Curbe eliptice peste corpuri finite

Adrian Manea

2 noiembrie 2019

Cuprins

SECȚIUNEA 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 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

Definim varietățile proiective ca fiind colecția de linii ce trec prin originea unui spațiu afin de dimensiune imediat superioară.

Definiție 1.7: *Spațiul n-proiectiv* peste K, notat $\mathbb{P}^n$ sau $\mathbb{P}^n(\overline{K})$, este mulțimea tuturor $(n+1)$-tuplurilor $(x_0, \dots, x_n) \in \mathbb{A}^{n+1}$, astfel încît cel puțin o coordonată x_i este nenulă modulo echivalența:

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n) \iff \exists \lambda \in \overline{K}^\times \text{ a.î. } x_i = \lambda y_i, \forall i.$$

Clasa de echivalență $\{(\lambda x_0, \dots, \lambda x_n) \mid \lambda \in \overline{K}^\times\}$ se notează $[x_0, \dots, x_n]$, iar $x_0, \dots, x_n$ se numesc *coordonatele omogene* ale punctului respectiv în $\mathbb{P}^n$.

De asemenea, mulțimea punctelor K-raționale din $\mathbb{P}^n$ este:

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

Observaţie 1.2: Pentru $P = [x_0, \dots, x_n] \in \mathbb{P}^n(K)$, *nu* rezultă că fiecare $x_i \in K$. În schimb, alegem un i cu $x_i \neq 0$ și rezultă că $x_j/x_i \in K$, pentru orice j.

Definiţie 1.8: Fie $P = [x_0, \dots, x_n] \in \mathbb{P}^n(\overline{K})$. *Corpul minimal de definiție* pentru P peste K este corpul:

$$K(P) = K(x_0/x_i, \dots, x_n/x_i), \quad \forall i, \text{ cu } x_i \neq 0.$$

Definiţie 1.9: Un polinom $f \in \overline{K}[X]$ se numește *omogen de grad d* dacă:

$$f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n), \quad \forall \lambda \in \overline{K}.$$

Un *ideal omogen* al lui $\overline{K}[X]$ este generat de polinoame omogene.

Fiecărui ideal omogen îi putem asocia o submulțime a $\mathbb{P}^n$:

$$V_I = \{P \in \mathbb{P}^n \mid f(P) = 0, \text{ pentru orice } f \in I \text{ omogen } \}.$$

Definiţie 1.10: O *mulțime (algebrică) proiectivă* este una de forma V_I ca mai sus.
Idealul omogen al unei mulțimi proiective, notat $I(V)$, este idealul lui $\overline{K}[X]$ generat de:

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

Similar putem descrie și V/K și $V(K) = V \cap \mathbb{P}^n(K)$.

Exemplu 1.8: O *dreaptă* în $\mathbb{P}^2$ este o mulțime algebrică dată de $aX + bY + cZ = 0$, cu $a, b, c \in \overline{K}$, nu toate nule.
Dacă, de exemplu, $c \neq 0$, atunci dreapta este definită peste orice corp care conține a/c și b/c.
În general, un *hiperplan* în $\mathbb{P}^n$ este dat de o ecuație:

$$a_0X_0 + a_1X_1 + \cdots + a_nX_n = 0, \quad a_i \in \overline{K}, \text{ nu toate nule.}$$

Exemplu 1.9: Fie V în $\mathbb{P}^2$ dată de $X^2 + Y^2 = Z^2$.
Atunci, pentru orice corp K, cu $\operatorname{char} K \neq 2$, avem $V(K) \simeq \mathbb{P}^1(K)$, de exemplu prin:

$$\begin{aligned} \mathbb{P}^1(K) &\longrightarrow V(K) \\ [s, t] &\longmapsto [s^2 - t^2, 2st, s^2 + t^2]. \end{aligned}$$

1.2.1 Aplicație aritmetică

Fie un punct din $\mathbb{P}^n(\mathbb{Q})$, de coordonate $[x_0, \dots, x_n]$, $x_i \in \mathbb{Q}$.

Putem presupune că am înmulțit cu numitorul comun și am eliminat factorii comuni, deci putem presupune $x_i \in \mathbb{Z}, \gcd(x_i) = 1$. Rezultă că punctul P determină coordonatele omogene x_i, *pînă la un semn.*

În general, dacă un ideal al unei mulțimi algebrice definite peste $\mathbb{Q}$, $V/\mathbb{Q}$, este generat de polinoame omogene $f_1, \dots, f_m \in \mathbb{Q}[X]$, descrierea $V(\mathbb{Q})$ revine la a rezolva ecuațiile omogene:

$$f_1(x_0, \dots, x_n) = \cdots = f_m(x_0, \dots, x_n) = 0, \quad \gcd(x_i) = 1.$$

Exemplu 1.10: Fie $V : X^2 + Y^2 = 3Z^2$, definit peste $\mathbb{Q}$, dar $V(\mathbb{Q}) = \emptyset$. Într-adevăr, presupunem că $[x, y, z] \in V(\mathbb{Q})$, cu $x, y, z \in \mathbb{Z}$ și $\gcd(x, y, z) = 1$. Rezultă $x^2 + y^2 \equiv 0 \bmod 3$, dar cum -1 nu este pătrat modulo 3, rezultă că $x \equiv y \equiv 0$ modulo 3, deci $x^2, y^2 \vdots 3^2$, adică $3 \mid z$, contradicție cu $\gcd(x, y, z) = 1$.

Așadar, ideea generală este că, pentru a arăta că $V(\mathbb{Q}) = \emptyset$, este suficient să arătăm că ecuațiile omogene corespunzătoare nu au soluții nenule *modulo p*, pentru orice prim p (sau pentru orice putere a unui prim).

Spus mai simplu, avem implicația $V(\mathbb{Q}) = \emptyset \implies V(\mathbb{Q}_p) = \emptyset$, pentru orice corp p-adic $\mathbb{Q}_p$. Mai departe, implicația poate continua cu $V(\mathbb{R}) = \emptyset$.

Însă *reciproca este falsă!* Se poate arăta că, pentru varietatea:

$$V : 3X^2 + 4Y^2 + 5Z^3 = 0,$$

avem $V(\mathbb{Q}_p) \neq \emptyset, \forall p$, dar $V(\mathbb{Q}) = \emptyset$.

Definiţie 1.11: O mulțime algebrică proiectivă se numește *varietate proiectivă* dacă idealul omogen $I(V)$ este prim în $\overline{K}[X]$.

Fie $f(Y) \in \overline{K}[Y]$. Definim:

$$f^*(x_0, \dots, x_n) = x_i^d f\left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i}\right),$$

unde $d = \deg f$ este cel mai mic întreg care face f^* polinom.

Spunem că f^* este *omogenizatul* lui f în raport cu x_i.

Definiţie 1.12: Fie $V \subseteq \mathbb{A}^n$ o mulțime algebrică afină, cu idealul $I(V)$ și fie V o submulțime a $\mathbb{P}^n$ prin:

$$V \subseteq \mathbb{A}^n \xrightarrow{\phi_i} \mathbb{P}^n$$
$$\phi_i(y_1, \dots, y_n) \mapsto [y_1, \dots, y_{i-1}, 1, y_i, \dots, y_n].$$

Închiderea proiectivă a lui V, notată $\overline{V}$, este mulțimea proiectivă al cărui ideal omogen $I(\overline{V})$ este generat de omogenizatele generatorilor lui $I(V)$.

Punctele din $V - \overline{V}$ se numesc *puncte la infinit* din V.

Exemplu 1.11: Fie V proiectivă, definită de $Y^2 = X^3 + 17$.

Rezultă că V este dată în $\mathbb{P}^2$ de:

$$\overline{Y}^2\overline{Z} = \overline{X}^3 + 17\overline{Z}^3, \quad X = \overline{X}/\overline{Z}, Y = \overline{Y}/\overline{Z}.$$

Varietatea are un singur punct la infinit, $[0, 1, 0]$, obținut din $\overline{Z} = 0$. Rezultă:

$$V(\mathbb{Q}) = \{(x, y) \in \mathbb{A}^2(\mathbb{Q}) \mid y^2 = x^3 + 17\} \cup \{[0, 1, 0]\}.$$

Definiție 1.13: Fie V/K o varietate proiectivă și fie $\mathbb{A}^n \subseteq \mathbb{P}^n$ astfel încît $V \cap \mathbb{A}^n \neq \emptyset$. Atunci se definește:

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

Corpul de funcții $K(V)$ este corpul de funcții al $V \cap \mathbb{A}^n$.

Observație 1.3: Pentru alegeri diferite ale lui $\mathbb{A}^n$, obținem izomorfisme canonice între rezultate.

Similar, *netezimea* în varietăți proiective V se traduce în $V \cap \mathbb{A}^n$.

SECȚIUNEA 2

CURBE ALGEBRICE

Printr-o *curbă algebrică* vom înțelege o varietate proiectivă de dimensiune 1. Vom lucra, în general, cu curbe netede.

Notațiile specifice sînt:

- C/K: curba C este definită peste corpul K;
- $\overline{K}(C)$: corpul de funcții al lui C peste K;
- $\overline{K}[C]_P$: inelul local al lui C în punctul P;
- M_P: idealul maximal al inelului local $\overline{K}[C]_P$.

Definiție 2.1: Fie C o curbă și $P \in C$ un punct neted.
Valuarea normalizată pe $\overline{K}[C]_P$ este dată de:

$$\begin{aligned} \mathrm{ord}_P \,:\, \overline{K}[C]_P &\longrightarrow \mathbb{N} \cup \{\infty\} \\ \mathrm{ord}_P(f) &= \sup\{d \in \mathbb{Z} \mid f \in M_P^d\}. \end{aligned}$$

Folosind $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$, putem extinde valuarea la $\mathbb{Z}$.

Un *uniformizator* pentru C în P este orice funcție $t \in \overline{K}(C)$, cu $\mathrm{ord}_P t = 1$, adică t este generator pentru dealul M_P.

Pentru C și P ca mai sus, fie $f \in \overline{K}(C)$. Se definește *ordinul* lui f în P prin $\mathrm{ord}_P f$. Dacă ordinul este pozitiv, spunem că f are zero în P; altfel, f are singularitate (pol) în P. Dacă ordinul este pozitiv, spunem că C este *definită* în P și putem calcula $f(P)$. Altfel, $f(P) = \infty$.

Exemplu 2.1: Reluăm unul dintre exemplele anterioare (exemplul 1.6):

$$C_1 \,:\, Y^2 = X^3 + X, \quad C_2 \,:\, Y^2 = X^3 + X^2.$$

Ambele curbe au cîte o singularitate la infinit. Fie $P = (0, 0)$. Atunci C_1 este netedă în P, dar C_2 nu este.

Idealul maximal M_P al lui $\overline{K}[C_1]_P$ are proprietatea că M_P/M_P^2 este generat de Y, deci:

$$\mathrm{ord}_P Y = 1, \quad \mathrm{ord}_P X = 2, \quad \mathrm{ord}_P(2Y^2 - X) = 2,$$

ultima egalitate rezultînd din $2Y^2 - X = 2X^3 + X$.

2.1 Divizori

Definiţie 2.2: Fie C o curbă algebrică. *Grupul divizorilor* curbei, notat $\mathrm{Div}C$, este grupul abelian liber ($\mathbb{Z}$-modulul) generat de punctele de pe C.

Deci orice $D \in \mathrm{Div}C$ este o sumă formală:

$$D = \sum_{P \in C} n_P(P),$$

unde $n_P \in \mathbb{Z}$ și $n_P = 0$ pentru majoritatea $P \in C$.

Gradul divizorului D se definește prin:

$$\deg D = \sum_{P \in C} n_P.$$

INDEX

BIBLIOGRAFIE

[Husemoller, 2004] Husemoller, D. (2004). *Elliptic Curves.* Springer.

[Silverman, 1994] Silverman, J. (1994). *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer.

[Silverman, 2009] Silverman, J. (2009). *The Arithmetic of Elliptic Curves.* Springer.

[Washington, 2008] Washington, L. (2008). *Elliptic Curves, Number Theory and Cryptography.* Chapman and Hall.