Elliptic curves (eller Elliptiske kurver?)

Denne uken: Man/Tir

Pensum: • [Ellingsrud-Ottem] 1-4, 7, 9
• Silverman - „Arithmetic of elliptic curves"
Kap. $\underbrace{1\text{-}2}$, 3, 5 (kanskje 6)
overlapp med [EO]

Alternativt materiale: • Hartshorne-kapittel om ell. kurver
• Milne sine notater

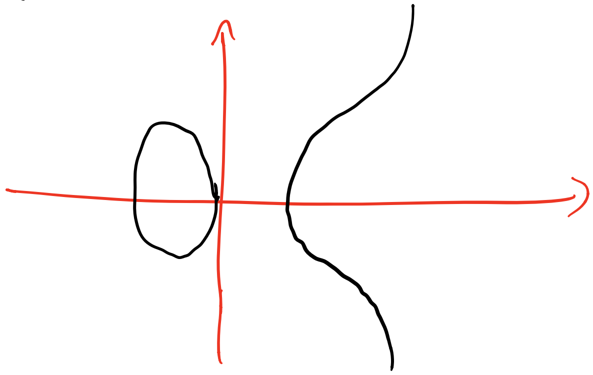
Elliptiske kurver: Hva? La K = alg. lukket kropp (for øyeblikket),
la $f \in K[X,Y,Z]$ være irredusibelt, homogent av grad 3.
Hvis den projektive varieteten

$$C = \{[x:y:z] \in \mathbb{P}^2 \mid f(x,y,z) = 0\}$$

er glatt (ikke singulær), er C en ell. kurve.

Eks: $f = ZY^2 - X(X-Z)(X+Z)$

C



Hvorfor? Geometri: Ell. kurver er tredje enkleste varieteten (etter „punkt" og $\mathbb{P}^1$)

$$\{\text{alle projektive varieter}\} \supset \{\text{kurver i } \mathbb{P}^2\} \supset \{\text{elliptiske kurver}\}$$

- C elliptisk $\Longrightarrow$ C har en gruppestruktur
$$p, q \in C \rightsquigarrow p + q \in C$$

- Spm: Kan vi klassifisere elliptiske kurver opp til isomorfi? (Svar: Ja)

Tallteori: Definer ell. kurve ved
$$f(X, Y, Z) = Y^2 Z - (X^3 + aXZ^2 + bZ^3) \qquad a, b \in \mathbb{Z}, \mathbb{Q}, \mathbb{Z}/p$$

(Vanskelig) problem: Finn løsningene av $f(X, Y, Z) = 0$ med $X, Y, Z \in \mathbb{Z}, \mathbb{Z}/p$

„Teorien om ell. kurver" $\rightsquigarrow$ generelle teknikker

Problem: I $\mathbb{Z}/p$-tilfellet, hvor mange løsninger?

Mål for oss: Weil-formodningene for elliptiske kurver

Fermats siste teorem (Wiles) Det fins ingen $X, Y, Z \in \mathbb{Z}_{>0}$ s.a.
$$X^n + Y^n = Z^n \qquad n > 2 \qquad (*)$$

Hvis $n = 3$, så gir $(*)$ en elliptisk kurve
— " — $n > 3$, så er $(*)$ ikke elliptisk, men Wiles' bevis er en påstand om én elliptisk kurve.

Kryptografi: Gruppestrukturen på en elliptisk kurve over $\mathbb{Z}/p$ brukes i „elliptisk kurve-kryptografi".

Bakgrunn om varieteter

Fikser konvensjoner:
- K en perfekt kropp
- $\bar{K}$ en alg. tillukning av K

K perfekt $\iff$ en irredusibel $f \in K[x]$ har bare simple nullpunkter i $\bar{K}$.

Ikke-eksempel: $K = \mathbb{Z}/p(t)$ $\quad f = x^p - t = (x - t^{1/p})^p$

Eksempler: K en karakteristikk 0-kropp er perfekt
- $K = \mathbb{Q}$, endelige utvidelser av $\mathbb{Q}$, $\bar{K} = \bar{\mathbb{Q}}$
- $K = \mathbb{R}$, $\bar{K} = \mathbb{C}$
- p primtall $K = \mathbb{F}_p = \mathbb{Z}/p$, kroppen av p elementer
- $q = p^n$ $\quad K = \mathbb{F}_q$, — " — q — " —
- $K = \bar{K}$, $\mathbb{C}$, $\bar{\mathbb{Q}}$, $\bar{\mathbb{F}}_p$

Affint rom $\mathbb{A}^n = \{(x_1, \dots, x_n) \mid x_i \in \bar{K}\}$

„K-rasjonale punkter i $\mathbb{A}^n$" $= \mathbb{A}^n(K) = \{(x_1, \dots, x_n) \mid x_i \in K\}$

En mengde $V \subseteq \mathbb{A}^n$ er **algebraisk** hvis $\exists$ ideal

$$I \subset \bar{K}[x_1, \dots, x_n]$$

$$V = V_I = \{ P \in \mathbb{A}^n \mid f(P) = 0 \quad \forall f \in I \}$$

Gitt $Z \subseteq \mathbb{A}^n$, definer idealet $I(Z) \subseteq \bar{K}[X_1, \ldots, X_n]$ ved

$$f \in I(Z) \iff f(P) = 0 \quad \forall P \in Z.$$

<u>Def</u>: En alg. mengde $V \subset \mathbb{A}^n$ er <u>definert over K</u> hvis $\exists\, f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$ s.a.

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

Skriver V/K for dette.

<u>Eksempler</u>: $K = \mathbb{Q}$ $\quad \bar{K} = \bar{\mathbb{Q}}$, $\quad n = 2$

- $I = (x_2^2 - 3x_1^3)$

  V_I definert over $\mathbb{Q}$ $\qquad 1, -3 \in \mathbb{Q}$

- $I = \left((\sqrt{2} - 1) x_2^2 + \frac{4}{\sqrt{2}+1} x_1^2 \right) = \left((\sqrt{2}-1)(x_2^2 + 4x_1^2) \right)$

  $= (x_2^2 + 4x_1^2)$,

  så V_I er definert over $\mathbb{Q}$

- $I = (x_1 - \sqrt{2}\, x_2) \rightsquigarrow V_I$ ikke def. over $\mathbb{Q}$.

La $V \subset \mathbb{A}^n$ være algebraisk. Definer idealet

$$I(V/K) \subset K[X_1, \ldots, X_n]$$

$$I(V/K) = I(V) \cap K[X_1, \ldots, X_n]$$

<u>Oppgave</u>: V definert over K

$$\Updownarrow$$

$$I(V) = (f)_{f \in I(V/K)} \subset \overline{K}[x_1, \dots, x_n]$$

<u>Def</u>: La V være alg. mengde def. over K, da er de <u>K-rasjonale punktene til V</u>

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

<u>Eksempel</u> $K = \mathbb{R}$, $\overline{K} = \mathbb{C}$ $\quad I(x^2+y^2-a)$ $\quad a \in \mathbb{R}$

$V = V_I$

$$V(\mathbb{R}) = \begin{cases} \phi & \text{hvis } a < 0 \\ \{(0,0)\} & \text{hvis } a = 0 \\ \text{en sirkel m/radius } \sqrt{a} & \text{hvis } a > 0 \end{cases}$$

- $K = \mathbb{Q}$ $\quad I = (x^n + y^n - 1)$ $\quad V = V_I$

Fermats siste teorem er at

$$V(\mathbb{Q}) \subset \{(1,0), (-1,0), (0,1), (0,-1)\}$$

hvis $n \geq 3$.

<u>Zariski-topologien på $\mathbb{A}^n$</u>

<u>Def</u> $Z \subset \mathbb{A}^n$ er lukket $\Leftrightarrow$ Z er algebraisk

<u>Def</u> En algebraisk mengde Z er en (affin) <u>varietet</u> hvis den er <u>irredusibel</u> i Zariski-topologien

$$Z = Z_1 \cup Z_2 \implies Z = Z_1 \text{ eller } Z = Z_2$$

Z_i lukket

Dette er hvis og bare hvis $I(Z) \subseteq \bar{K}[X_1, \ldots, X_n]$ er primideal.

Koordinatringer: Hvis $V \subset \mathbb{A}^n$ er en varietet, så er koordinatringen

$$\bar{K}[V] = \bar{K}[X_1, \ldots, X_n]/I(V).$$

Funksjonskroppen er

$$\bar{K}(V) = \text{brøkkroppen til } \bar{K}[V].$$

Hvis V def. over K, definer koord. ring over K

$I(V/K) = I(V) \cap K[X]$

$$K[V] = K[X_1, \ldots, X_n]/I(V/K)$$

$$K(V) = \text{brøkkroppen til } K[V].$$

Dimensjon til en varietet V er

Krull-dimensjon til $K[V]$

$=$ —— " —— $\bar{K}[V]$

$=$ transcendensgraden til $\bar{K}(V)/\bar{K}$

$=$ —— " —— $K(V)/K$.

Ikkesingulære varieteter: La V være algebraisk mengde $\subset \mathbb{A}^n$

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

Da er V ikkesingulær i $P \in V$ hvis

$$\text{rang } J_{\{f_i\}}(P) = \left(\frac{\partial f_i(P)}{\partial X_i}\right) = n - \dim V$$

Hvis $r = 1$, er dette hvis og kun hvis $\exists X_i$ s.a.

$$\frac{\partial f_1(P)}{\partial X_i} \neq 0.$$

V er ikkesingulær hvis dette holder i alle $P \in V$.

<u>Definisjons-lokus for $f \in \bar{K}(V)$</u> $V \subset \mathbb{A}^n$ er en varietet.

$f \in \bar{K}(V)$ er definert i $P \in V$ hvis det fins $g, h \in \bar{K}[V]$, slik at $f = \frac{g}{h}$, $h(P) \neq 0$.

Den lokale ringen i P

$$\bar{K}[V]_P = \{ f \in \bar{K}(V) \mid f \text{ er definert i } P \}.$$

$f \in \bar{K}(V)$, velger g, h slik at $f = \frac{g}{h}$ $h(P) \neq 0$

selv om $h(Q) = 0$ for en Q, så kan f fortsatt være def. i Q

Kan finne g', h' s.a $f = \frac{g'}{h'}$ $h'(Q) \neq 0$