrak{p}_2^{q_2}\cdot\dots\cdot\mathfrak{p}_n^{q_n}]$. Combining this, we conclude that the image of g is $Cl_K[3]$.

The kernel of g
We prove that the kernel of g is the subgroup of $\ker(v)$ given by $\mathcal{O}_K^*\cdot K^{*3}$.
($\subset$) Let $\alpha K^{*3} \in \ker(v)$ with $\alpha \in \mathcal{O}_K$ and suppose $g(\alpha K^{*3}) = 0$. Then we can write $\alpha\cdot\mathcal{O}_K = \mathfrak{p}_1^{3q_1}\cdot\mathfrak{p}_2^{3q_2}\cdot\ldots\cdot\mathfrak{p}_n^{3q_n}$ where $\mathfrak{p}_1^{q_1}\cdot\mathfrak{p}_2^{q_2}\cdot\ldots\cdot\mathfrak{p}_n^{q_n}$ is a principal $\mathcal{O}_K$-ideal (β). Therefore the prime ideal factorisation of $\frac{\alpha}{\beta^3}\cdot\mathcal{O}_K$ does not contain any prime ideal, and hence $\alpha K^{*3} = \frac{\alpha}{\beta^3}K^{*3}$ is an element of $\mathcal{O}_K^*\cdot K^{*3}$.

($\supset$) In the reverse direction, suppose $\alpha K^{*3} \in \mathcal{O}_K^* \cdot K^{*3}$. We may choose $\alpha \in \mathcal{O}_K^*$ which implies that $\alpha \cdot \mathcal{O}_K$ does not contain any prime ideal, and hence $g(\alpha K^{*3}) = 0$.
We conclude that the kernel of g is $\mathcal{O}_K^* \cdot K^{*3}$, which is isomorphic to ${\mathcal{O}_K^*}/{\mathcal{O}_K^*}^3$. □

So far we considered K^* modulo third powers and therefore we took valuations modulo three and constructed a map to $Cl_K[3]$. We can generalise this by choosing any natural number m instead of 3. This is described in the next diagram:

$$\begin{array}{ccccccc}
 & & & & \gamma & \longmapsto & (v_{\mathfrak{p}}(\gamma) \bmod m)_{\mathfrak{p} \text{ prime}} \\
 & & & & \cap & & \cap \\
\mathcal{O}_K{}^* \cdot K^{*m} & \subset & K^*/K^{*m} & \xrightarrow{v \text{ (“all } v_{\mathfrak{p}} \bmod m\text{”)}} & \bigoplus_{\text{all } \mathcal{O}_K\text{-prime ideals } \mathfrak{p}} & & \mathbb{Z}/m\mathbb{Z} \\
\| & & \cup & & & & \\
\ker(g) & \xrightarrow{\text{id}} & \ker(v) & \xrightarrow{g} & Cl_K[m] & \subset & Cl_K \\
 & & \cup & & \cup & & \\
 & & \alpha K^{*m} & \longmapsto & [\mathfrak{p}_1^{q_1}\mathfrak{p}_2^{q_2} \cdot \cdots \cdot \mathfrak{p}_n^{q_n}], & &
\end{array}$$

$$(\alpha \mathcal{O}_K = \mathfrak{p}_1^{mq_1}\mathfrak{p}_2^{mq_2} \cdot \cdots \cdot \mathfrak{p}_n^{mq_n}).$$

In this way, we get

Theorem 3.3. *The following sequence is exact:*

$$1 \longrightarrow {\mathcal{O}_K^*}/{\mathcal{O}_K^*}^m \longrightarrow \ker(v) \xrightarrow{g} Cl_K[m] \longrightarrow 0.$$

Proof. Analogous to the proof of Proposition 3.2. □

In the special case of imaginary quadratic number fields with discriminant < -4, and $m \geqslant 3$ odd, Theorem 3.3 reduces to the following.

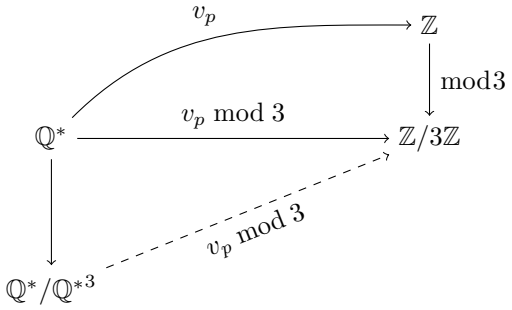
Proposition 3.4. *Suppose $m \in \mathbb{Z}_{\geqslant 3}$ is an odd integer. Let $D \in \mathbb{Z}_{>3}$ be square-free and take $K = \mathbb{Q}(\sqrt{-D})$. Then g defines an isomorphism $\ker(v) \cong Cl_K[m]$.*

Proof. For K as given here, we have $\mathcal{O}_K^* = \{\pm 1\}$ and therefore ${\mathcal{O}_K^*}/{\mathcal{O}_K^*}^m$ is trivial. (The unit -1 is an m-th power because m is odd.) The proposition now follows from Theorem 3.3. □

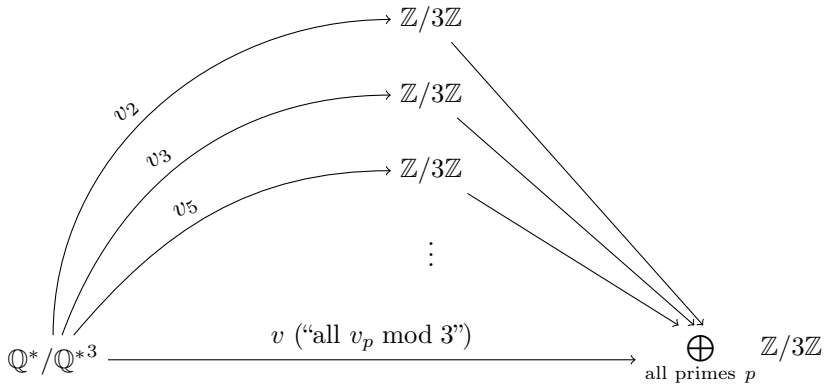
3.3. **Examples illustrating §3.1 and §3.2.**

Example 1: $K = \mathbb{Q}$
(In this example both Cl_K (the class group) and ${\mathcal{O}_K^*}/{\mathcal{O}_K^*}^3$ (the unit group of the ring of integers modulo cubes) are trivial.)

On $\mathbb{Q}^*$ we have for each prime p the valuation $v_p : \mathbb{Q}^* \longrightarrow \mathbb{Z}$. Composing this with reduction modulo 3 one obtains a homomorphism “$v_p \bmod 3$” : $\mathbb{Q}^* \longrightarrow \mathbb{Z}/3\mathbb{Z}$.
The subgroup $\mathbb{Q}^{*3}$ is in the kernel of this homomorphism, so one can divide out this subgroup and obtain a homomorphism “$v_p \bmod 3$” : $\mathbb{Q}^*/\mathbb{Q}^{*3} \longrightarrow \mathbb{Z}/3\mathbb{Z}$.



For each prime p we have this map v_p mod 3, so we can combine those maps into a homeomorphism v from $\mathbb{Q}^*/\mathbb{Q}^{*3}$ to a direct sum of copies of $\mathbb{Z}/3\mathbb{Z}$ [1].



Any element of $\mathbb{Q}^*/\mathbb{Q}^{*3}$ can be written as $\frac{s}{t}\mathbb{Q}^{*3} = st^2\mathbb{Q}^{*3}$ where we can choose s, t positive (since -1 is a cube) and cube free and such that $\gcd(s,t) = 1$.
We see that $v(st^2\mathbb{Q}^{*3})$ (which is an element of $\bigoplus_{\text{all primes } p} \mathbb{Z}/3\mathbb{Z}$) is 1 mod 3 at all primes that occur in the prime factorisation of s, and 2 mod 3 at all primes that occur in the prime factorisation of t. To be in the kernel of v, both s and t have to be one, so in this case $\ker(v) = \{\overline{1}\}$ $(= \mathbb{Z}^*/\mathbb{Z}^{*3})$ and v is an isomorphism. (It is easy to see that v is surjective.) In particular one obtains (again) the well known fact that the class group of $\mathbb{Q}$ is trivial.

Example 2a: $K = \mathbb{Q}(\sqrt{-3})$
(This is an example where Cl_K is trivial, but $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$ isn't.)

$K = \mathbb{Q}(\sqrt{-3})$ is a quadratic field with discriminant $-3 \equiv 1 \mod 4$, so the ring of integers $\mathcal{O}_K$ of K is given by $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{-3}]$. $\mathcal{O}_K$ is a principal ideal domain[2], so each prime ideal $\mathfrak{p}_i$ is generated by an irreducible element π_i of $\mathcal{O}_K$. The valuations on K correspond to the prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$. Those prime ideals are obtained by writing, for any prime number p in $\mathbb{Z}$, the ideal $(p) = p\mathcal{O}_K$ as a product of prime ideals of $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$. For example $(3) = {\mathfrak{p}_3}^2$ and $(5) = (5)$ and $(7) = \mathfrak{p}_7\mathfrak{q}_7$ in $\mathcal{O}_K$, where $\mathfrak{p}_3 = (\sqrt{-3})$, $\mathfrak{p}_7 = (2 + \sqrt{-3})$, $\mathfrak{q}_7 = (2 - \sqrt{-3})$, and $\sqrt{-3}$, $2 + \sqrt{-3}$ and $2 - \sqrt{-3}$ are irreducible elements of $\mathcal{O}_K$.
Like in the example above we can construct the homomorphism

$$v \text{ ("all } v_{\mathfrak{p}} \text{ mod 3")} \quad : \quad \mathbb{Q}(\sqrt{-3})^*/{\mathbb{Q}(\sqrt{-3})^*}^3 \longrightarrow \bigoplus_{\text{all } \mathcal{O}_K\text{-prime ideals } \mathfrak{p}} \mathbb{Z}/3\mathbb{Z}.$$

We will now look at the kernel of this map v. First, for every prime ideal $\mathfrak{p}$ choose a generator $\pi \in \mathcal{O}_K$.
The elements of $\mathbb{Q}(\sqrt{-3})^*$ can be written in the form $u \cdot \pi_{i_1}^{q_{i_1}} \cdot \ldots \cdot \pi_{i_n}^{q_{i_n}}$ with $u \in \mathcal{O}_K^*$ a unit and $\pi_{i_j}^{q_{i_j}}$ powers of the chosen generators of the prime ideals. Therefore the elements of $\mathbb{Q}(\sqrt{-3})^*/{\mathbb{Q}(\sqrt{-3})^*}^3$ can be represented by the elements $\overline{u} \cdot \pi_{i_1} \cdot \ldots \cdot \pi_{i_m} \cdot \pi_{i_{m+1}}^2 \cdot \ldots \cdot \pi_{i_n}^2$ where $\overline{u} \in \mathcal{O}_K^*/{\mathcal{O}_K^*}^3$.
To be in the kernel of v no π_i should occur here, so the only elements in the kernel of v are those represented by elements $\overline{u}$ of $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$.
The units $\mathcal{O}_K^*$ of $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{-3}]$ are ± 1, $\pm\left(\frac{1}{2} + \frac{1}{2}\sqrt{-3}\right)$ and $\pm\left(\frac{1}{2} - \frac{1}{2}\sqrt{-3}\right)$. So we get ${\mathcal{O}_K^*}^3 = \{\pm 1\}$ and $\ker(v)$ is (isomorphic to) $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3 = \left\{\overline{1}, \overline{\frac{1}{2} + \frac{1}{2}\sqrt{-3}}, \overline{\frac{1}{2} - \frac{1}{2}\sqrt{-3}}\right\} \cong \mathbb{Z}/3\mathbb{Z}$.

Because $\mathcal{O}_K$ is a principal ideal domain the class group Cl_K is trivial, and hence so is $Cl_K[3]$. We see that indeed $\ker(v)$ is isomorphic to $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3 \times Cl_K[3] \cong \mathbb{Z}/3\mathbb{Z}$ here.

[1] By definition, elements of this direct sum have to be nonzero at only finitely many of those copies of $\mathbb{Z}/3\mathbb{Z}$, but this is no problem because the valuation of any element of $\mathbb{Q}^*$ (and hence of any element of $\mathbb{Q}^*/\mathbb{Q}^{*3}$) is nonzero (or $\not\equiv 0 \mod 3$) at only finitely many primes.

[2] Indeed, here $\mathcal{O}_K$ is Euclidean with respect to the norm $N(z) = z \cdot \overline{z}$ as is easily verified.

Example 2b: $K = \mathbb{Q}(\sqrt{2})$
(This is another example where Cl_K is trivial, but $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$ isn't.)

Consider the norm map $N\colon K \to \mathbb{Q}$ given for $a, b \in \mathbb{Q}$ by $N(a+b\sqrt{2}) = a^2 - 2b^2$.
The norm of $1+\sqrt{2}$ is $N(1+\sqrt{2}) = -1$, so $1+\sqrt{2}$ is a unit, but not a cube in $\mathcal{O}_K$: if it were a cube, then $1+\sqrt{2} = (a+b\sqrt{2})^3$, hence $(a-b\sqrt{2})^3 = 1-\sqrt{2}$ and hence $\left(|a|+|b|\sqrt{2}\right)^3 \in \left\{\pm\left(1+\sqrt{2}\right), \pm\left(1-\sqrt{2}\right)\right\}$. But then $|a|$ and $|b|$ have to be less than or equal to 1, which is not possible. We conclude that $1+\sqrt{2}$ defines a nontrivial element of $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$. The Dirichlet unit theorem implies that $\mathcal{O}_K^* \cong \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})$, so as a consequence

$$\mathcal{O}_K^*/{\mathcal{O}_K^*}^3 \cong \mathbb{Z}/3\mathbb{Z}.$$

We conclude that the class of $1+\sqrt{2}$ generates this group of order 3.

The ring $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ is Euclidean with respect to the absolute value of the norm, hence in particular it is a principal ideal domain. This means that its class group is trivial, and $\ker(v) \subset K^*/{K^*}^3$ is therefore generated by the class of $1+\sqrt{2}$ in the present case.

Example 3: $K = \mathbb{Q}(\sqrt{-23})$
(An example where $Cl_K[3]$ is not trivial, but $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$ is.)

Because $K = \mathbb{Q}(\sqrt{-23})$ is a quadratic field with discriminant $-23 \equiv 1 \mod 4$, its ring of integers $\mathcal{O}_K$ is $\mathbb{Z}[\frac{1}{2}+\frac{1}{2}\sqrt{-23}]$.
Again we can construct the "all valuations mod 3"-homomorphism v from $K^*/{K^*}^3$ to the direct sum over all $\mathcal{O}_K$-prime ideals $\mathfrak{p}$:

$$v\ (\text{"all } v_{\mathfrak{p}} \text{ mod 3"}) \quad : \quad \mathbb{Q}(\sqrt{-23})^*/{\mathbb{Q}(\sqrt{-23})^*}^3 \longrightarrow \bigoplus_{\text{all } \mathbb{Z}[\frac{1}{2}+\frac{1}{2}\sqrt{-23}]\text{-prime ideals } \mathfrak{p}} \mathbb{Z}/3\mathbb{Z}$$

The units of $\mathbb{Z}[\frac{1}{2}+\frac{1}{2}\sqrt{-23}]$ are 1 and -1 which are both cubes in $\mathcal{O}_K^*$, therefore $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$ is trivial and we conclude that $\ker(v)$ is isomorphic to $Cl_K[3]$.

In $\mathbb{Z}[\frac{1}{2}+\frac{1}{2}\sqrt{-23}]$ not all prime ideals are principal, for example:
$(2) = \mathfrak{p}_2\mathfrak{q}_2$ where $\mathfrak{p}_2 = \left(2, \frac{1}{2}+\frac{1}{2}\sqrt{-23}\right)$ and $\mathfrak{q}_2 = \left(2, \frac{1}{2}-\frac{1}{2}\sqrt{-23}\right)$ are nonprincipal prime ideals of $\mathcal{O}_K$. Indeed, if $\mathfrak{p}_2$ were principal, then a generator of it would have norm 2, and the ring $\mathbb{Z}[\frac{1}{2}+\frac{1}{2}\sqrt{-23}]$ contains no such elements. However,

$$\begin{aligned}
\mathfrak{p}_2^3 &= \left(2, \frac{1}{2}+\frac{1}{2}\sqrt{-23}\right)^3 \\
&= \left(8, 2+2\sqrt{-23}, -11+\sqrt{-23}, -\frac{17}{2}-\frac{5}{2}\sqrt{-23}\right) \\
&= \left(\frac{3}{2}-\frac{1}{2}\sqrt{-23}\right)\left(\frac{3}{2}+\frac{1}{2}\sqrt{-23}, -\frac{5}{2}+\frac{1}{2}\sqrt{-23}, -\frac{7}{2}-\frac{1}{2}\sqrt{-23}, 2-\sqrt{-23}\right) \\
&= \left(\frac{3}{2}-\frac{1}{2}\sqrt{-23}\right),
\end{aligned}$$

where one uses $\left(\frac{3}{2}+\frac{1}{2}\sqrt{-23}\right) + \left(-\frac{5}{2}+\frac{1}{2}\sqrt{-23}\right) + \left(2-\sqrt{-23}\right) = -1$. So $\mathfrak{p}_2$ yields an element of order 3 in Cl_K.
The ideal $(3) = \mathfrak{p}_3\mathfrak{q}_3$, where $\mathfrak{p}_3 = \left(3, \frac{1}{2}+\frac{1}{2}\sqrt{-23}\right)$ and $\mathfrak{q}_3 = \left(3, \frac{1}{2}-\frac{1}{2}\sqrt{-23}\right)$ are nonprincipal prime ideals of $\mathcal{O}_K$.
The ideal (5) is a principal prime ideal of $\mathcal{O}_K$.
Therefore $\ker(v)$ contains elements $\alpha{K^*}^3$ where (α) is the cube of a nonprincipal ideal, but α is not the cube of any element of K^*. For example $\frac{3}{2}-\frac{1}{2}\sqrt{-23}$ is not a cube in K^* (its norm equals 8 and K does not contain elements of norm 2), but $\left(\frac{3}{2}-\frac{1}{2}\sqrt{-23}\right) = {\mathfrak{p}_2}^3$ and hence we have that $\ker v$ contains $(\frac{3}{2}-\frac{1}{2}\sqrt{-23}){K^*}^3$ $(\neq 1 \cdot {K^*}^3)$.

Suppose that we have two elements $\alpha{K^*}^3$ and $\beta{K^*}^3$ of $\ker(v)$. Because $\alpha{K^*}^3$ and $\beta{K^*}^3$ are in $\ker(v)$ there exists ideals I and J such that $(\alpha) = I^3$ and $(\beta) = J^3$. If I and J are in the same ideal class, then there exists some $k \in {K^*}^3$ for which $J = k \cdot I$. But then we have $(k^3\alpha) = (\beta)$, and because $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$ is trivial $\alpha{K^*}^3 = \beta{K^*}^3$. In the other direction we have that if $\alpha{K^*}^3 = \beta{K^*}^3$,

then I and J are in the same ideal class.
Therefore we have that the elements of $\ker(v)$ correspond to the ideal classes of order dividing 3, so $\ker(v) \cong Cl_K[3]$.

To complete this example, we show that the class group of $\mathbb{Q}(\sqrt{-23})$ has order 3.
By Minkowski's bound, any ideal class in this class group contains an ideal of norm $\leqslant \frac{2}{\pi}\sqrt{|-23|} \approx 3.05$. The nontrivial ideals of norm $\leqslant 3$ are $\mathfrak{p}_2, \mathfrak{q}_2, \mathfrak{p}_3$ and $\mathfrak{q}_3$, which are all nonprincipal, and we know some relations:
$[\mathfrak{p}_2] + [\mathfrak{q}_2] = [\mathfrak{p}_2\mathfrak{q}_2] = [(2)] = 0$ (the trivial class of all principal ideals)
$[\mathfrak{p}_3] + [\mathfrak{q}_3] = [\mathfrak{p}_3\mathfrak{q}_3] = [(3)] = 0$
$3 \cdot [\mathfrak{p}_2] = [\mathfrak{p}_2^3] = [(\frac{3}{2} - \frac{1}{2}\sqrt{-23})] = 0$
and $[\mathfrak{p}_2] + [\mathfrak{p}_3] = [\mathfrak{p}_2\mathfrak{p}_3] =$

$$= \left[\left(2, \frac{1}{2} + \frac{1}{2}\sqrt{-23}\right)\left(3, \frac{1}{2} + \frac{1}{2}\sqrt{-23}\right)\right] = \left[\left(6, 1 + \sqrt{-23}, \frac{3}{2} + \frac{3}{2}\sqrt{-23}, -\frac{11}{2} + \frac{1}{2}\sqrt{-23}\right)\right]$$
$$= \left[\left(\frac{1}{2} + \frac{1}{2}\sqrt{-23}\right)\right] = 0.$$

Therefore $[\mathfrak{p}_2]^{-1} = [\mathfrak{q}_2] = [\mathfrak{p}_3] = [\mathfrak{p}_2^2] \neq [\mathfrak{p}_2]$ and $[\mathfrak{p}_2] = [\mathfrak{q}_3]$. So the elements of the class group Cl_K are $0, [\mathfrak{p}_2]$ and $[\mathfrak{q}_2]$, and Cl_K is cyclic of order 3 (and $Cl_K = Cl_K[3]$).

Example 4: $K = \mathbb{Q}(\sqrt{10})$
(An example where Cl_K and $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$ are not trivial, but where $Cl_K[3]$ is.)

Because $K = \mathbb{Q}(\sqrt{10})$ is a quadratic field and $10 \not\equiv 1 \mod 4$ is square-free, its ring of integers $\mathcal{O}_K$ is $\mathbb{Z}[\sqrt{10}]$ and its discriminant is $4 \cdot 10 = 40$.

Let us first compute the class group Cl_K of K.
By Minkowski's bound, any ideal class in the class group Cl_K contains an ideal of norm $\leqslant \frac{1}{2}\sqrt{40} \approx 3.16$. So we have to look at the prime ideals lying over 2 and 3. To do this, we use the Kummer-Dedekind theorem and look at factorisation of the minimum polynomial $X^2 - 10$ of $\sqrt{10}$ over $\mathbb{Q}$ modulo these primes.
For 2 we have $X^2 - 10 \equiv X \cdot X \mod 2$, so 2 is ramified (this can also be seen from the fact that 2 divides the discriminant). In fact $(2) = \mathfrak{p}_2^2$ with $\mathfrak{p}_2 = (2, \sqrt{10})$ the unique prime ideal containing 2.
For 3 we get $X^2 - 10 \equiv (X+1)(X-1) \mod 3$, so (3) splits into $\mathfrak{p}_3\mathfrak{q}_3$ with $\mathfrak{p}_3 = (3, 1 + \sqrt{10})$ and $\mathfrak{q}_3 = (3, 1 - \sqrt{10})$.
Now we want to find relations between these prime ideals.
One computes $(1 + \sqrt{10}) = \mathfrak{p}_3^2$ so we have the relations $2[\mathfrak{p}_2] = 0$ and $[\mathfrak{p}_3] + [\mathfrak{q}_3] = 0$ and $2[\mathfrak{p}_3] = 0$. In particular this shows that Cl_K is generated by at most two elements, which both have order at most 2. Hence $Cl_K[3] = (0)$.

We now show that in fact $Cl_K \cong \mathbb{Z}/2\mathbb{Z}$. The ideal norm of $(2 + \sqrt{10})$ is $2 \cdot 3$, so $(2 + \sqrt{10})$ is either $\mathfrak{p}_2\mathfrak{p}_3$ or $\mathfrak{p}_2\mathfrak{q}_3$, combining this with what we already know about $\mathfrak{p}_3$ and $\mathfrak{q}_3$ we have that $\mathfrak{p}_2$ is in the same ideal class as $\mathfrak{p}_3$ and $\mathfrak{q}_3$.
To complete this class group calculation, we now only have to show that this ideal class is not the trivial one. Suppose it is, then $\mathfrak{p}_2$ should be generated by one element $a + b\sqrt{10}$ of norm $a^2 - 10b^2 = \pm 2$. But if we look at this modulo 5 we get $a^2 \equiv 2$ or $3 \mod 5$ which has no solution. Therefore $\mathfrak{p}_2$ is nonprincipal, so $[\mathfrak{p}_2]$ has order 2 and Cl_K is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and is generated by $[\mathfrak{p}_2]$.

To describe $\ker(v) \subset K^*/{K^*}^3$ in this case, we conclude from the calculation above that it is given by the image of $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$ under the map induced by inclusion $\mathcal{O}_K^* \subset K^*$. Similar to the case of $\mathbb{Z}[\sqrt{2}]$ one shows that $3 + \sqrt{10}$ is a unit which is not a third power, hence its class generates $\ker(v) \cong \mathbb{Z}/3\mathbb{Z}$.

Example 5: $K = \mathbb{Q}(\sqrt{79})$
(An example where both $Cl_K[3]$ and $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$ are nontrivial.)

Because $K = \mathbb{Q}(\sqrt{79})$ is a quadratic field and the integer $79 \not\equiv 1 \mod 4$ is square-free, the ring of integers $\mathcal{O}_K$ is $\mathbb{Z}[\sqrt{79}]$ with discriminant $4 \cdot 79 = 316$. Similar to the previous real quadratic

examples, one finds that the unit group $\mathbb{Z}[\sqrt{79}]^*$ is generated by -1 and $80+9\sqrt{79}$, both of norm 1. In particular the class of $80+9\sqrt{79}$ generates the group $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$, a group of order 3.

It remains to compute the class group Cl_K of K.
By Minkowski's bound, any ideal class in the class group Cl_K contains an ideal of norm $\leqslant \frac{1}{2}\sqrt{316} \approx 8.89$. So we have to look at the prime ideals lying over $2, 3, 5$ and 7. To do this, we use the Kummer-Dedekind theorem and present the factorisation of the minimum polynomial X^2-79 of $\sqrt{79}$ over $\mathbb{Q}$ modulo these primes as well as the prime ideals over $2, 3, 5$, and 7 in the table below.

p	$X^2-79 \mod p$	factorisation of (p)
2	$(X+1)(X-1)$	$\mathfrak{p}_2\mathfrak{q}_2$ with $\mathfrak{p}_2=(2,1+\sqrt{79})$ and $\mathfrak{q}_2=(2,1-\sqrt{79})$
3	$(X+1)(X-1)$	$\mathfrak{p}_3\mathfrak{q}_3$ with $\mathfrak{p}_3=(3,1+\sqrt{79})$ and $\mathfrak{q}_3=(3,1-\sqrt{79})$
5	$(X+2)(X-2)$	$\mathfrak{p}_5\mathfrak{q}_5$ with $\mathfrak{p}_5=(5,2+\sqrt{79})$ and $\mathfrak{q}_5=(5,2-\sqrt{79})$
7	$(X+3)(X-3)$	$\mathfrak{p}_7\mathfrak{q}_7$ with $\mathfrak{p}_7=(7,3+\sqrt{79})$ and $\mathfrak{q}_7=(7,3-\sqrt{79})$

Now we give relations between these prime ideals. Some obvious ones can be seen in the table above, namely $[\mathfrak{p}_j]+[\mathfrak{q}_j]=0$ for $j\in\{2,3,5,7\}$. To obtain more relations we consider the norm of various elements of $\mathcal{O}_K$ in order to draw conclusions about the factorisation of the corresponding principal ideals.

$a\in\mathcal{O}_K$	$N(a)$	
$9+\sqrt{79}$	2	so $(9+\sqrt{79})$ is either $\mathfrak{p}_2$ or $\mathfrak{q}_2$, and therefore $\mathfrak{p}_2$ and $\mathfrak{q}_2$ are principal;
$17+2\sqrt{79}$	$-27=-3^3$	$(17+2\sqrt{79})$ is not divisible by 3 hence this ideal equals either $\mathfrak{p}_3^3$ or $\mathfrak{q}_3^3$, hence $\mathfrak{p}_3^3$ and $\mathfrak{q}_3^3$ are principal;
$8+\sqrt{79}$	$-15=-3\cdot 5$	so $\mathfrak{p}_5$ and $\mathfrak{q}_5$ belong to the same ideal classes as $\mathfrak{p}_3$ and $\mathfrak{q}_3$;
$4+\sqrt{79}$	$-63=-3^2\cdot 7$	because $4+\sqrt{79}$ is not divisible by 3 and $\mathfrak{p}_3^3$ and $\mathfrak{q}_3^3$ are principal, this implies that $\mathfrak{p}_7$ and $\mathfrak{q}_7$ belong to the same ideal classes as $\mathfrak{p}_3$ and $\mathfrak{q}_3$.

Now we have enough relations to conclude that Cl_K is generated by $[\mathfrak{p}_3]$ which has order 1 or 3. Moreover $17+2\sqrt{79}=5\cdot 3+2\cdot(1+\sqrt{79})\in\mathfrak{p}_3$, so $\mathfrak{p}_3^3=(17+2\sqrt{79})$. Suppose $\mathfrak{p}_3$ is principal: $\mathfrak{p}_3=(\alpha)$ $(\alpha\in\mathcal{O}_K)$, then $\alpha^3=u\cdot(17+2\sqrt{79})$ for some unit $u\in\mathcal{O}_K^*$. Therefore either $17+2\sqrt{79}, (17+2\sqrt{79})(80+9\sqrt{79})$ or $(17+2\sqrt{79})(80+9\sqrt{79})^2$ should be a cube in $\mathcal{O}_K$.
A cube in $\mathcal{O}_K$ can be written in the form $(a+b\sqrt{79})^3=a^3+3ab^2 79+(3a^2b+b^3)\sqrt{79}$.
If $(a+b\sqrt{79})^3=17+2\sqrt{79}$, then $a^3+3ab^2 79=17$ and $3a^2b+b^3=2$ and there is no integer solution for a and b.
If $(a+b\sqrt{79})^3=(17+2\sqrt{79})(80+9\sqrt{79})=2782+313\sqrt{79}$, then $a^3+3ab^2 79=2782=2\cdot 13\cdot 107$ and $3a^2b+b^3=313$ is prime. Therefore a should be in $\{\pm1,\pm2,\pm13,\pm107\}$ and b should be in $\{\pm1,\pm313\}$ and there is no integer solution for a and b.
If $(a+b\sqrt{79})^3=(17+2\sqrt{79})(80+9\sqrt{79})^2=445103+50078\sqrt{79}$, then $a^3+3ab^2 79=445103$ is prime, and $3a^2b+b^3=50078=2\cdot 7^3\cdot 73$, therefore a should be 1 but then there is no integer solution for b.
We conclude that $\mathfrak{p}_3$ is nonprincipal and hence $Cl_K\cong\mathbb{Z}/3\mathbb{Z}$.

So $\ker(v)\cong\mathcal{O}_K^*/{\mathcal{O}_K^*}^3\times Cl_K[3]\cong(\mathbb{Z}/3\mathbb{Z})^2$. Moreover the group $\ker(v)\subset K^*/K^{*3}$ is generated by the classes of $80+9\sqrt{79}$ and $17+2\sqrt{79}$.

Example 6: $K=\mathbb{Q}(\sqrt{-5703})$
(An example where $Cl_K[3]$ contains more than one independent element.)

Because $K=\mathbb{Q}(\sqrt{-5703})$ is a quadratic field where $-5703\equiv 1 \mod 4$, its ring of integers $\mathcal{O}_K$ is $\mathbb{Z}[\frac{1}{2}+\frac{1}{2}\sqrt{-5703}]$ and its discriminant is $5703=3\cdot 1901$.

Let us first compute the class group Cl_K of K.
By Minkowski's bound, any ideal class in the class group Cl_K contains an ideal of norm $\leqslant \frac{2}{\pi}\sqrt{5703}\approx 48.08$. So we have to look at the prime ideals lying over $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$ and 47. To do this, we use the Kummer-Dedekind theorem and look at factorisation of the minimum polynomial $X^2-X+1426$ of $(1+\sqrt{-5703})/2$ over $\mathbb{Q}$ modulo these primes.

p	$X^2 - X + 1426 \mod p$	factorisation of (p)
2	$X \cdot (X+1)$	$\mathfrak{p}_2\mathfrak{q}_2$ with $\mathfrak{p}_2 = \left(2, \frac{1}{2} + \frac{1}{2}\sqrt{-5703}\right)$ and $\mathfrak{q}_2 = \left(2, \frac{3}{2} + \frac{1}{2}\sqrt{-5703}\right)$
3	$(X+1)^2$	$\mathfrak{p}_3^2$ with $\mathfrak{p}_3 = \left(3, \frac{3}{2} + \frac{1}{2}\sqrt{-5703}\right)$
5	irreducible	(5)
7	$(X+1)(X+5)$	$\mathfrak{p}_7\mathfrak{q}_7$ with $\mathfrak{p}_7 = \left(7, \frac{3}{2} + \frac{1}{2}\sqrt{-5703}\right)$ and $\mathfrak{q}_7 = \left(7, \frac{11}{2} + \frac{1}{2}\sqrt{-5703}\right)$
11	irreducible	(11)
13	$(X+5)(X+7)$	$\mathfrak{p}_{13}\mathfrak{q}_{13}$ with $\mathfrak{p}_{13} = \left(13, \frac{11}{2} + \frac{1}{2}\sqrt{-5703}\right)$ and $\mathfrak{q}_{13} = \left(13, \frac{15}{2} + \frac{1}{2}\sqrt{-5703}\right)$
17	$(X+1)(X+15)$	$\mathfrak{p}_{17}\mathfrak{q}_{17}$ with $\mathfrak{p}_{17} = \left(17, \frac{3}{2} + \frac{1}{2}\sqrt{-5703}\right)$ and $\mathfrak{q}_{17} = \left(17, \frac{31}{2} + \frac{1}{2}\sqrt{-5703}\right)$
19	$(X+7)(X+11)$	$\mathfrak{p}_{19}\mathfrak{q}_{19}$ with $\mathfrak{p}_{19} = \left(19, \frac{15}{2} + \frac{1}{2}\sqrt{-5703}\right)$ and $\mathfrak{q}_{19} = \left(19, \frac{23}{2} + \frac{1}{2}\sqrt{-5703}\right)$
23	$X \cdot (X+22)$	$\mathfrak{p}_{23}\mathfrak{q}_{23}$ with $\mathfrak{p}_{23} = \left(23, \frac{1}{2} + \frac{1}{2}\sqrt{-5703}\right)$ and $\mathfrak{q}_{23} = \left(23, \frac{45}{2} + \frac{1}{2}\sqrt{-5703}\right)$
29	irreducible	(29)
31	$X \cdot (X+30)$	$\mathfrak{p}_{31}\mathfrak{q}_{31}$ with $\mathfrak{p}_{31} = \left(31, \frac{1}{2} + \frac{1}{2}\sqrt{-5703}\right)$ and $\mathfrak{q}_{31} = \left(31, \frac{61}{2} + \frac{1}{2}\sqrt{-5703}\right)$
37	irreducible	(37)
41	$(X+11)(X+29)$	$\mathfrak{p}_{41}\mathfrak{q}_{41}$ with $\mathfrak{p}_{41} = \left(41, \frac{23}{2} + \frac{1}{2}\sqrt{-5703}\right)$ and $\mathfrak{q}_{41} = \left(41, \frac{59}{2} + \frac{1}{2}\sqrt{-5703}\right)$
43	$(X+19)(X+23)$	$\mathfrak{p}_{43}\mathfrak{q}_{43}$ with $\mathfrak{p}_{43} = \left(43, \frac{39}{2} + \frac{1}{2}\sqrt{-5703}\right)$ and $\mathfrak{q}_{43} = \left(43, \frac{47}{2} + \frac{1}{2}\sqrt{-5703}\right)$
47	irreducible	(47)

Now we describe relations between these prime ideals. The obvious ones are $[\mathfrak{p}_j] + [\mathfrak{q}_j] = 0$ for $j \in \{2, 7, 13, 17, 19, 23, 31, 41, 43\}$ and $[2[\mathfrak{p}_3] = 0$. To obtain more relations we look at the norm $N(\alpha)$ of various elements $\alpha \in \mathcal{O}_K$.
Since $N(\frac{39}{2} + \frac{1}{2}\sqrt{-5703}) = 1806 = 2 \cdot 3 \cdot 7 \cdot 43$, the ideal class of $\mathfrak{p}_{43}$ or of $\mathfrak{q}_{43}$ (and therefore by complex conjugation the ideal classes of both) can be expressed in terms of classes of prime ideals of smaller index.

In the same way one discards:
the classes above 41 using $N(\frac{23}{2} + \frac{1}{2}\sqrt{-5703}) = 1558 = 2 \cdot 19 \cdot 41$,
the classes above 31 using $N(\frac{1}{2} + \frac{1}{2}\sqrt{-5703}) = 1426 = 2 \cdot 23 \cdot 31$,
the classes above 23 using $N(\frac{45}{2} + \frac{1}{2}\sqrt{-5703}) = 1932 = 2^2 \cdot 3 \cdot 7 \cdot 23$,
the classes above 19 using $N(\frac{15}{2} + \frac{1}{2}\sqrt{-5703}) = 1482 = 2 \cdot 3 \cdot 13 \cdot 19$,
the classes above 17 using $N(\frac{3}{2} + \frac{1}{2}\sqrt{-5703}) = 1628 = 2^2 \cdot 3 \cdot 7 \cdot 17$,
the classes above 13 using $N(\frac{11}{2} + \frac{1}{2}\sqrt{-5703}) = 1456 = 2^4 \cdot 7 \cdot 13$,
and the class above 3 using $N(\frac{21}{2} + \frac{1}{2}\sqrt{-5703}) = 1536 = 2^9 \cdot 3$.

Therefore Cl_K is generated by the ideal classes of $\mathfrak{p}_2$ and $\mathfrak{p}_7$.

$N(\frac{877}{2} + \frac{7}{2}\sqrt{-5703}) = 262144 = 2^{18}$, so $\mathfrak{p}_2$ has order dividing 18.
$N(6352 + \sqrt{-5703}) = 40353607 = 7^9$, so $\mathfrak{p}_7$ has order dividing 9.

The only principal ideal of norm $2^6 = 64$ is $(8) = \mathfrak{p}_2^3\mathfrak{q}_2^3$ (Because $(\frac{1}{2} + \frac{1}{2}\sqrt{-5703})$ already has norm 1426.) Therefore $\mathfrak{p}_2^6$ is nonprincipal.

If $\mathfrak{p}_3$ were principal, then there should be an element of norm 3 in $\mathcal{O}_K$. But that is not possible because the norm of $\frac{1}{2} + \frac{1}{2}\sqrt{-5703}$ is already 1426. Therefore $\mathfrak{p}_3$ is nonprincipal. Using $N(\frac{21}{2} + \frac{1}{2}\sqrt{-5703}) = 1536 = 2^9 \cdot 3$, and $\frac{21}{2} + \frac{1}{2}\sqrt{-5703} \notin (2) = \mathfrak{p}_2\mathfrak{q}_2$, we conclude that $\mathfrak{p}_2^9$ is nonprincipal and $\mathfrak{p}_2$ has order 18.

Next, $N(\frac{191}{2} + \frac{3}{2}\sqrt{-5703}) = 21952 = 2^6 \cdot 7^3$, therefore, because $\mathfrak{p}_2$ has order 18, $\mathfrak{p}_7^3$ can not be principal, so $\mathfrak{p}_7$ has order 9. From this norm, we also get a relation between the ideal classes of the ideals above 2 and 7: either $6 \cdot [\mathfrak{p}_2] + 3 \cdot [\mathfrak{p}_7] = 0$ or $6 \cdot [\mathfrak{p}_2] - 3 \cdot [\mathfrak{p}_7] = 0$.

Now there are two possibilities for Cl_K: either $[\mathfrak{p}_7]$ is in the subgroup generated by $[\mathfrak{p}_2]$ (and $2 \cdot [\mathfrak{p}_2] + [\mathfrak{p}_7] = 0$ or $2 \cdot [\mathfrak{p}_2] - [\mathfrak{p}_7] = 0$), which would imply that Cl_K is cyclic of order 18, or $[\mathfrak{p}_7]$ is not in the subgroup generated by $[\mathfrak{p}_2]$ and Cl_K is isomorphic to $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
Suppose we are in the first situation, so $[\mathfrak{p}_7]$ is in the subgroup generated by $[\mathfrak{p}_2]$. Then there should exist an element of norm $2^2 \cdot 7 = 28$ in $\mathcal{O}_K$, but that is clearly not possible: $\frac{1}{2} + \frac{1}{2}\sqrt{-5703}$

already has norm 1426.
We conclude that Cl_K is isomorphic to $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, where an isomorphism is given by $[\mathfrak{p}_2] \mapsto (1,0)$ and either $[\mathfrak{p}_7] \mapsto (2,1)$ or $[\mathfrak{p}_7] \mapsto (16,1)$.

Hence $Cl_K[3]$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$ and generated by $6 \cdot [\mathfrak{p}_2]$ and either $[\mathfrak{p}_7] + 2 \cdot [\mathfrak{p}_2]$ or $[\mathfrak{p}_7] - 2 \cdot [\mathfrak{p}_2]$.

Because K is an imaginary quadratic field, the unit group of its ring of integers consists of ± 1, so $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$ is trivial, and $\ker(v) \cong Cl_K[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$.
To obtain explicit generators of $\ker(v) \subset K^*/{K^*}^3$, first observe that

$$13 \cdot 7 + 3 \cdot (\frac{3}{2} + \frac{1}{2}\sqrt{-5703}) = \frac{191}{2} + \frac{3}{2}\sqrt{-5703} = 47 \cdot 2 + 3 \cdot (\frac{1}{2} + \frac{1}{2}\sqrt{-5703})$$

has norm $2^6 \cdot 7^3$ and is in $\mathfrak{p}_2$ and in $\mathfrak{p}_7$, but not in (2) and not in (7). Hence $\mathfrak{p}_2^6\mathfrak{p}_7^3 = (\frac{191}{2} + \frac{3}{2}\sqrt{-5703})$. This shows that $[\mathfrak{p}_7] + 2 \cdot [\mathfrak{p}_2]$ has order 3, and it corresponds to the class of $\frac{191}{2} + \frac{3}{2}\sqrt{-5703}$ in $\ker(v) \subset K^*/{K^*}^3$. Similarly $\frac{877}{2} + \frac{7}{2}\sqrt{-5703}$ (of norm 2^{18}) yields another element in $\ker(v)$, independent of the previous one.

3.4. **Proving independence in $Cl_K[m]$ using p-adic techniques.**

Now we discuss a method to show that elements of $Cl_K[m]$ (that we found using the map $g : \ker(v) \to Cl_K[m]$ above) are different or even independent. This will be done by considering pre-images in $K^*/{K^*}^m$ of the given elements. A common way to see if two numbers are different is to look if they differ modulo some prime. In $K^*/{K^*}^m$ - because of the equivalence modulo m-th powers - we can not simply reduce modulo a prime number, but we can - for different appropriate primes p - construct a homomorphism to a certain p-adic group. In many cases, we can see that the images of elements of $K^*/{K^*}^m$ in such a group are different, and therefore the elements of $K^*/{K^*}^m$ differ as well as their images in $\mathcal{O}_K^*/{\mathcal{O}_K^*}^m \times Cl_K[m]$ (if existing). Likewise, considering the images in those p-adic groups for different p at the same time could yield independence of elements in $Cl_K[m]$.

Let K be a quadratic field $\mathbb{Q}(\sqrt{-D})$. For the rational numbers and the field of p-adic numbers $\mathbb{Q}_p$, we have the natural inclusion homomorphism $\mathbb{Q} \to \mathbb{Q}_p$. Assume p is chosen such that $X^2 + D = 0$ has a solution a in $\mathbb{Q}_p$, then we can extend this homomorphism to a homomorphism $K \to \mathbb{Q}_p$ in two ways, mapping $\sqrt{-D}$ to either a or $-a$. So on the multiplicative groups of K and $\mathbb{Q}_p$ we have two group homomorphisms $h_\pm : K^* \to \mathbb{Q}_p^*$ defined by $h_\pm(r + s\sqrt{-D}) = r \pm as$.
Because the m-th powers form a normal subgroup in K^* and in $\mathbb{Q}_p^*$, we can reduce modulo m-th powers to get homomorphisms $h_\pm : K^*/{K^*}^m \longrightarrow \mathbb{Q}_p^*/{\mathbb{Q}_p^*}^m$.

Like we constructed valuations modulo 3 on $K^*/{K^*}^3$ before (Section 3.1), we have here the p-adic valuation modulo m denoted by $v_p \bmod m \ : \ \mathbb{Q}_p^*/{\mathbb{Q}_p^*}^m \longrightarrow \mathbb{Z}/m\mathbb{Z}$.
The kernel of this map consists of the p-adic units modulo m-th powers. We have a short exact sequence

$$1 \longrightarrow \mathbb{Z}_p^*/{\mathbb{Z}_p^*}^m \xrightarrow{\text{id}} \mathbb{Q}_p^*/{\mathbb{Q}_p^*}^m \xrightarrow{v_p \bmod m} \mathbb{Z}/m\mathbb{Z} \longrightarrow 0$$

and therefore we have an isomorphism $\mathbb{Q}_p^*/{\mathbb{Q}_p^*}^m \cong \mathbb{Z}_p^*/{\mathbb{Z}_p^*}^m \times \mathbb{Z}/m\mathbb{Z}$. This map depends on choosing an element $x \in \mathbb{Q}_p^*$ with $v_p(x) = 1$. The choice $x = p$ results in the isomorphism $\varphi_p \colon \mathbb{Q}_p^*/{\mathbb{Q}_p^*}^m \cong \mathbb{Z}_p^*/{\mathbb{Z}_p^*}^m \times \mathbb{Z}/m\mathbb{Z}$ given by $\xi{\mathbb{Q}_p^*}^m \mapsto \big(\xi \cdot p^{-v_p(\xi)}{\mathbb{Z}_p^*}^m, v_p(\xi) \bmod m\big)$.

The elements of $\ker(v) \subset K^*/{K^*}^m$ are in the kernel of $v_p \bmod m$. Hence the composition $\varphi_p \circ h_\pm$ maps $\ker(v)$ to $\mathbb{Z}_p^*/{\mathbb{Z}_p^*}^m \times (0) \cong \mathbb{Z}_p^*/{\mathbb{Z}_p^*}^m$.
If $p \not| m$, then $\mathbb{Z}_p^*/{\mathbb{Z}_p^*}^m \cong \mathbb{F}_p^*/{\mathbb{F}_p^*}^m$. Indeed, this follows by reducing modulo p and using Hensel's lemma.

In the case $m = 3$ and $p > 3$ we have $\mathbb{Z}_p^*/{\mathbb{Z}_p^*}^m \cong \mathbb{F}_p^*/{\mathbb{F}_p^*}^3 \cong \begin{cases} 1 & \text{if} \quad p \not\equiv 1 \bmod 3, \\ \mathbb{Z}/3\mathbb{Z} & \text{if} \quad p \equiv 1 \bmod 3. \end{cases}$
So if p satisfies the two conditions $-D$ is a square in $\mathbb{Q}_p$ and $p \equiv 1 \bmod 3$, then, by choosing an isomorphism $i \ : \ \mathbb{F}_p^*/{\mathbb{F}_p^*}^3 \to \mathbb{Z}/3\mathbb{Z}$ we get homomorphisms $\tilde{\varphi}_{p_\pm} = (i, id) \circ \varphi_p \circ h_\pm : \ker(v) \to \mathbb{Z}/3\mathbb{Z} \times \{0\} \cong \mathbb{Z}/3\mathbb{Z}$.
Recall that $\ker(v) \cong \mathcal{O}_K^*/{\mathcal{O}_K^*}^3 \times Cl_K[3]$, so it is clear that elements of $\ker(v)$ whose images under

$\tilde{\varphi_p}$ are different either differ by something nontrivial in $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3 \subset \ker(v)$ or yield different elements of $Cl_K[3]$. To prove that some elements of $\ker(v)$ will give independent elements of $Cl_K[3]$, we need different homomorphisms $\tilde{\varphi_{p_1\pm}}, \tilde{\varphi_{p_2\pm}}, ...$ as described above - at the same time: if the images of some elements of $\ker(v)$ under $(\tilde{\varphi_{p_1\pm}}, \tilde{\varphi_{p_2\pm}}, ...)$ are independent over $\mathbb{Z}/3\mathbb{Z}$, then also the corresponding elements in $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3 \times Cl_K[3]$ are independent over $\mathbb{Z}/3\mathbb{Z}$. When $D > 3$, $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$ is trivial and we have independence in $Cl_K[3]$.

Example:
Take $d = -D = 79$.
The quadratic field $K = \mathbb{Q}(\sqrt{d})$ has discriminant $\Delta_K = 316 = 2^2 \cdot 79$ and ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. The class group of K satisfies $Cl_K \cong \mathbb{Z}/3\mathbb{Z}$, and the unit group is $\mathcal{O}_K^* = \{\pm 1\} \times \langle 9\sqrt{d} - 80\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. A generator of the class group is the ideal class $[I]$ of the prime ideal $I = \left(3, 1 + \sqrt{d}\right)$, and $I^3 = \left(17 + 2\sqrt{d}\right)$ is principal.

Consider the elements $9\sqrt{d} - 80$ and $17 + 2\sqrt{d}$ in $\ker(v)$.
We first search for some primes $p \equiv 1 \bmod 3$ for which d is a square in $\mathbb{Q}_p$ such that we can made homomorphisms $\tilde{\varphi_p} : \ker(v) \longrightarrow \mathbb{Z}/3\mathbb{Z}$ as described above.
To find such primes, we look at the prime factorisation of $d - m^2$ for various integers $m > 1$. In this way we find:
$d \equiv 1^2 \bmod 13$ and $d \equiv 3^2 \bmod 7$.
Take $\sqrt{d} \in \mathbb{Z}_7$ with $\sqrt{d} \equiv 3 \bmod 7$. This results in a map $\ker(v) \to \mathbb{F}_7^*/{\mathbb{F}_7^*}^3$ with $17 + 2\sqrt{d} \mapsto (17 + 2 \cdot 3){\mathbb{F}_7^*}^3 = 2 \cdot {\mathbb{F}_7^*}^3$ and $-80 + 9\sqrt{d} \mapsto (-80 + 9 \cdot 3){\mathbb{F}_7^*}^3 = 3 \cdot {\mathbb{F}_7^*}^3$. Using the isomorphism $\mathbb{F}_7^*/{\mathbb{F}_7^*}^3 \cong \mathbb{Z}/3\mathbb{Z}$ with $2^n \cdot {\mathbb{F}_7^*}^3 \mapsto n \bmod 3$, this yields the composition $\tilde{\varphi_7}$ such that $\tilde{\varphi_7}(17+2\sqrt{d}) = \bar{1}$ and $\tilde{\varphi_7}(-80 + 9\sqrt{d}) = \bar{2}$.

Next, with $\sqrt{d} \in \mathbb{Z}_{13}$ such that $\sqrt{d} \equiv 1 \bmod 13$ and $2{\mathbb{F}_{13}^*}^3 \mapsto \bar{1} \in \mathbb{Z}/3\mathbb{Z}$ one finds completely analogously that $\tilde{\varphi_{13}}(17 + 2\sqrt{d}) = \bar{2} = \tilde{\varphi_{13}}(-80 + 9\sqrt{d})$.

As the elements $(\bar{1}, \bar{2})$ and $(\bar{2}, \bar{2})$ are independent in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, the map $\tilde{\varphi_7} \times \tilde{\varphi_{13}}$ shows that the two given elements in $\ker(v)$ are independent.

Example: To produce an example with more independent elements of order 3 in the class group, we consider the imaginary quadratic field $K := \mathbb{Q}(\sqrt{-D})$ with $D = 3321607$ which is according to F. Diaz y Diaz [DyD74] the smallest D for which Cl_K has 3-rank 3.
Here $D = 3321607$ is a prime number. In the ring of integers $\mathcal{O}_K$ of K we have the ideal equalities: $\left(152, \frac{23173+23103\sqrt{-D}}{2}\right)^3 = \left(\frac{3275+\sqrt{-D}}{2}\right)$, $\left(284, \frac{241659+80655\sqrt{-D}}{2}\right)^3 = \left(\frac{9397+\sqrt{-D}}{2}\right)$, and $\left(367, \frac{117+\sqrt{-D}}{2}\right)^3 = \left(4420 - 3\sqrt{-D}\right)$. Therefore the elements $\frac{3275+\sqrt{-D}}{2}$, $\frac{9397+\sqrt{-D}}{2}$ and $4420 - 3\sqrt{-D}$ are in $\ker(v)$.
Analogous to the previous example, we first search for suitable primes to make homomorphisms $\tilde{\varphi_p}$. We find:

p	reduction mod p of $\sqrt{-D} \in \mathbb{Z}_p$	cubes mod p
415201	± 1	...
103801	± 5	...
13	± 6	$1, 5, 8, 12$
255511	± 6	...
19	± 7	$1, 7, 8, 11, 12, 18$
8539	± 8	...
4111	± 9	...
43	± 10	$1, 2, 4, 8, 11, 16, 21, 22, 27, 32, 35, 39, 41, 42$
25951	± 11	...
...	...	...
97	± 35	$1, 8, 12, 18, 19, 20, 22, 27, 28, 30, 33, 34, 42, 45, 46, 47,$ $50, 51, 52, 55, 63, 64, 67, 69, 70, 75, 77, 78, 79, 85, 89, 96$
...	...	...

At $p=13$, we choose h_+ such that $h_+(\sqrt{-D}) = 6+13\cdot * \in \mathbb{Z}_{13}$. This gives the homomorphism $\varphi_{13}\circ h_+ : \ker(v) \to \mathbb{Z}_{13}^*/{\mathbb{Z}_{13}^*}^3$. Choose $\tilde{\varphi_{13}}_\pm$ to be the composition of $\varphi_{13}\circ h_\pm$ with the isomorphism $i : \mathbb{Z}_{13}^*/{\mathbb{Z}_{13}^*}^3 \cong \mathbb{F}_{13}^*/{\mathbb{F}_{13}^*}^3 \cong \mathbb{Z}/3\mathbb{Z}$ which maps $2^n\cdot {\mathbb{F}_{13}^*}^3 \in \mathbb{F}_{13}^*/{\mathbb{F}_{13}^*}^3$ to n mod 3.

Analogous, at $p=19$ we choose $h_+(\sqrt{-D}) = 7+19\cdot ...$ and again map $2^n\cdot \mathbb{F}_{19}^*$ to n mod 19 to obtain homomorphisms $\tilde{\varphi_{19}}_\pm$. At 43 we choose $h_+(\sqrt{-D}) = 10+43\cdot ...$, but now 2 is a cube in $\mathbb{F}_{43}^*$, so instead of using $2^n\cdot \mathbb{F}_p^{*3} \mapsto n$ mod 3 we choose the isomorphism $\mathbb{F}_{43}^*/{\mathbb{F}_{43}^*}^3 \cong \mathbb{Z}/3\mathbb{Z}$ defined by mapping $3^n\cdot {\mathbb{F}_{43}^*}^3$ to n mod 3. At 97 we choose $h_+(\sqrt{-D}) = 35$ and $2^n\cdot \mathbb{F}^{*3} \mapsto n$ mod 3.
This yields:

elt. $\in \ker(v)$	$\tilde{\varphi_{13}}_+$	$\tilde{\varphi_{13}}_-$	$\tilde{\varphi_{19}}_+$	$\tilde{\varphi_{19}}_-$	$\tilde{\varphi_{43}}_+$	$\tilde{\varphi_{43}}_-$	$\tilde{\varphi_{97}}_-$
$\frac{3275+\sqrt{-D}}{2}$	$\bar{2}$,	$\bar{1}$	$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{1}$	$\bar{1}$
$\frac{9397+\sqrt{-D}}{2}$	$\bar{1}$	$\bar{2}$	$\bar{2}$	$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{2}$
$\frac{8843-6\sqrt{-D}}{2}$	$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{1}$	$\bar{0}$	$\bar{0}$	$\bar{1}$

For example, in the calculation of $\tilde{\varphi_{19}}_-\left(\frac{3275+\sqrt{-D}}{2}\cdot K^{*3}\right) = (i,id)\circ\varphi_{19}\circ h_-\left(\frac{3275+\sqrt{-D}}{2}\cdot K^{*3}\right)$ the valuation at 19 of $h_-\left(\frac{3275+\sqrt{-D}}{2}\right)$ is nonzero and therefore we need either to use another representant of $\frac{3275+\sqrt{-D}}{2}\cdot K^{*3}$ for which this valuation is zero, or, more general, to use also higher order terms of $h_-(\sqrt{-D})$.
Solving $\left(h_-(\sqrt{-D})\right)^2 \equiv -D \bmod 19^4$ with $h_-(\sqrt{-D}) \equiv -7 \bmod 19$ gives:
$h_-(\sqrt{-D}) = 12+17\cdot 19+9\cdot 19^2+15\cdot 19^3+...\cdot 19^4$ and
$h_-\left(\frac{3275+\sqrt{-D}}{2}\right) = \frac{(7+1\cdot 19+9\cdot 19^2)+(12+17\cdot 19+9\cdot 19^2+15\cdot 19^3+...\cdot 19^4)}{2} = 8\cdot 19^3+...\cdot 19^4$.
Therefore $v_{19}(h_-\left(\frac{3275+\sqrt{-D}}{2}\right)) = v_{19}(8\cdot 19^3+...\cdot 19^4) = 3$, and
$\varphi_{19}\circ h_-\left(\frac{3275+\sqrt{-D}}{2}\right) = \left((8\cdot 19^3+...\cdot 19^4)\cdot 19^{-3}\cdot \mathbb{Z}_p^{*3}, 3 \bmod 3\right) = ((8+...\cdot 19)\cdot \mathbb{Z}_p^{*3}, 0 \bmod 3)$.
At last, the element $8\cdot \mathbb{F}_p^{*3} = 2^3\cdot \mathbb{F}_p^{*3}$ is mapped to $\bar{0} \in \mathbb{Z}/3\mathbb{Z}$.

Consider for example the first component of the elements at $\tilde{\varphi_{13}}_+$, $\tilde{\varphi_{19}}_+$, and $\tilde{\varphi_{97}}_-$. The elements $(\bar{2},\bar{0},\bar{1})$, $(\bar{1},\bar{2},\bar{2})$ and $(\bar{0},\bar{2},\bar{1})$ are independent in $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$. We conclude that the given elements of $\ker(v)$ are independent, and as $\mathcal{O}_K^*/{\mathcal{O}_K^*}^3$ is trivial, they yield independent elements of $Cl_K[3]$.
Representants of those elements in $Cl_K[3]$ are given by the three nonpricipal ideals we started with.

In the following sections we describe and discuss various methods people have used to find class groups with elements of a specific order and we investigate to which extend these methods can be understood in terms of the isomorphism from $\ker(v)$ to $\mathcal{O}_K^*/{\mathcal{O}_K^*}^m \times Cl_K[m]$ described above.

4. A relation between norm equations and elements of a specific order in Cl_K

4.1. **Introduction: the idea used by D.A. Buell and by D. Shanks & R. Serafin.** Given a quadratic field, we look at the correspondence between solutions of a certain cubic equation and ideals of order three as described by Duncan Buell in [Bue76] which refers to an article by Daniel Shanks and Richard Serafin [SS73]. We will see (§4.2) that this correspondence does not exist exactly in the way [Bue76] and [SS73] describe it, but if we talk about ideals $\in CL_K[3]$ not divisible by any $\mathbb{Z}$-prime p, and impose some conditions on $\gcd(a,b)$, the statement is nearly correct. Furthermore, the correspondence can be generalised from cubic norm equations and ideals in classes of order three to norm equations with an m-th power and ideals in classes of order m for odd $m \geqslant 3$ (§4.3), and can be interpreted in terms of the isomorphism of Proposition 3.4 (§4.4).

Let $D > 0$ be a square-free integer.

Buell and Shanks & Serafin state [Bue76], [SS73]:

> *The solutions of*
>
> $$4a^3 = b^2 + c^2 D \quad \textit{with} \quad 0 < a < \sqrt{\frac{D}{3}},\ 0 < b,\ \gcd(b,c) \leq 2$$
>
> *correspond to ideals*
>
> $$\mathfrak{a} = \left(a, \frac{b + c\sqrt{-D}}{2}\right)$$
>
> *in the ring of integers of $\mathbb{Q}(\sqrt{-D})$ whose cube is principal:*
>
> $$\mathfrak{a}^3 = \left(\frac{b + c\sqrt{-D}}{2}\right).$$

We will now discuss this statement and then try to make it precise.

Note that $\frac{b+c\sqrt{-D}}{2}$ has norm $\frac{b^2+c^2D}{4}$ and trace b.
First of all, if $c = 0$ then we lose the dependence on D, and we get $b = 2$ and $a = 1$ so $\mathfrak{a} = (1, \frac{2+0}{2}) = (1)$ which indeed satisfies $\mathfrak{a}^3 = (1) = ((b + c\sqrt{-D})/2)$.
So in the following we assume c to be nonzero.

We first consider the correspondence in one direction: assume integers (a, b, c) satisfy $4a^3 = b^2 + c^2 D$. We will consider the ideal $\mathfrak{a} = \left(a, \frac{b+c\sqrt{-D}}{2}\right)$, which in this case is indeed an ideal in the ring of integers of $\mathbb{Q}(\sqrt{-D})$.
We want to check whether $\mathfrak{a}^3 = \left(\frac{b+c\sqrt{-D}}{2}\right)$. Now compute:

$$
\begin{aligned}
\mathfrak{a}^3 &= \left(a,\ \frac{b+c\sqrt{-D}}{2}\right)^3 \\
&= \left(a^3,\ a^2\frac{b+c\sqrt{-D}}{2},\ a\left(\frac{b+c\sqrt{-D}}{2}\right)^2,\ \left(\frac{b+c\sqrt{-D}}{2}\right)^3\right) \\
&= \left(\frac{b^2+c^2D}{4},\ a^2\frac{b+c\sqrt{-D}}{2},\ a\left(\frac{b+c\sqrt{-D}}{2}\right)^2,\ \frac{b+c\sqrt{-D}}{2}\left(\frac{b^2-c^2D}{4}+\frac{bc\sqrt{-D}}{2}\right)\right) \\
&= \left(\frac{b+c\sqrt{-D}}{2}\frac{b-c\sqrt{-D}}{2},\ a^2\frac{b+c\sqrt{-D}}{2},\ a\left(\frac{b+c\sqrt{-D}}{2}\right)^2,\ \frac{b+c\sqrt{-D}}{2}\left(-a^3+\frac{b^2}{2}+b\frac{c\sqrt{-D}}{2}\right)\right) \\
&= \left(\frac{b+c\sqrt{-D}}{2}\right)\left(\frac{b-c\sqrt{-D}}{2},\ a^2,\ a\frac{b+c\sqrt{-D}}{2},\ -a^3+\frac{b^2}{2}+b\frac{c\sqrt{-D}}{2}\right) \\
&= \left(\frac{b+c\sqrt{-D}}{2}\right)\left(\frac{b-c\sqrt{-D}}{2},\ a^2,\ a\frac{b+c\sqrt{-D}}{2}+a\frac{b-c\sqrt{-D}}{2},\ -a^3+\frac{b^2}{2}+b\frac{c\sqrt{-D}}{2}+a^3+b\frac{b-c\sqrt{-D}}{2}\right) \\
&= \left(\frac{b+c\sqrt{-D}}{2}\right)\left(\frac{b-c\sqrt{-D}}{2},\ a^2,\ ab,\ b^2\right) \\
&= \left(\frac{b+c\sqrt{-D}}{2}\right)\left(\frac{b-c\sqrt{-D}}{2},\ (\gcd(a,b))^2\right) \\
&\subset \left(\frac{b+c\sqrt{-D}}{2}\right),
\end{aligned}
$$

and we have equality precisely when $1 \in \left(\frac{b-c\sqrt{-D}}{2},\ (\gcd(a,b))^2\right)$. In particular equality holds if $\gcd(a,b)=1$.
If $\gcd(a,b) \neq 1$, then there exists a prime p dividing $\gcd(a,b)$. Using $4a^3 = b^2+c^2D$ we find that p^2 divides c^2D, and because D is square-free this implies $p|c$. In the case $p \neq 2$, it is clear that p divides $\frac{b-c\sqrt{-D}}{2}$ in $\mathcal{O}_K$. In the case $p=2$ we use $4a^3 = b^2+c^2D$ to see that $D \equiv 3 \mod 4$, which implies that $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}+\frac{1}{2}\sqrt{-D}]$, so also in this case have that p divides $\frac{b-c\sqrt{-D}}{2}$ in $\mathcal{O}_K$. Therefore we have $\left(\frac{b-c\sqrt{-D}}{2},\ (\gcd(a,b))^2\right) \subset (p)$ and hence $1 \notin \left(\frac{b-c\sqrt{-D}}{2},\ (\gcd(a,b))^2\right)$. The argument given here proves the following result.

Proposition 4.1. *Let $a,b,c,D \in \mathbb{Z}$ with $D>0$ square-free and $4a^3 = b^2+c^2D \neq 0$. Then $\mathfrak{a} := \left(a, \frac{b+c\sqrt{-D}}{2}\right)$ is an ideal in $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$, and*

$$\mathfrak{a}^3 = \left(\frac{b+c\sqrt{-D}}{2}\right) \quad \textit{if and only if} \quad \gcd(a,b)=1.$$

Note that the condition $\gcd(a,b)=1$ used here is stronger than $\gcd(b,c) \leq 2$ (as was used by Buell and by Shanks & Serafin), as the following example shows:
Choose $a=6$, $b=2$, $c=2$ and $D = 215 = 5\cdot 43$ (square-free). Then $4a^3 = b^2+c^2D$, $0<a<\sqrt{\frac{D}{3}}$, $0<b$ and $\gcd(b,c)\leq 2$, but we don't have $\gcd(a,b)=1$. Computing $\mathfrak{a}^3$ as was done above yields

$$
\begin{aligned}
\mathfrak{a}^3 &= \left(\frac{2+2\sqrt{-215}}{2}\right)\left(\frac{2-2\sqrt{-215}}{2}, (\gcd(6,2))^2\right) \\
&= \left(1+\sqrt{-215}\right)\left(1-\sqrt{-215}, 4\right) \\
&= \left(2+2\sqrt{-215}\right)\left(\frac{1-\sqrt{-215}}{2}, 2\right).
\end{aligned}
$$

The ideal $\left(\frac{1-\sqrt{-215}}{2}, 2\right)$ is a prime ideal (of norm 2) and it is not principal since elements of norm 2 do not exist in $\mathcal{O}_{\mathbb{Q}(\sqrt{-215})}$. Therefore $\mathfrak{a}^3$ is also not principal.

In the reverse direction, a natural guess might be to show that every ideal $\mathfrak{a}$ for which $\mathfrak{a}^3$ is principal can be written uniquely as $\mathfrak{a} = \left(a, \frac{b+c\sqrt{-D}}{2}\right)$ with $4a^3 = b^2+c^2D$, $0<a<\sqrt{D/3}$, $0<b$ and $\gcd(a,b)=1$.

However, this guess is false, as the next example shows. Take $D = 26 = 2\cdot 13$ (square-free, positive). The quadratic field $K = \mathbb{Q}(\sqrt{-26})$ has ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-26}]$ and class group

Cl_K isomorphic to $\mathbb{Z}/6\mathbb{Z}$. The ideal classes of $(3, \sqrt{-26}+1)$ and $(3, \sqrt{-26}-1)$ are of order 3, but the equation $4a^3 = b^2 + 26c^2$ has no integer solutions for which $0 < a < \sqrt{D/3}$ and $c \neq 0$. (The integer solution with smallest positive a is $a = 3$ and $b = c = 2$.)

An even simpler reason why the first guess is false, is that one could multiply a given example ideal $\mathfrak{a}$ by a principal ideal. This increases the value of a and of $\gcd(a, b)$. As an example, take $D = 23$ and $\alpha = (1 + \sqrt{-23})/2$, so $\alpha^2 = \alpha - 6$. In this case the ring of integers is $\mathbb{Z}[\alpha]$, and $(2, \alpha)$ is a prime ideal of norm 2 that is not principal. We have $(2, \alpha)^3 = (-\alpha + 2)$, corresponding to the solution $a = 2, b = 3, c = -1$ of $4a^3 = b^2 + 23c^2$. Here indeed $a < \sqrt{D/3}$ and $\gcd(a, b) = 1$. Multiplying by 2 one obtains $(4, 2\alpha)^3 = (-8\alpha + 16)$ leading to $a = 4, b = 24, c = -8$. So here both the gcd-condition and the inequality $a < \sqrt{D/3}$ do not hold.

4.2. **Solutions of a cubic norm equation versus elements of $Cl_K[3]$.**

To resolve these issues, we change the conditions on $\gcd(a, b)$ and require the ideals to be not divisible by any prime $p \in \mathbb{Z}$.
From the condition that the ideals are not divisible by any $\mathbb{Z}$-prime p and the upper bound on a proposed by Buell and Shanks & Serafin, it seems a natural choice to use ideal classes instead of ideals. Indeed, in the end we get a surjective (although in general not injective) map to ideal *classes* of order dividing 3 instead of a map to ideals whose cube is principal. The results are described by the following theorem:

Theorem 4.2. *Let $K = \mathbb{Q}(\sqrt{-D})$ be a quadratic field with $D \in \mathbb{Z}$ square-free and $D > 3$. Consider the ideals $\mathfrak{a}$ of ideal classes in $Cl_K[3]$ which are not divisible by any prime $p \in \mathbb{Z}$. Those ideals correspond bijectively to solutions of the equation $4a^3 = b^2 + c^2 D$ with $a, b, c \in \mathbb{Z}$, $b \geq 0$, $c \geq 0$ if $b = 0$, $\gcd(a, b)$ square-free, and the primes dividing $\gcd(a, b)$ ramifying in $\mathcal{O}_K$. The bijection f is given by*

$$f^{-1} \quad : \quad \mathfrak{a} \quad \longmapsto \quad (a, b, c), \text{ with } a := N(\mathfrak{a}) \text{ and } b, c \text{ determined by } \mathfrak{a}^3 = \left(\tfrac{b + c\sqrt{-D}}{2}\right) \text{ where we choose } b \geq 0 \text{ and } c \geq 0 \text{ if } b = 0,$$

and

$$f \quad : \quad (a, b, c) \quad \longmapsto \quad \mathfrak{a} := \left(a, \frac{b + c\sqrt{-D}}{2\gcd(a, b)}\right).$$

Furthermore, each ideal class $[\mathfrak{a}] \in Cl_K[3]$ contains a unique ideal of minimal norm $a < \sqrt{|\Delta_K|/3}$. This gives us that (the restriction to (a, b, c) with $a < \sqrt{|\Delta_K|/3}$ of) f can be seen as a surjective map to $Cl_K[3]$.

Remark: There could be more ideals of norm $a < \sqrt{|\Delta_K|/3}$ belonging to the same ideal class in $Cl_K[3]$, but there is a unique one of minimal norm.

Proof. (Of Theorem 4.2) The proof consists of the following propositions (4.3 and 4.4), and Theorem 2.6. □

Proposition 4.3. *Let $K = \mathbb{Q}(\sqrt{-D})$ be a quadratic field with $D \in \mathbb{Z}$ square-free and $D > 3$, let $[\mathfrak{a}] \in Cl_K[3]$, and let $\mathfrak{a}$ be an ideal class representative of $[\mathfrak{a}]$ which is not divisible by any prime $p \in \mathbb{Z}$. Then we have $\mathfrak{a}^3 = \left(\frac{b + c\sqrt{-D}}{2}\right)$ for unique $b, c \in \mathbb{Z}$ with $b \geq 0$ and $c \geq 0$ if $b = 0$.*
As a result, $\mathfrak{a}$ can be written as $\left(a, \frac{b + c\sqrt{-D}}{2\gcd(a,b)}\right)$ with $4a^3 = b^2 + c^2 D$ or, equvuivalently, $a = N(\mathfrak{a})$. Furthermore, $\gcd(a, b)$ is square-free, and the primes dividing $\gcd(a, b)$ ramify.

Proof. Suppose we have some ideal class of order dividing three: $[\mathfrak{a}] \in Cl_K[3]$, and let $\mathfrak{a} \subset \mathcal{O}_K$ be an ideal which is not divisible by any prime $p \in \mathbb{Z}$.

The cube of $\mathfrak{a}$ is a principal ideal, so we can write $\mathfrak{a}^3 = \left(\frac{b + c\sqrt{-D}}{2}\right)$ for some $\frac{b + c\sqrt{-D}}{2} \in \mathcal{O}_K$ ($b, c \in \mathbb{Z}$). For the norm of this ideal we have $N(\mathfrak{a}^3) = N(\mathfrak{a})^3 = a^3$ (for some unique $a \in \mathbb{Z}$), but

also $N(\mathfrak{a}^3) = N\left(\frac{b+c\sqrt{-D}}{2}\right) = \frac{b^2+c^2D}{4}$. Hence $4a^3 = b^2 + c^2D$.

The unit group of an imaginary quadratic field with $D > 3$ square-free consists of only two elements: $\{\pm 1\}$, so the element $\frac{b+c\sqrt{-D}}{2} \in \mathcal{O}_K$ generating $\mathfrak{a}^3$ is unique up to a sign. We can choose b to be nonnegative, and if $b = 0$ choose c nonnegative to make our choice of b and c unique.

If we have $b = 0$, then $4a^3 = c^2D$. Since D is square-free it follows that $2a|c$ and $D|a$ and $4D^3|4a^3 = c^2D$. All primes dividing the integer $\left(\frac{a}{D}\right)^3 = \left(\frac{c}{2D}\right)^2$ occur a multiple of $\operatorname{lcm}(3,2) = 6$ times. Therefore $\sqrt[3]{\frac{c}{2D}}$ is in $\mathbb{Z}$ and $\mathfrak{a} = \left(\sqrt[3]{\frac{c}{2D}}\sqrt{-D}\right)$ which is a principal ideal. By assumption, there is no prime dividing $\mathfrak{a}$. Therefore $|\sqrt[3]{\frac{c}{2D}}| = 1$ which implies $|c| = 2D = 2a$, so the only solution corresponding to $b = 0$ is: $(a,b,c) = (D,0,2D)$, $\mathfrak{a} = (\sqrt{-D})$.

By now, we have integers a, b and c for which $N(\mathfrak{a}) = a$, $4a^3 = b^2 + c^2D$, $b \geq 0$, and $c \geq 0$ if $b = 0$, and those are the unique ones for which additionally $\mathfrak{a}^3 = \left(\frac{b+c\sqrt{-D}}{2}\right)$.

We already saw that when $\gcd(a,b) = 1$, $\mathfrak{a} := \left(a, \frac{b+c\sqrt{-D}}{2}\right)$ gives us indeed $\mathfrak{a}^3 = \left(\frac{b+c\sqrt{-D}}{2}\right)$.
So now consider the general case: $\gcd(a,b)$ not necessarily equal to 1. Suppose some prime p divides $\gcd(a,b)$, then $p^3|4a^3 = b^2 + c^2D$ which implies $p^2|c^2D$, and because D is square-free we have $p|c$. But then p is a divisor of $\frac{b+c\sqrt{-D}}{2}$ in $\mathcal{O}_K$, by the following argument. For $p \neq 2$ it is clear. In the remaining case $p = 2$ the equality $4a^3 = b^2 + c^2D$ implies that either $b \equiv c \equiv 0 \mod 4$ or $b^2 \equiv c^2 \equiv 1 \mod 4$ and $D \equiv 3 \mod 4$, and in both cases 2 is a divisor of $\frac{b+c\sqrt{-D}}{2}$ in $\mathcal{O}_K$.
So we have $(p)|\left(\frac{b+c\sqrt{-D}}{2}\right) = \mathfrak{a}^3$. If p splits or p is inert, then it follows directly that $(p)|\mathfrak{a}$ which is in contradiction with our choice of $\mathfrak{a}$ as an ideal not divisible by any prime. Therefore $\gcd(a,b)$ is a product of ramifying primes.
If the square of such a prime p divides $\gcd(a,b)$, then $p^6|4a^3 = b^2 + c^2D$. Hence $p^4|c^2D$, and because D is square-free, $p^2|c$.
If $p \neq 2$, it follows directly that p^2 is a divisor of $\frac{b+c\sqrt{-D}}{2}$ in $\mathcal{O}_K$.
If $p = 2$ then we have $2^8|b^2+c^2D$, $4|b$ and $4|c$. So $b^2+c^2D \equiv 0 \mod 64$ whilst b^2 and c^2 are 0 or 16 modulo 64. In the case $b^2 \equiv 16 \mod 64$ we have $c^2D \equiv 3 \cdot 16 \mod 64$ which implies $D \equiv 3 \mod 4$ which is not possible because $2 = p$ was a ramifying prime and therefore divides Δ_K. Therefore $b^2 \not\equiv 16 \mod 64$. It follows that $2^6|b^2$ and $2^6|c^2D$, and hence 2^3 divides both b and c. So also in the case $p = 2$ we have that p^2 is a divisor of $\frac{b+c\sqrt{-D}}{2}$.
So we have $\mathfrak{p}^4 = (p)^2|\left(\frac{b+c\sqrt{-D}}{2}\right) = \mathfrak{a}^3$ and therefore $\mathfrak{p}^2 = (p)|\mathfrak{a}$, which is in contradiction with the assumptions on $\mathfrak{a}$. Therefore, $\gcd(a,b)$ is square-free.

Recall that every prime dividing $\gcd(a,b)$ divides $\frac{b+c\sqrt{-D}}{2}$ in $\mathcal{O}_K$. Therefore from $\gcd(a,b)$ being square-free we now conclude that $\frac{b+c\sqrt{-D}}{2\gcd(a,b)}$ is an element of $\mathcal{O}_K$.

We saw that if $p|\gcd(a,b)$, then $p|\Delta_K = \begin{cases} D & \text{for } D \equiv 3 \mod 4 \\ 4D & \text{for } D \not\equiv 3 \mod 4 \end{cases}$ and $p^3|4a^3 = b^2 + c^2D$. If p is odd, $p|D$ and $p^3|b^2$. If p is even, either $p|D$ and $p^3|b^2$ or $D \equiv 1 \mod 4$. In the latter case $b^2 + c^2D \equiv 0 \mod 16$ where b^2 and c^2 are 0 or 4 mod 16 and $D \equiv 1 \mod 4$, which implies $b^2 \equiv 0 \mod 16$.
So any prime $p|\gcd(a,b)$ satisfies $p^3|b^2$ and hence $p^2|b$. Since $\gcd(a,b)$ is square-free, it follows that $\gcd(a,b)^2|b$.
In the ring $\mathcal{O}_K$ we conclude

$$\begin{aligned} \gcd(a,b) \text{ divides } & \frac{-a^3}{\gcd(a,b)^2} + \frac{b}{\gcd(a,b)}\frac{b+c\sqrt{-D}}{2\gcd(a,b)} \\ = & \frac{-4a^3 + 2b^2 + 2bc\sqrt{-D}}{4\gcd(a,b)^2} \\ = & \frac{b^2 + 2bc\sqrt{-D} - c^2D}{4\gcd(a,b)^2} \\ = & \left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^2. \end{aligned}$$

Now consider the integral $\mathcal{O}_K$-ideal $I := \left(a, \frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)$. The cube of I is given by

$$\begin{aligned}
I^3 &= \left(a, \ \frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^3 \\
&= \left(a^3, \ a^2\frac{b+c\sqrt{-D}}{2\gcd(a,b)}, \ a\left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^2, \ \left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^3\right) \\
&= \left(\frac{b^2+c^2D}{4}, \ a^2\frac{b+c\sqrt{-D}}{2\gcd(a,b)}, \ a\left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^2, \ \left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^3\right) \\
&= \left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)\left(\gcd(a,b)\frac{b-c\sqrt{-D}}{2}, \ a^2, \ a\frac{b+c\sqrt{-D}}{2\gcd(a,b)}, \ \left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^2\right) \\
&= \left(\frac{b+c\sqrt{-D}}{2}\right)\left(\frac{b-c\sqrt{-D}}{2}, \ \frac{a^2}{\gcd(a,b)}, \ \frac{a}{\gcd(a,b)}\frac{b+c\sqrt{-D}}{2\gcd(a,b)}, \ \frac{1}{\gcd(a,b)}\left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^2\right) \\
&= \mathfrak{a}^3\left(\frac{b-c\sqrt{-D}}{2}, \ \frac{a^2}{\gcd(a,b)}, \ \frac{a}{\gcd(a,b)}\frac{b+c\sqrt{-D}}{2\gcd(a,b)}, \ \frac{1}{\gcd(a,b)}\left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^2\right).
\end{aligned}$$

We will show that $I = \mathfrak{a}$ by proving that the norm of the ideal on the right equals 1. Note that

$$N(I^3) = a^3 \cdot N\left(\left(\frac{b-c\sqrt{-D}}{2}, \ \frac{a^2}{\gcd(a,b)}, \ \frac{a}{\gcd(a,b)}\frac{b+c\sqrt{-D}}{2\gcd(a,b)}, \ \frac{1}{\gcd(a,b)}\left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^2\right)\right).$$

Consider the inclusion of rank 2 $\mathbb{Z}$-modules

$$\mathbb{Z}a + \mathbb{Z}\frac{b+c\sqrt{-D}}{2\gcd(a,b)} \subset I \subset \mathcal{O}_K \subset \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-D}}{2}.$$

It implies

$$\begin{aligned}
\left[I \ : \ \mathbb{Z}a + \mathbb{Z}\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right] \cdot [\mathcal{O}_K \ : \ I] \cdot \left[\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-D}}{2} \ : \ \mathcal{O}_K\right] &= \left[\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-D}}{2} \ : \ \mathbb{Z}a + \mathbb{Z}\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right] \\
&= a\frac{|c|}{\gcd(a,b)},
\end{aligned}$$

where the last equality is seen as follows. Identifying $\mathbb{Z}+\mathbb{Z}\frac{1+\sqrt{-D}}{2} \cong \mathbb{Z}^2$ via $n+m\frac{1+\sqrt{-D}}{2} \mapsto (n,m)$, the subgroup $\mathbb{Z}a + \mathbb{Z}\frac{b+c\sqrt{-D}}{2\gcd(a,b)}$ corresponds to $\mathbb{Z}\cdot(a,0) + \mathbb{Z}\cdot(\frac{b-c}{2\gcd(a,b)}, \frac{c}{\gcd(a,b)})$. Clearly the latter subgroup has index $a|c|/\gcd(a,b)$ in $\mathbb{Z}^2$.

The argument above implies that $N(I) = [\mathcal{O}_K \ : \ I]$ divides $a\frac{c}{\gcd(a,b)}$ (note that $c/\gcd(a,b) \in \mathbb{Z}$ since $\gcd(a,b)$ is square-free). As a consequence $N(I^3) \ \mid \ a^3\frac{c^3}{\gcd(a,b)^3}$.

Therefore the norm of $\left(\frac{b-c\sqrt{-D}}{2}, \ \frac{a^2}{\gcd(a,b)}, \ \frac{a}{\gcd(a,b)}\frac{b+c\sqrt{-D}}{2\gcd(a,b)}, \ \frac{1}{\gcd(a,b)}\left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^2\right)$ divides $\frac{c^3}{\gcd(a,b)^3}$.

This norm is also a divisor of $N\left(\frac{1}{\gcd(a,b)}\left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^2\right) = \frac{a^6}{\gcd(a,b)^6}$, therefore it divides

$$\gcd\left(\frac{c^3}{\gcd(a,b)^3}, \frac{a^6}{\gcd(a,b)^6}\right) = \gcd\left(\frac{c}{\gcd(a,b)}, \frac{a^2}{\gcd(a,b)^2}\right)^3.$$

We claim that the latter gcd equals 1. Indeed, write $g = \gcd(a,b)$ and $a = ga_1, b = gb_1, c = gc_1$. Then $\gcd(a_1,b_1) = 1$ and $4ga_1^3 = b_1^2 + c_1^2D$. A prime dividing both a_1 and c_1 would also divide b_1, implying $\gcd(a_1,c_1) = 1$ from which the claim is immediate.

So $\left(\frac{b-c\sqrt{-D}}{2}, \ \frac{a^2}{\gcd(a,b)}, \ \frac{a}{\gcd(a,b)}\frac{b+c\sqrt{-D}}{2\gcd(a,b)}, \ \frac{1}{\gcd(a,b)}\left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^2\right)$ is the unit ideal, and we conclude that $I = \mathfrak{a}$, so $\mathfrak{a} = \left(a, \frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)$.

□

In the reverse direction, given a solution to the equation $4a^3 = b^2 + c^2D$ and possibly some extra conditions, we want to find an ideal class in $Cl_K[3]$ of which an ideal should be given by $\left(a, \frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)$.

We saw that if $\gcd(a,b) = 1$ then indeed $\left(a, \frac{b+c\sqrt{-D}}{2}\right)$ has order dividing 3. We may guess that,

because now we are dividing the $\frac{b+c\sqrt{-D}}{2}$ by $\gcd(a,b)$, we don't need any condition on $\gcd(a,b)$. But that is not true as the following example shows:

Example: $K=\mathbb{Q}(\sqrt{-263})$
For $D=263$, one of the solutions to the equation $4a^3=b^2+c^2D$, not necessarily with $a<\sqrt{|\Delta_K|}/3$, is: $a=18$, $b=45$, and $c=9$.
If we consider the $\mathcal{O}_K$-ideal generated by a and $\frac{b+c\sqrt{-D}}{2\gcd(a,b)}$ we would like to see if its cube is probably the principal ideal given by $\left(\frac{b+c\sqrt{-D}}{2}\right)$. But in fact, $\left(18, \frac{45+9\sqrt{-D}}{2\cdot 9}\right)$ is a nonprincipal ideal of order 13, and $Cl_K\cong\mathbb{Z}/13\mathbb{Z}$ not even contains any ideal class of order 3.

A condition on $\gcd(a,b)$ that turns out to be sufficient to give us ideals of order dividing 3 is that $\gcd(a,b)$ has to be square-free and that the primes dividing $\gcd(a,b)$ ramify in $\mathcal{O}_K$, as is shown in the following proposition.

Proposition 4.4. *Let $K:=\mathbb{Q}(\sqrt{-D})$ be a quadratic field with $D\in\mathbb{Z}$ square-free and $D>3$, and let $a,b,c\in\mathbb{Z}$ with $4a^3=b^2+c^2D$, $\gcd(a,b)$ square-free and the primes dividing $\gcd(a,b)$ ramifying in $\mathcal{O}_K$.*
Then $\mathfrak{a}:=\left(a,\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)$ is an integral $\mathcal{O}_K$-ideal in $Cl_K[3]$, and $\mathfrak{a}^3=\left(\frac{b+c\sqrt{-D}}{2}\right)$. Furthermore, this ideal $\mathfrak{a}$ is not divisible by any $\mathbb{Z}$-prime p.

Proof. We have $4a^3\equiv b^2+c^2D\equiv 0 \mod 8$. Any square is either 0, 1, or 4 mod 8, so b and c are even, or D has to be $\equiv 3 \mod 4$.
Suppose we have some prime $p|\gcd(a,b)$, then $p^3|4a^3=b^2+c^2D$. Therefore $p^2|c^2D$. But D is square-free, so $p|c$. Furthermore, if $p=2$ then $b^2+c^2D\equiv 0 \mod 32$, hence $\left(\frac{b}{2}\right)^2+\left(\frac{c}{2}\right)^2D\equiv 0 \mod 8$, and therefore either $\frac{b}{2}\equiv\frac{c}{2}\equiv 1 \mod 2$ and $D\equiv 3 \mod 4$, or $\frac{b}{2}\equiv\frac{c}{2}\equiv 0 \mod 2$. So in all cases, p divides $\frac{b+c\sqrt{-D}}{2}$ in $\mathcal{O}_K$. Because $\gcd(a,b)$ is square-free, it follows that $\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\in\mathcal{O}_K$.

Consider the integral $\mathcal{O}_K$-ideal $\mathfrak{a}:=\left(a,\ \frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)$. We first show that the norm of this ideal is equal to a.
The cube of $\mathfrak{a}$ is given by

$$\begin{aligned}
\mathfrak{a}^3 &= \left(a,\ \frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^3\\
&= \left(a^3,\ a^2\frac{b+c\sqrt{-D}}{2\gcd(a,b)},\ a\left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^2,\ \left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^3\right)\\
&= \left(\frac{b^2+c^2D}{4},\ a^2\frac{b+c\sqrt{-D}}{2\gcd(a,b)},\ a\left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^2,\ \left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^3\right)\\
&= \left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)\cdot\left(\gcd(a,b)\frac{b-c\sqrt{-D}}{2},\ a^2,\ a\frac{b+c\sqrt{-D}}{2\gcd(a,b)},\ \left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^2\right)
\end{aligned}$$

So on one hand, $N\left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)=\frac{a^3}{\gcd(a,b)^2}$ is a divisor of $N(\mathfrak{a}^3)$, and $N(\mathfrak{a}^3)$ is a divisor of $N\left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)\cdot N\left(\left(\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)^2\right)=\frac{a^9}{\gcd(a,b)^6}$.
On the other hand, if we look at $\mathfrak{a}$ and $\mathcal{O}_K$ as $\mathbb{Z}$-modules, then we have the following inclusion of rank 2 $\mathbb{Z}$-modules:

$$\mathbb{Z}a+\mathbb{Z}\frac{b+c\sqrt{-D}}{2\gcd(a,b)}\subset\mathfrak{a}\subset\mathcal{O}_K\subset\mathbb{Z}+\mathbb{Z}\frac{1+\sqrt{-D}}{2}.$$

This implies

$$\left[\mathfrak{a}\ :\ \mathbb{Z}a+\mathbb{Z}\tfrac{b+c\sqrt{-D}}{2\gcd(a,b)}\right]\cdot[\mathcal{O}_K\ :\ \mathfrak{a}]\cdot\left[\mathbb{Z}+\mathbb{Z}\tfrac{1+\sqrt{-D}}{2}\ :\ \mathcal{O}_K\right]$$
$$=$$
$$\left[\mathbb{Z}+\mathbb{Z}\tfrac{1+\sqrt{-D}}{2}\ :\ \mathbb{Z}a+\mathbb{Z}\tfrac{b+c\sqrt{-D}}{2\gcd(a,b)}\right]=a\tfrac{|c|}{\gcd(a,b)},$$

and therefore $N(\mathfrak{a})=[\mathcal{O}_K\ :\ \mathfrak{a}]$ divides $a\frac{c}{\gcd(a,b)}$, hence $N(\mathfrak{a}^3)\ |\ a^3\frac{c^3}{\gcd(a,b)^3}$. Because $N(\mathfrak{a}^3)$ divides both $\frac{a^9}{\gcd(a,b)^6}$ and $a^3\frac{c^3}{\gcd(a,b)^3}$, it also divides $\gcd\left(\frac{a^9}{\gcd(a,b)^6},a^3\frac{c^3}{\gcd(a,b)^3}\right)=a^3\gcd\left(a_1^2,c_1\right)^3$,

where $a_1 = \frac{a}{\gcd(a,b)}$, $b_1 = \frac{b}{\gcd(a,b)}$ and $c_1 = \frac{c}{\gcd(a,b)} \in \mathbb{Z}$. We have $4\gcd(a,b)a_1^3 = \frac{1}{\gcd(a,b)^2}4a^3 = \frac{1}{\gcd(a,b)^2}\left(b^2 + c^2D\right) = b_1^2 + c_1^2 D$ with $\gcd(a_1, b_1) = 1$. It follows that $\gcd(a_1, c_1) = 1$ and therefore $\gcd(a_1^2, c_1)^3 = 1$ and $N(\mathfrak{a}^3) \mid a^3$.
Now we have $\frac{a^3}{\gcd(a,b)^2} \mid N(\mathfrak{a}^3) \mid a^3$. Because $\gcd(a,b)$ is square-free, this implies $N(\mathfrak{a}^3) = a^3$, hence $N(\mathfrak{a}) = a$.

Now we show that $\mathfrak{a}^3$ is a principal ideal.
The primes dividing $\gcd(a,b)$ ramify, therefore any prime p dividing $\gcd(a,b)$ also divides Δ_K.
If $p \neq 2$, then p divides a, b, c and D. Hence $p^3 | a^3 - c^2 D = b^2$, and therefore $p^2 | b$.
If $p = 2$, then either $p|D$ and hence $p^2|b$, or $D \equiv 1 \mod 4$. In the latter case $2^5 \mid b^2 + c^2 D$, so $\left(\frac{b}{2}\right)^2 + \left(\frac{c}{2}\right)^2 D \equiv 0 \mod 8$ which implies either $\left(\frac{b}{2}\right)^2 \equiv \left(\frac{c}{2}\right)^2 \equiv 1 \mod 8$ and $D \equiv 7 \mod 8$, which is not possible if $D \equiv 1 \mod 4$, or $2 \mid \frac{b}{2}$.
In all cases, we can conclude $p^2 \mid b$. This holds for all primes dividing $\gcd(a,b)$ which is square-free, therefore $\gcd(a,b)^2 \mid b$.
So in $\mathcal{O}_K$ we have

$$\begin{aligned}
\gcd(a,b) \text{ divides } & \frac{-a^3}{\gcd(a,b)^2} + \frac{b}{\gcd(a,b)}\frac{b + c\sqrt{-D}}{2\gcd(a,b)} \\
= & \frac{-4a^3 + 2b^2 + 2bc\sqrt{-D}}{4\gcd(a,b)^2} \\
= & \frac{b^2 + 2bc\sqrt{-D} - c^2 D}{4\gcd(a,b)^2} \\
= & \left(\frac{b + c\sqrt{-D}}{2\gcd(a,b)}\right)^2.
\end{aligned}$$

Hence we can write

$$\begin{aligned}
\mathfrak{a}^3 &= \left(\frac{b + c\sqrt{-D}}{2\gcd(a,b)}\right) \cdot \left(\gcd(a,b)\frac{b - c\sqrt{-D}}{2},\ a^2,\ a\frac{b + c\sqrt{-D}}{2\gcd(a,b)},\ \left(\frac{b + c\sqrt{-D}}{2\gcd(a,b)}\right)^2\right) \\
&= \left(\frac{b + c\sqrt{-D}}{2}\right) \cdot \left(\frac{b - c\sqrt{-D}}{2},\ \frac{a^2}{\gcd(a,b)},\ \frac{a}{\gcd(a,b)}\frac{b + c\sqrt{-D}}{2\gcd(a,b)},\ \frac{1}{\gcd(a,b)}\left(\frac{b + c\sqrt{-D}}{2\gcd(a,b)}\right)^2\right)
\end{aligned}$$

where the last ideal on the right hand side is integral in $\mathcal{O}_K$. Because $N(\mathfrak{a}) = a$ and $N\left(\frac{b+c\sqrt{-D}}{2}\right) = a^3$, the norm of this integral ideal is equal to 1, hence it is the unit ideal.
We conclude $\mathfrak{a}^3 = \left(\frac{b+c\sqrt{-D}}{2}\right)$.

To complete the proof we now show that $\mathfrak{a}$ is not divisible by any $\mathbb{Z}$-prime p.
Suppose $\mathfrak{a}$ is divisible by some $\mathbb{Z}$-prime p, then both a and $\frac{b+c\sqrt{-D}}{2\gcd(a,b)}$ are divisible by p (as elements of $\mathcal{O}_K$). But then also $\frac{b-c\sqrt{-D}}{2\gcd(a,b)}$ is divisible by p, and hence $p \mid \frac{b+c\sqrt{-D}}{2\gcd(a,b)} + \frac{b-c\sqrt{-D}}{2\gcd(a,b)} = \frac{b}{\gcd(a,b)}$ and $p^2 \mid \frac{b+c\sqrt{-D}}{2\gcd(a,b)}\frac{b-c\sqrt{-D}}{2\gcd(a,b)} = \frac{a^3}{\gcd(a,b)^2}$. From this it follows that $p^2 \mid \gcd(a,b)$, which is in contradiction with $\gcd(a,b)$ being square-free. We conclude that there is no $\mathbb{Z}$-prime p dividing $\mathfrak{a}$. □

In conclusion, without discussing ideal classes we have constructed in this section a correspondence similar to the one proposed by Buell and Shanks & Serafin, but with slightly different conditions. And the restriction to solutions with $a < \sqrt{|\Delta_K|/3}$ - which is only a finite set - can be seen as a surjection to $Cl_K[3]$.

4.3. **Generalisation of §4.2 to arbitrary odd $m \geqslant 3$.**

We can try to generalise the correspondence discussed in the previous section to general positive m instead of cubic equations and ideals of classes in $Cl_K[m]$. For even m, this does not work directly, but for odd $m \geqslant 3$, the results and the proofs are roughly the same. So throughout this section, let $m \geqslant 3$ be an odd integer. (Note that m not necessarily needs to be a prime number.)

Theorem 4.5. *Let $K = \mathbb{Q}(\sqrt{-D})$ be a quadratic field with $D \in \mathbb{Z}$ square-free and $D > 3$. Consider the ideals $\mathfrak{a}$ of ideal classes in $Cl_K[m]$ which are not divisible by any prime $p \in \mathbb{Z}$. Those ideals correspond bijectively to solutions of the equation $4a^m = b^2 + c^2 D$ with $a, b, c \in \mathbb{Z}$, $b \geq 0$, $c \geq 0$ if $b = 0$, $\gcd(a, b)$ square-free, and the primes dividing $\gcd(a, b)$ ramifying in $\mathcal{O}_K$. The bijection f is given by*

$$f^{-1} \quad : \quad \mathfrak{a} \quad \longmapsto \quad (a, b, c), \text{ with } a := N(\mathfrak{a}) \text{ and } b, c \text{ determined by } \mathfrak{a}^m = \left(\tfrac{b+c\sqrt{-D}}{2}\right) \text{ where we choose } b \geq 0 \text{ and } c \geq 0 \text{ if } b = 0,$$

and

$$f \quad : \quad (a, b, c) \quad \longmapsto \quad \mathfrak{a} := \left(a, \frac{b + c\sqrt{-D}}{2\gcd(a, b)^{(m-1)/2}}\right).$$

Furthermore, each ideal class $[\mathfrak{a}] \in Cl_K[m]$ contains a unique ideal of minimal norm $a < \sqrt{|\Delta_K|/3}$. This gives us that (the restriction to (a, b, c) with $a < \sqrt{|\Delta_K|/3}$ of) f can be seen as a surjective map to $Cl_K[m]$ (see the remark at Theorem 4.2).

Proof. The proof consists of the following propositions (4.6 and 4.7), and Theorem 2.6. □

Proposition 4.6. *Let $D \in \mathbb{Z}_{>3}$ be square-free and put $K = \mathbb{Q}(\sqrt{-D})$. Take $m \geqslant 3$ an odd integer and $[\mathfrak{a}] \in Cl_K[m]$ with $\mathfrak{a} \subset \mathcal{O}_K$ an ideal representing $[\mathfrak{a}]$, such that for all prime numbers $p \in \mathbb{Z}$ one has $p\mathcal{O}_K \not\supset \mathfrak{a}$.*
Then $\mathfrak{a}^m = \left(\tfrac{b+c\sqrt{-D}}{2}\right)$ for unique $b, c \in \mathbb{Z}$ with $b \geq 0$ and $c > 0$ if $b = 0$.
As a result, $\mathfrak{a}$ can be written as $\left(a, \frac{b+c\sqrt{-D}}{2\gcd(a,b)^{(m-1)/2}}\right)$ with $4a^m = b^2 + c^2 D$ or, equivalently, $a = N(\mathfrak{a})$. Furthermore, $\gcd(a, b)$ is square-free, and the primes dividing $\gcd(a, b)$ ramify.

Proof. Let $m \in \mathbb{Z}_{\geqslant 3}$, and suppose we have some ideal class $[\mathfrak{a}] \in Cl_K[m]$, with $\mathfrak{a} \subset \mathcal{O}_K$ an ideal which is not divisible by any prime $p \in \mathbb{Z}$.

The m-th power of $\mathfrak{a}$ is a principal ideal, so we can write $\mathfrak{a}^m = \left(\tfrac{b+c\sqrt{-D}}{2}\right)$ for some $\frac{b+c\sqrt{-D}}{2} \in \mathcal{O}_K$ ($b, c \in \mathbb{Z}$). Put $a := N(\mathfrak{a})$, then $\frac{b^2+c^2D}{4} = N\left(\tfrac{b+c\sqrt{-D}}{2}\right) = N(\mathfrak{a}^m) = N(\mathfrak{a})^m = a^m$ hence $4a^m = b^2 + c^2 D$.

Since $D > 3$ is square-free, the unit group $\mathcal{O}_K^*$ equals $\{\pm 1\}$, so the element $\frac{b+c\sqrt{-D}}{2} \in \mathcal{O}_K$ generating $\mathfrak{a}^m$ is unique up to a sign. We can choose b to be nonnegative, and if $b = 0$ choose $c > 0$ (note that $\mathfrak{a} \neq (0)$) to make our choice of b, c unique.

In the special case $b = 0$ we have $4a^m = c^2 D$.
Suppose m is even, then $4a^m$ is a square, and since c^2 is a square and D is square-free it follows that $D = 1$ which contradicts $D > 3$. So we conclude that m is odd.
Since D is square-free it follows that $2a^{\frac{m-1}{2}} | c$ and $D | a$. Therefore $4D^m | 4a^m = c^2 D$ and $D^{\frac{m-1}{2}} | \frac{c}{2}$. All primes dividing the integer $\left(\frac{a}{D}\right)^m = \left(\frac{c}{2D^{\frac{m-1}{2}}}\right)^2$ occur a multiple of $\operatorname{lcm}(m, 2) = 2m$ times. Therefore $\sqrt[m]{\frac{c}{2D^{\frac{m-1}{2}}}}$ is in $\mathbb{Z}$ and $\mathfrak{a} = \left(\sqrt[m]{\frac{c}{2D^{\frac{m-1}{2}}}}\sqrt{-D}\right)$ which is a principal ideal. By assumption, there is no prime dividing $\mathfrak{a}$. Therefore $\sqrt[m]{\frac{c}{2D^{\frac{m-1}{2}}}} = 1$ which implies $c = 2D^{\frac{m-1}{2}}$ and hence $D = a$, so one concludes $(a, b, c) = (D, 0, 2D^{\frac{m-1}{2}})$ and $\mathfrak{a} = (\sqrt{-D})$.

By now, we have integers a, b and c for which $N(\mathfrak{a}) = a$, $4a^m = b^2 + c^2 D$, $b \geq 0$, and $c \geq 0$ if $b = 0$, and those are the unique ones for which additionally $\mathfrak{a}^m = \left(\tfrac{b+c\sqrt{-D}}{2}\right)$.

If $\gcd(a,b)=1$ then we have like before

$$\begin{aligned}\left(a,\ \frac{b+c\sqrt{-D}}{2}\right)^m &= \left(a^m,\ a^{m-1}\frac{b+c\sqrt{-D}}{2},\ a^{m-2}\left(\frac{b+c\sqrt{-D}}{2}\right)^2,\ \dots\ ,\ \left(\frac{b+c\sqrt{-D}}{2}\right)^m\right)\\ &= \left(\frac{b^2+c^2D}{4},\ a^{m-1}\frac{b+c\sqrt{-D}}{2},\ a^{m-2}\left(\frac{b+c\sqrt{-D}}{2}\right)^2,\ \dots\ ,\ \left(\frac{b+c\sqrt{-D}}{2}\right)^m\right)\\ &= \left(\frac{b+c\sqrt{-D}}{2}\right)\left(\frac{b-c\sqrt{-D}}{2}, a^{m-1}, a^{m-2}\frac{b+c\sqrt{-D}}{2},\ \dots\ ,\ \left(\frac{b+c\sqrt{-D}}{2}\right)^{m-1}\right)\end{aligned}$$

We now use the equality $X\cdot\frac{b+c\sqrt{-D}}{2} = X\cdot b - X\cdot\frac{b-c\sqrt{-D}}{2}$ (for $X\in\mathcal{O}_K$) to replace the powers of $\frac{b+c\sqrt{-D}}{2}$ by powers of b:

$$\begin{aligned}\cdots &= \left(\frac{b+c\sqrt{-D}}{2}\right)\left(\frac{b-c\sqrt{-D}}{2}, a^{m-1}, a^{m-2}b,\ \dots,\ b^{m-1}\right)\\ &= \left(\frac{b+c\sqrt{-D}}{2}\right)\left(\frac{b-c\sqrt{-D}}{2},\ (\gcd(a,b))^{m-1}\right).\end{aligned}$$

So if $\gcd(a,b)=1$ then $\mathfrak{a}^m = \left(\frac{b+c\sqrt{-D}}{2}\right) = \left(a,\ \frac{b+c\sqrt{-D}}{2}\right)^m$ and therefore $\mathfrak{a} = \left(a, \frac{b+c\sqrt{-D}}{2}\right)$.

Now consider the general case: $\gcd(a,b)$ not necessarily equal to 1. Suppose some prime p divides $\gcd(a,b)$, then $p^m|4a^m = b^2+c^2D$ which implies $p^2|c^2D$, and because D is square-free we have $p|c$. But then p is a divisor of $\frac{b+c\sqrt{-D}}{2}$ in $\mathcal{O}_K$, by the following argument. For $p\neq 2$ it is clear. In the remaining case $p=2$ the equality $4a^m = b^2+c^2D$ and the assumption $p|\gcd(a,b)$ imply that $b\equiv c\equiv 0 \mod 4$, so indeed 2 is a divisor of $\frac{b+c\sqrt{-D}}{2}$ in $\mathcal{O}_K$.
So we have $(p)|\left(\frac{b+c\sqrt{-D}}{2}\right) = \mathfrak{a}^m$. If p splits or p is inert, then it follows that $(p)|\mathfrak{a}$ which is in contradiction with our choice of $\mathfrak{a}$ as an ideal not divisible by any prime. Therefore $\gcd(a,b)$ is a product of ramifying primes.

If the square of such a prime p divides $\gcd(a,b)$, then $p^2|N(\mathfrak{a})$ and p ramifies: $(p)=\mathfrak{p}^2$ where $\mathfrak{p}$ is the unique prime ideal of norm p. Therefore $\mathfrak{p}^2|\mathfrak{a}$, but then also $p|\mathfrak{a}$, which is in contradiction with the assumption that $\mathfrak{a}$ is not divisible by any $\mathbb{Z}$-prime p. We conclude that $\gcd(a,b)$ is square-free.

Recall that every prime dividing $\gcd(a,b)$ divides $\frac{b+c\sqrt{-D}}{2}$ in $\mathcal{O}_K$. Therefore from $\gcd(a,b)$ being square-free we now conclude that $\frac{b+c\sqrt{-D}}{2\gcd(a,b)}$ is an element of $\mathcal{O}_K$.

We will now show that $\gcd(a,b)^2|b$. Indeed, suppose $p|\gcd(a,b)$. As we saw earlier, this implies $p|c$ and p ramifies. Therefore $p|\Delta_K = \begin{cases} D & \text{for } D\equiv 3 \mod 4\\ 4D & \text{for } D\not\equiv 3 \mod 4.\end{cases}$
If p is odd, then $p^3|c^2D = 4a^m - b^2$. This implies $p^3|b^2$, and $p^2|b$.
If p is even, then $p^5|4a^m$ (since $m\geq 3$), and either $p|D$ or $D\equiv 1 \mod 4$.
In the first case, as before one concludes $p^3|c^2D = 4a^m - b^2$, hence $p^3|b^2$ and $p^2|b$.
In the latter case $b^2+c^2D = 4a^m \equiv 0 \mod 32$, where b and c are even and $D\equiv 1 \mod 4$. This implies $b^2\equiv c^2\equiv 0 \mod 16$, so also in this case p^2 divides b and c.
So any prime $p|\gcd(a,b)$ satisfies $p^2|b$. Since $\gcd(a,b)$ is square-free, it follows that $\gcd(a,b)^2|b$.

We will now show that for all primes $p|\gcd(a,b)$, we have $v_p(\frac{1}{2}\gcd(b,c)) = \lfloor\frac{m}{2}\rfloor$, and hence $\gcd(a,b)^{\lfloor\frac{m}{2}\rfloor}$ divides $\frac{b+c\sqrt{-D}}{2}$ in $\mathcal{O}_K$ whilst $p^{\lfloor\frac{m}{2}\rfloor+1}$ does not for any prime $p|\gcd(a,b)$. (Note that if $2|\gcd(a,b)$, then $D\not\equiv 3 \mod 4$, and therefore $\frac{1+\sqrt{-D}}{2}\notin\mathcal{O}_K$.)

Let $p|\gcd(a,b)$. All primes dividing $\gcd(a,b)$ ramify, so $p|\Delta_K = \begin{cases} D & \text{for } D\equiv 3 \mod 4,\\ 4D & \text{for } D\not\equiv 3 \mod 4.\end{cases}$
If p is odd, then $p|D$. Because D is square-free, $v_p(D)=1$. So, considering the equation $4a^m = b^2+c^2D$, we have that $v_p(4a^m)$ is a multiple of m, $v_p(b^2)$ is even, and $v_p(c^2D)$ is odd. Therefore $v_p(b^2)\neq v_p(c^2D)$, and hence either $v_p(4a^m)=v_p(b^2)<v_p(c^2D)$ if m is even, or $v_p(4a^m)=v_p(c^2D)<v_p(b^2)$ if m is odd (otherwise, some power of p would divide two out of those three without dividing the third, which is clearly impossible). Because $\gcd(a,b)$ is square-free and $m>2$, this implies $v_p(a)=1$, and hence $v_p(\gcd(b,c)) = \lfloor\frac{m}{2}\rfloor$.
If $p=2$, either $2|D$ or $D\equiv 1 \mod 4$.

In the first case, like before, either $v_p(4a^m) = v_p(b^2) < v_p(c^2D)$ or $v_p(4a^m) = v_p(c^2D) < v_p(b^2)$. Here $v_p(4a^m) = m+2$, so $v_p(\gcd(b,c)) = \lfloor \frac{m}{2} \rfloor + 1$.
In the second case, if $v_p(b^2) \neq v_p(c^2D)$ then, like before, $v_p(\gcd(b,c)) = \lfloor \frac{m}{2} \rfloor + 1$. Else $v_p(b^2) = v_p(c^2D)$, and because both D and odd squares are equivalent to 1 mod 4 we have: $v_p(4a^m) = v_p(b^2 + c^2D) = v_p(b^2) + 1$. Because $\gcd(a,b) = 1$ and $m > 2$, this implies $v_p(a) = 1$ and $v_p(b) = v_p(c) = \frac{m+2-1}{2} = \frac{m}{2} + 1$.
So in all cases, $v_p(\frac{1}{2}\gcd(b,c)) = \lfloor \frac{m}{2} \rfloor$.

In the following, let $m \in \mathbb{Z}_{\geqslant 3}$ be an odd integer.
Now consider the integral $\mathcal{O}_K$-ideal $I := \left(a, \frac{b+c\sqrt{-D}}{2y}\right)$ with $y = \gcd(a,b)^{\lfloor \frac{m}{2} \rfloor} = \gcd(a,b)^{\frac{m-1}{2}}$.
As shown above, any prime p dividing $\gcd(a,b)$ does not divide $\frac{b+c\sqrt{-D}}{2y}$, hence I is not divisible by any prime.
For I^2 we have:

$$\begin{aligned} I^2 &= \left(a, \frac{b+c\sqrt{-D}}{2y}\right)^2 \\ &= \left(a^2, a\frac{b+c\sqrt{-D}}{2y}, \frac{b^2+2bc\sqrt{-D}-c^2D}{4y^2}\right) \\ &= \left(a^2, a\frac{b+c\sqrt{-D}}{2y}, \frac{-4a^m+2b^2+2bc\sqrt{-D}}{4y^2}\right) \\ &= \left(a^2, a\frac{b+c\sqrt{-D}}{2y}, \frac{-a^m}{\gcd(a,b)^{2\lfloor \frac{m}{2} \rfloor}} + \frac{b}{\gcd(a,b)^{\lfloor \frac{m}{2} \rfloor}}\frac{b+c\sqrt{-D}}{2y}\right), \end{aligned}$$

which we will show to be divisible by $\gcd(a,b)$.
The first two generating elements are divisible by a, hence divisible by $\gcd(a,b)$. Because m is odd, we have $2\lfloor \frac{m}{2} \rfloor = m-1$, so $\frac{-a^m}{\gcd(a,b)^{2\lfloor \frac{m}{2} \rfloor}} = \frac{-a^m}{\gcd(a,b)^{m-1}}$ is divisible by $\gcd(a,b)$. To see that also $\frac{b}{\gcd(a,b)^{\lfloor \frac{m}{2} \rfloor}}$ is divisible by $\gcd(a,b)$, note that m is odd, so for each prime p dividing $\gcd(a,b)$ we have $v_p(b) > \lfloor \frac{m}{2} \rfloor$ as is shown above. As $y = \gcd(a,b)^{\lfloor \frac{m}{2} \rfloor}$ and $\gcd(a,b)$ is square-free, this implies $\gcd(a,b) \mid \frac{b}{\gcd(a,b)^{\lfloor \frac{m}{2} \rfloor}}$.
We conclude that I^2 is divisible by $\gcd(a,b)$.

The m-th power I^m of I is given by

$$\begin{aligned} &\left(a, \tfrac{b+c\sqrt{-D}}{2y}\right)^m \\ &= \left(a^m, a^{m-1}\tfrac{b+c\sqrt{-D}}{2y}, a^{m-2}\left(\tfrac{b+c\sqrt{-D}}{2y}\right)^2, \ \cdots\ , \left(\tfrac{b+c\sqrt{-D}}{2y}\right)^m\right) \\ &= \left(\tfrac{b^2+c^2D}{4}, a^{m-1}\tfrac{b+c\sqrt{-D}}{2y}, a^{m-2}\left(\tfrac{b+c\sqrt{-D}}{2y}\right)^2, \ \cdots\ , \left(\tfrac{b+c\sqrt{-D}}{2y}\right)^m\right) \\ &= \left(\tfrac{b+c\sqrt{-D}}{2y}\right)\left(y\tfrac{b-c\sqrt{-D}}{2}, a^{m-1}, a^{m-2}\tfrac{b+c\sqrt{-D}}{2y}, \ \cdots\ , \left(\tfrac{b+c\sqrt{-D}}{2y}\right)^{m-1}\right) \\ &= \left(\tfrac{b+c\sqrt{-D}}{2y}\right)\left(\left(y\tfrac{b-c\sqrt{-D}}{2}\right) + \left(a^{m-1}, a^{m-2}\tfrac{b+c\sqrt{-D}}{2y}, \ \cdots\ , \left(\tfrac{b+c\sqrt{-D}}{2y}\right)^{m-1}\right)\right) \\ &= \left(\tfrac{b+c\sqrt{-D}}{2y}\right)\left(\left(y\tfrac{b-c\sqrt{-D}}{2}\right) + I^{m-1}\right) \end{aligned}$$

Because I^2 is divisible by $\gcd(a,b)$ and m is odd, we have that I^{m-1} is divisible by $\gcd(a,b)^{\frac{m-1}{2}} = y$. Therefore the integral $\mathcal{O}_K$-ideal on the right is divisible by y, and

$$\begin{aligned} I^m &= \left(\frac{b+c\sqrt{-D}}{2}\right)\left(\left(\frac{b-c\sqrt{-D}}{2}\right) + \frac{I^{m-1}}{y}\right) \\ &= \mathfrak{a}^m\left(\frac{b-c\sqrt{-D}}{2}, \frac{a^{m-1}}{y}, \frac{a^{m-2}}{y}\frac{b+c\sqrt{-D}}{2y}, \ \cdots\ , \frac{1}{y}\left(\frac{b+c\sqrt{-D}}{2y}\right)^{m-1}\right). \end{aligned}$$

We will show that $I = \mathfrak{a}$ by proving that the norm of the ideal on the right equals 1.

Note that $N(I^m) =$

$$a^m \cdot N\left(\left(\frac{b-c\sqrt{-D}}{2},\ \frac{a^{m-1}}{y},\ \frac{a^{m-2}}{y}\frac{b+c\sqrt{-D}}{2y},\ \cdots\ ,\ \frac{1}{y}\left(\frac{b+c\sqrt{-D}}{2y}\right)^{m-1}\right)\right).$$

Consider the inclusion of $\mathbb{Z}$-modules (all free of rank two)

$$\mathbb{Z}a + \mathbb{Z}\frac{b+c\sqrt{-D}}{2y} \subset I \subset \mathcal{O}_K \subset \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-D}}{2}.$$

It implies

$$\left[I\ :\ \mathbb{Z}a + \mathbb{Z}\tfrac{b+c\sqrt{-D}}{2y}\right] \cdot [\mathcal{O}_K\ :\ I] \cdot \left[\mathbb{Z} + \mathbb{Z}\tfrac{1+\sqrt{-D}}{2}\ :\ \mathcal{O}_K\right]$$
$$=$$
$$\left[\mathbb{Z} + \mathbb{Z}\tfrac{1+\sqrt{-D}}{2}\ :\ \mathbb{Z}a + \mathbb{Z}\tfrac{b+c\sqrt{-D}}{2y}\right] = a\tfrac{|c|}{y},$$

where the last equality is seen as follows. Identifying $\mathbb{Z}+\mathbb{Z}\frac{1+\sqrt{-D}}{2} \cong \mathbb{Z}^2$ via $n+m\frac{1+\sqrt{-D}}{2} \mapsto (n,m)$, the subgroup $\mathbb{Z}a + \mathbb{Z}\frac{b+c\sqrt{-D}}{2y}$ corresponds to $\mathbb{Z}\cdot(a,0) + \mathbb{Z}\cdot(\frac{b-c}{2y}, \frac{c}{y})$. Clearly the latter subgroup has index $\frac{a|c|}{y}$ in $\mathbb{Z}^2$.

The argument above implies that $N(I) = [\mathcal{O}_K\ :\ I]$ divides $a\frac{c}{y}$. As a consequence $N(I^m) \mid a^m\frac{c^m}{y^m}$, which in turn implies $N\left(\left(\frac{b-c\sqrt{-D}}{2},\ \frac{a^{m-1}}{y},\ \frac{a^{m-2}}{y}\frac{b+c\sqrt{-D}}{2y},\ \cdots\ ,\ \frac{1}{y}\left(\frac{b+c\sqrt{-D}}{2y}\right)^{m-1}\right)\right) \mid \frac{c^m}{y^m}$. This norm is also a divisor of $N\left(\frac{1}{y}\left(\frac{b+c\sqrt{-D}}{2y}\right)^{m-1}\right) = \frac{a^{m(m-1)}}{y^{2m}}$, therefore it divides

$$\gcd\left(\frac{c^m}{y^m},\ \frac{a^{m(m-1)}}{y^{2m}}\right) = \gcd\left(\frac{c}{y},\ \frac{a^{m-1}}{y^2}\right)^m = \gcd\left(\frac{c}{\gcd(a,b)^{\frac{m-1}{2}}},\ \frac{a^{m-1}}{\gcd(a,b)^{m-1}}\right).$$

We claim that the latter gcd equals 1. This indeed follows from the fact that $\gcd(a,c) \mid \gcd(a,b)$, and the fact that for every prime p dividing $\gcd(a,b)$ we have $v_p(a) = 1$.

So $\left(\frac{b-c\sqrt{-D}}{2},\ \frac{a^{m-1}}{y},\ \frac{a^{m-2}}{y}\frac{b+c\sqrt{-D}}{2y},\ \cdots\ ,\ \frac{1}{y}\left(\frac{b+c\sqrt{-D}}{2y}\right)^{m-1}\right)$ is the unit ideal, and we conclude that, for odd m, $I = \mathfrak{a}$, so $\mathfrak{a} = \left(a, \frac{b+c\sqrt{-D}}{2y}\right)$ with $y = \gcd(a,b)^{\frac{m-1}{2}}$.

□

In the reverse direction, analogous to the cubic case of the previous section, a condition on $\gcd(a,b)$ that turns out to be sufficient to give us ideals of order dividing m is that $\gcd(a,b)$ has to be square-free and that the primes dividing $\gcd(a,b)$ ramify in $\mathcal{O}_K$, as is shown in the following proposition.

Proposition 4.7. *Let $K := \mathbb{Q}(\sqrt{-D})$ be a quadratic field with $D \in \mathbb{Z}$ square-free and $D > 3$, and let $m \geqslant 3$ be an odd integer, $a, b, c \in \mathbb{Z}$ with $4a^m = b^2 + c^2D$, $\gcd(a,b)$ square-free and the primes dividing $\gcd(a,b)$ ramifying in $\mathcal{O}_K$.*
Then $\mathfrak{a} := \left(a, \frac{b+c\sqrt{-D}}{2y}\right)$ with $y = \gcd(a,b)^{(m-1)/2}$ is an integral $\mathcal{O}_K$-ideal in $Cl_K[m]$, and $\mathfrak{a}^m = \left(\frac{b+c\sqrt{-D}}{2}\right)$. Furthermore, this ideal $\mathfrak{a}$ is not divisible by any $\mathbb{Z}$-prime p.

Proof. Suppose we have some prime $p|\gcd(a,b)$, then $p^m|4a^m = b^2 + c^2D$. Therefore $p^2|c^2D$. But D is square-free, so $p|c$. Furthermore, if $p = 2$ then $b^2 + c^2D \equiv 0 \mod 32$, hence $\left(\frac{b}{2}\right)^2 + \left(\frac{c}{2}\right)^2 D \equiv 0 \mod 8$, and therefore either $\frac{b}{2} \equiv \frac{c}{2} \equiv 1 \mod 2$ and $D \equiv 3 \mod 4$, or $\frac{b}{2} \equiv \frac{c}{2} \equiv 0 \mod 2$. So in all cases, p divides $\frac{b+c\sqrt{-D}}{2}$ in $\mathcal{O}_K$. Because $\gcd(a,b)$ is square-free, it follows that $\frac{b+c\sqrt{-D}}{2\gcd(a,b)} \in \mathcal{O}_K$. Like in the proof of Proposition 4.6 above, we have that $v_p(\frac{1}{2}\gcd(b,c)) = \lfloor \frac{m}{2} \rfloor$, and hence $\gcd(a,b)^{\lfloor \frac{m}{2} \rfloor}$ divides $\frac{b+c\sqrt{-D}}{2}$ in $\mathcal{O}_K$ whilst $p^{\lfloor \frac{m}{2} \rfloor + 1}$ does not for any prime $p|\gcd(a,b)$.

Consider the integral $\mathcal{O}_K$-ideal $\mathfrak{a} := \left(a, \frac{b+c\sqrt{-D}}{2y}\right)$ with $y = \gcd(a,b)^{(m-1)/2}$. We first show that the norm of this ideal is equal to a.

The m-th power of $\mathfrak{a}$ is given by

$$\begin{aligned}
\mathfrak{a}^m &= \left(a, \quad \frac{b+c\sqrt{-D}}{2y}\right)^m \\
&= \left(a^m, \quad a^{m-1}\frac{b+c\sqrt{-D}}{2y}, \quad a^{m-2}\left(\frac{b+c\sqrt{-D}}{2y}\right)^2, \quad \ldots, \quad \left(\frac{b+c\sqrt{-D}}{2y}\right)^m\right) \\
&= \left(\frac{b^2+c^2D}{4}, \quad a^{m-1}\frac{b+c\sqrt{-D}}{2y}, \quad a^{m-2}\left(\frac{b+c\sqrt{-D}}{2y}\right)^2, \quad \ldots, \quad \left(\frac{b+c\sqrt{-D}}{2y}\right)^m\right) \\
&= \left(\frac{b+c\sqrt{-D}}{2y}\right)\cdot\left(y\frac{b-c\sqrt{-D}}{2}, \quad a^{m-1}, \quad a^{m-2}\frac{b+c\sqrt{-D}}{2y}, \quad \ldots, \quad \left(\frac{b+c\sqrt{-D}}{2y}\right)^{m-1}\right)
\end{aligned}$$

So on one hand, $N\left(\frac{b+c\sqrt{-D}}{2y}\right) = \frac{a^m}{\gcd(a,b)^{m-1}}$ is a divisor of $N(\mathfrak{a}^m)$, and $N(\mathfrak{a}^m)$ is a divisor of $N\left(\frac{b+c\sqrt{-D}}{2y}\right)\cdot N\left(\left(\frac{b+c\sqrt{-D}}{2y}\right)^{m-1}\right) = \frac{a^{m^2}}{\gcd(a,b)^{m(m-1)}}$.
On the other hand, if we look at $\mathfrak{a}$ and $\mathcal{O}_K$ as $\mathbb{Z}$-modules, then we have the following inclusion of rank 2 $\mathbb{Z}$-modules:

$$\mathbb{Z}a + \mathbb{Z}\frac{b+c\sqrt{-D}}{2y} \subset \mathfrak{a} \subset \mathcal{O}_K \subset \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-D}}{2}.$$

This implies

$$\begin{gathered}
\left[\mathfrak{a} \ : \ \mathbb{Z}a + \mathbb{Z}\tfrac{b+c\sqrt{-D}}{2y}\right]\cdot[\mathcal{O}_K \ : \ \mathfrak{a}]\cdot\left[\mathbb{Z} + \mathbb{Z}\tfrac{1+\sqrt{-D}}{2} \ : \ \mathcal{O}_K\right] \\
= \\
\left[\mathbb{Z} + \mathbb{Z}\tfrac{1+\sqrt{-D}}{2} \ : \ \mathbb{Z}a + \mathbb{Z}\tfrac{b+c\sqrt{-D}}{2y}\right] = a\tfrac{|c|}{y},
\end{gathered}$$

and therefore $N(\mathfrak{a}) = [\mathcal{O}_K \ : \ \mathfrak{a}]$ divides $a\frac{c}{y}$, hence $N(\mathfrak{a}^3) \mid a^m\frac{c^m}{y^m}$. Because $N(\mathfrak{a}^m)$ divides both $\frac{a^{m^2}}{\gcd(a,b)^{m(m-1)}}$ and $a^m\frac{c^m}{y^m}$, it also divides $\gcd\left(\frac{a^{m^2}}{\gcd(a,b)^{m(m-1)}}, \quad a^m\frac{c^m}{y^m}\right) = a^m\gcd\left(a_1^{m-1}, c_1\right)^m$, where $a_1 = \frac{a}{\gcd(a,b)}$, and $c_1 = \frac{c}{y} \in \mathbb{Z}$. We have $4\gcd(a,b)a_1^m = \frac{1}{y^2}4a^3 = \frac{1}{y^2}\left(b^2+c^2D\right) = b_1^2 + c_1^2D$ with $b_1 = \frac{b}{y}$. Here $\gcd(a_1,b_1) = 1$, and therefore $\gcd(a_1,c_1) = 1$. It follows that $\gcd(a_1^{m-1},c_1)^3 = 1$ and $N(\mathfrak{a}^m) \mid a^m$.
Now we have $\frac{a^m}{\gcd(a,b)^{m-1}} \mid N(\mathfrak{a}^m) \mid a^m$. Because $\gcd(a,b)$ is square-free, this implies $N(\mathfrak{a}^m) = a^m$, hence $N(\mathfrak{a}) = a$.

Now we show that $\mathfrak{a}^m$ is a principal ideal.

Like in the proof of Proposition 4.6, we get that $\gcd(a,b)$ divides $\mathfrak{a}^2$ in $\mathcal{O}_K$.
Hence we can write

$$\begin{aligned}
\mathfrak{a}^m &= \left(\frac{b+c\sqrt{-D}}{2y}\right)\cdot\left(y\frac{b-c\sqrt{-D}}{2}, \quad a^{m-1}, \quad a^{m-2}\frac{b+c\sqrt{-D}}{2y}, \quad \ldots, \quad \left(\frac{b+c\sqrt{-D}}{2y}\right)^{m-1}\right) \\
&= \left(\frac{b+c\sqrt{-D}}{2y}\right)\cdot\left(y\frac{b-c\sqrt{-D}}{2}, \quad \mathfrak{a}^{m-1}\right) \\
&= \left(\frac{b+c\sqrt{-D}}{2}\right)\cdot\left(\frac{b-c\sqrt{-D}}{2}, \quad \frac{\mathfrak{a}^{m-1}}{\gcd(a,b)^{(m-1)/2}}\right)
\end{aligned}$$

where the last ideal on the right hand side is integral in $\mathcal{O}_K$. Because $N(\mathfrak{a}) = a$ and $N\left(\frac{b+c\sqrt{-D}}{2}\right) = a^m$, the norm of this right hand side integral ideal is equal to 1, hence it is the unit ideal.
We conclude $\mathfrak{a}^m = \left(\frac{b+c\sqrt{-D}}{2}\right)$.

To complete the proof we now show that $\mathfrak{a}$ is not divisible by any $\mathbb{Z}$-prime p.
Suppose $\mathfrak{a}$ is divisible by some $\mathbb{Z}$-prime p, then the generators of $\mathfrak{a}$ are divisible by p, so $\frac{b+c\sqrt{-D}}{2y}$ and its conjugate element $\frac{b-c\sqrt{-D}}{2y}$ are divisible by p, hence $p \mid \frac{b+c\sqrt{-D}}{2y} + \frac{b-c\sqrt{-D}}{2y} = \frac{b}{y}$. Furthermore, $p^2 \mid N(\mathfrak{a}) \mid N\left(\frac{b+c\sqrt{-D}}{2y}\right) = \frac{a^m}{\gcd(a,b)^{m-1}}$. By now, it is clear that $p \mid \gcd(a,b)$, so it follows that $p^2|a$ and $p|\frac{b}{p}$, hence p^2 divides $\gcd(a,b)$ which is in contradiction with $\gcd(a,b)$ being square-free.

We conclude that there is no $\mathbb{Z}$-prime p dividing $\mathfrak{a}$.

□

We conclude that the correspondence of Section 4.2 can be generalised to a correspondence between certain solutions of the norm equation $4a^m = b^2 + c^2D$ and ideals representing classes in $Cl_K[m]$ for general odd integers $m \geqslant 3$, and that the restriction of this correspondence to the finite set of solutions with $a < \sqrt{|\Delta_K|/3}$ can be seen as a surjection to $Cl_K[m]$.

4.4. Comparing the correspondence in §4.3 with the isomorphism of Proposition 3.4.

In this section we deal with an imaginary quadratic number field K, and an odd integer $m \geqslant 3$. Section 4.3 relates ideals representing ideal classes of order dividing m, to solutions of a norm equation. Also, the proof of Theorem 4.5 relates such ideal classes to certain elements in K^*/K^{*m}.

Now we compare and combine these two results.

On one hand, it is clear that the ideals mentioned in Theorem 4.5 can be seen as representants of the elements of $Cl_K[m]$ which occur at the right hand side of the isomorphism of Proposition 3.4.

We will show that on the other hand, representants of elements in $\ker(v)$ occurring at the left hand side of Proposition 3.4 correspond to solutions of the equation $4a^m = b^2 + c^2D$ as mentioned in Theorem 4.5 in the following way:

Proposition 4.8. *Let $m \in \mathbb{Z}_{\geqslant 3}$ be an odd integer and $D \in \mathbb{Z}_{>3}$ square-free, as in Proposition 3.4 and Theorem 4.5.*

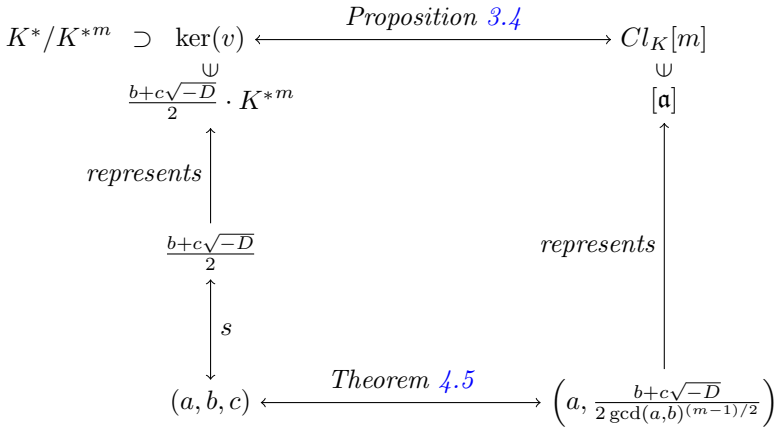
The representants $\frac{\tilde{b}+\tilde{c}\sqrt{-D}}{2}$ of elements in $\ker(v) \subset K^*/K^{*m}$ with $\frac{\tilde{b}+\tilde{c}\sqrt{-D}}{2}$ integral and not divisible by the m-th power of any $\mathbb{Z}$-prime p in $\mathcal{O}_K$ and with $\tilde{b} \geqslant 0$ and $\tilde{c} \geqslant 0$ if $\tilde{b} = 0$, correspond bijectively to solutions (a, b, c) of the equation $4a^m = b^2 + c^2D$ with $a, b, c \in \mathbb{Z}$, $b \geqslant 0$, $c \geqslant 0$ if $b = 0$, $\gcd(a, b)$ square-free, and the primes dividing $\gcd(a, b)$ ramifying in $\mathcal{O}_K$. The bijection is given by

$$s \;:\; \frac{b+c\sqrt{-D}}{2} \;\longmapsto\; (a,b,c) \text{ where } a := \sqrt[m]{N\left(\frac{b+c\sqrt{-D}}{2}\right)},$$

and

$$s^{-1} \;:\; (a,b,c) \;\longmapsto\; \frac{b+c\sqrt{-D}}{2}.$$

This bijection satisfies: for such a solution (a, b, c), the corresponding ideal (by Theorem 4.5) belongs to the ideal class which (by Proposition 3.4) corresponds to $\frac{b+c\sqrt{-D}}{2}$.



Proof. First in one direction:

Suppose we have a representant $\frac{b+c\sqrt{-D}}{2}$ of an element $\frac{b+c\sqrt{-D}}{2} \cdot K^{*m} \in \ker(v) \subset K^*/K^{*m}$ with $\frac{b+c\sqrt{-D}}{2}$ integral and not divisible by the m-th power of any $\mathbb{Z}$-prime p in $\mathcal{O}_K$ and satisfying $b \geqslant 0$ and $c \geqslant 0$ if $b = 0$.

Because $\frac{b+c\sqrt{-D}}{2} \cdot K^{*m}$ is in $\ker(v)$, we have that all prime ideals occurring in the unique prime ideal factorisation of $\left(\frac{b+c\sqrt{-D}}{2}\right)$ occur with multiplicity divisible by m, hence $\left(\frac{b+c\sqrt{-D}}{2}\right) = I^m$ for some

integral $\mathcal{O}_K$-ideal I. Therefore $N\left(\frac{b+c\sqrt{-D}}{2}\right)$ is an m-th power and $a := \sqrt[m]{N\left(\frac{b+c\sqrt{-D}}{2}\right)} = N(I)$ is a well defined integer, which indeed satisfies $4a^m = b^2 + c^2 D$.

Now we show that the fact that $\frac{b+c\sqrt{-D}}{2}$ is not divisible by any non-unit m-th power imposes the remaining conditions on $\gcd(a, b)$:

Suppose some prime p divides $\gcd(a, b)$, then also $p^2 \mid c^2 D$ and hence $p|c$. If $p = 2$ then - because $4a^m \equiv 0 \mod 4$ - either both $\frac{b}{2}$ and $\frac{c}{2}$ are even, or $\left(\frac{b}{2}\right)^2 \equiv \left(\frac{c}{2}\right)^2 \equiv 1 \mod 4$ and hence $D \equiv 3 \mod 4$ which implies $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-D}}{2}]$. So in all cases, $p \mid \frac{b+c\sqrt{-D}}{2}$. It follows that $(p) \mid \left(\frac{b+c\sqrt{-D}}{2}\right) = I^m$. If p splits or is inert, this implies $(p) \mid I$ and hence $(p)^m \mid I^m = \left(\frac{b+c\sqrt{-D}}{2}\right)$, which is in contradiction with $\frac{b+c\sqrt{-D}}{2}$ not being divisible by any non-unit m-th power in $\mathcal{O}_K$. We conclude that p ramifies, and hence all primes dividing $\gcd(a, b)$ ramify.

Suppose p^2 divides $\gcd(a, b)$ for some prime p. Then p ramifies: $p = \mathfrak{p}^2$, and $p^2 \mid a = N(I)$. This implies $(p) = \mathfrak{p}^2 \mid I$, and hence $(p)^m \mid I^m = \left(\frac{b+c\sqrt{-D}}{2}\right)$, which is in contradiction with $\frac{b+c\sqrt{-D}}{2}$ not being divisible by any non-unit m-th power in $\mathcal{O}_K$. We conclude that $\gcd(a, b)$ is square-free.

In the other direction:
Suppose we have some solution (a, b, c) to the equation $4a^m = b^2 + c^2 D$ with $a, b, c \in \mathbb{Z}$, $b \geqslant 0$ and $c \geqslant 0$ if $b = 0$, $\gcd(a, b)$ square-free, and the primes dividing $\gcd(a, b)$ ramifying in $\mathcal{O}_K$. By Theorem 4.5, $\left(\frac{b+c\sqrt{-D}}{2}\right)$ is the m-th power of $\mathfrak{a} := \left(a, \frac{b+c\sqrt{-D}}{2\gcd(a,b)^{(m-1)/2}}\right)$ and $\mathfrak{a}$ is not divisible by any $\mathbb{Z}$-prime p. Therefore, $\left(\frac{b+c\sqrt{-D}}{2}\right)$ is in $\ker(v)$, and not divisible by the m-th power of any $\mathbb{Z}$-prime p.

To complete the proof:
Suppose we have some (a, b, c) as in the Proposition. Then by Theorem 4.5, this corresponds to the ideal $\mathfrak{a} := \left(a, \frac{b+c\sqrt{-D}}{2\gcd(a,b)^{(m-1)/2}}\right)$, where $\mathfrak{a}^m = \left(\frac{b+c\sqrt{-D}}{2}\right)$. Hence by Proposition 3.4, the ideal class $[\mathfrak{a}]$ of $\mathfrak{a}$ corresponds to the element $\alpha K^{*m} \in \ker(v)$ for which $\alpha\mathcal{O}_K = \mathfrak{a}^m = \left(\frac{b+c\sqrt{-D}}{2}\right)$, and hence αK^{*m} is obviously indeed represented by $\frac{b+c\sqrt{-D}}{2}$. □

Combining the bijection of Proposition 4.8 with the theory of Section 3.4, we now are able to determine when different solutions (a, b, c) to the equation $4a^m = b^2 + c^2 D$ as described in Theorem 4.5 give rise to ideals that represent different or even independent elements of $Cl_K[m]$.

Example: Let K be the imaginary quadratic field given by $\mathbb{Q}(\sqrt{-D})$ with $D = 974 = 2 \cdot 487$; note that 487 is a prime number.
Suppose we want to discuss $Cl_K[m]$ for given odd $m \geqslant 3$.
Since $D \equiv 2 \bmod 4$ the ring of integers of K is given by $\mathcal{O}_K = \mathbb{Z}[\sqrt{-D}]$ and its discriminant is $\Delta_K = -4D = -3896$.

First we find the solutions of $a^m = \frac{b^2+c^2 D}{4}$ as in Theorem 4.5 with $0 < a < \sqrt{|\Delta_K|/3} \approx 36.04$ and with $c \neq 0$.
For $m = 3$, we find that the solutions to this equation are: $(a, b, c) = (15, 98, \pm 2)$, $(18, 88, \pm 4)$, $(30, 304, \pm 4)$, $(31, 290, \pm 6)$ or $(33, 358, \pm 4)$. Via the bijection of Proposition 4.8 those represent the elements $\frac{89\pm 2\sqrt{-D}}{2} \cdot K^{*3}$, $\frac{88\pm 4\sqrt{-D}}{2} \cdot K^{*3}$, $\frac{304\pm 4\sqrt{-D}}{2} \cdot K^{*3}$, $\frac{290\pm 6\sqrt{-D}}{2} \cdot K^{*3}$, and $\frac{358\pm 4\sqrt{-D}}{2} \cdot K^{*3}$ in $\ker(v)$.
Following Section 3.4 we construct for various suitable p (via inclusion of K^* in $\mathbb{Q}_p^*$ and the p-adic valuation modulo 3 on $\mathbb{Q}_p^*/\mathbb{Q}_p^{*3}$) different homomorphisms from $\ker(v)$ to $\mathbb{Z}/3\mathbb{Z}$.
First we construct some primes p such that $p \equiv 1 \bmod 3$ and $-D$ is a square mod$p$. A way to do

this is to use prime divisors $\equiv 1 \bmod 3$ of $D+1, D+4, D+9, \ldots$. In this way we find:

p	reduction mod p of $\sqrt{-D} \in \mathbb{Z}_p$	cubes mod p
13	± 1	$1, 5, 8, 12$
163	± 2	$1, 5, 6, 8, 13, 17, 21, 22, 23, 25, 27, 28, 30, 31,$ $36, 37, 38, 40, 48, 53, 58, 59, 61, 64, 65, 77, 78,$ $85, 86, 98, 99, 102, 104, 105, 110, 115, 123, 125, 126, 127, 132,$ $133, 135, 136, 138, 140, 141, 142, 146, 150, 155, 157, 158, 162$
37	± 5	$1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36$
31	± 7	$1, 2, 4, 8, 15, 16, 23, 27, 29, 30$
211	± 9	...
179	± 10	...
...	...	...

At $p = 13$, we choose the homomorphisms $h_\pm : K^* \to \mathbb{Q}_{13}^*$ such that $h_+(\sqrt{-D}) = 1 + * \cdot 13$, and the isomorphism $i : \mathbb{Z}_{13}^*/{\mathbb{Z}_{13}^*}^3 \to \mathbb{F}_{13}^*/{\mathbb{F}_{13}^*}^3 \to \mathbb{Z}/3\mathbb{Z}$ which maps $2^n \cdot {\mathbb{F}_{13}^*}^3 \in \mathbb{F}_{13}^*/{\mathbb{F}_{13}^*}^3$ to $n \bmod 3$. This gives us the homomorphism $\varphi_{\tilde{13}_+} = (i, id) \circ \varphi_{13} \circ h_+ : \ker(v) \to \mathbb{Z}/3\mathbb{Z}$.
Analogue, at $p = 163$ we choose $h_+(\sqrt{-D}) = 2 + * \cdot 163$ and $i(2^n) = n \bmod 163$ to get $\varphi_{\tilde{163}_+}$,
at $p = 37$ we choose $h_+(\sqrt{-D}) = 5 + * \cdot 35$ and $i(2^n) = n \bmod 37$ to get $\varphi_{\tilde{37}_+}$,
and at $p = 31$ we choose $h_+(\sqrt{-D}) = 7 + * \cdot 31$ and $i(3^n) = n \bmod 31$ to get $\varphi_{\tilde{31}_+}$.
This yields the following table

	$13-$adic $\varphi_{\tilde{13}_+}$	$163-$adic $\varphi_{\tilde{163}_+}$	$37-$adic $\varphi_{\tilde{37}_+}$	$31-$adic $\varphi_{\tilde{31}_+}$
$\frac{98+2\sqrt{-D}}{2}$	1	2	1	1
$\frac{88+4\sqrt{-D}}{2}$	2	0	1	0
$\frac{304+4\sqrt{-D}}{2}$	1	1	0	2
$\frac{290+6\sqrt{-D}}{2}$	0	1	1	2
$\frac{358+4\sqrt{-D}}{2}$	0	2	2	1

The first two rows of this table are independent in $(\mathbb{Z}/3\mathbb{Z})^4$, wheras the other rows are linear combinations of these two. So we can conclude that $(15, 98, 2)$ and $(18, 88, 4)$ correspond to ideals representing different independent ideal classes of order 3 in $Cl_K[3]$, hence Cl_K contains at least two independent elements of order 3.

In fact, it is known that in the present example $Cl_K[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

5. Independent elements in $Cl_K[m]$

5.1. **Solderitsch.**

In this section a result of J.J. Solderitsch [Sol92] is recalled. It discusses elements of prime order $p \geqslant 5$ in class groups of imaginary quadratic fields K. Solderitsch states that an alalogous statement can be established for $p = 3$. Our aim is to formulate such a statement for the case $p = 3$ and interpret this in terms of the groups K^*/K^{*3}.

Solderitsch states the following theorem [Sol92][3]. In fact, he formulated the result under the condition $p \geqslant 5$, but the result, with the same proof, also holds for $p = 3$.

Theorem 5.1. ***(Solderitsch)*** *Let $p \geqslant 5$ be a prime and let $\tilde{a}, \tilde{b}, \tilde{c} \in \mathbb{Z}$ with $\gcd(\tilde{a}, 2\tilde{b}) = 1$ and with $\tilde{a}^p = \tilde{c}^2 - \tilde{b}^2$. Suppose that $\tilde{a}^p = \tilde{b}^2 + D$ for some $D > 0$. Let K be the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ with ring of integers $\mathcal{O}_K$ and discriminant Δ_K. Let I and J be the two $\mathcal{O}_K$-ideals given by $I = (\tilde{a}, \tilde{b} + \sqrt{-D})$ and $J = (\tilde{a}^2, \tilde{b}^2 + \tilde{c}\sqrt{-D})$.*
If $1 < \tilde{a}^{p-1} < |\Delta_K|/4$, then the group generated by the classes of I and J generates a subgroup isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ in Cl_K.

Proof. Note that $1 < \tilde{a}^{p-1} < |\Delta_K|/4$ implies $|\Delta_K|/4 > 2$ and hence $D > 3$ and $\mathcal{O}_K^* = \{\pm 1\}$.

Analogous to the reasoning on page 29, the equation $\tilde{a}^p = \tilde{b}^2 + D$ gives rise to the ideal $I = \left(\tilde{a}, \tilde{b} + \sqrt{-D}\right)$. Writing the equation as $4a^m = b^2 + c^2 D$ with $m = p$, $a = \tilde{a}$, $b = 2\tilde{b}$,

[3] For clarity and consistency within this thesis, I changed some of the notation.

and $c = 2$, one has by assumption $\gcd(a, b) = \gcd(\tilde{a}, 2\tilde{b}) = 1$. Hence the computation on page 29 shows $I = \left(a, \frac{b+c\sqrt{-D}}{2}\right)$ satisfies $I^p = \left(\tilde{b} + \sqrt{-D}\right)$ is a principal ideal. In particular I has norm $\tilde{a}$ which by assumption is strictly smaller than $|\Delta_K|/4$, and all powers of I are not divisible by any $\mathbb{Z}$-prime (otherwise - by unique ideal factorisation - at least I^2 and hence I^p would be divisible by such a prime, which is clearly not the case). By Proposition 2.5, the only principal ideal with norm smaller than $|\Delta_K|/4$ and which is not divisible by any $\mathbb{Z}$-prime is the trivial ideal. But the trivial ideal has norm 1, which is by assumption stricly smaller than $\tilde{a}$. Therefore $[I]$ has order p in Cl_K.

We now use the additional equation $\tilde{a}^p = \tilde{c}^2 - \tilde{b}^2$ to construct another solution of $4a^m = b^2 + c^2 D$, as follows.
Take squares of both sides of the equality $\tilde{a}^p = \tilde{b}^2 + D$. This gives

$$(\tilde{a}^2)^p = \left(\tilde{b}^2\right)^2 + \left(2\tilde{b}^2 + D\right) D = \left(\tilde{b}^2\right)^2 + \left(\tilde{a}^p + \tilde{b}^2\right) D = \left(\tilde{b}^2\right)^2 + \tilde{c}^2 D,$$

so we have $4a^m = b^2 + c^2 D$ with $m = p$, $a = \tilde{a}^2$, $b = 2\tilde{b}^2$, and $c = 2\tilde{c}$. Here $\gcd(a, b) = \gcd\left(\tilde{a}^2, 2\tilde{b}^2\right) \leqslant \gcd(\tilde{a}, 2\tilde{b})^2 = 1$, hence $\gcd(a, b) = 1$. The computation on page 29 then shows that $J = \left(a, \frac{b+c\sqrt{-D}}{2}\right)$ satisfies $J^p = \left(\tilde{b}^2 + \tilde{c}\sqrt{-D}\right)$. So $[J]$ has order dividing p in Cl_K and J has norm $\sqrt[p]{\tilde{b}^4 + \tilde{c}^2 D} = \tilde{a}^2$. By assumption, $1 < \tilde{a}^2 < |\Delta_K|/4$, so J is not the trivial ideal. Note that J is not divisible by any $\mathbb{Z}$-prime. Therefore we have by Proposition 2.5 that $[J]$ is not a principal ideal, hence $[J]$ has order p in Cl_K.

To show that $[I]$ and $[J]$ are independent in $Cl_K[p]$, Solderitsch uses the condition $\tilde{a}^{p-1} < |\Delta_K|/4$ and Proposition 2.5:
Suppose $[I]$ and $[J]$ generate the same subgroup of order p in Cl_K, then $[J] = k[I]$ for some $k \in \{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\}$. Since the conjugate ideal $\overline{I}$ of I satisfies $[I] + [\overline{I}] = 0$, we conclude $[J] = |k| \cdot [I_1]$ where I_1 is one of $I, \overline{I}$. Because neither J nor $I_1^{|k|}$ is divisible by any $\mathbb{Z}$-prime, and the norms of J and $I_1^{|k|}$ are both smaller than $|\Delta_K|/4$, we have by Proposition 2.5 that $J = I_1^{|k|}$. It follows that $\tilde{a}^{|k|} = N(I)^{|k|} = N(I_1^{|k|}) = N(J) = \tilde{a}^2$, so $k = \pm 2$ and either $J = I^2$ or $J = \overline{I}^2$. Taking the p-th power on both sides gives us the following equality of principal ideals $\left(\tilde{b}^2 + \tilde{c}\sqrt{-D}\right) = J^p = I_1^{2p} = \left(\tilde{b} \pm \sqrt{-D}\right)^2$. Because $\mathcal{O}_K^* = \{\pm 1\}$, this implies $\tilde{b}^2 + \tilde{c}\sqrt{-D} = \pm\left(\tilde{b} \pm \sqrt{-D}\right)^2$ as elements in $\mathcal{O}_K$. The real part of this equation is $\tilde{b}^2 = \pm\left(\tilde{b}^2 - D\right)$. Therefore $2\tilde{b}^2 = D$ and $K = \mathbb{Q}(\sqrt{-D}) = \mathbb{Q}(\sqrt{-2})$ which is in contradiction with $|\Delta_K|/4 > 2$.
We conclude that $[I]$ and $[J]$ are independent in $Cl_K[p]$.

□

Indeed this proof not only holds for $p \geqslant 5$, but for all odd primes p.

Now we interpret this theorem in terms of the isomorphism $K^*/K^{*m} \supset \ker(v) \cong \mathcal{O}_K^*/\mathcal{O}_K^{*m} \times Cl_K[m]$ of Section 3. In the present situation we have $m = p$ an odd prime. As already observed in the proof, the conditions imply that $\mathcal{O}_K^* = \{\pm 1\}$, so $\mathcal{O}_K^*/\mathcal{O}_K^{*m}$ is trivial and $K^*/K^{*p} \supset \ker(v) \cong Cl_K[p]$.
The ideals I^p and J^p are generated by the elements $\tilde{b} + \sqrt{-D}$ respectively $\tilde{b}^2 + \tilde{c}\sqrt{-D}$, which both represent elements in $\ker(v)$. The statement that $[I]$ and $[J]$ generate a subgroup isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ in $Cl_K[p]$ then corresponds to te statement that $\tilde{b}^2 + \tilde{c}\sqrt{-D}$ and powers of $\tilde{b} + \sqrt{-D}$ are not p-th powers and do not differ by a p-th power in K^*, i.e.

$$K^{*p} \neq \left(\tilde{b} + \sqrt{-D}\right)^k \cdot K^{*p} \neq \left(\tilde{b}^2 + \tilde{c}\sqrt{-D}\right)^l \cdot K^{*p} \neq K^{*p} \quad \text{for all } k, l \in \{1, \ldots, p-1\}.$$

In his article [Sol92], Solderitsch states the following corollary for finding examples to which the theorem is applicable. Again, he formulated the result under the condition $p \geqslant 5$, but the result, with the same proof as given in his article, also holds for $p = 3$.

Corollary 5.2. *Let $p \geqslant 3$ be a prime. The class groups of*

$$K = \mathbb{Q}(\sqrt{x^{2p} - 6x^p + 1})$$

contain a subgroup isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ *whenever* $x = \frac{s}{t} \in \mathbb{Q}$ *satisfies* $3 - \sqrt{8} < x^p < 3 + \sqrt{8}$,$s, t \in \mathbb{Z}$ *both odd, and* $1 < (st)^{p-1} < |\Delta_K|/4$.

We now give an explicit example for $p = 3$: Choose $s = 7$ and $t = 9$, then $x = \frac{s}{t}$ satisfies $3 - \sqrt{8} < x < 3 + \sqrt{8}$ and the integers s and t are both odd. Following Solderitsch, we find that the discriminant of $K := \mathbb{Q}(\sqrt{x^{2p} - 6x^p + 1})$ is given by $\Delta_K = -4D = t^{2p} - 6t^p s^p + s^{2p} = 7^6 - 6 \cdot 7^3 \cdot 9^3 + 9^6 = -851192 = -4 \cdot 2 \cdot 103 \cdot 1033$ and $1 < (st)^{p-1} = 63^2 < |\Delta_K|/4$.
Therefore $\tilde{a} = st = 63$, $\tilde{b} = (t^p - s^p)/2 = 193$, $\tilde{c} = \sqrt{\tilde{a}^p + \tilde{b}^2} = 536$ and $D = 2 \cdot 103 \cdot 1033 = 212798$ satisfy the conditions of theorem 5.1 and the class group Cl_K of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-212798})$ contains a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, generated by the ideal classes of $I = (63, 193 + \sqrt{-D})$ and $J = (63^2, 193^2 + 536\sqrt{-D})$.
Indeed, in this example $Cl_K \cong \mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. The class of the integral ideal $I_1 := (117, 5591 + 122\sqrt{-D})$ has order 72 in Cl_K, and $I_2 := (423, 178673 + 178928\sqrt{-D})$ yields a class of order 6 generating a subgroup of Cl whose only intersection with the group generated by $[I_1]$ is the trivial class. We have $[I] = 24 \cdot [I_1]$ and $[J] = 2 \cdot [I_2]$.

5.2. **Craig, Yamamoto.**

In his paper [Cra73], M. Craig proves the existence of infinitely many imaginary quadratic fields with a class group containing a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and the existence of infinitely many real quadratic fields with a class group containing a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. He proves this using the following three propositions. For the first two he refers to Y. Yamamoto [Yam70].

Proposition 5.3. *Let* $D > 4$ *be a square-free integer and* $K = \mathbb{Q}(\sqrt{-D})$.
Suppose m *is an odd prime, and* $a, b, c \in \mathbb{Z}$ *satisfy* $4a^m = b^2 + c^2 D$ *and* $\gcd(a, b) = 1$.
If a rational prime $p|a$ *exists such that* b *is not an* m*-th power* mod p*, then the ideal* $\mathfrak{a} = \left(a, \frac{b+c\sqrt{-D}}{2}\right)$ *belongs to a class of order* m.

Proposition 5.4. *Let* $D > 4$ *be a square-free integer and* $K = \mathbb{Q}(\sqrt{-D})$.
Suppose m *is an odd prime, and* $a_1, b_1, a_2, b_2, c \in \mathbb{Z}$ *satisfy* $b_1^2 - 4a_1^m = -c^2 D = b_2^2 - 4a_2^m$ *and* $\gcd(a_1, b_1) = gcd(a_2, b_2) = 1$.
If rational primes $p_1|a_1$, $p_2|a_2$ *exist such that* $b_1 \not\equiv m$*-th power* mod p_1 *and* $b_2 \not\equiv m$*-th power* mod p_2*, and in addition* $\frac{b_1+b_2}{2} \equiv$ *some non-zero* m*-th power* mod p_2*, then the ideal classes of* $\mathfrak{a}_1 = \left(a_1, \frac{b_1+c\sqrt{-D}}{2}\right)$ *and* $\mathfrak{a}_2 = \left(a_2, \frac{b_2+c\sqrt{-D}}{2}\right)$ *are of order* m *in* Cl_K*, and independent.*

Craig extends Proposition 5.4 to Proposition 5.5; in fact in the same way it can be extended to any number n of (a_i, b_i) generating a subgroup of Cl_K isomorphic to $(\mathbb{Z}/m\mathbb{Z})^n$:

Proposition 5.5. *Let* $D > 4$ *be a square-free integer and* $K = \mathbb{Q}(\sqrt{-D})$.
Suppose m *is an odd prime, and* $a_1, b_1, a_2, b_2, a_3, b_3, c \in \mathbb{Z}$ *satisfy* $b_1^2 - 4a_1^m = b_2^2 - 4a_2^m = b_3^2 - 4a_3^m = -c^2 D$ *and* $\gcd(a_1, b_1) = gcd(a_2, b_2) = gcd(a_3, b_3) = 1$.
If rational primes $p_1|a_1$, $p_2|a_2$, $p_3|a_3$ *exist such that* $b_i \not\equiv m$*-th power* mod p_i*, and in addition*

$$\begin{aligned} \frac{b_1 + b_2}{2} &\equiv \textit{ some non-zero } m\textit{-th power } \mod p_2, \\ \frac{b_1 + b_3}{2} &\equiv \textit{ some non-zero } m\textit{-th power } \mod p_3, \quad \textit{and} \\ \frac{b_2 + b_3}{2} &\equiv \textit{ some non-zero } m\textit{-th power } \mod p_3, \end{aligned}$$

then the ideal classes of $\mathfrak{a}_i = \left(a_i, \frac{b_i+c\sqrt{-D}}{2}\right)$ *generate a subgroup of* Cl_K *isomorphic to* $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

We will now use the theory of §3.4 and §4.4 to interpret these propositions, and to present a simpler and more abstract proof compared to the original ones.

Suppose D, m, a, b, c, p satisfy the conditions described in the statement of Proposition 5.3. Then $p|(b^2 + c^2 D)$. Because $\gcd(a, b) = 1$, this implies $-c^2 D \equiv b^2 \not\equiv 0 \mod p$. Therefore $X^2 + D$ has solutions in $\mathbb{Q}_p$, given by $\pm\frac{b}{c} + \ldots \cdot p$, and we obtain homomorphisms $h_\pm : K^*/K^{*m} \to \mathbb{Q}_p^*/\mathbb{Q}_p^{*m}$.

Because b is not an m-th power mod p and m is prime, we have $p \neq m$ and $\mathbb{Z}_p^*/\mathbb{Z}_p^{*m} \cong \mathbb{F}_p^*/\mathbb{F}_p^{*m} \cong \mathbb{Z}/m\mathbb{Z}$ hence it is possible to choose homomorphisms $\tilde{\varphi_p} : \ker(v) \to \mathbb{Z}/m\mathbb{Z}$ as in §3.4.
Note that $\left(a_i, \frac{b_i+c\sqrt{-D}}{2}\right)^m = \left(\frac{b_i+c\sqrt{-D}}{2}\right)$ as described in §4.3.
The condition "b is not an m-th power mod p" in Proposition 5.3 is the same as saying that $\tilde{\varphi_p}\left(\frac{b+c\sqrt{-D}}{2}\right) = i \circ \varphi_p\left(\frac{b+c(\frac{b}{c}+\ldots\cdot p)}{2}\right) = i(b \bmod p)$ is nonzero in $\mathbb{Z}/m\mathbb{Z}$.
Analogous, the conditions $\frac{b_i+b_j}{2} \equiv$ some non-zero m-th power mod p_j in Propositions 5.4 and 5.5 correspond to
$\tilde{\varphi_{p_j}}\left(\frac{b_i+c\sqrt{-D}}{2}\right) = i \circ \varphi_{p_j}\left(\frac{b_i+c(\frac{b_j}{c}+\ldots\cdot p_j)}{2}\right) = i(\frac{b_i+b_j}{2} \bmod p)$ is zero in $\mathbb{Z}/m\mathbb{Z}$.
Using $(\tilde{\varphi}_{p_1}, \tilde{\varphi}_{p_2}, \tilde{\varphi}_{p_2}) : \ker(v) \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ this shows that the image of $\frac{b_1+c\sqrt{-D}}{2}$ is $(\neq 0, 0, 0)$ and the image of $\frac{b_2+c\sqrt{-D}}{2}$ has the shape $(*, \neq 0, 0)$ and the image of $\frac{b_3+c\sqrt{-D}}{2}$ is of the form $(*, *, \neq 0)$. This proves the three propositions above. □

6. From rational points on certain elliptic curves to $Cl_K[3]$

6.1. **Van Beek: $E_{A,B}(\mathbb{Q}) \longrightarrow \mathbb{Q}(\sqrt{A})^*/\mathbb{Q}(\sqrt{A})^{*3}$.** The master's thesis of Monique van Beek [Bee10] contains an elementary and explicit proof of a relation between the group of rational points on a certain type of elliptic curves, and groups K^*/K^{*3} as discussed in the present text. We briefly recall this result.

Consider the polynomial $f(x) = x^3 + A(x-B)^2$ over $\mathbb{Q}$. Suppose $A, B \in \mathbb{Q}^*$ satisfy $4A+27B \neq 0$. Then $\Delta_{f(x)} = -A^2B^3(4A+27B) \neq 0$, and

$$E_{A,B} \quad : \quad y^2 = x^3 + A(x-B)^2$$

defines an elliptic curve over $\mathbb{Q}$. The points on $E_{A,B}$ with coordinates in $\mathbb{Q}$ together with the point at infinity P_∞ yield the abelian group denoted $E_{A,B}(\mathbb{Q})$. Write $\mathbb{Q}(\sqrt{A})$ for the extension of $\mathbb{Q}$ obtained by adjoining the zeros of the polynomial $X^2 - A$ to $\mathbb{Q}$. This is a quadratic extension of $\mathbb{Q}$ in case A is not a square, and it is the field of rational numbers otherwise. Because we are interested in quadratic fields, let A be non-square. Note that we can rewrite the equation for $E_{A,B}$ as $E_{A,B} : x^3 = \left(y + (x-B)\sqrt{A}\right)\left(y - (x-B)\sqrt{A}\right)$.

The result we recall from [Bee10] is that

$$\alpha \quad : \quad E_{A,B}(\mathbb{Q}) \longrightarrow \mathbb{Q}(\sqrt{A})^*/\mathbb{Q}(\sqrt{A})^{*3}$$

given by

$$\alpha(P) = \begin{cases} (y + (x-B)\sqrt{A}) \cdot \mathbb{Q}(\sqrt{A})^{*3} & \text{if } P = (x,y) \text{ a point on } E_{A,B} \text{ with rational coordinates} \\ 1 \cdot \mathbb{Q}(\sqrt{A})^{*3} & \text{if } P = P_\infty \end{cases}$$

defines a homomorphism of groups.
From this result it follows directly that for all rational points P on the curve, $3P$ is in the kernel of α, and therefore all rational points P of order $i \in \mathbb{Z}$ with $\gcd(3, i) = 1$ are in $\ker(\alpha)$.

Let (x, y) be a rational point on $E_{A,B}$, then we can write $(x, y) = (\frac{m}{\tilde{m}}, \frac{n}{\tilde{n}})$ with $m, \tilde{m}, n, \tilde{n} \in \mathbb{Z}$ and $\gcd(m, \tilde{m}) = \gcd(n, \tilde{n}) = 1$. Because (x, y) is a point on E we obtain $\frac{n^2}{\tilde{n}^2} = \frac{m^3 + A\tilde{m}\left(m^2 - 2mB\tilde{m} + B^2\tilde{m}^2\right)}{\tilde{m}^3}$.
If A and B are integral, then it follows that $\tilde{n}^2 = \tilde{m}^3$ which has to be equal to e^6 for some $e \in \mathbb{Z}$.
So $(x, y) = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$, and we can multiply with e^6 to get $n^2 = m^3 + Ae^2\left(m^2 - 2mBe^2 + B^2e^4\right)$ which can be written as

$$m^3 = \left(n + (me - Be^3)\sqrt{A}\right)\left(n - (me - Be^3)\sqrt{A}\right), \text{ with } m, n \in \mathbb{Z}.$$

So we have:

$$\begin{aligned} \alpha(x,y) = \left(y + (x-B)\sqrt{A}\right) \cdot \mathbb{Q}(\sqrt{A})^{*3} &= \left(\tfrac{n}{e^3} + \left(\tfrac{m}{e^2} - B\right)\sqrt{A}\right) \cdot e^3 \cdot \mathbb{Q}(\sqrt{A})^{*3} \\ = \left(n + \left(m - e^2B\right)\sqrt{Ae^2}\right) \cdot \mathbb{Q}(\sqrt{A})^{*3}, & \end{aligned}$$

which can be seen as α applied to the integral point (m, n) on the elliptic curve

$$E_{Ae^2, Be^2} : m^3 = n^2 - Ae^2(m - Be^2)^2.$$

6.2. **From Van Beek's elliptic curves to the norm equation of §4.2.**

We now compare the equation in m, n, e derived in the previous section:

$$m^3 \quad = \quad n^2 - Ae^2(m - Be^2)^2$$

with the cubic norm equation of §4.2:

$$4a^3 \quad = \quad b^2 + c^2 D.$$

If we take $D = -A$, $a = m$, $b = 2n$ and $c = 2(me - Be^3)$, then we see that each solution in integers to the first equation (with parameters A, B) yields a solution to the second one (with parameter $D = -A$). In other words, a rational point $(x, y) = (\frac{m}{e^2}, \frac{n}{e^3})$ on the elliptic curve $E_{A,B}$ gives us a solution to the cubic norm equation of §4.2.
Note that in this case α maps (x, y) to $\frac{b+c\sqrt{-D}}{2} \cdot K^{*3}$, where $K = \mathbb{Q}(\sqrt{-D})$.
We saw in Theorem 4.2 that an integral solution to the equation $4a^3 = b^2 + c^2 D$ with $D > 3$ square-free, $b \geq 0$, $c \geq 0$ if $b = 0$, $\gcd(a, b)$ square-free, and the primes dividing $\gcd(a, b)$ ramifying in $\mathcal{O}_K$ gives us an $\mathcal{O}_K$-ideal $\mathfrak{a} = \left(a, \frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right)$ such that its cube is principal: $\mathfrak{a}^3 = \left(\frac{b+c\sqrt{-D}}{2}\right)$. So to get such an ideal, we want to find rational points $(m/e^2, n/e^3)$ on an elliptic curve $E = E_{A,B}$ for integers A, B such that

$$\begin{aligned} A = -D \text{ is square-free} \quad & (D > 3); \\ m(= a) \in \mathbb{Z}; & \\ n \in \mathbb{Z} \quad & (n \geq 0); \\ 2(me - Be^3) = c \in \mathbb{Z} \quad & (c \geq 0 \text{ if } n = 0); \\ \gcd(m, 2n) \text{ square-free, and the primes dividing it ramifying in } \mathcal{O}_K. & \end{aligned}$$

Example. Choose $A = -23$ and $B = 2$, and consider the elliptic curve $E_{A,B} : y^2 = x^3 - 23(x-2)^2$. A rational point on this curve is given by $(x, y) = (m/e^2, n/e^3) = (3, 2)$ with $m, n \in \mathbb{Z}$ and $e = 1$. This curve and point satisfy the conditions given above, so $\mathfrak{a} = \left(a, \frac{b+c\sqrt{-D}}{2\gcd(a,b)}\right) = \left(3, \frac{4+2\sqrt{-23}}{2}\right)$ is an ideal which cube is principal: $\mathfrak{a}^3 = \left(\frac{b+c\sqrt{-D}}{2}\right) = \left(\frac{4+2\sqrt{-23}}{2}\right)$. In fact, $[\mathfrak{a}]$ is of order 3 in the class group of $\mathbb{Q}(\sqrt{-23})$.

Example. Choose $A = -974$ and $B = 14$, and consider the elliptic curve $E_{A,B} : y^2 = x^3 - 974(x - 14)^2$.
Using MAGMA, we find that a set of generators of the Mordell-Weil group of $E_{A,B}$ (the group of rational points on $E_{A,B}$) is given by $P_1 = (x_1, y_1) = (30591, 5264665)$ and $P_2 = (x_2, y_2) = (15, 49)$. Writing $(x_i, y_i) = (m_i/{e_i}^2, n_i/{e_i}^3)$ with $m_i, n_i \in \mathbb{Z}$ and $\gcd(m_i, e_i) = \gcd(n_i, e_i) = 1$, we find: $(m_1, n_1) = (30591, 5264665)$, $e_1 = 1$, and $(m_2, n_2) = (15, 49)$, $e_2 = 1$.
Note that $\gcd(m_i, 2n_i) = 1$, and $D = -A = 974$ is square-free, so this curve and these points satisfy the conditions given above. Therefore these two points give rise to two ideals in the ring of integers of $K = \mathbb{Q}\sqrt{-D}$ of which the cubes are principal:
$\mathfrak{a}_1 = \left(30591, 5264665 + (30591 - 14)\sqrt{-974}\right) = \left(30591, 5264665 + 30577\sqrt{-974}\right)$,
$\mathfrak{a}_1^3 = \left(5264665 + 30577\sqrt{-974}\right)$,
$\mathfrak{a}_2 = \left(15, 49 + (15 - 14)\sqrt{-974}\right) = \left(15, 49 + \sqrt{-6226}\right)$,
$\mathfrak{a}_2^3 = \left(49 + \sqrt{-974}\right)$.
Using MAGMA, we find that the class group Cl_K is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, and for a certain isomorphism $f : Cl_K \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ we have $f([\mathfrak{a}_1]) = (2, 8)$ and $f([\mathfrak{a}_2]) = (2, 0)$.
So the ideals corresponding to the rational points on $E_{A,B}$ generate a subgroup of Cl_K, isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Example. Choose $A = -6226$ and $B = 1$, and consider the elliptic curve $E_{A,B} : y^2 = x^3 - 6226(x - 1)^2$.
Using MAGMA, we find that a set of generators of the Mordell-Weil group of $E_{A,B}$ (the group of rational points on $E_{A,B}$) is given by $P_1 = (x_1, y_1) = (116689, 38782745)$, $P_2 = (x_2, y_2) = (23906969/1369, 93770651453/50653)$, and $P_3 = (x_3, y_3) = (647881/640000, 156401029/512000000)$. Writing $(x_i, y_i) = (m_i/{e_i}^2, n_i/{e_i}^3)$ with $m_i, n_i \in \mathbb{Z}$ and $\gcd(m_i, e_i) = \gcd(n_i, e_i) = 1$, we find: $(m_1, n_1) = (116689, 38782745)$, $e_1 = 1$, $(m_2, n_2) = (23906969, 93770651453)$, $e_2 = 37$, and $(m_3, n_3) = (647881, 156401029)$, $e_3 = 800$.

Note that $\gcd(m_i, 2n_i) = 1$, and $D = -A = 6226$ is square-free, so this curve and these points satisfy the conditions given above. Therefore these three points give rise to three ideals in the ring of integers of $K = \mathbb{Q}\sqrt{-D}$ of which the cubes are principal:
$\mathfrak{a}_1 = \big(116689, 38782745 + (116689 - 1)\sqrt{-6226}\big) = \big(116689, 38782745 + 116688\sqrt{-6226}\big)$,
$\mathfrak{a}_1^3 = \big(38782745 + 116688\sqrt{-6226}\big)$,
$\mathfrak{a}_2 = \big(23906969, 93770651453 + (23906969 \cdot 37 - 37^3)\sqrt{-6226}\big)$,
$\mathfrak{a}_2^3 = \big(93770651453 + 884507200\sqrt{-6226}\big)$,
$\mathfrak{a}_3 = \big(647881, 156401029 + (647881 \cdot 800 - 800^3)\sqrt{-6226}\big)$,
$\mathfrak{a}_3^3 = \big(156401029 + 6304800\sqrt{-6226}\big)$.
Using MAGMA, we find that the class group Cl_K is isomorphic to $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, and for a certain isomorphism $f : Cl_K \mapsto \mathbb{Z}/12\mathbb{Z}$, we find:
$f([\mathfrak{a}_1]) = (4, 4)$,
$f([\mathfrak{a}_2]) = (0, 8)$,
$f([\mathfrak{a}_3]) = (0, 4)$.
So the ideals corresponding to the rational points on $E_{A,B}$ generate a subgroup of Cl_K, isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. We see that in this example $2[\mathfrak{a}_3] = [\mathfrak{a}_2]$, although these classes come from the independent points $P_2,\ P_3 \in E_{A,B}(\mathbb{Q})$.

7. Conclusions and outlook

Throughout this section, let K be an algebraic number field with discriminant Δ_K, ring of integers $\mathcal{O}_K$, and class group Cl_K.

The main part of this thesis consists of deriving an isomorphism between some subgroup of K^*/K^{*m} and $Cl_K[m]$: the elements of order dividing m in the Cl_K, and of interpreting various results about elements of specific order in Cl_K in terms of this isomorphism.
First, besides this, recalling some basic results from algebraic number theory, we proved that for imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-D})$ with $D > 3$ every ideal class of order $\neq 2$ contains a unique ideal of minimal norm, which is less than $\sqrt{|\Delta_K|/3}$ - a useful statement which remarkably seems to be (relatively?) unknown.

We constructed a surjection g from the subgroup $\ker(v) \subset K^*/K^{*3}$ which consists of all elements with valuation 0 mod 3 at all primes, to $Cl_K[3]$, with $\ker(g) = \mathcal{O}_K^*/{\mathcal{O}_K^*}^3$.
Generalisation of this result to all natural numbers m yielded the exact sequence

$$1 \to \mathcal{O}_K^*/{\mathcal{O}_K^*}^m \to \ker(v) \to Cl_K[m] \to 0.$$

For imaginary quadratic fields with discriminant < -4 and general $m \geqslant 3$, this reduces to an isomorphism $\ker(v) \cong Cl_K[m]$, providing a way to describe $Cl_K[m]$ in terms of K^*/K^{*m}.
Furthermore, using homomorphisms from K^*/K^{*3} to p-adic groups $\mathbb{Q}_p^*/\mathbb{Q}_p^{*m}$, we constructed homomorphisms on $\ker(v)$, which in the case $m = 3$ end up in groups isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Combinations of those homomorphisms for various primes p can be used to determine if elements of $\ker(v)$ yield independent elements in $Cl_K[m]$. In this way, considering elements of $\ker(v) \subset K^*/K^{*m}$ can yield lower bounds of the p-rank of Cl_K (for primes p dividing m).
We haven't done these last steps for $m \neq 3$, but it seems reasonable to assume that the same technique will work to show independence.
A more difficult question which we left open is whether this method is always sufficient to show independence of elements and whether we can say anything about how many primes are needed.

Having constructed - for imaginary quadratic fields - an isomorphism between $\ker(v) \subset K^*/K^{*3}$ and $Cl_K[m]$ and a way to see if elements in $\ker(v)$ yield independent elements in Cl_K, we used this to interpret various results described or used by Buell [Bue76], Shanks and Serafin [SS73], Solderitsch [Sol92], Craig [Cra73] and Yamamoto [Yam70].

Buell [Bue76] and Shanks and Serafin [SS73] make use of a correspondence between solutions to a cubic norm equation and ideals of classes of order dividing three. Their description of this correspondence is not entirely satisfying. We have proved a precise and correct version of this statement. Next, we generalised it to a correspondence between solutions of the norm equation $4a^m = b^2 + c^2D$ (satisfying some extra conditions) and specific ideals in classes in $Cl_K[m]$, for general odd $m \geqslant 3$.
It was shown that this correspondence could be considered as the same as the isomorphism described above, but now on elements representing the elements of $\ker(v)$ and ideals representing the ideal classes in $Cl_K[m]$. Therefore, the method to prove independence of elements of $Cl_K[m]$ could be applied in this case to prove that solutions of the norm equation yield ideals in independent classes.
We don't discuss the case where m is even. Of course it is possible to simply ignore the even part of m, but it would be interesting to investigate what happens at the even part of m, as the isomorphism also exists for even m.

Solderitsch [Sol92] describes a way to find imaginary quadratic fields where the class groups have p-rank at least two. We showed that this result can be interpreted and proved in terms of the isomorphism and the way to prove independency of elements in Cl_K described above, providing a more general understanding of Solderitschs method.
Likewise, the theory used by Craig [Cra73] and Yamamoto [Yam70] to find imaginary quadratic fields where the class group has 3-rank 2, 3 or 4 can be understood directly as a special case of the isomorphism and the way to prove independency of elements in Cl_K described above.

We now have discussed the relation between norm equations an and $Cl_k[m]$, but this thesis lacks the actual finding of class groups where the p-rank of the class group is high, or analogue, finding appropriate norm equations with many solutions yieling independent elements in $Cl_K[p]$.
The articles by Buell [Bue76], Shanks and Serafin [SS73], Solderitsch [Sol92], Craigh [Cra73], Yamamoto [Yam70] and others show that it is certainly possible to find methods for explicitely constructing or finding such equations and solutions. Discussing also this part of their articles in light of the general isomorphism discussed in this thesis would be interesting. Possibly this in combination with the independence-showing of §3.4 can be used to easily find better or more general methods of finding actual examples of norm equations (and their corresponding imaginary quadratic fields) with many solutions yielding independent elements of specific order in the class group, and hence to find imaginary quadratic fields where the class group has higher p-rank.

In the end, we showed that also the relation between rational points on certain elliptic curves $E_{A,B}(\mathbb{Q})$ and elements of the group $\mathbb{Q}(\sqrt{A})^*/\mathbb{Q}(\sqrt{A})^{*3}$ as occurs in the master's thesis of Van Beek [Bee10] can be interpreted as a special case of the correspondence between solutions of cubic norm equations and ideals in classes of order dividing 3 discussed above (assigning quadratic fields to such curves). Hence the rational points on such a curve could yield independent elements of order dividing 3 in the class group corresponding to the curve, as is shown in an example.
It would be interesting to investigate if it is possible to extend this relation to for example a bijection between elliptic curves of a certain type and quadratic fields, and if we can make use also in this case of the p-adic techniques used to show whether elements in Cl_K were independent.

References

[Bee10] Monique van Beek. On elliptic curves of the form $y^2 = x^3 + a(x-b)^2$. Master's thesis, Rijksuniversiteit Groningen, 2010.
[Bel04] Karim Belabas. On quadratic fields with large 3-rank. *Mathematics of Computation*, 73:2061–2074, 2004.
[Bue76] Duncan A. Buell. Class groups of quadratic fields. *Mathematics of Computation*, 30(135):610–623, July 1976.
[Cra73] Maurice Craig. A type of class group for imaginary quadratic fields. *Acta Arithmetica*, 22(4):449–459, 1973.
[DyD74] Francisco Diaz y Diaz. Sur les corps quadratiques imaginaires dont le 3-rang du groupe des classes est supérieur à 1. *Séminaire Delange-Pisot-Poitout*, 15(2):G15–01–G15–10, 1974.
[Kob77] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Number 58 in Graduate texts in mathamatics. Springer-Verlag, New York Inc., 1977.
[Sol92] James Joseph Solderitsch. Quadratic fields with special class groups. *Mathematics of Computation*, 59(200):633–638, 1992.
[SS73] Daniel Shanks and Richard Serafin. Quadratic fields with four invariants divisible by 3. *Mathematics of Computation*, 27(121):183–187, 1973.
[Ste17] Peter Stevenhagen. Number rings, 2017.
[Yam70] Yoshihiko Yamamoto. On unramified galois extensions of quadratic number fields. *Osaka J. Math.*, 7:57–76, 1970.

8. Appendix: Tables

Here is a list of all imaginary quadratic fields $\mathbb{Q}(\sqrt{-D})$ for positive, square-free $D \leq 10000$ and (at least) two independent elements of order 3 in the class group:

$D = 974$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$
$D = 2437$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
$D = 3299$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$
$D = 3886$	$Cl_K = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
$D = 4027$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
$D = 5069$	$Cl_K = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$
$D = 5142$	$Cl_K = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
$D = 5306$	$Cl_K = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$
$D = 5417$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$
$D = 5703$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$
$D = 5857$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$
$D = 6085$	$Cl_K = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
$D = 6221$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/42\mathbb{Z}$
$D = 6226$	$Cl_K = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$
$D = 6583$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$
$D = 6690$	$Cl_K = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
$D = 6789$	$Cl_K = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
$D = 6910$	$Cl_K = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
$D = 6914$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$
$D = 7977$	$Cl_K = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
$D = 8242$	$Cl_K = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
$D = 8522$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$
$D = 8751$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$
$D = 9069$	$Cl_K = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$
$D = 9385$	$Cl_K = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$
$D = 9497$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$
$D = 9574$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$
$D = 9934$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$

K. Belabas produced a list of all imaginary quadratic fields with $|\Delta_K| < 10^{10}$ and (at least) four independent elements of order 3 in the class group [Bel04]. Here we recall his list and add for each of those fields the structure of the class group:

$D = 653329427$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/210\mathbb{Z}$
$D = 1876623871$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/1239\mathbb{Z}$
$4D = 2520963512$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/276\mathbb{Z}$
$D = 2676277123$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/240\mathbb{Z}$
$4D = 3146813128$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/324\mathbb{Z}$
$D = 3972542271$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2826\mathbb{Z}$
$D = 4724490703$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/795\mathbb{Z}$
$D = 5252241199$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/360\mathbb{Z}$
$D = 5288116947$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/378\mathbb{Z}$
$D = 5866841451$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/252\mathbb{Z}$
$D = 6127792087$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/588\mathbb{Z}$
$4D = 6223830596$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/1500\mathbb{Z}$
$D = 6903777631$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/1767\mathbb{Z}$
$4D = 6905985272$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/1320\mathbb{Z}$
$4D = 7189850292$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/204\mathbb{Z}$
$4D = 7309564084$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/786\mathbb{Z}$
$D = 7311232679$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2994\mathbb{Z}$
$D = 7592829611$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/1422\mathbb{Z}$
$D = 7993105123$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/486\mathbb{Z}$
$D = 8308370723$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/738\mathbb{Z}$
$D = 8417780779$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/546\mathbb{Z}$
$D = 8418280523$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/450\mathbb{Z}$
$D = 8624990111$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4224\mathbb{Z}$
$D = 9552870967$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/1977\mathbb{Z}$
$D = 9775810067$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/1074\mathbb{Z}$
$D = 9906365947$	$Cl_K = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/516\mathbb{Z}$

According to the same paper [Bel04] by Belabas, the smallest imaginary quadratic field with at least five independent elements of order 3 in the class group has discriminant -5393946914743. In fact $K = \mathbb{Q}(\sqrt{-5393946914743})$ yields $Cl_K \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/11436\mathbb{Z}$.