Uvod u aritmetiku eliptičkih krivulja

Galoisova reprezentacija, primjeri - 17. lekcija
Eliptičke krivulje s kompleksnim množenjem 18. lekcija

Opisat ćemo primjere Galoisovih grupa $G = Gal(K/\mathbf{Q}$ pridruženih točkama drugog ili četvrtog reda nekih eliptičkih krivulja, i pripadne grupe matrica.

Primjer 1. Neka je $E : y^2 = x^3 - x$ i $n = 2$. Tada je $E[2] = \{O, (0,0), (1,0), (-1,0)$, pa je $K = \mathbf{Q}(E[2]) = \mathbf{Q}$ i $G = \sigma_0$ je jedinična grupa. Takodjer $\rho_2(\sigma_0) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, bez obzira koje smo P_1, P_2 izabrali.

Primjer 2. Neka je $E : y^2 = x^3 + x$ i $n = 2$. Tada je $E[2] = \{O, (0,0), (i,0), (-i,0)$, pa je $K = \mathbf{Q}(E[2]) = \mathbf{Q}(i)$ i $G = \sigma_0, \sigma$, gdje je σ kompleksno konjugiranje. Znamo da je $\rho_2(\sigma_0) = I$ bez obzira koje smo P_1, P_2 izabrali. Neka je $P_1 = (0,0)$ i $P_2 = (i,0)$. Tada je $\sigma(P_1) = P_1$ i $\sigma P_2 = (-i,0) = P_1 + P_2$ pa je $\rho_2(\sigma) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.
Da smo izabrali $P_1 = (i,0),\ P_2 = (-i,0)$, bilo bi $\sigma P_1 = P_2$ i $\sigma P_2 = P_1$ pa bi bilo $\rho_2(\sigma) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Primjer 3. Neka je $E : y^2 = x^3 + x$ i $n = 4$. Da bismo odredili $E[4]$ napišimo formulu za dupliciranje. Dobijemo, ako je $P(x,y)$, onda je

$$2P = (\frac{x^4 - 2x^2 + 1}{4y^2}, \frac{x^6 + 5x^4 - 5x^2 - 1}{8y^3}).$$

Sad zaključujemo ovako: $4P = O$ akko $2(2P) = O$ a to je akko $y(2P) = 0$ tj. $x^6 + 5x^4 - 5x^2 - 1 = 0$. Rješenja te jednadžbe jesu $1, -1$ te rješenja bikvadratne jednadžbe $x^4 + 6x^2 + 1 = 0$, tj. $\pm\alpha, \pm\alpha^{-1}$, gdje je $\alpha := (\sqrt{2} - 1)i$. Ako još stavimo $\beta := (1+i)(\sqrt{2} - 1)$, dobijemo:
$E[4] = \{O, (0,0), (\pm i, 0), (1, \pm\sqrt{2}),$
$(-1, \pm i\sqrt{2}), (\alpha, \pm\beta), (-\alpha, \pm i\beta), (\alpha^{-1}, \pm\alpha^{-2}\beta), (-\alpha^{-1}, \pm i\alpha^{-2}\beta)\}$.
Vidimo da je

$$K = \mathbf{Q}(E[4]) = \mathbf{Q}(i, \sqrt{2}) = \{a + bi + c\sqrt{2} + d\sqrt{2}i : a, b, c, d \in \mathbf{Q}\},$$

proširenje četvrtog stupnja. Vidimo dalje da je

$$G := Gal(K/\mathbf{Q} = \{\sigma_0, \sigma, \tau, \sigma\tau\},$$

umnožak cikličkih grupa drugog reda σ_0, σ i σ_0, τ, gdje je:
$\sigma(i) = -i,\ i\ \sigma(\sqrt{2}) = \sqrt{2}$ i $\tau(i) = i,\ i\ \tau(\sqrt{2}) = -\sqrt{2}$.
Vidimo da vrijedi $\sigma\tau = \tau\sigma$ i da taj automorfizam mijenja predznak i od i i od $\sqrt{2}$.
Da bismo odredili ρ_4 treba izabrati bazu P_1, P_2. Prve tri navedene točke su iz $E[2]$ pa nisu dobre. Neka je $P_1 = (1, \sqrt{2})$ i $P_2 = (\alpha, \beta)$. To je baza od $E[4]$.
Naime, $2P_1 = (0,0),\ 3P_1 = (1, -\sqrt{2}) = -P_1,\ 4P_1 = O$. Takodjer,
$2P_2 = (i, 0),\ 3P_2 = (\alpha, -\beta) = -P_2,\ 4P_2 = O$.
Vidimo dalje $\sigma P_1 = P_1,\ \sigma P_2 = (-\alpha, -i\beta)$, dok je
$\tau P_1 = -P_1,\ \tau P_2 = (\alpha^{-1}, \alpha^{-2}\beta)$.
Odredite $\rho_4(\sigma)$ i $\rho_4(\tau)$ u toj bazi.

Primjer 4. Neka je $E : y^2 = x^3 - 2$ i $n = 2$. Vidimo da je
$E[2] = \{O, (\sqrt[3]{2}, 0), (\rho\sqrt[3]{2}, 0), (\bar{\rho}\sqrt[3]{2}, 0)\}$,
gdje je ρ primitivni treći korijen iz jedinice, na primjer $\rho = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ (uočite da je $\bar{\rho} = \rho^2$ - taj broj treba razlikovati od reprezentacije ρ_n). Tada je $K = \mathbf{Q}(E[2]) = \mathbf{Q}(\rho, \sqrt[3]{2}) = \mathbf{Q}(\sqrt{-3}, \sqrt[3]{2})$. To je proširenje šestog stupnja (kompozit proširenja drugog i trećeg stupnja). Galoisova grupa je simetrična grupa S_3, konkretnije:
$Gal(K/\mathbf{Q} = \{\sigma_0, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, gdje su σ, τ definirani tako da bude:
$\sigma(\sqrt[3]{2}) := \rho\sqrt[3]{2},\ \sigma(\sqrt{-3}) = \sqrt{-3}$ i $\tau(\sqrt[3]{2}) := \sqrt[3]{2},\ \tau(\sqrt{-3}) = -\sqrt{-3}$
Izravno se provjeri da je $\sigma^3 = \tau^2 = \sigma_0$, i da je $\tau\sigma = \sigma^2\tau$ i $\tau\sigma^2 = \sigma\tau$.
Na primjer, $\tau\sigma^2(\sqrt[3]{2}) = \tau\sigma(\rho\sqrt[3]{2}) = \tau(\rho^2\sqrt[3]{2}) = (\bar{\rho})^2\sqrt[3]{2} = \rho\sqrt[3]{2}$, dok je $\sigma\tau(\sqrt[3]{2})\sigma(\sqrt[3]{2} = \rho\sqrt[3]{2}$, pa se ta dva automorfizma poklapaju na $\sqrt[3]{2}$. Slično bismo dobili s $\sqrt{-3}$ itd.
Stavimo $P_1 = (\sqrt[3]{2}, 0)$ i $P_2 = (\rho\sqrt[3]{2}, 0)$. Tada je P_1, P_2 baza od $E[2]$ i $P_1 + P_2 = (\bar{\rho}\sqrt[3]{2}, 0)$.
Vidimo da je $\sigma(P_1) = P_2,\ \sigma(P_2) = P_1 + P_2$ i da je $\tau(P_1) = P_1 + P_2$. Zato je
$\rho_2(\sigma) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ i $\rho_2(\tau) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.
Sad se lako dobije da je $\rho_2(\sigma^2) = (\rho_2(\sigma))^2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, $\rho_2(\sigma\tau) = \rho_2(\sigma)\rho_2(\tau) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, i, konačno $\rho_2(\sigma^2\tau) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

Vidimo da smo dobili da je $\rho_2(G) = Gl_2(\mathbf{Z}/2\mathbf{Z})$, odnosno da su u slici sve moguće matrice nmad poljem od dva elementa.
Sad je relativno lako provjeriti da je G simetrična grupa S_3, točnije da je njoj izomorfna (tako što se pokaže da je $\rho_2(G)$ izomorfna S_3). Što se tiče strukture podgrupa od G, element σ generira cikličku grupu (koja odgovara alternativnoj grupi A_3 i ona je normalna), dok $\tau, \sigma\tau, \sigma^2\tau$ generiraju cikličke poodgrupe 2. reda (koje nisu normalne). Na primjer,
$(\sigma\tau)^2 = \sigma\tau\sigma\tau = \sigma\sigma^2\tau\tau = \sigma_0$.
Izravna realizacija grupe G kao S_3, jest da ona permutira skup $\{\sqrt[3]{2}, \sqrt[3]{2}\rho, \sqrt[3]{2}\rho^2\}$.

To je bio prvi primjer u kojemu konstruirano polje K nije bilo abelovo. Naime, kako smo vidjeli, grupa S_3 nije abelova (to je najmanja neabelova grupa). To je ujedno bio i prvi primjer kad je slika grupe G pri reprezentaciji ρ_n čitava opća linearna grupa nad brojevima modulo n. Može se pokazati (iako ne lako) da je to pravilo, a ne izuzetak (s obzirom na eliptičke krivulje, a na neki način, i na brojeve n). Naime, eliptičke krivulje dijelimo na one s **kompleksnim množenjem**, tj. koje imaju netrivijalne homomorfizme (endomorfizme)

$$\phi : E \to E$$

(nad $\mathbf{Q}$, a i općenito, one su rijetkost), i ostale. Trivijalni homomorfizmi su oni oblika $P \mapsto mP$ za $m \in \mathbf{Z}$. J.P.Serre je dokazao da za svaku eliptičku krivulju nad $\mathbf{Q}$ bez kompleksnog množenja postoji prirodan broj N tako da za sve $n \geq N$ koji su relativno prosti s N vrijedi $\rho_n(G) = Gl_2(\mathbf{Z}/n\mathbf{Z})$.
Kako su grupe $Gl_2(\mathbf{Z}/n\mathbf{Z})$ neabelove (osim za $n = 1$), tako smo dobili mnogo neabelovih proširenja od $\mathbf{Q}$ (pridruženih eliptičkim krivuljama).

Treba napomenuti da Primjer 4 nije dobar za ilustraciju Serreova rezultata. Naime, $E : y^2 = x^3 - 2$ je eliptička krivulja s kompleksnim množenjem. Zaista, preslikavanje

$$\phi : E \to E;\ (x, y) \mapsto (\rho x, y)$$

je automorfizam od E, što se izravno provjeri (tu je, opet, ρ primitivni treći korijen iz 1).
On je zato različit od svakog preslikavanja $P \mapsto mP$, pa je to primjer kompleksnog množenja.
Ovdje treba uočiti da je polje $\mathbf{Q}(E[3])$ abelovo nad poljem $\mathbf{Q}(\rho)$ (upravo poljem nad kojim je definirano kompleksno množenje). Može se pokazati da

slično vrijedi za sve eliptičke krivulje s kompleksnim množenjem, naime da su pripadne grupe abelove ili "gotovo abelove".

Sad ćemo samo skicirati jedan primjer, koji upotpunjuje Primjere 1, 2 i 3. Za detalje pogledajte [S-T, str. 191].

Primjer 5. Neka je $E : y^2 = x^3 + x$ i $n = 3$. Koristeći se duplikacijskom formulom iz Primjera 3. i činjenicom da $3P = O$ ako i samo ako je $2P = -P$, dobije se da je G nekomutativna grupa reda 16 (inače $Gl_2(\mathbf{Z}/3\mathbf{Z})$ ima 48 elemenata, pa tu slika od G nije maksimalna.

Eliptičke krivulje s kompleksnim množenjem.

U nastavku ćemo se poslužiti identifikacijom kompleksnih eliptičkih krivulja s kompleksnim torusima $\mathbf{C}/L$ da bismo opisali eliptičke krivulje s kompleksnim množenjem i njihove endomorfizme.

Sjetimo se da za svaku kompleksnu eliptičku krivulju E postoji dvostruko periodna funkcija $\mathcal{P}$ (s rešetkom perioda $L := \{r\omega_1 + s\omega_2$ gdje su r, s cijeli brojevi, a ω_1, ω_2 dva izabrana nezavisna perioda), tako da preslikavanje kompleksne ravnine

$$z \mapsto (\mathcal{P}(z), \mathcal{P}'(z))$$

postaje analitički izomorfizam izmedju $\mathbf{C}/L$ i $E(\mathbf{C})$ (tu treba pravilno tretirati beskonačno daleke točke, a E napisati u posebnom obliku). Naime, tu pripadnu krivulju E treba predočiti jednadžbom, tradicionalno pisanom kao

$$y^2 = 4x^3 - g_2x - g_3$$

što se uvijek može, a g_2, g_3 jednoznačno su odredjeni s L.
Kako su $\mathcal{P}, \mathcal{P}'$ analitičke kompleksne funkcije osim točkama rešetke L, analitičnost gornjeg preslikavanja, upravo znači da su gornje koordinatne funkcije analitičke. Kako vidimo, to i jest, ali za $\mathbf{C}/L\backslash\{\tilde{0}\}$ i afine točke na $E(\mathbf{C})$, tj na $E(\mathbf{C}) \setminus \{\mathbf{O}\}$ (tu smo s tildom označili klase kompleksnih brojeva modulo L, i napomenimo da ima malo problema s dokazivanjem surjektivnosti gornjeg preslikavanja).
Ostaje vidjeti da se preslikavanje analitički produžuje i na neutralne elemente, tj. na okoline oko nule u torusu odnosno od O u eliptičkoj krivulji. Oko O su, kako smo vidjeli, koordinate (u, v) pri čemu je $O = (0, 0)$, a izvan O vrijedi
$(u, v) = (\frac{x}{y}, \frac{1}{y})$.
Kako je $(x, y) = (\mathcal{P}(z), \mathcal{P}'(z))$ za z oko 0 (ili, što je ekvivalentno za z oko nekog elementa od L), onda je

$$z \mapsto (\frac{\mathcal{P}'(z)}{\mathcal{P}(z)}, \frac{1}{\mathcal{P}'(z)})$$

analitičko preslikavanje iz otvorene okoline 0 (bez nule), u otvorenu okolinu od O (bez O). Medjutim, kako $\mathcal{P}$ ima u 0 pol 2. reda, a $\mathcal{P}'$ pol 3. reda, vidimo da su prekidi u gornjim razlomcima za $z = 0$ uklonjivi, pa se preslikavanje

produljuje po analitičnosti i na 0, s vrijednošću O, kako smo i trebali.
Tome treba dodati da je ova anlitička bijekcija medju točkama kompleksnog torusa i $E(\mathbf{C})$ ujedno i izomorfizam grupa. To proizlazi iz transformacijskih svojstava funkcija $\mathcal{P}, \mathcal{P}'$ s jedne strane i definicije grupnog zakona na na E (odnosno pripadnih formula).

Sad je svakom (netrivijalnom) endomorfizmu

$$\phi : E \to E$$

jednoznačno pridružen analitički endomorfizam

$$f : \mathbf{C}/L \to \mathbf{C}/L$$

(to da je f analitički upravo znači da se lokalno zapisuje analitičkim funkcijama). Razlog tomu ješto se endomorfizam oko svake točke zapisuje racionalnim funkcijama (kojima se nazivnik ne poništava u toj točki), a to onda kod torusa prelazi u analitičke funkcije.
Netrivijalniji je dio da svakom analitičkom endomorfizmu f torusa odgovara racionalno preslikavanje kod eliptičkih krivulja (s grupnom strukturom nema problema). Općenito ova se problematika najbolje opisuje u terminima Riemannovih ploha, ali mi ćemo postapak provesti izravno. Na malim okolinama U, V oko 0 u $\mathbf{C}$ funkcija f odredjuje običnu analitičku funkciju
$F : U \to V$ tako da je $F(0) = 0$ (jer f klasu od nule preslikava u klasu od nule).
Nadalje f je homomorfizam pa je

$$F(z_1 + z_2) - F(z_1) - F(z_2) \in L$$

za sve $z_1, z_2 \in U$ tako da je i $z_1 + z_2 \in U$. Kako u V ima samo konačno mnogo elemenata od L, možemo ga smanjiti (U takodjer - sve to jer je F neprekinuta) tako da tu bude samo 0 i da svaki rezultat $t_3 - t_1 - t_2$ za $t_1, t_2, t_3 \in V$ bude u krugu oko 0 koji od L sadrži samo 0. Tada će biti

$$F(z_1 + z_2) = F(z_1) + F(z_2)$$

za svaka dva $z_1, z_2 \in U$ tako da je i $z_1 + z_2 \in U$. Fiksirajmo sad $z_0 \in U$. Neka je U' mali otvoreni krug oko 0 u U, takav da je za svaki $z \in U'$ ispunjeno da je $z + z_0 \in U$. Tada je

$$F(z + z_0) = F(z) + F(z_0),$$

za svaki $z \in U'$. Sad je
$F'(z_0) := \lim_{h\to 0} \frac{F(z_0+h)-F(z_0)}{h}$,
a kako h možemo uzimati iz U' i kako je $F(0) = 0$, dobijemo $F'(z_0) = F'(0)$ (tu smo koristili da je f analitičko preslikavanje, pa je F analitička funkcija). Kako to možemo uraditi za svaki $z_0 \in U$ vidimo da postoji kompleksan broj $c \neq 0$ tako da bude
$F(z) = cz$, za sve $z \in U$. Zato je (uz dogovor da tildom označavamo klase modulo L i podsjećanje da je $\widetilde{(z+t)} = \tilde{z} + \tilde{t}$ i $m\tilde{z} = \widetilde{(mz)}$):
$f(\tilde{z}) = \tilde{cz}$ za $\tilde{z}$ oko $\tilde{0}$.
Dalje, neka je sad $z \in \mathbf{C}$ bilo koji. Tada postoji n tako da $\frac{z}{n} \in U$, pa je $f(\widetilde{(\frac{z}{n})}) = (c\widetilde{\frac{z}{n}})$, odakle se množenjem s n i uzimajući u obzir da su f i tilda homomorfizmi dobije $f(\tilde{z}) = \tilde{cz}$, tj.

$$f(z \text{ modulo } L) = cz \text{ modulo } L.$$

Posebno, za svaki $\omega \in L$ vrijedi $\tilde{0} = f(\tilde{0}) = f(\omega) = \tilde{c\omega}$, što znači da c nije bilo kakav, već da vrijedi

$$cL \subset L.$$

Sad je sve spremno za opisivanje endomorfizama eliptiqv ckih krivulja (nad kompleksnim brojevima).

Kompleksno množenje eliptičkih krivulja. Taj pojam ima smisla u svakoj karakteristici, ali mi se ograničavamo na karakteristiku 0.

Teorem 1. (i) Skup endomorfizama $End(\mathbf{C}/L)$ od $\mathbf{C}/L$ je u bijekciji sa skupom svih kompleksnih brojeva c sa svojstvom $cL \subset L$.
(ii) Skup endomorfizama je komutativni prsten s 1 obzirom na zbrajanje i kompoziciju (koji se kod pripadnih kompleksnih brojeva svode na zbrajanje i množenje).
(iii) $End(\mathbf{C}/L)$ je podprsten prstena cijelih brojeva u nekom kvadratno imaginarnom polju.
Taj podprsten sadrži $\mathbf{Z}$, a ako sadrži nešto više, onda je eliptička krivulja s kompleksnim množenjem.

Napomenimo prije dokaza da (iii) govori da je kompleksno množenje rijetkost.
Dokaz. (i) Prema predhodnom razmatranju, ostaje pokazati samo jedan smjer (jednostavniji), naime da svaki kompleksni broj c sa svojstvom $cL \subset L$

odredjuje endomorfizam. To je upravo endomorfizam f zadan kao $f(\tilde{z}) = \tilde{cz}$. Uvjet $cL \subset L$ omogućuje da je f dobro definiran, tj. da klasa od nule odlazi u klasu od nule. Sad ostaje samo uočiti da različiti takvi c odredjuju različite endomorfizme (a to je lako).

(ii) Za zbrajanje je jasno; takodjer je jasno da je kompozicija dobro definirana operacija. Jedino ostaje komutativnost. Neka endomorfizmima f, g odgovaraju kompleksni brojevi c, d. Tada je

$(g \circ f)(\tilde{z}) := g(f(\tilde{z})) = g(\tilde{(cz)}) = \tilde{(dcz)} = \tilde{(cdz)} = (f \circ g)(\tilde{z})$.

(iii) Neka je L generirana s ω_1, ω_2 i neka c odgovara nekom f, tj. neka je $cL \subset L$, tj. vrijedi

$c\omega_1 = A\omega_1 + B\omega_2;\ c\omega_2 = C\omega_1 + D\omega_2$,

za neke cijele A, B, C, D. Stavimo $\tau := \frac{\omega_1}{\omega_2}$ i napomenimo da τ nije realan. Sad dobijemo

$c\tau = A\tau + B;\ c = C\tau + D$, odakle izlazi $C\tau^2 + D\tau = A\tau + B$, tj.

$$(C\tau)^2 + (D - A)(C\tau) - CD = 0,$$

odakle vidimo da $C\tau$ cijeli kvadratno imaginarni broj (jer nije realan). Kako je $c = C\tau + D$ vidimo da je i c cijeli kvadratno imaginaran broj.

Napomenimo da činjenica da je τ kvadratno imaginaran govori da je kompleksno množenje rijetkost (naime, τ je omjer perioda ω_1, ω_2, pa može biti gotovo svaki broj, a kvadratno imaginarnih prema svima ima zanemarivo malo - ta se tvrdnja može još preciznije izreći).

Takodjer, vidi se da $EndE$ uvijek sadrži $\mathbf{Z}$.