Topics: Automorphisms; more elliptic curves.

8.1. Recall that a (group) homomorphism $\varphi : G \longrightarrow H$ from one abelian group to another is a map such that $\varphi(x+y) = \varphi(x) + \varphi(y)$ for all $x, y \in G$.

(a) Let $G = \langle g \rangle$ be a cyclic group. Let H be an arbitrary abelian group.

For a group homomorphism $\varphi : G \longrightarrow H$, what property must $\varphi(g)$ satisfy?

(b) Find all the group homomorphisms from $\mathbf{Z}/6\mathbf{Z}$ to $\mathbf{Z}/9\mathbf{Z}$.

(c) Find all the group homomorphisms from $\mathbf{Z}/9\mathbf{Z}$ to $\mathbf{Z}/6\mathbf{Z}$.

(d) Find all the group homomorphisms from $\mathbf{Z}/6\mathbf{Z}$ to $\mathbf{Z}/6\mathbf{Z}$.

(e) An *automorphism* of a group G is a bijective homomorphism $G \longrightarrow G$.

Prove that for a cyclic group $G = \langle g \rangle$, a homomorphism $\varphi : G \longrightarrow G$ is an automorphism if and only if $\varphi(g)$ is a generator of G.

(f) Find all the automorphisms of $\mathbf{Z}$.

(g) Find all the automorphisms of $\mathbf{Z}/n\mathbf{Z}$, where $n \in \mathbf{Z}_{\geqslant 1}$.

(h) Find all the automorphisms of $(\mathbf{Z}/p\mathbf{Z})^\times$, where p is prime.

Solution.

(a) If $g \in G$ has infinite order, then $\varphi(g)$ can be any element of H.

Otherwise, let e be the order of g in G, so that $eg = 0$ in G. Then since φ is a homomorphism we have that $e\varphi(g) = 0$ in H, in other words the order of $\varphi(g)$ in H must divide e.

(b) Since $\mathbf{Z}/6\mathbf{Z} = \langle 1 \rangle$, it suffices to specify $\varphi(1)$.

The element 1 has order 6 in $\mathbf{Z}/6\mathbf{Z}$, so $\varphi(1)$ should have order 1, 2, 3, or 6 in $\mathbf{Z}/9\mathbf{Z}$.

No elements of $\mathbf{Z}/9\mathbf{Z}$ have even order since the cardinality of the group is odd. So either $\varphi(1) = 0$ or $\varphi(1)$ has order 3, for which there are two possibilities, $\varphi(1) = 3$ or $\varphi(1) = 6$.

So we get 3 possible group homomorphisms.

(c) By the same argument, for $\varphi : \mathbf{Z}/9\mathbf{Z} \longrightarrow \mathbf{Z}/6\mathbf{Z}$ we need $\varphi(1)$ to have order 1, 3, or 9 in $\mathbf{Z}/6\mathbf{Z}$. Order 9 is impossible. Order 1 is $\varphi(1) = 0$. Order 3 is $\varphi(1) = 2$ or $\varphi(1) = 4$.

(d) Same argument as above. We need $\varphi(1)$ to have order 1, 2, 3, or 6. Order 1 is $\varphi(1) = 0$. Order 2 is $\varphi(1) = 3$. Order 3 is $\varphi(1) = 2$ or $\varphi(1) = 4$. Order 6 is $\varphi(1) = 1$ or $\varphi(1) = 5$.

So $\varphi(1)$ can be any element of $\mathbf{Z}/6\mathbf{Z}$, and we get 6 different homomorphisms.

(e) Suppose that φ is an automorphism. Let $y \in G$. By the surjectivity of φ, exists $x \in G$ such that $\varphi(x) = y$ and as G is cyclic there exists $n \in \mathbf{Z}$ such that $x = n \cdot g$. Then $y = n \cdot \varphi(g)$ which shows that $\varphi(g)$ is a generator of G. Conversely, now suppose that $\varphi(g)$ is a generator of G. First we show φ is surjective. Given $x \in G$, there exists $n \in \mathbf{Z}$ such that $x = n \cdot \varphi(g)$. Then $\varphi(n \cdot g) = x$ which shows that φ is surjective. Now suppose that $\varphi(g_1) = \varphi(g_2)$. As G is generated by g we can write $g_1 = n \cdot g$ and $g_2 = m \cdot g$ for some $n, m \in \mathbf{Z}$. Then $(n-m) \cdot \varphi(g) = 0$. If G has infinite order then $\varphi(g)$ does as well and so $m = n$ which implies $g_1 = g_2$. If G has finite order, then $\mathrm{ord}(g) = \mathrm{ord}(\varphi(g)) \mid m - n$, which implies $(n-m) \cdot g = 0$ and so $g_1 = g_2$.

(f) By part (e) we must have $\varphi(1)$ as a generator of $\mathbf{Z}$, but there are only two of these, namely ± 1.

(g) We need $\varphi(1)$ to be a generator of $\mathbf{Z}/n\mathbf{Z}$, that is $a \in \mathbf{Z}/n\mathbf{Z}$ such that $\gcd(a, n) = 1$. So the automorphisms of $\mathbf{Z}/n\mathbf{Z}$ are identified with $(\mathbf{Z}/n\mathbf{Z})^\times$.

(h) Fix a primitive root g modulo p. It generates the group $(\mathbf{Z}/p\mathbf{Z})^\times$, and all the generators are of the form g^a for some a with $\gcd(a, p-1) = 1$. So we must put $\varphi(g) = g^a$ for such a. □

8.2. Consider an elliptic curve over the complex numbers $\mathbf{C}$ given by

$$E: \ y^2 = x^3 + ax + b.$$

Let j be the j-invariant of E, that is

$$j = -1728\,\frac{(4a)^3}{\Delta} = 1728\,\frac{4a^3}{4a^3 + 27b^2}.$$

An *automorphism of E* is an isomorphism from E to itself.

(a) Prove that if $j \neq 0, 1728$ then there are exactly 2 automorphisms of E (given by multiplication by $u = \pm 1$).

(b) Prove that if $j = 1728$ then there are exactly 4 automorphisms of E.

(c) Prove that if $j = 0$ then there are exactly 6 automorphisms of E.

Solution. Any automorphism of E is given by a change of variables $x = u^2\hat{x}$, $y = u^3\hat{y}$ for some $u \in \mathbf{C}^\times$. In order for the Weierstrass equation to be preserved we must have $a = u^4\hat{a} = u^4 a$ and $b = u^6\hat{b} = u^6 b$.

Note also, from the expression for j given above, that $j = 0$ iff $a = 0$, and $j = 1728$ iff $b = 0$.

(a) If $j \neq 0, 1728$ then $a \neq 0$ and $b \neq 0$. Therefore from $a = u^4 a$ and $b = u^6 b$ we get that $u^4 = 1$ and $u^6 = 1$, so by dividing we have $u^2 = 1$, which has the two solutions $u = \pm 1$.

(b) If $j = 1728$ then $b = 0$ and $a \neq 0$, so from $a = u^4 a$ we get $u^4 = 1$, which has four complex solutions $e^{2\pi i k/4}$ with $k = 0, 1, 2, 3$.

(c) If $j = 0$ then $a = 0$ and $b \neq 0$, so from $b = u^6 b$ we get $u^6 = 1$, which has six complex solutions $e^{2\pi i k/6}$ with $k = 0, 1, 2, 3, 4, 5$. □

8.3. Let $p > 3$ be a prime number and consider the elliptic curve over $\mathbf{Q}$ defined by

$$E_p: \ y^2 = f(x), \qquad \text{where } f(x) = x^3 + px.$$

We (more precisely: you) will determine all the points of finite order of $E_p(\mathbf{Q})$.

(a) How many real roots does the function $f(x)$ have?

(b) That was too easy. Given a constant $C \in \mathbf{R}$, how many real roots does the function $g(x) = f(x) + C$ have?

[**Hint**: Think about the derivative.]

(c) What are the points of order 2 of $E_p(\mathbf{Q})$?

(d) Use the Lutz–Nagell Theorem to find a complete set of possibilities for y^2, given that $P = (x, y)$ is a point of finite order > 2.

(e) Rule out all the possibilities from part (d) one by one, keeping in mind that $p > 3$.

[**Hint**: Use part (b) in each of the cases.]

(f) What happens if $p = 3$ or $p = 2$?

Solution.

(a) $0 = f(x) = x^3 + px = x(x^2 + p)$ clearly has the unique solution $x = 0$.

(b) We have $g'(x) = f'(x) = 3x^2 + p > 0$ for all $x \in \mathbf{R}$, so $g(x)$ is strictly increasing on $\mathbf{R}$, and it is a cubic polynomial, so it has exactly one real root.

(c) We have $y = 0 = f(x)$ so $x = 0$ from part (a), hence a single point $(0, 0)$ of order 2.

(d) We know that y^2 divides $4a^3 + 27b^2 = 4p^3$, hence $y^2 \in \{1, 4, p^2, 4p^2\}$.

(e) We proceed in order:

- $y^2 = 1$, then $g(x) = f(x) - 1 = x^3 + px - 1 = 0$. By part (b) this has exactly one real root, but $g(0) = -1 < 0$ and $g(1) = p > 0$, so the unique real root is strictly between 0 and 1, hence is not an integer.
- $y^2 = 4$, then $g(x) = f(x) - 4 = x^3 + px - 4 = 0$. Same argument as above, since $g(0) = -4 < 0$ and $g(1) = p - 3 > 0$ by assumption.
- $y^2 = p^2$, then $g(x) = f(x) - p^2 = x^3 + px - p^2 = 0$. Arguing as above, we have $g(0) = -p^2 < 0$ and $g(p) = p^3 > 0$, so $0 < x < p$. But $x^3 + px - p^2 = 0$ forces $p \mid x$, contradiction.
- $y^2 = 4p^2$, then $g(x) = f(x) - 4p^2 = x^3 + px - 4p^2 = 0$. Arguing as above, we have $g(0) = -4p^2 < 0$ and $g(p) = p^3 - 3p^2 = p^2(p-3) > 0$, so $0 < x < p$. But $x^3 + px - 4p^2 = 0$ forces $p \mid x$, contradiction.

We conclude that there are no points of finite order other than $\mathcal{O}$ and $(0, 0)$.

(f) In part (e) we used the assumption $p > 3$ for the cases $y^2 = 4$ and $y^2 = 4p^2$. So these are the only cases we need to check.

- If $p = 2$ and $y^2 = 4$, we have $g(x) = f(x) - 4 = x^3 + 2x - 4 = 0$. Since $g(1) = -1 < 0$ and $g(2) = 8 > 0$, the unique real root is not an integer.
- If $p = 2$ and $y^2 = 4p^2 = 16$, we have $g(x) = f(x) - 16 = x^3 + 2x - 16 = 0$. Since $g(2) = -4 < 0$ and $g(3) = 17 > 0$, the unique real root is not an integer.
- If $p = 3$ and $y^2 = 4$, we have $g(x) = f(x) - 4 = x^3 + 3x - 4 = 0$. The unique solution is $x = 1$, so we get the two points $(1, \pm 2)$. But then we compute

$$[2](1, 2) = \left(\frac{1}{4}, -\frac{7}{8}\right)$$

and conclude by Lutz–Nagell that $[2](1, 2)$ does not have finite order, hence neither do $(1, \pm 2)$.

- If $p = 3$ and $y^2 = 4p^2 = 36$, we have $g(x) = f(x) - 36 = x^3 + 3x - 36$. The unique solution is $x = 3$, so we get the two points $(3, \pm 6)$. As before we compute

$$[2](3, 6) = \left(\frac{1}{4}, \frac{7}{8}\right),$$

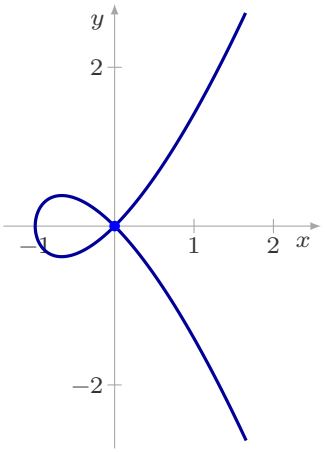
which again shows that the points do not have finite order. □

8.4. [Singularities, revisited] Consider the curves over $\mathbf{R}$ given by the equations

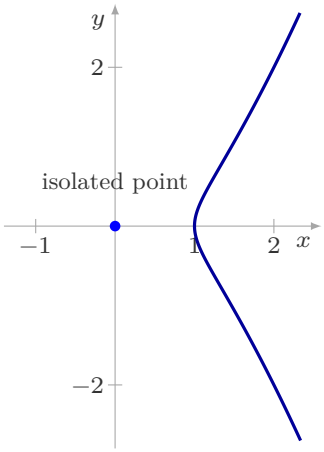
$$C_1 : \ y^2 = x^3 + x^2 = x^2(x + 1) \qquad \text{and} \qquad C_2 : \ y^2 = x^3 - x^2 = x^2(x - 1).$$

(a) Using calculus methods, find all the singular points of C_1 and C_2.

Judging by the equations of C_1 and C_2, we may expect the curves to look somewhat similar. The reality (or perhaps $\mathbf{R}$-ity?) is that they look very different:



$C_1 : \ y^2 = x^3 + x^2$



$C_2 : \ y^2 = x^3 - x^2$

Can we detect this difference algebraically?

Given a curve $C : \ F(x, y) = 0$ that passes through the point $(0, 0)$, the *tangent cone to C at $(0, 0)$* is obtained as follows: write

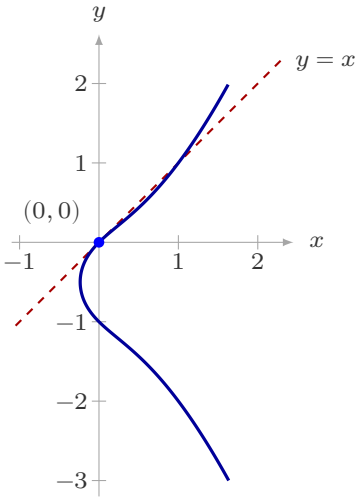
$$F(x, y) = F_m(x, y) + F_{m+1}(x, y) + \cdots + F_d(x, y),$$

where for each $m \leqslant j \leqslant d$, $F_j(x, y)$ contains all the terms of total degree j in $F(x, y)$ and we ask that $F_m(x, y) \neq 0$.
Then the tangent cone is defined by the equation $F_m(x, y) = 0$.

For example, if $F(x, y) = y^2 + y - x^3 - x$, then

$$F_m(x, y) = F_1(x, y) = y - x,$$

so the tangent cone has equation $y - x = 0$ (so it is the line $y = x$).
We can visualise this as in the graph on the right.



$C : \ y^2 + y = x^3 + x$

(b) Compute the equations of the tangent cones of the above two curves C_1 and C_2, and draw them on the same graphs as the curves themselves.

Can you tell from the equations that something is very different (at least if we are working over $\mathbf{R}$) between the two curves?

What if we work over $\mathbf{C}$ instead?

Solution.

(a) Let $F_1(x, y) = y^2 - x^3 - x^2$, then

$$\frac{\partial F_1}{\partial x} = -3x^2 - 2x, \qquad \frac{\partial F_1}{\partial y} = 2y.$$

For a point (x_0, y_0) to be singular we need therefore $-x_0(3x_0 + 2) = 0$ and $2y_0 = 0$, so $(x_0, y_0) = (0, 0)$ or $(-2/3, 0)$. Only the first point lies on the curve, so the only singular point of C_1 is $(0, 0)$.

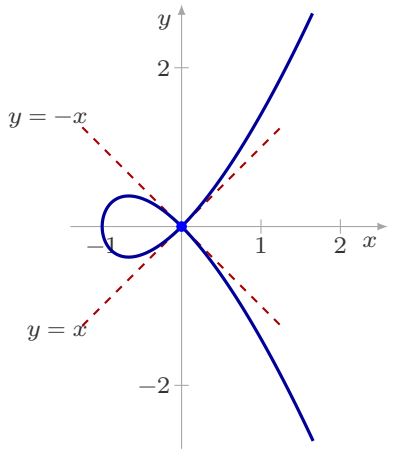
Let $F_2(x, y) = y^2 - x^3 + x^2$, then

$$\frac{\partial F_2}{\partial x} = -3x^2 + 2x, \qquad \frac{\partial F_2}{\partial y} = 2y.$$

Suppose (x_0, y_0) is singular, then $-x_0(3x_0 - 2) = 0$ and $y_0 = 0$, so $(x_0, y_0) = (0, 0)$ or $(2/3, 0)$. Only the first point lies on the curve, so the only singular point of C_2 is $(0, 0)$.

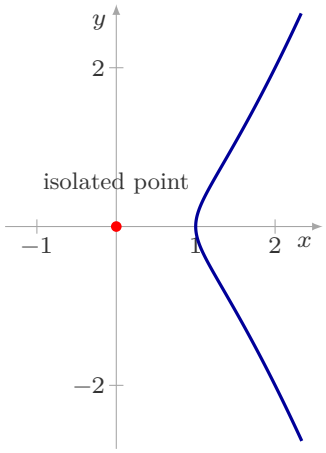
(b) For C_1, the tangent cone is given by $y^2 - x^2 = 0$, which factors as $(y - x)(y + x) = 0$ and is therefore the union of the two lines $y = \pm x$.

For C_2, the tangent cone is given by $y^2 + x^2 = 0$. The graph of this is the single point $(0, 0)$.



$C_1 : \ y^2 = x^3 + x^2$

tangent cone $y^2 - x^2 = 0$: lines $y = \pm x$



$C_2 : \ y^2 = x^3 - x^2$

tangent cone $y^2 + x^2 = 0$: single point $(0, 0)$

The difference is that $y^2 - x^2$ factors over $\mathbf{R}$, but $y^2 + x^2$ does not.

Over $\mathbf{C}$ that difference disappears: $y^2 + x^2 = (y - ix)(y + ix)$, so we again get the union of two lines. □