§ Arithmetic Dynamics over Local fields

On $\mathbb{P}^1(\mathbb{C})$, define the chordal metric via

$$\rho_\infty([x_1:y_1],[x_2:y_2]) = \frac{|x_1y_2 - x_2y_1|}{\sqrt{|x_1|^2+|y_1|^2}\sqrt{|x_2|^2+|y_2|^2}}$$

$$[x_1:y_1] = [cx_1:cy_1]$$

If we identify $\mathbb{P}^1(\mathbb{C})$ with the sphere via

then

$$\rho_\infty(z,w) = \frac{1}{2}|z^* - w^*|$$

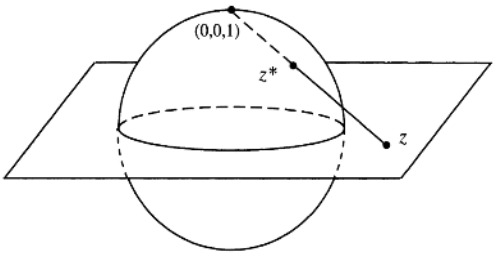


Figure 1.1: Identifying $\mathbb{C} \cup \infty$ with the Riemann sphere.

Properties:

- Δ-inequality: $\rho_\infty(P_1,P_3) \le \rho_\infty(P_1,P_2) + \rho_\infty(P_2,P_3)$.
- Lipschitz property: Given $\phi: \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ rational map

  $\exists$ constant $C(\phi)$ s.t.

$$\rho_\infty(\phi(P_1),\phi(P_2)) \le C(\phi)\rho_\infty(P_1,P_2).$$

Now over $(K, |\cdot|_v)$ a non-archimedian valued field.

Defn: the chordal metric on $\mathbb{P}^1(K)$ is defined as

$$\rho_v([x_1:y_1],[x_2:y_2]) = \frac{|x_1y_2 - x_2y_1|_v}{\max\{|x_1|_v, |y_1|_v\}\max\{|x_2|_v, |y_2|_v\}}.$$

Properties: (ρ_v is an ultrametric)

$|x_1y_2 - x_2y_1| \le \max\{|x_1x_2|, |x_2y_1|\}$

$\le \max\{|x_1|_v, |y_1|_v\}\max\{|x_2|_v, |y_2|_v\}$

- $0 \le \rho_v(P_1, P_2) \le 1$
- $\rho_v(P_1, P_2) = 0$ iff $P_1 = P_2$
- $\rho_v(P_1, P_2) = \rho_v(P_2, P_1)$
- $\rho_v(P_1, P_3) \le \max\{\rho_v(P_1, P_2), \rho_v(P_2, P_3)\}$.

Lemma: Let $R = \{\alpha \in K : |\alpha|_v \le 1\}$

Let $f : \mathbb{P}^1 \to \mathbb{P}^1$ be a linear fractional transformation.

$$f([x:y]) = \frac{ax+by}{cx+dy}$$

$a, b, c, d \in R$, $ad - bc \in R^*$. (In other words $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PGL_2(R)$)

Then

$$\rho_v(f(P_1), f(P_2)) = \rho_v(P_1, P_2).$$

§ Reduction mod p

- K - field w/ discrete valuation $v: K^\times \to \mathbb{Z}$.
- $|\cdot|_v = c^{-v(\cdot)}$ associated abs value.
- $R = \mathcal{O}_K = \{x \in K \mid v(x) \geq 0\}$ Ring of integers
- $R^\times = \{x \in K \mid v(x) = 0\}$. Group of units.
- $\mathfrak{p} = \{x \in K \mid v(x) \geq 1\}$ max ideal of R.
- $k = R/\mathfrak{p}$ Residue field.

We will use $\sim$ to denote reduction mod $\mathfrak{p}$

$$R \longrightarrow R/\mathfrak{p}$$
$$a \longmapsto \tilde{a}$$

Reduction of points in $\mathbb{P}^N(K)$

Suppose $P = [x_0 : \cdots : x_N] \in \mathbb{P}^N(K)$, how do we reduce to a point $\tilde{P} \in \mathbb{P}^N(k)$?

We say that P has normalised co-ordinates if

$$\min\{v(x_0), \ldots, v(x_N)\} = 0.$$

Then $\tilde{P} = [\tilde{x}_0 : \cdots : \tilde{x}_N]$.

In general, want to multiply by some c so

$P = [cx_1, \ldots, cx_n]$ is normalised.

We need to pick $c \in K^\times$ s.t.

$$v(c) = -\min\{v(x_0), \cdots, v(x_N)\}.$$

Then

$$\widehat{P} = [\widetilde{cx}_1 : \cdots : \widetilde{cx}_N].$$

Fact: $\widehat{P}$ is independent of the choice of c.

pf: If c, c' both work, $v(c) = v(c')$.

$$cc'^{-1} \in R^\times \qquad \widetilde{cc'^{-1}} \in k^\times$$

Lemma: Let $P_1, P_2 \in \mathbb{P}^1(K)$, then

$$\widetilde{P}_1 = \widetilde{P}_2 \iff \rho_v(P_1, P_2) < 1$$

pf: Write $P_i = [x_i : y_i]$ in normalised coordinates.

$$\max\{|x_i|, |y_i|\} = 1$$

So $\rho_v(P_1, P_2) = |x_1 y_2 - x_2 y_1|$

$(\Rightarrow)$ $\widehat{P}_1 = \widehat{P}_2$, $\exists\, \widehat{u} \in k^\times$ s.t.

$$(\widetilde{x}_1, \widetilde{y}_1) = (\widehat{u}\,\widetilde{x}_2, \widehat{u}\,\widetilde{y}_2) \text{ in } k^2$$

Let u be any lift of $\widehat{u}$ in $R^\times$, then.

$$x_1 \equiv u x_2 \bmod \mathfrak{p} \qquad y_1 \equiv u y_2 \bmod \mathfrak{p}$$

$$\Rightarrow x_1 y_2 - x_2 y_1 \equiv u x_2 y_2 - u x_2 y_2 \bmod \mathfrak{p}$$

$$\equiv 0$$

$$\Rightarrow |x_1 y_2 - x_2 y_1| < 1$$

($\Leftarrow$) Suppose $\rho_v(P_1, P_2) < 1$, then

$$X_1 Y_2 \equiv X_2 Y_1 \mod \mathfrak{p} \qquad [X_1 : Y_1]$$

If $X_1 X_2 \equiv 0 \mod \mathfrak{p}$, then $X_1 \equiv X_2 \equiv 0 \mod \mathfrak{p}$.

$\widetilde{P_1} = \widetilde{P_2} = [0:1]$.

Otherwise, $X_1 X_2 \not\equiv 0 \mod \mathfrak{p}$, so $\widetilde{X_1}, \widetilde{X_2} \in k^\times$, so.

$$\widehat{P_1} = [\widetilde{X_1} : \widetilde{Y_1}] = [\widetilde{X_1}\widetilde{X_2} : \widetilde{Y_1}\widetilde{X_2}] = [\widetilde{X_2}\widetilde{X_1} : \widetilde{X_1}\widetilde{Y_2}] = [\widetilde{X_2} : \widetilde{Y_2}] = \widehat{P_2}.$$ □

Corollary: Let $P_1, P_2 \in \mathbb{P}^1(K)$, $f \in PGL_2(R)$

$$\widetilde{P_1} = \widetilde{P_2} \iff \widetilde{f(P_1)} = \widetilde{f(P_2)}$$

If P_1, P_2, P_3 are distinct points in $\mathbb{P}^1(K)$, then

$\exists f \in PGL_2(K)$ s.t

$$f(P_1) = 0, \quad f(P_2) = 1, \quad f(P_3) = \infty.$$

What about in $PGL_2(R)$?

Prop: If $\widetilde{P_1}, \widetilde{P_2}, \widetilde{P_3}$ are distinct pts in $\mathbb{P}^1(k)$, then

$\exists f \in PGL_2(R)$ s.t

$$f(P_1) = 0, \quad f(P_2) = 1, \quad f(P_3) = \infty.$$

Reduction of a map

Let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map of degree d.
How do we get a map $\tilde{\phi} : \mathbb{P}^1(k) \to \mathbb{P}^1(k)$?

ϕ is given by homogenous polynomials F, G of degree d.

$$\phi[x:y] = [F(x,y) : G(x,y)]$$

F, G are unique up to scaling by $c \in K^\times$.

Defn: $\phi = [F:G]$ is normalised if $F, G \in R[x,y]$, and at least 1 coeff of F or G is in $R^\times$.

If ϕ is normalised, then we define $\tilde{\phi}$ as

$$\tilde{\phi} = [\tilde{F} : \tilde{G}]$$ ← also should divide by $H = \gcd(\tilde{F}, \tilde{G})$

$\tilde{\phi} : \mathbb{P}^1(k) \longrightarrow \mathbb{P}^1(k)$.

Example: Let $a \in K^\times$, and consider

$$\phi_a[x:y] = [ax^d : y^d].$$

- If $a \in R^\times$, then $\tilde{a} \in k^\times$, so
$$\tilde{\phi}_a[x:y] = [\tilde{a}x^d : y^d].$$
- If $v(a) > 0$, then $\tilde{a} = 0$
$$\tilde{\phi}_a[x:y] = [0 : y^d].$$ ← $\gcd(0, y^d) = y^d$
$$= [0:1].$$

- If $v(a) < 0$, then scale by a^{-1}, $\widetilde{a^{-1}} = 0$

$$\phi_a[x:y] = [x^d : a^{-1}y^d].$$

$$\widetilde{\phi}_a[x:y] = [x^d : 0]$$

$$= [1 : 0].$$

Motivation: $\widetilde{\phi(P)} = \widetilde{\phi}(\widetilde{P})$, $\widetilde{\phi^n(P)} = \widetilde{\phi}^n(\widetilde{P})$.

To study orbits of ϕ in $\mathbb{P}^1(K)$, first study the orbits of $\widetilde{\phi}$ in $\mathbb{P}^1(k)$.

§ Resultant of a Rational map

The resultant of polynomials F, G characterizes when they have common factors.

Prop/Defn: Let

$$A(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n$$

$$B(X,Y) = b_0X^m + \cdots + b_mY^m$$

be homogeneous polynomials of degree n and m in $K[X,Y]$.

There exists a polynomial.

$$\mathrm{Res}(a_0, \cdots, a_n, b_0, \cdots, b_m) \in \mathbb{Z}[a_0, \cdots, a_n, b_0, \cdots, b_m].$$

Such that:

a) $\mathrm{Res}(A,B) = 0$ iff A, B have a common zero in $\overline{k}$

b) If $a_0 b_0 \neq 0$, and we write

$$A = a_0 \prod_i (x - \alpha_i y), \quad B = b_0 \prod_j (x - \beta_j y)$$

then

$$\mathrm{Res}(A,B) = a_0^m b_0^n \prod_i \prod_j (\alpha_i - \beta_j)$$

c) $\exists$ Polynomials $F_1, G_1, F_2, G_2 \in \mathbb{Z}[a_0, \dots, a_n, b_1, \dots, b_n][x,y]$ homogenous w/ degree $m-1$ and $n-1$ s.t.

$$F_1 A + G_1 B = \mathrm{Res}(A,B)\, x^{m+n-1}$$
$$F_2 A + G_2 B = \mathrm{Res}(A,B)\, y^{m+n-1}$$

d) The resultant is equal to the $(m+n)\times(m+n)$ determinant.

$$\mathrm{Res}(A,B) = \begin{vmatrix} a_0 & a_1 & \cdots & a_n & & \\ & a_0 & a_1 & \cdots & a_n & \\ & & a_0 & \cdots & a_n & \\ & & & \ddots & & \\ & & & & a_0 & \cdots & a_n \\ b_0 & \cdots & b_m & & & \\ & b_0 & \cdots & b_m & & \\ & & \ddots & & \ddots & \\ & & & b_0 & \cdots & b_m \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \\ \} m \\ \\ \\ \\ \} n \end{matrix}$$

In particular $\mathrm{Res}(A,B)$ is homogenous of degree m in $a_0, \dots, a_n$

n in $b_0, \dots, b_m$.

Let $\phi = [F:G]$ be a normalised rational map over $(K, |\cdot|_v)$ non-arch.

We write $\mathrm{Res}(\phi) = \mathrm{Res}(F, G)$

This is well defined up to scaling by u^{2d}, $u \in R^\times$.

In particular: $v(\mathrm{Res}(\phi))$ is an invariant.

Theorem: Let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map, then

$$\rho_v(P_1, P_2) \leq |\mathrm{Res}(\phi)|^{-2} \rho_v(\phi(P_1), \phi(P_2))$$