BINARY CUBIC FORMS AND CUBIC NUMBER FIELDS

K. Belabas and H. Cohen

Laboratoire A2X, URA 9936 du CNRS, Université
Bordeaux I, 351 Cours de la Libération, 33405 Talence Cedex

The aim of this paper is to present in a naïve manner a small part of the theory of binary cubic forms and in particular its application to cubic number fields. Most of the results are due to Davenport-Heilbronn ([5],[6]), but the algorithmic applications seem to be new.

1. General Binary Forms

Before specializing to the cubic case, we consider the general case of binary forms of degree n. Let K be a field (usually $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$).

A *binary form* of degree n with coefficients in K is a homogeneous polynomial in two variables of degree n with coefficients in K, *i.e* an expression of the form

$$F(x,y)=\sum_{i=0}^{n} a_i x^i y^{n-i} \quad ,$$

with $a_i \in K$. We will write $F=(a_n,a_{n-1},\dots,a_0)$ as an abbreviation for the above notation. In particular $F=(a,b,c)$ is the binary quadratic form $F(x,y)=ax^2+bxy+cy^2$, and $F=(a,b,c,d)$ is the cubic form $F(x,y)=ax^3+bx^2y+cxy^2+dy^3$.

The *roots* of F in K are the solutions $(x:y)\in\mathbb{P}_1(K)$ of $F(x,y)=0$. If $a_j=0$ for $m<j\le n$ and $a_m\neq 0$, the point at infinity $(1:0)$ is a root of order exactly $n-m$ (if $m=n$, *i.e* $a_n\neq 0$, it is of course not a root), and the other roots are the roots in K of the polynomial $F(x,1)$ of degree m. In particular if K is algebraically closed, F has always exactly n roots, counted with multiplicity. Note that the point at infinity is rational over any base field, algebraically closed or not.

Denote by $(\alpha_i:\beta_i)\in\mathbb{P}_1(\mathbb{C})$, with $1\le i\le n$, the roots of F in $\mathbb{C}$. It is easily seen that we can choose representatives in $\mathbb{P}_1(\mathbb{C})$ so that we have

$$F(x,y)=\prod_{1\le i\le n}(\beta_i x-\alpha_i y) \quad .$$

Of course the choice of representative is not unique: for each i we can change (α_i,β_i) into $(\lambda_i\alpha_i,\lambda_i\beta_i)$ as long as $\prod_{1\le i\le n}\lambda_i=1$. We will always assume that the representatives of the roots are chosen in this manner.

We define the *discriminant* of the form F by the following formula:

$$\operatorname{disc}(F)=\prod_{1\le i<j\le n}(\alpha_i\beta_j-\alpha_j\beta_i)^2 \quad .$$

This makes sense since if we change (α_i, β_i) into $(\lambda_i\alpha_i, \lambda_i\beta_i)$ with $\prod_{1\le i\le n}\lambda_i = 1$, the product is multiplied by

$$\prod_{1\le i<j\le n}(\lambda_i\lambda_j)^2 = \Big(\prod_{1\le i\le n}\lambda_i\Big)^{2n-2} = 1\ .$$

If $F(x,1)$ is a polynomial of degree exactly equal to n ($i.e$ if $a_n \neq 0$), then one immediately checks that $\operatorname{disc}(F) = \operatorname{disc}(F(x,1))$.

In degrees up to 3 we have the following formulas.

$$\operatorname{disc}(ax+by) = 1\ ,$$

$$\operatorname{disc}(ax^2+bxy+cy^2) = b^2-4ac\ ,$$

$$\operatorname{disc}(ax^3+bx^2y+cxy^2+dy^3) = b^2c^2-27a^2d^2+18abcd-4ac^3-4b^3d\ .$$

If F is a form of degree n and $\gamma = \left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right)$ is a 2×2 matrix with coefficients in K we define the action of γ on F by $F\circ\gamma(x,y) = F(Ax+By, Cx+Dy)$.

Proposition 1.1. *Let* $\gamma = \left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right)$. *Then*

$$\operatorname{disc}(F\circ\gamma) = (AD-BC)^{n(n-1)}\operatorname{disc}(F)\ .$$

Proof. Let $(\alpha_i : \beta_i)$ be the roots of F chosen as above so that

$$F(X,Y) = \prod_{1\le i\le n}(\beta_i x - \alpha_i y)\ .$$

Therefore

$$F\circ\gamma(X,Y) = \prod_{1\le i\le n}(\beta_i(Ax+By)-\alpha_i(Cx+Dy)) = \prod_{1\le i\le n}(\beta_i' x - \alpha_i' y)\ ,$$

with

$$\begin{pmatrix}\alpha_i'\\ \beta_i'\end{pmatrix} = \begin{pmatrix}D & -B\\ -C & A\end{pmatrix}\begin{pmatrix}\alpha_i\\ \beta_i\end{pmatrix}\ .$$

Hence

$$\begin{aligned}\operatorname{disc}(F\circ\gamma) &= \prod_{1\le i<j\le n}(\alpha_i'\beta_j' - \alpha_j'\beta_i')^2\\ &= \prod_{1\le i<j\le n}((AD-BC)(\alpha_i\beta_j-\alpha_j\beta_i))^2\\ &= (AD-BC)^{n(n-1)}\operatorname{disc}(F)\ .\end{aligned}$$

□

We now restrict to the case of *integral* binary forms, $i.e$ binary forms whose coefficients are all in $\mathbb{Z}$. As a corollary of the proposition, we see that the action of $\mathrm{GL}_2(\mathbb{Z})$ preserves the discriminant of F, since $n(n-1)$ is even.

We will say that the form F is *irreducible* if $F(x,y)$ is irreducible as a polynomial in $\mathbb{Q}[x,y]$. Equivalently, F is irreducible if $a_n \neq 0$ and the polynomial $F(x,1)$ is irreducible in $\mathbb{Q}[x]$ (or $\mathbb{Z}[x]$).

We will say that an integral form F is *primitive* if the GCD of all its coefficients is equal to 1.

Proposition 1.2. *Let F be an integral form and $\gamma \in \mathrm{GL}_2(\mathbb{Z})$. Then $F \circ \gamma$ is irreducible if and only if F is, and $F \circ \gamma$ is primitive if and only F is.*

Proof. This immediately follows from the fact that the action of $\mathrm{GL}_2(\mathbb{Z})$ is reversible, *i.e* that $F = (F \circ \gamma) \circ \gamma^{-1}$. □

2. Binary Cubic Forms and Cubic Number Fields

The aim of this section is to generalize to the cubic case the well known correspondence between binary quadratic forms and quadratic number fields. These results are due to Davenport and Heilbronn (see [5] and [6]). Before stating and proving the main theorem, we need a few preliminary results. We let Φ be the set of classes of primitive irreducible binary cubic forms. This makes sense, thanks to Proposition 1.2.

Let K be a cubic number field, and $(1, \alpha, \beta)$ an integral basis of $\mathbb{Z}_K$ with first element equal to 1. Denote by $\mathrm{disc}(K)$ the discriminant of the number field K. If $x \in K$, denote by $x_1 = x$, x_2 and x_3 the conjugates of x in K^{Gal}, and let $\mathrm{disc}(x)$ be the discriminant of the (monic) characteristic polynomial of x, so that $\mathrm{disc}(x) = ((x_1 - x_2)(x_1 - x_3)(x_2 - x_3))^2$.

Note that if $x \in K$ and $x = x'/d$ with $x' \in \mathbb{Z}_K$ and $d \in \mathbb{Z}$, then

$$\mathrm{disc}(x) = \mathrm{disc}(x')/d^6 = \mathrm{disc}(K) f^2/d^6 \ ,$$

where $f = [\mathbb{Z}_K : \mathbb{Z}[x']]$. So that, for every $x \in K$, we have $\sqrt{\mathrm{disc}(x)/\mathrm{disc}(K)} \in \mathbb{Q}$.

Proposition 2.1. *Let $\mathcal{B} = (1, \alpha, \beta)$ be an integral basis of a cubic number field K as above. For x and y elements of $\mathbb{Q}$, set*

$$F_{\mathcal{B}}(x, y) = \frac{\displaystyle\prod_{1 \le i < j \le 3} \big((\beta_i - \beta_j)x - (\alpha_i - \alpha_j)y\big)}{\displaystyle\sum_{1 \le i < j \le 3} (-1)^{i-j}(\alpha_i \beta_j - \alpha_j \beta_i)} \ .$$

(1) *For x and y in $\mathbb{Q}$, we have*

$$F_{\mathcal{B}}(x, y) = \pm\sqrt{\frac{\mathrm{disc}(\beta x - \alpha y)}{\mathrm{disc}(K)}} = \pm\frac{\mathcal{N}_{K/\mathbb{Q}}\big((\beta_1 - \beta_2)x - (\alpha_1 - \alpha_2)y\big)}{\sqrt{\mathrm{disc}(K)}} \ .$$

(2) *The function $F_{\mathcal{B}}$ is the restriction to $\mathbb{Q} \times \mathbb{Q}$ of a binary cubic form (again denoted by $F_{\mathcal{B}}$) with rational coefficients.*
(3) $\mathrm{disc}(F_{\mathcal{B}}) = \mathrm{disc}(K)$.
(4) *The form $F_{\mathcal{B}}$ is an integral primitive irreducible cubic form.*
(5) *The class of $F_{\mathcal{B}}$ in Φ is independent of the integral basis $(1, \alpha, \beta)$ that we have chosen (hence by abuse of notation we will denote this class by F_K).*
(6) *Let the number field K be defined by a root θ of the polynomial $x^3 + px^2 + qx + r$ with p, q, r in $\mathbb{Z}$, such that there exists an integral basis of the form $(1, \theta, (\theta^2 + t\theta + u)/f)$ with t, u, f in $\mathbb{Z}$ and $f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ – this is always possible. Then, when we choose $\alpha = \theta$ and $\beta = (\theta^2 + t\theta + u)/f$, we have explicitly:*

$$\begin{aligned} F_{\mathcal{B}}(x, y) = {} & ((t^3 - 2t^2p + t(q + p^2) + r - pq)/f^2)x^3 \\ & + ((-3t^2 + 4tp - (p^2 + q))/f)x^2y + (3t - 2p)xy^2 - fy^3 \ . \end{aligned}$$

Proof. (1) follows directly from the definitions, after noting that $\sqrt{\operatorname{disc}(K)}$ is the determinant of the matrix

$$\begin{pmatrix} 1 & \alpha_1 & \beta_1 \\ 1 & \alpha_2 & \beta_2 \\ 1 & \alpha_3 & \beta_3 \end{pmatrix} .$$

Note that if we take one of the expressions on the RHS of (1) for definition of $F_{\mathcal{B}}$ there is a sign ambiguity. However, this will not matter in the sequel since $F_{\mathcal{B}}(-x,-y) = -F_{\mathcal{B}}(x,y)$, so that $F_{\mathcal{B}}$ and $-F_{\mathcal{B}}$ are $\mathrm{SL}_2(\mathbb{Z})$-equivalent.

(2) The definition of $F_{\mathcal{B}}$ shows that $F_{\mathcal{B}}$ is the restriction to $\mathbb{Q}\times\mathbb{Q}$ of a cubic form with coefficients in K^{Gal}. Furthermore Galois theory shows that the coefficients of $F_{\mathcal{B}}(x,y)$ are invariant under the Galois group of K^{Gal} over $\mathbb{Q}$, so that in fact $F_{\mathcal{B}}$ is a rational cubic form. Note that the rationality of $F_{\mathcal{B}}(x,y)$ when x and y are rational also follows from the remark made before the proposition.

(3) The roots of $\sqrt{\operatorname{disc}(K)}F_{\mathcal{B}}$ (with any choice for the square root) are by assumption the $(\alpha_i - \alpha_j : \beta_i - \beta_j)$ for $1 \le i < j \le 3$, and this respects the convention for the choice of roots made at the beginning. Hence one checks that

$$\begin{aligned} \operatorname{disc}(\sqrt{\operatorname{disc}(K)}F_{\mathcal{B}}) &= \Big(\big[(\alpha_1-\alpha_2)(\beta_2-\beta_3) - (\alpha_2-\alpha_3)(\beta_1-\beta_2)\big] \\ &\quad \cdot \big[(\alpha_2-\alpha_3)(\beta_3-\beta_1) - (\alpha_3-\alpha_1)(\beta_2-\beta_3)\big] \\ &\quad \cdot \big[(\alpha_3-\alpha_1)(\beta_1-\beta_2) - (\alpha_1-\alpha_2)(\beta_3-\beta_1)\big]\Big)^2 \\ &= \operatorname{disc}(K)^3 \ . \end{aligned}$$

So that $\operatorname{disc}(F_{\mathcal{B}}) = \operatorname{disc}(K)$ since, by the explicit formula for $\operatorname{disc}(F_{\mathcal{B}})$, we have $\operatorname{disc}(\lambda F_{\mathcal{B}}) = \lambda^4 \operatorname{disc}(F_{\mathcal{B}})$.

(4) This is the longest part of the proof. Let $F_{\mathcal{B}} = (a,b,c,d)$ with a, b, c, d in $\mathbb{Q}$ by (2). First, we note that if x and y are in $\mathbb{Z}$ then $\gamma = \beta x - \alpha y$ is in $\mathbb{Z}_K$, hence by the remark made above, $F_{\mathcal{B}}(x,y) = f$ where $f = [\mathbb{Z}_K : \mathbb{Z}[\gamma]]$ so $F_{\mathcal{B}}(x,y) \in \mathbb{Z}$. Applying this to $(x,y) = (1,0)$ and $(x,y) = (0,1)$ we deduce that $a \in \mathbb{Z}$ and $d \in \mathbb{Z}$. Then applying this to $(x,y) = (1,1)$ and $(x,y) = (1,-1)$ we deduce that $b+c \in \mathbb{Z}$ and $b-c \in \mathbb{Z}$. It follows that b and c belong to $\frac{1}{2}\mathbb{Z}$ with $b \equiv c \pmod 1$. Now, by (3) we know that $\operatorname{disc}(F_{\mathcal{B}}) = \operatorname{disc}(K)$ is an integer. By the explicit formula for $\operatorname{disc}(F_{\mathcal{B}})$ and using that b and c belong to $\frac{1}{2}\mathbb{Z}$ we obtain that $2\operatorname{disc}(F_{\mathcal{B}}) \equiv 2b^2c^2 \in \mathbb{Z}$. Since $b \equiv c \pmod 1$, we cannot have $b \equiv c \equiv \frac{1}{2} \pmod 1$, hence $b \equiv c \equiv 0 \pmod 1$, thus proving that $F_{\mathcal{B}}$ is integral.

Recall that by (1), if x and y are in $\mathbb{Z}$, we have $F_{\mathcal{B}}(x,y) = \pm f(\beta x - \alpha y)$, where for $\gamma \in \mathbb{Z}_K$, $f(\gamma) = [\mathbb{Z}_K : \mathbb{Z}[\gamma]]$. Now let δ be the GCD of the coefficients of $F_{\mathcal{B}}$. We thus have for each x, y in $\mathbb{Z}$, $\delta \mid f(\beta x - \alpha y)$. But since $f(\gamma + n) = f(\gamma)$ for any $n \in \mathbb{Z}$ and since $(1,\alpha,\beta)$ is an integral basis, it follows that for *any* $\gamma \in \mathbb{Z}_K$ we have $\delta \mid f(\gamma)$.

This means by definition that δ is an inessential discriminant divisor, and according to a theorem of Dedekind, for a cubic field this implies that either $\delta = 1$, or else $\delta = 2$ and 2 is totally split in K. Assume the latter. We thus have $F_{\mathcal{B}} = 2G$ for an integral cubic form G, and $\operatorname{disc}(G) = \operatorname{disc}(F_{\mathcal{B}})/16 = \operatorname{disc}(K)/16$ by (3). However since 2 is totally split in K, it is in particular unramified, hence $2 \nmid \operatorname{disc}(K)$, which is absurd since this implies that the integral cubic form G has non-integral discriminant. Thus we have $\delta = 1$ hence $F_{\mathcal{B}}$ is primitive.

Finally, let us show that $F_{\mathcal{B}}$ is irreducible. Since we are in the cubic case, this means that $F_{\mathcal{B}}(x,y)$ has no linear factor in $\mathbb{Q}[x,y]$. Assume the contrary. By definition of $F_{\mathcal{B}}$, we may assume that such a linear factor is proportional to $((\beta_1-\beta_2)x-(\alpha_1-\alpha_2)y)$. It follows that there exist integers r and s not both zero such that $s(\alpha_1-\alpha_2)=r(\beta_1-\beta_2)$, so that $s\alpha_1-r\beta_1=s\alpha_2-r\beta_2$. Taking conjugates, we see that we have $s\alpha_1-r\beta_1=s\alpha_2-r\beta_2=s\alpha_3-r\beta_3$, so that the conjugates of $s\alpha-r\beta$ are equal, hence by Galois theory $s\alpha-r\beta\in\mathbb{Q}$, and since r and s are not both zero, this is in contradiction with $(1,\alpha,\beta)$ being an integral basis. It follows that $F_{\mathcal{B}}$ is irreducible.

(5) Let $\mathcal{B}'=(1,\alpha',\beta')$ be another integral basis. This means that there exists integers A, B, C, D, E, F such that

$$\begin{pmatrix}\alpha'\\ \beta'\end{pmatrix}=\begin{pmatrix}A & B\\ C & D\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}+\begin{pmatrix}E\\ F\end{pmatrix}$$

with $AD-BC=\pm1$, since $(\alpha'-E,\beta'-F)$ and (α,β) must generate the same lattice. It follows that

$$\begin{aligned}\operatorname{disc}(\beta'x-\alpha'y)&=\operatorname{disc}((C\alpha+D\beta+F)x-(A\alpha+B\beta+E)y)\\&=\operatorname{disc}((C\alpha+D\beta)x-(A\alpha+B\beta)y)\\&=\operatorname{disc}(\beta(Dx-By)-\alpha(-Cx+Ay))\end{aligned}$$

where the second equality follows from $\operatorname{disc}(x+n)=\operatorname{disc}(x)$ for all $x\in K$ and $n\in\mathbb{Q}$. Since $AD-BC=\pm1$, it follows from (1) that $F_{\mathcal{B}'}=\pm F_{\mathcal{B}}\circ\gamma^{-1}$ with $\gamma=\left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right)$, so $F_{\mathcal{B}'}$ and $F_{\mathcal{B}}$ are equivalent.

(6) This follows from a straightforward but tedious computation. ∎

Conversely, given an integral primitive irreducible binary cubic form F, we can define a number field K_F associated to F by $K_F=\mathbb{Q}(\theta)$ where θ is any root of $F(x,1)$. Since F is irreducible, θ is an algebraic number of degree exactly equal to 3, so K_F is a cubic field. Choosing another root of F gives an isomorphic (in fact conjugate) field K_F, hence the isomorphism class of K_F is well defined. Finally, if F and G are equivalent under $\mathrm{GL}_2(\mathbb{Z})$, K_F and K_G are clearly again conjugate.

It follows that if we let $\mathcal{C}$ be the set of isomorphism classes of cubic number fields we have defined maps $\phi_{\mathcal{C}\Phi}:\ K\mapsto F_K$ from $\mathcal{C}$ to Φ and $\phi_{\Phi\mathcal{C}}:\ F\mapsto K$ from Φ to $\mathcal{C}$.

Proposition 2.2. *We have $\phi_{\Phi\mathcal{C}}\circ\phi_{\mathcal{C}\Phi}=1$, hence $\phi_{\mathcal{C}\Phi}$ is injective and $\phi_{\Phi\mathcal{C}}$ is surjective.*

Proof. Let K be a cubic field and $(1,\alpha,\beta)$ an integral basis. We have (for example) $K_{F_K}=\mathbb{Q}((\alpha_2-\alpha_3)/(\beta_2-\beta_3))\subset K^{\mathrm{Gal}}$. If K is a Galois cubic field, then $K_{F_K}=K$. Otherwise, K^{Gal} is a number field of degree 6, with Galois group isomorphic to S_3, and $(\alpha_2-\alpha_3)/(\beta_2-\beta_3)$ is fixed by the transposition (23) of order 2, hence belongs to a cubic subfield, and so K_{F_K} is isomorphic to K. In fact, by choosing the numbering such that $\alpha=\alpha_1$ and $\beta=\beta_1$, K_{F_K} is even *equal* to K, not only conjugate to it. Note also that we cannot have $(\alpha_2-\alpha_3)/(\beta_2-\beta_3)\in\mathbb{Q}$ otherwise F_K would be reducible. ∎

Let $I\subset\Phi$ be the image of $\phi_{\mathcal{C}\Phi}$. It follows from this proposition that $\phi_{\mathcal{C}\Phi}$ and the restriction of $\phi_{\Phi\mathcal{C}}$ to I are inverse discriminant preserving bijections between

$\mathcal{C}$ and I, and this is the Davenport-Heilbronn correspondence that we are looking for. There now remains to determine the image I.

Before doing so, we will show that the form F_K determines the simple invariants of a cubic number field.

Proposition 2.3. *Let K be a cubic field, $F_K = (a, b, c, d)$ the associated cubic form, θ a root of F_K such that $K = \mathbb{Q}(\theta)$ (we have seen above that such a θ exists). Then:*

(1) $\mathrm{disc}(K) = \mathrm{disc}(F_K)$.
(2) $(1, a\theta, a\theta^2 + b\theta)$ *is an integral basis of* $\mathbb{Z}_K$.
(3) *A prime $p \in \mathbb{Z}$ decomposes in K as F decomposes in $\mathbb{F}_p[X, Y]$. More precisely, if*

$$F_K(X, Y) \equiv \prod_{1 \le i \le g} \overline{T_i}^{e_i}(X, Y) \pmod{p}$$

is a decomposition of F into irreducible homogeneous factors in $\mathbb{F}_p[X, Y]$ then we have

$$p\mathbb{Z}_K = \prod_{1 \le i \le g} \mathfrak{p}_i^{e_i}$$

where the $\mathfrak{p}_i$ are distinct prime ideals of $\mathbb{Z}_K$ given as follows. Call T_i any lift of $\overline{T_i}$ in $\mathbb{Z}[X, Y]$ and set $d_i = \mathrm{degree}(\overline{T_i})$.

If $p \nmid a$, then

$$\mathfrak{p}_i = p\mathbb{Z}_K + T_i(\theta, 1)\mathbb{Z}_K \ .$$

If $p \mid a$ but $p \nmid d$, then

$$\mathfrak{p}_i = p\mathbb{Z}_K + T_i(\theta, 1)/\theta^{d_i}\mathbb{Z}_K \ .$$

If $p \mid a$, $p \mid d$, then if $p \neq 2$ or $F(X, Y) \not\equiv X^2Y + XY^2 \pmod{2}$ there exists $C \in \mathbb{Z}$ such that $C \not\equiv 0$ and $C \not\equiv -b/c \pmod{p}$ (any $C \not\equiv 0 \pmod{p}$ if $p \mid c$), and then

$$\mathfrak{p}_i = p\mathbb{Z}_K + T_i(\theta, 1)/(1 - C\theta)^{d_i}\mathbb{Z}_K \ .$$

Finally, if $p = 2$ and $F(X, Y) \equiv X^2Y + XY^2 \pmod{2}$, we can take

$$p_1 = 2\mathbb{Z}_K + a\theta\mathbb{Z}_K, \ \mathfrak{p}_2 = 2\mathbb{Z}_K + (a\theta^2 + b\theta + 1)\mathbb{Z}_K \quad \textit{and}$$

$$\mathfrak{p}_3 = 2\mathbb{Z}_K + (a\theta^2 + (a + b)\theta)\mathbb{Z}_K \ .$$

Proof. (1) has been proved in the preceding section.

(2) θ is a root of $a\theta^3 + b\theta^2 + c\theta + d = 0$. It follows from [3], Chapter 4 Exercise 15, and easily checked anyhow, that $\mathcal{O} = \{x + ya\theta + z(a\theta^2 + b\theta),\ x, y, z \in \mathbb{Z}\}$ is an order in K, *i.e* it is an algebra and a $\mathbb{Z}$-module of finite type, and in particular is a suborder of the maximal order $\mathbb{Z}_K$. If θ_i denotes the 3 roots of $F_K(x, 1)$, an easy computation shows that

$$\mathrm{disc}(\mathcal{O}) = a^4 \prod_{1 \le i < j \le 3} (\theta_i - \theta_j)^2 = \mathrm{disc}(F_K) = \mathrm{disc}(\mathbb{Z}_K)$$

hence $\mathcal{O} = \mathbb{Z}_K$.

(3) Assume first that $p \nmid a$. Set

$$f(X) = a^2 F_K(X/a, 1) = X^3 + bX^2 + acX + a^2 d \ .$$

Then f is a monic irreducible polynomial over $\mathbb{Q}$ with a root $a\theta \in K$.

Now $\mathbb{Z}[a\theta] \subset \mathbb{Z}_K$ and

$$\operatorname{disc}(\mathbb{Z}[a\theta]) = a^6 \prod_{1 \le i < j \le 3} (\theta_i - \theta_j)^2 = a^2 \operatorname{disc}(\mathbb{Z}_K)$$

so $[\mathbb{Z}_K : \mathbb{Z}[a\theta]] = a$ (this also follows directly from (2)). Since p does not divide the index of $\mathbb{Z}[a\theta]$, it follows from basic algebraic number theory that $p\mathbb{Z}_K = \prod_{1 \le i \le g} \mathfrak{p}_i^{e_i}$, where $\mathfrak{p}_i = p\mathbb{Z}_K + U_i(a\theta)\mathbb{Z}_K$, where $f \equiv \prod_{1 \le i \le g} \overline{U_i}^{e_i} \pmod{p}$ is an irreducible decomposition of f in $\mathbb{F}_p[X]$.

But then

$$F_K(X,Y) = Y^3 F_K(X/Y, 1) = Y^3/a^2 f(aX/Y) \equiv \prod_{1 \le i \le g} \epsilon_i (Y^{d_i} U_i(aX/Y))^{e_i} \pmod{p}$$

for some $\epsilon_i \in \mathbb{F}_p^*$ and so $T_i(X,Y) = \epsilon_i Y^{d_i} U_i(aX/Y)$ and $T_i(\theta, 1) = \epsilon_i U_i(a\theta)$. Finally, we note that for $\epsilon \not\equiv 0 \pmod{p}$, we have

$$p\mathbb{Z}_K + \alpha\mathbb{Z}_K = p\mathbb{Z}_K + \epsilon\alpha\mathbb{Z}_K \ ,$$

and the case where $p \nmid a$ follows.

Assume now that $p \mid a$. If we can find a matrix $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ such that $G = F_K \circ M = (a', b', c', d')$ is such that $p \nmid a'$, we can apply the preceding case since K is also generated by a root of G.

One easily checks that if $p \mid a$ but $p \nmid d$ we can take $M = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and if $p \mid a$, $p \mid d$ but either $p \neq 2$ or $F_K(X,Y) \not\equiv X^2Y + XY^2 \pmod{2}$ then there exists $C \in \mathbb{Z}$ such that $C \not\equiv 0$ and $C \not\equiv -b/c \pmod{p}$ (any $C \not\equiv 0 \pmod{p}$ if $p \mid c$), and we then take $M = \left(\begin{smallmatrix} 1 & 0 \\ C & 1 \end{smallmatrix}\right)$. This immediately gives the formulas of the proposition.

Finally, if $p = 2$ and $F_K(X,Y) \equiv X^2Y + XY^2 \pmod{2}$, then 2 divides the coefficient of x^3 of any form equivalent to F_K, and from the definition of F_K this means that 2 divides the index of any $\alpha \in \mathbb{Z}_K$, in other words that it is an inessential discriminantal divisor. We then know that 2 is totally split, and hence 2 still factors as $F_K \equiv XY(X+Y)$ modulo 2. To find the factors explicitly, we must split the étale algebra $\mathbb{A} = \mathbb{Z}_K/2\mathbb{Z}_K \simeq (\mathbb{Z}/2\mathbb{Z})^3$. All its elements are thus idempotents. If we set $e_1 = 1$, $e_2 = a\theta$ and $e_3 = a\theta^2 + b\theta$ considered as elements of $\mathbb{A}$ (they are in $\mathbb{Z}_K$, see above), we check that $e_2 e_3 = a^2\theta^3 + ab\theta^2 = -ac\theta - ad = a\theta = e_2$ in $\mathbb{A}$ since c is odd and a and d even. It follows that e_2, $e_1 + e_3$ and $e_2 + e_3$ are orthogonal idempotents of sum 1, thus giving the desired splitting of $\mathbb{A}$, hence of $p\mathbb{Z}_K$. $\square$

3. Algorithmic Characterization of the set U

We will now introduce a set U of cubic forms, and study some of its properties. In the next section, we will prove that U is the sought after image I of the Davenport-Heilbronn correspondence.

We first need some notation. For a prime p, we let V_p be the set of $F \in \Phi$ such that $p^2 \nmid \operatorname{disc}(F)$ if $p \neq 2$ or $\operatorname{disc}(F) \equiv 1 \pmod 4$ or $\operatorname{disc}(F) \equiv 8$ or $12 \pmod{16}$ if $p = 2$. In other words, if $\operatorname{disc}(F) = d_k f^2$ with d_k a fundamental discriminant, $F \in V_p$ if and only if $p \nmid f$.

In particular $\bigcap_p V_p$ is the set of fundamental discriminants, *i.e* of discriminants of quadratic fields.

Furthermore, let U_p be the set of $F \in \Phi$ such that either $F \in V_p$, or else

$$F(x, y) \equiv \lambda(\delta x - \gamma y)^3 \pmod p$$

for some $\lambda \in \mathbb{F}_p^*$ and x, y in $\mathbb{F}_p$ not both zero, and in addition $F(\gamma, \delta) \not\equiv 0 \pmod{p^2}$.

We will summarize the condition $F(x, y) \equiv \lambda(\delta x - \gamma y)^3 \pmod p$ for some $\lambda \in \mathbb{F}_p^*$ by saying that F has three identical roots in $\mathbb{F}_p$, and we will write $(F, p) = (1^3)$.

Finally, we set $U = \bigcap_p U_p$. The Davenport-Heilbronn theorem states that $U = I$, the image of the map $\phi_{\mathcal{C}\Phi}$ that we are looking for. Before proving this theorem, we must study in detail the set U.

Fot this, a very useful notion is that of the *Hessian* of a form F.

Definition 3.1. *Let $F = (a, b, c, d)$ be a cubic form. We define the Hessian of F by the formula*

$$H_F(x, y) = -\frac{1}{4} \begin{vmatrix} \frac{\partial^2 F}{\partial x \partial x} & \frac{\partial^2 F}{\partial x \partial y} \\ \frac{\partial^2 F}{\partial y \partial x} & \frac{\partial^2 F}{\partial y \partial y} \end{vmatrix} = Px^2 + Qxy + Ry^2 \ .$$

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

Proposition 3.2. *Let $F = (a, b, c, d)$ be a cubic form and $H_F = (P, Q, R)$ its Hessian.*

1. *For any $M \in \mathrm{GL}_2(\mathbb{C})$ we have $H_{F \circ M} = H_F \circ M$.*
2. $\operatorname{disc}(H_F) = -3 \operatorname{disc}(F)$.
3. $F(Q, -2P) = \operatorname{disc}(F)(2bP - 3aQ)$.
4. $3dP - cQ + bR = 3aR - bQ + cP = 0$.

These formulas are easily proved by a direct computation. □

We are now ready to give an algorithmic description of the set U. We need two propositions.

Proposition 3.3. *Let $F = (a, b, c, d)$ be a* primitive *form, and let $H_F = (P, Q, R)$ its Hessian. Recall that we write $(F, p) = (1^3)$ if F has a triple root in $\mathbb{F}_p$. Then*

1. *$p \mid \operatorname{disc}(F)$ if and only if F has at least a double root in $\overline{\mathbb{F}_p}$, and if this is the case all the roots of F are in fact in $\mathbb{F}_p$ itself.*
2. *$(F, p) = (1^3)$ if and only if $p \mid \gcd(P, Q, R)$.*
3. *If $(F, p) = (1^3)$ and $p \neq 3$, then $F \in U_p$ if and only if $p^3 \nmid \operatorname{disc}(F)$. If $F \in U_3$ then $3^6 \nmid \operatorname{disc}(F)$.*
4. *If $(F, 3) = (1^3)$ then we have the following:*
   If $3 \mid a$, then $F \in U_3 \iff 9 \nmid a$.
   If $3 \nmid a$ but $3 \mid d$, then $F \in U_3 \iff 9 \nmid d$.
   If $3 \nmid a$ and $3 \nmid d$, then there exists $\epsilon = \pm 1$ such that $3 \mid (a - \epsilon d)$, and then $F \in U_3 \iff 9 \nmid ((a + c) - \epsilon(b + d))$.

Proof. (1) Assume that $p \mid \operatorname{disc}(F)$. We know that any polynomial in one variable over $\mathbb{F}_p$ can be written as $\prod_{i\geq 1} A_i^i$ where $A_i \in \mathbb{F}_p[X]$ are pairwise coprime and squarefree polynomials, and essentially in a unique manner (up to multiplication of each A_i by suitable constants). This result can be homogenized and transformed into an identical one for homogeneous polynomials in 2 variables.

Since $p \mid \operatorname{disc}(F)$, by definition of the discriminant this means that F has at least a double root in $\mathbb{P}_1(\overline{\mathbb{F}_p})$, in other words in the decomposition above there exists $i > 1$ such that A_i is not equal to a constant. Since F is of degree 3, this means that $F = A_3^3$ or else $F = A_1 A_2^2$ with A_1, A_2 and A_3 of degree 1. It follows in particular that all the roots of F modulo p are in $\mathbb{F}_p$ itself.

(2) We have just seen that if $p \mid \operatorname{disc}(F)$ then all the roots of F are in $\mathbb{F}_p$ and there is at least a double root. Hence write

$$F(x,y) \equiv (\delta x - \gamma y)^2(\beta x - \alpha y) \pmod{p}\ .$$

Then one finds that

$$H(x,y) \equiv (\delta x - \gamma y)^2(\alpha\delta - \beta\gamma)^2 \pmod{p}\ .$$

Now since F is primitive, γ and δ cannot both be zero modulo p, hence

$$H(x,y) \equiv 0 \pmod{p} \iff \alpha\delta - \beta\gamma \equiv 0 \pmod{p} \iff (F,p) = (1^3)\ .$$

On the other hand, if $p \nmid \operatorname{disc}(F)$ then we cannot have $p \mid \gcd(P,Q,R)$ otherwise $p^2 \mid \operatorname{disc}(H_F) = -3\operatorname{disc}(F)$ so $p \mid \operatorname{disc}(F)$, absurd.

(3) From now on we assume that $(F,p) = (1^3)$. Replacing F by an equivalent form G, we may assume that the triple root of G modulo p is at $(0:1)$, *i.e* that $G = (A,B,C,D) \equiv (A,0,0,0) \pmod{p}$ for some $A \in \mathbb{Z}$. This implies that $\operatorname{disc}(G) \equiv -27A^2D^2 \pmod{p^3}$. Since G is primitive, we have $p \nmid A$.

Assume first $p \neq 3$. We thus have

$$p^3 \mid \operatorname{disc}(G) \iff p^2 \mid D \iff p^2 \mid G(0,1) \iff G \notin U_p$$

by definition of U_p.

We could also have written $F(x,y) = \lambda(\delta x - \gamma y)^3 + pF_1(x,y)$ for an integral form F_1, from which we obtain $\operatorname{disc}(F) \equiv -27\lambda^2 F_1^2(\gamma,\delta)p^2 \pmod{p^3}$, which immediately implies the result.

Now assume $p = 3$ and that $F \in U_3$, or equivalently that $9 \nmid D$. Then $\operatorname{disc}(G) \equiv -4AC^3 \pmod{3^4}$, hence $3^2 \mid C$, so $\operatorname{disc}(G) \equiv -4B^3D \pmod{3^5}$, hence $3^2 \mid B$, so finally $\operatorname{disc}(G) \equiv -27A^2D^2 \not\equiv 0 \pmod{3^6}$.

(4) Assume $p = 3$ and that $(F,3) = (1^3)$. Then since $F(x,y) \equiv \lambda(\delta x - \gamma y)^3 \pmod{3}$, we see that $3 \mid b$ and $3 \mid c$. It follows that

$$F(-d,a) \equiv -ad^3 + da^3 \equiv -ad + da \equiv 0 \pmod{3}\ ,$$

and since F is primitive we cannot have $3 \mid a$ and $3 \mid d$, so $(-d:a)$ is a root of F modulo 3, hence *the* root of F modulo 3. Hence $F \in U_3$ if and only if $F(-d,a) \not\equiv 0 \pmod{9}$. Since b and c are divisible by 3, the value of $F(x,y)$ modulo 9 depends only on x and y modulo 3, hence

$$F(-d,a) \equiv -\epsilon a^4 + ba^3 - c\epsilon a^3 + da^3$$

and the result follows. ◻

Proposition 3.4. *Let F be a primitive form. We can write* $\operatorname{disc}(F) = d_k f^2$ *with d_k a fundamental discriminant. Then $p \mid f$ if and only if either $(F,p) = (1^3)$, or if*

$$F(x,y) \equiv (\delta x - \gamma y)^2(\beta x - \alpha y) \pmod{p} \quad \text{and} \quad F(\gamma,\delta) \equiv 0 \pmod{p^2}\ .$$

Proof. An explicit computation show that $\operatorname{disc}(F)$ is a square modulo 4. Hence, it can always be written as $d_k f^2$. Assume first $p \mid f$. Then $p \mid \operatorname{disc}(F)$ and so we can write

$$F(x,y) = (\delta x - \gamma y)^2(\beta x - \alpha y) + pF_1(x,y)$$

with F_1 integral.

Assume $p \neq 2$. A computation shows that

$$\operatorname{disc}(F) \equiv 4p(\alpha\delta - \beta\gamma)^3 F_1(\gamma,\delta) \pmod{p^2}\ .$$

Since $p \mid f$ we have $p^2 \mid \operatorname{disc}(F)$ hence if $p \neq 2$, either $p \mid (\alpha\delta - \beta\gamma)$, *i.e* $(F,p) = (1^3)$, or $p \mid F_1(\gamma,\delta)$, *i.e* $F(\gamma,\delta) \equiv 0 \pmod{p^2}$.

Assume now that $p = 2$. If $F_1 = (a_1, b_1, c_1, d_1)$, we have

$$\operatorname{disc}(F) \equiv 8(\alpha\delta - \beta\gamma)^3 F_1(\gamma,\delta) + 4((a_1\alpha + b_1\beta)\gamma^2 + (c_1\alpha + d_1\beta)\delta^2)^2 \pmod{16}\ .$$

Since $2 \mid f$, $\operatorname{disc}(F) = d_k f^2 \equiv 0$ or $4 \pmod{16}$. Since the square of an integer is congruent to 0 or 1 modulo 4, it follows that

$$8(\alpha\delta - \beta\gamma)^3 F_1(\gamma,\delta) \equiv -4,\ 0 \text{ or } 4 \pmod{16}\ ,$$

in other words $(\alpha\delta - \beta\gamma)^3 F_1(\gamma,\delta) \equiv 0 \pmod{2}$, hence once again either $(F,2) = (1^3)$ or $2 \mid F_1(\gamma,\delta)$ as before.

Conversely, assume that either $(F,p) = (1^3)$ or $F(\gamma,\delta) \equiv 0 \pmod{p^2}$. If $(F,p) = (1^3)$, then since F is primitive, by Proposition 3.3 (2), we have $p \mid \gcd(P,Q,R)$.

Assume first $p > 3$. Then $p^2 \mid \operatorname{disc}(H_F) = -3\operatorname{disc}(F)$, hence $p^2 \mid \operatorname{disc}(F)$, so $p \mid f$.

Assume now that $p = 2$. Then $H_F = 2H'$ for some other quadratic form H', hence $\operatorname{disc}(H_F)/4 \equiv 0$ or $1 \pmod{4}$, hence the same is true for $\operatorname{disc}(F) = \operatorname{disc}(H_F)/(-3)$ and hence $2 \mid f$.

Finally, assume that $p = 3$. From the explicit formulas, $p \mid \gcd(P,Q,R)$ is equivalent to $3 \mid b$ and $3 \mid c$, from which it follows by the formula for the discriminant that $27 \mid \operatorname{disc}(F)$, and in particular $3 \mid f$.

Assume now that $F(x,y) \equiv (\delta x - \gamma y)^2(\beta x - \alpha y) \pmod{p}$, and $F(\gamma,\delta) \equiv 0 \pmod{p^2}$. We may assume that $\alpha\delta - \beta\gamma \not\equiv 0 \pmod{p}$, otherwise we are in the case $(F,p) = (1^3)$ which we have just dealt with.

By the same reasoning as before, writing $F(x,y) = (\delta x - \gamma y)^2(\beta x - \alpha y) + pF_1(x,y)$, we have

$$\operatorname{disc}(F) \equiv 4p(\alpha\delta - \beta\gamma)^3 F_1(\gamma,\delta) \pmod{p^2}\ .$$

Hence $F(\gamma,\delta) \equiv 0 \pmod{p^2}$ is equivalent to $F_1(\gamma,\delta) \equiv 0 \pmod{p}$ which implies $\operatorname{disc}(F) \equiv 0 \pmod{p^2}$, hence if $p > 2$ we have $p \mid f$.

For $p = 2$ and $F_1 = (a_1, b_1, c_1, d_1)$, we have as before

$$\operatorname{disc}(F) \equiv 8(\alpha\delta - \beta\gamma)^3 F_1(\gamma,\delta) + 4((a_1\alpha + b_1\beta)\gamma^2 + (c_1\alpha + d_1\beta)\delta^2)^2 \pmod{16}\ ,$$

and since $F_1(\gamma,\delta) \equiv 0 \pmod{2}$, we deduce that

$$\operatorname{disc}(F)/4 \equiv ((a_1\alpha + b_1\beta)\gamma^2 + (c_1\alpha + d_1\beta)\delta^2)^2 \pmod{4}\ ,$$

and hence $2 \mid f$, thus finishing the proof of the proposition. □

Corollary 3.5. *Let F be a primitive cubic form and p be a prime. Then $F \notin U_p$ if and only if F has at least a double root $(\gamma : \delta)$ modulo p, and $F(\gamma, \delta) \equiv 0 \pmod{p^2}$.*

Proof. If $F \notin U_p$, then in particular $F \notin V_p$, hence $p \mid f$, and so by Proposition 3.4, either $F(\gamma, \delta) \equiv 0 \pmod{p^2}$ if F has a double root, or $(F, p) = (1^3)$ but then by definition of U_p, we again have $F(\gamma, \delta) \equiv 0 \pmod{p^2}$. Conversely, if F has at least a double root $(\gamma : \delta)$ modulo p, and $F(\gamma, \delta) \equiv 0 \pmod{p^2}$, then if it is a triple root, by definition $F \notin U_p$, and if it is only a double root, by Proposition 3.4 we have $p \mid f$, hence $F \notin V_p$, hence $F \notin U_p$. Note that when (γ, δ) is at least double root modulo p, it is easily checked that the condition $F(\gamma, \delta) \equiv 0 \pmod{p^2}$ depends only on γ and δ modulo p. □

4. The Heilbronn-Davenport Theorem

We first recall the following results from algebraic number theory.

Proposition 4.1. *Let K be a cubic number field of discriminant* $\operatorname{disc}(K)$, *and write* $\operatorname{disc}(K) = d_k f^2$ *where d_k is a fundamental discriminant (including 1). Then:*

(1) *$p \mid f$ if and only if p is totally ramified, i.e if and only if $p\mathbb{Z}_K = \mathfrak{p}^3$.*
(2) *$p \mid (d_k, f)$ implies $p = 3$.*
(3) *$p^2 \mid f$ implies $p = 3$.*

See [7] for a proof.

We can now state and prove the theorem of Davenport-Heilbronn.

Theorem 4.2. *We have $I = \operatorname{Im}(\phi_{\mathcal{C}\Phi}) = U$. In other words, the maps $\phi_{\mathcal{C}\Phi}$ and $\phi_{\Phi\mathcal{C}}$ are discriminant preserving inverse bijections between isomorphism classes of cubic fields and binary cubic forms belonging to U.*

Proof. Let K be a cubic number field, and F_K the image by $\phi_{\mathcal{C}\Phi}$ of K. We will first show that $F_K \in U$. As in Proposition 4.1, write $\operatorname{disc}(F_K) = \operatorname{disc}(K) = d_k f^2$ with d_k a fundamental discriminant.

Let p be a prime. If $p \nmid f$, then $F_K \in V_p \subset U_p$, so $F_K \in U_p$. Hence we now assume that $p \mid f$.

By Proposition 4.1 (1), it follows that p is totally ramified. By Proposition 2.3, this means that F_K splits as the cube of a linear form, *i.e* that $(F_K, p) = (1^3)$. We consider three cases.

• $p > 3$. In this case, it follows from Proposition 4.1 (2) and (3) that $p^3 \nmid \operatorname{disc}(K)$, hence that $F_K \in U_p$ by Proposition 3.3 (3).

• $p = 2$. Since $2 \mid f$, we have $2 \nmid d_k$ by Proposition 4.1 (2), hence by Proposition 4.1 (3) we deduce that $2^3 \nmid \operatorname{disc}(K)$ hence $F_K \in U_2$ as before.

• $p = 3$. This is the only difficult case. Since 3 cannot be a nonessential discriminantal divisor, there exists $\gamma \in \mathbb{Z}_K \setminus \mathbb{Q}$ such that $3 \nmid [\mathbb{Z}_K : \mathbb{Z}[\gamma]]$. Now since 3 is totally ramified, write $3\mathbb{Z}_K = \mathfrak{p}^3$ for a prime ideal $\mathfrak{p}$ of degree 1. Since $\mathbb{Z}_K/\mathfrak{p}$ is isomorphic to $\mathbb{F}_3$, we have $\gamma^3 \equiv \gamma \pmod{\mathfrak{p}}$, hence either γ, $\gamma - 1$ or $\gamma + 1$ belongs to $\mathfrak{p}$. Replacing if necessary γ by $\gamma - 1$ or $\gamma + 1$ (which does not change the property $3 \nmid [\mathbb{Z}_K : \mathbb{Z}[\gamma]]$, we may assume that $\gamma \in \mathfrak{p}$.

We clearly have

$$\operatorname{disc}(\gamma^2) = \operatorname{disc}(\gamma)((\gamma + \gamma')(\gamma + \gamma'')(\gamma' + \gamma''))^2 = \operatorname{disc}(\gamma)\mathcal{N}^2(\operatorname{Tr}(\gamma) - \gamma) \ .$$

Assume first that $\gamma \in \mathfrak{p}^2$. Thus $\gamma^2/3$ has non-negative valuation for every prime ideal except perhaps those above 3, but the only prime ideal above 3 is $\mathfrak{p}$ and the $\mathfrak{p}$-adic valuation of $\gamma^2/3$ is at least equal to 1, hence $\gamma^2/3 \in \mathbb{Z}_K$. By the above formula we have $3^6 \operatorname{disc}(\gamma^2/3)/\operatorname{disc}(K) = \operatorname{disc}(\gamma)/\operatorname{disc}(K)\,\mathcal{N}^2(\operatorname{Tr}(\gamma)-\gamma)$, and since $3 \nmid \operatorname{disc}(\gamma)/\operatorname{disc}(K) = [\mathbb{Z}_K : \mathbb{Z}[\gamma]]^2$, it follows that $3^3 \mid \mathcal{N}(\operatorname{Tr}(\gamma)-\gamma)$. Since $\mathfrak{p}$ is the only prime ideal above 3, this means that the $\mathfrak{p}$-adic valuation of $\operatorname{Tr}(\gamma)-\gamma$ is at least equal to 3, hence that $\operatorname{Tr}(\gamma)-\gamma \in \mathfrak{p}^3 = 3\mathbb{Z}_K$, in other words that $3 \mid \operatorname{Tr}(\gamma)-\gamma$. Now since $3 \nmid [\mathbb{Z}_K : \mathbb{Z}[\gamma]]$, 3 splits in K as the characteristic polynomial $A(X)$ of γ splits modulo 3. It follows that $A(X) \equiv (X-u)^3 \pmod 3$ for a certain $u \in \mathbb{F}_3$. Write

$$A(X) = X^3 - \operatorname{Tr}(\gamma)X^2 + S(\gamma)X - \mathcal{N}(\gamma)\ .$$

We thus have $3 \mid \operatorname{Tr}(\gamma)$ and $3 \mid S(\gamma)$. Since $3 \mid \operatorname{Tr}(\gamma)-\gamma$ we have $3 \mid \gamma$. But this is absurd since we would then have

$$3 \mid [\mathbb{Z}[\gamma/3] : \mathbb{Z}[\gamma]] \mid [\mathbb{Z}_K : \mathbb{Z}[\gamma]]\ .$$

Thus $\gamma \notin \mathfrak{p}^2$. Since we still have $3 \mid \operatorname{Tr}(\gamma)$ and $3 \mid S(\gamma)$ we obtain

$$\begin{aligned}\mathcal{N}(\operatorname{Tr}(\gamma)-\gamma) &= (\operatorname{Tr}(\gamma)-\gamma)(\operatorname{Tr}(\gamma)-\gamma')(\operatorname{Tr}(\gamma)-\gamma'') \\ &= -\mathcal{N}(\gamma) + \operatorname{Tr}(\gamma)S(\gamma) \equiv -\mathcal{N}(\gamma) \pmod 9\ ,\end{aligned}$$

and since $v_{\mathfrak{p}}(\gamma) = 1$ we have $v_3(\mathcal{N}(\gamma)) = 1$ so $\mathcal{N}(\gamma) \equiv \pm 3 \pmod 9$. Furthermore by our choice of γ we have

$$\operatorname{disc}(\gamma)/\operatorname{disc}(K) = [\mathbb{Z}_K : \mathbb{Z}[\gamma]]^2 \equiv 1 \pmod 3$$

hence

$$\operatorname{disc}(\gamma^2)/\operatorname{disc}(K) = \operatorname{disc}(\gamma)\,\mathcal{N}^2(\operatorname{Tr}(\gamma)-\gamma) \equiv 9 \pmod{27}\ .$$

Let $(1, \alpha, \beta)$ be the integral basis used to define the form F_K. Thus $\gamma^2 = \beta u - \alpha v + w$ for some u, v and w in $\mathbb{Z}$, and hence by definition we have $F_K(u, v) \equiv \pm 3 \pmod 9$. We have the following lemma:

Lemma 4.3. *Assume that F is a primitive cubic form and p a prime such that $(F, p) = (1^3)$. Then $F \in U_p$ if and only if there exists $(u, v) \in \mathbb{Z}^2$ such that $F(u, v) = ep$ with $p \nmid e$.*

Assuming this lemma for a moment, we see that since $F_K(x, y)$ represents an integer congruent to ± 3 modulo 9, we have $F_K \in U_3$, thus finishing the proof that $F \in U$.

Let us prove the lemma. By lifting the condition $(F, p) = (1^3)$ to $\mathbb{Z}$, we can write

$$F(x, y) = \lambda(\delta x - \gamma y)^3 + pG(x, y)$$

with λ, γ, δ in $\mathbb{Z}$ and G an integral cubic form. Then $F \in U_p$ if and only if $p \nmid G(\gamma, \delta)$. Thus if $F \in U_p$ we have $F(\gamma, \delta) = ep$ with $e = G(\gamma, \delta) \not\equiv 0 \pmod p$.

Conversely, assume that there exists $(u, v) \in \mathbb{Z}^2$ such that $F(u, v) = ep$ with $p \nmid e$. Then $F(u, v) \equiv 0 \pmod p$, hence $\lambda(\delta u - \gamma v) \equiv 0 \pmod p$. Since F is primitive, $p \nmid \lambda$ hence $\delta u - \gamma v \equiv 0 \pmod p$. Again F being primitive, γ and δ cannot both be divisible by p, from which it follows that there exists μ such that

$\gamma \equiv \mu u \pmod{p}$ and $\delta \equiv \mu v \pmod{p}$, and since $p \nmid e$ we have $p \nmid \mu$. But then $ep = F(u,v) \equiv pG(u,v) \pmod{p^3}$ hence $G(u,v) \equiv e \pmod{p^2}$ and so $G(\gamma,\delta) \equiv \mu^3 G(u,v) \equiv \mu^3 e \not\equiv 0 \pmod{p}$, so $F \in U_p$, thus proving the lemma. □

To finish the proof of the Davenport-Heilbronn Theorem 4.2, we must now prove that if $F \in U$, there exists a cubic field K such that F is equivalent to F_K. For this, we introduce a definition.

Definition 4.4. *We will say that two cubic forms F_1 and F_2 are* rationally equivalent *if there exists $M \in \mathrm{GL}_2(\mathbb{Q})$ such that $F_1 \circ M = \lambda F_2$ for $\lambda \in \mathbb{Q}^*$.*

We first show the following lemma.

Lemma 4.5. *Let F be any form in Φ (i.e primitive and irreducible). Then there exists a number field K such that F is rationally equivalent to F_K.*

Proof. In some algebraic closure of $\mathbb{Q}$, write $F = a(x-\lambda y)(x-\lambda' y)(x-\lambda'' y)$. Since F is irreducible, λ is a cubic irrationality, and we will take $K = \mathbb{Q}(\lambda)$. Write $F_K = a_K(x-\nu y)(x-\nu' y)(x-\nu'' y)$ so that $\nu \in K$ (we have seen above that this is always possible). Since K is a $\mathbb{Q}$-vector space of dimension 3, there exist 4 integers k, l, m and n not all zero such that $l + k\lambda - n\nu - m\lambda\nu = 0$. Taking conjugates, we obtain the same equality with $'$ and $''$. Using $\lambda = (\nu n - l)/(k - \nu m)$, we obtain

$$F_K(kx+ly, mx+ny) = \rho(x-\lambda y)(x-\lambda' y)(x-\lambda'' y) = (\rho/a)F$$

with $\rho = a_K \mathcal{N}(k - \nu m) \in \mathbb{Q}$. Furthermore the determinant $kn - lm$ is nonzero since otherwise either λ or ν would be in $\mathbb{Q}$. Thus F_K is rationally equivalent to F. □

Finally, we have the following lemma.

Lemma 4.6. *Let F_1 and F_2 be two forms belonging to U. Then if F_1 and F_2 are rationally equivalent, they are equivalent.*

Since F_K belongs to U, it follows from Lemma 4.5 and this lemma that any form in U is equivalent to F_K for a certain K, and this finishes the proof of Davenport-Heilbronn's Theorem 4.2.

Proof. Assume that $F_1 \circ M = \lambda F_2$ for some $M \in \mathrm{GL}_2(\mathbb{Q})$ and $\lambda \in \mathbb{Q}^*$. Since we want to show that F_1 and F_2 are equivalent, we can replace them by equivalent forms. In other words, without changing the equivalence classes of F_1 and F_2 we may replace M by any matrix of the form UMV with U and V in $\mathrm{GL}_2(\mathbb{Z})$. The elementary divisor theorem (*i.e* the Smith normal form) tells us that we can choose U and V so that

$$UMV = \begin{pmatrix} \alpha m & 0 \\ 0 & \alpha \end{pmatrix} \quad (\alpha \in \mathbb{Q}^*,\ m \in \mathbb{Z}_{>0}) \ .$$

Replacing λ by $\alpha^3\lambda$, we may assume $\alpha = 1$. To summarize, by replacing F_1 and F_2 by equivalent forms and modifying λ and M, we may assume that $M = \left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with $m \in \mathbb{Z}_{>0}$.

If $m = 1$, then $F_1 = \lambda F_2$ and, since F_1 and F_2 are in U, they are primitive. Hence $\lambda = \pm 1$ so F_1 and F_2 are equivalent.

Otherwise, there exists a prime p such that $p \mid m$. Write $m = p^k m_0$ and $\lambda = p^l \lambda_0$ with m_0 and λ_0 prime to p (*i.e* of zero p-adic valuation). Since $p \mid m$ we have $k \geq 1$. Now, writing for $i = 1$ or 2, $F_i = (a_i, b_i, c_i, d_i)$, the equality $F_1(p^k m_0 x, y) = p^l \lambda_0 F_2(x, y)$ is equivalent to

$$\begin{cases} a_1 &= \tau_a p^{l-3k} a_2 \\ b_1 &= \tau_b p^{l-2k} b_2 \\ c_1 &= \tau_c p^{l-k} c_2 \\ d_1 &= \tau_d p^l d_2 \end{cases}$$

where the τ_x are rational numbers prime to p.

Assume $l - k > 0$, hence $l > k \geq 1$. Then $p \mid c_1$ and $p^2 \mid d_1$. If on the other hand $l - k \leq 0$ then $l \leq k$ hence $p \mid b_2$ and $p^2 \mid a_2$. Replacing $(F_1(x, y), F_2(x, y))$ by $(F_2(y, x), F_1(y, x))$ we obtain again $p \mid c_1$ and $p^2 \mid d_1$.

The formula for the discriminant implies $p^2 \mid \operatorname{disc}(F_1)$. If $p > 2$ this immediately implies $F_1 \notin V_p$. If $p = 2$, the formula for the discriminant shows that $\operatorname{disc}(F_1)/4 \equiv b_1^2 (c_1/2)^2 \pmod 4$ and this is congruent to 0 or 1 modulo 4, so $F_1 \notin V_2$.

Since $F_1 \in U_p$ we must have $(F_1, p) = (1^3)$, and $F_1(x, y) \equiv \lambda(\delta x - \gamma y)^3 \pmod p$ with $F_1(\gamma, \delta) \not\equiv 0 \pmod p)^2$. Since $p \nmid \lambda$, $p \mid d_1$ means that $p \mid \gamma$, hence $p \mid b_1 \equiv -3\lambda\delta^2\gamma \pmod p$. But then, since $p \mid \gamma$, $F_1(\gamma, \delta) \equiv 0 \pmod{p^2}$, contradiction. This finishes the proof of Lemma 4.6, and hence of Davenport-Heilbronn's Theorem 4.2. $\square$

As a consequence of this theorem and of the results of the previous section, we now have an effficient algorithm to test whether a cubic form corresponds to the image of a cubic field by the Davenport-Heilbronn map as follows

Algorithm 4.7. *Let $F = (a, b, c, d)$ be a cubic form. This algorithm outputs* `true` *or* `false` *according to whether F corresponds to the image of a cubic field by the Davenport-Heilbronn map.*

(1) *If F is not irreducible, return* `false`.
(2) *If F is not primitive, return* `false`.
(3) *Compute the Hessian $H_F = (P, Q, R)$ by the formulas given. Set $f = \gcd(P, Q, R)$, $D = 4PR - Q^2$ (so $D = 3\operatorname{disc}(F)$). Using Proposition 3.3, check that $F \in U_2$ and $F \in U_3$, otherwise return* `false`.
(4) *If $p^2 \mid f$ for some $p > 3$, return* `false`.
(5) *Set $t = D/f^2$. Remove all powers of 2 and 3 from t (in fact at most 2^3 and 3^2), and let again t be the result. If $\gcd(t, f) > 1$ return* `false`.
(6) *If t is squarefree return* `true`, *otherwise return* `false`.

Proof. Steps 1, 2 and 3 are clear since F_K is irreducible, primitive and belongs to U_p for all p.

If $p^2 \mid f$, then $p^4 \mid D = 3\operatorname{disc}(F)$. If $p \mid f$ and $p \mid D/f^2$, we have $p^3 \mid D$. It follows in both cases that if $p > 3$, we have $p^3 \mid \operatorname{disc}(F)$ so $F \notin U_p$ by Proposition 3.3, thus Steps 4 and 5.

Assume that for every prime $p > 3$, we have $p^2 \nmid f$ and $p \nmid \gcd(t, f)$, which is the situation at the beginning of Step 6. Then if t is not squarefree, there exists $p > 3$

such that $p^2 \mid t$ and hence $p \nmid f$. Since $p > 3$, it follows that $p^2 \mid \mathrm{disc}(F)$, hence that $p \mid f(F)$, denoting by $f(F)$ what we called "f" in the preceding sections, such that $\mathrm{disc}(F) = d_k f(F)^2$ for a fundamental discriminant d_k. But by Proposition 3.4, this means that either $(F, p) = (1^3)$, or else F has a double root $(\gamma : \delta)$ modulo p such that $F(\gamma, \delta) \equiv 0 \pmod{p^2}$. Since $p \nmid f$, by Propostion 3.3 (2), (F, p) is not of the form (1^3), hence (F, p) must be of the second form which means that $F \notin U_p$ as we have seen.

On the other hand if t is squarefree, then for every $p > 3$ we have either $p \nmid f$, and since $D = tf^2$ and $\gcd(t, f) = 1$, $p^2 \nmid \mathrm{disc}(F)$ so $F \in V_p \subset U_p$, or else $p \mid f$, but then $(F, p) = (1^3)$ by Proposition 3.3 (2), and since $\gcd(t, f) = 1$ we have $p \nmid t$ hence since $p^2 \nmid f$ we have $p^3 \nmid \mathrm{disc}(F)$ so $F \in U_p$ by Proposition 3.3 (3).

This terminates the proof of the algorithm. □

Remarks.

(1) Step 1 will in practice not be necessary since we will always use this algorithm with *reduced forms* (see later), which are automatically irreducible when they belong to U.

(2) Although Step 2 seems to be necessary, this is in fact not the case since nonprimitive forms will be excluded in the subsequent steps. Indeed, let p be a prime dividing all the coefficients of F. Then clearly $p^2 \mid f$. If $p > 3$, Step 4 will return `false`. Assume now $p = 2$ or $p = 3$. Then $F \notin V_p$ and F has at least a double root modulo p. If F has only a double and not a triple root, then $F \notin U_p$. On the other hand if F has a triple root, *i.e* if $(F, p) = (1^3)$ then $F(x, y) = \lambda(\delta x - \gamma y)^3$ with $\lambda \in \mathbb{F}_p^*$ and hence $p \mid \gcd(\delta^3, \gamma^3)$ so γ and δ are equal to zero modulo p, hence $F \notin U_p$.

(3) Even though it seems useful to include the unnecessary Step 2, it can be shown that on average it *slows* the algorithm, so in the final form thanks to the preceding remark we will suppress it.

We end this section by the following proposition.

Proposition 4.8. *Let K be a cubic number field, and as above write* $\mathrm{disc}(K) = d_k f^2$ *where d_k is a fundamental discriminant. Let F_K be the cubic form associated to K by the Davenport-Heilbronn map, and let $H_K = (P, Q, R)$ its Hessian. Finally, set $f_H = \gcd(P, Q, R)$. Then:*

(1) *$f_H = f$ or $f_H = 3f$ and apart from powers of 3, f and f_H are squarefree.*
(2) *If $f_H = 3f$ then $3 \mid f$.*
(3) *If $3 \| f$ then $f_H = 3f$.*
(4) *In particular $f \mid f_H$, f and f_H have the same prime divisors, and we can have $(v_3(f), v_3(f_H))$ only equal to* $(0, 0)$, $(1, 2)$, $(2, 2)$ *and* $(2, 3)$.

Proof. By Proposition 3.3 (2) we have $p \mid f_H$ iff $(F, p) = (1^3)$, and by Proposition 2.3 (3) this is true iff p is totally ramified, hence by Proposition 4.1 (1) iff $p \mid f$. Hence f and f_H have the same prime divisors. Let p be such a prime divisor. By Davenport-Heilbronn's theorem, $F_K \in U$ hence by Proposition 3.3 (3) we have $p^3 \nmid \mathrm{disc}(K)$ if $p \neq 3$, hence if $p \neq 3$ we have $p^2 \nmid f$ and $p \nmid d_k$, so up to powers of 3, f is squarefree, and since $f_H^2 \mid 3\,\mathrm{disc}(K) = d_k f^2$ we have $v_p(f_H^2) \leq 2$ hence up to powers of 3, f_H is also squarefree.

Assume now that $p = 3$ and that p divides f (hence also f_H). By Proposition 3.3 (3) we have $v_3(f) \leq 2$ and since $f_H^2 \mid 3\,\mathrm{disc}(K)$ we have $v_3(f_H) \leq 3$. Furthermore, if $v_3(f) = 1$ we have $v_3(f_H^2) \le 3^4$ hence $v_3(f_H) \le 2$. Finally, since $3 \mid (P, Q, R)$, using the explicit formulas in terms of the coefficients of the form F_K we see that $3 \mid b$ and $3 \mid c$, which implies $9 \mid (P, Q, R)$ hence $v_3(f_H) \ge 2$. This proves all the assertions of the proposition. □

5. Real cubic fields

We now would like to single out a unique representative of a cubic form $F \in U$, which we will call reduced. For this purpose, as in the quadratic case, we must now distinguish according to the signature of the corresponding cubic field. In this section, we assume that the field $K = K_F$ is totally real, or equivalently that $\operatorname{disc}(K) = \operatorname{disc}(F) > 0$.

Then the Hessian $\operatorname{disc}(H_F) = -3\operatorname{disc}(F) < 0$ is a (positive or negative) definite quadratic form for which the notion of reduction is well defined. We will essentially define F to be reduced when H_F is, but for this we must make a few technical modifications to the usual definitions.

Definition 5.1. *Let $H = (P, Q, R)$ be a quadratic form with real coefficients. We will say that H is* reduced *if $0 \le Q \le P \le R$ and $R > 0$ (to exclude the trivial case of the zero form).*

Note that this is stronger than the usual definition, which would be $|Q| \le P \le R$ with $Q \ge 0$ when one of the inequalities is an equality. The reason for the modification to the usual definition is that we must work with forms modulo $\mathrm{GL}_2(\mathbb{Z})$ and not only $\mathrm{SL}_2(\mathbb{Z})$.

That the above definition works follows from the following lemma.

Lemma 5.2. *Let $H = (P, Q, R)$ and $H' = (P', Q', R')$ be two reduced definite integral binary quadratic forms such that there exists $M \in \mathrm{GL}_2(\mathbb{Z})$ with $H \circ M = H'$. Then $H = H'$. Furthermore*

$$M = \begin{cases} \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \\ \text{or } \pm\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \text{if } P = R \\ \text{or } \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & \text{if } P = R \text{ and } Q = 0 \\ \text{or } \pm\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} & \text{if } P = Q \\ \text{or } \pm\begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}, \pm\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \pm\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} & \text{if } P = Q = R \\ \text{or } \pm\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & \text{if } Q = 0\ , \end{cases}$$

these cases being inclusive.

Proof. Since H and H' are equivalent, they have the same discriminant and represent the same integers. To say that H is reduced implies that P is the minimum of H on $\mathbb{Z}^2 - \{(0, 0)\}$ and that R is the second minimum, hence $P = P'$ and $R = R'$.

Equality of discriminants implies $Q = \pm Q'$, hence $Q = Q'$ since they are both nonnegative.

Let as usual $T = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ be the generators of the modular group $\mathrm{PSL}_2(\mathbb{Z})$, let $\mathcal{F}$ be the usual compact fundamental domain for the modular group in the upper half plane $\mathcal{H}$.

Let $H = (P, Q, R)$ be a definite binary quadratic form, $\tau \in \mathcal{H}$ and $\bar{\tau}$ the roots of $H(x, 1) = 0$. Since H is reduced in the usual sense, we have $\tau \in \mathcal{F}$.

Now let $M = \left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ be an automorphism of H.

If $M \in \mathrm{SL}_2(\mathbb{Z})$, then it fixes $\tau \in \mathcal{F}$, hence by the usual theory, is either $\pm I$, $\pm S$ (if $H = (P, 0, P)$), $\pm ST$ or $\pm(ST)^2$ (if $H = (P, P, P)$).

If $M \notin \mathrm{SL}_2(\mathbb{Z})$, then it swaps τ and $\bar{\tau}$, so that

$$a\tau + b = c\tau\bar{\tau} + d\bar{\tau}\ \ .$$

Taking imaginary parts, we get $a = -d$. Taking real parts, then using $\tau+\bar{\tau} = -Q/P$ and $\tau\bar{\tau} = R/P$, we obtain $bP = aQ + cR$. Finally, the determinant condition gives $a^2 + bc = 1$. One easily checks that the three conditions $a = -d$, $a^2 + bc = 1$ and $bP = aQ+cR$ are necessary and sufficient conditions for M to be an automorphism of H.

Now we clearly have $H(a, c) = P$ and $H(a, c) \geq (P - Q + R) \min(a^2, c^2)$, and since H is reduced we have $0 \leq Q \leq P \leq R$. Thus we obtain the following:

• If $ac \neq 0$, then $a^2 = c^2 = 1$ and $P = Q = R$, so $b = 0$ hence $c = -a$, $d = -a$ and $a = \pm 1$.

• If $a = 0$, then $bc = 1$ and $Rc^2 = P$ so $R = P$ and $c = \pm 1$, hence $b = c$ and $d = 0$.

• If $c = 0$, then $a^2 = 1$ and $bP = aQ$. This implies that either $b = 0$ and $Q = 0$, or $b = a$ and $P = Q$.

This finishes the proof of the lemma. Note that it follows from this result that the group G of automorphisms of H is always isomorphic to a group of the form $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, with $m = 1$, $m = 2$ (when $Q = 0$ or $P = R$ or $P = Q$ are the only equalities), $m = 4$ (when $P = R$ and $Q = 0$), or $m = 6$ (when $P = Q = R$). □

We can now give the definition of a reduced cubic form in the case of positive discriminant.

Definition 5.3. *Let $F = (a, b, c, d)$ be an integral binary cubic form of positive discriminant. We will say that F is* reduced *if its Hessian H_F is reduced in the above sense, and if in addition:*

1. $a > 0$.
2. *If $Q = 0$, then $b > 0$.*
3. *If $P = Q$, then $|b| < |3a - b|$.*
4. *If $P = R$, then $a \leq |d|$ and $|b| < |c|$ when $|d| = a$.*

With this definition, we have:

Proposition 5.4.

1. *Two equivalent reduced real cubic forms are equal.*
2. *A reduced real cubic form belonging to U is irreducible.*
3. *Any irreducible real cubic form is equivalent to a unique reduced form.*

Proof. (1) Let F and F' be two reduced cubic forms and $M \in GL_2(\mathbb{Z})$ such that $F' = F \circ M$. Then $H_{F'} = H_F \circ M$ and since H_F and $H_{F'}$ are reduced, it follow from Lemma 5.2 that $H_{F'} = H_F$ and that M is an automorphism of H_F. We now have only a finite number of possibilities (exactly 16) to test for M. Let $F = (a, b, c, d)$.

First, if $M = \pm I$, we have $F' = \pm(a, b, c, d)$ hence the conditions $a > 0$ on F and F' imply $M = I$.

If $P = R$ and $M = \pm\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, we have $F' = \pm(d, c, b, a)$ hence the conditions $a \le |d|$ on F and F' imply $a = |d|$, hence the additional conditions $|b| < |c|$ on F and F' give a contradiction.

In the case $P = R$ and $Q = 0$ and $M = \pm\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, then we have $F' = \pm(-d, c, -b, a)$, and the conditions $a \le |d|$ on F and F' imply $a = |d|$ and the additional conditions $|b| < |c|$ also lead to a contradiction. Note that an easy calculation shows that in this case $F = (a, -3d, -3a, d)$.

If $P = Q$ and $M = \pm\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$, we have $F \circ M = \pm(a, 3a - b, 3a - 2b + c, a - b + c - d)$ and hence the conditions $|b| < |3a - b|$ on F and F' give a contradiction.

If $Q = 0$ and $M = \pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, we have $F \circ M = \pm(a, -b, c, -d)$ and hence the conditions $b > 0$ on F and F' give a contradiction.

Finally assume that $P = Q = R$ and M is one of the six matrices given by Lemma 5.2. Then an easy computation shows that F is of the form $F = (a, b, b - 3a, -a)$. The reducedness of F is equivalent to $a > 0$, $|b| < |3a - b|$. For the six matrices of Lemma 5.2, we have respectively $F' = \pm(a, 3a - b, -b, -a)$, $F' = \mp F$ and $F' = \mp F$. The first two leads to a contradiction because of the condition $|b| < |3a - b|$, and the other four together with $a > 0$ imply $F = F'$, and the matrices $\left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ as automorphisms of F. Thus in this case, and only in this case, the automorphism group of F is nontrivial and is cyclic of order 3 generated by one of the above two matrices. This finishes the proof of (1).

(2) Let $F = (a, b, c, d) \in U$ be a reducible real cubic form. We will successively replace F by equivalent forms, which we will still denote (a, b, c, d) by abuse of notation, until we can conclude. Set $\Delta = \operatorname{disc}(F)$. Assume by contradiction that F is reducible. Then by transforming F by a suitable element of $\mathrm{GL}_2(\mathbb{Z})$ we may assume that $a = 0$ and hence $b \ne 0$ since $\Delta \ne 0$. By changing if necessary F into $-F$, we may assume that $b \ge 0$. Changing (x, y) into $(x - ky, y)$ for a suitable k, we may assume that $|c| \le b$ and finally by changing if necessary (x, y) into $(-x, y)$, we may assume $0 \le c \le b$. We thus have $\Delta = b^2c^2 - 4b^3d$, and $(P, Q, R) = (b^2, bc, c^2 - 3bd)$.

Let p be an odd prime dividing b. Since $b^2 \mid \Delta$, we have $F \notin V_p$, but since $F \in U_p$, by definition this means that $(F, p) = (1^3)$ plus an additional condition. In particular, by Proposition 3.3 (2) we have $p \mid \gcd(P, Q, R)$, hence $p \mid (c^2 - 3bd)$, so $p \mid c$, hence $p^3 \mid \Delta$, and this leads to a contradiction unless $p = 3$ by Proposition 3.3 (3). But if $p = 3$, we have $a = 0$ hence $3 \mid a$ and $9 \mid a$ so Proposition 3.3 (4) implies that $F \notin U_p$, contradiction again.

There remains the case of $p = 2$ dividing b. In that case we have $\Delta \equiv b^2c^2 \pmod{16}$ hence $(\Delta/4) \equiv ((b/2)c)^2 \equiv 0$ or $1 \pmod 4$, so $F \notin V_2$. Since $F \in U_2$, we have $(F, 2) = (1^3)$. We conclude as before by Proposition 3.3 (2) that $2 \mid (c^2 - bd)$, hence $2 \mid c$ hence $16 \mid \Delta$, in contradiction with $8 \nmid \Delta$ coming from Proposition 3.3 (3).

We deduce from the different cases above that $b = 1$, and hence $c = 0$ or $c = 1$. Hence if we call G the final cubic form that we have obtained, we have $F = G \circ M$ for a certain $M \in GL_2(\mathbb{Z})$, and $G = (0, 1, c, d)$ with $c = 0$ or 1. Hence $H_G = (1, 0, -3d)$ or $H_G = (1, 1, 1 - 3d)$. Since these are reduced quadratic forms equivalent to H_F which is reduced, we have $H_G = H_F = H_G \circ M$. Now, since $d < 0$ (otherwise $\Delta \le 1$ and $\Delta = 1$ is impossible), the only automorphisms of H_F are $\pm I$, and since we must have $a > 0$, this implies $M = I$ hence $F = G$, contradiction.

(3) The uniqueness statement follows from (1). Let $F = (a, b, c, d)$ be an irreducible real cubic form and H_F its Hessian. By the usual theory of reduction of quadratic forms (with the added twist that matrices of determinant -1 are allowed), we can find $M \in \mathrm{GL}_2(\mathbb{Z})$ such that $H_F \circ M$ is reduced, hence by changing F into $F \circ M$ we may assume $H_F = (P, Q, R)$ reduced.

In all the cases of Definition 5.3, it is easily checked that the use of the 16 matrices of Lemma 5.2 will lead to a reduced form. Note that it is essential to assume F irreducible, otherwise the result would be false. More precisely, it is enough to check that the forms with $a = 0$, or $b = 0$ when $Q = 0$, or $|b| = |3a - b|$ when $P = Q$ or $a = |d|$ and $|b| = |c|$ when $P = R$ are all reducible. This finishes the proof of the proposition. $\square$

To be able to produce all reduced binary cubic forms of discriminant bounded by X, we must be able to give bounds on the coefficients of such a form. Such a result is as follows.

Proposition 5.5. *Let $F = (a, b, c, d)$ be a reduced form such that $0 < \mathrm{disc}(F) \le X$. We have the following inequalities:*

$$1 \le a \le \frac{2}{3\sqrt{3}} X^{1/4}, \quad -X^{1/4} \le b \le \frac{2}{\sqrt{3}} X^{1/4} \ ,$$

$$\frac{-35 - 13\sqrt{13}}{216} X \le ac^3 \le \frac{-35 + 13\sqrt{13}}{216} X, \quad -\frac{\sqrt{3}}{4} X^{1/2} \le bc \le X^{1/2} \ ,$$

$$b < 0 \implies c < 0 \ ,$$

$$-\frac{4}{27} X^{1/2} \le ad \le \frac{\sqrt{3}}{36} X^{1/2}, \quad \frac{-35 - 13\sqrt{13}}{216} X \le b^3 d \le \frac{-35 + 13\sqrt{13}}{216} X \ ,$$

$$0 \le c^2(bc - 9ad) \le \frac{4}{3} X \ .$$

Proof. We only give a sketch of parts of the proof, leaving all the details to the reader.

Set $D = \mathrm{disc}(F)$ so that $4PR - Q^2 = 3D$. On the other hand, set

$$f(b, P, Q) = \pm\sqrt{P(3D + Q^2) - 3b^2 D} \ .$$

An explicit computation shows that we have

$$a = \frac{2P(bQ - f(b, P, Q))}{3(3D + Q^2)}, \quad c = \frac{bQ + f(b, P, Q)}{2P}, \quad d = \frac{b(Q^2 - 3D) + 2Qf(b, P, Q)}{12P^2} \ .$$

We express these quantities on purpose only in terms of b, P, Q and D, and will use the inequalities $0 \le Q \le P \le D^{1/2} \le X^{1/2}$. When we want to find an upper bound for an expression in a, b, c, d, we consider this expression first as a function of the single parameter b which is constrained to satisfy $P(3D+Q^2)-3b^2D\ge 0$. This is done by taking derivatives and looking at the value of the expression where the derivative vanishes and at the endpoints. We then have a function of P, Q and D only. In most cases, this expression does not even depend on P, and hence we again compute derivatives and look at endpoints to find the maximum as Q varies from 0 to $D^{1/2}$. When the expression depends on P, we use the inequalities $Q\le P\le D^{1/2}$.

We give one example, the bound for bc. We set $B=b^2$. Then

$$2Pbc = BQ \pm \sqrt{P(3D+Q^2)B-3B^2D}\ .$$

We find that the derivative in B of the RHS vanishes for

$$B=(P(3D+Q^2)\pm PQ\sqrt{3D+Q^2})/(6D)\ ,$$

and for these values we have $bc=(Q(3D+Q^2)+(\pm Q^2\pm 3D)\sqrt{3D+Q^2})/(12D)$, the $\pm$ signs being independent. The study of the 4 functions

$$\left|x(3+x^2)+(\pm x^2\pm 3)\sqrt{x^2+3}\right|$$

on the interval $[0,1]$ shows that the largest maximum is attained with both $+$ signs for $x=1$, and is equal to 12, hence a local maximum of $|bc|$ is attained for $Q=D^{1/2}$ and is equal to $D^{1/2}$. Furthermore, looking at the endpoints $B=0$ and $B=P(3D+Q^2)/(3D)$, we see that bc is respectively 0 and $Q(3D+Q^2)/(6D)\le (2/3)D^{1/2}$, which is smaller that $D^{1/2}$ thus giving the desired inequality for $|bc|$. However, in addition we have $b^2=P+3ac$, hence since $a>0$, $b^2\le P$ if and only if $c\le 0$.

When $b\le 0$, we must have $a\ge 0$, hence in the expression for a the expression under the square root must be larger than b^2Q^2, or equivalently $b^2\le P\le X^{1/2}$ which shows the lower inequality for b. Hence $b\le 0$ implies $c<0$. This implies that if $bc<0$, we must have $b>0$ and $c<0$. But in that case, the $-$ sign must hold in the expression for c, and hence since $b>0$, in the 4 functions above the second $\pm$ sign must in fact be a $-$ sign. If we look at the remaining two functions, we see that the local maximum of $|bc|$ is now only $\sqrt{3}/4D^{1/2}$. The endpoints are $B=0$ and $B=P$ in this case, but then bc vanishes at both endpoints so the maximum is really $\sqrt{3}/4D^{1/2}$ for $bc<0$.

For the two inequalities involving $\sqrt{13}$, we get in fact a fourth degree equation in $B=b^2$, but luckily this equation has $B=P$ as double root, hence we are reduced to a second degree equation one again.

The details of this and of the other inequalities are left to the patient reader. $\square$

Using only the inequalities of Proposition 5.5, it is not difficult to show that the number of quadruplets (a,b,c,d) which will have to be checked is *linear* in X. However, in the actual implementation, we will first loop on a, then on b, then on c and finally on d satisfying the inequalities coming from $0\le Q\le P\le R$ and from $\operatorname{disc}(F)\le X$. The total number of triplets (a,b,c) satisfying the above inequalities is $O(X^{3/4})$. For some of these triplets the loop on d will be empty, and for the others we will have to examine essentially the number $H_3^+(X)$ of reduced real binary cubic forms of discriminant up to X (essentially because the special cases have to be considered, but they add a negligible number of forms). Hence the total number of cases to be examined will be $H_3^+(X) + O(X^{3/4})$. Now recall the following theorem.

Theorem 5.6. *Let $H_3^+(X)$ (resp. $N_3^+(X)$) be the number of equivalent real cubic forms (resp. of isomorphism classes of real cubic fields) of discriminant less than or equal to X. Then as $X \to \infty$, we have:*

$$H_3^+(X) = \frac{\pi^2}{72}X + C^+ \cdot X^{5/6} + O(X^{2/3+\epsilon}) \sim 0.137\,X$$

$$N_3^+(X) = \frac{1}{12\zeta(3)}X + O\left(Xe^{-(c\log X\log\log X)^{1/2}}\right) \sim 0.0693\,X \;\;,$$

for any $c < 1/24$.

Remark. The precise form for the remainder term for $H_3^+(X)$ is due to Shintani ([10]), improving on Davenport's original result. A remainder term for $N_3^+(X)$ was proved by the first author in [1], and the present one will appear in [2].

It follows that the total number of steps in our algorithm will be linear in X, and in fact approximately $0.137/.0693 \sim 1.977$ times more than the number of fields that we have to find, hence there is very little waste.

We could still gain a little by avoiding the $O(X^{3/4})$ empty loops that we have mentioned. For this, we would need to find the exact range of values of a, then of b given a, and finally of c, given a and b. The result involves a very large number of cases and algebraic equations of large degree, and the gain is marginal, hence we do not do it.

We can also easily characterize subclasses of real cubic fields. For example, we have the following:

Proposition 5.7. *Let K be a totally real cubic number field, F_K the unique reduced form associated to K and $H_K = (P,Q,R)$ its Hessian. Then:*

1. *K is cyclic (i.e $\operatorname{disc}(K) = f^2$) if and only if $H_K = (P,P,P)$.*
2. *$\operatorname{disc}(K) = 5f^2$ if and only if $H_K = (P,P,4P)$ or $H_K = (2Q,Q,2Q)$.*
3. *$\operatorname{disc}(K) = 8f^2$ if and only if $H_K = (P,0,6P)$ or $H_K = (2P,0,3P)$.*
4. *$\operatorname{disc}(K) = 12f^2$ if and only if $H_K = (P,0,9P)$, $H_K = (P,P,5P/2)$ or $H_K = (P,0,P)$.*

Proof. Using Proposition 4.8, this is just a matter of listing reduced quadratic forms and is left to the reader. □

6. Complex cubic fields

We now consider the case where $\operatorname{disc}(F) < 0$, *i.e* when F corresponds to a complex cubic field. In this case the Hessian is an indefinite quadratic form, and in general there will be many reduced quadratic forms equivalent to it. Instead of using the Hessian, we will use a clever idea due to Matthews and Berwick (see [9]). If $\operatorname{disc}(F) < 0$, then F has a unique real root θ, and $\theta \notin \mathbb{Q}$ if F is irreducible, so if we factor F in $\mathbb{R}[X,Y]$ as

$$F(x,y) = (x - \theta y)(Px^2 + Qxy + Ry^2)$$

the quadratic form (P, Q, R) will be definite ($i.e$ $Q^2 - 4PR < 0$), but with real nonrational coefficients. We are going to show that the form (P, Q, R) has many of the properties of the Hessian.

An easy computation gives

$$\operatorname{disc}(F) = (Q^2 - 4PR)(P\theta^2 + Q\theta + R)^2 \ .$$

By changing (x, y) to $(-x, -y)$, $i.e$ F into $-F$, we may assume that $P \geq 0$, and if $F = (a, b, c, d)$ we have

$$P = a, \ Q = a\theta + b, \ R = a\theta^2 + b\theta + c$$

hence

$$a = P, \ b = Q - \theta P, \ c = R - \theta Q \text{ and } d = -\theta R \ ,$$

If $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, then a simple computation shows that

$$H_{F \circ M} = |a - \theta c| \cdot H_F \circ M \ ,$$

the absolute value sign coming from the choice $P \geq 0$.

Definition 6.1. *Let $F = (a, b, c, d)$ be an integral binary complex cubic form, and let (P, Q, R) as above. We say that F is* reduced *if $0 < |Q| < P < R$ and if in addition $a > 0$, $b \geq 0$, $d \neq 0$ and $d > 0$ if $b = 0$.*

Note that when F is irreducible, θ is irrational, hence the special cases $Q = 0$, $P = |Q|$ or $P = R$ which occurred in the real case cannot occur here. Another nice fact is that we do not need to compute the irrational numbers P, Q and R at all:

Lemma 6.2. *Let $F = (a, b, c, d)$ be a complex cubic form. Then F is reduced if and only if:*

$$d^2 - a^2 + ac - bd > 0$$

$$-(a - b)^2 - ac < ad - bc < (a + b)^2 + ac$$

$$a > 0, \ b \geq 0, \ d \neq 0 \textit{ and } d > 0 \textit{ if } b = 0 \ .$$

Proof. The condition $Q < P$ is equivalent to $a\theta + b < a$ hence to $\theta < (a - b)/a$ since $a > 0$. Since F has only one real root (and again $a > 0$), this is equivalent to $F(a - b, a) > 0$ which gives $-(a - d)^2 - ac < ad - bc$. Similarly, the condition $-Q < P$ is equivalent to $-a\theta - b < a$ hence to $\theta > -(a+b)/a$, so $F(-(a+b), a) < 0$ which gives $ad - bc < (a + b)^2 + ac$. Finally, the condition $P < R$ is equivalent to $a\theta^2 + b\theta + (c - a) > 0$, and this is equivalent to $\mathcal{R}(F_1, G) > 0$ where $\mathcal{R}$ is the resultant, $F_1(X) = F(X, 1)$ and $G(X) = aX^2 + bX + (c - a)$. An immediate computation shows that $\mathcal{R}(F_1, G) = a^3(d^2 - a^2 + ac - bd)$, and this gives the last unproved condition. □

For this notion to be useful, we must have the analogue of Proposition 5.4.

Proposition 6.3.

(1) *Two equivalent reduced complex cubic forms are equal.*
(2) *A reduced complex cubic form belonging to U is irreducible.*
(3) *Any irreducible complex cubic form is equivalent to a unique reduced form.*

Proof. (1) Let $F' = F \circ M$ where F and F' are reduced and $M \in \mathrm{GL}_2(\mathbb{Z})$. Then by the formula proved above, there exists $\lambda > 0$ such that $H_{F'} = \lambda H_F \circ M$. As before, we deduce from the inequalities $|Q| < P < R$ and $|Q'| < P' < R'$ that $H_{F'} = \lambda H_F$, and hence that M is an automorphism of H_F. The proof then terminates as in the real case, except that there are no special cases to consider since the forms are irreducible.

(2) As in the real case, a complex reducible form F belonging to U must be equivalent to $G = y(x^2 + \delta y^2)$ or to $G = y(x^2 + xy + \delta y^2)$ with $\delta \geq 1$. If $F = (x-\theta y)(Px^2+Qxy+Ry^2)$ and $F = G \circ M$ with $M \in \mathrm{GL}_2(\mathbb{Z})$, then $H_F = \lambda H_G \circ M$ for some $\lambda > 0$. Hence the reduced form H_F is equivalent to a multiple of H_G with $H_G = (1, 0, \delta)$ or $H_G = (1, 1, \delta)$ respectively which are also reduced, and hence it is equal to that multiple, hence we have either $Q = 0$ or $Q = P$ for the form F, which are both excluded from the definition of a reduced form in the complex case.

(3) is clear: we can always reduce first H_F by an element of $\mathrm{GL}_2(\mathbb{Z})$ so that it satisfies $0 < |Q| < P < R$, the strict inequalities being guaranteed by the irreducibility of F. We must have $d \neq 0$ otherwise F is reducible, and since $P = a$, we have $a > 0$. Changing (x, y) into $(x, -y)$ if necessary (which changes Q into $-Q$ and leave P and R unchanged), we may also assume that $b \geq 0$. Finally, if $b = 0$, changing again (x, y) into $(x, -y)$ of necessary we may assume $d > 0$ since $d \neq 0$. ∎

We have bounds on the coefficients of a reduced complex cubic form as follows.

Lemma 6.4. *Let $F = (a, b, c, d)$ be a reduced form such that $-X \leq \mathrm{disc}(F) < 0$. We have the following inequalities:*

$$|a| \leq \frac{2X^{1/4}}{3^{3/4}},\ |b| \leq \frac{2X^{1/4}}{3^{1/4}},\ |ac^3| \leq \frac{(11+5\sqrt{5})X}{8},\ |bc| \leq \frac{4X^{1/2}}{\sqrt{3}} \tag{3}$$

$$|ad| \leq \frac{X^{1/2}}{\sqrt{3}},\ |b^3d| \leq \frac{(11+5\sqrt{5})X}{8},\ c^2|bc-ad| \leq 4X\ . \tag{4}$$

Proof. Set

$$A = \sqrt{PR^3},\ B = \sqrt{P^3R\theta^4},\ \alpha = \frac{A}{(4X/3)^{1/2}},\ \beta = \frac{B}{(4X/3)^{1/2}},\ \Delta = 4PR - Q^2\ .$$

Then $\Delta > 3PR$, and

$$|\,\mathrm{disc}(F)| = \Delta(P\theta^2+Q\theta+R)^2 \geq 3PR(P\theta^2-P|\theta|+R)^2 \geq 3(A+B-A\sqrt{AB}/R^2)^2\ ,$$

and since $R^2 \geq A$ we have $A+B-A\sqrt{AB}/R^2 \geq 0$ and hence the RHS is an increasing function of R, so the inequality must be true at least for $R^2 = A$, thus giving

$$A+B-\sqrt{AB} \leq \left(\frac{X}{3}\right)^{1/2} \quad \text{or equivalently} \quad \alpha+\beta-\sqrt{\alpha\beta} \leq 1/2 \ . \tag{5}$$

In particular, this implies

$$A+B \leq 2(A+B-\sqrt{AB}) \leq \left(\frac{4X}{3}\right)^{1/2} \quad \text{or equivalently} \quad \alpha+\beta \leq 1 \ .$$

We also obtain from above

$$X \geq (3R/P)((P\theta+Q/2)^2+\Delta/4)^2 \geq 27A^2/16$$

and

$$X \geq (3P/R)((R+Q\theta/2)^2+\Delta\theta^2/4)^2 \geq 27B^2/16$$

thus giving the inequalities $A \leq (16X/27)^{1/2}$ and $B \leq (16X/27)^{1/2}$, or in other words $\alpha \leq 2/3$ and $\beta \leq 2/3$. The same inequalities can be obtained directly from (5).

Hence we obtain:

$$\begin{aligned}
a &= P \leq A^{1/2} \\
|b| &= |Q-\theta P| \leq |P|+|\theta P| \leq A^{1/2}+B^{1/2} \leq \sqrt{2}(A+B)^{1/2} \\
|ad| &= PR|\theta| = (AB)^{1/2} \leq (A+B)/2 \\
|bc| &\leq (P+|\theta|P)(R+P|\theta|) = PR+(P^2+PR)|\theta|+P^2\theta^2 \\
&\leq A+2(AB)^{1/2}+B \leq 2(A+B) \\
|ac^3| &\leq P(R+P|\theta|)^3 = A^2(1+\sqrt{AB}/R^2)^3 \leq A^{1/2}(A^{1/2}+B^{1/2})^3 \\
&\leq \frac{4X}{3}\alpha^{1/2}(\alpha^{1/2}+\beta^{1/2})^3 \\
|b^3d| &\leq |\theta|R(P+|\theta|P)^3 = B^{1/2}(B^{1/2}+A^{3/2}/R^2)^3 \leq B^{1/2}(A^{1/2}+B^{1/2})^3 \\
&\leq \frac{4X}{3}\beta^{1/2}(\alpha^{1/2}+\beta^{1/2})^3 \ .
\end{aligned}$$

Now an easy computation shows that the maximum of $x(x+y)^3$ subject to x, y nonnegative and $x^2+y^2-xy \leq 1/2$ is attained for

$$x = \frac{1}{2\sqrt{3}}\left(\frac{1+\sqrt{5}}{2}\right)^2 \quad \text{and} \quad y = \frac{\sqrt{15}}{6} \ ,$$

and is equal to $3/16((1+\sqrt{5})/2)^5 = 3(11+5\sqrt{5})/32$, thus giving all but the last inequality of the lemma.

For the last inequality using $(x+y)^2 \leq 2(x^2+y^2)$ and $2(x^2+xy+y^2) \leq 3(x^2+y^2)$, we obtain

$$\begin{aligned}
c^2|ad-bc| &= |R-Q\theta|^2(Q^2\theta - QR - \theta^2 PQ)\\
&\le 2(R^2+P^2\theta^2)(P^2|\theta| + PR + P^2\theta^2)\\
&\le 2(P^2R^2|\theta| + PR^3 + P^2R^2\theta^2 + P^4|\theta|^3 + P^3R\theta^2 + P^4\theta^4)\\
&\le 2(A(AB)^{1/2} + A^2 + AB + B(AB)^{1/2} + AB + B^2)\\
&\le 3(A+B)^2 \le 4X
\end{aligned}$$

thus proving all the inequalities of the lemma.

Note that in the first four inequalities, we have used only the bound for $A+B$ and not the stronger bound for $A+B-\sqrt{AB}$. However it can be checked that this would not improve the final bounds. However, this is not the case for the next two inequalities. □

In the actual implementation we will proceed essentially as in the real case. The analogue of Theorem 5.6 is as follows.

Theorem 6.5. *Let $H_3^-(X)$ (resp. $N_3^-(X)$) be the number of equivalent complex cubic forms (resp. of isomorphism classes of complex cubic fields) of discriminant greater than or equal to $-X$. Then as $X\to\infty$, we have:*

$$H_3^-(X) = \frac{\pi^2}{24}X + C^-\cdot X^{5/6} + O(X^{2/3+\epsilon}) \sim 0.411\,X$$

$$N_3^-(X) = \frac{1}{4\zeta(3)}X + O\left(Xe^{-(c\log X\log\log X)^{1/2}}\right) \sim 0.208\,X\ ,$$

for any $c < 1/24$.

Once again, we see that the algorithm will be linear in X, and the number of loops will be approcimately 1.977 times the number of cubic fields found.

7. Implementation and results

The following table gives the total number of real fields of discriminant up to $X = 10^n$ for $1 \leq n \leq 11$, as well as the elapsed time on a DEC Alpha.

n	# of Fields	Time
1	0	0.000 s
2	2	0.000 s
3	27	0.000 s
4	382	0.005 s
5	4,804	0.05 s
6	54,600	0.5 s
7	592,922	5.7 s
8	6,248,290	64 s (1 min 04 s)
9	64,659,361	774 s (12 min 54 s)
10	661,448,081	18,641 s (5 h 11 min)
11	6,715,824,025	714,488 s (8 days 7 h)

The following table gives the total number of complex fields of discriminant greater or equal to to $-X$ with $X = 10^n$ for $1 \leq n \leq 11$, as well as the elapsed time on a DEC Alpha.

n	# of Fields	Time
1	0	0.000 s
2	7	0.000 s
3	127	0.004 s
4	1520	0.04 s
5	17,041	0.3 s
6	182,417	2.2 s
7	1,905,514	21.3 s
8	19,609,185	224 s (3 min 44 s)
9	199,884,780	2,575 s (42 min 55 s)
10	2,024,660,098	58,247 s (16 h 11 min)
11	20,422,230,540	2,427,276 s (28 days 2 h)

It should be remarked that, thanks to the notion of reducedness, our algorithm gives for every cubic field a canonical equation, which we can call *reduced*, and which in addition has all the nice properties described in Section 4. In particular the integral basis and decomposition of primes is immediate. One consequence is that, when the cubic number field does not have a power basis, the equation that we will find will not be monic. On the other hand, if there exists a power basis, the reduced equation produced by our algorithm is not necessarily monic. We give a few examples.

(1) The cyclic number field with discriminant 961 can be given by the monic equation $X^3 + X^2 - 10X - 8 = 0$, but does not have a power basis (an integral basis is $(1, \alpha, (\alpha^2 + \alpha)/2)$, where α is a root of the above equation). Our algorithm finds the nonmonic reduced equation $2X^3 + X^2 - 5X - 2 = 0$.

(2) The noncyclic number field of discriminant 1304 can be given by the monic equation $X^3 - X^2 - 11X - 1 = 0$, but does not have a power basis (an inte-

gral basis is $(1, \alpha, (\alpha^2+1)/2))$. Our algorithm finds the nonmonic reduced equation $2X^3+3X^2-4X-2$.

(3) The noncyclic number field of discriminant 2228 can be given by the monic equation $X^3-14X-18=0$, and this times it has a power basis. On the other hand our algorithm finds the nonmonic reduced equation $2X^3+2X^2-6X-1=0$.

References

[1] K. Belabas, *Crible et 3-rang des corps quadratiques*, Ann. Institut Fourier (to appear).

[2] K. Belabas, *Densités de classes de formes cubiques et calculs heuristiques du 3-rang des corps de nombres*, preprint.

[3] H. Cohen, *A course in computational algebraic nuumber theory*, Graduate Texts in Maths, vol. 138, Springer-Verlag, 1993; Second corrected printing, 1995.

[4] H. Davenport, *On the class number of binary cubic forms (I)*, J. Lond. Math. Soc. **26** (1951), 183–192; Erratum, ibid **27** (1952), 512.

[5] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields (I)*, Bull. Lond. Math. Soc. **1** (1969), 345–348.

[6] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields (II)*, Proc. Roy. Soc. Lond. A **322** (1971), 405–420.

[7] H. Hasse, *Arithmetische Theorie der kubischen Zahlkorper auf klassenkorpertheoretischer Grundlage*, Math. Zeitschrift **31** (1930), 565–582.

[8] H. Hasse, *Zahlentheorie*, Akademie-Verlag GmbH, 1949.

[9] G.-B. Mathews, *On the reduction and classification of binary cubics which have a negative discriminant*, Proc. London Math. Soc. **10** (1912), 128–138.

[10] T. Shintani, *On zeta-functions associated with the vector space of quadratic forms*, J. Fac. Sci. Univ. Tokyo, Sec. 1a **22** (1975), 25–66.