# Uvod u aritmetiku eliptičkih krivulja

## Frobeniusov element beskonačnog proširenja (skica) - 24. lekcija

Neka je sad $L/\mathbf{Q}$ Galoisovo proširenje beskonačnog stupnja (tj. unija svojih Galoisovih podproširenja $K/\mathbf{Q}$ konačnog stupnja). Uskladjena familija $(\mathcal{P}_K)$ prostih ideala iznad prostog broja $p$, prema definiciji je familija za koju je svaki $\mathcal{P}_K$ prost ideal u prstenu cijelih algebarskih brojeva $O_K$ od $K$ i koji dijeli ideal $pO_K$, ali takva da ako je $K' \subset K$, onda je $\mathcal{P}_K \cap O_{K'} = \mathcal{P}_{K'}$. Tada je $\mathcal{P}_L := \bigcup \mathcal{P}_K$ prost ideal u $O_L$ i obratno, svaki se prosti ideal u $O_L$ tako dobije.
Ako su sad za neki $\mathcal{P}_L$ svi pripadni $\mathcal{P}_K$ nerazgranati, onda kažemo da je i $\mathcal{P}_K$ nerazgranat. Ako su svi $\mathcal{P}_L$ iznad $p$ nerazgranati, kažemo de je $p$ nerazgranat u $L$, odnosno da je $L$ nerazgranato u $p$ (inače je razgranato). Jasno je da je, općenito, nerazgranatost kod proširenja beskonačna stupnja rijetkost, ali nije potpuno isključena.

**Primjer 1.** (i) Neka je $L := \bigcup_n \mathbf{Q}(\mu_{l^n})$ unija proširenja generiranih $l^n$-tim korijenima iz jedinice, za fiksiran prost broj $l$, dok $n$ prolazi skupom svih prirodnih brojeva. Može se pokazati da je $\mathcal{P}_L$ razgranat ako i samo ako je $\mathcal{P}_L$ iznad $l$. Drugim riječima, tu je $L$ nerazgranato osim u $l$ (gdje je razgranato).
(ii) (**vrlo važan primjer**) Neka je $L := K_{E,l}$ polje generirano koordinatama točkama $l^n$-tog reda fiksirane eliptičke krivulje $E$ nad $\mathbf{Q}$, pri fiksiranom prostom broju $l$, i prirodnim brojevima $n$. Prema teoremu Serrea i Tatea, $L$ je nerazgranat upravo u onim prostim brojevima $p \neq l$ u kojima $E$ ima dobru redukciju (posebice, ono je nerazgranato izvan konačnog skupa prostih brojeva).
(iii) Neka je $L := \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ polje svih algebarskih brojeva. Tada je $L$ Galoisovo beskonačnog stupnja u kojemu je svaki $\mathcal{P}_L$ razgranat (pa je $L$ razgranato u svim prostim $p$). Naime, neka je $\mathcal{P}_L$ iznad $p$ i neka je $K$ kvadratno proširenje u kojemu se $p$ grana (na primjer $K := \mathbf{Q}(\sqrt{p})$). Tada je pripadni $\mathcal{P}_K$ razgranat.

Ako je neki $\mathcal{P}_L$ iznad $p$ nerazgranat onda definiramo Frobeniusov automorfizam $Frob_{\mathcal{P}_L}$ u $\mathcal{P}_L$ kao uskladjenu familiju Frobeniusovih automorfizama $(Frob_{\mathcal{P}_K})$ gdje $K$ ide svim konačnim Galoisovim podproširenjima od $L$ (tu

uskladjenost znači da se Frobeniusov automorfizam manjeg polja dobije restrikcijom Frobeniusova automorfizma s većega, što slijedi iz definicije). Zato je $Frob_{\mathcal{P}_L}$ element Galoisove grupe od $L$ nad $\mathbf{Q}$.
Nije teško vidjeti da ako je neki $\mathcal{P}_L$ iznad $p$ nerazgranat onda je i svaki $\mathcal{P}_L$ iznad $p$ nerazgranat i da su svaka dva pripadna Frobeniusova automorfizma konjigirana, i svaki automorfizam iz klase konjugiranosti jednoga $\mathcal{P}_L$ je Frobeniusov automorfizam nekoga prostoga ideala nad $p$. Zato je jednoznačno definirana klasa konjugiranosti Frobeniusova automorfizma $Frob_{\mathcal{P}_L}$ koja se zove **Frobeniusov element** prostog broja $p$ i označava se kao $Frob_p$ (da ne dodje do zabune, kadkad se u oznaci stavi i $L$ da se dade do znanja koje je gornje polje).

**Trag i determinanta Frobeniusova elementa pri $l$-adskoj reprezentaciji.** Zaključujemo, prema Primjeru 1(ii), da je za $K_{E,l}$ uvijek jednoznačno definirana klasa konjugiranosti $Frob_p$ uz uvjet da $E$ ima dobru redukciju u $p$ i da je $p \neq l$. Kako je pripadna $l$-adska reprezentacija

$$\rho_{E,l} : \mathrm{Gal}(K_{E,l}/\mathbf{Q}) \to \mathrm{Gl}_2(\mathbf{Z}_l)$$

injektivna, razumno je definirati tragom, odnosno determinantom svakog automorfizma, kao tragom odnosno determinantom pripadne $2 \times 2$ matrice. Kako konjugirani automorfizmi pri reprezentaciji prelaze u konjugirane matrice, i kako konjugirane matrice imaju jednake tragove i determinante, jednoznačno su definirani
$tr(Frob_p)$ i $det(Frob_p)$ kao $tr(\rho_{E,l}Frob_{\mathcal{P}})$ i $det(\rho_{E,l}Frob_{\mathcal{P}})$
gdje je $\mathcal{P}$ **bilo koji** prosti ideal u prstenu cijelih od $O_{K_{E,l}}$ iznad $p$.

Općenito, trag automorfizma grupe $\mathrm{Gal}(K_{E,l}/\mathbf{Q})$ je cijeli $l$-adski broj, a determinanta invertibilni cijeli algebarski broj (jer pripadna matrica ima koeficijente u $\mathbf{Z}_l$). Vrlo važno svojstvo Froneniusovih elemenata (odnosno klase konjugiranosti pripadnih Frobeniusovih automorfizama) jest da su njihovi trag i determinanta obični cijeli brojevi (iako pripadne matrice u pravilu nemaju cijele koeficijente). To se dobije pažljivom analizom koju sad ne možemo prezentirati. Vrijedi naime, puno preciznija tvrdnja.

**Teorem.** Neka je $E$ fiksirana eliptička krivulja nad $\mathbf{Q}$ i neka je $l$ fiksiran prost broj. Tada za svaki prosti $p \neq l$ u kojemu $E$ ima dobru redukciju vrijedi:

$$trFrob_p = a_p \text{ i } detFrob_p = p$$

gdje je $a_p = p + 1 - N_p$, a $N_p$ je broj $\mathbf{F}_p$-racionalnih točaka na redeciranoj eliptičkoj krivulji modulo $p$. Prema Hasseovu teoremu vrijedi $|a_p| < 2\sqrt{p}$.

**Frobeniusovi elementi u razgranatim prostim brojevima i idealima.**
Prema dosadašnjem razmatranju, definirali smo Frobeniusove automorfizme i elemente samo u nerazgranatom slučaju. Kao posljedicu imali smo, na primjer, da tako ne možemo definirati Frobeniuosove elemente u $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ niti za jedan prosti $p$. Zato ćemo sad naše definicije proširiti i na razgranati slučaj. Startat ćemo, kao i obično, s konačnim Galoisovim proširenjima. Kao što je poznato, eksplicitno se može definirati diskriminanta $D$ svakog takvog proširenja, koja je cijeli broj različit od $0, -1, 1$ i vrijedi:
$p$ se grana u proširenju ako i samo ako $p|D$.
Podsjetimo, ako je $K/\mathbf{Q}$ konačno Galoisovo proširenje s Galoisovom grupom $G$, $p$ prost broj i $\mathcal{P}$ neki prost ideal u $K$ koji je iznad $p$. Tada smo definirali grupu razlaganja u $\mathcal{P}$:
$D_{\mathcal{P}} = \{\sigma \in G : \sigma(\mathcal{P}) = \mathcal{P}\}$,
i grupu inercije $I_{\mathcal{P}}$ u $\mathcal{P}$ kao jezgru prirodnog surjektivnog homomorfizma $D_{\mathcal{P}} \to \mathrm{Gal}(\mathbf{F}_{p^f}/\mathbf{F}_p)$, gdje je $f$ indeks inercije u $p$. Napomenimo da je ta jezgra trivijalna ako i samo ako je $p$ nerazgranat. Dakle imamo prirodni izomorfizam

$$D_{\mathcal{P}}/I_{\mathcal{P}} \cong \mathrm{Gal}(\mathbf{F}_{p^f}/\mathbf{F}_p).$$

Zato je jednoznačno definiran automorfizam $Frob_{\mathcal{P}}$ iz $D_{\mathcal{P}}/I_{\mathcal{P}}$ koji pri tom izomorfizmu prelazi u Frobeniusov automorfizam konačnog polja.
Napomenimo da za razgranati $p$ svi $\mathcal{P}$ koji sudjeluju u rastavu od $pO_K$ dolaze s fiksnim eksponentom $e \geq 2$ (indeks grananja) i da vrijedi

$$efm = n \ (***)$$

gdje je $m$ broj različitih prostih faktora u rastavu.
Ako je proširenje Abelovo onda $D_{\mathcal{P}}, I_{\mathcal{P}}, D_{\mathcal{P}}/I_{\mathcal{P}}$ i $Frob_{\mathcal{P}}$ ne ovise o $\mathcal{P}$ već samo o $p$ pa je, prema definiciji, $Frob_p := Frob_{\mathcal{P}}$, za bilo koji $\mathcal{P}$ iznad $p$.
Uočite da $Frob_p$ nije više element od $G$ (ako je u $p$ grananje), već klasa elemenata iz $G$ koja ima bar dva elementa, pa nije klasa konjugiranosti (u abelovom slučaju).

**Primjer 2.** (i) U $K = \mathbf{Q}(i)$ je $G = \{1, \sigma\}$, gdje je $\sigma$ kompleksno konjugiranje; grana se samo 2 i jer je $2O_K = (1-i)^2$ vidimo da je $\mathcal{P} = (1-i)$

(glavni ideal), s indeksom grananja $e = 2$. Izravno se dobije:
$D_{\mathcal{P}} = G$ (jer je $\sigma(1-i) = 1+i = -i(1-i)$). Kako je $O_K = \mathbf{Z}[i]$ vidi se da je $O_K/\mathcal{P} \cong \mathbf{F}_2$ pa je $f = 1$, tj. $I_{\mathcal{P}} = G$ i $Frob_2$ je 1 kao jedini element od $G/G$.
(ii) U $K = \mathbf{Q}(\mu_5)$ je $G = \{1, \sigma, \sigma^2, \sigma^3\}$, gdje je $\sigma$ jednoznačno zadano kao $\sigma(\mu_5) := \mu_5^2$. Grana se jedino 5. Naime $X^4+X^3+X^2+X+1 = (X-1)^4$ modulo 5, pa je $5O_K = \mathcal{P}^4$ za prosti ideal $\mathcal{P}$ (koji se može eksplicitno napisati, štoviše tu ideali nisu ni potrebni).
Zato je tu opet $Frob_5 = 1 \in G/G$.
(iii) Neka je $K := \mathbf{Q}(\sqrt{3}, i)$. To je proširenje 4-tog stupnja s abelovom Galoisovom grupom $G$ koja je direktni produkt dviju cikličkih grupa 2-gog reda $\{1, \sigma\}$ i $\{1, \tau\}$, gdje je $\sigma(i) = -i$ i $\sigma(\sqrt{3}) = \sqrt{3}$, dok je $\tau(i) = i$ i $\tau(\sqrt{3}) = -\sqrt{3}$. Lako se vidi da se samo 2 i 3 granaju, a može se pokazati da su ostali prosti brojevi nerazgranati. Nije teško vidjeti da je

$$2O_K = \mathcal{P}^2$$

za neki prosti ideal $\mathcal{P}$. Zato je $e = f = 2$, i takodjer $D_{\mathcal{P}} = G$. Zaključujemo da je $I_{\mathcal{P}} = \{1, \sigma\}$ (jer je restrikcija te grupe na $\mathbf{Q}(i)$ netrivijalna - naime 2 se grana i u tom polju). Zato je $Frob_2$ klasa od $\tau$ u $G/\{1, \sigma\}$.
Potpuno analogno $Frob_3$ je klasa od $\sigma$ u $G/\{1, \sigma\tau\}$. Naime, restrikcija grupe inercije na $\mathbf{Q}(\sqrt{-3})$ (koje je takodjer podpolje od $K$) mora biti netrivijalna, kako se 3 grana i u tom polju. Kako su $\sigma$ i $\tau$ trivijalni na tom polju, ostaje nam $\sigma\tau$.

Ako je $G$ nekomutativna grupa, onda se sve malo usložnjuje. Opet je za svaki fiksirani prosti broj $p$ i svaki prosti ideal $\mathcal{P}$ u $O_K$ koji je iznad $p$ jednoznačno definiran automorfizam $Frob_{\mathcal{P}}$ iz $D_{\mathcal{P}}/I_{\mathcal{P}}$. Ako je $\mathcal{Q}$ neki drugi prosti ideal iznad $p$, onda postoji $g \in G$ tako da bude $g\mathcal{P} = \mathcal{Q}$; tada je $D_{\mathcal{Q}} = gD_{\mathcal{P}}g^{-1}$ i $I_{\mathcal{Q}} = gI_{\mathcal{P}}I^{-1}$. Takodjer,
za $Frob_{\mathcal{P}} \in D_{\mathcal{P}}/I_{\mathcal{P}}$ i $Frob_{\mathcal{Q}} \in D_{\mathcal{Q}}/I_{\mathcal{Q}}$, vrijedi $Frob_{\mathcal{Q}} = gFrob_{\mathcal{P}}g^{-1}$,
gdje definiramo prirodno djelovanje od $G$ na klase kao $h(\sigma I_{\mathcal{P}}) := (h\sigma)(hI_{\mathcal{P}})$, za $h \in G$ i $\sigma \in D_{\mathcal{P}}$, i slično za djelovanje zdesna.
Sad definiramo $Frob_p$ kao familiju $Frob_{\mathcal{P}}$ za sve $\mathcal{P}$ iznad $p$. Vidimo, ako je klasa od $Frob_{\mathcal{P}}$ oblika $\sigma I_{\mathcal{P}}$, onda je $g\sigma I_{\mathcal{P}}g^{-1} = g\sigma g^{-1}gI_{\mathcal{P}}g^{-1} = g\sigma g^{-1}I_{\mathcal{Q}}$, a to je klasa od $Frob_{\mathcal{Q}}$.
Uočite da $Frob_p$, za razgranati $p$ (shvaćen kao skup svih automorfizama koji u njemu sudjeluju) nije nužno klasa konjugiranosti u $G$ (iako može biti, za razliku od abelova slučaja). To ćemo vidjeti u sljedećem primjeru.

**Primjer 3.** Neka je $K := \mathbf{Q}(\sqrt[3]{2}, \sqrt{-3})$. Kako smo vidjeli, ono je Galoisovo i neabelovo stupnja 6, s Galoisovom grupom $\{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ uz $\sigma^3 = \tau^2 = 1$ i $\tau\sigma = \sigma^2\tau$. Može se uzeti da je $\sigma(\sqrt[3]{2}) = \rho\sqrt[3]{2}$ i $\sigma(\rho) = \rho$. Lako se vidi da se 2 i 3 granaju u $K$, a može se pokazati da su ostali prosti brojevi nerazgranati.
Opišimo $Frob_2$. Kako je 2 inertan u $\mathbf{Q}(\rho)$, zaključujemo da mora biti $2O_K = \mathcal{P}^3$ za neki prosti ideal $\mathcal{P}$. Zato je $f = 2$, a restrikcija od $I_\mathcal{P}$ na $\mathbf{Q}(\rho)$ treba biti trivijalna pa je $I_\mathcal{P} =< \sigma >$, i konačno $Frob_2$ klasa $\tau$ modulo $< \sigma >$.
Vidimo da $Frob_2$ shvaćen kao skup elemenata od $G$ čini jednu klasu konjugiranosti.
Opiv simo sad $Frob_3$. Kako se 3 grana u $\mathbf{Q}(\rho)$ i u $\mathbf{Q}(\sqrt[3]{2}$, vrijedi $3O_K = Q^6$ za neki prosti ideal $Q$. Sad je $e = 6$ pa je $f = 1$, $D_\mathcal{P} = I\mathcal{P} = G$, tj. $Frob_3 = 1$ kao element od $G/G$, a kao skup elemenata od $G$ to je cijeli $G$, što nije klasa onjugiranosti.

**Definicija $Frob_p$ za bilo koji $p$ i proširenje**.
Neka je $L$ bilo koje Galoisovo proširenje od $\mathbf{Q}$, neka je $p$ fiksirani prost broj i neka je $\mathcal{P}$ fiksirani prosti ideal u $L$ iznad $p$. To znači da imamo uskladjenu familiju prostih ideala $\mathcal{P}_K$ za konačna Galoisova proširenja $K$. Za svaki $\mathcal{P}_K$ imamo $Frob_{\mathcal{P}_K} \in D_{\mathcal{P}_K}/I_{\mathcal{P}_K}$ koji su uskladjeni u smislu da su i svi $D_{\mathcal{P}_K}$ i svi $I_{\mathcal{P}_K}$ uskladjeni, pa su dobro definirani $D_\mathcal{P}$, $I_\mathcal{P}$ i $Frob_\mathcal{P} \in D_\mathcal{P}/I_\mathcal{P}$.
Ako je $\mathcal{Q}$ neki drugi prosti ideal iznad $p$, onda je $g\mathcal{P} = \mathcal{Q}$ za neki $g \in G$, pa su pripadni Frobeniusovi (odnosno klase) konjugirani itd., pa je dobro definirana klasa $Frob_p$ koju zovemo Frobeniusov element u $p$.