# Section 1

## Projektive varieteter

# Projektive varieteter

$I = (f)$, $f \in K[X, Y, Z]$

$V_I \subset \mathbb{P}^2$

## Definisjoner

Gitt ideal $I \subset \overline{K}[X_0, \ldots, X_n]$ generert av homogene polynomer, er

$$V_I = \{P \in \mathbb{P}^n \mid f_i(P) = 0 \ \forall \text{homogene } f \in I\}.$$

Hvis $I$ er et primideal, er $V_I$ en **projektiv varietet**.

- Den homogene koordinatringen $\overline{K}[V_I] = \overline{K}[X_0, \ldots, X_n]/I$.
- Kroppen av rasjonale funksjoner

$$\overline{K}(V) = \{g/h \mid g, h \in \overline{K}[V_I] \text{ homogene av samme grad}\}^1$$

- En rasjonal funksjon $f$ er **regulær** i $P \in V_I$ hvis $f$ kan skrives som $g/h$ og $h(P) \neq 0$.

[1] Opp til relasjoner g/h = fg/fh

# Rasjonale avbildninger og morfier

$\forall P \in V_1$ er $\phi(P) \in V_2$ hvor $\phi$ er regulær, $\phi : V_1 \longrightarrow V_2$

## Rasjonale avbildninger

Gitt $V_1 \subseteq \mathbb{P}^m$ og $V_2 \subseteq \mathbb{P}^n$, er en **rasjonal avbildning** gitt ved

$$\phi = [f_0 : \ldots : f_n] \quad f_i \in \overline{K}(V_1).$$

slik at hvis alle $f_i$ er regulære i $P \in V_1$ og ikke alle $f_i(P) = 0$, er

$$\phi(P) = [f_0(P) : \ldots : f_n(P)] \in V_2.$$

## Morfi

En rasjonal avbildning er en **morfi** hvis det i hver $P \in V_1$ finnes en representasjon

$$\phi = [f_0 : \ldots : f_n]$$

slik at $[f_0(P) : \ldots : f_n(P)]$ er et veldefinert punkt.

# Varieteter over $K$

## Varieteter definert over $K$

En projektiv varietet $V \subset \mathbb{P}^n$ er **definert over** $K$ hvis den kan defineres av polynomer $f_i$ med koeffisienter i $K$. Mer formelt: Hvis idealet $I(V) \subset \overline{K}[X_0, \ldots, X_n]$ er generert av homogene elementer $f_i \in K[X_0, \ldots, X_n]$. $\subset \overline{K}[X_0, \ldots, X_n]$

## $K$-rasjonale punkter

Hvis $V$ er definert over $K$, er mengden av $K$-**rasjonale punkter**

$$V(K) = \{[\alpha_0 : \ldots : \alpha_n] \in V \mid \forall i, \alpha_i \in K\}.$$

# Section 2

## Ikkesingulære kurver

# Ikkesingulære kurver

$\mathfrak{m}_P/\mathfrak{m}_P^2$ = dualt til tangentrommet

## Definisjon

En **kurve** er en projektiv varietet $C$ av dimensjon 1.
En kurve $C \subset \mathbb{P}^n$ er **ikkesingulær** hvis for alle punkter $P \in C$ har vi at $\mathfrak{m}_P/\mathfrak{m}_P^2 \cong \overline{K}$, hvor $\mathfrak{m}_P \subset \overline{K}[C]_P$ er det maksimale idealet.

## Jacobi-kriteriet

Hvis $C \subset \mathbb{P}^2$ er en kurve definert av polynomet $F \in \overline{K}[X, Y, Z]$, så er $C$ ikkesingulær hvis det ikke finnes noe punkt $P \in \mathbb{P}^2$ slik at

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = F(P) = 0$$

# Ordensfunksjonen

Fra nå: $C$ ikkesing. kurve

La $P \in C$, og la $\mathfrak{m}_P \subset \overline{K}[C]_P$ være det maksimale idealet i den lokale ringen til $C$ i $P$.

$\overline{K}[C]_P$ er en DVR

## Definisjon

For $C$ ikkesingulær og $P \in C$, så er **ordensfunksjonen**

$$\operatorname{ord}_P \colon \overline{K}(C) \to \mathbb{Z}$$

definert ved $\operatorname{ord}_P(f) = k$ hvis $f \in \mathfrak{m}_P^k \setminus \mathfrak{m}_P^{k+1}$, og $\operatorname{ord}_P(fg) = \operatorname{ord}_P(f) \operatorname{ord}_P(g)$.

## Tolkning av $\operatorname{ord}_P$

Hvis $f \in \overline{K}(C)$, så er

- $\operatorname{ord}_P(f) \geq 0 \Leftrightarrow f$ er regulær i $P$
- $\operatorname{ord}_P(f) = 0 \Leftrightarrow f(P) \neq 0$
- $\operatorname{ord}_P(f) = 1 \overset{def}{\Leftrightarrow} f$ er en **lokal parameter i** $P$

# Morfier av ikkesingulære kurver

## Teorem

Hvis $\phi\colon C \to V$ er en rasjonal avbildning fra en ikkesingulær kurve til en projektiv varietet, så er $\phi$ en morfi. Bruker ordensfunksjonen!

## Teorem

En morfi $\phi\colon C_1 \to C_2$ av kurver er enten surjektiv eller konstant.

## Eksempel

Hvis $C_2 = \mathbb{P}^1$, er en morfi $\phi\colon C_1 \to \mathbb{P}^1$ det samme som en rasjonal funksjon, vi kan skrive

$$\phi = [f : 1], \qquad f \in \overline{K}(C_1)$$

så vi får resultatet at en rasjonal funksjon $f$ enten er konstant eller tar alle verdier.

# Kurver er kropper

Hvis $C$ er en ikkesingulær kurve, er $\overline{K}(C)$ en kropp av transcendensgrad 1 over $\overline{K}$. En ikkekonstant morfi $\phi\colon C_1 \to C_2$ definerer en kroppinklusjon $\phi^*\colon \overline{K}(C_2) \to \overline{K}(C_1)$, ved

$$\phi^*(f) = f \circ \phi. \in \overline{K}(C_1)$$

## Teorem

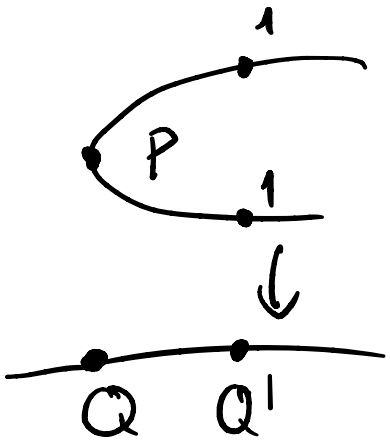
Hvis $\overline{K} \hookrightarrow L$ er en kroppsutvidelse med transcendensgrad 1, så finnes en unik ikkesingulær kurve $C$ slik at $\overline{K}(C) \cong L$ som kropper over $\overline{K}$.
Gitt to kurver $C_1, C_2$, så gir $\phi \mapsto \phi^*$ en *bijeksjon*

$$\{\text{Ikkekonstante morfier } C_1 \to C_2\}$$
$$\updownarrow$$
$$\{\text{Homomorfier } \overline{K}(C_2) \to \overline{K}(C_1) \text{ som fikserer } \overline{K}\}.$$

# Ramifikasjon og grad

La $\phi\colon C_1 \to C_2$ være ikkekonstant, la $P \in C_1$, og la $Q = \phi(P)$.
**Ramifikasjonsindeksen** $e_\phi(P) \in \mathbb{Z}_{\geq 1}$ er gitt ved

$$e_\phi(P) = \operatorname{ord}_P(\phi^*(t_Q)),$$




hvor $t_Q \in \overline{K}(Q)$ er en lokal parameter i $Q$.
**Graden** til $\phi$ er $\deg(\phi) = [\overline{K}(C_1) : \phi^*(\overline{K}(C_2))]$.

## Proposisjon

For alle $Q \in C_2$, er

$$\deg(\phi) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)$$

# Divisorer

Eks: $\mathrm{Pic}(\mathbb{P}^1) = \mathbb{Z}$

$\mathrm{Pic}^0(\mathbb{P}^1) = \{0\}$

## Definisjon

$\mathrm{Div}(C) =$ den frie abelske gruppa generert av punkter i $C$.
Skriver $D \in \mathrm{Div}(C)$ som $D = \sum_{i=1}^{k} n_i(P_i), \quad n_i \in \mathbb{Z},\ P_i \in C.$

## Divisoren til en funksjon

Gitt $f \in \overline{K}(C)^*$, er

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P).$$

## Rasjonal ekvivalens og Picard-gruppa

Skriver $D_1 \sim D_2$ hvis $\exists f \in \overline{K}(C)^*$ slik at $D_1 - D_2 = \mathrm{div}(f)$. Definerer **Picard-gruppa**

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\sim = \mathrm{Div}(C)/\mathrm{div}(\overline{K}(C)^*).$$

# Differensialer

## Definisjon

Rommet av differensialer $\Omega_C$ er $\overline{K}(C)$-vektorrommet utspent av symboler $df$, $f \in \overline{K}(C)$, med relasjoner

$$d(fg) = gdf + fdg, \qquad \forall f, g \in \overline{K}(C)$$
$$da = 0, \qquad \forall a \in \overline{K} \subset \overline{K}(C)$$

## Beregning

Velg en $f$ s.a. $df \neq 0$, da er $\Omega_C = \overline{K}(C) \cdot df$

Vi har $\Omega_C \cong \overline{K}(C)$ som $\overline{K}(C)$-vektorrom.

## Regulære differensialer

Et differensial $\omega \in \Omega_C$ er **regulært** i $P \in C$ hvis vi kan skrive

$$\omega = fdt, \qquad (\text{Her alltid } dt \neq 0)$$

hvor $t$ er lokal parameter i $P$ og $f \in \overline{K}(C)$ er regulær. i $P$.

# Differensialer og genus

## Regulære differensialer

Vi sier at $\omega \in \Omega_C$ er regulært hvis $\omega$ er regulært i alle $P \in C$.

## Genus KJERNEVIKTIG

La $\mathcal{L}(K_C)$ være $\overline{K}$-vektorrommet av regulære differensialer. **Genus** til $C$ er

$$g(C) = \dim_{\overline{K}} \mathcal{L}(K_C).$$

## Eksempler

- $C = \mathbb{P}^1$: Det eneste regulære differensialet er $0 \rightsquigarrow g(\mathbb{P}^1) = 0$.
- $C$ definert av $y^2 = x^3 + Ax + B$: Opp til $\overline{K}$-skalering er det eneste regulære differensialet er $\omega = \frac{dx}{y} \rightsquigarrow g(C) = 1$.

# Riemann–Roch

**Riemann–Roch-spørsmålet:** Hvor "mange" $f \in \overline{K}(C)$ finnes under betingelsene

- $f$ har nullpunkter av orden $\geq n_i \in P_i$, for gitte $n_i > 0, P_i \in C$
- $f$ har poler av orden $\leq m_i \in Q_i$, for gitte $m_i > 0, Q_i \in C$
- $f$ er regulær ellers.

## Seksjoner av en divisor

Gitt $D \in \mathrm{Div}(C)$, er $D \geq 0$ hvis $D = \sum n_i P_i$ med $n_i \geq 0$.

"Rommet av seksjoner av $D$" $= \mathcal{L}(D) = \{f \in \overline{K}(C)^* \mid \mathrm{div}(f) + D \geq 0\}$

Ekvivalent: Hvis $D = \sum n_i P_i - \sum m_i Q_i$ med $m_i, n_i > 0$,

$$f \in \mathcal{L}(D) \Leftrightarrow \mathrm{ord}_{P_i}(f) \geq n_i, \mathrm{ord}_{Q_i}(f) \geq -m_i, \mathrm{ord}_P(f) \geq 0$$

for andre $P \in C$.

# Riemann–Roch-teoremet

Definer **den kanoniske divisoren** $K_C \in \mathrm{Pic}(C)$ ved, for en $\omega \in \Omega_C$,

$$K_C = \mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)(P)$$

$\deg(K_C) = 2g(C) - 2$

## Teorem (Riemann–Roch) (*)

For $D \in \mathrm{Div}(C)$, har vi

$$\dim_K \mathcal{L}(D) - \dim_K \mathcal{L}(K_C - D) = \deg(D) + 1 - g(C)$$

## Et viktig spesialtilfelle

Hvis $g(C) = 1$ og $\deg(D) > 0$, har vi

$\dim \mathcal{L}(K_C - D) = 0$
$g(C) = 1$

$$\dim_K \mathcal{L}(D) = \deg(D)$$

# Section 3

~~Ikkesingulære kurver~~

Elliptiske kurver, én og én

# Elliptiske kurver

## Definisjon

En **elliptisk kurve** er et par $(E, O)$ hvor $E$ er en ikkesingulær kurve av genus 1 og $O \in E$.

## Teorem (*) VIKTIG (+BEVIS)

Hvis $(E, O)$ er en elliptisk kurve, så finnes det en isomorfi $\phi\colon E \to C$, hvor $C \subset \mathbb{P}^2$ er en kurve på *Weierstraß-form*, dvs. definert av

$$y^2 = x^3 + Ax + B, \qquad A, B \in \overline{K}$$

og $\phi(O) = [0 : 1 : 0]$.

# Weierstraß-kurver

Hvis vi har gitt en kurve $E$ på Weierstraß-form

$$y^2 = x^3 + Ax + B \qquad A, B \in \overline{K},$$

så kan vi definere **diskriminanten** $\Delta$ og $j$-**invarianten** som funksjoner av $A, B$.

- $\Delta \neq 0 \Leftrightarrow E$ er ikkesingulær (og dermed elliptisk).
- $j(E_1) = j(E_2) \Leftrightarrow E_1$ er isomorf til $E_2$.

$x^3 + Ax + B$ har 3 distinkte røtter.

For alle $j \in \overline{K}$, så finnes det valg av $A, B$ slik at $j(E) = j$, så altså har vi en bijeksjon

$$\{\text{Elliptiske kurver over } \overline{K}\}/\text{isomorfi} \leftrightarrow \overline{K}$$

$$E \longmapsto j(E)$$

# Gruppestrukturen

Definerer en gruppestruktur på $E$ via

## Teorem

Hvis $D$ er en divisor av grad 0 på $E$, så finnes et unikt punkt $P \in E$ slik at

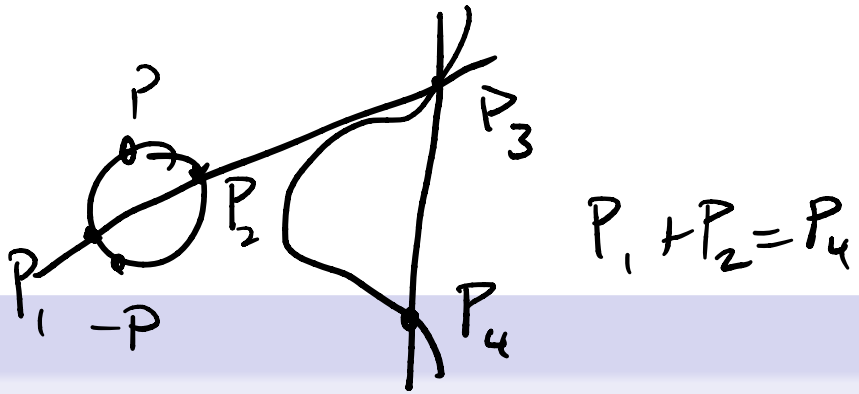
$$D \sim (P) - (O).$$

## Korollar

Avbildningen $D \mapsto P$ (som over) definerer en isomorfi $\mathrm{Pic}^0(E) \to E$, og vi definerer en gruppestruktur på $E$ ved å bruke gruppestrukturen på $\mathrm{Pic}^0(E)$:

$$P_1 + P_2 = P_3 \Leftrightarrow (P_1) - (O) + (P_2) - (O) \sim (P_3) - (O).$$

# Gruppestruktur, geometrisk




## Teorem

Gruppestrukturen på $E$ kan beregnes slik. La $P_1, P_2 \in E$. Trekk linja $l(P_1, P_2)$ gjennom disse, anta at den skjærer $E$ i $P_3$. Trekk linja $l(O, P_3)$, anta at den skjærer $E$ i $P_4$. Da er

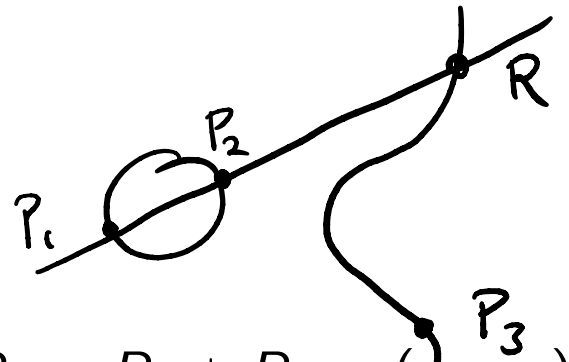
$$P_1 + P_2 = P_4.$$

## Eksempler

- Hvis $P = (x, y) \in E$, så er $-P = (x, -y)$.
- Hvis $2P = O$, så er enten $P = O$, eller $P = (x, 0)$ med $x^3 + Ax + B = 0$.

$2P = 0 \iff P = -P$ $\quad E[2] \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2.$

# Gruppestruktur, formler




La $P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_3 = P_1 + P_2 = (x_3, y_3)$. Da finnes det formler for $x_3$ og $y_3$ som rasjonale funksjoner av $x_i, y_i$. $i = 1, 2$

## Teorem

- Avbildningen $\tau_P \colon E \to E$ gitt ved $\tau_P(Q) = P + Q$ er en morfi.
- Hvis $\phi, \psi \colon V \to E$ er to morfier, så er avbildningen $\phi + \psi$ gitt ved

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

også en morfi.

# Section 4

## Isogenier

# Isogenier

En **isogeni** mellom elliptiske kurver er en morfi $\phi\colon E_1 \to E_2$ slik at $\phi(O_1) = O_2$.

Prop: Hvis $\phi: E_1 \to E_2$ er morfi, så er $\phi = \tau_Q \circ \psi$, $\psi$ er isogeni; $(Q = -\phi(O_1))$

## Teorem

Hvis $\phi$ er en isogeni, så er $\phi$ en gruppehomomorfi.

## Proposisjon

Mengden av isogenier $\mathrm{Hom}(E_1, E_2)$ er en gruppe, med

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

Mengden av isogenier $\mathrm{Hom}(E_1, E_1) =: \mathrm{End}(E_1)$ er en ring, med $\phi\psi = \phi \circ \psi$.

## Eksempel

For alle $n \in \mathbb{Z}$ er avbildningen $[n]\colon E \to E$ gitt ved $[n](P) = nP$ en isogeni.

# Isogenier versus undergrupper (antar her at char $K = 0$)

$\phi : E_1 \to E_2$ $\subset E_1$

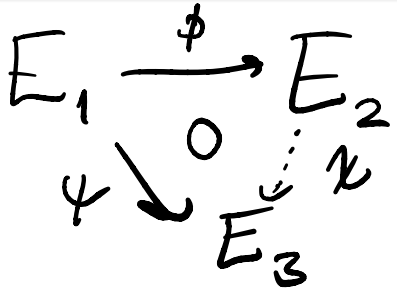
Hvis $\phi$ er en ikkekonstant isogeni, så er $\ker \phi$ en endelig undergruppe, og $|\ker \phi| = \deg \phi$.

**Teorem**

La $G \subset E_1$ være en endelig undergruppe av en elliptisk kurve. Da finnes det en unik elliptisk kurve $E_2$ og en isogeni $\phi\colon E_1 \to E_2$ slik at $\ker \phi = G$.

**Teorem**

La $\phi\colon E_1 \to E_2$ og $\psi\colon E_1 \to E_3$ være isogenier slik at $\ker \phi \subset \ker \psi$. Da finnes det en unik isogeni $\chi\colon E_2 \to E_3$ slik at $\psi = \chi \circ \phi$.

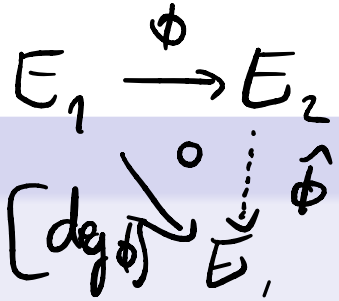


# Den duale isogenien

Gitt en $\phi \in \mathrm{Hom}(E_1, E_2)$, definerer vi **den duale isogenien** $\hat{\phi}$ ved å kreve at

$$\hat{\phi} \circ \phi = [\deg \phi].$$

$\hat{\phi} : E_2 \to E_1$




## Teorem

- $\hat{\phi}$ finnes og er unikt bestemt.
- $\widehat{\phi \circ \psi} = \hat{\psi} \circ \hat{\phi}$
- $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$ ← Vanskelig, viser ikke.
- $\hat{\hat{\phi}} = \phi$

# Beregning av torsjonsgruppene

og $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$

Med den duale isogenien i hende, får vi

## Proposisjon

$\deg[n] = n^2$ for alle $n \in \mathbb{Z}$.

## Korollar

Hvis $\operatorname{char} K = 0$ eller $\operatorname{char} K = p$ og $n \neq 0 \pmod{p}$, så er $|E[n]| = n^2$

$$E[n] := \ker[n] \cong \mathbb{Z}/n \oplus \mathbb{Z}/n.$$

$\deg(\phi\psi) = \deg(\phi)\deg(\psi) \quad \forall\, \phi, \psi \qquad n\phi \neq 0.$

Hvis $\phi \neq 0$ er $\deg(\phi) \neq 0$

$\deg(n\phi) = \deg([n])\deg(\phi) = n^2 \deg(\phi) \neq 0$

# Tate-modulen

Vet nå at $\mathrm{Hom}(E_1, E_2)$ er torsjonsfri abelsk gruppe

Vil vise $\cong \mathbb{Z}^n$ $n \leq 4$.

**Mål:** Begrense rangen til $\mathrm{Hom}(E_1, E_2)$.
**Middel:** Tate-modulen.
La $l$ være primtall, forskjellig fra $\mathrm{char}\, K$.

## $l$-adiske heltall

Ringen $\mathbb{Z}_l$ har elementer sekvenser $a_1, a_2, \ldots$, hvor $a_i \in \mathbb{Z}/l^i$, og vi krever at $a_i = a_{i-1} \pmod{l^{i-1}}$.

## Tate-modulen til $E$

**Tate-modulen** $T_l(E)$ har elementer sekvenser $P_1, P_2, \ldots$, hvor $P_i \in E[l^i]$ og vi krever at $lP_i = P_{i-1}$. Har naturlig struktur av $\mathbb{Z}_l$-modul.

## Beregning

Som $\mathbb{Z}_l$-modul har vi $T_l(E) \cong \mathbb{Z}_l^{\oplus 2}$.

Bruker $E[l^i] = (\mathbb{Z}/l^i)^{\oplus 2}$

# Isogenier til

## Pushforward, Tate-modulen

Gitt $\phi \in \mathrm{Hom}(E_1, E_2)$, har vi $\phi_* \colon T_l(E_1) \to T_l(E_2)$ ved

$$\phi_*((P_i)_{i=1}^{\infty}) = (\phi(P_i))_{i=1}^{\infty}$$

## Injektivitet, svak versjon

Avbildningen $\phi \mapsto \phi_*$ gir en inklusjon
$\mathrm{Hom}(E_1, E_2) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2))$.

## Injektivitet, sterk versjon

Avbildningen $\phi \mapsto \phi_*$ gir en inklusjon
$\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2)) = \mathbb{Z}_l^4$.

## Korollar

$\cong \mathbb{Z}^n \quad n \leq 4.$

$\mathrm{Hom}(E_1, E_2)$ er en fri abelsk gruppe av rang $\leq 4$.

# Strukturen til $\mathrm{End}(E)$

$\mathrm{End}(E) \longrightarrow \mathrm{End}(E)$

$\phi \longmapsto \hat{\phi}$

## Orden

En **orden** i en $\mathbb{Q}$-algebra $\mathcal{K}$ er en ring $R \subset \mathcal{K}$ slik at $R \otimes \mathbb{Q} = \mathcal{K}$.

## Teorem (*)

Ringen $\mathrm{End}(E)$ er en orden i en av følgende tre typer ringer:

1. $\mathbb{Q}$ (og da er $\mathrm{End}(E) = \mathbb{Z}$)
2. $\mathbb{Q}(\sqrt{d})$ for et negativt heltall $d$.
3. $\mathcal{K}(a, b) = \mathbb{Q} \oplus \mathbb{Q}\alpha \oplus \mathbb{Q}\beta \oplus \mathbb{Q}\gamma$, hvor $\alpha^2 = a$, $\beta^2 = b$, $a, b \in \mathbb{Q}_{<0}$, og $\alpha\beta = -\beta\alpha = \gamma$.

Kvaternionisk algebra.

# Elliptiske kurver over endelige kropper

La $q = p^n$, og la $K = \bar{\mathbb{F}}_q$.
Hvis $E$ er definert over $\mathbb{F}_q$, er mengden $E(\mathbb{F}_q)$ endelig. Vi vil estimere kardinaliteten til $E(\mathbb{F}_q)$.

## Frobenius-morfien

Hvis $E$ er definert over $\mathbb{F}_q$, så har vi en morfi $\mathrm{Fr}_q : E \to E$ definert ved

$$\mathrm{Fr}_q(X : Y : Z) = [X^q : Y^q : Z^q]$$

## Teorem

Et punkt $P \in E$ ligger i $E(\mathbb{F}_q)$ hvis og bare hvis $\mathrm{Fr}_q(P) = P$.

$\Updownarrow$

$(1 - \mathrm{Fr}_q)(P) = 0$

## Korollar

Hvis $\phi = \mathrm{Fr}_q - 1 \in \mathrm{Hom}(E, E)$, så er $E(\mathbb{F}_q) = \ker(\mathrm{Fr}_q - 1)$.

# Separabilitet

## Definisjon

En morfi av ikkesingulære kurver $\phi\colon C_1 \to C_2$ er **separabel** hvis kroppinklusjonen $\phi^*\colon \overline{K}(C_2) \to \overline{K}(C_1)$ er det.

## Geometrisk tolkning

$\phi$ separabel $\Leftrightarrow e_\phi(P) = 1$ unntatt i endelig mange $P$.
$\phi$ inseparabel $\Leftrightarrow e_\phi(P) > 1$ i alle $P$.

## Proposisjon

Isogenien $\mathrm{Fr}_q - 1 \in \mathrm{Hom}(E, E)$ er separabel $\rightsquigarrow$
$|\ker(\mathrm{Fr}_q - q)| = \deg(\mathrm{Fr}_q - 1). = |E(\mathbb{F}_q)|$

# Hasses teorem

## Hasses teorem

Hvis $E$ er definert over $\mathbb{F}_q$, så er $|E(\mathbb{F}_q)| = 1 + q + \epsilon$, hvor $|\epsilon| \leq 2\sqrt{q}$.

## Skisse av bevis

- Funksjonen $\phi \to \deg(\phi)$ er kvadratisk.
- Vi vet at $\deg(1) = 1$, $\deg \mathrm{Fr}_q = q$.
- Cauchy–Schwartz' ulikhet gir

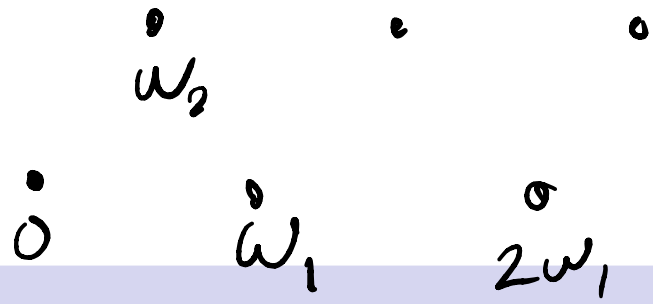
$$\deg(1 - \mathrm{Fr}_q) - \deg(1) - \deg(\mathrm{Fr}_q) \leq 2\sqrt{\deg(1)\deg(\mathrm{Fr}_q)},$$

som gir Hasses teorem.

Section 6

# Elliptiske kurver over $\mathbb{C}$

# Komplekse elliptiske kurver




## Gitter

Et **gitter** er en diskret undergruppe $\Lambda \subset \mathbb{C}$ slik at $\Lambda = \mathbb{Z}^2$.

## Kompleks torus

Gitt et gitter $\Lambda$, får vi en **kompleks torus** $\mathbb{C}/\Lambda$.

## Elliptiske funksjoner

En elliptisk funksjon er en meromorf funksjon $f$ på $\mathbb{C}$ slik at

$$f(z+\omega) = f(z) \quad \forall \omega \in \Lambda$$

$\rightsquigarrow$ $f$ definerer fun. på $\mathbb{C}/\Lambda$

# Elliptiske funksjoner

## Weierstraß' $\wp$-funksjon

Har elliptiske funksjoner

$$\wp(z) = z^{-2} + \sum_{\omega \in \Lambda \setminus \{0\}} ((z-\omega)^{-2} - \omega^{-2})$$

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} (z-\omega)^{-3}.$$

## Fra kompleks torus til elliptisk kurve

Det finnes tall $g_2(\Lambda), g_3(\Lambda) \in \mathbb{C}$ slik at

$$\wp'(z)^2 = 4\wp(z) - g_2(\Lambda)\wp(z) - g_3(\Lambda),$$

og $\phi(z) = [\wp(z) : \wp'(z) : 1]$ definerer en bijeksjon mellom $\mathbb{C}/\Lambda$ og den elliptiske kurven $E_\Lambda$, gitt ved

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$