ALGEBRAIC CURVES
SOLUTIONS SHEET 12

Unless otherwise specified, k is an algebraically closed field.

Exercise 1. Let $a \in k^*$ and consider the elliptic curve E with equation

$$X^3 + Y^3 = aZ^3,$$

and base point $O = [1, -1, 0]$.

(1) Prove that three points on E add to O if and only if they are collinear.
(2) Let $P = [x : y : z] \in E$. Prove $-P = [y : x : z]$.
(3) Prove that E has j-invariant 0.

Solution 1.

(1) We need to show that O is a flex. Indeed, if this is the case, then $\varphi(O, O) = O$, and thus by point (3) of Exercise 3 on Sheet 12 we have $P_1 + P_2 + \varphi(P_1, P_2) = O$ for all $P_1, P_2 \in E$. Thus if $P, Q, R \in E$ are collinear, then $\varphi(P, Q) = R$ and thus $P + Q + R = O$, and conversely, if $P, Q, R \in E$ add to E, then

$$P + Q + R = O = P + Q + \varphi(P, Q)$$

and thus $\varphi(P, Q) = R$, and thus P, Q, R are collinear.

So let us show that O is a flex. We first compute the tangent at O. The partial derivatives of $E = X^3 + Y^3 - aZ^3$ are $E_X = 3X^2$, $E_Y = 3Y^2$ and $E_Z = -3aZ^2$. Evaluating at O (and dividing by 3), we obtain that the tangent is given by $L = X + Y$. To show that O is a flex, we need to show that $I(O, E \cap L) = 3$. To do this, we dehomogenize with $X = 1$, denote $P = (-1, 0)$ and compute

$$\begin{aligned} I(O, E \cap L) &= I(P, (1 + Y^3 - aZ^3) \cap (1 + Y)) \\ &= I(P, (-aZ^3) \cap (1 + Y)) \\ &= 3I(P, Z \cap (1 + Y)) \\ &= 3. \end{aligned}$$

Hence O is a flex and we conclude.

(2) By point (1), if $x \neq y$, it suffices to prove that $P = [x : y : z]$, $Q = [y : x : z]$ and O are collinear. This can be done e.g. by computing that

$$0 = \det \begin{pmatrix} x & y & 1 \\ y & x & -1 \\ z & z & 0 \end{pmatrix},$$

which is straightforward (equivalently, you can see that $p = (x, y, z)$, $q = (y, x, z)$ and $o = (1, -1, 0)$ are linearily dependent, e.g. as $p - q = (x - y)o$). Hence $P + Q + O = O$, i.e. $Q = -P$.

If $x = y$, we need to show that P is 2-torsion, which translates to showing that the tangent at P contains O. One computes that the tangent at P is

$$x^2X + y^2Y - az^2Z,$$

so if $x = y$, then O is on the tangent. Hence also in this case, we have $-P = P = [x : x : z]$.

(3) To compute the j-invariant, we have to put E into Weierstrass normal form with a projective change of coordinates. Replacing X by $X - Y$ and Y by $X + Y$ we obtain the curve

$$\begin{aligned}\widetilde{F} &= (X - Y)^3 + (X + Y)^3 - aZ^3 \\ &= 2X^3 + 6XY^2 - aZ^3.\end{aligned}$$

In the chart $\{Z \neq 0\}$ and dividing by 6, we obtain the equation

$$Y^2 = -\frac{1}{3}X^3 + \frac{a}{6}.$$

This is now in Weierstrass normal form, and as no X appears, we have that $j(E) = 0$.

Exercise 2. Let $O = [0 : 1 : 0]$ be a flex on an irreducible cubic F and $Z = 0$ the tangent line to F at O.

(1) Show that $F = ZY^2 + bYZ^2 + cYXZ +$ terms in X, Z.

(2) Find a projective change of coordinates (using $Y \mapsto Y - \frac{b}{2}Z - \frac{c}{2}X$) to get F to the form

$$ZY^2 = \text{ cubic in } X, Z.$$

(3) Show that any non-singular cubic is projectively equivalent to

$$Y^2Z = X(X - Z)(X - \lambda Z),$$

for a $\lambda \in k$, $\lambda \neq 0, 1$. This is called the Legendre form of an elliptic curve.

Solution 2. (1) As O is a flex with tangent Z, we obtain that $I(O, F \cap Z) = 3$. Dehomogenizing with $Y = 1$ and denoting $P = (0, 0)$, we hence obtain $I(P, F_* \cap Z) = 3$, where F is the dehomogenization of F w.r.t. Y. If we write $F_* = p(X) + ZQ(X, Z)$ for some polynomial p of degree ≤ 3, then we obtain

$$\begin{aligned}3 &= I(P, F_* \cap Z) \\ &= I(P, p(X) \cap Z) \\ &= \text{exponent of monomial of minimal degree in } p.\end{aligned}$$

Hence we obtain $p(X) = p_3X^3$ for some $p_3 \neq 0$, i.e. $F_* = p_3X^3 + ZQ(Z, X)$. As F is irreducible, we have $F = (F_*)^*$, and writing this out gives that F has the form

$$F = aZY^2 + bYZ^2 + cYXZ + \text{terms in } X, Z.$$

We are left to argue that $a \neq 0$ so that we can divide by a. From the above description, we can see that if $a = 0$, then the multiplicity of $P = (0, 0)$ on F_* is at least 2, which contradicts the fact that F is non-singular at O (as we have a unique tangent).

(2) As we have

$$\begin{aligned} Z(Y - \frac{b}{2}Z - \frac{c}{2}X)^2 &= ZY^2 - bYZ^2 - cYXZ + \text{terms in } X, Z, \\ b(Y - \frac{b}{2}Z - \frac{c}{2}X)Z^2 &= bYZ^2 + \text{terms in } X, Z \\ c(Y - \frac{b}{2}Z - \frac{c}{2}X)XZ &= cYXZ + \text{terms in } X, Z, \end{aligned}$$

the claim follows.

(3) Let us admit that F has a flex. Using a projective change of coordinates, we can assume that it is O, and that the tangent is Z. By the previous points, and factoring the cubic on the right hand side of (2) (which isn't divisible by Z as F is irreducible), we obtain that F has the form

$$Y^2Z = a(X - \lambda_1Z)(X - \lambda_2Z)(X - \lambda_3Z)$$

for some $a, \lambda_1, \lambda_2, \lambda_3 \in k$. Scaling Y appropriately we may assume that $a = 1$, and replacing X with $X + \lambda_3Z$ we may assume that $\lambda_3 = 0$. So we arrived at

$$Y^2Z = X(X - \lambda_1Z)(X - \lambda_2Z).$$

Note that one of the λ_i has to be non-zero, as the curve $Y^2Z = X^3$ is singular at $[0 : 0 : 1]$. So replacing Z by Z/λ_i we arrive at

$$Y^2Z = X(X - Z)(X - \lambda Z).$$

To conclude, we need to argue that $\lambda \neq 0, 1$. This is because in the chart $Z \neq 0$, we can write the curve as $Y^2 = X(X-1)(X-\lambda)$, and if $\lambda \in \{0, 1\}$, then the origin is a singular point of this curve. Hence we must have $\lambda \neq 0, 1$.

Remark. To see that F has a flex, you can look at the determinant of the Hessian matrix of F, i.e. the 3×3 matrix whose components are all possible partial derivatives of order 2. One can show that a point on F is a flex if and only if the Hessian is not invertible. As F is a cubic, all partial derivatives of order 2 are linear, and thus the determinant of the Hessian defines a cubic curve as well. By Bézout, F intersects this curve in 9 points, and these are precisely the flexes of F.

Exercise 3. (1) Use Ex. 5.4 to show that given two triples (p_1, p_2, p_3) and (q_1, q_2, q_3) each of distinct points in $\mathbb{P}^1$ there exists a unique projective change of coordinates sending p_i to q_i for $i = 1, 2, 3$.

(2) The *cross-ratio* of four distinct ordered points (p_1, p_2, p_3, p_4) in $\mathbb{P}^1$ is defined as $\lambda \in k \setminus \{0, 1\}$, where λ is the image of p_4 under the unique projective change of coordinates sending (p_1, p_2, p_3) to $(\infty, 0, 1)$.

(3) Show that this defines an action of S_3 on $k \setminus \{0, 1\}$ and the orbit $\mathcal{O}_\lambda$ of $\lambda \in k \setminus \{0, 1\}$ is

$$\mathcal{O}_\lambda = \{\lambda, 1/\lambda, 1 - \lambda, 1/(1 - \lambda), (\lambda - 1)/\lambda, \lambda/(\lambda - 1)\}.$$

Solution 3. (1) By Exercise 4 on Sheet 5, there exists a projective change of coordinates sending (p_1, p_2) to (q_1, q_2). Hence we may assume that $(p_1, p_2) = (q_1, q_2)$, and we need to show that there exists a projective change of coordinates fixing q_1, q_2 and sending p_3 to q_3.

If we write $q_i = [b_i]$ for some column vectors b_i, then as $q_1 \neq q_2$ we have that b_1, b_2 is a basis of k^2. Saying that $A \in k^{2\times 2}$ fixes q_1 and q_2 is equivalent to saying that b_1, b_2 are eigenvectors of A, so if we denote $B = (b_1\ b_2)$, we look for matricies of the form

$$A = BDB^{-1}$$

with D diagonal. That is, we are looking for a diagonal matrix D such that

$$BDB^{-1}a_3 = b_3$$

where $p_3 = [a_3]$, i.e. D sends $B^{-1}a_3$ to $B^{-1}b_3$. Note that $B^{-1}p_1 = B^{-1}q_1 = [1 : 0]$ and $B^{-1}p_2 = B^{-1}q_2 = [0 : 1]$, so as p_3 and q_3 are different from p_1, p_2, we obtain that $B^{-1}a_3$ and $B^{-1}b_3$ don't have entries equal to 0. Therefore, we see that there exists an invertible diagonal matrix D sending $B^{-1}a_3$ to $B^{-1}b_3$. Hence the matrix $A = BDB^{-1}$ gives a projective change of coordinates sending fixing p_1, p_2 and sending p_3 to q_3.

To see unicity, it suffices to treat the case where (p_1, p_2, p_3) and (q_1, q_2, q_3) are equal to $([1 : 0], [0 : 1], [1 : 1])$ (because if $T\colon \mathbb{P}^1 \to \mathbb{P}^1$ sends (p_1, p_2, p_3) to (q_1, q_2, q_3), we can use a projective change of coordinates on the source resp. target sending the triple to $([1 : 0], [0 : 1], [1 : 1])$). Assume that T is given by $A \in k^{2\times 2}$, then we obtain

$$\begin{aligned} T([1 : 0]) &= [1 : 0] \implies A_{21} = 0 \\ T([0 : 1]) &= [0 : 1] \implies A_{12} = 0, \end{aligned}$$

so A is a diagonal matrix. But then $T([1 : 1]) = [1 : 1]$ implies that the values on the diagonal of A agree, i.e. $A = aI_2$ for some $a \in k^*$. Hence $T = \mathrm{Id}$.

(2) Nothing to show :) just note that we identify $\mathbb{P}^1$ with $k \cup \{\infty\}$ such that $a \in k$ corresponds to $[a : 1] \in \mathbb{P}^1$ and $\infty = [1 : 0]$.

(3) Set $p_1 \coloneqq \infty$, $p_2 \coloneqq 0$ and $p_3 \coloneqq 1$. For $\sigma \in S_3$ and $\lambda \in k \setminus \{0,1\}$, we define $\sigma \cdot \lambda$ to be the cross-ratio of $(p_{\sigma^{-1}(1)}, p_{\sigma^{-1}(2)}, p_{\sigma^{-1}(3)}, \lambda)$. To see that this is an action, let T_σ be the unique projective change of coordinates sending $(p_{\sigma^{-1}(1)}, p_{\sigma^{-1}(2)}, p_{\sigma^{-1}(3)})$ to (p_1, p_2, p_3). In other words, we have $T_\sigma(p_i) = p_{\sigma(i)}$ for $i = 1, 2, 3$. Therefore, it follows that

$$T_\tau \circ T_\sigma(p_i) = p_{\tau\circ\sigma(i)} = T_{\tau\circ\sigma}(p_i),$$

so by unicity we have $T_\tau \circ T_\sigma = T_{\tau\circ\sigma}$. Hence we obtain

$$(\tau \circ \sigma) \cdot \lambda = T_{\tau\circ\sigma}(\lambda) = T_\tau \circ T_\sigma(\lambda) = \tau \cdot (\sigma \cdot \lambda).$$

As by unicity we also have $T_{\mathrm{Id}} = \mathrm{Id}$ and so $\mathrm{Id} \cdot \lambda = \lambda$, we conclude that we have a group action of S_3 on $k \setminus \{0,1\}$.

To compute the orbit, we start by computing $(23) \cdot \lambda$ and $(123) \cdot \lambda$. Notice that $T_{(23)}$ is given by mapping $a \mapsto 1 - a$, which corresponds to the projective change of coordinates given by the matrix

$$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix},$$

and $T_{(123)}$ is given by sending $a \mapsto \frac{1}{1-a}$, which corresponds to the projective change of coordinates given by the matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.$$

Hence $(23) \cdot \lambda = 1 - \lambda$ and $(123) \cdot \lambda = 1/(1 - \lambda)$. As S_3 is generated by (23) and (123), one can use this to compute the whole orbit:

$$(132) \cdot \lambda = 1 - \frac{1}{\lambda}, \quad (12) \cdot \lambda = \frac{1}{\lambda}, \quad (13) \cdot \lambda = \frac{\lambda}{\lambda - 1}.$$

Exercise 4. Let E_λ be an elliptic curve given in its Legendre form

$$Y^2 = X(X-1)(X-\lambda),$$

with $\lambda \neq 0, 1$.

(1) Show that the j-invariant is given by

$$j(E_\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

(2) Show that $E_\lambda \cong E_\mu$ if and only if $\mu \in \mathcal{O}_\lambda$.

In fact one can use (2) to find the formula for the j-function, as it is a generator of the fixed field $k(\lambda)^{S_3}$.

Solution 4.

(1) We have to put E_λ into Weierstrass normal form. To this end, we use the change of coordinates $X \mapsto X + \frac{1+\lambda}{3}$, which gives

$$Y^2 = X^3 + \left(\frac{(1+\lambda)^2}{3} - \frac{2(1+\lambda)^2}{3} + \lambda\right) X + \frac{(1+\lambda)^3}{27} - \frac{(1+\lambda)^3}{9} + \lambda\frac{1+\lambda}{3}$$

and thus $a = -(\lambda^2 - \lambda + 1)/3$ and $b = -(2\lambda^3 - 3\lambda^2 - 3\lambda + 2)/27$. Plugging this into the formula

$$j = 1728\frac{4a^3}{4a^3 + 27b^2}$$

then gives that

$$j(E_\lambda) = 2^8\frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

(2) From the above expression and using the description of $\mathcal{O}_\lambda$, it is straightforward to show that if $\mu \in \mathcal{O}_\lambda$, then $j(E_\mu) = j(E_\lambda)$ and thus $E_\mu \cong E_\lambda$; we just plug-in all elements of the orbit into the expression of the j-invariant.

On the other hand, given $\lambda \in k \setminus \{0, 1\}$, we want to show that only elements of $\mathcal{O}_\lambda$ yield the same j-invariant. That is, we want to find the roots of the polynomial

$$F_\lambda(X) = \lambda^2(\lambda - 1)^2(X^2 - X + 1)^3 - (\lambda^2 - \lambda + 1)^3 X^2(X - 1)^2.$$

Indeed, the elements $\mu \in k \setminus \{0, 1\}$ with $j(E_\mu) = j(E_\lambda)$ are precisely the roots of F_λ. As we want to show that the roots are precisely $\mathcal{O}_\lambda$ and the leading coefficient of $F_\lambda(X)$ is $\lambda^2(\lambda - 1)^2$, let us define also

$$\begin{aligned} G_\lambda(X) &= \lambda^2(\lambda - 1)^2 \prod_{\alpha \in \mathcal{O}_\lambda} (X - \alpha) \\ &= (X - \lambda)(X\lambda - 1)(X + \lambda - 1)(X - X\lambda - 1)(X\lambda - \lambda + 1)(X\lambda - X - \lambda). \end{aligned}$$

If we can show that $F_\lambda(X) = G_\lambda(X)$, then we are done. In principle we could just compute this, but here is a slightly smarter way to do it: notice that there is a non-empty open subset $U \subseteq \mathbb{A}^1 \setminus \{0, 1\}$ such that for all $\lambda \in U$, the orbit $\mathcal{O}_\lambda$ has precisely 6 elements. To see this, note that if two expressions in the orbit agree, this gives a quadratic equation for λ, so if we exlude the finitely many solutions to these finitely many equations, we get the desired U. As we computed that all the elements of the orbit give the same j-invariant, we conclude that for $\lambda \in U$, G_λ is a polynomial with 6 simple roots and leading coefficient $\lambda^2(\lambda - 1)^2$, and every root of G_λ is also a root of the degree 6 polynomial F_λ, which also has leading coefficient $\lambda^2(\lambda - 1)^2$. Hence in this case we have $F_\lambda = G_\lambda$. But then, if we define

$F, G \in k[X, Y]$ by

$$F(X,Y) \coloneqq Y^2(Y-1)^2(X^2-X+1)^3 - (Y^2-Y+1)^3X^2(X-1)^2$$
$$G(X,Y) \coloneqq (X-Y)(XY-1)(X+Y-1)(X-XY-1)(XY-Y+1)(XY-X-Y),$$

we obtain by the above argument that $V(F-G)$ contains the non-empty open subset $\mathbb{A}^1 \times U$, and thus $V(F-G) = \mathbb{A}^2$, i.e. $F = G$. This concludes the exercise.