AMPLIACIÓ DE GEOMETRIA. FME 2009-2010

Exercici d'avaluació continuada 4

Tema: Estructura de grup de la cúbica llisa

Entrega prevista per al 7 de maig de 2010

Bibliografia proposada:

W. Fulton, *Algebraic Curves*, Cap. V.6.
M. Reid, *Undergraduate Algebraic Geometry*, Chap. I.2.
E. Brieskorn and H. Knörrer, *Plane Algebraic Curves*, 7,4, pàg. 306.

Requisits mínims:

L' objectiu és provar que una cúbica plana projectiva no singular admet una estructura de grup.

Definicions. Sigui C una cúbica plana projectiva no singular. Donats p, $q \in C$ sigui L la recta que passa per p i q, aleshores:

$$L \cdot C = p + q + r\,,$$

amb $p = r$ ó $q = r$ si L és la recta tangent a C en p o en q, respectivament.

Definim $\varphi : C \times C \longrightarrow C$ per $\varphi(p, q) = r$. Fixem ara $o \in C$ i definim una addició, $\oplus$, sobre C de la manera següent:

$$p \oplus q \ = \varphi(o, \varphi(p, q))\,.$$

1. Proveu que C amb l'operació $\oplus$ és un grup abelià, considerant o com element neutre.

2. Sigui $o' \in C$ un altre punt i definim l'addició $\oplus'$

$$p \oplus' q = \varphi(o', \varphi(p, q))\,.$$

Sigui $r = \varphi(o, o')$ i definim

$$\begin{aligned} \alpha :\ (C, o, \oplus) \ &\longrightarrow (C, o', \oplus') \\ p \ &\longmapsto \varphi(p, r)\,. \end{aligned}$$

Proveu que α és un isomorfisme de grups. Deduïu-ne que l'estructura de grup és independent del punt o.

3. Sigui C una cúbica projectiva lisa amb un punt d'inflexió fixat, O, com a element neutre. Proveu que:

(1) Tres punts de E estan alineats si i només si la seva suma és zero.
(2) Els punts d'inflexió són exactament el subgrup de 3-torsió de $E(\mathbb{C})$ i aquest subgrup és isomorf a $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (recordeu que un element, x, d'un grup és es diu de n-torsió si $nx = 0$). La recta que uneix dos punts d'inflexió talla a la corba en un altre punt d'inflexió.
(3) La 2-torsió es isomorfa a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
(4) Donat $p \in E$, calculeu el nombre de rectes tangents a E que passen per p.
(5) Si $p_1, \ldots, p_{3n}$ són $3n$ punts diferents d'una corba el·líptica, proveu que $p_1 \oplus \cdots \oplus p_{3n} = 0$ si i només si existeix una corba de grau n que talla a la corba en $p_1, \ldots, p_{3n}$ (Indicació: Useu inducció).

Treball complementari:

4. Si $27B^2 + 4A^3 \neq 0$ considerem, C, la corba el·líptica $y^2 = x^3 + Ax + B$ amb element neutre el punt d'inflexió $[0 : 1 : 0]$.

(1) Si $p_1 = (x_1, y_1)$ i $p_2 = (x_2, y_2)$ són dos punts diferents de C proveu que el punt $p_1 \oplus p_2$ té coordenades $(\mu^2 - x_1 - x_2, 3x_1\mu + y_2 - 2y_1 - \mu^3)$ on $\mu = \frac{y_2 - y_1}{x_2 - x_1}$.
(2) Si $p_1 = (x_1, y_1)$ és un punt de C trobeu $2p_1$.
(3) Trobeu quatre solucions racionals de l'equació diofàntica $y^2 = x^3 + 7x + 1$.