Uvod u aritmetiku eliptičkih krivulja

Galoisova reprezentacija - 16. lekcija

Polje $K = \mathbf{Q}(E[n])$.
Polazimo od eliptičke krivulje nad poljem racionalnih brojeva, tj. od E s jednadžbom oblika

$$y^2 = x^3 + ax^2 + bx + c \tag{1}$$

gdje su $a, b, c \in \mathbf{Z}$. Njoj je pridružena grupa

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

koja ima n^2 elemenata Dakle,

$$E[n] = \{O, (x_1, y_1), (x_2, y_2), ..., (x_m, y_m)$$

za neke kompleksne brojeve $x_1, y_1, x_2, y_2, ..., x_m, y_m$ (tu je $m = n^2 - 1$).
Tim točkama konačnog reda pridruženo je polje K generirano njenim koordinatama

$$K = \mathbf{Q}(E[n]) := \mathbf{Q}(x_1, y_1, x_2, y_2, ..., x_m, y_m).$$

To je polje **konačno generirano nad Q**, ali nije odmah jasno da je ono **konačna stupnja nad Q**, naime nije jasno da su svi x_i, y_i algebarski brojevi. Takodjer, nije odmah jasno da je K Galoisovo. Pokazat ćemo i jedno i drugo.

Teorem 1. (i) Svi x_i, y_i su algebarski brojevi. Posebno, $K = \mathbf{Q}(E[n])$ je polje algebarskih brojeva (konačna stupnja nad $\mathbf{Q}$).
(ii) Polje K je Galoisovo.
Dokaz. (i) Neka je (x, y) bilo koja točka iz $E(\mathbf{C})$. Tada mogu nastupiti dvije mogućnosti. Prva je da su i x i y algebarski brojevi, a druga je da su oba transcendentna. Naime, ako je x algebarski, onda je $\mathbf{Q}(x)$ polje algebarskih brojeva konačna stupnja, a y je drugog stupnja nad tim poljem, pa je i on algebarski (to je standardna činjenica iz teorije proširenja polja). Slično je x trećeg stupnja nad $\mathbf{Q}(y)$, pa je x algebarski ukoliko je to y.
Predpostavimo sad da su x, y oba transcendentna. Tvrdimo da ima beskonačno mnogo ulaganje polja $\mathbf{Q}(x, y)$ u $\mathbf{C}$. Naime, kako je $\mathbf{Q}(x, y) = \{A(x) + B(x)y\}$, gdje su $A(x), B(x)$ racionalne funkcije u varijabli x s racionalnim keficijentima, uz uvjet $y^2 = x^3 + ax^2 + bx + c$ (i taj je prikaz jednoznačan), za svaki

kompleksni transcendentni broj t i $s := \sqrt{t^3 + at^2 + bt + c}$ (gdje po volji biramo jedan od drugih korijena), preslikavanje

$$A(x) + B(x)y \mapsto A(t) + B(t)s$$

je ulaganje (tu $x \mapsto t$; $y \mapsto s$).
Neka je sad $(x, y) \in E[n]$ i neka je $\sigma : \mathbf{Q}(x, y) \hookrightarrow \mathbf{C}$ neko ulaganje. Tada je, kako smo vidjeli, $(\sigma(x), \sigma(y)) \in E[n]$. Zato je $\sigma x = x_i$ i $\sigma y = y_i$, za neke x_i, y_i iz gornjeg popisa. Kako ima samo konačno mogućnosti za $\sigma(x)$ i $\sigma(y)$, postoji samo konačno mnogo takvih σ. Zato x, y ne mogu biti transcendentni, pa su oba algebarski brojevi, kako smo i tvrdili.
Sad je i K konačna stupnja nad $\mathbf{Q}$, jer je generiran s konačno mnogo algebarskih brojeva (standardan zaključak) (ii) Neka je $\sigma : K \hookrightarrow \mathbf{C}$ neko ulaganje. Ono je jednoznačno odredjeno vrijednostima $\sigma(x_i), \sigma(y_i)$ za sve i. Kako su te vrijednosti opet neki x_j, y_j, vrijedi $\sigma(K) = K$, a to upravo znači da je K Galoisovo proširenje.

Analogija izmedju jedinične kružnice $\mathbf{S}^1$ i eliptičkih krivulja.
Postavlja se pitanje zašto je za matematiku relevantno razmatranje polja $K = \mathbf{Q}(E[n])$. Pokušat ćemo skicirati odgovor na to pitanje. Riječ je o jednoj manifestaciji analogije izmedju jedinične kružnice i eliptičkih krivulja, prema kojoj su ta polja viši analogoni ciklotomskih polja.
Topološka razina. Za svaki E, topološki prostor $E(\mathbf{C})$ je torus pa je $E(\mathbf{C}) \cong S^1 \times S^1$ (topološki izomorfizam).
Geometrijska razina. S^1 možemo realizirati u kompleksnoj Gaussovoj ravnini kao skup T kompleksnih rješenja jednadžbe $|z| = 1$. Multiplikativnost apsolutne vrijednosti $|z_1 z_2| = |z_1||z_2|$ uvjetuje grupnu strukturu na T (obično množenje kompleksnih brojeva).
Takodjer, S^1 se može realizirati kao skup **realnih** rješenja $C(\mathbf{R})$ jednadžbe

$$x^2 + y^2 = 1.$$

C je afina krivulja definirana nad $\mathbf{Q}$. Prirodna bijekcija izmedju točaka tih dviju realizacija $(x, y) \leftrightarrow x + iy$ prenosi grupnu strukturu na C, tako da vrijedi $(x_1, y_1)(x_2, y_2) = (x_1 y_1 - x_2 y_2, x_1 y_2 + x_2 y_1)$.
S obzirom na to da je C definirana nad $\mathbf{Q}$, prirodno je razmatrati eliptičke krivulje E definirane nad $\mathbf{Q}$. I skup E ima grupnu strukturu, ali tek nakon dodavanja beskonačno daleke točke.
Analizom točaka konačnog reda na ovim grupama vidimo:

$T[n] := \{z \in \mathbf{C} : z^n = 1\} \cong \mathbf{Z}/n\mathbf{Z}$ (izomorfizam apstraktnih grupa, ostvaruje se biranjem primitivnog n-tog korijena ζ iz 1 (na primjer $\zeta = e^{\frac{2\pi i}{n}}$), pa pridruživanja $\zeta \mapsto 1$ modulo n ; prva je grupa multiplikativna, a druga aditivna).
Potpuno je analogno s $C(\mathbf{R})[n]$, tj. $C(\mathbf{R})[n] \cong T[n] \cong \mathbf{Z}/n\mathbf{Z}$ (tu samo treba uočiti da na C gledamo samo realne točke).
Kako smo vidjeli, za svaku E (bez obzira je li definirana nad $\mathbf{Q}$ ili nad nekim većim poljem) vrijedi:
$E[n] \cong \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}$.
Vidimo da se tu topološka analogija nastavlja i na geometrijskoj razini (uz pravilnu interpretaciju).
Aritmetička razina. Sad ćemo razmatrati koordinate točaka konačnog reda na ovim krivuljama i pripadna polja koja generiraju.
Kod T dobivamo ciklotomska polja $\mathbf{Q}(\zeta)$ koja odavno zauzimaju važno mjesto u aritmetici (na primjer, Gauss ih je iskoristio za rješenje problema konstrukcije pravilnih mnogokuta). U terminima tih polja Kronecker i Weber su u drugoj polovici 19. st. opisali abelova proširenja od $\mathbf{Q}$, tj. takva Galoisova polja L za koje je Galoisova grupa $Gal(L/\mathbf{Q})$ abelova:
$L/\mathbf{Q}$ je abelovo ako i samo ako je sadržano u nekom ciklotomskom polju $\mathbf{Q}(\zeta)$.
Viši analogoni ciklotomskih polja $\mathbf{Q}(\zeta)$ trebala bi biti polja $K = \mathbf{Q}(E[n])$ (ili njima vrlo bliska). Kronecker je, s obzirom na uočenu analogiju, puno očekivao od $\mathbf{Q}(E[n])$ za eliptičke krivulje nad $\mathbf{Q}$ - njegov *Jugendtraum*
(mladenački san) bio je da pomoću njih opiše abelova proširenja kvadratno imaginarnih polja (i znao je to provesti na primjerima). Tako je nastala **teorija kompleksnog množenja** kojim je to i ostvareno.
Napomenimo da nije odmah jasno da baš $\mathbf{Q}(E[n])$ pravilno poopćuju ciklotomska polja $\mathbf{Q}(\zeta)$. Na primjer, eliptičke krivulje E (odnosno njihove jednadžbe) više sliče krivulji C, medjutim kod nje gledamo samo realne točke konačnog reda a kod E gledamo sve. Ako usporedjujemo $C[n]$ i $T[n]$ aritmetički (a ne samo kao apstraktne grupe), i ako svaku točku $(x, y) \in C[n]$ gledamo pridruženu točku $z = x + iy \in T[n]$, onda je prirodno usporedjivati polja $\mathbf{Q}(x, y)$ i $\mathbf{Q}(z)$ koja su bliska, ali ne jednaka. Vidimo da je $\bar{z} \in T[n]$, takodjer, pa je

$$x = \frac{1}{2}(z + \bar{z});\ y = \frac{1}{2i}(z - \bar{z})$$

pa je $\mathbf{Q}(i, x, y) = \mathbf{Q}(i, z)$.
Jošu veća očekivanja od polja $\mathbf{Q}(E[n])$ imali matematičari druge polovice

20. st. Nadali su se da će ih ona dovesti do netrivijalnih opisa **neabelovih proširanja** od $\mathbf{Q}$ i do tzv. neabelovih **zakona reciprociteta**. U okviru toga bilo je i rješenje slutnje Taniyama-Shimure, koja je za posljedicu imala rješenje Fermatova problema.

Reprezentacija Galoisove grupe $Gal(K/\mathbf{Q}$ **na** $E[n]$.
U ovome dijelu je fiksirana eliptička krivulja E nad $\mathbf{Q}$ i prirodan broj n. Kako smo vidjeli, postoji Galoisovo polje $\mathbf{Q}(E[n])$, generiran koordinatama točaka iz $E[n]$. Fiksirajmo i dva nezavisna rješenja P_1, P_2 jednadžbe $nP = O$ tako da je

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

tj. r, s su cijeli brojevi jednoznačno zadani modulo n.
Zato $E[n]$ možemo identificirati skupom svih dvodimenzionalnih vektora stupaca

$$\begin{bmatrix} \mathrm{r} \\ \mathrm{s} \end{bmatrix}.$$

Tako, na primjer, točkama P_1, P_2 odghovaraju vektori $\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

Kako vrijedi $\sigma(P+Q) = \sigma(P) + \sigma(Q)$, a onda i $\sigma(mR) = m\sigma(R)$ za sve točke $P, Q, R \in E[n]$ i svaki $\sigma \in Gal(K/\mathbf{Q}$, vidimo da je $\sigma(rP_1 + sP_2) = r\sigma(P_1) + s\sigma(P_2)$, za sve $r, s \in \mathbf{Z}/n\mathbf{Z}$, pa svaki σ djeluje poput **linearnog operatora** na gornjem vektorskom prostoru (točnije na slobodnom $\mathbf{Z}/n\mathbf{Z}$-modulu ranga 2).
Zato svakom σ jednoznačno pridružujemo 2×2 matricu $\rho_n(\sigma)$ s koeficijentima iz $\mathbf{Z}/n\mathbf{Z}$. Naime, jednoznačno su odredjeni $\alpha, \beta, \gamma, \delta \in \mathbf{Z}/n\mathbf{Z}$, tako da bude

$$\sigma(P_1) = \alpha P_1 + \gamma P_2; \ i \ \sigma(P_2) = \beta P_1 + \delta P_2.$$

Sad definiramo

$$\rho_n(\sigma) := \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

Djelovanje od σ na vektoru

$$\begin{bmatrix} \mathrm{r} \\ \mathrm{s} \end{bmatrix}$$

ostvaruje se običnim množenjem matrica

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} \mathrm{r} \\ \mathrm{s} \end{bmatrix}$$

sad vidimo da vrijedi

$$\rho_n(\tau \circ \sigma) = \rho_n(\tau) \cdot \rho_n(\sigma).$$

Takodjer vidimo da je

$$\rho_n(\sigma_0) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

gdje je σ_0 identički automorfizam.

Odavde dobijemo $I = \rho_n(\sigma^{-1} \circ \sigma) = \rho_n(\sigma^{-1}) \cdot \rho(\sigma)$, pa su sve $\rho_n(\sigma)$ invertibilne matrice tj. iz $Gl_2(\mathbf{Z}/n\mathbf{Z})$ i vrijedi

$$\rho_n(\sigma^{-1}) = (\rho_n\sigma)^{-1}.$$

Treba napomenuti da ovdje, za razliku od matrica nad poljem, uvjet invertibilnosti matrice A nije $det(A) \neq 0$ već $det(A) \in (\mathbf{Z}/n\mathbf{Z})^\star$, tj. da je $det(A)$ invertibilan, (izravne račune pogledajte u [S-T]).

Formuliramo važan teorem.

Teorem 2. $\rho_n : Gal(K/\mathbf{Q}) \to Gl_2(\mathbf{Z}/n\mathbf{Z})$ je injektivna **reprezentacija grupa**.

Da je ρ_n reprezentacija upravo znači $\rho_n(\tau \circ \sigma) = \rho_n(\tau) \cdot \rho_n(\sigma)$, za svaka dva τ, σ i $\rho_n(\sigma_0) = I$, što smo već vidjeli. Ostaje pokazati injektivnost, što je gotovo očito, jer ako je $\rho_n(\sigma) = I$, onda je $\sigma(P_1) = P_1$ i $\sigma(P_2) = P_2$ pa je $\sigma(P) = P$ za sve P, tj. $\sigma = \sigma_0$.