Theorem .0.1

There's an equivalence of categories between projective nonsingular curves with non-constant maps and finite extensions of $k(t)$.

This is given by $C \leftrightarrow k(C)$, and is contravariant.

Proof Sketch. There is an equivalence

$$\text{varieties}/k \leftrightarrow \mathbb{K}/k$$

where the left hand side is dominant rational maps (dense image defined on an open).

This can be upgraded to curves/k with finite extensions $\mathbb{K}$ of $k(t)$ by de-singularizing and compactifying (nontrivial, but reasonable).

For divisors, we can look at $h : C \to C'$ over k, then $h : \overline{k}(C') \to \overline{k}(C)$. Then $\deg h = [\overline{k}(C) : \overline{k}(C')]$.

We then have for $Q \in C'$ that

$$\sum_{p \in h^{-1}(Q)} e_p(h) = \deg h$$

where $e_p(h) = v_p(t' \circ h)$, where t' is a uniformizer at $h(p)$.

We can define $\text{Div}, \text{Div}^0, \text{Div}^\ell, \text{Pic}^0$ as before, and we get for each $h : C \to C'$ a pushforward and pullback

$$h_* : \text{Pic}^0(C) \to \text{Pic}^0(C') h^* : \text{Pic}^0(C') \to \text{Pic}^0(C)$$

We have h_* sends $[p]$ to $[h(p)]$ and h^* sends $[Q]$ to $\sum_{p \in h^{-1}(Q)} e_p(h)[p]$. Then $h_* \circ h^* = [\deg h]$.

Theorem .0.2

If $\mathcal{E}$ is an elliptic curve, then the map $\text{Div}(\mathcal{E}) \to \mathcal{E}$ induces an isomorphism

$$\text{Pic}^0(\mathcal{E}) \xrightarrow{\sim} \mathcal{E}.$$

Proof. Map is a homomorphism, and restriction to $\text{Div}^0(\mathcal{E})$ si surjective as $[p] - [0] \mapsto p$.

We want to show the kernel is Div^ℓ. The Lemma is

Lemma .0.3 (1) $p \neq q$ if and only if $[p] - [q]$ is not principal.

(2) $[p] - [0] + [Q] - [0] \equiv [P + Q] - [0]$ modulo Div^ℓ.

Suppose $[p] - [q]$ is principal, that is $[p] - [q] = \text{div}(f)$. Then $f : \mathcal{E} \twoheadrightarrow \mathbb{P}^1(k)$ with p being sent to 0, q being sent to ∞.

The genus tells us this is a big problem, becasue $\mathbb{P}^1(k)$ has genus zero, and $\mathcal{E}$ has genus one. For the second part write $f(x, y) = ax + by + c$ in $k(\mathcal{E})$. Then

$$\text{div}(f) = [P] + [Q] + [R] - 3[0].$$

Likewise the line through $R, -R$ has divisor $[R] - [0] + [-R] - [0]$. Thus

$$[P] + [Q] - 3[0] + 2[0] - [-R] \in \text{Div}^\ell.$$

Then we have

$$[P] + [Q] - [P + Q] - [0] \in \mathrm{Div}^{\ell}.$$

Then $[P] + [Q] \equiv [P + Q] + [0]$, which is equvialent to what we wanted.

Now suppose we have $\sum_p [n_p]p = 0$ (that is the divisor $\sum_p n_p[p]$ goes to 0). By (1) this is true if and only if $\left(\sum_p n_p[p]\right) - [0]$ is principial.

By (2) this is if and only if $\left(\sum_p n_p([p] - [0])\right)$ is principal. By (1) this becomes $\sum n_p[p] \in \mathrm{Div}^{\ell}$. This is what we wanted!

Corollary .0.4

$\sum n_p[p]$ is principal if and only if $\sum n_p = 0$ and $\sum [n_p]p = 0$.

Weil Pairing! We'll look at

$$\mu_N = \{x \in \overline{k} \mid x^N = 1\},$$

while this might look like $\mathbb{Z}/N\mathbb{Z}$, it carries a nontrivial Galois action to keep track of. The Weil pairing is a map

$$e_N : \mathcal{E}[N] \times \mathcal{E}[N] \to \mu_N.$$

Let $P, Q \in \mathcal{E}[N]$ Then $N[Q] - N[0] \in \mathrm{Div}^{\ell}$ from our corollary. Say this is $\mathrm{div}(f)$. We now want to compute $\mathrm{div}(f \circ [N])$, which is

$$\sum_{R:[N]R=Q} N[R] - \sum_{S:[N]S=0} N[S].$$

We then fix $Q' \in \mathcal{E}[N^2]$ such that $[N]Q' = Q$. Then

$$\mathrm{div}(f \circ [N]) = N \sum_{S \in \mathcal{E}[N]} [Q' + S] - [S],$$

which we're supposed to see is principal, without the N! This is because $\mathcal{E}[N]$ has N^2 points. We then have this as $\mathrm{div}(g)$ and $\mathrm{div}(f \circ [N]) = \mathrm{div}(g^N)$.

For all $x \in E$, we have

$$g(x + p)^N = f([N]x + [N]P) = f([N]x) = g(x)^N,$$

Hence $\frac{g(x+P)}{g(x)} \in \mu_N$ and is constant. Thus we define

$$e_n(P, Q) = \frac{g(x + P)}{g(x)}.$$

Theorem .0.5

This map is bilinear in a multiplicative sense, i.e.

$$e_N(aP, cQ) = e_N(P, Q)^{ac}.$$

It's also alternating $e_N(Q,Q)=1$. This implies that it's skew-symmetric.

Furthermore it's non-degenerate. Even more incredibly it is Galois equivariant $e_N(P,Q)^\sigma = e_N(P^\sigma, Q^\sigma)$.

Finally, it is isomorphism invariant.

A lot of these are not that hard to check.

Corollary .0.6

We have $e_n(P',Q') = e_n(P,Q)^{\det \gamma}$ if

$$\begin{bmatrix} P' \\ Q' \end{bmatrix} = \gamma \begin{bmatrix} P \\ Q \end{bmatrix}.$$

Now we're going to look at function fields of modular curves. Recall that $\mathbb{C}(X(1)) = \mathbb{C}(j)$. We would like to compute $\mathbb{C}(X(N)), \mathbb{C}(X_1(N)), \mathbb{C}(X_0(N))$.

Take $v \in \mathbb{Z}^2$ with $\overline{v} \in (\mathbb{Z}/N\mathbb{Z})^2$ nonzero. We write

$$f_0^{\overline{v}}(\tau) = \frac{g_2(\tau)}{g_3(\tau)} \wp\left(\frac{cv\tau + dv}{N}\right),$$

and one can check this is weight 0 and $\Gamma(N)$-invariant, and it is meromorphic on the upper half plane and the cusps.

We define

$$\begin{aligned} f_0 &\coloneqq \sum_{d=0}^{N-1} f_0^{\overline{(0,d)}} \\ f_1 &\coloneqq f_0^{\overline{(0,1)}} \\ f_{(1,0)} &\coloneqq f_0^{\overline{(1,0)}} \\ j_N(\tau) &\coloneqq j(N\tau). \end{aligned}$$

Then we have the following proposition

Proposition .0.7

We have

$$\begin{aligned} \mathbb{C}(X(N)) &= \mathbb{C}(j, f_{1,0}, f_1) \\ \mathbb{C}(X_1(N)) &= \mathbb{C}(j, f_1) \\ \mathbb{C}(X_0(N)) &= \mathbb{C}(j, f_0) = \mathbb{C}(j, j_N). \end{aligned}$$

Moreover, $\mathbb{C}(X(N))/\mathbb{C}(X(1))$ is galois with group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$

We'll talk about this more next time. Of course we get a tower of Galois extensions of all of these.