Tema 7. Curvas de géneros 0 y 1. Curvas elípticas.

7.1. La estructura de grupo. Interpretación geométrica.

Trabajaremos en el plano proyectivo $\mathbf{P}_2(\mathbf{k})$ sobre un cuerpo base algebraicamente cerrado. Recordemos del primer parcial los siguientes hechos: una cúbica proyectiva no singular es siempre birracionalente equivalente a una dada por una ecuación del tipo

$$\mathcal{C} : Y^2Z = X^3 + AXZ^2 + BZ^3, \;\; A, B \in \mathbf{k}.$$

Fijado un punto cualquiera de una tal curva $\mathcal{C}$ (pongamos $E = (0 : 1 : 0)$, que es el único punto de $\mathcal{C}$ fuera de U_3), se puede dotar de una estructura de grupo a la curva de la siguiente forma: dados P y Q en $\mathcal{C}$, denominamos $P * Q$ al tercer punto de corte (bien definido siempre) de $\mathcal{C}$ y la recta PQ. Entonces definimos

$$P + Q = E * (P * Q).$$

Esta operación es conmutativa, el elemento neutro es el propio E y además verifica que, si P y Q están en la pieza afín de $\mathcal{C}$ en U_3 y tienen sus coordenadas en un subcuerpo $L \subset \mathbf{k}$, otro tanto se puede decir de $P + Q$, con lo cual la estrucutra de grupo se puede extender a los puntos de $\mathcal{C}$ con coordenadas afines en $\mathbf{A}^2(L)$.

7.2. El grupo $\mathrm{Pic}^0\mathcal{C}$.

Teorema de Riemann–Roch para curvas elípticas. Sea $\mathcal{C}$ una curva de género 1 irreducible. $D \in \mathrm{div}(\mathcal{C})$. Entonces

$$d(D) = \begin{cases} 0 & \text{si } \mathrm{grado}(D) < 0. \\ 1 & \text{si } \mathrm{grado}(D) = 0. \\ \mathrm{grado}(D) & \text{si } \mathrm{grado}(D) < 0. \end{cases}$$

Definición.– Una curva elíptica es un par $(\mathcal{C}, E)$ formado por una curva plana proyectiva de género 1 no singular, $\mathcal{C}$, y un punto fijado $E \in \mathcal{C}$.

Definición.– En las condiciones anteriores, denotamos $\mathrm{Pic}(\mathcal{C})$ el conjunto de los divisores en $\mathcal{C}$ módulo la relación de equivalencia "ser linealmente equivalente".

Este conjunto hereda de manera natural una estructura de grupo donde, además, se puede definir de manera consistente (y obvia) la noción de grado. Además, el conjunto

$$\mathrm{Pic}^0(\mathcal{C}) = \left\{ \overline{D} \in \mathrm{Pic}(\mathcal{C}) \mid \mathrm{grado}(\overline{D}) = 0 \right\}$$

es un subgrupo de $\mathrm{Pic}(\mathcal{C})$.

Proposición.– Existe una biyección entre los puntos de $\mathcal{C}$ y las clases de $\mathrm{Pic}^0(\mathcal{C})$, dada por

$$P \in \mathcal{C} \longmapsto \overline{D_P} = \overline{P - E}, \;\; \overline{D} \in \mathrm{Pic}^0(\mathcal{C}) \longmapsto P_D,$$

donde P_D es el único punto[1] de $\mathcal{C}$ que verifica $D + E \equiv P$.

Corolario.– El conjunto de los puntos de la curva $\mathcal{C}$ puede dotarse de estructura natural de grupo, definiendo, para $Q, R \in \mathcal{C}$,

$$Q + R = P_{\overline{D_Q} + \overline{D_P}}.$$

Este grupo es abeliano y tiene a E como elemento neutro. En lo sucesivo, para evitar confusiones, notaremos $[2]Q$ al punto obtenido sumando Q a sí mismo y reservaremos la notación $2Q$ para el divisor.

[1] Obviamente P_D depende de la clase $\bar{D}$, no de D propiamente dicho.

7.3. Forma normal de Weierstrass.

Proposición 1.– Toda curva de género 1 es birracionalmente equivalente a una de ecuación afín

$$Y^2 + a_1XY + a_3Y = a_0X^3 + a_2X^2 + a_4X + a_6, \text{ con } a_i \in \mathbf{k}.$$

Proposición 2.– Toda curva dada por una ecuación como la anterior es isomorfa por un cambio de variables a una de la forma

$$Y^2 = X^3 + AX + B, \text{ con } A, B \in \mathbf{k}.$$

Esta ecuación se llama forma normal (breve) de Weierstrass de la curva.

Proposición.– Para una curva de género 1 dada en forma normal de Weierstrass, las operaciones internas definidas en 7.1. y en 7.2. son iguales.

Observación.– Para una curva dada en forma normal de Weierstrass, se definen los siguientes números:

$$\Delta = 4A^3 + 27B^2, \;\; j = \frac{4 \cdot 1728 \cdot A^3}{\Delta}.$$

$\Delta \neq 0$ si y sólo si la curva es no singular. Dos curvas en forma normal de Weierstrass son isomorfas mediante cambios de variables lineales si y sólo si tiene el mismo número j.

7.4. El Teorema de Mordell-Weil. Torsión y rango.

De los resultados anteriores, observamos que toda curva elíptica es birracionalmente equivalente a una en forma normal de Weierstrass, $\mathcal{C}$, con elemento neutro $E = (0 : 1 : 0)$. En estas condiciones, los puntos de coordenadas racionales de la pieza afín $\mathcal{C} \cap U_3$ junto con E también tienen estructura de grupo, como se reseñó en 7.1. Este grupo se suele denotar $\mathcal{C}(\mathbf{Q})$.

Teorema de Mordell–Weil.– El grupo $\mathcal{C}(\mathbf{Q})$ está finitamente generado.

Corolario.– $\mathcal{C}(\mathbf{Q}) = \mathcal{C}_T \oplus \mathcal{C}_L$, donde

$$\mathcal{C}_T = \{P \in \mathcal{C} \mid \exists m \in \mathbf{Z} \text{ con } [m]P = E\}, \;\; \mathcal{C}_L \simeq \mathbf{Z}^r.$$

7.5. Cálculo efectivo de la torsión racional.

En toda esta sección $\mathcal{C}$ será una curva elíptica dada en su forma normal de Weierstrass. En concreto, podemos suponer $A, B \in \mathbf{Z}$.

Teorema de Mazur.– $\mathcal{C}_T$ es de una de las siguientes formas:

$\mathbf{Z}/\mathbf{Z}n$	para $n = 1, 2, ..., 10, 12.$
$\mathbf{Z}/\mathbf{Z}2 \times \mathbf{Z}/\mathbf{Z}2n$	para $n = 1, 2, 3, 4.$

Teorema de Nagell–Lutz.– Si $P(a, b) \in \mathcal{C}_T$, entonces $a, b \in \mathbf{Z}$ y, o bien $[2]P = E$, o bien $b^2 | \Delta$.

Teorema de reducción módulo p.– Sea p un primo tal que

(i) p no divide a Δ.

(ii) No existen puntos de orden p en $\mathcal{C}_T$.

Consideremos entonces

$$\mathcal{C}_p = \left\{(a, b) \in \mathbf{A}^2(\mathbf{F}_p) \mid b^2 = a^3 + Aa + B\right\},$$

que tiene estructra de grupo por lo visto en 7.1. Se tiene que $\mathcal{C}_T \hookrightarrow \mathcal{C}_p$.