Rational Divisors in Rational Divisor Classes

N. Bruin[⋆1] and E.V. Flynn[⋆⋆2]

[1] Department of Mathematics, Simon Fraser University
Burnaby, BC, Canada V5A 1S6
nbruin@cecm.sfu.ca
[2] Mathematical Institute, 24–29 St. Giles, University of Oxford
Oxford OX1 3LB, United Kingdom
flynn@maths.ox.ac.uk

Abstract. We discuss the situation where a curve $\mathcal{C}$, defined over a number field K, has a known K-rational divisor class of degree 1, and consider whether this class contains an actual K-rational divisor. When $\mathcal{C}$ has points everywhere locally, the local to global principle of the Brauer group gives the existence of such a divisor. In this situation, we give an alternative, more down to earth, approach, which indicates how to compute this divisor in certain situations. We also discuss examples where $\mathcal{C}$ does not have points everywhere locally, and where no such K-rational divisor is contained in the K-rational divisor class.

1 Introduction

The following result is typically proved as a direct consequence of the local to global principle of the Brauer group (see, for example, [2] or p.30 of [3]).

Lemma 1 *Let $\mathcal{C}$ be a curve defined over a number field K with points everywhere locally. Then any K-rational degree* 1 *divisor class $\mathcal{D}$ contains a K-rational divisor D.*

Such divisor classes have relevance to the application of second descents [4], as well as the application of the Brauer-Manin obstruction to higher genus curves, where such a class $\mathcal{D}$ is used to obtain an embedding $P \mapsto [P] - \mathcal{D}$ from $\mathcal{C}(K)$ to $J(K)$, the Mordell-Weil group of the Jacobian. This embedding can sometimes be used to find information about $\mathcal{C}(K)$.

Our intention here is to describe, in a concise and explicit manner, how the problem of finding a rational divisor in a rational divisor class corresponds to finding a rational point on a certain algebraic variety. We give an example of how this description can be used in practice to find a rational divisor explicitly, given a rational divisor class.

⋆ Partially supported by an NSERC grant.
⋆⋆ Supported by EPSRC grant GR/R82975/01.

2 The Brauer-Severi variety of a divisor class

Let $\mathcal{C}$ be a curve defined over a field K and let $\overline{K}$ be a separable closure of K. We say a divisor class $\mathcal{D} \in \mathrm{Pic}_{\mathcal{C}}(\overline{K})$ is *rational* if it is fixed under the action of $\mathrm{Gal}(\overline{K}/K)$. This means that for any divisor $D \in \mathcal{D}$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$, we have that ${}^{\sigma}D$ and D are linearly equivalent. In the language of Galois modules and Galois cohomology, we have

$$\mathrm{Pic}_{\mathcal{C}}(\overline{K})^K = H^0(K, \mathrm{Pic}_{\mathcal{C}}(\overline{K})) = \{\mathcal{D} \in \mathrm{Pic}_{\mathcal{C}}(\overline{K}) : \mathcal{D} \text{ is a rational divisor class}\}.$$

This group is different from $\mathrm{Pic}_{\mathcal{C}}(K)$, which simply consists of the linear equivalence classes in $\mathrm{Div}_{\mathcal{C}}(K)$. There is an obvious embedding $\mathrm{Pic}_{\mathcal{C}}(K) \subset \mathrm{Pic}_{\mathcal{C}}(\overline{K})^K$ and we identify $\mathrm{Pic}_{\mathcal{C}}(K)$ with its image.

For $D \in \mathrm{Div}_{\mathcal{C}}(\overline{K})$, we adopt the standard notation

$$\mathcal{L}(D) = \{f \in \overline{K}(\mathcal{C}) : (f) \geq -D\}. \tag{1}$$

This is a finite dimensional vector space over $\overline{K}$. We write $l(D)$ for its dimension. The Riemann-Roch theorem asserts that, for any divisor $D \in \mathrm{Div}_{\mathcal{C}}(\overline{K})$ and any canonical divisor κ of $\mathcal{C}$, we have $l(D) - l(\kappa - D) = \deg D - g + 1$. Furthermore $l(D)$ only depends on the equivalence class of D and we write $l([D]) = l(D)$.

We write

$$\mathcal{V}_D(\overline{K}) = \mathbb{P}\mathcal{L}(D) \tag{2}$$

for the complete linear system of D. Via the map $f \mapsto (f) + D$, we see that this set is in bijection with the set of effective divisors linearly equivalent to D:

$$\mathcal{V}_D(\overline{K}) \simeq \mathcal{V}_{[D]}(\overline{K}) := \{D' \in \mathrm{Div}_{\mathcal{C}}(\overline{K}) : D' \geq 0 \text{ and } D' \sim D\}. \tag{3}$$

Let $\mathcal{D}$ be a rational divisor class with $l(\mathcal{D}) > 0$. Then $\mathcal{V}_{\mathcal{D}}(\overline{K})$ is fixed under $\mathrm{Gal}(\overline{K}/K)$ and has the structure of a Galois set. Generalizing the above notation, for an extension L of K, we write $\mathcal{V}_{\mathcal{D}}(L)$ for the effective divisors of $\mathcal{C}$ defined over L and in $\mathcal{D}$.

The functor $\mathcal{V}_{\mathcal{D}}$ is represented by a scheme over K, which is called the *Brauer-Severi variety* associated to $\mathcal{D}$.

It follows that the following are equivalent.

- $\mathcal{V}_{\mathcal{D}}(K) \neq \emptyset$
- $\mathcal{V}_{\mathcal{D}}(K) \simeq \mathbb{P}^{(l(\mathcal{D})-1)}(K)$.
- $\mathcal{D}$ contains a rational divisor.

In some cases it is easy to see that the conditions above hold. For instance, if $\mathcal{D}$ is a rational divisor class with $l(\mathcal{D}) = 1$, then over $\overline{K}$, there is a unique effective divisor D representing $\mathcal{D}$. Consequently, D is fixed under $\mathrm{Gal}(\overline{K}/K)$ and therefore is itself rational.

If a curve has a rational point P_0 then the property above is sufficient to deduce that any rational divisor class contains rational divisors. We use that for any divisor D and point P the following inequalities hold:

$$l(D) \leq l(D + P) \leq l(D) + 1. \tag{4}$$

It follows from (4) that for any divisor class $\mathcal{D}$ there exists an integer n such that $l(\mathcal{D}+[nP_0])=1$. The argument above shows that the rational divisor class $\mathcal{D}+[nP_0]$ contains a rational divisor D and therefore $D-nP_0\in\mathcal{D}$.

In particular, if a curve $\mathcal{C}$ over a number field K has points everywhere locally and $l(\mathcal{D})>0$ then $\mathcal{V}_{\mathcal{D}}$ has rational points everywhere locally. Hence, Lemma 1 is equivalent to the assertion that the local-to-global principle applies to the Brauer-Severi varieties $\mathcal{V}_{\mathcal{D}}$. For $l(\mathcal{D})=2$, we have that $\mathcal{V}_{\mathcal{D}}$ is a curve of genus 0, and the Hasse-Minkowski theorem confirms that such varieties obey a local-to-global principle.

In fact, without assuming local solvability of $\mathcal{C}$, the geometry of $\mathcal{V}_{\mathcal{D}}$ still allows deductions to be made about representability of divisor classes by rational divisors. For instance, any $\mathcal{D}$ with $l(\mathcal{D})=2$ is representable by a divisor over a quadratic extension of K, since any curve of genus 0 has quadratic points.

We now sketch how one can proceed, given a rational divisor class $\mathcal{D}$, to derive an explicit model of $\mathcal{V}_{\mathcal{D}}$ in such a way that finding a rational point on it allows the construction of a representing rational divisor. Suppose that $\mathcal{D}$ is represented by a divisor D over some finite extension $L=K(\alpha)$ of K of degree, say, d.

1. Determine a basis $f_1,\dots,f_{l(D)}\in L(\mathcal{C})$ of $\mathcal{L}(D)$.
2. Over L, we have $\mathcal{V}_{\mathcal{D}}\simeq\mathbb{P}^{l(D)-1}$ via the inverse of the map

$$(t_1:\cdots:t_{l(D)})\mapsto D+(t_1f_1+\cdots+t_{l(D)}f_{l(D)}).$$

   This establishes a model of $\mathcal{V}_{\mathcal{D}}$ over L, with $(t_1:\ldots:t_{l(D)})$ as projective coordinates. Putting $t_1=1$ yields an affine chart $(t_2,\dots,t_{l(D)})$ of $\mathcal{V}_{\mathcal{D}}$ over L.
3. In order to descend our model of $\mathcal{V}_{\mathcal{D}}$ over L to a model over K, we compute a representation of $D_t=D+(f_1+t_2f_2+\cdots t_{l(D)}f_{l(D)})\in\mathrm{Div}_{\mathcal{C}}(L(t_2,\dots,t_{l(D)}))$ corresponding to the generic point $(1:t_2:\ldots:t_{l(D)})$ on $\mathcal{V}_{\mathcal{D}}$ as a scheme over L.
   Let $\mathcal{C}$ be given as a plane curve with coordinates X and Y in general position over K. The effective divisor D_t can be described by the equations $g(X)=0, Y=h(X)$, with $g,h\in L(t_2,\dots,t_{l(D)})[X]$, with g monic, $\deg(g)=\deg(D)$ and $\deg(h)=\deg(D)-1$, since we have taken X and Y such that degeneracies do not occur.
4. We substitute $t_i=\sum_{j=0}^{d-1}t_{i,j}\alpha^j$ and write

$$g(X)=\sum_{k=0}^{d-1}g_k(X)\alpha^j,\ \text{where } g_k(X)\in K(\{t_{i,j}\}_{i,j})[X],$$

   and similarly for $h(X)$. A point $(1:t_1:\cdots:t_{l(D)})$ corresponds to a divisor over K precisely when that divisor can be described by equations not involving α. Thus, we are led to consider the equations obtained by insisting that $g_k(X)=h_k(X)=0$ for $k=1,\dots,d-1$ as polynomials in X. Those equations define an affine chart of $\mathcal{V}_{\mathcal{D}}$ over K, with coordinates $t_{i,j}$ over K. To get a model of $\mathcal{V}_{\mathcal{D}}$, one can take the projective closure.

5. If one finds a point $(t_{i,j})$, one can reconstruct g, h from these values and obtain a description of a K-rational divisor in $\mathcal{D}$. Equivalently, one can reconstruct $(1 : t_2 : \cdots : t_{l(D)})$ and thus obtain a K-rational specialization of D_t.

Of course, the procedure described above only applies to divisor classes satisfying $l(\mathcal{D}) > 0$. In general, one should select some divisor D_0 over K, preferrably of minimal positive degree, and an integer n such that $l(\mathcal{D} + [nD_0])$ is minimally positive. One can then apply the procedure to that divisor class and derive a suitable representative of $\mathcal{D}$ from the result, or conclude that none exists.

3 Finding a rational divisor on a curve of genus 2

We will give an example of this for a genus 2 curve

$$\mathcal{C} : Y^2 = f_6X^6 + f_5X^5 + \cdots + f_0 = F(X), \text{ with } F(X) \in K[X] \tag{5}$$

and a rational divisor class $\mathcal{B}$ of degree 3, represented by an effective divisor defined over a quadratic extension of K.

We assume that $\mathcal{B}$ is a rational divisor class with $\mathcal{B} = [P_1 + P_2 + P_3]$ and $P_1, P_2, P_3 \in \mathcal{C}(K(\sqrt{d}))$, where the P_i are not all Weierstrass points. It follows that $l(\mathcal{B}) = 2$. We can arrive at an equation for $\mathcal{V}_\mathcal{B}$ in the by following the outline in Section 2. We will give an account that can be read independently, but point out the correspondences with the general algorithm.

Let $G_t(x) \in K(\sqrt{d})[t][x]$ be the cubic in x such that $y = G_t(x)$ passes through the points P_1, P_2, P_3 for all values of t. For any value $t \in K(\sqrt{d})$ we have

$$\frac{(x - x_1)(x - x_2)(x - x_3)}{y - G_t(x)} \in \mathcal{L}(\mathcal{B}).$$

This allows us to write down a basis of $\mathcal{L}(\mathcal{B})$ for Step 1 in Section 2. We find $f_1 = 1$, $f_2 = \frac{(x-x_1)(x-x_2)(x-x_3)}{y-G_0(x)}$. We get the coordinates $(1 : t)$ on $\mathcal{L}(\mathcal{B})$.

For any value of t, we have that the identity

$$\{y = G(x)\} \cap \mathcal{C} = P_1 + P_2 + P_3 + (x_1, y_1) + (x_2, y_2) + (x_3, y_3) \simeq 3\mathcal{O}, \tag{6}$$

where $\mathcal{O}$ is any canonical divisor[3] of $\mathcal{C}$. The divisor $(x_1, y_1)+(x_2, y_2)+(x_3, y_3)$ can be described by $\{C_t(x) = 0, y = H_t(x)\}$, where $C_t(x), H_t(x) \in K(\sqrt{d})[t][x]$ are a monic cubic and a quadratic in x respectively. This is the required description for Step 3 of Section 2.

Substituting $t = t_1 + \sqrt{d}\, t_2$, we get that the coefficients c_i of $C_{t_1+\sqrt{d}\, t_2}$ are of the form $c_i = c_{i,0}(t_1, t_2) + \sqrt{d}\, c_{i,1}(t_1, t_2)$, with $c_{i,j} \in K[t_1, t_2]$, and similarly for H_t. Setting the $\sqrt{d}$-components to 0 yields 6 equations in t_1, t_2 over K, which

[3] The divisor $\mathcal{O} = \infty^+ + \infty^-$, consisting of the intersection of $\mathcal{C}$ with $X = \infty$, is a popular choice among people computing with curves of genus 2.

describe the genus 0 curve $\mathcal{V}_{\mathcal{B}}$. This corresponds to Step 4 of Section 2, where we put $t_2 = t_{2,1} + \sqrt{d}\, t_{2,2}$.

If $\mathcal{C}$ has points everywhere locally, then Lemma 1 asserts that $\mathcal{V}_{\mathcal{B}}$ has a rational point. Let $C_{t_0}(x), H_{t_0}(x)$ correspond to such a point. Then the divisor class $\mathcal{B}$ is represented by the rational divisor $B = 3\mathcal{O} - \{C_{t_0}(x) = 0, y = H_{t_0}(x)\}$. This corresponds to Step 5 of Section 2.

Of course, since there exists $\mathcal{O}$, which is of degree 2 and defined over K, the above can be applied to the rational divisor class $\mathcal{D} = [P_1 + P_2 + P_3 - \mathcal{O}]$ of degree 1, which is represented by the rational divisor $D = B - \mathcal{O}$.

We illustrate the above ideas with a detailed worked example. We first observe how a K-rational divisor class can arise naturally, in such a way that the contained K-rational divisor is not immediately apparent.

Let $\mathcal{C}$ be the genus 2 curve, defined over $\mathbb{Q}$,

$$\mathcal{C} : Y^2 = F(X) = -X^6 - X^5 - 2X^4 - 2X^3 + X^2 - 2X + 2, \tag{7}$$

which is easily checked to have points in $\mathbb{R}$ and every $\mathbb{Q}_p$. One can perform a 2-descent on the Mordell-Weil group $\mathcal{J}(\mathbb{Q})$ of the Jacobian, as described in [6], using the map

$$\mu : \mathcal{J}(\mathbb{Q}) \to \mathbb{Q}(\theta)^*/\mathbb{Q}^*(\mathbb{Q}(\theta)^*)^2 : [\sum(x_i, y_i)] \mapsto \prod(x_i - \theta), \tag{8}$$

where θ is a root of $F(X)$. One of the steps of the 2-descent on $\mathcal{J}(\mathbb{Q})$ is the computation of the kernel of μ, generated by $2\mathcal{J}(\mathbb{Q})$ and $[P_1 + P_1' - \mathcal{O}]$, where $P_1 = (\frac{1}{2} + \frac{1}{5}\alpha, \frac{7}{40} + \frac{12}{25}\alpha)$ and $\alpha = \sqrt{-55}$, with P_1' denoting the conjugate of P_1 with respect to $\mathbb{Q}(\alpha)/\mathbb{Q}$. Let P_1^- be the hyperelliptic involute of P_1. Then general properties of μ (see [6] or p.55 of [3]) guarantee that $[P_1^- + P_1' - \mathcal{O}] \in 2\mathcal{J}(\mathbb{Q}(\alpha))$, and computing preimages under the multiplication by 2 map on $\mathcal{J}(\mathbb{Q}(\alpha))$, one finds $\mathcal{D}_1 = [(1+\sqrt{-5}, 2\alpha)+(1-\sqrt{-5}, 2\alpha)-\mathcal{O}]$ which satisfies $[P_1^- + P_1' - \mathcal{O}] = 2\mathcal{D}_1$. Clearly $\mathcal{D}_1' = -\mathcal{D}_1$, since conjugation merely negates the y-coordinates. Let

$$\begin{array}{l} P_1 = (\frac{1}{2} + \frac{1}{5}\alpha, \frac{7}{40} + \frac{12}{25}\alpha), P_2 = (1 + \sqrt{-5}, 2\alpha), P_3 = (1 - \sqrt{-5}, 2\alpha), \\ \mathcal{D} = [P_1] + \mathcal{D}_1 = [P_1 + P_2 + P_3 - \mathcal{O}], \text{ where } \alpha = \sqrt{-55}. \end{array} \tag{9}$$

Then

$$\mathcal{D}' = [P_1'] + \mathcal{D}_1' = [P_1'] - \mathcal{D}_1 = [P_1'] - 2\mathcal{D}_1 + \mathcal{D}_1 = [P_1'] - [P_1^- + P_1' - \mathcal{O}] + \mathcal{D}_1 = \mathcal{D},$$

so that $\mathcal{D}$ is defined over $\mathbb{Q}$. We now have a naturally occurring divisor class $\mathcal{D}$ of degree 1, which is defined over $\mathbb{Q}$, but whose naturally occurring representative $P_1 + P_2 + P_3 - \mathcal{O}$ is not itself defined over $\mathbb{Q}$. This is a common outcome of an application of 2-descent on $\mathcal{J}(\mathbb{Q})$ for genus 2 curves. Note that such $\mathcal{D}$ are of some interest, as they allow an embedding of $\mathcal{C}(\mathbb{Q})$ into $\mathcal{J}(\mathbb{Q})$ via the map $P \mapsto [P] - \mathcal{D}$, even when no obvious member of $\mathcal{C}(\mathbb{Q})$ is available.

Since our curve has points everywhere locally, we know that $\mathcal{D}$ does contain an actual $\mathbb{Q}$-rational divisor. We now illustrate how this can be found in practice. One first finds the general $Y = G(X)$, through P_1, P_2, P_3, where $G(X)$ is cubic

in X, and where there is a free parameter t, since we have one less than the number of points required to define the cubic uniquely. This parametrized family of cubics is

$$\begin{aligned} G(X) = tX^3 + (\tfrac{3}{2} - \tfrac{5t}{2} - \tfrac{2\alpha}{5} - \tfrac{t\alpha}{5})X^2 \\ +(-3 + 7t + \tfrac{4\alpha}{5} + \tfrac{2t\alpha}{5})X + 9 - 3t - \tfrac{2\alpha}{5} - \tfrac{6t\alpha}{5}. \end{aligned} \tag{10}$$

Computing $G(X)^2 - F(X)$, where $F(X)$ is as in (7), and removing the cubic factor $(X - X(P_1))(X - X(P_2))(X - X(P_3))$ leaves the residual cubic

$$\begin{aligned} C(X) = 10(1 + t^2)X^3 + (35 + 2\alpha + 30t - 8t\alpha - 25t^2 - 2t^2\alpha)X^2 \\ +(-50 - 4\alpha - 60t + 16t\alpha + 70t^2 + 4t^2\alpha)X \\ +30 + 12\alpha + 180t - 8t\alpha - 30t^2 - 12t^2\alpha. \end{aligned} \tag{11}$$

Let $(x_1, y_1) + (x_2, y_2) + (x_3, y_3) - \mathcal{O} \in \mathcal{D}$. Then x_1, x_2, x_3 are the roots of $C(X)$, for some choice of $t \in \mathbb{Q}(\alpha)$. Furthermore, the $y_i = -G(x_i)$, where $G(X)$ is as in (10). We now compute the quadratic $Y = H(X)$ which passes through $(x_1, -G(x_1)), (x_2, -G(x_2)), (x_3, -G(x_3))$, namely

$$\begin{aligned} H(X) = ((15 - 60t - 15t^2 - 4\alpha - 4t\alpha + 4t^2\alpha)X^2 \\ +(-30 + 120t + 30t^2 + 8\alpha + 8t\alpha - 8t^2\alpha)X \\ +90 - 60t - 90t^2 - 4\alpha - 24t\alpha + 4t^2\alpha)/(10 + 10t^2). \end{aligned} \tag{12}$$

We have now parametrized divisors of the form $(x_1, y_1) + (x_2, y_2) + (x_3, y_3) - \mathcal{O}$ which are in $\mathcal{D}$. Our requirement for $(x_1, y_1) + (x_2, y_2) + (x_3, y_3) - \mathcal{O}$ to be $\mathbb{Q}$-rational is the same as requiring that the ratios of the coefficients of $C(x)$ are $\mathbb{Q}$-rational (giving six polynomials in t, which can be reduced to three polynomials on the assumption that a given cofficient of $C(x)$ is nonzero; however, we shall prefer to write out all six polynomials in full), and that the actual coefficients of $H(x)$ are also $\mathbb{Q}$-rational (giving three polynomials in t). This gives in total nine polynomials in t total that must be $\mathbb{Q}$-rational. Let $t = t_1 + t_2\alpha$. Then on computing the coefficients on α in our nine expressions, we find nine quartics in t_1, t_2, all with a common factor of $t_1^2 + 55t_2^2 + 15t_2 + 1$. Then

$$t_1^2 + 55t_2^2 + 15t_2 + 1 = 0 \tag{13}$$

is our desired curve of genus 0, which has points everywhere locally, and hence globally. The solution of smallest height is $t_1 = 1/7, t_2 = -1/7$, corresponding to $t = 1/7 - \alpha/7$. Substituting this into $C(X)$ and $H(X)$, and removing from $C(X)$ a factor of $-5(5 + 2\alpha)/49$ (permissible, since the roots of $C(X)$ are unaffected), gives

$$C(X) = 2X^3 + X^2 + 2X + 2, \quad H(X) = -\frac{1}{2}X^2 + X - 1. \tag{14}$$

These $C(X), H(X)$ define $(x_1, y_1) + (x_2, y_2) + (x_3, y_3) - \mathcal{O}$, which is our desired $\mathbb{Q}$-rational divisor in our given $\mathbb{Q}$-rational divisor class $\mathcal{D}$. We summarize the above as follows.

Example 1 *Let $\mathcal{C}$ be the curve (7) and $\mathcal{D}$ be the $\mathbb{Q}$-rational divisor class in (9). Then $\mathcal{D}$ contains the $\mathbb{Q}$-rational divisor $(x_1, y_1) + (x_2, y_2) + (x_3, y_3) - \mathcal{O}$, where x_1, x_2, x_3 are the roots of $C(X)$ and $y_i = H(x_i)$ for $i = 1, 2, 3$, with $C(X), H(X)$ as in (14).*

We have written a Maple file at [1] which performs the above computation for any curve of genus 2.

4 Examples where the rational divisor class contains no rational divisor

Suppose now that our genus 2 curve is defined over a number field K and is of the form

$$\begin{array}{l} \mathcal{H} : Y^2 = kF_1(X)F_2(X), \text{ with } F_1(X) = a_3X^3 + a_2X^2 + a_1X + a_0, \\ k \in K^*, \text{ each } a_i = g_i + h_i\sqrt{d} \in K(\sqrt{d}), \text{ and } F_1(X), F_2(X) \text{ conjugate.} \end{array} \tag{15}$$

We shall also assume that $F_1(X)$ is not defined over K. Let e_1, e_2, e_3 denote the roots of $F_1(X)$. This is another situation where we have a naturally occurring degree 1 divisor class $\mathcal{D} = [(e_1, 0)+(e_2, 0)+(e_3, 0)-\mathcal{O}]$ which is defined over K, even though the given representative is defined over $K(\sqrt{d})$ and not generally over K. If $\mathcal{H}$ has points everywhere locally, we know that $\mathcal{D}$ must contain a divisor defined over K, but we do not make that assumption in this section. The parametrized familiy of cubics through $(e_1, 0), (e_2, 0), (e_3, 0)$ is simply $Y = G(X) = tF_1(X)$, where $t = t_1+t_2\sqrt{d}$ and t_1, t_2 are K-rational parameters. Replacing Y by $tF_1(X)$ in $Y^2 - kF_1(X)F_2(X)$ and removing the known factor $F_1(X)$ gives the residual cubic $C(X) = t^2F_1(X) - kF_2(X)$. Let $(x_1, y_1) + (x_2, y_2) + (x_3, y_3) - \mathcal{O} \in \mathcal{D}$. Then x_1, x_2, x_3 are the roots of $C(X)$, for some choice of $t \in K(\sqrt{d})$. Furthermore, each $y_i = -G(x_i)$; we compute the quadratic $Y = H(X)$ passing through the $(x_i, -G(x_i))$, namely

$$\begin{array}{r} H(X) = 2k\ell\big((g_2h_3 - g_3h_2)X^2 + (g_1h_3 - g_3h_1)X + g_0h_3 - g_3h_0\big), \text{ where} \\ \ell = (-k + t_2^2d - t_1^2)(g_3t_2 + h_3t_1)d - (k + t_2^2d - t_1^2)(g_3t_1 + h_3t_2d)\sqrt{d}. \end{array} \tag{16}$$

Now, suppose that $(x_1, y_1) + (x_2, y_2) + (x_3, y_3) - \mathcal{O}$ is defined over K. Then the ratios of coefficients of $C(X)$ must be in K, giving the six equations

$$(k+t_2^2d-t_1^2)(-k+t_2^2d-t_1^2)(g_ih_j - g_jh_i) = 0, \text{ for } \{i, j\} \subset \{0, 1, 2, 3\},\ i < j. \tag{17}$$

Furthermore, the coefficients of $H(X)$ must be in K, giving the three equations

$$(k + t_2^2d - t_1^2)(g_3t_1 + h_3t_2d)(g_ih_3 - g_3h_i) = 0, \text{ for } i = 0, 1, 2. \tag{18}$$

Inspecting (17), we note that we cannot have all $g_ih_j - g_jh_i = 0$, since then our original curve $\mathcal{H}$ would have zero discriminant. So, one of the first two factors in (17) must be 0, giving that $\mathrm{Norm}(t) = \pm k$. If $\mathrm{Norm}(t) = -k$ then a similar argument (we have placed the details in the file [1]) applied to the equations (18)

shows that either $\mathcal{H}$ has zero discriminant (which is not permitted) or that F_1, F_2 are each defined over K (which is also not permitted). In summary, if $\mathcal{D}$ contains a K-rational divisor then we must have $\mathrm{Norm}(t) = k$ for some t.

Conversely, if $\mathrm{Norm}(t) = k$ for some $t \in K(\sqrt{d})$, then the K-rational divisor $(x_1, y_1) + (x_2, y_2) + (x_3, y_3) - \mathcal{O}$ in $\mathcal{D}$ is defined by

$$C_0(X) = tF_1 - t'F_2(X), \quad H_0(X) = -4k^2 d(g_3 t_2 + h_3 t_1) \sum_{i=0}^{2} (g_i h_3 - g_3 h_i) X^i. \quad (19)$$

We summarize this as follows.

Lemma 2 *Let $\mathcal{H} : Y^2 = kF_1(X)F_2(X)$ be a curve of genus 2 of the type (15), defined over a number field K, where $F_1(X)$ is defined over $K(\sqrt{d})$ and not over K. Let $\mathcal{D}$ be the K-rational divisor class $[(e_1, 0) + (e_2, 0) + (e_3, 0) - \mathcal{O}]$, where e_1, e_2, e_3 are the roots of $F_1(X)$. Then $\mathcal{D}$ contains a K-rational divisor if and only if $\mathrm{Norm}(t) = k$ for some $t \in K(\sqrt{d})$, in which case the required divisor is $(x_1, y_1) + (x_2, y_2) + (x_3, y_3) - \mathcal{O}$, where x_1, x_2, x_3 are the roots of $C_0(X)$ and each $y_i = H_0(x_i)$, with C_0, H_0 as in (19).*

In this situation, our genus 0 curve is simply the curve $t_1^2 - dt_2^2 = k$. Of course, any choice of K, d, k (such as $\mathbb{Q}, 2, 5$), where k is not a norm in $K(\sqrt{d})$, will give an example where $\mathcal{D}$ does not contain a K-rational divisor.

References

1. N. Bruin and E.V. Flynn. Maple programs for computing rational divisors in rational divisor classes. Available at www.maths.ox.ac.uk/~flynn/genus2/maple/ratdiv
2. D. Coray and C. Manoil. On large Picard groups and the Hasse principle for curves and K3 surfaces. *Acta. Arith.*, **LXXVI.2** (1996), 165–189.
3. J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* LMS–LNS 230. Cambridge University Press, Cambridge, 1996.
4. J.W.S. Cassels. Second descents for elliptic curves. *J. reine angew. Math.* **494** (1998), 101–127.
5. V. Scharaschkin. Local Global Problems and the Brauer-Manin Obstruction. PhD Thesis, University of Michigan, 1999.
6. M. Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.* **98** (2001), 245–277.