Uvod u aritmetiku eliptičkih krivulja

Točke konačnog reda - 15. lekcija

Vraćamo se na eliptičke krivulje nad poljem racionalnih brojeva, tj. na E s jednadžbama oblika

$$y^2 = x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3) \tag{1}$$

gdje su $a, b, c \in \mathbf{Z}$, a e_j su medjusobno različiti kompleksni brojevi. Sjetimo se oznake

$$E[n] = \{P \in E(\mathbf{C}) : nP = O\}.$$

Već smo vidjeli da su točke O, E_1, E_2, E_3, gdje su $E_i = (e_i, 0)$, rješenja jednadžbe $2P = O$. Lako se vidi da je $E_1 + E_2 = E_3$ itd. pa je $E[2]$ produkt cikličkih grupa drugog reda. Jednako tako, mogli bismo pokazati da je

$$E[3] \cong \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$$

i da se, kao skup, $E[3]$ sastoji od inleksijskih točaka (fleksova) na E. Geometrijski opisi grupe $E[n]$ za veće n bili bi vrlo složeni. Ipak, vrijedi općenito

$$E[n] \cong \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}.$$

Dakle, jednadžba $nP = O$ ima n^2 rješenja koji čine grupu izomorfnu produktu cikličkih grupa reda n. Zato postoje rješenja P_1, P_2 te jednadžbe tako da bude

$$E[n] = \{rP_1 + sP_2 : \ r, s = 0, 1, ..., n - 1\}$$

tj. r, s su cijeli brojevi jednoznačno zadani modulo n.
To najlakše vidimo ako iskoristimo činjenicu da je grupa $E(\mathbf{C})$ izomorfna grupi $\mathbf{C}/L$ za neku rešetku

$$L := \{k\omega_1 + m\omega_2\},$$

gdje su ω_1, ω_2 dva $\mathbf{R}$-linearno nezavisna kompleksna broja. Sad odmah vidimo da je

$$E[n] \cong \{r\frac{\omega_1}{n} + s\frac{\omega_1}{n} : \ r, s = 0, 1, ..., n - 1\},$$

kako smo i trebali.
Nedostatak ovog pristupa jest o tomu što vrijedi samo u karakteristici nula. Ista tvrdnja vrijedi u svakoj karakteristici p, uz uvjet da p ne dijeli n (ako p dijeli n onda vrijedi nešto slično). Za dokaz te tvrdnje (koja vrijedi i u karakteristici 0), analizira se formula za grupni zakon, pa se rekurzivno definiraju ireducibilni polinomi ϕ_n, ψ_n, ω_n u dvije varijable, s cjelobrojnim koeficijentima, tako da ϕ_n i ω_n budu relativno prostis ψ_n, a da za afinu točku $P(x, y)$ bude

$$nP = (\frac{\phi_n(P)}{\psi_n^2(P)}, \frac{\omega_n(P)}{\psi_n^3(P)}).$$

Sad se koristi činjenica da je $nP = O$ ako i samo ako je $\psi_n(P) = 0$ (vidi [S-T] ili [S]).
Vratimo se nad eliptičke krivulje nad $\mathbf{Q}$ i najavimo važan rezultat:
Za takve krivulje E točke iz $E[n]$ imaju za koordinate **algebarske brojeve**. To smo izravno vidjeli za $n = 2$, a relativno lako bismo vidjeli i za $n = 3$. Ako bismo iskoristili one rekurzivno definirane polinome, to bismo lako dokazali i općenito, medjutim dat ćemo drugi dokaz.
Prije dokaza podsjetimo na neke činjenice iz algebarske teorije brojeva.
Za broj $\alpha \in \mathbf{C}$ postoje dvije moguć nosti:
(I) Skup $\{1, \alpha, \alpha^2, ...\}$ nezavisan je nad $\mathbf{Q}$, tj. ako je $f(\alpha) = 0$ i f polinom s racionalnim koeficijentima, onda je $f = 0$.
Tada kažemo da je α **transcendentalan** Na primjer, π je transcendentalan.
(II) Skup $\{1, \alpha, \alpha^2, ...\}$ linearno je nezavisan nad $\mathbf{Q}$. Tada postoji najmanji prirodni broj n tako da $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ bude linearno nezavisan nad Q, tj. postoji **ireducibilan polinom** f stupnja n nad $\mathbf{Q}$ tako da bude $f(\alpha) = 0$ (taj je f jednoznačno definiran do na umnožak, tj. jedinstven je uz pretpostavku da mu je vodeći koeficijent jednak 1 - uočite i to da mu je, zbog ireducibilnosti, slobodni koeficijent različit od nule).
Tada kažemo da je α **algebarski broj** (stupnja n). Algebarski brojevi čine polje - **polje svih algebarskih brojeva**.
Podjela na algebarske i transcendentalne brojeve α ima karakterizaciju i u terminima polja $\mathbf{Q}(\alpha)$. Sjetimo se:
$\mathbf{Q}(\alpha) =$ [**najmanje polje koje sadrži** α] $= \{\frac{g(\alpha)}{h(\alpha)}\}$,
gdje su g, h polinomi nad $\mathbf{Q}$ i $g(\alpha) \neq 0$. Vrijedi:
(I) Ako je α transcendentalan, onda je polje $\mathbf{Q}(\alpha)$ izomorfno polju racionalnih funkcija jedne varijable $\mathbf{Q}(t)$ nad $\mathbf{Q}$. To znači da su za svaka dva transcendalna broja α, β polja $\mathbf{Q}(\alpha)$ i $\mathbf{Q}(\beta)$ izomorfna. Piosebno, to znači da ima

beskonačno mnogo ulaganja polja $\mathbf{Q}(\alpha)$ u polje kompleksnih brojeva.
(II) Ako je α transcendentalan, onda je polje $\mathbf{Q}(\alpha)$ izomorfno prstenu
$\mathbf{Q}[\alpha]$ =[**najmanji prsten koji sadrži** α] $= \{g(\alpha)\}$,
gdje su g polinomi nad $\mathbf{Q}$, što je jednako skupu svih brojeva oblika
$b_0 + b_1\alpha + b_2\alpha^2 + ... + b_{n-1}\alpha^{n-1}$; $bj \in \mathbf{Q}$, uz uvjet $f(\alpha) = 0$ za pripadni ireducibilni poliniom f stupnja n (drugim riječima, svi se nazivnici mogu racionalizirati).

Primjer 1. (i) $\mathbf{Q}(i) = \{a + bi : a, b \in \mathbf{Q}\}$. Tu je $\alpha := i,\ f(x) = x^2 + 1$.
Tu je $\frac{1}{a+bi} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$, pa se svaki nazivnik racionalizira.
(ii) $\mathbf{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbf{Q}\}$. Tu je $\alpha := \sqrt[3]{2},\ f(x) = x^3 - 2$ (kako se tu svaki nazivnik racionalizira?).
(iii) Ciklotomsko polje generirano petim korijenima iz jedinice je polje $\mathbf{Q}(\zeta) := \{b_0+b_1\zeta+b_2\zeta^2+b_3\zeta^3\}$, gdje su b_j racionalni brojevi, a ζ neki primitivni peti korijen iz jedinice (u ovom slučaju netrivijalni), na primjer $\zeta := \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$.
Tu je $f(x) = x^4+x^3+x^2+x+1$. Analogno je za svaki p-ti korijen iz jedinice, za prosti p, a za složeni je slično.

Za razliku od transcendentalnog slučaja tu je polje $\mathbf{Q}(\alpha)$ (konačnog) stupnja n nad $\mathbf{Q}$ (kao vektorski prostor) i postoji konačno, točnije točno n ulaganje polja $\mathbf{Q}(\alpha)$ u polje $\mathbf{C}$. Naime, neka je

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdot ... \cdot (x - \alpha_n).$$

Tada je α jedan od ovih α_i, a ko je

$$\sigma : \mathbf{Q}(\alpha) \hookrightarrow \mathbf{C}$$

neko ulaganje polja, tj. preslikavanje različito od nule za koje vrijedi $\sigma(x + y) = \sigma(x) + \sigma(y)$ i $\sigma(xy) = \sigma(x)\sigma(y)$ - tj. netrivijalni homomorfizam, onda je:
$0 = \sigma(0) = \sigma(f(\alpha)) = f(\sigma(\alpha))$,
pa je $\sigma(\alpha)$ neki od α_i, dakle n moguńosti. Kako je svako ulaganje σ jednoznačno odredjeno s vrijednošću $\sigma(\alpha)$ vidimo da ima konačno i to točno n ulaganja polja $\mathbf{Q}(\alpha)$ u $\mathbf{C}$.

Primjer 2.(i) Polje $\mathbf{Q}(i) = \{a + bi : a, b \in \mathbf{Q}\}$ ima dva ulaganja u $\mathbf{C}$:
(a) identitet $a + bi \mapsto a + bi$ i (b) konjugiranje $a + bi \mapsto a - bi$.

(ii) Polje $\mathbf{Q}(\sqrt[3]{2})$ ima tri ulaganja u $\mathbf{C}$:
(a) identitet
(b) $a+b\sqrt[3]{2}+c\sqrt[3]{4} \mapsto a+b\sqrt[3]{2}\rho+c\sqrt[3]{4}\bar{\rho}$, odredjeno preslikavanjem $\sqrt[3]{2} \mapsto \sqrt[3]{2}\rho$, gdje je ρ netrivijalni treći korijen iz jedinice.
(c) $a+b\sqrt[3]{2}+c\sqrt[3]{4} \mapsto a+b\sqrt[3]{2}\bar{\rho}+c\sqrt[3]{4}\rho$, odredjeno preslikavanjem $\sqrt[3]{2} \mapsto \sqrt[3]{2}\bar{\rho}$.
(iii) Polje $\mathbf{Q}(\zeta)$ iz prvog primjera ima 4 ulaganja u $\mathbf{C}$, koja se mogu opisati djelovanjem na ζ kao $\sigma_a(\zeta) := \zeta^a$, za $a = 1, 2, 3, 4$.
To je zato što je

$$x^4 + x^3 + x^2 + x + 1 = (x - \zeta)(x - \zeta^2)(x - \zeta^3)(x - \zeta^4).$$

Primjeri (i) i (iii) razlikuju se od (ii). Naime u njima je svaki σ **automorfizam** polja, tj. ulaganje u sama sebe, dok je u (2) to samo identitet, dok druga dva preslikavaju početno polje u dva druga podpolja od $\mathbf{C}$, različita od njega, ali njemu izomorfna.
U prvom slučaju kažemo da je polje **Galoisovo**. Pokazuje se da za svako polje K konačnog stupnja nad $\mathbf{Q}$ (kao vektorski prostor), postoji algebarski broj α stupnja n, tako da bude $K = \mathbf{Q}(\alpha)$ (to je **teorem o primitivnom elementu**). Zato svako Galoisovo polje K stupnja n ima točno n automorfizama. Ti automorfizmi čine grupu s obzirom na **kompoziciju** kao operaciju, to je Galoisova grupa $Gal(K/\mathbf{Q})$.

Primjer 3. U 2. primjeru (i) galoisova grupa je ciklička reda 2, a galoisova grupa u (iii) je ciklička reda 4.
Općenito Galoisove grupe ne moraju biti ni abelove, a kamoli cikličke.

Djelovanje Galoisove grupe na točke eliptičke krivulje.
Ako je

$$E : y^2 = x^3 + ax^2 + bx + c$$

definirana nad $\mathbf{Q}$, K neko Galoisovo polje (konačnog stupnja nad $\mathbf{Q}$) i $P(x, y)$ točka od E s koordinatama iz K (tj. iz $E(K)$), onda za svaki $\sigma \in Gal(K/\mathbf{Q}$ definiramo djelovanje

$$\sigma(P) := (\sigma x, \sigma y).$$

Uz dodatak $\sigma(O) = O$, to je zaista preslikavanje

$$\sigma : E(K) \to E(K).$$

Za to treba dokazati da je $\sigma(P) \in E(K)$. To je lako, naime samo treba znati da σ aditivna i multiplikativna funkcija, te da racionalne brojeve ostavlja na

miru:
$(x, y) \in E(K)$ znači da je $E = y^2 = x^3 + ax^2 + bx + c$ i $x, y \in K$. Zato je
$\sigma(y^2) = \sigma(x^3 + ax^2 + bx + c)$, tj. $\sigma(y)^2 = \sigma(x)^+ a\sigma(x)^2 + b\sigma(x) + c$,
što upravo znači da je $(\sigma(x), \sigma(y)) \in E(K)$.

Dakle, σ je dobro definirano preslikavanje, medjutim vrijedi puno više: svaki σ je automorfizam grupe $E(K)$. To znači da je

$$\sigma(P + Q) = \sigma(P) + \sigma(Q)$$

za sve $P, Q \in E(K)$ (to izlazi izravno iz definicije zbrajanja točaka, samo što dosta toga treba provjeriti - vidi [S-T]),
i da je σ injektivan (to je očito jer afine točke preslikava u afine, pa jedino O preslikava u O).

Teorem. Ako je $P \in E(K)$ i $P \in E[n]$, onda je $\sigma P \in E[n]$ za svaki $\sigma \in Gal(K/\mathbf{Q}$.
Dokaz. $P \in E[n]$ znači $nP = O$, pa je $O = \sigma(O) = \sigma(nP) = n\sigma(P)$, jer je σ automorfizam grupe $E(K)$, što znači da $\sigma(P) \in E[n]$.