FROM ALGEBRAIC CURVES TO FIELD THEORY

Reference: Sections 1.3, 1.4 in "Basic Algebraic Geometry 1", Shafarevich:

- "Relation with Field Theory" (1.3)
- "Rational maps" (1.4)

In the previous lecture we saw that all curves of degree 1 and 2 are rational curves, but, in general, not all curves are rational.

Then, how can we determine whether an algebraic curve is rational?

In this lecture we will see that to any irreducible algebraic (plane) curve we can associate a field, called the "function field" of the curve, in an analogous way we associate to an irreducible polynomial its splitting field.

We will see that this function field contains a lot of information about the curve.

INTRODUCTION

Recall: Let K_0 be a (non algebraically closed) field.

If $g(x) \in K_0[x]$ is an irreducible polynomial, then the field

$$F = \frac{K_0[x]}{(g(x))}$$

Since $K_0[x]$ is a PID the ideal $(g(x))$ is maximal thus the quotient ring is a field

is called the splitting field of $g(x)$ and is the smallest field extension of K_0 over which $g(x)$ splits into linear factors.

If $\alpha \in \overline{K_0}$ is a root of $g(x)$, i.e. $g(\alpha) = 0$, then it is easy to show that:

$$\frac{K_0[x]}{(g(x))} \cong K_0[\alpha] \cong K_0(\alpha)$$

the smallest field containing K_0 and α.

e.g: $g(x) = x^2 - 2 \in \mathbb{Q}[x] \Longrightarrow \dfrac{\mathbb{Q}[x]}{(x^2-2)} \cong \mathbb{Q}(\sqrt{2})$

from now on we will denote algebraic curves with X instead of $\mathcal{C}$

Let now $X : f(x,y) = 0$ be an irreducible algebraic plane curve.

Since $f(x,y) \in K[x,y]$ is irreducible and $K[x,y]$ is an UFD, the ideal $(f(x,y))$ is prime. Then the quotient ring

but not a PID

$$\frac{K[x,y]}{(f(x,y))}$$

is an integral domain, but not a field in general.

The field obtained as the field of fractions of $\dfrac{K[x,y]}{(f(x,y))}$, denoted $K(X)$, is called the function field of X:

$$K(X) = \mathrm{Frac}\left(\frac{K[x,y]}{(f(x,y))}\right)$$

RATIONAL FUNCTIONS DEFINED ON A CURVE

Let K be an algebraically closed field.

Let us consider the field of rational functions in two variables x and y with coefficients in K:

$$K(x,y) := \left\{ \frac{p(x,y)}{q(x,y)} \, , \; p, q \in K[x,y] \, , \; q \neq 0 \right\}$$

Every element $\dfrac{p(x,y)}{q(x,y)} \in K(x,y)$ defines a function from $\mathbb{A}^2(K)$ to K:

$$\begin{aligned} \mathbb{A}^2(K) &\longrightarrow K \\ (x_0, y_0) &\longmapsto \frac{p(x_0,y_0)}{q(x_0,y_0)} \end{aligned}$$

This function is defined for all $(x_0, y_0) \in \mathbb{A}^2(K)$ such that $q(x_0,y_0) \neq 0$, i.e. on all points of the affine plane, except those on the curve $q(x,y) = 0$.

In $K(x,y)$ it is implicitely defined an equivalence relation between rational functions:

$$\frac{p(x,y)}{q(x,y)} \sim \frac{p_1(x,y)}{q_1(x,y)} \iff p(x,y)\,q_1(x,y) - p_1(x,y)\,q(x,y) = 0$$

If $\frac{p(x,y)}{q(x,y)} \sim \frac{p_1(x,y)}{q_1(x,y)}$ then $\frac{p(x_0,y_0)}{q(x_0,y_0)} = \frac{p_1(x_0,y_0)}{q_1(x_0,y_0)}$ for all $(x_0,y_0) \in \mathbb{A}^2(K)$ such that $q(x_0,y_0) \neq 0$ and $q_1(x_0,y_0) \neq 0$, i.e. for all points of the affine plane except the points on the curves $q(x,y)=0$ and $q_1(x,y)=0$.

e.g.: Consider the rational functions:

$$\frac{x^2}{xy}, \quad \frac{xy}{y^2} \quad \in K(x,y).$$

We have $\frac{x^2}{xy} \sim \frac{xy}{y^2}$, and the two functions return the same value if evaluated at all points of the affine plane except those on the lines $x=0$ and $y=0$.

Let now $X: f(x,y)=0$ be an irreducible algebraic plane curve.
Since $X \subseteq \mathbb{A}^2(K)$, for each rational function $\frac{p(x,y)}{q(x,y)} \in K(x,y)$ we can consider its restriction to the points on X.

Note that, if $f(x,y) \mid q(x,y)$ (i.e. $q(x,y) \in \underbrace{(f(x,y))}_{\text{the ideal generated by } f(x,y)}$), then $q(x_0,y_0)=0 \;\; \forall\, (x_0,y_0) \in X$ and $\frac{p(x,y)}{q(x,y)}$ is not defined at any point on X.

Otherwise, if $f(x,y) \nmid q(x,y)$ (i.e. $q(x,y) \notin (f(x,y))$), then $\frac{p(x,y)}{q(x,y)}$ is defined at all points $(x_0,y_0) \in X$, except those such that $q(x_0,y_0)=0$ (which are finitely many).

Thus we call a function:

$$u(x,y) = \frac{p(x,y)}{q(x,y)}, \quad p(x,y),\, q(x,y) \in K[x,y], \; f(x,y) \nmid q(x,y)$$

a RATIONAL FUNCTION DEFINED ON X.

THE FUNCTION FIELD OF X

We define an equivalence relation between rational functions defined on X:

$$\frac{p(x,y)}{q(x,y)} \sim \frac{p_1(x,y)}{q_1(x,y)} \iff f(x,y) \mid p(x,y)\,q_1(x,y) - p_1(x,y)\,q(x,y)$$

Note that if $\frac{p(x,y)}{q(x,y)} \sim \frac{p_1(x,y)}{q_1(x,y)}$ then $\frac{p(x_0,y_0)}{q(x_0,y_0)} = \frac{p_1(x_0,y_0)}{q_1(x_0,y_0)}$

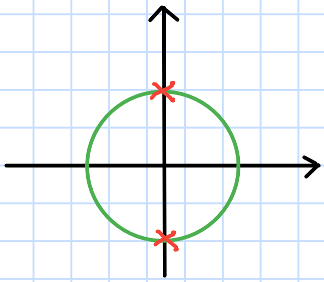
$\forall\ (x_0,y_0) \in X$ such that $q(x_0,y_0) \neq 0$ and $q_1(x_0,y_0) \neq 0$

(i.e. at all points on X, except possibly finitely many).

The set of rational functions defined on X up to equivalence is a field denoted by $K(X)$ and called the function field of X:

$$K(X) = \left\{ u(x,y) = \frac{p(x,y)}{q(x,y)}\ ,\ p,q \in K[x,y]\ ,\ f(x,y) \mid q(x,y) \right\} \Big/ \sim$$

e.g.: $X : x^2 + y^2 = 1$



The rational function

$$u(x,y) = \frac{1-y}{x}$$

is defined at all points on X except $(0,1)$ and $(-1,0)$.

For all $(x,y) \in X$ different from $(0,1)$ and $(-1,0)$ we have:

$$u(x,y) = \frac{1-y}{x} \underset{x \neq 0}{=} \frac{1-y}{x} \cdot \frac{x}{x} = \frac{x(1-y)}{x^2} \underset{x^2+y^2=1}{\sim} \frac{x(1-y)}{1-y^2} = \frac{x}{1+y}$$

This means that $\frac{1-y}{x}$ and $\frac{x}{1+y}$ are considered the same function in $K(X)$, with the only difference that $\frac{x}{1+y}$ is now defined on $(0,1)$.

Then, since $u(x,y)$ has a representation which is defined at $(0,1)$, we say that $u(x,y)$ is regular at $(0,1)$.

As we saw in the example, it can happen that $u(x,y)$ has two different expressions:

$$\frac{p(x,y)}{q(x,y)} \sim \frac{p_1(x,y)}{q_1(x,y)} \quad \text{with} \quad q(\alpha,\beta)=0 \text{ and } q_1(\alpha,\beta)\neq 0,$$

where $(\alpha,\beta)\in X$.
In this case we say that $u(x,y)$ is regular at (α,β).

Recall: Let $E\subseteq F$ be a field extension and $S=\{s_1,\dots,s_n\}\subseteq F$ a finite subset of F.
We say that S is algebraically independent over E if for all nonzero polynomials $p(x_1,\dots,x_n)\in E[x_1,\dots,x_n]$ we have $p(s_1,\dots,s_n)\neq 0$.

S is algebraically dependent over E if it is not algebraically independent, i.e. if there exists a nonzero polynomial $p(x_1,\dots,x_n)$ such that $p(s_1,\dots,s_n)=0$.

We call transcendental degree of the field extension $E\subseteq F$ the largest cardinality of an algebraically independent subset of F over E.

e.g.:
- If $E\subseteq F$ is an algebraic extension, i.e. $[F:E]<\infty$, then the transcendental degree is 0.
- For $\mathbb{Q}\subseteq\mathbb{Q}(\pi)$ the transcendental degree is 1 and $S=\{\pi\}$ is one of the algebraically independent subset of $\mathbb{Q}(\pi)$ over $\mathbb{Q}$ with largest cardinality $(=1)$.
- Every element in an algebraically independent set of F over E is a transcendental element of F over E.

Since $x,y\in K(X)$ are algebraically dependent over K (indeed $f(x,y)=0$, where $f(x,y)\in K[x,y]$), then $K(X)$ has transcendental degree 1 over K.

$\Updownarrow$

dimension 1 (curves)

EXAMPLES

$\longrightarrow$ LINES

We can assume X defined by the equation $y=0$.

Then, for every $u(x,y) \in K(X)$ we have:

$$u(x,y) = \frac{p(x,y)}{q(x,y)} \underset{y=0}{\sim} \frac{p(x,0)}{q(x,0)} = \frac{\tilde{p}(x)}{\tilde{q}(x)} \in K(x)$$

Hence, when X is a line the function field $K(X)$ is isomorphic to $K(x)$, the field of rational functions in one variable.

$$X \text{ line} \implies K(X) \approx K(x)$$

→ RATIONAL CURVES

Let $X: f(x,y)=0$ be a rational curve.

Then, by definition, there exist two rational functions $\varphi(t)$ and $\psi(t)$, at least one nonconstant, such that

$$f(\varphi(t), \psi(t)) \equiv 0.$$

So we have a map:

$$K(X) \longrightarrow K(t)$$

$$u(x,y) = \frac{p(x,y)}{q(x,y)} \longmapsto u(\varphi(t), \psi(t)) = \frac{p(\varphi(t),\psi(t))}{q(\varphi(t),\psi(t))}$$

This mapping is well-defined since $q(\varphi(t),\psi(t)) \not\equiv 0$.

Indeed, assume that $q(\varphi(t),\psi(t)) \equiv 0$. Then, since we have also $f(\varphi(t),\psi(t)) \equiv 0$ and K is infinite, $f(x,y)=0$ and $q(x,y)=0$ would have infinitely many common solutions.

But this is not possible, since $f \nmid q$.

Moreover, rational functions that are equal on X are sent to the same rational function in t.

Hence the previous map is an injection of $K(X)$ in $K(t)$, i.e. $K(X)$ is isomorphic to a subfield of $K(t)$.

We will use the following result:

Lüroth theorem: If F is a field such that
$$K \subseteq F \subseteq K(t),$$
then $F = K(g(t))$ where $g(t) \in K(t)$.

Note that if $g(t)$ is nonconstant, i.e. $F \neq K$, then the map

$$\begin{aligned} K(u) &\longrightarrow K(g(t)) \\ \frac{p(u)}{q(u)} &\longmapsto \frac{p(g(t))}{q(g(t))} \end{aligned}$$

is an isomorphism. Therefore $K(g(t)) \approx K(u)$ and we can restate Lüroth theorem in the following way:

Lüroth theorem (v.2): If F is a field such that
$$K \subsetneq F \subseteq K(t),$$
then $F \approx K(t)$.

Lüroth theorem implies the following result for rational curves:

Theorem: X is a rational curve if and only if $K(X) \approx K(t)$.

Proof

($\Rightarrow$) If X is rational, we have seen that $K(X)$ is a subfield of $K(t)$ different from K.

Then, by Lüroth theorem (v.2) $K(X) \approx K(t)$.

($\Leftarrow$) Let $X: f(x,y)=0$ be an irreducible plane curve and assume $K(X) \approx K(t)$.

Let ϕ be an isomorphism between $K(X)$ and $K(t)$:

$$\begin{aligned} \phi : K(X) &\longrightarrow K(t) \\ x &\longmapsto \varphi(t) \\ y &\longmapsto \psi(t) \end{aligned}$$

Since $f(x,y)=0$, we have:

$$\phi(f(x,y)) = f(\phi(x), \phi(y)) = f(\varphi(t), \psi(t)) \equiv 0$$

Then X is rational and $(\varphi(t), \psi(t))$ is a parametrization.

$\square$

<u>Proposition</u>: Let X be a rational curve and $(\varphi(t), \psi(t))$ a parametrization such that

$$\begin{aligned} K(X) &\xrightarrow{\sim} K(t) \\ x &\longmapsto \varphi(t) \\ y &\longmapsto \psi(t) \end{aligned}$$

is an isomorphism.

Then the parametrization $(\varphi(t), \psi(t))$ satisfies:

1) $\forall (x_0, y_0) \in X$ (except possibly finitely many points) $\exists\, t_0 \in K$ such that

$$(x_0, y_0) = (\varphi(t_0), \psi(t_0)).$$

2) This representation is unique, except possibly a finite number of points.

In other terms we have a bijection:

$$\begin{aligned} K \setminus \begin{Bmatrix} \text{finite set} \\ \text{of values} \end{Bmatrix} &\longrightarrow X \setminus \begin{Bmatrix} \text{finite set} \\ \text{of points} \end{Bmatrix} \\ t &\longmapsto (\varphi(t), \psi(t)) \\ \chi(x,y) &\longleftarrow\!\shortmid\ (x,y) \end{aligned}$$

Proof

Consider the isomorphism

$$\begin{aligned} \phi : K(X) &\longrightarrow K(t) \\ x &\longmapsto \varphi(t) \\ y &\longmapsto \psi(t) \end{aligned}$$

and its inverse

$$\begin{aligned} \tilde{\phi} : K(t) &\longrightarrow K(X) \\ t &\longmapsto \chi(x,y) = \frac{p(x,y)}{q(x,y)} \end{aligned}$$

We have:

$$\left.\begin{array}{lll} \tilde{\phi}(\phi(x)) = x & \Leftrightarrow & \varphi(\chi(x,y)) = x \\ \tilde{\phi}(\phi(y)) = y & \Leftrightarrow & \psi(\chi(x,y)) = x \\ \phi(\tilde{\phi}(t)) = t & \Leftrightarrow & \chi(\varphi(t), \psi(t)) = t \end{array}\right\} \quad (\clubsuit)$$

Let $\{\alpha_1, \dots, \alpha_n\} \subseteq K$ be the set of values at which either φ or ψ are not defined and $\{P_1, \dots, P_m\} \subseteq X$ be the set of points such that $q(P_i) = 0$.

Moreover, let $\{B_1, \dots, B_s\} \subseteq K$ be the set of solutions to the systems

$$\begin{cases} \varphi(t) = x_i \\ \psi(t) = y_i \end{cases}, \text{ where } P_i(x_i, y_i), \text{ for some } i,$$

and let $\{Q_1, \dots, Q_r\} \subseteq X$ the points (x,y) such that

$$\chi(x,y) = \alpha_j, \text{ for some } j.$$

Then, because of $(\clubsuit)$, we have a bijection:

$$\begin{array}{ccc} X \setminus \{P_1, \dots, P_m, Q_1, \dots, Q_r\} & \longleftrightarrow & K \setminus \{\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_s\} \\ (x,y) & \longmapsto & \chi(x,y) \\ (\varphi(t_0), \psi(t_0)) & \longleftarrow\!\!\shortmid & t_0 \end{array}$$

$\square$

<u>Remark</u>: In order to get a bijection, the parametrization $(\varphi(t), \psi(t))$ needs to correspond to an isomorphism between $K(X)$ and $K(t)$:

$$\begin{array}{ccc} K(X) & \xrightarrow{\sim} & K(t) \\ x & \longmapsto & \varphi(t) \\ y & \longmapsto & \psi(t) \end{array}$$

e.g.: For $X: y^2 = x^2 + x^3$ a parametrization is given by

$$\begin{array}{ccc} K & \longrightarrow & X \\ t & \longmapsto & (t^2 - 1, t(t^2 - 1)) \end{array}$$

but, if we replace t with t^2, also the map

$$\gamma : K \longrightarrow X$$
$$t \longmapsto (t^4-1,\ t^2(t^4-1))$$

is a parametrization of X. Nevertheless, there is no chance to obtain a bijection from γ, even by removing finite sets from both K and X. Indeed, for all $t \in K$ $\gamma(t) = \gamma(-t)$, so that γ is not injective if $\mathrm{char}(K) \neq 2$.

Note that via the parametrization γ we obtain an isomorphism:

$$\begin{array}{ccccc} K(X) & \xrightarrow{\sim} & K(t^2) & \xrightarrow[\sim]{t^2 \mapsto u} & K(u) \\ x & \longmapsto & t^4-1 & \longmapsto & u^2-1 \\ y & \longmapsto & t^2(t^4-1) & \longmapsto & u(u^2-1) \end{array}$$

RATIONAL MAP

Parametrizations are particular cases of rational maps, which are defined more in general between two irreducible algebraic curves.

Let $X: f(x,y)=0$ and $Y: g(x,y)=0$ be two irreducible algebraic plane curves.

If $u(x,y), v(x,y) \in K(X)$, the map:

$$\varphi : X \longrightarrow Y$$
$$(x,y) \longmapsto (u(x,y), v(x,y))$$

is called a rational map if $\varphi(P) \in Y$ fore every point $P \in X$ at which φ is defined.

In this case $g\big(u(x,y),\ v(x,y)\big) = 0$.

e.g: We can see a parametrization as a rational map between a line and a rational curve.

A rational map $\varphi : X \to Y$ is birational if φ has a rational inverse, i.e. if there exists a rational map

$$\psi : Y \dashrightarrow X$$

such that $\psi \circ \varphi$ and $\varphi \circ \psi$ are the identity (at the points where they are defined)

In this case we say that X and Y are birationally equivalent.

e.g: we have seen, for instance, that rational curves are birationally equivalent to a line.

In algebraic geometry we use to classify curves (and more in general varieties) up to birational equivalence.

ill see that this is equivalent to the problem of classifying finitely generated extension fields of K of transcendental degree 1 up to isomorphism.

We have indeed the following result.

Theorem: X and Y are birationally equivalent if and only if $K(X)$ and $K(Y)$ are isomorphic.

Proof:

($\Rightarrow$) If X and Y are birationally equivalent, then there exist birational maps:

$$\varphi : X \dashrightarrow Y \qquad\qquad \psi : Y \dashrightarrow X$$

$$(x,y) \longmapsto (u(x,y), v(x,y)) \qquad\qquad (x,y) \longmapsto (\xi(x,y), \eta(x,y))$$

where $u(x,y), v(x,y) \in K(X)$ where $\xi(x,y), \eta(x,y) \in K(Y)$

with $\varphi \circ \psi = id_Y$ and $\psi \circ \varphi = id_X$.

It is not difficult to show that the following maps are isomorphisms of fields:

$$\phi : K(Y) \longrightarrow K(X)$$

$$w(x,y) \longmapsto w(\varphi(x,y)) = w(u(x,y), v(x,y))$$

$$\tilde{\phi} : K(X) \longrightarrow K(Y)$$

$$b(x,y) \longmapsto b(\psi(x,y)) = b(\xi(x,y), \eta(x,y))$$

with $\phi \circ \tilde{\phi} = id_{K(X)}$ and $\tilde{\phi} \circ \phi = id_{K(Y)}$.

($\Leftarrow$) Since $K(X) \approx K(Y)$ we have two isomorphisms of fields.

$$\phi : K(Y) \longrightarrow K(X) \qquad \tilde{\phi} : K(X) \longrightarrow K(Y)$$

$$x \longmapsto u(x,y) \qquad x \longmapsto \xi(x,y)$$

$$y \longmapsto v(x,y) \qquad y \longmapsto \eta(x,y)$$

Then the maps:

$$\varphi : X \longrightarrow Y \qquad \psi : Y \longrightarrow X$$

$$(x,y) \longmapsto (u(x,y), v(x,y)) \qquad (x,y) \longmapsto (\xi(x,y), \eta(x,y))$$

are birational maps, such that $\varphi \circ \psi = id_Y$ and $\psi \circ \varphi = id_X$. Thus X and Y are birationally equivalent.