ELLIPTIC CURVES AND NUMBER FIELDS — AN EXAMPLE

N. P. STRICKLAND

Let E be the elliptic curve $f(x, y) = 0$, where $f(x, y) = y^2 - x^3 + x$. Let K be the subfield of $\mathbb{C}$ obtained from $\mathbb{Q}$ by adjoining the coordinates of all the points of order five on E. In this note we record the structure of K and the action of $G := \text{Gal}(K/\mathbb{Q})$.

For the sake of definiteness, we agree that $z^{1/n}$ always denotes the principal branch, so $(re^{i\theta})^{1/n} = r^{1/n}e^{i\theta/n}$ if $r > 0$ and $-\pi < \theta \leq \pi$. Put

$$\pi = 1 + 2i$$
$$\lambda = \pi^{1/4}$$
$$\zeta = \exp(2\pi i/5)$$

Theorem 1. *The field K is generated over $\mathbb{Q}$ by λ and $\overline{\lambda}$. It has a basis consisting of the monomials $i^a\lambda^b\overline{\lambda}^c$ with $a \in \{0, 1\}$ and $b, c \in \{0, 1, 2, 3\}$. The Galois group G is generated by the conjugation map $\gamma: z \mapsto \overline{z}$ together with elements $\alpha, \overline{\alpha}$ acting as follows:*

$$\alpha(i) = \overline{\alpha}(i) = i$$
$$\alpha(\lambda) = i\lambda$$
$$\alpha(\overline{\lambda}) = \overline{\lambda}$$
$$\overline{\alpha}(\lambda) = \lambda$$
$$\overline{\alpha}(\overline{\lambda}) = -i\overline{\lambda}.$$

The relations are

$$\alpha^4 = \overline{\alpha}^4 = \gamma^2 = [\alpha, \overline{\alpha}] = 1$$
$$\gamma\alpha\gamma = \overline{\alpha}.$$

The rest of this note constitutes the proof of the theorem. Let L be the field generated by i, λ and $\overline{\lambda}$, so we must show that $K = L$. The claimed basis B is certainly a spanning set for L over $\mathbb{Q}$. Note that π and $\overline{\pi}$ are inequivalent irreducibles in $\mathbb{Z}[i]$; I think this implies that B is indeed a basis for L. Moreover, if we put $M = \mathbb{Q}(i, \lambda)$ and $\overline{M} = \mathbb{Q}(i, \overline{\lambda})$, this argument should show that $L = M \otimes_{\mathbb{Q}(i)} \overline{M}$, and thus that $\text{Gal}(L/\mathbb{Q}(i)) = \text{Gal}(M/\mathbb{Q}(i)) \times \text{Gal}(\overline{M}/\mathbb{Q}(i))$. Given this, it is easy to check that the Galois group is as claimed.

Now recall that E has complex multiplication by $\mathbb{Z}[i]$, given by the formula $i(x, y) = (-x, iy)$ (or $i[x : y : z] = [ix : y : -iz]$).

Put $a = \lambda^{-2}$ and $b = (1 - i)\lambda^{-3}$ and $P = (a, b)$. One checks directly that $f(P) = 0$, so $P \in E$. It is clear that $iP \neq P$, so there is a unique line L joining P to iP, with equation $g(t) = ((1 - 2t)a, (1 + (i - 1)t)b)$. One can again check directly that $f(g(t)) = 0 \pmod{t^2}$, which means that L is tangent to E at P. From the usual geometric description of addition in E, we see that $2P + iP = 0$, so $\overline{\pi}P = -i(2 + i)P = 0$, so $5P = \pi\overline{\pi}P = 0$. This shows that $a, b \in K$.

Next, we note that $iP = (-a, ib)$ is another point of order 5, so $-a, ib \in K$. It follows that $i = (ib)/b \in K$ and thus that $\lambda = (1 - i)a/b \in K$. Similarly, we see that the point $\overline{P} = (\overline{a}, \overline{b})$ satisfies $\pi\overline{P} = 0$, and deduce that $\overline{\lambda} \in K$.

Let A be the group of complex points of $E[5]$. We claim that P and $\overline{P}$ form a basis for A over $\mathbb{Z}/5$. Indeed, both P and $\overline{P}$ are nonzero points of order 5, so it is enough to check that the intersection of the subgroups that they generate is trivial. This intersection is annihilated by both π and $\overline{\pi}$, and these elements are coprime in in $\mathbb{Z}[i]$, so the intersection is trivial as claimed. It follows that all points in A are defined over L, so $K = L$.

Put $Q = P + \overline{P}$, which is easily seen to generate A over $\mathbb{Z}[i]/5$. One checks that

$$Q = ((\lambda^2 + \lambda\overline{\lambda} + \overline{\lambda}^2 + \lambda^3\overline{\lambda}^3)/2, (\lambda + \overline{\lambda})(\lambda\overline{\lambda}(\lambda^2 + \overline{\lambda}^2) + 2)/2)$$

Note that the coordinates here are real. One can check that

$$\lambda\overline{\lambda} = 5^{1/4}$$

$$\lambda^2 + \overline{\lambda}^2 = \sqrt{2(1 + \sqrt{5})}$$

$$\lambda + \overline{\lambda} = \sqrt{\sqrt{2(1 + \sqrt{5})} + 2\sqrt{\sqrt{5}}}$$

Moreover, $\lambda + \overline{\lambda}$ is a root of the irreducible polynomial

$$256 - 1152t^4 - 656t^8 - 8t^{12} + t^{16}$$

and is thus a primitive element for the field $K \cap \mathbb{R}$ over $\mathbb{Q}$.

The Weil pairing gives us an element $\zeta' = e_5(P, \overline{P})$ which is a primitive 5'th root of one. It follows that ζ is a power of ζ' and so lies in K. In fact, we have the formula

$$\zeta = (\lambda^2\overline{\lambda}^2 - 1 + i\lambda\overline{\lambda}(\lambda^2 + \overline{\lambda}^2))/4.$$

We have not checked whether $\zeta' = \zeta$.

Another parametrisation

In any context where we can interpret the relevant square roots, we define

$$f(u) = [u^2 - u^{-2} : 2\sqrt{u^2 - u^{-2}} : (u - u^{-1})^2].$$

This lies on our curve. We have $f(\pm 1) = [0 : 1 : 0]$, but $f(\pm i)$ is ill-defined. The invariant differential pulls back to $(u^4 - 1)^{-1/2}\, du$, so the logarithm is the elliptic function $F_i(iu)$. One of the points of order 3 on the curve is $f(u)$ where $u = (1 + 3^{1/2} + 12^{1/4})/2$.

Alternatively, we have $[x : 1 : z] \in C$ where

$$z = \frac{\sqrt{1 + 4x^4} - 1}{2x} = \frac{1}{x}\sum_{n=0}^{\infty} \binom{2n}{n} \frac{(-x^4)^{n+1}}{n+1}$$