Sist:

- Introduserte *Frobenius-morfien*: La p være prim, la $q = p^n$. Hvis $K = \mathbb{F}_q$ og $V \subset \mathbb{P}^N$ er en projektiv varietet definert over $\mathbb{F}_q$, så har vi $\mathrm{Fr}_q \colon V \to V$ gitt ved
$$\mathrm{Fr}_q([X_0 : \ldots : X_n]) = [X_0^q : \ldots : X_n^q].$$
- Separabel kropputvidelse: $E \hookrightarrow F$ slik at for alle $\alpha \in F$ er det minimale polynomet til α lik f hvor $f' \neq 0$ (alltid sant hvis $\operatorname{char} E = 0$).
- Separabel morfi av kurver: $\phi \colon C \to D$ hvor $\phi^* \colon \overline{K}(D) \to \overline{K}(C)$ er separabel kropputvidelse.
- For en kurve $C/\mathbb{F}_q$, er $\mathrm{Fr}_q \colon C \to C$ en inseparabel morfi og $\deg(\mathrm{Fr}_q) = q$.

Geometrisk tolkning av separabilitet. Følgende gir litt geometrisk forståelse for hva separabilitet betyr.

La $\phi \colon C \to D$ være morfi av kurver. *Husk:*

- For $P \in C$, er *ramifikasjonsindeks* $e_\phi(P) = \operatorname{ord}(\phi \circ t_{\phi(P)})$, hvor $t_{\phi(P)}$ er lokal parameter i $\phi(P)$.
- $e_\phi(P) \geq 1$, og ϕ er *ramifisert i* P hvis $e_\phi(P) > 1$.
- For alle $Q \in D$, er
$$\deg(\phi) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P).$$

Proposisjon. *Hvis ϕ er separabel, så er ϕ ramifisert i bare endelig mange punkter.*

Hvis ϕ er inseparabel, så er $e_\phi(P) > 0$ og $e_\phi(P) = 0 \pmod p$, hvor $p = \operatorname{char} K$.

Korollar. *Hvis ϕ er separabel, så er $|\phi^{-1}(Q)| = \deg \phi$ unntatt for endelig mange Q.*

Hvis ϕ er inseparabel, så er $|\phi^{-1}(Q)| \leq \frac{\deg \phi}{p} < \deg \phi$ for alle Q, hvor $p = \operatorname{char} K$.

Bevis for korollar. Hvis ϕ er separabel, så finnes det endelig mange P slik at $e_\phi(P) > 1$. Hvis $Q \in D$ ikke er i bildet av noen slik P, har vi
$$\deg(\phi) = \sum_{P \in \phi^{-1}(D)} e_\phi(P) = \sum_{P \in \phi^{-1}(Q)} 1 = |\phi^{-1}(Q)|.$$

Hvis ϕ er inseparabel, så er $e_\phi(P) \geq p$ for alle P, slik at
$$\deg(\phi) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P) \geq p|\phi^{-1}(Q)|,$$
som gir $|\phi^{-1}(Q)| \leq \deg(\phi)/p$. □

Eksempel. La C være definert over $\mathbb{F}_q$. Da er $\deg(\mathrm{Fr}_q) = q$.

Vi har vist at $\mathrm{Fr}_q\colon \mathbb{P}^N \to \mathbb{P}^N$ er en bijeksjon. Det impliserer at $\mathrm{Fr}_q\colon C \to C$ er injektiv, og som morfi av kurver er den da også surjektiv. Dermed er $\mathrm{Fr}_q\colon C \to C$ en bijeksjon.

Dette betyr at det finnes et unikt $P \in C$ slik at $\mathrm{Fr}_q(P) = Q$, og vi har

$$q = \deg(\mathrm{Fr}_q) = e_\phi(P).$$

Eksempel. La $C = \mathbb{P}^1$, og la $Q = [\alpha : 1] \in \mathbb{P}^1$, hvor $P = [\alpha^{1/q} : 1]$ er slik at $\mathrm{Fr}_q(P) = Q$.

Da er $t_Q = x - \alpha$ og $t_P = x - \alpha^{1/q}$ lokale parametere i Q og P, og vi har

$$t_Q \circ \mathrm{Fr}_p = x^q - \alpha = (x - \alpha^{1/q})^q = t_P^q,$$

så $e_{\mathrm{Fr}_q}(P) = q$.

La E være en elliptisk kurve definert over $\mathbb{F}_q$. Vi er interessert i å estimere

$$E(\mathbb{F}_q) = \{P \in E \mid \mathrm{Fr}_q(P) = P\}.$$

Morfien Fr_q er en isogeni. Vi kan dermed danne en ny isogeni $1 - \mathrm{Fr}_q \in \mathrm{End}(E)$, og vi har

$$\mathrm{Fr}_q(P) = P \Leftrightarrow (1 - \mathrm{Fr}_q)(P) = O,$$

og dermed

$$E(\mathbb{F}_q) = \ker(1 - \mathrm{Fr}_q).$$

Vi har

Proposisjon. *Hvis $\phi \in \mathrm{Hom}(E_1, E_2)$ er en separabel isogeni, så er $|\ker\phi| = \deg(\phi)$.*

(Dette viste vi tidligere bare når $\mathrm{char}\, K = 0$, det samme beviset fungerer med *separabilitet* som hypotese i stedet for $\mathrm{char}\, K = 0$.)

Hvis vi kan vise at $1 - \mathrm{Fr}_q$ er separabel, har vi altså $|E(\mathbb{F}_q)| = \deg(1 - \mathrm{Fr}_q)$, som vi kan håpe å estimere.

Differensialer og separabilitet. For å vise at $1 - \mathrm{Fr}_q$ er separabel, må vi knytte separabilitet til differensialer.

La $\phi\colon C \to D$ være en morfi av kurver. Vi har at Ω_C og Ω_D er 1-dimensjonale vektorrom over henholdsvis $\overline{K}(C)$ og $\overline{K}(D)$, henholdsvis. Vi har da en avbildning $\phi^*\colon \Omega_D \to \Omega_C$ definert ved

$$\phi^*(gdf) = (g \circ \phi)d(f \circ \phi).$$

Proposisjon. *Avbildningen $\phi^*\colon \Omega_D \to \Omega_C$ er*

- *injektiv hvis ϕ er separabel.*
- *lik 0 hvis ϕ er inseparabel.*

Eksempel. La $K = \mathbb{F}_q$, og se på $\mathbb{P}^1$, med $\overline{K}(\mathbb{P}^1) = \overline{K}(x)$. Vi vil anvende proposisjonen på $\phi = \mathrm{Fr}_q \colon \mathbb{P}^1 \to \mathbb{P}^1$.

Da er $\Omega_{\mathbb{P}^1}$ generert av dx, og vi har

$$\mathrm{Fr}_q^*(dx) = d(x \circ \mathrm{Fr}_q) = d(x^q) = qx^{q-1}dx = 0,$$

som stemmer med at Fr_q er inseparabel.

Differensialer og gruppestrukturen. La $E \subset \mathbb{P}^2$ være en elliptisk kurve på Weierstrass-form $y^2 = x^3 + Ax + B$.

Se på differensialet $\omega = dx/y \in \Omega_E$. Vi har tidligere vist at ω er regulært, altså at for alle $P \in E$ er $\omega = f dt_P$ hvor t_P er en lokal parameter i P og $\mathrm{ord}_P(f) \geq 0$.

Siden E har genus 1, så er rommet av regulære differensialer

$$\mathcal{L}(K_E) = \{\omega \in \Omega_E \mid \omega \text{ er regulært}\} = \overline{K}. \text{(definisjon av genus)}$$

Proposisjon. *For alle $P \in E$, så er $\tau_P^*(\omega) = \omega$.*

Skisse av bevis. Merk først at $\tau_P^*(\omega)$ er et regulært differensial. (For alle morfier $\phi\colon C \to D$, og $\omega_D \in \Omega_D$, så er $\phi^*(\omega_D)$ regulært hvis ω_D er regulært).

Dermed har vi at $\tau_P^*(\omega) = a_P\omega$ for en $a_P \in \overline{K}$. Man sjekker at avbildningen $P \mapsto a_P$ er definert av en rasjonal funksjon på E, som er regulær i alle punkter. Men en regulær funksjon på E er konstant. Dermed er $a_P = a_O = 1$ for alle P. $\square$

Proposisjon (Vanskelig, vises ikke)**.** *La $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, og la ω være et regulært differensial på E_2. Da er*

$$(\phi + \psi)^*(\omega) = \phi^*(\omega) + \psi^*(\omega)$$

Merk at addisjon på venstre side bruker gruppestrukturen til E_2, mens addisjon på høyre side er med hensyn til gruppestrukturen på Ω_{E_1}.

Korollar. *La E være en elliptisk kurve definert over $\mathbb{F}_q$, og la $m, n \in \mathbb{Z}$. Da er $m + n\,\mathrm{Fr}_q \in \mathrm{End}(E)$ separabel hvis og bare hvis $m \not\equiv 0 \pmod{p}$.*

Bevis. La $\omega \in \Omega_E$ være et regulært differensial. Da er

$$(m+n\,\mathrm{Fr}_q)^*(\omega) = m^*(\omega) + (n\,\mathrm{Fr}_q)^*(\omega) = \omega + \cdots + \omega + \mathrm{Fr}_q^*(\omega) + \cdots + \mathrm{Fr}_q^*(\omega) = m\omega,$$

som er lik 0 hvis og bare hvis $m = 0 \pmod{p}$. Men $(m + n\,\mathrm{Fr}_q)^*\colon \Omega_E \to \Omega_E$ er enten injektiv eller lik 0, avhengig av om $m + n\,\mathrm{Fr}_q$ er separabel, så konklusjonen følger. $\square$

Korollar. *Isogenien $1 - \mathrm{Fr}_q \in \mathrm{End}(E)$ er separabel.*