

A “class group” obstruction for the equation

$$Cy^d = F(x, z)$$

par DENIS SIMON

Dedicated to Henri Cohen.

RÉSUMÉ. L’objet de cet article est d’étudier les équations de la forme $Cy^d = F(x, z)$ où $F \in \mathbb{Z}[x, z]$ est une forme binaire homogène de degré n , supposée primitive et irréductible, et d est un entier quelconque fixé. Par des méthodes algébriques classiques, nous donnons un critère nécessaire pour l’existence de solutions primitives de cette équation. Ce critère repose sur l’existence d’un idéal de norme donnée dans un certain ordre d’un corps de nombres et sur une relation dans le groupe de classes satisfaite par cet idéal. De nombreux exemples sont donnés pour illustrer ce critère. Dans une seconde partie, un lien est fait entre ce critère et les propriétés de la différentielle du corps de nombres considéré.

ABSTRACT. In this paper, we study equations of the form $Cy^d = F(x, z)$, where $F \in \mathbb{Z}[x, z]$ is a binary form, homogeneous of degree n , which is supposed to be primitive and irreducible, and d is any fixed integer. By using classical algebraic methods, we give a necessary condition for the existence of primitive solutions for this equation. This condition rests on the existence of an ideal of given norm in some order in a number field, and on a relation satisfied by this ideal in the class group. Numerous examples are given to illustrate this result. In a second part, we make a link between this condition and the properties of the different in the considered number field.

Let $F(x, z) \in \mathbb{Z}[x, z]$ be a homogeneous polynomial of degree n . Throughout this paper, we will assume that F is irreducible over \mathbb{Q} and that F is primitive (its coefficients are coprime integers).

Our interest is to study the existence of proper solutions to the equation

$$(1) \quad y^d = F(x, z)$$

or more generally

$$(2) \quad Cy^d = F(x, z)$$

where $d \geq 2$ and $C \neq 0$ are fixed integers. A solution (x, y, z) of (1) or (2) is called *proper* if x, y and z are integers such that x and z are coprime.

If d is a divisor of n , then any rational solution (x, y, z) of (1) is equivalent to a proper solution in the sense that there exists a proper solution of the form $(\lambda x, \lambda^{n/d} y, \lambda z)$. This is also the case for (2) if C is d -th power free. On the opposite, if d and n are coprime, say for example $ad = nb + 1$ for some positive integers a and b , then any value of the parameters t and u lead to the solutions $x = tF(t, u)^b$, $y = F(t, u)^a$, $z = uF(t, u)^b$ of (1). These trivial solutions are in general highly nonproper, and we want to avoid them in our study, this is why we consider proper solutions only.

The main application we have in mind is the case $d = 2$ and $n = 4$. These equations arise naturally during the algorithm of 2-descent on elliptic curves, and have been studied by different authors : [1], [3] or [12]. The general case is also of some importance among the general Diophantine equations. By [6], we know that the equations have finitely many solutions, except maybe if $d = 2$ and $n \leq 4$, or $d = n = 3$. But the question remains whether there is a solution at all. It happens that some class group computations can help answering this question.

In [2, §14.2, lemma 2.5], equation (1) is considered in the case where $n = 2$ and $d \geq 2$ is any integer. Here, F is a quadratic form of discriminant Δ . We can associate to F its class $cl(F)$ in the class group $Cl(\Delta)$ of primitive quadratic forms of discriminant Δ under composition and modulo proper equivalence. The result is the following :

Theorem 1 (Cassels, [2]). *If $n = 2$, and $d \geq 2$, then equation (1) has a proper solution (x, y, z) with y coprime to 2Δ if and only if $cl(F)$ is a d -th power in $Cl(\Delta)$.*

In this result, we see that there is a condition on the class of F in some class group. Another result is given in [6, §8] for equation (2), but only when the form F is monic (its coefficient in x^2 is 1) :

Theorem 2 (Darmon–Granville, [6]). *Suppose that $d \geq 2$ and B and C are coprime positive integers with $B \equiv 1 \pmod{4}$ and squarefree, and C odd.*

There are proper integer solutions to $x^2 + Bz^2 = Cy^d$ if and only if there exist coprime ideals J_+ and J_- in $\mathbb{Q}(\sqrt{-B})$ with $J_+ J_- = (C)$, whose ideal classes are d -th powers inside the class group of $\mathbb{Q}(\sqrt{-B})$.

Contrary to the result of Cassels, the condition now rests on the class of an ideal of norm C . A similar result is proved by Cohen in [5, Th. 6.4.8] in the case of equations of the type $x^p + Bz^p = Cy^p$ (in fact just the *only* part is given).

Our goal in this paper is to generalize the *only if* part of these statements for arbitrary values of n . In the case of equation (2), we will consider simultaneously the two conditions : the first on the existence of an ideal with given norm and a second on a d -th power relation in some class group. The first condition is a local condition, whereas the second is not : this is what we call the class group condition, or the class group obstruction. In the case of equation (1), the first condition disappears, exactly as in Theorem 1. The main result that we prove in section 2 will give us a necessary condition for the existence of proper solutions of (1) and (2) or equivalently a sufficient condition for the nonexistence of such solutions. Unfortunately, we are not able to generalize the *if* part of the theorems, which is very probably false in the general case.

In section 3, many examples are given to illustrate the results. While looking for these examples, we observed that the class group obstruction never applies to the equation $y^2 = F(x, z)$ when the degree of F is odd and its index is 1. This observation is proved in section 4. The two main ingredients of this proof are the Theorem of Hecke stating that the class of the different is always a square in the class group, and an explicit relation between the different and the $(n - 2)$ -th power of the class of F . When the degree of F is even, this relation exhibits an explicit square root for the class of the different.

1. Construction of useful objects

1.1. Construction of $cl(F)$. In [15], we have associated to the polynomial $F(x, z) = a_0x^n + a_1x^{n-1}z + \dots + a_nz^n$ the following construction :

- (1) Define the field $K = \mathbb{Q}(\theta)$, with $F(\theta, 1) = 0$. This field is isomorphic to $\mathbb{Q}[x]/F(x, 1)$.
- (2) For $i = 0, \dots, n$, define the polynomials $P_i = a_0x^i + a_1x^{i-1} + \dots + a_i$.
- (3) Construct an order \mathbb{Z}_F in K with discriminant $\text{Disc}(\mathbb{Z}_F) = \text{Disc}(F)$. As a module this order is given by its \mathbb{Z} -basis $\mathbb{Z}_F = \mathbb{Z} \oplus P_1(\theta)\mathbb{Z} \oplus P_2(\theta)\mathbb{Z} \oplus \dots \oplus P_{n-1}(\theta)\mathbb{Z}$.
- (4) In \mathbb{Z}_F , two submodules are of great importance, namely $\mathfrak{b} = P_0(\theta) \oplus P_1(\theta)\mathbb{Z} \oplus P_2(\theta)\mathbb{Z} \oplus \dots \oplus P_{n-1}(\theta)\mathbb{Z}$ and $\mathfrak{a} = \theta\mathfrak{b}$. The modules \mathfrak{a} and \mathfrak{b} are in fact coprime invertible ideals of \mathbb{Z}_F . They satisfy $\mathcal{N}_{\mathbb{Z}_F/\mathbb{Z}}(\mathfrak{b}) = a_0$ and $\mathcal{N}_{\mathbb{Z}_F/\mathbb{Z}}(\mathfrak{a}) = a_n$. The ideal \mathfrak{b} can be seen as the denominator of θ and \mathfrak{a} its numerator. They can also be defined by $\mathfrak{b}^{-1} = \mathbb{Z}_F + \theta\mathbb{Z}_F$ and $\mathfrak{a}^{-1} = \mathbb{Z}_F + \theta^{-1}\mathbb{Z}_F$.
- (5) At last, consider the class of \mathfrak{b} in the ideal class group $Cl(\mathbb{Z}_F)$ and call it $cl(F)$ (the ideal \mathfrak{a} is also in the same class).

It was proved in [15] that the field K , the ring \mathbb{Z}_F and the class $cl(F)$ in $Cl(\mathbb{Z}_F)$ only depend on the class of F modulo the action on $SL_2(\mathbb{Z})$. When

F is a quadratic polynomial, this construction is the standard correspondence between classes of quadratic forms of given discriminant Δ modulo $SL_2(\mathbb{Z})$ and ideal classes modulo principal ideals in the quadratic ring of discriminant Δ .

1.2. Invertible and prime ideals of \mathbb{Z}_F . This section summarizes useful results of [7].

Let \mathbb{Z}_K be the ring of integers of K . We have $\mathbb{Z}_F \subset \mathbb{Z}_K$ and $Ind(F) = [\mathbb{Z}_K : \mathbb{Z}_F]$ is an integer such that $Disc(F) = Ind(F)^2 Disc(K)$. If an ideal I_F of \mathbb{Z}_F is invertible then we can identify it with the ideal I_K of \mathbb{Z}_K through the relations $I_F \mathbb{Z}_K = I_K$ and $I_K \cap \mathbb{Z}_K = I_F$. If an ideal I_F of \mathbb{Z}_F is coprime to $Ind(F)$, then it is invertible, but these ideals are not the only invertible ideals in \mathbb{Z}_F .

Let p be a prime number. The prime ideals of \mathbb{Z}_F above p can be read from the factorization of the polynomial $F(x, z)$ modulo p : $F(x, z) = \prod_{i=1}^s F_i(x, z)^{e_i} \pmod{p}$. The polynomials $F_i \in \mathbb{F}_p[x, z]$ are irreducible and coprime. If f_i is the degree of F_i , then we will identify the polynomial $F_i \in \mathbb{F}_p[x, z]$ with any homogeneous lift of F_i in $\mathbb{Z}[x, z]$ having the same degree f_i . Associated with this factorization, we define several ideals of \mathbb{Z}_F . The first ones are

$$\mathfrak{q}_i = p\mathbb{Z}_F + (\mathfrak{b}^{f_i} F_i(\theta, 1))^{e_i} .$$

These coprime integral ideals satisfy the relation $p\mathbb{Z}_F = \prod_{i=1}^s \mathfrak{q}_i$. They are invertible and their norm is $\mathcal{N}_{\mathbb{Z}_F/\mathbb{Z}}(\mathfrak{q}_i) = p^{e_i f_i}$. The next ideals are

$$\mathfrak{p}_i = p\mathbb{Z}_F + \mathfrak{b}^{f_i} F_i(\theta, 1) .$$

These coprime integral ideals are prime ideals and are the only prime ideals of \mathbb{Z}_F above p . Their norm is $\mathcal{N}_{\mathbb{Z}_F/\mathbb{Z}}(\mathfrak{p}_i) = p^{f_i}$. Each ideal \mathfrak{p}_i satisfies $\mathfrak{p}_i^{e_i} \subset \mathfrak{q}_i \subset \mathfrak{p}_i$, and it is an invertible ideal if and only if the first inclusion is an equality. Note that if \mathfrak{p}_i is not invertible, then $p \mid Ind(F)$ hence $p^2 \mid Disc(F)$.

2. The main result : a condition on $cl(F)$

To a couple (x_0, y_0) of integers (not both zero), we associate the element $\delta = (x_0 - \theta z_0) \in K^*$. The norm of this element satisfies $a_0 \mathcal{N}_{K/\mathbb{Q}}(\delta) = F(x_0, z_0)$. We also associate to this couple the invertible integral ideal $\mathfrak{D} = \mathfrak{b}(x_0 - \theta z_0)$ of \mathbb{Z}_F . The norm of this ideal is given by the simpler relation

$$\mathcal{N}_{\mathbb{Z}_F/\mathbb{Z}}(\mathfrak{D}) = F(x_0, z_0).$$

Proposition 1. *Let x_0 and z_0 be coprime integers. Let $\mathfrak{D} = \mathfrak{b}(x_0 - \theta z_0)$ be its associated ideal in \mathbb{Z}_F . Let p be a prime divisor of $F(x_0, z_0)$. Then*

there exists a unique prime ideal \mathfrak{p} of \mathbb{Z}_F above p such that $\mathfrak{D} \subset \mathfrak{p}$. This ideal satisfies $f(\mathfrak{p}) = 1$ and $\mathfrak{p} = p\mathbb{Z}_F + \mathfrak{D}$.

Proof: The factorization of F into irreducible factors modulo p gives the relation $\prod F_i(x_0, z_0)^{e_i} = 0 \pmod{p}$, from which we deduce that at least one of the F_i satisfies $F_i(x_0, z_0) = 0$. Since x_0 and z_0 are coprime, this implies that F_i is divisible by the nontrivial linear factor $(z_0x - x_0z)$, hence $F_i = (z_0x - x_0z)$ (up to an invertible constant modulo p). This proves the unicity of F_i . We clearly have $\mathfrak{D} \subset p\mathbb{Z}_F + \mathfrak{D} = p\mathbb{Z}_F + \mathfrak{b}F_i(\theta, 1) = \mathfrak{p}_i$. The degree f_i of \mathfrak{p}_i is equal to the degree of F_i , which is 1.

Assume now that $\mathfrak{D} \subset \mathfrak{p}_j$ for some other j . Since $p\mathbb{Z}_F \subset \mathfrak{p}_j$, we have $\mathfrak{p}_i = \mathfrak{D} + p\mathbb{Z}_F \subset \mathfrak{p}_j$, whence $i = j$. ■

Because the property given by this proposition will play an important role in the sequel, we propose the following definition :

Definition: We say that an integral ideal \mathfrak{J} of \mathbb{Z}_F satisfies the *property (P)* if it is only contained in prime ideals of degree 1 and in at most one such prime ideal above each $p \mid \mathcal{N}_{\mathbb{Z}_F/\mathbb{Z}}(\mathfrak{J})$.

Theorem 3. Let $F(x, z)$ be a primitive irreducible binary form. Let (x_0, y_0, z_0) be a proper solution of (2) and $\mathfrak{D} = \mathfrak{b}(x_0 - \theta z_0)$ its associated ideal in \mathbb{Z}_F . There exist three invertible integral ideals \mathfrak{c} , \mathfrak{g} and \mathfrak{h} of \mathbb{Z}_F such that

- (1) $\mathfrak{D} = \mathfrak{c}\mathfrak{h}\mathfrak{g}^d$
- (2) the ideals \mathfrak{D} , \mathfrak{c} , \mathfrak{g} and \mathfrak{h} satisfy the property (P).
- (3) the primes containing \mathfrak{c} and \mathfrak{g} are all invertible, whereas those containing \mathfrak{h} are all noninvertible.
- (4) if \mathfrak{p} is a prime above p containing \mathfrak{g} , then $v_{\mathfrak{p}}(\mathfrak{g}) = v_{\mathfrak{p}}(y_0)$.
- (5) if \mathfrak{p} is a prime above p containing \mathfrak{c} , then $v_{\mathfrak{p}}(\mathfrak{c}) = v_{\mathfrak{p}}(C)$.

Proof: Let $\mathfrak{D} = \prod_i \mathfrak{P}_i$ be the primary decomposition of \mathfrak{D} : the ideals \mathfrak{P}_i are coprime invertible integral ideals, all contained in a single prime \mathfrak{p}_i above some prime divisor p_i of $F(x_0, z_0)$. By Proposition 1, the p_i are pairwise distinct.

We define \mathfrak{h} as the product of all the \mathfrak{P}_i such that \mathfrak{p}_i is noninvertible.

Consider now a primary factor \mathfrak{P}_i of \mathfrak{D} such that \mathfrak{p}_i is invertible. By Proposition 1, \mathfrak{p}_i is the only prime ideal above p_i , and has degree $f_i = 1$, hence we have

$$v_{p_i}(C) + dv_{p_i}(y_0) = v_{p_i}(\mathcal{N}_{\mathbb{Z}_F/\mathbb{Z}}(\mathfrak{P}_i)) = f_i v_{\mathfrak{p}_i}(\mathfrak{D}) = v_{\mathfrak{p}_i}(\mathfrak{P}_i)$$

We can now define $\mathfrak{c}_i = \mathfrak{p}_i^{v_{p_i}(C)}$ and $\mathfrak{g}_i = \mathfrak{p}_i^{v_{p_i}(y_0)}$. We have $\mathfrak{P}_i = \mathfrak{c}_i \mathfrak{g}_i^d$. The ideals $\mathfrak{c} = \prod_i \mathfrak{c}_i$ and $\mathfrak{g} = \prod_i \mathfrak{g}_i$ satisfy 1 to 5. ■

We can deduce several corollaries from this theorem.

Corollary 2. *Let $F(x, z)$ be a primitive irreducible binary form. Assume that the polynomial F satisfies the property that all the noninvertible prime ideals \mathfrak{p}_i of \mathbb{Z}_F are such that $f_i > 1$ (this is for example the case if $\text{Ind}(F) = 1$, which is itself the case if $\text{Disc}(F)$ is squarefree).*

A necessary condition for the existence of a nontrivial proper solution of (2) is that there exists an invertible integral ideal \mathfrak{c} of \mathbb{Z}_F of norm C such that

- (1) \mathfrak{c} satisfies the property (P).
- (2) $cl(F) \times cl(\mathfrak{c})^{-1}$ is d -th power in $Cl(\mathbb{Z}_F)$.

Proof: Let (x_0, y_0, z_0) be a proper solution and \mathfrak{D} its associated ideal, with decomposition $\mathfrak{D} = \mathfrak{c}\mathfrak{h}\mathfrak{g}^d$ as given by Theorem 3. The ideal \mathfrak{h} is only contained in noninvertible primes of degree 1. But the assumption implies that such primes do not exist, hence $\mathfrak{h} = 1$. The properties 2, 4 and 5 of Theorem 3 now imply that \mathfrak{c} satisfies the property (P) and $\mathcal{N}_{\mathbb{Z}_F/\mathbb{Z}}(\mathfrak{c}) = C$. The conclusion is a simple consequence of the relation $\mathfrak{b}(x_0 - \theta z_0) = \mathfrak{D} = \mathfrak{c}\mathfrak{g}^d$. ■

Remark: The first condition on \mathfrak{c} is just a local condition, given by congruences. The second condition concerns the class group and is usually a nonlocal condition. The examples given in section 3 will illustrate this fact.

Corollary 3. *Let $F(x, z)$ be a primitive irreducible binary form. A necessary condition for the existence of a nontrivial proper solution (x_0, y_0, z_0) of (2), such that y_0 is coprime to $\text{Ind}(F)$, is that there exists an invertible integral ideal \mathfrak{c} of \mathbb{Z}_F of norm C such that*

- (1) \mathfrak{c} satisfies the property (P).
- (2) $cl(F) \times cl(\mathfrak{c})^{-1}$ is d -th power in $Cl(\mathbb{Z}_F)$.

Proof: Let (x_0, y_0, z_0) be a proper solution and \mathfrak{D} its associated ideal, with decomposition $\mathfrak{D} = \mathfrak{c}_1\mathfrak{h}\mathfrak{g}^d$ as given by Theorem 3. Since y_0 is coprime to $\text{Ind}(F)$, it is only contained in invertible prime ideals and $\mathcal{N}_{\mathbb{Z}_F/\mathbb{Z}}(\mathfrak{g}) = y_0$. Consider the ideal $\mathfrak{c} = \mathfrak{c}_1\mathfrak{h}$. Its norm is equal to C and by Proposition 1, it satisfies the property (P). We have now the relation $\mathfrak{b}(x_0 - \theta z_0) = \mathfrak{D} = \mathfrak{c}\mathfrak{g}^d$, whence the relation in the class group. ■

Example: The “only if” part of Theorem 2 is a consequence of our Corollary 2. Indeed, the assumption B squarefree and $B \equiv 1 \pmod{4}$ implies that the binary form $F(x, z) = x^2 + Bz^2$ is irreducible and has index 1. The field K is $\mathbb{Q}(\sqrt{-B})$. The fact that F is monic implies that $cl(F)$ is trivial $Cl(F)$. We get the conclusion of Theorem 2 by writing $J_+ = \mathfrak{c}$ and $J_- = C\mathfrak{c}^{-1}$ in Corollary 2.

We now focus on equation (1), that is on the case $C = 1$ of equation (2). Because this particular case is of some importance, we rewrite the previous results in this case.

Theorem 4. *Let $F(x, z)$ be a primitive irreducible binary form. Let (x_0, y_0, z_0) be a proper solution of (1) and $\mathfrak{D} = \mathfrak{b}(x_0 - \theta z_0)$ its associated ideal in \mathbb{Z}_F . There exist two invertible integral ideals \mathfrak{g} and \mathfrak{h} of \mathbb{Z}_F such that*

- (1) $\mathfrak{D} = \mathfrak{h}\mathfrak{g}^d$
- (2) *the ideals \mathfrak{D} , \mathfrak{g} and \mathfrak{h} satisfy the property (P).*
- (3) *the primes containing \mathfrak{g} are all invertible, whereas those containing \mathfrak{h} are all noninvertible.*
- (4) *if \mathfrak{p} is a prime above p containing \mathfrak{g} , then $v_{\mathfrak{p}}(\mathfrak{g}) = v_{\mathfrak{p}}(y_0)$.*

Corollary 4. *Let $F(x, z)$ be a primitive irreducible binary form. Assume that the polynomial F satisfies the property that all the noninvertible prime ideals \mathfrak{p}_i of \mathbb{Z}_F are such that $f_i > 1$ (this is for example the case if $\text{Ind}(F) = 1$, which is itself the case if $\text{Disc}(F)$ is squarefree).*

A necessary condition for the existence of a nontrivial proper solution of (1) is that $cl(F)$ is d -th power in $Cl(\mathbb{Z}_F)$.

Corollary 5. *Let $F(x, z)$ be a primitive irreducible binary form. A necessary condition for the existence of a nontrivial proper solution (x_0, y_0, z_0) of (1), such that y_0 is coprime to $\text{Ind}(F)$, is that $cl(F)$ is d -th power in $Cl(\mathbb{Z}_F)$.*

Remark: In the case where F is of degree 2, we recover a part of Theorem 1 but with the weaker condition that y_0 is coprime to the $\text{Ind}(F)$ instead of coprime to $\text{Disc}(F)$.

Example: Consider the equation $y^2 = 7x^3 + 10x^2z + 5xz^2 + 6z^3$. In this case, the index is 2. If a solution exists with y odd, then by Corollary 5, $cl(F)$ would be a square in $Cl(\mathbb{Z}_F)$. Through the natural morphism $Cl(\mathbb{Z}_F) \rightarrow Cl(\mathbb{Z}_K)$, we see that the image of $cl(F)$ in $Cl(\mathbb{Z}_K)$ would also be a square. This image is the class of the inverse of the ideal $\mathbb{Z}_K + \theta\mathbb{Z}_K$. Using \mathfrak{gp} ([13]), we find that the group $Cl(\mathbb{Z}_K)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and that the considered class is not a square in $Cl(\mathbb{Z}_K)$. This proves that there is no solution with y odd.

Consider now the existence of a proper solution (x, y, z) with y even. The factorization of F modulo 2 is $x(x - z)^2$. If a proper solution exists with $y \equiv 0 \pmod{2}$, this means that one exactly of the two conditions $x \equiv 0 \pmod{2}$, or $x - z \equiv 0 \pmod{2}$ holds. The case $x \equiv 0 \pmod{2}$ corresponds to the case where the prime ideal above 2 containing \mathfrak{D} is $2\mathbb{Z}_F + \mathfrak{b}\theta\mathbb{Z}_F$. Since this ideal is invertible, we are in the case where this ideal divides \mathfrak{g} , hence $\mathfrak{h} = 1$. We deduce from Theorem 4 that $cl(F)$ must be a square in $Cl(\mathbb{Z}_F)$, a property that we have already proved to be false.

The last case that has to be considered is when $y \equiv x - z \equiv 0 \pmod{2}$. Such a solution exists, for example $(-1, 2, 1)$. This solution satisfies $\mathfrak{b}(\theta - 1) = \mathfrak{D} = \mathfrak{h} = 2\mathbb{Z}_K + \mathfrak{b}^2(\theta - 1)^2$.

3. Examples

3.1. An example with $\text{Ind}(F) = 1$.

Lemma 6. *Let $F(x, z)$ be an homogeneous quartic polynomial in $\mathbb{Z}[x, z]$. The equation $y^2 = F(x, z)$ has nontrivial solutions everywhere locally except maybe over \mathbb{R} , over \mathbb{Q}_2 and over \mathbb{Q}_p for the odd prime numbers p such that $p^2 \mid \text{Disc}(F)$.*

Proof: Let p be an odd prime number. In [12] we find that $y^2 = F(x, z)$ has a nontrivial solution in \mathbb{Q}_p except maybe if $F = 0 \pmod{p}$ or $F = aG^2 \pmod{p}$, with $a \in \mathbb{F}_p^*$ and G is a nontrivial quadratic polynomial over \mathbb{F}_p . In both cases we have $p^2 \mid \text{Disc}(F)$. ■

Proposition 7. *The equation*

$$y^2 = 2x^4 + x^3z + 8x^2z^2 + 2xz^3 + 7z^4$$

is everywhere locally soluble, but has no global solution.

Proof: The discriminant of $F(x, z) = 2x^4 + x^3z + 8x^2z^2 + 2xz^3 + 7z^4$ is $\text{Disc}(F) = 8069$, which is a prime number. The equation clearly has real solutions since the leading coefficient of F is $2 > 0$. We also have $F(17, 1) = 4 \times 43577$, which is a square in \mathbb{Q}_2 (because $43577 \equiv 1 \pmod{8}$). Hence, by Lemma 6, we know that $y^2 = F(x, z)$ is everywhere locally soluble.

The polynomial F is irreducible over \mathbb{Q} . Let θ be a root of $F(\theta, 1) = 0$ and $K = \mathbb{Q}(\theta)$. Since $\text{Disc}(F)$ is squarefree, the ring \mathbb{Z}_F is exactly the ring of integers \mathbb{Z}_K of K . The ideal class group of \mathbb{Z}_K is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, generated precisely by the class of \mathfrak{b} . In this situation, Corollary 4 shows that $y^2 = F(x, z)$ has no proper solution, hence no rational solution at all. ■

This equation is a homogeneous space for an elliptic curve. The I and J invariants of F are $I = 226$ and $J = 6679$, and the corresponding elliptic curve is named “129104b1” in Cremona’s data base [4]. This elliptic curve is known to have rank 0 and analytic order of Sha 4. The present computation shows that this quartic indeed represents a nontrivial element of order 2 in the Tate–Shafaravich group. The same answer could have been obtained using a 4–descent, as described in [12] and implemented in `magma` ([11]) by the function `FourDescent`.

3.2. A family of examples with $\text{Ind}(F) = 1$. We still consider the polynomial F of the previous example, but we also consider

$$G(x, z) = x^4 - 2x^2z^2 - xz^3 + 4z^4$$

This new polynomial defines the same quartic number field K as F . Since it also satisfies $\text{Disc}(G) = 8069 = \text{Disc}(K)$, we have $\mathbb{Z}_F = \mathbb{Z}_G = \mathbb{Z}_K$.

Lemma 8. *Let p be a prime number. The factorizations of F and G modulo p are exactly of the same type.*

Proof: Since $\mathbb{Z}_F = \mathbb{Z}_K$, we know from the results listed in section 1.2 that the factorization of F modulo p into irreducible factors, with given degree and multiplicity, corresponds to the factorization of the ideal $p\mathbb{Z}_K$ into prime ideals, with the same degree and multiplicity. Since we also have $\mathbb{Z}_G = \mathbb{Z}_K$, we get the conclusion. ■

Lemma 9. *Let $k \neq 0$ be a squarefree integer coprime to 8069. The following conditions are equivalent :*

- (i) $ky^2 = F(x, z)$ is everywhere locally soluble.
- (ii) $k > 0$ and if p is a prime divisor of k then $F(x, z)$ has a linear factor modulo p .

Proof: (ii) \Rightarrow (i)

If $k > 0$, then $(x, y, z) = (k^{1/4}, 2^{1/2}, 0)$ is a real solution.

The discriminant of F is equal to the prime number 8069, hence by Lemma 6, we know that $ky^2 = F(x, z)$ is always soluble at finite primes coprime to $2k$.

Let now p be a prime divisor of k . Since $p \neq 8069$, a linear factor of F modulo p lifts to a linear factor $(z_0x - x_0z)$ of F over the p -adics. Then $(x_0, 0, z_0)$ is a local solution of $ky^2 = F(x, z)$.

If $p = 2$, then F has a linear factor, hence the previous argument still works.

(i) \Rightarrow (ii)

If (x_0, y_0, z_0) is a real solution, then $ky_0^2 = F(x_0, z_0) > 0$, since F has no real root. Hence $k > 0$.

Let p be a prime divisor of k and (x_0, y_0, z_0) be a p -adic solution. We may assume that x_0 and y_0 are p -adic integers, not both divisible by p . Since k is squarefree, this implies that y_0 is also a p -adic integer. It is clear that $(z_0x - x_0z)$ is a linear factor of F modulo p . ■

Lemma 10. *Let $k \neq 0$ be a squarefree integer coprime to 8069. The following conditions are equivalent :*

- (i) $ky^2 = F(x, z)$ is everywhere locally soluble.
- (ii) $ky^2 = G(x, z)$ is everywhere locally soluble.

Proof: Exactly the same proof as for Lemma 9 would prove that the local solubility of $ky^2 = G(x, z)$ only depends on the factorization type of G at some places. But by Lemma 8 the factorization types of F and G are identical. Hence they are locally soluble exactly at the same time. ■

Proposition 11. *Let $\mathcal{S} = \{5, 13, 29, 41, 47, 59, 67, 79, 97 \dots\}$ be the set of prime numbers $p \neq 8069$ such that $x^4 - 2x^2 - x + 4$ has a single root modulo p . Let $k > 0$ be a squarefree integer divisible only by primes in \mathcal{S} .*

Then the equations

$$ky^2 = 2x^4 + x^3z + 8x^2z^2 + 2xz^3 + 7z^4$$

and

$$ky^2 = x^4 - 2x^2z^2 - xz^3 + 4z^4$$

are both everywhere locally soluble. However, at most one of them can have a global solution.

Proof: Let k be such an integer. By Lemma 9 and Lemma 10, we know that $ky^2 = F(x, z)$ and $ky^2 = G(x, z)$ are everywhere locally soluble.

In the previous section, we have proved that $cl(F)$ is the nontrivial class in the class group $Cl(K)$ (which is isomorphic to $\mathbb{Z}/2\mathbb{Z}$). On the contrary, since G is monic, $cl(G)$ is the trivial class. Assume now that these equations simultaneously have a rational solution. Applied to $ky^2 = F(x, z)$, Corollary 2 tells us that there exists an integral ideal \mathfrak{c}_F of norm k , such that $cl(\mathfrak{c}_F) = cl(F)$ is nontrivial. According to the section 1.2, the assumption on k implies that there exists a single prime ideal of degree 1 above each prime divisor of k . The ideal \mathfrak{c}_F must be the product of these ideals. Similarly, Corollary 2 applied to $ky^2 = G(x, z)$ tells us that there exists another ideal \mathfrak{c}_G of norm k such that $cl(\mathfrak{c}_G) = cl(G)$ is trivial. The same argument shows that \mathfrak{c}_G is also the product of the prime ideals of degree 1 above the prime factors of k , hence $\mathfrak{c}_G = \mathfrak{c}_F$. This is a contradiction since the class of this ideal should be at the same time trivial and nontrivial. ■

Remark: The Galois group of $x^4 - 2x^2 - x + 4$ is S_4 . Hence, by Frobenius's Theorem [8], the set of primes \mathcal{S} is infinite and has density $\frac{1}{3}$.

Remark: The invariants of F are $I(F) = 226$ and $J(F) = 6779$. Hence $ky^2 = F(x, z)$ corresponds to a homogeneous space for the elliptic curve $\mathcal{F}_k : ky^2 = x^3 - 27 \cdot 226x - 27 \cdot 6779$. Similarly, the invariants of G are $I(G) = 52$ and $J(G) = -587$. Hence $ky^2 = G(x, z)$ corresponds to a homogeneous space for the elliptic curve $\mathcal{G}_k : ky^2 = x^3 - 27 \cdot 52x + 27 \cdot 587$. Proposition 11 shows that for the given values of k , the homogeneous spaces are elements of the 2-Selmer groups of \mathcal{F}_k and \mathcal{G}_k , and that at least one of them corresponds to a nontrivial element of order 2 in the Tate-Shafarevich group. It is interesting to observe that the j -invariant of the elliptic curve \mathcal{F}_k is $2^{14}13^38069^{-1}$, whereas for \mathcal{G}_k it is equal to $2^{11}113^38069^{-1}$, hence the curves are not isomorphic over \mathbb{C} . The conductor of \mathcal{F}_1 is 2^48069 , whereas the conductor of \mathcal{G}_1 is 2^28069 , hence the curves are not isogenous.

Remark: The same kind of result can be obtained for the following examples, where the class group of the corresponding field is always isomorphic to $\mathbb{Z}/2\mathbb{Z}$, the class of F is nontrivial and the class of G is trivial. In this table, a horizontal line is used to separate forms that generate different number fields. I do not know the origin of the symmetries that appear in this table.

Disc	F	$I(F)$	$J(F)$	G	$I(G)$	$J(G)$
8069	$2x^4 + x^3 + 8x^2 + 2x + 7$	226	6679	$x^4 - 2x^2 - x + 4$	52	-587
8069	$2x^4 + x^3 + 8x^2 + 2x + 7$	226	6679	$x^4 + 6x^2 + x + 8$	132	2997
8069	$3x^4 + 2x^3 + 8x^2 + 3x + 5$	226	6679	$x^4 + x^3 + x^2 - 5x + 3$	52	-587
8069	$3x^4 + 2x^3 + 8x^2 + 3x + 5$	226	6679	$x^4 + x^3 + 6x^2 + 4x + 9$	132	2997
7537	$2x^4 + x^3 + 4x^2 + x + 3$	85	1501	$x^4 + 5x^2 + x + 4$	73	1163
7537	$2x^4 + x^3 + 4x^2 + x + 3$	85	1501	$x^4 + 2x^3 - 3x^2 - 5x + 6$	111	-2295
7537	$2x^4 + 3x^3 + 7x^2 + 4x + 3$	85	1501	$x^4 + x^3 + 5x^2 + 4x + 5$	73	1163
7537	$2x^4 + 3x^3 + 7x^2 + 4x + 3$	85	1501	$x^4 + 3x^3 - 7x + 4$	111	-2295

3.3. A collection of examples with $Ind(F) = 1$. In this section, we give a collection of examples illustrating Corollary 4. All the following examples are about the proper solutions of equations of the form (1) where F is an homogeneous irreducible polynomial with integral coefficients, such that the index $Ind(F)$ is trivial. If $cl(F)$ is not the trivial class, then Corollary 4 tells us that a necessary condition for the existence of proper solutions to (1) is that d is not a multiple of some integer k .

The following table gives a list of polynomials F , together with the structure of the class group $Cl(\mathbb{Z}_F) = Cl(K)$ as the product of cyclic groups, and the image of $cl(F)$ in this group as given by **gp**. From these values, the best value of k just defined is easy to determine. Since we have not observed any dependence on the signature of F , the polynomials given have the smallest possible number of real roots.

Disc(F)	F	$Cl(K)$	$cl(F)$	k
-648	$2x^3 + 3x^2 + 2$	$\mathbb{Z}/3\mathbb{Z}$	(1)	3
-1879	$2x^3 + x^2 - x + 4$	$\mathbb{Z}/4\mathbb{Z}$	(2)	4
-1572	$2x^3 + 2x^2 + x + 4$	$\mathbb{Z}/5\mathbb{Z}$	(2)	5
-2856	$2x^3 + 2x^2 + 5x - 3$	$\mathbb{Z}/7\mathbb{Z}$	(3)	7
-18628	$4x^3 - 9x^2 + 4x + 7$	$\mathbb{Z}/8\mathbb{Z}$	(4)	8
-22443	$8x^3 + 5x^2 - 3x + 3$	$\mathbb{Z}/9\mathbb{Z}$	(3)	9
-12244	$3x^3 - 4x^2 + 7x + 4$	$\mathbb{Z}/11\mathbb{Z}$	(1)	11
-19919	$2x^3 - 5x^2 + 7x + 10$	$\mathbb{Z}/12\mathbb{Z}$	(2)	3 or 4
-9064	$5x^3 - 4x^2 - 5x + 6$	$\mathbb{Z}/13\mathbb{Z}$	(9)	13

It is surprising that, despite of quite a long search, we have not been able to find the least example in degree 3 with $k = 2$, and more generally where

$cl(F)$ is not a square in $Cl(K)$.

Disc(F)	F	$Cl(K)$	$Cl(F)$	k
2448	$2x^4 + 2x^3 - 5x^2 - 2x + 5$	$\mathbb{Z}/2\mathbb{Z}$	(1)	2
13785	$4x^4 - 3x^3 + 14x^2 - 5x + 11$	$\mathbb{Z}/3\mathbb{Z}$	(1)	3
14504	$4x^4 - 5x^3 - 6x^2 + 5x + 4$	$\mathbb{Z}/4\mathbb{Z}$	(2)	4
13396	$2x^4 - 2x^3 + 6x^2 - 3x + 5$	$\mathbb{Z}/5\mathbb{Z}$	(3)	5
43245	$2x^4 - 3x^3 + x^2 + 3x + 2$	$\mathbb{Z}/6\mathbb{Z}$	(1)	2 or 3
25205	$2x^4 - x^3 + 5x^2 + x + 2$	$\mathbb{Z}/7\mathbb{Z}$	(1)	7
438445	$3x^4 - 2x^3 + 8x^2 + x + 4$	$\mathbb{Z}/8\mathbb{Z}$	(4)	8
235901	$2x^4 - x^3 - 7x^2 + x + 10$	$\mathbb{Z}/9\mathbb{Z}$	(3)	9
77648	$2x^4 - 6x^3 + 5x^2 + 10x + 3$	$\mathbb{Z}/10\mathbb{Z}$	(7)	2 or 5
330781	$3x^4 - 4x^3 + 4x^2 + 5x + 2$	$\mathbb{Z}/11\mathbb{Z}$	(1)	11
122728	$4x^4 + 3x^3 - 6x^2 - 3x + 4$	$\mathbb{Z}/12\mathbb{Z}$	(10)	3 or 4
146548	$2x^4 - 2x^3 + 8x^2 - x + 3$	$\mathbb{Z}/13\mathbb{Z}$	(12)	13
141681	$3x^4 - 4x^3 + 11x^2 - 5x + 7$	$\mathbb{Z}/14\mathbb{Z}$	(3)	2 or 7

Disc(F)	F	$Cl(K)$	$cl(F)$	k
212449	$5x^5 - 11x^4 + 11x^3 + 2x^2 - 9x + 7$	$\mathbb{Z}/3\mathbb{Z}$	(1)	3
3374829	$3x^5 + 4x^4 + 5x^3 - 2x^2 - 3x - 3$	$\mathbb{Z}/4\mathbb{Z}$	(2)	4
753652	$2x^5 + x^4 - x^3 - x^2 - x - 2$	$\mathbb{Z}/5\mathbb{Z}$	(3)	5
3013976	$2x^5 + 3x^4 - 3x^3 - x^2 + 2x + 2$	$\mathbb{Z}/7\mathbb{Z}$	(6)	7
36204064	$2x^5 - 2x^4 - 5x^3 + 4x^2 + 3x + 4$	$\mathbb{Z}/8\mathbb{Z}$	(4)	8
41417024	$4x^5 - 3x^4 + 10x^3 + x^2 + 4x + 6$	$\mathbb{Z}/9\mathbb{Z}$	(3)	9
12714804	$2x^5 - 3x^4 + 5x^3 - 3x^2 + x + 4$	$\mathbb{Z}/11\mathbb{Z}$	(3)	11
20601837	$2x^5 + 3x^4 + 2x^3 - 2x^2 - 3x + 4$	$\mathbb{Z}/12\mathbb{Z}$	(10)	3 or 4
10677952	$2x^5 + 2x^4 + 3x^3 - 3x^2 + 2x + 2$	$\mathbb{Z}/13\mathbb{Z}$	(8)	13
63632529	$2x^5 - 3x^4 + 11x^3 - 6x^2 + 7x + 4$	$\mathbb{Z}/15\mathbb{Z}$	(2)	3 or 5

Similarly to the degree 3 case, $cl(F)$ is always a square in $Cl(K)$.

Disc(F)	F	$Cl(K)$	$cl(F)$	k
-8923959	$2x^6 - 5x^5 + 6x^4 - 3x^3 + x^2 - x + 2$	$\mathbb{Z}/2\mathbb{Z}$	(1)	2
-4936112	$2x^6 - 3x^5 + x^4 - 4x^3 + 2x^2 + x + 3$	$\mathbb{Z}/3\mathbb{Z}$	(2)	3
-37462463	$3x^6 + x^5 + 5x^4 + 4x^3 + 7x^2 + 3x + 2$	$\mathbb{Z}/4\mathbb{Z}$	(2)	4
-31859379	$2x^6 + x^5 - 3x^4 - 4x^3 + 2x^2 + 3x + 2$	$\mathbb{Z}/5\mathbb{Z}$	(4)	5
-25016224	$2x^6 - 2x^5 - x^4 + x^3 - x^2 + x + 2$	$\mathbb{Z}/6\mathbb{Z}$	(5)	2 or 3
-22115792	$2x^6 - x^5 + 5x^4 + x^3 + 5x^2 + x + 3$	$\mathbb{Z}/7\mathbb{Z}$	(6)	7
-575577900	$3x^6 + 3x^3 + 4x^2 - 3x + 3$	$\mathbb{Z}/8\mathbb{Z}$	(4)	8
-765513112	$2x^6 - x^5 + 4x^4 - 2x^3 + x^2 + 4x + 2$	$\mathbb{Z}/9\mathbb{Z}$	(6)	9
-96526268	$3x^6 + 2x^5 - x^4 - x^3 - 2x^2 - x + 2$	$\mathbb{Z}/10\mathbb{Z}$	(1)	2 or 5
-181202524	$2x^6 + 4x^4 - x^3 + x^2 + x + 2$	$\mathbb{Z}/11\mathbb{Z}$	(9)	11
-162484272	$2x^6 - x^5 + 4x^3 + 2x^2 + 2$	$\mathbb{Z}/12\mathbb{Z}$	(10)	3 or 4
-293129280	$3x^6 + 3x^2 - 2x + 2$	$\mathbb{Z}/13\mathbb{Z}$	(6)	13
-150393564	$3x^6 - x^4 + x^3 - 2x^2 - x + 2$	$\mathbb{Z}/14\mathbb{Z}$	(9)	2 or 7

Similar tables were also obtained for higher degrees. In all the cases we have looked at, we could make the same observation :

Observation 12. *If F is a primitive integral irreducible polynomial with index $Ind(F) = 1$ and with odd degree, then $cl(F)$ is a square in $Cl(K)$.*

This condition that the class of an ideal is always a square in the class group reminds us of a result of Hecke [9, Th. 176].

Theorem 5 (Hecke). *Let K be a number field with ring of integers \mathbb{Z}_K . The class of the different of \mathbb{Z}_K in the class group $Cl(K)$ is always a square.*

Thus we will now investigate a relation between our ideal \mathfrak{b} and the different of \mathbb{Z}_F .

4. The Different of \mathbb{Z}_F and a proof of the observation

The codifferent (or the dual) of a submodule $M \subset K$ is by definition the set

$$M' = \{x \in K, Tr_{K/\mathbb{Q}}(xM) \subset \mathbb{Z}\}.$$

If $M = \sum \mathbb{Z}w_i$, where w_1, \dots, w_n is a \mathbb{Q} -basis of K , then $M' = \sum \mathbb{Z}w'_i$, where w'_1, \dots, w'_n is the dual basis relative to the trace $Tr_{K/\mathbb{Q}}$.

We want to compute the codifferent of the ring \mathbb{Z}_F . For this, we will compute the dual basis of $(1, P_1(\theta), \dots, P_{n-1}(\theta))$, where the the polynomials P_i were already defined in section 1.1 from $P(x) = F(x, 1) = a_0x^n + a_1x^{n-1} +$

... + a_n by

$$\begin{aligned} P_0 &= a_0 \\ P_1 &= a_0x + a_1 \\ &\dots \\ P_{n-1} &= a_0x^{n-1} + \dots + a_{n-1} \\ P_n &= a_0x^n + \dots + a_{n-1}x + a_n = P(x) \end{aligned}$$

Proposition 13. *The dual basis of $(P_0(\theta), P_1(\theta), \dots, P_{n-1}(\theta))$, is*

$$\left(\frac{\theta^{n-1}}{P'(\theta)}, \frac{\theta^{n-2}}{P'(\theta)}, \dots, \frac{\theta}{P'(\theta)}, \frac{1}{P'(\theta)} \right)$$

Proof: We have the relation

$$P(x) = (x - \theta)(P_{n-1}(\theta) + P_{n-2}(\theta)x + \dots + P_1(\theta)x^{n-2} + P_0(\theta)x^{n-1})$$

hence we can apply [10, prop III.2] and deduce that the dual basis of $1, \theta, \dots, \theta^{n-1}$ is

$$\left(\frac{P_{n-1}(\theta)}{P'(\theta)}, \frac{P_{n-2}(\theta)}{P'(\theta)}, \dots, \frac{P_0(\theta)}{P'(\theta)} \right)$$

from which we we easily deduce the result. ■

Proposition 14. *A \mathbb{Z} -basis of the codifferent of \mathbb{Z}_F is given by*

$$\frac{1}{P'(\theta)}, \frac{\theta}{P'(\theta)}, \dots, \frac{\theta^{n-2}}{P'(\theta)}, \frac{a_0\theta^{n-1}}{P'(\theta)}$$

It is equal to the fractionnal ideal $(\mathfrak{b}^{n-2}P'(\theta))^{-1}$ of \mathbb{Z}_F .

Proof: A \mathbb{Z} -basis of \mathbb{Z}_F is by definition $1, P_1(\theta), \dots, P_{n-1}(\theta)$. By Proposition 13, we indeed find that its dual is given by $\frac{1}{P'(\theta)}I$, where $I = \mathbb{Z} \oplus \theta\mathbb{Z} \oplus \dots \oplus \theta^{n-2}\mathbb{Z} \oplus a_0\theta^{n-1}\mathbb{Z}$. First, we remark that $P_i(\theta) \in I$ for all $i = 0, \dots, n-1$, hence $\mathbb{Z}_F \subset I$. Now, we extend the sequence a_i to subscripts $i \geq n+1$ by $a_i = 0$, and we can also define P_i for large values of i by $P_i = a_0x^i + a_1x^{i-1} + \dots + a_i$. For $i \geq n$, we have $P_i(\theta) = 0$, and certainly $P_i(\theta) \in I$ for all $i \geq 0$. Now, we have $\theta^j P_i(\theta) = P_{i+j}(\theta) - (a_{i+1}\theta^{j-1} + \dots + a_{i+j}\theta^0) \in I$ for all i and all $j \leq n-2$. For $j = n-1$, the same relation shows that $a_0\theta^{n-1}P_i(\theta) \in I$. This proves that I is a fractional ideal of \mathbb{Z}_F . We can now write

$$\begin{aligned} I &= \mathbb{Z} \oplus \theta\mathbb{Z} \oplus \dots \oplus \theta^{n-2}\mathbb{Z} \oplus a_0\theta^{n-1}\mathbb{Z} \\ &= \mathbb{Z}_F + \theta\mathbb{Z}_F + \dots + \theta^{n-2}\mathbb{Z}_F + a_0\theta^{n-1}\mathbb{Z}_F \\ &= \mathbb{Z}_F + \left(\frac{\mathfrak{a}}{\mathfrak{b}}\right) + \dots + \left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)^{n-2} + a_0 \left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)^{n-1} \end{aligned}$$

But \mathfrak{a} and \mathfrak{b} are coprime integral ideals in \mathbb{Z}_F , hence

$$\begin{aligned} I &= \left(\frac{1}{\mathfrak{b}}\right)^{n-2} + a_0 \left(\frac{\mathfrak{a}}{\mathfrak{b}}\right)^{n-1} \\ &= \left(\frac{1}{\mathfrak{b}}\right)^{n-1} (\mathfrak{b} + a_0\mathfrak{a}^{n-1}) \\ &= \left(\frac{1}{\mathfrak{b}}\right)^{n-1} (\mathfrak{b} + a_0\mathbb{Z}_F) \end{aligned}$$

By definition of \mathfrak{b} , we have $a_0 \in \mathfrak{b}$, hence $\mathfrak{b} + a_0\mathbb{Z}_F = \mathfrak{b}$, whence the relation

$$I = \mathfrak{b}^{-(n-2)}$$

■

Corollary 15. *The different of \mathbb{Z}_F is the ideal $\mathfrak{b}^{n-2}P'(\theta)$ of \mathbb{Z}_F .*

Corollary 16. *Let K be a number field. If \mathbb{Z}_K is equal to \mathbb{Z}_F for some polynomial F , then the class of the different of \mathbb{Z}_K in the class group $Cl(K)$ is an $(n - 2)$ th power.*

For quadratic extensions, this says that the different is always a principal ideal, but this is well known. For larger degrees, it is well known that if $\mathbb{Z}_K = \mathbb{Z}[\theta]$ for some algebraic integer θ , then the different is principal, generated by $P'(\theta)$, where P is the minimal polynomial of θ . This corollary gives a generalization of this result for rings of integers of the type \mathbb{Z}_F for a nonmonic polynomial.

For number fields of even degree, Corollary 15 gives explicitly a square root of the class the different in $Cl(K)$, the existence of which being proved by Hecke in Theorem 5.

We are now able to prove that Observation 12 is always true.

Corollary 17. *Let F be a primitive irreducible polynomial with integral coefficients. If the degree of F is odd and $Ind(F) = 1$, then $cl(F)$ is a square in $Cl(K)$.*

Proof: By Theorem 5, we know that the class of the different of \mathbb{Z}_F in $Cl(K)$ is a square. By Corollary 15, this different is $\mathfrak{b}^{n-2}P'(\theta)$. Since $n - 2$ is odd, we conclude that the class of \mathfrak{b} is a square in $Cl(K)$. ■

Example: In section 2, we have considered the polynomial $F = 7x^3 + 10x^2z + 5xz^2 + 6z^3$, having index 2. The class $cl(F)$ was proved to be not equal to a square in $Cl(\mathbb{Z}_F)$, because its image in $Cl(\mathbb{Z}_K)$ was also not a square. We deduce that the class of the different of \mathbb{Z}_F is not a square, neither in $Cl(\mathbb{Z}_F)$, nor its image in $Cl(\mathbb{Z}_K)$.

From this example, we know that it is false in general that the class of the different is a square when the index is not 1.

We now investigate the relation between the different \mathfrak{d}_K of \mathbb{Z}_K and the different \mathfrak{d}_F of \mathbb{Z}_F . Let \mathfrak{f} be the conductor ideal of the nonmaximal order \mathbb{Z}_F . It can be defined as the largest ideal (in the sense of inclusion) of \mathbb{Z}_K which is contained in \mathbb{Z}_F . I use the notation \mathfrak{b}_K for $\mathfrak{b}\mathbb{Z}_K$.

Proposition 18. *The different \mathfrak{d}_F is an invertible ideal of \mathbb{Z}_F , satisfying the relations*

$$\mathfrak{d}_F\mathbb{Z}_K = \mathfrak{f}\mathfrak{d}_K = \mathfrak{b}_K^{n-2}P'(\theta)$$

Proof: By [14, Th. 4.34], the dual of \mathfrak{f} is the fractional ideal $\mathfrak{f}^{-1}\mathfrak{d}_K^{-1}$ of \mathbb{Z}_K . Since \mathfrak{f} is the largest fractional ideal of \mathbb{Z}_K contained in \mathbb{Z}_F , its dual is the smallest fractional ideal of \mathbb{Z}_K containing the codifferent of \mathbb{Z}_F . Hence, by Proposition 14 we have $\text{Codiff}(\mathbb{Z}_F)\mathbb{Z}_K = \mathfrak{f}^{-1}\mathfrak{d}_K^{-1} = (\mathfrak{b}^{n-2}P'(\theta)\mathbb{Z}_K)^{-1} = (\mathfrak{b}_K^{n-2}P'(\theta))^{-1}$. ■

Using this description of the different of \mathbb{Z}_F , we can now give a generalization of Corollary 17 in the case where $\text{Ind}(F) \neq 1$.

Corollary 19. *Let F be an irreducible polynomial with integral coefficients. We assume that F is primitive. If the degree of F is odd, then $cl(\mathfrak{fb}_K)$ is a square in $Cl(K)$.*

Proof: By Theorem 5, we know that the class $cl_K(\mathfrak{d}_K)$ in $Cl(K)$ is a square. By Corollary 15, we know that $cl(\mathfrak{fb}_K^{n-2})$ is also a square in $Cl(K)$. Since $n - 2$ is odd, we conclude that the class of \mathfrak{fb}_K is a square in $Cl(K)$. ■

Références

- [1] B.J. Birch and H.P.F. Swinnerton-Dyer : *Notes on elliptic curves*, J. Reine Angew. Math. 212 (1963), 7–25.
- [2] J.W.S. Cassels : *Rational Quadratic Forms*, L.M.S. Monographs, Academic Press (1978).
- [3] J.E. Cremona : *Algorithms for Modular Elliptic Curves*, Cambridge University Press (1997), Second Edition.
- [4] J.E. Cremona : *Elliptic Curve Data*, <http://modular.math.washington.edu/cremona/INDEX.html>
- [5] H. Cohen : *Number Theory. Vol I : Tools and Diophantine Equations*, GTM **239**, Springer Verlag (2007).
- [6] H. Darmon, A. Granville : *On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$* , Bull. London Math. Soc **27** (1995), 513–543.
- [7] I. Delcorso, R. Dvornicich and D. Simon : *The decomposition of primes in nonmaximal orders*, Acta Arithmetica **120** (2005), 231–244.
- [8] F. G. Frobenius : *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe*, Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin (1896), 689–703; Gesammelte Abhandlungen II, 719–733.
- [9] E. Hecke : *Vorlesungen über die Theorie der algebraischen Zahlen*, 2te Unveränderte Auflage (1954), Leipzig, Akademische Verlagsgesellschaft (1923).
- [10] S. Lang : *Algebraic number theory*, GTM 110, second edition, New York, Springer-Verlag (1994).
- [11] MAGMA Computational Algebra System : <http://magma.maths.usyd.edu.au/magma/>
- [12] J. R. Merriman, S. Siksek and N. P. Smart : *Explicit 4-descent on an elliptic curve*, Acta Arithmetica **77** (1996), 385–404.
- [13] `pari/gp`, The Pari group (K. Belabas, H. Cohen,...), <http://pari.math.u-bordeaux.fr/>
- [14] I. Reiner : *Maximal Orders*, L.M.S. Monographs, Academic Press (1975).
- [15] D. Simon : *La classe invariante d'une forme binaire*, Comptes Rendus Mathématiques, **336**, Issue 1 , (2003) 7–10.

Université de Caen – France
Campus II – Boulevard Mal Juin
BP 5186 – 14032 Caen Cedex
E-mail : `simon@math.unicaen.fr`