Uvod u aritmetiku eliptičkih krivulja

Izomorfizmi, automorfizmi, izogenije - 7.lekcija

Izomorfni Weierstrassovi modeli - jednadžbe.

Neka su eliptičke krivulje $(E_1, O_1), (E_2, O_2)$ zadane Weierstrassovim jednadžbama (ako ih zadamo u istoj projektivnoj ravnini onda je $O_1 = O_2 = O = [0, 1, 0]$). Projektivne transformacije ravnine koje fiksiraju O, ujedno preslikavaju afine dijelove u afine, pa možemo razmatrati samo afine transformacije. Načelno bi se moglo dogoditi da jedna Weierstrassova jednadžba prelazi u drugu i transformacijama koje nisu afine. Pokazat ćemo da to nije moguće, tj. da su dva Weierstrassova modela izomorfna ako i samo ako su afino izomorfna.
Neka su, radi jednostavnosti, eliptičke krivulje zadane afinim jednadžbama:

$$E_1 : y^2 = x^3 + Ax + B,\ E_2 : y'^2 = x'^3 + A'x' + B'$$

i neka je

$$\phi : E_1 \to E_2$$

izomorfizam algebarskih krivulja (grupni zakon privremeno zaboravljamo) koji neutralni element preslikava u neutralni, tj. $\phi(O) = O$. Tada je, za $P(x, y) \in E_1$:

$$\phi(x, y) = (\phi_1(x, y), \phi_2(x, y)) \in E_2$$

gdje su ϕ_1, ϕ_2 racionalne funkcije na E_1. Kako je ϕ izomorfizam afinih dijelova, te su funkcije regularne (svugdje definirane), pa su, prema definiciji, restrikcije polinoma dviju varijabla (na E_1). Zbog izomorfizma, postoje inverzno preslikavanje, tj.

$$\psi : E_2 \to E_1;\ \psi = (\psi_1, \psi_2)$$

gdje su ψ_1, ψ_2 restrikcije polinoma dviju varijabla (na E_2), tako da bude:

$$\psi_1(\phi_1(x, y), \phi_2(x, y)) = x \text{ i } \psi_2(\phi_1(x, y), \phi_2(x, y)) = y \tag{1}$$

što treba shvatiti kao jednakost regularnih funkcija na E_1. Osnovna poteškoća kod razmatranja ovakvih identiteta jest u tome što prsten restrikcija polinoma na afinu eliptičku krivulju E_1 nema jednoznačnu faktorizaciju, a i

inače, zapisi tih funkcija nisu jednoznačni (za razliku od jednozačnog zapisa polinoma dviju varijabla i jednoznačne faktorizacije). Uočite da svaku regularnu funkciju r na afinom dijelu od E_1 možemo jednoznačno zapisati kao $r(x,y) = r_1(x) + r_2(x)y$, gdje su r_1, r_2 polinomi i $y^2 = x^3 + Ax + B$, što dobijemo tako da y^2 sustavno zamijenimo s $x^3 + Ax + B$ itd. (slično je za regularne funkcije na afinom dijelu od E_2). Zato zapišimo:
$\phi_1(x,y) = f_1(x) + f_2(x)y;\ \phi_2(x,y) = g_1(x) + g_2(x)y,$
$\psi_1(x',y') = h_1(x') + h_2(x')y',\ \psi_2(x',y') = k_1(x') + k_2(x')y'$
gdje su $f_1, f_2, g_1, g_2, h_1, h_2, k_1, k_2$ polinomi jedne varijable (i $y'^2 = x'^3 + A'x' + B'$). Sad (1), uz ispuštanje varijable x u zapisu postaje

$$h_1(f_1 + f_2 \cdot y) + h_2(f_1 + f_2 y) \cdot (g_1 + g_2 \cdot y) = x \tag{2}$$

i

$$k_1(f_1 + f_2 \cdot y) + k_2(f_1 + f_2 y) \cdot (g_1 + g_2 \cdot y) = y. \tag{3}$$

Iako nam intuicija govori da tu mora biti da su:
f_1 i h_1 linearni, $f_2 = h_2 = g_1 = k_1 = 0$, g_2, k_2 ne-nul konstante (*),
ipak to nije tako lako izravno dokazati. Prigodna metoda za to je usporedjivanje valuacija v_O u beskonačno dalekoj točki, tj. razmatranje razvoja u beskonačni red po lokalnoj varijabli u toj točki. Ako bismo imali osnovna znanja o prstenima diskretne valuacije pridruženim nesingularnim točkama algebarske krivulje, lako bismo zaključili da je da je $v_O(x) = -2$ i $v_O(y) = -3$. Mi ćemo to sad izvesti izravno.

Valuacija u beskonačno dalekoj točki.
Jednadžbu $y^2 = x^3 + Ax + B$, kako smo već vidjeli, zamjenom $y = \frac{1}{v},\ x = \frac{u}{v}$ (što su koordinate oko O), postaje

$$v = u^3 + Auv^2 + Bv^3 \tag{4}$$

a O u (u,v) koordinatama postaje $(0,0)$. Gornju bismo jednadžbu mogli predočiti kao

$$v = \frac{u^3}{1 - Auv - Bv^2}$$

što u terminima lokalnih prstena znači da je u lokalni parametar u O, v je treća potencija od u pomnožena invertibilnom funkcijom u tom prstenu (naime $(1 - Auv - Bv^2)(0,0) = 1 \neq 0$); sve skupa znači da u ima valuaciju 1, a v valuaciju 3, što znači da $y = \frac{1}{v}$ ima valuaciju -3, a $x = \frac{u}{v}$ valuaciju $1 - 3 = -2$. Ako želimo izbjeći takvo razmatranje, primijenimo teorem o implicitnoj funkciji, prema kojemu je, oko točke $(0,0)$ jednadžbom (4) zadana

funkcija v u ovisnosti o u (tj. $v = v(u)$, tako da je $v(0) = 0$, a Taylorov razvoj te funkcije počinje s u^3. Naime, iz (4) dobijemo (u nastavku se crtice odnose na derivacije po u):
$v' = 3u^2 + Av^2 + 2Auvv' + 3Bv^2v'$, odakle je $v'(0) = 0$. Slično se dobije:
$v'' = 6u + 2Avv' + 2Avv' + 2Auv'^2 + 2Auvv'' + 6Bvv'^2 + 3Bv^2v''$, odakle je $v''(0) = 0$. Derivirajući još jednom dobijemo $v'''(0) = 6$. Zato je
$v(u) = u^3+$ članovi višeg reda
(kako smo već ranije najavili). Sad definiramo $v_O(u) = 1$, pa je $v_0(v) = 3$, odakle je $v_O(x) = -2,\ v_O(y) = -3$ itd.
U nastavku demonstriramo snagu razmatranja valuacije u beskonačnosti. Prije dokaza od $*$, ilustrirajmo kako bi dokaz izgledao na jednom višem jeziku, kojeg, nažalost, nismo razvili. Pridruživanje $x' \mapsto \phi_1(x, y);\ y' \mapsto \phi_2(x, y)$ je izomorfizam polja racionalnih funkcija na E_2 i E_1. Pri tom izomorfizmu lokalni prsteni koji odgovaraju točkama u beskonačnosti prelaze jedan u drugi. Zato mora biti $v_O(\phi_1) = -2,\ v_O(\phi_2) = -3$, odakle lako dobijemo $\phi_1(x, y) = ax + b\ phi_2(x, y) = ex + cy + d$ itd.

Izravan dokaz relacija (*)

Pri ovom dokazu, temeljni argument je da za racionalne funkcije r_1, r_2 na E_1 (odnosno E_2) očito vrijedi $v_O(r_1 + r_2) = \min\{v_O(r_1), v_O(r_2)\}$ uz uvjet da je $v_O(r_1) \neq v_O(r_2)$ (u stvari to nam je dovoljno za regularne funkcije na afinom dijelu od E_1). Kako (ϕ_1, ϕ_2) zadovoljava jednadžbu od E_2, vrijedi:

$$(g_1 + g_2 \cdot y)^2 = (f_1 + f_2 \cdot y)^3 + A'(f_1 + f_2 \cdot y) + B'. \tag{5}$$

Svaki od f_1, f_2, g_1, g_2 je ili 0 ili ima stupanj $d_1, d_2, \delta_1, \delta_2$ pa je valuacija u O lijeve strane parna (vidimo čak da je jednaka $-4\delta_1$ ili $-4\delta_2 - 6$), pa mora takva biti i na desnoj. Na desnoj strani treba gledati samo kubni dio, pa je tamo valuacija jednaka $-6d_1$ ili $-6d_2 - 9$, dakle ono prvo. To posebno za sobom povlači da je $f_1 \neq 0$ i da je valuacija od f_1 manja od valuacije od $f_2 \cdot y$. Takodjer, analogno, zbog simetrije, vrijedi za h_1 i $h_2 \cdot y$.
Sad, ako je $h_2 = 0$, onda iz (2) slijedi da je $f_2 = 0$, h_1, f_1 linearni, a onda iz (3) proizlazi da su k_2, g_2 ne-nul konstante i da je $k_1 = g_1 = 0$.
Pokažimo da predpostavka $h_2 \neq 0$ vodi u kontradikciju. Prvo, iz (2) slijedi da je valuacija od $g_1 + g_2 \cdot y$ parna, a to znači da je u (5) na lijevoj strani valuacija jednaka $-4\delta_1$, tj. $2\delta_1 = 3d_1$ pa je $\delta_1 = 3s,\ d_1 = 2s$. Još uvedimo D_1, D_2 kao stupnjeve od h_1, h_2. Sad je razlika valuacija pribrojnika s lijeve strane od (3) broj: $-2[2s(D_1 - D_2) - 3] \neq 0$, što znači da je valuacija lijeve

strane parna, a to je kontradikcija s činjenicom da je $v_O(y) = -3$.

Teorem. Neka je $E_1 : y^2 = x^3 + Ax + B,\ E_2 : y^2 = x^3 + A'x + B'$ i neka je $\phi : E_1 \to E_2$ izomorfizam algebarskih krivulja takav da je $\phi(O) = O$. Tada postoji broj $\mu \neq 0$ tako da je
$\phi(x, y) = (\mu^2 x, \mu^3 y)$. Pri tom je $A' = \mu^4 A,\ B' = \mu^6 B$.
Dokaz. Lako je provjeriti da je ovo gore izomorfizam krivulja. Obratno, prema predhodnim razmatranjima vrijedi $\phi(x, y) = (ax + b, cy + d)$. Odavde se lako dobije tvrdnja. Dovoljno je gledati relaciju

$$(cy + d)^2 = (ax + b)^3 + A'(ax + b) + B'$$

i iz nje zaključiti da je $b = d = 0$ i $c^2 = a^3$, tj. $c = \mu^3,\ a = \mu^2$ za neki μ itd.

Napomena. Slična tvrdnja vrijedi za eliptičke krivulje s Weierstrassovim modelom oblika $y^2 = x^3 + ax^2 + bx + c$. Za to je dovoljno gledati redom kompoziciju preslikavanja: prvo koje E_1 preslikava u oblik iz teorema (kratka Weierstrassova jednadžba), potom preslikavanje kao u teoremu, potom preslikavanje koje kratku W. jednadžbu vraća u običnu. Izvedite formule!

Korolar 1. Svaki izomorfizam eliptičkih krivulja (kao algebarskih krivulja) koji O preslikava u O, ujedno je i izomorfizam grupa.
I to ćemo ilustrirati za kratke W. jednadžbe (a vrijedi općenito). Sjetimo se formula iz predhodne lekcije:

$$x_3 = -x_1 - x_2 + \lambda^2 - a,\ y_3 = \lambda(x_1 - x_3) - y_1$$

gdje je $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ ako je $P \neq Q$, i $\lambda = \frac{f'(x_1)}{2y_1}$ ako je $P = Q$.
Tu je $a = 0$ i $f'(x) = 3x^2 + A$, pa uz gornja ograničenja, i uz napomenu da, ako s λ_μ označimo pripadni koeficijent smjera za točke $\phi(x_1, y_1)$ i $\phi(x_2, y_2)$, onda je $\lambda_\mu = \mu\lambda$, dobijemo:
$\phi((x_1, y_1) \oplus (x_2, y_2)) = \phi(-x_1 - x_2 + \lambda^2, \lambda(x_1 - x_3) - y_1)$
$= (\mu^2(-x_1 - x_2 + \lambda^2), \mu^3(\lambda(x_1 - x_3) - y_1)) = (-\mu^2 x_1 - \mu^2 x_2 + \lambda_\mu^2, ...)$.
Tu smo, uz gornja ograničenja, tvrdnju pokazali za prvu koordinatu. Dokažite je i za drugu i bez gornjih ograničenja.

Korolar 2. Grupa automorfizama eliptičke krivulje (kao algebarske krivulje i grupe, tj. kao algebarske grupe u karakteristici različitoj od $2, 3$) je, u pravilu grupa drugog reda $(x, y) \mapsto (x, \pm y)$, iznimno je ciklička grupa 4. ili 6. reda.

Kako svaka eliptička krivulja u karakteristici različitoj od $2, 3$ ima kratku W. jednadžbu, možemo iskoristiti teorem. Zato, iz $A' = A$ i $B' = B$ slijedi $\mu^4 = \mu^6 = 1$ (uz uvjet $A, B \neq 0$), tj. $\mu = \pm 1$, kako smo i tvrdili.
Ako je, pak, $B' = B = 0$, onda je $\mu = \pm 1, \pm i$, a ako je $A' = A = 0$, onda je $\mu = \pm 1, \pm\rho, \pm\rho^2$, gdje je ρ treći korijen iz jedinice. Pokažite da se ove grupe zaista realiziraju.

Definicija 1. Homomorfizam eliptičkih krivulja je svaki homomorfizam pripadnih grupa, koji je ujedno i morfizam algebarskih krivulja. Izogenija eliptičkih krivulja je homomorfizam koji nije nula preslikavanje. Ako postoji izogenija medju dvjema eliptičkim krivuljama, onda kažemo da su izogene. Endomorfizam je homomorfizam eliptičke krivulje u sebe. Skup svih endomorfizama od E označavamo kao End$E$.

Uočite da je End$E$ prsten s obzirom na standardno zbrajanje: $(\phi_1 + \phi_2)(P) = \phi_1(P) \oplus \phi_2(P)$; $(\phi_1 \circ \phi_2)(P) = \phi_1(\phi_2(P))$.

Napomena. (i) Sjetite se da je svaki homomorfizam surjektivan ili nula-homomorfizam - iako to nismo dokazali.
(ii) Ako primijeninimo Hurwitzowu formulu za $\phi : E_1 \to E_2$ uz standradne oznake za genus (koji je tu jednak 1) i n za stupanj morfizma, iz $2g_1 - 2 = n(2g_2 - 2) + R$, dobijemo $0 = n \cdot 0 + R$, tj. $R = 0$, pa ϕ nema grananja, tj. svaka točka iz E_2 ima točno n originala. Ta je činjenica karakteristična samo za krivulje genusa 1.
(iii) Kako je bilo za izomorfizam (iz korolara 1.), tako je za svaki morfizam eliptičkih krivulja, koji neutralni element preslikava u neutralni; može se pokazati da je on automatski i homomorfizam grupa.

Primjer 1. - homomorfizmi $[m] : E \to E$**.**
Preslikavanje $[m]$ za $m \in \mathbf{Z}$ definirano je kao

$$[m](P) = mP = P + P + ... + P \ (m \text{ puta}).$$

Iz definicije zbrajanja vidi se da su ovo homomorfizmi eliptičkih krivulja. Tvrdimo da su to različiti homomorfizmi, tj. da je $h : \mathbf{Z} \to \text{End}E;\ m \mapsto [m]$ Već smo vidjeli, da za eliptičke krivulje s jednadžbom $y^2 = f(x) := (x - e_1)(x - e_2)(x - e_3)$ vrijedi $[2](P) = O$ akko $P = O, (e_1, 0), (e_2, 0), (e_3, 0)$ što znači da $[2]$ nije konstanta pa je surjekcija (naravno, to možemo izravno

pokazati iz formula za zbrajanje). S druge, strane, ako je m neparan, a P točka 2. reda, onda je $[m]P = P$. Koristeći te dvije činjenice dokazujemo tvrdnju.

Primjer 2. Neka je $E : y^2 = x^3 + x^2 + x$; $\bar{E} = y^2 = x^3 - 2x^2 - 3x$. Definirajmo $\phi : E \to \bar{E}$ lokalno formulom $\phi(x, y) = (\frac{y^2}{x^2}, y\frac{x^2-1}{x^2})$, za $P \neq T := (0, 0)$ i $P \neq O$. Tada je ϕ definirano za svaki P i vrijedi $\phi(T) = \phi(O) = O$ pa je ϕ je izogenija eliptičkih krivulja. Pokažimo prvi dio tvrdnje izravno, a izravni dokaz druge ostavljamo vama, kao i dokaz da je gornje preslikavanje dobro definirano, tj. da je slika u $\bar{E}$.
Dokaz da je $\phi(O) = O$. ϕ proširimo na homogene koordinate:

$$\phi[X, Y, Z] = [Y^2Z, Y(X^2 - Z^2), X^2Z].$$

U lokalnim koordinatama oko O, koje smo već uveli, $u := \frac{X}{Y}$, $v := \frac{Z}{Y}$, jednadžba krivulje E je

$$v = u^3 + u^2v + uv^2,$$

a O je $(0, 0)$. Nadalje, naše preslikavanje (dijeljenjem sa srednjim v clanom, potom brojnika i nayivnika s Y^3) postaje

$$\phi(u, v) = (\frac{v}{u^2 - v^2}, \frac{u^2v}{u^2 - v^2}).$$

Iz jednadžbe dobijemo $v = u^3+u^2v+uv^2 = u^3+u^2(u^3+u^2v+uv^2)+u(u^3+u^2v+uv^2)^2 = u^3[1+(u^2+uv+v^2)+(u^2+uv+v^2)^2]$. Ako to sustavno uvrstimo u formulu za ϕ dobijemo da je $\phi(0, 0) = (0, 0)$ kako smo i tvrdili.
Slično dobijemo za preslikavanje oko $(x, y) = (0, 0)$ u (u, v) koordinate (opet nakon dijeljenja homogenih koordinata sa srednjom, potom dijeljenja brojnika i nayivnika sa Z^3) : $\phi(x, y) = (\frac{y}{x^2-1}, \frac{x^2}{y(x^2-1}) = (\frac{y}{x^2-1}, \frac{y^3}{(x^2-1)(x^2+x+1)^2})$ (nakon zamjene $x = \frac{y^2}{x^2+x+1}$ na odgovarajućem mjestu). Zato je $\phi(T) = \phi(0, 0) = (0, 0) = O$.