Uvod u aritmetiku eliptičkih krivulja

Homogene (projektivne) kordinate - 4. lekcija

Za pravilno definiranje mnogih pojmova i formuliranje mnogih tvrdnja često je potrebno upotpuniti (proširiti) područje razmatranja. Tipične konstrukcije tog tipa su
(1) proširivanje brojnog područja do polja kompleksnih brojeva (ili do nekog algebarski zatvorenog polja)
(ii) upotpunjenje (do potpunog prostora - u kojemu Cauchyjevi nizovi konvergiraju) (iii) kompaktifikacija.

Uvodjenje homogenih koordinata odnosno dodavanje geometrijskim objektima "beskonačno dalekih točaka" u biti je proširenje tipa (iii) iako je nastalo daleko prije topologije. Razmotrit ćemo dva aspekta homogenih koordinata: aritmetički i geometrijski.
Aritmetički aspekt. Razmotrimo jednadžbu

$$x^2 + y^2 = 1 \tag{1}$$

gdje rješenja gledamo u skupu racionalnih brojeva (ta je jednadžba **nehomogena**). Zamjenom $x = \frac{X}{Z},\ y = \frac{Y}{Z}$, gdje su X, Y, Z cijeli brojevi i množenjem s nazivnikom dobijemo **homogenu jednadžbu**

$$X^2 + Y^2 = Z^2 \tag{2}$$

čija rješenja razmatramo u skupu cijelih brojeva. Ako želimo uspostaviti korespodenciju medju rješenjima jednadžba (1) i (2) prirodno je:
(i) izbaciti trivijalno rješenje $(0, 0, 0)$ koje je rješenje svake homogene jednadžbe.
(ii) poistovjetiti ekvivalentna rješenja, tj. rješenja (a, b, c) i $(ka, kb, kc),\ k \neq 0$ homogene jednadžbe (na primjer, rješenja $(3, 4, 5)$ i $(30, 40, 50)$) jer oni odgovaraju istom rješenju nehomogene jednadžbe.
Slično bismo postupili s jednadžbom

$$x^2 - y^2 = 1 \tag{3}$$

i pripadnom homogenom jednadžbom

$$X^2 - Y^2 = Z^2 \tag{4}$$

samo što bi se tu javila jedna novina: homogena jednadžba ima i klasu cjelobrojnih rješenja za koje je $Z = 0$, to je klasa rješenja ekvivalentnih $(1, -1, 0)$ koja ne dolazi od rješenja nehomogene jednadžbe.
Zaključimo: Svakoj polinomijalnoj jednadžbi $f(x, y) = 0$ s cjelobrojnim koeficijentima može pridružiti homogena polinomijalna jednadžba $F(X, Y, Z)$ s cjelobrojnim koeficijentima. Rješenje homogene jednadžbe je klasa ekvivalentnosti trojaka (a, b, c), različitih od $(0, 0, 0)$, tako da je $F(a, b, c) = 0$ (da bismo naznačili da je riječ o klasi često pišemo $[a, b, c]$). Tako see skup racionalnih rješenja od $f(x, y) = 0$ prirodno ulaže u skup rješenja jednadžbe $F(X, Y, Z) = 0$. Medjutim, to ulaganje općenito nije surjekcija, tj. postoji (najviše konačno) dodatnih rješenja homogene jednadžbe (sa svojstvom $Z = 0$).
Geometrijski aspekt. Ako jednadžbe (1)-(4) ili, općenito, jednadžbu

$$f(x, y) = 0$$

shvatimo geometrijski, onda su njihova rješenja točke na pripadnoj (afinoj, ravninskoj) krivulji, pa se postavlja pitanje kako geometrijski treba interpretirati moguća nova rješenja homogene jednadžbe

$$F(X, Y, Z) = 0.$$

Pri tom ne moramo ostati samo na racionalnim rješenjima već i na realnim, kompleksnim i sl. Odgovor je da ih treba interpretirati u **projektivnoj ravnini** koja je proširenje **afine ravnine** beskonačno dalekim točkama. Ta je konstrukcija nastala neovisno o postavljenom problemu, iz čisto geometrijskih razloga, odnosno problema s perspektivom koju su započeli slikari talijanske renesanse.
U **afinoj ravnini** $\mathbf{A}^2$ dvije točke odredjuju točno jedan pravac (koji njima prolazi), dok dva pravca gotovo uvijek odredjuju jednu točku (njihovo sjecište - postoji ako pravci nisu usporedni). Da bi se otklonila ta nesimetrija, geometri su uveli dodatne (beskonačno daleke) točke kao sjecišta usporednih pravaca, za svaki smjer po točku i dobili projektivnu ravninu $\mathbf{A}^2$. Same beskonačno daleke točke organizirane su u **projektivni pravac** $\mathbf{P}^1$ koji je upotpunjenje afinog pravca $\mathbf{A}^1$ beskonačno dalekom točkom ∞. Dakle, na skupovnoj razini:

$$\mathbf{P}^2 = \mathbf{A}^2 \cup \mathbf{P}^1, \ \mathbf{P}^1 = \mathbf{A}^1 \cup \infty$$

Naime smjerovi u ravnini u korespodenciji su s koeficijentima smjerova, a to su svi realni brojevi i ∞ kao koeficijent smjera y-osi.

Sve ovo vrijedi ako gledamo realne točke, kada pišemo $\mathbf{A}^1(\mathbf{R})$, $\mathbf{P}^1(\mathbf{R})$ $\mathbf{A}^2(\mathbf{R})$, $\mathbf{P}^2(\mathbf{R})$, kompleksne $\mathbf{A}^1(\mathbf{C})$, $\mathbf{P}^1(\mathbf{C})$ $\mathbf{A}^2(\mathbf{C})$, $\mathbf{P}^2(\mathbf{C})$, racionalne $\mathbf{A}^1(\mathbf{Q})$, $\mathbf{P}^1(\mathbf{Q})$ $\mathbf{A}^2(\mathbf{Q})$, $\mathbf{P}^2(\mathbf{Q})$ itd.

Veza homogenih koordinata i projektivnog pravca. Možemo pisati:
$\mathbf{P}^1(\mathbf{R})$ = skup svih smjerova u afinoj ravnini $\mathbf{A}^2(\mathbf{R})$
= skup svih pravaca kroz ishodište u $\mathbf{A}^2(\mathbf{R})$
$= \{Au - Bv = 0 :\ A, B \in \mathbf{R},\ A \neq 0 \ ili \ B \neq 0\}/\sim$, gdje se $\sim$ odnosi na ekvivalentne jednadžbe
$= \{(A, B) \in \mathbf{R}^2,\ A \neq 0 \ ili \ B \neq 0\}/\sim$.
Vidimo da smo dobili homogene koordinate (samo sad su dvije). Klasa koordinata $[1, 0]$ odgovara beskonačno dalekoj točki pravca (ili koeficijentu smjera ∞, dok afinim točkama odgovara koeficijent smjera $\frac{A}{B}$). Uočite ulaganje afinog pravca u projektivni pravac formulom

$$x \mapsto [x, 1]$$

gdje je x afina koordinata, dok za homogene koordinate X, Z imamo vezu

$$x = \frac{X}{Z}$$

za afine točke (tj. za $Z \neq 0$).
Analogno, projektivna ravnina zadaje se homogenim koordinatama X, Y, Z, gdje je $Z = 0$ jednadžba beskonačno dalekog pravca (to je projektivni pravac i svaki se afini pravac nadopunjuje po jednom točkom beskonačno dalekog pravca i tako se dobije projektivni pravac). U analogiji s tim pravcem imamo ulaganje afine ravnine u homogenu formulom

$$(x, y) \mapsto [x, y, 1]$$

a za afine točke (tj. za $Z \neq 0$) imamo

$$x = \frac{X}{Z},\ y = \frac{Y}{Z}.$$

Zaključak. "Nova" rješenja iz homogene jednadžbe interpretiraju se kao rješenja u projektivnoj ravnini, tj. rješenja u beskonačnosti (odnosno na beskonačno dalekom pravcu).

Primjer 1. $E_0 : y^2 = x^3 + Ax + B$ tipična je jednadžba afine eliptičke krivulje. Pripadna homogena jednadžba je $E : Y^2Z = X^3 + AXZ^2 + BZ^3$.

Ako želimo odrediti "nove" točke, u tu jednadžbu stavimo $Z = 0$ i dobijemo $X = 0$, a odatle $Y \neq 0$, pa možemo staviti $Y = 1$, tj. $O = [0, 1, 0]$ jedina je beskonačno daleka točka, što pišemo kao $E = E_0 \cup O$. Možemo zamišljati da beskonačno daleki pravac $Z = 0$ siječe krivulju E u jednoj točki (taj pravac je tangenta, a O je trostruka točka - kažemo da je to **točka infleksije** ili **fleks**).

Afini pokrivači projektivnog pravca i ravnine.
Skup zadan jednadžbom $Z \neq 0$ na projektivnom pravcu obični je afini pravac $\mathcal{U}$ s prirodnom koordinatom $x = \frac{X}{Z}$. Slično je sa skupom $\mathcal{V} : X \neq 0$ - i to je afini pravac koji sadrži ∞, a na njemu je prirodna koordinata $t = \frac{Z}{X}$. Uočite da na $\mathcal{U} \cap \mathcal{V}$ vrijedi $t = \frac{1}{x}$. Sjetite se Riemannove sfere kod koje je $\frac{1}{z}$ koordinata "oko ∞". Skupovi $\mathcal{U}, \mathcal{V}$ su najjednostavniji otvoreni afini pokrivač projektivnog pravca u **topologiji Zariskog**. U toj topologiji zatvoreni su: prazni skup, cijeli pravac i konačni skupovi točaka.
Slično, skup zadan jednadžbom $Z \neq 0$ u projektivnoj ravnini, obična je afina ravnina $\mathcal{U}$ s prirodnim koordinatama $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$. Slično je sa skupovima $\mathcal{V} : X \neq 0$ i $\mathcal{W} : Y \neq 0$ - i to su afine ravnine, a na njima su prirodne koordinate $r = \frac{Y}{X}$, $w = \frac{Z}{X}$, odnosno $u = \frac{X}{Y}$, $v = \frac{Z}{Y}$. Uočite da na $\mathcal{U} \cap \mathcal{V}$ vrijedi $r = \frac{y}{x}$ i $w = \frac{1}{x}$, dok na $\mathcal{U} \cap \mathcal{W}$ vrijedi $u = \frac{x}{y}$ i $v = \frac{1}{y}$. Skupovi $\mathcal{U}, \mathcal{V}, \mathcal{W}$ su najjednostavniji otvoreni afini pokrivač projektivne ravnine u **topologiji Zariskog**. U toj topologiji zatvoreni su: prazni skup, cijeli pravac, konačni skupovi točaka, konačne unije krivulja i njihove konačne unije.

Singularne točke .
Ravninskom krivuljom smatramo skupom (kompleksnih) rješenja u projektivnoj ravnini jednadžbe

$$F(X, Y, Z) = 0$$

gdje je F nerastavljiv (ireducibilan) homogeni polinom različit od 0. Pripadna afina krivulja ima jednadžbu

$$f(x, y) = 0$$

gdje je $f(x, y) := F(x, y, 1)$. Naravno da ima i drugih izbora za afinu jednadžbu, na primjer $g(u, v) = 0$, gdje je $g(u, v) := F(u, 1, v)$. Projektivna krivulja može imati najviše *novih* točaka koliki je stupanj polinoma F.
Intuitivno, točka na krivulji je **nesingularna** ako je u njoj jednoznačno definirana tangenta, inače je **singularna**. Za afinu krivulju, to znači:
Točka $P = (a, b)$ na $C_0 : f(x, y) = 0$ je nesingularna ako je $\frac{\partial f}{\partial x}(a, b) \neq 0$ ili

$\frac{\partial f}{\partial y}(a,b) \neq 0$. Tada je jednadžba tangente

$$\frac{\partial f}{\partial x}(a,b)(x-a) + \frac{\partial f}{\partial y}(a,b)(y-b) = 0 \tag{5}$$

Drugim riječima, ako f rastavimo u Taylorov red oko (a,b) kao

$$f = f_0 + f_1 + ... + f_d,$$

gdje je f_i homogeni dio i-tog stupnja po $x-a$ i $y-b$, onda je:
(i) $P(a,b)$ je na krivulji akko $f_0 = 0$,
(ii) $P(a,b)$ je nesingularna akko $f_0 = 0$ i $f_1 \neq 0$. Uočite da je, općenito, $f_1 =$ lijeva strana od (5), tj. jednadžba tangente je $f_1 = 0$.

Primjer 2. (i) Točka $(0,0)$ singularna je točka krivulje $C_0 : y^2 = x^3 - x^2$. To se vidi izravno iz funkcije $f(x,y) := y^2 + x^2 - x^3$ što je razvoj oko $(0,0)$ pa vidimo da je linearni dio jednak nuli, ali i iz $\frac{\partial f}{\partial x}(0,0) = \frac{\partial f}{\partial y}(0,0) = 0$.
(ii) Točka $O = [0,1,0]$ na krivulji $E : Y^2Z = X^3 + AXZ^2 + BZ^3$ je nesingularna. Da to dokažemo, afinu jednadžbu gledamo u ravnini $Y \neq 0$:

$$v = u^3 + Auv^2 + Bv^3, \ tj. \ v - u^3 - Auv^2 - Bv^3 = 0$$

gdje je $u = \frac{X}{Y}$, $v = \frac{Z}{Y}$, a O postaje $(0,0)$. Vidimo da je linearni dio u rastavu po u, v različit od 0, točnije, jednak je v pa je $v = 0$ jednadžba tangente, što bismo dobilio i parcijalnim integriranjem (formula (5)). Ako želimo jednadžbu tangente u projektivnim (homogenim) koordinatama, pišemo $\frac{Z}{Y} = 0$, tj. $Z = 0$ (beskonačno daleki pravac - što je i logično).

Umjesto (5) možemo se služiti formulom za jednadžbu tangente u homogenim koordinatama. Točka P krivulje $F(X,Y,Z) = 0$ je nesingularna akko $\frac{\partial F}{\partial X}(P) \neq 0$ ili $\frac{\partial F}{\partial Y}(P) \neq 0$ ili $\frac{\partial F}{\partial Z}(P) \neq 0$. Ako je tako, jednadžba tangente je

$$X\frac{\partial F}{\partial X}(P) + Y\frac{\partial F}{\partial Y}(P) + Z\frac{\partial F}{\partial Z}(P) = 0 \tag{6}$$

Kažemo da je krivulja nesingularna ako su joj sve točke nesingularne. Krivulja može imati najviše konačno singularnih točaka (objasnite).

Afine i projektivne zamjene koordinata.

Dvije ravninske krivulje $F(X,Y,Z) = 0$ i $G(X,Y,Z) = 0$ jednake su kao skupovi ako i samo ako su F i G proporcionalni polinomi (slično je za afine jednadžbe $f(x, y) = 0$ i $g(x, y) = 0$). Postoje medjusobno različite krivulje koje "nisu bitno različite", pa ih smatramo ekvivalentnim. Najjednostavniji primjeri ekvivalentnih krivulja jesu onih dobivenih linearnom zamjenom koordinata.

Afina zamjena koordinata - afina transformacija ravnine. To je zamjena:

$$x = ax' + by' + r, \ y = cx' + dy' + s$$

gdje su a, b, c, d, r, s koeficijenti, a da bi inverzna transformacija postojala determinanta matrice

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

treba biti različita od nule.

Takva transformacija prebacuje krivulju $f(x, y) = 0$ u njoj **afino ekvivalentnu** $g(x', y') = 0$. Pri tom se zadržava stupanj, nesingularnost, tangente itd.

Afinu transformaciju možemo shvatiti i kao transformaciju afine ravnine zadane formulom

$$(x, y) \mapsto (x', y').$$

Primjer 3. Afina transformacija $x = x' + y', \ y = x' - y'$ krivulju $xy = 1$ prebacuje u krivulju $x'^2 - y'^2 = 1$. Takjodjer, tu transformaciju možemo interpretirati kao preslikavanje afine ravnine zadane formulom

$$(x, y) \mapsto (x', y'), \ tj. \ (x, y) \mapsto (\frac{x+y}{2}, \frac{x-y}{2}).$$

Pri tom preslikavanju krivulja $xy = 1$ prelazi u krivulju $x^2 - y^2 = 1$ (tu nema crtica).

Afinoj zamjeni koordinata (transformaciji ravnine) pridružena je projektivna:

$$X = aX' + bY' + rZ', \ Y = cX' + dY' + sZ', \ Z = Z'$$

To nisu sve projektivne transformacije ravnine (već samo one koje čuvaju standardnu afinu ravninu, tj. standardni beskonačno daleki pravac). Općenito, projektivna transformacija ravnine je oblika

$$X = aX' + bY' + rZ', \ Y = cX' + dY' + sZ', \ Z = mX' + nY' + kZ'.$$