Uvod u aritmetiku eliptičkih krivulja

Konstrukcija l-adske reprezentacije Galoisove grupe pridružene eliptičkoj krivulji - 22. lekcija

Fiksirajmo:
prost broj l
eliptičku krivulju E nad $\mathbf{Q}$.
Podsjetimo na niz abelovih grupa indeksiranih prirodnim brojevima n:
$E[l^n] := \{T \in E(\mathbf{C}) : l^n T = O\} \cong \mathbf{Z}/l^n\mathbf{Z} \oplus \mathbf{Z}/l^n\mathbf{Z}$,
ovo posljednje znači da je $E[l^n]$ slobodni modul ranga 2 nad prstenom ostataka $\mathbf{Z}/l^n\mathbf{Z}$, posebno, ta grupa ima n^2 elemenata.
Za svaki n postoji **prirodan** surjektivni homomorfizam množenja s l:
$[l] : E[l^{n+1}] \to E[l^n]$, $T_{n+1} \mapsto lT$, za $T_{n+1} \in E[l^{n+1}]$.
Definiramo **Tateov modul** $T_l(E)$ kao skup svih nizova točaka konačnog reda na E uskladjenih ovim homomorfizmima. Preciznije

$$T_l(E) := \{T = (T_1, T, 2, T_3, ...) : T_n \in E[l^n],\ i\ lT_{n+1} = T_n,\ \text{za sve } n\}.$$

Uočite sličnost s konstrukcijom cijelih l-adskih brojeva. Opet je riječ o inverznom limesu, tj. $T_l(E)$ je inverzni limes modula $E[l^n]$. Iz te opće konstrukcije slijedi da je $T_l(E)$ slobodan modul ranga 2 nad prstenom cijelih brojeva, medjutim to se vidi i izravno. Naime,
(i) uz zbrajanje po komponentama $T_l(E)$ je očito abelova grupa s neutralnim elementom $\mathcal{O} = (O, O, O, ...)$ i suprotnim elementom $-T := (-T_1, -T, 2, -T_3, ...)$.
(ii) $T_l(E)$ je $\mathbf{Z}_l$-modul uz pokomponentno množenje, tj.

$$aT = (a_1, a_2, a_3, ...)(T_1, T_2, T_3, ...) := (a_1T_1, a_2T_2, a_3T_3, ...).$$

Lako se može dokazati da je taj modul slobodan i ranga 2 (jer svaki od $T_l(E)$ slobodan ranga 2), medjutim dokaz ćemo na kratko izostaviti, a poslije ćemo izravno konstruirati bazu.
Prednost rada s modulom $T_l(E)$ umjesto s beskonačno modula $E[l^n]$ upravo je u tome što je to modul nad komutativnim prstenom s jedinicom bez djelitelja nule pa se može prijeći na vektorske prostore nad poljem. Tu je konstrukciju predložio Tate pedesetih godina 20. st.

Podsjetimo na polja generirana s $E[l^n]$ (uz nešto potpunije oznake):
$K_{E,l,n} = \mathbf{Q}(E[l^n])$:= polje definirano nad $\mathbf{Q}$ koordinatama točaka iz $E[l^n]$.
Vidjeli smo da je to konačno Galoisovo proširenje od $\mathbf{Q}$ jer su koordinate točaka iz $E[l^n]$ algebarski brojevi.
Kako je $E[l] \subset E[l^2] \subset ...$, vrijedi
$\mathbf{Q}(E[l]) \subset \mathbf{Q}(E[l^2]) \subset ...$, tj.
$K_{E,l,1} \subset K_{E,l,2} \subset ....$ Uvedimo oznaku:
$K_{E,l} := \bigcup_{n\geq 1} K_{E,l,n}$. Polje $K_{E,l}$ je algebarsko Galoisovo (beskonačnog stupnja). Naime, neka je $\sigma : K_{E,l} \hookrightarrow \mathbf{C}$ ulaganje polja. Treba pokazati da je $\sigma(K_{E,l}) = K_{E,l}$. Neka je $x \in K_{E,l}$, tada postoji n tako da bude $x \in K_{E,l,n}$, pa je $\sigma(x) = (\sigma|K_{E,l,n})(x) \in K_{E,l,n} \subset K_{E,l}$ (jer je $K_{E,l,n}$ Galoisovo.
Imamo, dakle, Galoisovu grupu $\mathrm{Gal}(K_{E,l}/\mathbf{Q})$, pridruženu krivulji E i prostom broju l.
Kako izgleda ta grupa?. Prije svega, ona je beskonačna. Kako je $K_{E,l,n} \subset K_{E,l}$, za svaki n, imamo prirodni homomorfizam (restrikciju):
$\mathrm{Gal}(K_{E,l}/\mathbf{Q}) \to \mathrm{Gal}(K_{E,l,n}/\mathbf{Q})$, $\sigma \mapsto \sigma|K_{E,l,n} := \sigma_n$,
s veće (beskonačne) grupu na manju, konačnu (dodatno je svojstvo da je ta restrikcija surjektivna,što je opće svojstvo Galoisovih grupa - naime automorfizam se uvijek može proširiti s Galoisova polja na Galoisovo proširenje).
Dakle, svakom σ pridružen je niz $(\sigma_1, \sigma_2, ...)$ gdje je $\sigma_n := \sigma|K_{E,l,n}$.
Taj je niz restrikcija uskladjen, tj. vrijedi $\sigma_{n+1}|K_{E,l,n} = \sigma_n$ za sve n. Automorfizam σ jednoznačno je odredjen tim restrikcijama, što opravdava oznaku

$$\sigma = (\sigma_1, \sigma_2, ...)$$

(to je jednakost u projektivnom limesu, naime $\mathrm{Gal}(K_{E,l}/\mathbf{Q})$ je projektivni limes konačnih grupa $\mathrm{Gal}(K_{E,l,n}/\mathbf{Q})$ - što mi tu nećemo koristiti već sve izravno računati).
Da to dokažemo, uočimo da svaki uskladjeni niz automorfizama $(\sigma_1, \sigma_2, ...)$ jednoznačno odredjuje automorfizam σ polja $K_{E,l}$, prema formuli $\sigma(x) := \sigma_n(x)$ za $x \in K_{E,l}$, gdje je n bilo koji indeks za koji vrijedi $x \in K_{E,l,n}$ (koji postoji jer je $K_{E,l}$ unija konačnih polja $K_{E,l,n}$ - treba uočiti da definicija ne ovisi ozboru indeksa n, što je posljedica uskladjenosti).
Podsjetimo da smo imali niz reprezentacija Galoisovih grupa (uz malo potpunije oznake)

$$\rho_{E,l,n} : \mathrm{Gal}(K_{E,l,n}/\mathbf{Q}) \to \mathrm{Aut}E[l^n]$$

u grupu automorfizama modula $E[l^n]$ (samo što smo prije te automorfizme odmah zapisivali kao 2×2 matrice - nakon izbora baze u $E[l^n]$). Ta je

reprezentacija definirana ovako: neka je $\sigma_n \in \mathrm{Gal}(K_{E,l,n}/\mathbf{Q})$ i neka je $(x_n, y_n) = T_n \in E[l^n]$ afina točka; tada je

$$(\rho_{E,l,n}\sigma_n)(T_n) = \sigma_n(T_n) := (\sigma_n x_n, \sigma_n y_n)$$

(naravno $(\rho_{E,l,n}\sigma_n)(O) := O$, gdje je O neutralni element - beskonačno daleka točka).
Reprezentacije $\rho_{E,l,n}$ su uskladjene u smislu: ako je $lT_{n+1} = T_n$, onda je

$$l(\rho_{E,l,n+1}\sigma_{n+1})(T_{n+1}) = (\rho_{E,l,n}\sigma_n)(T_n).$$

Zato je dobro definirana reprezentacija

$$\rho_{E,l} : \mathrm{Gal}(K_{E,l}/\mathbf{Q}) \to \mathrm{Aut}T_l(E)$$

$(\rho_{E,l}\sigma)(T) := ((\rho_{E,l,1}\sigma_1)(T_1), (\rho_{E,l,2}\sigma_2)(T_2), ...)$,
gdje je $\sigma = (\sigma_1, \sigma_2, ...)$ i $T = (T_1, T_2, ...)$.
Da to sve konkretiziramo, prijedjimo na matrice, a za to je dovoljno odabrati uskladjene baze u modulima $E[l^n]$. To se može napraviti na više načina. Evo jedne takve konstrukcije.
Izaberimo bazu (P_1, Q_1) za $E[l]$, tj. $E[l] = \{rP_1 + sP_2 : r, s \in \mathbf{Z}/l\mathbf{Z}\}$.
Tada možemo (vidjeli smo) izabrati bazu za (P_2, Q_2) za $E[l^2]$ tako da bude $lP_2 = P_1$ i $lQ_2 = Q_1$.
Dalje,, m ožemo izabrati bazu za (P_3, Q_3) za $E[l^3]$ tako da bude $lP_3 = P_2$ i $lQ_3 = Q_2$ itd.
Neka je, sad $\sigma = (\sigma_1, \sigma_2, ...)$. U bazi (P_1, Q_1) automorfizmu $\rho E, l, 1\sigma_1$ pridružena je 2×2 matrica $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \in Gl_2(\mathbf{Z}/l\mathbf{Z})$. Tu ćemo matricu poistovjećivati s automorfizmom, tj.
$\rho_{E,l,1}\sigma_1 = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$. Napomenimo da to znači da je $\sigma_1(P_1) = a_1P_1 + c_1Q_1$ i $\sigma_2(Q_1) = b_1P_1 + d_1Q_1$.
Slično dobijemo $\rho_{E,l,2}\sigma_2 = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in Gl_2(\mathbf{Z}/l^2\mathbf{Z})$, što znači da je $\sigma_2(P_2) = a_2P_2 + c_2Q_2$ i $\sigma_2(Q_2) = b_2P_2 + d_2Q_2$ itd.
Matrice $\begin{bmatrix} a_n & b_n \\ c_n & d_n \end{bmatrix} \in Gl_2(\mathbf{Z}/l^n\mathbf{Z})$ medjusobno su uskladjene, što znači da je
$a_{n+1} = a_n$ modulo l^n, $b_{n+1} = b_n$ modulo l^n, $c_{n+1} = c_n$ modulo l^n i $d_{n+1} = d_n$

modulo l^n za sve n.
Na primjer, kako je $\sigma_2|K_{E,l,1} = \sigma_1$ i $lP_2 = P_1$ i $lQ_2 = Q_1$, vrijedi
$a_1P_1 + c_1Q_1 = \sigma_1(P_1) = \sigma_2(P_1) = \sigma_2(lP_2) = l(\sigma_2(P_2)) = l(a_2P_2 + c_2Q_2) = a_2P_1 + c_2Q_1$. Sad iz činjenice da je (P_1, Q_1) baza s koeficijentima modulo l, iz jednoznačnosti prikaza zaključujemo da je $a_2 = a_1$ i $c_2 = c_1$ modulo l.
Tako smo dobili reprezentaciju s matricama nad prstenom cijelih l-adskih brojeva $\rho_{E,l}(\sigma) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Gl_2(\mathbf{Z}_l)$, gdje je
$a := (a_1, a_2, ...)$, $b := (b_1, b_2, ...)$, $c := (c_1, c_2, ...)$ i $d := (d_1, d_2, ...)$.
Postavlja se pitanje u kojoj bazi u modulu $T_l(E)$ je prikaz te reprezentacije. To je prikaz u bazi (P, Q) gdje je $P = (P_1, P_2, ...)$ i $Q = (Q_1, Q_2, ...)$. P, Q nisu točke eliptičke krivulje E u uobičajenom smislu, posebice, one nisu točke konačnog reda. U svakom slučaju ovako smo eksplicitno pokazali da je $T_l(E)$ slobodan modul ranga 2 nad prstenom cijelih l-adskih brojeva $\mathbf{Z}_l$.
Napomenimo da je reprezentacija $\rho_{E,l} : \mathrm{Gal}(K_{E,l}/\mathbf{Q}) \to \mathrm{Gl}_2(\mathbf{Z}_\mathrm{l}$.
Tako smo dobili familiju injektivnih reprezentacija indeksiranih eliptičkim krivuljama E nad $\mathbf{Q}$ i prostim brojevima l. To su reprezentacije različitih grupa. Da bismo uniformizirali gledište, razmotrima polje $\bar{\mathbf{Q}}$ polje svih algebarskih brojeva (ono je jedinstveno ako ga razmatramo kao podpolje polja kompleksnih brojeva $\mathbf{C}$). Tada je jednoznačno definirana Galoisova grupa $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Sad se reprezentacija $\rho_{E,l}$ može proširiti do reprezentacije od $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, tako da najprije djelujemo s restrikcijom na $\mathrm{Gal}(K_{E,l}/\mathbf{Q})$, potom da komponiramo s reprezentacijom $\rho_{E,l}$. Tu kompoziciju označavamo istom oznakom. Dakle, za $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ definiramo:
$\rho_{E,l}(\sigma) := \rho_{E,l}(\sigma|K_{E,l})$,
gdje je lijevo nova oznaka, a desno ona od prije. Tu reprezentaciju nazivamo l-adskom reprezentacijom Galoisove grupe $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, pridruženoj eliptičkoj krivulji E.
Uočimo da je jezgra reprezentacije $\rho_{E,l} : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gl}_2(\mathbf{Z}_\mathrm{l}$ grupa $\mathrm{Gal}(\bar{\mathbf{Q}}/K_{E,l})$.
Uočimo, takodjer, da je prsten cijelih l-adskih brojeva podprsten polja l-adskih brojeva $\mathbf{Q}_l$, pa imamo prirodno ulaganje grupe $\mathrm{Gl}_2(\mathbf{Z}_\mathrm{l}$ u grupu $\mathrm{Gl}_2(\mathbf{Q}_\mathrm{l}$, a time i reprezentaciju Galoisove grupe u invertibilne 2×2 matrice nad $\mathbf{Q}_l$.
Pripadni vektorski prostor je $V_l(E)$ koji se dobije iz $T_l(E)$ proširenjem skalara, tj., pomoću tenzoriranja

$$V_l(E) := T_l(E) \otimes_{\mathbf{Z}_l} \mathbf{Q}_l.$$