ON THE ARITHMETIC OF POLYNOMIALS OVER A NUMBER FIELD

W. DUKE

Abstract. Counterparts of several classical results of number theory are proven for the ring of polynomials with coefficients in a number field. A theorem of Milnor that determines the Witt group of a function field is applied to prove an analogue of Gauss's principal genus theorem for binary quadratic forms with polynomial coefficients. This is used to relate the rank of the Mordell-Weil group of an associated hyperelliptic curve to quadratic reciprocity in one of these polynomial rings. Other results connect the solvability of certain Diophantine equations with the structure of the torsion subgroups of these Mordell-Weil groups.

1. Introduction

The main aim of this paper is to prove new counterparts of some old and well-known results of classical number theory when $\mathbb{Z}$ is replaced by the ring of polynomials over a number field. Let k be a field. As a Euclidean domain with respect to polynomial degree, the ring $k[t]$ shares some number theoretic properties with the integers $\mathbb{Z}$, since it has a division algorithm and unique factorization into primes (monic irreducibles). Consider quadratic reciprocity. Given $p, q \in k[t]$ with $p(t)$ prime and $p \nmid q$, write $\left(\frac{q}{p}\right) = 1$ if $q(t)$ is a square modulo $p(t)$ and $\left(\frac{q}{p}\right) = -1$ otherwise. If k is finite, quadratic reciprocity holds between any pair of distinct primes p and q, meaning that

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right), \tag{1.1}$$

where $p^* = (-1)^{|p|}p$ with $|p| := \deg p$. This was shown by Dedekind [12, p.58 in Werke] when $k = \mathbb{F}_p$. See also Artin's thesis [2] and [38].

When k is a number field, for which the residue field $k[t]/(p)$ is infinite, it is easy to show that (1.1) does not always hold. One problem considered here is to characterize those q with odd degree for which $\left(\frac{q}{p}\right) = 1$ implies $\left(\frac{p^*}{q}\right) = 1$ *for all primes* $p \neq q$. The approach to it is inspired by Gauss's second proof of classical quadratic reciprocity in [16, Art. 262] (or [17]), which is an application of the genus theory of binary quadratic forms. That proof relies on the finiteness of the class group. For any square-free $D \in k[t]$, let $\mathcal{J}_D$ (or $\mathcal{J}_D(k)$ if k is not understood) be the Mordell-Weil group of k-rational divisor classes of degree zero on the hyperelliptic curve over k determined by $s^2 = D(t)$. Naturally, $\mathcal{J}_D$ plays the role of the class group. After Mordell-Weil, $\mathcal{J}_D$ is a finitely generated abelian group that might, or might not be, finite.

Theorem 1. *Let k be a number field and $q(t) \in k[t]$ be a fixed prime with odd degree. Then the following holds if and only if $\mathcal{J}_q$ is finite:*

$$\left(\frac{q}{p}\right) = 1 \ \textit{implies} \ \left(\frac{p^*}{q}\right) = 1 \ \textit{for all primes } p(t) \neq q(t). \tag{1.2}$$

In words, whether or not $\mathcal{J}_q$ is finite determines whether or not (one way) quadratic reciprocity holds for a prime $q \in k[t]$ of odd degree, when k is a number field. Once $\mathcal{J}_q$ is identified with a certain class group of forms over $k[t]$, the proof of the "if" part of

Theorem 1 is similar in spirit to arguments of Gauss. The proof of the "only if" part is more involved and relies on an analogue of Gauss's principal genus theorem.

Theorem 1 implies the following version of quadratic reciprocity, one connecting monic irreducible polynomials of odd degree. It is deduced by using the map $t \mapsto -t$.

Corollary 1. *Suppose that $p, q \in k[t]$ are distinct primes of odd degree and that both $\mathcal{J}_q$ and $\mathcal{J}_p$ are finite. Then $\left(\frac{q}{p}\right) = \left(\frac{-p}{q}\right)$.*

It can happen that (1.2) holds for a prime $q(t) \in k[t]$ of odd degree over k and all primes $p \in k[t]$ with $p \neq q$, and where q is still irreducible over a finite extension k'/k, but (1.2) fails for some $p \in k'[t]$. By Theorem 1, the rank of $\mathcal{J}_q(k)$ is zero while that of $\mathcal{J}_q(k')$ is at least one.

Example. Suppose that $q(t) = t^3 + at + b$ with $a, b \in \mathbb{Z}$ is a prime in $\mathbb{Q}[t]$. Assume that $s^2 = q(t)$ gives an elliptic curve over $\mathbb{Q}$ with rank 0. Then by Theorem 1, (1.2) holds for any prime $p \in \mathbb{Q}[t]$ with $p \neq q$. For any non-zero square-free $d \in \mathbb{Z}$ we have that q is still irreducible over $k' = \mathbb{Q}(\sqrt{d})$. If (1.2) fails for some prime $p \in k'[t]$ with $p \neq q$, then by Theorem 1 the twisted curve $ds^2 = q(t)$ has positive rank, since its rank equals that of the curve over k'. Conversely, if the rank of a twisted curve is positive then (1.2) must fail for some prime $p \in k'[t]$ with $p \neq q$.

The analogue of Gauss's principal genus theorem is also used to prove the following result connecting polynomial solvability of a Legendre equation with a Mordell-Weil group.

Theorem 2. *Suppose that $p, q \in k[t]$ are non-constant primes with $|p|$ even and $|q|$ odd. Then the equation*

$$p(t)x^2 - q(t)y^2 - z^2 = 0$$

has non-trivial polynomial solutions $x, y, z \in k[t]$ if and only if the Mordell-Weil group $\mathcal{J}_{pq}$ of the hyperelliptic curve $s^2 = p(t)q(t)$ contains elements of order 4.

Theorem 2 corresponds to a combination of classical results of Legendre and Gauss on the integral solvability of the equation $px^2 - qy^2 - z^2 = 0$ when $p, q \in \mathbb{Z}$.

Some known results about the arithmetic of $k[t]$ address the question of when solvability of a polynomial equation in several variables over k, usually with constraints on these scalar solutions, implies solvability over $k[t]$ or over $k(t)$. An elegant result of this type for Legendre equations, when $k = \mathbb{Q}$, was obtained by Davenport-Schinzel-Lewis in [11]. Its generalization where k is any number field was given in [40, p. 202] (see also [41, p. 325]) and states the following.

Theorem (Schinzel)**.** *Suppose that $D_1, D_2 \in k[t]$ have the property that every arithmetic progression $P \subset \mathbb{Z}$ contains an integer t_0 so that when $t = t_0$ the equation*

$$D_1(t)x^2 - D_2(t)y^2 - z^2 = 0 \tag{1.3}$$

has non-trivial solutions $x, y, z \in k$. Then (1.3) has non-trivial solutions with $x, y, z \in k[t]$.

When combined with this statement, the method used in the proof of Theorem 2 yields a criterion for the non-solvability over k of some families of Legendre equations.

Theorem 3. *Suppose that $D \in k[t]$ is monic and squarefree of odd degree. Assume that the Mordell-Weil group of the hyperelliptic curve $s^2 = D(t)$ contains no element of order 4. Then for any factorization $D = D_1 D_2$ with D_1, D_2 monic and where $|D_1|$ is even and positive, an arithmetic progression $P \subset \mathbb{Z}$ exists with the property that for each $t_0 \in P$ the equation*

$$D_1(t_0)x^2 - D_2(t_0)y^2 - z^2 = 0$$

has no non-trivial solutions $x, y, z \in k$.

Example. It is easy to find elliptic curves over $\mathbb{Q}$ given by equations of the form

$$s^2 = (a't^2 + b't + c')(d't + e'), \quad a', b', c', d', e' \in \mathbb{Z}$$

having no points of order 4. Each one of these will yield by Theorem 3 a quartic equation with integral coefficients of the form

$$(at^2 + bt + c)x^2 - (dt + e) = z^2 \tag{1.4}$$

that has no solutions with $x, z \in \mathbb{Q}$ and $t \in \mathbb{Z}$. A special case of a conjecture of Mordell [31, p.98] predicts that (1.4) will have infinitely many solutions if we allow t to be rational.

Fueter [15] discovered that the existence of classes of order 3 in the class group of $\mathbb{Q}(\sqrt{d})$ is necessary for the existence of non-trivial rational points on the elliptic curve $y^2 = x^3 + d$, at least for some $d < 0$. I will give an analogue of Fueter's result for the rational points on the elliptic curve over $k(t)$ determined by $y^2 = x^3 + D(t)$, where $D \in k[t]$ is monic and square-free of odd degree. This equation can also be considered to give an elliptic surface over k where, in general, it has many more points. For $D \in k[t]$ let

$$D'(t) = -27D(-3t). \tag{1.5}$$

Theorem 4. *Suppose that $D \in k[t]$ is square-free and non-constant, where k is a number field. Then either the equation*

$$y^2 = x^3 + D(t)$$

has an infinity of solutions $x, y \in k(t)$ or it has none. It has none if D is also monic of odd degree and neither $\mathcal{J}_D$ nor $\mathcal{J}_{D'}$ has points of order 3.

Examples. i) Suppose that $a, b \in k$ satisfy $4a^3 + 27b^2 \neq 0$ and that

$$3t^4 + 6at^2 + 12bt - a^2 = 0 \tag{1.6}$$

has no roots $t \in k$. Then the equation

$$y^2 = x^3 + t^3 + at + b \tag{1.7}$$

has no solutions $x, y \in k(t)$. To see this, note that (1.6) determines the t-coordinates of points of order 3 on the elliptic curve $\mathcal{J}_D : s^2 = t^3 + at + b$ and the change of variables $t \mapsto -\frac{t}{3}$ gives the corresponding equation for $s^2 = t^3 + 9at - 27b$, which is isomorphic to $\mathcal{J}_{D'}$. Thus, if (1.6) has no rational roots then neither $\mathcal{J}_D$ nor $\mathcal{J}_{D'}$ has rational points of order 3 and we may apply Theorem 4. Suppose that $k = \mathbb{Q}$. Using (1.6), an easy counting argument shows that the number $N(X)$ of admissible $(a, b) \in \mathbb{Z}$ with

$$\max(4|a|^3, 27|b|^2) \leq X$$

and such that (1.7) has solutions $x, y \in \mathbb{Q}(t)$, satisfies $N(X) \ll X^{\frac{1}{2}}$ (see [35] for refinements of this count). Therefore equations (1.7) with $a, b \in \mathbb{Z}$ and solutions $(x, y) \in \mathbb{Q}(t)^2$ are rare.

ii) The curve $y^2 = x^3 + t^3 - 3$ with $D(t) = t^3 - 3$ over $\mathbb{Q}(t)$ contains the point $(\frac{4-t^3}{t^2}, \frac{3t^3-8}{t^3})$. Now $\mathcal{J}_D$ has trivial torsion, while $\mathcal{J}_{D'}$ has points of order 3. Thus it is not enough in the second statement of Theorem 4 to assume only that $\mathcal{J}_D(k)$ has no points of order 3 to conclude that $y^2 = x^3 + D(t)$ has no solutions. Similarly, it is not enough to assume only that $\mathcal{J}_{D'}(k)$ has no points of order 3. This is in contrast to Fueter's result (c.f. [43]). On the other hand, if we only assume that $\mathcal{J}_D(k)$ has no points of order 3, then $y^2 = x^3 + D(t)$ has no *polynomial* solutions $x, y \in k[t]$. For a simple proof see the remark at the end of the paper.

Remarks. A number of variations of the specialization theorem of Schinzel et al stated above have been considered for polynomials of degree greater than two. As pointed out in [41, p. 338], the direct analogue over $\mathbb{Q}(t)$ of the Davenport-Schinzel-Lewis result from [11] already does not hold for the equation $y^2 = x^3 + t$. By Theorem 4 or otherwise, this equation has no solutions in $\mathbb{Q}(t)$. However, each arithmetic progression in $\mathbb{Z}$ contains some t_0 for which $y^2 = x^3 + t_0$ has nontrivial solutions $x, y \in \mathbb{Q}$. This follows since it can be shown that $y^2 \equiv x^3 + t \pmod{m}$ has solutions for each $t \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$ (c.f. [41]). For related results see [7] and [37]. On the other hand, some notable positive specialization results of the same basic type in higher degree have been found. Some of these are given in [21], [44] and [49].

Acknowledgements. I am grateful to David Rohrlich and Umberto Zannier for their valuable comments.

2. Overview and discussion of proofs

To prove the theorems of this paper, binary forms with polynomial coefficients provide an efficient tool whose theory is, to some extent, self contained and elementary. The theory for binary quadratic forms is developed in the next section §3. It meshes well with results of Milnor on quadratic forms over a function field that we need. We use a set of forms with coefficients in $k[t]$ that are analogous to positive definite binary quadratic forms with integral coefficients. They split into a set of classes $\mathcal{C}_D$ of forms with discriminant D. An adaptation of Dirichlet-Dedekind's version of Gaussian composition makes $\mathcal{C}_D$ into an abelian group. Following Gauss, we count classes of order two in terms of ambiguous forms. Genus characters are defined using certain Steinberg symbols that were studied in [27]. In the classical case, to prove quadratic reciprocity it is enough to know, in addition to the number of classes of order two, that the class number is finite and that a genus character is trivial when evaluated at a square. For us, the corresponding argument is enough to prove the "if" part of Theorem 1. We actually prove the theorems with $\mathcal{J}_D$ replaced by $\mathcal{C}_D$ in the statements, and later show that $\mathcal{J}_D$ is isomorphic to $\mathcal{C}_D$.

For the proof of the converse we need an analogue of Gauss's principal genus theorem, which is given as Proposition 3.10 near the end of §3. This result identifies $\mathcal{C}_D^2$ with the classes killed by all genus characters. When attempting to adapt the classical proofs of the principal genus theorem over $\mathbb{Z}$ one encounters new difficulties, some caused by the the fact that there are infinitely many polynomials of bounded degree. Here I apply the determination of the Witt group of $k(t)$ given by Milnor [28] and formulated in Proposition 3.8. This result implies a kind of Hasse principle (see Proposition 3.9) that allows us to identify genera with rational classes (i.e. $k(t)$-classes) of forms and prove the genus theorem. It is to be observed that the theorem of Milnor is not formulated in terms of the p-adic fields but in terms of their residue class fields, which for us are number fields. Also, our assumption that $D(t)$ is square-free greatly simplifies certain important details in the proof.

The proof of the "only if" part of Theorem 1 also requires that if $\mathcal{C}_D$ is infinite, it must contain a class that is not a square. For this it is enough to know that $\mathcal{C}_D$ is finitely generated, which is a consequence of the Mordell-Weil theorem. In §4 we show that $\mathcal{C}_D$ is isomorphic to the Mordell-Weil group $\mathcal{J}_D$. This result is based in part on work of Jacobi [22], Mumford [32] and David Cantor [4]. Cantor translated divisor arithmetic into computations with polynomials that also occur in the composition formulas. His algorithms have been extensively applied when k is a finite field. For my purpose, I need to make the relation between divisor classes and the classes of binary quadratic forms

that I have defined, completely explicit. In terms of quadratic forms, the weak Mordell-Weil theorem is equivalent to the finiteness of the number of genera. In view of this, the result we give in Proposition 3.7 that forms are in the same genus if and only if they are rationally equivalent, is of independent interest.

A third ingredient in the proof of the "only if" part of Theorem 1 is an application of Hilbert's irreducibility theorem over k. Thanks to this result, it is not hard to make a binary quadratic form over $k[t]$ represent primes.

The proofs of Theorems 2 and 3 rely on a $k[t]$ version of a well-known result of Redei-Reichart [36] that determines the number of subgroups of order 2^m, where $m \geq 2$, in a representation of the class group of a quadratic field as a direct product of cyclic subgroups of prime power order. The result we need is given in Proposition 4.3, which is an essentially direct consequence of the $k[t]$ principle genus theorem. As already mentioned, Theorem 3 combines this result with the specialization theorem of Schinzel. The proofs of Theorems 1, 2 and 3 are completed at the end of §4.

Theorem 4 is proven in §5. The first statement is a straightforward application of taking powers in the elliptic curve. The proof of the second statement, which is more difficiult, is based on the theory of binary cubic forms with coefficients in $k[t]$. That binary cubic forms over $\mathbb{Z}$ give information about classes of binary quadratic forms of order 3 was discovered by Eisenstein [14]. We make essential use of a $k(t)$-version of a familiar pair of dual 3-isogenies connecting the elliptic curves E_d and E_{-27d}, one that was employed by Fueter in his result over $\mathbb{Q}$ (see [15, p.71.]). Fueter's proof uses algebraic number theory. It would be natural to give a proof of Theorem 4 along similar lines directly using quadratic extensions of $k(t)$.[1]

It is also shown in §5 that the number of classes of binary cubic forms with coefficients in $k[t]$ and with a fixed discriminant $4D$ is finite, when D is monic and square-free with odd degree (see Proposition 5.3).

The changes needed to include discriminants $D \in k[t]$ with even degree in our results lead to interesting problems that are not addressed in this paper.

3. Binary quadratic forms over $k[t]$

The theory of binary quadratic forms over $k[t]$ can be developed in a way that is quite similar to that over $\mathbb{Z}$, especially when the discriminant has odd degree, where the forms are similar to positive definite ones. An excellent overview of the classical theory of positive definite binary quadratic forms is given in [10]. I assume throughout that k is a fixed number field. However, most of the results presented here remain valid when k is any perfect field of characteristic not 2. This section ends with the proof of the $k[t]$ version of Gauss's principle genus theorem.

Preliminaries. The gcd of a finite set of polynomials in $k[t]$ is the monic polynomial of largest degree that divides each. Two polynomials are coprime if their gcd is 1. If $c = \gcd(a, b)$ then there are $x, y \in k[t]$ with $c = ax + by$. For $a \in k[t]$ the inequality $|a| < 0$ is equivalent to $a = 0$.

Associated to $Q = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ with $a, b, c \in k[t]$ is the binary quadratic form

$$Q(x, y) = (a, b, c) = a(t)x^2 + 2b(t)xy + c(t)y^2$$

with discriminant (= Gaussian determinant) $D = b^2 - ac$. Unless otherwise specified, in this paper we will always assume that $D \in k[t]$ is square-free. Note that any form

[1]It is possible to give a simple proof of the first statement of Theorem 4 in this way, as Zannier has kindly shown me.

$Q = (a, b, c)$ with $b^2 - ac = D$ is primitive in that $\gcd(a, b, c) = 1$. Let $M \in \mathrm{SL}_2(k[t])$ act on Q by

$$Q|M := MQM^t. \tag{3.1}$$

For $M = \left(\begin{smallmatrix} m & r \\ n & s \end{smallmatrix}\right)$ we have $Q|M(x, y) = Q(mx + ny, rx + sy) = Q'(x, y)$ and the coefficients of $Q' = (a', b', c')$ are given by

$$\begin{aligned} a' =& am^2 + 2bmn + cn^2 \\ b' =& amr + b(ms + rn) + cns \\ c' =& ar^2 + 2brs + cs^2. \end{aligned} \tag{3.2}$$

Clearly $b'^2 - a'c' = D$. The two forms Q and Q' are said to be equivalent, written $Q \sim Q'$.

Say that $n \in k[t]$ is *represented* by Q if $Q(x, y) = n$ for $x, y \in k[t]$ and that n is *properly represented* by Q if $Q(x, y) = n$ for coprime $x, y \in k[t]$. Equivalent forms represent and properly represent the same polynomials.

The integral version of the following useful result was given by Dirichlet [13, §60]. The proof for $k[t]$ is similar.

Lemma 3.1. *Let $Q = (a, b, c)$ and $Q' = (a', b', c')$, both with discriminant D, be given. They are equivalent if there exist $m, n, r, s \in k[t]$ with*

$$\begin{aligned} & a' = am^2 + 2bmn + cn^2, \\ & (b + b')n + am = a's \quad \textit{and} \\ & (b' - b)m - cn = a'r, \end{aligned} \tag{3.3}$$

in which case $Q|M = Q'$ with $M = \left(\begin{smallmatrix} m & r \\ n & s \end{smallmatrix}\right) \in \mathrm{SL}_2(k[t])$. Conversely, if Q, Q' satisfy $Q' = Q|M$ with this M, then (3.3) holds.

A proof of the next standard result may be found in [34, Thm VII.3]).

Lemma 3.2. $\mathrm{SL}_2(k[t])$ *is generated by*

$$C_\alpha = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{smallmatrix}\right), T_n = \left(\begin{smallmatrix} 1 & n(t) \\ 0 & 1 \end{smallmatrix}\right) \quad \text{and} \quad S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$$

for $n \in k[t]$ and $\alpha \in k^\bullet$.

We have the formulas

$$\begin{aligned} & (a, b, c)|C_\alpha = (\alpha^2 a, b, \alpha^{-2} c) \\ & (a, b, c)|T_n = (a, b + na, c + 2nb + n^2 a) \\ & (a, b, c)|S = (c, -b, a). \end{aligned} \tag{3.4}$$

The following Lemma is easily verified.

Lemma 3.3. *Suppose that $D \in k[t]$ is square-free and that $Q = (a, b, c)$ has $D = b^2 - ac$. The group of automorphs of Q, that is those $M \in \mathrm{SL}_2(k[t])$ with $Q|M = Q$, are all of the form*

$$M = \pm \left(\begin{smallmatrix} x - by & ay \\ -cy & x + by \end{smallmatrix}\right), \tag{3.5}$$

for $x, y \in k[t]$ solutions of the Pell equation

$$x^2 - D(t)y^2 = 1. \tag{3.6}$$

Transformations M_1 with $Q|M_1 = (-a, b, -c)$ exist if and only if the negative Pell equation

$$x^2 - D(t)y^2 = -1 \tag{3.7}$$

has solutions, in which case each such M_1 is given by

$$M_1 = \pm \left(\begin{smallmatrix} x-by & ay \\ cy & -x-by \end{smallmatrix}\right).$$

For a solution x, y of (3.7), the transformation M from (3.5) has $\det M = -1$ *and satisfies* $Q|M = -Q$.

Solutions with $y \neq 0$ to (3.6) can exist only for even degree D and then only in special cases. The problem of solving polynomial Pell equations has a long history going back to Abel and Chebyshev. See [42] and [50] for more information.

Lemma 3.4. *Let Q have discriminant D.*

i) If $a' \in k[t]$ is properly represented by Q then there exists $Q' = (a', b', c')$ that is equivalent to Q, where $|b'| < |a'|$.

ii) Q can properly represent a polynomial $n \in k[t]$ with $|n| \leq \frac{1}{2}|D|$.

iii) Q can properly represent some $n \in k[t]$ that is prime to any fixed $f \in k[t]$.

Proof. i) If $Q(m, n) = a'$ where m, n are coprime then there exist $r, s \in k[t]$ with

$$M = \left(\begin{smallmatrix} m & r \\ n & s \end{smallmatrix}\right) \in \mathrm{SL}_2(k[t]).$$

Thus $Q|M = (a', *, *)$. Using T_f from (3.4) with an appropriate f found by the division algorithm, we can force $|b'| < |a'|$.

ii) Let $n \in k[t]$ be a polynomial of minimal degree represented by Q. The representation is proper. By i) we may assume that $Q = (n, b, c)$, where $|b| < |n|$. Since c is properly represented by Q we must have $|b| < |n| \leq |c|$, which implies that $2|n| \leq |nc| = |D|$.

iii) Let $p_1 \in k[t]$ be the product of all primes dividing a, c and f. Let p_2 be the product of all primes dividing a and f but not c. Let p_3 be the product of all primes dividing c and f but not a. Let p_4 be the product of all remaining primes dividing f. Then

$$n = Q(p_2, p_3p_4) = a(p_2)^2 + 2bp_2(p_3p_4) + c(p_3p_4)^2$$

is prime to f and $\gcd(p_2, p_3p_4) = 1$. □

Forms with a negative discriminant. The following definition streamlines the formulation of theorems and is suggestive, if unconventional.

Definition 1. Say that $n \in k[t]$ is *positive* (and write $n \succ 0$) if the leading coefficient of $n^* = (-1)^{|n|}n$ is in $k^{\bullet 2}$ and *negative* ($n \prec 0$) if $-n$ is positive. Here $|n| = \deg n$.

The product of two positive or two negative polynomials is positive and the product of one positive and one negative polynomial is negative.

Definition 2. When $D \in k[t]$ is negative and square-free with $|D|$ odd, let $\mathcal{Q}_D$ denote the set of those $Q = (a, b, c)$ with discriminant D, for which $a \succ 0$.

Observe that $\mathcal{Q}_D$ is non-empty, since it contains the principal form $(1, 0, -D)$. The following lemma shows that the action $Q \mapsto Q|M$ splits $\mathcal{Q}_D$ into a set of equivalence classes and that the forms in $\mathcal{Q}_D$ are analogous to positive definite integral binary quadratic forms.

Lemma 3.5. *Suppose that $D \in k[t]$ is negative and square-free with $|D|$ odd. If $Q = (a, b, c) \in \mathcal{Q}_D$, then $Q|M \in \mathcal{Q}_D$ for $M \in \mathrm{SL}_2(k[t])$. In particular, any n properly represented by Q is positive.*

Proof. From $D = b^2 - ac$ and $a \succ 0$, we will show that $c \succ 0$. Clearly $c \neq 0$. Next use that the leading coefficient of D is in $k^{\bullet 2}$ with $|D|$ odd to check the different combinations of parities of the degrees of a and c. If they are both even or both odd the leading terms of b^2 and ac must cancel. Otherwise the leading term of $-ac$ must be in $k^{\bullet 2}$.

The first statement for any M now follows from Lemma 3.2 and the formulas (3.4). The second statement follows from the first and i) of Lemma 3.4.

□

Definition 3. For $D \in k[t]$ negative and square-free with $|D|$ odd, let $\mathcal{C}_D$ be the set of all $\mathrm{SL}_2(k[t])$-classes of forms $Q \in \mathcal{Q}_D$.

We have the following version of Lagrangian reduction.

Proposition 3.1. *Each class $C \in \mathcal{C}_D$ contains a unique form $Q = (a, b, c)$ with*

$$|b| < |a| < \tfrac{1}{2}|D|,$$

where a^* is monic.

Proof. The existence follows from Lemmas 3.4 and 3.5, after applying the appropriate C_α from (3.4) to achieve the monic condition. Here we use that $|D|$ is odd.

For uniqueness, suppose that $Q' = (a', b', c') \in C$ has $|b'| < |a'| < \frac{1}{2}|D|$ with $\pm a'$ monic. By completing the square,

$$aa' = (am + bn)^2 - Dn^2,$$

where $Q' = Q|M$ with $M = \left(\begin{smallmatrix} m & r \\ n & s \end{smallmatrix}\right) \in \mathrm{SL}_2(k[t])$. Therefore

$$|D| > |a| + |a'| = |(am + bn)^2 - Dn^2|.$$

This implies that $n = 0$ and so from the first equation of (3.2) we have that $am^2 = a'$. By symmetry we deduce that $m = s = 1$ and $a = a'$. The second equation of (3.2) yields $b' = b + ra$, which implies that $r = 0$ since

$$|b' - b| < |a'| = |a|.$$

Thus $Q = Q'$. □

Class group and ambiguous classes. A straightforward modification of Dirichlet and Dedekind's [13] version of Gaussian composition can be defined for classes in $\mathcal{C}_D$, making it into an abelian group. We do, however, have to account for our condition on $(a, b, c) \in \mathcal{Q}_D$ that $a \succ 0$, but this leads to no problem since if $a \succ 0$ and $a' \succ 0$ then $aa' \succ 0$. Say two forms $Q = (a, b, c), Q' = (a', b', c') \in \mathcal{Q}_D$ are *concordant* if

$$\gcd(a, a', b + b') = 1.$$

By Lemma 3.4, any pair of classes will contain a pair of concordant forms. The following result can be proven by adapting §145-§148 of [13] (see also [46, pp.129–132]). Use is made of Lemma 3.1 to show that the product of classes is well-defined.

Proposition 3.2. *Let $D(t) \in k[t]$ be negative, square-free with $|D|$ odd and $C, C' \in \mathcal{C}_D$.*

i) If $(a, b, c) \in C$ and $(a', b', c') \in C'$ are concordant, there exist $e, f \in k[t]$ such that $(a, e, a'f) \in C$ and $(a', e, af) \in C'$.

ii) The class $C'' \in \mathcal{C}_D$ of (aa', e, f) is well-defined and makes $\mathcal{C}_D$ into an abelian group through $C \otimes C' = C''$, where the identity is the class containing $(1, 0, -D)$ and the inverse C^{-1} of the class C is the class of $(a, -b, c)$.

Letting $Q = (a, e, a'f), Q' = (a', e, af)$ and $Q'' = (aa', e, f)$ we have that Q'' is directly composed of Q and Q' in the sense of Gauss [17, Art. 235]:

$$Q(x, y)Q'(x, y) = Q''(X, Y), \quad \text{where } (X, Y) = (xx' - fyy', axy' + a'x'y + 2eyy').$$

Together with this and Proposition 3.2, arguments of Gauss [17, Art. 237–239] showing that composition of classes is well-defined adapt to give the following.

Proposition 3.3. *Suppose that $Q \in C$ and $Q' \in C'$ where $C, C' \in \mathcal{C}_D$. If*

$$Q''(X,Y) = Q(x,y)Q'(x',y') \quad \text{with} \tag{3.8}$$
$$(X,Y) = (a_1xx' + b_1xy' + c_1yx' + d_1yy', a_2xx' + b_2xy' + c_2yx' + d_2yy'),$$

where $a_j, b_j, c_j, d_j \in k[t]$ for $j = 1, 2$ are such that

$$a_1b_2 - a_2b_1 = Q(1,0) \quad \text{and} \quad a_1c_2 - a_2c_1 = Q'(1,0),$$

then the class C'' of Q'' equals $C \otimes C'$.

An important consequence of Proposition 3.2 is the following result.

Proposition 3.4. *Suppose that $Q = (a,b,c) \in C$ and $Q' = (a',b',c') \in C'$, where $C, C' \in \mathcal{C}_D$ are not necessarily distinct.*

i) If a and a' are coprime, then any form in $C \otimes C'$ will properly represent aa'.

ii) If a is prime to D, then any form in $C \otimes C$ will properly represent a^2.

Proof. For i), observe that Q and Q' are then concordant. For ii), if a is prime to D then it is prime to b and so Q and Q are concordant. □

The following easily proven result shows that for our purposes we may assume if convenient that a negative D is monic.

Lemma 3.6. *For any fixed $\alpha \in k^\bullet$, the map $(a,b,c) \mapsto (a, \alpha b, \alpha^2 c)$ defines a group isomorphism from $\mathcal{C}_D$ to $\mathcal{C}_{\alpha^2 D}$.*

By an ambiguous form is meant a form of type $(a,0,c)$. Note: over $k[t]$ we need not consider non-diagonal ambiguous forms, which are necessary over $\mathbb{Z}$. A class $C \in \mathcal{C}_D$ is called *ambiguous* if it has order 1 or 2.

Lemma 3.7. *A class of $\mathcal{C}_D$ is ambiguous if and only if it contains an ambiguous form.*

Proof. Clearly the class of $(a,0,c)$ has order 1 or 2. For the converse, we adapt an argument of Georg Cantor [5] from the classical case. Suppose that the square of the class of $Q = (a,b,c)$ is the identity. What is the same, (a,b,c) is equivalent to $(a,-b,c)$. By Lemma 3.1 there are $m,n,r,s \in k[t]$ such that $ms - nr = 1$ and where

$$a = am^2 + 2bmn + cn^2, \quad am = as, \quad -ar = 2bm + cn. \tag{3.9}$$

It follows that $m = s$ so from $ms - nr = 1$ we see that $Q' = (r,m,n)$ has discriminant 1. By Lemma 3.4, Q' is equivalent to $(\alpha, 0, -\alpha^{-1})$ for some $\alpha \in k^\bullet$, which is equivalent to

$$(0,-1,0) = (\alpha, 0, -\alpha^{-1})| \begin{pmatrix} 1 & -1/(2\alpha) \\ \alpha & 1/2 \end{pmatrix}.$$

Hence there will exist $N = \left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in \mathrm{SL}_2(k[t])$ with $(0,-1,0)|N = (r,m,n)$. Thus

$$r = -2a_1a_3 \quad m = -a_1a_4 - a_2a_3 \quad n = -2a_2a_4.$$

Finally, using these identities with the middle equation of (3.2) we get

$$(a,b,c)|N^t = (*, -2bm - cn - ar, *),$$

so the last equation of (3.9) shows that $(a,b,c)|N^t = (*,0,*)$ is ambiguous. □

For $n \in k[t]$, let $\omega(n)$ be the number of distinct primes dividing n.

Proposition 3.5. *The subgroup of $\mathcal{C}_D$ of elements of order at most two has order $2^{\omega(D)-1}$.*

Proof. By Proposition 3.1 and Lemma 3.7, an ambiguous class of $\mathcal{C}_D$ contains a unique ambiguous form $(a,0,c)$ where $|a| < |c|$ and a^* is monic. The number of such forms is $2^{\omega(D)-1}$. □

Principal genus theorem. In this subsection I will prove the $k[t]$ version of the principal genus theorem. We will use a Hilbert-type Steinberg symbol to define "genus characters." A reference with proofs of those properties to be given is [28, p.98]. The field extension of k determined by $F_p = k[t]/(p)$ for a prime $p \in k[t]$, has degree $|p|$ and can be identified with $k(\alpha)$, where $\alpha \in \bar{k}$ has $p(\alpha) = 0$. Here $\bar{k}$ is the algebraic closure of k. Define for $a, b \in k(t)^\bullet$

$$(a,b)_p = (-1)^{v_p(a)v_p(b)} a^{v_p(b)} b^{-v_p(a)} \in F_p^\bullet / F_p^{\bullet 2}, \tag{3.10}$$

where $v_p(a)$ is determined by $a = p^{v_p(a)}u$ with u prime to p. Let $a_0 \in k^\bullet$ be defined through $a(t^{-1}) = t^{-\ell}(a_0 + a_1 t + \dots)$. For $p = \infty$ let

$$(a,b)_\infty = (-1)^{|a||b|} a_0^{|b|} b_0^{-|a|} \in k^\bullet / k^{\bullet 2}. \tag{3.11}$$

For any p (including $p = \infty$) and $a, b \in k(t)^\bullet$ the following hold

$$(a,b)_p = (b,a)_p \tag{3.12}$$

$$(ab,c)_p = (a,c)_p (b,c)_p \tag{3.13}$$

$$(a, 1-a)_p = 1, \ a \neq 1 \tag{3.14}$$

$$(a, b^2)_p = 1. \tag{3.15}$$

We also have the product formula

$$(a,b)_\infty \prod_p N_{F_p/k}(a,b)_p = 1, \tag{3.16}$$

where $N_{F_p/k} : F_p \to k$ is the norm.

For any p (including $p = \infty$) define the genus "character" $\chi_p : \mathcal{Q}_D \to F_p^\bullet / F_p^{\bullet 2}$ by

$$\chi_p(Q) = (n, D)_p, \tag{3.17}$$

where n is any polynomial prime to p that is properly represented by Q.

Lemma 3.8. *The value of $\chi_p(Q)$ is well-defined; it is independent of the n chosen. In addition, $\chi_p(Q) = 1$ for any $p \nmid d$, including $p = \infty$.*

Proof. We have the identity[2]

$$Q(x,y)Q(x',y') = (axx' + b(xy' + x'y) + cyy')^2 - D(t)(xy' - x'y)^2. \tag{3.18}$$

Suppose that n and n' are prime to D and properly represented by Q. For $p|D$ it follows from (3.18), (3.15) and (3.13) that $1 = (nn', D)_p = (n, D)_p (n', D)_p$. Suppose that $p|n$. By Lemmas 3.4 i) and 3.5, we have that Q is properly equivalent to some $(n, b, c) \in \mathcal{Q}_D$, so $D = b^2 - nc$ and D is a square modulo p. Thus $(n, D)_p = 1$. For $p = \infty$, since $n \succ 0$, we have that $(n, D)_\infty = 1$ from (3.11). For any other p, that $(n, D)_p = 1$ is immediate from the definition. □

Each χ_p is well defined on the class of Q. It induces a homomorphism from $\mathcal{C}_D$ to $F_p^\bullet / F_p^{\bullet 2}$ by (3.13) and i) of Proposition 3.4 together with Lemma 3.4. The intersection of the kernels of χ_p for $p|D$ will be called the *principal genus* and the cosets of the principal genus the *genera*. Let $\mathcal{G}_D = \mathcal{G}_D(k)$ denote the group of genera. The principal genus is that genus containing $(1, 0, -D)$. Thus we have

Proposition 3.6. *The genera $\mathcal{G}_D$ comprise an abelian group in which every non-identity element is of order two. Each genus G is characterized by the values $\chi_p(Q)$ for $p|D$, where Q is any form in G.*

[2]This is not a direct composition; it fails to satisfy the last conditions given in Proposition 3.3.

It follows from (3.16) that the characters are not independent but satisfy

$$\prod_{p|D} N_{F_p/k}\big(\chi_p(Q)\big) = 1. \tag{3.19}$$

Remark. The product formula (3.16) is equivalent to Weil reciprocity for $k(t)$. For $a = p$ and $b = q$ with p, q distinct primes in $k[t]$, it's truth is obvious when it is written in the form

$$(-1)^{|p||q|} \prod_{\beta;\, q(\beta)=0} p(\beta) = \prod_{\alpha;\, p(\alpha)=0} q(\alpha).$$

Weil reciprocity can be used to prove quadratic reciprocity (1.1) when k is finite (see [38]).

Say two forms $Q, Q' \in \mathcal{Q}_D$ are *rationally equivalent*, or *equivalent over* $k(t)$, if (3.1) holds for some $M \in \mathrm{GL}_2(k(t))$. Such an M must have $\det M = \pm 1$.

Proposition 3.7. *For $D \in k[t]$ square-free of odd degree, two forms $Q, Q' \in \mathcal{Q}_D$ are in the same genus if and only if they are rationally equivalent.*

The proof of the corresponding result over $\mathbb{Z}$ given in [3] is based on the Hasse-Minkowski theorem in the important special case given by Legendre. Most proofs of Legendre's theorem are based on some sort of reduction method and rely on the fact that there are only finitely many integers of a bounded absolute value. In order to prove Proposition 3.7 we must use a method that is different. The result we need is a determination of the Witt group of $k(t)$ [48], obtained in the form we need by Milnor [27] (c.f. [23], [29]). A useful exposition of this result can be found in [24]. I will give here a consequence that is easy to apply. See [6, Thm. 11.1] for an analogous statement about the Witt group of $\mathbb{Q}$.

For a field F let $W(F)$ be its Witt group. See [29] or [24, Chap. II] for its definition and basic properties (assuming that the characteristic of F is not 2). We define a set of maps between Witt groups as follows. For each prime $p \in k[t]$ let

$$\psi(p) : W(k(t)) \to W(F_p)$$

be defined through

$$\psi(p)\langle a\rangle = \begin{cases} \langle \bar{u}\rangle, & \text{if } \ell \text{ is odd} \\ 0, & \text{otherwise,} \end{cases} \qquad \text{where } a = p^\ell u \text{ with } v_p(u) = 0.$$

Also, define $\psi(\infty) : W(k(t)) \to W(k)$ by

$$\psi(\infty)\langle a\rangle = \begin{cases} \langle \bar{a}_0\rangle, & \text{if } \ell \text{ is even} \\ 0, & \text{otherwise} \end{cases} \qquad \text{when } a(t^{-1}) = t^{-\ell}(a_0 + a_1 t + \dots). \tag{3.20}$$

Here $\bar{a}$ gives the natural image of $a \in k(t)^\bullet$ in $F_p^\bullet / F_p^{\bullet 2}$ (or of $a \in k^\bullet$ in $k^\bullet / k^{\bullet 2}$ when $p = \infty$). Then the following result is a consequence of [24, Milnor's Thm. p. 306]:

Proposition 3.8. *The map $\psi = \psi(\infty) \times \prod_p \psi(p)$ induces a group isomorphism*

$$W(k(t)) \to W(k) \times \prod_{p<\infty} W(F_p). \tag{3.21}$$

Here we use the first residue homomorphisms associated to the valuation at infinity to derive the map $\psi(\infty)$ in (3.21) from Milnor's split exact sequence (see the proof in [24]).

Proposition 3.7 follows from the next proposition and the definition of genera from above.

Proposition 3.9. *Let $D \in k[t]$ be square-free and negative with $|D|$ odd. Suppose that the forms $Q = (a, b, c)$ and $Q' = (a', b', c')$ are in $\mathcal{Q}_D$ with a, a' prime to D. Then Q and Q' are equivalent over $k(t)$ if and only if*

$$(a, D)_p = (a', D)_p \tag{3.22}$$

for all p, including $p = \infty$.

Proof. Each $Q = (a, b, c) \in \mathcal{Q}_D$ is equivalent over $k(t)$ to $\langle a, -\frac{D}{a}\rangle := (a, 0, -\frac{D}{a})$. We will use Proposition 3.8 to show that $\langle a, -aD\rangle$ and $\langle a', -a'D\rangle$ are Witt-equivalent if and only if $(a, D)_p = (a', D)_p$ for all p. This is enough since as forms over $k(t)$ they have the same dimension, namely 2 (see e.g. [24, Prop.1.4, p.29]).

For $p < \infty$ we have

$$\psi(p)\langle a, -aD\rangle = \begin{cases} \langle -\bar{u}\bar{a}\rangle, & D = pu \\ 0, & \text{otherwise} \end{cases} \qquad (a, D)_p = \begin{cases} \bar{a}, & p|D \\ 1, & \text{otherwise.} \end{cases} . \tag{3.23}$$

In both statements we use that D is a square modulo any p with $p|a$; in the first $\psi(p)\langle a, -aD\rangle$ is isotropic and in the second $(a, D)_p = 1$. Note that u in (3.23) only depends on D. Also, we have

$$\psi(\infty)\langle a, -aD\rangle = \langle 1\rangle, \quad (a, D)_\infty = 1. \tag{3.24}$$

Here the first statement follows using $a \succ 0$ and by referring to (3.20). That $(a, D)_\infty = 1$ was shown in Lemma 3.8. Comparison of both sides of (3.23) and (3.24) for each prime p and ∞, together with Proposition 3.8, completes the proof. □

Now we apply Proposition 3.7 to prove the following analogue of Gauss's principal genus theorem.

Proposition 3.10. *The principal genus coincides with $\mathcal{C}_D^2$ and hence $\mathcal{G}_D = \mathcal{C}_D/\mathcal{C}_D^2$.*

Proof. First suppose that the class of Q is the square of the class of $Q' = (a', b', c')$, where a' is chosen to be prime to D. By ii) of Proposition 3.4 we have that Q properly represents a'^2 and so $\chi_p(Q) = 1$ for all $p|D$, hence Q is in the principal genus.

Conversely, suppose that $Q = (a, b, c)$ is in the principal genus. By Proposition 3.7 we know that Q is rationally equivalent to $(1, 0, -D)$, so there are $q_1, q_2, r \in k[t]$ with $r \neq 0$ such that

$$a(\tfrac{q_1}{r})^2 + 2b(\tfrac{q_1}{r})(\tfrac{q_2}{r}) + c(\tfrac{q_2}{r})^2 = 1.$$

Hence Q represents r^2, but perhaps improperly. In any case, by Lemma 3.4 there are $s, b', c' \in k[t]$ with $s \succ 0$ so that Q is properly equivalent to (s^2, b', c') where $D = b'^2 - s^2c'$. If b' and s share a prime factor q, then q^2 divides both s^2 and b'^2 so must also divide D. But D is square-free. Thus s is prime to b'. By Proposition 3.2, the form $Q' = (s, b', c's) \in \mathcal{Q}_D$ will have the property that the square of its class is the class of Q.

□

4. The class group $\mathcal{C}_D$ and the Mordell-Weil group $\mathcal{J}_D$

Let k be a number field. Let $D \in k[t]$ be square-free and negative with odd degree $|D| = 2g+1$. In this section I will show that $\mathcal{C}_D$ is isomorphic to $\mathcal{J}_D$ and so, in particular, is finitely generated as a consequence of the Mordell Weil theorem.

Let $\mathcal{H}$ be a complete smooth curve with function field $k(t, s)$, where

$$s^2 = D(t).$$

The function t on $\mathcal{H}$ has a double pole that we denote ∞. Let $Q = (a, b, c)$ represent a class $C \in \mathcal{C}_D$. Then since $a \succ 0$ we can write

$$a(t) = \alpha^2 \prod_{i=1}^{m} (t_i - t)^{n_i} \tag{4.1}$$

with $\alpha \in k^\bullet$ and distinct $t_i \in \bar{k}$ and $n_i \in \mathbb{Z}^+$. Set $s_i = b(t_i)$. Let $\operatorname{div}(1, 0, -D) = 0$ and otherwise associate to Q the degree zero divisor on $\mathcal{H}$ given by

$$\operatorname{div}(Q) = \sum_{i=1}^{m} n_i(t_i, s_i) - N\infty, \tag{4.2}$$

where $N = \sum_{i=1}^{m} n_i$. It is defined over k and is semi-reduced in that if (t, s) occurs in $\operatorname{div}(Q)$, then $(t, -s)$ does not, unless $s = 0$, in which case the multiplicity of $(0, t)$ is one.

As before, let $\mathcal{J}_d$ be the group of k-rational divisor classes of degree 0 on $\mathcal{H}$. We want to prove the following.

Proposition 4.1. *The map $Q \mapsto \operatorname{div}(Q)$ induces an isomorphism of groups from $\mathcal{C}_D$ onto $\mathcal{J}_D$.*

Lemma 4.1. *The map $Q \mapsto \operatorname{div}(Q)$ induces a map ϕ from $\mathcal{C}_D$ to $\mathcal{J}_D$.*

Proof. We must show that $Q \sim Q'$ implies that $\operatorname{div}(Q)$ is equivalent to $\operatorname{div}(Q')$. Let $a(t)$ be as in (4.1). If Q' results from Q by a translation $Q' = Q|T_n$ with $n \in k[t]$, we see that $\operatorname{div}(Q) = \operatorname{div}(Q')$ since from (3.4),

$$b(t_i) + n(t_i)a(t_i) = b(t_i).$$

By Lemma 3.2, we are reduced to showing the needed equivalence when $Q' = Q|S = (c, -b, a)$. As in the proof of Lemma 3.5, we know that $c \succ 0$, so we have

$$c(t) = \gamma^2 \prod_{j=1}^{m'} (t'_j - t)^{n'_j}$$

with $\gamma \in k^\bullet$ and $N' = \sum_{j=1}^{m'} n'_j$, where $n'_j \in \mathbb{Z}^+$. Thus by (4.2) we need to show that

$$\operatorname{div}(a, b, c) = \sum_{i=1}^{m} n_i(t_i, b(t_i)) - N\infty \quad \text{and} \quad \operatorname{div}(c, -b, a) = \sum_{j=1}^{m'} n'_j(t'_j, -b(t'_j)) - N'\infty$$

are equivalent. Define the rational function f on $\mathcal{H}$ by

$$f = \frac{c(t)}{s - b(t)} = -\frac{s + b(t)}{a(t)}.$$

Now we will show that

$$(f) = \big(\operatorname{div}(c, -b, a) - \operatorname{div}(a, b, c)\big)$$

where, as usual, (f) is the divisor of f. This will prove the claim.

Suppose first that $b(t_i) \neq 0$ and $b(t'_j) \neq 0$. Clearly $(t_i, b(t_i)) \neq (t'_j, -b(t'_j))$. The factors

$$s - b(t) \ \text{ and } \ c(t)$$

have zeros of order n_i at $(t_i, b(t_i))$ and n'_j at $(t'_j, \mp b(t'_j))$, respectively. Of the latter, the zeros at $(t'_j, b(t'_j))$ are cancelled by the factor $s - b(t)$. A similar argument works for any points $(t_i, 0)$ or $(t'_j, 0)$ that occur. Since d is square-free, $(t_i, 0) \neq (t'_j, 0)$.

Finally, the behavior at infinity also matches since t has a double pole at ∞.

□

Lemma 4.2. *The map $\phi : \mathcal{C}_D \to \mathcal{J}_D$ is a group homomorphism.*

Proof. By Lemma 3.4 and Proposition 3.2, any two classes $C, C' \in \mathcal{C}_D$ contain forms $Q = (a, b, ca')$ and $Q' = (a', b, ac)$, resp., where a, a' are coprime and prime to D, and the composition of C and C' contains the form $Q'' = (aa', b, *)$. Thus $\mathrm{div}(Q) + \mathrm{div}(Q') = \mathrm{div}(Q'')$. □

Proposition 4.1 now follows from the next lemma.

Lemma 4.3. *The map $\phi : \mathcal{C}_D \to \mathcal{J}_D$ is bijective.*

Proof. By Proposition 3.1, every class $C \in \mathcal{C}_D$ contains a unique form $Q = (a, b, c)$ where

$$|b| < |a| \leq g,$$

with $(-1)^{|a|}a$ monic. By the Riemann-Roch theorem (see e.g. [25]) and a straightforward argument (c.f. [4, pp. 96-97]), every divisor class has a unique representative of the form $\mathrm{div}(Q)$ for such a Q. Here b is uniquely determined by the condition $|b| < |a|$. □

Proposition 4.2. *For k a number field, $D \in k[t]$ square-free and negative of odd degree, the group $\mathcal{C}_D$ is finitely generated.*

Proof. This follows from Proposition 4.1 and the Mordell-Weil Theorem [47], [26]. □

Remark. As already mentioned, that a result like Proposition 4.1 should hold can be inferred from the paper of D. Cantor [4] (see also [32]). However, the isomorphism we give does not seem to be well-known.

The four part of $\mathcal{J}_D$. For any finitely generated abelian group G, let $e_n = e_n(G)$ be the number of subgroups of order 2^m, where $m \geq n$, in a representation of the torsion part of G as a direct product of cyclic subgroups of prime power order.

Again, let $\mathcal{J} = \mathcal{J}_D$ be the Mordell-Weil group of the hyperelliptic curve over a number field k given by $s^2 = D(t)$. As is well-known (and also follows from Propositions 3.5 and 4.1), for $D \in k[t]$ monic and square-free of odd degree, there are $2^{e_1(\mathcal{J})}$ factorizations $D = D_1 D_2$ into co-prime monic polynomials, where D_2 has odd degree. Our next result determines $e_2(\mathcal{J})$.

Proposition 4.3. *Let $D \in k[t]$ be square-free and monic of odd degree. Then there are $2^{e_2(\mathcal{J})}$ factorizations $D = D_1 D_2$ into monic polynomials each in $k[t]$ with D_2 of odd degree, where $(\frac{D_1}{p}) = 1$ for each prime $p|D_2$ and $(\frac{-D_2}{p}) = 1$ for each prime $p|D_1$.*

Proof. By Proposition 4.1, we require a characterization of those classes in $\mathcal{C}_D$ of order at most 2 that are contained in $\mathcal{C}_D^2$.

Claim: the number of such classes is given by $2^{e_2(\mathcal{J})}$, where as before we write $\mathcal{J} = \mathcal{J}_D$. To see this, let m be the number of primary cyclic subgroups of order 2. The number of classes C for which $C^4 = 1$ is

$$2^m 4^{e_2(\mathcal{J})} = 2^{m+e_2(\mathcal{J})} 2^{e_2(\mathcal{J})} = 2^{e_1(\mathcal{J})} 2^{e_2(\mathcal{J})} = \#\,(\text{classes of order at most 2}) \times 2^{e_2(\mathcal{J})}. \tag{4.3}$$

For each class in $C_2 \in \mathcal{C}_D$ of order at most 2 contained in $\mathcal{C}_D^2$, choose a fixed $C_1 \in \mathcal{C}_D$ with $C_1^2 = C_2$. By multiplication of each C_1 by all classes of order at most 2, we get all classes C with $C^4 = 1$. The claim follows by a comparison with (4.3).

Proposition 3.10 implies that $2^{e_2(\mathcal{J})}$ is the number of classes of order at most 2 that are contained in the principal genus of $\mathcal{C}_D$. By (the proof of) Proposition 3.5, these classes are in one-to-one correspondence with the ambiguous forms $(D_1, 0, -D_2)$ that are killed by all genus characters, where $D = D_1 D_2$ is as in the statement of the theorem. Using the definition of the genus characters given in (3.17), these forms correspond to the decompositions described in Proposition 4.3. □

Proof of Theorem 1. i) ($\mathcal{J}_q$ finite implies that (1.2) holds.) Suppose that $\mathcal{J}_q$ is finite. By Proposition 4.1 we know that $\mathcal{C}_q$ is finite. Since q is a prime, it follows from Proposition 3.5 that $\mathcal{C}_q$ has no classes of positive even order and so any class $C \in \mathcal{C}_q$ is in $\mathcal{C}_q^2$. Let p be any prime different from q. If $\left(\frac{q}{p}\right) = 1$ then $q = b^2 + pc$ for some b, c, so $Q = (p^*, b, \pm c) \in \mathcal{Q}_q$. If $Q \in C$ then since $C \in \mathcal{C}_q^2$, we have that $\chi_q(Q) = (p^*, q)_q = 1$ and $\left(\frac{p^*}{q}\right) = 1$.

ii) ($\mathcal{J}_q$ infinite implies (1.2) does not hold.) By Proposition 4.1 again, if $\mathcal{J}_q$ is infinite so is $\mathcal{C}_q$ and by Proposition 4.2 it must contain a class C not in $\mathcal{C}_q^2$. Let $Q(x, y) = (a, b, c) \in C$, so $b^2 - ac = q$. By Proposition 3.1 and the proof of Lemma 3.5, we may assume that $|b| < |a| < |c|$ with c^* monic. The polynomial

$$F(x, t) = a(t)x^2 + 2b(t)x + c(t)$$

is irreducible in $k[y, t]$. To see this, observe that $\gcd(a, b, c) = 1$ and, as a quadratic in x, the discriminant of F is $4q(t)$, which is not a square. By Hilbert's irreducibility theorem [19], [26] there are infinitely many $x \in k$ such that $F(x, t) = Q(x, 1)$ is irreducible in $k[t]$. For any such x, it follows from Lemma 3.4 that C contains the form $Q' = (p^*, b', c')$, where

$$p(t) = (-1)^{|c|}Q(x, 1) \neq q(t)$$

is prime. Thus $q = b'^2 - p^*c'$ and so $\left(\frac{q}{p}\right) = 1$. Since $C \notin \mathcal{C}_q^2$, by the principal genus theorem Proposition 3.10, we must have that $\chi_q(Q') = (p^*, q)_q \neq 1$. Thus $\left(\frac{p^*}{q}\right) \neq 1$. □

Remark. It is easy to modify the above argument to produce infinitely many primes p of either odd or even degree with $\left(\frac{p^*}{q}\right) \neq 1$.

Proof of Theorem 2. i) If $p(t)x^2 - q(t)y^2 = z^2$ has nontrivial solutions $x, y, z \in k[t]$ then clearly $\left(\frac{p}{q}\right) = 1$ and $\left(\frac{-q}{p}\right) = 1$. Proposition 4.3 implies that $\mathcal{J}_{pq}$ has an element of order 4.

ii) As before, we may identify $\mathcal{C}_{pq}$ with $\mathcal{J}_{pq}$. Since p, q are primes with $|p|$ even and $|q|$ odd, by Proposition 3.5 the form $Q = (p, 0, -q)$ represents the unique class of order 2 in $\mathcal{C}_{pq}$. If $\mathcal{C}_{pq}$ has an element of order 4 the class of Q is a square in $\mathcal{C}_{pq}$ and so by Proposition 3.4, $p(t)x^2 - q(t)y^2 = z^2$ has nontrivial solutions. □

Proof of Theorem 3. Suppose that a factorization $D = D_1D_2$ exists where D_1, D_2 are monic with the degree of D_1 even and positive, and that for every arithmetic progression $P \subset \mathbb{Z}$ there is a $t_0 \in P$ so that $D_1(t_0)x^2 - D_2(t_0)y^2 - z^2 = 0$ has a non-trivial solution $x, y, z \in k$. Then by the theorem of Schinzel quoted above Theorem 3, we know that $D_1(t)x^2 - D_2(t)y^2 - z^2 = 0$ has a non-trivial solution with $x, y, z \in k[t]$. By Proposition 4.3 it follows that $\mathcal{J}_D$ must have elements of order 4. □

5. Binary cubic forms over $k[t]$

Preliminaries. Many of the general identities and transformation properties of binary cubic forms over $\mathbb{Z}$ can be readily adapted to forms with coefficients in $k[t]$. Some references for the classical theory are [20] and [39]. For $a, b, c, d \in k[t]$ let

$$F(u, v) = au^3 + 3bu^2v + 3cuv^2 + dv^3 = (a, b, c, d)(u, v).$$

Its discriminant is

$$\Delta = \Delta_F = a^2d^2 - 6abcd + 4b^3d + 4ac^3 - 3b^2c^2 = (ad - bc)^2 - 4(ac - b^2)(bd - c^2).$$

The Hessian of F is

$$H_F(u, v) = (ac - b^2)u^2 + (ad - bc)uv + (bd - c^2)v^2 = (ac - b^2, \tfrac{1}{2}(ad - bc), bd - c^2)(u, v) \tag{5.1}$$

and the cubic covariant is

$$J_F(u,v) = (2b^3 - 3abc + a^2d, b^2c - 2ac^2 + abd, -bc^2 + 2b^2d - acd, -2c^3 + 3bcd - ad^2).$$

The discriminant of H_D is $D = \frac{1}{4}\Delta_F$. The group $\mathrm{SL}_2(k[t])$ acts as expected on F, H_F, J_F: thus for $M = \left(\begin{smallmatrix} m & r \\ n & s \end{smallmatrix}\right)$ we have $F|M(x,y) = F(mx+ny, rx+sy)$. The discriminant Δ_F is invariant and the forms H_F and J_F are covariants of F, meaning that $H_{F|M} = H_F|M$ and $J_{F|M} = J_F|M$. The principal form of discriminant $\Delta = 4D$

$$F_0 = (0,1,0,D) \tag{5.2}$$

has $-H_0 := -H_{F_0} = (1,0,-D)$ and $\frac{1}{2}J_0 := \frac{1}{2}J_{F_0} = (1,0,D,0)$.

The syzygy and its converse. After Eisenstein [14] and Cayley [8], a cubic form and its covariants satisfy the syzygy

$$J_F^2 = -4H_F^3 + \Delta F^2,$$

which can be checked directly. Setting $X = -H_F$, $Y = \frac{1}{2}J_F$ and $Z = F$ we have

$$Y^2 = X^3 + DZ^2, \tag{5.3}$$

where $D = \frac{1}{4}\Delta$ is the discriminant of H_F. The following converse result is crucial. Over $\mathbb{Z}$ the corresponding result is due to Arndt [1] and Mordell [30], [31, p.216].

Proposition 5.1. *Suppose that $D \in k[t]$ is square-free. If $X, Y, Z \in k[t]$ satisfy* $\gcd(X,Z) = \gcd(Y,Z) = 1$ *and*

$$Y^2 = X^3 + DZ^2,$$

then there exists a binary cubic form $F = (Z,b,c,d)$ with $b,c,d \in k[t]$ and discriminant $4D$ for which $-H_F = (X,*,*)$ and $\frac{1}{2}J_F = (Y,*,*,*)$.

Proof. First note that $\gcd(X,Y) = 1$ since D is square-free. Thus both X and Y are prime to D. From (5.3) we see that D is a square modulo X so there exists a binary form (X,B,C) with $B^2 - XC = D$. We have that $\gcd(Z,X) = 1$ and from (5.3) we may suppose that

$$ZB \equiv -Y \pmod{X^3}. \tag{5.4}$$

The class of (X,B,C) is uniquely determined once we force B to satisfy condition (5.4). Clearly $X \neq 0$. After Arndt [1], set

$$b = \tfrac{1}{X}(Y+BZ) \quad c = \tfrac{1}{X^2}(DZ+2YB+ZB^2) \quad d = \tfrac{1}{X^3}(YD+3BDZ+3YB^2+ZB^3). \tag{5.5}$$

A calculation shows that the discriminant of $F = (Z,b,c,d)$ is $4D$, that $-H_F = (X,B,C)$ and that $\frac{1}{2}J_F = (Y,*,*,*)$.

We need to show that $b,c,d \in k[t]$. Clearly $b \in k[t]$.

To see that $c \in k[t]$, consider

$$\begin{aligned} U \times V =& (DZ + 2YB + ZB^2)(DZ - 2YB + ZB^2) \\ &= Z^2(D+B^2)^2 - 4Y^2B^2 \\ &\equiv Z^2(D+B^2)^2 - 4DZ^2B^2 \pmod{X^3} \text{ by (5.3)} \\ &= Z^2(B^2-D)^2 \equiv 0 \pmod{X^2}. \end{aligned}$$

Now U and V cannot share any primes with X since $U - V = 4YB$. That $c \in k[t]$ will follow if we can show that $X|ZU$. From $X|(ZB+Y)$ we have that

$$ZU \equiv Z(DZ+YB) \equiv Y(Y+ZB) \equiv 0 \pmod{X}.$$

Finally, from (5.5) we must prove that

$$X^3d = YD + 3BDZ + 3YB^2 + ZB^3 \equiv 0 \pmod{X^3}.$$

Using (5.4) we have that

$$Z^2X^3d \equiv Z^2YD - 3YDZ^2 + (3Y^3 - Y^3) \equiv 2Y(Y^2 - DX^2) \equiv 0 \pmod{X^3},$$

as desired. □

Proposition 5.2. *Suppose that $D \in k[t]$ is square-free and negative with odd degree. Let $F = (a, b, c, d)$ with $a, b, c, d \in k[t]$ have discriminant $4D$. Then $Q = -H_F = (A, B, C) \in \mathcal{Q}_D$ and its class has order 1 or 3 in $\mathcal{C}_D$. The only other cubic form with Hessian $-Q$ is $-F$.*

Proof. To show that $Q \in \mathcal{Q}_D$, first note that the discriminant of Q is D. We also must have $A \succ 0$. To see this we can apply (5.3). First, if $|A|$ is even we need the leading coefficient A_0 of A to be in $k^{\bullet 2}$. Since DZ^2 has odd degree we have $A_0^3 = Y_0^2$ where Y_0 is the leading coefficient of Y, so $A_0 = (\frac{Y_0}{A_0})^2$. If $|A|$ is odd the leading coefficients of A^3 and DZ^2 must cancel so again $A_0 \in k^{\bullet 2}$.

Next we show that the class of $Q = (A, B, C)$ has order 1 or 3. We have the following identity (from [9]) that can be verified directly:

$$\begin{aligned}(A, -B, C)&(buu' + cuv' + cu'v + dvv', auu' + buv' + bu'v + cvv') \\ &= (A, B, C)(u, v) \times (A, B, C)(u', v'),\end{aligned} \tag{5.6}$$

where $A = b^2 - ac, B = bc - ad$ and $C = c^2 - bd$. Thus by Proposition 3.3 and ii) of Proposition 3.2 we have $Q \otimes Q = Q^{-1}$, so that the class of Q has order 1 or 3 in $\mathcal{C}_D$.

The proof of the final statement is also adapted from [9, 2nd letter], but the argument required some reworking to make it more understandable. Suppose that $F' = (a', b', c', d')$ has $-H_{F'} = (A, B, C)$. By (5.6) we have

$$(A, -B, C)(x, y) = (A, -B, C)(x', y')$$

where

$$\begin{aligned} x &= buu' + cuv' + cu'v + dvv' \\ y &= auu' + buv' + bu'v + cvv' \\ x' &= b'uu' + c'uv' + c'u'v + d'vv' \\ y' &= a'uu' + b'uv' + b'u'v + c'vv'. \end{aligned} \tag{5.7}$$

Also by assumption

$$A = b^2 - ac = b'^2 - a'c' \quad B = bc - ad = b'c' - a'd' \quad C = c^2 - bd = c'^2 - b'd'. \tag{5.8}$$

First we will show that

$$(x', y')^t = M(x, y)^t \quad \text{for} \quad M = \left(\begin{smallmatrix} m & r \\ n & s \end{smallmatrix}\right) \in \mathrm{SL}_2(k(t)). \tag{5.9}$$

After verifying this, we will show that in fact we may take $m, r, n, s \in k[t]$. Given this, the uniqueness of F up to sign follows from Lemma 3.3, which implies that Q has only trivial automorphs.

A calculation shows that if

$$m = \tfrac{bb'-ac'}{A} \quad r = \tfrac{-cb'+bc'}{A} \quad n = \tfrac{ba'-ab'}{A} \quad s = \tfrac{-ca'+bb'}{A} \tag{5.10}$$

then $\det M = 1$. Here we use the first formula of (5.8) and that $A \neq 0$. Another calculation using (5.10) gives that

$$\begin{aligned} bm + ar &= b' \quad & bn + as &= a' \\ cm + br &= c' \quad & cn + bs &= b'. \end{aligned}$$

To verify (5.9) it is now enough to show that $dm + cr = d'$ and $dn + cs = c'$. By (5.10) and (5.8)

$$d(bb' - cc') + c(-cb' + bc') = -Cb' + c'B = b'^2 d' - a'c'd' = d'A,$$

which gives $dm + cr = d'$. That $dn + cs = c'$ follows similarly.

Finally, we must show that $m, r, n, s \in k[t]$. In case $B = 0$ we have from (5.7) and (5.9) that

$$cm + br = c', \quad dm + cr = d' \quad \text{and} \quad cn + bs = b', \quad dn + cs = c',$$

hence that

$$m = \tfrac{cc'-bd'}{C} \quad r = \tfrac{-dc'+cd'}{C} \quad n = \tfrac{cb'-bd'}{C} \quad s = \tfrac{-db'+cc'}{C}.$$

Since $\gcd(A, C) = 1$, from this and (5.10) we must have that $m, r, n, s \in k[t]$. If $B \neq 0$ we argue similarly by giving a third set of fractions from (5.7) and (5.9) for m, r, n, s, now with denominator B, starting with

$$bm + ar = b', \quad dm + cr = d' \text{ and } bn + as = a', \quad dn + cs = c'.$$

□

Propositions 5.2 and 4.1 imply the following result about the number of classes of binary cubic forms defined with respect to $\mathrm{SL}_2(k[t])$.

Proposition 5.3. *Let k be a number field and $D \in k[t]$ be negative, square-free and of odd degree $|D|$. Then the class number of binary cubics over $k[t]$ with discriminant $4D$ is at most $3^{|D|-1}$.*

Elliptic curves over $k(t)$. Consider the elliptic curve with j-invariant zero over $k(t)$ defined by

$$\mathcal{E}_D : y^2 = x^3 + D(t) \tag{5.11}$$

where $D \in k[t]$ is square-free. Recall that $D' = -27D(-3t)$, which is also square-free and that if D is negative with odd degree so is D'. By the Mordell-Weil theorem over function fields ([33], see also [45, p.230]) the rational points on $\mathcal{E}_D$ and $\mathcal{E}_{D'}$ form finitely generated abelian groups.

We have the pair of dual 3-isogenies $\psi : \mathcal{E}_D \to \mathcal{E}_{D'}$ and $\psi' : \mathcal{E}_{D'} \to \mathcal{E}_D$ given by

$$\begin{aligned} \psi : (x, y) &\mapsto \Big(\big(\tfrac{x^3+4D}{x^2}\big)^{\sigma}, \big(\tfrac{y(x^3-8D)}{x^3}\big)^{\sigma} \Big) \quad \text{and} \\ \psi' : (x', y') &\mapsto \Big(\big(\tfrac{x'^3+4D'}{9x'^2}\big)^{\sigma^{-1}}, \big(\tfrac{y'(x'^3-8D')}{27x'^3}\big)^{\sigma^{-1}} \Big), \end{aligned} \tag{5.12}$$

where $\sigma : k(t) \to k(t)$ is the automorphism defined by $t \mapsto -3t$. Then $\psi' \circ \psi$ and $\psi \circ \psi'$ give the tripling maps on $\mathcal{E}_D$ and $\mathcal{E}_{D'}$, respectively.

Suppose that D is negative and of odd degree. Given a (finite) rational point $P = (x, y)$ on $\mathcal{E}_D$ we can write $(x, y) = (\frac{X}{V^2}, \frac{Y}{V^3})$ where $V \in k[t]$ is monic and $\gcd(X, V) = \gcd(Y, V) = 1$. Taking $Z = V^3$, we associate to P the class C_P of any form $Q = -H_F$ that, together with F and J_F, gives rise to P via Proposition 5.1. Note that the class of Q is uniquely determined by (5.4). Thus by Proposition 5.2, C_P has order 1 or 3 in $\mathcal{C}_D$. Similarly we associate to any point $P' = (x', y')$ on $\mathcal{E}_{D'}$ the class $C_{P'}$, which has order 1 or 3 in $\mathcal{C}_{D'}$.

Lemma 5.1. *The class $C_P \in \mathcal{C}_D$ has order 1 if and only if P is the image of some $Q' \in \mathcal{E}_{D'}$ under ψ'. The class $C_{P'} \in \mathcal{C}_{D'}$ has order 1 if and only if P' is the image of some $Q \in \mathcal{E}_D$ under ψ.*

Proof. Note that $F(u,v)=V^3$ if and only if $F(\frac{u}{V},\frac{v}{V})=1$. Recall the principal form F_0 from (5.2). It is readily checked that there is a bijection between the set

$$\{(x,y)\in k(t)^2; F_0(x,y)=3x^2y+Dy^3=1\} \tag{5.13}$$

and the finite rational points (x',y') on $\mathcal{E}_{D'}$ given by

$$(x',y')=\big((\tfrac{3}{y})^{\sigma},(\tfrac{9x}{y})^{\sigma}\big) \quad\text{and}\quad (x,y)=\big((\tfrac{y'}{3x'})^{\sigma^{-1}},(\tfrac{3}{x'})^{\sigma^{-1}}\big). \tag{5.14}$$

A computation using (5.12) and (5.2) shows that for (x,y) with $3x^2y+Dy^3=1$ and (x',y') from (5.14) we have

$$\psi'(x',y')=\big(-H_0(x,y),\tfrac{1}{2}J_0(x,y)\big).$$

The first statement follows since we have from Proposition 5.2 that $-H_F$ is principal if and only if F is principal.

The proof of the second statement is similar, using that for $F_0'=(0,1,0,D')$ there is a bijection between the set

$$\{(x',y')\in k(t)^2; F_0'(x',y')=3x'^2y'+D'y'^3=1\}$$

and the finite rational points (x,y) on $\mathcal{E}_D$ from (5.11) given by

$$(x,y)=\big((\tfrac{1}{3y'})^{\sigma^{-1}},(\tfrac{x'}{3y'})^{\sigma^{-1}}\big) \quad\text{and}\quad (x',y')=\big((\tfrac{y}{x})^{\sigma},(\tfrac{1}{3x})^{\sigma}\big).$$

Now use that

$$\psi(x,y)=\big(-H_0'(x',y'),\tfrac{1}{2}J_0'(x',y')\big),$$

where $-H_0'=-H_{F_0'}=(1,0,-D')$ and $\frac{1}{2}J_0'=\frac{1}{2}J_{F_0'}=(1,0,D',0)$ and apply Proposition 5.2 as before. □

Proof of Theorem 4. To prove the first statement, suppose that $P=(x,y)\in\mathcal{E}_D$. Then

$$2P=(x',y')=\big(\tfrac{9x^4}{4y^2}-2x,\tfrac{8y^4-36x^3y^2+27x^6}{8y^3}\big).$$

Write $(x,y)=(\frac{X}{V^2},\frac{Y}{V^3})$ where $X,Y,V\in k[t]$ with $\gcd(X,V)=\gcd(Y,V)=1$. Then we have

$$Y^2=X^3+DV^6 \quad\text{and} \tag{5.15}$$

$$V^2x'=\tfrac{9X^4}{4Y^2}-2X \quad\text{and}\quad V^3y'=\tfrac{8Y^4-36X^3Y^2+27X^6}{8Y^3}. \tag{5.16}$$

Since D is square-free we must have $\gcd(X,Y)=1$. There are two cases to consider.

i) If $|Y|>0$ then the denominator of x' has larger degree than that of x and so the first statement of Theorem 4 follows.

ii) If $Y\in k^{\bullet}$ then we may write $(x',y')=(\frac{X'}{V^2},\frac{Y'}{V^3})$ where $X',Y'\in k[t]$. Here $\gcd(X',V)=\gcd(Y',V)=1$, since by (5.15) and (5.16) we have for any prime $P|V$

$$\begin{aligned}&4Y^2X'=X(9X^3-8Y^2)\equiv XY^2 \pmod P \quad\text{and}\\ &8Y^3Y'=8Y^4-36X^3Y^2+27X^6=27D^2V^{12}-18DV^6Y^2-Y^4\equiv -Y^4 \pmod P,\end{aligned} \tag{5.17}$$

where $Y\neq 0$ and $P\nmid X$. Since $|D|>0$ we have from (5.15) that $|X|>0$, hence from the first equation of (5.17) that $|Y'|>0$. Repeat the argument from the beginning with $P=(x',y')\in\mathcal{E}_D$ in place of (x,y). Now i) applies and again the first statement of Theorem 4 follows.

Now we prove the (contrapositive of the) second statement of Theorem 4. By the first statement and Mordell-Weil for $\mathcal{E}_D$, if $\mathcal{E}_D$ has a finite rational point, it is of infinite order and we may assume that it is not the triple of any other point. Let P be such a point. If the $C_P\in\mathcal{C}_D$ that corresponds to P as above Lemma 5.1 is not trivial we are done,

since P is then of order 3. Otherwise, by Lemma 5.1, P is the image under ψ' of some point $P' \in \mathcal{E}_{D'}$. In that case the class $C_{P'}$ in $\mathcal{C}_{D'}$ corresponding to P' is of order 3, since otherwise $P' = \psi(Q)$ for some $Q \in \mathcal{E}_D$ and then $P = \psi'(\psi(Q)) = 3Q$, and P is a triple. The second statement now follows since $\mathcal{J}_D$ is isomorphic to $\mathcal{C}_D$ and $\mathcal{J}_{D'}$ is isomorphic to $\mathcal{C}_{D'}$ by Proposition 4.1. □

Remark. To prove the last statement of Example ii) from the end of the Introduction, note that if $b^2 - a^3 = D(t)$ where $a, b \in k[t]$ with D monic and square-free of odd degree, then $Q = (a, b, a^2) \in \mathcal{C}_D$. By the formula for composition, Q has order dividing 3. It must have order 3 by Proposition 3.1, since $|a| > 0$ and the unique reduced form equivalent to Q is of the form $(a, *, *)$.

References

[1] Arndt, F. Zur Theorie der binären kubischen Formen. J. Reine Angew. Math. 53, 309-321 (1857).

[2] Artin, E. Quadratische Körper im Gebiete der höheren Kongruenzen, I. Math. Zeit. 19 (1924), 153–206, Thesis in Collected Papers.

[3] Borevich, A. I.; Shafarevich, I. R. Number theory. Translated from the Russian by Newcomb Greenleaf Pure Appl. Math., Vol. 20 Academic Press, New York-London, 1966.

[4] Cantor, D. Computing in the Jacobian of a hyperelliptic curve. Math. Comp. 48 (1987), no.177, 95–101.

[5] Cantor, G. Zwei Sätze aus der Theorie der binären und quadratischen Formen. Zeit. Math. Physik, 13, 259-261 (1868), in Gesammelte Abhandlungen I #2.

[6] Cassels, J. W. S. Rational quadratic forms. Academic Press, Inc. , London-New York, 1978.

[7] Cassels, J. W. S.; Schinzel, A. Selmer's conjecture and families of elliptic curves. Bull. London Math. Soc. 14 (1982), no.4, 345–348.

[8] Cayley, A. Note sur les covariants d'une fonction quadratique, cubique, ou biquadratique à deux indéterminnées, J. Reine Angew. Math. 50 (1855), 285–287, in Collected Papers Vol. 2. #135.

[9] Cayley, A. Two letters on cubic forms, Quarterly J. I (1857), 85–87, 90-91, in Collected Papers Vol. 3. #162.

[10] Cox, D. A. Primes of the form $x^2 + ny^2$—Fermat, class field theory, and complex multiplication. with solutions. With contributions by Roger Lipsett AMS Chelsea Pub. Providence, RI, (2022).

[11] Davenport, H.; Lewis, D. J.; Schinzel, A. Quadratic Diophantine equations with a parameter. Acta Arith.11 (1965/66), 353–358.

[12] Dedekind, R. Abriss einer Theorie der höhreren Kongruenzen in bezug auf einen reelen Primzahl-Modulus, J. für reine und angew. Math. 54, (1857), 1–26, V. in Werke.

[13] Dirichlet, G. L. Vorlesungen über Zahlentheorie, 4th ed., with Supplements added by R. Dedekind, Vieweg und Sohn, Braunschweig, 1894.

[14] Eisenstein, G. Untersuchungen über die kubischen Formen mit zwei Variabeln. J. Reine Angew. Math. 27, 89-104 (1844), in Werke, I, p.10.

[15] Fueter, R. Über kubische diophantische Gleichungen. Commentarii Math. Helvetici 2, 69-89 (1930).

[16] Gauss, C. F. Werke I. Göttingen (1870).

[17] Gauss, C. F. Disquisitiones arithmeticae. Translated and with a preface by Arthur A. Clarke. Springer-Verlag, New York, 1986.

[18] Hermite, C. Lettre à Cayley sur les formes cubiques, Quarterly. J. I, (1857), in Oeuvres I p.437–439.

[19] Hilbert, D. Uber die Irreducibilitat ganzer rationaler Functionen mit ganzzahligen Coefficienten, J. reine angew. Math. 110 (1892) 104–129, #18 in Gesammelte Abhandlungen II.

[20] Hilbert, D. Theory of algebraic invariants. Translated from the German and with a preface by R. C. Laubenbacher. Edited and with an introduction by B. Sturmfels Cambridge University Press, Cambridge, 1993.

[21] Hooley, C. On polynomials that are sums of two cubes. Rev. Mat. Complut. 20 (2007), no.1, 207–238.

[22] Jacobi, C.G.J. Über eine neue Methode zur Integration der hyperelliptischen Differentialgleichungen und über die rationale Form ihrer vollständigen algebraischen Integralgleichungen. J. Reine Angew. Math. 32 (1846), 220–226. #13 in Werke II.

[23] Knebusch, M. Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinearformen. S.-B. Heidelberger Akad. Wiss. Math.-Natur. Kl. 1969/70 (1969/70/1970), 93–157.

[24] Lam, T. Y. The Algebraic Theory of Quadratic Forms, Benjamin/Cummings, Reading, MA, 1980.

[25] Lang, S. Introduction to algebraic geometry. Interscience Pub., New York-London, 1958.
[26] Lang, S. Fundamentals of Diophantine geometry. Springer-Verlag, New York, 1983.
[27] Milnor, J. Algebraic K-theory and quadratic forms. Invent. Math. 9 (1969/70/1970), 318–344.
[28] Milnor, J. Introduction to algebraic K-theory. Ann. of Math. Stud., No. 72 Princeton University Press, Princeton, NJ; University of Tokyo Press, Tokyo, 1971.
[29] Milnor, J.; Husemoller, D. Symmetric bilinear forms. Ergeb. Math. Grenzgeb., Band 73, Springer-Verlag, New York-Heidelberg, 1973.
[30] Mordell, L. J. The Diophantine equation $y^2 - k = x^3$. Proc. Lond. Math. Soc. (2) 13, 60-80 (1914).
[31] Mordell, L. J. Diophantine equations. Pure Appl. Math., Vol. 30 Academic Press, London-NY, 1969.
[32] Mumford, D. Tata lectures on theta. II. Jacobian theta functions and differential equations. Progr. Math., 43 Birkhäuser Boston, Inc., Boston, MA, 1984.
[33] Néron, A. Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps. Bull. Soc. Math. France 80 (1952), 101–166.
[34] Newman, M. Integral matrices. Pure Appl. Math., Vol. 45 Academic Press, New York, (1972).
[35] Pizzo, M.; Pomerance, C.; Voight, J. Counting elliptic curves with an isogeny of degree three. Proc. Amer. Math. Soc. Ser. B7 (2020), 28–42.
[36] Rédei, L.; Reichardt, H. Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers. J. Reine Angew. Math. 170 (1934), 69–74.
[37] Rohrlich, D.E. Variation of the root number in families of elliptic curves. Compositio Math. 87 (1993), 119–151.
[38] Rosen, M. Number theory in function fields. Grad. Texts in Math., 210 Springer-Verlag, NY, 2002.
[39] Salmon, G. Lessons introductory to the modern higher algebra, 5th ed. Chelsea, N.Y.
[40] Schinzel, A. Selected topics on polynomials. University of Michigan Press, Ann Arbor, MI, 1982.
[41] Schinzel, A. Polynomials with special regard to reducibility. With an appendix by Umberto Zannier Encyclopedia Math. Appl., 77 Cambridge University Press, Cambridge, 2000.
[42] Schmidt, W. M. On continued fractions and Diophantine approximation in power series fields. Acta Arith. 95 (2000), no.2, 139–166.
[43] Scholz, A. Über die Beziehung der Klassenzahlen quadratischer Körper zueinander. J. Reine Angew. Math.166 (1932), 201–203.
[44] Serre, J.P. Spécialisation des éléments de $Br_2(\mathbb{Q}(T_1 \cdots, T_n))$ C. R. Acad. Sci. Paris Sér. I Math. 311 (1990), no.7, 397–402.
[45] Silverman, J. H. Advanced topics in the arithmetic of elliptic curves. Grad. Texts in Math., 151 Springer-Verlag, New York, 1994.
[46] Venkov, B. A. Elementary number theory. Translated by Helen Alderson Wolters-Noordhoff Publishing, Groningen, 1970.
[47] Weil, A. L'arithmétique sur une courbe algébrique. Acta. Math. 52, 1–35 (1928), in Oeuvres I, 11–45.
[48] Witt, E. Theorie der quadratischen Formen in beliebigen Körpern, J. Reine Angew. Math. 176 (1937), 31–44, #1 in Gesammelte Abhandlungen.
[49] Zannier, U. A local-global principle for norms from cyclic extensions of Q(t) (a direct, constructive and quantitative approach). Enseign. Math. (2) 5 (1999), no.3-4, 357–377.
[50] Zannier, U. Hyperelliptic continued fractions and generalized Jacobians. Amer. J. Math. 141 (2019), no.1, 1–40.

UCLA Mathematics Department, Box 951555, Los Angeles, CA 90095-1555
Email address: wdduke@g.ucla.edu