Lecture 6 The group of divisors

Recall that $\mathrm{Spec}(R)$ is the set of prime ideals $\mathfrak{p} \subseteq R$..

A discrete valuation ring is a PID $\mathcal{O}$ s.t. $|\mathrm{Spec}(\mathcal{O})| = 2$, so

$$\mathrm{Spec}(\mathcal{O}) = \{\{0\}, \mathfrak{m}\}, \qquad \{0\} \neq \mathfrak{m}.$$

Thus we may pick $t \in \mathfrak{m}$ s.t. $\mathfrak{m} = t\mathcal{O}$ and we call t a local parameter. Clearly PID $\Rightarrow$ UFD, so $\forall\, x \in \mathcal{O}$, $x \neq 0$,

$$x = u t^{\nu(x)}$$

where $x \in \Omega^X$ and $\nu(x) \in \mathbb{Z}_{\geq 0}$. Hence the map

$$F^{X} \longrightarrow \mathbb{Z}$$

$$x \longmapsto \nu(x)$$

where F is the field of fractions of Ω, is clearly a group homomorphism. It is known as the *valuation map*.

We'll show how these things help us get geometric information at the points $P \in C$ where C is one-dimensional.

Example Let $\alpha \in K$. Then

$$\mathcal{O} := \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x] \text{ s.t. } g(\alpha) \neq 0 \right\}$$

is a DVR with maximal ideal

$$\mathfrak{m} := \left\{ \frac{f(x)}{g(x)} \in \mathcal{O} \;\middle|\; f(\alpha) = 0 \right\};$$

we may view $\mathcal{O}$ as the ring of "nice" functions $\mathcal{O}_{\mathbb{A}^1, P}$ of $\mathbb{A}^1$ at $P = \alpha$.

For each $r(X) \neq 0$ in the field of fractions $F = K(X)$ of Ω we may write

$$r(X) = u(X)\,(X-\alpha)^n,$$

where $u(X) \in \Omega^X$ and $n = v(r(X))$, so $r(X)$ has zero (resp. pole) of order n (resp. $-n$) if $n > 0$ (resp. $n < 0$).

Given a projective variety $V \subseteq \mathbb{P}^m$ and $P \in V$, the ring of regular functions $\mathcal{O}_{V,P}$ of V at P is the localisation

$$\mathcal{O}_{V,P} := K[V \cap \mathcal{U}_r]_P ,$$

where $\mathcal{U}_r$ is the image of an embedding

$$\begin{array}{ccc} \mathbb{A}^m & \xrightarrow{\nu_r} & \mathbb{P}^m \\ (x_1, \dots, x_m) & \longmapsto & (x_1 : \dots : x_{r-1} : 1 : x_{r+1} : \dots : x_m) \end{array}$$

s.t. $P \in \mathcal{U}_r$.

Propn Let C be projective curve. Then for each smooth $P \in C$ the ring $\mathcal{O}_{C,P}$ is a DVR.

Defn If C is a smooth curve, the divisor (f) of a given $f \in \overline{K}(C)^\times$ is

$$(f) := \sum_{P \in C} \nu_P(f)\, e_P \in \mathrm{Div}^0_C$$

where $\mathrm{Div}_C := \langle C \rangle_{\mathbb{Z}} = \left\{ \sum_{P \in C} n_P e_P \;\middle|\; \text{almost all } n_P = 0 \right\}$ and

$$\mathrm{Div}_C^0 := \left\{ \sum_{P \in C} n_P e_P \in \mathrm{Div}(C) \;\middle|\; \sum_{P \in C} n_P = 0 \right\}.$$

We have a group homomorphism

$$\begin{aligned} \overline{K}(C)^\times &\xrightarrow{\Psi} \mathrm{Div}_C^0 \\ f &\longmapsto (f) \end{aligned}$$

Let Pic_C^0 denote its cokernel, i.e.

$$\mathrm{Pic}_C^0 := \mathrm{Div}_C^0 / \mathrm{Im}(\Psi).$$

Thm Suppose that we happen to have a point $P_0 \in C(k)$.

Then the canonical map

$$\begin{array}{ccc} C & \longrightarrow & \mathrm{Pic}^0_C \\ P & \longmapsto & \ell_P - \ell_{P_0} \end{array}$$

is an embedding defined over K.

Given $D \in \mathrm{Div}_C$ we have a k-vector space

$$\mathcal{L}(D) := \left\{ f \in k(C)^{\times} \;\middle|\; (f) + D \geq 0 \right\} \cup \{0\}.$$

We say that C is an *elliptic curve* if

(0) $\exists\ P_0 \in C(k)$

and either of the following two equivalent conditions hold

(1) $\forall\, n \in \mathbb{Z}_{>0} : \dim_k \mathcal{L}(n\, e_{P_0}) = n$,

(2) the embedding $(\bigstar)$ is an isomorphism.

So for C as above we have

$$\mathcal{L}(1 \cdot e_{P_0}) = k$$

$$\mathcal{L}(2 \cdot e_{P_0}) = k \oplus kx,$$

$$\mathcal{L}(3 \cdot e_{P_0}) = k \oplus kx \oplus ky$$

$$\mathcal{L}(4 \cdot e_{P_0}) = k \oplus kx \oplus ky \oplus kx^2$$

$$\mathcal{L}(5 \cdot e_{P_0}) = k \oplus kx \oplus ky \oplus kx^2 \oplus kxy$$

$$\mathcal{L}(6\, e_{P_0}) = k \oplus kx \oplus ky \oplus kx^2 \oplus kxy \oplus k \begin{cases} x^3 \\ y^2 \end{cases}$$

$\therefore \{1, x, y, x^2, xy, x^3, y^2\}$ is linearly dependent.

Therefore $\exists\ a_1, a_2, a_3, a_4, a_6 \in K$ s.t.

$$y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

which is known as a *Weierstraß equation* for C.

If we replace condition (0) by

(0') $\exists\ P_0 \in C(K')$, for some algebraic field extn K'/K

then we say that C is just a *genus one curve*.

Example (Selmer*) The plane cubic curve $C \subseteq \mathbb{P}^2$ over $K = \mathbb{Q}$ defined by the eq'n

$$3x^3 + 4y^3 + 5z^3 = 0$$

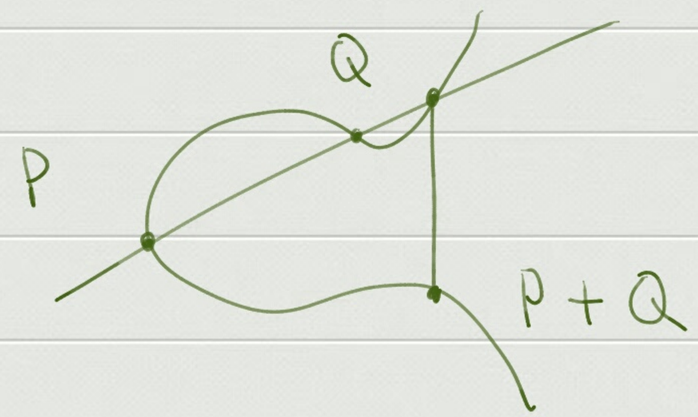
Fails (0) but satisfies (0') as well as (1) and thus (2).

So $C/\mathbb{Q}$ is just a genus one curve — not an elliptic curve.

---

* Selmer, E., *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Mathematica 85 (1951) pp 203-362.

If E is an elliptic curve over K, then the bijection $(\star)$ gives E a group structure. Later we'll show that this group structure is the same as the one from the construction



The coordinates of $P+Q$ may be easily computed once we have a Weierstraß eqn for E.