14

A 2-isogeny

An *isogeny* is a map

$$\mathcal{C} \to \mathcal{D}$$

of elliptic curves defined over the ground field and taking the specified rational point $\mathbf{o}_{\mathcal{C}}$ on $\mathcal{C}$ into that on $\mathcal{D}$. Clearly the kernel of the isogeny, i.e. the set of points mapped into $\mathbf{o}_{\mathcal{D}}$ is a finite group and is defined over the ground field as a whole.

In this section we consider the case when $\mathcal{C}$ has a rational point of order 2. It is convenient to modify our canonical form to

$$\mathcal{C}: \ Y^2 = X(X^2 + aX + b),$$

the point of order 2 being $(0,0)$. The function on the right hand side may not have a double root, so

$$b \neq 0, \qquad a^2 - 4b \neq 0.$$

We take $\mathbb{Q}$ to be the ground field. Let $\mathbf{x} = (x, y)$ be a *generic point* of $\mathcal{C}$; that is, x is transcendental and y is defined by

$$y^2 = x(x^2 + ax + b).$$

The field $\mathbb{Q}(x, y)$ is known as the *function field* of $\mathcal{C}$ over $\mathbb{Q}$.

Let

$$\mathbf{x}_1 = \mathbf{x} + (0,0).$$

The transformation

$$\mathbf{x} \to \mathbf{x}_1$$

is an automorphism of $\mathbb{Q}(x, y)$ of order 2. We will find the fixed field.

The line through $(0,0)$ and (x, y) is

$$X = tx, \qquad Y = ty,$$

which meets $\mathcal{C}$ in $(0,0)$, $\mathbf{x}$ and $-\mathbf{x}_1 = (x_1, -y_1)$. We get

$$x_1 = b/x$$

$$y_1 = -by/x^2.$$

One invariant under $\mathbf{x} \to \mathbf{x}_1$ is clearly t^2, which is

$$t^2 = (y/x)^2 = \frac{x^2 + ax + b}{x}$$

$$= \lambda \qquad \text{(say)} \quad [= x + x_1 + a].$$

Another is

$$y + y_1 = \mu \qquad \text{(say)}.$$

To find an algebraic relation between λ, μ we compute

$$\mu^2 = y^2(1 - b/x^2)^2$$

$$= \frac{x^2 + ax + b}{x}(x^2 - 2b + b^2/x^2).$$

Here the first factor is just λ. The second is

$$(x + b/x)^2 - 4b = (\lambda - a)^2 - 4b$$

$$= \lambda^2 - 2a\lambda + (a^2 - 4b).$$

Hence

$$\mu^2 = \lambda(\lambda^2 - 2a\lambda + (a^2 - 4b)).$$

Conversely, we can express x, y in terms of λ, μ and

$$\lambda^{1/2} = y/x,$$

since

$$\lambda^{-1/2}\mu = x - b/x$$

$$\lambda = x + (b/x) + a.$$

Hence

$$x = \frac{1}{2}(\lambda + \lambda^{-1/2}\mu - a), \qquad y = \lambda^{1/2}x. \qquad (*)$$

The field extension $\mathbb{Q}(x, y)/\mathbb{Q}(\lambda, \mu)$ is of degree 2 and so by Galois theory $\mathbb{Q}(\lambda, \mu)$ is the complete field of invariants.

The point (λ, μ) is a generic point of

$$\mathcal{D}: \ Y^2 = X(X^2 - 2aX + (a^2 - 4b)).$$

The map

$$\phi: \ \mathcal{C} \to \mathcal{D}$$

given by

$$\mathbf{x} = (x, y) \to \boldsymbol{\lambda} = (\lambda, \mu)$$

preserves the group law[12]. For let $\mathbf{a}$, $\mathbf{b}$ be points on $\mathcal{C}$ and let $f \in \mathbb{Q}(\mathbf{x})$ be a function with simple poles at $\mathbf{a}$, $\mathbf{b}$ and simple zeros at $\mathbf{o}$, $\mathbf{a}+\mathbf{b}$. Let f_1 be the conjugate under $\mathbf{x} \to \mathbf{x}_1$. Then $ff_1 \in \mathbb{Q}(\boldsymbol{\lambda})$: as a function of $\boldsymbol{\lambda}$ it clearly has simple poles at $\phi(\mathbf{a})$, $\phi(\mathbf{b})$ and simple zeros at $\phi(\mathbf{o}) = \mathbf{o}$ and $\phi(\mathbf{a}+\mathbf{b})$. Hence

$$\phi(\mathbf{a}+\mathbf{b}) = \phi(\mathbf{a}) + \phi(\mathbf{b}).$$

The equation for $\mathcal{D}$ has the same general shape as that for $\mathcal{C}$. On repeating the process with $\boldsymbol{\lambda}$ and $\mathcal{D}$, we get ρ, σ with

$$\sigma^2 = \rho(\rho^2 + 4a\rho + 16b);$$

and so

$$\xi = \rho/4, \qquad \eta = \sigma/8$$

is a generic point of $\mathcal{C}$ again.

The points mapping into $(\lambda, \mu) = (0,0)$ are just the 2-division points other than $(0,0)$. Hence the kernel of the map $(x,y) \to (\xi, \eta)$ is just the 2-division points and $\mathbf{o}$. So the map must be multiplication by ± 2.

We now consider the effect of the isogeny

$$\phi: \ \mathcal{C} \to \mathcal{D}$$

on rational points. Denote the rational points on $\mathcal{C}$, $\mathcal{D}$ by $\mathfrak{G}$, $\mathfrak{H}$ respectively.

We denote the multiplicative group of nonzero elements of $\mathbb{Q}$ by $\mathbb{Q}^*$.

Lemma 1. *Let $(u,v) \in \mathfrak{H}$. Then $(u,v) \in \phi\mathfrak{G}$ precisely when either $u \in (\mathbb{Q}^*)^2$ or $u = 0$, $a^2 - 4b \in (\mathbb{Q}^*)^2$.*

Proof. For $u \neq 0$, this follows by specializing $\lambda \to u$, $\mu \to v$ in (*). The point $(\lambda,\mu) = (0,0)$ comes from the points $(\alpha, 0)$ where $\alpha^2 + a\alpha + b = 0$: and $a \in \mathbb{Q}$ if and only if $a^2 - 4b \in (\mathbb{Q}^*)^2$.

This suggests the map

$$q: \ \mathfrak{H} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

given by

$$q((u,v)) = u(\mathbb{Q}^*)^2 \qquad (u \neq 0)$$
$$= (a^2 - 4b)(\mathbb{Q}^*)^2 \qquad (u = 0)$$
$$q(\mathbf{o}) = (\mathbb{Q}^*)^2.$$

[12] The argument is quite general for isogenies of any degree. Note that ff_1 is the norm of f for the extension $\mathbb{Q}(\mathbf{x})/\mathbb{Q}(\boldsymbol{\lambda})$, cf. §24, Lemma 1.

We note that the equation

$$v^2 = u(u^2 - 2au + a^2 - 4b)$$

implies that

$$q((u,v)) = (u^2 - 2au + a^2 - 4b)(\mathbb{Q}^*)^2$$

whenever the right hand side is defined.

Lemma 2. *The map*

$$q: \mathfrak{H} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

is a group homomorphism.

Proof. Write the equation of $\mathcal{D}$ as

$$\mathcal{D}: \quad V^2 = U(U^2 + a_1 U + b_1).$$

Let $\mathbf{u}_j = (u_j, v_j)$ $(j = 1,2,3) \in \mathfrak{H}$ with

$$\mathbf{u}_1 + \mathbf{u}_2 + \mathbf{u}_3 = \mathbf{o},$$

so they are the intersection of $\mathcal{D}$ with a line

$$V = lU + m.$$

Substituting in the equation for $\mathcal{D}$, we have

$$U(U^2 + a_1 U + b_1) - (lU + m)^2$$
$$= (U - u_1)(U - u_2)(U - u_3).$$

Hence

$$u_1 u_2 u_3 = m^2.$$

This implies that

$$q(\mathbf{u}_1)q(\mathbf{u}_2)q(\mathbf{u}_3) = (\mathbb{Q}^*)^2$$

except, possibly, when one of the $\mathbf{u}_j$ is $(0,0)$. The verification in this case is left to the reader.

Lemma 3. *The image of*

$$q: \ \mathfrak{H} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

is finite.

Proof. Without loss of generality

$$a_1 \in \mathbb{Z}, \qquad b_1 \in \mathbb{Z}.$$

An element of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ may be written $r(\mathbb{Q}^*)^2$, where

$$r \in \mathbb{Z}, \qquad \text{square free.}$$

We show that $r(\mathbb{Q}^*)^2$ is in the image of q only when $r \mid b_1$.

Suppose that $q((u,v)) = r(\mathbb{Q}^*)^2$. Then there are $s,\ t \in \mathbb{Q}$ such that

$$u^2 + a_1 u + b_1 = rs^2$$
$$u = rt^2.$$

Put $t = l/m$, where

$$l, m \in \mathbb{Z}, \qquad \gcd(l,m) = 1.$$

Then, on eliminating u,

$$r^2 l^4 + a_1 r l^2 m^2 + b_1 m^4 = rn^2,$$

where $n = m^2 s \in \mathbb{Z}$.

Suppose that there is a prime p with $p \mid r$, $p \nmid b_1$. Then $p \mid m$, so $p^2 \mid rn^2$ and hence $p \mid n$ because r is square-free. Then $p^3 \mid r^2 l^4$, so $p \mid l$, contrary to $gcd(l,m) = 1$.

Putting the three lemmas together, we get the

Theorem 1. *$\mathfrak{H}/\phi\mathfrak{G}$ is finite.*

Corollary. *$\mathfrak{G}/2\mathfrak{G}$ is finite.*

Proof. Consider the exact triangle

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\times 2} & \mathcal{C} \\ & \phi\searrow \quad \nearrow\psi & \\ & \mathcal{D} & \end{array}$$

where $\mathfrak{H}/\phi\mathfrak{G}$ and $\mathfrak{G}/\psi\mathfrak{H}$ are both finite.

By considering in detail the equations arising in the Lemma 3, we can get more information about $\mathfrak{G}/2\mathfrak{G}$; e.g. by looking at the equations locally. There is, however, no local-global theorem and indeed even today there is no algorithm for deciding whether or not there is a solution. We shall come back to these questions in a late section. So one should not conclude from the fact that we can determine $\mathfrak{G}/2\mathfrak{G}$ in the examples that one can always do so.

We first enunciate more precisely what was proved.

Lemma 4. *The group $\mathfrak{H}/\phi\mathfrak{G}$ is isomorphic to the group of $q(\mathbb{Q}^*)^2$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ where*

(i) *$q \in \mathbb{Z}$ is square-free and $q \mid b_1$*
(ii) *The equation*

$$ql^4 + a_1 l^2 m^2 + (b_1/q)m^4 = n^2$$

has a solution in $l,\ m,\ n \in \mathbb{Z}$ not all 0.

Further, the point $(0,0)$ of $\mathfrak{H}$ corresponds to $q =$ the square-free kernel of b_1.

Example 1.

$$\mathcal{C}: \ Y^2 = X(X^2 - X + 6)$$
$$\mathcal{D}: \ Y^2 = X(X^2 + 2X - 23)$$

For $\mathfrak{H}/\phi\mathfrak{G}$ we have $q \mid (-23)$. Since -23 corresponds to $(0,0)$, we need look at only one of $q = +23$, $q = -1$, say the latter. The equation of Lemma 4 is

$$-l^4 + 2l^2m^2 + 23m^4 = n^2$$

i.e.

$$-(l^2 - m^2)^2 + 24m^4 = n^2$$

which is impossible in $\mathbb{Q}_3$. Hence $\mathfrak{H}/\phi\mathfrak{G}$ is generated by $(0,0)$.

For $\mathfrak{G}/\psi\mathfrak{H}$, we have $q \mid 6$, so $q = -1$ or $q = \pm 2,\ \pm 3,\ \pm 6$. Since the form $X^2 - X + 6$ is definite, we must have $q > 0$. Hence $q = 2, 3$ or 6; and 6 belongs to $(0,0)$. Thus it is enough to look at one of $2, 3$, say 2. The equation is

$$2l^4 - l^2m^2 + 3m^4 = n^2,$$

which is seen to have the solution $(l,m,n) = (1,1,2)$. This corresponds to $(x,y) = (2,4)$.

It follows that $\mathfrak{G}/\psi\mathfrak{H}$ is generated by $(0,0)$ and $(2,4)$. To find generators for $\mathfrak{G}/2\mathfrak{G}$ we need to look at the effect of ψ on the generators of $\mathfrak{H}/\phi\mathfrak{G}$. In this case $\phi(0,0) = \mathbf{o}$, so $\mathfrak{G}/2\mathfrak{G}$ is also generated by $(0,0)$ and $(2,4)$.

Second example. This is related to Fermat's equation

$$U^4 + V^4 = V^4.$$

Then

$$Y = V^2W^2/U^4, \qquad X = W^2/U^2$$

satisfy

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

so

$$\mathcal{D}: Y^2 = X(X^2+4).$$

For $\mathfrak{H}/\phi\mathfrak{G}$, we have $q \mid 4$, so $q = -1, \pm 2$. Since X^2+4 is definite, we need $q>0$, so only $q=2$ needs to be looked at. The relevant equation is

$$2l^4 + 2m^4 = n^2,$$

which has the solution $(l,m,n) = (1,1,2)$, giving $(X,Y) = (2,4)$ as the generator of $\mathfrak{H}/\phi\mathfrak{G}$. The point $(0,0)$ is in $\phi\mathfrak{G}$.

For $\mathfrak{G}/\psi\mathfrak{H}$, we have $q \mid (-1)$. Since -1 belongs to $(0,0)$, there is nothing to do. Then $\mathfrak{G}/\psi\mathfrak{H}$ is generated by $(0,0)$ and $\mathfrak{G}/2\mathfrak{G}$ is generated by $(0,0)$ and $\psi(2,4) = (1,0)$.

§14. Exercises

1. Find

(i) a set of generators for $\mathfrak{G}/2\mathfrak{G}$, where $\mathfrak{G}$ is the group of rational points and

(ii) the 2-power torsion, for the following curves

$$Y^2 = X(X^2+3X+5)$$
$$Y^2 = X(X^2-4X+15)$$
$$Y^2 = X(X^2+4X-6)$$
$$Y^2 = X(X^2-X+6)$$
$$Y^2 = X(X^2+2X+9)$$
$$Y^2 = X(X^2-2X+9)$$

2. Invent similar questions to 1 and solve them. [*Note.* You cannot expect to determine $\mathfrak{G}/2\mathfrak{G}$ in every case, but you can majorize its order. It might be helpful to write a Mickey Mouse program to look for points with small co-ordinates.]

3. Let $\mathcal{C}: Y^2 = X(X^2+aX+b)$, $\mathcal{D}: Y^2 = X(X^2+a_1X+b_1)$ with $a_1 = -2a$, $b_1 = a^2-4b$.

(i) Show that the odd torsion groups are isomorphic

(ii) Assuming the finite basis theorem, show that the ranks [= number of generators of infinite order] are the same

(iii) give an example to show that the orders of the groups of 2-power torsion need not be the same. Determine what the possibilities are.

4. (i) Construct an elliptic curve with a torsion element of order 8.

(ii) Show that no torsion element can have order 16.

(iii) Determine all abstract groups of 2-power order which can isomorphic to the 2-power torsion of an elliptic curve. Give elliptic curves in the possible cases and give a proof of impossibility for the others.

5. (Another kind of isogeny). Let

$$\mathcal{C}: Y^2 = X^3 + B$$

be defined over $\mathbb{Q}$ and let $\beta^2 = B$, $\beta \in \overline{\mathbb{Q}}$.

(i) Show that $Y = \pm\beta$ are inflexions and that $2(0,\beta) = (0,-\beta)$.

(ii) Let $\mathbf{x} = (x,y)$ be generic and put

$$\mathbf{x}_1 = \mathbf{x} + (0,\beta), \qquad \mathbf{x}_2 = \mathbf{x} + (0,-\beta).$$

Show that

$$\xi = x + x_1 + x_2, \qquad \eta = y + y_1 + y_2$$

are functions of (x,y) defined over $\mathbb{Q}$ and that

$$\mathcal{D}:\ \eta^2 = \xi^3 - 27B.$$

(iii) Show that the repetition of the above map is (essentially) multiplication by 3.

(iv) Denote by $\mathfrak{G}$, $\mathfrak{H}$ the groups of rational points on $\mathcal{C}$, $\mathcal{D}$ respectively. Denote by $\mathbb{Q}(\beta)^*$ the multiplicative group of non zero elements of $\mathbb{Q}(\beta)$. If $(x,y) \in \mathfrak{G}$ and

$$y + \beta \in \{\mathbb{Q}(\beta)^*\}^3$$

show that $\mathbf{x}$ is in the image of $\mathfrak{H}$ under $\mathcal{D} \to \mathcal{C}$.
[*Hint.* Put $y + \beta = (u + v\beta)^3$ and equate the coefficients of β.]

(v) Show that

$$(x,y) \to (y+\beta)\{\mathbb{Q}(\beta)^*\}^3$$

is a homomorphism

$$\mu:\quad \mathfrak{G} \to \mathbb{Q}^*(\beta)/\{\mathbb{Q}(\beta)^*\}^3$$

whose kernel is the image of $\mathfrak{H}$.

(vi) (Requires algebraic number theory). Show that the image of μ is finite [*Hint.* cf. §16].

(vii) Deduce that $\mathfrak{G}/3\mathfrak{G}$ is finite.