Curbe eliptice peste corpuri finite

Adrian Manea

2 noiembrie 2019

Cuprins

SEMINAR 1

PRELIMINARII

1.1 Varietăți algebrice

Începem prezentarea cu cîteva preliminarii privitoare la varietăți algebrice și alte noțiuni elementare de algebră comutativă.

Vom folosi următoarele notații și obiecte:

- K este un corp perfect, i.e. unul pentru care orice extindere algebrică este separabilă;
- $\overline{K}$ este o închidere algebrică fixată a lui K;
- $\mathrm{Gal}(\overline{K}/K) = G_{\overline{K}/K}$ este grupul Galois al extinderii $K \subseteq \overline{K}$.

În majoritatea exemplelor, K va fi (o extindere algebrică a lui) $\mathbb{Q}$, $\mathbb{Q}$ sau $\mathbb{F}_p$.

Definiție 1.1: *Spațiul afin* peste corpul K este mulțimea de n-tupluri:

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

Similar, se definește *spațiul punctelor K-raționale* din $\mathbb{A}^n$, care conține restricția $P \in K^n$.

Fie $\overline{K}[X] = \overline{K}[X_1, \dots, X_n]$ un inel de polinoame în n nedeterminate și fie $I \trianglelefteq \overline{K}[X]$ un ideal. Putem asocia fiecărui astfel de ideal o submulțime a lui $\mathbb{A}^n$:

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

Definiție 1.2: O *mulțime algebrică afină* este o mulțime de forma V_I ca mai sus.

Dacă V este o astfel de mulțime, *idealul* lui V este:

$$I(V) = \{f \in \overline{K}[X] \mid f(P) = 0, \quad \forall P \in V\}.$$

Spunem că o mulțime algebrică este *definită* peste K dacă idealul său $I(V)$ poate fi generat de polinoame din $K[X]$ și notăm aceasta cu V/K.

Dacă V este definită peste K, *mulțimea punctelor K-raționale* ale lui V este mulțimea:

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

Observaţie 1.1: Conform teoremei bazei a lui Hilbert, idealele lui $\overline{K}[X]$ și $K[X]$ sînt finit generate.

Fie V o mulțime algebrică și considerăm idealul:

$$I(V/K) = \{f \in K[X] \mid f(P) = 0, \quad \forall P \in V\} = I(V) \cap K[X].$$

Se poate observa că V este definită peste K dacă și numai dacă are loc relația:

$$I(V) = I(V/K) \cdot \overline{K}[X].$$

Presupunem acum că V este definită peste K și fie $f_1, \dots, f_m \in K[X]$, generatori ai idealului $I(V/K)$. Rezultă că $V(K)$ este mulțimea soluțiilor $x = (x_1, \dots, x_n)$ pentru ecuațiile polinomiale:

$$f_1(x) = \cdots = f_m(x) = 0, \quad x_1, \dots, x_n \in K.$$

Exemplu 1.1: Fie V mulțimea algebrică din $\mathbb{A}^2$ dată de ecuația $X^2 - Y^2 = 1$.

Atunci V este definită peste orice corp K.

Presupunem acum $\mathrm{char} K \neq 2$. Rezultă $V(K) \simeq \mathbb{A}^1(K) - \{0\}$, o bijecție fiind, de exemplu:

$$\begin{aligned} \mathbb{A}^1(K) - \{0\} &\longrightarrow V(K) \\ t &\longmapsto \left(\frac{t^2+1}{2t}, \frac{t^2-1}{2t}\right). \end{aligned}$$

Exemplu 1.2: Mulțimea algebrică $V : X^n + Y^n = 1$ este definită peste $\mathbb{Q}$ și, folosind Marea Teoremă a lui Fermat, pentru orice $n \geq 3$, are loc:

$$V(\mathbb{Q}) = \begin{cases} \{(1,0),(0,1)\}, & n \text{ impar} \\ \{(\pm 1, 0), (0, \pm 1)\}, & n \text{ par} \end{cases}.$$

Exemplu 1.3: Mulțimea algebrică $V : X^2 = Y^3 + 17$ are multe puncte $\mathbb{Q}$-raționale. De fapt, se poate arăta că $V(\mathbb{Q})$ este infinită. Cîteva exemple sînt:

$$V(\mathbb{Q}) = \{(3, -2), (378661, 5234), \left(\frac{2651}{512}, \frac{137}{64}\right)\}.$$

Definiţie 1.3: O mulțime algebrică (afină) se numește *varietate algebrică (afină)* dacă $I(V)$ este un ideal prim al lui $\overline{K}[X]$.

Remarcăm că dacă V este definită peste K, atunci este suficient să verificăm dacă $I(V/K)$ este ideal prim al lui $K[X]$.

Fie V/K o varietate, adică V este varietate definită peste K. Atunci *inelul coordonatelor afine* al V/K este:

$$K[V] = \frac{K[X]}{I(V/K)}.$$

De asemenea, deoarece $I(V/K)$ este ideal prim, rezultă că $K[V]$ este domeniu de integritate. Corpul său de fracții se notează $K(V)$ și se numește *corpul de funcții* al lui V/K.

Similar putem formula înlocuind K cu $\overline{K}$.

În plus, orice element al $\overline{K}[V]$ se definește pînă la un element din $I(V/\overline{K})$, deci pînă la un polinom ce se anulează pe V. Rezultă că $f \in \overline{K}[V]$ induce o funcție $f : V \longrightarrow \overline{K}$.

Definiție 1.4: Fie V o varietate algebrică.

Dimensiunea varietății, notată $\dim V$, este gradul de transcendență al extinderii $\overline{K}(V)$ peste $\overline{K}$.

Exemplu 1.4: $\dim \mathbb{A}^n = n$, deoarece $\overline{K}(\mathbb{A}^n) = \overline{K}(X_1, \dots, X_n)$.

Dacă $V \subseteq \mathbb{A}^n$ este dat de o ecuație polinomială neconstantă $f(X_1, \dots, X_n) = 0$, atunci $\dim V = n - 1$.

Vom fi interesați de proprietatea de *netezime*, care se definește prin analogul condiției de existență a planului tangent:

Definiție 1.5: Fie V o varietate algebrică, $P \in V, f_1, \dots, f_m \in \overline{K}[X]$ o mulțime de generatori pentru $I(V)$.

V se numește *nesingulară (netedă)* în P dacă matricea jacobiană $\left(\frac{\partial f_i}{\partial X_j}(P)\right)$ are rangul $n - \dim V$.

Exemplu 1.5: Fie V dată de o ecuație polinomială neconstantă $f(x_1, \dots, x_n) = 0$.

Atunci $\dim V = n - 1$, deci P este singularitate dacă și numai dacă $\frac{\partial f}{\partial x_i}(P) = 0, \forall 1 \leq i \leq n$. Totodată, $f(P) = 0$, deci în total obținem $n + 1$ condiții pe n nedeterminate.

Exemplu 1.6: Fie două varietăți:

$$V_1 : Y^2 = X^3 + X \quad \text{și} \quad V_2 : Y^2 = X^3 + X^2.$$

Punctele lor singulare trebuie să satisfacă:

$$V_1^{\text{sing}} : 3X^2 + 1 = 2Y = 0 \quad \text{și} \quad V_2^{\text{sing}} : 3X^2 + 2X = 2Y = 0.$$

Rezultă că V_1 nu are singularități, dar V_2 are, originea $(0, 0)$.

Putem formula și o altă caracterizare a netezimii, prin funcții definite pe varietate. Fie P un punct arbitrar din V. Definim idealul $M_P \trianglelefteq \overline{K}[V]$ prin:

$$M_P = \{f \in \overline{K}[V] \mid f(P) = 0\}.$$

Se poate observa că M_P este maximal, deoarece avem izomorfismul:

$$\begin{aligned} \overline{K}[V]/M_P &\longrightarrow \overline{K} \\ f &\longmapsto f(P). \end{aligned}$$

Rezultă că grupul factor M_P/M_P^2 este un $\overline{K}$-spațiu vectorial finit dimensional.

Are loc:

Propoziție 1.1: *Fie V o varietate algebrică.*

Punctul $P \in V$ este nesingular dacă și numai dacă $\dim_{\overline{K}} M_P/M_P^2 = \dim V$.

Exemplu 1.7: Reluăm cazul anterior al varietăților V_1 și V_2 (exemplul 1.6) și fie $P = (0, 0)$.

În ambele cazuri, M_P este generat de X și Y, deci M_P^2 este generat de X^2, XY și Y^2.

Pentru V_1 avem:

$$X = Y^2 - X^3 \equiv 0 \bmod M_P^2,$$

deci M_P^2 este generat doar de Y.

Dar pentru V_2 nu avem nicio relație netrivială între X și Y modulo M_P^2, deci ambele nedeterminate sînt necesare ca generatori.

Rezultă că V_1 e netedă, dar V_2 nu este, deoarece $\dim V_{1,2} = 1$.

Folosind idealul maximal, avem:

Definiție 1.6: *Inelul local* al varietății V în P, notat $\overline{K}[V]_P$, este localizatul în M_P, adică:

$$\overline{K}[V]_P = \{F \in \overline{K}(V) \mid F = f/g, \quad f, g \in \overline{K}[V], g(P) \neq 0\}.$$

Remarcăm că din $F = f/g$ rezultă că $F(P) = f(P)/g(P)$ este corect definită.

Funcțiile din $\overline{K}[V]_P$ se numesc *regulate* (sau *definite*) în P.

1.2 Varietăți proiective

INDEX