

INTEGRAL TRACE FORMS ASSOCIATED TO CUBIC EXTENSIONS

GUILLERMO MANTILLA-SOLER

ABSTRACT. Given a nonzero integer d , we know by Hermite's Theorem that there exist only finitely many cubic number fields of discriminant d . However, it can happen that two non-isomorphic cubic fields have the same discriminant. It is thus natural to ask whether there are natural refinements of the discriminant which completely determine the isomorphism class of the cubic field. Here we consider the trace form $q_K : \text{Tr}_{K/\mathbb{Q}}(x^2)|_{\mathcal{O}_K^{\circ}}$ as such a refinement. For a cubic field of fundamental discriminant d we show the existence of an element T_K in Bhargava's class group $Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; -3d)$ such that q_K is completely determined by T_K . By using one of Bhargava's composition laws, we show that q_K is a complete invariant whenever K is totally real and of fundamental discriminant.

CONTENTS

1. Introduction	1
2. Basic facts	4
3. Galois fields and rational 3-torsion	5
4. Cubic fields with fundamental discriminant	8
5. Trace form and class groups	10
6. From cubic fields to cubes and trace forms	14
Acknowledgements	18
References	18

1. INTRODUCTION

1.1. **Generalities.** A difference between quadratic and non-quadratic number fields is that in the former case, the fields are totally characterized by their discriminant. One natural choice for a "refined discriminant" is given by the isometry class with respect to the trace form of the lattice defined by the maximal order. The purpose of this paper is to give a detailed analysis of this refinement for cubic extensions, and to show under which conditions this refinement characterizes the field. Given a number field K with maximal order \mathcal{O}_K we consider the trace form $\text{Tr}_{K/\mathbb{Q}}(x^2)|_{\mathcal{O}_K}$. A natural question is:

Question 1.1. *Do there exist two non-isomorphic number fields K and L such that their corresponding trace forms are isomorphic?*

In this paper we analyze Question 1.1 in the case of cubic extensions.

Definition 1.2. *Let K be a number field and let O_K be its maximal order. The trace zero module O_K^0 is the set $\{x \in O_K : \text{tr}_{K/\mathbb{Q}}(x) = 0\}$.*

Our main result is the following:

Theorem A (Theorem 6.5 below). *Let K be a cubic number field of positive, fundamental discriminant. Let L be a number field such that there exists an isomorphism of quadratic modules*

$$\langle O_K^0, \text{Tr}_{K/\mathbb{Q}}(x^2)|_{O_K^0} \rangle \cong \langle O_L^0, \text{Tr}_{K/\mathbb{Q}}(x^2)|_{O_L^0} \rangle,$$

and assume $9 \nmid d_L$. Then $K \cong L$.

1.2. Outline of the paper. We start by analyzing Question 1.1 for general cubic fields. For this purpose we consider first the case in which the common discriminant of K and L is not fundamental.¹

1.2.1. Non-fundamental discriminants. In this case, we find that our proposed refinement does not characterize the field. In other words, for non-fundamental discriminants we have an affirmative answer to Question 1.1. We divide the class of non-fundamental discriminants into 2 groups according to sign. Among the positive discriminants, we divide them again into groups according to those that are perfect squares, and those that are not. For each one of these cases we show that there are some non-fundamental discriminants such that 1.1 has an affirmative answer.

- i) (Negative non-fundamental discriminants) We define a sequence of positive integers Σ and a family of triples $\{K_m, L_m, E_m\}_{m \in \Sigma}$, with the following properties (see Lemma 3.4):
 - K_m, L_m are two non-isomorphic cubic fields with discriminant $-3n^2$, where n is a positive integer depending only on m .
 - An elliptic curve E_m defined over \mathbb{Q} such that $E_m[3](\mathbb{Q})$ determines completely a ternary quadratic form equivalent to both $\text{Tr}_{K/\mathbb{Q}}(x^2)|_{O_{K_m}}$ and $\text{Tr}_{K/\mathbb{Q}}(x^2)|_{O_{L_m}}$.
- ii) (Square discriminants) In this case we prove (see Theorem 3.1) a generalization of a result of Conner and Perlis ([C-P], Theorem IV.1.1 with $p = 3$). Let K and L be two Galois cubic number fields of the same discriminant and let M be either O_K or O_K^0 . Then $\text{Tr}_{K/\mathbb{Q}}(x^2)|_M$ and $\text{Tr}_{L/\mathbb{Q}}(x^2)|_M$ are equivalent. Since there are examples of non-isomorphic Galois cubic fields of the same discriminant, Question 1.1 has a positive answer for such cases.
- iii) (Positive, non-fundamental, non-square discriminants) See example 3.6 for two fields with positive, non-square free, non perfect square discriminant and isometric integral trace forms.

¹ d is a fundamental discriminant if it is the discriminant of a quadratic field.

1.2.2. *Reduction to a rank 2 form.* For fields of fundamental discriminant, we see thanks to Lemma 2.5, that the binary quadratic form $\text{Tr}_{K/\mathbb{Q}}(x^2)|_{\mathcal{O}_K^0}$ is a refinement of the discriminant. Hence, we reformulate Question 1.1.

Question 1.3. *Do there exist two non-isomorphic cubic fields K and L such that the forms $\text{Tr}_{K/\mathbb{Q}}(x^2)|_{\mathcal{O}_K^0}$ and $\text{Tr}_{L/\mathbb{Q}}(x^2)|_{\mathcal{O}_L^0}$ are isomorphic?*

Although Question 1.3 has relevance for us only for fundamental discriminants, we note that the examples i), ii) and iii) described above also answer 1.3 in an affirmative way. On the other hand, for fundamental discriminants, (see Figure 1), class field theory provides examples of non isomorphic cubic fields of the same discriminant. Among the fields with negative discriminants we found examples giving an affirmative answer to Question 1.3.

1.2.3. *Main results.* It is clear thanks to the results developed so far, that one should consider working over cubic fields of fundamental discriminant. We show for such discriminants that the trace form is equal, as an element of a narrow class group, to the Hessian multiplied by an element that only depends on the discriminant.

Theorem B (Theorem 5.5 below) *Let K be a cubic field with discriminant d_K . Assume that d_K is fundamental and that $3 \nmid d_K$. Let $F_K = (a, b, c, d)$ be a cubic in the $GL_2(\mathbb{Z})$ -equivalence class defined by K . Then $\frac{1}{2}q_K * C_{d_K} = H_K^{\pm 1}$ as elements of $Cl_{\mathbb{Q}(\sqrt{-3d_K})}^+$, where $C_{d_K} = (3, 0, \frac{d_K}{4})$ or $C_{d_K} = (3, 3, \frac{d_K+3}{4})$ in accordance with whether $d_K \equiv 0 \pmod{4}$ or $d_K \equiv 1 \pmod{4}$.*

By reformulating all of this in the language of Bhargava's composition of cubes (see [Bha]), we show that the trace form arises naturally as a projection of a cube determined by the field.

Theorem C (Theorem 6.2 below) *Let K be a cubic field with discriminant d_K and associated cubic form $F_K = (a, b, c, d)$. Assume that d_K is fundamental and that 3 does not ramify. Then there exists $T_{F_K} \in Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; -3d_K)$ such that $(\pi_1 \circ \phi)(T_{F_K})^{\pm 1} = \frac{1}{2}q_K$ as elements of $Cl_{\mathbb{Q}(\sqrt{-3d_K})}^+$.*

In this setting, Theorem A follows from Theorem 5.11 which is the modern version of a theorem of Eisenstein (see[E]). By reformulating Theorem A, see Theorem 6.8 and its corollary, we obtain one inequality of the classical Scholz reflection principle(see [Sch]).

We remark that Theorem A can be obtained with the tools developed by Eisenstein in ([E]). However, we have decided to use Bhargava's theory of $2 \times 2 \times 2$ orbits of cubes, to suggest that it might be possible to use some other prehomogeneous spaces to "generalize " Theorem A to higher dimensions.

2. BASIC FACTS

Definition 2.1. Let G be a free abelian group. We say that a map

$$q : G \rightarrow \mathbb{Z}$$

is a quadratic form if :

- $q(nx) = n^2q(x)$ for all integer n ,
- The map $B_q : G \times G \rightarrow \frac{1}{2}\mathbb{Z}$ defined as $B_q(x, y) = \frac{1}{2}(q(x+y) - q(x) - q(y))$ is \mathbb{Z} -bilinear.

Remark 2.2. Let $\langle G, q \rangle$ be a quadratic \mathbb{Z} -module of rank $n = \text{Rank}(G)$. After choosing a basis, we can think of q as a homogeneous polynomial in n variables of degree two, i.e $q \in (\text{Sym}^2\mathbb{Z}^n)^*$. There is a natural action of $GL_2(\mathbb{Z})$ on $(\text{Sym}^2\mathbb{Z}^n)^*$. Under this action, q and q_1 belong to the same orbit if and only if $\langle G, q \rangle$ is isometric to $\langle G_1, q_1 \rangle$. Abusing notation we will denote this by $q \sim_{GL_2(\mathbb{Z})} q_1$.

Now let K be a number field and let O_K be its maximal order. The map

$$\begin{aligned} \tilde{q}_K : O_K &\rightarrow \mathbb{Z} \\ x &\mapsto \text{tr}_{K/\mathbb{Q}}(x^2) \end{aligned}$$

defines a quadratic form with corresponding bilinear form

$$B_K(x, y) = \text{tr}_{K/\mathbb{Q}}(xy)|_{O_K}.$$

Thus, we have that $\langle O_K, \tilde{q}_K \rangle$ is a quadratic \mathbb{Z} -module and its discriminant is precisely the discriminant of K . Thus, if K and L are two number fields such that $\langle O_K, \tilde{q}_K \rangle$ and $\langle O_L, \tilde{q}_L \rangle$ are isomorphic quadratic \mathbb{Z} -modules, then we have

- $[K : \mathbb{Q}] = [L : \mathbb{Q}]$,
- $\text{Disc}(K) = \text{Disc}(L)$.

Therefore the isomorphism class of $\langle O_K, \tilde{q}_K \rangle$ is to us a natural refinement of the discriminant.

Lemma 2.3. Let K be a number field of degree n and let $G_K = \mathbb{Z} + O_K^0$. We have

$$|O_K/G_K| = |\text{Tr}(O_K)/n\mathbb{Z}|.$$

Corollary 2.4. Let K and L be number fields. If

$$f : \langle O_K, B_K \rangle \rightarrow \langle O_L, B_L \rangle$$

is an isomorphism, then $\text{Disc}(G_K) = \text{Disc}(G_L)$.

Proof. Since $\text{tr}_L(f(x)f(y)) = \text{tr}_K(xy)$ for all $x, y \in O_K$ we have that $\text{tr}_K : O_K \rightarrow \mathbb{Z}$ implies $\text{tr}_L : O_L \rightarrow \mathbb{Z}$. Since f is an isometry, the argument is symmetric in K and L . By Lemma 2.3 we have $|O_K/G_K| = |O_L/G_L|$. Hence

$$\text{Disc}(G_K) = |O_K/G_K|^2 \text{Disc}(O_K) = |O_L/G_L|^2 \text{Disc}(O_L) = \text{Disc}(G_L).$$

□

For a number field K , we denote $q_k = \tilde{q}_K|_{O_K^0}$.

Lemma 2.5. *Let K, L be two number fields of degree n . Assume that K and L both have discriminants that are squarefree at all primes dividing n . Further, suppose that $\langle O_K^0, q_K \rangle$ and $\langle O_L^0, q_L \rangle$ are isomorphic. Then K and L have the same discriminant.*

Proof. Since $\text{Disc}(G_K) = \text{Disc}(G_L)$, we have that $|O_K/G_K|^2 \text{Disc}(O_K) = |O_L/G_L|^2 \text{Disc}(O_L)$. The result now follows from Lemma 2.3. \square

Proposition 2.6. *Let K be a Galois number field of prime degree p . Then p ramifies in K if and only if $\text{tr}_K(O_K) = p\mathbb{Z}$.*

Proof. It is clear that $\text{tr}_K(O_K) = p\mathbb{Z}$ implies that p -ramifies in K . Next, assuming that p ramifies, let P be the unique prime of O_K lying above p . By hypothesis we have that $|O_K/P| = p$. In particular P is a maximal \mathbb{Z} -submodule of O_K . Since $1 \notin P$, we must have that $O_K = \mathbb{Z} + P$. Since P is Galois invariant, $\text{tr}_K(P) \subseteq P \cap \mathbb{Z} = p\mathbb{Z}$. Thus $\text{tr}_K(O_K) = \text{tr}_K(\mathbb{Z} + P) \subseteq p\mathbb{Z}$. \square

3. GALOIS FIELDS AND RATIONAL 3-TORSION

In this section we explain some situations in which Questions 1.1 and 1.3 have positive answers. The examples in this section are characterized by having discriminants with a nontrivial square factor.

The following result is a generalization of a theorem of Conner and Perlis ([C-P], Theorem IV.1.1) for $p = 3$.

Theorem 3.1. *Let K and L be two Galois, cubic number fields of discriminant $D = d^2$. We have*

$$\langle O_K^0, q_K \rangle \cong \langle O_L^0, q_L \rangle \cong \begin{cases} 2d(x^2 + xy + y^2) & \text{if } 3 \nmid d \\ \frac{2d}{3}(x^2 + xy + y^2) & \text{otherwise.} \end{cases}$$

Moreover, there exists such an isometry that extends to one between $\langle O_K, \tilde{q}_K \rangle$ and $\langle O_L, \tilde{q}_L \rangle$.

Proof. Assume first that $3 \nmid D$. By Hilbert's 132 (see [Hi]) we have $O_K = e_1\mathbb{Z} \oplus e_2\mathbb{Z} \oplus e_3\mathbb{Z}$, where $\sigma(e_1) = e_2$, $\sigma(e_2) = e_3$, and σ is a generator of $\text{Gal}(K/\mathbb{Q})$. Since 3 does not ramify, Proposition 2.6 implies that $\text{tr}_{F/\mathbb{Q}}(e_1) = 1$, and furthermore, that $O_K^0 = (e_1 - e_2)\mathbb{Z} \oplus (e_1 - e_3)\mathbb{Z}$. Let $a = \text{tr}_{F/\mathbb{Q}}(e_1^2)$ and $b = \text{tr}_{F/\mathbb{Q}}(e_1e_2)$.

$$\text{Then } M = \begin{pmatrix} \frac{1+2a-2b}{3} & a-b & a-b \\ a-b & 2a-2b & a-b \\ a-b & a-b & 2a-2b \end{pmatrix} \text{ (respectively } M_0 = (a-b) \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \text{)}$$

represents the trace form over O_K in the basis $\{e_1, e_1 - e_2, e_1 - e_3\}$ (respectively the trace form over O_K^0 in the basis $\{e_1 - e_2, e_2 - e_3\}$). Note that $a + 2b = (\text{tr}_{F/\mathbb{Q}}(e_1))^2 = 1$, thus $D = \det(M) = (a-b)^2(a+2b) = (a-b)^2$. By the Cauchy-Schwartz inequality, $a - b > 0$, hence $d = a - b$, which implies that $a = \frac{1+2d}{3}$ and $b = \frac{1-d}{3}$. Thus, every cubic field of discriminant d^2 , $3 \nmid d$, has an integral basis for which the trace form over

O_K has representative matrix M (respectively trace form over O_K^0 has representative matrix M_0).

On the other hand, if $3 \mid d$, Proposition 2.6 and Lemma 2.3 imply that $O_K = \mathbb{Z} \oplus O_K^0$. Hence, \tilde{q}_K is totally determined by $q_K = \tilde{q}_K|_{O_K^0}$. Theorem 3.1 follows from the following claim and the observation after it.

Claim: $\frac{3}{2d}q_K$ is an integral, primitive, binary quadratic form of discriminant -3 .

Since $\mathbb{Q}(\sqrt{-3})$ has trivial class group, every integral quadratic form of discriminant -3 is $\text{SL}_2(\mathbb{Z})$ -equivalent to $(x^2 + xy + y^2)$. In particular, they are all $\text{GL}_2(\mathbb{Z})$ -equivalent. \square

Proof of claim: Let $\{\alpha, \beta\}$ an integral basis for O_K^0 . Let $O_\alpha \subseteq O_K^0$ be the \mathbb{Z} -module generated by $\{\alpha, \sigma(\alpha)\}$, where σ is a generator for $\text{Gal}(K/\mathbb{Q})$. Since $\alpha \notin \mathbb{Z}$, we know that α and $\sigma(\alpha)$ are distinct elements of O_K with the same norm. In particular, $\sigma(\alpha)$ cannot be a rational multiple of α , so $\text{Rank}_{\mathbb{Z}}(O) = 2$. Thus, $[O_K^0 : O_\alpha]$ is finite, and moreover $\sigma(\alpha) = m\alpha + [O_K^0 : O_\alpha]\beta$ for some integer m . Note that $(\text{tr}_K(\alpha^2), 2\text{tr}_K(\alpha\beta), \text{tr}_K(\beta^2))$ and $(\text{tr}_K(\alpha^2), 2\text{tr}_K(\alpha\sigma(\alpha)), \text{tr}_K(\sigma(\alpha)^2))$ represent q_K in the bases $\{\alpha, \beta\}$ and $\{\alpha, \sigma(\alpha)\}$ respectively. Hence

$$(3.1) \quad \text{tr}_K(\alpha^2)\text{tr}_K(\sigma(\alpha)^2) - \text{tr}_K^2(\alpha\sigma(\alpha)) = [O_K^0 : O_\alpha]^2(\text{tr}_K(\alpha^2)\text{tr}_K(\beta^2) - \text{tr}_K(\alpha\beta)).$$

Since $\text{disc}(K) = d^2$ and $O_K = \mathbb{Z} + O_K^0$, $\frac{d^2}{3} = \text{tr}_K(\alpha^2)\text{tr}_K(\beta^2) - \text{tr}_K(\alpha\beta)$. On the other hand since $\alpha \in O_K^0$, $\text{tr}_K(\alpha^2) = -2\text{tr}_K(\alpha\sigma(\alpha))$, and the left hand side of (3.1) is $3\text{tr}_K^2(\alpha\sigma(\alpha))$. Thus,

$$(3.2) \quad \text{tr}_K(\alpha\sigma(\alpha)) = \pm [O_K^0 : O_\alpha] \frac{d}{3}.$$

In particular we see that $\frac{d}{3}$ divides $\frac{1}{2}\text{tr}_K(\alpha^2)$. Exchanging the roles of α and β we see that $\frac{d}{3}$ also divides $\frac{1}{2}\text{tr}_K(\beta^2)$. Now consider $\sigma(\alpha) = m\alpha + [O_K^0 : O_\alpha]\beta$. Multiplying both sides by α and then taking traces we see that $\frac{d}{3}$ divides $\text{tr}_K(\alpha\beta)$. We conclude that $(\text{tr}_K(\alpha^2), 2\text{tr}_K(\alpha\beta), \text{tr}_K(\beta^2))$ can be written as $\frac{2d}{3}f$, with f an integral quadratic form of discriminant -3 . \square

Example 3.2. Let K and L be cubic fields defined by $x^3 + 6x^2 - 9x + 1$ and $2x^3 + 3x^2 - 9x + 2$ respectively. One sees that K and L are non-isomorphic fields of discriminant 3969 by direct computation, for instance $\text{regulator}(K) \neq \text{regulator}(L)$.

We conclude that the trace form does not characterize the field in the case that the discriminant is a square. Proposition 3.4 below is an indication that the case of square discriminant is not the only case that should be reconsidered. Namely; one should also consider the non-square free case. Cubic fields of a fixed discriminant Δ can be parametrized by a subset of rational points on a certain elliptic curve. Assume that $L = \mathbb{Q}(\beta)$ is a cubic field defined by the equation $x^3 + px + q \in \mathbb{Z}[x]$. If $O_L = \mathbb{Z}[\beta]$, then $\text{disc}(L) = -27q^2 - 4p^3$. Hence if K is a cubic field of discriminant Δ , one could try to find a cubic field L of the same discriminant by finding rational points $(-\frac{p}{3}, \pm\frac{q}{2})$ of $y^2 = x^3 - \frac{\Delta}{108}$. Using this idea, we construct a family of non isomorphic cubic fields

with prescribed discriminant. We need the following result from algebraic number theory (see [Ma]).

Proposition 3.3. *Let m be a non perfect cube integer and α a root of $x^3 - m$. Write $m = m_f m_s^2$ with m_f square free and $\gcd(m_f, m_s) = 1$. Suppose that $m \not\equiv \pm 1 \pmod{9}$. Then $\{1, \alpha, \alpha^2/m_s\}$ is an integral basis for $K_m = \mathbb{Q}(\alpha)$; in particular $\text{disc}(K_m) = -27(m_s m_f)^2$.*

Let $\Sigma = \{m \in \mathbb{N} \setminus \mathbb{N}^3 \mid m_s \neq 1, m_f m_s \not\equiv \pm 1 \pmod{9}, m \not\equiv \pm 1 \pmod{9}\}$.

Proposition 3.4. *Let $m \in \Sigma$ and K_m, L_m be the cubic fields defined by $x^3 - m$ and $x^3 - m_f m_s$ respectively, with m_f, m_s as in Proposition 3.3. Then K_m, L_m are cubic fields with equivalent trace forms, and have discriminant $-3(3m_f m_s)^2$.*

Proof. By the discussion above and Proposition 3.3 we have that K_m defines the rational elliptic curve $E_m : y^2 = x^3 + \frac{m_f^2 m_s^2}{4}$. A simple calculation shows that $E_m[3](\mathbb{Q}) = \{\infty, (0, \frac{m_f m_s}{2}), (0, -\frac{m_f m_s}{2})\}$, and these points define the field L_m . Let P be a generator of $E_m[3](\mathbb{Q})$ and $M_m = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 6y(p) \\ 0 & 6y(p) & 0 \end{pmatrix}$. Then M_m represents simultaneously the trace form in O_{K_m} and O_{L_m} with respect to the bases given by Proposition 3.3. \square

The pair of number fields given by Proposition 3.4 need not to be isomorphic, as the following example demonstrates.

Example 3.5. *Let $m = 12$ so that K_{12} and L_{12} are the cubic fields defined by $x^3 - 12$ and $x^3 - 6$ respectively. Then $\langle O_K, \tilde{q}_{K_{12}} \rangle$ and $\langle O_L, \tilde{q}_{L_{12}} \rangle$ are isomorphic to $\langle \mathbb{Z}^3, 3x^2 + 36yz \rangle$. One sees that K_{12} and L_{12} are non-isomorphic fields of discriminant $-2^2 3^5$ by direct computation, for instance 7 splits in L_{12} but it is inert in K_{12} .*

Recall that for Galois cubic fields of fixed discriminant there is only one possibility for the trace form (see Theorem 3.1). This follows, since after a suitable scaling we are left with a binary quadratic form of discriminant -3 . Inspired by this, we began looking for discriminants D of totally real cubic fields satisfying the following conditions:

- (i) D is a non-perfect square.
- (ii) D is non-fundamental.
- (iii) Up to squares factors and factors of 3, $-D$ defines an imaginary quadratic field of class number 1.
- (iv) There are at least two cubic fields of discriminant D .

It turns out that the first D satisfying the above conditions, (see tables at the end of [E-T]), is $D = 66825 = 3^5 5^2 11$. For this value of D we have:

Example 3.6. *Let K and L be the cubic fields defined by $2x^3 + 3x^2 - 21x + 4$ and $x^3 + 9x^2 - 18x - 3$ respectively. Then $\langle O_K, \tilde{q}_K \rangle$ and $\langle O_L, \tilde{q}_L \rangle$ are isomorphic to $\langle \mathbb{Z}^3, 3x^2 + 90(y^2 + yz + 3z^2) \rangle$. One sees that K and L are non-isomorphic fields of discriminant $3^5 5^2 11$ by direct computation, for instance $\text{regulator}(K) \neq \text{regulator}(L)$.*

None of our results so far yield positive answers to Questions 1.1 or 1.3 with fundamental discriminant. It is thus natural to ask whether those questions have negative answers in the special case where the discriminant of the cubic field is fundamental. Moreover, under this circumstances we will exhibit a more convenient refinement. To describe this, let K be a cubic number field and recall our notation $q_k = \tilde{q}_K|_{O_K^0}$. Then q_K is an integral, binary quadratic form. Moreover under the fundamental discriminant hypothesis, the isometry class of $\langle O_K^0, q_K \rangle$ is a refinement of the discriminant, as shown in Lemma 2.5.

4. CUBIC FIELDS WITH FUNDAMENTAL DISCRIMINANT

Throughout section 4, all cubic fields are assumed to have fundamental discriminant. The first question that comes to mind is the following: for which fundamental discriminants d does there exist a cubic field with discriminant d ? Moreover, we would like to know for which values of d there is more than one isomorphism class of cubic fields of discriminant d . It turns out that class field theory gives nice answers to these questions. Let K be a cubic field of fundamental discriminant d and Galois closure \tilde{K} . Clearly, $\mathbb{Q}(\sqrt{d}) \subseteq \tilde{K}$, and moreover, this extension is unramified. Since d is a fundamental discriminant, $\text{Gal}(\tilde{K}/\mathbb{Q}) \cong S_3$. Hence $[\tilde{K} : \mathbb{Q}(\sqrt{d})] = 3$, and $\tilde{K}/\mathbb{Q}(\sqrt{d})$ is abelian. Therefore, if H_d denotes the Hilbert class field of $\mathbb{Q}(\sqrt{d})$, and $Cl_{\mathbb{Q}(\sqrt{d})}$ denotes the ideal class group of $\mathbb{Q}(\sqrt{d})$, we have the following diagram:

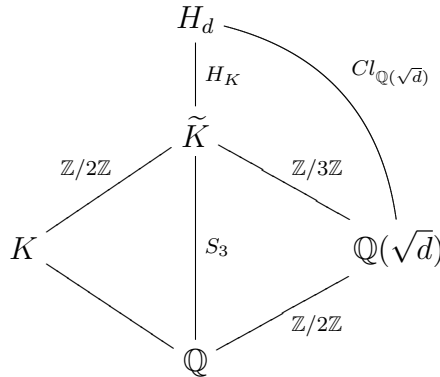


Figure 1

Thus, if we start with K as above, we obtain H_K , an index three subgroup of $Cl_{\mathbb{Q}(\sqrt{d})}$. Conversely, it can be shown (see [H]) that the fixed field of an index 3 subgroup of $Cl_{\mathbb{Q}(\sqrt{d})}$ corresponds to the Galois closure of a cubic field of discriminant d . Hence we have the following proposition:

Proposition 4.1 (Hasse, [H]). *The number of isomorphism classes of cubic fields of discriminant d is $(3^{r_3(d)} - 1)/2$, where $r_3(d) = 3\text{-rank}(Cl_{\mathbb{Q}(\sqrt{d})})$.*

Corollary 4.2 (Hasse, [H]). *There exists a cubic field K of discriminant d if and only if $Cl_{\mathbb{Q}(\sqrt{d})}[3] \neq 0$.*

Section 3 has given affirmative answers to Questions 1.1 and 1.3 for non-fundamental discriminants. The following example shows us that among fundamental discriminants one still finds positive answers to Questions 1.1 and 1.3 .

Example 4.3. *The fundamental discriminant of least absolute value with $r_3(d) > 1$ is $d = -3299$. For this value of d , $Cl_{\mathbb{Q}(\sqrt{d})} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$; hence there exist four non isomorphic cubic fields of discriminant -3299 . Among these four fields, the ones defined by $x^3 + 2x + 11$ and $x^3 - 16x + 27$ have isometric trace zero parts.*

Cubic fields with square free discriminants lead us to 3-torsion of class groups of quadratic fields. There is another very well known source of class groups of quadratic fields, namely binary quadratic forms. Let us recall briefly how these two are connected. Let Δ be a non square integer and let Γ_Δ (respectively Γ_Δ^1) be the set of $GL_2(\mathbb{Z})$ -equivalence classes (respectively $SL_2(\mathbb{Z})$ -equivalence classes) of primitive, binary quadratic forms of discriminant Δ . Gauss composition gives a group structure to Γ_Δ^1 , and furthermore this group is isomorphic to *the narrow class group* $Cl_{\mathbb{Q}(\sqrt{\Delta})}^+$. In particular $|\Gamma_\Delta| \leq |Cl_{\mathbb{Q}(\sqrt{\Delta})}^+|$. Now, let K be a cubic field of discriminant d not divisible by 3. Thanks to the next lemma, the $GL_2(\mathbb{Z})$ -equivalence class of $[\frac{1}{2}q_K]$ defines an element of Γ_{-3d} . Thus, if we denote by \mathcal{C}_d the set of isomorphism classes of cubic fields of discriminant d , we have the following map:

$$\begin{aligned} \Phi_d : \mathcal{C}_d &\longrightarrow \Gamma_{-3d} \\ K &\longmapsto [\tfrac{1}{2}q_K]. \end{aligned}$$

Since $Cl_{\mathbb{Q}(\sqrt{9897})}^+ \cong \mathbb{Z}/3\mathbb{Z}$ and $|\mathcal{C}_{-3299}| = 4$, the previous example can be restated as the non-injectivity of Φ_{-3299} .

Lemma 4.4. *Let K be a cubic field with fundamental discriminant d . Then $\frac{1}{2}q_K$ is an integral, binary quadratic form of discriminant $-3d$.*

Proof. Note that $\text{Disc}(q_K) = -4\text{Disc}(O_K^0) = \frac{-4|O_K/G_K|^2 d}{3}$. Since d is fundamental, $9 \nmid d$. In particular, $\text{tr}_{K/\mathbb{Q}}$ is a surjection from O_K to \mathbb{Z} and thanks to Lemma 2.3 we have $\text{Disc}(q_K) = -12d$. Note that if $x \in O_K^0$, then $\text{tr}(x^2) = \text{tr}(x^2) - \text{tr}^2(x) \in 2\mathbb{Z}$, hence $\frac{1}{2}q_K$ is integral. □

Remark 4.5. In fact, if $3 \nmid d$, then $\frac{1}{2}q_K$ is primitive as seen in Corollary 5.4.

Often it is more convenient to work with primitive forms rather than general ones. Since $q_K \sim_{GL_2(\mathbb{Z})} q_L$ if and only if $aq_K \sim_{GL_2(\mathbb{Z})} aq_L$ for any non zero rational number a , the previous remark will allow us to restrict ourselves to primitive forms.

5. TRACE FORM AND CLASS GROUPS

In this section we calculate q_K explicitly, and then show that for positive fundamental discriminants, q_K characterizes the field. To this end, we start by recalling the theorem of Delone-Faddeev-Gan-Gross-Savin on parametrization of cubic rings. (See [DF], [GG] or [B-C]). Every conjugacy class of a cubic ring R , has associated to it a unique integral binary cubic form $(a, b, c, d) := F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ up to $\mathrm{GL}_2(\mathbb{Z})$ -equivalence. Let K be a cubic number field and F the form associated to its maximal order. Among the properties of F we have the following:

- $K = \mathbb{Q}(\theta)$, where $\theta \in K$ is a root of $F_K(x, 1)$.
- $d_K := \mathrm{Disc}(K) = \mathrm{Disc}(a, b, c, d) = b^2c^2 - 27a^2d^2 + 18abcd - 4ac^3 - 4b^3d$.
- The Hessian form of F , $H_F = (P, Q, R) := Px^2 + Qxy + Ry^2$, has discriminant $-3d_K$, where

$$P = b^2 - 3ac, Q = bc - 9ad, R = c^2 - 3bd.$$

- H_F is covariant with respect to the $\mathrm{GL}_2(\mathbb{Z})$ -action on binary cubic forms and on binary quadratic forms.
- $\mathcal{B} = \{1, -a\theta, \frac{d}{\theta}\}$ is a \mathbb{Z} -basis of O_K .
- If d_K is fundamental, then H_F is a primitive, binary quadratic form.

Lemma 5.1. *Let $\alpha = -a\theta$ and $\beta = \frac{d}{\theta}$. Then H_F is realized as the integral quadratic form $\frac{3}{2} \mathrm{Tr}_{K/\mathbb{Q}}(X^2)$ over the \mathbb{Z} -module $O_K^{\mathcal{B}} = \mathrm{Span}_{\mathbb{Z}}\{\alpha - \frac{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)}{3}, \beta - \frac{\mathrm{Tr}_{K/\mathbb{Q}}(\beta)}{3}\}$.*

Proof. Note that $a^2F(\frac{x}{a}, 1)$ and $d^2F(1, \frac{x}{d})$ are the minimal polynomials over \mathbb{Q} of α and β respectively. Hence, $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = b$, $\mathrm{Tr}_{K/\mathbb{Q}}(\beta) = -c$, $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta) = -3ad$, $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^2) = b^2 - 2ac$, and $\mathrm{Tr}_{K/\mathbb{Q}}(\beta^2) = c^2 - 2bd$. From this and a simple calculation the result follows. \square

Proposition 5.2. *Let $\alpha_0 = \alpha - \frac{\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)}{3}$ and $\beta_0 = \beta - \frac{\mathrm{Tr}_{K/\mathbb{Q}}(\beta)}{3}$. Then*

$$O_K^0 = \begin{cases} O_1 = \mathrm{Span}_{\mathbb{Z}}\{\alpha_0, 3\beta_0\} & \text{if } b \equiv 0 \pmod{3} \\ O_2 = \mathrm{Span}_{\mathbb{Z}}\{3\alpha_0, \beta_0\} & \text{if } c \equiv 0 \pmod{3} \\ O_3 = \mathrm{Span}_{\mathbb{Z}}\{\alpha_0 - \beta_0, 3\beta_0\} & \text{if } b \equiv -c \pmod{3} \\ O_4 = \mathrm{Span}_{\mathbb{Z}}\{\alpha_0 + \beta_0, 3\beta_0\} & \text{if } b \equiv c \pmod{3}. \end{cases}$$

Proof. By Lemma 5.1, $(\frac{3}{2}\mathrm{Tr}_{K/\mathbb{Q}}(X^2)|O_K^{\mathcal{B}}) = -3d_K$ or, equivalently, $(\frac{1}{2}\mathrm{Tr}_{K/\mathbb{Q}}(X^2)|O_K^{\mathcal{B}}) = -\frac{1}{3}d_K$. On the other hand,

$$(5.1) \quad -3d_K = (\frac{1}{2}\mathrm{Tr}_{K/\mathbb{Q}}(X^2)|O_K^0) = [O_K^{\mathcal{B}} : O_K^0]^2 (\frac{1}{2}\mathrm{Tr}_{K/\mathbb{Q}}(X^2)|O_K^{\mathcal{B}}).$$

It follows that $[O_K^{\mathcal{B}} : O_K^0] = 3$. Notice that for each i , the given congruence conditions on b and c imply that $O_i \subseteq O_K^0$. Since $[O_K^{\mathcal{B}} : O_i] = 3$ for $i \in \{1, 2, 3, 4\}$, the result follows. \square

Corollary 5.3. *Let K be a cubic field and let $F_K = (a, b, c, d)$ be a cubic form associated to K . Let $H_K = (P, Q, R)$ be the Hessian of F_K . Then the binary quadratic form $\frac{1}{2}\text{Tr}_{K/\mathbb{Q}}(X^2)$ on the lattice O_K^0 can be explicitly described as follows:*

$$\begin{cases} (P/3, Q, 3R) & \text{if } b \equiv 0 \pmod{3} \\ (3P, Q, R/3) & \text{if } c \equiv 0 \pmod{3} \\ (3P, 2P - Q, \frac{P+R-Q}{3}) & \text{if } b \equiv -c \pmod{3} \\ (3P, 2P + Q, \frac{P+Q+R}{3}) & \text{if } b \equiv c \pmod{3}. \end{cases}$$

Proof. By Lemma 5.1, the matrix of $\frac{3}{2}\text{Tr}_{K/\mathbb{Q}}(X^2)$ over O_K^0 in the basis $\{\alpha_0, \beta_0\}$ is given by

$$M = \begin{pmatrix} P & Q/2 \\ Q/2 & R \end{pmatrix}.$$

$$\text{Let } N_1 = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}, N_2 = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, N_3 = \begin{pmatrix} 1 & -1 \\ 0 & 3 \end{pmatrix}, \text{ and } N_4 = \begin{pmatrix} 1 & 0 \\ -1 & 3 \end{pmatrix}.$$

Then the coordinates of the vector $N_i(\alpha_0, \beta_0)^t$ form a basis of O_i , for $i \in \{1, 2, 3, 4\}$. Hence, $\frac{1}{3}N_i M N_i^t$ is the matrix that represents $\frac{1}{2}\text{Tr}_{K/\mathbb{Q}}(X^2)$ over O_i in such a basis. After applying Proposition 5.2, the result follows. \square

From now on whenever we choose a cubic form F_K in the $\text{GL}_2(\mathbb{Z})$ -class given by the field K , what we mean by $\frac{1}{2}q_K$ is the quadratic form in the coordinates given by Corollary 5.3.

Corollary 5.4. *Let K be a cubic field with fundamental discriminant d not divisible by 3. Then $\frac{1}{2}q_K$ is a primitive, integral, binary quadratic form of discriminant $-3d$.*

Proof. By Lemma 4.4, it remains only to prove that $\frac{1}{2}q_K$ is primitive. Since H_K is primitive and $9 \nmid -3d$, the result follows from Corollary 5.3. \square

For a fixed F_K in the $\text{GL}_2(\mathbb{Z})$ -class given by the field K , we have found explicit relations between the binary quadratic forms $\frac{1}{2}q_K$ and H_K . Since they have the same discriminant, namely $-3d_K$, one could ask: what is their relation as elements of the group $Cl_{\mathbb{Q}(\sqrt{-3d_K})}^+$? A small objection to this question is that even though H_K represents a valid element of this group, $\frac{1}{2}q_K$ need not, since it may not be primitive. The problem is that the latter is not always primitive. Yet, as Corollary 5.4 shows, $\frac{1}{2}q_K$ is primitive whenever 3 does not ramify in K . In this setting we are able to find the following connection between forms.

Theorem 5.5. *Let K be a cubic field with discriminant d_K . Assume that d_K is fundamental and that $3 \nmid d_K$. Let $F_K = (a, b, c, d)$ be a cubic in the $\text{GL}_2(\mathbb{Z})$ -equivalence class defined by K . Then $\frac{1}{2}q_K * C_{d_K} = H_K^{\pm 1}$ as elements of $Cl_{\mathbb{Q}(\sqrt{-3d_K})}^+$, where $C_{d_K} = (3, 0, \frac{d_K}{4})$ or $C_{d_K} = (3, 3, \frac{d_K+3}{4})$ in accordance with whether $d_K \equiv 0 \pmod{4}$ or $d_K \equiv 1 \pmod{4}$.*

Proof. We work out the case when $d_k \equiv 1 \pmod{4}$, the other case being completely analogous. By Arndt's composition algorithm, (see [Bu], Theorem 4.10)

$$\begin{cases} C_K * (P, Q, R) = (P/3, Q, 3R) & \text{if } b \equiv 0 \pmod{3} \\ C_K * (3P, Q, R/3) = (P, Q, R) & \text{if } c \equiv 0 \pmod{3} \\ C_K * (3P, 2P - Q, \frac{P+R-Q}{3}) = (P, 2P - Q, P + R - Q) & \text{if } b \equiv -c \pmod{3} \\ C_K * (3P, 2P + Q, \frac{P+Q+R}{3}) = (P, 2P + Q, P + R + Q) & \text{if } b \equiv c \pmod{3}. \end{cases}$$

Using the matrix $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, we see that we have identities in $Cl_{\mathbb{Q}(\sqrt{-3d_K})}^+$

$$(P, 2P - Q, P + R - Q) = H_K^{-1} \quad \text{and} \quad (P, 2P + Q, P + R + Q) = H_K.$$

Since C_K is its own inverse, the result follows from the explicit description of $\frac{1}{2}q_K$ given in Corollary 5.3. □

Remark 5.6. Note that given K we have freedom on choosing F_K in such a way that $b \not\equiv -c \pmod{3}$. Hence Theorem 5.5 can be actually interpreted as $\frac{1}{2}q_K * C_{d_K} = H_K$

Remark 5.7. We denote the form C_K by C_{d_K} in order to stress the fact that this form only depends on the discriminant of K .

5.1. Bhargava's composition laws on cubes and their relation to the trace form. We have related the trace form, in the cubic case, to class groups of quadratic fields. There is a well known generalization of Gauss' composition of quadratic forms to cubic forms. Inspired by this generalization, we expected some connection between the cubic forms attached to cubic number fields, and the quadratic forms given by the traces of these fields. We briefly recall some of the basics of Bhargava's laws on cubes and then we explain how to get such a connection (see Theorem 6.2).

In his PhD thesis, (see [Bha]), Bhargava generalizes the composition laws on binary quadratic forms of a fixed discriminant Δ discovered by Gauss. Bhargava defines a $SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$ -action on the set of $2 \times 2 \times 2$ integral cubes of discriminant Δ . Let $Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; \Delta)$ be the space of orbits given of action. Using the generalization of Gauss' composition mentioned above, Bhargava discovered a composition law on $Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; \Delta)$.

In explicit terms one can think of a $2 \times 2 \times 2$ integral cube \mathcal{C} as a pair of 2×2 integral matrices (A, B) , where A is the front face and B is the back face. Let

$$Q_1(\mathcal{C}) = -Det(Ax+By), Q_2(\mathcal{C}) = -Det\left(\begin{bmatrix} x \\ y \end{bmatrix} \middle| B \begin{bmatrix} x \\ y \end{bmatrix}\right), Q_3(\mathcal{C}) = -Det\left(A^t \begin{bmatrix} x \\ y \end{bmatrix} \middle| B^t \begin{bmatrix} x \\ y \end{bmatrix}\right).$$

It can be verified that $Disc(Q_1) = Disc(Q_2) = Disc(Q_3)$, moreover this common discriminant Δ is precisely the definition of the discriminant of \mathcal{C} . If $g := (g_1, g_3, g_3) \in \Gamma := SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$, and (A, B) is a cube, then $g \cdot (A, B) := g_1 \begin{pmatrix} g_3 A g_2^t \\ g_3 B g_2^t \end{pmatrix}$. This action preserves the discriminant. Moreover, if Q_1, Q_2, Q_3 are primitive forms,

one has that $Q_1 * Q_2 * Q_3 = 0$ as elements of $Cl_{\mathbb{Q}(\sqrt{\Delta})}^+$. Conversely, let (Q_1, Q_2, Q_3) be a triple of primitive, binary quadratic forms of discriminant Δ such that $Q_1 * Q_2 * Q_3 = 0$. Then there is a unique class on $Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; \Delta)$ giving rise to (Q_1, Q_2, Q_3) as above. With this in hand, it is simple to define a composition law on cubes: $(A, B) + (A', B')$ is the cube that corresponds to the triple $(Q_1 * Q'_1, Q_2 * Q'_2, Q_3 * Q'_3)$. Furthermore:

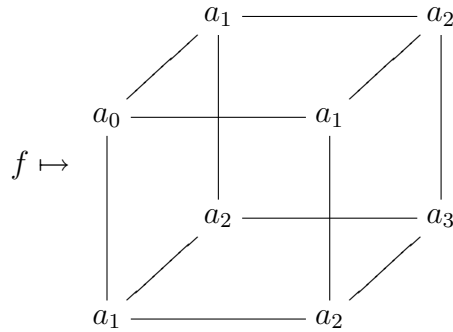
Theorem 5.8 (Bhargava, [Bha]). *There is an isomorphism*

$$\phi : Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; \Delta) \rightarrow Cl_{\mathbb{Q}(\sqrt{\Delta})}^+ \times Cl_{\mathbb{Q}(\sqrt{\Delta})}^+$$

defined by $(A, B)_\Gamma \mapsto ([Q_1]_{SL_2(\mathbb{Z})}, [Q_2]_{SL_2(\mathbb{Z})})$.

Definition 5.9. A binary cubic form $f(x, y) \in \mathbb{Z}[x, y]$ is called a Gaussian cubic form if it is of the form $(a_0, 3a_1, 3a_2, a_3)$. The set of Gaussian cubic forms is denoted by $Sym^3\mathbb{Z}^2$.

One may naturally associate to a Gaussian cubic form $f = (a_0, 3a_1, 3a_2, a_3)$ a triple symmetric cube:



The correspondence between cubic forms and cubes is identified with a map $\iota : Sym^3\mathbb{Z}^2 \rightarrow \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$.

If we replace f by a Gaussian form in the same $SL_2(\mathbb{Z})$ equivalence class as f , one obtains a well defined element under the Γ -action on cubes.

Let $Cl(Sym^3\mathbb{Z}^2; \Delta)$ be the set of Gaussian forms, up to $SL_2(\mathbb{Z})$ -action, such that the corresponding cubes have fundamental discriminant Δ .

Remark 5.10. One must distinguish between the notions of the discriminant of cubic forms and the discriminant of cubes. For example, let f be a Gaussian form of discriminant D . Then cube corresponding to f has discriminant $\Delta = \frac{-D}{27}$.

It turns out that $Cl(Sym^3\mathbb{Z}^2; \Delta)$ is an abelian group. Furthermore, we have that

$$[\iota] : [f]_{SL_2(\mathbb{Z})} \mapsto [\iota(f)]_\Gamma$$

is a group homomorphism. By composing the homomorphisms

$$Cl(Sym^3\mathbb{Z}^2; \Delta) \xrightarrow{[u]} Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; \Delta) \xrightarrow{\phi} Cl_{\mathbb{Q}(\sqrt{\Delta})}^+ \times Cl_{\mathbb{Q}(\sqrt{\Delta})}^+ \xrightarrow{\pi_1} Cl_{\mathbb{Q}(\sqrt{\Delta})}^+,$$

Bhargava obtains:

Theorem 5.11 (Bhargava [Bha], Hoffman-Morales [H-M]). *There is a surjective homomorphism*

$$\phi_1 : Cl(Sym^3\mathbb{Z}^2; \Delta) \rightarrow Cl_{\mathbb{Q}(\sqrt{\Delta})}^+[3],$$

where ϕ_1 is the first projection of ϕ composed with $[u]$. The cardinality of the kernel is equal to $|U/U^3|$, where U denotes the group of units in $\mathbb{Q}(\sqrt{\Delta})$. In other words, the Kernel has order 1 if $\Delta < -3$, or 3 otherwise.

This theorem was in essence first obtained by Eisenstein, but he incorrectly asserted that the kernel of the map was always trivial. (see [E]). Later Arnt and Cayley pointed out that it is not a bijection if $\Delta \geq -3$.

Remark 5.12. Explicitly, $\phi_1(a_0, 3a_1, 3a_2, a_3) = (a_1^2 - a_0a_2, a_1a_2 - a_0a_3, a_2^2 - a_1a_3)$.

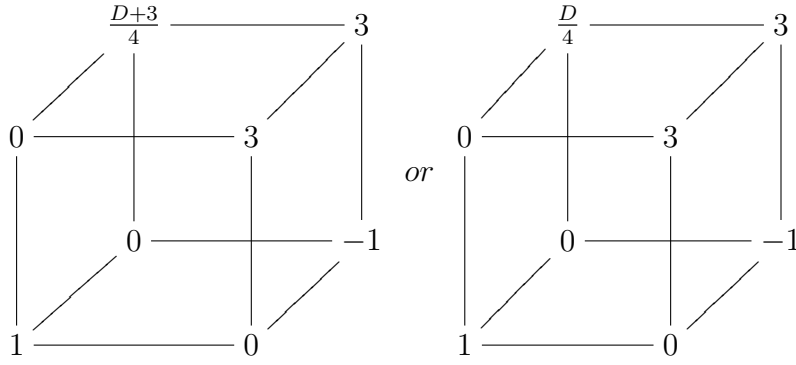
6. FROM CUBIC FIELDS TO CUBES AND TRACE FORMS

Given K , a cubic field of discriminant d_K , and representative form $F_K(x, y) = (a, b, c, d)$, we naturally associate a cube as follows:

$$K : ax^3 + bx^2y + cxy^2 + dy^3 \mapsto$$

We obtain in this way an element $\mathcal{K}_F \in [u](Cl(Sym^3\mathbb{Z}^2; -3d_K)) \subseteq Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; -3d_K)$.

Let D be a fundamental discriminant . Let $\mathcal{C}_D \in Cl(\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2; -3D)$ be given by



in accordance with whether $D \equiv 0 \pmod{4}$ or $D \equiv 1 \pmod{4}$.

Lemma 6.1. *Let K be a cubic field with a fixed cubic form $F = (a, b, c, d)$. Then $Q_1(\mathcal{K}_F) = H_F$ and $Q_1(\mathcal{C}_{d_K}) = \mathcal{C}_{d_K}$.*

Proof. The result follows easily using the definition $Q_1(A, B) = -\text{Det}(Ax + By)$ for a cube (A, B) . □

Theorem 6.2. *Let K be a cubic field with discriminant d_K and associated cubic form $F_K = (a, b, c, d)$. Assume that d_K is fundamental and that 3 does not ramify. Let $T_{F_K} = \mathcal{K}_F + \mathcal{C}_{d_K}$. Then $(\pi_1 \circ \phi)(T_{F_K})^{\pm 1} = \frac{1}{2}q_K$ as elements of $Cl_{\mathbb{Q}(\sqrt{-3d_K})}^+$.*

Proof. Since ϕ is a group homomorphism we have that $\phi(T_{F_K}) = \phi((K)_F) * \phi(\mathcal{C}_{d_K})$. Projecting to the first component by π_1 we get that $(\pi_1 \circ \phi)(T_{F_K}) = H_K * \mathcal{C}_{d_K}$. Since all of the functions involved are group homomorphisms, the result follows from Theorem

5.5. In other “words”

$$\begin{array}{ccc}
\begin{array}{ccc} & b & c \\ & \diagdown & \diagup \\ 3a & & b \\ | & & | \\ b & & c \\ & \diagup & \diagdown \\ & c & 3d \end{array} & + & \begin{array}{ccc} & \frac{D+3}{4} & 3 \\ & \diagdown & \diagup \\ 0 & & 3 \\ | & & | \\ 1 & & 0 \\ & \diagup & \diagdown \\ & 0 & -1 \end{array} & \xrightarrow{\phi_1} & \frac{1}{2}\mathrm{Tr}_K(x^2)
\end{array}$$

□

Remark 6.3. We note that we could choose F_K , see Remark 5.6, so that the conclusion of Theorem 6.2 is $(\pi_1 \circ \phi)(T_{F_K}) = \frac{1}{2}q_K$.

Theorem 6.4. *Let K be a cubic field with discriminant d_K , and let $F_K(x, y) = (a, b, c, d)$ be a cubic form associated to K . Assume that d_K is fundamental and that 3 ramifies in K/\mathbb{Q} . Then we have:*

$$\begin{aligned}
\phi_1 : Cl(\mathrm{Sym}^3 \mathbb{Z}^2; -\frac{d_K}{3}) &\rightarrow Cl_{\mathbb{Q}(\sqrt{-\frac{d_K}{3}})}^+ [3] \\
(f_K)_{SL_2(\mathbb{Z})} &\mapsto (\frac{1}{6}q_K)_{SL_2(\mathbb{Z})},
\end{aligned}$$

where $f_K(x, y)$ is defined as follows:

$$f_K(x, y) = \begin{cases} \frac{1}{3}F(x, 3y) & \text{if } b \equiv 0 \pmod{3} \\ \frac{1}{3}F(3x, y) & \text{if } c \equiv 0 \pmod{3} \\ \frac{1}{3}F(x, 3(y-x)) & \text{if } b \equiv -c \pmod{3} \\ \frac{1}{3}F(x, 3(y+x)) & \text{if } b \equiv c \pmod{3}. \end{cases}$$

Proof. Replacing $F(x, y)$ with either $F(y, x)$, $F(x, y-x)$ or $F(x, y+x)$ we may assume that $b \equiv 0 \pmod{3}$. With this in hand, we have that $d_K \equiv -ac^3 \pmod{3}$, and since 3 ramifies, $ac \equiv 0 \pmod{3}$. On the other hand since d_K is fundamental we see that $3|a$. By Corollary 5.3, $\frac{1}{2}q_K = ((b^2 - 3ac)/3, bc - 9ad, 3(c^2 - 3bd))$, thus $\frac{1}{6}q_K = ((\frac{b}{3})^2 - \frac{a}{3}c, \frac{b}{3}c - \frac{a}{3}9d, (c^2 - \frac{b}{3}9d))$, which is $\phi_1(\frac{1}{3}F(x, 3y))$. □

Theorem 6.5. *Let K be a cubic number field of positive, fundamental discriminant, and let L be a number field such there exists an isomorphism of quadratic modules*

$$\langle O_K^0, q_K \rangle \cong \langle O_L^0, q_L \rangle.$$

Further assume $9 \nmid d_L$. Then $K \cong L$.

Proof. By Lemma 2.5 we have $d_K = d_L$. As usual, fix cubic forms $F_K(x, y)$ and $F_L(x, y)$ in the classes given by K and L respectively. Suppose first that $3 \nmid d_K$.

Since the isometry between the forms need not to be proper, we only can ensure that as elements of $Cl_{\mathbb{Q}(\sqrt{-3d_K})}^+$, $\frac{1}{2}q_K = (\frac{1}{2}q_L)^{\pm 1}$. By Theorem 6.2 we have that $(\pi_1 \circ \phi)(T_{F_K})^{\pm 1} = (\pi_1 \circ \phi)(T_{F_L})$. Replacing $F_K(x, y)$ by $F_K(x, -y)$ has the effect of replacing $H_{F_K}(x, y)$ by $H_{F_K}(x, -y)$. On the other hand $H_{F_K}(x, -y)$ is inverse to H_{F_K} in the narrow class group. Since C_{d_K} has order 2, Theorem 5.5 says that we may replace $F_K(x, y)$ by $F_K(x, -y)$, if necessary, so we may assume that

$$(\pi_1 \circ \phi)(T_{F_K}) = (\pi_1 \circ \phi)(T_{F_L}).$$

Equivalently,

$$(\pi_1 \circ \phi)(\mathcal{K}_{F_K}) = (\pi_1 \circ \phi)(\mathcal{K}_{F_L}).$$

Notice that $\mathcal{K}_F = \iota(3F)$, hence $\phi_1(3F_K) = \phi_1(3F_L)$. Since $d_K > 1$, Theorem 5.11 implies that $3F_K$ and $3F_L$ are $SL_2(\mathbb{Z})$ -equivalent. Since we could have replaced $F_K(x, y)$ by $F_K(x, -y)$, the equivalence between $3F_K$ and $3F_L$ is up to $GL_2(\mathbb{Z})$. In any case this implies that $K \cong L$. If $3 \mid d_K$, we apply Theorem 6.4 and the argument follows the same lines as in the case without 3-ramification. \square

6.1. Observations. Given $\Delta \in \mathbb{Z}$, let X_Δ be the set of integral, primitive, binary quadratic forms of discriminant Δ . Recall our notation $\Gamma_\Delta = GL_2(\mathbb{Z}) \setminus X_\Delta$ and $\Gamma_\Delta^1 = SL_2(\mathbb{Z}) \setminus X_\Delta$.

Let d be a positive fundamental discriminant, $n_d := \gcd(3, d)$, and \mathcal{C}_d the set of isomorphism classes of cubic fields of discriminant d .

Remark 6.6. Theorem 6.5 is equivalent to the injectivity of

$$\begin{aligned} \Phi_d : \mathcal{C}_d &\longrightarrow \Gamma_{\frac{-3d}{n_d^2}} \\ K &\longmapsto \left[\frac{1}{2n_d} q_K \right]. \end{aligned}$$

Recall that Gauss' composition induces a group isomorphism between $Cl_{\mathbb{Q}(\sqrt{\frac{-3d}{n_d^2}}}^+$ and $\Gamma_{\frac{-3d}{n_d^2}}^1$. Hence, we have a double cover $\pi : Cl_{\mathbb{Q}(\sqrt{\frac{-3d}{n_d^2}}}^+ \rightarrow \Gamma_{\frac{-3d}{n_d^2}}^1$, with the property that the fiber of every point consists of an element and its inverse. Therefore, even though $\frac{1}{2n_d} q_K$ does not define a point in $Cl_{\mathbb{Q}(\sqrt{\frac{-3d}{n_d^2}}}^+$, it defines a cyclic subgroup, namely

the group generated by $\pi^{-1}(\Phi_d(K))$. Corollary 5.3 and Lemma 6.4 provide us with a generator of this group. Let g_K be such a generator. Using Arndt's composition algorithm (see [Bu]), one sees that $g_K^3 = C_K$ when $3 \nmid d$, and that g_K has order 3 otherwise. Since C_{d_K} has order 2, it follows that $\langle \pi^{-1}(\Phi_d(K)) \rangle$ has order $2n_d$.

Proposition 6.7. *Let $d > 0$ be a fundamental discriminant. The map $K \mapsto \langle g_K \rangle$ is injective.*

Proof. Since $\langle g_K \rangle$ has order 3 or 6, its set of generators is $\{g_K^{\pm 1}\}$. Thus, if $\langle g_K \rangle = \langle g_L \rangle$, then $g_K^{\pm 1} = g_L$. Projecting under π we obtain that $\Phi_d(K) = \Phi_d(L)$, and the result follows from Remark 6.6. \square

Note that the unique subgroup of order 3 of $\langle g_K \rangle$ is given by $\langle g_K^2 \rangle$. Hence, from Proposition 6.7 we have:

Theorem 6.8. *Let $d > 0$ be a fundamental discriminant such that $\mathcal{C}_d \neq \emptyset$. Let $\mathcal{P}_3(\text{Cl}_{\mathbb{Q}(\sqrt{-3d})}^+)$ be the set of subgroups of size 3 of $\text{Cl}_{\mathbb{Q}(\sqrt{-3d})}^+$. Then*

$$\begin{aligned} \Theta_d : \mathcal{C}_d &\longrightarrow \mathcal{P}_3(\text{Cl}_{\mathbb{Q}(\sqrt{-3d})}^+) \\ K &\longmapsto \langle g_K^2 \rangle \end{aligned}$$

is injective.

The injection Θ_d gives an alternative proof of one inequality of the Scholz Reflection Principle (see [Sch]).

Corollary 6.9. *Let d be a positive fundamental discriminant, and let $r = 3\text{-rank}(\text{Cl}_{\mathbb{Q}(\sqrt{-3d})})$ and $s = 3\text{-rank}(\text{Cl}_{\mathbb{Q}(\sqrt{d})})$. Then $s \leq r$.*

Proof. $(3^s - 1)/2 = |\mathcal{C}_d|$ and $(3^r - 1)/2 = |\mathcal{P}_3(\text{Cl}_{\mathbb{Q}(\sqrt{-3d})}^+)|$. \square

ACKNOWLEDGEMENTS

I would like to thank Jordan Ellenberg for introducing me to this subject, and for many helpful discussions, suggestions and advice during the writing of this paper. I also thank Manjul Bhargava, Amanda Folsom, and Yongqiang Zhao for thorough and helpful comments on an earlier version of this paper.

REFERENCES

- [Bha] Bhargava. Manjul, *Higher composition laws I: A new view on Gauss composition, and quadratic generalizations*, Annals of Mathematics, **159** (2004), 217-250.
- [Bu] Duncan A. Buell, *BINARY QUADRATIC FORMS: Classical theory and modern computations*, Springer Verlag, 1989.
- [B-C] K. Belabas, H. Cohen, *Binary cubic forms and cubic number fields*, in Computational perspectives in Number Theory (Chicago 1995), Eds. D. Buell et J. Teitelbaum, Studies in Advanced Mathematics, 1998
- [C-P] P.E. Conner, R. Perlis, *A survey of trace forms of algebraic number fields*, World Scientific, Singapore, 1984.
- [D-H1] H. Davenport and H.Heilbronn, *On the density of discriminants of cubic fields I*, Bull. Lond. Math. Soc., **1** (1969), 345-348.
- [D-H2] H. Davenport and H.Heilbronn, *On the density of discriminants of cubic fields II*, Proc. Roy. Soc. London A, **322** (1971), 405-420.
- [DF] B.N. Delone and D.K. Faddeev, *The theory of irrationalities of third degree*, AMS Translations of Mathematical Monographs, **10** (1964).
- [E] G. Eisenstein, *Théorèmes sur le formes cubiques et d'une équation du quatrième degré indéterminées*, J. reine angew. Math**27** (1844), 75-79.

- [E-T] V. Ennola, R. Turunen, *On Totally real cubic fields*, Mathematics of computation. vol. 44, No. 170 (Apr.,1985), pp. 495-518.
- [GG] W.-T. Gan, B.H Gross, and G. Savin, *Fourier coefficients of modular forms on G_2* , Duke Math. J. **115**, (2002) 105-169.
- [H] H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage*, Math. Zeitschrift. **31**, 1930, 565-582.
- [Hi] D. Hilbert, *Theorie der algebraischen Zahlkörper*, Gesammelte Abhanduglen, Bd I, Springer-Verlag, 1932.
- [H-M] J. W. Hoffman and J. Morales, *Arithmetic of binary cubic forms*, Enseign. Math. (2) **46**, 2000, 61-94.
- [Ma] D. Marcus, *Number Fields*, Universitext. Springer-Verlag, New York-Heidelberg, 1977. viii+279 pp.
- [Ne] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer, Berlin, 1999.
- [Sil] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, New York: Springer-Verlag, 1986.
- [Sch] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Zahlkörper*, J. reine angew. Math., **166**, 1932 201-203

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, MADISON, 53706
E-mail address: mantilla@math.wisc.edu