MAT4240 – Elliptiske Kurver

Innhold

KAPITTEL 1

Introduksjon

1. Konvensjoner

- Hvis p er et primtall og $q = p^n$, skriver vi $\mathbb{F}_q$ for den unike kroppen med q elementer (Seksjon 6).
- K er en perfekt[1] kropp, og $\overline{K}$ er en algebraisk tillukning av K. I eksempler lar vi K være $\mathbb{F}_q$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ eller en algebraisk tillukningen av en av disse.
- Vi antar alltid at $\operatorname{char} K \neq 2, 3$.
- For en mengde (gruppe, ring, ...) S, skriver vi $|S|$ for kardinaliteten til mengden.
- I polynomringen $\overline{K}[x_1, x_2, x_3]$ skriver vi ofte x, y, z i stedet for x_1, x_2, x_3 og tilsvarende X, Y, Z i stedet for X_1, X_2, X_3.

2. Motivasjon

Tema for dette kurset er, som navnet antyder, *elliptiske kurver*. Vi vil etter hvert (Kap. 4) se ulike ekvivalente definisjoner av en elliptisk kurve. For øyeblikket lar vi $\overline{K}$ være en algebraisk lukket kropp av karakteristikk 0 (f.eks. $\mathbb{C}$).

En elliptisk kurve over $\overline{K}$ er da det samme som en *ikkesingulær* kurve i $\mathbb{P}^2$ definert av et homogent polynom $F \in \overline{K}[X, Y, Z]$ av grad 3.

Hvorfor ser man på disse?

2.1. Geometri. Kurver i $\mathbb{P}^2$ noen av de enkleste varietetene man kan definere og studere geometrien til. Man kan vise at hvis $C \subset \mathbb{P}^2$ er en ikkesingulær kurve av grad 1 eller 2, så er C isomorf til $\mathbb{P}^1$ som varietet (og dermed litt kjedelig), men som vi skal se er en elliptisk kurve aldri isomorf til $\mathbb{P}^1$. Elliptiske kurver er på denne måten de enkleste ikketrivielle eksempler på kurver i planet.

Det er mange naturlige spørsmål å stille.

- Gitt en kurve $C \subset \mathbb{P}^n$, kan vi avgjøre om denne er en elliptisk kurve? Det vil si, kan vi avgjøre om C er isomorfi til en tredjegradskurve i $\mathbb{P}^2$?
- Gitt to elliptiske kurver C_1, C_2, kan vi avgjøre om C_1 og C_2 er isomorfe kurver?
- Hvis C_1, C_2 er elliptiske kurver, finnes det morfier mellom C_1 og C_2, og hvordan ser i så fall mengden av morfier ut?

[1] En kropp K er perfekt hvis ethvert irredusibelt polynom $f \in K[x]$ av grad d har d distinkte røtter i $\overline{K}$. Eksempler er:
- Alle kropper av karakteristikk 0.
- Alle algebraisk lukkede kropper.
- Alle endelige kropper.

Alle disse spørsmålene viser seg å ha gode svar som vi skal komme inn på i dette kurset.

En videre egenskap ved elliptiske kurver, som langt fra er opplagt fra definisjonen, er at punktene på en elliptisk kurve på en naturlig måte kan gis struktur av en gruppe, og vi skal se at vi får mye ut av dette for å forstå for eksempel mengden av morfier mellom to elliptiske kurver.

2.2. Tallteori. I den delen av kurset som overlapper med MAT4210, har vi studert algebraiske varieteter definert over en algebraisk lukket kropp. Men algebraisk geometri er også veldig anvendelig i studiet av polynomligninger som skal ha løsninger i en kropp som ikke er algebraisk lukket, f.eks. $\mathbb{Q}$ eller $\mathbb{F}_p$.

Det mest berømte spørsmålet av denne typen er *Fermats siste sats*, som sier at hvis $n > 2$, finnes det ingen positive heltall x, y, z slik at

$$x^n + y^n = z^n.$$

MER HER

KAPITTEL 2

Varieteter

Her vil vi definere varieter, morfier og så videre, se Kap. 1 i [**Sil09**]. Ettersom vi innimellom jobber med en ikke algebraisk lukket kropp K, er definisjonene formulert noe annerledes enn i [**EO**], men i tilfellet hvor $K = \overline{K}$, er de ekvivalente.

Vi lar K være en (perfekt) kropp, og lar $\overline{K}$ være en algebraisk tillukning.

Det affine n-rommet er

$$\mathbb{A}^n = \{(\alpha_1, \ldots, \alpha_n) \mid \alpha_i \in \overline{K}\}.$$

Gitt et ideal $I \subseteq \overline{K}[x_1, \ldots, x_n]$, så definerer vi $V_I \subseteq \mathbb{A}^n$ ved

$$(\alpha_i)_{i=1}^n \in V_I \Leftrightarrow f(\alpha_i) = 0 \forall f \in I.$$

En mengde $V \subseteq \mathbb{A}^n$ er **algebraisk** hvis det finnes et ideal $I \subseteq \overline{K}[x_1, \ldots, x_n]$ slik at $V = V_I$.

Motsatt, hvis $V \subseteq \mathbb{A}^n$ er en algebraisk mengde, kan vi definere idealet $I(V) \subseteq \overline{K}[x_1, \ldots, x_n]$ ved

$$f \in I(V) \Leftrightarrow f(P) = 0 \forall P \in V.$$

THEOREM 2.1 (REF?). *Vi har en bijeksjon*

$$\{\textit{Algebraiske mengder } V \subset \mathbb{A}^n\} \leftrightarrow \{\textit{Idealer } I \subset \overline{K}[x_1, \ldots, x_n] \textit{ slik at } \sqrt{I} = I\}$$
$$V \mapsto I(V)$$
$$V_I \hookleftarrow I$$

DEFINISJON 2.2. En algebraisk mengde $V \subset \mathbb{A}^n$ er **definert over** K, vi skriver V/K, hvis det finnes $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ slik at

$$I(V) = (f_1, \ldots, f_r).$$

Med andre ord er V definert over K hvis vi kan beskrive punktene i V som løsninger av polynomligninger $f_1, \ldots, f_r$ med koeffisienter i K.

EKSEMPEL 2.3. La $K = \mathbb{Q}$, $n = 2$.

- La $I = (y^2 - 3x^3)$. Da er V_I definert over $\mathbb{Q}$, siden $x^2 - 3y^3 \in \mathbb{Q}[x, y]$.
- La $I = ((\sqrt{2} - 1)y^2 + \frac{4}{\sqrt{2}+1}x^2)$. Da er V_I definert over $\mathbb{Q}$, siden

  $$I = ((\sqrt{2} + 1)((\sqrt{2} - 1)y^2 + \frac{4}{\sqrt{2}+1}x^2)) = (y^2 + 4x^2),$$

  og $y^2 + 4x^2 \in \mathbb{Q}[x, y]$.
- La $I = (x - \sqrt{2}y)$. Da er V_I ikke definert over $\mathbb{Q}$. Bevis?

Hvis $V \subseteq \mathbb{A}^n$ er algebraisk, defererer vi idealet $I(V/K) \subseteq K[x_1, \ldots, x_n]$ ved

$$I(V/K) = K[x_1, \ldots, x_n] \cap I(V).$$

PROPOSISJON 2.4. *En algebraisk mengde $V \subset \mathbb{A}^n$ er definert over K hvis og bare hvis*

$$I(V) = (f)_{f \in I(V/K)}.$$

BEVIS. Oppgave. □

DEFINISJON 2.5. **De K-rasjonale punktene til** $\mathbb{A}^n$ er mengden $\mathbb{A}^n(K) \subset \mathbb{A}^n$ gitt ved

$$\mathbb{A}^n(K) = \{(\alpha_i)_{i=1}^n \mid \alpha_i \in K \text{ for alle } i\}.$$

DEFINISJON 2.6. La $V \subseteq \mathbb{A}^n$ være en algebraisk mengde definert over K. Da er **de K-rasjonale punktene til** V delmengden $V(K) \subseteq V$ gitt ved

$$V(K) = V \cap \mathbb{A}^n(K).$$

MERKNAD 2.7. Vi kunne i prinsippet definert $V(K)$ også for en algebraisk mengde $V \subset \mathbb{P}^n$ som ikke er definert over K, ved bare å sette $V(K) = V \cap \mathbb{P}^n(K)$. En slik hypotetisk definisjon av $V(K)$ for vilkårlige V oppfører seg nokså uanstendig, for eksempel har vi ikke noe resultat som sier at hvis V_1 er isomorf til V_2, så er $V_1(K)$ lik $V_2(K)$ (jf. Proposisjon 2.25). Vi krever derfor at V er definert over K for at $V(K)$ skal være definert.

MERKNAD 2.8. En algebraisk mengde V er en type delmengde av $\mathbb{A}^n$, men en algebraisk mengde definert over K er *ikke* en type delmengde av $\mathbb{A}^n(K)$. Gitt en algebraisk mengde $V \subseteq \mathbb{A}^n$ som er definert over K, så kan vi definere $V(K) \subseteq \mathbb{A}^n(K)$, men vi har generelt ingen måte å gjenfinne V fra $V(K)$ på. Som neste eksempel viser, kan for eksempel $V(K) = \varnothing$ selv om $V \neq \varnothing$.

EKSEMPEL 2.9. La $K = \mathbb{R}$, $\overline{K} = \mathbb{C}$, og la $I = (x^2 + y^2 - a)$. Da er

$$V_I(\mathbb{R}) = \varnothing \text{ hvis } a < 0$$
$$V_I(\mathbb{R}) = \{(0,0)\} \text{ hvis } a = 0$$
$$V_I(\mathbb{R}) = \text{ en sirkel med radius } \sqrt{a} \text{ hvis } a > 0.$$

EKSEMPEL 2.10. La $K = \mathbb{Q}$, og la $I = (x^n + y^n - 1)$. Da er Fermats siste sats ekvivalent til påstanden at for $n \geq 3$, så er

$$V_I(\mathbb{Q}) \subseteq \{(-1,0), (1,0), (0,-1), (0,1)\}.$$

1. Projektive varieteter

DEFINISJON 2.11. En mengde $V \subset \mathbb{P}^n$ er en **projektiv varietet** hvis det finnes et homogent primideal $I \subset \overline{K}[X_0, \ldots, X_n]$ slik at

$$V = V_I = \{P \in \mathbb{P}^n \mid F(P) = 0 \text{ for alle homogene } F \in I\}.$$

Notasjonen $F(P) = 0$ over er egentlig en hvit løgn. Merk at et polynom $F \in \overline{K}[X_0, \ldots, X_n]$ ikke definerer en funksjon på $\mathbb{P}^n$. Vi kunne prøve oss med å erklære, for $P = [\alpha_0 : \ldots : \alpha_n] \in \mathbb{P}^n$, at

$$F(P) = F(\alpha_0, \ldots, \alpha_n)?$$

Men siden de homogene koordinatene α_i til P kun er veldefinert opp til skalering, gir ikke dette noen entydig bestemt verdi for $F(P)$.

Men hvis F er et *homogent* polynom, så har vi at

$$F(\lambda\alpha_i) = \lambda^{\deg F} F(\alpha_i),$$

for alle $\lambda \in \overline{K}^*$.

EKSEMPEL 2.12. Tar vi $I = (0)$, får vi den projektive varieteten $\mathbb{P}^n$

EKSEMPEL 2.13. Hvis $f \in \overline{K}[X, Y, Z]$ er et irredusibelt homogent polynom, får vi en projektiv varietet $V = V(f) \subset \mathbb{P}^2$. En slik varietet V kalles en **plan kurve**. Som vi skal se, er elliptiske kurver alle beskrevet på denne måten, så denne klassen av projektive varieteter er den viktigste for våre formål.

Hvis $V \subset \mathbb{P}^n$ er en projektiv varietet, så er $I(V) \subset \overline{K}[X_0, \ldots, X_n]$ idealet generert av homogene $f \in \overline{K}[X_0, \ldots, X_n]$ slik at $f(P) = 0$ for alle $P \in V$.

DEFINISJON 2.14. Hvis $V \subset \mathbb{P}^n$ er en projektiv varietet, så er **den homogene koordinatringen**

$$\overline{K}[V] = \overline{K}[X_0, \ldots, X_n]/I_V$$

Siden I_V er generert av homogene elementer, så er ringen $\overline{K}[V]$ gradert.

Elementene $F \in \overline{K}[V]$ er ikke funksjoner på V. Vi kunne forsøke å sette, for $P = [\alpha_0 : \ldots : \alpha_n] \in V$ og $F \in \overline{K}[V]$, at

$$F(P) = F(\alpha_0, \ldots, \alpha_n),$$

hvor vi representerer F som et polynom i $X_0, \ldots, X_n$. Men de homogene koordinatene α_i til P er ikke entydig bestemt, de er bare definert opp til skalering, og dermed er ikke dette en gyldig definisjon av $F(P)$.

Men merk at hvis F er homogent av grad n, så er

$$F(\lambda\alpha_0, \ldots, \lambda\alpha_n) = \lambda^n F(\alpha_0, \ldots, \alpha_n).$$

Hvis nå $G \in \overline{K}[V]$ er et annet homogent element av grad n, får vi at

$$\frac{F(\lambda\alpha_i)}{G(\lambda\alpha_i)} = \frac{\lambda^n F(\alpha_i)}{\lambda^n G(\alpha_i)} = \frac{F(\alpha_i)}{G(\alpha_i)},$$

så i de punktene $P \in V$ som er slik at $G(\alpha_i) \neq 0$, vil uttrykket F/G gi en veldefinert funksjon. Dette motiverer følgende definisjon.

DEFINISJON 2.15. La V være en projektiv varietet, og la $F(\overline{K}[V])$ være brøkkroppen til $\overline{K}[V]$. **Funksjonskroppen** til V, med notasjon $\overline{K}(V)$, er underkroppen av $F(\overline{K}[V])$ gitt ved

$$\overline{K}(V) = \left\{ \frac{F}{G} \in F(\overline{K}(V)) \mid F, G \in \overline{K}[V] \text{ er homogene av samme grad} \right\}$$

DEFINISJON 2.16. En rasjonal funksjon $f \in \overline{K}(V)$ er **regulær** eller **definert** i et punkt $P \in V$ hvis vi kan finne homogene $G, H \in \overline{K}[V]$ slik at $f = \frac{G}{H}$ og $H(P) \neq 0$.

Hvis f er regulær i P, kan vi definere $f(P) = \frac{G(P)}{H(P)} \in \overline{K}$. Ved diskusjonen over gir dette et veldefinert element av $\overline{K}$.

MERKNAD 2.17. En rasjonal funksjon $f = \frac{G}{H} \in \overline{K}(V)$ kan være regulær i P selv om $H(P) = 0$, for det kan likevel tenkes at vi kan finne en annen presentasjon $f = \frac{G'}{H'}$, med $H'(P) = 0$.

Hvis $V \subset \mathbb{P}^n$, og $f = G/H \in \overline{K}(V)$, så kan $G, H \in \overline{K}[V]$ representeres ved polynomer i variablene $X_0, \ldots, X_n$. La oss si at

$$G = \sum_{i_0,\ldots,i_n} a_{i_0,\ldots,i_n} X_0^{i_0} \cdots X_n^{i_n} \qquad a_{i_0,\ldots,i_n} \in \overline{K}$$
$$H = \sum_{i_0,\ldots,i_n} b_{i_0,\ldots,i_n} X_0^{i_0} \cdots X_n^{i_n} \qquad b_{i_0,\ldots,i_n} \in \overline{K}$$

La oss anta at V ikke er inneholdt i mengden

$$V_{(X_0)} = \{[0 : \alpha_1 : \ldots : \alpha_n] \mid \alpha_i \in \overline{K}\} \subset \mathbb{P}^n.$$

Da er $0 \neq X_0 \in \overline{K}[V]$, så vi har funksjoner $x_i = X_i/X_0 \in \overline{K}(V)$. Vi kan dermed uttrykke

$$f = \frac{G}{H} = \frac{\sum_{i_0,\ldots,i_n} a_{i_0,\ldots,i_n} X_0^{i_0} \cdots X_n^{i_n}}{\sum_{i_0,\ldots,i_n} b_{i_0,\ldots,i_n} X_0^{i_0} \cdots X_n^{i_n}} = \frac{\sum_{i_0,\ldots,i_n} a_{i_0,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}}{\sum_{i_0,\ldots,i_n} b_{i_0,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}}.$$

Siden vi har en slik presentasjon av f for enhver $f \in \overline{K}(V)$, har vi nå vist følgende resultat.

PROPOSISJON 2.18. *Hvis $V \subsetneq \mathbb{P}^n$ er en projektiv varietet som ikke er inneholdt i mengden $V_{(X_0)} \subset \mathbb{P}^n$, så er $\overline{K}(V)$ generert som kropp av de rasjonale funksjonene $x_1, \ldots, x_n \in \overline{K}(V)$.*

1.1. Projektive varieteter over K.

DEFINISJON 2.19. En projektiv varietet $V \subset \mathbb{P}^n$ er **definert over** K hvis det finnes et homogent primideal $I \subset \overline{K}[X_0, \ldots, X_n]$ slik at

$$V = V_I = \{P \in \mathbb{P}^n \mid F(P) = 0\},$$

og som tilfredsstiller at I er generert av homogene elementer $F_1, \ldots, F_i \in K[X_0, \ldots, X_n]$.

2. Morfier

Hvis $V_1 \subseteq \mathbb{P}^m$ og $V_2 \subset \mathbb{P}^n$ er projektive varieteter, så er en **rasjonal avbildning** $\phi\colon V_1 \to V_2$ definert av elementer $f_0, \ldots, f_n \in \overline{K}(V_1)$, og vi skriver

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

Vi krever at hvis $P \in V_1$ er slik at alle f_i er definert i P og ikke alle f_i er 0, så er $[f_0(P) : \ldots : f_n(P) \in V_2$.

MERKNAD 2.20. For en rasjonal avbildning ϕ er ikke f_i entydig bestemt: Vi har, for alle $g \in \overline{K}(V_1)^*$, at

$$\phi = [f_0 : \ldots : f_n] = [gf_0 : \ldots : gf_n].$$

Hvis $V \subset \mathbb{P}^m$ er en projektiv varietet, så kan en morfi $\phi\colon V \to \mathbb{P}^n$ også defineres av $[F_0 : \ldots : F_n]$ med $F_i \in \overline{K}[V_1]$, hvor F_i er homogene av samme grad, ved å sette

$$\phi = [F_0 : \ldots : F_n] = [\frac{F_0}{F_i} : \ldots : \frac{F_n}{F_i}].$$

EKSEMPEL 2.21. Vi har to ekvivalente presentasjoner av en morfi $\phi : \mathbb{P}^1 \to \mathbb{P}^2$ ved

$$\phi([X : Y]) = [X/Y : 1 : Y^2/X^2] \quad \text{eller} \quad \phi([X : Y]) = [X^3 : YX^2 : XY^2]$$

DEFINISJON 2.22. En rasjonal avbildning $\phi\colon V \to \mathbb{P}^n$ er **definert** eller **regulær** i $P \in V$ hvis det finnes en $g \in \overline{K}(V)^*$ slik at

$$[gf_0(P) : \ldots : gf_n(P)]$$

er et veldefinert punkt (dvs. at alle gf_i er definert i P, og ikke alle $gf_i(P) = 0$).

ϕ er **morfi** hvis den er regulær i alle punkter.

PROPOSISJON 2.23. *Hvis V_1, V_2 er projektive varieteter definert over K og $\phi\colon V_1 \to V_2$ er en morfi definert over K, så er $\phi(V_1(K)) \subseteq V_2(K)$.*

BEVIS. La $P \in V_1(K)$. Siden ϕ en morfi og definert over K, kan vi skrive $\phi = [f_0 : \ldots, f_n]$, hvor $f_i \in K(V_1)$ og alle f_i definert i P. Dermed er $\phi(P) = [f_0(P) : \ldots : f_n(P)] \in \mathbb{P}^n(K) \cap V_2 = V_2(K)$. □

DEFINISJON 2.24. La V_1, V_2 være projektive varieteter. Vi sier V_1 og V_2 er isomorfe (skriver $V_1 \cong V_2$) hvis $\exists$ morfier $\phi\colon V_1 \to V_2$, $\psi\colon V_2 \to V_1$, slik at $\phi \circ \psi = \mathrm{id}_{V_2}$ og $\psi \circ \phi = \mathrm{id}_{V_1}$.

Hvis V_1, V_2 er definert over K, sier vi at V_1 og V_2 er isomorfe over K hvis vi kan finne ϕ, ψ som over, definert over K.

PROPOSISJON 2.25. *Hvis V_1, V_2 er isomorfe over K, så er $V_1(K)$ i bijeksjon med $V_2(K)$.*

BEVIS. Vi har avbildninger $\phi : V_1(K) \to V_2(K)$ og $\psi : V_2(K) \to V_1(K)$ slik at $\phi \circ \psi = \mathrm{id}_{V_1(K)}$ og $\psi \circ \phi = \mathrm{id}_{V_2(K)}$. □

EKSEMPEL 2.26. La $K = \mathbb{R}$. La $V_a \subset \mathbb{P}^2$ være gitt ved

$$X^2 + Y^2 + aZ^2.$$

Påstand 1: $V_a \cong V_b$ når $a, b \neq 0$.

Bevis: Definer morfiene $\phi\colon V_a \to V_b$ og $\psi\colon V_b \to V_a$ ved

$$\phi([x : y : z]) = [x : y : (b/a)^{1/2}z], \quad \psi([x : y : z]) = [x : y : (a/b)^{1/2}z]$$

Påstand 2: $V_a/\mathbb{R} \cong V_b/\mathbb{R} \Leftrightarrow a$ og b har samme fortegn.

Bevis $\Leftarrow$: $(a/b)^{\pm 1/2} \in \mathbb{R}$ betyr at ϕ, ψ er definert over $\mathbb{R}$.

Bevis $\Rightarrow$: $V_a(\mathbb{R}) = \varnothing$ hvis $a < 0$, $V_a(\mathbb{R}) =$ sirkel hvis $a > 0$.

KAPITTEL 3

Kurver

DEFINISJON 3.1. En **kurve** er en projektiv varietet av dimensjon 1.

EKSEMPEL 3.2. Det enkleste eksempelet er kurven $\mathbb{P}^1$, og for alle definisjoner og resultater i dette kapittelet er det verdt å spørre hva som skjer i tilfellet $\mathbb{P}^1$.

Vi har den homogene koordinatringen $\overline{K}[\mathbb{P}^1] = \overline{K}[X, Y]$. Vi skriver $x = \frac{X}{Y}$, og har at kroppen av rasjonale funksjoner $\overline{K}(\mathbb{P}^1) = \overline{K}(x)$.

Gitt $\alpha \in \overline{K}$, skriver vi noen ganger $\alpha \in \mathbb{P}^1$ for punktet med homogene koordinater $[\alpha : 1]$, og $\infty \in \mathbb{P}^1$ for punktet med homogene koordinater $[1 : 0]$. Dette gir en bijeksjon $\overline{K} \cup \{\infty\} \leftrightarrow \mathbb{P}^1$.

1. Ordensfunksjonen

For $P \in C$, er $\overline{K}[C]_P$ **den lokale ringen** til C, definert som

$$\overline{K}[C]_P = \{f \in \overline{K}(C) \mid f \text{ regulær i } P\}.$$

Ringen *er* en lokal ring i kommutativ-algebra-forstand: Det finnes et unikt maksimalt ideal $\mathfrak{m}_P \subset \overline{K}[C]_P$ gitt ved

$$\mathfrak{m}_P = \{f \in \overline{K}[C]_P \mid f(P) = 0\}.$$

DEFINISJON 3.3. En lokal ring R med maksimalt ideal $\mathfrak{m}$ er en **diskret valuasjonsring** (DVR) hvis R er Noethersk og $\mathfrak{m}$ er et prinsipalt ideal.

EKSEMPEL 3.4. La $P = \alpha = [\alpha : 1] \in \mathbb{P}^1$. En rasjonal funksjon $f \in \overline{K}(\mathbb{P}^1) = \overline{K}(x)$ kan faktoriseres som

$$f = \beta(x - \alpha)^n \left(\prod_{i=1}^{m} (x - \alpha_i)^{n_i} \right),$$

hvor $\beta \in \overline{K}$ og $\alpha, \alpha_1, \ldots, \alpha_n \in \overline{K}$ er distinkte.

Funksjonene $(x - \alpha_i)^{n_i}$ er alle regulære i P, og $(x - \alpha)^n$ er regulær i P hvis og bare hvis $n \geq 0$. Dermed er $f \in \overline{K}[\mathbb{P}^1]_P$ hvis og bare hvis $n \geq 0$.

Hvis $f \in \overline{K}[\mathbb{P}^1]_P$, så er $f(P) = 0$ hvis og bare hvis $n \geq 1$. Dette er hvis og bare hvis $f = (x - \alpha)g$ med $g \in \overline{K}[\mathbb{P}^1]_P$, som betyr at $(x - \alpha)$ er en generator for $\mathfrak{m}_P \subset \overline{K}[\mathbb{P}^1]_P$, og dermed er $\overline{K}[\mathbb{P}^1]_P$ er en DVR.

På samme måte som over kan vi se på et punkter $[1 : \alpha] \in \mathbb{P}^1$, og finner at $x^{-1} - \alpha$ er en lokal parameter i $[1 : \alpha]$. Spesielt er x^{-1} en lokal parameter i $\infty = [1 : 0]$.

Det finnes et utall ekvivalente kriterier for når en ring er en DVR, Wikipedia gir minst 11 ulike.

PROPOSISJON 3.5 ([**EO**, Proposjoner 7.4. & 9.3.]). *En kurve C er ikkesingulær i et punkt P hvis og bare hvis $\overline{K}[C]_P$ er en DVR.*

Vi lar fra nå av C være en kurve med et gitt ikkesingulært punkt P, og ser nærmere på strukturen til $\overline{K}[C]_P$. De fleste resultatene nedenfor gjelder også for en generell DVR, men vi nøyer oss med å formulere dem for $\overline{K}[C]_P$.

Strukturen til en DVR er veldig enkel, i hvert fall hvis vi ser på idealene den inneholder.

PROPOSISJON 3.6 ([**EO**, Prop. 9.3]). *La P være et ikkesingulært punkt på en kurve C.*

Hvis $I \subseteq \overline{K}[C]_P$ er et ideal, har vi enten $I = \mathfrak{m}_P^i$ for $i \geq 0$ eller $I = (0)$.

For $0 \leq i < j$ er $\mathfrak{m}_P^j \subsetneq \mathfrak{m}_P^i$.

DEFINISJON 3.7. Hvis $t \in \overline{K}[C]_P$ er slik at $\mathfrak{m}_P = (t)$, så sier vi at t er en **lokal parameter** for C i P.

EKSEMPEL 3.8. Ved Eksempel 3.4 er $x-\alpha$ en lokal parameter i punktet $[\alpha : 1] \in \mathbb{P}^1$.

La $0 \neq f \in \overline{K}[C]_P$. Ved Proposisjon 3.6, er $(f) = \mathfrak{m}_P^n$ for en eller annen n. Vi bruker dette til å definere følgende funksjon på $\overline{K}[C]_P$.

DEFINISJON 3.9 (Ordensfunksjonen på den lokale ringen). Funksjonen $\mathrm{ord}_P \colon \overline{K}[C]_P \to \mathbb{N} \cup \{\infty\}$ er gitt ved

$$\mathrm{ord}(0) = \infty$$
$$\mathrm{ord}(f) = n \Leftrightarrow (f) = \mathfrak{m}_P^n \quad \forall f \in \overline{K}[C]_P \setminus \{0\}$$

Vi kaller ofte tallet $\mathrm{ord}_P(f)$ for **forsvinningsordenen** til f i P.

PROPOSISJON 3.10. *For $f_1, f_2 \in \overline{K}[C]_P$ har vi*

$$\mathrm{ord}_P(f_1 f_2) = \mathrm{ord}_P(f_1) + \mathrm{ord}_P(f_2)$$
$$\mathrm{ord}_P(f_1 + f_2) \geq \min(\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2)).$$

Hvis $\mathrm{ord}_P(f_1) < \mathrm{ord}_P(f_2)$, har vi $\mathrm{ord}_P(f_1 + f_2) = \mathrm{ord}_P(f_1)$.

BEVIS. Opplagt hvis enten f_1 eller f_2 er lik 0.

Hvis ikke, har vi

$$(f_1 f_2) = (f_1)(f_2) = \mathfrak{m}_P^{\mathrm{ord}_P(f_1)} \mathfrak{m}_P^{\mathrm{ord}_P(f_2)} = \mathfrak{m}_P^{\mathrm{ord}_P(f_1)+\mathrm{ord}_P(f_2)},$$

som viser at $\mathrm{ord}_P(f_1 f_2) = \mathrm{ord}_P(f_1) + \mathrm{ord}_P(f_2)$.

Vi har

$$f_1 + f_2 \in (f_1, f_2) = \mathfrak{m}_P^{\mathrm{ord}_P(f_1)} + \mathfrak{m}_P^{\mathrm{ord}_P(f_2)} = \mathfrak{m}_P^{\min(\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2)},$$

så

$$\mathfrak{m}_P^{\mathrm{ord}_P(f_1+f_2)} = (f_1 + f_2) \subseteq \mathfrak{m}_P^{\min(\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2))},$$

altså er $\mathrm{ord}_P(f_1 + f_2) \leq \min(\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2)$.

Hvis $\mathrm{ord}_P(f_1) < \mathrm{ord}_P(f_2)$, så har vi at

$$\mathrm{ord}_P(f_1 + f_2) \geq \min(\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2)) = \mathrm{ord}_P(f_1).$$

Anta for en motsigelse at $\operatorname{ord}_P(f_1+f_2) > \operatorname{ord}_P(f_1)$. Da er

$$\operatorname{ord}_P(f_1) \geq \min(\operatorname{ord}_P(f_1+f_2), \operatorname{ord}_P(-f_2)) = \min(\operatorname{ord}_P(f_1+f_2), \operatorname{ord}_P(f_2)) > \operatorname{ord}_P(f_1),$$

som gir en motsigelse. Altså er $\operatorname{ord}_P(f_1+f_2) = \operatorname{ord}_P(f_1)$. □

Enhver rasjonal funksjon $f \in \overline{K}(C)$ kan skrives som en brøk $f = g/h$ med $g, h \in \overline{K}[C]_P$ (oppgave 2.6) Vi kan dermed utvide $\operatorname{ord}_P \colon \overline{K}[C]_P \to \mathbb{Z} \cup \infty$ til en funksjon $\operatorname{ord}_P \colon \overline{K}(C) \to \mathbb{Z} \cup \{\infty\}$ ved å sette

$$\operatorname{ord}_P\left(\frac{g}{h}\right) = \operatorname{ord}_P(g) - \operatorname{ord}_P(h), \qquad \forall g, h \in \overline{K}[C]_P.$$

For $f \in \overline{K}(C)$ har vi:

- $\operatorname{ord}_P(f) \geq 0 \Leftrightarrow f$ er definert i P.
- $\operatorname{ord}_P(f) > 0 \Leftrightarrow f(P) = 0$.
- $\operatorname{ord}_P(f) = 1 \Leftrightarrow f$ er en lokal parameter i P.
- $\operatorname{ord}_P(f) < 0 \overset{def}{\Leftrightarrow} f$ har en pol i P.

EKSEMPEL 3.11. For en $\alpha \in \overline{K}$, så er funksjonen $x - \alpha \in \overline{K}(\mathbb{P}^1)$ regulær i alle P, unntatt i ∞.

PROPOSISJON 3.12. *Hvis t er en lokal parameter i P, så er $\operatorname{ord}_P(f)$ tallet n slik at*

$$f = t^n g,$$

hvor g er regulær i P og $g(P) \neq 0$.

BEVIS. Betingelsene på g er ekvivalente med at $\operatorname{ord}_P(g) = 0$, så

$$\operatorname{ord}_P(f) = \operatorname{ord}_P(t^n)\operatorname{ord}_P(g) = n.$$

□

EKSEMPEL 3.13. Vi ser igjen på tilfellet $\mathbb{P}^1$. Ved Eksempel 3.4, så er x en lokal parameter i $[0:1]$, den er regulær og ulik 0 i $[\alpha:1]$ for $\alpha \neq 0$. Siden x^{-1} er en lokal parameter i $\infty = [1:0]$, får vi altså

$$\operatorname{ord}_{[0:1]}(x) = 1$$
$$\operatorname{ord}_{[\alpha:1]}(x) = 0 \text{ for } \alpha \neq 0$$
$$\operatorname{ord}_{[1:0]}(x) = -1.$$

I Eksempel 3.4 har vi også sett at $x-\alpha$ er en lokal parameter i $[\alpha:1]$, og er regulær og ulik 0 i $[\beta:1]$ for $\beta \neq \alpha$. Videre er

$$\operatorname{ord}_{[0:1]}(x-\alpha) = \operatorname{ord}_{[0:1]}(x) = -1,$$

siden $\operatorname{ord}_{[0:1]}(-\alpha) = 0$ (se Proposisjon 3.10). Dermed har vi

$$\operatorname{ord}_{[\alpha:1]}(x-\alpha) = 1$$
$$\operatorname{ord}_{[\beta:1]}(x-\alpha) = 0 \text{ for } \beta \neq \alpha$$
$$\operatorname{ord}_{[1:0]}(x-\alpha) = -1.$$

En generell rasjonal funksjon $f = \beta \prod_{i=1}^{m} (x-\alpha_i)^{n_i} \in \overline{K}(\mathbb{P}^1)$, med distinkte $\alpha_i \in \overline{K}$ har dermed

$$\begin{aligned} \operatorname{ord}_{[\alpha_i:1]}(f) &= n_i \\ \operatorname{ord}_{\infty}(f) &= -\sum_{i=1}^{m} n_i \\ \operatorname{ord}_{[\alpha:1]}(f) &= 0 \text{ for } \alpha \notin \{\alpha_1, \ldots, \alpha_m\}. \end{aligned}$$

EKSEMPEL 3.14. La $C \subset \mathbb{P}^2$ være definert ved

$$y^2 - x^3 - x = 0 \quad \text{altså } ZY^2 - X^3 - Z^2X = 0$$

Vi påstår at y er lokal parameter i $(0,0) \in C$. Må sjekke at $(y) = \mathfrak{m}_{(0,0)} \subseteq \overline{K}[C]_{(0,0)}$, holder å sjekke $\overline{K}[C]_{(0,0)}/(y) = \overline{K}$.

Vi regner:

$$\overline{K}[C]_{(0,0)} = (\overline{K}[x,y]/(y^2 - x^3 - x))_{(x,y)} = \overline{K}[x,y]_{(x,y)}/(y^2 - x^3 - x),$$

så

$$\begin{aligned} \overline{K}[C]_{(0,0)}/(y) &= \overline{K}[x,y]_{(x,y)}/(y, y^2 - x^3 - x) \\ &= \overline{K}[x,y]_{(x,y)}/(y, x^3 - x) = \overline{K}[x,y]_{(x,y)}/(y,x) = \overline{K}, \end{aligned}$$

siden $x^3 - x = (x^2 - 1)x$ og $x^2 - 1$ er invertibelt i $\overline{K}[x,y]_{(x,y)}$.

Hva med $\operatorname{ord}_{(0,0)}(x)$? Her kan vi skrive

$$xy^{-2} = x(x^3 + x)^{-1} = (1 + x^2)^{-1}$$

har vi

$$0 = \operatorname{ord}_{(0,0)}(xy^{-2}) = \operatorname{ord}_{(0,0)}(x) - 2\operatorname{ord}_{(0,0)}(y),$$

og dermed $\operatorname{ord}_{(0,0)}(x) = 2$.

PROPOSISJON 3.15 ([**Sil09**, Prop. II.1.2], [**EO**, Thm. 10.40]). *Hvis $0 \neq f \in \overline{K}(C)$, så er*

- $\operatorname{ord}_P(f) = 0$ *bortsett fra i endelig mange punkter*
- $\sum_{P \in C} \operatorname{ord}_P(f) = 0$
- *Hvis f ikke har noen poler (f er regulær overalt), så er f konstant.*

2. Morfier av kurver

Gitt to projektive varieteter V_1, V_2, har vi i Kapittel 2 introdusert to ulike typer avbildninger $\phi\colon V_1 \to V_2$. Vi har for det første *rasjonale avbildninger*, definert av formler $\phi = [f_0 : \ldots : f_n]$, med $f_i \in \overline{K}(V_1)$. Hvis en rasjonal avbildning ϕ er regulær i alle $P \in V_1$, er ϕ en *morfi*, og dermed kan vi også tenke på ϕ som en funksjon fra V_1 til V_2. Det viser seg at hvis V_1 er en ikkesingulær kurve, er vi så heldig stilt at en rasjonal avbildning ϕ alltid vil være en morfi.

PROPOSISJON 3.16. *La C være en ikkesingulær kurve, la $V \subset \mathbb{P}^N$ være en projektiv varietet, og la $\phi\colon C \to V$ være en rasjonal avbildning. Da er ϕ regulær overalt, med andre ord er ϕ en morfi.*

BEVIS. Gitt $P \in C$ må vi sjekke at ϕ er regulær i P. Skriv

$$\phi = [f_0 : \ldots : f_N] \text{ med } f_i \in \overline{K}(C),$$

la $n_i = \operatorname{ord}_P(f_i)$ og $n = \min n_i$.

La $t \in \overline{K}(C)$ være lokal parameter for C i P, og skriv ϕ som

$$\phi = [t^{-n} f_0 : \ldots : t^{-n} f_N].$$

For alle i er $\operatorname{ord}_P(t^{-n} f_i) = n_i - n \geq 0 \Rightarrow t^{-n} f_i$ definert i P.

Det fins en i slik at $\operatorname{ord}_P(t^{-n} f_i) = n_i - n = 0 \Rightarrow (t^{-n} f_i)(P) \neq 0$.

Så ϕ er regulær i P. □

MERKNAD 3.17. Det er viktig her både at C er ikkesingulær og at den er en kurve (se oppg. 1.6, 1.7 i [**Sil09**]).

EKSEMPEL 3.18. La C være en ikkesingulær kurve, og la $f \in \overline{K}(C)$. Vi kan definere en rasjonal avbildning

$$\phi_f = [f : 1] \colon C \to \mathbb{P}^1.$$

Ved Proposisjon 3.16, er ϕ_f morfi, beskrevet på punkter ved:

- Hvis f er definert i P,

$$\phi_f(P) = [f(P) : 1].$$

- Hvis f har en pol i P, bruker vi

$$\phi_f = [1 : f^{-1}].$$

Siden $\operatorname{ord}_P(f^{-1}) = -\operatorname{ord}_P(f) > 0$, er $f^{-1}(P) = 0$, så

$$\phi_f(P) = [1 : 0].$$

En morfi $\phi = [f_0 : f_1] \colon C \to \mathbb{P}^1$ kan skrives unikt som $[f_0/f_1 : 1] = \phi_{f_0/f_1}$ hvis $f_1 \neq 0$. Hvis $f_1 = 0$ har vi $\phi = [1 : 0]$, og skriver vi ϕ_∞ for denne morfien vi får vi altså en bijeksjon

$$\begin{aligned} \overline{K}(C) \cup \{\infty\} &\leftrightarrow \{\text{morfier } \phi \colon C \to \mathbb{P}^1\} \\ f &\mapsto \phi_f \end{aligned}$$

PROPOSISJON 3.19. *Hvis $\phi \colon C_1 \to C_2$ er en morfi av kurver, så er ϕ enten surjektiv, eller så er $\phi(C_1) = P$ for en $P \in C_2$.*

Bevis hvis $C_2 = \mathbb{P}^1$: Anta at ϕ ikke er surjektiv, så $\exists Q \in \mathbb{P}^1$ slik at $\phi(P) \neq Q$ for alle $P \in C_1$. Skriv $\phi = \phi_f$ for $f \in \overline{K}(C_1)$.

- Case 1: $Q = [1 : 0] = \infty$. Da er f regulær i alle P, altså konstant.
- Case 2: $Q = [a : 1]$. Da er $f(P) \neq a$ for alle P. Følger at $(f - a)^{-1}$ er regulær i alle P, altså konstant.

3. Korrespondansen mellom kurver og kropper

Gitt en ikkesingulær kurve C, kan vi skrive ned funksjonskroppen dens, $\overline{K}(C)$. Vi begynner med å beskrive en bestemt egenskap til denne kroppen, nemlig dens transcendensgrad over $\overline{K}$.

DEFINISJON 3.20. **Transcendensgraden** $\operatorname{tr.deg.}(L/K)$ til en kroppsutvidelse $K \subset L$ er største n slik at det finnes en kroppinklusjon $K(x_1, \ldots, x_n) \hookrightarrow L$.

Hvis L er en endelig generert kropp over K og $\operatorname{tr.deg.}(L/K) = n$, så er L en endelig utvidelse av $K(x_1, \ldots, x_n)$.

DEFINISJON 3.21. Gitt L/K og L'/K, sier vi at $\iota\colon L \to L'$ er *en homomorfi over* K hvis $\iota(x) = x$ for alle $x \in K$.

PROPOSISJON 3.22 ([**EO**, Thm. 6.24]). *Hvis V er en varietet, så er $\overline{K}(V)$ endelig generert over $\overline{K}$ og* $\operatorname{tr.deg.}(\overline{K}(V)/\overline{K}) = \dim V$.

DEFINISJON 3.23. La $\phi\colon C_1 \to C_2$ være en ikkekonstant morfi av ikkesingulære kurver. **Den assosierte avbildningen av funksjonskropper** er

$$\phi^*\colon \overline{K}(C_2) \to \overline{K}(C_1),$$

definert ved

$$\phi^*(f)(P) = (f \circ \phi)(P) \qquad \forall P \in \overline{K}(C_2).$$

Mer eksplisitt, hvis $C_1 \subset \mathbb{P}^m$ og $C_2 \subset \mathbb{P}^n$, så har vi

$$\phi = [f_0 : \ldots : f_n], \qquad f_i \in \overline{K}(C_1).$$

La nå $f = G/H \in \overline{K}(C_2)$, hvor $G, H \in \overline{K}[C_2]$ er homogene elementer av samme grad. Vi kan representere G og H ved polynomer i $X_0, \ldots, X_n$, og får da

$$\phi^*(f) = \phi^*\left(\frac{G}{H}\right) = \frac{G(f_0, \ldots, f_n)}{H(f_0, \ldots, f_n)} \in \overline{K}(C_1).$$

PROPOSISJON 3.24. *Kroppsutvidelsen $\overline{K}(C_1)/\phi^*(\overline{K}(C_2))$ er endelig.*

BEVIS. Velg et element $x \in \overline{K}(C_2) \setminus \overline{K}$. Da har vi inklusjoner

$$\phi^*(\overline{K}(x)) \subset \phi^*(\overline{K}(C_2)) \subset \overline{K}(C_1).$$

Siden $\operatorname{tr.deg.} \overline{K}(C_1)/K = 1$, er $\overline{K}(C_1)/\phi^*(\overline{K}(x))$ endelig, så $\overline{K}(C_1)/\phi^*(\overline{K}(C_2))$ er endelig. □

EKSEMPEL 3.25. La $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ være gitt ved

$$\phi = [x^n : 1].$$

Da er $\phi^*(x) = x^n$, så $\phi^*\overline{K}(\mathbb{P}^1) = \overline{K}(x^n) \subset \overline{K}(x)$. Dette er en endelig kroppsutvidelse av grad n.

PROPOSISJON 3.26. *La $\iota\colon \overline{K}(C_2) \hookrightarrow \overline{K}(C_1)$ være en homomorfi over $\overline{K}$. Da finnes en unik $\phi\colon C_1 \to C_2$ slik at $\iota = \phi^*$.*

BEVIS. La $C_2 \subset \mathbb{P}^n$, og for $i = 1, \ldots, n$, la $x_i = \frac{X_i}{X_0} \in \overline{K}(C_2)$. Ved Proposisjon 2.18 er kroppen $\overline{K}(C_2)$ generert over $\overline{K}$ av elementene x_i.

Så hvis $\phi\colon C_1 \to C_2$ er en morfi, så er $\phi^* = \iota$ hvis og bare hvis $\phi^*(x_i) = \iota(x_i)$ for $i = 1, \ldots, n$.

La oss si at $\phi = [f_0, \ldots, f_n]$ med $f_i \in \overline{K}(C_1)$. Da er

$$\phi^*(x_i) = x_i \circ \phi = \frac{X_i}{X_0} \circ \phi = \frac{f_i}{f_0},$$

så vi må ha

$$\frac{f_i}{f_0} = \iota(x_i)$$

for $i = 1, \ldots, n$. Men da er

$$\phi = [f_0 : \ldots : f_n] = [1 : f_1 f_0^{-1} : \ldots : f_n f_0^{-1}] = [1\colon \iota(x_1) : \ldots : \iota(x_n)],$$

så ϕ er unikt bestemt av ι.

Man kan sjekke at ϕ definert av ligningen over faktisk gir en morfi fra C_1 til C_2, men det dropper vi å gjøre. □

PROPOSISJON 3.27 ([**EO**, Thm. 9.19]). *Hvis $L/\overline{K}$ er en kroppsutvidelse med*

$$\text{tr. deg.}(L/\overline{K}) = 1,$$

så fins en ikkesingulær kurve C, unik opp til isomorfi, slik at $L \cong \overline{K}(C)$ som kroppsutvidelser av $\overline{K}$.

Ved Proposisjon 3.26 & 3.27 kan spørsmål om ikkesingulære kurver og morfier mellom dem oversettes til spørsmål om kropper av transcendensgrad 1 over $\overline{K}$ og kropphomomorfier mellom dem, og vice versa.

Dette bruker vi i hovedsak på to måter. For det første kan vi nå definere egenskaper av en morfi ϕ ved å se på egenskapene til den assosierte kroppsinklusjonen ϕ^*, hovedeksemplene er **graden** til ϕ og egenskapen at ϕ er **separabel/inseparabel**. For det andre kan vi bruke dette til å konstruere kurver og morfier mellom dem. La oss si at vi har gitt en ikkesingulær kurve C_1 og ønsker å konstruere en morfi $\phi\colon C_1 \to C_2$ med visse egenskaper. Ved proposisjonene over kan vi gjøre dette ved å konstruere en underkropp $L \subset \overline{K}(C_1)$ som har transcendensgrad 1 over $\overline{K}$. Se Avsnitt 5.2 for en illustrasjon av dette.

4. Ramifikasjon og grad til en morfi av kurver

Ønsker vi å forstå en morfi $\phi\colon C_1 \to C_2$ er det naturlig å prøve å forstå, for et gitt punkt $Q \in C_2$, hvordan mengden $\phi^{-1}(Q) \subset C_1$ ser ut. La oss si at $C_2 \subset \mathbb{P}^n$, $\phi = [1 : f_1 : \ldots : f_n]$ med $f_i \in \overline{K}(C_1)$ og for enkelhets skyld at $Q = [1 : 0 : \ldots : 0]$. Da er $P \in \phi^{-1}(Q)$ hvis og bare hvis

$$f_i \text{ regulær i } P \text{ og } f_i(P) = 0 \quad \text{for } i = 1, \ldots, n.$$

Skriver vi ut dette får vi et mengde polynomligninger. Analogt med hvordan røttene i et polynom i én variabel kan opptre med multiplisitet, kan vi tilordne punktene $P \in \phi^{-1}(Q)$ en multiplisitet, som vi kaller **ramifikasjonsindeksen** til ϕ i P. Og på samme måte som antall røtter i et polynom er lik graden når vi tar høyde for at røtter har multiplisitet, vil vi se at antall elementer i $\phi^{-1}(Q)$ talt med multiplisitet er beregnet av **graden** til ϕ.

DEFINISJON 3.28. Hvis $\phi\colon C_1 \to C_2$ er en morfi av kurver, så er **graden** til ϕ definert ved

$$\deg \phi = 0 \text{ hvis } \phi \text{ er konstant.}$$

og

$$\deg \phi = [\overline{K}(C_1) : \phi^* \overline{K}(C_2)]$$

ellers.

EKSEMPEL 3.29. For $\phi = [x^n : 1]\colon \mathbb{P}^1 \to \mathbb{P}^1$, er

$$\deg \phi = [\overline{K}(x)\colon \overline{K}(x^n)] = n.$$

DEFINISJON 3.30. La $\phi\colon C_1 \to C_2$ være ikkekonstant morfi av ikkesingulære kurver, la $P \in C_1$ med $\phi(P) = Q$, og la t_P, t_Q være lokale parametere i P og Q.

Da er **ramifikasjonsindeksen** til ϕ i P gitt ved

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

Siden t_Q er regulær i Q og $t_Q(Q) = 0$, så er $\phi^* t_Q$ regulær i P og $(\phi^* t_Q)(P) = 0$. Dermed er $e_\phi(P) \geq 1$ for alle $P \in C_1$. Vi sier at ϕ er **ramifisert** i P hvis $e_\phi(P) > 1$.

EKSEMPEL 3.31. La C være en ikkesingulær kurve, la $f \in \overline{K}(C) \setminus \overline{K}$, og la

$$\phi = \phi_f = [f : 1]\colon C \to \mathbb{P}^1.$$

La $Q = [\alpha : 1]$. Da er $\phi(P) = Q$ hvis og bare hvis $f(P) = \alpha$. Ved Eksempel 3.4 er $x - \alpha \in \overline{K}(\mathbb{P}^1)$ en lokal parameter i Q, så

$$e_\phi(P) = \operatorname{ord}_P(\phi^*(x - \alpha)) = \operatorname{ord}_P(f - \alpha).$$

Vi har $\phi(P) = \infty = [1 : 0]$ hvis og bare hvis f har en pol i P. Siden x^{-1} er en lokal parameter i ∞, så er da

$$e_\phi(P) = \operatorname{ord}_P(\phi^*(x^{-1})) = \operatorname{ord}_P(f^{-1}) = -\operatorname{ord}_P(f).$$

MERKNAD 3.32. Hvis ϕ er separabel (f.eks. hvis $\operatorname{char} K = 0$), så er $e_\phi(P) = 1$ unntatt i endelig mange P. Se Avsnitt 6.3.

Følgende proposisjon gir en viktig geometrisk tolkning av graden til en morfi.

PROPOSISJON 3.33. *For alle $Q \in C_2$, har vi at*

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

EKSEMPEL 3.34. For $\phi = [X^n : Y^n]\colon \mathbb{P}^1 \to \mathbb{P}^1$, så er

$$e_\phi(P) = 1 \text{ når } P \notin \{[1 : 0], [0 : 1]\},$$

og

$$e_\phi([1 : 0]) = e_\phi([0 : 1]) = n.$$

Beregning i $[0 : 1]$: Her er x lokal parameter, og $\phi^*(x) = x^n$, med $\operatorname{ord}_{[0:1]}(x^n) = n$.

EKSEMPEL 3.35. La $C \subset \mathbb{P}^2$ være en kurve definert av ligningen

$$y^n + y^{n-1} f_{n_1} + \cdots + y f_1 + f_0 = 0 \tag{1}$$

hvor f_i er polynomer i x. La $\phi = \phi_x = [x : 1] \colon C \to \mathbb{P}^1$. Ved Proposisjon 2.18, er $\overline{K}(C)$ generert over $\overline{K}$ av x og y. Kroppinklusjonen $\phi^* \colon \overline{K}(\mathbb{P}^1) \to \overline{K}(C)$ sender x til x, så $\overline{K}(C)$ er generert over $\phi^*(\overline{K}(\mathbb{P}^1))$ av y. Man kan vise at (1) er det irredusible polynomet til y over $\phi^*(\overline{K}(\mathbb{P}^1))$, og dermed er

$$\deg \phi = [\overline{K}(C) : \phi^*(\overline{K}(\mathbb{P}^1))] = \deg_{\overline{K}(\mathbb{P}^1)}(y) = n.$$

La nå $Q = [\alpha : 1] \in \mathbb{P}^1$. Et punkt $P = (\alpha, \beta)$ ligger i $\phi^{-1}(Q)$ hvis og bare hvis β er en rot av polynomet

$$y^n + f_{n-1}(\alpha) y^{n-1} + \cdots + f_0(\alpha),$$

og man kan vise at $e_\phi(P)$ er lik multiplisiteten til β som rot av dette polynomet.

5. Divisorer

La C være en ikkesingulær kurve.

DEFINISJON 3.36. Divisorgruppen $\mathrm{Div}(C)$ er den frie abelske gruppa generert av punktene til C.

Et element $D \in \mathrm{Div}(C)$ kan altså representeres entydig som en sum

$$D = \sum_{i=1}^{r} n_i (P_i)$$

hvor $n_i \in \mathbb{Z}$ og P_i er distinkte punkter i C.

Vi setter

$$\deg D = \sum n_i,$$

og

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) \mid \deg(D) = 0\}.$$

DEFINISJON 3.37. Hvis $f \in \overline{K}(C)^*$, definer divisoren

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

Siden $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$, gir dette en gruppehomomorfi

$$\mathrm{div} \colon \overline{K}(C)^* \to \mathrm{Div}(C).$$

DEFINISJON 3.38. En divisor $D \in \mathrm{Div}(C)$ er **prinsipal** hvis det finnes en $f \in \overline{K}(C)^*$ slik at $D = \mathrm{div}(f)$.

To divisorer D_1, D_2 er **lineært ekvivalente** ($D_1 \sim D_2$), hvis $D_1 - D_2$ er prinsipal.

Picard-gruppa til C, skrives $\mathrm{Pic}(C)$, er definert ved

$$\mathrm{Div}(C)/\mathrm{div}(\overline{K}(C)^*),$$

altså er elementene "divisorer opp til lineær ekvivalens".

PROPOSISJON 3.39. *For alle $f \in \overline{K}(C)^*$, har vi*

$$\deg(\mathrm{div}(f)) = 0,$$

altså har vi $\mathrm{div}(\overline{K}(C)^*) \subset \mathrm{Div}^0(C)$.

BEVIS. Fra definisjonene er

$$\deg(\mathrm{div}(f)) = \deg(\sum_{P\in C} \mathrm{ord}_P(f)(P)) = \sum_{P\in C} \mathrm{ord}_P(f) = 0,$$

ved Proposisjon 3.15. □

DEFINISJON 3.40. Definerer

$$\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{div}(\overline{K}(C)^*).$$

EKSEMPEL 3.41. Alle $D \in \mathrm{Div}^0(\mathbb{P}^1)$ er prinsipale, altså er $\mathrm{Pic}^0(\mathbb{P}^1) = 0$.

Bevis: La $D = \sum n_{P_i} P_i + n_\infty P_\infty$, med $P_i = [a_i : 1]$, $P_\infty = [1 : 0]$, og $\sum n_i + n_\infty = 0$. Bruker $\overline{K}(\mathbb{P}^1) = \overline{K}(x)$, og ser på

$$f = \prod_{i=1}^{r} (x - a_i)^{n_i}.$$

Fra Eksempel 3.13 veit vi at

$$\mathrm{ord}_{P_i}(f) = n_i \quad \forall i, \quad \mathrm{ord}_{P_\infty}(f) = -\sum n_i = n_\infty, \quad \mathrm{ord}_P(f) = 0 \text{ for andre } P.$$

Dette betyr at $\mathrm{div}(f) = D$.

EKSEMPEL 3.42. La $C \subseteq \mathbb{P}^2$ være kurven gitt ved

$$y^2 - (x^3 - x) = 0, \quad \text{dvs. } ZY^2 - (X^3 - Z^2X) = 0.$$

Kurven er ikkesingulær og har ett punkt i uendelig (dvs. med koordinater $[a : b : 0]$), nemlig $O = [0 : 1 : 0]$.

Vi har $y = Y/Z \in \overline{K}(C)$. Da er

$$\mathrm{div}(y) = P_1 + P_2 + P_3 - 3O \tag{2}$$

hvor $P_1 = (0, 0), P_2 = (1, 0), P_3 = (-1, 0)$. Dette fordi y er definert i alle punkter unntatt O, og forsvinner i P_i, med $\mathrm{ord}_{P_i}(y) = 1$ (se Eksempel 3.14 for beregningen i P_1). Siden $\sum_{P\in C} \mathrm{ord}_P(y) = 0$, må da $\mathrm{ord}_O(y) = -3$, som gir (2).

DEFINISJON 3.43. La $\phi\colon C_1 \to C_2$ være en ikkekonstant morfi av kurver. Vi definerer homomorfier

$$\phi_*\colon \mathrm{Div}(C_1) \to \mathrm{Div}(C_2) \qquad \phi^*\colon \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$$

ved å sette

$$\phi_*(P) = \phi(P) \qquad \phi^*(Q) = \sum_{P\in\phi^{-1}(Q)} e_\phi(P)P,$$

og utvider disse til gruppehomomorfier.

EKSEMPEL 3.44. Hvis $\phi\colon C \to \mathbb{P}^1$ er gitt ved $\phi = [f : 1]$, med $f \in \overline{K}(C)$, så er

$$\mathrm{div}(f) = \phi^*((0) - (\infty)).$$

For å se dette bruker vi først at $\mathrm{ord}_P(f) > 0$ hvis og bare hvis $\phi(P) = 0$, at $\mathrm{ord}_P(f) < 0$ hvis og bare hvis $\phi(P) = \infty$. Ved Eksempel 3.31 at

$$e_\phi(P) = \mathrm{ord}_P(f) \text{ hvis } \phi(P) = 0$$
$$e_\phi(P) = -\mathrm{ord}_P(f) \text{ hvis } \phi(P) = \infty.$$

Dermed er

$$\begin{aligned}\operatorname{div}(f) &= \sum_{P\in C} \operatorname{ord}_P(f)(P) = \sum_{P\in\phi^{-1}(0)} \operatorname{ord}_P(f)(P) + \sum_{P\in\phi^{-1}(\infty)} \operatorname{ord}_P(f)(P) \\ &= \sum_{P\in\phi^{-1}(0)} e_\phi(P)(P) - \sum_{P\in\phi^{-1}(\infty)} e_\phi(P)(P) = \phi^*((0)-(\infty)).\end{aligned}$$

PROPOSISJON 3.45. *La $\phi\colon C_1 \to C_2$ være en ikkekonstant morfi av kurver. Da har vi*

(1) $\deg(\phi^* D) = \deg(\phi)\deg(D) \quad \forall D \in \operatorname{Div}(C_2)$.

(2) $\phi^*(\operatorname{div}(f)) = \operatorname{div}(\phi^*(f)) \quad \forall f \in \overline{K}(C_2)^*$.

(3) $\deg(\phi_*(D)) = \deg D \quad \forall D \in \operatorname{Div}(C_1)$.

(4) $\phi_*(\phi^*(D)) = \deg\phi \cdot D \quad \forall D \in \operatorname{Div}(C_2)$.

(5) Hvis $\psi\colon C_2 \to C_3$ er en morfi av ikkesingulære kurver, så er

$$\psi_* \circ \phi_* = (\psi\circ\phi)_* \qquad \phi^* \circ \psi^* = (\psi\circ\phi)^*.$$

(6) Hvis $f \in \overline{K}(C_1)^*$, så finnes det en $g \in \overline{K}(C_2)^*$ slik at

$$\operatorname{div}(g) = \phi_*(\operatorname{div}(f)).$$

BEVIS. (1), (3), (4) er enklest, og overlates til dere (bruk Proposisjon 3.33).

(2) og (5) er vanskeligere, men fortsatt mulige.

(6) er for vanskelig, se [**Sil09**, Prop. II.3.6] for referanser til bevis. Den naive ideen er å definere g via

$$g(Q) = \prod_{P\in\phi^{-1}(Q)} f(P)^{e_\phi(P)},$$

men å vise at dette er en rasjonal funksjon med egenskapene vi trenger er litt jobb. □

KOROLLAR 3.46. *La $\phi\colon C_1 \to C_2$ være en ikkekonstant morfi av ikkesingulære kurver.*

(1) La $D, E \in \operatorname{Div}(C_2)$. Hvis $D \sim E$, så er $\phi^*(D) \sim \phi^*(E)$.

(2) La $D, E \in \operatorname{Div}(C_1)$. Hvis $D \sim E$, så er $\phi_*(D) \sim \phi_*(E)$.

BEVIS. (1): Det finnes en $f \in \overline{K}(C_2)^*$ slik at $\operatorname{div}(f) = D - E$. Ved Proposisjon 3.45, (2), så er

$$\operatorname{div}(\phi^*(f)) = \phi * (\operatorname{div}(f)) = \phi^*(D-E) = \phi^*(D) - \phi^*(E),$$

og dermed er $\phi^*(D) \sim \phi^*(E)$.

(2): Det finnes en $f \in \overline{K}(C_1)^*$ slik at $\operatorname{div}(f) = D - E$. Ved Proposisjon 3.45, (6), så finnes en $g \in \overline{K}(C_2)^*$ slik at

$$\operatorname{div}(g) = \phi_*(\operatorname{div}(f)) = \phi_*(D-E) = \phi_*(D) - \phi_*(E),$$

og dermed er $\phi_*(D) \sim \phi_*(E)$. □

Påstanden over impliserer at homomorfiene $\phi_*\colon \operatorname{Div}(C_1) \to \operatorname{Div}(C_2)$ og $\phi^*\colon \operatorname{Div}(C_2) \to \operatorname{Div}(C_1)$ induserer homomorfier $\phi_*\colon \operatorname{Pic}(C_1) \to \operatorname{Pic}(C_2)$ og $\phi^*\colon \operatorname{Pic}(C_2) \to \operatorname{Pic}(C_1)$.

6. Differensialer

DEFINISJON 3.47. La C være en ikkesingulær kurve. Definer **vektorrommet av differensialer** som $\overline{K}(C)$-vektorrommet utspent av symboler df for alle $f \in \overline{K}(C)$, med relasjoner

- $d(f+g) = df + dg$.
- $d(fg) = fdg + gdf$.
- $da = 0$ for $a \in \overline{K}$.

MERKNAD 3.48. Et differensial $\omega \in \Omega_C$ er ikke en funksjon på C, men vi kan likevel gi en konkret funksjonsaktig beskrivelse av ω. Vi vil seinere definere hva det vil si at ω er regulær i et punkt $P \in C$. Hvis ω er regulært i P, kan vi evaluere ω i P og definere $\omega(P) \in \mathfrak{m}_P/\mathfrak{m}_P^2$. Rommet $\mathfrak{m}_P/\mathfrak{m}_P^2$ er et 1-dimensjonalt $\overline{K}$-vektorrom, så ω kan altså tenkes på som en delvis definert funksjon som tar verdier i ulike 1-dimensjonale $\overline{K}$-vektorrom.

Som et eksempel på en slik evaluering, la $f \in \overline{K}(C)$ og anta at f er regulær i P. Da er $f - f(P) \in \mathfrak{m}_P$, og vi definerer

$$df(P) = f - f(P) \in \mathfrak{m}_P/\mathfrak{m}_P^2$$

PROPOSISJON 3.49 ([**Sil09**, Prop. II.4.2]). *Vektorrommet Ω_C er 1-dimensjonalt som $\overline{K}(C)$-vektorrom.*

Hvis $\operatorname{char} K = 0$*, så er $df \neq 0$ for alle ikkekonstante $f \in \overline{K}(C)$.*

EKSEMPEL 3.50. Hvis $\operatorname{char} K = p$ og $f \in \overline{K}(C)$, så er $d(f^p) = pf^{p-1}df = 0$.

PROPOSISJON 3.51 ([**Sil09**, Prop. II.4.3]). *La C være en ikkesingulær kurve, la $P \in C$, la $t \in \overline{K}(C)$ være en lokal parameter i P.*

(1) Vi har $dt \neq 0$, og for alle $\omega \in \Omega_C$ finnes en unik funksjon $g \in \overline{K}(C)$ slik at

$$\omega = gdt.$$

Vi skriver $g = \omega/dt$.

(2) Hvis $f \in \overline{K}(C)$ er regulær i P, så er df/dt regulær i P.

La nå $\omega \in \Omega_C$, la $P \in C$ og la $t \in \overline{K}(C)$ være en lokal parameter.

DEFINISJON 3.52. **Ordenen til et differensial** ω i punktet P er gitt ved

$$\operatorname{ord}_P(\omega) = \operatorname{ord}_P\left(\frac{\omega}{dt}\right).$$

Vi sier at ω er **regulært i** P hvis $\operatorname{ord}_P(\omega) \geq 0$, og videre at ω er **regulært** hvis det er regulært i alle $P \in C$.

Proposisjon 3.51 impliserer nokså lett at dette er en gyldig definisjon, altså at $\operatorname{ord}_P\left(\frac{\omega}{dt}\right)$ ikke avhenger av hvilken lokal parameter t som velges.

MERKNAD 3.53. Hvis ω er regulært i P, så er

$$\omega(P) = (\omega/dt)(P)dt(P) \in \mathfrak{m}_P/\mathfrak{m}_P^2$$

veldefinert.

PROPOSISJON 3.54. *Med samme antagelser som i Proposisjon 3.51.*

(1) *La* $\omega \in \Omega_C \setminus 0$. *Da er*
$$\operatorname{ord}_P(\omega) := \operatorname{ord}_P(\omega/dt)$$
veldefinert (altså uavhenging av valg av t*).*

(2) *La* $x, f \in \overline{K}(C)$*, og la* $x(P) = 0$. *Hvis* $\operatorname{char} K = 0$*, så er*
$$\operatorname{ord}_P(fdx) = \operatorname{ord}_P(f) + \operatorname{ord}_P(x) - 1.$$

(3) *La* $\omega \in \Omega_C$. *Da er* $\operatorname{ord}_P(\omega) = 0$ *unntatt i endelig mange* P.

DEFINISJON 3.55. **Divisoren assosiert til et differensial** $\omega \in \Omega_C \setminus \{0\}$ er
$$\operatorname{div}(\omega) = \sum_{P \in C} \operatorname{ord}_P(\omega) P \in \operatorname{Div}(C).$$

PROPOSISJON 3.56. *Hvis* $0 \neq \omega_1, \omega_2 \in \Omega_C$*, så er* $\operatorname{div}(\omega_1) \sim \operatorname{div}(\omega_2)$.

BEVIS. Gitt ω_1 og ω_2, har vi en $f \in \overline{K}(C)^*$ slik at $\omega_1 = f\omega_2$. Da er $\frac{\omega_1}{dt} = \frac{f\omega_2}{dt} = f\frac{\omega_2}{dt}$, som betyr at
$$\operatorname{ord}_P(\omega_1) = \operatorname{ord}_P(f) + \operatorname{ord}_P(\omega_2).$$
Dermed er
$$\operatorname{div}(\omega_1) = \operatorname{div}(f) + \operatorname{div}(\omega_2),$$
så $\operatorname{div}(\omega_1) \sim \operatorname{div}(\omega_2)$. □

DEFINISJON 3.57. Den **kanoniske divisorklassen** $K_C \in \operatorname{Pic}(C)$ er klassen til $\operatorname{div}(\omega)$ for et differensial $0 \neq \omega \in \Omega_C$ – ved proposisjonen over er denne klassen uavhengig av valg av ω.

En divisor $D \in \operatorname{Div}(C)$ slik at divisorklassen til D er K_C kalles **kanonisk**.

Dette er kjempebra! Nå har vi, helt uten å gjøre noen valg, fått definert et element i Picard-gruppen, som vi kan bruke til å si ting om kurven.

PROPOSISJON 3.58. *La* $C = \mathbb{P}^1$. *Vi har* $K_{\mathbb{P}^1} = -2(\infty) \in \operatorname{Pic}(\mathbb{P}^1)$.

BEVIS. La $\omega = dx$, og $\alpha \in \overline{K}$. I punktet $[\alpha : 1]$, så er $x - \alpha$ en lokal parameter, og vi har
$$d(x - \alpha) = dx - d\alpha = dx$$
så $\operatorname{ord}_{[\alpha:1]} dx = 0$. I punktet $\infty = [1 : 0]$, så er x^{-1} en lokal parameter. Siden
$$0 = d1 = d(xx^{-1}) = xdx^{-1} + x^{-1}dx$$
så er $dx = -x^2 d(x^{-1})$, og dermed er
$$\operatorname{ord}_\infty(dx) = \operatorname{ord}_\infty\left(\frac{dx}{dx^{-1}}\right) = \operatorname{ord}_\infty(-x^2) = -2.$$
□

MERKNAD 3.59. For alle punkter $P_1, P_2 \in \mathbb{P}^1$, så er $P_1 \sim P_2$ prinsipal, ved Eksempel 3.41. Dermed er $\infty \sim P$ for alle $P \in \mathbb{P}^1$, og vi kan altså også skrive $K_{\mathbb{P}^1} = -P_1 - P_2 \in \operatorname{Pic}(\mathbb{P}^1)$ for vilkårlige $P_1, P_2 \in \mathbb{P}^1$.

KOROLLAR 3.60. *Hvis* $\omega \in \Omega_{\mathbb{P}^1}$ *er regulær i alle* $P \in \mathbb{P}^1$*, så er* $\omega = 0$.

BEVIS. Hvis $\operatorname{ord}_P(\omega) \geq 0$ for alle P, så er $\operatorname{div}(\omega) = \sum n_i P_i$ med $n_i \geq 0$, så $\deg(\operatorname{div}(\omega)) = \sum n_i \geq 0$. Men $\deg(\operatorname{div}(\omega)) = \deg(K_{\mathbb{P}^1}) = -2$. □

EKSEMPEL 3.61. La $C \subset \mathbb{P}^1$ være kurven definert av $y^2 - (x^3 - x) = 0$, og la $P_1 = (-1, 0), P_2 = (0, 0), P_3 = (1, 0), P_\infty = [0 : 1 : 0]$.

For differensialet $dx \in \Omega_C$, har vi

$$\operatorname{ord}_P(dx) = 0, \quad P \in C \setminus P_1, P_2, P_3,$$

siden $\operatorname{ord}_P(x - x(P)) = 1$ for slike P.

Har

$$\operatorname{ord}_{P_1}(dx) = \operatorname{ord}_{P_2}(dx) = \operatorname{ord}_{P_3}(dx) = 1,$$

siden $\operatorname{ord}_{P_i}(x - x(P_i)) = 2$.

Har

$$\operatorname{ord}_{P_\infty}(x) = -2 \Rightarrow {}^1 \operatorname{ord}_{P_\infty}(dx) = -3$$

Har også $\operatorname{ord}_{P_1}(y) = \operatorname{ord}_{P_2}(y) = \operatorname{ord}_{P_3}(y) = 1$, $\operatorname{ord}_{P_\infty}(y) = -3$, $\operatorname{ord}_P(y) = 0$ ellers.

La $\omega = dx/y$. Da er $\operatorname{ord}_P(\omega) = \operatorname{ord}_P(dx) - \operatorname{ord}_P(y) = 0$ for alle P, så $K_C = \operatorname{div}(\omega) = 0$.

KOROLLAR 3.62. *Kurven C er ikke isomorf til $\mathbb{P}^1$.*

7. Riemann–Roch

La C være en ikkesingulær kurve. Vi veit fra 3.15 at en rasjonal funksjon $f \in \overline{K}(C)$ som er regulær i alle punkter må være konstant.

Hva med "litt" ikke-regulære funksjoner? Gitt en kurve C, noen punkter $P_1, \ldots, P_i$, og noen tall $m_1, \ldots, n_i \geq 0$, kan vi beskrive mengden av rasjonale funksjon som bare har poler i P_i, med pol-orden $\leq n_i$?

Riemann–Roch-teoremet gir veldig presis informasjon om dimensjonen på dette rommet av funksjoner. Vi introduserer først litt notasjon.

DEFINISJON 3.63. En divisor D er *effektiv*, vi skriver $D \geq 0$, hvis $D = \sum n_i P_i$ med $n_i \geq 0$. Mer generelt, skriver vi $D_1 \geq D_2$ hvis $D_1 - D_2 \geq 0$.

EKSEMPEL 3.64. La $P \in C$, $n \geq 0$, og $f \in \overline{K}(C)$.

$\operatorname{div}(f) \geq -n(P) \Leftrightarrow f$ er regulær på $C \setminus P$, og har (i verste fall) en pol av orden $\leq n$ i P.

Mer generelt, gitt $Q \in C$, $m \geq 0$, så er $\operatorname{div}(f) \geq m(Q) - n(P) \Leftrightarrow f$ er regulær på $C \setminus P$, har en pol av orden $\leq n$ i P, og et nullpunkt av orden $\geq m$ i Q.

DEFINISJON 3.65. La $D \in \operatorname{Div}(C)$. Vi definerer $\overline{K}$-vektorrommet

$$\mathcal{L}(D) = \{f \in \overline{K}(C) \mid \operatorname{div}(f) \geq -D\} \cup \{0\}$$

Dette er endeligdimensjonalt, og vi lar $l(D) = \dim_{\overline{K}} \mathcal{L}(D)$.

[1]Her jukser vi litt og antar $\operatorname{char}(K) \neq 2$. Hvis t er lokal parameter i P_∞, så er $x = ft^{-2}$ med f regulær og ikke null i P_∞. Har da $dx = dft^{-2} - 2t^{-3}fdt$, som hvis $2 \neq 0$ impliserer at $\operatorname{ord}_{P_\infty}(x) = \operatorname{ord}_{P_\infty}(2t^{-3}fdt) = -3$.

EKSEMPEL 3.66. $f \in \mathcal{L}(0)$ hvis og bare hvis f er regulær overalt, som skjer hvis og bare hvis f er konstant.

Altså er $\mathcal{L}(0) = \overline{K} \subset \overline{K}(C)$, $l(0) = 1$.

TEOREM 3.67. *(1) Hvis* $\deg D < 0$*, så er* $\mathcal{L}(D) = \{0\}$.

(2) Hvis $D' \sim D$*, så er* $\mathcal{L}(D) \cong \mathcal{L}(D')$*, og altså* $l(D) = l(D')$.

BEVIS. (1): Hvis $f \in \mathcal{L}(D)$, så er $\operatorname{div}(f) \geq -D$, og dermed er

$$0 = \deg(\operatorname{div}(f)) \geq \deg(-D) = -\deg(D) > 0.$$

(2): Hvis $D = D' + \operatorname{div}(g)$, og $f \in \mathcal{L}(D)$, så er $gf \in \mathcal{L}(D')$, siden

$$\operatorname{div}(gf) = \operatorname{div}(g) + \operatorname{div}(f) \geq \operatorname{div}(g) - D = -(D - \operatorname{div}(g)) = -D'.$$

Motsatt, hvis $f \in \mathcal{L}(D')$, så er $g^{-1}f \in \mathcal{L}(D)$, og vi har $\mathcal{L}(D) \cong \mathcal{L}(D')$. □

EKSEMPEL 3.68. La $\omega \in \Omega_C$, og la $K_C = \operatorname{div}(\omega) \in \operatorname{Div}(C)$. Da er $f \in \mathcal{L}(K_C)$ hvis og bare hvis

$$\operatorname{div}(f) + \operatorname{div}(\omega) \geq 0 \Leftrightarrow \operatorname{div}(f\omega) \geq 0 \Leftrightarrow f\omega \in \Omega_C \text{ er regulær overalt.}$$

Altså er $\mathcal{L}(K_C)$ identifisert med rommet av regulære differensialer.

DEFINISJON 3.69. Tallet $g(C) = l(K_C)$ kalles *genus* til C.

EKSEMPEL 3.70. Vi har vist at $\mathcal{L}(K_{\mathbb{P}^1}) = \{0\}$, så $g(\mathbb{P}^1) = l(K_C) = 0$.

For kurven C gitt ved $y^2 - (x^3 - x)$, har vi vist at $K_C = 0$, så $g(C) = l(K_C) = l(0) = 1$.

TEOREM 3.71 (Riemann–Roch). *La C være en ikkesingulær kurve og la K_C være en kanonisk divisor. For en divisor D, har vi*

$$l(D) - l(K_C - D) = \deg(D) - g(C) + 1$$

KOROLLAR 3.72. *(1)* $\deg K_C = 2g(C) - 2$.

(2) Hvis $\deg D > \deg K_C$*, så er*

$$l(D) = \deg D - g(C) + 1.$$

BEVIS. (1) Sett $D = K_C$. Da er

$$l(K_C) - l(0) = \deg(K_C) - g(C) + 1.$$

Vi har $l(0) = 1$, og $l(K_C) = g(C)$, som gir resultatet. (2) Hvis $\deg D > \deg K_C$, så er $\deg(K_C - D) < 0 \Rightarrow l(K_C - D) = 0$. □

KAPITTEL 4

Elliptiske kurver, én og én

DEFINISJON 4.1. En **elliptisk kurve** er et par (E, O), hvor E er en ikkesingulær kurve med $g(E) = 1$, og $O \in E$ er et valgt punkt.

Vi sier at (E, O) er **definert over** K hvis E er definert over K (Def. 2.19) og $O \in E(K)$.

1. Weierstrass-ligninger

Vi skal se at alle elliptiske kurver kan beskrives som kurver i $E \subset \mathbb{P}^2$ definert av en bestemt type ligning, som kalles Weierstrass-ligningen. Den generelle formen ser slik ut:

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3}$$

Homogeniserer vi denne ligningen, får vi

$$E\colon ZY^2 + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Hvis et punkt på formen $[\alpha : \beta : 0] \in \mathbb{P}^2$ skal ligge i E må vi ha

$$0 = \alpha^3,$$

så $\alpha = 0$, og punktet er $[0 : 1 : 0]$. For en kurve på Weierstrass-form vil dette punktet spille en spesiell rolle, og vi kaller det O.

Alle andre punkter i E kan skrives som $(\alpha, \beta) = [\alpha : \beta : 1] \in \mathbb{P}^2$, og er løsniger av ligning (3).

Anta nå at $\operatorname{char} K \neq 2, 3$: Kan da gjøre variabelskifte $y \mapsto y - \frac{a_1x + a_3}{2}$, og får

$$y^2 = x^3 + a_2'x^2 + a_4'x + a_6'.$$

Vi kan videre gjøre variabelskiftet $x \mapsto x - \frac{a_2'}{3}$, og får da

$$y^2 = x^3 + a_4''x + a_6'',$$

som vi skriver om til

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

MERKNAD 4.2. Vi kommer heretter alltid til å anta $\operatorname{char} K \notin \{2, 3\}$. Det meste av teorien kan utvikles uten denne antakelsen, men utregningene blir en god del mer kompliserte.

MERKNAD 4.3. Vi kan også faktorisere høyre side i Weierstrass-ligningen og få

$$y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3), \qquad \lambda_i \in \overline{K},$$

hvor $\lambda_1 + \lambda_2 + \lambda_3 = 0$.

DEFINISJON 4.4. Vi kaller et polynom f på formen $f = y^2 - (x^3 + Ax + B)$ et **Weierstrass-polynom**.

DEFINISJON 4.5. Gitt et Weierstrass-polynom f, er **diskriminanten** til f gitt ved

$$\Delta(f) = -16(4A^3 + 27B^2)$$

LEMMA 4.6. *Vi har $\Delta(f) = 0$ hvis og bare hvis $x^3 + Ax + B$ har en dobbel rot (altså hvis det finnes $i \neq j$ slik at $\lambda_i = \lambda_j$).*

BEVIS. Polynomet $f = x^3 + Ax + B$ har en dobbel rot i $\overline{K}$ hvis og bare hvis det finnes en x som er rot av både f og $f' = 3x^2 + A$, og det er lett å sjekke dette er hvis og bare hvis $\Delta(f) = 0$:

Anta først at $A = 0$. Da er $f'(x) = 0$ hvis og bare hvis $x = 0$, og $f(0) = 0$ hvis og bare hvis $B = 0$, så vi har en dobbel rot hvis og bare hvis $B = 0$, som er hvis og bare hvis $\Delta(f) = 0$.

Hvis $A \neq 0$, har vi

$$\begin{aligned}
x^3 + Ax + B = 0 \wedge 3x^2 + A = 0 \\
\Updownarrow \\
x^3 + Ax + B - \frac{x}{3}(3x^2 + A) = 0 \wedge 3x^2 + A = 0 \\
\Updownarrow \\
\frac{2A}{3}x + B = 0 \wedge 3x^2 + A = 0 \\
\Updownarrow \\
x = -\frac{3B}{2A} \wedge 3x^2 + A = 0,
\end{aligned}$$

som er hvis og bare hvis $27B^2 + 4A^3 = 0$. □

PROPOSISJON 4.7. *Kurven $E \in \mathbb{P}^2$ gitt ved et Weierstrass-polynom f er singulær hvis og bare hvis $\Delta(f) = 0$.*

I så fall har E nøyaktig ett singulært punkt, $(\alpha, 0)$, hvor α er en dobbel rot av $x^3 + Ax + B$.

BEVIS. Kurven E er singulær i $(\alpha, \beta) \in E$ hvis og bare hvis $\frac{\partial}{\partial x}(f)(\alpha, \beta) = \frac{\partial}{\partial y}(f(\alpha, \beta)) = 0$.

Må da ha $\beta = 0$ og $3\alpha^2 + A\alpha = 0$, som sammen med $\alpha^3 + A\alpha + B = 0$ er ekvivalent med at $x^3 + Ax + B$ har en dobbel rot i $(\alpha, 0)$. Dette betyr at $\Delta = 0$.

I punktet $O = [0 : 1 : 0]$ kan vi bruke koordinater $[x' : 1 : z']$, altså $z' = Z/Y$, $x' = X/Y$. Den homogene formen til f, nemlig

$$ZY^2 - (X^3 + AXZ^2 + BZ^3)$$

gir da den inhomogene ligningen

$$g = z - (x^3 + Axz^2 + Bz^3).$$

Her er $\frac{\partial}{\partial z}g(0, 0) = 1$, så kurven er ikkesingulær i $[0 : 1 : 0]$. □

MERKNAD 4.8. Hvis $A, B \in \mathbb{R}$, så er E definert over $\mathbb{R}$. Mengden $E(\mathbb{R}) \setminus O$ er en delmengde av $\mathbb{A}^2(\mathbb{R}) = \mathbb{R}^2$, og vi kan gi $E(\mathbb{R}) \setminus O$ den induserte topologien fra $\mathbb{R}^2$. Det viser seg at med denne topologien har $E(\mathbb{R}) \setminus O$ to sammenhengskomponenter hvis $\Delta(f) > 0$ og én sammenhengskomponent hvis $\Delta(f) < 0$.

1.1. Tilfellet $\Delta(f) = 0$ – singulære Weierstrass-kurver. Hvis $\Delta = 0$, hvordan ser singularitetene til C ut?

Vi har to tilfeller:

- $A, B \neq 0$, som er hvis og bare hvis $\lambda_1 = \lambda_2 \neq \lambda_3$.
- $A, B = 0$, som er hvis og bare hvis $\lambda_1 = \lambda_2 = \lambda_3 = 0$.

I det første tilfellet kan gjøre variabelskiftet $x \mapsto x + \lambda_1$, og får

$$y^2 - x^2(x + 3\lambda_1),$$

som er lik

$$(y - (3\lambda_1)^{1/2}x)(y + (3\lambda_1)^{1/2}x) + x^3,$$

som betyr at C har en *node* i $(0, 0)$.

Hvis alle $\lambda_i = 0$, er ligningen $y^2 - x^3$, dette kalles en *cusp*.

EN FLOTT TEGNING.

MERKNAD 4.9. Hvis E er singulær (hvis $\Delta = 0$), så finnes det rasjonale avbildninger $\mathbb{P}^1 \to E$ og $E \to \mathbb{P}^1$ som er inverse til hverandre. Det vil si at slike E er birasjonale til $\mathbb{P}^1$.

DEFINISJON 4.10. Gitt en Weierstrass-ligning $y^2 = x^3 + Ax + B$, så er *j-invarianten* lik

$$j = -1728\frac{(4A)^3}{\Delta}.$$

EKSEMPEL 4.11. To eksempler skiller seg ut med spesielle koeffisienter:

- $A = 0 \rightsquigarrow j = 0$
- $B = 0 \rightsquigarrow j = 1728$ (kurven jeg alltid tegner)

Se Avsnitt 5.8 for mer om automorfier av disse speiselle kurvene.

PROPOSISJON 4.12. *La (E_1, O_1) og (E_2, O_2) være elliptiske kurver gitt av Weierstrass-ligninger*

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

og

$$y^2 = x^3 + A'x + B.$$

Da er $E_1 \cong E_2$ over K hvis og bare hvis vi kan transformere ligning 1 til ligning to ved variabelskiftet $x \mapsto u^2x$, $y \mapsto u^3y$ for en $u \in K$.

Vi utsetter beviset for dette litt, se Teorem 4.18.

Med andre ord er $E_1 \cong E_2$ (over K) hvis og bare hvis det finnes en $u \in K$ slik at

$$A = u^4A', B = u^6B'.$$

PROPOSISJON 4.13. *Hvis E_1, E_2 er kurver gitt av Weierstrass-ligninger f_1, f_2, så er $E_1 \cong E_2$ hvis og bare hvis $j(f_1) = j(f_2)$.*

BEVIS. Hvis E_1 er isomorf med E_2, så sendes f_1 til f_2 under en bestemt transformasjon. Men

$$j = 2^8 3^3 \frac{A^3}{4A^3 + 27B^2}$$

er invariant under $A \mapsto u^4 A$, $B \mapsto u^6 B$, så $j(f_1) = j(f_2)$.

Anta nå at $j(f_1) = j(f_2)$. Det betyr enten at $A_1 = A_2 = 0$, eller at

$$\frac{B_1^2}{A_1^3} = \frac{B_2^2}{A_2^3}.$$

Vi må vise at $E_1 \cong E_2$, som skjer hvis det finnes en $u \in \overline{K}$ slik at $A_1 = u^4 A_2$ og $B_1 = u^6 B_2$.

Tilfelle 1: $A_1 = A_2 = 0$: Ta $u = (B_1/B_2)^{1/6}$.

Tilfelle 2: $B_1 = B_2 = 0$: Ta $u = (A_1/A_2)^{1/4}$.

Tilfelle 3: Ingen A_i, $B_i = 0$: Ta $u = (\frac{B_1 A_2}{A_1 B_2})^{1/2}$, og får

$$u^4 A_2 = \frac{B_1^2 A_2^3}{B_2^2 A_1^2} = \frac{B_1^2 A_1^3}{B_1^2 A_1^2} = A_1,$$

tilsvarende får vi $u^6 B_2 = B_1$. □

PROPOSISJON 4.14. *(1) Hvis E er en Weierstrass-kurve definert over K, så er $j(E) = j(f) \in K$.*

(2) For ethvert element $j \in K$, så finnes det en elliptisk kurve E definert over K med $j(E) = j$.

BEVIS. (1) er opplagt fra definisjonen av j.

For (2), må vi finne $A, B \in K$ slik at

$$2^6 3^3 \frac{A^3}{4A^3 - 27B^2} = j.$$

Hvis $j = 0$, sett $A = 0$, $B = 1$. Hvis $j = 1728$, sett $B = 0$, $A = 1$. Ellers reduserer ligningen til

$$\frac{B^2}{A^3} = \alpha,$$

med $0 \neq \alpha \in K$, og vi kan sette $B = A = \alpha^{-1}$. □

DEFINISJON 4.15. Hvis E er en elliptisk kurve, så er

$$j(E) = j(f)$$

hvor f er et Weierstrass-polynom for E.

1.2. Legendre-formen. Det finnes en alternativ normalisering av Weierstrass-ligningen til en elliptisk kurve, som kalles **Legendre-formen**. For å beskrive denne, faktoriserer vi først høyre side av Weierstrass-ligningen $y^2 = x^3 + Ax + B$ over $\overline{K}$ og får

$$y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$$

PROPOSISJON 4.16. *(1) For en elliptisk kurve E, finnes en $\lambda \in \overline{K}$ slik at $E = E_\lambda$, hvor E_λ er kurven definert ved Weierstrass-ligningen i Legendre-form*

$$E_\lambda : y^2 = x(x - 1)(x - \lambda).$$

(2) Vi har

$$j(E_\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

BEVIS. (1): La E være gitt av Weierstrass-ligningen

$$y^2 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3).$$

Variabelskiftet $x \mapsto x + \lambda_1$ gir ligningen formen

$$y^2 = x(x - \lambda_2')(x - \lambda_3').$$

Variabelskiftet $x \mapsto u^2 x$, $y \mapsto u^3 y$, med $u = (\lambda_2')^{1/2}$, gir ligningen formen

$$u^6 y^2 = u^2 x(u^2 x - \lambda_2')(u^2 x - \lambda_3'),$$

som ved å dele på u^6 gir

$$y^2 = x(x - 1)(x - \lambda_3'').$$

(2): Ligningen

$$y^2 = x(x-1)(x-\lambda) = x^3 - (1+\lambda)x^2 - \lambda x$$

blir etter variabelskiftet $x \mapsto x + \frac{1+\lambda}{3}$ til $y^2 = x^3 + Ax + B$, med A og B eksplisitte funksjoner av λ. Sett inn i $j(E) = -1728\frac{(4A^3)}{\Delta}$ og regn ut. □

2. Fra en elliptisk kurve til en Weierstrass-ligning

Vi skal nå vise at abstrakte elliptiske kurver svarer til kurver definert av Weierstrass-ligninger.

Husk fra tidligere: For $D \in \mathrm{Div}(C)$, så er

$$\mathcal{L}(D) = \{f \in \overline{K}(C) \mid \mathrm{div} f + D \geq 0\}, \quad l(D) = \dim_{\overline{K}} \mathcal{L}(D).$$

Spesielt, hvis $P \in C$ og $n \geq 0$, er

$$\mathcal{L}(nP) = \{f \in \overline{K}(C) \mid f \text{ har pol av orden } \leq n \text{ i } P, \text{ regulær ellers}\}.$$

THEOREM 4.17 (Riemann–Roch for en genus 1 kurve). *Hvis C er en ikkesingulær kurve av genus 1 og $D \in \mathrm{Div}(C)$ er en divisor med $\deg D > 0$, så er*

$$l(D) = \deg D$$

THEOREM 4.18. *La (E, O) være en elliptisk kurve.*

(a) Det finnes $x, y \in \overline{K}(E)$, slik at

$$\phi \colon E \to \mathbb{P}^2, \quad \phi = [x : y : 1]$$

gir en isomorfi fra E til en Weierstrass-kurve

$$C \subset \mathbb{P}^2 \colon y^2 = x^3 + Ax + B,$$

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

Vi kaller x, y for Weierstrass-koordinater for E.

(b) To ulike Weierstrass-koordinater x, y og x', y' for E er relatert ved $x = u^2 x', y = u^3 y'$ for en $u \in \overline{K}$.

(c) Hvis en Weierstrass-kurve C som over er ikkesingulær, så er den en elliptisk kurve.

MERKNAD 4.19. Hvis (E, O) er definert over K, så kan x, y velges slik at $A, B \in K$, og i punkt 2 er da $u \in K$.

LEMMA 4.20. *Hvis C er en ikkesingulær kurve, $D_1, D_2 \in \mathrm{Div}(C)$, $f_1 \in \mathcal{L}(D_1)$ og $f_2 \in \mathcal{L}(D_2)$, så er $f_1 f_2 \in \mathcal{L}(D_1 + D_2)$.*

BEVIS.

$$\begin{aligned}\mathrm{div}(f_1 f_2) + D_1 + D_2 &= \mathrm{div}(f_1) + \mathrm{div}(f_2) + D_1 + D_2 \geq 0 \\ &(\mathrm{div}(f_1) + D_1) + (\mathrm{div}(f_2) + D_2) \geq 0.\end{aligned}$$

□

BEVIS FOR TEOREM 4.18. Vi studerer vektorrommene $\mathcal{L}(nO)$ for $n \geq 0$, disse danner en kjede

$$\overline{K} = \mathcal{L}(0O) \subseteq \mathcal{L}(O) \subseteq \mathcal{L}(2O) \subseteq \cdots$$

For $n \geq 1$, har vi $\dim \mathcal{L}(nO) = \deg(nO) = n$. Vi beskriver basiser for de første rommene

$$\begin{aligned}\mathcal{L}(0) &= \langle 1 \rangle, \text{ siden } l(0) = 1 \\ \mathcal{L}(O) &= \langle 1 \rangle, \text{ siden } l(O) = 1 \\ \mathcal{L}(2O) &= \langle 1, x \rangle, \text{ siden } l(2O) = 2, \text{ velger en vilkårlig } x\end{aligned}$$

Siden $x \in \mathcal{L}(2O) \setminus \mathcal{L}(O)$, er $\mathrm{ord}_O(x) = -2$. Videre

$$\mathcal{L}(3O) = \langle 1, x, y \rangle, \text{ siden } l(3O) = 3, \text{ velger vilkårlig } y.$$

Siden $y \in \mathcal{L}(3O) \setminus \mathcal{L}(2O)$, er $\mathrm{ord}_O(y) = -3$.

Vi har $\mathrm{ord}_O(x^a y^b) = 2a + 3b$, så $x^a y^b \in \mathcal{L}((2a+3b)O) \setminus \mathcal{L}((2a+3b-1)O)$. Følger at

$$\begin{aligned}\mathcal{L}(4O) &= \langle 1, x, y, x^2 \rangle \\ \mathcal{L}(5O) &= \langle 1, x, y, x^2, xy \rangle\end{aligned}$$

I $\mathcal{L}(6O)$ har vi de 7 elementene $1, x, y, x^2, xy, y^2, x^3$, så vi får en lineær relasjon mellom disse. Mer presist har vi $y^2, x^3 \in \mathcal{L}(6O) \setminus \mathcal{L}(5O)$, så vi kan finne $a, b \neq 0$, slik at $ay^2 + bx^3 \in \mathcal{L}(5O)$.

La oss omdefinere $x \mapsto -\frac{a}{b}x$, $y \mapsto \frac{a}{b}y$, får da $y^2 - x^3 \in \mathcal{L}(5O)$. Dette betyr at

$$y^2 - x^3 = cxy + dx^2 + ey + fx + g,$$

som vi sist gang viste at vi kan transformere til

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

ved å gjøre noen variabelskifter.

Da har vi vist at $\phi\colon E \to \mathbb{P}^2$ har bilde i kurven

$$C : y^2 = x^3 + Ax + B,$$

Vi må nå vise (1) at $\phi\colon E \to C$ har grad 1, og (2) at C er ikkesingulær.

For (1): ϕ er opplagt ikke konstant, så den er surjektiv. La $Q_1 = (x_0, y_0) \in C$, med $y_0 \neq 0$. Da er $Q_2 = (x_0, -y_0) \in C$, og $(x_0, \alpha) \in C$ hvis og bare hvis $\alpha = \pm y_0$. Et punkt $P \in E$ er slik at $\phi(P) \in \{Q_1, Q_2\}$, hvis og bare hvis $(x - x_0)(P) = 0$.

Men $x - x_0 \in \overline{K}(E)$ har en dobbel pol i O, og er ellers regulær, så den har maks to nullpunkter. Dermed er $|\phi^{-1}(\{Q_1, Q_2\})| \leq 2 \Rightarrow |\phi^{-1}(Q_1)| = |\phi^{-1}(Q_2)| = 1$.

For (2), hvis C er singulær, så finnes en rasjonal avbildning $\psi\colon C \to \mathbb{P}^1$ av grad 1. Dermed er $\psi \circ \phi\colon E \to \mathbb{P}^1$ en rasjonal avbildning av grad 1. Men da er E isomorf med $\mathbb{P}^1$, som motsier at E har genus 1.

(b): Variabelskiftet: Vi har at $\{1, x\}$ og $\{1, x'\}$ er to basiser for $\mathcal{L}(2O)$, altså er $x = u_1 x' + r$. Videre har vi at $\{1, x, y\}$ og $\{1, x', y'\}$ er to basiser for $\mathcal{L}(3O)$, altså er $y = u_2 y' + s_2 x' + t$.

Siden vi har $y^2 = x^3 + Ax + B$ skal transformeres til $(y')^2 = (x')^3 + A'x' + B'$, så må relasjonene over forenkles til $x = u^2 x'$ og $y = u^3 y'$.

(c): Hvis C er Weierstrass-kurve. La $\omega = \frac{dx}{y} \in \Omega_C$, da er $\operatorname{div}(\omega) = 0$, så $\mathcal{L}(\omega) = \mathcal{L}(0) = \overline{K}$. □

3. Gruppestrukturen til en elliptisk kurve

La (E, O) være en elliptisk kurve.

Spørsmål: Kan vi beregne (grad 0) Picard-gruppa $\operatorname{Pic}^0(E) = \operatorname{Div}^0(E)/\operatorname{div}(\overline{K}(E)^*)$?

LEMMA 4.21. *La $P \in E$. Hvis $f \in \mathcal{L}(P)$, så er f konstant.*

BEVIS. Ved Riemann–Roch er $\dim \mathcal{L}(P) = \deg(P) = 1$, og vi har $1, f \in \mathcal{L}(P)$. Dermed er $f = a \cdot 1$ for en $a \in \overline{K}$. □

LEMMA 4.22. *La $P, Q \in E$ med $P \neq Q$. Da er $P - Q \not\sim 0$.*

BEVIS. Hvis $P - Q \sim 0$, så finnes en $f \in \overline{K}(E)^*$ slik at $\operatorname{div}(f) = P - Q$. Da er $f \in \mathcal{L}(P - Q) \subseteq \mathcal{L}(P)$, så f er konstant. Altså er $\operatorname{div}(f) = 0$, så $P = Q$. □

PROPOSISJON 4.23. *La $D \in \operatorname{Div}^0(E)$. Da finnes et unikt punkt $P \in E$ slik at $D \sim P - O$.*

BEVIS. *Det finnes et punkt P:* Ved Riemann–Roch er

$$\dim \mathcal{L}(D + O) = \deg(D + O) = 1$$

og dermed finnes $f \in \mathcal{L}(D + O)$. Har

$$\operatorname{div}(f) + D + O \geq 0,$$

altså $\operatorname{div}(f) + D + O = \sum n_i P_i$ med $n_i \geq 0$. Har også

$$\deg(\operatorname{div}(f)) + \deg(D + O) = 0 + 1 = 1,$$

dermed er $\sum n_i = 1$, så $\operatorname{div}(f) + D + O = P$ for et $P \in E$. Dermed er $D \sim P - O$.

Punktet er unikt: Hvis $Q - O \sim D$, så er $Q - O \sim P - O$, dermed er $Q \sim P$, dermed er $Q = P$. □

La $\sigma\colon \operatorname{Div}^0(E) \to E$ være avbildingen $\sigma(D) = P$.

LEMMA 4.24. *Avbildningen σ er surjektiv.*

BEVIS. $\sigma(P - O) = P$. □

LEMMA 4.25. *For $D_1, D_2 \in \operatorname{Div}^0(E)$, så er $\sigma(D_1) = \sigma(D_2)$ hvis og bare hvis $D_1 \sim D_2$.*

BEVIS. *Hvis:* Opplagt fra definisjonen.

Bare hvis: $D_1 - D_2 \sim (\sigma(D_1) - O) - (\sigma(D_2) - O) = 0$. □

PROPOSISJON 4.26. *Avbildningen* $\sigma\colon \mathrm{Pic}^0(E) \to E$ *er en bijeksjon. Inversavbildningen* $\sigma^{-1} = \kappa\colon E \to \mathrm{Pic}^0(E)$ *er gitt ved*

$$\kappa(P) = P - O.$$

Siden $\mathrm{Pic}^0(E)$ er en abelsk gruppe, blir nå E også en abelsk gruppe:

DEFINISJON 4.27. *Gruppestrukteren på en elliptisk kurve* er gitt ved

$$P + Q = \sigma(\kappa(P) + \kappa(Q)).$$

MERKNAD 4.28. Hvis (E, O) er definert over K, så vil $E(K) \subset E$ danne en undergruppe.

3.1. Geometrisk definisjon av gruppestrukturen. La nå (E, O) være Weierstrass-kurven gitt ved

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

Gitt en linje $l \subset \mathbb{P}^2$, så vil $l \cap E$ bestå av 3 punkter (telt med multiplisitet), skriver

$$l \cap E = P_1 + P_2 + P_3$$

DEFINISJON 4.29. Gitt to punkter $P, Q \in E$, skriver vi $l(P, Q) \in \mathbb{P}^2$ for linja utspent av P, Q hvis $P \neq Q$, eller for tangentlinja i P hvis $P = Q$. Vi har $l(P, Q) \cap E = P + Q + R$, og skriver $T(P, Q) = R$.[1]

EKSEMPEL 4.30. $T(O, O) = O$, siden tangentlinja til O er linja i uendelig $l_\infty = \{[\alpha : \beta : 0]\}$, og $l_\infty \cap E = O$.

DEFINISJON 4.31. *Komposisjonsloven av punkter på* E er operasjonen $\oplus\colon E \times E \to E$ gitt som følger.

Gitt $(P, Q) \in E$, la $R = T(P, Q)$. La $R' = T(O, R)$. Vi setter $P \oplus Q = R'$.

PROPOSISJON 4.32. *For komposisjonsloven gjelder*

a) Hvis $T(P, Q) = R$*, så er* $(P \oplus Q) \oplus R = O$.

b) For alle $P \in E$*, så er* $O \oplus P = P$.

c) For alle $P = (x, y) \in E$*, så* $P' = (x, -y) \in E$ *slik at* $P \oplus P' = O$.

BEVIS. TEGN OG FORKLAR □

Hvis vi visste at $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$, så ville $\oplus$ definert en gruppestruktur på E. Vi kan gjøre mer enn det:

PROPOSISJON 4.33. *Den geometriske addisjonen* $\oplus$ *stemmer overens med Picard-gruppe-addisjonen definert tidligere.*

Først et lemma.

[1] Forelesers notasjon.

LEMMA 4.34. *Hvis l er en linje i $\mathbb{P}^2$, slik at*

$$l \cap E = P_1 + P_2 + P_3,$$

så er $P_1 + P_2 + P_3 \sim 3O \in \mathrm{Div}^0(E)$.

BEVIS. La $F = aX + bY + cZ$ være ligningen til l, og la $f = F/Z$. Da er $f \in \overline{K}(E)$, og $\mathrm{div}(f) = P_1 + P_2 + P_3 - 3O$. Dermed er

$$P_1 + P_2 + P_3 \sim 3O.$$

□

BEVIS FOR PROPOSISJON. La $P, Q \in E$, la $R = T(P, Q)$, og $R' = T(O, R) = P \oplus Q$. Har (1) $P + Q + R \sim 3O$ og (2) $R + R' + O \sim 3O$. Lignin (1) gir

$$(P - O) + (Q - O) \sim O - R,$$

og (2) gir $O - R \sim R' - O$, altså

$$(P - O) + (Q - O) \sim R' - O = P \oplus Q - O.$$

□

3.2. Formler for gruppeoperasjonen. Skriver heretter $P + Q$ i stedet for $P \oplus Q$.

La E være gitt ved Weierstrass-polynom $f = y^2 - (x^3 + Ax + B)$.

Spørsmål: Gitt $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$, kan vi beregne $P_1 + P_2 = (x_3, y_3)$?

EKSEMPEL 4.35. Hvis $x_1 = x_2$, og $y_1 = -y_2$, så er $T(P_1, P_2) = O$, og vi har $P_1 + P_2 = O$.

Anta $x_1 \neq x_2$. Sett $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, og $\nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$, da er

$$y = \lambda x + \nu$$

ligningen til linja $l(P_1, P_2)$ gjennom P_1, P_2.

TEOREM 4.36. *Hvis $x_1 \neq x_2$, så er*

$$x_3 = \lambda^2 - x_1 - x_2$$

og

$$y_3 = -\lambda x_3 - \nu.$$

BEVIS. Finner først $T(P_1, P_2) = (x_3', y_3')$, siden $(x_3, y_3) = (x_3', -y_3')$. Beregner snittpunktene $l(P_1, P_2) \cap E$. Setter inn

$$y = \lambda x + \nu.$$

i $(x^3 + Ax + B) - y^2$, og får

$$x^3 - \lambda^2 x^2 + (A - 2\lambda)x + B - \nu^2 = (x - x_1)(x - x_2)(x - x_3').$$

Dette gir

$$x_3' = \lambda^2 - x_1 - x_2, \quad y_3' = \lambda x_3 + \nu$$

som gir $y_3 = -\lambda x_3 - \nu$. □

Vi tar med formelen for dobling av et punkt også.

PROPOSISJON 4.37. *For $P = (x_1, y_1) \in E$, har vi at $2P = (x_2, y_2)$, med*

$$x_2 = \frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4(x_1^3 + Ax_1 + B)}$$
$$y_2 = \frac{3x_1^2 + A}{2y_1}x_2 + \frac{-x_1^3 + Ax_1 + 2B}{2y_1}$$

PROPOSISJON 4.38. *La E være en elliptisk kurve. Det finnes en morfi $-\colon E \to E$ slik at*

$$-(P) = -P \quad \forall P \in E$$

BEVIS. Bruker $x, y \in \overline{K}(E)$, definerer den rasjonale avbildningen

$$- = [x : -y : 1]\colon E \to E.$$

Hvis $P \neq O$, så er x, y regulære, så $-$ er regulær i P, og for $P = (x_0, y_0)$ er $-(P) = (x_0, -y_0) = -P$.

I punktet O bruker vi

$$- = [xy^{-1} : -1 : y^{-1}].$$

Sjekker at xy^{-1} og y^{-1} er regulære og lik 0 i O, så $-(O) = [0 : 1 : 0] = O$. □

KOROLLAR 4.39. *La (E, O) være en elliptisk kurve definert over K. Da er $E(K) \subset E$ en undergruppe.*

BEVIS. Vi har per antakelse at $O \in E(K)$.

Hvis $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(K) \setminus \{O\}$, må vi sjekke at $P_1 + P_2 = (x_3, y_3) \in E(K)$, altså at $x_3, y_3 \in K$.

Hvis $x_1 \neq x_2$ følger dette fra Teorem 4.36. Hvis $x_1 = x_2$ og $y_1 = y_2$, følger dette fra Proposisjon 4.37. Hvis $x_1 = x_2$ og $y_1 \neq y_2$, må vi ha $y_1 = -y_2$, og da er $P_1 + P_2 = O \in E(K)$.

Til slutt, hvis $P = (x, y) \in E(K)$, så er $-P = (x, -y) \in E(K)$. □

3.3. Morfier definert via gruppestrukturen. De ovenstående formlene indikerer at diverse naturlige avbildninger definert via gruppestrukturen er gitt av rasjonale funksjoner. Her følger noen resultater som gjør dette mer presist.

PROPOSISJON 4.40. *La $P \in E$. Det finnes en morfi $\tau_P\colon E \to E$ slik at*

$$\tau_P(Q) = P + Q \qquad \forall Q \in E.$$

BEVIS. Hvis $P = O$, lar vi $\tau_O = \mathrm{id}_E$.

Ellers, skriv $P = (x_1, y_1)$, la

$$\lambda = \frac{y - y_1}{x - x_1}, \quad \nu = \frac{y_1 x - y x_1}{x - x_1} \in \overline{K}(E).$$

Hvor er λ, ν regulære? For $Q \in E$, er $Q = O$ eller $Q = (x, y)$ for $x, y \in \overline{K}$. Hvis $x \neq x_1$ er da både λ og ν regulære. Altså: λ, μ er regulære i Q i hvert fall hvis $Q \notin \{O, P, -P\}$.

Definer en rasjonal avbildning $\tau_P = [f_0 : f_1 : f_2]\colon E \to E$ ved

$$f_0 = \lambda^2 - x - x_1, \quad f_1 = -\lambda f_0 + \nu, \quad f_2 = 1.$$

Hvis $Q \notin \{O, P, -P\}$, så er f_1, f_2 regulære i Q, så τ_P er regulær i Q. Da er $\tau_P(Q) = Q + P$, ved beregningene fra forrige forelesning:

$$[f_0(Q) : f_1(Q) : 1] = (f_0(Q), f_1(Q)) = P + Q$$

Er τ_P en morfi? Ja, siden E er en ikkesingulær kurve.

I hver av $Q = O, P, -P$ kan vi altså finne en $g \in \overline{K}(E)$ slik at gf_0, gf_1, gf_2 er regulære i Q.

Lar være å sjekke at også for $Q = O, P, -P$ er da

$$\tau_P(Q) = [gf_0(Q) : gf_1(Q) : gf_2(Q)] = Q + P.$$

□

Morfiene $\tau_P \colon E \to E$ for ulike P er slik at for $P, Q \in E$, er

$$\tau_P \circ \tau_Q = \tau_Q \circ \tau_P = \tau_{P+Q}.$$

Spesielt er τ_P for alle P en isomorfi, med invers τ_{-P}, siden $\tau_O = \mathrm{id}_E$.

PROPOSISJON 4.41. *La X være en varietet, og la $\phi, \psi \colon X \to E$ være to morfier. Da finnes en morfi $\phi + \psi \colon X \to E$ slik at*

$$(\phi + \psi)(P) = \phi(P) + \psi(P) \quad \forall P \in X.$$

IDÉ TIL BEVIS. La $\phi = [f_0' : f_1' : f_2']$, la $\psi = [g_0' : g_1' : g_2']$, med $f_i', g_i' \in \overline{K}(X)$, og anta for enkelhets skyld at $f_2', g_2' \neq 0$. Kan da skrive $\phi = [f_0 : f_1 : 1]$ og $\psi = [g_0 : g_1 : 1]$, med $f_i = f_i'/f_2'$ og $g_i = g_i'/g_2'$.

La $\lambda = \frac{g_1 - f_1}{g_0 - f_0}$, $\nu = \frac{f_1 g_0 - f_0 g_1}{g_0 - f_0} \in \overline{K}(X)$, og definer

$$\phi + \psi = [h_0 : h_1 : 1] \colon X \to E$$

med

$$h_0 = \lambda^2 - g_0 - f_0, \quad h_1 = -\lambda h_1 - \nu.$$

Hvis h_0, h_1 er regulære i $P \in X$, så er

$$(\phi + \psi)(P) = [h_0(P) : h_1(P) : 1] = \phi(P) + \psi(P).$$

Det vanskelige punktet som vi dropper å vise er at den rasjonale avbildningen $\phi + \psi \colon X \to E$ definert på denne måten er regulær overalt, og at vi da har $(\phi + \psi)(P) = \phi(P) + \psi(P)$ for alle $P \in X$. □

KAPITTEL 5

Isogenier

1. Gruppa av isogenier

DEFINISJON 5.1. La (E_1, O_1), (E_2, O_2) være to elliptiske kurver, og la $\phi\colon E_1 \to E_2$ være en morfi. Hvis $\phi(O_1) = O_2$ så er ϕ en *isogeni*.

Vi har ved følgende lemma at enhver morfi mellom elliptiske kurver er en komposisjon av en isogeni og en translasjon (så selv om vi bryr oss om vilkårlige morfier gir det god mening å først prøve å forstå isogeniene).

LEMMA 5.2. *Hvis $\phi\colon E_1 \to E_2$ er en morfi, så er $\tau_{-\phi(O_1)} \circ \phi$ en isogeni.*

BEVIS. $\tau_{-\phi(O_1)} \circ \phi(O_1) = \tau_{-\phi(O_1)}(\phi(O_1)) = -\phi(O_1) + \phi(O_1) = O_2$. □

DEFINISJON 5.3. Gitt E_1, E_2, skriver vi $\mathrm{Hom}(E_1, E_2)$ for mengden av isogenier.

Vet at en morfi av kurver $\phi\colon E_1 \to E_2$ er enten konstant eller surjektiv. Har den spesielle isogenien

$$[0]\colon E_1 \to E_2$$

gitt ved

$$[0](P) = O_2 \quad \forall P \in E_1,$$

og alle andre isogenier ϕ er surjektive. Slike ϕ er bestemt av kroppinklusjonen

$$\phi^*\colon \overline{K}(E_2) \hookrightarrow \overline{K}(E_1).$$

PROPOSISJON 5.4. *Gitt $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, ligger $\phi + \psi$ i $\mathrm{Hom}(E_1, E_2)$. Med denne operasjonen blir $\mathrm{Hom}(E_1, E_2)$ en abelsk gruppe.*

BEVIS. Må sjekke (1) assosiativitet, (2) $\exists$ enhetselement, (3) $\exists$ inverser.

(1): Rett fram.

(2): [0] er et enhetselement.

(3): Gitt $\phi \in \mathrm{Hom}(E_1, E_2)$, så er $- \circ \phi \in \mathrm{Hom}(E_1, E_2)$ en invers til ϕ, med $-\colon E_2 \to E_2$. □

DEFINISJON 5.5. Skriver $\mathrm{End}(E) = \mathrm{Hom}(E, E)$.

EKSEMPEL 5.6. For $m > 0$, definer $[m] = \mathrm{id}_E + \cdots + \mathrm{id}_E \in \mathrm{End}(E)$. For $m < 0$, definer $[m] = -[-m]$.

Konkret er $[m](P) = mP \in E$ for alle P og alle $m \in \mathbb{Z}$.

Har $[m_1] + [m_2] = [m_1 + m_2]$ og $[m_1] \circ [m_2] = [m_1 m_2]$.

DEFINISJON 5.7. Gitt en $m \in \mathbb{Z}$, er gruppa av *m-torsjonspunkter* i E gitt ved

$$E[m] = \{P \in E \mid mP = O\} \subset E.$$

LEMMA 5.8. *La E være Weierstrass-kruven gitt ved $y^2-(x^3+Ax+B)$. Hvis $P \in E$, så er $2P = O$ hvis og bare hvis enten $P = O$ eller $P = (x_0, 0)$, hvor x_0 er rot av $x^3 + Ax + B$.*

BEVIS. Hvis $P = O$, så er $2P = O$. Hvis $P \neq O$, så er $P = (x, y)$ og $-P = (x, -y)$. Har $2P = O \Leftrightarrow P = -P \Leftrightarrow y = 0 \Rightarrow x_0^3 + Ax_0 + B = 0$. □

PROPOSISJON 5.9. *For alle $m \in \mathbb{Z}$, så er $[m] \neq [0] \in \mathrm{End}(E)$.*

BEVIS. Har $[m] \neq [0] \Leftrightarrow [m]$ er ikke surjektiv. Dermed, hvis $[m_1], [m_2] \neq [0]$, så er $[m_1 m_2] = [m_1] \circ [m_2] \neq 0$, siden komposisjonen av surjektive morfier er surjektiv.

Ved lemmaet over finnes Q slik at $2Q \neq O$, så $[2] \neq [0]$. Dermed er $[2]$ surjektiv, så for alle $n \geq 1$ er

$$[2^n] = [2] \circ \cdots \circ [2],$$

også surjektiv.

Hvis m er odde og $P \in E[2]$, så skriver vi $m = 2k + 1$ og får

$$[m](P) = mP = 2kP + P = O + P = P,$$

altså er $[m] \neq [0]$.

For $0 \neq m \in \mathbb{Z}$ kan vi skrive $m = 2^n k$ med k odde. Siden $[2^n]]$ og $[k]$ er surjektive, så er $[m] = [2^n][k]$ surjektiv, og altså er $[m] \neq [0]$. □

PROPOSISJON 5.10. *Gruppen $\mathrm{Hom}(E_1, E_2)$ er torsjonsfri, dvs. hvis $0 \neq \phi \in \mathrm{Hom}(E_1, E_2)$ og $n \geq 1$, så er $n\phi \neq 0$.*

BEVIS. Har $n\phi = [n] \circ \phi$, hvor $[n] \in \mathrm{End}(E_2)$, siden for alle $P \in E_1$ er

$$(n\phi)(P) = n(\phi(P)) = ([n] \circ \phi)(P).$$

Siden $[n], \phi \neq 0$, er både $[n]$ og ϕ surjektive, så $[n] \circ \phi$ er surjektiv og altså ulik $[0]$. □

TEOREM 5.11. *La $\phi \in \mathrm{Hom}(E_1, E_2)$. Da definerer ϕ en gruppehomomorfi, det vil si at for alle $P, Q \in E_1$ har vi*

$$\phi(P + Q) = \phi(P) + \phi(Q).$$

Husk fra Avsnitt 3.5 følgende generelle konstruksjon:

DEFINISJON 5.12. Gitt en morfi av ikkesingulære kurver $\phi\colon C_1 \to C_2$, er *pushforward langs ϕ* homomorfien $\phi_*\colon \mathrm{Div}(C_1) \to \mathrm{Div}(C_2)$ gitt ved

$$\phi_*(\sum_{i=1}^{r} n_i P) = \sum_{i=1}^{r} n_i \phi(P).$$

PROPOSISJON (Fra Prop. 3.45, punkt (6)). *Hvis $D_1 \sim D_2 \in \mathrm{Div}(C_1)$, så er $\phi_*(D_1) \sim \phi_*(D_2)$.*

KOROLLAR 5.13. *Homomorfien $\phi_*\colon \mathrm{Div}(C_1) \to \mathrm{Div}(C_2)$ induserer en homomorfi $\phi_*\colon \mathrm{Pic}(C_1) \to \mathrm{Pic}(C_2)$.*

BEVIS FOR TEOREM. La $P, Q \in E_1$ og $R = P + Q$. Har da (per def. av $+$)

$$R - O_1 \sim (P - O_1) + (Q - O_1) = P + Q - 2O_1 \in \mathrm{Div}(E_1)$$

Dermed er

$$\phi(R) - O_2 = \phi_*(R - O_1) \sim \phi_*(P + Q - 2O_1) = \phi(P) + \phi(Q) - 2O_2,$$

som betyr at $\phi(R) = \phi(P) + \phi(Q)$. □

KOROLLAR 5.14. *Hvis $\phi \in \mathrm{Hom}(E_1, E_2)$, så er $\phi(E_1[k]) \subset E_2[k]$ for alle $k \geq 1$.*

BEVIS. Hvis $P \in E_1$ med $kP = O_1$, så er $k\phi(P) = \phi(kP) = \phi(O_1) = O_2$. □

TEOREM 5.15. *For en elliptisk kurve E, så er $\mathrm{End}(E)$ en (muligens ikke-kommutativ) ring, med sum som tidligere definert, og produkt gitt ved $\phi\psi = \phi \circ \psi$.*

I denne ringen er $\phi\psi \neq 0$ hvis ϕ og $\psi \neq 0$.

BEVIS. Vet at $\mathrm{End}(E)$ med $+$ er abelsk gruppe.

Må sjekke

(1) $(\phi\psi)\chi = \phi(\psi\chi)$: Opplagt.

(2) $\exists$ multiplikativ enhet: Ta $[1]$, opplagt at $[1]\psi = \psi = \psi[1]$.

(3) a) $\phi(\psi + \chi) = \phi\psi + \phi\chi$ og b) $(\psi + \chi)\phi = \psi\phi + \chi\phi$.

For a), har

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

merk at vi bruker at ϕ er en homomorfi. b) er tilsvarende, men enklere.

Hvis $\phi, \psi \neq 0$, så er ϕ, ψ surjektive, som betyr at $\phi\psi$ er surjektiv og ulik 0. □

EKSEMPEL 5.16. For alle E, gir $n \mapsto [n] \in \mathrm{End}(E)$ en ringinklusjon $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$.

Kan vises at hvis $\mathrm{char}\, K = 0$, så er $\mathrm{End}(E) = \mathbb{Z}$ for "de fleste" E. Hvis $\mathrm{End}(E) \neq \mathbb{Z}$, sies E å *ha kompleks multiplikasjon.*

EKSEMPEL 5.17. La E være gitt ved $y^2 = x^3 - x$. Definer en morfi $[i] \colon E \to E$ ved

$$[i] = [-x : iy : 1].$$

Da har vi $[i]^2 = [x : -y : 1] = [-1]$, så $[i] \in \mathrm{End}(E) \setminus \mathbb{Z}$, og vi får en inklusjon $\mathbb{Z}[i] \hookrightarrow \mathrm{End}(E)$.

2. Isogenier og endelige undergrupper

Vi antar i denne delen (for enkelhets skyld) at $\mathrm{char}\, K = 0$, se [**Sil09**, III.4.10-12] for presise resultater når $\mathrm{char}\, K \neq 0$. Poenget med dette er følgende resultat fra for litt siden.

PROPOSISJON 5.18. *Anta at $\mathrm{char}\, K = 0$, og la $\phi \colon C_1 \to C_2$ være en morfi av ikkesingulære kurver. For $Q \in C_2$, så er $|\phi^{-1}(Q)| = \deg \phi$ unntatt i endelig mange punkter.*

TEOREM 5.19. *La $\phi \colon E_1 \to E_2$ være en ikkekonstant isogeni. For alle $Q \in E_2$, så er $|\phi^{-1}(Q)| = \deg \phi$.*

BEVIS. Homomorfien ϕ er surjektiv. Hvis vi velger $P \in \phi^{-1}(Q)$, så har vi en bijeksjon $\phi^{-1}(O) \leftrightarrow \phi^{-1}(Q)$ gitt ved

$$R \in \phi^{-1}(O_2) \leftrightarrow R + P \in \phi^{-1}(Q).$$

Dermed er $|\phi^{-1}(Q)| = |\phi^{-1}(O_2)|$ for alle Q. Siden det finnes en Q slik at $|\phi^{-1}(Q)| = \deg \phi$, så gjelder dette for alle Q. □

EKSEMPEL 5.20. Kan nå beregne $\deg[2] = |\ker[2]| = |E[2]|$. Har $P \in E[2] \Leftrightarrow 2P = O$, som er hvis og bare hvis $P = O$ eller $P = (\alpha, 0)$ med $\alpha^3 + A\alpha + B = 0$. Dermed er $|E[2]| = 4$.

Vi ønsker nå å vise noen resultater som oppsummert sier omtrent at det å spesifisere en isogeni $\phi\colon E_1 \to E_2$ er det samme som å spesifisere en endelig undergruppe $(\ker \phi)$ av E_1.

TEOREM 5.21. *La $\phi\colon E_1 \to E_2$ være en ikkekonstant isogeni. Da er*

$$\ker \phi \to \mathrm{Aut}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2)))$$

gitt ved

$$T \mapsto \tau_T^*\colon \overline{K}(E_1) \to \overline{K}(E_1).$$

en isomorfi av grupper.

BEVIS. Sjekker først at $\tau_T^* \in \mathrm{Aut}(\overline{K}(E_1), \phi^*\overline{K}(E_2))$. La $T \in \ker \phi$. Da er $\phi \circ \tau_T = \phi$, siden

$$\phi(\tau_T(P)) = \phi(P + T) = \phi(P) + \phi(T) = \phi(P).$$

Hvis $f \in \overline{K}(E_2)$, så er

$$\tau_T^* \circ \phi^*(f) = f \circ \phi \circ \tau_T = f \circ \phi = \phi^*(f),$$

så $\tau_T^* \in \mathrm{Aut}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$.

Har

$$\tau_{T_1}^* \tau_{T_2}^* = (\tau_{T_1} \circ \tau_{T_2})^* = \tau_{T_1+T_2}^*$$

så $T \mapsto \tau_T$ er en gruppehomomorfi.

Siden $|\ker \phi| = \deg \phi \geq |\mathrm{Aut}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2)))|$, så holder det å vise at avbildningen $T \mapsto \tau_T^*$ er injektiv. Men hvis $\tau_T^* = \mathrm{id}_{\overline{K}(E_1)}$, så må $\tau_T = \mathrm{id}_{E_1}$, som betyr at $T = O_1$. Altså er avbildningen injektiv. □

TEOREM 5.22. *La $\phi\colon E_1 \to E_2$ være en ikkekonstant isogeni. Da er kroppsutvidelsen $\phi^*(\overline{K}(E_2)) \subset \overline{K}(E_1)$ en Galois-utvidelse.*

BEVIS. Vi har

$$[\overline{K}(E_1) : \phi^*(\overline{K}(E_2))] = \deg \phi = |\ker \phi| = |\mathrm{Aut}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2))|,$$

som betyr at ϕ^* er Galois. □

TEOREM 5.23. *La $\phi\colon E_1 \to E_2$ og $\psi\colon E_1 \to E_3$ være ikkekonstante isogenier. Hvis $\ker \phi \subset \ker \phi$, så finnes en unik isogeni $\lambda\colon E_2 \to E_3$ slik at $\lambda \circ \phi = \psi$.*

BEVIS. Har at $\overline{K}(E_1)$ er en Galois-utvidelse av $\phi^*(\overline{K}(E_2))$ og av $\psi^*(\overline{K}(E_3))$. Dermed er $\phi^*(\overline{K}(E_2)) = \overline{K}(E_1)^{\ker\phi}$ og $\psi^*(\overline{K}(E_3)) = \overline{K}(E_1)^{\ker\psi}$. Siden $\ker\phi \subset \ker\psi$ har vi da

$$\psi^*(\overline{K}(E_3)) \subseteq \phi^*(\overline{K}(E_2)) \subseteq \overline{K}(E_1),$$

så det finnes en unik $\chi\colon \overline{K}(E_3) \to \overline{K}(E_2)$ slik at $\phi^* \circ \lambda^* = \psi^*$. Vi lar $\lambda\colon E_2 \to E_3$ være bestemt av at $\lambda^* = \chi$. □

PROPOSISJON 5.24. *La $\phi\colon E_1 \to E_2$ være ikkekonstant isogeni.* $\ker\phi \subset E_1$ *er en endelig abelsk gruppe, og kroppsutvidelsen $\phi^*\colon \overline{K}(E_2) \to \overline{K}(E_1)$ er Galois med Galois-gruppe* $\ker\phi$.

$$\begin{array}{lll} \ker\phi \subset & E_1 & \overline{K}(E_1) \\ & \big\downarrow{\scriptstyle \phi} & {\scriptstyle \phi^*}\big\uparrow \\ & E_2 & \overline{K}(E_2) \end{array}$$

PROPOSISJON 5.25. *Gitt et diagram av isogenier*

$$\begin{array}{ccc} E_1 & \xrightarrow{\psi} & E_2 \\ & {\scriptstyle \phi}\searrow & \\ & & E_3 \end{array}$$

slik at $\ker\phi \subseteq \ker\psi$*, så finnes en unik $\lambda\colon E_2 \to E_3$ slik at $\lambda \circ \phi = \psi$.*

$$\begin{array}{ccc} E_1 & \xrightarrow{\psi} & E_2 \\ & {\scriptstyle \phi}\searrow & \circ \;\; \exists!\,\big\downarrow{\scriptstyle \lambda} \\ & & E_3 \end{array}$$

TEOREM 5.26. *La E være en elliptisk kurve og la $\Phi \subset E$ være en endelig undergruppe. Da finnes en unik elliptisk kurve E' og en isogeni $\phi\colon E \to E'$ slik at $\Phi = \ker\phi$.*

$$\begin{array}{lll} \Phi \subset & E_1 & \\ & \exists!\,\big\downarrow{\scriptstyle \phi} & \\ & \exists!\;\; E_2 & \qquad \ker\phi = \Phi \end{array}$$

BEVIS. For hvert punkt $T \in \Phi$ har vi $\tau_T^* \in \mathrm{Aut}(\overline{K}(E)/\overline{K})$, og dette gir en inklusjon $\Phi \subset \mathrm{Aut}(\overline{K}(E)/\overline{K})$. Vi ser på

$$\overline{K}(E)^\Phi = \{f \in \overline{K}(E) \mid \tau_T^*(f) = f, \forall T \in \Phi\} \subset \overline{K}(E)$$

Et resultat fra Galois-teori sier at kroppsutvidelsen $\overline{K}(E)/\overline{K}(E)^\Phi$ er Galois med $\mathrm{Aut}(\overline{K}(E)/\overline{K}(E)^\Phi) = \Phi$.

Spesielt er utvidelsen $\overline{K}(E)/\overline{K}(E)^\Phi$ endelig. Dermed er

$$\mathrm{tr.deg.}(\overline{K}(E)^\Phi/\overline{K}) = \mathrm{tr.deg.}(\overline{K}(E)/K) = 1,$$

så det finnes en unik ikkesingulær kurve E' med $\overline{K}(E') \cong \overline{K}(E)^\Phi$, og en morfi $\phi\colon E \to E'$ slik at $\phi^*\colon \overline{K}(E') \to \overline{K}(E)^\Phi$ identifiserer $\overline{K}(E')$ med $\overline{K}(E)^\Phi$.

Kan sjekke at genus til E' er 1, vi gjør ikke det.

Lar vi $O' = \phi(O) \in E'$, så blir (E', O') en elliptisk kurve, ϕ en isogeni. Vet da ved resultatet over at

$$\mathrm{Aut}(\overline{K}(E)/\phi^*\overline{K}(E')) = \ker\phi,$$

så

$$\Phi = \mathrm{Aut}(\overline{K}(E)/\overline{K}(E)^\Phi) = \mathrm{Aut}(\overline{K}(E)/\phi^*(\overline{K}(E')) = \ker\phi.$$

□

Eksempel 5.27. La E_1 være en gitt elliptisk kurve. Hvis $\phi\colon E_1 \to E_2$ er en isogeni av grad 2, hvordan kan E_2 og ϕ se ut? Resultatet over sier at $\phi\colon E_1 \to E_2$ er entydig bestemt av $\ker\phi$.

Hvis $\deg\phi = 2$, så er $|\ker\phi| = 2$, så $\ker\phi \cong \mathbb{Z}/2\mathbb{Z}$. Det betyr at $\ker\phi = \{O, P\}$, hvor $2P = O$, og altså er

$$P \in \{P_1, P_2, P_3\},$$

hvor $P_i = (\alpha_i, 0)$ og α_i er røttene av $x^3 + Ax + B$.

Uformelt oppsummert finnes det tre ulike isogenier ut av E_1 med grad 2, en for hvert 2-torsjonspunkt (unntatt O).

3. Den duale isogenien

Teorem 5.28 (+ Definisjon). *La $\phi\colon E_1 \to E_2$ være en ikkekonstant isogeni. Da finnes en unik isogeni $\hat{\phi}\colon E_2 \to E_1$ slik at*

$$\hat{\phi}\circ\phi = [\deg\phi] \in \mathrm{End}\, E_1.$$

Vi kaller $\hat{\phi}$ den duale isogenien til ϕ (og setter $\widehat{[0]} = [0]$).

Bevis. Vi har isogenier

$$\begin{array}{ccc} E_1 & \xrightarrow{\ \phi\ } & E_2 \\ & \searrow^{[\deg\phi]} & \\ & & E_1 \end{array}$$

Vi vet at $|\ker\phi| = \deg\phi$. For alle $P \in \ker\phi$ har vi da $(\deg\phi)P = 0$, så dermed har vi $P \in \ker[\deg\phi]$. $\ker\phi \subseteq \ker[\deg\phi]$. Altså finnes en unik $\hat{\phi}\colon E_2 \to E_1$ slik at $\hat{\phi}\circ\phi = [\deg\phi]$.

$$\begin{array}{ccc} E_1 & \xrightarrow{\ \phi\ } & E_2 \\ & \searrow^{[\deg\phi]}\ \circlearrowright & \downarrow{\scriptstyle\hat{\phi}} \\ & & E_1 \end{array}$$

□

Fra definisjonen kan vi også gi en konkret beskrivelse av $\hat{\phi}$:

Proposisjon 5.29. *La $\phi\colon E_1 \to E_2$ være ikkekonstant isogeni, og la $Q \in E_2$ med $P \in E_1$ slik at $\phi(P) = Q$. Da er*

$$\hat{\phi}(Q) = (\deg\phi)P \in E_1.$$

Bevis. $\hat{\phi}(Q) = \hat{\phi}(\phi(P)) = (\hat{\phi}\circ\phi)(P) = [\deg\phi](P) = (\deg\phi)P.$ □

Proposisjon 5.30. *La $\phi\colon E_1 \to E_2$ være en isogeni.*

a) $\hat{\phi}\circ\phi = [\deg\phi] \in \mathrm{End}(E_1)$ og $\phi\circ\hat{\phi} = [\deg\phi] \in \mathrm{End}(E_2)$.

b) Hvis $\psi\colon E_2 \to E_3$ er en isogeni, så er

$$\widehat{(\psi \circ \phi)} = \hat{\phi} \circ \hat{\psi}.$$

BEVIS. a) $\hat{\phi} \circ \phi = [m]$ per def. Får da

$$(\phi \circ \hat{\phi}) \circ \phi = \phi \circ [m] = [m] \circ \phi,$$

så siden ϕ er ikkekonstant er $[m] = \phi \circ \hat{\phi}$.

b) Må sjekke at

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

Har

$$\begin{aligned}(\hat{\phi} \circ \hat{\psi}) \circ \psi \circ \phi = \hat{\phi} \circ [\deg \psi] \circ \phi = [\deg \psi] \circ \hat{\phi} \circ \phi = [\deg \psi] \circ [\deg \phi] \\ = [(\deg \psi)(\deg \phi)] = [\deg \psi \circ \phi]\end{aligned}$$

□

PROPOSISJON 5.31 (Vanskelig, vises ikke). *Hvis $\psi\colon E_1 \to E_2$ er en isogeni, så er*

$$\widehat{(\psi + \phi)} = \hat{\psi} + \hat{\phi}.$$

PROPOSISJON 5.32. *For alle $m \in \mathbb{Z}$, så er $\widehat{[m]} = [m]$ og $\deg[m] = m^2$.*

BEVIS. Har at $\widehat{[0]} = [0]$ og $\widehat{[\pm 1]} = [\pm 1]$. Gitt at $\widehat{[m]} = [m]$, så er

$$\widehat{[m+1]} = \widehat{[m] + [1]} = [m] + [1] = [m+1],$$

og tilsvarende for $[m-1]$, så ved induksjon får vi et bevis.

For påstanden om graden vet vi nå at

$$[\deg[m]] = \widehat{[m]} \circ [m] = [m][m] = [m^2].$$

□

KOROLLAR 5.33. *For alle $m \in \mathbb{Z}$ er $E[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$.*

BEVIS. Vi gjør tilfellet $m = p$ for et primtall p. Siden $E[p] = p^2$, er enten

$$E[p] = \mathbb{Z}/p \oplus \mathbb{Z}/p \text{ eller } E[p] = \mathbb{Z}/p^2$$

Men siden $px = 0$ for alle $x \in E[p]$, må det første tilfellet være det riktige.

For en generell m har vi, for alle divisorer d av m, at $E[d] \subset E[m]$ med

$$E[d] = \{x \in E[m] \mid dx = 0\}.$$

□

PROPOSISJON 5.34. *a) $\deg \hat{\phi} = \deg \phi$.*

b) ϕ er den duale isogenien til $\hat{\phi}$, altså: $\hat{\hat{\phi}} = \phi$.

BEVIS. a) Siden $\hat{\phi} \circ \phi = [\deg \phi]$, så er

$$\deg(\hat{\phi}) \deg(\phi) = \deg([\deg \phi]) = (\deg \phi)^2,$$

som gir $\deg(\hat{\phi}) = \deg \phi$.

b) Vi har vist at $\phi \circ \hat{\phi} = [\deg \phi] = [\deg \hat{\phi}]$, som betyr at ϕ er den duale isogenien til $\hat{\phi}$.

□

Spørsmål: Hvordan beskrive $\mathrm{Hom}(E_1, E_2)$ og $\mathrm{End}(E)$?

Ide: Gitt en isogeni $\phi\colon E_1 \to E_2$, se på hva ϕ gjør med torsjonsgruppene $E_i[n]$. For å utnytte dette skikkelig trenger vi *Tate-modulen*. Først litt bakgrunn om l-adiske heltall.

4. l-adiske heltall

La l være et primtall. I ringen $\mathbb{Z}$ har vi idealene (l^n), som gir en kjede av ringer og surjeksjoner

$$\cdots \to \mathbb{Z}/l^3 \xrightarrow{\delta_3} \mathbb{Z}/l^2 \xrightarrow{\delta_2} \mathbb{Z}/l \xrightarrow{\delta_1} 0.$$

Definisjon 5.35. La l være et primtall. Ringen av l-adiske heltall, $\mathbb{Z}_l$, er ringen av sekvenser $a_1, a_2, \ldots$, hvor $a_i \in \mathbb{Z}/(l^i)$, og vi krever at $\delta_i(a_i) = a_{i-1}$.

Addisjon og multiplikasjon er komponentvis:

$$(a_i)(b_i) = (a_i b_i) \qquad (a_i) + (b_i) = (a_i + b_i)$$

4.1. l-adiske tall som rekker. Et element $a_i \in \mathbb{Z}/(l^i)$ kan representeres av et tall mellom 0 og $l^i - 1$. Dermed kan a_i skrives unikt som

$$a_i = c_0 + c_1 l + c_2 l^2 + \cdots + c_{i-1} l^{i-1}$$

med $c_j \in \{0, \ldots, l-1\}$ (en base l-representasjon). Vi har da

$$\delta_i(a_i) = a_i \bmod l^{i-1} = c_0 + c_1 l + \cdots + c_{i-2} l^{i-2},$$

Dermed vil et l-adisk tall $a = (a_i)_{i=1}^{\infty}$ kunne skrives som

$$a_1 = c_0$$
$$a_2 = c_0 + c_1 l$$
$$a_3 = c_0 + c_1 l + c_2 l^2, \text{ osv.}$$

Vi kan dermed representere a ved en uendelig rekke

$$a = c_0 + c_1 l + c_2 l^2 + \cdots$$

med alle $c_i \in \{0, \ldots, l-1\}$.

Addisjon i $\mathbb{Z}_l$ fungerer da slik:

$$\left(\sum_{i=0}^{\infty} c_i l^i\right) + \left(\sum_{i=0}^{\infty} b_i' l^i\right) = \sum_{i=0}^{\infty} c_i'' l^i,$$

hvor for alle k, så er

$$\sum_{i=0}^{k-1} c_i l^i + \sum_{i=0}^{k-1} b_i' l^i = \sum_{i=0}^{k-1} c_i'' l^i \pmod{l^k},$$

Produktet fungerer på tilsvarende måte.

Alternativt: Still opp som på barneskolen (lat som $l = 10$):

$$\begin{array}{cccccc} & \cdots & c_2 & c_1 & c_0 \\ + & \cdots & c_2' & c_1' & c_0' \\ \hline = & \cdots & c_2'' & c_1'' & c_0'' \end{array}$$

EKSEMPEL 5.36. Et heltall n gir et l-adisk tall $\phi(n) = (a_i)_{i=1}^{\infty}$ hvor $a_i = n \pmod{l^i}$. (Alternativt: Skriv $n = \sum_{i=0}^{k} c_i l^i$.) Dette gir en ringinklusjon $\phi\colon \mathbb{Z} \hookrightarrow \mathbb{Z}_l$.

EKSEMPEL 5.37. La $a = 1 + l + l^2 + l^3 + \cdots \in \mathbb{Z}_l$. Da er $(1-l)a = 1 \in \mathbb{Z}_l$.

PROPOSISJON 5.38. *Ringen $\mathbb{Z}_l$ er*

- *et helområde.*
- *lokal, med unikt maksimal ideal*
$$(l) = \{c_1 l + c_2 l^2 + \cdots\} \in \mathbb{Z}_l.$$
- *en DVR, og idealene i $\mathbb{Z}_l$ er (l^i) og (0).*

MERKNAD 5.39. Brøkkroppen til $\mathbb{Z}_l$ skrives $\mathbb{Q}_l$, og er ringen av elementer på formen $\sum_{i=n}^{\infty} c_i l^i$ for $n \in \mathbb{Z}$.

5. Tate-modulen til en elliptisk kurve

Vi har sett at hvis $\phi\colon E_1 \to E_2$ er en isogeni, så gir ϕ en avbildning av torsjonspunktene, $\phi[n]\colon E_1[n] \to E_2[n]$, for alle n. Vi vil utnytte dette til å forstå mengden isogenier bedre. For å gjøre det, må vi introdusere *Tate-modulen* til en elliptisk kurve.

La l være et primtall, og anta nå at $\operatorname{char} K = 0$ eller $\operatorname{char} K = p$, $p \neq l$. Vi ser på de endelige gruppene $E[l^i]$, som vi har beregnet til[1]

$$E[l^i] \cong \mathbb{Z}/l^i\mathbb{Z} \oplus \mathbb{Z}/l^i\mathbb{Z}$$

Hvis $P \in E[l^i]$, så ligger $[l](P) = lP \in E[l^{i-1}]$. Vi har dermed en kjede av abelske grupper

$$\cdots \xrightarrow{[l]} E[l^3] \xrightarrow{[l]} E[l^2] \xrightarrow{[l]} E[l]$$

DEFINISJON 5.40. Den l-adiske Tate-modulen til E, skrevet $T_l(E)$, er den abelske gruppa av sekvenser $P_1, P_2, P_3, \ldots$, hvor $P_i \in E[l^i]$ og $[l](P_i) = P_{i-1}$.

PROPOSISJON 5.41. *Den abelske gruppa $T_l(E)$ blir en modul over $\mathbb{Z}_l$ ved å sette, for $a = (a_i)_{i=1}^{\infty} \in \mathbb{Z}_l$ og $v = (P_i)_{i=1}^{\infty} \in T_l(E)$, at*

$$av = (a_i P_i)_{i=1}^{\infty} \in T_l(E).$$

PROPOSISJON 5.42. *Vi har en isomorfi av $\mathbb{Z}_l$-moduler: $T_l(E) \cong \mathbb{Z}_l \oplus \mathbb{Z}_l$.*

BEVIS. Har en isomorfi $E[l] \cong \mathbb{Z}/l \oplus \mathbb{Z}/l$. La $P_1, Q_1 \in E[l]$ være slik at $P_1 = (1,0)$ og $Q_1 = (0,1)$ under denne isomorfien. Velg så, for alle i, punkter $P_i, Q_i \in E[l^i]$ slik at $lP_i = P_{i-1}$ og $lQ_i = Q_{i-1}$.

Vi påstår at P_i, Q_i genererer $E[l^i]$. Mer presist:

LEMMA 5.43. *For alle i er avbildningen*

$$\psi\colon \mathbb{Z}/l^i \oplus \mathbb{Z}/l^i \to E[l^i]$$

definert ved $(a,b) \mapsto aP_i + bQ_i$ en isomorfi.

[1] Vi har hoppet over å vise dette for $\operatorname{char} K = p \neq l$.

BEVIS. Opplagt for $i = 1$, vi bruker (sterk) induksjon på i.

Vi vet at $E[l^i] \cong \mathbb{Z}/l^i \oplus \mathbb{Z}/l^i$, så ved å telle elementer i gruppene, holder det å vise at ψ er en injeksjon. Med andre ord må vi sjekke at hvis $a, b \in \mathbb{Z}$ er slik at $aP_i + bQ_i = 0$, så er både a, b delelig med l^i.

Skriv $a = a'l^j$ og $b = b'l^k$ med $a', b' \neq 0 \pmod{l}$, og anta WLOG[2] at $j \leq k$. Anta for en motsigelse at $j < i$. Da er

$$aP_i + bQ_i = a'l^j P_i + b'l^{k-j} l^j Q_i = a'P_{i-j} + b'l^{k-j} Q_{i-j} = 0.$$

Ved induksjonsantagelsen brukt på $i - j$, må vi da ha at l^{i-j} deler a' (og $b'l^{k-j}$), som gir en motsigelse. □

Definer nå en avbildning $\phi\colon \mathbb{Z}_l \oplus \mathbb{Z}_l \to T_l(E)$ ved å sette

$$\phi((a_i), (b_i)) = (a_i P_i + b_i Q_i)$$

Lett å sjekke at dette er en avbildning av $\mathbb{Z}_l$-moduler.

La $v = (R_i) \in T_l(E)$. Lemmaet ovenfor viser at vi for alle i kan finne unike $a_i, b_i \in \mathbb{Z}/l^i$ slik at $a_i P_i + b_i Q_i = R_i$.

Lett å sjekke[3] at $a_i = a_{i-1} \pmod{l^{i-1}}$ og $b_i = b_{i-1} \pmod{l^{i-1}}$, så $((a_i), (b_i))$ definerer et element i $\mathbb{Z}_l \oplus \mathbb{Z}_l$ slik at $\phi((a_i), (b_i)) = (R_i)$. Siden a_i, b_i alltid finnes og er unike, har vi vist at ϕ er en isomorfi. □

MERKNAD 5.44. Det finnes ingen kanonisk isomorfi $\mathbb{Z}_l \oplus \mathbb{Z}_l \cong T_l(E)$, vi har bare definert den ved å gjøre uendelig mange valg.

MERKNAD 5.45. Hvis E er definert over K, så har $\mathbb{Z}_l$-modulen $T_l(E)$ mer struktur: Enhver kroppautomorfi $\sigma \in \mathrm{Gal}(\overline{K}/K)$ virker på $E[l^i]$ på en slik måte at σ også virker på $T_l(E)$. Dette gir en gruppehomomorfi $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_l(E))$ som forteller mye om E.

Vil bruke $T_l(E)$ til å forstå isogenigruppa $\mathrm{Hom}(E_1, E_2)$ og endomorfiringen $\mathrm{End}(E)$.

La $\phi\colon E_1 \to E_2$ være en isogeni. Da får vi, for alle n, en gruppehomomorfi $\phi[n]\colon E_1[n] \to E_2[n]$, og spesielt får vi homomorfier $\phi[l^i]\colon E_1[l^i] \to E_2[l^i]$ for alle i.

La $p = (P_i)_{i=1}^{\infty} \in T_l(E_1)$, og la $Q_i = \phi(P_i) \in E_2$ for alle i. Siden $P_i \in E_1[l^i]$, er $\phi(P_i) \in E_2[l^i]$, og siden $lP_i = P_{i-1}$, har vi

$$lQ_i = l\phi(P_i) = \phi(lP_i) = \phi(P_{i-1}) = Q_{i-1}$$

Dermed er $q = (Q_i)_{i=1}^{\infty}$ et veldefinert element i $T_l(E_2)$.

PROPOSISJON 5.46. *Gitt en isogeni $\phi\colon E_1 \to E_2$, får vi en homomorfi av $\mathbb{Z}_l$-moduler*

$$\phi_l\colon T_l(E_1) \to T_l(E_2)$$

ved

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

BEVIS. Vi har vist at dette er veldefinert, og det er lett å sjekke at dette er en homomorfi av $\mathbb{Z}_l$-moduler.[4] □

[2] UTAG?

[3] $(a_i - a_{i-1})P_{i-1} + (b_i - b_{i-1})Q_{i-1} = a_i lP_i + b_i lQ_i - a_{i-1}P_{i-1} - b_{i-1}Q_{i-1} = lR_i - R_{i-1} = 0$, som betyr at $a_i - a_{i-1} = b_i - b_{i-1} = 0 \pmod{l^{i-1}}$.

[4] Gitt (P_i) og (P_i') i $T_l(E_1)$, sendes $(P_i) + (P_i') = (P_i + P_i')$ til $(\phi(P_i + P_i')) = (\phi(P_i) + \phi(P_i')) = (\phi(P_i)) + (\phi(P_i'))$, så avbildningen er additiv.

PROPOSISJON 5.47. *La $\phi\colon E_1 \to E_2$ og $\psi\colon E_2 \to E_3$ være isogenier. Da er*

$$(\psi \circ \phi)_l = \psi_l \circ \phi_l \colon T_l(E_1) \to T_l(E_3).$$

BEVIS. Rett fram fra definisjonen av ϕ_l, ψ_l.[5] □

5.1. Endomorfiringen til Tate-modulen. La nå E være en elliptisk kurve, og se på $\mathrm{End}_{\mathbb{Z}_l}(T_l(E)) = \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E), T_l(E))$, gruppa av $\mathbb{Z}_l$-homomorfier fra $T_l(E)$ til $T_l(E)$. Vi kan definere et produkt på $\mathrm{End}(T_l(E))$ ved å sette $fg = f \circ g$, og med dette produktet blir $\mathrm{End}(T_l(E))$ en ring.

Siden $T_l(E) \cong \mathbb{Z}_l^{\oplus 2}$ som $\mathbb{Z}_l$-modul, så har vi en ringisomorfi

$$\mathrm{End}(T_l(E)) = \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E), T_l(E)) \cong \mathrm{Hom}_{\mathbb{Z}_l}(\mathbb{Z}_l^{\oplus 2}, \mathbb{Z}_l^{\oplus 2}) = M_2(\mathbb{Z}_l),$$

hvor $M_2(\mathbb{Z}_l)$ angir ringen av (2×2)-matriser med koeffisienter i $\mathbb{Z}_l$.

Vi har vist tidligere at $\mathrm{End}(E)$ er en ring, med multiplikasjon $\phi\psi = \phi \circ \psi$.

PROPOSISJON 5.48. *Avbildningen $\mathrm{End}(E) \to \mathrm{End}(T_l(E))$ gitt ved $\phi \mapsto \phi_l$ er en ringhomomorfi.*

BEVIS. Vi vet at avbildningen er en gruppehomomorfi, så vi må vite at den respekterer multiplikasjon. Men vi har

$$(\phi\psi)_l = (\phi \circ \psi)_l = \phi_l \circ \psi_l = \phi_l \psi_l.$$

□

6. Injektivitet

Vi har altså en gruppehomomorfi $\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2))$, og når $E_1 = E_2$, er dette også en ringhomomorfi.

PROPOSISJON 5.49. *La E_1, E_2 være elliptiske kurver. Avbildningen*

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2))$$

er injektiv.

BEVIS. La $\phi \in \mathrm{Hom}(E_1, E_2)$ være slik at $\phi_l = 0$. La $0 \neq p = (P_i) \in T_l(E_1)$. Da finnes en i slik at $P_i \neq O$.

Vi påstår at punktene $P_i, P_{i+1}, P_{i+2}, \ldots$ alle er forskjellige. Anta for en motsigelse at $P_i = P_j$ med $i < j$. Da er $P_j = P_i = l^{i-j} P_j$. Dermed er $P_j = l^{i-j} l^{i-j} \cdots l^{i-j} P_j = l^{n(i-j)} P_j$ for alle $n \geq 0$. Men siden $l^j P_j = O$, betyr det at $P_j = O$, som motsier at $P_j = P_i \neq O$.

Hvis $\phi_l = 0$, så er $\phi_l(p) = (\phi(P_i))_{i=1}^{\infty} = 0$, som betyr at $\phi(P_i) = O$ for alle i. Men da er $|\ker \phi| = \infty$, som bare kan skje hvis $\phi = 0$. □

Altså sitter $\mathrm{Hom}(E_1, E_2)$ inni $\mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2)) \cong \mathrm{Hom}_{\mathbb{Z}_l}(\mathbb{Z}_l^{\oplus 2}, \mathbb{Z}_l^{\oplus 2}) = \mathbb{Z}_l^{\oplus 4}$. Dessverre er gruppa $\mathbb{Z}_l^{\oplus 4}$ en veldig stor gruppe, som f.eks. inneholder frie grupper på formen $\mathbb{Z}^N$ for alle N, så det er vanskelig å få konkret informasjon om $\mathrm{Hom}(E_1, E_2)$ ut av dette.

Vi trenger følgende sterkere resultat:

Hvis $a = (a_i) \in \mathbb{Z}_l$, så er $\phi(a(P_i)) = \phi((a_i P_i)) = (a_i \phi(P_i)) = a(\phi(P_i))$, så avbildningen respekterer $\mathbb{Z}_l$-modulstrukturen.

[5] For $(P_i) \in T_l(E_1)$, er $\psi_l \circ \phi_l((P_i)) = \psi_l((\phi(P_i)) = (\psi(\phi(P_i))) = ((\psi \circ \phi)(P_i)) = (\psi \circ \phi)_l((P_i))$.

TEOREM 5.50. *Gruppa* $\mathrm{Hom}(E_1, E_2)$ *er endeliggenerert, og homomorfien*

$$\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2))$$

gitt ved

$$\sum_{i=1}^{k} \phi_i \otimes a_i \mapsto \sum_{i=1}^{k} a_i(\phi_i)_l$$

er injektiv.

KOROLLAR 5.51. *Vi har en gruppeisomorfi* $\mathrm{Hom}(E_1, E_2) \cong \mathbb{Z}^n$*, med* $n \leq 4$*.*

BEVIS. Siden $\mathrm{Hom}(E_1, E_2)$ er endeliggenerert, har vi

$$\mathrm{Hom}(E_1, E_2) = \mathbb{Z}^n \oplus \bigoplus_{i=1}^{k} \mathbb{Z}/p_i^{e_i}$$

for primtall p_i og heltall e_i. Men vi vet at $\mathrm{Hom}(E_1, E_2)$ er torsjonsfri, dvs. at $k\phi = 0 \Rightarrow \phi = 0$ for $0 \neq k \in \mathbb{Z}$. Dermed må vi ha $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}^n$.

Det følger at $\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \cong \mathbb{Z}_l^n$, og siden avbildningen

$$\mathbb{Z}_l^n \cong \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2)) = \mathbb{Z}_l^4$$

er injektiv, må $n \leq 4$. □

BEVIS FOR TEOREM 5.50. Vi må bruke følgende tidligere resultat:

LEMMA 5.52. *Hvis* $\phi \in \mathrm{Hom}(E_1, E_2)$ *er slik at* $E_1[n] \subset \ker \phi$*, så finnes en* $\gamma \in \mathrm{Hom}(E_1, E_2)$ *slik at* $n\gamma = \phi$*.*

$$\begin{array}{ccc} E_1 & \xrightarrow{[n]} & E_1 \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists \gamma} \\ & & E_2 \end{array}$$

Vi *antar*, og hopper over å bevise, at $\mathrm{Hom}(E_1, E_2)$ er endeliggenerert (se Silverman for fullstendig bevis). Da må vi ha $\mathrm{Hom}(E_1, E_2) \cong \mathbb{Z}^n$, siden $\mathrm{Hom}(E_1, E_2)$ er torsjonsfri.

La $\psi_1, \ldots, \psi_n$ være generatorer for $\mathrm{Hom}(E_1, E_2)$. Et element $\phi \in \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ kan da uttrykkes som

$$\phi = \sum_{i=1}^{n} \alpha_i \psi_i \qquad \alpha_i \in \mathbb{Z}_l,$$

og vi skriver $\alpha_i = \sum_{j=1}^{\infty} c_{ij} l^j$ med $c_{ij} \in \{0, \ldots, l-1\}$.

For alle $k \geq 1$, definer isogenien

$$\phi_k = \sum_{j=0}^{k-1} c_{ij} l^j \psi_i \in \mathrm{Hom}(E_1, E_2), \tag{4}$$

som vi kan tenke på som "forkortingen av ϕ modulo l^k". Gitt et element $p = (P_i)_{i=1}^{\infty} \in T_l(E_1)$, så er $\phi_l(p) = (\phi_i(P_i))_{i=1}^{\infty}$.

Anta nå at ϕ er slik at $\phi_l = 0$.

Fikser en $k \geq 0$, og la $P \in E[l^k]$. Det finnes en $p = (P_i) \in T_l(E)$ slik at $P_k = P$. Siden $\phi_l(p) = (\phi_i(P_i)) = 0$, så er $\phi_k(P) = \phi_k(P_k) = O$.

Siden dette gjelder for alle $P \in E[l^k]$, så er $E[l^k] \in \ker \phi_k$. Men ved lemmaet er da $\phi_k = l^k \gamma_k$ for en $\gamma_k \in \mathrm{Hom}(E_1, E_2)$. Dette kan bare skje hvis $\phi_k = 0$ (fra formen til ϕ_k (4)). Siden dette gjelder for alle k, må vi ha $\phi = 0$. □

7. Kandidatringer

Vi har nå vist at $\mathrm{Hom}(E_1, E_2)$, og spesielt $\mathrm{End}(E)$, er på formen $\mathbb{Z}^n$ for $n \geq 4$.

I dag: Hva er den multiplikative strukturen til ringen $\mathrm{End}(E)$?

Vi vet en hel del om ringen $\mathrm{End}(E)$.

- $\mathrm{End}(E) \cong \mathbb{Z}^n$, $n \leq 4$ som gruppe
- For $0 \neq \phi, \psi \in \mathrm{End}(E)$, har vi $\phi\psi \neq 0$
- Vi har operasjonen $\phi \mapsto \hat{\phi}$, som tilfredsstiller:
  - Linearitet: $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$
  - Anti-multiplikativitet: $\widehat{\phi\psi} = \hat{\psi}\hat{\phi}$
  - Den er en *involusjon*: $\hat{\hat{\phi}} = \phi$
  - For alle ϕ er $\phi\hat{\phi} = \hat{\phi}\phi = n$, hvor $n = \deg \phi \geq 0$ er et heltall.

Hva kan $\mathrm{End}(E)$ nå potensielt være?

Trivielt eksempel: $\mathrm{End}(E) = \mathbb{Z}$, $\phi \mapsto \hat{\phi}$ er identiteten.

7.1. Ordener. La $\mathcal{K}$ være en endelig-dimensjonal (muligens ikkekommutativ) $\mathbb{Q}$-algebra. En *orden* $\mathcal{R}$ i $\mathcal{K}$ er en underring som er endelig generert som gruppe, og slik at $\mathcal{R} \otimes \mathbb{Q} = \mathcal{K}$.

Eksempel: $\mathbb{Z}$ er en orden i $\mathbb{Q}$.

Kvadratiske kropper: En *kvadratisk kropp* er en utvidelse av $\mathbb{Q}$ på formen $\mathbb{Q}(\sqrt{d})$, hvor d er et heltall. For alle heltall $k > 0$ er ringen

$$\mathcal{R} = \{x + yk\sqrt{d} \mid x, y \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{d})$$

en orden i $\mathbb{Q}(\sqrt{d})$.

Definer involusjonen $X \mapsto \hat{X}$, $X \in \mathcal{R}$, ved $x + y\sqrt{d} \mapsto x - y\sqrt{d}$. Da er $X\hat{X} = x^2 - dy^2$, så hvis $d < 0$, tilfredsstiller $\mathcal{R}$ alt vi vet om $\mathrm{End}(E)$, og er en kandidat.

Kvaternioniske algebraer: En *kvaternionisk algebra* (over $\mathbb{Q}$) er en algebra $\mathcal{K}$ med basis $1, \alpha, \beta, \gamma$ som tilfredsstiller $\alpha^2, \beta^2 \in \mathbb{Q}$, og videre

$$\alpha^2 < 0, \quad \beta^2 < 0, \quad \beta\alpha = -\alpha\beta,$$

dette er nok til å bestemme strukturen til algebraen. Vi setter $\alpha^2 = a$ og $\beta^2 = b$, og skriver $\mathcal{K}(a, b)$ for denne algebraen.

For alle $a, b < 0$ har vi at $\mathcal{K}(a, b) \otimes_{\mathbb{Q}} \mathbb{R}$ er isomorf med den "vanlige" kvaternionringen, altså ringen

$$K = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$$
$$\text{med relasjoner } i^2 = j^2 = k^2 = ijk = -1$$

Hvis $a = b = -1$ setter vi $\alpha = i, \beta = j, \gamma = k$. Generelt kan vi reskalere α, β for å få en isomorfi.

Hvis $a, b \in \mathbb{Z}$, så får vi ordenen

$$\mathcal{R}(a,b) = \{x + y\alpha + z\beta + w\alpha\beta \mid x, y, z, w \in \mathbb{Z}\} \subset \mathcal{K}(a,b).$$

Definerer, for alle $X = x + y\alpha + z\beta + w\alpha\beta \in \mathcal{K}(a,b)$, at $\hat{X} = x - y\alpha - z\beta - w\alpha\beta$. Hvis $X \in \mathcal{R}(a,b)$, så blir da

$$X\hat{X} = -\hat{X}X = x^2 - ay^2 - bz^2 + abw^2 \in \mathbb{Z}_{\geq 0}.$$

så $\mathcal{R}(a,b)$ er en kandidat for $\mathrm{End}(E)$.

Teorem 5.53. *Ringen* $\mathrm{End}(E)$ *er en av følgende tre typer ringer:*

(1) $\mathbb{Z}$

(2) En orden i $\mathbb{Q}(\sqrt{d})$ *hvor* $d < 0$

(3) En orden i en kvaternioniske algebra $\mathcal{K}(a,b)$

Merknad 5.54. Som gruppe har vi altså $\mathrm{End}(E) = \mathbb{Z}, \mathbb{Z}^2$ eller $\mathbb{Z}^4$.

Merknad 5.55. Hvis $\mathrm{End}(E)$ er kommutativ (som vi skal se gjelder dette alltid når $\mathrm{char}\, K = 0$), så er $\mathrm{End}(E)$ enten (1) eller (2), og vice versa, hvis $\mathrm{End}(E)$ er ikkekommutativ så er $\mathrm{End}(E)$ tilfelle (3).

Bevis. La $\mathcal{K} = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Per definisjon er $\mathrm{End}(E)$ en orden i $\mathcal{K}$, så det holder å finne ut hva slags ring $\mathcal{K}$ er. Vi vet at $1 \leq \dim_{\mathbb{Q}} \mathcal{K} \leq 4$, og vi utvider involusjonen $\phi \mapsto \hat{\phi}$ på $\mathrm{End}(E)$ lineært til en involusjon $X \mapsto \hat{X}$ på $\mathcal{K}$.

Hvis $\mathcal{K} = \mathbb{Q}$, så må $\mathbb{Z} \subset \mathrm{End}(E) \subset \mathbb{Q}$. Hvis $\mathbb{Z} \neq \mathrm{End}(E)$, så finnes en $\frac{a}{b} \in \mathrm{End}(E) \setminus \mathbb{Z}$, men da inneholder $\mathrm{End}(E)$ også $\frac{a^n}{b^n}$ for alle n, som er umulig siden $\mathrm{End}(E)$ er endeliggenerert som gruppe.[6]

Så anta at $\mathbb{Q} \subsetneq \mathcal{K}$. For $X \in \mathcal{K}$, definer *normen* $N(X) = X\hat{X}$, hvor $N(X) \in \mathbb{Q}_{\geq 0}$ med $N(X) = 0$ hvis og bare hvis $X = 0$. Definer *trasen* $T(X) = X + \hat{X}$.

Hvis $x \in \mathbb{Q} \subset \mathcal{K}$, har vi $\hat{x} = x$, så

$$N(x) = x^2 \quad T(x) = 2x.$$

Følgende triks viser at vi alltid har $T(X) \in \mathbb{Q}$:

$$N(X+1) = (X+1)\widehat{(X+1)} = X\hat{X} + X + \hat{X} + 1 = N(X) + T(X) + 1,$$

så

$$T(X) = N(X+1) - N(X) - 1 \in \mathbb{Q}$$

La $\alpha \in \mathcal{K} \setminus \mathbb{Q}$. Bytter vi α med $\alpha - \frac{1}{2}T(\alpha)$, så får vi at

$$T(\alpha) = T(\alpha) - T\left(\frac{1}{2}T(\alpha)\right) = 0.$$

Dermed har vi $\hat{\alpha} = -\alpha$, og slik at

$$\alpha^2 = -\alpha\hat{\alpha} = -N(\alpha) \in \mathbb{Q}_{<0}$$

Så $\alpha^2 = a \in \mathbb{Q}$, med $a < 0$. Hvis $\dim_{\mathbb{Q}} \mathcal{K} = 2$ er vi nå ferdige, og har vist at $\mathcal{K} = \mathbb{Q}(\sqrt{a})$.

[6]Dette avsnittet viser egentlig at $\mathbb{Z}$ er den eneste ordenen i $\mathbb{Q}$.

Hvis $\dim_{\mathbb{Q}} \mathcal{K} > 2$, så finnes en $\beta \in \mathcal{K} \setminus \mathbb{Q}(\alpha)$. Bytter vi nå ut β med $\beta - \frac{1}{2}T(\beta) - \frac{T(\alpha\beta)}{2\alpha^2}\alpha$, så får vi etter litt regning at

$$T(\beta) = T(\alpha\beta) = 0.$$

På samme måte som med α har vi at

$$T(\beta) = 0 \Rightarrow \beta = -\hat{\beta} \Rightarrow \beta^2 = -\beta\hat{\beta} = -N(\beta) \in \mathbb{Q}_{<0}$$

Nå har vi vist at $\alpha^2, \beta^2 \in \mathbb{Q}_{<0}$, og

$$\beta\alpha = (-\beta)(-\alpha) = \hat{\beta}\hat{\alpha} = \widehat{\alpha\beta} = -\alpha\beta,$$

hvor siste ligning bruker $T(\alpha\beta) = 0$. Altså har vi vist at ligningene for en kvaternionisk algebra er tilfredssstilt.

Hvis vi kan vise at $\alpha\beta$ er lineært uavhengig av $1, \alpha, \beta$, så utgjør $1, \alpha, \beta, \alpha\beta$ en basis for $\mathcal{K}$, siden $\dim_{\mathbb{Q}} \mathcal{K} \leq 4$, og dermed er da $\mathcal{K}$ en kvaternionisk algebra.

For å se dette, la x, y, z, w være slik at

$$X = x + y\alpha + z\beta + w\alpha\beta = 0.$$

Da er $T(X) = 2x = 0$, så $x = 0$. Videre er $\alpha X\beta = (y\alpha^2)\beta + (z\beta^2)\alpha + w\alpha^2\beta^2 = 0$. Vi vet at $1, \alpha, \beta \in \mathcal{K}$ er lineært uavhengige siden $\beta \notin \mathbb{Q}(\alpha$. Dermed er

$$y\alpha^2 = z\beta^2 = w\alpha^2\beta^2 = 0,$$

og altså er $y = z = w = 0$. □

8. Automorfier

La $\phi\colon E \to E$ være en *automorfi* av elliptiske kurver (så vi krever at $\phi(O) = O$). Da er spesielt ϕ et inverterbart element i $\mathrm{End}(E)$. Men vi har faktisk mye bedre kontroll over automorfier enn over hele $\mathrm{End}(E)$.

Husk at vi tidligere har vist at for to kurver på Weierstrass-form

$$E_1\colon y^2 = x^3 + A_1x + B_1 \qquad E_2\colon y^2 = x^3 + A_2x + B_2,$$

så kan enhver isomorfi skrives som $\phi_u\colon E_1 \to E_2$, for en $u \in \overline{K}^*$, hvor

$$\phi_u(x, y) = (u^2x, u^3y).$$

Morfien ϕ_u er bare veldefinert hvis den faktisk sender punkter i E_1 til E_2, som er det samme som å si at $(x, y) \mapsto (u^2x, u^3y)$ transformerer ligning 2 til ligning 1:

$$\begin{aligned}(u^3y)^2 &= (u^2x)^3 + A_2(u^2x) + B_2\\ u^6y^2 &= u^6x^3 + u^2A_2x + B_2\\ y^2 &= x^3 + u^{-4}A_2x + u^{-6}B_2,\end{aligned}$$

altså hvis $A_1 = u^{-4}A_2$ og $B_1 = u^{-6}B_2$.

La nå E være gitt ved $y^2 = x^3+Ax+B$. Hvis $u \in \overline{K}^*$ er slik at $u^4A = A$ og $u^6B = B$, så er $\phi_u\colon E \to E$ som over en isomorfi, og det er lett å se at $\phi_{u_1u_2} = \phi_{u_1}\phi_{u_2}$.

Dermed har vi en gruppeisomorfi

$$\mathrm{Aut}(E) = \{u \in \overline{K}^* \mid A = u^4A, B = u^6B\}.$$

Tre tilfeller:

Hvis $A, B \neq 0$, så er $u^4 = u^6 = 1$, altså er $u^2 = 1$, så $\mathrm{Aut}(E) \cong \mathbb{Z}/2$.

Hvis $A = 0$, $B \neq 0$, får vi at $u^6 = 1$, så $\mathrm{Aut}(E) \cong \mathbb{Z}/6$ (dette tilsvarer $j(E) = 0$).

Hvis $A \neq 0$, $B = 0$, får vi at $u^4 \cong 1$, så $\mathrm{Aut}(E) \cong \mathbb{Z}/4$ (dette tilsvarer $j(E) = 1728$).

KAPITTEL 6

Endelige kropper og telling av punkter

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 $A, B \in K$?

1. Endelige kropper

Vi repeterer litt om endelige kropper.

La p være et primtall, la $\mathbb{F}_p = \mathbb{Z}/(p)$, og la $\overline{\mathbb{F}}_p$ være en algebraisk tillukning. La **Frobenius-homomorfien** $\operatorname{Fr}_p \colon \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ være avbildningen definert ved

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

LEMMA 6.1. *Avbildningen* Fr_p *er en kroppautomorfi.*

BEVIS. Vi har

$$\operatorname{Fr}_p(x+y) = (x+y)^p = x^p + \left(\sum_{i=1}^{p-1} \binom{p}{i} x^p y^{p-i} \right) + y^p = x^p + y^p = \operatorname{Fr}_p(x) + \operatorname{Fr}_p(y),$$

siden $\binom{p}{i} = 0 \pmod{p}$ for $1 \leq i \leq p-1$. Siden $\operatorname{Fr}_p(xy) = \operatorname{Fr}_p(x) \operatorname{Fr}_p(y)$, $\operatorname{Fr}_p(0) = 0$ og $\operatorname{Fr}_p(1) = 1$, er da Fr_p en kropphomomorfi.

Siden $\overline{\mathbb{F}}_p$ er algebraisk lukket, så finnes det for enhver $x \in \overline{\mathbb{F}}_p$ en $y \in \overline{\mathbb{F}}_p$ slik at $y^p = x$. Dermed er Fr_p surjektiv, og altså en automorfi. □

La nå $q = p^n$ for et heltall $n \geq 1$, og la $\operatorname{Fr}_q \colon \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ være gitt ved $\operatorname{Fr}_q(x) = x^q$.

PROPOSISJON 6.2. *Mengden*

$$\overline{\mathbb{F}}_p^{\operatorname{Fr}_q} := \{x \in \overline{\mathbb{F}}_p \mid \operatorname{Fr}_q(x) = x\}$$

er en underkropp av $\overline{\mathbb{F}}_p$ *med* q *elementer.*

Hvis K *er en endelig kropp med* $\operatorname{char} K = p$*, så er* K *isomorf til* $\overline{\mathbb{F}}_p^{\operatorname{Fr}_q}$ *for en verdi av* q*.*

BEVIS. Siden $\mathrm{Fr}_q = \mathrm{Fr}_p \circ \cdots \circ \mathrm{Fr}_p$, hvor vi tar komposisjonen n ganger, så er Fr_q en kroppautomorfi. Det følger da formelt at $\overline{\mathbb{F}}_p^{\mathrm{Fr}_q}$ er lukket under addisjon, multiplikasjon og divisjon, så $\overline{\mathbb{F}}_p^{\mathrm{Fr}_q}$ er en underkropp av $\overline{\mathbb{F}}_p$.

Et element $\alpha \in \overline{\mathbb{F}}_p$ ligger i $\overline{\mathbb{F}}_p^{\mathrm{Fr}_q}$ hvis og bare hvis α er rot i $f = x - x^q \in \overline{\mathbb{F}}_p[x]$. Siden den deriverte $f' = 1 - qx^{q-1} = 1$, har f ingen doble røtter, så det finnes nøyaktig q røtter av f. Dermed er $|\overline{\mathbb{F}}_p^{\mathrm{Fr}_q}| = q$.

Hvis K er en endelig kropp av karakteristikk p, så må $|K| = q$ for en eller annen $q = p^n$.[1] Siden den multiplikative gruppa K^* har kardinalitet $q-1$, så må vi ha $x^{q-1} = 1$ for alle $x \in K^*$. Det følger at $x^q = x$ for alle $x \in K$.

Siden K er en algebraisk utvidelse av $\mathbb{F}_p$, så finnes det en inklusjon $K \hookrightarrow \overline{\mathbb{F}}_p$, og siden $x^q = x$ for alle $x \in K$, må K avbildes inn i $\overline{\mathbb{F}}_p^{\mathrm{Fr}_q}$. Men $|K| = |\overline{\mathbb{F}}_p^{\mathrm{Fr}_q}| = q$, så K avbildes isomorft på $\overline{\mathbb{F}}_p^{\mathrm{Fr}_q}$. □

Vi skriver $\mathbb{F}_q$ for kroppen $\overline{\mathbb{F}}_p^{\mathrm{Fr}_q} \subset \overline{\mathbb{F}}_p$.

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 6.3. *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 6.4. 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 6.5. *Et punkt* $P \in \mathbb{P}^n$ *er definert over* $\mathbb{F}_q$ *hvis og bare hvis* $\mathrm{Fr}_q(P) = P$.

[1] Legg til begrunnelse?

BEVIS. La $P = [X_0 : \ldots : X_n]$, og anta uten tap av generalitet 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 $\mathbb{F}_q$. □

2.1. 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 6.6. *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

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

□

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.

3. 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 $\mathrm{char}\, E = p$ og vi har

$$f = c_0 + c_p x^p + c_{2p} x^{2p} + \cdots + c_{ip} x^{ip}. \tag{5}$$

DEFINISJON 6.7. En endelig kropputvidelse $E \hookrightarrow F$ er *separabel* hvis alle $\alpha \in F$ er separable over E.

EKSEMPEL 6.8. Hvis $\mathrm{char}\, E = 0$, så er alle endelige utvidelser separable.

EKSEMPEL 6.9. 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 (5).

DEFINISJON 6.10. La $\phi\colon C \to D$ være en ikkekonstant morfi av ikkesingulære kurver. Vi sier at ϕ er **separabel** hvis kropputvidelsen $\phi^*\colon \overline{K}(D) \to \overline{K}(C)$ er separabel.

EKSEMPEL 6.11. Hvis $\operatorname{char} K = 0$ eller $\operatorname{char} K = p$, $\deg \phi \neq 0 \pmod p$, så er ϕ separabel.

PROPOSISJON 6.12 ([**Sil09**, Prop. II.2.11]). *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 irredusibelt polynom $x^q - t^q$ av grad q, og som opplagt ikke er separabelt. □

3.1. Geometrisk tolkning av separabilitet. Følgende gir litt geometrisk forståelse for hva separabilitet betyr. Se Avsnitt 3.4 for notasjonen $e_\phi(P)$.

PROPOSISJON 6.13. *La $\phi\colon C \to D$ være en ikkekonstant morfi av kurver. 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 6.14. *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 6.15. La C være definert over $\mathbb{F}_q$. Da er $\deg(\mathrm{Fr}_q) = q$, ved Prop. 6.12.

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.

For alle $P \in C$ har vi da at $\mathrm{Fr}_q^{-1}(\mathrm{Fr}_q(P)) = \{P\}$, så

$$q = \deg(\mathrm{Fr}_q) = \sum_{Q \in \mathrm{Fr}_q^{-1}(\mathrm{Fr}_q(P))} e_\phi(Q) = e_\phi(P).$$

EKSEMPEL 6.16. For en eksplisitt beregning av resultatet i forrige 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 6.17. *Hvis $\phi \in \mathrm{Hom}(E_1, E_2)$ er en separabel isogeni, så er $|\ker \phi| = \deg(\phi)$.*

Dette viste vi i Teorem 5.19 under antakelsen at $\mathrm{char}\, K = 0$, men 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.

3.2. 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

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

PROPOSISJON 6.18. *Avbildningen $\phi^* \colon \Omega_D \to \Omega_C$ er*

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

EKSEMPEL 6.19. La $K = \mathbb{F}_q$, og se på $\mathbb{P}^1$, med $\overline{K}(\mathbb{P}^1) = \overline{K}(x)$. Vi vil anvende nproposisjonen 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.

3.3. 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 6.20. *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. □

PROPOSISJON 6.21 (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 6.22. *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 $m \neq 0 \pmod p$.*

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. □

KOROLLAR 6.23. *Isogenien $1 - \mathrm{Fr}_q \in \mathrm{End}(E)$ er separabel.*

4. Hasses teorem

4.1. Telle punkter, et grovt anslag. La nå $K = \mathbb{F}_q$, og la E være en elliptisk kurve definert over $\mathbb{F}_q$, med Weierstrass-ligning

$$y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{F}_q.$$

Vi viser to måter å estimere $|E(\mathbb{F}_q)|$ på.

*Måte 1:*La $g = x^3 + Ax + B$, vi har da

$$E(\mathbb{F}_q) = \{O\} \sqcup \{(\alpha, \beta) \in \mathbb{F}_q^2 \mid \beta^2 = g(\alpha)\}.$$

Se på avbildningen $\beta \mapsto \beta^2$, som sender 0 til 0, og som er 2-til-1 på $\mathbb{F}_q \setminus \{0\}$. Vi har

$$\mathbb{F}_q = \{0\} \sqcup R \sqcup S,$$

hvor

$$R = \{\gamma \in \mathbb{F}_q \mid x^2 = \gamma \text{ har 2 røtter}\}, \quad |R| = \frac{q-1}{2}$$
$$S = \{\gamma \in \mathbb{F}_q \mid x^2 = \gamma \text{ har 0 røtter}\}, \quad |S| = \frac{q-1}{2}$$

Vi har altså

$$|E(\mathbb{F}_q)| = 1+|\{\alpha \in \mathbb{F}_q \mid g(\alpha) = 0\}|+2|\{\alpha \in \mathbb{F}_q \mid g(\alpha) \in R\}|+0|\{\alpha \in \mathbb{F}_q \mid g(\alpha) \in S\}|.$$

Hvis vi nå antar at verdiene $g(\alpha)$ tar er *tilfeldig* (uniformt) fordelt, får vi estimatet

$$|E(\mathbb{F}_q)| \approx 1 + 1 + 2\left(\frac{q-1}{2}\right) + 0\left(\frac{q-1}{2}\right) = q + 1.$$

Måte 2: Se på funksjonen $h\colon \mathbb{F}_q^2 \to \mathbb{F}_q$ gitt ved $h(\alpha, \beta) \mapsto \beta^2 - (\alpha^3 + A\alpha + B)$, og anta at h kan approksimeres som en tilfeldig (uniformt fordelt) funksjon av α, β. Sannsynligheten for at $h(\alpha, \beta) = 0$ da er q^{-1} og $|\mathbb{F}_q^2| = q^2$, så vi får $|\{(\alpha, \beta \in \mathbb{F}_q^2 \mid h(\alpha, \beta) = 0\}| \approx q$, som gir $|E(\mathbb{F}_q)| \approx q + 1$.

Hasses teorem sier at dette estimatet ikke er altfor gæli:

Teorem 6.24 (Hasses teorem). *Vi har*

$$|E(\mathbb{F}_q) - (1 + q)| \leq 2\sqrt{q}$$

Første steg i beviset har vi gjort, vi vet at $|E(\mathbb{F}_q)| = \deg(1 - \mathrm{Fr}_q)$. Det gjenstår å få has på $\deg(1 - \mathrm{Fr}_q)$.

Hvordan ser funksjonen $\deg\colon \mathrm{End}(E) \to \mathbb{Z}$ ut? Vi vet

- $\deg(\mathrm{Fr}_q) = q$,
- $\deg([n]) = n^2$ for alle $n \in \mathbb{Z}$.
- Vi vet at $\deg(\phi\psi) = \deg(\phi)\deg(\psi)$ for alle $\phi, \psi \in \mathrm{End}(E)$, slik at for eksempel
$$\deg(n\phi) = \deg([n]\phi) = n^2 \deg(\phi).$$
.

Denne siste ligningen hinter til at $\deg(\phi)$ er en *kvadratisk* funksjon av ϕ.

Definisjon 6.25. La G være en abelsk gruppe, og la $d\colon G \to \mathbb{R}$ være en funksjon. Definer $b\colon G \times G \to \mathbb{R}$ ved

$$b(\alpha, \beta) = \frac{q(\alpha + \beta) - q(\alpha) - q(\beta)}{2}.$$

Vi sier at d er en *kvadratisk form* hvis

(1) For alle $\alpha \in G$, så er $d(\alpha) = d(-\alpha)$

(2) Funksjonen b er bilineær.

Vi sier d er *positiv definitt* hvis $d(\alpha) \geq 0$ for alle $\alpha \in G$ og $d(\alpha) = 0 \Leftrightarrow \alpha = 0$.

Den kvadratiske formen d bestemmer altså en bilineær avbildning b, og motsatt er d bestemt av b, siden

$$b(\alpha,\alpha) = -b(\alpha,-\alpha) = -\frac{d(0)-d(\alpha)-d(-\alpha)}{2} = d(\alpha).$$

Skriver man ut dette får man en bijeksjon

$$\begin{aligned}\{\text{Kvadratiske former på } G\} &\leftrightarrow \{\text{Symmetriske bilineære avbildninger } G\times G\to\mathbb{R}\}\\ q &\mapsto b(\alpha,\beta) = \frac{q(\alpha+\beta)-q(\alpha)-q(\beta)}{2}\\ q(\alpha) = b(\alpha,\alpha) &\hookleftarrow b\end{aligned}$$

LEMMA 6.26. *Hvis $G=\mathbb{Z}^n$, så er det en bijektiv korrespondanse mellom (positiv definitte) kvadratisk former $d\colon G\to\mathbb{R}$ og (positiv definitte) symmetriske reelle $(n\times n)$-matriser, gitt ved*

$$M=(a_{ij})\in M_n(\mathbb{R}) \leftrightarrow d((b_i)_{i=1}^n) = \sum_{i,j} b_i b_j a_{ij}.$$

BEVIS. Bijeksjonen over er komposisjonen av naturlige bijeksjoner

$$\begin{aligned}\{\text{Kvadratiske former på } \mathbb{Z}^n\} &\leftrightarrow \{\text{Symmetriske bilineære avbildninger } \mathbb{Z}^n\times\mathbb{Z}^n\to\mathbb{R}\}\\ &\leftrightarrow \{\text{Symmetriske avbildninger } \mathbb{Z}^n\otimes\mathbb{Z}^n\to\mathbb{R}\}\\ &\leftrightarrow \{\text{Symmetriske reelle } (n\times n)\text{-matriser}\},\end{aligned}$$

og det er lett å se at M er positiv definitt hvis og bare hvis d er det. □

For $\mathrm{End}(E)=\mathbb{Z}^n$ har vi altså en konkret beskrivelse av kvadratiske former på gruppen. Poenget med den abstrakte definisjonen over er at den er lett å sjekke.[2]

PROPOSISJON 6.27. *Funksjonen* $\deg\colon \mathrm{End}(E)\to\mathbb{Z}$ *er en positiv definitt kvadratisk funksjon.*

BEVIS. Vi må vise at funksjonen

$$b(\phi,\psi) = \deg(\phi+\psi)-\deg(\phi)-\deg(\psi)$$

er bilineær. Vi bruker at for alle $\alpha\in\mathrm{End}(E)$, så er

$$\deg(\alpha) = \alpha\hat{\alpha}.$$

Altså er

$$b(\phi,\psi) = (\phi+\psi)(\hat{\phi}+\hat{\psi}) - \phi\hat{\phi}hi - \psi\hat{\psi} = \phi\hat{\psi}+\psi\hat{\phi}$$

som opplagt er lineært i både ϕ og ψ.

For alle $\phi\in\mathrm{End}(E)$ har vi $\deg(\phi)=\deg(-\phi)$, $\deg(\phi)\geq 0$, og $\deg(\phi)=0\Leftrightarrow\phi=0$, som fullfører beviset. □

Vi har nå den kvadratiske formen $\deg\colon \mathrm{End}(E)\to\mathbb{Z}$, som vi skal evaluere i $1-\mathrm{Fr}_q$. Vi lar $b\colon \mathrm{End}(E)\times\mathrm{End}(E)\to\mathbb{R}$ være den assosierte bilineære formen.

PROPOSISJON 6.28 (Cauchy–Schwarz' ulikhet). *La $\phi,\psi\in\mathrm{End}(E)$. Da er*

$$\deg(\phi)\deg(\psi)\geq(b(\phi,\psi))^2$$

[2]Ett annet poeng er at Silvermans fullstendige bevis for at $\mathrm{End}(E)$ er endeliggenerert bruker den kvadratiske formen deg på $\mathrm{End}(E)$, så man ønsker å bruke begrepet "kvadratisk form" også for grupper som man ikke veit at er endelig genererte.

BEVIS. Siden $\mathrm{End}(E) = \mathbb{Z}^n$, så er $\deg\colon \mathrm{End}(E) \to \mathbb{R}$ definert av en positiv definitt $(n\times n)$-matrise. Vi kan dermed si at b definerer et indreprodukt på $\mathrm{End}(E)\otimes \mathbb{R} = \mathbb{R}^n$, og resultatet over er da den vanlige Cauchy–Schwarz' ulikhet. □

KOROLLAR 6.29. *Hvis $\phi, \psi \in \mathrm{End}(E)$, så er $|\deg(\phi+\psi) - \deg(\phi) - \deg(\psi)| \leq 2\sqrt{\deg(\phi)\deg(\psi)}$.*

BEVIS. Vi har

$$\begin{aligned}\deg(\phi+\psi) &= b(\phi+\psi, \phi+\psi)\\ &= b(\phi,\phi) + b(\psi,\psi) + b(\phi,\psi) + b(\psi,\phi) = \deg(\phi) + \deg(\psi) + 2b(\phi,\psi).\end{aligned}$$

Dermed er

$$|\deg(\phi+\psi) - \deg(\phi) - \deg(\psi)| = 2|b(\phi,\psi)| \leq 2\sqrt{\deg(\phi)\deg(\psi)}.$$

□

BEVIS FOR HASSES TEOREM. Anvend lemmaet over på $\phi = 1$ og $\psi = -\mathrm{Fr}_q$.

Vi får da

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

og siden $\deg(1) = 1$, og $\deg(-\mathrm{Fr}_q) = q$, gir dette

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

og altså

$$|E(\mathbb{F}_q) - 1 - q| \leq 2\sqrt{q}.$$

□

5. Bonus: Weil-formodningene

Denne delen er med for dannelsens skyld, og er ikke pensum.

La E være en elliptisk kurve definert over $\mathbb{F}_q$. Kroppen $\mathbb{F}_q$ er inneholdt i større kropper $\mathbb{F}_{q^n}$ for alle n, så kurven E er også definert over $\mathbb{F}_{q^n}$ for alle n. Det gir dermed mening å spørre om størrelsen til mengden $E(\mathbb{F}_{q^n})$, og hvordan denne avhenger av n.

Ved estimatet vi ga tidligere, har vi at $|E(\mathbb{F}_{q^n})| \approx 1 + q^n$. Setter vi $\epsilon_n = (1+q^n) - |E(\mathbb{F}_{q^n})|$, så sier Hasses teorem at

$$|\epsilon_n| \leq 2\sqrt{q^n}.$$

TEOREM 6.30 ("Weil-formodningene[3] for en elliptisk kurve"). *Gitt en E definert over $\mathbb{F}_q$, så finnes det et komplekst tall α med $|\alpha| = \sqrt{q}$ slik at for alle n har vi*

$$\epsilon_n = \alpha^n + \bar{\alpha}^n = 2Re(\alpha^n).$$

[3]Hvorfor ikke "Weil-formodningen" i entall? Weil-formodningene kan formuleres mer generelt for algebraiske varieteter definert over $\mathbb{F}_q$, og i den generelle formen er det naturlig å presentere dette som flere underformodninger. For en elliptisk kurve er resultatet enklere, så vi dropper å stykke det opp.

Siden

$$2|\mathrm{Re}(\alpha^n)| \leq 2|\alpha^n| = 2\sqrt{q^n},$$

så er Hasses teorem et korollar av dette teoremet.

Fra $\alpha + \alpha^{-1} = \epsilon_1$ og $|\alpha| = \sqrt{q}$, følger det at α må være en av de to konjugerte røttene til polynomet

$$x^2 - \epsilon_1 x + q$$

og α er derfor entydig bestemt av ϵ_1. Dermed er $|E(\mathbb{F}_{q^n})|$ bestemt for alle n straks man kjenner $|E(\mathbb{F}_q)|$.

EKSEMPEL 6.31. Ta kurven definert av ligningen $y^2 = x^3 - x$. Denne er definert over $\mathbb{F}_5$ (den er for så vidt definert over alle K!), så la oss ta $q = 5$. Man sjekker at $|E(\mathbb{F}_5)| = 7$, så $\epsilon_1 = 1 + 5 - |E(\mathbb{F}_5)| = -1$. Dermed er α en rot av

$$x^2 + x + 5,$$

så

$$\alpha = -\frac{1}{2} \pm \frac{\sqrt{19}}{2} i,$$

og vi får

$$E(\mathbb{F}_{5^n}) = 1 + 5^n - 2\mathrm{Re}(\alpha^n)$$

for alle n.

5.1. Beviset for Weil-formodningene. På samme måte som $E(\mathbb{F}_q) = \ker(1 - \mathrm{Fr}_q)$, har vi at

$$|E(\mathbb{F}_{q^n})| = |\ker(1 - \mathrm{Fr}_{q^n})| = \deg(1 - \mathrm{Fr}_{q^n}).$$

Siden $\mathrm{Fr}_{q^n}(\alpha) = \alpha^{q^n}$ for alle $\alpha \in \overline{\mathbb{F}}_q$, har vi at $\mathrm{Fr}_{q_n} = \mathrm{Fr}_q^n$, hvor vi tenker på Fr_q som et element i ringen $\mathrm{End}(E)$. For å bestemme $\deg(1 - \mathrm{Fr}_{q^n})$ analyserer vi mer generelt hvordan man kan beregne $\deg(1 - \phi^n)$ for en vilkårlig $\phi \in \mathrm{End}(E)$.

Vi har tidligere vist et teorem som sier at ringen $\mathrm{End}(E)$ enten er $\mathbb{Z}$, en orden i en kvadratisk kropp, eller en orden i en kvaternionisk algebra. I dette beviset viste vi også at for alle $\phi \in \mathrm{End}(E)$, så er trasen $T(\phi) = \phi + \hat{\phi}$ inneholdt i $\mathbb{Z} \subset \mathrm{End}(E)$.

LEMMA 6.32. *For alle $\phi \in \mathrm{End}(E)$ gjelder*

$$\phi^2 - T(\phi)\phi + \deg(\phi) = 0,$$

BEVIS. Bruk $\deg(\phi) = \phi\hat{\phi} = \hat{\phi}\phi$ og skriv ut. □

For $\phi \in \mathrm{End}(E)$, la $R_\phi \subseteq \mathrm{End}(E)$ være underringen av $\mathrm{End}(E)$ generert av ϕ.

LEMMA 6.33. *Hvis $\phi \notin \mathbb{Z}$, har vi $R_\phi \cong \mathbb{Z}[x]/(x^2 - T(\phi)x + \deg(\phi))$.*

BEVIS. Ringen R_ϕ er bildet av avbildningen $\chi\colon \mathbb{Z}[x] \to \mathrm{End}(E)$ gitt ved $x \mapsto \phi$. Ved lemmaet over, er $x^2 - T(\phi)x + \deg(\phi) \in \ker(\chi)$, så $(x^2 - T(\phi)x + \deg(\phi)) \subseteq \ker(\chi)$.

Homomorfien χ faktoriserer dermed gjennom en surjeksjon $\mathbb{Z}[x]/(x^2 - T(\phi) + \deg(\phi))$, og vi har at $\mathbb{Z}[x]/(x^2 - T(\phi) + \deg(\phi))$ har rang 2 som $\mathbb{Z}$-modul. Siden $\phi \notin \mathbb{Z}$, har R_ϕ rang ≥ 2 som $\mathbb{Z}$-modul, og dermed må surjeksjonen $\mathbb{Z}[x]/(x^2 - T(\phi) + \deg(\phi)) \to R_\phi$ være en isomorfi. □

La $\phi \in \mathrm{End}(E) \setminus \mathbb{Z}$, og la $\alpha \in \mathbb{C}$ være en rot av $x^2 - T(\phi)x + \deg(\phi)$. Vi kan definere en homomorfi $\iota \colon R_\phi \to \mathbb{C}$ ved $\iota(\phi) = \alpha$.

LEMMA 6.34. *For alle $\psi \in R_\phi$, så er $\hat{\psi} \in R_\phi$, og*

$$\iota(\hat{\psi}) = \overline{\iota(\psi)}.$$

BEVIS. Siden R_ϕ er genererert av ϕ, holder det å vise at $\hat{\phi} \in R_\phi$ og at $\iota(\hat{\phi}) = \overline{\iota(\phi)}$.

For den første påstanden: $\hat{\phi} = T(\phi) - \phi$.

For den andre påstanden: Vi har at $\iota(\phi) = \alpha$ er en rot av $x^2 - T(\phi)x + \deg(\phi)$, og $\bar{\alpha}$ er den andre roten av dette polynomet. Dermed er $\bar{\alpha} = T(\phi) - \alpha$, som betyr at

$$\iota(\hat{\phi}) = \iota(T(\phi) - \phi) = T(\phi) - \iota(\phi) = T(\phi) - \alpha = \bar{\alpha} = \overline{\iota(\phi)}.$$

□

PROPOSISJON 6.35. *Med α som over, har vi*

$$\deg(1 - \phi^n) = 1 + \deg(\phi)^n - (\alpha^n + \bar{\alpha}^n).$$

BEVIS. Vi har

$$\deg(1 - \phi^n) = (1 - \phi^n)(1 - \hat{\phi}^n).$$

Siden $(1 - \phi^n)(1 - \hat{\phi}^n) \in \mathbb{Z}$, har vi

$$(1 - \phi^n)(1 - \hat{\phi}^n) = \iota((1 - \phi^n)(1 - \hat{\phi}^n)) = (1 - \alpha^n)(1 - \bar{\alpha}^n) = 1 + (\alpha\bar{\alpha})^n - (\alpha^n + \bar{\alpha}^n),$$

og siden $\deg(\phi) = \phi\hat{\phi} = \alpha\bar{\alpha}$, er vi i mål. □

Bruker vi proposisjonen over på $\phi = \mathrm{Fr}_q$, har vi vist Weil-formodningene for elliptiske kurver.

KAPITTEL 7

Komplekse elliptiske kurver

Vi skal nå se på det spesielle tilfellet hvor $K = \overline{K} = \mathbb{C}$, og se at vi kan beskrive slike komplekse elliptiske kurver på en annen (og på sett og vis enklere) måte.

Gitter i det komplekse planet

DEFINISJON. Et **gitter** i det komplekse planet er en diskret undergruppe $\Lambda \subset \mathbb{C}$ hvor $\Lambda \cong \mathbb{Z}^2$.

TEGNING AV ET GITTER

Et gitter $\Lambda \subset \mathbb{C}$ er typisk definert ved å spesifisere to generatorer ω_1, ω_2 av Λ. Betingelsen at Λ er *diskret* er ekvivalent med at ω_1 og ω_2 ikke ligger på samme linje gjennom 0 i $\mathbb{C}$.

EKSEMPEL 7.1. For et konkret eksempel, la $\Lambda_0 \subset \mathbb{C}$ være undergruppen av $\mathbb{C}$ generert av 1 og i, det vil si

$$\Lambda_0 = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Vi kan se på det topologiske kvotientrommet $\mathbb{C}/\Lambda$. Vi skal forstå, og delvis vise: Punktene til en elliptisk kurve E over $\mathbb{C}$ er i bijeksjon med $\mathbb{C}/\Lambda$ for et eller annet gitter Λ.

TEGNING AV EN TORUS

For å relatere $\mathbb{C}/\Lambda$ til E, trenger vi noen funksjoner på $\mathbb{C}/\Lambda$.

DEFINISJON. En **elliptisk funksjon** (relativ til Λ) på $\mathbb{C}$ er en *meromorf* funksjon $f\colon \mathbb{C} \to \mathbb{C}$ slik at for alle $\omega \in \Lambda$, har vi

$$f(z + \omega) = f(z)$$

Mengden av elliptiske funksjoner danner en kropp, som vi kaller $\mathbb{C}(\Lambda)$.

En elliptisk funksjon f definerer en funksjon på $\mathbb{C}/\Lambda$, som vi også kaller f.

DEFINISJON. Et **fundamentalområde** for Λ er en mengde på formen

$$D = \{a + t_1\omega_1 + t_2\omega_2 \mid 0 \leq t_1, t_2 < 1\}$$

hvor $a \in \mathbb{C}$ og $\{\omega_1, \omega_2\}$ genererer Λ.

Hvis $D \subset \mathbb{C}$ er et fundamentalområde, så inneholder D ett element for hver restklasse til Λ, så den naturlige avbildningen $D \to \mathbb{C}/\Lambda$ er en bijeksjon.

PROPOSISJON. *La f være en elliptisk funksjon. Hvis f er holomorf, så er f konstant.*

BEVIS. Velg et fundamentalområde $D \subset \mathbb{C}$. Siden $\overline{D}$ er kompakt og f er holomorf, så finnes en N slik at $|f(z)| \leq N$ for alle $z \in \overline{D}$. Men for alle $z \in \mathbb{C}$ finnes en $\omega \in \Lambda$ slik at $z + \omega \in \overline{D}$, og dermed er $|f(z)| \leq N$ for alle $z \in \mathbb{C}$. Dermed er f en holomorf, begrenset funksjon på f, og dermed konstant (Liouvilles teorem). □

DEFINISJON. La f være en meromorf funksjon på $\mathbb{C}$, og la $w \in \mathbb{C}$.

Vi lar $\text{ord}_w(f)$ være **forsvinningsordenen** til f i w, og lar $\text{res}_w(f)$ være **residyen** til f i w.

Dvs. i Laurent-utvidelsen til f om w,

$$f(z) = a_n(z-w)^n + a_{n+1}(z-w)^{n+1} + \cdots,$$

har vi $\text{ord}_w(f) = n$ og $\text{res}_w(f) = a_{-1}$.

Hvis f er elliptisk, $w \in \mathbb{C}$ og $\omega \in \Lambda$, så er

$$\text{ord}_{w+\omega}(f) = \text{ord}_w(f), \quad \text{res}_w(f) = \text{res}_{w+\omega}(f).$$

Dermed gir det mening å snakke om $\text{ord}_w(f), \text{res}_w(f)$ for $w \in \mathbb{C}/\Lambda$.

PROPOSISJON. *La f være en elliptisk funksjon.*

(1) $\sum_{w \in \mathbb{C}/\Lambda} \text{res}_w(f) = 0$.

(2) $\sum_{w \in \mathbb{C}/\Lambda} \text{ord}_w(f) = 0$.

BEVIS. 1): For alle fundamentalområder $D \subset \mathbb{C}$ har vi

$$\sum_{w \in \mathbb{C}/\Lambda} \text{res}_w(f) = \sum_{w \in D} \text{res}_w(f).$$

Velg et fundamentalområde D slik at f ikke har noen poler på randa til D.

Cauchys residyteorem sier at

$$\sum_{w \in D} \text{res}_w(f) = \frac{1}{2\pi i} \int_{\partial D} f(z)dz,$$

men siden f er elliptisk, vil bidraget fra motstående sider i parallellogrammet D kansellere, så $\int_{\partial D} f(z)dz = 0$.

2): Vi har at $\text{ord}_w(f) = \text{res}_w(\frac{f'}{f})$. Siden $\frac{f'}{f}$ er elliptisk, følger 2) da fra 1). □

DEFINISJON. **Ordenen** til en elliptisk funksjon f er antall poler til f i et fundamentalområde, talt med multiplisitet.

Siden $\sum_{w \in \mathbb{C}/\Lambda} \text{ord}_w(f) = 0$, har en elliptisk funksjon av orden d også d nullpunkter, talt med multiplisitet.

PROPOSISJON 7.2. *En ikkekonstant elliptisk funksjon f har orden ≥ 2.*

BEVIS. Hvis f har orden 0, er den holomorf, dermed konstant.

Anta for en motsigelse at f har orden 1. Da har den en enkelt pol i et punkt $w_0 \in D$. Det betyr at

$$\sum_{w \in \mathbb{C}/\Lambda} \text{res}_w(f) = \text{res}_{w_0}(f) \neq 0,$$

som er umulig. □

1. Eksempler på elliptiske funksjoner

Vi vil nå lage noen elliptiske funksjoner.

Vi veit at hvis f ikke er konstant, så må den ha orden ≥ 2, så la oss prøve å lage en med orden 2. La oss si at den skal ha en dobbel pol i 0. Vi kan prøve

$$f(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z-\omega)^2}.$$

Denne formelen tilfredsstiller opplagt $f(z) = f(z+\omega)$ for alle $\omega \in \Lambda$. Ett problem: Rekka viser seg å ikke konvergere.

I stedet ser man på:

DEFINISJON. Weierstrass $\wp$-funksjon er funksjonen

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

PROPOSISJON. *(1) Rekka som definerer $\wp$ konvergerer uniformt, så $\wp$ er veldefinert.*

(2) $\wp$ er en jevn elliptisk funksjon.

Vi kan nå lage en ny elliptisk funksjon ved å derivere:

$$\wp'(z) = \sum_{\omega \in \Lambda} -2 \frac{1}{(z-\omega)^3}.$$

Siden $\wp$ er elliptisk, så er $\wp'$ elliptisk. Den er en odde funksjon.

MERKNAD. Alle elliptiske funksjoner kan uttrykkes som en rasjonal funksjon av $\wp$ og $\wp'$ – med andre ord er kroppen $\mathbb{C}(\Lambda)$ generert over $\mathbb{C}$ av $\wp$ og $\wp'$.

Relasjonen mellom $\wp$ og $\wp'$. Siden $\wp(z)$ er jevn og $\wp(z) - \frac{1}{z^2}$ konvergerer mot 0 når z går mot 0, har vi Laurent-rekke-utvidelsen

$$\wp(z) = z^{-2} + a_2 z^2 + a_4 z^4 + \cdots,$$

og dermed at

$$\wp'(z) = -2z^{-3} + 2a_2 z + \cdots$$

PROPOSISJON. *Det finnes tall $g_2, g_3 \in \mathbb{C}$ (avhengig av Λ) slik at for alle $z \in \mathbb{C}/\Lambda \setminus \{0\}$ har vi*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2 \wp(z) - g_3.$$

BEVIS. Gitt en meromorf funksjon f med Laurent-rekke

$$f(z) = \sum_{n \geq \mathrm{ord}_0(f)} a_n z^n,$$

er *prinsipaldelen* $\mathcal{P}(f)$ leddene med negativ z-eksponent, dvs. $\sum_{n=\mathrm{ord}_0(f)}^{0} a_n z^n$.

Ser vi på funksjonene $\wp'(z)^2$, $\wp(z), \wp(z)^3$, kan prinsipaldelene skrives som

$$\mathcal{P}(\wp'(z)^2) = 4z^{-6} - 8a_2 z^{-2}$$
$$\mathcal{P}(\wp(z)) = z^{-2}$$
$$\mathcal{P}(\wp(z)^3) = z^{-6} + 3a_2 z^{-2},$$

Det finnes dermed en g_2 slik at $h(z) = \wp'(z)^2 - 4\wp(z)^3 - g_2\wp(z)$ har prinsipaldel 0. Funksjonen $h(z)$ er elliptisk, og kan bare ha poler i $w \in \Lambda$. Men siden $\mathcal{P}(h(z)) = 0$, har h ikke pol i 0. Dermed er h holomorf, dermed konstant, og vi kan sette $g_3 = h$.[1] □

2. Divisorgruppa til $\mathbb{C}/\Lambda$

På nøyaktig samme måte som for en algebraisk kurve, kan vi definere divisorgruppa til $\mathbb{C}/\Lambda$:

DEFINISJON. Gruppa $\mathrm{Div}(\mathbb{C}/\Lambda)$ er gruppa av formelle lineære summer $\sum n_i(w_i)$, hvor $w_i \in \mathbb{C}/\Lambda$.

Vi kan nå gi parallelle definisjoner av alt det vi tidligere har definert ved divisorer på en algebraisk kurve, ved å la elliptiske funksjoner spille rollen til rasjonale funksjoner:

- **Graden** til en divisor $D = \sum n_i(w_i) \in \mathrm{Div}(\mathbb{C}/\Lambda)$ er $\deg(D) = \sum n_i$.
- $\mathrm{Div}^0(\mathbb{C}/\Lambda) = \{D \in \mathrm{Div}(\mathbb{C}/\Lambda) \mid \deg(D) = 0\}$.
- For en $f \in \mathbb{C}(\Lambda)^*$, er
$$\mathrm{div}(f) = \sum_{w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(f) \in \mathrm{Div}^0(\mathbb{C}/\Lambda).$$
- Avbildningen $\mathrm{div}\colon \mathbb{C}(\Lambda)^* \to \mathrm{Div}^0(\mathbb{C}/\Lambda)$ er en homomorfi, og $\mathrm{div}(f) = 0$ hvis og bare hvis f er konstant.
- Picard-gruppa $\mathrm{Pic}(\mathbb{C}/\Lambda) = \mathrm{Div}(\mathbb{C}/\Lambda)/\mathrm{div}(\mathbb{C}(\Lambda)^*)$, og
$$\mathrm{Pic}^0(\mathbb{C}/\Lambda) = \mathrm{Div}^0(\mathbb{C}/\Lambda)/\mathrm{div}(\mathbb{C}(\Lambda)^*).$$

LEMMA. *Hvis $w_1, w_2 \in \mathbb{C}/\Lambda$, så er $(w_1) \sim (w_2)$ hvis og bare hvis $w_1 = w_2$.*

BEVIS. La $f \in \mathbb{C}(\Lambda)^*$ være slik at $\mathrm{div}(f) = (w_1) - (w_2)$. Da er f en funksjon av orden ≤ 1, altså konstant, så $\mathrm{div}(f) = 0$. □

Noen prinsipale divisorer. For å forstå hvordan $\mathrm{div}(f)$ ser ut for generelle elliptiske f, begynner vi med å studere $\mathrm{div}(f)$ for noen f relatert til $\wp(z)$ og $\wp'(z)$.

La $\omega_1, \omega_2 \in \Lambda$ være en basis for Λ, og la $\omega_3 = \omega_1 + \omega_2$.

LEMMA. *Vi har*
$$\mathrm{div}(\wp'(z)) = \left(\frac{\omega_1}{2}\right) + \left(\frac{\omega_2}{2}\right) + \left(\frac{\omega_3}{2}\right) - 3(0).$$

BEVIS. Siden $\wp'(z)$ er en odde elliptisk funksjon, og
$$-\frac{\omega_i}{2} = \frac{\omega_i}{2} \pmod{\Lambda},$$
har vi at
$$\wp'\left(\frac{\omega_i}{2}\right) = -\wp'\left(-\frac{\omega_i}{2}\right) = -\wp'\left(\frac{\omega_i}{2}\right),$$

[1] Eksplisitte formler for g_2 og g_3 som en funksjon av Λ kan gis, og disse viser seg å være såkalte *modulære former*.

så

$$\wp'\left(\frac{\omega_i}{2}\right) = 0.$$

Siden $\wp'$ har orden 3, så har $\wp'$ maksimalt 3 distinkte nullpunkter i $\mathbb{C}/\Lambda$. Siden $\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_3}{2}$ er distinkte, har vi altså at nullpunktene til $\wp'$ er nøyaktig disse tre. □

LEMMA. *La $w \in (\mathbb{C}/\Lambda) \setminus \{0\}$, og la $f(z) = \wp(z) - \wp(w)$. Da er*

$$\operatorname{div}(f(z)) = (w) + (-w) - 2(0)$$

BEVIS. Ordenen til f er 2, så f har to nullpunkter talt med multiplisitet. Vi har alltid $f(w) = 0$. To caser

(1) $w = \frac{\omega_i}{2}$ for en $i \in \{1, 2, 3\}$: Da er $f'(w) = \wp'(w) = 0$, så dermed er w et dobbelt nullpunkt.

(2) $w \neq \frac{\omega_i}{2}$ for noen i: Da er $w \neq -w$, så $f(-w) = f(w) = 0$ og $-w$ er det andre nullpunktet til f.

□

LEMMA. *For $w_1, w_2 \in (\mathbb{C}/\Lambda) \setminus \{0\}$, så finnes en elliptisk funksjon g slik at*

$$\operatorname{div}(g) = (w_1 + w_2) + (w_1 - w_2) - 2(w_1).$$

BEVIS. Sett $g(z) = f(z - w_1)$ med f som i forrige lemma. □

PROPOSISJON. *Homomorfien $\operatorname{Div}^0(\mathbb{C}/\Lambda) \to \mathbb{C}/\Lambda$ gitt ved*

$$\sum n_i(w_i) \mapsto \sum n_i w_i$$

er surjektiv, med kjerne $\operatorname{div}(\mathbb{C}(\Lambda)^*)$, dvs. at vi har en gruppeisomorfi

$$\operatorname{Pic}^0(\mathbb{C}/\Lambda) \cong \mathbb{C}/\Lambda.$$

BEVIS. Det vanskelige punktet er å vise

$$\sum n_i(w_i) \sim 0 \Leftrightarrow \sum n_i w_i = 0.$$

Gitt en divisor $D = \sum n_i(w_i)$, kan vi bruke den generelle relasjonen[2]

$$(z_1 + z_2) + (z_1 - z_2) \sim 2(z_1)$$

til å vise at $D \sim (\sum n_i w_i) - (0)$, som er lik 0 hvis og bare hvis $\sum n_i w_i = 0$. □

Mer konkret betyr dette at alle $D \in \operatorname{Pic}^0(\mathbb{C}/\Lambda)$ kan representeres som

$$D = (z) - (0)$$

for en $z \in \mathbb{C}/\Lambda$, og $(z_1) - (0) + (z_2) - (0) = (z_1 + z_2) - (0)$.

[2]Gitt $a, b, c \in \mathbb{C}$, får vi

$$(a) + (b) \sim 2(\frac{a+b}{2})$$
$$(c) + (a+b-c) \sim 2(\frac{a+b}{2})$$
$$\Downarrow$$
$$(a) + (b) - (c) \sim (a+b-c).$$

Med denne relasjonen kan man ved induksjon på n vise at en divisor på formen $\sum_{i=1}^n (z_i) - \sum_{i=1}^n (w_i)$ er rasjonalt ekvivalent til $(\sum_{i=1}^n z_i - \sum_{i=1}^n w_i) - (0)$.

TEOREM 7.3. *(1) Kurven E_Λ definert av $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ er elliptisk.*

(2) Avbildningen $\phi\colon \mathbb{C}/\Lambda \to E_\Lambda$ definert av

$$\phi(z) = [\wp(z) : \wp'(z) : 1]$$

er en bijeksjon.

(3) Avbildningen bevarer gruppestrukturene.

(4) $E_\Lambda[n] \cong \mathbb{Z}/n \oplus \mathbb{Z}/n$.

(5) Gitt en elliptisk kurve E, finnes det en $\Lambda \subset \mathbb{C}$ slik at $E \cong E_\Lambda$.

(6) Avbildningen ϕ gir en bijeksjon mellom elliptiske funksjoner på $\mathbb{C}/\Lambda$ og rasjonale funksjoner på E_Λ.

BEVIS. Må sjekke at $f = 4x^3 - g_2x - g_3$ har 3 distinkte røtter. Siden $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$, så har vi

$$\wp'(z) = 0 \Rightarrow \wp(z) \text{ er rot i } f.$$

Vi har vist at $\wp'(\frac{\omega_i}{2}) = 0$ for $i = 1, 2, 3$, og at

$$\wp(z) - \wp(\frac{\omega_i}{2})$$

har dobbelt nullpunkt i $\frac{\omega_i}{2}$. Dermed er $\{\wp(\frac{\omega_i}{2})\}_{i=1,2,3}$ tre distinkte røtter av f.

2) Bildet er opplagt inneholdt i E_Λ.

Vi viser først at ϕ er surjektiv. La $(x, y) \in E$, og se på funksjonen $\wp(z) - x$. Denne er elliptisk og ikkekonstant, så det finnes en z slik at $\wp(z) - x = 0$.

Vi har dermed at $\wp(z) = x$, som siden $(\wp(z), \wp'(z)), (x, y) \in E$ betyr at $\wp'(z) = \pm y$. Hvis $\wp'(z) = -y$, har vi at

$$\phi(-z) = (\wp(-z), \wp'(-z)) = (\wp(z), -\wp'(z)) = (x, y).$$

For injektivitet: La $w_1, w_2 \in \mathbb{C}/\Lambda \setminus \{0\}$ slik at $\phi(w_1) = \phi(w_2)$. Vi har vist at

$$\operatorname{div}(\wp(z) - \wp(w_1)) = (w_1) + (-w_1) - 2(0),$$

så

$$\wp(w_2) - \wp(w_1) = 0 \Rightarrow w_2 = \pm w_1.$$

Hvis $w_2 = -w_1$, så er $\wp'(w_2) = -\wp'(w_1)$. Da må $\wp'(w_2) = \wp'(w_1) = 0$, som betyr at $w_1, w_2 \in \{\omega_1/2, \omega_2/2, \frac{\omega_3}{2}\}$. Men da er $w_2 = -w_1 = w_1$.

3) Siden ϕ er en bijeksjon, holder det å vise at ϕ^{-1} er en gruppehomomorfi. La $P_1, P_2 \in E$, og la $P_3 = P_1 + P_2$.

Da finnes en $f \in \mathbb{C}(E_\Lambda)$ slik at

$$\operatorname{div}(f) = (P_1 - O) + (P_2 - O) - (P_3 - O) = P_1 + P_2 - P_3 - O.$$

Siden $f \circ \phi$ er en rasjonal funksjon av $\wp, \wp'$, så er den en elliptisk funksjon. Man kan vise at for alle $z \in \mathbb{C}/\Lambda$, så er

$$\operatorname{ord}_z(f \circ \phi) = \operatorname{ord}_{\phi(z)}(f),$$

og dermed er

$$\operatorname{div}(f \circ \phi) = \phi^{-1}(P_1) + \phi^{-1}(P_2) - \phi^{-1}(P_3) - (0),$$

som betyr at $\phi^{-1}(P_3) = \phi^{-1}(P_1) + \phi^{-1}(P_2)$.

4) Beregn gruppen av n-torsjonspunkter i $\mathbb{C}/\Lambda$.

5) Vanskelig, vi viser ikke dette.

6) Hvis $f \in \mathbb{C}(E)$, så er $f \circ \phi$ et rasjonalt uttrykk i $\wp(z), \wp'(z)$, og dermed elliptisk. Vi har påstått (uten bevis) at enhver elliptisk funksjon g er en rasjonal funksjon i $\wp(z)$ og $\wp'(z)$, så dermed er $g \circ \phi^{-1}$ en rasjonal funksjon i x, y på E_Λ. $\square$

KAPITTEL 8

Oppgaver

Oppgaver vi gjennomgår: 3.7 3.9 3.12, 4.1, 4.2, 4.6, 5.1, 5.2, 6.2, 6.3, 6.4, 7.1, 7.3.

Oppgaver til siste forelesning 27. mai: 5.15, 6.5, 7.4.

(*) = Vanskelig oppgave

(**) = Skikkelig vanskelig.

Kapittel 2 – Varieteter

2.1. La V være en projektiv varietet, la $P \in V$, og la $f = \frac{G}{H} \in \overline{K}(V)$, hvor $G, H \in \overline{K}[V]$ er homogene elementer av samme grad. Vis at hvis $G(P) \neq 0$ og $H(P) = 0$, så er f ikke regulær i P.

2.2. (*) La $g, h \in \overline{K}[\mathbb{P}^n] = \overline{K}[X_0, \ldots, X_n]$ være homogene polynomer av samme grad, og anta at disse ikke har noen felles ikkekonstant faktor i $\overline{K}[X_0, \ldots, X_n]$. Vis at den rasjonale funksjonen $f = g/h$ er regulær i $P \in \mathbb{P}^n$ hvis og bare hvis $h(P) \neq 0$. (Bruk at $\overline{K}[X_0, \ldots, X_n]$ er et UFD.)

2.3. (*) Vis at den rasjonale avbildningen $\phi\colon \mathbb{P}^2 \to \mathbb{P}^1$ gitt ved

$$\phi = [X : Y]$$

ikke er regulær i $[0 : 0 : 1] \in \mathbb{P}^2$.

2.4. La $C \subset \mathbb{P}^2$ være definert av ligningen $ZY - X^2$. Vis direkte, uten å bruke Proposisjon 3.16, at den rasjonale avbildningen $\phi\colon C \to \mathbb{P}^1$ gitt ved

$$\phi = [X : Y]$$

er regulær i $[0 : 0 : 1] \in C$.

2.5. Hvis $V \subseteq \mathbb{P}^n$ er en projektiv varietet definert over K, så er V også definert over L for alle kroppsutvidelser L av K. Dermed gir det mening å snakke om $V(L)$ for alle slike utvidelser L. Vis at for alle $P \in V$ så finnes det en *endelig* kroppsutvidelse $K \hookrightarrow L$ slik at $P \in V(L)$.

2.6. La V være en projektiv varietet, la $P \in V$ og la $f \in \overline{K}(V)$. Vis at vi kan skrive $f = g/h$, hvor $g, h \in \overline{K}(V)$ er regulære i P.

Kapittel 3 – Kurver

3.1. La $E \subset \mathbb{P}^2$ være definert av $y^2 = x^3 + Ax + B$ med $A, B \in \overline{K}$. La $\phi = [x : 1] \to \mathbb{P}^1$ og $\psi = [y : 1] \to \mathbb{P}^1$. Avgjør hvor ϕ og ψ er ramifisert og bestem ramifikasjonsindeksene.

3.2. Vis Proposisjon 3.26 i tilfellet $C_2 = \mathbb{P}^1$.

3.3. Vis (1)-(5) i Proposisjon 3.45.

3.4. La C være en ikkesingulær kurve. Vis at $\mathrm{Pic}(C) \cong \mathrm{Pic}^0(C) \times \mathbb{Z}$.

3.5. Vis at hvis $\phi\colon \mathbb{P}^1 \to C$ er en morfi, så er $\phi(P) \sim \phi(Q)$ for alle $P, Q \in \mathbb{P}^1$.

3.6. Vis at hvis $\phi\colon \mathbb{P}^1 \to C$ er en morfi og $g(C) > 0$, så er ϕ konstant.

3.7. Vis at hvis $f, g \in \overline{K}(C)^*$ er slik at $\mathrm{div}(f) = \mathrm{div}(g)$, så er $f = ag$ for en eller annen $a \in \overline{K}^*$.

3.8. La C være en ikkesingulær kurve av genus g. Vis at hvis $D \in \mathrm{Div}(C)$ har $\deg(D) = 2g - 2$ og $\dim \mathcal{L}(D) = g$, så er $D \sim K_C$.

3.9. (1) La C være en ikkesingulær kurve, la $P \in C$, og la $0 \neq f_1, f_2 \in \overline{K}(C)$ være slik at $\mathrm{ord}_P(f_1) = \mathrm{ord}_P(f_2) = n$. Vis at det finnes $a_1, a_2 \in \overline{K}$, ikke begge lik 0, slik at $\mathrm{ord}_P(a_1 f_1 + a_2 f_2) > n$. Hint i fotnote:[1]

(2) La $D \in \mathrm{Div}(C)$ og $P \in C$. Vis at $l(D) \leq l(D + (P)) \leq l(D) + 1$. Hint for $l(D + (P)) \leq l(D) + 1$ i fotnote.[2]

(3) Vis at $l(D) \leq \deg(D) + 1$ for alle $D \in \mathrm{Div}(C)$ hvor $\deg(D) \geq 0$.

3.10. La $f \in \overline{K}(C)^*$, og skriv

$$\mathrm{div}(f) = \sum n_i(P_i) - \sum m_i(Q_i),$$

hvor alle $m_i, n_i > 0$ og alle P_i og Q_i er distinkte. Definer **ordenen** til f som $\mathrm{ord}(f) = \sum n_i = \sum m_i$. Vis at hvis $g(C) > 0$, så er $\mathrm{ord}(f) \neq 1$. (Jf. Proposisjon 7.2).

3.11. Vis at hvis $\phi\colon C_1 \to C_2$ er en morfi av ikkesingulære kurver, så er $\deg \phi = 1$ hvis og bare hvis ϕ er en isomorfi.

3.12. La C være en kurve av genus 0, og la $P \neq Q \in C$.

(1) Vis at $l(P - Q) = 1$.

(2) La $0 \neq f \in l(P - Q)$. Vis at $\phi = [f : 1]\colon C \to \mathbb{P}^1$ har grad 1.

(3) Vis at ϕ er en isomorfi, og altså at $C \cong \mathbb{P}^1$.

3.13. Bruk 3.6 og 3.12 til å vise *Lüroths teorem*: Hvis $\overline{K} \subsetneq L \subset \overline{K}(x)$ er en kjede av kropper, så finnes det en $y \in L$ slik at $L = \overline{K}(y)$.

3.14. La C være en ikkesingulær kurve, og la $\omega \in \Omega_C$ være et differensial slik at $\mathrm{ord}_P(\omega) = 0$ for alle $P \in C$. Vis at $g(C) = 1$.

---

[1] Skriv $f_i = t^n g_i$ hvor t er lokal parameter i P.

[2] La $f_1, f_2 \in \mathcal{L}(D + (P)) \setminus \mathcal{L}(D)$, og bruk punkt (1).

Kapittel 4 – Elliptiske kurver, én og én

4.1. Vis at kurven $E \subset \mathbb{P}^2$ definert av $X^3 + Y^3 + Z^3 = 0$ er isomorf til kurven definert av

$$Y^2Z = X^3 + Z^3.$$

4.2. La $E \subset \mathbb{P}^2$ være en kurve med ligning $y^2 = x^3 + Ax + B$. Bruk morfien $\phi\colon E \to \mathbb{P}^1$ gitt av $\phi = [x : 1]$ til å vise at en rasjonal funksjon $f \in \overline{K}(E)$ kan skrives entydig som

$$f = f_0 + yf_1,$$

hvor $f_0, f_1 \in \overline{K}(x)$.

4.3. La $E \subset \mathbb{P}^2$ være en kurve på Weierstrass-form, la $F \in \overline{K}[X, Y, Z]$ være et irredusibelt homogent polynom av grad 2 og la $C \subset \mathbb{P}^2$ være kurven definert av F. Ved Bezouts teorem består snittet av C og E av 6 punkter $P_1, \ldots, P_6$, talt med multiplisitet. Vis at

$$\sum_{i=1}^{6} P_i = O$$

4.4. Generaliser oppgaven over til et polynom F av grad d.

4.5. La E være gitt ved $y^2 = x^3 + Ax$. Beregn de fire punktene $P_1, \ldots, P_4$ slik at $2P_i = (0, 0)$.

4.6. La D være en divisor på E med $\deg(D) = d \neq 0$. Vis at det finnes en P slik at $dP \sim D$. Hvor mange ulike slike P finnes?

4.7. La E være en elliptisk kurve, og la $E_{tors} = \bigcup_{n\geq 1} E[n] \subset E$ være gruppa av torsjonspunkter.

(1) Vis at E_{tors} er tellbar uendelig.

(2) Vis at det finnes tellbart uendelig mange endelige undergrupper av E.

Kapittel 5 – Isogenier

5.1. Vis at hvis $\phi \in \mathrm{End}(E)$ er en isogeni og $\phi(P) = P$, så er P et torsjonspunkt.

5.2. Si at $E_1 \sim E_2$ hvis det finnes en ikkekonstant isogeni $\phi\colon E_1 \to E_2$. Vis at $\sim$ definerer en ekvivalensrelasjon.

5.3. Vis at hvis $\overline{K}$ er overtellbart uendelig, og E er en elliptisk kurve definert over K, så finnes det uendelig mange E' slik at $E \not\sim E'$.

5.4. (*) La $\phi\colon E \to E$ være en isomorfi av kurver (hvor vi kan ha $\phi(O) \neq O$). Vis at hvis ϕ ikke er lik τ_P for noen $P \in E$, så har ϕ endelig orden.

5.5. La G, H være abelske grupper, og la $\phi\colon G \to H$ være en surjektiv homomorfi slik at $\ker\phi$ er endelig.

a) Vis at det finnes en homomorfi $\hat{\phi}\colon H \to G$ slik at $\hat{\phi} \circ \phi = |\ker\phi|$.

b) Gi et eksempel på to homomorfier $\phi, \psi\colon G \to H$ som over, slik at $\hat{\phi} + \hat{\psi}$ ikke er lik $\widehat{\phi + \psi}$ (så Proposisjon 5.33 er ikke en "formell" konsekvens av definisjonen).

5.6. Fullfør beviset for Korollar 5.33 ved å vise følgende lemma: La $n \geq 0$ og G være en abelsk gruppe slik at $ng = 0$ for alle $g \in G$. Anta at for alle divisorer d av n, så er $|\{g \in G \mid dg = 0\}| = d^2$. Da er $G \cong \mathbb{Z}/n \oplus \mathbb{Z}/n$.

5.7. La $\mathcal{K}(a, b)$ være kvaternionalgebraen fra Avsnitt 5.7. Vis at

$$\mathcal{K}(a, b) \otimes_{\mathbb{Q}} \mathbb{R} \cong K$$

hvor K er ringen av kvaternioner

$$K = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$$
$$i^2 = j^2 = k^2 = ijk = -1.$$

5.8. Vis at hvis E_1, E_2 er elliptiske kurver, så er $\mathrm{Hom}(E_1, E_2)$ en høyremodul over ringen $\mathrm{End}(E_1)$ og en venstremodul over ringen $\mathrm{End}(E_2)$.[3]

5.9. (*) Vis at rangen til $\mathrm{Hom}(E_1, E_2)$ er delelig med rangen til $\mathrm{End}(E_1)$ og med rangen til $\mathrm{End}(E_2)$.

5.10. Vis at $P \in E$ er et torsjonspunkt hvis og bare hvis det finnes en kurve E' og en surjektiv isogeni $\phi\colon E \to E'$ slik at $\phi(P) = \phi(O)$.

5.11. Fra obligen: La $E \subset \mathbb{P}^2$ være en elliptisk kurve. Et *infleksjonspunkt* er et punkt $P \in E$ slik at tangentlinja gjennom P ikke skjærer E i noen andre punkter. Vis at P er et infleksjonspunkt hvis og bare hvis $P \in E[3]$.

5.12. Vis at hvis $l \subset \mathbb{P}^2$ er en linje som skjærer E i P_1, P_2, P_3 hvor P_1, P_2 er infleksjonspunkter, så er også P_3 et infleksjonspunkt.

5.13. (*) Sylvester–Gallai-teoremet sier: *La $S \subset \mathbb{R}^2$ være en mengde av distinkte punkter slik at linja gjennom to punkter i S alltid inneholder et tredje punkt i S. Da ligger alle punkter i S på én linje.*

La E være en elliptisk kurve definert over $\mathbb{R}$, og bruk Sylvester–Gallai-teoremet til å vise at $E(\mathbb{R})$ inneholder enten 1 eller 3 infleksjonspunkter for E.

5.14. (*) Vis at hvis $\mathrm{char}\, K = 0$, så er gruppa av torsjonspunkter $E_{tors} = \bigcup_{k=1}^{\infty} E[k]$ isomorf til $\mathbb{Q}/\mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z}$.

5.15. La E_1, E_2 være elliptiske kurver, la $P \in E_1$, og la $\phi_1, \phi_2, \phi_3, \phi_4, \phi_5\colon E_1 \to E_2$ være isogenier, og la $Q_i = \phi_i(P)$ for $i = 1, \ldots, 5$. Vis at det finnes $a_1, \ldots, a_5 \in \mathbb{Z}$, ikke alle lik 0, slik at

$$\sum_{i=1}^{5} a_i Q_i = O_2.$$

---

[3]En **venstremodul** over en ikkekommutativ ring R er en abelsk gruppe M utstyrt med en avbildning $R \otimes M \to M$ som skrives $r \otimes m \mapsto rm$, slik at $1m = m$ og for alle $r_1, r_2 \in R$, $m \in M$, så er

$$r_1(r_2 m) = (r_1 r_2)m.$$

En **høyremodul** er en abelsk gruppe M utstyrt med en avbildning $M \otimes R \to M$ som skrives $m \otimes r \mapsto mr$, slik at $m1 = m$ og for alle $r_1, r_2 \in R$, $m \in M$, så er

$$(mr_1)r_2 = m(r_1 r_2).$$

Kapittel 6 – Endelige kropper og telling av punkter

6.1. La $q_1 = p^{n_1}$ og $q_2 = p^{n_2}$, og se på kroppene $\mathbb{F}_{q_1}, \mathbb{F}_{q_2} \subset \overline{\mathbb{F}}_p$.

(1) Vis at $\mathbb{F}_{q_1} \subseteq \mathbb{F}_{q_2}$ hvis og bare hvis n_1 deler n_2.

(2) Anta at $\mathbb{F}_{q_1} \subseteq \mathbb{F}_{q_2}$, og vis at da er $\mathrm{Gal}(\mathbb{F}_{q_2}/\mathbb{F}_{q_1}) \cong \mathbb{Z}/n$, hvor $n = n_2/n_1$.

6.2. La E være en elliptisk kurve (ikke nødvendigvis definert over en endelig kropp). Tilpass beviset for Hasses teorem og vis at hvis $\phi\colon E \to E$ er en isomorfi slik at $\phi(O) = O$, og $\phi \neq \mathrm{id}_E$, så finnes det maksimalt 4 punkter P slik at $\phi(P) = P$.

6.3. La E være en elliptisk kurve definert over $\mathbb{F}_q$, og la $P \in E(\mathbb{F}_q)$. Vis at $\widehat{\mathrm{Fr}}_q(P) = P$ hvis og bare hvis $\mathrm{Fr}_q(P) = qP$.

6.4. La $K = \mathbb{F}_7$, la E være gitt av $y^2 = x^3 + x$, og la $\phi \in \mathrm{End}(E)$ være en automorfi av orden 4. Vis at ϕ og Fr_7 ikke kommuterer som elementer av ringen $\mathrm{End}(E)$.

6.5. La $K = \mathbb{F}_q$, og la E være en elliptisk kurve gitt ved $y^2 = x^3 + Ax + B$ med $A, B \in \mathbb{F}_q$. Vi har en homomorfi $\mathrm{Fr}_q[2]\colon E[2] \to E[2]$. Vis at $\mathrm{Fr}_q[2] = \mathrm{id}_{E[2]}$ hvis og bare hvis $x^3 + Ax + B$ har tre røtter i $\mathbb{F}_q$.

6.6. Vis at hvis E er en elliptisk kurve definert over $\mathbb{F}_q$ og $P \in E$, så er P et torsjonspunkt.

6.7. Vis at hvis E er en elliptisk kurve definert over $\mathbb{F}_q$, så er $\mathrm{End}(E) \cong \mathbb{Z}^2$ eller $\mathbb{Z}^4$ (som gruppe).

Kapittel 7 – Komplekse elliptiske kurver

7.1. Bruk resultatene i dette kapittelet til å vise at hvis E er en elliptisk kurve over $\mathbb{C}$, så er $\deg[n] = n^2$ for alle $n \in \mathbb{Z}$.

7.2. Bruk resultatene i dette kapittelet til å vise at $E_\Lambda[n] = \mathbb{Z}/n \oplus \mathbb{Z}/n$ og beskriv elementene i $E_\Lambda[n]$ som punkter i $\mathbb{C}/\Lambda$.

7.3. Gitt $z_1, z_2 \in \mathbb{C}$, beskriv $\wp(z_1+z_2)$ som rasjonal funksjoner av $\wp(z_1), \wp(z_2), \wp'(z_1), \wp'(z_2)$.

7.4. Bruk identifikasjonen $\phi\colon \mathbb{C}/\Lambda \to T_l(E_\Lambda)$, og gi en eksplisitt beskrivelse av et ikketrivielt element av Tate-modulen til $T_l(E_\Lambda)$ som en sekvens av punkter i $\mathbb{C}/\Lambda$.

7.5. Vis at når E er en elliptisk kurve definert over $\mathbb{C}$, så er torsjonsgruppa $E_{tors} = \bigcup_{m=1}^{\infty} E[m]$ isomorf til $\mathbb{Q}/\mathbb{Z} \oplus \mathbb{Q}/\mathbb{Z}$.

KAPITTEL 9

Hint

6.4: Bruk Avsnitt 5.8 til å gi en eksplisitt formel for ϕ.

5.14: Vis først at hvis G er en abelsk gruppe G slik at

$$G[n] = \{g \in G \mid ng = 0\} \cong \mathbb{Z}/n,$$

og $G = \bigcup_{n\geq 1} G[n]$, så er $G \cong \mathbb{Q}/\mathbb{Z}$.

Generaliser dette: La $d \geq 1$ være gitt, og vis at hvis $G[n] \cong (\mathbb{Z}/n)^d$ alle n og $G = \bigcup_{n\geq 1} G[n]$, så er $G \cong (\mathbb{Q}/\mathbb{Z})^d$.

7.3: Bruk Teorem 7.3 og Avsnitt 3.2.

KAPITTEL 10

Løsninger

2.1: Anta for en motsigelse at f er regulær i P. Da kan vi skrive $f = \frac{G}{H} = \frac{I}{J}$ hvor $I, J \in \overline{K}[V]$ er homogene av samme grad og $J(P) \neq 0$. Da er $GJ = IH$, og siden $H(P) = 0$, så er $G(P)J(P) = I(P)H(P) = 0$. Siden $G(P) \neq 0$, må $J(P) = 0$, som gir en motsigelse.

2.2: Hvis $h(P) \neq 0$, så er g/h per definisjon regulær i P.

Anta nå at $h(P) = 0$. Vi kan faktorisere h som $h = h_1 \dots h_n$, hvor h_i er homogene primelementer i $\overline{K}[X_0, \dots, X_n]$. Det må da finnes en i slik at $h_i(P) = 0$.

Vi har at $f = g/h$ er regulær i P hvis vi kan finne homogene $g', h' \in \overline{K}[X_0, \dots, X_n]$ slik at $g/h = g'/h'$ og $h'(P) \neq 0$. Dette betyr at $gh' = hg'$. Siden h_i deler h, så må h_i dele gh'. Men siden g, h ikke har noen felles faktor, så kan h_i ikke dele g, og dermed må h_i dele h'. Det følger at $h'(P) = 0$, så f er ikke regulær i P.

2.3: Vi har $\phi = [\frac{X}{Y} : 1]$, og lar $P = [0 : 0 : 1]$. Vi må vise at det ikke finnes noen $f \in \overline{K}(\mathbb{P}^2)^*$ slik at $f\frac{X}{Y}, f$ begge er regulære i P og minst én er ulik 0.

Anta for en motsigelse at det finnes en slik f, og skriv $f = \frac{g}{h}$ med $g, h \in \overline{K}[X, Y, Z]$ homogene av samme grad, uten felles faktorer i $\overline{K}[X, Y, Z]$. Siden f er regulær i P, så er $h(P) \neq 0$, ved oppgave 2.2.

Vi ser på $\frac{X}{Y}f = \frac{gX}{hY}$, og kan skrive $\frac{gX}{hY} = \frac{g'}{h'}$ hvor g', h' ikke har noen felles faktorer (forkortingen av brøken). Siden $\frac{g'}{h'}$ er regulær i P, må $h'(P) \neq 0$, og dermed er Y ikke en faktor i h'. Da må Y ha blitt forkortet bort, så Y må være en faktor i g. Det betyr at $\frac{g}{h}(P) = 0$.

Dermed må vi ha at $\frac{g'}{h'}(P) \neq 0$. Det betyr at X ikke er en faktor i g', som betyr at X må ha blitt forkortet bort, som igjen betyr at X er en faktor i h. Men da er $h(P) = 0$, som gir en motsigelse (puh!).

2.5: La $P = [\alpha_0 : \dots : \alpha_n] \in V$. Siden $\alpha_i \in \overline{K}$ for alle i, så er alle α_i algebraiske over K. Dermed er kroppsutvidelsen $K \hookrightarrow K(\alpha_0, \dots, \alpha_n)$ en endelig kroppsutvidelse. Tar vi $L = K(\alpha_0, \dots, \alpha_n)$, så er $P \in V(L)$.

2.6: La $f = G/H$, hvor $G, H \in \overline{K}[V]$ er homogene elementer av samme grad. Velg et homogent element $E \in \overline{K}[V]$ slik at $E(P) \neq 0$, og la $g = G/E$, $h = H/E$.

3.2: Vi har $\overline{K}(\mathbb{P}^1) = \overline{K}(x)$, så en kroppinklusjon $\psi\colon \overline{K}(x) \to \overline{K}(C_1)$ er bestemt av hvor den sender x. Vi må ha at $\psi(x) \notin K$, siden ψ er injektiv. Dermed er $\psi(x)$ en ikkekonstant rasjonal funksjon på C_1, som vi kan tenke på som en morfi til $\mathbb{P}^1$.

3.4: Velg et punkt $P \in C$. Vi sender $(D, n) \in \mathrm{Pic}^0(C) \times \mathbb{Z}$ til $D + nP \in \mathrm{Pic}(C)$, med invers avbildning $D \mapsto (D - \deg(D)P, \deg(D))$. Disse avbildningene er veldefinerte og opplagt inverse, så vi er ferdige.

3.5: Vi bruker Korollar 3.46, som sier at $\phi_*(D_1) \sim \phi_*(D_2)$ hvis $D_1 \sim D_2$. Ved Eksempel 3.41 veit vi at for alle punkter P_1, P_2 på $\mathbb{P}^1$, så er $P_1 \sim P_2$.

3.6: Ved oppgave 3.5, veit vi at for alle $P, Q \in \mathbb{P}^1$, så er $\phi(P) \sim \phi(Q)$. Men siden C har genus 1, så har vi ved Lemma 4.22, at $\phi(P) \sim \phi(Q) \Leftrightarrow \phi(P) = \phi(Q)$.

3.9: (1) La $t \in \overline{K}(C)$ være en lokal parameter i P. Ved Proposisjon 3.12, kan vi da, for $i = 1, 2$, skrive $f_i = t^n g_i$, hvor $\mathrm{ord}_P(g_i) = 0$. Dette betyr, at g_1 og g_2 begge er regulære i P og at $g_1(P), g_2(P)$ begge er ulike null. Vi kan dermed ta $a_1 = g_2(P)$ og $a_2 = -g_1(P)$, slik at vi får

$$a_1 f_1 + a_2 f_2 = t^n (g_2(P) g_1 - g_1(P) g_2).$$

Funksjonen $g_2(P)g_1 - g_1(P)g_2$ er regulær i P, og vi har

$$(g_2(P)g_1 - g_1(P)g_2) = g_2(P)g_1(P) - g_1(P)g_2(P) = 0,$$

så $\mathrm{ord}_P(g_2(P)g_1 - g_1(P)g_2) \geq 1$. Men da er

$$\mathrm{ord}_P(a_1 f_1 + a_2 f_2) = \mathrm{ord}_P(t^n) + \mathrm{ord}_P(g_2(P)g_1 - g_2(P)g_1) > n.$$

(2) Vi viser først

$$l(D) \leq l(D + (P)). \tag{6}$$

Hvis $f \in \mathcal{L}(D)$, så er $\mathrm{div}(f) + D \geq 0$, og det følger at $\mathrm{div}(f) + D + (P) \geq (P) \geq 0$, så $f \in \mathcal{L}(D + (P))$. Dermed er $\mathcal{L}(D) \subseteq \mathcal{L}(D + (P))$, så vi må ha $l(D) \leq l(D + (P))$.

For ulikheten $l(D + (P)) \leq l(D) + 1$, har vi to løsninger:

Ellas løsning: Ved Riemann–Roch (Teorem 3.71), har vi at

$$l(D + (P)) - l(K_C - D - (P)) = 1 - g(C) + \deg(D + (P))$$
$$l(D) - l(K_C - D) = 1 - g(C) + \deg(D)$$

Differansen av disse to ligningene gir oss at

$$\begin{aligned} l(D + (P)) - l(D) &= \deg(D + (P)) - \deg(D) + l(K_C - D - (P)) - l(K_C - D) \\ &= 1 + l(K_C - D - (P)) - l(K_C - D) \leq 1, \end{aligned}$$

hvor vi først bruker $\deg(D + (P)) = \deg(D) + 1$, og så at $l(K_C - D - (P)) \leq l(K_C - D)$, som følger av ligning (6).

Alternativ løsning: Vi bruker følgende lineær algebra-lemma: La $V \subset W$ være endelig-dimensjonale $\overline{K}$-vektorrom, og anta at for alle par $w_1, w_2 \in W \setminus V$, så finnes det $a_1, a_2 \in \overline{K}$, ikke begge 0, slik at $a_1 w_1 + a_2 w_2 \in V$. Da er $\dim W \leq \dim V + 1$.

Bevis for linalglemma: La $v_1, \ldots, v_{\dim V}$ være en basis for V, og utvid denne til en basis $v_1, \ldots, v_{\dim V}, w_1, \ldots, w_{\dim W - \dim V}$ for W. Hvis $\dim W > \dim V + 1$, så har vi vektorene $w_1, w_2 \in W \setminus V$. Per antagelsen vår, så finnes det $a_1, a_2 \in \overline{K}$, ikke begge 0, slik at $a_1 w_1 + a_2 w_2 = v \in V$. Men dette gir en lineær relasjon mellom $w_1, w_2, v_1, \ldots, v_{\dim V}$, så vi har en motsigelse.

For oppgaven holder det altså å vise at hvis $f_1, f_2 \in \mathcal{L}(D + (P)) \setminus \mathcal{L}(D)$, så finnes det $a_1, a_2 \in \overline{K}$, ikke begge 0, slik at $a_1 f_1 + a_2 f_2 \in \mathcal{L}(D)$. La oss skrive

$$D = nP \sum n_i P_i,$$

hvor P og $P_i \in C$ alle er distinkte. Da er $f \in \mathcal{L}(D)$ hvis og bare hvis

$$\mathrm{ord}_P(f) \geq -n, \mathrm{ord}_{P_i}(f) \geq -n_i, \text{ for alle } i, \text{ og } \mathrm{ord}_P(f) \geq 0 \text{ for alle } Q \neq P_i.$$

Tilsvarende er $f \in \mathcal{L}(D+(P))$ hvis og bare hvis

$$\operatorname{ord}_P(f) \geq -n-1, \operatorname{ord}_{P_i}(f) \geq -n_i, \text{ for alle } i, \text{ og } \operatorname{ord}_P(f) \geq 0 \text{ for alle } Q \neq P_i.$$

Med andre ord er $\mathcal{L}(D) \subseteq \mathcal{L}(D+(P))$ underrommet av de f som tilfredsstiller $\operatorname{ord}_P(f) \geq -n$.

Hvis $f_1, f_2 \in \mathcal{L}(D+(P))$, må vi dermed ha $\operatorname{ord}_P(f_1) = \operatorname{ord}_P(f_2) = -n-1$. Ved punkt (1) i denne oppgaven kan vi finne $a_1, a_2 \in \overline{K}$, ikke begge 0, slik at $\operatorname{ord}_P(a_1 f_1 + a_2 f_2) \geq -n$. Dermed er $a_1 f_1 + a_2 f_2 \in \mathcal{L}(D)$, som var det vi trengte å vise.

(3): La $d = \deg(D)$, og la $P \in C$. Divisoren $D-(d+1)P$ har grad -1, og dermed er $l(D-(d+1)P) = 0$. Bruker vi ulikheten fra punkt (2) i denne oppgaven gjentatte ganger, får vi

$$l(D) \leq l(D-(P))+1 \leq l(D-2(P))+2 \leq \cdots \leq l(D-(d+1)P)+d+1 = d+1.$$

3.6: (1) Ved Riemann–Roch (Teorem 3.71), er

$$l(P-Q) - l(K_C-(P-Q)) = 1-g(C)+\deg(P-Q) = 1.$$

Men Korollar 3.72 gir at $\deg K_C = 2g(C)-2 = -2$, så $\deg K_C-(P-Q) = -2$, og dermed er $l(K_C-(P-Q)) = 0$. Det følger at $l(P-Q) = 1$.

(2): Siden $\operatorname{div}(f)+P-Q \geq 0$ og $\deg(\operatorname{div}(f)+P-Q) = 0$, har vi at

$$\operatorname{div}(f)+P-Q = 0.$$

Med andre ord har vi $\operatorname{ord}_P(f) = -1, \operatorname{ord}_Q(f) = 1$, og $\operatorname{ord}_R(f) = 0$ for $R \neq P, Q$.

Vi bruker Proposisjon 3.33, og studerer fiberen til ϕ over punktet $[0:1] \in \mathbb{P}^1$. Vi har da

$$\deg\phi = \sum_{R \in \phi^{-1}([0:1])} e_\phi(R).$$

Siden $\phi = [f:1]$, har vi $\phi(R) = [0:1]$ hvis og bare hvis $f(R) = 0$, som skjer hvis og bare hvis $R = Q$. Dermed er

$$\deg(\phi) = e_\phi(Q) = \operatorname{ord}_Q(x \circ \phi) = \operatorname{ord}_Q(f) = 1,$$

hvor vi bruker definisjonen av e_ϕ (Def. 3.30), og at $x \in \overline{K}(\mathbb{P}^1)$ er en lokal parameter i $[0:1]$.

(3): Følger av oppgave 3.11.

3.14: To mulige løsninger. *Ved Riemann–Roch:* Bruker vi at $\deg K_C = 2g(C)-2$ (Korollar 3.72), og at

$$K_C = \sum_{P \in C} \operatorname{ord}_P(\omega)(P) = 0,$$

får vi at $\deg K_C = 0$ og $g(C) = 1$.

Uten Riemann–Roch: Pre definisjon av genus er $g(C) = l(K_C)$, og vi har som over at $K_C = 0 \in \operatorname{Pic}(C)$. Vektorrommet $\mathcal{L}(K_C) = \mathcal{L}(0)$ består av $f \in \overline{K}(C)$ slik at $\operatorname{div}(f) \geq 0$, som betyr at $\operatorname{ord}_P(f) \geq 0$ for alle $P \in C$. Men da er f regulær, og altså konstant. Vi ser at hvis f er konstant, så er $f \in \mathcal{L}(0)$, så $\mathcal{L}(0) = \overline{K}$, og vi får $g(C) = l(K_C) = 1$.

4.1: Vi gjør variabelskifter, og kvitter oss først med Y^3-leddet ved å substituere $Z \mapsto (Z-Y)^3$:

$$X^3+Y^3+Z^3 \rightsquigarrow X^3+Y^3+(Z-Y)^3 = X^3-3YZ^2+3Y^2Z+Z^3.$$

Vi kvitter oss så med YZ^2-leddet ved å substituere $Y \mapsto Y + \frac{Z}{2}$:

$$X^3 - 3(Y + \frac{Z}{2})Z^2 + 3(Y + \frac{Z}{2})^2 Z + Z^3 = X^3 + 3Y^2 Z + \frac{Z^3}{4}$$

Ved å reskalere først Z og så Y får vi da ligningen på formen

$$X^3 + Z^3 - Y^2 Z = 0,$$

som var det vi ville.

4.2: Det finnes flere måter å argumentere.

I: Vi kan først vise geometrisk at morfien ϕ har grad 2, ved for eksempel å velge et punkt $P \in \mathbb{P}^1$, og så sjekke at

$$\sum_{Q \in \phi^{-1}(P)} e_\phi(Q) = 2.$$

La $P = [\alpha : 1]$ med $\alpha \in \overline{K}$. Da er

$$\phi^{-1}(P) = \{(\alpha, \beta) \mid \beta^2 = \alpha^3 + A\alpha + B\},$$

så hvis α ikke er rot i $x^3 + Ax + B$, så har vi to punkter $Q_1, Q_2 = (\alpha, \pm\beta) \in \phi^{-1}(P)$.

Vi vet at $x - \alpha$ er lokal parameter i P. Man kan sjekke ved derivasjonskriteriet (jf. oblig) at

$$\operatorname{ord}_{Q_1}(x - \alpha) = \operatorname{ord}_{Q_2}(x - \alpha) = 1,$$

så $e_\phi(Q_1) = e_\phi(Q_2) = 1$, og dermed er $\deg \phi = 2$.

Kroppsutvidelsen

$$\phi\colon \overline{K}(\mathbb{P}^1) = \overline{K}(x) \hookrightarrow \overline{K}(C)$$

har dermed grad 2, så $\overline{K}(C)$ er et 2-dimensjonalt $\overline{K}(x)$-vektorrom. Elementet $y \in \overline{K}(C)$ ligger ikke i $\phi^*(\overline{K}(\mathbb{P}^1))$, så dermed utgjør $1, y$ en basis for $\overline{K}(C)$ som $\overline{K}(\mathbb{P}^1)$-vektorrom, som er det vi trengte å vise.

II: Mer algebraisk kan vi si at vi vet at x, y genererer kroppen $\overline{K}(C)$ som en kroppsutvidelse av $\overline{K}$, og vi har $\overline{K}(x) \subsetneq \overline{K}(C)$. Siden $y^2 = x^3 + Ax + B$, så må kroppsutvidelsen $\overline{K}(x) \hookrightarrow \overline{K}(C)$ ha grad 2, og vi kan argumentere videre som over.

4.6: La $D' = D - dO \in \operatorname{Div}^0(C)$. Da kan vi skrive $D' = Q - O$ for et unikt punkt $Q \in E$.

Betingelsen $dP \sim D$ er ekvivalent til $d(P - O) \sim D' \sim Q - O$, som er ekvivalent til påstanden at $dP = Q$ som elementer i gruppa E.

Vi veit (men uff da, ikke egentlig før i Kapittel 5) at avbildningen $[d]\colon E \to E$ har grad d^2, slik at det finnes d^2 elementer P med $dP \sim D$ (hvis $\operatorname{char} K = 0$ eller $\operatorname{char} K$ ikke deler d).

5.1: Hvis $\phi(P) = P$, så er $(\phi - [1])(P) = O$, altså er $P \in \ker(\phi - [1])$. Men siden $\phi \neq [1]$, så er $\phi - [1] \neq [0]$, så $\ker(\phi - [1])$ er en endelig gruppe. Dermed er $|\ker(\phi - [1])|P = O$, så P er et torsjonspunkt.

5.2: Tre ting å vise:

- $E \sim E$: Isogenien id_{E_1} finnes og er ikkekonstant.
- $E_1 \sim E_2 \wedge E_2 \sim E_3 \Rightarrow E_1 \sim E_3$: Hvis $\phi\colon E_1 \to E_2$ og $\psi\colon E_2 \to E_3$ er ikkekonstante, så er de surjektive, og dermed er $\psi \circ \phi\colon E_1 \to E_3$ surjektiv og altså ikkekonstant.

- $E_1 \sim E_2 \Rightarrow E_2 \sim E_1$: Hvis $\phi\colon E_1 \to E_2$ er en ikkekonstant isogeni, så er $\hat{\phi}\colon E_2 \to E_1$ en ikkekonstant isogeni.

5.10: *Hvis:* Hvis $\phi\colon E \to E'$ er en surjektiv isogeni slik at $\phi(P) = \phi(O)$, så er $P \in \ker\phi$. Siden $\ker\phi$ er en endelig gruppe, har vi da at $|\ker\phi|P = O$, så P er et torsjonspunkt.

Bare hvis (Viktors enkle bevis): Hvis $P \in E$ er et torsjonspunkt, så er $nP = O$ for en n, så $P \in E[n] = \ker[n]$, så $[n](P) = O$.

Bare hvis (Jørgens unødvendig kompliserte bevis): Hvis $P \in E$ er et torsjonspunkt, så er gruppa $G = \{nP \mid n \in \mathbb{Z}\} \subset E$ en endelig gruppe. Ved Teorem 5.26, finnes det en surjektiv isogeni $\phi\colon E \to E'$ slik at $G = \ker\phi$. Dermed er $\phi(P) = O$, som var det vi ville vise.

6.2: Vi har at $P = \phi(P)$ hvis og bare hvis $(\phi - [1])(P) = O$, altså hvis og bare hvis $P \in \ker(\phi - [1])$. Ved Korollar 6.29 har vi at

$$|\deg(\phi - [1]) - \deg(\phi) - \deg([-1])| \leq 2\sqrt{\deg(\phi)\deg([-1])}.$$

Siden både ϕ og $[-1]$ er isomorfier, har vi $\deg(\phi) = \deg([-1]) = 1$, som gir at

$$|\deg(\phi - [1]) - 2| \leq 2.$$

Siden $\phi \neq [1]$, har vi at $\deg(\phi - [1]) \neq 0$, så vi får at $\deg(\phi - [1]) = 1, 2, 3$ eller 4. I alle tilfeller er da $|\ker(\phi - [1])| \leq 4$.

6.3: Vi bruker at Fr_q er en bijeksjon. Dermed er $\hat{\mathrm{Fr}}_q(P) = P$ hvis og bare hvis $\mathrm{Fr}_q(\hat{\mathrm{Fr}}_q)(P) = \mathrm{Fr}_q(P)$, men siden $\mathrm{Fr}_q \circ \hat{\mathrm{Fr}}_q = [\deg \mathrm{Fr}_q] = q$, er dette hvis og bare hvis $qP = \mathrm{Fr}_q(P)$.

6.4: Ved resultatene i Avsnitt 5.8 er alle automorfier av en Weierstrass-kurve E på formen $\phi_u\colon E \to E$, med $\phi_u(x, y) = (u^2x, u^3y)$, hvor $u^4A = A$ og $u^6B = B$.

For kurven i oppgaven er $A = 1$, $B = 0$, så vi krever at $u^4 = 1$. Hvis ϕ_u skal ha orden 4, så må $u^2 = -1$, med andre ord er u en primitiv fjerderot av 1.

Vi fikserer en slik $u \in \overline{\mathbb{F}}_7$, og ser at automorfien blir

$$\phi_u(x, y) = (u^2x, u^3y) = (-x, -uy).$$

Vi kan nå beregne

$$(\mathrm{Fr}_7 \circ \phi_u)(x, y) = \mathrm{Fr}_7(-x, -uy) = ((-x)^7, (-uy)^7) = (-x^7, -u^7y^7) = (-x^7, uy^7).$$

og

$$(\phi_u \circ \mathrm{Fr}_7)(x, y) = \phi_u(x^7, y^7) = (-x^7, -uy^7),$$

og vi ser at $\phi_u \circ \mathrm{Fr}_7 \neq \mathrm{Fr}_7 \circ \phi_u$.

6.6: La $P \in E$. Ved oppgave 2.5, så finnes det en endelig kroppsutvidelse $\mathbb{F}_q \hookrightarrow L$ slik at $P \in E(L)$. Siden L er en endelig utvidelse av $\mathbb{F}_q$, er den selv en endelig kropp, så mengden $E(L)$ er endelig. Mengden $E(L) \subset E$ er en undergruppe, ved Korollar 4.39, så dermed er $|E(L)|(P) = O$, og P er et torsjonspunkt.

7.1: Hvis E er definert over $\mathbb{C}$, så har vi, siden $\mathrm{char}\,\mathbb{C} = 0$, at $\deg[n] = |\ker[n]|$. Vi kan finne et gitter $\Lambda \subset \mathbb{C}$ slik at $E \cong E_\Lambda$, og dermed en gruppeisomorfi $E \cong \mathbb{C}/\Lambda$. Det holder dermed å vise at antall punkter P i $\mathbb{C}/\Lambda$ slik at $nP = 0$ er n^2.

La ω_1, ω_2 være to generatorer for Λ. Da har vi at $nP = 0$ hvis og bare hvis P kan representeres av et punkt $z \in \mathbb{C}$ slik at det finnes $j, k \in \mathbb{Z}$ slik at $nz = j\omega_1 + k\omega_2$.

Dette er hvis og bare hvis det finnes $j, k \in \mathbb{Z}$ slik at $z = j\frac{\omega_1}{n} + k\frac{\omega_2}{n}$. Det følger at mengden punkter $P \in \mathbb{C}/\Lambda$ slik at $nP = 0$ er

$$\{a\frac{\omega_1}{n} + b\frac{\omega_2}{n} \mid 0 \leq a, b \leq n-1\} \subset \mathbb{C}/\Lambda,$$

som har kardinalitet n^2.

7.3: Siden avbildningen $\phi\colon \mathbb{C}/\Lambda \to E_\Lambda$ gitt av

$$\phi(z) = [\wp(z) : \wp'(z) : 1]$$

er en gruppeisomorfi, så er

$$\phi(z_1 + z_2) = [\wp(z_1 + z_2) : \wp'(z_1 + z_2) : 1] = [\wp(z_1) : \wp'(z_1) : 1] + [\wp(z_2) : \wp'(z_2) : 1],$$

hvor addisjonen på høyre side er addisjon av punkter på E_Λ.

Vi har lyst til å bruke Teorem 4.36, som sier at hvis E er en kurve på Weierstrass-form $y^2 = x^3 + Ax + B$, så er

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

med

$$x_3 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_2, \tag{7}$$

forutsatt at $x_1 \neq x_2$.

Vi må være litt forsiktige, siden kurven E_Λ er gitt ved

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

og dermed (pga. 4-tallet) ikke er på vår Weierstrass-form. Vi kan i stedet definere kurven $E'_\Lambda \subset \mathbb{P}^2$ ved

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

Vi har en isomorfi $\psi\colon E_\Lambda \to E'_\Lambda$ gitt ved

$$\psi(x, y) = (x, \frac{y}{2}),$$

hvor $\psi^{-1}(x, y) = (x, 2y)$.

Avbildningen $\psi \circ \phi\colon \mathbb{C}/\Lambda \to E'_\Lambda$ er en gruppeisomorfi siden ψ og ϕ er det, og er konkret gitt ved

$$(\psi \circ \phi)(z) = \left[\wp(z) : \frac{\wp'(z)}{2} : 1\right].$$

Bruker vi nå (7), får vi at

$$\wp(z_1 + z_2) = \left(\frac{\wp'(z_1)/2 - \wp'(z_2)/2}{\wp(z_1) - \wp(z_2)}\right)^2 - \wp(z_1) - \wp(z_2).$$

KAPITTEL 11

Noen gamle oppgaver

Disse oppgavene dreier seg om de første delene av pensum – jeg vil anbefale å se mer på oppgavene i Kapittel 8 i første omgang.

Kapittel 2 – Varieteter

1. Uke 15.2-21.2, Kap. 1.1-1.2. i [Sil09]

Fra Silverman, oppgaver 1.1, 1.2 og 1.3 (men se [**EO**] side 137–141 for en grundigere gjennomgang av påstanden i 1.3).

Noen oppgaver om varieteter definert over K og K-rasjonale punkter.

(1) Beskriv de K-rasjonale punktene $V(K)$ til varieteten $V \subset \mathbb{A}^2$ definert av idealet $I = (x^2 - 2y^2)$ når K er $\mathbb{Q}$ og når $K = \mathbb{Q}(\sqrt{2})$.

(2) La $V \subset \mathbb{A}^n$ være en algebraisk mengde. Vi har definert $I(V/K) = I(V) \cap K[X_1, \ldots, X_n]$. Vis at V er definert over K hvis og bare hvis $I(V)$ er idealet i $\overline{K}[X_1, \ldots, X_n]$ generert av mengden $I(V/K)$. (Dette er Remark 1.2. i [**Sil09**].)

(3) Vis at hvis $V \subset \mathbb{A}^n$ er en affin varietet definert over K, så er $I(V/K)$ er primideal av $K[X_1, \ldots, X_n]$.

(4) Gi et eksempel på en algebraisk mengde $V \subset \mathbb{A}^1$, definert over K, slik at $I(V/K)$ er et primideal i $K[X_1, \ldots, X_n]$, men slik at $I(V)$ ikke er et primideal i $\overline{K}[X_1, \ldots, X_n]$. (Med andre ord: For å sjekke at V er en varietet holder det ikke å sjekke at $I(V/K)$ er prim.)

(5) For $K = \mathbb{R}, \mathbb{Q}$ eller $\mathbb{F}_p$, gi eksempler på en ikketom algebraisk mengde $V \subset \mathbb{A}^1$ slik at $V(K) = \varnothing$.

(6) Vis at hvis K ikke er algebraisk lukket, så finnes en ikketom algebraisk mengde $V \subset \mathbb{A}^1$ such that $V(K) = \varnothing$.

(7) For $K = \mathbb{R}$, gi et eksempel på en ikketom affin varietet V slik at $V(K) = \varnothing$.

(8) For $K = \mathbb{F}_7$, bevis at den algebraiske mengden $V(X^3 + Y^3 - 3) \subset \mathbb{A}^2$ er en varietet og $V(K) = \varnothing$.

(9) (*) Vår definisjon av når en algebraisk mengde $V \subset \mathbb{A}^n$ er definert over K er en betingelse på idealet $I(V)$. Det viser seg at dette også kan formuleres som en betingelse på punktene til V, på følgende måte.

La $G = \mathrm{Gal}_{\overline{K}/K}$, Galois-gruppa til $\overline{K}$ over K, altså gruppa av kroppisomorfier $\sigma\colon \overline{K} \to \overline{K}$ slik at for alle $x \in K$, så $\sigma(x) = x$. Gruppa G virker på punktene til $\mathbb{A}^n$ koordinatvis

$$(\sigma, (x_1, \ldots, x_n)) \mapsto (\sigma(x_1), \ldots, \sigma(x_n)).$$

La nå $V \subset \mathbb{A}^n$ være en algebraisk mengde. Da er V definert over K hvis og bare hvis G-virkningen sender V til V, dvs. "for alle $\sigma \in G$ og $P \in V$, har vi $\sigma(P) \in V$".

For eksempel, hvis $K = \mathbb{R}$, så er G gruppa med to elementer, og det ikke-trivielle elementet virker på $\mathbb{C}$ ved komplekskonjugering $z \mapsto \bar{z}$. Dermed er en algebraisk mengde $V \subset \mathbb{A}^n$ definert over K hvis og bare hvis for alle $(x_1, \ldots, x_n) \in V$, har vi $(\bar{x}_1, \ldots, \bar{x}_n) \in V$.

La $V \subset \mathbb{A}^n$ være en algebraisk mengde.

- Vis at hvis V er definert over K, så vil G-virkningen sende V til V.
- La $K = \mathbb{R}$, og vis at hvis G-virkningen sender V til V, så er V definert over K.
- (**) La K være vilkårlig, og vis at hvis G-virkningen sender V til V, så er V definert over K. Du blir nødt til å bruke antagelsen at K er perfekt.

Kapittel 3 – Kurver

Fra [**Sil09**]: 1.6, 1.7, 1.8, 2.2, 2.3 a) i).

I 1.8, ta gjerne $q = p$ for et primtall p for enkelhets skyld. I punkt d) trenger man å vite at et element $x \in \overline{\mathbb{F}}_q$ ligger i $\mathbb{F}_q$ hvis og bare hvis $x^q = x$.

(1) La C være en ikkesingulær kurve, og la $P \in C$. Vis at hvis $f \in \overline{K}[C]_P$ er slik at $\dim_{\overline{K}} \overline{K}[C]_P/(f) = 1$, så er f en lokal parameter for C i P.

(2) La C være en ikkesingulær kurve, og la $P \in C$. Vis at hvis $f \in \overline{K}[C]_P$, så er
$$\mathrm{ord}_P(f) = \dim_{\overline{K}} \overline{K}[C]_P/(f).$$

Lokale parametere til plane kurver. For en plan kurve C, er det ofte lett å sjekke om en funksjon f er en lokal parameter i ett punkt:

(1) For $P = (a, b) \in \mathbb{A}^2$, la $T_{\mathbb{A}^2,P} = \overline{K}^2$, vi kaller dette tangentrommet til $\mathbb{A}^2$ i P. La $C \subset \mathbb{A}^2$ være kurven definert av ligningen $f \in \overline{K}[x, y]$, og anta at $P \in C$. Tangentrommet til C i P er vektorrommet
$$T_{C,P} = \{(\alpha, \beta) \in T_{\mathbb{A}^2,P} \mid \alpha \frac{\partial}{\partial x}(f(a, b)) + \beta \frac{\partial}{\partial y}(f(a, b)) = 0\} \subset T_{\mathbb{A}^2,P}.$$
Vis at C er ikkesingulær hvis og bare hvis $\dim_{\overline{K}} T_{C,P} = 1$.

(2) La $f, g \in \overline{K}[x, y]$, og la $C = V_f$, $D = V_g$. La $P = (a, b) \in C \cap D$. Vi sier at C og D er *transverse* i P hvis $\dim_{\overline{K}} T_{C,P} \cap T_{D,P} = 0$.

- Anta at
$$(\overline{K}[x, y]/(f, g))_{(x-a,y-b)} \cong \overline{K},$$
og vis at
$$(x - a, y - b)^2 + (f, g) = (x - a, y - b) \subset \overline{K}[x, y].$$
Bruk dette til å vise at C og D transverse i P.
- (*) Vis det motsatte av påstanden over: At hvis C og D er transverse i P, så er
$$(\overline{K}[x, y]/(f, g))_{(x-a,y-b)} \cong \overline{K}.$$

Du vil trenge Nakayamas lemma fra kommutativ algebra.

(3) Vis at hvis $C \subset \mathbb{A}^2$ er en ikkesingulær kurve, og $f \in \overline{K}[x,y]$, så er f en lokal parameter for C i P hvis og bare hvis

- $f(P) = 0$
- $\frac{\partial}{\partial x}(f(a,b)) + \beta\frac{\partial}{\partial y}(f(a,b)) \neq 0$ når $0 \neq (\alpha,\beta) \in T_{C,P}$.

(4) La $a_1, \ldots, a_n \in \overline{K}$. Sjekk at kurven $C \in \mathbb{A}^2$ definert av

$$y^2 = (x-a_1)(x-a_2)\cdots(x-a_n)$$

er ikkesingulær hvis og bare hvis alle a_i er distinkte.

(5) For kurven over, med a_i distinkte, sjekk at y er en lokal parameter i punktet $(a_i, 0)$

(6) For kurven over, med a_i distinkte, sjekk at $x - a_i$ *ikke* er en lokal parameter i punktet $(a_i, 0)$ (og beregn $\mathrm{ord}_{(a_i,0)}(x)$).

(7) Hvis $C \in \mathbb{A}^2$ er en ikkesingulær kurve og $P = (a,b) \in C$, vis at funksjonen $\alpha(x-a) + \beta(x-b)$ er en lokal parameter for C i P så lenge $(\beta,\alpha) \notin T_{C,P}$ (dvs: De *fleste* lineære funksjoner som forsvinner i P er lokale parametere).

Morfier av ikkesingulære kurver.

(1) Vi vet, men har ikke bevist, at en morfi av kurver $\phi\colon C \to D$ er enten surjektiv eller konstant. Her finner vi et delvis bevis, gitt følgende antakelse: Anta at for ethvert punkt $P \in D$, så finnes en $g \in \overline{K}(D)$ slik at g har en pol i P og er regulær i alle andre punkter (dette er ikketrivielt, men sant!). Bruk dette til å vise at ϕ er surjektiv ved å se på morfien $\phi_g \circ \phi\colon C \to \mathbb{P}^1$ og bruke at en morfi $C \to \mathbb{P}^1$ er konstant eller surjektiv (som vi viste i forelesning).

Hvis $\phi\colon C \to D$ er en morfi av ikkesingulære kurver, har vi definert ramifikasjonsindeksen til ϕ i $P \in C$, med notasjon $e_\phi(P)$. Når $D = \mathbb{P}^1$, kan vi tenke på morfien som en rasjonal funksjon, og se at dette

(1) La $C = D = \mathbb{P}^1$, og la $\phi = [f : 1]$, med $f \in \overline{K}(\mathbb{P}^1) = \overline{K}(x)$. Skriv $f = \prod_{i=1}^{r}(x-a_i)^{n_i}$ med distinkte a_i, og vis at

$$e_\phi([a_i : 1]) = \mathrm{ord}_{[a_i:1]}(f) = |n_i|.$$

(2) La $C = D = \mathbb{P}^1$, og la $\phi = [f : 1]$, med $f \in \overline{K}(\mathbb{P}^1) = \overline{K}(x)$. Vis at hvis f er definert i P og $f(P) = a$, så er

$$e_\phi(P) = \mathrm{ord}_P(f - a).$$

(3) La C være en ikkesingulær kurve, la $D = \mathbb{P}^1$, og la $\phi\colon C \to D$ være en morfi med $\phi = [f : 1]$ for en $f \in \overline{K}(C)$. La P være slik at f er definert i P, og la $a = f(P)$. Vis at $e_\phi(P) = \mathrm{ord}_P(f - a)$.

(4) La $\phi = [f : 1]\colon \mathbb{P}^1 \to \mathbb{P}^1$ være en morfi med $f \in \overline{K}(\mathbb{P}^1) = \overline{K}(x)$. Skriv $f = g/h$ med $g, h \in \overline{K}[x]$, og anta at g og h ikke har noen felles faktor. Vis at for alle $P \in \mathbb{P}^1$ har vi

$$\sum_{Q \in \phi^{-1}(P)} e_\phi(Q) = \max\{\deg g, \deg h\}.$$

Vis at

$$[\overline{K}(x) : \overline{K}(f)] = \max\{\deg g, \deg h\}.$$

Bibliografi

[EO] Geir Ellingsrud and John Christian Ottem. *MAT4210 - Algebraic Geometry*. PDF.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Number 106 in Graduate texts in mathematics. Springer, New York, NY, 2nd ed edition, 2009.