# Elliptic Curves - Assignment 1

Matteo Durante, s2303760, Leiden University

22nd February 2019

**Exercise 2**

($b$) Consider the following system of equations:

$$\begin{cases} y^2 = x^3 + 2x^2 \\ y = \lambda x \end{cases} \quad \begin{cases} x^3 + (2-\lambda^2)x^2 = x^2(x + (2-\lambda^2)) = 0 \\ y = \lambda x \end{cases}$$

The second order equation in $x$ has solutions given by 0 and $\lambda^2 - 2$ and, since $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$, $2 - \lambda^2 \neq 0$ for $\lambda \in \mathbb{Q}$, thus the only solution $\neq (0,0)$ of the system of equations is $P_\lambda = (\lambda^2 - 2, \lambda^3 - 2\lambda)$.

($c$) Notice that, as $\lambda \in \mathbb{Q}$ varies, we get every point of $C$ (except for those with $x = 0$) as a solution of the previous system of equations.

Indeed notice that, if $x = 0$, then $y = 0$ for any point in $C$. This means that, given $P = (a, b) \in C \setminus (0,0)$, $a \neq 0$. Then, since $a, b \in \mathbb{Q}$, $b/a \in \mathbb{Q}$ and thus $(a, b) = P_\lambda$ for a unique $\lambda = b/a \in \mathbb{Q}$.

Now, since each $\lambda \in \mathbb{Q}$ locates a unique $P_\lambda \in C \setminus (0,0)$ (the one s.t. $b/a = \lambda$), we may parametrize bijectively the $\mathbb{Q}$-rational points in $C$ through the following function:

$$f : \mathbb{P}^1_{\mathbb{Q}} \to C$$
$$(\lambda : i) \mapsto \begin{cases} ((\lambda/i)^2 - 2, (\lambda/i)^3 - 2(\lambda/i)) \ \textit{if } i \neq 0 \\ (0,0) \ \textit{otherwise} \end{cases}$$

**Exercise 3**

($b$) Consider the polynomial $g(x, y) = f(x) - y^2$, $f(x) \in \mathbb{K}[x]$. It is s.t. $\nabla g = (f'(x), -2y)$. Since an affine curve $C$ is s.t. $\dim C = 1$, it is smooth at $P \in C$ if and only if $\nabla g(P) \neq (0,0)$, i.e. if and only if it has rank $2 - 1 = 1$.

Now, given $P \in C$, $\nabla g(P) = (0,0)$ if and only if $f'(p_1) = -2y(p_2) = 0$, which combined with $g(P) = 0$ is equivalent to $f(p_1) = f'(p_1) = 0, p_2 = 0$, i.e. $p_1 \in \overline{\mathbb{K}}$ is a multiple root of $f(x)$ and the second coordinate is 0. This means that such a curve presents a singular point if and only if $f(x)$ has a multiple root over $\overline{\mathbb{K}}$.

($c$) We know that $f(x) = x^3 + ax + b$ defines a smooth curve $C$ if and only if it is separable. i.e. it doesn't have a multiple root. This is equivalent to $\Delta(f) \neq 0$. Remember that $\Delta(f) = (-1)^{\frac{3\cdot 2}{2}} Res(f, f') = -Res(f, f') = -Res(f', f)$.

Let $char(\mathbb{K}) = 3$. Then, $f'(x) = a$.

If $a = 0$, $f(x) = x^3 + b = (x + \sqrt[3]{b})^3$ has a triple root, $\sqrt[3]{b}$, and $4a^3 + 27b^2 = 4 \cdot 0 + 0 \cdot b^2 = 0$.

If $a \neq 0$, $Res(f', f) = a^3 \neq 0$ and $4a^3 + 27b^2 = 4a^3 \neq 0$.

Let $char(\mathbb{K}) \neq 2,3$. Then, $f'(x) = 3x^2 + a$ has roots $\pm\sqrt{-\frac{a}{3}}$. It follows that $Res(f', f) = 3^3 \cdot f(\sqrt{-\frac{a}{3}}) \cdot f(-\sqrt{-\frac{a}{3}}) = 3^3(-\frac{a}{3}\sqrt{-\frac{a}{3}} + a\sqrt{-\frac{a}{3}} + b)(\frac{a}{3}\sqrt{-\frac{a}{3}} - a\sqrt{-\frac{a}{3}} + b) = 4a^3 + 27b^3$, hence $f(x)$ has a multiple root if and only if $4a^3 + 27b^2 = 0$.

**Exercise 6**

$(b)$ Let $a \in \mathbb{K}^*$. Then, since $v$ is a group homomorphism, $v(a^{-1}) = -v(a)$, thus for any $a \in R_v \setminus \{0\}$ we have that $v(a) = 0$ implies $v(a^{-1}) = 0$ and therefore $a^{-1} \in R_v$, i.e. $a \in R_v^*$, while $v(a) > 0$ implies $v(a^{-1}) < 0$ and $a^{-1} \notin R_v$.

Observe that $v(-a) = v(a) + v(-1) = v(a)$ for every $a \in \mathbb{K}$.

Let $a, b \in R_v \setminus \{0\}$ and suppose $v(a) \geq v(b)$. Then, $v(ab^{-1}) = v(a) - v(b) \geq 0$, thus $ab^{-1} \in R_v$ and, since $a = a(b^{-1}b) = (ab^{-1})b$, $a \in (b)$. This implies that $R_v$ is a PID, as every non-zero ideal is generated by its element of lowest norm, which exists because $v(\mathfrak{a}) \subset \mathbb{N}$ is bounded below for every non-zero ideal $\mathfrak{a}$ of $R_v$.

Consider now $\mathfrak{m} = \{0\} \cup \{a \in R_v \mid v(a) > 0\}$ and take $a, b \in \mathfrak{m}$, $c \in R_v$. Since $v(a - b) \geq \min\{v(a), v(-b)\} > 0$ and $v(ac) = v(a) + v(c) \geq v(a) > 0$, $a - b, ac \in \mathfrak{m}$. It follows that $\mathfrak{m}$ is a proper ideal of $R_v$, hence it is principal. Furthermore, it contains every non-invertible element of $R_v$, which will then be local with maximal ideal $\mathfrak{m}$.

Let $\pi \in \mathfrak{m}$ be s.t. $v(\pi) = 1$. Any element $a \in \mathfrak{m}$ has norm $\geq 1$, thus by what we observed $a \in (\pi)$ and we are done.

$(c)$ As stated earlier, every non-zero ideal $\mathfrak{a} \subset R_v$ is principal and generated by its element of lowest norm. Let $(a) = \mathfrak{a}$. Then, for some $n \in \mathbb{Z}_{n \geq 0}$, $v(a) = n = v(\pi^n)$ and therefore, by previous observations, $a \in (\pi^n)$, but at the same time $\pi^n \in (a)$. It follows that $\mathfrak{a} = (\pi^n)$.