Algebraic curves
Solutions sheet 12

June 6, 2024

Unless otherwise specified, k is an algebraically closed field.

Exercise 1. We recall the setting of the Cayley-Bacharach theorem: $F_1, F_2 \subseteq \mathbb{P}^2_k$ are two plane projective cubics intersecting cubics intersecting in 9 pairwise distinct points $A_i \in \mathbb{P}^2_k,\ 1 \leq i \leq 9$ and G is another cubic containing $A_i,\ 1 \leq i \leq 8$. Show that no 6 points among $\{A_i,\ 1 \leq i \leq 8\}$ lie on a quadric, unless G is a linear combination of F_1, F_2.

Solution 1. $F_1,\ F_2$ cubics. $F_1 \cap F_2 = \{A_1, \ldots, A_9\}$. WLOG assume $A_1, \ldots, A_6 \in Q$ quadric. Then $A_7, A_8 \notin Q$ and define a line L. Consider $B \in Q \setminus \{A_1, \ldots, A_6\}$, $C \in \mathbb{P}^2 \setminus Q \cup L$ and $H = \alpha F_1 + \beta F_2 + \gamma G$ such that $B, C \in H$.
If $H = 0$, $\gamma \neq 0$. Hence G is a linear combination of F_1 and F_2.
If $H \neq 0$, H vanishes on $A_1, \ldots, A_6, B$ hence $Q | H$. Then $\frac{H}{Q}$ vanishes on A_7, A_8 since $F_1 \cap Q = F_2 \cap Q = \{A_1, \ldots, A_6\}$. Hence $H = Q \times L$ and $C \notin H$ which is a contradiction.

Exercise 2. Let $A_1, A_2, A_3, B_1, B_2, B_3$ be pairwise distinct points on an irreducible plane projective quadric $Q \subseteq \mathbb{P}^2_k$. For $(i, j) \in \{(1, 2),\ (2, 3),\ (3, 1)\}$, denote by C_{ij} the intersection point of lines $\overline{A_i B_j}$ and $\overline{A_j B_i}$ (show that these lines intersect in exactly one point). Show that C_{12}, C_{23}, C_{31} are collinear. This result is known as Pascal's theorem.

Solution 2. Define the following cubics :

- $F_1 := \overline{A_1 B_2} \cdot \overline{A_2 B_3} \cdot \overline{A_3 B_1}$
- $F_2 := \overline{A_2 B_1} \cdot \overline{A_3 B_2} \cdot \overline{A_1 B_3}$
- $G := \overline{c_{12} c_{31}} \times Q$

F_1 and F_2 intersect in $A_1, A_2, A_3, B_1, B_2, B_3, c_{12}, c_{31}, c_{23}$. G contains the 8 first points of this list. By Cayley-Bacharach, $c_{23} \in G$. But $c_{23} \notin Q$ otherwise $\sharp Q \cap F_1 > 6$ and $Q \mid F_1$ which cannot be the case since Q is irreducible. Hence $c_{23} \in \overline{c_{12} c_{31}}$.

Exercise 3. Let (E, O) be an elliptic curve.

1. Show that the addition defined in class has neutral element O and that any point $P \in E$ has a (unique) inverse $-P$ (you may assume associativity of $+$ to prove uniqueness of the inverse).
2. Show that $+$ is commutative.

If we further assume that $+$ is associative, $(E,+,O)$ is an abelian group. Consider $O \neq O' \in E$ and $Q = \varphi(O,O')$. We define $\alpha : E \to E$ by $\alpha(P) = \varphi(Q,P)$.

3. Show that for $P_1, P_2 \in (E,+,O)$, $P_1 + P_2 + \varphi(P_1,P_2) = \varphi(O,O)$.

4. Show that $\alpha : (E,+,O) \to (E,+,O')$ is a group isomorphism.

Therefore, the group structure on E does not depend on the choice of O.

Solution 3.

1. Neutral. Let $L := \overline{O\phi(O,A)}$. Then $E.L = O + A + \phi(O,A)$. Hence $\phi(O,\phi(O,A)) = A$.

   Inverse. $-A := \phi(A,\phi(O,O))$. Indeed, let $B = \phi(A,\phi(O,O))$. $\phi(A,B) = \phi(O,O)$.

2. Commutativity. $\phi(A,B) = \phi(B,A)$.

3. Let $P,Q \in E$. Then $P + Q + \phi(P,Q) = \phi(O,\phi(P+Q,\phi(P,Q))) = \phi(O,O)$ because $\phi(P+Q,\phi(P,Q)) = \phi(\phi(P,Q),\phi(O,\phi(P,Q))) = O$.

4. $\alpha(P_1+P_2) = O' - P_1 - P_2$ and $\alpha(P_1) +' \alpha(P_2) = \phi(O',\phi(\alpha(P_1),\alpha(P_2)) = \phi(O,O) - O' - (\phi(O,O) - \alpha(P_1) - \alpha(P_2)) = \alpha(P_1) + \alpha(P_2) - O' = O' - P_1 - P_2$.

Exercise 4. Let E,O be an elliptic curve. We say that an element x in an abelian group $(G,+)$ is p-torsion ($p \in \mathbb{Z}$) if $p \cdot x = \underbrace{x + \ldots + x}_{p \text{ times}} = 0$.

A simple point $P \in E$ with tangent line L is called a flex if $I(P, E \cap L) > 2$. We admit that, if $char(k) = 0$, any nonsingular cubic has 9 distinct flexes (see Fulton, Problem 5.23). Suppose $char(k) = 0$ and O is a flex.

1. Show that flexes are exactly 3-torsion points of E and that they form a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

2. Let $P \in E$. How many lines through P are tangent to E at some point $P \neq Q \in E$? (Hint: show that $P + 2Q = O$ and use exercise 5.)

Solution 4.

1. If P is a flex, the tangent of E at P intersects P only in P, hence $\phi(P,P) = P$. $2P = \phi(O,O) - P = -P$ (O is a flex). Hence $3P = O$.

   Conversely, if $3P = O$, $\phi(P,P) = -2P = P$ hence P is a flex.

   We admit that E has 9 distinct ordinary flexes. Since all flexes are $3-$torsion, their group structure is $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

2. Suppose the tangent to Q goes through P ($P \neq Q$). Then $P + 2Q = O$. Since $2-$torsion points form a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $P \mapsto 2P$ is surjective (ex 5), there are 4 Q's such that $P + 2Q = O$. P is a flex iff P is one of them, so the number of Q's such that the tangent at Q goes through P and $P \neq Q$ is 3 if P is a flex and 4 otherwise.

Exercise 5. Let (E,O) be an elliptic curve. Suppose $char(k) = 0$ and O is a flex (for the definition of flex, see exercise 4).

1. Show that $P \in E$ is 2-torsion if, and only if, the tangent to E at P passes through O. (See exercise 4 for the definition of torsion points.)

We may assume that $E = Y^2Z - X(X-Z)(X-\lambda Z)$ and $O = [0:1:0] \in E$, where $\lambda \neq 0, 1$ (see Fulton, Problem 5.24).

2. Find 2-torsion points of E. Draw a real picture. Show that 2-torsion points of E form a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. Show that the endomorphism $P \mapsto 2P$ of E is surjective. (Hint: if $2P \neq O$, find an explicit expression for the coordinates of $2P$ depending on coordinates of P.)

Solution 5.

1. P is $2-$torsion $\iff 2P = 2P + O = O \iff \phi(P,P) = O$.

   $E \setminus O$ is contained in the affine chart $z \neq 0$. A line in the $(x,y)-$plane passes through $[0:1:0]$ iff it is vertical.

   Tangent to E : $y^2 - x(x-1)(x-\lambda) = y^2 - \mathcal{P}(x)$. At P, L : $-\mathcal{P}'(x_P)(x-x_P) + 2y_P(y-y_P) = 0$.

   L is vertical $\iff y_P = 0 = \mathcal{P}(x_P) \iff x_P \in \{0,1,\lambda\}$, $y_P = 0 \iff P$ is $2-$torsion. There are 4 $2-$torsion points hence they form a group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$.

2. If P is not $2-$torsion, $y_P \neq 0$, L has equation $y - y_P = \nu(x - x_P)$, $\lambda = \frac{\mathcal{P}'(x_P)}{2y_P}$. Adding that $y^2 = \mathcal{P}(x)$, get

$$2y_P(y-y_P) + (y-y_P)^2 = \mathcal{P}'(x_P)(x-x_P) + \frac{1}{2}\mathcal{P}''(x_P)(x-x_P)^2 + (x-x_P)^3$$

   Hence if $x \neq x_P$, $\nu^2 = 3x_P - (\lambda+1) + x - x_P$ and $x_{2P} = \nu^2 + \lambda + 1 - 2x_P$ (rational fraction of degree 1 in P hence surjective in k alg closed). y is determined up to sign by x and $y_{-P} = -y_P$ since the line through $(x_P, y_P), (x_P, -y_P)$ is vertical for non $2-$torsion points. We deduce from this that $P \mapsto 2P$ is surjective.