Vi skal nå se nøyere på tilfellet $\operatorname{char} K = p$, og spesielt på tilfellet der K er en endelig kropp. Spørsmålet vi etter noen forelesninger ønsker å kunne besvare (eller i hvert fall gi et estimat på) er følgende:

Spørsmål: Gitt en elliptisk kurve E definert over en endelig kropp K, hvor mange punkter har $E(K)$? Ekvivalent: Hvor mange $x, y \in K$ finnes det som løser

$$y^2 = x^3 + Ax + B$$

gitt $A, B \in K$?

Endelige kropper

Vi repeterer litt om endelige kropper.

Proposisjon. *La p være et primtall, la $n \geq 0$ være et heltall, og la $q = p^n$. Det finnes (opp til isomorfi), en unik kropp med q elementer, som vi kaller $\mathbb{F}_q$.*

Proposisjon (Fermats lille teorem)**.** *Hvis $x \in \mathbb{F}_q$, så er $x^q = x$.*

Bevis. Ok hvis $x = 0$. Hvis $x \neq 0$, se på den multiplikative gruppa $\mathbb{F}_q^*$. Denne har $q - 1$ elementer, så for alle $x \in \mathbb{F}_q^*$ er $x^{q-1} = 1$, og dermed er $x^q = x$. □

0.1. **Frobenius-homomorfien.** Se på den algebraiske tillukningen $\overline{\mathbb{F}}_p$. Definer en avbildning $\mathrm{Fr}_p \colon \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ ved

$$\mathrm{Fr}_p(x) = x^p.$$

Da er Fr_p en homomorfi av kropper:

$$\mathrm{Fr}_p(xy) = (xy)^p = x^p y^p.$$

$$\mathrm{Fr}_p(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p$$

Her bruker vi at hvis $1 \leq k \leq p-1$, så er $\binom{p}{k} = 0 \pmod{p}$.

Homomorfien Fr_p er faktisk en *isomorfi*:

- Surjektiv: For alle $a \in \overline{\mathbb{F}}_p$ finnes en x slik at $\mathrm{Fr}_p(x) = x^p = a$, siden $\overline{\mathbb{F}}_p$ er algebraisk lukket.
- Injektiv: La $\mathrm{Fr}_p(x) = \mathrm{Fr}_p(y)$. Da er $\mathrm{Fr}_p(x-y) = (x-y)^p = 0$, som betyr at $x - y = 0$ og altså $x = y$.

Ser på mengden

$$\overline{\mathbb{F}}_p^{\mathrm{Fr}_p} = \{x \in \overline{\mathbb{F}}_p \mid \mathrm{Fr}_p(x) = x\} = \{x \in \overline{\mathbb{F}}_p \mid x^p - x = 0\}.$$

Lett å se at denne er lukket under addisjon og multiplikasjon, og er dermed en underkropp av $\overline{\mathbb{F}}_p$. Den består av løsningene til polynomet $x^p - x$, som ikke har doble røtter. Dermed er $|\overline{\mathbb{F}}_p^{\mathrm{Fr}_p}| = p$, så vi har at $\overline{\mathbb{F}}_p^{\mathrm{Fr}_p} = \mathbb{F}_p$.

Mer generelt, for $q = p^n$, la $\mathrm{Fr}_q \colon \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ være $\mathrm{Fr}_q(x) = x^q$. På samme måte som for Fr_p, finner vi Fr_q er en kroppisomorfi og $\overline{\mathbb{F}}_p^{\mathrm{Fr}_q} \cong \mathbb{F}_q$.

0.2. **Frobenius-morfien.** La nå $\overline{K} = \overline{\mathbb{F}}_p$, og se på varieteten $\mathbb{P}^n$ (for oss er n som regel 2). Vi definerer en morfi $\mathrm{Fr}_q \colon \mathbb{P}^n \to \mathbb{P}^n$ ved

$$\mathrm{Fr}_q([X_0 : \ldots : X_n]) = [X_0^q : \ldots : X_n^q].$$

Proposisjon. *Morfien* Fr_q *er en bijeksjon.*

Bevis. Surjektiv: Følger fra at $\overline{K}$ er algebraisk lukket.

Injektiv: La $P = [X_0 : \ldots : X_n] \neq P' = [X_0' : \ldots : X_n']$. Da finnes i, j slik at $X_i/X_j \neq X_i'/X_j'$. Men siden $x \mapsto x^q$ er injektiv, så er da $X_i^q/X_j^q \neq (X_i')^q/(X_j')^q$, som betyr at

$$\mathrm{Fr}_q(P) = [X_0^q : \ldots : X_n^q] \neq \mathrm{Fr}_q(P') = [(X_0')^q : \ldots : (X_n')^q].$$

□

Merknad. Morfien $\mathrm{Fr}_q \colon \mathbb{P}^n \to \mathbb{P}^n$ er *ikke* en isomorfi av varieteter, for den inverse avbildningen (av mengder) $\mathrm{Fr}_q^{-1} \colon \mathbb{P}^n \to \mathbb{P}^n$ gitt ved

$$\mathrm{Fr}_q^{-1}[X_0 : \ldots : X_n] = [X_0^{\frac{1}{q}} : \ldots : X_n^{\frac{1}{q}}]$$

er ikke en morfi.

Her er hovedgrunnen til at Frobeniusmorfien er interessant for oss.

Proposisjon. *Et punkt* $P \in \mathbb{P}^n$ *er definert over* $\mathbb{F}_q$ *hvis og bare hvis* $\mathrm{Fr}_q(P) = P$.

Bevis. La $P = [X_0 : \ldots : X_n]$, og anta WLOG at $X_n \neq 0$. Reskaler slik at $X_n = 1$. Vi har da

$$\begin{gathered} P = [X_0 : \ldots : X_{n-1} : 1] = [X_0^q : \ldots : X_{n-1}^q : 1] = \mathrm{Fr}_q(P) \\ \Updownarrow \\ X_i = X_i^q \quad \forall i \\ \Updownarrow \\ X_i \in \mathbb{F}_q \quad \forall i, \end{gathered}$$

som er hvis og bare hvis P er definert over $\mathbb{F}_q$. □

0.3. **Frobeniusmorfien for generelle varieteter.** La nå $K = \mathbb{F}_q \subset \overline{\mathbb{F}}_p = \overline{K}$. La nå V være en projektiv varietet i $\mathbb{P}^n$ (for oss som regel en elliptisk kurve). Anta at V er definert over $\mathbb{F}_q$.

Lemma. *Hvis* $P \in V$*, så er* $\mathrm{Fr}_q(P) \in V$*. Dermed får vi en morfi* $\mathrm{Fr}_q \colon V \to V$*.*

Bevis. La $f_1, \ldots, f_n \in K[X_0, \ldots, X_n]$ være generatorer av idealet $I_V \subset \overline{K}[X_0, \ldots, X_n]$. Et punkt $P \in \mathbb{P}^n$ ligger i V hvis og bare hvis $f_i(P) = 0$ for alle i. Vi må vise at også $f_i(\mathrm{Fr}_q(P)) = 0$. La

$$f_i = \sum a_{i_0 i_1 \ldots i_n} X_0^{i_0} \cdots X_n^{i_n}, \quad a_\bullet \in \mathbb{F}_q$$

Hvis $P = [y_0 : \ldots : y_n]$, har vi da

$$\begin{aligned} f_i(\mathrm{Fr}_q(P)) &= \sum a_{i_0 i_1 \ldots i_n} x_0^{qi_0} \cdots x_n^{qi_n} \overset{a_\bullet \in \mathbb{F}_q}{=} \sum a^q_{i_0 i_1 \ldots i_n} x_0^{qi_0} \cdots x_n^{qi_n} \\ &= \left(\sum a_{i_0 i_1 \ldots i_n} x_0^{i_0} \cdots x_n^{i_n} \right)^q = (f_i(P))^q = 0. \end{aligned}$$

□

Siden $V \subset \mathbb{P}^n$, har vi at $P \in V$ er definert over $\mathbb{F}_q$ hvis og bare hvis $\mathrm{Fr}_q(P) = P$. For å forstå $V(\mathbb{F}_q)$ (f.eks. antallet punkter i denne mengden), kan vi prøve å forstå morfien Fr_q best mulig.

Separable morfier. La $E \hookrightarrow F$ være en kropputvidelse, la $\alpha \in F$, og la $f = \sum_{i=0}^n c_i x^i$ være det irredusble polynomet til α over E. Vi sier at α er *separabelt* over E hvis den formelle deriverte

$$f' := \sum_{i=0}^{n-1} (i+1) c_{i+1} x^i \neq 0,$$

eller ekvivalent hvis f ikke har noen dobbel rot i $\overline{E}$. Altså er α ikke-separabelt hvis og bare hvis $\operatorname{char} E = p$ og vi har

$$f = c_0 + c_p x^p + c_{2p} x^{2p} + \cdots + c_{ip} x^{ip}. \tag{1}$$

Definisjon. En endelig kropputvidelse $E \hookrightarrow F$ er *separabel* hvis alle $\alpha \in F$ er separable over E.

Eksempel. Hvis $\operatorname{char} E = 0$, så er alle endelige utvidelser separable.

Eksempel. Hvis $\operatorname{char} E = p$ og $[F : E] \neq 0 \pmod p$, så er utvidelsen $E \hookrightarrow F$ separabel.

Bevis for dette: La $\alpha \in F$. Siden

$$[F : E] = [F : E(\alpha)][E(\alpha) : E]$$

og $[F : E]$ ikke er delelig med p, så er $[E(\alpha) : E]$ ikke delelig med p. Dermed er graden til det irredusible polynomet til α ikke delelig med p, så α er separabelt (se (1).

Separable morfier av kurver. La nå $\phi \colon C \to D$ være en ikkekonstant morfi av ikkesingulære, projektive kurver. Vi sier at ϕ er *separabel* hvis kropputvidelsen $\phi^* \colon \overline{K}(D) \to \overline{K}(C)$ er separabel.

Eksempel. Hvis $\operatorname{char} K = 0$ eller $\operatorname{char} K = p$, $\deg \phi \neq 0 \pmod p$, så er ϕ separabel.

Proposisjon. *La $K = \mathbb{F}_q$, og la C være definert over K. Da er $\mathrm{Fr}_q \colon C \to C$ en inseparabel morfi av grad q.*

Bevis i tilfelle $C = \mathbb{P}^1$. La $t = X_0/X_1$, slik at $\overline{K}(\mathbb{P}^1) = \overline{K}(t)$. Da er $\mathrm{Fr}_q^*\colon \overline{K}(t) \to \overline{K}(t)$ gitt ved $\mathrm{Fr}_q^*(f) = f^q$. Altså har vi

$$\begin{array}{ccc} \overline{K}(\mathbb{P}^1) & \xrightarrow{\mathrm{Fr}_q^*} & \overline{K}(\mathbb{P}^1) \\ \| & & \| \\ \overline{K}(t^q) & \hookrightarrow & \overline{K}(t) \end{array}$$

så vi kan se på utvidelsen $\overline{K}(t^q) \hookrightarrow \overline{K}(t)$. Denne er generert av t, som har irreducibelt polynom $x^q - t^q$ av grad q, og som opplagt ikke er separabelt. $\square$