ACTA ARITHMETICA
LXVI.1 (1994)

Descent via isogeny in dimension 2

by

E. V. Flynn (Cambridge)

0. Introduction. The study of curves of genus 2 and their Jacobians is rapidly becoming more constructive in nature. An explicit embedding of the Jacobian variety has been described in $\mathbb{P}^9$ for the case when there is a rational Weierstrass point [10], and in $\mathbb{P}^{15}$ for the general situation [7]. The defining equations have been determined in a manner which preserves the arithmetic information of the original curve, and a number of additional structures concerning the Kummer surface [8], the formal group [7], [10] and the global group law [8] have been made both constructive and computable in practice.

The most glaring gap in the constructive literature is the lack of a viable and widely applicable procedure for determining the rank of the Mordell–Weil group of the Jacobian. The motivation for such a procedure is considerable, as there is a large body of general theory and conjecture which has so far existed in a vacuum. For example, theorems of Chabauty [5] and Coleman [6] (relating the rank of the Jacobian to finding the rational points on the curve) have not so far had an opportunity to be applied (apart from conditional bounds on the number of solutions to the Fermat curves in [11]); the higher dimensional analogues of the conjectures of Birch and Swinnerton-Dyer have not had a chance to be tested; branches of the Mathematics of Computation (such as the search for large rank) have so far been restricted to elliptic curves. Apart from the new classes of Diophantine problems in genus 2 which could be solved, there is also the reasonable chance that a constructive genus 2 theory will serve as a testing ground for developing more general explicit structures for curves of any genus.

The best attempt so far is due to Gordon and Grant [9], which describes a complete 2-descent. This applies to the Jacobian of any curve of the form:

$$Y^2 = (X-a_1)(X-a_2)(X-a_3)(X-a_4)(X-a_5)\,, \qquad a_i \in \mathbb{Z}\,.$$

The author thanks SERC for financial support.

The problem here is that this severe arithmetic restriction on the curve forces up the number of primes of bad reduction: no such curve has < 3 bad primes and only a few have < 4 bad primes. As a consequence, we find that, apart from a tiny handful of examples, the number of homogeneous spaces to be checked becomes large. Only two examples were computed in [9] and significant enhancements will be required before the strategy in [9] can yield more than a few additional ranks.

We overcome this difficulty by developing a technique applicable to curves of the form:

$$(*) \qquad \mathcal{C} : Y^2 = q_1(X)q_2(X)q_3(X)$$

where the $q_i(X)$ are quadratics with coefficients in $\mathbb{Z}$. It is straightforward to compute many curves of this form with only 2 or 3 bad primes (for example the infinite family of curves: $Y^2 = p(X^2+1)(X^2+2)(X^2+2X+2)$ has bad reduction only at 2, 5 and p), and so the technique can be expected to produce substantial rank tables. We illustrate this by deriving ranks of a selection of curves in Section 3, and indicate how many can reasonably be expected in the near future as enhancements are introduced. The technique employed will be descent by 4-isogeny, which is analogous to descent by 2-isogeny on an elliptic curve. An unexpected bonus (which significantly eases the computations) is that the isogenous variety is also the Jacobian of a curve of the same type, given in Section 2; this feature is discussed in [1] in a different context.

In Section 1, we present results which are a well known and elementary part of the classical theory of elliptic curves (descent by 2-isogeny), but in a manner somewhat different from the standard textbook treatment such as that in [4], [12]. Specifically, we use a particular $\mathbb{P}^3$ embedding (relating to the eigenvectors of a translation map) of the elliptic curve which allows the underlying linear algebra to be exploited, simplifying and motivating both the isogeny and the twisting of the curve to obtain the homogeneous spaces. In Section 2 we present the analogous structures on the Jacobian of a curve of genus 2 of the form $(*)$, including a concise description of a group L^ϕ which lies above the Selmer group and assists in computing the rank. Section 3 illustrates the technique with a selection of worked examples for which the rank of the Jacobian is determined. A fringe benefit is that, in the rank 0 case, it is easy to find all $\mathbb{Q}$-rational points on the original curve.

1. Descent via 2-isogeny on elliptic curves.

The results in this section are well known; however, we still suggest that a perusal will assist even the well informed reader, as the presentation of Section 2 will closely imitate the format and style of this section. The purpose of this section is to present a slightly unorthodox development of descent via 2-isogeny on elliptic curves using a $\mathbb{P}^3$ embedding of the curve, which allows some of the underlying linear algebra to be exploited. The presentation will be entirely elementary in spirit; in particular, we bypass any mention of cocycles, cohomology and so on. We also introduce a group L^ϕ which lies above the Selmer group and enhances the computation of the rank. The emphasis will be on formulating structures in a way which is highly amenable to generalisation to higher dimension.

For a general elliptic curve $\mathcal{C} : Y^2 = X^3 + aX^2 + bX + c$ $(a, b, c \in \mathcal{F}$ of characteristic $\neq 2$, discriminant of $\mathcal{C} \neq 0)$, we define $J(\mathcal{C})$ to be the embedding of the curve in $\mathbb{P}^3$ given by $\mathbf{a} = (a_{0..3})$, where a_0, a_1, a_2, a_3 are the functions $1, X, Y, X^2$, respectively (we shall often use $(a_{i..j})$ as a shorthand notation for the column vector with entries $a_i, a_{i+1}, \ldots, a_j$). See [12], p. 27, for a brief discussion of the geometric properties of this embedding. This has the structure of an abelian variety with defining equations given by a pair of quadratic forms: $a_1^2 = a_0 a_3$; $a_2^2 = a_1 a_3 + a a_1^2 + b a_0 a_1 + c a_0^2$, and group law given by a biquadratic map. We now assume that our curve has a rational point of order 2, which can be taken to be at $(0, 0)$. From now on, the curve $\mathcal{C}$ will be taken to have the form

$$\mathcal{C} : Y^2 = X(X^2 + aX + b)\,, \qquad b \neq 0\,,\ a^2 - 4b \neq 0. \tag{1}$$

The key advantage of embedding into $\mathbb{P}^3$ (rather than the usual $\mathbb{P}^2$) is that addition by $(0, 0)$ induces a linear map on the curve. In terms of the coordinate functions, addition by $(0, 0)$ gives $x \mapsto b/x$, $y \mapsto -by/x^2$, which induces the following linear map T on $J(\mathcal{C})$:

$$T = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & b & 0 & 0 \\ 0 & 0 & -b & 0 \\ b^2 & 0 & 0 & 0 \end{pmatrix}.$$

Note that $T^2 = b^2 I_4$, and that T has $\mathcal{F}$-rational eigenvalues: b, $-b$, each occurring with multiplicity 2. We therefore perform a change of basis to new functions: v_0, v_1, v_2, v_3 so that T becomes diagonalised as $b\begin{pmatrix} I_2 & 0 \\ 0 & -I_2 \end{pmatrix}$. The resulting embedding of the curve provides a better foundation for constructing twists and isogenies.

Definition 1.1. Let $\mathcal{C}$ be as in (1). Define $\mathcal{J} = \mathcal{J}(\mathcal{C})$ to be the embedding in $\mathbb{P}^3$ given by $\mathbf{v} = (v_{0..3})$, where v_0, v_1, v_2, v_3 are $X^2 + b$, X, $X^2 - b$, Y, respectively. For any (x, y) on $\mathcal{C}$, we let $\lfloor x, y \rfloor$ denote the corresponding vector $\mathbf{v} \in \mathcal{J}$. The defining equations of $\mathcal{J}$ are

$$A : v_2^2 = v_0^2 - 4b v_1^2\,, \qquad B : v_3^2 = v_0 v_1 + a v_1^2\,. \tag{2}$$

With this embedding, the identity, $\mathcal{O} = \lfloor\infty\rfloor$, the rational point of order 2, $\alpha = \lfloor 0, 0\rfloor$, and the translation-by-α map, $T_\alpha : \mathbf{v} \mapsto \mathbf{v} + \alpha$, have the form

$$\mathcal{O} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \mathbf{j}_2 \\ \mathbf{j}_2 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} = \begin{pmatrix} \mathbf{j}_2 \\ -\mathbf{j}_2 \end{pmatrix},$$

$$(3) \qquad T_\alpha(\mathbf{v}) = \begin{pmatrix} v_0 \\ v_1 \\ -v_2 \\ -v_3 \end{pmatrix} = \begin{pmatrix} v_{0..1} \\ -v_{2..3} \end{pmatrix},$$

where $\mathbf{j}_2 = \binom{1}{0}$. We now discard our original $J(\mathcal{C})$ entirely, and exclusively use $\mathcal{J} = \mathcal{J}(\mathcal{C})$ of Definition 1.1 as the embedding of the curve for any curve of the form (1). An immediate benefit of using $\mathcal{J}$ is that we can instantly write down a spanning set of all quadratics in $\mathbf{v}$ invariant under T_α. Namely, all quadratic monomials $v_i v_j$ where v_i, v_j lie in the dual of the same eigenspace; these are: v_0^2, $v_0 v_1$, v_1^2, v_2^2, $v_2 v_3$ and v_3^2. However, the defining equations (2) give two linear conditions on these monomials so that we may discard v_1^2 and v_3^2. The map τ from $\mathbf{v}$ to the member of $\mathbb{P}^3$ given by the remaining 4 monomials clearly satisfies $\tau(\mathbf{v} + \alpha) = \tau(\mathbf{v})$, and composing τ with a linear adjustment creates a 2-isogeny from $\mathcal{J}(\mathcal{C})$ to $\widehat{\mathcal{J}} = \mathcal{J}(\widehat{\mathcal{C}})$, where $\widehat{\mathcal{C}}$ is described in the following lemma.

Lemma 1.2. *Let M, U, τ, ϕ, $\widehat{\phi}$, $\widehat{\mathcal{C}}$ be as follows*:

$$M = \begin{pmatrix} 2a^2 & 8ab & 2(2b-a^2) & 0 \\ a & 4b & -a & 0 \\ 8b & 8ab & -4b & 0 \\ 0 & 0 & 0 & 4b \end{pmatrix}, \qquad U = \begin{pmatrix} 17 & 0 & -15 & 0 \\ 0 & 8 & 0 & 0 \\ -15 & 0 & 17 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix},$$

$$(4) \qquad \tau : \begin{pmatrix} v_{0..1} \\ v_{2..3} \end{pmatrix} \mapsto \begin{pmatrix} v_0 v_{0..1} \\ v_2 v_{2..3} \end{pmatrix}, \qquad \phi = M\tau,$$

$$\widehat{\phi} = U\widehat{M}\tau, \qquad \widehat{\mathcal{C}} : Y^2 = X(X^2 + \widehat{a}X + \widehat{b}),$$

where $\widehat{a} = -2a$ and $\widehat{b} = a^2 - 4b$. Then the following hold:

(i) $\phi : \mathcal{J} \mapsto \widehat{\mathcal{J}}$, $\widehat{\phi} : \widehat{\mathcal{J}} \mapsto \mathcal{J}$ *are* 2*-isogenies.*

(ii) $\ker\phi = \{\mathcal{O}, \alpha\}$, $\ker\widehat{\phi} = \{\widehat{\mathcal{O}}, \widehat{\alpha}\}$.

(iii) $\widehat{\phi} \circ \phi = \phi \circ \widehat{\phi} = [2]$.

(iv) $\phi(\lfloor(-a \pm \sqrt{\widehat{b}})/2, 0\rfloor) = \widehat{\alpha}$, $\widehat{\phi}(\lfloor(-\widehat{a} \pm 4\sqrt{b})/2, 0\rfloor) = \alpha$. ∎

We now assume, for the rest of the section, that $\mathcal{F} = \mathbb{Q}$, so that we may take $a, b \in \mathbb{Z}$. The following two lemmas construct the usual injection from $\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$ into $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

LEMMA 1.3. *Let $\mathbf{w} \in \widehat{\mathcal{J}}(\mathbb{Q})$. Then there exists a unique $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ such that every $\mathbf{v} \in \phi^{-1}(\mathbf{w})$ is defined over $\mathbb{Q}(\sqrt{d})$. When $d \neq 1$ this gives the existence of $\mathbf{v}$ such that*:

(i) $\{\mathbf{v}, \sigma_d(\mathbf{v})\} = \phi^{-1}(\mathbf{w})$,

(ii) $T_\alpha(\mathbf{v}) = \sigma_d(\mathbf{v})$, *where σ_d represents conjugation in $\mathbb{Q}(\sqrt{d})$.*

Proof. Define $\mathbf{r} = M^{-1}\mathbf{w}$, $d = r_2/r_0$. Then

$$\phi^{-1}(\mathbf{w}) = \tau^{-1}(\mathbf{r}) = \begin{pmatrix} r_2 r_{0..1} \\ \pm(r_0 r_{2..3})\sqrt{d} \end{pmatrix}. \ \blacksquare$$

LEMMA 1.4. *Let $\psi : \widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : \mathbf{w} \mapsto d$, where d is as in Lemma* 1.3. *Then ψ is a well defined*, *injective homomorphism*, *and $\widehat{b} = \psi(\widehat{\alpha}) \in \operatorname{im}\psi$.*

Proof. Let φ be the same map, but defined on $\widehat{\mathcal{J}}(\mathbb{Q})$. Let $\mathbf{w}'' = \mathbf{w} + \mathbf{w}'$ on $\widehat{\mathcal{J}}(\mathbb{Q})$, and $\mathbf{v} \in \phi^{-1}(\mathbf{w})$ over $\mathbb{Q}(\sqrt{d})$, $\mathbf{v}' \in \phi^{-1}(\mathbf{w}')$ over $\mathbb{Q}(\sqrt{d'})$. Then $\mathbf{v}'' = \mathbf{v} + \mathbf{v}' \in \phi^{-1}(\mathbf{w}'')$ is over $\mathbb{Q}(\sqrt{d}, \sqrt{d'})$. Under the action $\sqrt{d} \to -\sqrt{d}$, $\sqrt{d'} \to -\sqrt{d'}$, we have $\mathbf{v}'' \to \sigma_d(\mathbf{v}) + \sigma_{d'}(\mathbf{v}') = T_\alpha(\mathbf{v}) + T_\alpha(\mathbf{v}') = \mathbf{v}''$, giving that $\mathbf{v}'' \in \mathbb{Q}(\sqrt{dd'})$. Hence, $\varphi(w'') = dd'$, and so φ is a homomorphism from $\widehat{\mathcal{J}}(\mathbb{Q})$ to $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. Clearly $\ker\varphi = \phi(\mathcal{J}(\mathbb{Q}))$, hence the induced homomorphism ψ on the quotient is injective. $\blacksquare$

It is easy to check that the map ψ is the same as the usual "x-coordinate" map; that is, if $\mathbf{w} = \lfloor \widehat{x}, \widehat{y} \rfloor \in \widehat{\mathcal{J}}(\mathbb{Q})$, where (x, y) lies on $\widehat{\mathcal{C}}$, then $d = \psi(\mathbf{w}) = \widehat{x}$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. The advantage of the above approach to Lemmas 1.3, 1.4 (and Lemma 1.5 to follow) is that it both is elementary and does not require properties special to elliptic curves; these features increase amenability to generalisation to higher dimension. In the same spirit, the finiteness of $\operatorname{im}\psi$ can be demonstrated using only a reduction mod p argument.

LEMMA 1.5. *Let $\mathcal{S} = \{p : p \mid b(a^2 - 4b)\} \cup \{2\} = \{p_1, \ldots, p_r\}$, and $\mathbb{Q}(\mathcal{S}) = \{\pm p_1^{e_1} \ldots p_r^{e_r} : e_i = 0, 1\} \leq \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Then $\operatorname{im}\psi \leq \mathbb{Q}(\mathcal{S})$.*

Proof. Suppose otherwise, that there exist $d \in \operatorname{im}\psi$, $p \notin \mathcal{S}$, such that $p \mid d$. Then there is a $\mathbf{w} \in \widehat{\mathcal{J}}(\mathbb{Q})$ with $\psi(\mathbf{w}) = d$, and so (by the definition of ψ), there is a pair $\mathbf{v}, \sigma_d(\mathbf{v}) \in \mathcal{J}(\mathbb{Q}(\sqrt{d}))$ with $\sigma_d(\mathbf{v}) = \mathbf{v} + \alpha$. Write $\mathbf{v} = (v_{0..3})$ so that $\max_i |v_i|_p = 1$. Since $p \notin \mathcal{S}$, p is a prime of good reduction and we let $\widetilde{\ }$ represent the reduction map from $\mathcal{J}(\mathbb{Q}_p(\sqrt{d}))$ to $\widetilde{\mathcal{J}}(\mathbb{F}_p)$. Since $|\sqrt{d}\,|_p < 1$, $\widetilde{\sigma_d(\mathbf{v})} = (\sigma_d(\widetilde{v}_{0..3})) = (\widetilde{v}_{0..3}) = \widetilde{\mathbf{v}}$. Hence, $\widetilde{\mathbf{v}} = \widetilde{\sigma_d(\mathbf{v})} = \widetilde{\mathbf{v} + \alpha} = \widetilde{\mathbf{v}} + \widetilde{\alpha}$, and so $\widetilde{\alpha} = \widetilde{\mathcal{O}}$, contradicting the fact that p is a prime of good reduction. $\blacksquare$

As usual, the above lemmas immediately give the weak Mordell–Weil theorem.

THEOREM 1.6. *The groups* $\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$, $\mathcal{J}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}))$ *and* $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ *are finite.*

Proof. The finiteness of $\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$ and $\mathcal{J}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}))$ is immediate from Lemmas 1.4, 1.5. The finiteness of $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ follows from the usual exact sequence:

$$0 \to \{\widehat{\mathcal{O}}, \widehat{\alpha}\} \to \widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q})) \xrightarrow{\hat{\phi}} \mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) \to \mathcal{J}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q})) \to 0\,. \ \blacksquare$$

To find $\widehat{\mathcal{J}}/\phi(\mathcal{J}(\mathbb{Q}))$ in practice, we construct, for each $d \in \mathbb{Q}(\mathcal{S})$, a homogeneous space $\mathcal{J}_d/\mathbb{Q}$, isomorphic to $\mathcal{J}$ over $\mathbb{Q}(\sqrt{d})$, which contains a $\mathbb{Q}$-rational point if and only if $d \in \operatorname{im}\psi$. A further advantage of our choice of embedding $\mathcal{J}$ now becomes apparent, as we find that the processes of twisting $\mathcal{J}$ and constructing $\mathcal{J}_d$ are immediate.

DEFINITION 1.7. Let $tw_d : \mathbf{v} \mapsto \mathbf{z}$, where $z_{0..1} = v_{0..1}$, $z_{2..3} = v_{2..3}/\sqrt{d}$. Then tw_d is an isomorphism from $\mathcal{J}$ to the *homogeneous space* $\mathcal{J}_d$, whose defining equations may be obtained simply by substituting $v_0 = z_0, v_1 = z_1, v_2 = \sqrt{d}z_2, v_3 = \sqrt{d}z_3$ into (2):

$$(5) \qquad A_d : dz_2^2 = z_0^2 - 4bz_1^2\,, \qquad B_d : dz_3^2 = z_0z_1 + az_1^2\,.$$

We define: $S_p^\phi = \{d : \mathcal{J}_d(\mathbb{Q}_p) \neq \emptyset\}$, $S^\phi = \bigcap_p S_p^\phi$, with $\bigcap_p$ over all primes including ∞.

THEOREM 1.8. $\operatorname{im}\psi = \{d : \mathcal{J}_d(\mathbb{Q}) \neq \emptyset\}$.

Proof. Let $d \in \operatorname{im}\psi$ so that (by definition) there are $\mathbf{w} \in \widehat{\mathcal{J}}(\mathbb{Q})$, $\mathbf{v} \in \mathcal{J}(\mathbb{Q}(\sqrt{d}))$, with $\mathbf{w} = \phi(\mathbf{v})$ and $\sigma_d(\mathbf{v}) = T_\alpha(\mathbf{v})$. Let $\mathbf{z} = tw_d(\mathbf{v})$. Then

$$\sigma_d(\mathbf{z}) = \begin{pmatrix} \sigma_d(v_{0..1}) \\ \sigma_d(v_{2..3}/\sqrt{d}) \end{pmatrix} = \begin{pmatrix} \sigma_d(v_{0..1}) \\ -\sigma_d(v_{2..3})/\sqrt{d} \end{pmatrix} = \begin{pmatrix} T_\alpha(v_{0..1}) \\ -T_\alpha(v_{2..3})/\sqrt{d} \end{pmatrix} = \mathbf{z}\,.$$

Hence $\mathbf{z} \in \mathcal{J}_d(\mathbb{Q})$, giving $\mathcal{J}_d(\mathbb{Q}) \neq \emptyset$. Conversely, if $\mathbf{z} \in \mathcal{J}_d(\mathbb{Q})$ then taking

$$\mathbf{v} = tw_d^{-1}\mathbf{z}\,, \qquad \mathbf{w} = \phi(\mathbf{v}) = M\begin{pmatrix} z_0z_{0..1} \\ dz_2z_{2..3} \end{pmatrix} \in \widehat{\mathcal{J}}(\mathbb{Q})$$

clearly gives $d \in \operatorname{im}\psi$. $\blacksquare$

By way of comparison, using a $\mathbb{P}^2$ embedding generally involves an ad hoc calculation on $\mathcal{C}$ to compute the inverse of tw_d (for example [12], p. 294), whereas in our case this is immediate. If we wish, we can obtain the affine piece $z_1 = 1$ by substituting $B_d : z_0 = dz_3^2 - a$ into A_d, giving the more common version of $\mathcal{J}_d : dz_2^2 = d^2z_3^4 + \widehat{a}z_3^2 + \widehat{b}$ in affine 2-space; this introduces a singularity at infinity. Our form of $\mathcal{J}_d$ has the advantage that it is nonsingular, so that Hensel's Lemma is more easily applied in calculating S^ϕ. A second advantage is that the first equation A_d defines a projective variety (containing $\mathcal{J}_d$ as a subvariety) which simplifies the resolution of $\mathcal{J}_d$ for some choices of d.

DEFINITION 1.9. $L_p^\phi = \{d \in \mathbb{Q}(\mathcal{S}) : A_d(\mathbb{Q}_p) \neq \emptyset\}$, $L^\phi = \bigcap_p L_p^\phi$.

THEOREM 1.10. *Each A_d satisfies the Hasse principle, so $L^\phi = \{d \in \mathbb{Q}(\mathcal{S}) : A_d(\mathbb{Q}) \neq \emptyset\}$. The set L^ϕ is a group, $S^\phi \leq L^\phi$, and the following are equivalent*:

(i) $d \in L^\phi$.

(ii) *There exists an element*, ϱ, *of norm b in* $\mathbb{Q}(\sqrt{d})$.

(iii) $(b, d)_p = 1$ *for all* $p \in \mathcal{S}$, *where* $(\ ,\ )_p$ *is the norm residue symbol in* $\mathbb{Q}_p$.

(iv) *There exists an element*, ϱ', *of norm d in* $\mathbb{Q}(\sqrt{b})$.

Proof. The equivalence of (i), (ii), (iv) is immediate from the defining equation A_d, and it is well known and elementary that the Hasse principle is satisfied and that (ii)$\Leftrightarrow$(iii). The fact that L^ϕ is a group follows from criterion (iv). ∎

As illustration, consider $\mathcal{C}^p : Y^2 = X^3 + pX$, $\widehat{\mathcal{C}}^p : Y^2 = X^3 - 4pX$, $p \equiv 3$ or $5 \pmod 8$. The bad primes are $\mathcal{S} = \{2, p\}$, and the only members of $\mathbb{Q}(\mathcal{S})$ which can occur as norms in $\mathbb{Q}(\sqrt{p})$ are $L^\phi = \{1, -2, -p, 2p\}$ $(p \equiv 3)$ and $L^\phi = \{1, -1, p, -p\}$ $(p \equiv 5)$, which combined with Lemma 1.2(iv) gives $\{1, -p\} \leq \operatorname{im} \psi \leq L^\phi$, where $|L^\phi| = 4$. Similarly, $\{1, p\} \leq \operatorname{im} \widehat{\phi} \leq L^{\hat{\phi}} = \{1, p\}$, for both of $p \equiv 3, 5$. Hence, the rank of $\mathcal{C}^p$ has been bounded above by one, merely by considering norms in $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{-p})$. If, in addition, we have a point of infinite order (such as $(1, 2)$ when $p = 3$) then the rank has been shown to be 1 without requiring the calculation of a single homogeneous space $\mathcal{J}_d$. Even when we do not have such a point, the initial calculation of L^ϕ and $L^{\hat{\phi}}$ significantly reduces the number of homogeneous spaces $\mathcal{J}_d$ to be checked.

2. Descent via 4-isogeny on the Jacobian of a curve of genus 2.

For a general curve $\mathcal{C} : Y^2 = f_6X^6 + \ldots + f_0$, of genus 2 ($f_i \in \mathcal{F}$ of characteristic $\neq 2, 3, 5$, discriminant of $\mathcal{C} \neq 0$), we let $\mathrm{Pic}^0(\mathcal{C})$ denote the Picard group of $\mathcal{C}$; that is, the group of divisors of $\mathcal{C}$ of degree 0 modulo linear equivalence. It is convenient (following [3]) to represent any element of $\mathrm{Pic}^0(\mathcal{C})$ by an unordered pair of points $\{(x_1, y_1), (x_2, y_2)\}$ on $\mathcal{C}$, where we also allow $+\infty$, $-\infty$ to appear in the unordered pair. This representation is unique except that we must identify all pairs of the form $\{(x, y), (x, -y)\}$ to give the canonical equivalence class, which we denote by $\mathcal{O}$. As a group, the Jacobian may be identified with $\mathrm{Pic}^0(\mathcal{C})$. Let Θ^+, Θ^- be the images of $\mathcal{C}$ in the Jacobian via the embedding $P \mapsto P - (+\infty), P \mapsto P - (-\infty)$, respectively. We may give the Jacobian the structure of a smooth projective variety $\mathcal{J} = \mathcal{J}(\mathcal{C})$ by an embedding $\mathbf{a} = (a_{0..15})$ in $\mathbb{P}^{15}$, where $a_0, \ldots, a_{15}$ are a basis for $\mathcal{L}(2(\Theta^+ + \Theta^-))$. Such a basis is in [7], where $a_0, \ldots, a_{15}$ are given as explicit symmetric functions (10 even and 6 odd) in the points (x_1,y_1), (x_2,y_2). The embedding is defined over $\mathcal{F}$ and so members of the Mordell–Weil group—that is, pairs $\{(x_1,y_1),(x_2,y_2)\}$ where the points are either both defined over $\mathcal{F}$ or are conjugate over $\mathcal{F}$ and quadratic—correspond to points in $J(\mathcal{F})$. The embedding J in $\mathbb{P}^{15}$ is analogous to the embedding $(1,X,Y,X^2)$ for an elliptic curve. The defining equations are 72 quadratic forms in $a_0,\ldots,a_{15}$, and these are listed in [7], Appendix A. We do not reproduce $a_0,\ldots,a_{15}$ here, as we shall soon (as in §1) apply a linear change of basis to replace J with an embedding $\mathcal{J}$ better suited to developing isogenies.

The 16 points over the closure of $\mathcal{F}$ which are 2-torsion are $\mathcal{O}$ together with the 15 divisors in $\mathrm{Pic}^0(\mathcal{C})$ of the form $\{(x_1,0),(x_2,0)\}$, where x_1, x_2 are distinct roots of the sextic $f_6X^6+\ldots+f_0$. Any $\mathcal{F}$-rational quadratic factor of $f_6X^6+\ldots+f_0$ therefore corresponds to a rational point of order 2 in $J(\mathcal{F})$. From now on, the curve $\mathcal{C}$ will be taken to have the form

$$\text{(6)}\quad \mathcal{C}: Y^2 = q_1(X)q_2(X)q_3(X)\,, \qquad \text{where } q_i(X) = f_iX^2+g_iX+h_i\,, \quad f_i,g_i,h_i\in\mathcal{F}\,.$$

We shall require that $\varDelta$, b_{ij}, b_i, and δ_i are non-zero, where

$$b_{ij} = \mathrm{resultant}(q_i(X),q_j(X))\,, \qquad b_i = b_{ij}b_{ik}\,,$$
$$\delta_i = \mathrm{disc}(q_i(X))\,, \qquad \varDelta = \begin{vmatrix} h_1 & g_1 & f_1\\ h_2 & g_2 & f_2\\ h_3 & g_3 & f_3\end{vmatrix}\,.$$

The requirements $b_{ij}\neq 0$, $b_i\neq 0$, $\delta_i\neq 0$ are merely a restatement that the discriminant of $\mathcal{C}$ should be non-zero. The additional requirement $\varDelta\neq 0$ will ensure that the isogeny to be described is non-degenerate. Note that $b_3=b_1b_2$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$; the group $\{1,b_1,b_2,b_3\}$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ will perform an analogous arithmetic role to that of $\{1,b\}$ in Section 1.

Let T_i denote translation by the rational point of order 2 in J corresponding to the quadratic $q_i(X)$, namely

$$\left\{\left(\frac{-g_i+\sqrt{\delta_i}}{2f_i},0\right),\left(\frac{-g_i-\sqrt{\delta_i}}{2f_i},0\right)\right\}.$$

Then T_1,T_2,T_3 are 16×16 matrices over $\mathcal{F}$ (see [8]). The set of affine matrices I, T_1, T_2, T_3, satisfy $T_k=(b_k/b_ib_j)T_iT_j=(1/b_{ij}^2)T_1T_2$, $T_i^2=b_i^2I$, and $T_iT_j=T_jT_i$. The matrix T_i has the $\mathcal{F}$-rational eigenvalues b_i, $-b_i$, each occurring with multiplicity 8. Commutativity implies that we can simultaneously diagonalise, say, T_1 and T_2 (after which $T_3=(b_3/b_1b_2)T_1T_2$ is also diagonalised), so that I, $\frac{1}{b_1}T_1$, $\frac{1}{b_2}T_2$, $\frac{1}{b_3}T_3$ become

$$\begin{pmatrix} I_4 & 0 & 0 & 0 \\ 0 & I_4 & 0 & 0 \\ 0 & 0 & I_4 & 0 \\ 0 & 0 & 0 & I_4 \end{pmatrix}, \quad \begin{pmatrix} I_4 & 0 & 0 & 0 \\ 0 & I_4 & 0 & 0 \\ 0 & 0 & -I_4 & 0 \\ 0 & 0 & 0 & -I_4 \end{pmatrix},$$

$$\begin{pmatrix} I_4 & 0 & 0 & 0 \\ 0 & -I_4 & 0 & 0 \\ 0 & 0 & I_4 & 0 \\ 0 & 0 & 0 & -I_4 \end{pmatrix}, \quad \begin{pmatrix} I_4 & 0 & 0 & 0 \\ 0 & -I_4 & 0 & 0 \\ 0 & 0 & -I_4 & 0 \\ 0 & 0 & 0 & I_4 \end{pmatrix},$$

respectively, where I_4 represents the 4×4 identity. We now replace the basis $(a_{0..15})$ with the new basis $(v_{0..15})$ on which the T_i's have the above diagonal form.

Definition 2.1. Let $\mathcal{C}$ be as in (6). Define $\mathcal{J} = \mathcal{J}(\mathcal{C})$ to be the embedding in $\mathbb{P}^{15}$ given by $\mathbf{v} = (v_{0..15})$, where $v_0, \ldots, v_{15}$ are as in Appendix A. For any divisor $\{(x_1, y_1), (x_2, y_2)\}$ in $\mathrm{Pic}^0(\mathcal{C})$, we let $\lfloor (x_1, y_1), (x_2, y_2) \rfloor$ represent the corresponding vector $\mathbf{v} \in \mathcal{J}$.

A computational tool available here, which was not present in the elliptic curve situation, is the invariance of $\mathcal{C}$ under the action of the permutation group S_3 on the quadratics $q_i(X)$, which induces a natural action on all of the objects described so far, including the coordinate functions $v_0, \ldots, v_{15}$. The induced action may be described completely by observing that it is simply the natural action on the indices of $q_i(X)$, b_{ij}, b_i, δ_i, α_i and T_{α_i}. The action may be extended to $v_{0..15}$ by taking v_0 to be invariant, and identifying $\{1, 2, 3\}$ with $\{v_1, v_2, v_3\}$, $\{v_4, v_8, v_{12}\}$, $\{v_5, v_9, v_{13}\}$, $\{v_6, v_{10}, v_{14}\}$ and $\{v_7, v_{11}, v_{15}\}$. This can be made to be the natural action on the indices by expressing the functions as v_0, v_i, v_{4i}, v_{1+4i}, v_{2+4i}, v_{3+4i}, for $i = 1, 2, 3$. Note also that $\Delta \to -\Delta$ under an odd permutation and is invariant under an even permutation. This action simplifies the handling of the defining equations of $\mathcal{J}$, since the variety is invariant under the action. For example, there is a set of 20 equations in the even functions which perform an analogous role to equation A in (2) of Section 1. We can encode these as 6 equations in i, j, k, each representing the orbit under the action of S_3 on the indices:

$$\begin{aligned}
&A^{(1)} : b_{ij}(v_j^2 - v_{1+4j}^2) = b_{ik}(v_k^2 - v_{1+4k}^2)\,, \\
&A^{(2)} : 4b_i v_i v_{1+4i} = v_{4j} v_{4k} - v_0 v_{4i}\,, \\
&A^{(3)} : 4b_i(v_i^2 + v_{1+4i}^2) = v_0^2 + v_{4i}^2 - v_{4j}^2 - v_{4k}^2\,, \\
&A^{(4)} : 2b_{ij} v_i v_j = v_0 v_k + v_{4k} v_{1+4k}\,, \\
&A^{(5)} : 2b_{ij} v_{1+4i} v_{1+4j} = v_0 v_{1+4k} + v_k v_{4k}\,, \\
&A^{(6)} : 2b_{ij} v_{1+4i} v_j = -v_{4i} v_k - v_{4j} v_{1+4k}\,.
\end{aligned} \tag{7}$$

The number of independent equations in each of the above orbits is: $|A^{(1)}| = 2$, $|A^{(n)}| = 3$, for $n = 2, \ldots, 5$, and $|A^{(6)}| = 6$, giving a total of 20 equations represented.

With this embedding, the identity, $\mathcal{O}$, the rational points of order 2, $\alpha_i = \big\lfloor \big(\frac{-g_i+\sqrt{\delta_i}}{2f_i}, 0\big), \big(\frac{-g_i-\sqrt{\delta_i}}{2f_i}, 0\big) \big\rfloor$, and the translation-by-α_i maps T_{α_i}, for $i = 1, 2, 3$, are given by:

$$
\begin{array}{cccc}
\mathcal{O} & \alpha_1 & \alpha_2 & \alpha_3 \\
\begin{pmatrix} \mathbf{j}_4 \\ \mathbf{j}_4 \\ \mathbf{j}_4 \\ \mathbf{j}_4 \end{pmatrix}, &
\begin{pmatrix} \mathbf{j}_4 \\ \mathbf{j}_4 \\ -\mathbf{j}_4 \\ -\mathbf{j}_4 \end{pmatrix}, &
\begin{pmatrix} \mathbf{j}_4 \\ -\mathbf{j}_4 \\ \mathbf{j}_4 \\ -\mathbf{j}_4 \end{pmatrix}, &
\begin{pmatrix} \mathbf{j}_4 \\ -\mathbf{j}_4 \\ -\mathbf{j}_4 \\ \mathbf{j}_4 \end{pmatrix},
\end{array}
\tag{8}
$$

$$
\begin{array}{ccc}
T_{\alpha_1}(\mathbf{v}) & T_{\alpha_2}(\mathbf{v}) & T_{\alpha_3}(\mathbf{v}) \\
\begin{pmatrix} v_{0..3} \\ v_{4..7} \\ -v_{8..11} \\ -v_{12..15} \end{pmatrix}, &
\begin{pmatrix} v_{0..3} \\ -v_{4..7} \\ v_{8..11} \\ -v_{12..15} \end{pmatrix}, &
\begin{pmatrix} v_{0..3} \\ -v_{4..7} \\ -v_{8..11} \\ v_{12..15} \end{pmatrix},
\end{array}
$$

where $\mathbf{j}_4 = \left(\begin{smallmatrix} 1 \\ 0 \\ 0 \\ 0 \end{smallmatrix}\right)$. We now discard our original $J(\mathcal{C})$ entirely, and exclusively use $\mathcal{J} = \mathcal{J}(\mathcal{C})$ of Definition 2.1 as the projective embedding of the Jacobian for any curve of the form (6). Note that the block of functions $(v_{0..3})$ invariant under $\{I, T_{\alpha_1}, T_{\alpha_2}, T_{\alpha_3}\}$ are all even (and are analogous to the $(v_{0..1})$ of Section 1); the remaining eigenspace blocks $v_{4..7}$, $v_{8..11}$, $v_{12..15}$ each contain 2 even and 2 odd functions.

We now fix one function in (the dual of) each eigenspace: fix v_0, v_4, v_8, v_{12}, say, we can multiply each of these by the 4 functions in its eigenspace to give $v_0v_{0..3}, v_4v_{4..7}, v_8v_{8..11}, v_{12}v_{12..15}$. The map τ from $\mathbf{v}$ to the member of $\mathbb{P}^{15}$ given by these 16 functions clearly satisfies $\tau(\mathbf{v} + \alpha_i) = \tau(\mathbf{v})$, and composing τ with a linear adjustment creates a 4-isogeny from $\mathcal{J}(\mathcal{C})$ to $\widehat{\mathcal{J}} = \mathcal{J}(\widehat{\mathcal{C}})$ where $\widehat{\mathcal{C}}$ is described in the following lemma.

Lemma 2.2. *Let M, $\widehat{M}$, U be as in Appendix* A. *For any two polynomials $p(X)$, $q(X)$, let $[p, q]$ denote $[p'q - pq']$, and let τ, ϕ, $\widehat{\phi}$, $\widehat{q}_i$, $\widehat{\mathcal{C}}$, $\widehat{b}_{ij}$, $\widehat{b}_i$, $\widehat{\delta}_i$ be as follows*:

$$
\begin{gathered}
\tau : \mathbf{v} \mapsto \begin{pmatrix} v_0v_{0..3} \\ v_4v_{4..7} \\ v_8v_{8..11} \\ v_{12}v_{12..15} \end{pmatrix}, \qquad \phi = M\tau\,, \qquad \widehat{\phi} = U\widehat{M}\tau\,, \\
\widehat{q}_1 = [q_2, q_3]\,, \qquad \widehat{q}_2 = [q_3, q_1]\,, \qquad \widehat{q}_3 = [q_1, q_2]\,, \\
\widehat{\mathcal{C}} : \Delta Y^2 = \widehat{q}_1(X)\widehat{q}_2(X)\widehat{q}_3(X)\,, \\
\widehat{b}_{ij} = \mathrm{res}(\widehat{q}_i(X), \widehat{q}_j(X))\,, \qquad \widehat{b}_i = \widehat{b}_{ij}\widehat{b}_{ik}\,, \qquad \widehat{\delta}_i = \mathrm{disc}(\widehat{q}_i(X))\,.
\end{gathered}
\tag{9}
$$

Then $\widehat{\delta}_i = b_{jk}$, $\widehat{b}_{jk} = \delta_i$ *in* $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, *and the following hold*:

(i) $\phi : \mathcal{J} \mapsto \widehat{\mathcal{J}}$, $\widehat{\phi} : \widehat{\mathcal{J}} \mapsto \mathcal{J}$ *are* 4*-isogenies.*

(ii) $\ker\phi = \{\mathcal{O}, \alpha_1, \alpha_2, \alpha_3\}$, $\ker\widehat{\phi} = \{\widehat{\mathcal{O}}, \widehat{\alpha}_1, \widehat{\alpha}_2, \widehat{\alpha}_3\}$.

(iii) $\widehat{\phi} \circ \phi = \phi \circ \widehat{\phi} = [2]$.

(iv) $$\phi\Big(\Big[\Big(\frac{-g_j \pm \sqrt{\delta_j}}{2f_j}, 0\Big), \Big(\frac{-g_k \pm \sqrt{\delta_k}}{2f_k}, 0\Big)\Big]\Big) = \widehat{\alpha}_i\,,$$

$$\widehat{\phi}\Big(\Big[\Big(\frac{-\widehat{g}_j \pm \sqrt{\widehat{\delta}_j}}{2\widehat{f}_j}, 0\Big), \Big(\frac{-\widehat{g}_k \pm \sqrt{\widehat{\delta}_k}}{2\widehat{f}_k}, 0\Big)\Big]\Big) = \alpha_i\,. \ \blacksquare$$

The original conditions: $b_{ij} \neq 0$, $\delta_i \neq 0$, $\mathrm{char}(\mathcal{F}) \neq 2$ guarantee that all of the above matrices mentioned so far have non-zero determinant, and so are well defined maps on $\mathbb{P}^{15}$. The isogeny from $\mathcal{J}$ to $\widehat{\mathcal{J}}$, computed in this case by algebraic experimentation, turned out to be the same as an isogeny of Richelot, recently publicised [1] by Bost and Mestre in a different context. We now assume, for the rest of the section, that $\mathcal{F} = \mathbb{Q}$, so that we may take $f_i, g_i, h_i \in \mathbb{Z}$ (and so $b_{ij}, b_i, \delta_i \in \mathbb{Z}$). The following two lemmas construct an injection, analogous to that in Section 1, from $\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$ into $(\mathbb{Q}^*/(\mathbb{Q}^*)^2)^2$, where $(\mathbb{Q}^*/(\mathbb{Q}^*)^2)^2$ represents the product with itself of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

LEMMA 2.3. *Let* $\mathbf{w} \in \widehat{\mathcal{J}}(\mathbb{Q})$. *Then there exists a unique pair* $(d_1, d_2) \in (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^2$ *such that for every* $\mathbf{v} \in \phi^{-1}(\mathbf{w})$, *the sets* $\{\mathbf{v}\}$, $\{\mathbf{v}, T_{\alpha_i}(\mathbf{v})\}$, $\{\mathbf{v}, T_{\alpha_1}(\mathbf{v}), T_{\alpha_2}(\mathbf{v}), T_{\alpha_3}(\mathbf{v})\}$ *are defined over* $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, $\mathbb{Q}(\sqrt{d_i})$, $\mathbb{Q}$, *respectively* ($i = 1, 2, 3$, $d_3 = d_1 d_2$). *When* $d_1 \neq 1$, $d_2 \neq 1$, $d_3 \neq 1$, *this gives that*:

(i) $\{\mathbf{v}, \sigma_{d_1}(\mathbf{v}), \sigma_{d_2}(\mathbf{v}), \sigma_{d_3}(\mathbf{v})\} = \phi^{-1}(\mathbf{w})$,

(ii) $T_{\alpha_i}(\mathbf{v}) = \sigma_{d_i}(\mathbf{v})$, $i = 1, 2, 3$,

where σ_{d_i} *represents conjugation in* $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ *over* $\mathbb{Q}(\sqrt{d_i})$.

Proof. Let $\mathbf{r} = M^{-1}\mathbf{w}$, as in the proof of Lemma 1.3, taking $d_1 = v_4/v_0$, $d_2 = v_8/v_0$. $\blacksquare$

The explicit derivation of (d_1, d_2) is computationally useful, since there is not a simple function on $\widehat{\mathcal{C}}$ which performs the function of the x-coordinate on elliptic curves.

LEMMA 2.4. *Let* $\psi : \widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q})) \mapsto (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^2 : \mathbf{w} \mapsto (d_1, d_2)$, *where the ordered pair* (d_1, d_2) *is as in Lemma* 2.2. *Then* ψ *is a well defined injective homomorphism*, *and* $(\widehat{b}_{12}\widehat{b}_{13}, \widehat{b}_{12})$, $(\widehat{b}_{12}, \widehat{b}_{12}\widehat{b}_{23})$, $(\widehat{b}_{13}, \widehat{b}_{23}) \in \mathrm{im}\,\psi$.

Proof. Identical in nature to that of Lemma 1.4. The given points in $\mathrm{im}\,\psi$ are (using Lemma 2.2) the images of $\widehat{\alpha}_1$, $\widehat{\alpha}_2$, $\widehat{\alpha}_3$, respectively. $\blacksquare$

LEMMA 2.5. *Let* $\mathcal{S} = \{p : p \,|\, \Delta b_1 b_2 b_3 \delta_1 \delta_2 \delta_3\} \cup \{2\} = \{p_1 \ldots p_r\}$, *and* $\mathbb{Q}(\mathcal{S}) = \{\pm p_1^{e_1} \ldots p_r^{e_r}\} \le \mathbb{Q}^*/(\mathbb{Q}^*)^2$. *Then* $\operatorname{im}\psi \le (\mathbb{Q}(\mathcal{S}))^2$.

Proof. Suppose otherwise, that there exists $(d_1, d_2) \in \operatorname{im}\psi$, $p \notin \mathcal{S}$ such that p divides either d_1 or d_2: $p \,|\, d_1$, say. Now apply the reduction argument in the proof of Lemma 1.5 to give the contradiction that $\widehat{\alpha}_1 = \widehat{\mathcal{O}}$. ■

The same exact sequence as in Section 1 justifies deducing the weak Mordell–Weil theorem from the above lemmas.

THEOREM 2.6. *The groups* $\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$, $\mathcal{J}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}))$ *and* $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ *are finite.* ■

As in Section 1, our choice of embedding $\mathcal{J}$ eases the construction of the homogeneous spaces $\mathcal{J}_{d_1,d_2}$.

DEFINITION 2.7. Let $(d_1, d_2) \in (\mathbb{Q}(\mathcal{S}))^2$, and take $d_3 = d_1 d_2$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. We adopt the convention that d_1, d_2, d_3 are represented by square free integers. Further, define $d_{ij} = \gcd(d_i, d_j)$, also represented uniquely by square free integers. Note that the d_{ij} are pairwise coprime, and that $d_i = d_{ij} d_{ik}$. Let $tw_{d_1,d_2} : \mathbf{v} \mapsto \mathbf{z}$, where $z_{0..3} = v_{0..3}$, $z_{4..7} = v_{4..7}/\sqrt{d_1}$, $z_{8..11} = v_{8..11}/\sqrt{d_2}$, $z_{12..15} = v_{12..15}/\sqrt{d_3}$ ($d_3 = d_1 d_2$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$). Then tw_{d_1,d_2} is an isomorphism from $\mathcal{J}$ to the *homogeneous space* $\mathcal{J}_{d_1,d_2}$, whose defining equations are obtained simply by substituting $v_{0..3} = z_{0..3}$, $v_{4..7} = z_{4..7}\sqrt{d_1}$, $v_{8..11} = z_{8..11}\sqrt{d_2}$, $v_{12..15} = z_{12..15}\sqrt{d_3}$ into the defining equations of $\mathcal{J}$. The permutation group action can be extended to the indices of d_i, d_{ij}, so that the twists of the equations A in (7) become

$$\begin{aligned}
&A^{(1)}_{d_1,d_2} : b_{ij}(z_j^2 - d_j z_{1+4j}^2) = b_{ik}(z_k^2 - d_k z_{1+4k}^2)\,,\\
&A^{(2)}_{d_1,d_2} : 4b_i z_i z_{1+4i} = d_{jk} z_{4j} z_{4k} - z_0 z_{4i}\,,\\
&A^{(3)}_{d_1,d_2} : 4b_i(z_i^2 + d_i z_{1+4i}^2) = z_0^2 + d_i z_{4i}^2 - d_j z_{4j}^2 - d_k z_{4k}^2\,,\\
&A^{(4)}_{d_1,d_2} : 2b_{ij} z_i z_j = z_0 z_k + d_k z_{4k} z_{1+4k}\,,\\
&A^{(5)}_{d_1,d_2} : 2b_{ij} d_{ij} z_{1+4i} z_{1+4j} = z_0 z_{1+4k} + z_k z_{4k}\,,\\
&A^{(6)}_{d_1,d_2} : 2b_{ij} z_{1+4i} z_j = -z_{4i} z_k - d_{jk} z_{4j} z_{1+4k}\,.
\end{aligned}\tag{10}$$

The complete set of defining equations of $\mathcal{J}_{d_1,d_2}$ are given in Appendix A. We further define

$$S_p^{\phi} = \{(d_1, d_2) : \mathcal{J}_{d_1,d_2}(\mathbb{Q}_p) \ne \emptyset\}\,, \qquad S^{\phi} = \bigcap_p S_p^{\phi}\,,$$

with $\bigcap_p$ over all primes including ∞.

THEOREM 2.8. $\operatorname{im}\psi = \{(d_1, d_2) : \mathcal{J}_{d_1,d_2}(\mathbb{Q}) \ne \emptyset\}$.

Proof. Let $(d_1, d_2) \in \operatorname{im}\psi$ so that (by definition) there are $\mathbf{w} \in \widehat{\mathcal{J}}(\mathbb{Q})$, $\mathbf{v} \in \mathcal{J}(\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}))$, with $\mathbf{w} = \phi(\mathbf{v})$ and $\sigma_{d_i}(\mathbf{v}) = T_{\alpha_i}(\mathbf{v})$. Let $\mathbf{z} = tw_{d_1,d_2}(\mathbf{w})$. Then, as in the proof of Theorem 1.8, it is clear that $\sigma_i(\mathbf{z}) = \mathbf{z}$, so that $\mathcal{J}_{d_1,d_2}(\mathbb{Q}) \neq \emptyset$. Conversely, given $\mathbf{z} \in \mathcal{J}_{d_1,d_2}(\mathbb{Q})$, then taking $\mathbf{v} = tw^{-1}_{d_1,d_2}(\mathbf{z})$, $\mathbf{w} = \phi(\mathbf{v}) \in \widehat{\mathcal{J}}(\mathbb{Q})$ clearly gives $(d_1, d_2) \in \operatorname{im}\psi$. ■

As in Section 1, we find that the equations $A_{d_1,d_2} = \{A^{(n)}_{d_1,d_2} : n = 1, \ldots, 6\}$ define a projective variety (of dimension 3, containing $\mathcal{J}_{d_1,d_2}$ as a subvariety) which simplifies finding $\mathcal{J}_{d_1,d_2}(\mathbb{Q})$ for some choices of (d_1, d_2).

Definition 2.9. $L^\phi_p = \{d \in \mathbb{Q}(\mathcal{S}) : A_{d_1,d_2}(\mathbb{Q}_p) \neq \emptyset\}$, $L^\phi = \bigcap_p L^\phi_p$.

The group L^ϕ can be interpreted in terms of a pair of norm equations, which satisfy similar properties to the corresponding object in Section 1. In the following theorem, the properties of the norm equations (that is, (ii)⇔(iii)⇔(iv)) are due to J. W. S. Cassels. The symmetry of the norm form equations (that is: (ii)⇔(iv)) holds true not only for $\mathbb{Q}$, but for any field of characteristic $\neq 2$, and a proof of this fact is included as Appendix B. I am also grateful to B. J. Birch for helpful insight to the group L^ϕ (in a different context).

Theorem 2.10. *Each A_{d_1,d_2} satisfies the Hasse principle, so that $L^\phi = \{(d_1, d_2) \in (\mathbb{Q}(\mathcal{S}))^2 : A_{d_1,d_2}(\mathbb{Q}) \neq \emptyset\}$. The set L^ϕ is a group, $S^\phi \leq L^\phi$, and following are equivalent:*

(i) $(d_1, d_2) \in L^\phi$.

(ii) *There exist elements, $\varrho_i \in \mathbb{Q}(\sqrt{d_i})$ $(i = 1, 2, 3)$, such that:*

$$b_1 = N_2(\varrho_2)N_3(\varrho_3) \quad \text{and} \quad b_2 = N_1(\varrho_1)N_3(\varrho_3)\,.$$

(iii) $(b_1, d_2)_p(b_2, d_1)_p = 1$, *for all $p \in \mathbb{Q}(\mathcal{S})$.*

(iv) *There exist elements, $\varrho'_i \in \mathbb{Q}(\sqrt{b_i})$ $(i = 1, 2, 3)$, such that:*

$$d_1 = N_2(\varrho'_2)N_3(\varrho'_3) \quad \text{and} \quad d_2 = N_1(\varrho'_1)N_3(\varrho'_3)$$

where N_i represents $\operatorname{Norm}_{\mathbb{Q}(\sqrt{d_i})/\mathbb{Q}}$, *and $(\ ,\ )_p$ represents the norm residue symbol in $\mathbb{Q}_p$.*

Proof. We show the equivalence (ii)⇔(iii) ((iii)⇔(iv) follows by symmetry), then (i)⇔(ii).

(ii)⇒(iii). Let $r = N_1(\varrho_1)N_2(\varrho_2)N_3(\varrho_3)$. Then $N_i(\varrho_i)b_i = r$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ for $i = 1, 2, 3$, and so $(b_i, d_i) = (r, d_i)$, giving $(b_i, d_i)_p = (r, d_i)_p$ for any p. Hence,

$$\begin{aligned}(b_1, d_1)_p(b_2, d_2)_p &= (r, d_1)_p(r, d_2)_p = (r, d_3)_p = (b_3, d_3)_p \\ &= (b_1b_2, d_1d_2)_p = (b_1, d_1)_p(b_1, d_2)_p(b_2, d_1)_p(b_2, d_2)_p\,,\end{aligned}$$

giving $(b_1, d_2)_p(b_2, d_1)_p = 1$, as required.

(iii)⇒(ii). Let $p \in \mathcal{S}$. From (iii), $(b_1, d_2)_p = (b_2, d_1)_p = 1$ or -1. In the former case, define $r_p = b_3$; in the latter case, define $r_p = 1, b_2, b_1, b_1$, when $[(b_1, d_1)_p, (b_2, d_2)_p] = [1,1], [-1,1], [1,-1], [-1,-1]$, respectively. In all cases, $(r_p, d_i)_p = (b_i, d_i)_p$ for $i = 1,2,3$. By a standard global approximation, there exists $r \in \mathbb{Q}$ such that $(r, d_i)_p = (b_i, d_i)_p$, $i = 1,2,3$, for all primes p such that $p \,|\, r$ or $p \in \mathcal{S}$. Hence $(b_i/r, d_i)_p = 1$ for all such primes, and so b_i/r is globally a norm of an element $\varrho_i \in \mathbb{Q}(\sqrt{d_i})$. Clearly, ϱ_1, ϱ_2, $r\varrho_3$ satisfy the requirements of (ii).

(iii)⇔(iv). Symmetrical to (iii)⇔(ii).

(i)⇒(ii). Assume for simplicity that each $d_i \neq 1$. Let p be any prime, and by (i) let $z_0, \ldots, z_5, z_8, z_9, z_{12}, z_{13}$, not all 0, be a $\mathbb{Q}_p$-rational solution to the equations A_{d_1,d_2}. Then $z_i \neq 0$ or $z_{1+4i} \neq 0$ for $i = 1,2,3$, since otherwise the equations $A^{(1)}_{d_1,d_2}$, $A^{(3)}_{d_1,d_2}$ would force $\mathbf{z} = \mathbf{0}$. Now, equation $A^{(1)}_{d_1,d_2}$ gives the two equations:

$$b_{12}(z_2^2 - d_2 z_9^2) = b_{13}(z_3^2 - d_3 z_{13}^2)\,,$$
$$b_{12}(z_1^2 - d_1 z_5^2) = b_{23}(z_3^2 - d_3 z_{13}^2)\,.$$

Clearly, $\varrho_1 = z_1 + z_5\sqrt{d_1}$, $\varrho_2 = z_2 + z_9\sqrt{d_2}$, $\varrho_3 = b_{12}/(z_3 + z_{13}\sqrt{d_3})$ satisfy the requirements of (ii) with $\mathbb{Q}$ replaced be $\mathbb{Q}_p$, for any prime p. However, we have already seen from (ii)⇔(iii) above that the equations in (ii) satisfy the Hasse principle; therefore we can deduce (ii) globally, as required. It is straightforward to adjust the argument for the case when some $d_i = 1$.

(ii)⇒(i). Let ϱ_i satisfy (ii). Then there are rational z_i, z_{1+4i} such that $\varrho_i = z_i + \sqrt{d_i} z_{1+4i}$, $i = 1,2,3$. Further, $2\bar{\varrho}_1\bar{\varrho}_2\varrho_3 \in \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, so there are rational z_0, z_4, z_8, z_{12} such that $2\bar{\varrho}_1\bar{\varrho}_2\varrho_3 = z_0 + \sqrt{d_1}z_4 + \sqrt{d_2}z_8 + \sqrt{d_3}z_{12}$. It is straightforward to verify that the z_i satisfy the equations $A^{(1)}_{d_1,d_2}, \ldots, A^{(6)}_{d_1,d_2}$.

The fact that L^ϕ is a group immediately follows from criterion (iv) and the multiplicative property of norms (this would not have been at all obvious from criterion (ii)). ■

As with elliptic curves, the group L^ϕ is a useful computational device. It is quick to compute and, once computed, there are a smaller number of cosets to be checked when determining the Selmer group. We shall illustrate this (and the rest of the above theory) in the next section.

3. Worked examples. We illustrate the theory of Section 2 by computing the ranks of a selection of 12 Jacobians. For simplicity, we shall represent a member of $\mathcal{J}(\mathcal{C})$ as an unordered pair $\{(x_1, y_1), (x_2, y_2)\}$ of points on $\mathcal{C}$ (as described at the beginning of Section 2) and not as a member of $\mathbb{P}^{15}$. We have tried to choose a varied selection, indicating how the computations are affected by such things as the existence of additional torsion points, and the multiplication of the sextic by a non-square constant. In the various Boolean groups which occur, we shall use the notation $\langle g_1, \ldots, g_k\rangle$ to represent the group of size 2^k generated by $g_1, \ldots, g_k$.

EXAMPLE 3.1. *Let* $\mathcal{C}$, $\widehat{\mathcal{C}}$ *be as follows*:

$$\mathcal{C} : Y^2 = (X^2+1)(X^2+2)(X^2+2X+2)\,,$$
$$\widehat{\mathcal{C}} : Y^2 = (X^2-2)(X^2+X-1)(-X)\,.$$

Then $\mathcal{J}(\mathbb{Q})$ *and* $\widehat{\mathcal{J}}(\mathbb{Q})$ *have rank* 1.

Proof. The only bad primes are 2, 5, and so $\mathbb{Q}(\mathcal{S}) = \{\pm1, \pm2, \pm5, \pm10\}$. Finite field reductions modulo 3 and 7 give that no torsion points occur apart from the 2-torsion group of size 4 on each of $\mathcal{J}(\mathbb{Q})$ and $\widehat{\mathcal{J}}(\mathbb{Q})$.

$\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$: Using Theorem 2.10, $L^\phi = \langle(2,-1),(-1,1),(2,1),(1,5),(5,2)\rangle$. Applying Lemma 2.4 to the points of order 2 on $\widehat{\mathcal{J}}(\mathbb{Q})$ gives that $\psi(\langle\widehat{\alpha}_1,\widehat{\alpha}_2\rangle) = \langle(2,-1),(-1,1)\rangle$. Further, there is the divisor of infinite order:

$$D = \{(0,0),(-1,1)\} \xrightarrow{\psi} (2,1)\,.$$

Hence, $\langle(2,-1),(-1,1),(2,1)\rangle \le \operatorname{im}\psi \le L^\phi$. There are only three cosets to check: $(1,5),(5,2),(5,10)$. But a straightforward search in $\mathbb{Q}_5$ (modulo 5^4 was sufficient) gives $\mathcal{J}_{1,5}(\mathbb{Q}_5), \mathcal{J}_{5,2}(\mathbb{Q}_5), \mathcal{J}_{5,10}(\mathbb{Q}_5) = \emptyset$, so $(1,5),(5,2),(5,10) \notin S_5^\phi$. Hence $\operatorname{im}\psi = S^\phi = \langle(2,-1),(-1,1),(2,1)\rangle$ and $\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q})) = \langle\widehat{\alpha}_1,\widehat{\alpha}_2,D\rangle$.

$\mathcal{J}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}))$: Here, $L^{\hat\phi} = \langle(5,1),(1,2),(1,-1),(-1,1),(2,1)\rangle$, and $\widehat{\psi}(\langle\alpha_1,\alpha_2\rangle) = \langle(5,1),(1,2)\rangle$. Hence $\langle(5,1),(1,2)\rangle \le \operatorname{im}\widehat{\psi} \le L^{\hat\phi}$. There are seven cosets to check, none of which lie in $S_2^{\hat\phi}$. Hence $\operatorname{im}\widehat{\psi} = S^{\hat\phi} = \langle(5,1),(1,2)\rangle$, and $\mathcal{J}(\mathbb{Q})/\widehat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q})) = \langle\alpha_1,\alpha_2\rangle$.

Finally, we take $\widehat{\phi}(D) = \{+\infty,+\infty\}$ to obtain a point of infinite order on $\mathcal{J}(\mathbb{Q})$, and use the exact sequence of Theorem 2.6 to see that $\mathcal{J}(\mathbb{Q})$ and $\widehat{\mathcal{J}}(\mathbb{Q})$ have rank 1, with $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) = \langle\alpha_1,\alpha_2,\{+\infty,+\infty\}\rangle$ and $\widehat{\mathcal{J}}(\mathbb{Q})/2\widehat{\mathcal{J}}(\mathbb{Q}) = \langle\widehat{\alpha}_1,\widehat{\alpha}_2,D\rangle$. ∎

The initial calculation of L^ϕ, $L^{\hat\phi}$ in the above example meant that significantly fewer homogeneous spaces were required to be checked locally. An even more dramatic illustration of this is given by the following example, for which only two homogeneous spaces need to be checked in total.

EXAMPLE 3.2. *Let* $\mathcal{C}$, $\widehat{\mathcal{C}}$ *be as follows*:

$$\mathcal{C} : Y^2 = (X^2+6X+7)(X^2+4X+1)(X^2+2X+3)\,,$$
$$\widehat{\mathcal{C}} : Y^2 = (X^2-2X-5)(X^2+2X-1)(X^2+6X+11)\,.$$

Then $\mathcal{J}(\mathbb{Q})$ *and* $\widehat{\mathcal{J}}(\mathbb{Q})$ *have rank* 2.

Proof. The only bad primes are 2, 3, and so $\mathbb{Q}(\mathcal{S}) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Finite field reductions modulo 5 and 7 give that no torsion points occur apart from the 2-torsion group of size 4 on each of $\mathcal{J}(\mathbb{Q})$ and $\widehat{\mathcal{J}}(\mathbb{Q})$.

$\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$: We have $L^{\phi} = \langle(-6,-2),\ (-2,-1),\ (1,2),\ (2,3)\rangle$, $\psi(\langle\widehat{\alpha}_1, \widehat{\alpha}_2\rangle) = \langle(-6,-2), (-2,-1)\rangle$, and

$$D_1 = \big\{\big(-\tfrac{5}{3}+\tfrac{1}{3}\sqrt{-2}, \tfrac{32}{27}+\tfrac{80}{27}\sqrt{-2}\big), \big(-\tfrac{5}{3}-\tfrac{1}{3}\sqrt{-2}, \tfrac{32}{27}-\tfrac{80}{27}\sqrt{-2}\big)\big\} \xrightarrow{\psi} (1,2)\,.$$

Hence, $\langle(-6,-2),(-2,-1),(1,2)\rangle \le \operatorname{im}\psi \le L^{\phi}$. There is only one coset, $(2,3)$, to be checked; but $(2,3) \notin S_2^{\phi}$, giving $\operatorname{im}\psi = S^{\phi} = \langle(-6,-2), (-2,-1),(1,2)\rangle$.

$\mathcal{J}(\mathbb{Q})/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}))$: We have $L^{\hat{\phi}} = \langle(-1,-2),\ (-2,-3),\ (-2,-2),\ (3,2)\rangle$, $\psi(\langle\widehat{\alpha}_1, \widehat{\alpha}_2\rangle) = \langle(-1,-2), (-2,-3)\rangle$, and

$$D_2 = \{(-1+\sqrt{6}, 16+8\sqrt{6}), (-1-\sqrt{6}, 16-8\sqrt{6})\} \xrightarrow{\psi} (-2,-2)\,.$$

Hence, $\langle(-1,-2),(-2,-3),(-2,-2)\rangle \le \operatorname{im}\psi \le L^{\phi}$. There is only one coset, $(3,2)$, to be checked; but $(3,2) \notin S_3^{\hat{\phi}}$, giving $\operatorname{im}\widehat{\psi} = S^{\hat{\phi}} = \langle(-1,-2), (-2,-3),(-2,-2)\rangle$.

We therefore find that $\mathcal{J}(\mathbb{Q})$ and $\widehat{\mathcal{J}}(\mathbb{Q})$ both have rank 2 with

$$\begin{aligned}\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) &= \langle\alpha_1, \alpha_2, D_2, \{(-2,3),(-2,3)\}\rangle\,,\\ \widehat{\mathcal{J}}(\mathbb{Q})/2\widehat{\mathcal{J}}(\mathbb{Q}) &= \big\langle\widehat{\alpha}_1, \widehat{\alpha}_2, D_1, \big\{\big(-\tfrac{5}{2}, \tfrac{15}{8}\big), \big(-\tfrac{5}{2}, \tfrac{15}{8}\big)\big\}\big\rangle\,. \ \blacksquare\end{aligned}$$

In our final example, we exploit the fact that much of the work is in common between curves of the form $Y^2 = k \cdot q_1(X)q_2(X)q_3(X)$ where $k \in \mathbb{Q}(\mathcal{S})$. This allows us quickly to handle a group of curves at once. In the cases when the Jacobian has rank 0, it is straightforward to determine all the $\mathbb{Q}$-rational points on the underlying curve.

Example 3.3. *Let $\mathcal{C}^{(k)}$, $\widehat{\mathcal{C}}^{(k)}$ be as follows for $k = 1, 2, -2, 6$:*

$$\begin{aligned}\mathcal{C}^{(k)} &: Y^2 = k(X^2+1)(X^2+2)(X^2+X+1)\,,\\ \widehat{\mathcal{C}}^{(k)} &: Y^2 = k(X^2-2X-2)(X^2-1)(-X)\,.\end{aligned}$$

Then $\mathcal{J}^{(k)}(\mathbb{Q})$, $\widehat{\mathcal{J}}^{(k)}(\mathbb{Q})$ has rank 1 when $k = 1, 2, 6$, and rank 0 when $k = -2$. The curve $\widehat{\mathcal{C}}^{(-2)}$ has no rational points apart from $(0,0), (\pm 1, 0), \infty$.

Proof. The only bad primes are 2, 3, and so $\mathbb{Q}(\mathcal{S}) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$. For all k, there are four 2-torsion points $\langle\alpha_1, \alpha_2\rangle$, on $\mathcal{J}^{(k)}(\mathbb{Q})$, and for $k = 2$ there is the 4-torsion point $\beta = \{(0,2),(1,6)\}$ (where $2\beta = \alpha_1$). For all k, there are eight 2-torsion points $\langle\widehat{\alpha}_1, \widehat{\alpha}_2, \gamma\rangle$, on $\widehat{\mathcal{J}}^{(k)}(\mathbb{Q})$, where $\gamma = \{\infty, (-1,0)\}$. Finite field reductions modulo 5 and 7 show that these give the whole rational torsion group. We now observe that L^{ϕ}, $L^{\hat{\phi}}$ depend only on the values of $b_1, b_2, b_3, \widehat{b}_1, \widehat{b}_2, \widehat{b}_3$ modulo squares, which are not affected by the value of k. Hence, for any $k = 1, 2, -2, 6$, $L^{\phi} = \langle(6,-3), (-3,3), (1,-1),$

$(1,2),(1,3)\rangle$. Also, $\psi(\langle\widehat{\alpha}_1,\widehat{\alpha}_2,\gamma\rangle) = \langle(6,-3),(-3,3),(1,2k)\rangle$. Hence, $\langle(6,-3),(-3,3),(1,2k)\rangle \le \operatorname{im}\psi \le L^{\phi}$. Similarly, for any such k, $\psi(\langle\alpha_1,\alpha_2\rangle) = \langle(1,3)\rangle \le \operatorname{im}\widehat{\psi} \le L^{\hat{\phi}} = \langle(1,3),(1,-2),(-1,-1),(2,6),(-3,1)\rangle$.

In the same manner as Examples 3.1, 3.2, there are only a few cosets to check, and for each $k = 1,2,-2,6$ it can be shown that $\operatorname{im}\psi = S^{\phi}$, and $\operatorname{im}\widehat{\psi} = S^{\hat{\phi}}$. The set of generators for each $k = 1,2,-2,6$ is as follows, with the point of infinite order ($k = 1,2,6$) listed last in each case.

$$\begin{aligned}
\mathcal{J}^{(1)}(\mathbb{Q})/2\mathcal{J}^{(1)}(\mathbb{Q}) &= \langle\alpha_1,\alpha_2,\{+\infty,+\infty\}\rangle\,,\\
\widehat{\mathcal{J}}^{(1)}(\mathbb{Q})/2\widehat{\mathcal{J}}^{(1)}(\mathbb{Q}) &= \big\langle\widehat{\alpha}_1,\widehat{\alpha}_2,\gamma,\big\{(0,0),\big(-\tfrac{1}{2},\tfrac{3}{4}\big)\big\}\big\rangle\,,\\
\mathcal{J}^{(2)}(\mathbb{Q})/2\mathcal{J}^{(2)}(\mathbb{Q}) &= \langle\alpha_2,\beta,\{(0,2),(0,2)\}\rangle\,,\\
\widehat{\mathcal{J}}^{(2)}(\mathbb{Q})/2\widehat{\mathcal{J}}^{(2)}(\mathbb{Q}) &= \langle\widehat{\alpha}_1,\widehat{\alpha}_2,\gamma,\{(0,0),(-2,12)\}\rangle\,,\\
\mathcal{J}^{(-2)}(\mathbb{Q})/2\mathcal{J}^{(-2)}(\mathbb{Q}) &= \langle\alpha_1,\alpha_2\rangle\,,\\
\widehat{\mathcal{J}}^{(-2)}(\mathbb{Q})/2\widehat{\mathcal{J}}^{(-2)}(\mathbb{Q}) &= \langle\widehat{\alpha}_1,\widehat{\alpha}_2,\gamma\rangle\,,\\
\mathcal{J}^{(6)}(\mathbb{Q})/2\mathcal{J}^{(6)}(\mathbb{Q}) &= \langle\alpha_1,\alpha_2,\{(-1,6),(-1,6)\}\rangle\,,\\
\widehat{\mathcal{J}}^{(6)}(\mathbb{Q})/2\widehat{\mathcal{J}}^{(6)}(\mathbb{Q}) &= \langle\widehat{\alpha}_1,\widehat{\alpha}_2,\gamma,\{(0,0),(2,12)\}\rangle\,. \ \blacksquare
\end{aligned}$$

The most surprising feature of the above examples was how little actual computation was required to determine the rank. Once the equations defining $\mathcal{J}_{d_1,d_2}$ had been processed, the time required for determining whether there were points locally took only a few seconds on a Sun 3/60 work station (indeed Example 3.1 was computed by hand in about 12 hours). There are still gaps in the methodology—for example, we have not yet developed a technique for higher descents, and so our method currently requires $\operatorname{im}\psi = S^{\phi}$ and $\operatorname{im}\widehat{\psi} = S^{\hat{\phi}}$. It seems reasonable to expect (judging by analogous computations on elliptic curves) that sufficiently many curves will satisfy these requirements to allow rank tables for several thousand Jacobians to be produced.

Appendix A. The embedding $\mathcal{J}(\mathcal{C})$, and isogeny from $\mathcal{J}$ to $\widehat{\mathcal{J}}$. The equations defining the embedding $\mathcal{J}(\mathcal{C})$, the homogeneous spaces $\mathcal{J}_{d_1,d_2}$, and the isogeny ϕ would require roughly 50 pages to list, and so we do not include them here. Instead, they have been placed in the file: /pub/genus2/isogeny which is available by anonymous ftp from 131.111.24.1 (pmms.cam.ac.uk). The contents of this file are as follows.

(1) The embedding ($v_{0..15}$) of Definition 2.1.

(2) The defining equations satisfied by $v_0,\ldots,v_{15}$.

(3) The defining equations for $\mathcal{J}_{d_1,d_2}$ of Definition 2.7.

(4) The 16×16 matrices $M,\widehat{M},U$ which define ϕ, $\widehat{\phi}$ of Lemma 2.2.

These are given in full generality for any curve of the form $\mathcal{C} : Y^2 = q_1(X)q_2(X)q_3(X)$, where $q_i(X) = f_iX^2 + g_iX + h_i$. The file is suitable for input to the symbolic algebra package Maple, and may easily be modified for input to other similar packages.

Appendix B. A theorem about norms. The contents of this appendix are due to J. W. S. Cassels. Throughout this appendix k is any field of characteristic not 2 and we shall use Norm to indicate the norm from a quadratic extension; which extension will be clear from the context.

Theorem. *Let $d_1, d_2 \in k^*$ be multiplicatively independent modulo squares. Let*

$$\delta_1^2 = d_1\,, \qquad \delta_2^2 = d_2\,, \qquad \delta_3 = \delta_1\delta_2\,.$$

Let $e_1, e_2, e_3 \in k^*$ be of the shape

$$\begin{aligned} e_1 &= \mathrm{Norm}\,\gamma_2\ \mathrm{Norm}\,\gamma_3\,,\\ e_2 &= \mathrm{Norm}\,\gamma_3\ \mathrm{Norm}\,\gamma_1\,,\\ e_3 &= \mathrm{Norm}\,\gamma_1\ \mathrm{Norm}\,\gamma_2\,, \end{aligned}$$

where $\gamma_j \in k(\delta_j)$ $(j = 1, 2, 3)$. Let $\varepsilon_j^2 = e_j$ $(j = 1, 2, 3)$. Then there are $\xi_j \in k(\varepsilon_j)$ such that

$$d_1 = \mathrm{Norm}\,\xi_2\ \mathrm{Norm}\,\xi_3\,, \qquad d_2 = \mathrm{Norm}\,\xi_3\ \mathrm{Norm}\,\xi_1\,.$$

We shall first give a brief but entirely unilluminating verification. The rest of the appendix explains how it was obtained via a normal extension of k of degree 32. We motivate it here in terms of a simpler and well known result. Let $d, e \in k^*$ and let $\delta^2 = d$, $\varepsilon^2 = e$. Then d is a norm for $k(\varepsilon)$ precisely when e is a norm for $k(\delta)$: indeed, both are equivalent to the existence of a nontrivial solution $x,\ y,\ z$ of

$$z^2 = dx^2 + ey^2.$$

From our point of view it is more relevant that both are equivalent to the existence of a quadratic extension of $k(\delta, \varepsilon)$ which is normal but not abelian over k. More precisely, let $e = \mathrm{Norm}\,\gamma$, where $\gamma \in k(\delta)$ and put $\zeta^2 = \gamma$. Then $K = k(\delta, \varepsilon, \zeta)$ is normal of degree 8. Its group is generated, as is easy to see, by three automorphisms σ, τ, λ of order 2 given by

$$\begin{aligned} \sigma\delta &= -\delta\,, & \sigma\varepsilon &= \varepsilon\,, & \sigma\zeta &= \varepsilon/\zeta\,,\\ \tau\delta &= \delta\,, & \tau\varepsilon &= -\varepsilon\,, & \tau\zeta &= \zeta\,,\\ \lambda\delta &= \delta, & \lambda\varepsilon &= \varepsilon, & \lambda\zeta &= -\zeta\,. \end{aligned}$$

Here λ is in the centre and $\tau\sigma = \lambda\sigma\tau$. The rôles of d, e in the above are not symmetric, but can be made so by considering $\eta = \zeta - \sigma\zeta$. Then $\lambda\eta = -\eta$,

$\sigma\eta = -\eta$ and $\eta(\tau\eta) = \gamma - \sigma\gamma = u\delta$ for some $u \in k$. Let $\beta = \eta^2$. It follows that $\beta \in k(\varepsilon)$ and $\operatorname{Norm} \beta = du^2$.

For the corresponding result for pure cubic extensions, see [2], p. 87 (Lemma 13). Results of this nature are related to the theory of the Hilbert Norm Residue symbol, and could doubtless be proved by the theory of central simple algebras; but perhaps not so explicitly.

VERIFICATION. We may take

$$\gamma_j = x_j + y_j\delta_j,$$

where $x_j, y_j \in k$. Consider

$$(*)\qquad \begin{aligned} \eta_1 &= x_1y_2x_3 + d_1y_1x_2y_3 + y_2\varepsilon_1\,, \\ \eta_2 &= y_1x_2x_3 + d_2x_1y_2y_3 + y_1\varepsilon_2\,, \\ \eta_3 &= x_1x_2y_3 + y_1y_2x_3 + y_3\varepsilon_3\,, \end{aligned}$$

where $\varepsilon_j^2 = e_j$. One checks readily that

$$\operatorname{Norm} \eta_1 = d_1 \operatorname{Norm} \eta_3\,, \qquad \operatorname{Norm} \eta_2 = d_2 \operatorname{Norm} \eta_3\,.$$

The result follows.

Proof. We define first a group Γ of order 32. It is generated by λ, σ_1, σ_2, τ_1, τ_2 all of order 2. Further,

$$\text{(B.1)}\qquad \sigma_1\tau_2 = \lambda\tau_2\sigma_1\,, \qquad \sigma_2\tau_1 = \lambda\tau_1\sigma_2\,,$$

but otherwise the generators commute; in particular, the centre consists of just λ and the identity.

LEMMA. *Let K/k be a normal extension with Galois group Γ. Then there are d_j, e_j, γ_j satisfying the hypotheses of the Theorem and such that*

$$\text{(B.2)}\qquad K = k(\delta_1, \delta_2, \varepsilon_1, \varepsilon_2, \alpha),$$

where

$$\text{(B.3)}\qquad \alpha^2 = \gamma_1\gamma_2\gamma_3.$$

Conversely, if d_j, e_j, γ_j satisfy the conditions of the Theorem and d_1, d_2, e_1, e_2 are multiplicatively independent modulo squares, then the field K given by (B.2), (B.3) *has Galois group Γ.*

Proof. The fixed field of $\{\sigma_2, \tau_1, \tau_2, \lambda\}$ is an extension of k of degree 2, say $k(\delta_1)$, where

$$\sigma_1\delta_1 = -\delta_1\,, \qquad \delta_1^2 = d_1$$

for some $d_1 \in k^*$. Similarly we obtain δ_2, ε_1, ε_2 with

$$\sigma_2\delta_2 = -\delta_2\,, \qquad \tau_1\varepsilon_1 = -\varepsilon_1\,, \qquad \tau_2\varepsilon_2 = -\varepsilon_2\,,$$

but otherwise fixed by the group generators. Put $\delta_2^2 = d_2$, $\varepsilon_1^2 = e_1$, $\varepsilon_2^2 = e_2$. Clearly the fixed field of λ is $k(\delta_1, \delta_2, \varepsilon_1, \varepsilon_2)$ of degree 16.

The Galois group of $K/k(\delta_1, \delta_2)$ is generated by $\{\tau_1, \tau_2, \lambda\}$, and so of type $(2, 2, 2)$. Hence

$$K = k(\delta_1, \delta_2, \varepsilon_1, \varepsilon_2, \alpha) \tag{B.4}$$

for some α with

$$\lambda\alpha = -\alpha\,, \qquad \tau_1\alpha = \tau_2\alpha = \alpha, \tag{B.5}$$

so

$$\alpha^2 \in k(\delta_1, \delta_2). \tag{B.6}$$

Now

$$\tau_1\sigma_1\alpha = \sigma_1\tau_1\alpha = \sigma_1\alpha\,, \qquad \tau_2\sigma_1\alpha = \lambda\sigma_1\tau_2\alpha = \lambda\sigma_1\alpha = -\sigma_1\alpha$$

etc. Hence

$$h = \alpha(\sigma_1\alpha)(\sigma_2\alpha)(\sigma_1\sigma_2\alpha) \tag{B.7}$$

is fixed under all the generators of the group, that is,

$$h \in k^*\,. \tag{B.8}$$

Similarly one checks that $\alpha(\sigma_1\alpha)/\varepsilon_2$ is fixed under σ_1, τ_1, τ_2, λ, that is,

$$\alpha(\sigma_1\alpha) = \varepsilon_2\gamma_2\,, \qquad \gamma_2 \in k(\delta_2)\,. \tag{B.9}$$

In the same way,

$$\alpha(\sigma_2\alpha) = \varepsilon_1\gamma_1\,, \qquad \gamma_1 \in k(\delta_1)\,, \tag{B.10}$$

and

$$\alpha(\sigma_1\sigma_2\alpha) = \varepsilon_1\varepsilon_2\gamma_3\,, \qquad \gamma_3 \in k(\delta_1\delta_2)\,. \tag{B.11}$$

On applying σ_2, σ_1, $\sigma_1\sigma_2$ to (B.9), (B.10), (B.11) respectively, we have

$$h = e_2 \operatorname{Norm}\gamma_2 = e_1 \operatorname{Norm}\gamma_1 = e_1e_2 \operatorname{Norm}\gamma_3\,. \tag{B.12}$$

Further,

$$h\alpha^2 = e_1e_2\gamma_1\gamma_2\gamma_3 \tag{B.13}$$

by (B.7), (B.9), (B.10), (B.11). Finally, on replacing γ_3 by $(h/e_1e_2)\gamma_3$ we get (B.2), (B.3), as required.

The converse is straightforward and left to the reader with the hint to define $\sigma_1\alpha = \varepsilon_2\gamma_2/\alpha$.

Proof of Theorem. The structure of the field K of the Lemma is symmetric in the d's and the e's. More precisely, let

$$\beta = \alpha + \sigma_1\alpha + \sigma_2\alpha + \sigma_1\sigma_2\alpha\,. \tag{B.14}$$

Then

$$\lambda\beta = -\beta\,, \qquad \sigma_1\beta = \sigma_2\beta = \beta\,. \tag{B.15}$$

Hence β corresponds to α and we can go on to construct the analogues ξ_j of the γ_j. The formulae of the verification $(*)$ were obtained by going through this in detail.

References

[1] J. B. Bost et J.-F. Mestre, *Moyenne arithmético-géometrique et périodes des courbes de genre* 1 *et* 2, Gaz. Math. 38 (1988), 36–64.

[2] J. W. S. Cassels, *Arithmetic on curves of genus* 1, *I. On a conjecture of Selmer*, J. Reine Angew. Math. 202 (1959), 52–59.

[3] —, *The Mordell–Weil group of curves of genus* 2, in: Arithmetic and Geometry papers dedicated to I. R. Shafarevich on the occasion of his sixtieth birthday, Vol. 1, Arithmetic, Birkhäuser, Boston, 1983, 29–60.

[4] —, *Lectures on Elliptic Curves*, London Math. Soc. Stud. Texts 24, Cambridge University Press, 1991.

[5] C. Chabauty, *Sur les points rationnels des variétés algébriques dont l'irregularité et supérieur à la dimension*, C. R. Acad. Sci. Paris 212 (1941), 882–885.

[6] R. F. Coleman, *Effective Chabauty*, Duke Math. J. 52 (1985), 765–780.

[7] E. V. Flynn, *The Jacobian and formal group of a curve of genus* 2 *over an arbitrary ground field*, Math. Proc. Cambridge Philos. Soc. 107 (1990), 425–441.

[8] —, *The group law on the Jacobian of a curve of genus* 2, J. Reine Angew. Math., to appear.

[9] D. M. Gordon and D. Grant, *Computing the Mordell–Weil rank of Jacobians of curves of genus* 2, Trans. Amer. Math. Soc., to appear.

[10] D. Grant, *Formal groups in genus* 2, J. Reine Angew. Math. 411 (1990), 96–121.

[11] W. G. McCallum, *The arithmetic of Fermat curves*, Math. Ann. 294 (1992), 503–511.

[12] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS
CAMBRIDGE UNIVERSITY
16 MILL LANE
CAMBRIDGE CB2 1SB
ENGLAND

Received on 22.12.1992 (2356)