Lecture 5

• Rational maps and morphisms between curves.

$C = V(f)$ affine curve, $\tilde{C} = V(F)$ its homogeneous version. Supp f irreducible $\Rightarrow F$ is so.

Def: $K[C] = K[X,Y]/(f) \equiv$ the affine coordinate ring.

$K(C) \equiv$ fraction field of $K[C] = \left\{ \frac{g(\bar{x},\bar{y})}{h(\bar{x},\bar{y})} \;\middle|\; g,h \in K[C],\ h \notin (f) \right\}$.

A function $\varphi = \frac{g}{h} \in K(C)$ is regular at $P \in C$ if $\varphi = \frac{t}{s} \mid s(P) \neq 0$.

Def: $K[\tilde{C}] = K_h[X_0, X_1, X_2]/(F)$

$K(\tilde{C}) = \left\{ \frac{f(X_0:X_1:X_2)}{h(X_0:X_1:X_2)} \;\middle|\; f,g \text{ homogeneous same deg},\ g \notin (F) \right\}$.

A function $\varphi = \frac{g}{h} \in K(\tilde{C})$ is regular at P if $\varphi = \frac{t}{s} \mid s(P) \neq 0$.

Def: Let C_1, C_2 be projective curves. A rational map is

$\phi : C_1 \to C_2 \qquad \phi = (f_0 : f_1 : f_2)$ where $f_i \in K(\tilde{C})$

$\Rightarrow$ clearing denominators $\phi = (f_0 : f_1 : f_2)$, f_i homogeneous polynomials of same degree.

Def: ϕ is regular at $P \in C_1$ if $\exists\ g \in K(C_1)$ s.t. gf_i regular at P $i = 0,1,2$.

$\Rightarrow \phi(P) = (gf_0(P) : gf_1(P) : gf_2(P))$.

Def: A rational map which is regular at each $P \in C_1$ is called a morphism.

$\phi : C_1 \to C_2$ rational (morphism). If $\exists\ \phi^{-1} : C_2 \to C_1$ rational (morphism) ϕ is called birational map (isomorphism).

• Frobenius

Recall, $q = p^n$ (p prime, then $\varphi : \mathbb{F}_q \to \mathbb{F}_q$, $x \mapsto x^p$ is an automorphism

which fixes $\mathbb{F}_p$, called the Frobenius automorphism.

Let $C = V(F)$ a projective curve defined over $\mathbb{F}_p$, then, define

$$\varphi : C = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(\overline{\mathbb{F}}_p) \mid F(x_0, x_1, x_2)\} \longrightarrow C$$
$$(x_0 : x_1 : x_2) \longmapsto (x_0^p : x_1^p : x_2^p)$$

(check it's well defined). This is the Frobenius morphism acting on C.

Rem: $P \in C(\mathbb{F}_p) \iff \varphi(P) = P$

(hint, recall, $x \in \overline{\mathbb{F}}_p$, $x \in \mathbb{F}_p \iff x^p = x$, $\mathbb{F}_{p^n}^*$ is cyclic and abelian and $\mathbb{F}_p^* \leq \mathbb{F}_{p^n}^*$).

Def: $\phi : C_1 \to C_2$ morphism. We say ϕ separable / inseparable / purely inseparable if $K(C_1)/\phi^* K(C_2)$ is so.

Obs: purely inseparable means that $\forall Q \in C_2$ $\exists!$ $P \in C_1$ $\phi(P) = Q$ with $e_\phi(P) = \deg(\phi)$.

Frobenius is ~~not~~ all purely inseparable: indeed, enough to see that $\varphi : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ is so: $x \in \overline{\mathbb{F}}_p$, say $x \in \mathbb{F}_{p^n}$, $\varphi(y) = x$ has a unique solution y_0 in $\mathbb{F}_{p^n}$, since $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ automorphism, this solution has multiplicity. Indeed, $t^p - x$ has 0 derivative hence

$$t^p - y_0^p = y_0^p \left(\left(\frac{t}{y_0}\right)^p - 1\right) = 0$$

$$\iff \left(\frac{t}{y_0} - 1\right)^p y_0^p = (t - y_0)^p = 0.$$

• Isogenies

Let E_1, E_2 be (projective) elliptic curves.

Def: $\phi : E_1 \to E_2$ is an isogeny if it's a morphism as curves and as groups, i.e. $\phi(P+Q) = \phi(P) + \phi(Q)$.

Obs: ϕ isogeny $\Rightarrow \phi(O) = O$. (Non-trivial!!)

obs: $\phi \equiv 0$ or $\phi(E_1) = E_2$

Notice: $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3 \Rightarrow \deg(\phi \circ \psi) = \deg(\phi)\deg(\psi)$.

$(\deg[0] = 0)$.

Def: $\mathrm{Hom}(E_1, E_2) = \{\phi : E_1 \to E_2 \text{ isogeny}\} \cup \{0\}$.

Obs: $(\mathrm{Hom}(E_1, E_2), +)$ abelian group.

$(\mathrm{End}(E), +, \circ) \equiv$ endomorphism ring of E ($\circ$ associative, checked later)

$\mathrm{End}(E)^* \equiv$ automorphism group.

obs: $[m]$ is an isogeny.

$\ker[m] = \{P \in E(\bar{K}) \mid [m]P = 0\} =: E[m]$, $E[m](\bar{K})$.

Prop: Frobenius is an isogeny.

Proof: $\phi : E_1 \to E_2$ Frob.

Lemma: P, Q, R are aligned $\Leftrightarrow P + Q + R = 0$.

Hence $P + Q + P * Q = 0$.

Enough to check that ϕ respects lines / $\mathbb{F}_p$: $P, Q \in L \Rightarrow \phi(P), \phi(Q) \in L$. (check!)

Now: $P + Q + P * Q = 0 \longrightarrow$ Frob takes them to the same line

$\varphi(P) + \varphi(Q) + \varphi(P) * \varphi(Q) = 0$

$\Rightarrow \varphi(P) * \varphi(Q) = \varphi(P * Q) \Rightarrow$ $\varphi(P) + \varphi(Q) = \varphi(0) * \varphi(P * Q)$

$\phi(P) + \phi(Q) + \phi(P * Q) = 0$

$= 0$

$= \varphi(0 * P * Q)$

$= \varphi(P + Q)$ #.

Prop: $\deg[m] = m^2$ #

$\deg[\phi] = p$ / $\mathbb{F}_p$.

Homes

Example:

1) $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$

$(x:y) \mapsto (x^3(x-y) : y^3)$ morphism.

$Q = (0:1)$, $\phi^{-1}(Q) = \{(x:y) \in \mathbb{P}^1 \mid (x^3(x-y)^2 : y^5) = (0:1)\}$

$y \neq 0 \Rightarrow \dfrac{x^3(x-y)^2}{y^5} = t^3(t-1)^2 = 0 \Rightarrow t=0$ (multip. 3) - $t=1$ mult. 2

$\uparrow t = \frac{x}{y}$

$t=0$ gives $(0:1)$, $t=1$ gives $(1:1)$.

$t = \frac{x}{y}$ uniformising at 0, $e_\phi(0:1) = \operatorname{ord}_{(0:1)} \phi(t) = \operatorname{ord}_0 t^3(t-1)^2 = 3$

likewise $e_\phi(1:1) = 2$.

Notice, then, $e_\phi(1:1) + e_\phi(0:1) = 5 = \deg \phi$.

2) $C_1 = \{(x:y:z) \mid x^2+y^2 = z^2\}$, $C_2 = \{(x:y:z) \mid x^2+y^2 = 3z^2\}$

C_1, C_2 not isomorphic over $\mathbb{Q}$, since $C_2(\mathbb{Q}) = \emptyset$

but $\phi : C_1 \longrightarrow C_2$

$(x_0:x_1:x_2) \mapsto (x_0 : x_1 : \sqrt{3}x_2)$ isomorphism / $\mathbb{Q}(\sqrt{3})$.