Uvod u aritmetiku eliptičkih krivulja

Abelova proširenja od $\mathbf{Q}(i)$ - 19. lekcija

Opisat ćemo na primjeru eliptičke krivulje $E : y^2 = x^3 + x$ Kroneckerov Jugendtraum. Podsjetimo da Kronecker-Weberov teorem tvrdi da je svako Galoisovo proširenje $K/\mathbf{Q}$ (tj. takvo kojemu je Galoisova grupa abelova) sadržano u nekom ciklotomskom, tj. generiranom nekim korijenom iz jedinice (drugim riječima generirano vrijednošću $e^{\frac{2\pi i}{m}}$, za neki cijeli m, periodne analitičke funkcije $z \mapsto e^{2\pi iz}$ - s temeljnim periodom 1).
Naravno da je prirodno tražiti analogan rezultat za abelova proširenja K/k, gdje je k neko (konačno) proširenje od $\mathbf{Q}$, a najjednostavniji su slučajevi kad je k kvadratno proširenje od $\mathbf{Q}$. Poznato je da se kvadratna proširenja dijele na kvadratno realna i kvadratno imaginarna. Pokazuje se da je problem s kvadratno realnim puno tvrdji i do danas je vrlo nejasan, dok je, na osnovi primjera, Kronecker postavio slutnju da za kvadratno imaginarna proširenja funkciju $z \mapsto e^{2\pi iz}$ treba zamijeniti dvostrukoperiodnim Weiestrassovim funkcijama $\mathcal{P}$, $\mathcal{P}'$, za zgodno odabranu rešetku L perioda (vrlo gruba formulacija). Geometrijskim jezikom govoreći točke konačnog reda na jediničnoj kružnici (koje odgovaraju vrijednostima $e^{\frac{2\pi i}{m}}$) treba zamijeniti točkama konačnog reda na korespondirajućim eliptičkim krivuljama nad $\mathbf{Q}$. Da kažemo nešto preciznije, te eliptičke krivulje treba birati medju eliptičkim krivuljama s kompleksnim množenjem i to, ako je k pripadno kvadratno imaginarno polje, onda biramo eliptičke krivulje koje imaju kompleksno množenje s cjelim brojevima tog polja (vidite 18. lekciju).
U našem primjeru bit će $k := \mathbf{Q}(i)$, a pripadna eliptička krivulja

$$E : y^2 = x^3 + x$$

Tu smo eliptičku krivulju izabrali jer ona ima kompleksno množenje s i, tj.

$$\phi : E \to E;\ \phi(x, y) = (-x, iy)$$

je endomorfizam različit od svakog množenja $[m]$ s cijelim brojevima $P \mapsto mP$. Lako se pokaže da je ϕ i automorfizam od E. Naime, za $P = (x, y)$ je $(\phi \circ \phi)(P) = \phi(-x, iy) = (-(-x), i(iy)) = (x, -y) = -P$, pa je $\phi^{-1} = -\phi$.
Treba uočiti da ϕ nije definiran nad $\mathbf{Q}$ već nad $\mathbf{Q}(i)$. Nadalje, za sve cijele brojeve m, n, pripadno preslikavanje $m + n\phi$ definirano kao $(m + n\phi)(P) :=$

$mP + n\phi(P)$ je endomorfizam od E. Može se pokazati da je time prsten endomorfizama $EndE$ izomorfan prstenu cijelih Gaussovih brojeva $\mathbf{Z}[i]$, ali to nam sad nije važno, dovoljno će biti razmatranje s automorfizmom ϕ.
Podsjetimo najprije na primjere (uz oznaku $K_n := \mathbf{Q}(E[n])$). Vidjeli smo u predhodnoj lekciji da je:
(I) $K_2 = \mathbf{Q}(i) = k$, pa je $Gal(K/\mathbf{Q})$ ciklička grupa reda 2 (dakle abelova), a $Gal(K/k)$ je trivijalna (dakle abelova),
(II) $K_4 = \mathbf{Q}(i, \sqrt{2})$, pa je $Gal(K/\mathbf{Q})$ umnožak ciklička grupa reda 2 (dakle abelova), a $Gal(K/k)$ je trivijalna (dakle abelova),
(III) $K_3 = \mathbf{Q}(i, \beta)$, gdje je $\beta = \sqrt[4]{\frac{8\sqrt{3}-12}{9}}$ i pokazuje se da je $GalK/\mathbf{Q}$ **neabelova** grupa reda 16 (vidi [S-T, str.191]), a za $Gal(K/k)$ može se pokazati da je abelova.
Dakle $K_n/\mathbf{Q}$ općenito nije abelovo, a tvrdnja je (odnosno dio tvrdnje) da je K_n/k abelovo za sve n.
Izravno računanje je već za $n = 3$ mukotrpno i netrivijalno. Opći rezultat odakle će slijediti i ovaj posebni dokazat ćemo poslije. Tvrdnju lakše možemo ilustrirati za eliptičku krivulju $y^2 = x^3 - 2$ već za $n = 2$ (vidi predhodnu lekciju, samo što je u tom slučaju $k = \mathbf{Q}(\rho)$).
Prije nastavka komentirajmo dvije činjenice.
Prva je da polje K_n sadrži $\mathbf{Q}(i)$ za svaki $n \geq 2$. Naime, ako je $P = (x, y)$ i $nP = O$, onda je
$O = nP = \phi(np) = n\phi(P)$, pa je $\phi P \in E[n]$, čim je $P \in E[n]$.
Kako je $\phi(P) = (-x, iy)$, zaključujemo da je $y \in K_n$ i $iy \in K_n$, pa je $i \in K_n$ čim je $y \neq 0$. Ako je pak $y = 0$, za sve točke, onda je $n = 2$, pa podsjetimo da je $K_2 = \mathbf{Q}(i)$.
Važna posljedica jest to da je

$$K_n := \mathbf{Q}(E[n]) = \mathbf{Q}(i)(E[n]).$$

Druga ječinjenica dio osnovnog teorema Galoisove teorije, naime ako su k, K dva Galoisova (konačna) proširenja od $\mathbf{Q}$ i ako je $k \subseteq K$, onda je K/k takodjer Galoisovo (to je očito iz definicije), i sljedeći niz Galoisovih grupa je egzaktan (koji je nama važan samo za k kvadratno imaginarno, ili, još uže, za $k = \mathbf{Q}(i)$)

$$\{1\} \to Gal(K/k) \to Gal(K/\mathbf{Q}) \to Gal(k/\mathbf{Q}) \to \{1\}.$$

Tu je $\{1\}$ jedinična grupa generirana identitetom (označavali smo je i kao σ_0). Takodjer, $Gal(K/k) \to Gal(K/\mathbf{Q})$ je prirodno ulaganje grupa (nama

ovaj rezultat iz Galoisove teorije ne treba za razmatranje, već samo za bolje shvaćanje tvrdnje, naime velika grupa $Gal(K/\mathbf{Q})$ općenito ne mora biti abelova, a njena podgrupa $Gal(K/k)$ indeksa 2 mora). Preslikavanje $Gal(K/\mathbf{Q}) \to Gal(k/\mathbf{Q})$ prirodna je surjekcija dobivena restrikcijom automorfizama s K na k, i još nam je manje važno za daljnje razmatranje.

Formulirajmo sad tvrdnje.

Teorem 1. Neka je $E : y^2 = x^3 + x$ i $K_n := \mathbf{Q}(i)(E[n])$ za $n \in \mathbf{N}$ (a vidjeli smo da je $K_n = \mathbf{Q}(E[n])$ za $n \geq 2$). Tada je $K_n/\mathbf{Q}(i)$ Galoisovo abelovo proširenje.

Ta je tvrdnja analogna (gotovo trivijalnoj) tvrdnji da je ciklotomsko proširenje $\mathbf{Q}(e^{\frac{2\pi i}{n}})/\mathbf{Q}$ Galoisovo abelovo, za svaki prirodni n.
Ono što je netrivijalno jest obrat te tvrdnje, a to je Kronecker-Weberov teorem. Formulirajmo njen analogon i u ovoj složenijoj situaciji.

Teorem 2. Neka je $F/\mathbf{Q}(i)$ Galoisovo abelovo proširenje. Tada je $F \subseteq K_n := \mathbf{Q}(i)(E[n])$ za neki $n \in \mathbf{N}$, gdje je $E[n]$ skup rješenja jednadžbe $nP = O$ na eliptičkoj krivulji $E : y^2 = x^3 + x$.

Mi ćemo dokazati samo Teorem 1, a Teorem 2 je pretežak za dokazivanje na ovoj razini. Opet napomenimo da obje tvrdnje vrijede za svako kvadratno imaginarno polje k, a ne samo $\mathbf{Q}(i)$, samo se treba pravilno formulirati, na primjer za $k := \mathbf{Q}(\rho)$ treba gledati eliptičku krivulju $E : y^2 = x^3 + 1$, ili neku njoj srodnu (ima i dodatnih problema, na primjer općenito treba dodati vrijednost j-funkcije, što ovdje ne treba jer je $j(E) = 0$). Analogon teorema 1 relativno je lako dokazati, dok je analogon teorema 2 bitno teži.

Dokaz teorema 1. Možemo gledati samo za $n \geq 2$. To da je $K_n/\mathbf{Q}(i)$ Galoisovo je evidentno (naime $K_n/\mathbf{Q}$ je Galoisovo). Ono što je netrivijalno jest to da je $K_n/\mathbf{Q}(i)$ abelovo.
Sjetimo se injektivne reprezentacije $\rho_n : Gal(\mathbf{Q}(E[n])/\mathbf{Q}) \to Gl_2(\mathbf{Z}/n\mathbf{Z})$.
Kako je $G := Gal(\mathbf{Q}(i)(E[n])/\mathbf{Q}(i)) \subset Gal(\mathbf{Q}(E[n])/\mathbf{Q})$, onda s ρ_n označimo i restrikciju te reprezentacije na tu podgrupu (i ona je takodjer injektivna). Zato, da bismo dokazali da je G abelova, dovoljno je dokazati da je $\rho_n(G)$ abelova grupa.

Redom vrijedi:
(I) Automorfizam ϕ (kompleksno množenje) preslikava $E[n]$ u $E[n]$ i to je preslikavanje aditivno i linearno (s obzirom na množenje s cijelim brojevima modulo n). Naime $\phi(nP) = n\phi(P)$, pa ρ_n možemo proširiti i na ϕ. Zato je automorfizmu ϕ pridružena (invertibilna) matrica

$$\rho_n(\phi) = A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Gl_2(\mathbf{Z}/n\mathbf{Z}).$$

(II) ϕ komutira sa svakim elementom $\sigma \in G$. Naime, za $(x, y) = P \in E(K_n)$ vrijedi $\phi(\sigma(P)) = \phi(\sigma x, \sigma y) = (-\sigma x, i\sigma y) = (\sigma(-x), \sigma(iy)) = \sigma(\phi(P))$ (tu smo iskoritili da je $\sigma(i) = i$).
Zato matrica A komutira sa svakom matricom $\rho_n(\sigma)$ za $\sigma \in G$. Ta će činjenica biti presudna za konačan zaključak.
(III) Postoji baza od $E[n]$ oblika $\{P, \phi(P)\}$ za neku točku $P \in E[n]$.
Ako bismo znali da je to istina bili bismo gotovi. Naime u toj bazi bi bilo

$$\rho_n(\phi) := A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

jer je $\phi(P) = 0 \cdot P + 1 \cdot \phi(P)$ i $\phi(\phi(P)) = -P = (-1)P + 0 \cdot \phi(P)$.
Sad, ako je $B = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in Gl_2(\mathbf{Z}/n\mathbf{Z})$ bilo koja matrica sa svojstvom $AB = BA$, onda je

$$B = \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix}.$$

Zato skup svih invertibilnih matrica B sa svojstvom $AB = BA$ čini abelovu grupu (izravna provjera).
Kako je $\rho_n(G)$ podgrupa te grupe i ona je abelova.
Zato je preostalo pokazati da postoji takva baza. To se izravno vidi iz toga što je $E(\mathbf{C})$ izomorfna kvocijentu $\mathbf{C}/L$ gdje je L najjednostavnija moguća rešetka $L := \{r + si : r, s \in \mathbf{Z}\}$ (tj. L je razapeta s 1 i i). Naravno, pri tom izomorfizmu, endomorfizmi od E prelaze u endomorfizme od $\mathbf{C}/L$, a to su svi cijeli Gaussovi brojevi (kao skup poklapaju se s L). Endomorfizmi koji su automorfizmi prelaze u invertibilne cijele Gaussove brojeve, a to su $-1, 1, -i, i$. Kako je ϕ automorfizam njemu je pridružen broj i ili broj $-i$ (1 nije jer ϕ nije identitet, a -1 nije jer ϕ nije preslikavanje $T \mapsto -T$). Ako u $\mathbf{C}/L$ gledamo jednadžbu $nz = 0$, a upravo ona odgovara jednadžbi $nT = O$

u E, dobijemu bazu rješenja $\{\frac{1}{n}, \frac{i}{n}\}$, takodjer i bazu $\{\frac{1}{n}, \frac{-i}{n}\}$, a jedna od njih u E odgovara bazi oblika $\{P, \phi(P)\}$, gdje točka P odgovara broju $\frac{1}{n}$.
Za preciznu formulaciju izomorfizma izmedju E i torusa $\mathbf{C}/L$ vidi [S-T, zad. 6.21. na str. 219]. Za dokaz podsjetimo da smo u 3. lekciji pokazali da je $\mathbf{C}/L$ izomorfna s eliptičkom krivuljom C zadanom jednadžbom $y^2 = 4x^3 - g_2 x$ gdje je $g_2 > 0$ (to nije previše bitno). Izravnom provjerom (množimo jednadžbu od C s $\frac{16}{(2i\sqrt{g_2})^3}$) vidimo da je preslikavanje

$$(x, y) \mapsto (\frac{4x}{2i\sqrt{g_2}}, \frac{4y}{(\sqrt{2i\sqrt{g_2}})^3})$$

izomorfizam izmedju C i E.