Lecture 07

Jose Capco (jcapco@risc.jku.at)

We first define some notation and make adjustment to old usage of some. In this lecture and henceforth, when we work with elliptic curves we use the following definitions and notations

Notations and Definitions.

- K is an arbitrary field not necessarily algebraically closed, it's algebraic closure is denoted $\bar{K}$.
- $\mathbb{A}^2(K)$ and $\mathbb{P}^2(K)$ is the affine and projective plane respectively (we define this later). So $\mathbb{P}$ will not be used for the set of prime numbers anymore. If K is clear, we drop it and write $\mathbb{A}^2$ and $\mathbb{P}^2$.
- The letters $x, y, z, \ldots$ is reserved for indeterminates and letters $P, Q, R, \ldots$ used for points in $\mathbb{A}^2$ or $\mathbb{P}^2$ and their coordinates are written as $(p_1, p_2), \cdots \in \mathbb{A}^2$ or $(p_0 : p_1 : p_2), \cdots \in \mathbb{P}^2$.
- For any polynomial in $K[x, y, z]$ or $K[x, y]$ by the degree we mean its *total degree*.

We start by some historical remark on elliptic functions and elliptic curves.

Historical and Etymological Remarks.

- Real-valued functions (of x) of the form

$$\int_a^x \frac{1}{\sqrt{P(t)}}dt \qquad \int_a^x \sqrt{P(t)}dt$$

  for cubic and quartic polynomials $P(t)$ were being studied in 1700's (e.g. by Fagnano).
- For specific $P(t)$ these integrals are called *elliptic integrals*, because it arises when computing the arclength of san ellipse.
- By proper restriction, elliptic integrals are bijective and Abel showed in the 1820's that their inverses can be continued meromorphically in the whole of the complex plane. These inverse functions are called *elliptic functions*.
- An elliptic function is periodic function on the real line, but there is also a *complex period*. Thus, these functions are also called *doubly-periodic functions* and can be fully defined in a lattice of $\mathbb{C}$.
- The set of elliptic functions defined over a lattice L is a subfield of the meromorphic functions. One can show that this field is $\mathbb{C}(\wp_L) + \wp_L{}'\mathbb{C}(\wp_L)$ were $\wp_L$ is the *Weierstrass $\wp$-function* defined over a lattice $L \subset \mathbb{C}$.
- There is an irreducible cubic polynomial $f(x, y) \in \mathbb{C}[x, y]$ such that $f(\wp, \wp') \equiv 0$. This lead to the name *elliptic curve*. They are just any smooth plane cubic curve defined over a field.

To elaborate a little the above remarks:

Recall that a (additive) subgroup L of $\mathbb{C}$ is called a *lattice* if there are $\mathbb{R}$-linearly-independent elements $\omega_1, \omega_2 \in \mathbb{C}$ (this is equivalent to ω_1, ω_2 are both non-zero and $\omega_1/\omega_2 \in \mathbb{C}\backslash\mathbb{R}$) such that

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{m\omega_1 + n\omega_2 \ : \ m, n \in \mathbb{Z}\}$$

The following is the definition of the Weierstrass function over a lattice $L \subset \mathbb{C}$

$$\wp_L(z) := \frac{1}{z^2} + \sum_{\omega \in L^*} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

it can be shown that $\wp_L$ is a meromorphic function (it has a Laurent series) and has (second order) poles in L. We have a bijection

$$(\mathbb{C}/L)\backslash\{0\} \to C \qquad z \bmod L \mapsto (\wp(z), \wp'(z))$$

where C is a smooth affine curve defined by the polynomial f i.e.

$$C := \{(p_1, p_2) \in \mathbb{C}^2 \,:\, f(p_1, p_2) = 0\}$$

The points in the image satisfies a cubic equation $f(x, y) = 0$ defining a smooth cubic curve in $\mathbb{A}^2$. Extending the map to $0 \bmod L$ extends it to the whole group $\mathbb{C}/L$ and allows us to endow the (projective) curve with a group structure. The curve has the property that the points

$$\begin{aligned} P &= (\wp(z), \wp'(z)) \\ Q &= (\wp(w), \wp'(w)) \\ R &= (\wp(z+w), -\wp'(z+w)) \end{aligned}$$

are collinear. This allowed a modern definition of elliptic curves that generalizes to other fields which we will soon see ...

Definition.

- An *affine plane* over K, or $\mathbb{A}^2(K)$ (we write $\mathbb{A}^2$ for short if K is known) is just K^2.
- A *projective plane* over K, or $\mathbb{P}^2(K)$ is just $(K^3\backslash\{\vec{0}\})/\sim$ where

  $$(p_0, p_1, p_2) \sim (q_0, q_1, q_2) \Leftrightarrow \exists \lambda \in K^* \twoheadrightarrow (p_0, p_1, p_2) = \lambda(q_0, q_1, q_2)$$

  the elements in the equivalence class of (p_0, p_1, p_2) (i.e. an element in $\mathbb{P}^2$) is denoted by $(p_0 : p_1 : p_2)$. We can consider the projective plane covered by three affine planes, we we call its *canonical affine charts*, namely

  $$\begin{aligned} U_x &= \{(1 : p_1 : p_2) \,:\, p_1, p_2 \in K\} \cong \mathbb{A}^2 \\ U_y &= \{(p_0 : 1 : p_2) \,:\, p_0, p_2 \in K\} \cong \mathbb{A}^2 \\ U_z &= \{(p_0 : p_1 : 1) \,:\, p_0, p_1 \in K\} \cong \mathbb{A}^2 \end{aligned}$$

- An *affine plane curve* is the zero set of a polynomial $f \in K[x, y]\backslash K$ in $\mathbb{A}^2$ and we denote it by

  $$C_f := \{P \in \mathbb{A}^2 \,:\, f(P) = 0\}$$

  C_f is said to be irreducible if f is absolutely irreducible as a polynomial (i.e. irreducible over $\bar{K}$).
- If $L \geq K$ and $f \in K[x, y]$ then we say that f (or C_f) is *defined over* K and we denote

  $$C_f(L) := \{P \in \mathbb{A}^2(L) \,:\, f(P) = 0\}$$

  and call it the *L-rational points of C_f*. We may drop the subscript f if this is clear. In many literature (maybe also in our lectures) one sometimes write C/L instead of $C(L)$.

For those who have had a little introduction in algebraic geometry, I could offer an explanation why we write $\mathbb{A}^2$ instead of K^2. We often attach to $\mathbb{A}^2$ the Zariski topology whilst for K^2 we either think of it as a pure vector space or topological vector space with the Euclidean topology. On the other hand $\mathbb{P}^2$ is just a 'natural' way to compactify $\mathbb{A}^2$ by adding a point of infinity to every line in $\mathbb{A}^2$ with the same direction.

Example 1.

- For any $c \in K^*$ and $f \in K[x,y]\backslash K$ we have $C_f = C_{cf}$
- For $K = \mathbb{Q}$ and $f(x,y) = x^2 + y^2 - 1$, $C_f(\mathbb{R})$ is the unit circle in $\mathbb{A}^2(\mathbb{R})$ and we have

$$C_f = C_f(\mathbb{Q}) = \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) \,:\, t \in \mathbb{Q} \right\} \cup \{(-1,0)\}$$

- Let $K = \mathbb{Q}$ and $f(x,y) = x^n + y^n - 1$ for some $n \in \mathbb{N} + 2$ then by Fermat's last theorem (Wiles 1995)

$$C_f = \begin{cases} \{(0,1),(1,0)\} & n \in 2\mathbb{N}+1 \\ \{(0,\pm 1),(\pm 1,0)\} & n \in 2\mathbb{N}+2 \end{cases}$$

- Suppose K is of characteristic $p > 0$ and K is not a perfect field, i.e. there is an element $a \in K$ such that $x^p - a$ has no root in K (Note: in this case a is not an element of $\mathbb{F}_p$ because of Fermat's little theorem). Then $f(x,y) = x^p + ay^p$ is an irreducible polynomial over K (why?) but C_f is not an irreducible curve, because in $\bar{K}$ we have the factorization $f(x,y) = (x + \alpha y)^p$ for some p-th root of $a \in K$.

Definition.

- Let $f \in K[x,y]\backslash K$ irreducible. We say $P \in \mathbb{A}^2$ is a singular point of C_f iff

$$f(P) = \frac{\partial f(P)}{\partial x} = \frac{\partial f(P)}{\partial y} = 0$$

  We say that C_f is *non-singular* or *smooth* if any $P \in C_f(\bar{K})$ is not a singular point of $C_f(\bar{K})$. If $P \in C_f$ is not a singular point, then the *tangent line* of C_f at $P = (p_1, p_2)$ is given by

$$\frac{\partial f(P)}{\partial x}(x - p_1) + \frac{\partial f(P)}{\partial y}(y - p_2)$$

  Any point $P \in C_f$ that is not a singular point is also called a *non-singular/regular/smooth* point of C_f

- Let $f \in K[x,y]$ then the *homogenization* of f is the construction of the homogenous polynomial $z^{\deg f} f(\frac{x}{z}, \frac{y}{z})$. And if $F \in K[x,y,z]$ is a homogenous polynomial its *dehomogenization (to $K[x,y]$)* is just the polynomial $F(x,y,1) \in K[x,y]$

We similarly define *projective plane curve* but zeros of polynomial $f \in K[x,y]$, we require it to be non-trivial zeros of a homogenous polynomial[1] $F \in K[x,y,z]$ (i.e. a polynomial $f \in K[x,y,z]$ such that $f(\lambda P) = \lambda^{\deg f} f(P)$ for any lambda in K^*) representing points in $\mathbb{P}^2$, this *curve* is well-defined in $\mathbb{P}^2$. An affine plane curve $C_f \subset \mathbb{A}^2$ can be extended to the projective space $\mathbb{P}^2$ by homogenizing f to F and taking C_F (C_f is then the part of C_F in one *chart* of $\mathbb{P}^2$ contained in $U_z \subset \mathbb{P}^2$).

If we consider a projective plane curve $C_F \subset \mathbb{P}^2$ then we may define singular/regular point $P \in C_F$ by first considering this point in an affine chart, say without loss of generality $p_2 \neq 0$ so P is a point in U_z, then dehomogenizing F to this chart, i.e. to $f \in K[x,y]$, and check if (p_0, p_1) is a singular/regular point of the affine curve C_f in this chart. One can check that tangent line of C_F at $P \in C_F$ is defined by the linear form:

$$\frac{\partial F(P)}{\partial x}x + \frac{\partial F(P)}{\partial y}y + \frac{\partial F(P)}{\partial z}z$$

[1] homogenous polynomials are also called *forms*

Example 2.

1. Suppose $a, b \in K$ and assume $\operatorname{char} K \neq 2$. Consider now $f(x,y) = y^2 - g(x)$ were $g(x) = x^3 + ax + b$. We have
$$\frac{\partial f}{\partial x} = -(3x^2 + a) \qquad \frac{\partial f}{\partial y} = 2y$$
If $P = (\alpha, \beta) \in \mathbb{A}^2(\bar{K})$ is singular on C_f then it satisfies
$$\begin{aligned} 2\beta &= 0 \\ 3\alpha^2 + a &= 0 \\ \beta^2 - (\alpha^3 + a\alpha + b) &= 0 \end{aligned}$$
Thus, C_f is smooth iff g has a double root ($g'(\alpha) = g(\alpha) = 0$). The singularity point must lie on the x-axis. This is true for any g, not just the one in this example. So, C_f is smooth iff the discriminant of g, $4a^3 + 27b^2$, is not 0.

2. Consider the same $f(x,y) = y^2 - g(x)$ above with $\operatorname{char} K = 2$. Then the above equation for a singular point $P = (\alpha, \beta)$ becomes
$$\begin{aligned} 3\alpha^2 + a = \alpha^2 + a &= 0 \\ \beta^2 - b &= 0 \end{aligned}$$
This implies that $C_f(\bar{K})$ has a singular point.

3. Suppose $P := (0,0)$ and $C_1 : y^2 = x^3 + x$ be defined over a field K, then its defining polynomial $f(x,y) := y^2 - (x^3 + x)$ is an irreducible cubic polynomial. We also have
$$\nabla f(x,y) = (-(3x^2 + 1), 2y) \Rightarrow \nabla f(P) = (-1, 0) \neq (0,0)$$
so P is not a singular point of C. Suppose for the same P, we have $C_2 : y^2 = x^3 + x^2$, then it's defining polynomial $f(x,y) := y^2 - (x^3 + x^2)$ is once again irreducible. We have
$$\nabla f(x,y) = (-(3x^2 + 2x), 2y) \Rightarrow \nabla f(P) = (0,0)$$
and so P is a singular point of C

In most context when we say *curve* we mean irreducible plane curve. In case of an exception we will specifically state this (e.g. *space curves*, *reducible curves* etc.).

Definition.

- For any $f \in K[x,y]$ we know that $\langle f \rangle$ is a prime ideal iff f is irreducible. In the case f is irreducible and not a constant (i.e. defining a curve), we know then that $K[x,y]/\langle f \rangle$ is an integral domain. Let $C \subset \mathbb{A}^2$ be the curve defined by this f, then one often denotes this domain as $K[C]$ and its quotient field as $K(C)$.
- Let $f \in K[x,y] \backslash K$ be irreducible defining $C \subset \mathbb{A}^2$ and suppose that $P \in C$, then
$$m_P := \{g \bmod \langle f \rangle \in K[C] \,:\, g(P) = 0\}$$
is a maximal ideal of $K[C]$ and the *localization of* $K[C]$ over this ideal is the local ring (subring of $K(C)$)
$$K[C]_P := \left\{ \frac{\bar{g}}{\bar{h}} \,:\, h(P) \neq 0 \right\}$$
with maximal ideal induced by m_P (which we shall again denote m_P) i.e. $m_P K[C]_P$.

Remark 3. In the definition above, m_P/m_P^2 is a finite-dimensional K-vector-space. With a little more commutative algebra and algebraic geometry one can show that P is a regular point of C iff
$$\dim_K m_P/m_P^2 = 1$$