Galoisove reprezentacije pridružene eliptičkim krivuljama

Gužvić, Tomislav

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Tomislav Gužvić

GALOISOVE REPREZENTACIJE PRIDRUŽENE ELIPTIČKIM KRIVULJAMA

Diplomski rad

Voditelj rada:
prof. dr. sc. Filip Najman

Zagreb, rujan, 2016

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

U radu baviti ćemo se Galoisovim reprezentacijama na eliptičkoj krivulji C. Promatranjem djelovanja Galoisove grupe na torzijske točke dobivamo informacije o torzijskoj grupi eliptičke krivulje.
Prvo poglavlje rada odnosi se na endomorfizme i izogenije eliptičkih krivulja. Prirodno je promatrati homomorfizme između eliptičkih krivulja, no pokazalo se da je potrebno promatrati užu klasu homomorfizama; one koji su inducirani racionalnim funkcijama. Pokazati ćemo da uz tu dodatnu pretpostavku dobivamo korisne rezultate koji će biti korišteni u daljnjim poglavljima.
U drugom poglavlju opisujemo dokaz Mordellovog teorema kojeg je dokazao Louis Mordell 1922.godine.
Nastavljamo s definicijom djelidbenih polinoma. Djelidbeni polinomi osim u teoriji eliptičkih krivulja imaju primjene u kriptografiji. Koristeći rezultate o djelidbenim polinomima u mogućnosti smo saznati informacije o grupi torzijskih točaka na eliptičkoj krivulji. U ovom radu odrediti ćemo kako izgleda $C[n]$ koristeći djelidbene polinome, te vidjeti korisnu primjenu kod Galoisovih reprezentacija.
U glavnom poglavlju rada bavimo se Galoisovim reprezentacijama na eliptičkoj krivulji C. Promatrajući proširenje od $\mathbb{Q}$ inducirano koordinatama točaka iz $C[n]$, dolazi se do spoznaje da je to proširenje Galoisovo. U cilju određivanja Galoisove grupe koristimo se alatima reprezentacija grupa. Promatrajući Borelove i Cartanove podgrupe od $\mathrm{GL}(\mathbb{F}_p)$ možemo odrediti u kakvim se podgrupama slika reprezentacije može nalaziti.

Poglavlje 1

Izogenije

Neka je $K \subseteq \mathbb{C}$ potpolje, a $C : y^2 = x^3 + Ax + B$, gdje su $A, B \in K$ eliptička krivulja. Tada možemo promatrati skup

$$C(K) = \left\{(x, y) : x, y \in K; y^2 = x^3 + Ax + B\right\} \cup \{O\}. \tag{1.1}$$

Iz definicije zbrajanja i oduzimanja točaka na eliptičkoj krivulji jasno je da je skup $C(K)$ zatvoren na zbrajanje, pa taj skup zapravo čini podgrupu od $C(\mathbb{C})$.
Neka je $\alpha : C(\overline{K}) \to C(\overline{K})$ homomorfizam i neka postoje racionalne funkcije $R_1(x, y)$, $R_2(x, y)$ s koeficijentima u $\overline{K}$ takve da vrijedi:

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)) \tag{1.2}$$

za sve $(x, y) \in C(K)$. Jer je α homomorfizam, slijedi $\alpha(O) = O$.
Promatrajmo sada $C : y^2 = x^3 + Ax + B$ i $R(x, y)$ neka je bilo koja racionalna funkcija s koeficijentima u $\overline{K}$. Zbog $y^2 = x^3 + Ax + B$, ako je $(x, y) \in C$, onda na temelju toga možemo saznati nešto o obliku racionalne funkcije $R(x, y)$. Neka je $R(x, y) = P(x, y)/Q(x, y)$. Sve parne potencije od y u oba polinoma P i Q možemo zamijeniti s polinomom u varijabli x, a svaku neparnu potenciju od y zamijeniti s $yP'(x)$, gdje je P' neki polinom. Tada novodobivena racionalna funkcija poprima iste vrijednosti kao i $R(x, y)$ ako se točka (x, y) nalazi na C. Stoga možemo pretpostaviti da je

$$R(x, y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}. \tag{1.3}$$

Sada pomnožimo li nazivnik s $p_3(x) - p_4(x)y$ i zamijenimo li y^2 s $x^3 + Ax + B$ dobivamo konačno

$$R(x, y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}. \tag{1.4}$$

Promatrajmo sada endomorfizam

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)). \tag{1.5}$$

Jer je α homomorfizam i jer je $-(x, y) = (x, -y)$ slijedi $\alpha(x, -y) = \alpha(-(x, y)) = -\alpha(x, y)$, pa je $R_1(x, -y) = R_1(x, y)$ i $R_2(x, -y) = -R_2(x, y)$.
Ukoliko sada primjenimo prethodnu diskusiju na R_1 i R_2, slijedi da je α možemo zapisati u obliku

$$\alpha(x, y) = (r_1(x), r_2(x)y), \tag{1.6}$$

gdje su r_1 i r_2 racionalne funkcije.
Sada promatrajmo $r_1(x) = \frac{p(x)}{q(x)}$, gdje su p i q relativno prosti polinomi. Ukoliko je $q(x) = 0$ za neku točku $(x, y) \in E$, onda definirajmo $\alpha(x, y) := O$.
Za endomorfizam α za koji vrijedi prethodna diskusija kazati ćemo da je induciran racionalnim funkcijama.

Definicija 1.1. *Neka je α endomorfizam eliptičke krivulje C. Stupanj od α označavamo s $deg(\alpha)$ i definiramo s*

$$deg(\alpha) = Max\{deg(p(x)), deg(q(x))\} \tag{1.7}$$

ukoliko je α netrivijalan endomorfizam. Inače, definirajmo $deg(\alpha) := 0$.

Definicija 1.2. *Kažemo da je endomorfizam α separabilan ako derivacija $r_1'(x)$ nije jednaka nuli.*

Može se pokazati da je u poljima karakteristike 0 derivacija svakog nekonstantnog polinoma različita od 0, te da u poljima karakteristike $p > 0$ polinomi čija je derivacija identički jednaka 0 su upravo oni oblika $g(x^p)$.
Spomenimo sada posebni endomorfizam koji ima široku primjenu u teoriji eliptičkih krivulja.

Definicija 1.3. *Neka je C eliptička krivulja definirana nad poljem $\mathbb{F}_q$. Definiramo*

$$\phi_q(x, y) = (x^q, y^q). \tag{1.8}$$

Ovo preslikavanje nazivamo Frobeniusovo preslikavanje.

Sljedeća lema daje nam neke fundamentalne činjenice o Frobeniusovom preslikavanju.

Lema 1.4. *Neka je C eliptička krivulja definirana nad $\mathbb{F}_q$. Tada je ϕ_q endomorfizam od C stupnja q te nije separabilan.*

Dokaz. Pretpostavimo da je C dana u Weierstrassovom obliku. Kad pokažemo da je ϕ_q endomorfizam, iz definicije od $\phi_q(x, y) = (x^q, y^q)$ direktno slijedi da je stupanj od ϕ_q jednak upravo q. Neka su $(x_1, y_1), (x_2, y_2) \in C(\mathbb{F}_q)$ i $x_1 \neq x_2$, te neka je $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$. Tada znamo da su koordinate x_3 i y_3 dane sljedećim formulama:

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad m = \frac{y_2 - y_1}{x_2 - x_1}. \tag{1.9}$$

Potenciranjem jednadžbi i korištenjem činjenice da identitet $(a + b)^q = a^q + b^q$ vrijedi u F_q dobivamo

$$x_3^q = m'^2 - x_1^q - x_2^q, \quad y_3^q = m'(x_1^q - x_3^q) - y_1^q, \quad m' = \frac{y_2^q - y_2^q}{x_2^q - x_1^q}. \tag{1.10}$$

Ovime smo pokazali da je

$$\phi_q((x_1, y_1) + (x_2, y_2)) = \phi((x_3, y_3)) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2). \tag{1.11}$$

Slučajevi kada je $x_1 = x_2$ ili je jedna od točaka O pokazuju se analogno. Konačno, jer je ϕ_q homomorfizam definiran preko racionalnih funkcija, on je endomorfizam od C. Jer je derivacija od $x^q{=}qx^{q-1} = 0$ u $\mathbb{F}_q[x]$ slijedi da ϕ_q nije separabilan endomorfizam. □

Propozicija 1.5. *Neka je $\alpha \neq 0$ separabilan endomorfizam eliptičke krivulje C. Tada*

$$deg(\alpha) = |Ker(\alpha)| \tag{1.12}$$

gdje je $Ker(\alpha)$ jezgra homomorfizma α. Ukoliko α nije separabilan, tada je

$$deg(\alpha) > |Ker(\alpha)|. \tag{1.13}$$

Dokaz. Neka je α separabilan. Zapišimo $\alpha(x, y) = (r_1(x), yr_2(x))$, te $r_1(x) = p(x)/q(x)$. Iz separabilnosti slijedi $r_1' \neq 0$, što je ekvivalentno (deriviranjem $p(x)/q(x)$) da $p'q - p'q$ nije jednak 0. Neka je S skup svih $x \in \overline{K}$ takvih da je $(pq' - p'q)(x)q(x) = 0$ i neka je $(a, b) \in C(\overline{K})$ takav da

1. $a \neq 0, \quad b \neq 0, (a, b) \neq O$,
2. $deg(p(x) - aq(x)) = Max\{deg(p), deg(q)\} = deg(\alpha)$
3. $a \notin r_1(S)$,
4. $(a, b) \in \alpha(C(\overline{K}))$

Jer $pq' - p'q$ nije jednak nuli, te jer je S konačan skup, slijedi da je $\alpha(S)$ konačan. Jasno je da funkcija $r_1(x)$ poprima beskonačno mnogo različitih vrijednosti, za $x \in \overline{K}$. Jer je $\overline{K}$ algebarski zatvoreno polje, za svaki $x \in \overline{K}$ postoji $y \in \overline{K}$ takav da je $y^2 = x^3 + Ax + B$, tj. postoji točka $(x, y) \in E(\overline{K})$. Time dobivamo da je skup $\alpha(E(\overline{K}))$ beskonačan. Stoga točka (a, b) opisana svojstvima 1. – 4. zaista postoji.
Sada tvrdimo da postoji točno $deg(\alpha)$ točaka $(x_1, y_1) \in C(\overline{K})$ tako da vrijedi $\alpha(x_1, y_1) = (a, b)$. Ukoliko je (x_1, y_1) jedna takva točka, onda je

$$\frac{p(x_1)}{q(x_1)} = a, \quad y_1 r_2(x_1) = b. \tag{1.14}$$

Jer je $(a, b) \neq O$, mora biti $q_1(x_1) \neq 0$. Zbog $b \neq 0$ i $y_1 r_2(x_1) = b$ slijedi $y_1 = b/r_2(x_1)$. Stoga x_1 jedinstveno određuje y_1, pa preostaje odrediti koliko mogućnosti imamo za x_1.
Iz $deg(p(x) - aq(x)) = Max\{deg(p), deg(q)\} = deg(\alpha)$ slijedi da polinom $p(x) - aq(x)$ ima točno $deg(\alpha)$ korijena u $\overline{K}$ zbog algebarske zatvorenosti. Pokazati ćemo da taj polinom nema višestrukih korijena. Pretpostavimo suprotno, da postoji višestruki korijen x_0. Tada je

$$p(x_0) - aq(x_0) = 0, \quad p'(x_0) - aq'(x_0) = 0. \tag{1.15}$$

Množenjem jednadžbi dobivamo

$$ap(x_0)q'(x_0) = ap'(x_0)q(x_0). \tag{1.16}$$

Jer je $a \neq 0$, slijedi da je x_0 korijen od $p'q - pq'$, pa je $x_0 \in S$ i $a = r_1(x_0) \in r_1(S)$, što je u kontradikciji s 3.. Stoga polinom $p - aq$ nema višestrukih korijena te ima $deg(\alpha)$ različitih korijena u $\overline{K}$. Jer postoji točno $deg(\alpha)$ točaka (x_1, y_1) s $\alpha(x_1, y_1) = (a, b)$, jezgra od α ima $deg(\alpha)$ elemenata.
Ako α nije separabilan, svi koraci iz gornjeg dokaza se mogu primjeniti, te se samo treba primjetiti da je $p' - aq'$ nul-polinom pa $p(x) - aq(x) = 0$ ima višestruke korijene, pa je ukupan broj rješenja manji od $deg(\alpha)$. □

Teorem 1.6. *Neka je C eliptička krivulja definirana nad poljem K. Neka je $\alpha \neq 0$ endomorfizam od C. Tada je $\alpha : C(\overline{K}) \to C(\overline{K})$ surjekcija.*

Dokaz. Neka je točka $(a, b) \in C(\overline{K})$. Jer je $\alpha(O) = O$, možemo pretpostaviti da je $(a, b) \neq O$. Neka je $r_1(x) = p(x)/q(x)$. Ako $p(x) - aq(x)$ nije konstantan polinom, tada ima korijen x_0 u $\overline{K}$. Jer su p i q relativno prosti, onda nemaju zajedničkih korijena pa slijedi da je $q(x_0) \neq 0$ i $a = \frac{p(x_0)}{q(x_0)}$. Koristeći algebarsku zatvorenost od $\overline{K}$, izaberimo $y_0 \in \overline{K}$ takav da je $y_0^2 = x_0^2 + Ax_0 + B$. Tada je $\alpha(x_0, y_0)$ dobro definirana točka iz $C(\overline{K})$. Stavimo $\alpha(x_0, y_0) = (a, b')$. Iz $b'^2 = a^3 + Aa + B = b^2$ slijedi $b = \pm b'$. Ako je $b = b'$, gotovi smo. Ako je $b' = -b$, onda $\alpha(x_0, -y_0) = (a, -b') = (a, b)$, čime smo dobili surjektivnost.
Preostaje promatrati slučaj kada je $p - aq$ konstanta. Jer je $C(\overline{K})$ beskonačan skup i $Ker(\alpha)$

konačan zbog prethodne propozicije, ukoliko fiksiramo prvu koordinatu neke točke, postoji samo konačno mnogo točaka iz $E(\overline{K})$ takvih da ih α preslikava u točku s tom fiksnom prvom koordinatom. Stoga je barem jedan od polinoma $p(x)$, $q(x)$ nekonstantan. Zbog toga što je polinom $p - aq$ konstantan, lako se vidi da su ili oba p i q konstantni ili nekonstantni, pa stoga zaključujemo da su oba polinoma nekonstantni. Jer su $p(x)$ i $q(x)$ nekonstantni, tada postoji samo jedna konstanta a takva da je $p - aq$ konstantan polinom. Naime, kad bi postojala konstanta a' takva da je $p - a'q$ konstantan polinom, tada $(a' - a)q = (p - aq) - (p - a'q)$ povlači da je q konstantan. Analogno se pokazuje tvrdnja i za p. Stoga postoje najviše dvije točke (a, b) i $(a, -b)$ koje nisu u slici od α. Neka je (a_1, b_1) proizvoljna točka različita od O, (a, b), $(a, -b)$ i $-2(a, b)$. Tada postoji točka P_1 takva da je $\alpha(P_1) = (a_1, b_1)$. Zbog pretpostavke o (a_1, b_1), vrijedi da je $(a_1, b_1) + (a, b) \neq (a, \pm b)$, pa slijedi egzistencija točke P_2 takve da je $\alpha(P_2) = (a_1, b_1) + (a, b)$. Tada je $\alpha(P_2 - P_1) = (a, b)$ i $\alpha(P_1 - P_2) = (a, -b)$, pa je α surjekcija. □

Neka su sada C_1 i C_2 eliptičke krivulje nad poljem $\overline{K}$.

Definicija 1.7. *Izogenija s C_1 u C_2 je nekonstantni homomorfizam $\alpha : C_1(\overline{K}) \to C_2(\overline{K})$ koji je induciran s racionalnim funkcijama, takav da je $\alpha(O) = O$.*

Anagno kao i kod endomorfizama pokazuje se da iz $\alpha(x_1, y_1) = (x_2, y_2)$, gdje je $x_2 = R_1(x_1, y_1)$, $y_2 = R_2(x_1, y_1)$ slijedi $(x_2, y_2) = (r_1(x_1), y_1 r_2(x_1))$, gdje su r_1 i r_2 racionalne funkcije. Za α kažemo da je separabilan ako derivacija $r_1'(x)$ nije identički jednaka nuli.

Definicija 1.8. *Neka je α izogenija s C_1 u C_2. Stupanj od α definiramo kao*

$$deg(\alpha) = Max\{deg(p(x)), deg(q(x))\}. \tag{1.17}$$

Propozicija 1.9. *Neka je $\alpha : C_1 \to C_2$ izogenija. Ako je α separabilan, tada je*

$$deg(\alpha) = |Ker(\alpha)| \tag{1.18}$$

gdje je $Ker(\alpha)$ jezgra homomorfizma α. Ukoliko α nije separabilan, tada je

$$deg(\alpha) > |Ker(\alpha)|. \tag{1.19}$$

Teorem 1.10. *Neka je $\alpha : C_1 \to C_2$ izogenija. Tada je $\alpha : C_1(\overline{K}) \to C_2(\overline{K})$ surjekcija.*

Dokazi obje prethodne tvrdnje u potpunosti su analogni dokazima u slučaju kada je izogenija endomorfizam. Do sada promatrali smo homomorfizme α s C_1 u C_2 s dodatnim uvjetima da je $\alpha(O) = O$ te da je α induciran racionalnim funkcijama. Možemo se zapitati postoje li eliptičke krivulje C_1 i C_2 te nekonstantno preslikavanje $\phi : C_1 \to C_2$ takvo da je $\phi(O) = O$ i da je ϕ induciran racionalnim funkcijama ali da ϕ nije izogenija. Odgovor na to pitanje je negativan i dan sljedećim teoremom.

Teorem 1.11. *Neka su C_1 i C_2 eliptičke krivulje nad poljem $\overline{K}$. Neka je $\alpha : C_1(\overline{K}) \to C_2(\overline{K})$ nekonstantno preslikavanje inducirano racionalnim funkcijama. Ako je $\alpha(O) = O$, tada je α homomorfizam.*

Dokaz se može pronaći u [4].

Propozicija 1.12. *Neka je C eliptička krivulja i G konačna podgrupa od C. Tada postoji jedinstvena eliptička krivulja C' i separabilna izogenija $\alpha : C \to C'$ takva da je $Ker(\alpha) = G$.*

Dokaz se može pronaći u [2].
Navedimo sad nekoliko primjera izogenija.

Primjer 1.13. *Neka je $m \in \mathbb{Z}$. Promotrimo množenje s m na C, tj. funkciju*

$$[m] : C \to C. \tag{1.20}$$

Ako je $m > 0$, onda $[m](P) := P + P + ... + P$ (m puta), a ako je $m < 0$ onda $[m](P) := [-m](-P)$ i $[0](P) := O$. Da je $[m]$ izogenija slijedi direktnom provjerom, a da je $deg([m]) = m^2$ biti će pokazano u poglavlju 3.

Postavlja se pitanje je li svaki endomorfizam zapravo množenje sa m, za neki $m \in \mathbb{Z}$. Sljedeći primjer pokazuje da to nije slučaj.

Primjer 1.14. *Pretpostavimo da je $char(K) \neq 2$ i neka je C eliptička krivulja definirana s*

$$C : y^2 = x^3 - x. \tag{1.21}$$

Tada $End(E)$ osim množenja s m, $m \in \mathbb{Z}$ sadrži i preslikavanje

$$[i] : (x, y) \to (-x, iy), \tag{1.22}$$

gdje $i \in \overline{K}$ označava primitivni četvrti korijen jedinice.

Definicija 1.15. *Neka je C eliptička krivulja. Kažemo da C ima kompleksno množenje ako postoji endomorfizam $\phi : C \to C$ koji nije množenje s m.*

Poglavlje 2

Mordellov teorem

Definicija 1. Neka je $x = \frac{m}{n}$ racionalan broj te neka su m i n relativno prosti. Tada definiramo visinu $H(x)$ racionalnog broja x sa:

$$H(x) = H\left(\frac{m}{n}\right) := max\left\{|m|, |n|\right\}. \tag{2.1}$$

Neka je C eliptička krivulja. Sa $C(\mathbb{Q})$ i $C(\mathbb{C})$ označavamo grupe racionalnih i kompleksnih točaka na eliptičkoj krivulji C, respektivno.

Dokazi svih tvrdnji iz ovog poglavlja mogu se naći u [1].

Lema 2.1. *Za svaki realni broj M, skup*

$$\{P \in C(\mathbb{Q}) : h(P) \leq M\} \tag{2.2}$$

je konačan.

Lema 2.2. . *Neka je P_0 fiksna racionalna točka na C. Tada postoji konstanta κ_0 (koja ovisi o P_0, a, b i c) takva da*

$$h(P + P_0) \leq 2h(P) + \kappa_0, \forall P \in C(\mathbb{Q}). \tag{2.3}$$

Lema 2.3. *Postoji konstanta κ, (koja ovisi o a, b i c) takva da je*

$$h(2P) \geq 4h(P) - \kappa, \forall P \in C(\mathbb{Q}). \tag{2.4}$$

U svakoj komutativnoj grupu Γ, množenje s m inducira homomorfizam $f : \Gamma \to \Gamma$ tako da vrijedi $f(P) = mP$. Slika tog homomorfizma je podgrupa $m\Gamma$ od Γ.

Teorem 2.4. *Indeks $[C(\mathbb{Q}) : 2C(\mathbb{Q})]$ je konačan.*

Teorem 2.5. *Neka je* Γ *komutativna grupa. Prepostavimo da postoji funkcija* $h : \Gamma \to [0, \infty >$ *sa sljedećim svojstvima:*

1. *Za svaki realni broj* M*, skup*

$$\{P \in \Gamma : h(P) \leq M\}$$

je konačan.

2. *Neka je* $P_0 \in \Gamma$*. Tada postoji konstanta* κ_0 *takva da*

$$h(P + P_0) \leq 2h(P) + \kappa_0, \forall P \in \Gamma$$

3. *Postoji konstanta* κ *takva da je*

$$h(2P) \geq 4h(P) - \kappa, \forall P \in \Gamma.$$

4. *Podgrupa* 2Γ *ima konačan indeks u* Γ.

Tada je Γ *konačno generirana.*

Pretpostavimo da na našoj eliptičkoj krivulji $C : y^2 = x^3 + ax^2 + bx + c$ leži točka oblika $(x_0, 0)$. Tada translacijom koordinatnog sustava možemo točku $(x_0, 0)$ translatirati do ishodišta. Novodobivena jednadžba ima cjelobrojne koeficijente i oblika je

$$C : y^2 = f(x) = x^3 + ax^2 + bx. \tag{2.5}$$

Tada je $T = (0, 0)$ racionalna točka na C koja zadovoljava $2T = O$. Pokazuje se da je korisno promatrati krivulju C' definiranu s:

$$C' : y^2 = x^3 + a'x^2 + b'x, \tag{2.6}$$

gdje je

$$a' = -2a, b' = a^2 - 4b. \tag{2.7}$$

Napomena 2.6. *Eliptička krivulja* C' *se naziva* 2*-izogena krivulja od* C.

Bitno je napomenuti da ukoliko promatramo krivulju $C'' := (C')'$, da je grupa Γ'' racionalnih točaka na krivulji C'' izomorfna s grupom Γ racionalnih točaka na C.
Sada definirajmo preslikavanje $\phi : C \to C'$ na sljedeći način:
ako je $P = (x, y) \in C$ točka takva da je $x \neq 0$, tada je $\phi(x, y) = (x', y')$, gdje je

$$x' = x + a + \frac{b}{x}, y' = y\Big(\frac{x^2 - b}{x^2}\Big). \tag{2.8}$$

Ovime smo definirali ϕ na svim točkama osim T i O. Dodefinirat ćemo funkciju u tim točkama s

$$\phi(T) = O', \phi(O) = O'. \tag{2.9}$$

Propozicija 2.7. *Neka su C i C′ eliptičke krivulje dane jednadžbama*

$$C : y^2 = x^3 + ax^2 + bx \tag{2.10}$$

i

$$C' : y^2 = x^3 + a'x^2 + b'x, \tag{2.11}$$

gdje je

$$a' = -2a, b' = a^2 - 4b. \tag{2.12}$$

Neka je $T = (0, 0) \in C$.
a) Postoji homomorfizam $\phi : C \to C'$ definiran s:

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) & , \text{ako } P \neq T, O \\ O', & , \text{inače} \end{cases} \tag{2.13}$$

Jezgra od ϕ je $\{O, T\}$.
b)Krivulja C″ je izomorfna s C zbog preslikavanja $(x, y) \to (x/4, y/8)$. Stoga postoji homomorfizam $\psi : C' \to C$ koji je definiran s

$$\psi(P') = \begin{cases} \left(\frac{y'^2}{4x'^2}, \frac{y'(x'^2-b')}{8x'^2}\right) & , \text{ako } P' \neq T', O' \\ O', & , \text{inače} \end{cases} \tag{2.14}$$

Vrijedi da je $\psi \circ \phi(P) = 2P$.

Jasno je iz definicije da ϕ preslikava Γ u Γ', no nije jasno da li svaka racionalna točka iz Γ' oblika $\phi(x)$ za neku racionalnu točku $x \in \Gamma$.
Vrijede sljedeće tri tvrdnje:

1. $O' \in \phi(\Gamma)$
2. $T' = (0, 0) \in \phi(\Gamma)$ ako i samo ako je $b' = a^2 - 4b$ potpun kvadrat.
3. Neka je $P' = (x', y') \in \Gamma'$ te $x \neq 0$. Tada je $P' \in \phi(\Gamma)$ ako i samo ako je x' kvadrat racionalnog broja.

Propozicija 2.8.

1. *Preslikavanje* $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ *je homomorfizam.*

2. *Jezgra od* α *je slika* $\psi(\Gamma')$*. Stoga* α *inducira injektivni homomorfizam*

$$\Gamma/\psi(\Gamma') \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}. \tag{2.15}$$

3. *Neka su* $p_1, ..., p_t$ *različiti prosti brojevi koji dijele b. Tada je slika od* α *sadržana u podgrupi od* $\Gamma/\psi(\Gamma')$ *koja se sastoji od elemenata oblika* $\left\{\pm p_1^{\epsilon_1}...p_t^{\epsilon_t} : \epsilon_i \in \{0,1\}\right\}$

4. $[\Gamma : \psi(\Gamma')] \leq 2^{t+1}$.

Lema 2.9. *Neka su A i B abelove grupe i neka su* $\phi : A \to B$ *i* $\psi : B \to A$ *homomorfizmi. Pretpostavimo dodatno da vrijedi*

$$\psi(\phi(a)) = 2a, \forall a \in A \tag{2.16}$$

$$\phi(\psi(b)) = 2b, \forall b \in B \tag{2.17}$$

Pretpostavimo još da $\phi(A)$ *ima konačan indeks u B i da* $\psi(B)$ *ima konačan indeks u A. Tada* $2A$ *ima konačan index u A i vrijedi*

$$[A : 2A] \leq [A : \psi(B)][B : \phi(A)] \tag{2.18}$$

Teorem 2.10. *(Mordell-za krivulje s racionalnom točkom reda dva) Neka je C nesingularna kubična krivulja dana s*

$$C : y^2 = x^3 + ax^2 + bx$$

gdje su a i b cijeli brojevi. Tada je grupa racionalnih točaka $C(\mathbb{Q})$ *konačno generirana abelova grupa.*

Poglavlje 3

Djelidbeni polinomi

Definicija 3.1. *Neka je $C : y^2 = x^3 + Ax + B$ eliptička krivulja, te A i B cijeli brojevi. Definiramo djelidbene polinome $\psi_m \in \mathbb{Z}[x, y]$ na sljedeći način:*

$$\psi_0 = 0 \tag{3.1}$$

$$\psi_1 = 1 \tag{3.2}$$

$$\psi_2 = 2y \tag{3.3}$$

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 \tag{3.4}$$

$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \tag{3.5}$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, m \geq 2 \tag{3.6}$$

$$\psi_{2m} = (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), m \geq 3. \tag{3.7}$$

Lema 3.2. *ψ_n je polinom u $\mathbb{Z}[x, y^2]$ kad je n neparan, a ukoliko je n paran onda je $\psi_n \in 2y\mathbb{Z}[x, y^2]$.*

Dokaz. Za $n \leq 4$ tvrdnja očito vrijedi iz definicije ψ_n. Pretpostavimo sada da tvrdnja vrijedi za sve $n < 2m$. Pretpostavimo također da je $m > 2$, pa je $2m > m + 2$, pa za sve polinome koji se pojavljuju u definiciji od ψ_{2m} vrijedi naša induktivna pretpostavka. Ako je m paran, onda su $\psi_m, \psi_{m+2}, \psi_{m-2} \in 2y\mathbb{Z}[x, y^2]$, pa slijedi da je i $\psi_{2m} \in 2y\mathbb{Z}[x, y^2]$. Ukoliko je m neparan, tada su ψ_{m+1} i ψ_{m-1} elementi iz $2y\mathbb{Z}[x, y^2]$, pa slijedi da je $\psi_{2m} \in 2y\mathbb{Z}[x, y^2]$, induktivno tvrdnja slijedi i za $n = 2m$.
Pretpostavimo sada da tvrdnja vrijedi za sve $n < 2m + 1$. Ako je m neparan, onda su $\psi_{m+2}, \psi_m \in \mathbb{Z}[x, y^2]$ i $\psi_{m-1}, \psi_{m+1} \in 2y\mathbb{Z}[x, y^2]$ zbog induktivne pretpostavke, pa je onda $\psi_{m+2}\psi_m^3, \psi_{m-1}\psi_{m+1}^3 \in \mathbb{Z}[x, y^2]$, pa je i $\psi_{2m+1} \in \mathbb{Z}[x, y^2]$. Ako je m paran, onda imamo $\psi_{m+2}, \psi_m \in 2y\mathbb{Z}[x, y^2]$ i $\psi_{m-1}, \psi_{m+1} \in \mathbb{Z}[x, y^2]$ pa opet imamo na isti način $\psi_{2m+1} \in \mathbb{Z}[x, y^2]$. □

Radi jednostavnosti računanja uvodimo sljedeće polinome:

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1},$$

$$\omega_m = (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).$$

Lema 3.3. *$\phi_n \in \mathbb{Z}[x, y^2]$, $\forall n \in \mathbb{N}$. Ako je n neparan, tada je $\omega_n \in y\mathbb{Z}[x, y^2]$. Ako je n paran, tada je $\omega_n \in \mathbb{Z}[x, y^2]$*

Dokaz. Ako je n neparan, ψ_{n+1} i ψ_{n-1} su elementi iz $y\mathbb{Z}[x, y^2]$, pa je njihov produkt iz $\mathbb{Z}[x, y^2]$. Jer je $\psi_m \in 2y\mathbb{Z}[x, y^2]$, slijedi da je $\psi_m^2 \in \mathbb{Z}[x, y^2]$, pa je i $x\psi_m^2 \in \mathbb{Z}[x, y^2]$. Konačno iz definicije od ϕ_n slijedi da je $\phi_n \in \mathbb{Z}[x, y^2]$. Slučaj kada je n paran dokazuje se analogno koristeći prethodnu lemu. Iz prethodne leme i definicije polinoma ω_n, direktno slijedi da ako je n neparan, onda $y^{-1}\omega_n \in \mathbb{Z}[x, y^2]$ te ako je n paran onda je $\omega_n \in \frac{1}{2}\mathbb{Z}[x, y^2]$. Da je $\omega_n \in \mathbb{Z}[x, y^2]$ pokazuje se indukcijom. □

Lema 3.4. *Polinom $\phi_n(x)$ je normiran polinom stupnja n^2, a polinom $\psi_n^2(x)$ je stupnja $n^2 - 1$ s vodećim koeficijentom n^2.*

Dokaz. Tvrdimo da je

$$\psi_n = \begin{cases} y(nx^{(n^2-4)/2} + \cdots) & \text{, n paran} \\ nx^{(n^2-1)/2} + \cdots & \text{, n neparan} \end{cases} \tag{3.8}$$

Dokazujemo tvrdnju indukcijom. Pretpstavimo da tvrdnja vrijedi za sve $n < 2m + 1$. Ukoliko je $n = 2m + 1$ i m paran, tada je vodeći koeficijent od $\psi_{m+2}\psi_m^3$ jednak

$$(m + 2)m^3y^4x^{\frac{(m+2)^2-4}{2} + \frac{3m^2-12}{2}}. \tag{3.9}$$

Sada ukoliko umjesto y^4 pišemo $(x^3 + Ax + B)^2$ prethodni izraz poprima oblik

$$(m + 2)m^3x^{\frac{(2m+1)^2-1}{2}}. \tag{3.10}$$

Na analogan način dobivamo da je vodeći koeficijent od $\psi_{m-1}\psi_{m+1}^3$ jednak

$$(m - 1)(m + 1)^3x^{\frac{(2m+1)^2-1}{2}}, \tag{3.11}$$

pa stoga uvrštavanjem u rekurziju dobivamo tvrdnju. U ostalim slučajevima postupamo analogno. Tvrdnja za $\phi_n(x)$ slijedi direktno iz dokazane tvrdnje. □

Teorem 3.5. *Neka je $P = (x, y)$ točka na eliptičkoj krivulji $y^2 = x^3 + Ax + B$ i neka je n prirodan broj. Tada*

$$nP = \left(\frac{\phi_n(x)}{\psi_n(x, y)^2}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3}\right) \tag{3.12}$$

Dokaz teorema može se naći u [4].
Iskažimo prvo tehničku lemu.

Lema 3.6. *Neka je* $D = 4A^3 + 27B^2$ *i neka je*

$$F(x,z) = x^4 - 2Ax^2z^2 - 8Bxz^3 + A^2z^4, \tag{3.13}$$

$$G(x,z) = 4z(x^3 + Axz^2 + Bz^3), \tag{3.14}$$

$$f_1(x,z) = 12x^2z + 16Az^3, \tag{3.15}$$

$$g_1(x,z) = 3x^3 - 5Axz^2 - 27Bz^3, \tag{3.16}$$

$$f_2(x,z) = 4Dx^3 - 4A^2Bx^2z + 4A(3A^3 + 22B^2)xz^2 + 12B(A^3 + 8B^2)z^3, \tag{3.17}$$

$$g_2(x,z) = A^2Bx^3 + A(5A^3 + 32B^2)x^2z + 2B(13A^3 + 96B^2)xz^2 - 3A^2(A^3 + 8B^2)z^3. \tag{3.18}$$

Tada je $Ff_1 - Gg_1 = 4Dz^7$ *i* $Ff_2 + Gg_2 = 4Dx^7$.

Dokaz. Znamo da polinomi $F(x,1)$ i $G(x,1)$ nemaju zajedničkih korijena, pa primjenom Euklidovog algoritma dobivamo egzistenciju polinoma $f_1(x), g_1(x)$ tako da vrijedi

$$F(x,1)f_1(x) + G(x,1)g_1(x) = 1. \tag{3.19}$$

Zamjenom $x := \frac{x}{z}$ i množenjem jednadžbe sa $4Dz^7$ dobivamo $Ff_1 - Gg_1 = 4Dz^7$. Da $Ff_2 + Gg_2 = 4Dx^7$ vrijedi dobivamo analogno ukoliko zamijenimo x i z. □

Propozicija 3.7. *Neka je C eliptička krivulja. Tada endomorfizam na C koji je induciran množenjem s n ima stupanj* n^2.

Dokaz. Označimo taj endomorfizam s $[n]$. Po definiciji je $deg([n]) = Max\left\{deg(\phi_n), deg(\psi_n^2)\right\}$, a iz leme 3.4 imamo da je $deg([n]) \leq n^2$. Stupanj endomorfizma $[n]$ će stoga biti jednak n^2 ukoliko polinomi ϕ_n i ψ_n^2 nemaju zajedničkih korijena. Pretpostavimo suprotno, da ϕ_n i ψ_n^2 imaju zajednički korijen. Neka je n najmanji prirodan broj takav da ϕ_n i ψ_n^2.
Pretpostavimo prvo da je $n = 2m$. Vrijedi

$$\phi_2(x) = x^4 - 2Ax^2 - 8Bx + A^2, \tag{3.20}$$

$$\psi_2^2(x) = 4y^2 = 4(x^3 + Ax + B). \tag{3.21}$$

Uzmimo točku (x,y) na C i računamo x-koordinatu točke $2m(x,y)$ tako da prvo izračunamo $m(x,y)$ i onda množenjem s 2 dobivamo $2m(x,y)$.
Slijedi da je x-koordinata točke $2m(x,y)$ jednaka

$$\frac{\phi_{2m}}{\psi_{2m}^2} = \frac{\phi_2(\phi_m/\psi_m^2)}{\psi_2^2(\phi_m/\psi_m^2)} = \frac{\phi_m^4 - 2A\phi_m^2\psi_m^4 - 8B\phi_m\psi_m^6 + A^2\psi_m^8}{(4\psi_m^2)(\phi_m^3 + A\phi_m\psi_m^4 + B\psi_m^6)} = \frac{U}{V}. \tag{3.22}$$

Da bi pokazali da U i V nemaju zajedničkih korijena, koristiti ćemo prethodnu lemu. Primjenom leme na U i V imamo

$$U \cdot f_1(\phi_m, \psi_m^2) - V \cdot g_1(\phi_m, \psi_m^2) = 4\psi_m^{14} D, \tag{3.23}$$

$$U \cdot f_2(\phi_m, \psi_m^2) - V \cdot g_2(\phi_m, \psi_m^2) = 4\phi_m^7 D. \tag{3.24}$$

Ukoliko postoji $x_0 \in \overline{K}$ zajednički korijen od U i V; onda uvrštavanjem x_0 u obje gornje jednadžbe dobivamo da je x_0 korijen od ψ_m i ϕ_m, no to je kontradikcija s pretpostavkom da je $n = 2m$ najmanji prirodan broj takav da ψ_n i ϕ_n imaju zajednički korijen.
Preostaje još pokazati da je $U = \phi_{2m}$ i $V = \psi_{2m}^2$. Iz $\frac{\phi_{2m}}{\psi_{2m}^2} = \frac{U}{V}$ i činjenice da U i V nemaju zajednički korijen, slijedi da je $U = a\phi_{2m}$, $V = b\psi_{2m}^2$, za neke $a, b \in K$. Iz definicije polinoma U i V te primjenom leme vidi se da su U i V normirani polinomi, pa je konačno $U = \phi_{2m}$, $V = \psi_{2m}^2$. Slijedi da ϕ_{2m} i ψ_{2m}^2 nemaju zajedničkih korijena.
Neka je sada $n = 2m + 1$ najmanji prirodan broj takav da ψ_n i ϕ_n imaju zajednički korijen x_0. Jednakost

$$\phi_n = x\psi_n^2 - \psi_{n-1}\psi_{n+1} \tag{3.25}$$

Slijedi da je $(\psi_{n-1}\psi_{n+1})(x_0) = 0$, pa je i $(\psi_{n-1}^2\psi_{n+1}^2)(x_0) = 0$. Iz toga slijedi da je x_0 nultočka od $\psi_{n+\delta}^2(x)$, gdje je δ jednak 1 ili -1. Jer je n neparan, ψ_n i $\psi_{n+\delta}$ su polinomi u varijabli x i $(\psi_n\psi_{n+2\delta})^2(x_0) = 0$, pa je x_0 nultočka polinoma $(\psi_n\psi_{n+2\delta})$.
Jer je $\phi_{n+\delta} = x\psi_{n+\delta}^2 - \psi_n\psi_{n+2\delta}$ slijedi da je $\phi_{n+\delta}(x_0) = 0$. Stoga polinomi $\phi_{n+\delta}$ i $\psi_{n+\delta}^2$ imaju zajednički korijen x_0.
U slučaku kada je $n = 2m$ bio paran, pokazali smo da ako ϕ_{2m} i ψ_{2m}^2 imaju zajednički korijen, onda ga također imaju i ϕ_m i ψ_m^2. Primjenom te činjenice na $2m = n + \delta$ i minimalnosti od n slijedi da mora biti

$$\frac{n+\delta}{2} \geq n. \tag{3.26}$$

Iz nejednakosti slijedi da je $n = 1$. Jer je $\phi_1 = x$ i $\psi_1^2 = 1$, slijedi da oni nemaju zajednički korijen, što je kontradikcija s pretpostavkom.
Ovime je pokazano da ϕ_n i ψ_n^2 nemaju zajedničkih korijena, pa slijedi da je stupanj endomorfizma $[n]$ jednak n^2, $\forall n \in \mathbb{N}$. □

Definicija 3.8. *Neka je n prirodan broj i* $[n]$ *pripadni endomorfizam na C. Jezgra od* $[n]$ *je podgrupa od C. Tu podgrupu ćemo označavati s* $C[n]$.

Teorem 3.9. *Neka je K polje karakteristike nula i* C/K *eliptička krivulja. Grupa* $C[n]$ *je direktna suma dvije cikličke grupe reda n, tj.*

$$C[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}. \tag{3.27}$$

Dokaz. Označimo s $[n]$ endomorfizam induciran množenjem s n. Jer je $char(K) = 0$, endomorfizam $[n]$ je separabilan, pa primjenom propozicije 3 dobivamo da $|C[n]| = |Ker([n])| = n^2$. Strukturni teorem za konačne abelove grupe povlači da je

$$C[n] \simeq (\mathbb{Z}/n_1\mathbb{Z}) \oplus (\mathbb{Z}/n_2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/n_k\mathbb{Z}), \tag{3.28}$$

za neke prirodne brojeve $n_1, n_2, ..., n_k$ takve da $n_i|n_{i+1}, \forall i \leq k$. Neka je p prost djelitelj od n_1. Tada $p|n_i$, $i \leq k$. Iz toga slijedi da $C[p]$ ima red p^k. No već smo pokazali da $C[n]$ ima red n^2, pa posebno $C[p]$ ima red p^2, pa stoga mora biti $k = 2$, tj.

$$C[n] \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}. \tag{3.29}$$

Jer množenje s n poništava sve elemente iz $C[n]$, onda poništava sve elemente iz $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, pa mora biti $n_2|n$. Također znamo da je $card(\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}) = n_1 n_2 = |C[n]| = n^2$. Iz toga slijedi da je $n_1 = n_2 = n$ te je konačno

$$C[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n. \tag{3.30}$$

□

Poglavlje 4

Galoisove reprezentacije

4.1 Osnovni pojmovi i rezultati

Neka je sada K Galoisovo proširenje od $\mathbb{Q}$. Tada za svaku točku $P = (x, y) \in C(K)$ i svaki element $\sigma \in Gal(K/\mathbb{Q})$ definiramo

$$\sigma(P) = (\sigma(x), \sigma(y)). \tag{4.1}$$

Za početak, zanima nas nalazi li se uopće $\sigma(P)$ na C, te koje informacije o $\sigma(P)$ znamo ako nam je poznata točka P.

Propozicija 4.1. *Neka je C eliptička krivulja s koeficjentima u $\mathbb{Q}$ i neka je $K/\mathbb{Q}$ Galoisovo proširenje. Tada vrijedi:*
a) $C(K)$ je podgrupa od $C(\mathbb{C})$.
b) Za $P \in C(K)$ i $\sigma \in Gal(K/\mathbb{Q})$

$$\sigma(P) := \begin{cases} (\sigma(x), \sigma(y)) & , \text{ ako } P = (x, y) \\ O, & , \text{ inače} \end{cases} \tag{4.2}$$

Tada je $\sigma(P) \in C(K)$.
c) Za sve $P, Q \in C(K)$ i $\sigma \in Gal(K/\mathbb{Q})$,

$$\sigma(P + Q) = \sigma(P) + \sigma(Q), \quad \sigma(-P) = -\sigma(P). \tag{4.3}$$

Posebno vrijedi $\sigma(nP) = n(\sigma(P))$, $\forall n \in \mathbb{Z}$.
d) Ako $P \in C(K)$ ima red n i $\sigma \in Gal(K/\mathbb{Q})$, tada $\sigma(P)$ ima red n.

Dokaz. a)Ako su P_1 i P_2 u $C(K)$, onda su njihove x i y koordinate u K. Sada je jasno iz formule zbrajanja da točka $P_1 \pm P_2$ također ima koordinate u K. Stoga $C(K)$ je zatvoren na zbrajanje i oduzimanje pa je i podgrupa od $C(\mathbb{C})$.
b) Neka je $P = (x, y) \in C(K)$. Koordinate od $\sigma(P)$ su u K, pa samo treba procijeniti je li $\sigma(P)$ na C. Imamo sljedeći niz implikacija:
$P \in C \implies y^2 - x^3 - ax^2 - bx - c = 0$

$$\implies \sigma(y^2 - x^3 - ax^2 - bx - c = 0) = 0 \tag{4.4}$$

$$\implies \sigma(y)^2 - \sigma(x)^3 - \sigma(a)\sigma(x)^2 - \sigma(b)\sigma(x) - \sigma(c) = 0 \tag{4.5}$$

$$\implies \sigma(y)^2 - \sigma(x)^3 - a\sigma(x)^2 - b\sigma(x) - c = 0 \tag{4.6}$$

$$\implies \sigma(P) = (\sigma(x), \sigma(y)) \in C(K) \tag{4.7}$$

Implikacija 4.5 vrijedi zato jer je σ homomorfizam, a 4.7 zato jer σ fiksira $\mathbb{Q}$.
c) $P = (x_1, y_1)$, $Q = (x_2, y_2)$ i $P + Q = (x_3, y_3)$. Pretpostavimo prvo da je $P \neq \pm Q$. Iz formula

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a - x_1 - x_2, \quad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \tag{4.8}$$

te činjenice da je σ homomorfizam koji fiksira $\mathbb{Q}$, imamo da je

$$\sigma(x_3) = \left(\frac{\sigma(y_2) - \sigma(y_1)}{\sigma(x_2) - \sigma(x_1)}\right)^2 - \sigma(a) - \sigma(x_1) - \sigma(x_2) \tag{4.9}$$

$$\sigma(y_3) = \left(\frac{\sigma(y_2) - \sigma(y_1)}{\sigma(x_2) - \sigma(x_1)}\right)(\sigma(x_1) - \sigma(x_3)) - \sigma(y_1). \tag{4.10}$$

Sada se lako vidi da je

$$\sigma(P + Q) = (\sigma(x_3), \sigma(y_3)) = (\sigma(x_1), \sigma(y_1)) + (\sigma(x_2), \sigma(y_2)) = \sigma(P) + \sigma(Q). \tag{4.11}$$

Jednakost $\sigma(-P) = -\sigma(P)$ slijedi iz:

$$\sigma(-P) = \sigma(x, -y) = (\sigma(x), \sigma(-y)) = (\sigma(x), -\sigma(y)) = -\sigma(P). \tag{4.12}$$

Posljednja tvrdnja iz d) slijedi direktno iz $\sigma(P + Q) = \sigma(P) + \sigma(Q)$.
d) Pretpostavimo da $P \in C(K)$ ima red n. Tada iz d) imamo da $n\sigma(P) = \sigma(nP) = \sigma(O) = O$, pa red od $\sigma(P)$ dijeli n. Ako pretpostavimo da je $m\sigma(P) = O = \sigma(mP)$, pa djelovanjem sa σ^{-1} na drugu jednakost daje $O = \sigma^{-1}(O) = \sigma^{-1}(\sigma(mP)) = mP$, tj. $m \geq n$. Stoga $\sigma(P)$ ima red točno n. □

Propozicija 4.2. *Neka je C eliptička krivulja dana s*

$$C : y^2 = x^3 + ax^2 + bx + c \tag{4.13}$$

s racionalnim koeficijentima a, b i c.
a) Neka je $P = (x_1, y_1) \in C$ točka reda n. Tada su x_1 i y_1 algebarski nad $\mathbb{Q}$.
b) Neka je

$$\{(x_1, y_1), ..., (x_m, y_m), O\} = C[n]$$

skup točaka čiji red dijeli n. Stavimo $K = \mathbb{Q}(x_1, y_1, ..., x_m, y_m)$. Tada je $K/\mathbb{Q}$ Galoisovo.

Dokaz. a) Neka je $P = (x, y)$. Označimo sa $(nP)_x$ x-koordinatu točke nP. Iz teorema 3.5 slijedi da za svaki prirodan broj n, postoje polinomi $\phi_n(x), \psi_n^2(x) \in \mathbb{Q}[x]$ takvi da je

$$(nP)_x = \frac{\phi_n(x)}{\psi_n^2(x)}. \tag{4.14}$$

Tada točka $P = (x_1, y_1)$ ima red koji dijeli n ako i samo ako $\psi_n^2(x_1) = 0$, pa slijedi da je x_1 algebarski nad $\mathbb{Q}$. Nadalje, iz $y^2 = x^3 + ax^2 + bx + c$ slijedi da je y_1^2 algebarski, pa je i y_1 algebarski.
b) Neka je $\sigma : K \to \mathbb{C}$ homomorfizam polja. Da bi pokazali da je K Galoisovo nad $\mathbb{Q}$, trebamo pokazati da je $\sigma(K) = K$. Jasno je da je σ jedinstveno određeno s djelovanjem na x_i, y_i, $i \leq m$. Iz propozicije, slijedi da ako je $P_i \in C[n]$, onda je i $\sigma(P_i) \in C[n]$, pa je $\sigma(P_i) = P_j$, za neki $j \leq m$, pa pošto to vrijedi za sve $i \leq m$, onda je $\sigma(K) \subset K$, pa je K Galoisovo nad $\mathbb{Q}$. □

Od sada pa nadalje $\mathbb{Q}(x_1, y_1, ..., x_m, y_m)$ označavati ćemo s $\mathbb{Q}(C[n])$. Cilj je opisati strukturu grupe $Gal(\mathbb{Q}(C[n]))/\mathbb{Q})$. Zbog teorema 3.9 znamo da $C[n]$ možemo generirati sa dva elementa. Neka su to P_1 i P_2. Tada skup

$$\{a_1P_1 + a_2P_2 : a_1, a_2 \in \mathbb{Z}/n\mathbb{Z}\} \tag{4.15}$$

je upravo skup svih točaka iz $C[n]$. Za neki homomorfizam $h : C[n] \to C[n]$, tada

$$h(a_1P_1 + a_2P_2) = a_1h(P_1) + a_2h(P_2) \tag{4.16}$$

pa je h u potpunosti određen s djelovanjem na P_1 i P_2. Uzmimo sada $h : C[n] \to C[n]$ homomorfizam. Pošto P_1, P_2 generiraju $C[n]$, $h(P_1)$ i $h(P_2)$ su linearne kombinacije od P_1 i P_2:

$$h(P_1) = \alpha_hP_1 + \gamma_hP_2 \tag{4.17}$$

$$h(P_2) = \beta_hP_1 + \delta_hP_2 \tag{4.18}$$

gdje su $\alpha_h, \beta_h, \gamma_h, \delta_h \in \mathbb{Z}/n\mathbb{Z}$ jedinstveno određeni s h. Promatrajmo prethodnu jednakost u matričnom zapisu:

$$(h(P_1), h(P_2)) = (P_1, P_2)\begin{pmatrix}\alpha_h & \beta_h \\ \gamma_h & \delta_h\end{pmatrix}. \tag{4.19}$$

Ako je $g : C[n] \to C[n]$ proizvoljan homomorfizam, lako se provjeri da je kompozicija $g \circ h$ dana s

$$\begin{pmatrix}\alpha_{g\circ h} & \beta_{g\circ h} \\ \gamma_{g\circ h} & \delta_{g\circ h}\end{pmatrix} = \begin{pmatrix}\alpha_g & \beta_g \\ \gamma_g & \delta_g\end{pmatrix}\begin{pmatrix}\alpha_h & \beta_h \\ \gamma_h & \delta_h\end{pmatrix}. \tag{4.20}$$

Potaknuti ovim činjenicama, dolazimo do ideje da promatramo grupu invertibilnih 2×2 matrica s koeficjentima u $\mathbb{Z}/n\mathbb{Z}$.

Definicija 4.3. *Sa* $\mathrm{GL}_r(R)$ *označavamo skup* $r \times r$ *matrica* A *s koeficijentima u komutativnom prstenu* R *tako da je* $det(A) \in R^*$. *Taj skup je zapravo grupa (s operacijom množenja), te ju nazivamo generalna linearna grupa.*

Iz prethodne diskusije pokazali smo da $\sigma \in Gal(\mathbb{Q}(C[n])/\mathbb{Q})$ inducira izomorfizam grupe $C[n]$, te smo svakom izomorfizmu pridružili element iz $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ i time dobili preslikavanje

$$\rho_n : Gal(\mathbb{Q}(C[n]))/\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \tag{4.21}$$

$$\rho_n(\sigma) = \begin{pmatrix}\alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma\end{pmatrix}. \tag{4.22}$$

Lako se pokaže da vrijedi

$$\rho_n(\sigma\tau) = \rho_n(\sigma)\rho_n(\tau), \tag{4.23}$$

tj. ρ_n je homomorfizam.

Definicija 4.4. *Homomorfizam* ρ_n *nazivamo mod n Galoisovom reprezentacijom pridruženu eliptičkoj krivulji* C.

Teorem 4.5. *Neka je* C *eliptička krivulja s racionalnim koeficjentima i* $n \geq 2$. *Fiksirajmo generatore* P_1 *i* P_2 *od* $C[n]$. *Tada je preslikavanje*

$$\rho_n : Gal(\mathbb{Q}(C[n]))/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \tag{4.24}$$

monomorfizam.

Dokaz. Preostaje dokazati samo da je ρ_n injekcija. Pretpostavimo da je $\sigma \in Gal(\mathbb{Q}(C[n]))/\mathbb{Q})$ u jezgri od ρ_n, tj. $\rho_n(\sigma) = I$. Iz ovog slijedi da je $\sigma(P_1) = P_1$ i $\sigma(P_2) = P_2$, pa slijedi da je $\sigma(P) = P$, $\forall P \in C[n]$. Pošto je po definiciji $\sigma(x, y) = (\sigma(x), \sigma(y))$, slijedi da σ fiksira x i y koordinate svake točke iz $C[n]$, pa σ fiksira cijelo polje $\mathbb{Q}(C[n])$. Iz toga slijedi da je σ identiteta u $Gal(\mathbb{Q}(C[n]))/\mathbb{Q})$, pa i konačno da je ρ_n injekcija. □

Primjer 4.6. *Promatrajmo eliptičku krivulju*

$$C : y^2 = x^3 - 2. \tag{4.25}$$

Točke reda dva su

$$C[2] = \left\{O, (\sqrt[3]{2}, 0), (\zeta\sqrt[3]{2}, 0), (\zeta^2(\sqrt[3]{2}, 0)\right\} = \{O, P_1, P_2, P_3\},$$

gdje je $\zeta = \frac{-1+\sqrt{-3}}{2}$ *primitivni treći korijen iz jedinice. Lako se pokaže da je polje* $\mathbb{Q}(C[2])$ *generirano s točkama reda dva jednako* $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$.
Galoisova grupa $Gal(\mathbb{Q}(C[2])/\mathbb{Q})$ *je izomorfna grupi* S_3*, pa možemo pisati*

$$Gal(\mathbb{Q}(C[2])/\mathbb{Q}) = \left\{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\right\},$$

gdje su σ *i* τ *određeni s*

$$\sigma(\sqrt[3]{2}) = \zeta\sqrt[3]{2}, \quad \tau(\sqrt[3]{2}) = \sqrt[3]{2},$$
$$\sigma(\sqrt{-3}) = \sqrt{-3}, \quad \tau(\sqrt{-3}) = -\sqrt{-3}.$$

Tada σ *i* τ *zadovoljavaju relacije* $\sigma^3 = \tau^2 = e$ *i* $\sigma\tau = \tau\sigma^2$.
Za generatore od $C[2]$ *uzeti ćemo točke* P_1 *i* P_2*. Tada vrijedi:*

$$\sigma(P_1) = \sigma(\sqrt{2}, 0) = (\zeta\sqrt[3]{2}, 0) = P_2,$$

$$\sigma(P_2) = \sigma(\zeta\sqrt[3]{2}, 0) = (\zeta^2\sqrt[3]{2}, 0) = P_3 = P_1 + P_2.$$

Sada vidimo da je $\rho_2(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$*. Promotrimo sada i* τ*:*

$$\tau(P_1) = \tau(\sqrt[3]{2}, 0) = (\zeta\sqrt[3]{2}, 0) = P_1,$$

$$\tau(P_2) = \tau(\zeta\sqrt[3]{2}, 0) = (\zeta^2\sqrt[3]{2}, 0) = P_3 = P_1 + P_2,$$

pa imamo da je $\rho_2(\tau) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
Pošto σ *i* τ *generiraju* $Gal(\mathbb{Q}(C[2])/\mathbb{Q})$ *i jer znamo vrijednosti* $\rho(\sigma)$ *i* $\rho(\tau)$*, možemo lako izračunati* $\rho(x)$*, gdje je* x *bilo koji element u* $Gal(\mathbb{Q}(C[2])/\mathbb{Q})$.

Neka je sada $n = p$ prost broj. Zbog prvog teorema o izomorfizmu i prethodnog teorema, za određivanje strukture grupe $Gal(\mathbb{Q}(C[n]))/\mathbb{Q})$ dovoljno nam je odrediti strukturu grupe $\mathrm{Img}(\rho_n)$. Pokazati ćemo da $\mathrm{Img}(\rho_n)$ kao podgrupa od $\mathrm{GL}_2(\mathbb{F}_p)$ može biti sadržana u samo nekim maksimalnim podgrupama od $\mathrm{GL}_2(\mathbb{F}_p)$, koje ćemo klasificirati u narednim poglavljima.

4.2 Borelova podgrupa

Neka je V vektorski prostor dimenzije 2 nad poljem $\mathbb{F}_p$. Za naše potrebe korisno će biti promatrati djelovanje $\mathrm{GL}_2(\mathbb{F}_p)$ na V.

Definicija 4.7. *Standardnom Borelovom podgrupom B od $\mathrm{GL}_2(\mathbb{F}_p)$ nazivamo podgrupu koja se sastoji od elemenata oblika*

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \tag{4.26}$$

gdje su $a, d \in \mathbb{F}_p^x$ i $b \in \mathbb{F}_p$.

Definicija 4.8. *Borelova podgrupa je bilo koja podgrupa od $\mathrm{GL}_2(\mathbb{F}_p)$ koja je konjugat od standardne Borelove podgrupe.*

Lako se vidi da postoji bijekcija između Borelovih podgrupa i jednodimenzionalnih potprostora W od V.
Neka je W jednodimenzionalan potprostor od V i neka je $\{x\}$ baza za W. Nadopunimo ju s vektorom y do baze za V. Promotrimo regularan linearan operator $A : V \to V$ čiji je svojstveni potprostor W.
Tada je $Ax = ax$, za neki $a \in F_p^x$ i $Ay = bx + dy$, za $b, d \in F_p$ (b i d su takvi da je A regularan operator). Matrica operatora A obzirom na tu bazu je upravo

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}. \tag{4.27}$$

Lema 4.9. *Svaka Borelova grupa sastoji se od $p(p-1)^2$ elemenata.*

Dokaz. Promatrajmo standardnu Borelovu podgrupu B. Da bi gornje-trokutasta matrica

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \tag{4.28}$$

bila regularna, jasno je da $a \neq 0$, pa a možemo izabrati na $p-1$ načina, b na p načina. Preostaje samo primjetiti da zbog linearne nezavisnosti redaka d možemo izabrati na $p-1$ načina. Tvrdnja za proizvoljnu Borelovu podgrupu sada slijedi iz činjenice da svaka konjugirana podgrupa od B ima isti kardinalitet kao i B. □

Lema 4.10. *Neka je*

$$w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{4.29}$$

te B Borelova podgrupa. Tada je $\mathrm{GL}_2(\mathbb{F}_p) = B \cup BwB$, te su skupovi B i BwB disjunktni. Ovakva dekompozicija naziva se Bruhatova dekompozicija.

Sada navodimo korisnu činjenicu o Borelovim podgrupama B.

Propozicija 4.11. *Borelova podgrupa B je maksimalna prava podgrupa od* $\mathrm{GL}_2(\mathbb{F}_p)$.

Dokaz. Neka je $s \in \mathrm{GL}_2(\mathbb{F}_p) \setminus B$. Tada prema Bruhatovoj dekompoziciji je $s \in BwB$, pa kada bi postojala podgrupa M od $\mathrm{GL}_2(\mathbb{F}_p)$ koja sadrži B, te je $s \in M$, onda zbog $s \in BwB$ slijedi $s = awa$, za neki $a \in B$. Pa je $BwB \subset M$, iz čega slijedi $M = \mathrm{GL}_2(\mathbb{F}_p)$, pa je B maksimalna prava podgrupa. □

4.3 Cartanova podgrupa

Sada ćemo definirati još jednu klasu podgrupa od $\mathrm{GL}_2(\mathbb{F}_p)$ koja će nam biti bitna za daljnju analizu.

Definicija 4.12. *Rascjepiva Cartanova podgrupa od* $\mathrm{GL}_2(\mathbb{F}_p)$ *je bilo koja podgrupa koja je konjugat podgrupe dijagonalnih matrica.*

Analogno kao i u slučaju kod Borelovih podgrupa, može se vidjeti da postoji $1-1$ korespondencija između uređenih parova (W_1, W_2) gdje su W_1, W_2 različiti jednodimenzionalni potprostori od V i linearnih transformacija na V kojima su W_1 i W_2 svojstveni potprostori.
Neka su $W_1, W_2 \subseteq V$ dva jednodimenzionalna potprostora i neka je $\{x\}$ baza za W_1, $\{x, y\}$ baza za V i $\{x + ay\}$ baza za W_2, te $a \in \mathbb{F}_p^x$. Tada ako je A regularan operator na V čiji su W_1 i W_2 svojstveni potprostori, onda postoje $\lambda_1, \lambda_2 \in \mathbb{F}_p^x$ takvi da

$$Ax = \lambda_1 x, \tag{4.30}$$

$$A(x + ay) = \lambda_2(x + ay). \tag{4.31}$$

Preostaje primjetiti da je $\{x, x + ay\}$ također baza za V te da je matrični zapis od A u bazi $\{x, x + ay\}$ dijagonalna matrica s elementima λ_1 i λ_2 na dijagonali.
Rascjepiva Cartanova podgrupa je izomorfna direktnom produktu dvije cikličke grupe reda $(p-1)$, pa stoga ima red $(p-1)^2$.
Neka je V' vektorski prostor induciran s V' i kvadratnim proširenjem polja $\mathbb{F}_p$ i W' jednodimenzionalni potprostor od V' koji nije induciran nekim potprostorom od V. Nadalje, neka je W'' konjugat od W' nad $\mathbb{F}_p$.

Definicija 4.13. *Nerascjepiva Cartanova podgrupa je konjugat od*

$$C_{ns} := \left\{ \begin{pmatrix} a & \delta b \\ b & a \end{pmatrix} \right\}, \tag{4.32}$$

gdje je $(\frac{\delta}{p}) = -1$, $a, b \in \mathbb{F}_p$.

Nerascjepiva Cartanova podgrupa je izomorfna multiplikativnoj grupi polja s p^2 elemenata, a pošto je multiplikativna grupa konačnog polja nužno ciklička, slijedi da je nerascjepiva Cartanova podgrupa izomorfna cikličkoj grupi reda $p^2 - 1$.

Lema 4.14. *Matrice*

$$X(b) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \quad Y(c) = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \tag{4.33}$$

generiraju $\mathrm{SL}_2(\mathbb{F}_p)$.

Dokaz. Promotrimo prvo što se dešava ukoliko proizvoljni element $S \in \mathrm{SL}(\mathbb{F}_p)$ pomnožimo s $X(b)$.

$$S\,X(b) = \begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p & pb + q \\ r & rb + s \end{pmatrix} \tag{4.34}$$

što je zapravo zbrajanje prvog retka pomnoženog sa skalarom s drugim retkom matrice. Na analogan način zaključujemo da je množenje elementa S s $X(b), Y(c)$ s lijeva i s desna elementarna matrična operacija. Sada se lako vidi da se primjenom tih operacija, matrica S može zapisati u obliku

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}. \tag{4.35}$$

Za $a \neq 1$, pokazati ćemo da postoje $x, b, c, d \in \mathbb{F}_p$ tako da je

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}. \tag{4.36}$$

Neka je $x \neq 0$ proizvoljan. Množenjem navedenih matrica i stavljanjem

$$b = \frac{a-1}{x}, c = \frac{-x}{1+bc}, d = \frac{-b}{1+bc}, \tag{4.37}$$

čime smo pokazali egzistenciju zapisa. Preostaje samo primjetiti da je $X(b)X(-b) = X(-b)X(b) = I$, te analognu tvrdnju za za $Y(c)$, pa slijedi da je S generiran s elementima oblika $X(b), Y(c)$, čime je tvrdnja leme dokazana. □

Teorem 4.15. *Neka je G podgrupa od $\mathrm{GL}_2(\mathbb{F}_p)$. Ako je red od G djeljiv s p, tada je G sadržana u Borelovoj podgrupi od $\mathrm{GL}_2(\mathbb{F}_p)$ ili G sadrži $\mathrm{SL}_2(\mathbb{F}_p)$.*

Dokaz. Uzmimo $\sigma \in G$ čiji je red p. Tada postoji jedinstveni jednodimenzionalni potprostor W od V koji je svojstveni potprostor od σ. Jer je σ reda p, onda je $x^p - x$ polinom koji se poništava u σ. Jer je $x^p - x = x(x-1)(x-2)\cdots(x-(p-1))$ u $\mathbb{F}_p[x]$, onda iz $0 = \sigma^p - \sigma = \sigma(\sigma - I)(\sigma - 2I)\cdots(\sigma - (p-1)I)$ slijedi da je barem jedan operator oblika $\sigma - kI$ singularan, pa σ ima svojstveni potprostor. Ukoliko bi postojala dva svojstvena potprostora W_1, W_2 od σ, neka je bez smanjenja općenitosti $\{x\}$ baza za W_1, $\{x, y\}$ baza za V i

$\{x + ay\}$ baza za W_2, $a \in \mathbb{F}_p^x$. Tada je $Ax = \lambda_1 x$ i $A(x + ay) = \lambda_2(x + ay)$ za neke $\lambda_1, \lambda_2 \in \mathbb{F}_p^x$. Slijedi da je $\sigma^{p-1}(x) = \lambda_1^{p-1}(x) = x$ i $\sigma^{p-1}(x + ay) = \lambda_2^{p-1}(x + ay) = (x + ay)$ prema Malom Fermatovom teoremu. Jer je $\{x, x + ay\}$ baza za V, slijedi da je $\sigma^{p-1} = I$, pa $p = |\sigma|$ dijeli $p - 1$, što je kontradikcija.
Ako svaki element od G ima W kao svojstveni potprostor, tada je G sadržana u Borelovoj podgrupi asociranoj s W. Ako ne, neka je σ_1 element iz G koji preslikava W u neki drugi potprostor W'. Tada je $\sigma_1\sigma\sigma_1^{-1}$ element reda p čiji je jedini svojstveni potprostor W'. Uzmimo generatore x i y od W i W' te promatrajmo σ i $\sigma_1\sigma\sigma_1^{-1}$ u matričnom zapisu, obzirom na bazu $\{x, y\}$. Tada postoje nenul elementi $b, c \in F_p$ tako da je

$$\sigma = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \quad \sigma_1\sigma\sigma_1 = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}. \tag{4.38}$$

Prema lemi 4.14, slijedi da ove matrice generiraju $\mathrm{SL}(\mathbb{F}_p)$, pa G sadrži $\mathrm{SL}(\mathbb{F}_p)$.

Teorem 4.16. *Neka je G podgrupa od $\mathrm{GL}_2(\mathbb{F}_p)$. Ako je red od G relativno prost s p, neka je H slika od G u $\mathrm{PGL}_2(\mathbb{F}_p)$. Tada:*
a) H je ciklička i G je sadržana u Cartanovoj podgrupi;
b) H je dihedralna i G je sadržana u normalizatoru Cartanove podgrupe ali nije sadržana u samoj Cartanovoj podgrupi;
c) H je izomorfna s A_4, S_4, A_5, gdje S označava simetričnu, a A alternirajuću grupu.

Dokaz teorema može se naći u [3].

□

4.4 Weilovo sparivanje

Definicija 4.17. *Neka je K polje i n prirodan broj. Tada definiramo*

$$\mu_n = \left\{ x \in \overline{K} \mid x^n = 1 \right\}. \tag{4.39}$$

Skup μ_n čini grupu obzirom na množenje i tu grupu nazivamo grupom n-tih korijena iz jedinice u $\overline{K}$.

Teorem 4.18. *Neka je C eliptička krivulja definirana nad poljem K i neka je n prirodan broj. Pretpostavimo dodatno da karakteristika polja K ne dijeli n. Tada postoji preslikavanje*

$$e_n : C[n] \times C[n] \to \mu_n \tag{4.40}$$

sa sljedećim svojstvima:

1. *e_n je bilinearno preslikavanje u obje varijable, tj.*

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T),$$
$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2),$$

$\forall S, S_1, S_2, T, T_1, T_2 \in C[n]$.

2. *e_n je nedegenerirana u obje varijable, tj. $e_n(S, T) = 1, \forall T \in C[n]$, tada je $S = O$ i ako je $e_n(S, T) = 1, \forall S \in C[n]$ tada je $T = O$.*

3. *$e_n(T, T) = 1, \forall T \in C[n]$.*

4. *$e_n(T, S) = e_n(S, T)^{-1}, \forall S, T \in C[n]$*

5. *$e_n(\sigma(S), \sigma(T)) = \sigma(e_n(S, T))$ za sve automorfizme σ od $\overline{K}$ takve da σ fiksira koeficijente od C.*

6. *$e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{deg(\alpha)}$ za sve separabilne endomorfizme α od C. Ako koeficijenti od C leže u konačnom polju F_q, tada tvrdnja također vrijedi i za Frobeniusov automorfizam ϕ_q.*

Propozicija 4.19. *Neka je $\{T_1, T_2\}$ baza za $C[n]$. Tada je $e_n(T_1, T_2)$ primitivni n-ti korijen iz jedinice.*

Dokaz. Pretpostavimo da je $e_n(T_1, T_2) = \zeta$ i neka je $\zeta^d = 1$ Tada je zbog bilinearnosti $e_n(T_1, dT_2) = 1$ i $e_n(T_2, dT_2) = 1$. Neka je $S \in C[n]$. Zapišimo $S = aT_1 + bT_2$ (To možemo napraviti zato jer je $\{T_1, T_2\}$ baza za $C[n]$), $a, b \in \mathbb{Z}$.

$$e_n(S, dT_2) = e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b = 1. \tag{4.41}$$

Jer je S bio proizvoljan, slijedi da $e_n(S, dT_2) = 1 \forall S \in C[n]$. Svojstvo 2. implicira da je $dT_2 = O$. Pošto je $dT_2 = O$ ako i samo ako $n|d$ slijedi da je ζ primitivni n-ti korijen iz jedinice. □

Propozicija 4.20. *Neka je α endomorfizam eliptičke krivulje C definirane nad poljem K. Neka je n pozitivan cijeli broj koji nije djeljiv s karakteristikom polja K. Tada je* $\det(\alpha_n) \equiv deg(\alpha)(mod\ n)$.

Dokaz. Iz prethodnog korolara slijedi da je $\zeta = e_n(T_1, T_2)$ primitivni n-ti korijen iz jedinice. Iz svojstva 6. teorema o egzistenciji Weilovog sparivanja imamo:

$$\zeta^{deg(\alpha)} = e_n(\alpha(T_1), \alpha(T_2)) = e_n(aT_1 + cT_2, bT_1 + dT_2) = \tag{4.42}$$
$$e_n(T_1, T_1)^{ab} e_n(T_1, T_2)^{ad} e_n(T_2, T_1)^{bc} e_n(T_2, T_2)^{cd} = \zeta^{ad-bc} \tag{4.43}$$

Obzirom da je ζ primitivni korijen iz jedinice, slijedi da je $deg(\alpha) \equiv ad - bc(modn)$, što je i trebalo pokazati. □

Definicija 4.21. *Kažemo da je podgrupa G od $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ aplikabilna ako zadovoljava sljedeća svojstva:*

1. $G \neq GL_2(\mathbb{Z}/N\mathbb{Z})$
2. $-I \in G$ *i* $det(G) = (\mathbb{Z}/N\mathbb{Z})^x$
3. G *sadrži element traga* 0 *i determinante* -1 *koji fiksira točku u* $(\mathbb{Z}/N\mathbb{Z})^2$ *reda* N.

Lema 4.22. *Ne postoji prava podgrupa S od $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ takva da je $\pm S = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.*

Dokaz leme može se naći u [5].

Teorem 4.23. *Neka je C eliptička krivulja nad $\mathbb{Q}$ za koju mod N Galoisova reprezentacija nije surjektivna. Tada je $\pm\rho_N(Gal_\mathbb{Q})$ aplikabilna podgrupa od $GL_2(\mathbb{Z}/N\mathbb{Z})$.*

Dokaz. Grupa $G = \pm\rho_N(Gal_\mathbb{Q})$ očito sadrži $-I$ pošto sadrži I. Promotrimo preslikavanje $det \circ \rho_N : Gal_\mathbb{Q} \to (\mathbb{Z}/N\mathbb{Z})^x$. Pokazati ćemo da je to preslikavanje surjektivni homomorfizam grupa. Da je homomorfizam slijedi direktnom provjerom. Iz Weilovog sparivanja slijedi da ako je ζ N-ti korijen iz jedinice, onda je $\sigma(\zeta) = \zeta^{det(\rho_n(\sigma))}$, $\forall\sigma \in Gal_\mathbb{Q}$. No također vrijedi da za svaki $k \in (\mathbb{Z}/N\mathbb{Z})^x$ postoji $\sigma \in Gal_\mathbb{Q}$ tako da vrijedi $\sigma(\zeta) = \zeta^k$. Ovome smo pokazali da je dano preslikavanje surjektivno.
Pretpostavimo sada da je $G = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ i definirajmo $S = \rho_N(Gal_\mathbb{Q}) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Jer $\rho_N(Gal_\mathbb{Q})$ nije surjekcija, slijedi $\rho_N(Gal_\mathbb{Q}) \neq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Zbog $\det(\rho_N(Gal_\mathbb{Q})) = (\mathbb{Z}/N\mathbb{Z})^x$ i prvog teorema o izomorfizmu slijedi

$$\rho_N(Gal_\mathbb{Q})/(\rho_N(Gal_\mathbb{Q}) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})) = \rho_N(Gal_\mathbb{Q})/S \simeq (\mathbb{Z}/N\mathbb{Z})^x, \tag{4.44}$$

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\,\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = G/\,\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \pm\rho_N(Gal_\mathbb{Q})/\,\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \simeq (\mathbb{Z}/N\mathbb{Z})^x. \tag{4.45}$$

Sada iz prvog izomorfizma slijedi

$$\pm\,\rho_N(Gal_\mathbb{Q})/(\pm S) \simeq (\mathbb{Z}/N\mathbb{Z})^x, \tag{4.46}$$

a zbog $\pm\rho_N(Gal_\mathbb{Q})/S\,L_2(\mathbb{Z}/N\mathbb{Z}) \simeq (\mathbb{Z}/N\mathbb{Z})^x$ slijedi $\pm S = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Kada bi bilo $S = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, onda korištenjem prvog izomorfizma dobivamo $\rho_N(Gal_\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, pa je $S \neq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. No to je u kontradikciji s lemom 4.22, pa je $G \neq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.
Neka je c automorfizam od $\overline{\mathbb{Q}}$ induciran kompleksnim konjugiranjem. Neka je $g := \rho_N(c)$. Znamo da je $C(\mathbb{C})$ izomorfan s $\mathbb{C}/\Lambda$, te da je povezana komponenta od $C(\mathbb{R})$ izomorfna s $\mathbb{R}/\mathbb{Z}$. Stoga možemo odabrati točku $P = [1/N, 0]$ u $\mathbb{C}/\Lambda$ čiji je red N. Promatramo li matrični zapis od $\rho_N(c)$ u bazi koja sadrži točku P, slijedi da $\rho_N(c)$ ima oblik

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}. \tag{4.47}$$

Nadalje, znamo da je $\zeta^{det(\rho_N(c))} = c(\zeta) = \overline{\zeta} = \zeta^{-1}$, pa je $\det(g) = -1$ i $tr(g) = 0$. □

Teorem 4.24. *Neka je C eliptička krivulja nad poljem $\mathbb{Q}$ i neka postoji ciklička izogenija ϕ reda n na C. Tada je slika mod n Galoisove reprezentacije sadržana podgrupi od* $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ *koju čine matrice oblika*

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}. \tag{4.48}$$

Dokaz. Neka je $P = (x_0, y_0)$ generator od $Ker(\phi)$ i $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Vrijedi da je P reda n. Neka je (x_1, y_1) točka na C. Tada je

$$(x_1, y_1) \in Ker(\phi) \iff (x_1, y_1) = kP \iff \psi_n^2(x_1) = 0, \tag{4.49}$$

za neki $k \leq n$ i ψ_n definiran kao u poglavlju 3. Zato jer je ψ_n^2 polinom u $\mathbb{Z}[x]$, slijedi da ako je x_0 nultočka od ψ_n^2, onda je i $\sigma(x_0)$ također nultočka od ψ_n^2, pa je prema 4.49, $\sigma(P) = \sigma(x_0, y_0) \in Ker(\phi)$. Stoga postoji $\alpha \in \mathbb{Z}/n\mathbb{Z}$ takav da je $\sigma(P) = \alpha P$. Konačno, ako je $\{P, Q\}$ baza za $C[n]$, onda je u toj bazi

$$\rho_n(\sigma) = \begin{pmatrix} \alpha & * \\ 0 & * \end{pmatrix}. \tag{4.50}$$

□

Teorem 4.25. *Neka je C eliptička krivulja nad poljem $\mathbb{Q}$. Postoji točka reda N u $C(\mathbb{Q})$ ako i samo ako je*

$$\rho_N(Gal(\mathbb{Q}(C[N])/\mathbb{Q}) \subseteq \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}, a \in \mathbb{F}_p, b \in \mathbb{F}_p^x \right\}. \tag{4.51}$$

Dokaz. Neka je $T \in C(\mathbb{Q})$ reda N. Tada je $\sigma(T) = T$, $\forall \sigma \in Gal(\mathbb{Q}(C[N])/\mathbb{Q}$. Neka je $\{T, S\}$ baza za $C[N]$. Tada u toj bazi svaki element $\rho_N(\sigma)$ ima matrični zapis oblika

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}, a \in \mathbb{F}_p, b \in \mathbb{F}_p^x \right\}, \tag{4.52}$$

pa je jedan smjer tvrdnje pokazan.
Obratno neka je $\{T, S\}$ neka baza za $C[N]$ u kojoj sve matrice iz $\rho_N(Gal(\mathbb{Q}(C[N])/\mathbb{Q})$ imaju oblik

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}, a \in \mathbb{F}_p, b \in \mathbb{F}_p^x \right\}. \tag{4.53}$$

Tada svi elementi grupe $Gal(\mathbb{Q}(C[N])/\mathbb{Q}$ fiksiraju T, pa mora biti $T \in C(\mathbb{Q})$. □

Bibliografija

[1] Joseph H.Silverman,John Tate. *Rational Points on Elliptic Curves*. Springer-Verl, New York, 1992.

[2] Joseph H.Silverman. *The Arithmetic of Elliptic Curves* Springer-Verlag, New York, 1986.

[3] Willem Kuyk, J.P. Serre. *Modular functions of one variable III-1* Springer-Verlag, New York 1973.

[4] Lawrence C. Washington. *Elliptic Curves - Number Theory and Cryptography*, Taylor and Francis Group, 2008.

[5] David J.Zywina *On the possible images of the mod l representations associated to elliptic curves over* $\mathbb{Q}$
http://www.math.cornell.edu/ zywina/papers/PossibleImages/PossibleImages.pdf

[6] Serge Lang *Algebra* Springer-Verlag, New York, 1993.

Sažetak

U prvom poglavlju definirali smo pojam endomorfizma na eliptičkoj krivulji C i dokazali osnovna svojstva. Uveli smo pojam izogenije te pokazali kako se svojstva endomorfizama lako proširuju na izogenije. Spomenuli smo Frobeniusov endomorfizam i dali nekoliko primjera izogenija.
U drugom poglavlju definirali smo pojam visine te iskazali neka njezina bitna svojstva. Iskazali smo teorem spusta te iskazali Mordellov teorem.
U trećem poglavlju razvili smo osnove teorije djelidbenih polinoma te pokazali da je $C[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.
Četvrto poglavlje je glavni dio ovog rada. Definirali smo djelovanje elemenata Galoisove grupe $Gal(K/\mathbb{Q})$ na točke iz C te pokazali osnovne rezultate koji slijede iz djelovanja. Pokazali smo da su koordinate točaka konačnog reda algebarske nad $\mathbb{Q}$ te da je proširenje od $\mathbb{Q}$ inducirano x i y koordinatama točaka nekog fiksnog reda n Galoisovo. Definirali smo mod n Galoisovu reprezentaciju pridruženu krivulji C i pokazali da je to preslikavanje monomorfizam. Definirali smo Borelovu i Cartanovu podgrupu od $\mathrm{GL}(\mathbb{F}_p)$ i pokazali osnovna svojstva. Odredili smo u kojim se maksimalnim podgrupama od $\mathrm{GL}(\mathbb{F}_p)$ može nalaziti slika nesurjektivne mod p Galoisove reprezentacije. Definirali smo Weilovo sparivanje i pokazali u teoremu 4.15. kakva svojstva mora imati slika mod p Galoisove reprezentacije.

Summary

In the first chapter we defined endomorphisms of the elliptic curve C and proved their basic properties. We introduced isogenies and showed how properties of endomorphisms hold for isogenies. We mentioned the Frobenius endomorphism and give a few examples of isogenies.
In the second chapter we defined the height function and showed some important properties. We also introduced the Descent theorem and stated Mordell's theorem.
In the third chapter we developed basic division polynomials theory and we showed that $C[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.
The fourth chapter is the main part of this work. We defined the action of the Galois group $Gal(K/\mathbb{Q})$ on points on C and showed basic properties. We showed that coordinates of points of finite order are algebraic over $\mathbb{Q}$ and that the field extension induced by the x and y coordinates of points that are of finite order n is Galois. We defined the mod n Galois representation attached to the curve C and showed that it is a monomorphism. We defined the Borel and Cartan subgroup of $\mathrm{GL}(\mathbb{F}_p)$ and showed some basic properties. We determined in which maximal subgroups of $\mathrm{GL}(\mathbb{F}_p)$ can the image of non-surjective mod p Galois representation be. We defined the Weil pairing and showed in theorem 4.15 some properties of mod p Galois representation.

Životopis

Tomislav Gužvić rođen je 15.09.1991. godine u Puli, gdje također polazi u Osnovnu školu Stoja, a zatim i Srednju školu Gimnazija Pula. Na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu 2010.godine upisuje studij matematike. Akademske godine 2011./2012. održavao je demonstrature iz kolegija Matematička Analiza 1 i Matematička analiza 2. 2012. i 2013. godine sudjelovao je kao član ekipe Matematičkog odsjeka na studentskom natjecanju International Mathematics Competition (IMC) u Bugarskoj, te je za sudjelovanje nagrađen Dekanovom nagradom. Preddiplomski studij završava 2014. godine, te studij nastavlja na smjeru Teorijska matematika.