Journal of Number Theory 131 (2011) 2303–2309

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Hyperelliptic curves and homomorphisms to ideal class groups of quadratic number fields

Tormod Kalberg Sivertsen [1], Ragnar Soleng *

University of Tromsø, 9037 Tromsø, Norway

ARTICLE INFO

Article history:
Received 15 February 2010
Accepted 11 May 2011
Available online 11 August 2011
Communicated by Michael E. Pohst

Keywords:
Hyperelliptic curves
Quadratic fields
Ideal class groups

ABSTRACT

For the function field K of hyperelliptic curves over $\mathbb{Q}$ we define a subgroup of the ideal class group called the group of $\mathbb{Z}$-primitive ideals. We then show that there are homomorphisms from this subgroup to ideal class groups of certain quadratic number fields.

1. Introduction

Let $D(x) = x^{2g+1} + d_{2g}x^{2g} + \cdots + d_1x + d_0$ be a square-free polynomial of odd degree defined over the rational integers $\mathbb{Z}$. Let C be the hyperelliptic curve defined by the equation

$$y^2 = D(x).$$

The ideal class group of $K = \mathbb{Q}(C)$ is isomorphic to the Jacobian $J(C)$ and also to the group of strict ideal classes of binary quadratic forms over $\mathbb{Z}[x]$ of discriminant D (see [3]).

Each ideal class can be represented by an integral ideal of the form $(A, y - B/n)$ where $A, B \in \mathbb{Z}[x]$ and $n \in \mathbb{Z}$ such that $B^2 - n^2D = AC$ for some polynomial $C \in \mathbb{Z}[x]$. Only ideals such that the greatest common divisor $\gcd(A, B, C) = 1$ are considered. For square-free discriminants $D(x)$, this always is the case.

In the case of elliptic curves ($g = 1$) the Jacobian is also isomorphic to the group of rational points on the curve. In [2], this situation was studied and it was shown that there is a homomorphism from

* Corresponding author.
E-mail addresses: Tormod-Kalberg.Sivertsen@ffi.no (T.K. Sivertsen), ragnar@math.uit.no (R. Soleng).
[1] Present address: Norwegian Defence Research Establishment, 2027 Kjeller, Norway.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2011.05.002

the group of rational points on C to the ideal class group of the order $\mathbb{Z}[\sqrt{d_0}]$ of the quadratic field $\mathbb{Q}(\sqrt{d_0})$. This was done under the assumption that the constant term d_0 is square-free. The order $\mathbb{Z}[\sqrt{d_0}]$ has even discriminant $\Delta = 4d_0$.

The result above was rediscovered in [5], and generalized in the sense that the restriction to square-free d_0 was removed. This was made possible by restricting the homomorphism to a subgroup of the rational points called the group of *primitive* points. If d_0 is square-free, all points are primitive.

In [4] elliptic curves of the form $y^2 + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with odd a_3 were studied. It was shown that there is a homomorphism from the group of primitive points on such curves to the ideal class group of $\mathbb{Q}(\sqrt{\Delta})$ for $\Delta = a_3^2 + 4a_6$. Notice that the discriminant $\Delta = a_3^2 + 4a_6$ is odd.

Hyperelliptic curves were considered in [1]. Rational points on the curve are mapped to ideals in $\mathbb{Q}(\sqrt{d_0})$ in the same way as in the above articles, and a subgroup S of the class group Cl of $\mathbb{Q}(\sqrt{d_0})$ is defined to be generated by certain "exceptional" primes. It is proven that if all the points of intersection of a straight line with the curve are rational, then the product of the ideals derived from these collinear points is the identity of Cl/S.

In this article we generalize the above results to hyperelliptic curves. We consider hyperelliptic curves of odd degree and we prove that there is a homomorphism from a subgroup of the ideal class group of K to the ideal class group of the order $\mathbb{Z}[\sqrt{d_0}]$. Under a reasonable restriction the result is valid also for even degree curves.

2. Main theorem

For polynomials $A(x)$, $B(x)$, etc., we make the convention that $a = A(0)$, $b = B(0)$, etc. For the above polynomial $D(x)$ we then have $D(0) = d_0 = d$.

Let $\mathcal{O}_K = \mathbb{Q}[x, y]/(y^2 - D(x))$ denote the ring of integers in K. For the quadratic number field $k = \mathbb{Q}(\sqrt{d})$, we let $\mathcal{O}_k = [1, \sqrt{d}]$. This may or may not be the maximal order in k. A subring of $\mathcal{O}_k$ is in general denoted by $\mathcal{O}$, and if we consider a special conductor n, we denote it by $\mathcal{O}_n$.

For an ideal I of $\mathcal{O}_K$, the notation $I = [\alpha_1, \alpha_2]$ means that I is generated as a $\mathbb{Q}[x]$-module by α_1 and α_2. The notation $I = (\alpha_1, \alpha_2)$ means that I is generated as an $\mathcal{O}_K$-module by α_1 and α_2. The same convention is adopted for ideals in $\mathcal{O}_k$ and $\mathcal{O}_n$ with $\mathbb{Q}[x]$ replaced by $\mathbb{Z}$.

For a polynomial $T(x) = a_tx^t + a_{t-1}x^{t-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$, the content of $T(x)$ is $cont(T) = \gcd(a_t, a_{t-1}, \ldots, a_1, a_0)$.

Definition 2.1. An ideal $[A, y - B/n]$ with $B^2 - n^2D = AC$, is said to be in $\mathbb{Z}$-primitive form if $\gcd(a, 2b, c) = 1$. We say that the class of $[A, y - B/n]$ is $\mathbb{Z}$-primitive if it contains an ideal in $\mathbb{Z}$-primitive form.

Proposition 2.2. *The set of $\mathbb{Z}$-primitive ideal classes is a subgroup of the ideal class group of $\mathcal{O}_K$.*

To prove this proposition, we will need the tools developed in the proof of the main theorem. The proof is included in Section 3.

Lemma 2.3.

(a) *Let $I = [A, y - B/n]$ be an ideal of $\mathcal{O}_K$ and let M be any polynomial in $\mathbb{Z}[x]$. Then there is an equivalent ideal $[A', y - B'/n]$ with A' prime to M.*
(b) *Let $I = [A, y - B/n]$ be a $\mathbb{Z}$-primitive ideal of $\mathcal{O}_K$ and let m be any integer. Then there is an equivalent ideal $[A', y - B'/n']$ such that $\gcd(a', m) = 1$.*

Proof. (a) is a standard result from the literature. See for example [3]. We give the proof of (b).

By Lemma 3.2 below we may assume $n = 1$. Let $m = m_1m_2 \cdots m_r$ where each m_i is a power of a prime p_i. The binary quadratic form associated to $I = [A, y - B]$ is $q = AX^2 + 2BXY + CY^2$. It will be sufficient to find coprime (u, v) in $\mathbb{Z}^2$ such that $q(u, v)(0)$ is prime to m. To see this, let r and s be integers such that $us - rv = 1$. Then $q' = q(uX + vY, rX + sY) = A'X^2 + 2B'XY + C'Y^2$ is equivalent to q, and $A' = q(u, v)$.

If we can find, for each i, coprime integers u_i, v_i such that $d_i = q(u_i, u_i)(0)$ is prime to m_i, we can, by the Chinese remainder theorem, find u and v in $\mathbb{Z}$ such that

$$(u, v) \equiv (u_i, v_i) \bmod m_i.$$

Then $q(u, v)(0) \equiv d_i \bmod m_i$, so $q(u, v)(0)$ is prime to m.

Hence, we may assume that m is a prime p. Since q is a $\mathbb{Z}$-primitive quadratic form, i.e. $\gcd(a, 2b, c) = 1$, at least one of a, $a + 2b + c$ or c is prime to p. Thus, at least one $(u, v) \in \{(1, 0), (1, 1), (0, 1)\}$ gives $q(u, v)(0)$ prime to p. Note that primes dividing both u and m cannot divide v.

To finish the proof we have to prove that there are solutions (u, v) with $\gcd(u, v) = 1$. Assume we have a solution with $u > v$ and let $d = \gcd(u, m)$. We may replace u by any integer of the form $u + km$. By the Dirichlet theorem we may choose one such that $u' = u + km = dq$ for a prime q. Also we may choose $q > v$ and therefore v is prime to u'. This proves (b). $\square$

Proposition 2.4. *If an ideal $I = [A, y - B/n]$ is in $\mathbb{Z}$-primitive form, then* $\gcd(a, c, n) = 1$. *If d is square-free, then all ideal classes are $\mathbb{Z}$-primitive.*

Proof. Since $b^2 - n^2 d = ac$, any common prime factor of a and n will divide b also. Then it cannot divide c. Let $I = [A, y - B/n]$ be any ideal. By the above lemma we may assume that $\gcd(a, 2n) = 1$. If an odd prime p divides $\gcd(a, 2b, c)$, then since $b^2 - n^2 d = ac$, p^2 divides $n^2 d$. If d is square-free, this cannot happen. $\square$

Let $I = [A, y - B/n]$ be an ideal of $\mathcal{O}_K$ such that $\gcd(a, n, c) = 1$. Putting $x = 0$ in $B^2 - AC = n^2 D$ we get an ideal $J = [a, nw - b]$, $w^2 = d$, in $\mathcal{O}_n$, such that $b^2 - ac = n^2 d$.

Thus, we have a mapping φ sending the ideal $I = [A, y - B/n]$ of $\mathcal{O}_K$ to the ideal $J' = J\mathcal{O}_k$ of $\mathcal{O}_k$. This ideal is also equal to the $\mathcal{O}_k$ ideal $(a, nw - b)$.

We will prove that the mapping φ is indeed a homomorphism from ideal classes of $\mathcal{O}_K$ to ideal classes of $\mathcal{O}_k$. In particular it is well defined on ideal classes.

Main Theorem 2.1. *With the above notation, the mapping φ, sending the ideal $I = [A, y - B/n]$ of $\mathcal{O}_K$ to the ideal $J = (a, nw - b)$ in $\mathcal{O}_k$, is a homomorphism from the group of $\mathbb{Z}$-primitive ideal classes of $\mathcal{O}_K$ to ideal classes of $\mathcal{O}_k$.*

3. Proof of main theorem

By Proposition 2.4 we may assume that $\gcd(a, n, c) = 1$. We must prove that the mapping φ is independent of the representative of the ideal class, as long as the representative $I = [A, y - B/n]$ satisfies $\gcd(a, n, c) = 1$. Then we show that the mapping is multiplicative.

We begin with some preliminary lemmas.

Lemma 3.1. *Let $I = [A, y - B/n]$ be an ideal with* $\gcd(a, n, c) = 1$ *which maps to $J \subset \mathcal{O}_k$. Then, there is an equivalent ideal $I' = [A', y - B'/n]$ with* $\gcd(a', n) = 1$, *which maps to an ideal in $\mathcal{O}_k$, equivalent to J.*

Proof. Let $I = [A, y - B/n]$ satisfy $\gcd(a, n, c) = 1$ and write $n = n_1 n_2$ with $\gcd(a, n_1) = 1$, $\gcd(c, n_2) = 1$. If any prime factor of n_2 does not divide a, then we may transfer it to n_1. Hence, we may assume that all prime factors of n_2 divide a. Since $b^2 - ac = n^2 d$, all prime factors of n_2 also divide b. The ideal $I' = [A + 2Bn_1 + Cn_1^2, y - (B + Cn_1)/n]$ is equal to I and $a + 2bn_1 + cn_1^2$ is prime to n. Obviously the $\mathcal{O}_n$ ideal $[a + 2bn_1 + cn_1^2, nw - (b + c)]$ is equal to $[a, nw - b]$. Multiplication by $\mathcal{O}_k$ will give equivalent ideals in $\mathcal{O}_k$. $\square$

The next lemma shows that for an ideal $I = [A, y - B/n]$, we can find an equivalent ideal $I' = [A', y - B'/n']$ with n' as small as we desire, $n' = 1$ being no exception.

Lemma 3.2. *Let $I = [A, y - B/n]$, $n > 1$, be any $\mathcal{O}_K$ ideal. Then there exists an ideal $I' = [A', y - B'/n']$, equivalent to I such that n' divides n, and $n' < n$.*

Proof. Let p be a prime number dividing n. For a polynomial $T \in \mathbb{Z}[x]$ we denote by $\bar{T}$ the image of T in $\mathbb{Z}/p\mathbb{Z}[x]$ (reduction modulo p). Since $B^2 - AC = n^2 D$ we have $\bar{B}^2 = \bar{A}\bar{C}$. Then $2\deg\bar{B} = \deg\bar{A} + \deg\bar{C}$. Now, either all three degrees are equal, or either $\deg\bar{A}$ or $\deg\bar{C}$ is less than $\deg\bar{B}$. If $\deg\bar{C} < \deg\bar{B}$ we can replace $I = [A, y - B/n]$ by the equivalent ideal $[C, y + B/n]$.

Hence we may assume $\deg\bar{A} \leqslant \deg\bar{B}$. Write $\bar{B} = \bar{A}\bar{Q} + \bar{R}$ with $\bar{R} \in \mathbb{Z}/p\mathbb{Z}[x]$ satisfying $\deg\bar{R} < \deg\bar{A}$, and let Q be a lifting of $\bar{Q}$ to $\mathbb{Z}[x]$. We have $I = [A, y - B'/n']$ where $B'/n' = (B - AQ)/n$. Let $v_p(n)$ be the order of n at p. If $\bar{R} = 0$, we have $v_p(n') < v_p(n)$. If $\bar{R} \neq 0$, we have $\deg\bar{B}' = \deg\bar{R} < \deg\bar{B}$ and we repeat the process until $\bar{R} = 0$. $\square$

Example 3.3. Consider the ideal $[25x - 19, -\frac{103}{125} + y]$ of discriminant $x^3 - x + 1$ and $p = 5$. We have $\bar{A} = 1$, $\bar{B} = 3 = -2 * \bar{A}$. We replace B by $B + 2A = 50x + 65$. This gives the ideal $[25x - 19, -\frac{10x+13}{25} + y]$. In the next step we replace $10x + 13$ by $10x + 13 + 2(25x - 19) = 60x - 25$. We now have the ideal $[25x - 19, -\frac{12x-5}{5} + y]$. In the final step we replace $12x - 5$ by $12x - 5 - 2x(25x - 19) = -50x^2 + 50x - 5$ to end up with the ideal $[25x - 19, 10x^2 - 10x + 1 + y]$ with no denominators. Here we never had to interchange A and C.

Proposition 3.4. *Let $I_1 = [A_1, y - B_1/n_1]$ and $I_2 = [A_2, y - B_2/n_2]$ be two equivalent $\mathcal{O}_K$-ideals. Then the two $\mathcal{O}_k$-ideals $J_1 = (a_1, n_1 w - b_1)$ and $J_2 = (a_2, n_2 w - b_2)$ are equivalent.*

Proof. Note that by Lemma 3.1 we may assume that $\gcd(a_i, n_i) = 1$, $i = 1, 2$. We shall prove that there exist integers f', f, g such that

$$(f + gw)J_1 = (f')J_2.$$

Note also that $cont(A_i) = 1$. To see this, assume that a prime p divides $cont(A_i)$. Then $B_i^2 \equiv n_i^2 D \bmod p\mathbb{Z}[x]$, which is not possible since D is assumed to be monic of odd degree, unless p divides n_i. Since $\gcd(a_i, n_i) = 1$, we conclude that $cont(A_i) = 1$.

Since I_1 and I_2 are equivalent $\mathcal{O}_K$ ideals, there exist polynomials F, G, F' in $\mathbb{Q}[x]$ such that

$$[A_1, y - B_1/n_1](F + Gy) = [A_2, y - B_2/n_2](F'). \tag{1}$$

After multiplying the generators of the two principal ideals by suitable rational numbers if necessary, we may assume F, G, F' in $\mathbb{Z}[x]$, that $cont(F') = 1$, and that $\gcd(cont(F), cont(G)) = 1$.

We now prove that $J_1(f + gw) = J_2(f')$. We first consider norms. Since $I_1(F + Gy) = I_2(F')$, we know that

$$A_1(F^2 - G^2 D) = rA_2 F'^2 \tag{2}$$

for some non-zero integer r and obviously $r = cont(F^2 - G^2 D)$. If p is a prime dividing r, we would have $F^2 \equiv G^2 D \bmod p\mathbb{Z}[x]$, which is impossible since D is monic of odd degree. Therefore $r = 1$. Putting $x = 0$ in (2), we see that $a_1(f^2 - g^2 D) = a_2 f'^2$ and we conclude that

$$Norm(J_1(f + gw)) = Norm(J_2(f')).$$

Here we used the fact that $\gcd(a_i, n_i) = 1$, $i = 1, 2$.

The equality (1) means that $\{A_1(F+Gy), (y-B_1/n_1)(F+Gy)\}$ and $\{A_2F', (y-B_2/n_2)F'\}$ are bases for the same $\mathbb{Q}[x]$ module. Thus, there is a matrix

$$\begin{pmatrix} T_1/\tau_1 & T_2/\tau_2 \\ T_3/\tau_3 & T_4/\tau_4 \end{pmatrix} \in GL_2(\mathbb{Q}[x])$$

taking the first basis to the second. We may assume $T_i \in \mathbb{Z}[x]$, $\tau_i \in \mathbb{Z}$, and that $\gcd(cont(T_i), \tau_i) = 1$, $i = 1, 2, 3, 4$. This gives the two equations

$$(F+Gy)A_1 = \frac{T_1F'A_2}{\tau_1} + \frac{T_2F'(y - B_2/n_2)}{\tau_2}, \tag{3}$$

$$(F+Gy)(y - B_1/n_1) = \frac{T_3F'A_2}{\tau_3} + \frac{T_4F'(y - B_2/n_2)}{\tau_4}. \tag{4}$$

Looking at the coefficient of y in (3) we see that $GA_1\tau_2 = T_2F'$. Since τ_2 must divide $cont(T_2F') = cont(T_2)$, we conclude that $\tau_2 = 1$. The rational part of the same equation gives $FA_1n_2\tau_1 = T_1F'A_2n_2 - T_2F'B_2\tau_1$. Here τ_1 must divide $cont(T_1F'A_2n_2)$ and therefore $\tau_1|n_2$.

The coefficient of y in (4) gives $Fn_1\tau_4 - GB_1\tau_4 = T_4F'n_1$, which implies that $\tau_4|n_1$. The rational part of this equation gives

$$GDn_1n_2\tau_3\tau_4 - FB_1n_2\tau_3\tau_4 = T_3F'A_2n_1n_2\tau_4 - T_4F'B_2n_1\tau_3.$$

Since we already know that $\tau_4|n_1$ we conclude that $\tau_3|n_1n_2$.

Specializing $x \mapsto 0$ in (3) and (4) and multiplying by n_2 and n_1n_2 respectively gives the following two equations:

$$n_2(f+gw)a_1 = \frac{n_2t_1f'a_2}{\tau_1} + \frac{t_2f'(n_2w - b_2)}{\tau_2}, \tag{5}$$

$$n_2(f+gw)(n_1w - b_1) = \frac{n_1n_2t_3f'a_2}{\tau_3} + \frac{n_1t_4f'(n_2w - b_2)}{\tau_4}. \tag{6}$$

Since $\tau_1|n_2$, $\tau_2 = 1$, $\tau_3|n_1n_2$, $\tau_4|n_1$, the first Eq. (5) says that $n_2(f+gw)a_1 \in f'J_2$ and the second (6) says that $n_2(f+gw)(n_1w - b_1) \in f'J_2$. We can conclude that $n_2(f+gw)J_1 \subset f'J_2$. Assume first that $\gcd(n_2, f') = 1$. Then since $\gcd(n_2, a_2) = 1$, we also conclude that $(f+gw)J_1 \subset f'J_2$. But as we saw above, the norms on both sides are equal. Thus we must have $(f+gw)J_1 = f'J_2$ which is the desired result.

If $\gcd(n_2, f') \neq 1$, we can by Lemma 3.2 find an ideal $I_2' = [A_2', y - B_2'/n_2']$ equivalent to I_2 with n_2' as small as we want, and in particular we may assume $n_2' = 1$. Then by the above reasoning J_2 is equivalent to J_2'. Likewise J_1 is equivalent to J_2' and therefore J_1 is equivalent to J_2. This completes the proof of the proposition. □

To complete the proof of the main theorem we must prove that the mapping φ is multiplicative.

Proposition 3.5. *Let $[A_i, y - \frac{B_i}{n_i}]$, $i = 1, 2, 3$, be three $\mathcal{O}_K$ ideals such that I_1I_2 is equivalent to I_3. Let $J_i = (a_i, n_iw - b_i)$, $i = 1, 2, 3$, be the corresponding $\mathcal{O}_k$ ideals. Then J_1J_2 is equivalent to J_3 in the ideal class group of $\mathcal{O}_k$.*

Proof. Since the mapping φ is independent of choice of representative for the ideal classes we may, using Lemma 3.2, assume that $n_1 = n_2 = n_3 = 1$. Lemma 2.3(b) does not introduce new denominators.

Therefore we may also assume that a_1, a_2 and a_3 are relatively prime. As in the proof of Proposition 3.4 we assume that there are polynomials F, G, F' in $\mathbb{Q}[x]$ such that

$$I_1 I_2 \big(F'\big) = I_3(F + Gy). \tag{7}$$

And by multiplying the generators of the two principal ideals by suitable rational numbers, we may assume that F, G, F' in $\mathbb{Z}[x]$, $cont(F') = 1$, and that $\gcd(cont(F), cont(G)) = 1$.

As in Proposition 3.4 we find that $Norm(J_1 J_2 f') = Norm(J_3(f + gw))$.

Since $I_3(F + Gy) \subset I_1 F'$, the same reasoning as in Proposition 3.4 gives $J_3(f + gw) \subset J_1 f'$. And likewise we get $J_3(f + gw) \subset J_2 f'$.

Since $J_1 + J_2 = 1$, we conclude that $J_3(f + gw) \subset J_1 J_2 f'$. Since the norms on both sides are equal, the inclusion is actually an equality. $\square$

Proof of Proposition 2.2. Because the mapping φ is multiplicative we have $\varphi(I^{-1}) = \varphi(I)^{-1}$. Let $I = [A, y - B/n]$ be a $\mathbb{Z}$-primitive ideal with $B^2 - n^2 D = AC$, and let $\bar{I} = [A, y + B/n]$. Then

$$\begin{aligned} I\bar{I} &= \big[A^2 A(y + B/n), A(y - B/n), AC\big] \\ &= (A)[A, y + B/n, y - B/n, C]. \end{aligned}$$

If a square-free polynomial divides A, B and C, it would divide D at least twice, which is impossible since D is assumed to be square-free. Therefore the ideal $[A, y + B/n, y - B/n, C]$ is trivial and $I\bar{I} = (A)$. This means that $I^{-1} = \bar{I}$ in the ideal class group.

For the corresponding $\mathcal{O}_k$ ideals we have $J\bar{J} = (a, wn - b)(a, wn + b) = (a)(a, wn + b, wn - b, c)$, and again, if we assume $\gcd(a, 2b, c) = 1$, then $J\bar{J} = (a)$. So $J^{-1} = \bar{J}$ in the ideal class group of $\mathcal{O}_k$.

Let $I_1 = [A_1, y - B_1/n_1]$ and $I_2 = [A_2, y - B_2/n_2]$ be two $\mathbb{Z}$-primitive $\mathcal{O}_K$-ideals and let $I_3 = [A_3, y - B_3/n_3]$ be an ideal equivalent to their product $I_1 I_2$. Let $J_i = (a_i, wn_i - b_i)$, $i = 1, 2, 3$, be the corresponding $\mathcal{O}_k$-ideals and let $\bar{I}_i = [A_i, y + B_i/n_i]$ and $\bar{J}_i = [a_i, wn_i + b_i]$, $i = 1, 2, 3$.

We know that $I_i \bar{I}_i = (A_i)$, $i = 1, 2, 3$, and also that $J_i \bar{J}_i = (a_i)$, $i = 1, 2$. If also $J_3 \bar{J}_3 = (a_3)$, then $(a_3, wn_3 + b, wn_3 - b, c) = 1$ and therefore $\gcd(a_3, 2b_3, c_3) = 1$, which would prove that the product I_3 is also $\mathbb{Z}$-primitive.

Multiplying Eq. (7) with $\bar{I}_1 \bar{I}_2 \bar{I}_3$, we find that there are polynomials $F', F, G \in \mathbb{Z}[x]$ such that

$$F' A_1 A_2 \bar{I}_3 = A_3(F + Gy) \bar{I}_1 \bar{I}_2.$$

And multiplying by $(F - Gy)$ we obtain

$$A_3\big(F^2 - G^2 D\big) \bar{I}_1 \bar{I}_2 = A_1 A_2 F'(F - Gy) \bar{I}_3.$$

Since we may assume $cont(F' A_1 A_2) = 1$ and $\gcd(cont(F A_3), cont(G A_3)) = 1$, we may proceed as in the proof of Proposition 3.5 to get

$$a_3\big(f^2 - g^2 d\big) \bar{J}_1 \bar{J}_2 = a_1 a_2 f'(f - gw) \bar{J}_3.$$

We also have

$$(f + gw) J_3 = f' J_1 J_2.$$

Multiplying the last two equations, and cancelling common factors, we find that $J_3 \bar{J}_3 = (a_3)$. This proves that the set of $\mathbb{Z}$-primitive points is a group. $\square$

4. Even degree curves

There are two points where the above proofs fail for even degree curves. In the proof of Proposition 3.4 we use the fact that D is monic of odd degree to prove that $cont(A_i) = 1$. The argument is that if a prime p divides $cont(A_i)$ then $B_i^2 \equiv n_i^2 D \bmod p\mathbb{Z}[x]$. And therefore D is a square in $p\mathbb{Z}[x]$. This is not possible for monic polynomials of odd degree, unless p divides n_i. The same argument is also used to prove that $cont(F^2 - G^2 D) = 1$. For even degree curves the argument fails. One way to overcome this problem is to consider only even degree curves $y^2 = D(x)$ such that D is not a square modulo any rational prime p. Such a prime would have to divide the discriminant of D. We state this as a theorem.

Theorem 4.1. *Let $y^2 = D(x)$ be a hyperelliptic curve of even degree such that D is not a square modulo any prime p dividing the discriminant of D. Then the mapping φ, sending the ideal $I = [A, y - B/n]$ of $\mathcal{O}_K$ to the ideal $J = (a, nw - b)$ in $\mathcal{O}_k$, is a homomorphism from ideal classes of $\mathcal{O}_K$ to ideal classes of $\mathcal{O}_k$.*

References

[1] Reinhard Bölling, Über einen Homomorphismus der rationalen Punkte elliptischer Kurven, Math. Nachr. 96 (1980) 207–244.
[2] Duncan A. Buell, Elliptic curves and class groups of quadratic fields, J. Lond. Math. Soc. (2) 15 (1) (1977) 19–25.
[3] Y. Hellegouarch, Positive Definite Binary Quadratic Forms over $k[x]$, Sém. Théor. Nombres, Universite de Caen, France, 1987.
[4] T.K. Sivertsen, Klassegrupper, elliptiske kurver og kryptografi, Master's thesis, University of Tromsø, 2000.
[5] Ragnar Soleng, Homomorphisms from the group of rational points on elliptic curves to class groups of quadratic number fields, J. Number Theory 46 (2) (February 1994).