# Bacheloroppgave

Jørgen

28. mars 2019

## Innhold

# 1 Algebra

**Teorem 1.1.** *Sylow: La $G$ være en endelig gruppe og $p$ være et primtall. Dersom $p^m$ deler $|G|$ har $G$ en undergruppe av orden $p^m$. [1]*

**Teorem 1.2.** *Fundamentalteoremet av endeliggenererte abelske grupper: La $A$ være en endelig-generert abelsk gruppe. Da kan $A$ dekomponeres som en direktesum av et endelig anatall sykliske grupper $C_i$.*

$$A = C_1 \oplus \dots C_k$$

*For bevis, se [1]*

**Teorem 1.3.** *La $A$ være en endelig abelsk gruppe. Da finnes det en unik liste heltall $m_1, \dots m_k$ (alle større enn 1), slik at $|A| = m_1 \dots m_2$, og $A \cong \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_k}$*

*For bevis, se [1](3.1)*

**Definisjon 1.4.** La $K[X]$ være et integritetsområde over potensielt flere variable. Da er kvotientkroppen en utvidelse av $K[X]$ som danner en kropp med elementene

$$\{(f,g) \mid f,g \in K[X], g \neq 0\}$$

Med følgende ekvivalensrelasjon $(f,g) \sim (f',g') \Leftrightarrow fg' = sf'g$ for en $s \in K[X]$

Vi skriver ofte elementene $(f,g)$ som $\frac{f}{g}$

**Definisjon 1.5.** La $G$ være en gruppe, og $a, b \in G$ være to elementer i gruppa. Vi sier at $a$ og $b$ er lineart uavhengige dersom $[n]a + [m]b = e \Rightarrow n = m = 0$ for $n, m \in \mathbb{Z}$.

Der $[n]a = \underbrace{a * \dots * a}_{n \text{ ganger}}$, og $[0]a = e$

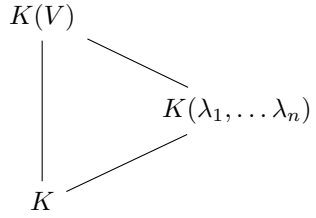
**Definisjon 1.6.** La $E$ være en kroppsutvidelse av $F$. Et element $\alpha \in E$ er **algebraisk** over $F$ dersom det finnes elementer $a_0, \dots a_n$ i $F$ (ikke alle lik 0), slik at

$$a_0 + a_1\alpha + \dots a_n\alpha^n = 0$$

**Definisjon 1.7.** La $E$ være en kroppsutvidelse av $F$. Vi sier at $E$ er en **transcendental utvidelse** dersom det finnes et element $x \in E$ som ikke er algebraisk i $F$.

**Definisjon 1.8.** La $E$ være en kroppsutvidelse av $F$ som konstrueres av elementene $x_1, \dots, x_n$. Altså er $E = F(x_1, \dots, x_n)$. Da er **graden** til $E$ lik antall elementer, $grad(E) = n$.

Litt mer galoaisteori, så kan grafen under forklares



**Eksempel 1.9.** Polynomet $f(x,y) = y^2 - x^3 - Ax - B$ er irredusibelt over $\overline{\mathbb{F}}_p$.

*Bevis.* Annta ad absurdum at $f(x,y)$ kan faktoriseres. Da må begge faktoriseringen være på formen $(y + f(x))(y + g(x))$ for polynomer $f, g \in \overline{\mathbb{F}}_p[X]$. Da har vi altså at $y^2 + y(f(x) + g(x)) + f(x)g(x) = y^2 - x^3 - ax - b$. Det gir oss to ligninger: $f(x) + g(x) = 0$ og $f(x)g(x) = x^3 - ax - b$. Altså er $f(x) = -g(x)$. Dette gir oss $f(x)g(x) = -f(x)^2$, men $deg(f(x)^2) = 2 * deg(f(x)$, altså har polynomet en partallsgrad, så vi kan aldri få et odde polynom ut. Dette er en motsigelse siden vi vil ha et polynom på formen $x^3 - ax - b$. Dermed har vi vist at $f(x,y)$ er irredusibelt. □

**TODO:** Noe er feil i beviset, jeg har ikke anntatt noe om kroppen, altså finnes det ingen algebraisk utvidelse?

# 2 Elliptiske kurver

## 2.1 Algebraisk geometri

**TODO: Idealet er primisk, funksjonen som genererer idealet er irredusibelt**

Overordnet ønsker vi å se nærmere på elliptiske kurver og spessielt avbildinger mellom disse. For å kunne bruke presis terminologi må vi gå via algebraisk geometri. Dette kapittelet kommer derfor først til å innføre noen grunnleggende begreper før vi ser nærmere på hva en elliptisk kurve er. Om du allerede har god kontroll på elliptiske kurver, og kan du fint hoppe over dette kapittelet.

Vi starter med det aller enkleste. Dette er i praksis bare en formalisering av mengden av alle punkter over n dimensjoner.

**Definisjon 2.1.** Et **affint n-rom**, $\mathbb{A}^n$ er alle $n$-tupler over en kropp

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{P = (x_1, \ldots, x_n) \in \overline{K}^n\}$$

Problemet er bare at den ikke har nok elementer. Vi er ofte interessert i såkalte punkter i uendeligheten, og da må vi introdusere en ekstra variabel, samt sette noen begrensninger på elementene i rommet

Et projektivt rom har en litt mer komplisert definisjon som baserer seg på ekvivalensklasser. Her sier vi at to (n+1)-tupler $(x_0, \ldots, x_n)$ og $(y_0, \ldots, y_n)$ er ekvivalente dersom det finnes et element $\lambda \in \overline{K}^*$ slik at $(\lambda x_0, \ldots, \lambda x_n) = (y_0, \ldots, y_n)$.

Denne ekvivalensklassen skriver vi som $[x_0, \ldots, x_n]$

**Definisjon 2.2.** Et **projektivt n-rom** $\mathbb{P}^n$ over $K$ består av ekvivalensklasser til $(n+1)$-tupler der minst én komponent er ikke-null

$$\mathbb{P}^n = \mathbb{P}^n(\overline{K}) = \{[x_0, \ldots, x_n] | (x_0, \ldots, x_n) \in \mathbb{A}^{n+1}(\overline{K}) \setminus \{(0, \ldots, 0)\}\}$$

**Definisjon 2.3.** La $\mathbb{P}^n(\overline{K})$ være et projektivt n-rom. Da er de $K-$**rasjonale punktene**, $\mathbb{P}^n(K)$, en delmengde av $\mathbb{P}^n(\overline{K})$ der restklassene defineres fra punkter med elementer i $K$.

$$\mathbb{P}^n(K) = \{[x_0, \ldots, x_n] \mid x_i \in K\}$$

**Eksempel 2.4.** $\mathbb{P}^2(\mathbb{F}_p) = \{[\lambda x_0, \ldots, \lambda x_n] \mid x_i \in \mathbb{F}_p, \lambda \in \overline{\mathbb{F}_p}\}$, altså de $\mathbb{F}_p$ rasjonelle punktene i $\mathbb{P}^2(\overline{\mathbb{F}_p})$. Legg merke til at de individuelle punktene, $\lambda x_i$ ligger i $\overline{\mathbb{F}_p}$, men siden alle har samme faktor fra $\overline{\mathbb{F}_p}$ kan vi hente ut elementer i $\mathbb{F}_p$ ved å dele to elementer på hverandre, $\frac{\lambda x_i}{\lambda x_j} = \frac{x_i}{x_j} \in \mathbb{F}_p$

Senere skal vi snakke om elliptiske kurver, og det er i praksis bare en delmengde av disse punktene/ekvivalensklassene, noe som er bakgrunnen for neste definisjon.

**Definisjon 2.5.** Le $I$ være et ideal i $\overline{K}[x_0, \ldots, x_n]$. Vi sier at en **projektiv algebraisk mengde** $V_I \subset \mathbb{P}^n$ er alle punktene som evalueres til null ved alle homogene polynomer i idealet $I$.

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

Affine algebraiske mengder defineres på en tilsvarende måte, bare uten kravet om homogene polynomer.

**Eksempel 2.6.** Polynomet $f(X, Y, Z) = ZY^2 - X^3 - Z^2X \in \overline{\mathbb{F}_p}[X, Y, Z]$ genererer idealet $I = \langle f \rangle \subset \overline{F_p}[X, Y, Z]$. Da blir den projektive algebraiske mengden $V_I$ ekvivalensklassene til nullpunktene til $f(X, Y, Z)$. Altså vil blant annet $[0, 1, ]$ være i $V_I$ siden $f(0, 1, 0) = 0$.

Legg merke til hvordan vi evaluerer polynomet $f$. Siden $f(x, y, z) = 0$ for en representant for ekvivalensklassen vet vi at den også er 0 for alle andre representanter. $f(\lambda x, \lambda y, \lambda z) = \lambda^3 y^2 z - \lambda^3 x^3 - \lambda^3 x z^2 = \lambda^3(y^2 z - x^3 - x z^2)$ noe som er 0 hvis og bare hvis $(y^2 z - x^3 - x z^2)$ (så fremt karakteristikken ikke er 3).

Tilsvarende kan vi definere idealet til en en algebraisk mengde basert på punktene den inneholder.

**Definisjon 2.7.** La $V$ være en algebraisk mengde. Da er **Idealet til** $V$, $I(V)$ idealet generert av alle polynomene som evalueres til 0 i hele $V$

$$I(V) = \langle \{f \in \overline{K}[x_1, \ldots, x_n] | f(P) = 0, \forall P \in V\} \rangle$$

**Proposisjon 2.8.** *Idealet er entydig bestemt av den algebraiske mengden.*

*Bevis.* La $I$ og $I'$ er to idealer til samme algebraiske mengde $V$. Annta at $I$ og $I'$ er ulike. Da har vi at det finnes et polynom $g \in I$ slik at $g(P) = 0$ for alle $P \in V$. Men da er også $g$ per definisjon i $I'$, altså har vi en motsigelse, og dermed vet vi at alle polynomer eksisterer i begge ideal. □

## 2.2 Planet

**Definisjon 2.9.** Et **projektivt plan** er alle ikke-null tripler $[x, y, z]$ i det projektive 2-rommet $\mathbb{P}^2$

**Definisjon 2.10.** La $I$ være et ideal generert av et homogent polynom i $\overline{K}[x, y, z]$ med koefisienter i $K$. Da sier vi at den projektive algebraiske mengden $V_I$ er en **kurve** i det projektive planet, og vi skriver i stedet $C/K$ for å indikere at det er en kurve med koefisienter i $K$.

**Definisjon 2.11.** La $C/K$ være en kurve. Da er de **$K'$-rasjonale punktene**, $C(K')$, alle punktene som kommer fra representanter i $K'$.

$$C(K') = \{[x, y, z] \in C/K \mid (x, y, z) \in K'\}$$

Merk at dette kun gjelder dersom $K'$ er en utvidelse av $K$.

**Eksempel 2.12.**

$$f(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3 \in \overline{\mathbb{F}}_p \text{ med } p \geq 5 \tag{1}$$

Der $a, b \in \mathbb{F}_p$ er et slikt homogent polynom. Den algebraiske mengden $V_I$ der idealet $I$ er generert av $f(x, y, z)$ er derfor en projektiv kurve $C/\mathbb{F}_p$.

**Definisjon 2.13.** La $V$ være en algebraisk mengde, og $I(V)$ være idealet til $V$. Da er $V$ en **algebraisk varietet** (enten projektiv eller affin) hvis $I(V)$ er irredusibelt i $\overline{K}[x_0, \ldots, x_n]$

En interessant egenskap ved varieteter er at det finnes en naturlig måte å gå mellom projektive og affine varieteter. La oss se på to avbildnger. Først definer inklusjonsavbildingen $\phi : \mathbb{A}^n \to \mathbb{P}^n$, $(x_1, \ldots, x_n) \mapsto [x_1, \ldots, x_{i-1}, 1, x_i, \ldots, x_n]$ Tilsvarende kan vi lage oss projeksjonsavbildingen: $\phi_i^{-1} : \mathbb{P}^n \to \mathbb{A}^n$, $[x_0, \ldots, x_n] \mapsto (\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i})$, legg merke til hvordan denne er veldefinert ved at alle representanter for en ekvivalensklasse reduseres til samme representant.

**Definisjon 2.14.** La $V_I$ være an affin varietet. Vi sier at den **projektive lukkingen** av $V_I$, $\overline{V_I}$, er den projektive varieteten vi får fra inkludsjonsavbildingen, $\phi_i$ (for én $i$), Der idealet blir den homogeniserte versjonen av $I$, altså $\overline{I} = \{f^* \mid f \in I\}$

**Proposisjon 2.15.** *La $I$ være et primisk ideal i $K[x, y]$ da vil $\overline{I}$ være et primisk ideal i $k[x, y, z]$.*

*Bevis.* Fulton 4.4 Projective and affine varieties □

Konsekvensen av proposisjonen over er at dersom vi har en varietet i det affine rommet, så vil den projektive lukkingen også være en varietet. Altså er definisjonen berettiget.

**Proposisjon 2.16.** *La $V$ være en affin varietet og $\overline{V}$ være en projektiv varietet slik at $V = \overline{V} \cap \mathbb{A}^n$ (Med $\overline{V} \cap \mathbb{A}^n$ mener vi projeksjonsavbildingen, $\pi_i$ for en fiksert i fra $\overline{V}$ foruten de ekvivalensklassene som har $x_i = 0$). Da vil alle affine varieteter identifiseres med en unik projektiv varietet.* ***Finn et bedre bevis for dette [111] I2.3 sier ikke dette***

**Eksempel 2.17.** La $f(x, y)$ være kurven definert i eksempel 1.9. Siden dette danner en affin varietet vil den også danne en projektiv varietet dersom vi homogeniserer polynomet til en av samme type som eksempel 2.12. Altså har vi at kurven definert i eksempel 2.12 er en projektiv varietet.

**Definisjon 2.18.** La $C/K$ være en kurve. Vi sier at $C/K$ er **singuær** i et punkt $P \in C(K)$ dersom $\frac{\delta f}{\delta x} = \frac{\delta f}{\delta y} = \frac{\delta f}{\delta z} = 0$ når de evalueres i punktet $P$

Hvis kurven $C/K$ ikke har noen singulære punkter sier vi at den er **glatt** (eller ikke-singulær).

**Eksempel 2.19.** La $f(x, y, z)$ være kurven definert i 1 med karakteristikk $p > 3$. La oss prøve å finne de singulære punktene. De partiellderiverte til polynomet er henholdsvis $3X^2 - aZ^2$, $2YZ$ og $Y^2 - 2aX - 3bZ^2$. De singulære punktene er når disse tre evalueres til null. Da må $Y = 0$ eller $Z = 0$. Dersom $Z = 0$ får vi $3X^2 = 0$ som gir $X = 0$ som igjen gir $Y^2 = 0$, altså er punktet $[0, 0, 0]$, men den er ikke i det projektive rommet så $Z = 0$ gir ingen singulære punkter.

Dersom vi ser på $Y = 0$, og bruker at punktene også må ligge på kurven, altså $Y^2Z - aX^3 - aXZ^2 - bZ^3 = 0$ (med $Y = 0$) får vi (etter en del regning) at $4a^3 - 27b^2 = 0$. Med andre ord, dersom idealet til kurven er generert av polynomer der $4a^3 - 27b^2 \neq 0$, så vil kurven være glatt.

**Definisjon 2.20.** La $C/K$ være en kurve i det projektive planen. Vi sier at $C/K$ er en **Elliptisk kurve** dersom den er glatt. Vi kommer til å bruke notasjonen $E/K$ for å vise til en slik kurve.

**Eksempel 2.21.** Kurven fra eksempel 2.12 er en elliptisk kurve dersom ligningen $4a^3 - 27b^2 \neq 0$ (se eksempel 2.19. Legg merke til hvordan denne minner mye om diskriminanten, $\Delta = 16(4a^3 - 27b^2)$.

Siden vi nå vet at en projektiv varietet samsvarer med en affin varietet kommer vi til å bruke den lettere notasjonen, og de forenklede eksemplene ved affine varieteter framover. Så når vi snakker om kurven $f(x, y) = y^2 - x^3 - ax - b$ så mener vi egentlig den homogeniserte $f(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$.

**TODO: Sannsynligvis kan vi fjerne de to definisjonene nedenfor**

**Definisjon 2.22.** La $V$ være en affin varietet. **Dimensjonen**, $dim(V)$, er graden til den største transcendentale kroppsutvidelsen som har $K(V)$ som sin algebraiske kroppsutvidelse.

**Definisjon 2.23.** Dimensjonen til en projektiv varietet er dimensjonen til den tilsvarende affine varieteten, nemlig $V \cap \mathbb{A}^n$.

## 2.3 Gruppestruktur

Vi har allerede definert elliptiske kurver som en varietet. I denne seksjonen skal vi vise at den også danner en abelsk gruppe under en spesifikk operasjon og noen viktige konsekvenser av det.

Aller først må vi introdusere noen flere geometriske begreper så vi kan definere selve operasjonen.

**Definisjon 2.24.** La $V/K$ være en varietet i det projektive rommet. Vi ser at $V/K$ er en **linje** dersom idealet er generert av et polynom av grad én, altså $f(X,Y,Z) = aX + bY + cZ$ for $a, b, c \in K$.

**Proposisjon 2.25.** *To unike punkter, $P_1$, $P_2$ i det projektive planet danner en unik linje.*

*Bevis.* La $P_1 = [x, y, z]$ og $P_2 = [x', y', z']$. En linje $L$ gjennom $P_1$ og $P_2$ der $f(X,Y,Z)$ er polynomet som genererer idealet. Da vil naturligvis $f(P_1) = f(P_2) =$, altså har vi $ax + by + cz = 0$ og $ax' + by' + cz' = 0$. Med vanlig lineær algebra kan vi skrive dette som

$$\begin{bmatrix} x & y & z \\ x' & y' & z \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

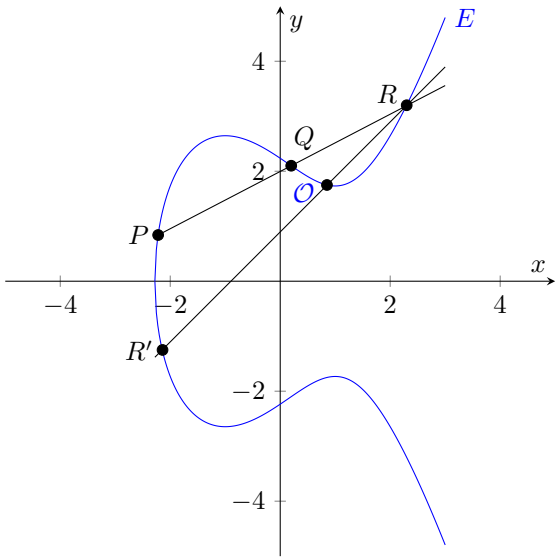
Siden $P_1$ og $P_2$ er ulike vil de to radene i den første matrisen være lineært uavhengige - altså har vi at $a, b, c$ er en unik løsning opp til skalarmultiplikasjon. Men siden vi jobber i det projektive planet vil $(a, b, c)$ og $(\lambda a, \lambda b, \lambda c)$ være samme punkt, så $(a, b, c)$ danner en unik linje $ax + by, cz$ i $\mathbb{P}^2$. **TODO: Bevis dette annerledes! - dette er sannsynligvis feil** □

**Definisjon 2.26.** La $V_1/K$ og $V_2/K$ være to varieteter. Vi sier at $P$ er et **skjæringspunkt** dersom $P \in V_1 \cap V_2$, altså ligger punktet i begge varietetene. Vi kommer i denne teksten til å skrive $V_1 \circ V_2$ for å betegne mengden av alle skjæringspunkter mellom varietetene.

Multiplisiteten til et skjæringspunkt er en relativt komplisert affære, og kunne fint fått sin egen seksjon i denne teksten. Men siden vi ikke kommer til å bruke det til noe annet enn for å bevise at en elliptisk kurve er en gruppe benytter vi oss av et av resultatene fra en mer generell beskrivelse. Her er blant annet kravet at $P$ er ikke-singulær, men siden $E$ er en elliptisk kurve får vi dette gratis. For mer informasjon om multiplisitet til skjæringspunkt kan du lese [3, s. 3.3]

**Definisjon 2.27.** La $P$ være et skjæringspunkt mellom en elliptisk kurve $E$ og en varietet $V$. Vi sier at **multiplisiteten** til punktet er $ord_p^E(V)$.

**Teorem 2.28.** ***Bézouts teorem*** *La $E/K$ være en elliptisk kurve, og $L$ en linje - begge i det projektive planet. Da vil Linjen og kurven skjære hverandre i nøyaktig tre punkter dersom vi teller multiplisiteten til punktene. [3, s. 5.3]*




Figur 1: Addisjon med baseelement $\mathcal{O}$

Merk, teoremet er mye mer generelt enn dette, men til våre formål er det dette som er essensielt.

**Skjæringspunkter**. La $C/K$ være en kurve som også er en varietet (tenk elliptisk kurve). Dersom vi tar to vilkårlige punkter $P, Q \in C$ får vi en unik linje, $L$, gjennom disse to punktene. Fra Bézouts teorem vet vi at denne linjen skjærer kurven i tre punkter. $L \circ C = \{P, Q, R\}$ for en $R \in C$. I spesialtilfellet der $P = Q$ setter vi linjen til å være tangentlinjen til $P$. Vi definerer nå avbildingen $\phi : C \times C \to C$ $(P, Q) \mapsto R$. Legg merke til at uansett hvilke to punkter du tar fra mengden av skjæringspunkter vil du alltid få den tredje. Dersom $L \circ C = \{P, Q, R\}$ vil $\phi(P, Q) = R$ og $\phi(P, R) = Q$ og $\phi(Q, R) = P$.

**Teorem 2.29.** *En elliptisk kurve $E/K$ sammen med et baseelement $\mathcal{O} \in E$ danner en abelsk gruppe under operasjonen $P + Q = \phi(\mathcal{O}, \phi(P, Q))$, der $\phi$ er definert som over.*

*Bevis.* Vi må vise at $E$ er en gruppe og at den er abelsk, altså at den er assosiativ, har identitetselement, at alle punkter har en invers, og at den er kommutativ. La $P, Q, R \in E$, med $\mathcal{O}$ som baseelement.

**Assosiativitet** Skal vise at $(P + Q) + R = P + (Q + R)$. La oss først definere noen punkter: $\phi(P, Q) = S'$, $\phi(\mathcal{O}, S') = S$, $\phi(S, R) = T'$, $\phi(Q, R) = U'$, $\phi(\mathcal{O}, U') = U$, $\phi(P, U) = T''$. Da har vi $(P + Q) + R) = \phi(\mathcal{O}, T')$ og $P + (Q + R) = \phi(\mathcal{O}, T'')$. Altså er det nok å vise at $T' = T''$.

Fra punktene over kan vi lage linjer som går gjennom punktene: $L_1 : \{P, Q, S'\}$, $M_1 : \{\mathcal{O}, S', S\}$, $L_2 : \{S, R, T'\}$, $M_2 : \{Q, R, U'\}$, $L_3 : \{\mathcal{O}, U', U\}$,

$M_3 : \{P, U, T''\}$ (Her er f.eks. $L_1$ linjen som går gjennom $P, Q, S'$ - det er der den skjærer $E$).

Vi kan nå sette sammen disse linjene ved enkel multiplikasjon. Husk at graden til hver linje er 1, så $L = L_1 * L_2 * L_3$ har grad 3 og er en kubisk kurve (ikke nødvendigvis irredusibel). Tilsvarende er $M = M_1 * M_2 * M_3$.

La oss nå se på skjæringspunktene mellom disse linjene og kurven $E$. $E \circ L = \{P, Q, S', S, R, \mathcal{O}, U', U, T'\}$, mens $E \circ M = \{\mathcal{O}, S', S, Q, R, U', P, U, T''\}$. Legg merke til at den eneste forskjellen er $T'$ og $T''$.

La oss nå lage en linje gjennom $T'$ som ikke går gjennom $T''$, Da har vi $N : \{T', W, W'\}$ for punkter $W, W' \in E$. Siden ingen av disse er i $M$ kan vi se på skjæringen mellom $N * M$ og $E$. $N * M \circ E = \{\mathcal{O}, S', S, Q, R, U', P, U, T'', T', W, W'\} = L \circ E \cup \{T'', W, W'\}$, altså finnes det en linje mellom $T'', W$ og $W'$. Denne linjen må nødvendigvis være lik $N$ da den deler to punkter, så $T' = T''$ og vi har vist at operasjonen ar assosiativ. [3, s. 5.6.4]

**Identitet** La $\phi(\mathcal{O}, P) = R$, da har vi $P + \mathcal{O} = \phi(\mathcal{O}, \phi(P, \mathcal{O})) = \phi(\mathcal{O}, R) = P$, samtidig er $\mathcal{O} + P = \phi(\mathcal{O}, \phi(P, \mathcal{O})) = \phi(\mathcal{O}, R) = P$

**Invers** La $\phi(\mathcal{O}, P) = R$, da har vi at $(P + \mathcal{O}) + R = \mathcal{O} + P + R = \mathcal{O} + \mathcal{O} = \phi(\mathcal{O}, \phi(\mathcal{O}, \mathcal{O}))$. Annta $\{\mathcal{O}, \mathcal{O}, Q\}$ ligger på samme linje ($\phi(\mathcal{O}, \mathcal{O}) = Q$), da har vi $\phi(\mathcal{O}, \phi(\mathcal{O}, \mathcal{O})) = \phi(\mathcal{O}, Q) = \mathcal{O}$.

**Kommutativitet** Siden $\phi(P, Q) = \phi(Q, P)$ da dette bare er det tredje punktet på linjen har vi $P + Q = \phi(\mathcal{O}, \phi(P, Q)) = \phi(\mathcal{O}, \phi(Q, P)) = Q + P$

□

Nå som vi vet at en elliptisk kurve danner en abelsk gruppe for et vilkårlig baseelement kan vi bestemme oss for et spesifikt. Det er vanlig å bruke punktet $[0, 1, 0]$ som baseelement/punkt i uendeligheten. Så videre i denne teksten anntar vi at $\mathcal{O} = [0, 1, 0]$ da det forenkler en del regning. Legg merke til hvordan $\phi((x, y), \mathcal{O}) = (x, -y)$ linjen mellom et punkt og $\mathcal{O}$ blir den vertikale linjen.

Dette fører til at dersom $P = (x, y)$ vil $-P = \phi(P, \mathcal{O}) = (x, -y)$.

Vi kommer til å bruke notasjonen $E(K)$ for å referere til de $K$-rasjonale punktene i $E$.

# 3 Avbildinger

## 3.1 Rasjonale avbildinger

Vi skal nå begynne å se på avbildinger mellom varieteter og etter hvert elliptiske kurver.

**Definisjon 3.1.** La $V/K$ være en varietet. Da er **koordinatringen** til $V$,

$$K[V] = K[X_0, \ldots, X_n]/I(V)$$

altså restklassen av polynomer med $n$ variable modulo $I(V)$.

**Eksempel 3.2.** La $V/\mathbb{F}_p$ være varieteten definert fra vår elliptiske kurvelikning $f(x, y)$. Da er koordinatringen på formen $\mathbb{F}_p[x, y]/\langle y^2 - x^3 - ax - b\rangle$. Altså er f.eks $y^2$ det samme som $x^3 + ax + b$ i koordinatringen.

**Definisjon 3.3.** La $V/K$ være en affine varieteten definert av idealet $f(x, y)$. Da er **funksjonskroppen**, $K(V)$, kvotientkroppen til den tilhørende koordinatringen $K[V]$.

**Definisjon 3.4.** La $V$ være en projektiv varietet definert av idealet $I = \langle f(X)\rangle$. Da er **funksjonskroppen**, $K(V)$, alle rasjonale funksjoner $g/h$ ($h \neq 0$) med følgende restriksjoner:

1. $g, h$ homogene polynomer i $K[x, y, z]$ av samme grad.
2. $h$ er ikke i idealet $I(V)$
3. $f_1/g_1$ og $f_2/g_2$ er ekvivalente dersom $f_1g_2 - f_2g_1 \in I(V)$

**TODO: vis at definisjonene er tilsvarende, og forklar hvorfor begge er med**

Vi er kun interessert i avbildinger mellom elliptiske kurver, vi kan derfor endre litt på måten vi skriver elementer i funksjonskroppen. Hver funksjon, $\phi$, er på formen $f(x, y)/g(x, y)$ for $f, g \in \overline{K}(E)$, altså i restklassen modulo idealet til et polynom på formen $y^2 - x^3 - Ax - B$. Dermed kan vi alltid erstatte $y^2$ med $x^3 - Ax - B$, så vi får at leddet med $y$ maksimalt kan ha grad 1. Dermed kan vi dele ut $y$, og vi får $f(x, y) = f_1(x) + f_2(x)y$ og $g(x, y) = g_1(x) + g_2(x)y$.

$$\phi = \frac{f_1(x) + f_2(x)y}{g_1(x) + g_2(x)y}$$

Men dette kan vi forkorte mer, vi kan multiplisere nevner og teller med $g_1(x) - g_2(x)y$ og så erstatte $y^2$ igjen, så vi sitter igjen med

$$phi = \frac{h_1(x) + h_2(x)y}{h_3(x)} \tag{2}$$

Altså kan vi alltid skrive et element i funksjonskroppen til en elliptisk kurve på denne måten.

**Definisjon 3.5.** La $V_1$ og $V_2$ være varieteter i det projektive planet, og $f_0, f_1, f_2 \in \overline{K}(V_1)$. Da er en **rasjonal avbilding** fra $V_1$ til $V_2$ en avbilding på formen

$$\phi : V_1 \to V_2,\ \phi = [f_0, f_1, f_2]$$

Der man evaluerer $\phi$ komponentvis, altså $\phi(P) = [f_0(P), f_1(P), f_2(P)]$ for alle $P \in V_1$ der $f_0, f_1 og f_2$ er definert og $P \neq 0$.

På samme måte som i seksjon 2 kan vi tenke på dette som affine varieteter mens vi i realiteten bruker projektive varieteter. Altså blir en rasjonal avbilding på formen $\phi : V_1 \to V_2, (x, y) \mapsto (f(x, y), g(x, y))$ i stedet for slik den er definert over.

**Definisjon 3.6.** La $\phi$ være en rasjonal avbilding. Vi sier at $\phi$ er **definert** i et punkt $P \in V_1$ dersom det finnes et funksjon $g \in \overline{K}(V_1)$ slik at

1. $gf_i$ er definert i punktet $P$
2. $(gf_i)(P) \neq 0$ for minst én $i$

Vi skriver så

$$\phi(P) = [(gf_0)(P), \ldots, (gf_n)(P)]$$

**Definisjon 3.7.** La $\phi : V_1 \to V_2$ være en rasjonal avbilding. Vi sier at $\phi$ er en **morfisme** hvis den er definert i alle punkt $P \in V_1$.

Vi kommer ikke til å være opptatt av å skille morfier fra rasjonale avbildinger da vi automatisk får slike morfier når vi ser på avbildinger fra en glatt projektiv kurve til en varietet, men vi må kjenne til begrepet for å vise at dette stemmer.

**Teorem 3.8.** *Dersom $C/K$ er en glatt projektiv kurve vil alle rasjonelle avbildinger fra $C/K$ til en projektiv varietet $V/K$ være morfier.*

*Bevis.* For å bevise dette må vi introdusere mange ting... **TODO: Prøv å fjerne ting som ikke er viktig**

La først $M_P = \{f \in \overline{K}(C) \mid f(P) = 0\}$

Så definerer vi ordenen til $f \in \overline{K}[C]$, $ord_P(f) = sup\{d \in \mathbb{Z} \mid f \in M_P^d\}$, det er lett å sjekke at $ord_P(f/g) = ord_P(f) - ord_P(g)$

La nå $t \in \overline{K}[C]$ være slik at $ord_P(t) = 1$ (dette kalles "Uniformizer")

La $\phi = [\phi_0, \ldots, \phi_n]$ være en vilkårlig rasjonal avbilding fra $C/K$ til $V/K$. $\phi$ er da definert i punktet $P$ hvis og bare hvis $ord_P(\phi_i) \geq 0$ for minst én $i$. **TODO: Bevis for dette - definisjon kan da ikke være nok**.

La oss nå se på alle ordenene til $\phi_i$, merk at hver funksjon er på formen $f_i/g_i \in \overline{K}(V)$, da er $ord_P(\phi_i) = ord_P(f_i) - ord_P(g_i)$, så denne kan potensielt være negativt og dermed udefinert i punktet $P$. Heldigvis kan vi multiplisere med en funksjon fra $\overline{K}(V)$, så la $n = min\{ord_P(\phi_i)\}$ da vil $ord_P(t^{-n}) = -n$ (Dette følger fra teoeremet innenfor diskre valueringsring). Hvis vi nå ser på $[t^{-n}\phi_0, \ldots, t^{-n}\phi_n]$ har vi at $ord_P(t^{-n}\phi_i) \geq 0$ for alle $i$, og $ord_p(t^{-n}\phi_j) = 0$ for minst én $j$. Altså er $\phi$ definert i punktet $P$, og tilsvarende kan gjøres for alle $P$ i $C/K$, så $\phi$ er en morfi.

**TODO: Dersom dette skal vises ordentlig må jeg gå om Diskre valueringsring - discrete valuation ring"og finne en bedre forklaring** □

**Teorem 3.9.** *La $\phi : E_1 \to E_2$ være en morfi mellom to elliptisk kurver. Da er enten $\phi$ konstant eller surjektiv.* ***MERKNAD: Vanligvis fra morfi mellom to kurver ikke nødvendigvis elliptiske kurver TODO: Finn ut, og bevis dette*** *Bevis: Se [243, I §5, theorem 4]*

*Bevis.* Først annta $E_1$ defineres av $y^2 - x^3 - Ax - B$, og $E_2$ defineres av $y^2 - x^3 - A'x - B'$ for $A, B, A', B' \in K$. Vi vet fra 2 at $\phi = (\frac{h_1(x)+h_2(x)y}{h_3(x)}, \frac{g_1(x)+g_2(x)y}{g_3(x)}$. La så $P = (a, b) \in E_2$.

Se på funksjonen $f(x) = h_1(x)+h_2(x)y-ah_3(x)$. $f$ kan da være konstant eller ikke. Annta $f$ er ikke-konstant. Da vil $f$ ha en rot, $x_0$ i $\overline{K}$, altså er $f(x_0) = 0$, og vi får $\frac{h_1(x_0)+h_2(x_0)y}{h_3(x_0)} = a$. Bruk så denne roten, $x_0$, og sett $y_0 = \sqrt{x_0^3 + Ax_0 + B}$. Da vet vi at $\phi$ er definert for $(x_0, y_0) \in E_1$, og $\phi(x_0, y_0) = (a, b')$ der $b = a^3 + A'a + B = b'$. Siden både $(a, b)$ og $(a, -b) = (a, b')$ er punkter i $E_2$ må vi vite at de begge har et prebilde. Dersom $b' = -b$ har vi også at $(x_0, -y_0) \in E_1$ og $\phi(x_o, -y_0) = (a, -b') = (a, b)$. Altså vil alle punkter i $E_2$ ha et prebilde i $E_1$.

Annta så at $f$ er konstant. **Her stemmer det ikke helt**

[6, s. II 2.1] □

**Definisjon 3.10.** Vi sier at to varieteter er isomorfe dersom det finnes en mrfi $\phi : V_1 \to V_2$ og en morfi $\psi : V_2 \to V_1$ slik at $\phi \circ \psi$ og $\psi \circ \phi$ er identitetsavbildinger på $V_2$ og $V_1$.

**TODO: Ikke-trivielt eksempel to isomorfe elliptiske kurver**

## 3.2 Isogenier

Isogenier er sentralt for protokollen vi skal studere.

Selve definisjonen av en isogeni kommer fra at vi ønsker oss en avbilding som bevarer strukturen til den elliptiske kurven som en varietet, og som en abelsk gruppe. Det finnes flere tilsvarende definisjorer, men vi kommer til å ta utgangspunkt i følgende.

**Definisjon 3.11.** La $E/K$ være en elliptisk kurve. Vi sier at en **isogeni**, $\phi$, er en morfi, $\phi : E \to E'$, som også tilfredsstiller $\phi(\mathcal{O}_E) = \mathcal{O}_{E'}$

Legg merke til at $\phi : E \to \{\mathcal{O}\}$ tilfredsstiller kravene til en isogeni. Dette kalles konstantavbildingen og er i praksis en ubrukelig isogeni. Derfor kommer vi framover til å anta at $\phi$ er ikke-konstant.

Nå som vi vet hva en isogeni er kan vi videre forkorte (2) slik at den tar hensyn til bevaring av gruppeoperasjonene. La $\phi = (\frac{f_1(x)+f_2(x)y}{f_3(x)}, \frac{g_1(x)+g_2(x)y}{g_3(x)})$. Siden $\phi(-P) = -\phi(P)$ for $P = (a, b) \in E/k$ har vi at $\frac{f_1(a)+f_2(a)(-b)}{f_3(a)} = \frac{f_1(a)+f_2(a)b}{f_3(a)}$, altså får vi $\frac{f_1(x)+f_2(x)y}{f_3(x)} = \frac{f_1(x)}{f_2(x)}$. Tilsvarende for $b$ har vi $\frac{g_1(a)+g_2(a)(-b)}{g_3(b)} = -\frac{g_1(a)+g_2(a)b}{g_3(a)}$, altså må $\frac{g_1(a)-g_2(a)b}{g_3(a)} = \frac{g_2(a)y}{g_3(a)}$. Med andre ord kan vi alltid skrive en isogeni på formen

$$\phi = (\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y) \tag{3}$$

**Definisjon 3.12.** La $\phi$ være en isogeni på den forenklede formen (3). Vi sier at **graden** til isogenien, $deg(\phi)$ er den største graden blant $u$ og $v$, altså

$$deg(\phi) = max\{deg(u), deg(v)\}$$

**Definisjon 3.13.** La $\phi : E_1 \to E_2$ være en isogeni, der $\mathcal{O} \in E_2$ er baseelementet til $E_2$. Vi sier at **kjernen**, $ker(\phi) = \{P \in E_2 \mid \phi(P) = \mathcal{O}\}$

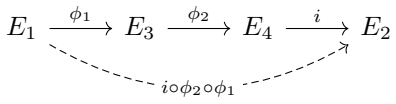
**Teorem 3.14.** *La $E$ være en elliptisk kurve og $\Phi$ være en endelig underrguppe av $E(K)$, da er det en unik elliptisk kurve $E'$ og en separabel isogeni $\phi$ der $\phi : E \to E'$ slik at $ker(\phi) = \Phi$*

*[7, s. 6.10]*

En viktig egenskap ved isogenier er at de kan dekomponeres i isogenier av lavere grad. Dette er særdeles gunstig da mengden arbeidskraft nødvendig er proposjonal med graden til isogenien.

**Korollar 3.15.** *La $\phi : E_1 \to E_2$ være en isogeni av sammensatt orden $n$. En slik isogeni kan alltid dekomponeres til en sekvens"av mindre isogenier av primtallsorden.*

*Bevis.* La $G = ker(\phi)$. Siden $G$ er en abelsk gruppe vet vi at den inneholder en undergruppe, $H \leq G$, av orden $p$ der $p$ er et primtall. Av teorem 3.14 har vi at det finnes en isogeni $\phi_1 : E_1 \to E_3$ der $ker(\phi_2) = H$. Videre vet vi at $\phi_1(G) \cong G/H$ (siden $\phi_1$ har kjerne $H$ og $\phi_1(G) \subset E_3(\overline{K})$). Med dette kan vi lage en til isogeni, $\phi_2 : E_3 \to E_4$ med kjerne $ker(\phi_2) = G/H$. Sammensetningen, $\phi_2 \circ \phi_1 : E_1 \to E_4$ er nå en isogeni med $ker(\phi_2 \circ \phi_1) = G/H \times H = G = ker(\phi)$, altså er $E_4$ og $E_2$ isomorfe. Med andre ord finnes det en isogeni av grad 1, $i : E_4 \to E_2$. Altså har vi $\phi = i \circ \phi_2 \circ \phi_1$, der $\phi_1$ har grad $p$, graden til $\phi_2$ er $n/p$, og graden til $i$ er 1. Dermed kan vi fortsette med $\phi_2$ til vi kun har primtall.




□

**Eksempel 3.16.** La $E/\mathbb{F}_q$ være en elliptisk kurve, og $\langle R \rangle \leq E(\mathbb{F}_q)$, der $|\langle R \rangle| = p^e$. Vi ønsker å lage en isogeni, $\phi$, fra $E$ med kjerne $\langle R \rangle$. Ved hjelp av korollar 3.15 har vi at $\phi = i \circ \phi_e \circ \ldots \circ \phi_1$. Der $i$ er en isomorfiavbilding. Siden vi her ikke er ute etter den spesifikke elliptiske kurven, men heller bare én vilkårlig, kan vi droppe isomorfiavbildingen.

Når vi skal beregne isogeniene $\phi_i$ gjør vi dette iterativt, og starter med $\phi_1$. Denne skal ha kjerne av grad $p$, noe vi får ved å regne ut $langlep^{e-1}R\rangle$. Altså blir $\phi_1 : E \to E/\langle p^{e-1}R \rangle = E_1$. Når vi skal beregne videre vil vi ikke nødvendigvis ha punktet $R \in E_1$, derfor må vi flytte det over med $R_1 := \phi_1(R)$. Merk at dette punktet har orden $p^{e-1}$ siden $\phi_1$ er en gruppehomomorfi med kjerne $p$. Dermed kan vi lage neste isogeni, $\phi_2 : E_1 \to E_1/\langle p^{e-2}R_1 \rangle = E_2$. Dette kan vi fortsette med helt til vi får $\phi_e : E_{e-1} \to E_{e-1}/langleR_{e-1}\langle$.

Når vi setter dette sammen igjen får vi

$$\phi = \phi_e \circ \phi_{e-1} \circ \ldots \circ \phi_1$$

Av med kjerne $ker(\phi) \cong (\mathbb{Z}_p)^e$, altså vil graden til $\phi$ være $p^e$.

Men vi er ikke bare interessert i den abstrakte teorien, vi er også interessert i hvordan vi kan bruke dette. Derfor introduserer vi nå noen algoritmer fra for å beregne isogenier ut fra kjernen. Merk at dette ikke nødvendigvis er de raskeste formlene for å beregne isogenier, men de er relativt enkle, og gir en god nok innføring for vår del.

Først tar vi algoritmen for å beregne isogenier av grad 2

**Teorem 3.17.** *(Vélu) [8] La $E_1/K$ være en elliptisk kurve definert av $y^2 - x^3 - Ax - B$. La så $x_0$ være en rot av $x^3 + Ax + B \in \overline{K}[x]$. Sett så $t = 3x_0^2 + A$ og $w = x_0 + t$. Den rasjonale avbildingen*

$$\phi(x, y) = \left( \frac{x^2 - x_0 x + t}{x - x_0}, \frac{(x - x_0)^2 - t}{(x - x_0)^2} y \right)$$

*er en separabel isogeni fra $E_1$ til $E_2$, der $E_2$ er den elliptiske kurven definert av $y^2 - x^3 - A'X - B$ der $A' = A - 5t$ og $B' = b - 7w$. Kjernen til $\phi$ er gruppen av orden 2 som genereres av $(x_0, 0)$.*

*Bevis.* Se [7, s. 6.12] □

Så har vi isogenier av odde grad.

**Teorem 3.18.** *(Vélu) [8] La $E_1/K$ være en elliptisk kurve definert av $y^2 - x^3 - Ax - B$. La så $G$ være en endelig undergruppe av $E(\overline{K})$ av oddetallsorden. For hver ikke-null $Q = (x_Q, y_Q) \in G$ definerer vi $t_Q = 3x_Q^2 + A$, $u_Q = 2y_Q^2$ og $w_Q = u_Q + t_Q x_Q$. Videre setter vi $t = \sum t_Q$, $w = \sum w_Q$ og*

$$r(x) = x + \sum \left( \frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right)$$

*. Da vil den rasjonale avbildingen*

$$\phi(x, y) = (r(x), r'(x)y)$$

*være en separabel isogeni fra $E_1$ til $E_2$ der $E_2$ er definer av $y^2 - x^3 - A'x - B'$ med $A' = A - 5t$ og $B' = B - 7w$ med kjerne $ker(\phi) = G$*

*Bevis.* Se [7, s. 6.14] □

Nå som vi kan beregne isogenier av grad 2 og odde grad, har vi mulitheten til å sette disse sammen til en isogeni av vilkårlig grad.

## 3.3 Endomorfier

**Definisjon 3.19.** La $E/K$ være en elliptisk kurve. Vi sier at en isogeni $\phi$ er en **endormorfi** dersom den avbilder $E$ på seg selv, altså $\phi : E \to E$.

Dersom den i tillegg er isomorfisk sier vi at det er en **automorfi**.

**TODO: Eksempel delvis tatt fra Washington, se om det bør fjernes/erstattes**

**Eksempel 3.20.** La $E$ være den elliptiske kurven gitt av $f(x,y) = y^2 - x^3 - B$. Da vil $\alpha(P) = [2]P$ være en endomorfi gitt av $\alpha(x,y) = (f_1(x,y), f_2(x,y))$, der

$$f_1(x,y) = \left(\frac{3x^2}{2y}\right)^2 - 2x \qquad f_2(x,y) = \frac{3x^2}{2y}\left(\left(\frac{3x^2}{2y}\right)^2 - 3x\right) - y$$

En spesielt interessant endomorfi er **Frobenius endomorfien**. La $\phi_q : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$, slik at $x \mapsto x^q$. Da er frobenius enomorfien $\pi_q : E \to E$, med $(x,y) \mapsto (x^q, y^q)$

**Lemma 3.21.** *La $E/\mathbb{F}_q$, og $(x,y) \in E(\overline{\mathbb{F}_q})$, da har vi*

1. $\pi_q(x,y) \in E(\overline{\mathbb{F}_q})$
2. $(x,y) \in E(\mathbb{F}_q)$ *hvis og bare hvis* $\pi(x,y) = (x,y)$

*Bevis.* Se [9, s. 93, 4.5] □

# 4 Struktur

**Teorem 4.1.** *La $q = p^2$, der $p$ er et primtall, og $\mathbb{F}_q$ være en endelig kropp, og $E/\mathbb{F}_q$ en supersingulær elliptisk kurve. Da har vi $\#E(\mathbb{F}_q) = (p \mp 1)^2$*

*Bevis.* Fra [5] har vi at $\#E(\mathbb{F}_q) = 1 + q - \beta$ der $\beta = \pm 2\sqrt{q}$, altså er $\beta = \pm p$. Da har vi $E(\mathbb{F}_q) = 1 + p^2 \mp p = (p-1)^2$ □

***TODO: Bedre bevis for dette, hvorfor må $E$ være supersingulær?***

Nå vet vi at $E(\mathbb{F}_q)$ er en abelsk gruppe med $(p \mp 1)^2$ punkter. Altså kan vi si noe om strukturen.

**Eksempel 4.2.** La $l_A$ og $l_B$ være to (små) primtall, $e_A, e_B$ og $f \in \mathbb{Z}^+$ være positive heltall slik at $p = l_A^{e_A} l_B^{e_B} f \pm 1$ er et primtall. Da er $\mathbb{F}_q = \mathbb{F}_{p^2}$ en endelig kropp. La så $\#E(\mathbb{F}_q) = (p \mp 1)^2 = (l_A^{e_A} l_B^{e_B} f)^2$. Da har vi fra Teorem 1.3 at $E(\mathbb{F}_q) \cong \mathbb{Z}/(l_A^{e_A} l_B^{e_B} f)\mathbb{Z} \times \mathbb{Z}/(l_A^{e_A} l_B^{e_B} f)\mathbb{Z}$

Siden vi vet at $E/\mathbb{F}_p$ danner en endeliggenerert abelsk gruppe har vi fra teorem 1.2 at denne kan dekomponeres til et direktesum av sykliske undergrupper. Altså finnes det undergrupper til den elliptiske kurven.

En interessant problemstilling er hvorvidt en restklasse til en elliptisk kurve også danner en elliptisk kurve.

Skal vise: $E/\Phi$ er også en elliptisk kurve

Oppgave 3.13

Undegrupper

## 4.1 J-invariant

I protokollen vi skal undersøke senere er vi interessert i å komme fram til samme verdi når vi har to potensielt ulike isomorfe elliptiske kurver. Derfor er det nyttig å finne en invariant over isomorfiavbildinger.

**Definisjon 4.3.** La $E/K$ være en elliptisk kurve på formen $y^2 = x^3 + Ax + B$. Vi sier at **diskriminanten**, $\Delta$, er definert som

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

Merk, diskriminanten sier noe om hvorvidt en kurve er singulær eller ikke. Når $\Delta \neq 0$ har vi at kurven er ikkesingulær, og altså en elliptisk kurve.

**Definisjon 4.4.** La $E/K$ være en elliptisk kurve på formen $y^2 = x^3 + Ax + B$. Vi sier at **j-invarianten**, j, er definert som

$$j = -12^3 \frac{(4A)^3}{\Delta}$$

**Proposisjon 4.5.** *To elliptiske kurver er isomorfe hvis og bare hvis avbildingen er på formen $[u^2x, u^3y]$ der $u \in \overline{K}$. (gjelder kun med karakteristikk $\notin \{2, 3\}$)*
***TODO: Bevis dette***

**Proposisjon 4.6.** *To elliptiske kurver er isomorfe over $\overline{K}$ hvis og bare hvis de har samme j-invariant.*

*Bevis.* La $E_1/K$ og $E_2/K$ være elliptiske kurver på formen $y^2 = x^3 + ax + b$ og $y^2 = x^3 + \alpha x + \beta$ slik at $\phi : E_1 \to E_2$ er en isomorfi. Da har vi at $\phi(x) = u^2x$ og $\phi(y) = u^3y$, eller med enkel substitusjon:

$$a = u^4\alpha \text{ og } b = u^6\beta$$

"$\Leftarrow$": La begge kurvene $E_1$ og $E_2$ ha samme j-invariant, $j$. Da har vi tre tilfeller vi må ta hensyn til:

**$\mathbf{j = 0}$** : Da har vi fra definisjonen av $j$-invariant at $a = \alpha = 0$. Da blir også $b \neq 0$ og $\beta \neq 0$ siden $\Delta \neq 0$ for elliiptiske kurver. Må vise at $b = u^6\beta$, altså at $\frac{b}{\beta}$ har en sjetterot i $\overline{K}$ **Hvordan vet vi dette?**

**$\mathbf{j = 12^3}$** : Fra definisjonen av $j$, må

$$\frac{(4a)^3}{-16(4a^3 + 27b^2)} = -1$$

så $a \neq 0$, noe som medfører at $b = 0$. (Tilsvarende for $\alpha$ og $\beta$. Da har vi at $a = u^4\alpha$, eller $u = \sqrt[4]{\frac{a}{\alpha}}$

**Resten** Siden hverken $a, b, \alpha$, eller $\beta = 0$ (dersom en av de var det ville j-invarianten vært 0 eller $12^3$, dersom begge var det blir $\Delta = 0$) har vi at $u = \sqrt[4]{\frac{a}{\alpha}} = \sqrt[6]{\frac{b}{\beta}}$

"⇒"**Må bevise dette** □

Konsekvensen av denne "hvis og bare hvisproposisjonen er at vi har en invariant over isomorfe elliptiske kurver, og denne er unik.

## 4.2 Torsiongrupper

Torsiongrupper er en viktig del av protokollen vi senere skal se på. Vi kommer til å bruke de til å lage kjerner av riktig størrelse og må vite litt om hvordan de ser ut.

**Definisjon 4.7.** La $E$ være en elliptisk kurve, og $m$ et heltall. Vi sier at multiplikasjon av $m$-avbildingen, $[m] : E \to E$ er definert som $[m] : P \mapsto \underbrace{P + \ldots, +P}_{m \text{ ganger}}$

**Definisjon 4.8.** La $E$ være en elliptisk kurve, og $m$ være et heltall. Vi sier at $m$-torsiongruppa, $E[m]$ er alle punktene som multiplisert med $m$ blir $\mathcal{O}$:

$$E[m] = \{P \in E \mid [m]P = \mathcal{O}\}$$

Merk, en torsongruppe inneholder ikke bare alle punktene av orden $m$. F.eks. vil $E[4]$ også inneholde punkter av orden 2 da $[4]P = [2][2]P = [2]\mathcal{O} = \mathcal{O}$.

**Proposisjon 4.9.** *La $E$ være en elliptisk kurve, og $m$ et heltall. Da er $deg[m] = m^2$.*

*Bevis.* **TODO: Bevis dette** □

**Korollar 4.10.** *La $E$ være en elliptisk kurve, $m$ være et positivt heltall og $p = char(K)$. Da har vi følgende:*

1. *Hvis $p = 0$ eller $p \nmid m$ da er*

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$$

2. *Ellers er en av følgende riktige*
   (a) *$E[p^e] = \{O\}$ for alle $e = 1, 2, 3, \ldots$*
   (b) *$E[p^e] \cong \frac{\mathbb{Z}}{p^e\mathbb{Z}}$ for alle $e = 1, 2, 3, \ldots$*

*Bevis.* [6, s. III 6.4] □

**Eksempel 4.11.** La $E/\mathbb{F}_q$ være en elliptisk kurve med orden $(l_A^{e_A} l_B^{e_B} f)^2$. der $l_A$, $l_B$, og $\sqrt{(}q)$ er (ulike) primtall. Siden $q \nmid l_A^{e_A}$ har vi at torsongruppa

$$E[l_A^{e_A}] \cong \frac{\mathbb{Z}}{l_A^{e_A}\mathbb{Z}} \times \frac{\mathbb{Z}}{l_A^{e_A}\mathbb{Z}}$$

. Altså vil to lineært uavhengige punkter $P, Q \in E$ generere hele torsongruppa.

**Proposisjon 4.12.** *La $E/\mathbb{F}_q$ være en elliptisk kurve og $E[p^e]$ være en torsongruppe der $p$ er et primtall og $char(\mathbb{F}_q) \nmid p$. Da vil $E[p^e]$ ha $(p^e - p^{e-1})^2$ elementer av orden $p^e$.*

*Bevis.* Siden $p$ er primtall vil $\mathbb{Z}/p^e\mathbb{Z}$ være en syklisk gruppe (av Gauss). Antall generatorer i denne gruppa vil være $\phi(p^e) = p^e - p^{e-1}$ (Eulers phi-funksjon). Siden $E[p^e] = \mathbb{Z}/p^e\mathbb{Z} \times \mathbb{Z}/p^e\mathbb{Z}$ finnes det $(p^e - p^{e-1})^2$ elementer av orden $p^e$ □

**Eksempel 4.13.** La $E/\mathbb{F}_q$ være en elliptisk kurve der $\#E(\mathbb{F}_q) = (l_A^{e_A})^2 H$ der $l_A^{e_A} \nmid H$

Siden vi vet at $E$ er en abelsk gruppe har vi at $E(\mathbb{F}_q) \cong \frac{\mathbb{Z}}{l_A^{e_A}\mathbb{Z}}^2 \oplus C_H$, der $C_H$ er en syklisk gruppe av orden $H$. Vi kan nå se på avbildingen $[H]$. Denne fungerer som en automorfi på på $E[l_A^{e_A}]$ fordi $l_A \nmid H$. I tillegg vil det sende alle elementer i $C_H$ til $e$. Altså blir det en avbilding på formen $[H] : E \to \frac{\mathbb{Z}}{l_A^{e_A}\mathbb{Z}} \times \frac{\mathbb{Z}}{l_A^{e_A}\mathbb{Z}}$.

Vi kan med andre ord bruke dette for å finne et element som ligger i torsongruppa $E[l_A^{e_A}]$.

**TODO: Skriv om lineart uavhengige punkter som generer torsongruppa, tegn bilde (gitter-aktig)**

## 4.3 Strukturen til $E$

**Teorem 4.14.** ***Mordell–Weil*** *La $K$ være en endelig kropp. Da vil de $K$-rasjonale punktene til en elliptisk kurve danne en endeliggenerert abelsk gruppe.*

*Bevis.* For bevis, se [6, s. 207, VIII] □

Vi vet nå at $E/K$ danner en endeliggenerert abelsk gruppe dersom $K$ er endelig. Vi er ofte interessert i kardinaliteten, antall elementer, til en elliptisk kurve - vi bruker den korte notasjonen $\#E(K)$ for å indikere antall $K$-rasjonale punkter i $E$.

**Teorem 4.15.** *La $E/\mathbb{F}_q$ være en ellliptisk kurve. Da vil enten*

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \text{ eller} \qquad E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

*Bevis.* fra teorem 1.3 har vi at $E(\mathbb{F}_q)$ er isomorf til en direktesum av sykliske grupper, $\mathbb{Z}/n_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_r\mathbb{Z}$. Med $n_i \mid n_{i+1}$. For hver $i$ vil gruppen $\mathbb{Z}/n_i\mathbb{Z}$ ha $n_i$ elementer av orden som deler $n_i$. Dette medfører at $E(\mathbb{F}_q)$ har $n_1^r$ elementer av orden $n_1$. Men fra teorem 4.10 har vi at det maksimalt er $n_1^2$ slike. Altså må $r \leq 2$. [9, 91, Teorem 4.1] □

**Teorem 4.16.** *(Hasse)* ***TODO: Finn riktig referanse til Hasses opprinnelige teorem****. La $E/\mathbb{F}_q$. Da vil ordenen til $F_1$ tilfredsstille*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$$

**TODO: Bruk hasses teorem til å sette begrensingen, vis så for elliptiske kurver at det finnes en kurve som er definert som den under.**

## 4.4 Supersingulære kurver

**Definisjon 4.17.** La $E/K$ være en elliptisk kurve definert over en kropp $K$ med karakteristikk $p$. Vi sier at $E$ er **supersingulær** dersom det eneste punktet i $E[p] = \{\mathcal{O}\}$

**Proposisjon 4.18.** *La $E$ være en elliptisk kurve over $\mathbb{F}_{p^n}$ der $p$ er et primtall og $n$ er et positivt heltall. La så $a = p^n + 1 - \#E(\mathbb{F}_{p^n})$. Da er $E$ supersingulær hvis og bare hvis $a \cong 0 \mod p$, eller tilsvarende $\#E(\mathbb{F}_{p^n}) \cong 1 \mod p$.*

**Proposisjon 4.19.** *La $q = p^n$ for et primtall $p$ og positivt heltall $n$ og $B \in \mathbb{F}_q^x$, der $q \cong 2 \mod 3$. Da vil den ellitpsike kurven gitt av polynomet $y^2 - x^3 - B$ være supersingulær.*

*Bevis.* La $\psi : \mathbb{F}_q^x \to \mathbb{F}_q^x$ være homomorfien definert av $\psi(x) = x^3$. Siden $q - 1$ ikke er en multippel av 3 er det ingen elementer av orden 3 i $\mathbb{F}_q^x$, altså er $ker(\psi) = \{0\}$. Med andre ord, $\psi$ er injektiv. Siden det er en avbilding fra en endelig gruppe til seg selv er den altså også surjektiv. Noe som betyr at alle elementer i $\mathbb{F}_q$ har en unik tredjerot i $\mathbb{F}_q$ (Merk at $\mathbb{F}_q^x = \mathbb{F}_q \setminus \{0\}$, og $0 = 0^3$. Spessielt har alle punkter, $y^2 - B$, en tredjerot, $x$ som gir oss $y^2 - x^3 - B = 0$ - altså har vi $q$ punkter. Dersom vi legger til punktet i uendeligheten, $\mathcal{O}$ har vi $q + 1$ punkter, og $E$ er supersingulær.**TODO: sjekk dette,Korollar 3:30 sier at dette gjelder dersom $q$ er primtall, ikke ellers.** [9, s. 4.3.1] □

# 5 SIDH/CSIDH

Supersingular Isogeny-based Diffie Hellman (eller bare SIDH) er et kroptosystem som inkluderer zero-knowledge, nøkkelutveksling og offentlig-nøkkel kryptering.

## 5.1 Nøkkelutveksling

$$\begin{array}{ccc} E_0 & \xrightarrow{\phi_A} & E_A \\ {\scriptstyle \phi_B}\downarrow & & \downarrow{\scriptstyle \phi_{AB}} \\ E_B & \xrightarrow{\phi_{BA}} & E_{AB} \cong E_{BA} \end{array}$$

Figur 2: Isogenidiagram

**Oppsett**: Velg en en supersingulær elliptisk kurve $E_0$ definert over $\mathbb{F}_p^2$, der $p = l_A^{e_A} l_B^{e_B} f \pm 1$. Finn så basiser $\{P_A, Q_A\}$ og $\{P_B, Q_B\}$ for $E_0[l_A^{e_A}]$ og $E_0[l_B^{e_B}]$.

Nøkkelutveksling SIDH

| **Alice** | | **Bob** |
|---|---|---|
| $m_A, n_A \leftarrow_\$ \mathbb{Z}/l_A^{e_A}\mathbb{Z}$ | | $m_B, n_B \leftarrow_\$ \mathbb{Z}/l_B^{e_B}\mathbb{Z}$ |
| $r_A \leftarrow m_A P_A + n_A Q_A$ | | $r_A \leftarrow m_B P_B + n_B Q_B$ |
| Lag: $\phi_A : E_0 \rightarrow E_0/\langle r_A \rangle$ | | Lag: $\phi_B : E_0 \rightarrow E_0/\langle r_B \rangle$ |
| $E_A \leftarrow \phi_A(E_0)$ | | $E_B \leftarrow \phi_B(E_0)$ |
| | $\xrightarrow{\phi_A(P_B),\ \phi_A(Q_B), E_A}$ | |
| | $\xleftarrow{\phi_B(P_A),\ \phi_B(Q_A), E_B}$ | |
| $r_{AB} \leftarrow m_A\phi_B(P_A) + n_A\phi_B(Q_A)$ | | $r_{BA} \leftarrow m\phi_A(P_B) + n\phi_A(Q_B)$ |
| Lag: $\phi_{AB} : E_B \rightarrow E_B/\langle r_{AB} \rangle$ | | Lag: $\phi_{BA} : E_A \rightarrow E_A/\langle r_{BA} \rangle$ |
| $Z \leftarrow j(E_{AB})$ | | $Z \leftarrow j(E_{BA})$ |

Legg merke til at $E_{AB}$ og $E_{BA}$ er isomorfe, så j-invarianten er den samme.

## 5.2 Komponenter

### 5.2.1 Finne primtallet P

Protokollen tar utgangspunkt i at det finnes et primtall, $P$, som er på formen $l_A^{e_A} l_B^{e_B} f + 1$. På grunn av primtallsteoremet vet vi at det finnes "XXslike av størrelsesorden "XXXbits, altså er det overkommelig å finne et primtall. Når vi går fram for å finne et primtall bestemmer vi oss for små primtall $l_A$ og $l_B$, disse kan være så små som 2 og 3. Deretter bestemmer vi eksponentene $e_A$ og $e_B$ slik at både $l_A^{e_A}$ og $l_B^{e_B}$ er store - det er tross alt der sikkerheten til protokollen ligger. Så velger vi oss tilfeldige partall, $f$, og sjekker om $P = l_A^{e_A} l_B^{e_B} f + 1$ eller $P = l_A^{e_A} l_B^{e_B} f - 1$ er et primtall. Hvis ikke velger vi kun en ny $f$.

### 5.2.2 Finne den elliptiske kurven

Når vi har $P$ velger vi oss en supersingulær elliptisk kurve $E$ definert over $\mathbb{F}_q = \mathbb{F}_p^2$ (Vi skriver $q$ for å forenkle notasjonen). Eneste kravet vi setter til kurven er at den skal være supersingulær og ha kardinalitet $(l_A^{e_A} l_B^{e_B} f)^2$. Av brökers algoritme har vi at dette kan konstrueres i $O(log(q)^3)$ tid [2].

Når det er sagt er det ikke sikkert vi ønsker å bruke denne fastekurven som vår elliptiske kurve. Bakgrunnen for dette er at det ikke er sikkert at løsningen for isogeni-sti-problemet til en elliptisk kurve lar seg redusere til løsningen for en spessiellelliptisk kurve. Heldigvis er det flere kurver å velge mellom, og det koster lite å finne en isomorf kurve (hvor vanskelig?)

### 5.2.3 Finne basiser for torsongruppene

Vi vet at $E/\mathbb{F}_q$ har $\#E(\mathbb{F}_q) = n = (l_A^{e_A} l_B^{e_B} f)^2$, altså kan vi lett finne elementer i $E[l_A^{e_A}]$ på samme måte som eksempel 4.13. Men vi ønsker basiser, så vi må finne

punkter av orden $l_A^{e_A}$. Av proposisjon 4.12 har vi at det finnes $(l_A^{e_A} - l_A^{e_A-1})^2$ slike. **TODO: Sannsynligheten for å finne ett slikt element** For å sjekke at et element har riktig orden sjekker man ganske enkelt bare $[l_A]P$, $[l_A^2]P$, ..., $[l_A^{e_A-1}]P$ og ser om de er $\mathcal{O}$. Hvis ikke har funnet et basiselement.

Når vi har funnet ett punkt, gjentar vi prosessen over til vi finner et annet punkt, $Q$. Deretter sjekker vi om de er lineært uavhengige. Siden både $Q$ og $P$ har orden $l_A^{e_A}$ vil de generere hver sin undergruppe, **TODO: Hva er sannsynligheten for at de genererer samme gruppe**.

For å sjekke om de er lineart uavhengige ser vi på $[l_A^{e_A-1}]PA + [nl_A^{e_A-1}]Q_A = 0$, om du kan finne en slik $n \in \mathbb{Z}/(e_A\mathbb{Z})$ er punktene lineært avhengige og du må finne en ny $Q$, ellers har du funnet to lineart uavhengige punkter. **Må vise at dette er en godtest for lineart avhengighet**

### 5.2.4 Beregne isogenien og kjernen

Kjernen $\langle R \rangle$ beregnes ved å først lage generatoren, $R = mP + nQ$, men siden dette genererer en undergruppe av torsongruppa spiller det ingen rolle hvilket element fra gruppa vi bruker. Siden vi også vet at $m$ ikke deler $l_A$ kan vi finne inversen $m^{-1} \mod l_A^{e_A}$. Samtidig vet vi at $mP + nQ$ er generator for samme gruppe som $m^{-1}(mP+nQ)$, altså har vi $P+m^{-1}nQ$ som generator. Denner forenklingen gjør det lettere å beregne generatoren da invertering og multiplikasjon modulo $l_A^{e_A}$ er raskere enn å gange og opphøye punktet $P$.

Vi ønsker å beregne en isogeni av grad $l_A^{e_A}$. Fra korollar 3.15 har vi at denne kan dekomponeres til $e_A$ isogenier av grad $l_A$. Eksempel 3.16 gir oss en god metode for å beregne isogenier.

# 6 Sikkerhet

Hvorfor er dette sikkert/vanskelig å knekke.

## 6.1 Noen problemer

For alle problemene, annta $p = l_A^{e_A} l_B^{e_B} f \pm 1$ er et primtall, $\{P_A, Q_A\}$ og $\{P_B, Q_B\}$ basiser for $E[l_A^{e_A}]$ og $E[l_B^{e_B}]$. Alt er hentet fra [4]

### 6.1.1 DSI

(Såkalt Decisional supersingular isogeny problem). La $E$ og $E_A$ være to kurver som er definert over $\mathbb{F}_{p^2}$. Er det mulig å sjekke om $E$ og $E_A$ har en isogeni av grad $l_A^{e_A}$ mellom seg (at de er $l_A^{e_A}$-isogene)?

### 6.1.2 CSSI

(Såkalt computational supersingular isogeny problem). La $\phi : E \to E_A$ være som i protokollen, altså med kjerne $\langle [m_A]P_A + [n_A]Q_A \rangle$ der $m_A$ og $n_A$ er tilfeldige.

Gitt $E_A$, $\phi(P_B)$ og $\phi(Q_B)$ - finn en generator $R_A$ for kjernen.

Angivelig enkelt å finne $m_A$ og $n_A$ ut i fra det?
Kan reduseres til å finne "utvidetdiskret logaritme via $R = [m]P + [n]Q$?

### 6.1.3 SSCDH

(Såkalt supersingular computational diffie hellman). La $\phi_A : E \to E_A$ være som over, og $\phi_B : E \to E_B$ der kjernen er $\langle [m_B]P_B + [n_B]Q_B \rangle$.

Gitt $E_A$, $E_B$, $\phi_A(P_B)$, $\phi_A(Q_B)$, $\phi_B(P_A)$, $\phi_B(Q_A)$, finn j-invarianten til kurven $E/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle$

# 7 Implementering og ytelse

# Referanser


[1] P. B. Bhattacharya, S. K. Jain og S. R. Nagpaul. *Basic abstract algebra*. Second. Cambridge University Press, Cambridge, 1994, s. xx+487. ISBN: 0-521-46081-6; 0-521-46629-6. DOI: 10.1017/CBO9781139174237. URL: https://doi.org/10.1017/CBO9781139174237.

[2] Reinier Bröker. "Constructing supersingular elliptic curves". I: *J. Comb. Number Theory* 1.3 (2009), s. 269–273.

[3] W. Fulton. *Algebraic curves: an introduction to algebraic geometry*. Advanced book classics. Addison-Wesley Pub. Co., Advanced Book Program, 1989. ISBN: 9780201510102. URL: https://books.google.no/books?id=SEbvAAAAMAAJ.

[4] David Jao og Luca De Feo. "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies". I: *Post-Quantum Cryptography*. Red. av Bo-Yin Yang. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, s. 19–34. ISBN: 978-3-642-25405-5.

[5] Hans-Georg Rück. "A Note on Elliptic Curves Over Finite Fields". I: *Math. Comp.* 49.179 (1989), s. 301–304.

[6] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Bd. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, s. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6. URL: https://doi.org/10.1007/978-0-387-09494-6.

[7] Andrew Sutherland. *MIT Mathematics 18.783, Lecture Notes: Elliptic Curves*. URL: https://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2017/lecture-notes/. Last visited on 2019/03/25. 2017.

[8] J. VELU. "Isogenies entre courbes elliptiques". I: *C. R. Acad. Sci. Paris, Series A* 273 (1971), s. 305–347. URL: https://ci.nii.ac.jp/naid/10029941471/en/.

[9] Lawrence C Washington. *Elliptic curves : number theory and cryptography*. eng. Boca Raton, Fla, 2003.