Torzijske grupe eliptičkih krivulja

Vukorepa, Borna

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Borna Vukorepa

TORZIJSKE GRUPE ELIPTIčKIH KRIVULJA

Diplomski rad

Voditelj rada:
izv. prof. dr. sc.
Filip Najman

Zagreb, srpanj 2018.

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

Primarni objekt od interesa u ovom radu su eliptičke krivulje i njihove torzijske grupe. Eliptička krivulja nad poljem K može se definirati kao nesingularna projektivna krivulja genusa 1 koja sadrži K-racionalnu točku. Mi ćemo eliptičku krivulju promatrati kao skup točaka koje zadovoljavaju pripadnu kubnu jednadžbu u dvije varijable. Na tom skupu točaka na prirodan se način može uvesti binarna operacija koja daje strukturu Abelove grupe. Točke konačnog reda tvore podgrupu te grupe i ona se naziva torzijskom podgrupom. Nakon nekoliko osnovnih definicija o eliptičkim krivuljama, proučavat ćemo poznate rezultate i dokaze koji govore o strukturi torzijskih podgrupa nad različitim poljima. Promatrat ćemo situaciju za polja $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, te za neka polja algebarskih brojeva. Prije nego što se fokusiramo na našu temu, dajmo kratku priču o elitičkim krivuljama i napretku pripadne teorije.
Grupovna struktura eliptičke krivulje može nam pomoći u nalaženju odgovora na pitanje koliko rješenja ima jednadžba slična ovoj:

$$y^2 = x^3 + 17.$$

Možemo se pitati koliko ima cjelobrojnih, a koliko racionalnih rješenja. Ima li ih konačno ili beskonačno? Ako ih je beskonačno, kakvu strukturu tvori tih beskonačno mnogo rješenja? Ako ih je konačno, koliko ih točno može biti? Da bismo u potpunosti odgovorili na ta pitanja, trebamo istražiti torzijske grupe eliptičkih krivulja, kao i njihov rang, koji ipak neće biti centralna tema ovog rada. Teoremi kao što su Nagell-Lutzov teorem, Mordell-Weilov teorem i Mazurov teorem mogu pomoći u davanju odgovora na to pitanje. Vidjet ćemo kasnije da nam Nagell-Lutzov teorem za gornju jednadžbu garantira da su sve točke koje se nalaze u torzijskoj grupi nad $\mathbb{Q}$ zapravo cjelobrojne. Mazur je 1978. dokazao važan teorem koji daje potpunu listu svih mogućih torzijskih grupa nad $\mathbb{Q}$ za racionalne eliptičke krivulje.
Tvrdnja koju je Mazur dokazao direktno otvara put novim pitanjima. Kako može izgledati torzijska grupa racionalne eliptičke krivulje nad nekim proširenjem od $\mathbb{Q}$? Što ako krivulja nije racionalna, nego definirana nad nekim drugim poljem? Koliko članova torzijska grupa može imati i o čemu to ovisi? Odgovori su poznati za proširenja od $\mathbb{Q}$ malog stupnja i za neka specifična polja. Što se samog kardinaliteta torzijske grupe tiče, Merel je 1994.

dokazao takozvani teorem uniformne ograničenosti koji pokazuje da se red torzijske grupe eliptičke krivulje definirane nad K može ograničiti stupnjem proširenja $[K : \mathbb{Q}]$. Iako je ograda eksponencijalna, taj rezultat je od iznimne važnosti, a otvoren problem je slutnja da postoji i polinomijalna ograda.
Mnogi otvoreni problemi, i to mnogo poznatiji, vežu se za pitanje ranga eliptičke krivulje. Mordell-Weilov teorem otvara priču ranga eliptičke krivulje. On jednostavno kaže da je za racionalnu eliptičku krivulju grupa $E(\mathbb{Q})$ konačno generirana, što znači da se u grupovnoj strukturi javlja određen broj kopija od $\mathbb{Z}$ i taj broj zovemo rangom eliptičke krivulje. Slutnja je da postoje eliptičke krivulje proizvoljno velikog ranga, ali nije pronađena krivulja ranga većeg od 28. Uz rang je vezan i jedan od najpoznatijih neriješenih problema u matematici, legendarna Birch-Swinnerton-Dyerova slutnja. Zanimljivo je da su nedavna istraživanja došla do rezultata koja pokazuju određenu poveznicu ranga eliptičke krivulje i strukture torzijske grupe.
Ovo je bio vrlo kratak pregled nekih rezultata iz teorije eliptičkih krivulja iz kojeg je jasno da je ta teorija vrlo bogata i razgranata s mnogo otvorenih problema koje vrijedi rješavati. Kao što smo rekli, fokus ovog rada je na torzijskim grupama eliptičkih krivulja.

Poglavlje 1

Osnovno o eliptičkim krivuljama

1.1 Zapis eliptičkih krivulja

Definicija 1.1.1. *Neka je E nesingularna projektivna krivulja genusa 1 i neka je $O \in E$. Uređen par (E, O) zovemo eliptičkom krivuljom i uglavnom označavamo samo s E.*

Definicija 1.1.2. *Ako je K polje, tada za eliptičku krivulju E kažemo da je definirana nad K, i pišemo E/K, ako je E definirana nad K kao krivulja i vrijedi $O \in E(K)$. S $E(K)$ ćemo označavati skup točaka s koordinatama iz K koje se nalaze na E.*

Koristeći Riemann-Rochov teorem (pogledati [5], poglavlje III.3), možemo pokazati sljedeći važan rezultat:

Teorem 1.1.3. *Neka je K polje i E eliptička krivulja definirana nad K. Tada se ona može prikazati kao skup točaka u $\mathbb{P}^2$ koji zadovoljavaju kubnu jednadžbu oblika*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1.1}$$

pri čemu vrijedi $a_1, a_2, a_3, a_4, a_6 \in K$.

Gornja jednadžba zove se Weierstrassova jednadžba eliptičke krivulje. Jasno je da vrijedi $O = [0 : 1 : 0] \in E(K)$. Stavljajući $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, dobijemo Weierstrassovu jednadžbu u nehomogenim koordinatama:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.2}$$

Ne smijemo zaboraviti da E sadrži i dodatnu točku O u beskonačnosti. Ako pretpostavimo da je $char(K) \neq 2$, zamjenom $y \mapsto y - \frac{1}{2}(a_1x + a_3)$ eliminiramo iz Weierstrassove jednadžbe članove linearne po y i dobijamo oblik:

$$y^2 = x^3 + ax^2 + bx + c. \tag{1.3}$$

Dodatno, ako je $char(K) \neq 3$, možemo uvesti zamjenu $x \mapsto x - \frac{1}{3}a$ i dobijemo takozvanu kratku Weierstrassovu formu eliptičke krivulje:

$$y^2 = x^3 + bx + c. \tag{1.4}$$

Gotovo sva polja koja ćemo promatrati će zadovoljavati $char(K) = 0$. Jasno je da ako znamo koje točke zadovoljavaju (1.4), trivijalno znamo koje točke zadovoljavaju (1.2). Uočimo da smo iz duge Weierstrassove forme prešli u kratku koristeći samo linearne transformacije.
Regularnost eliptičke krivulje može se provjeriti preko diskriminante polinoma $x^3 + bx + c$. Njegova diskriminanta je $D = -4b^3 - 27c^2$. Pripadna krivulja će biti regularna točno onda kada je $D \neq 0$.

1.2 Grupovna operacija

Motivacija

Znamo da pravac može sjeći graf polinoma trećeg stupnja u jednoj ili tri (realne) točke, brojeći multiplicitet. Potpuno analogno, uvrštavanjem možemo vidjeti da pravac $y = kx + l$ siječe skup točaka (x, y) koje zadovoljavaju (1.2) u jednoj ili tri (realne) točke. To nam daje ideju da ako uzmemo dvije točke na krivulji i provučemo pravac kroz njih, dobit ćemo još točno jednu točku na krivulji. Već i ova jednostavna ilustracija nagoviješta grupovnu strukturu. Općenitije, motivacija dolazi iz Bezoutovog teorema koji nam kaže da ako je E eliptička krivulja definirana nad K, a L neki pravac, tada njihov presjek sadrži tri točke u $\mathbb{P}^2$, brojeći multiplicitete. Računaju se i kompleksne točke, odnosno točke s koordinatama iz algebarskog zatvorenja promatranog polja K.

Definicija grupovne operacije

Kako ćemo većinom baratati s poljima karakteristike 0, možemo uzeti da je E eliptička krivulja dana svojom kratkom Weierstrassovom jednadžbom (1.4). Ona sadrži točke $P = (x, y)$ koje zadovoljavaju tu jednadžbu i dodatnu točku $O = [0 : 1 : 0]$ u beskonačnosti. Neka imamo $P, Q \in E$ i neka je L pravac kroz P i Q (tangenta ukoliko je $P = Q$) i neka L siječe E još u R. Neka je L_1 pravac kroz R i O (tangenta ukoliko je $R = O$). Njegovo treće sjecište s E definiramo kao zbroj točaka P i Q i označavamo kao $P + Q$.

Propozicija 1.2.1. *Gornje opisano pravilo pridruživanja čini Abelovu grupu na skupu točaka na eliptičkoj krivulji E s neutralnim elementom O.*

Svakako nam je bitno odrediti koordinate točke $P + Q$. Nećemo provoditi cijeli postupak, nego samo izreći pravilo, jer se radi samo o algebarskim manipulacijama. Neka je

$P, Q \in E$. Znamo da je $-O = O$. Ako je $Q = O$, tada je $P + Q = P$, slično za $P = O$. Inače, imamo $P = (x_1, y_1)$, $Q = (x_2, y_2)$. Tada je $-P = (x_1, -y_1)$. Ako je $Q = -P$, tada je $P + Q = O$. Ako je $P \neq \pm Q$, tada je:

$$x(P + Q) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \tag{1.5}$$

$$y(P + Q) = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3). \tag{1.6}$$

Posebno će nam biti važan slučaj $P = Q$. Tada umjesto pravca kroz dvije točke povlačimo tangentu u točki $P = (x, y)$ i dalje je sve samo algebarsko manipuliranje. Dolazimo do važne duplikacijske formule:

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2}{4x^3 + 4bx + 4c}. \tag{1.7}$$

Ako stavimo u kratkoj Weierstrassovoj formi $y^2 = x^3 + bx + c = f(x)$, tada uz malo igranja ta formula postaje:

$$x(2P) = \frac{f'(x)^2}{4f(x)} - 2x. \tag{1.8}$$

Važno pitanje

Sjetimo se da smo do kratke Weierstrassove forme došli linearnim transformacijama. Pošto će nas zanimati struktura grupe, moramo se zapitati je li ona očuvana nakon primjena tih transformacija. Da, jer su one linearne pa preslikavaju pravce u pravce, što znači da imamo homomorfizam (u linearnom slučaju i izomorfizam). Međutim, postoje i manje očiti slučajevi, npr. ako imamo krivulju danu s

$$u^3 + v^3 = c. \tag{1.9}$$

Ako stavimo zamjenu

$$u = \frac{36c + y}{6x}, \quad v = \frac{36c - y}{6x}, \tag{1.10}$$

tada dobijamo eliptičku krivulju u Weierstrassovoj formi $y^2 = x^3 - 432c^2$. Nije ni najmanje očito da je grupovna struktura očuvana jer se pravci ne preslikavaju u pravce pri ovoj transformaciji. Ipak, moguće je pokazati da biracionalna transformacija čuva grupovnu strukturu pa je transformacija iz ovog primjera opravdana.

Poglavlje 2

Grupa kompleksnih i realnih točaka

2.1 Točke malog reda

Točke reda 2

U cijelom ovom poglavlju pretpostavljamo da je karakteristika promatranog polja 0, pa je dovoljno promatrati eliptičku krivulju E danu svojom kratkom Weierstrassovom formom:

$$y^2 = f(x) = x^3 + bx + c. \tag{2.1}$$

Točke reda 2 nije teško karakterizirati i njih opisuje iduća lagana propozicija.

Propozicija 2.1.1. *Neka je $E/\mathbb{Q}$ eliptička krivulja definirana nad $\mathbb{Q}$ i neka je $P \in E$. Tada je $P = (x, y)$ reda 2 ako i samo ako je $y = 0$. Dodatno, ako dozvolimo da P ima kompleksne koordinate, tada E sadrži točno četiri točke čiji red dijeli 2 i one tvore grupu izomorfnu grupi $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*

Dokaz. Znamo da je $2P = O$ ako i samo ako je $P = -P$ tj. ako i samo ako je $(x, y) = (x, -y)$. Dakle, P je reda 2 ako i samo ako je $y = 0$. Mogućnosti za x-koordinatu točke P su upravo nultočke polinoma $f(x) = x^3 + bx + c$. One su različite zbog regularnosti krivulje. Dakle, imamo tri točke reda 2 i one zajedno s točkom O tvore četveročlanu grupu čiji svaki netrivijalni element je reda 2, pa je ona izomorfna s $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. □

Slične rezultate bismo mogli dobiti ako za P tražimo da ima realne ili racionalne koordinate, ovisno o broju realnih i racionalnih nultočaka od f.

Točke reda 3

Slično, točke reda 3 možemo opisati kroz iduću propoziciju:

Propozicija 2.1.2. *Neka je $E/\mathbb{Q}$ eliptička krivulja definirana nad $\mathbb{Q}$ i neka je $P \in E$. Tada je $P = (x, y)$ reda 3 ako i samo ako je x nultočka polinoma $g(x) = 3x^4 + 6bx^2 + 12cx - b^2$. E sadrži točno osam točaka reda 3 i one zajedno s O tvore grupu izomorfnu s $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.*

Dokaz. Ako je $3P = O$, tada je $2P = -P$ pa je $x(2P) = x(-P) = x(P)$. Ako je $x(P) = x(2P)$, tada je $y(2P) = \pm y(P)$, što znači da je ili $2P = P$ ili $2P = -P$. Prvi slučaj bi dao $P = O$, a drugi daje $3P = O$ tj P je reda 3. Dakle, točke reda 3 su karakterizirane uvjetom $x(P) = x(2P)$. Sada se samo trebamo sjetiti duplikacijske formule (1.7) i izjednačiti x-koordinate:

$$x = \frac{x^4 - 2bx^2 - 8cx + b^2}{4x^3 + 4bx + 4c} \Leftrightarrow 3x^4 + 6bx^2 + 12cx - b^2 = 0.$$

Uočimo da takav x ne može zadovoljavati $f(x) = 0$ jer bi tada bilo $y = 0$, pa bi P bila reda 2. Kako bismo dobili da imamo osam kompleksnih točaka reda 3, moramo pokazati da $g(x) = 3x^4 + 6bx^2 + 12cx - b^2$ nema višestrukih nultočaka. Za to je dovoljno provjeriti da $g(x)$ i $g'(x)$ nemaju zajedničkih nultočaka. Ovdje će nam lakše biti računati pomoću duplikacijske formule (1.8), pa uvjet $x(P) = x(2P)$ možemo zapisati ovako:

$$x = \frac{f'(x)^2}{4f(x)} - 2x \Leftrightarrow 12xf(x) - f'(x)^2 = 0,$$

pa imamo da je:

$$g(x) = 12xf(x) - f'(x)^2,$$
$$g'(x) = 12xf'(x) + 12f(x) - 2f''(x)f'(x).$$

Jasno je da je $f''(x) = 6x$, pa imamo zapravo:

$$g'(x) = 12f(x).$$

Sada zbog regularnosti $f(x)$ i $f'(x)$ nemaju zajedničkih nultočaka, pa ni $g(x)$ i $g'(x)$. Dakle, imamo osam kompleksnih točaka reda 3 i jasno je sada da one s točkom O tvore grupu izomorfnu s $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. □

Mogli bismo ovako nastaviti dalje, no situacija bi postajala sve složenija za redove 4, 5, itd.

2.2 Grupa kompleksnih točaka

Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada je ona dana kratkom Weierstrassovom formom $y^2 = x^3 + bx + c$, a zamjenom y s $4y$ i x s $4x$ možemo dobiti oblik $y^2 = 4x^3 - g_2x - g_3$, gdje su $g_2, g_3 \in \mathbb{Q}$. Bit će jasno zašto nam je ovaj oblik pogodan za ovo poglavlje. Cilj nam

je odrediti grupovnu strukturu kompleksnih točaka na E, pa će nakon toga biti jasno što je pripadna torzijska grupa. Uvest ćemo nekoliko novih pojmova kao što su eliptičke funkcije i Weierstrassova funkcija. Također ćemo rezultate dobivene ovdje iskoristiti za određivanje grupe realnih točaka u idućem dijelu. Većinu stvari nećemo dokazivati, nego samo navesti i izvesti zaključke. Detalji i dokazi tvrdnji u ovoj sekciji mogu se pronaći u ([5], VI.).

Definicija 2.2.1. *Neka su $\omega_1, \omega_2 \in \mathbb{C}$ linearno nezavisni nad $\mathbb{R}$. Skup dan s $\Lambda = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\}$ zovemo rešetka.*

Definicija 2.2.2. *Neka je $\Lambda \subseteq \mathbb{C}$ rešetka i $f : \mathbb{C} \to \mathbb{C}$ meromorfna funkcija koja zadovoljava*

$$(\forall z \in \mathbb{C})(\forall \omega \in \Lambda) \quad f(z + \omega) = f(z).$$

Tada za f kažemo da je eliptička funkcija.

Definicija 2.2.3. *Neka je $\Lambda \subseteq \mathbb{C}$ rešetka. Weierstrassova $\wp$ funkcija s obzirom na Λ je zadana redom*

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Definicija 2.2.4. *Neka je $\Lambda \subseteq \mathbb{C}$ rešetka i $k \in \mathbb{N}$, $k \geq 2$. Eisensteinov red težine $2k$ je red*

$$G_{2k}(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-2k}.$$

Uz malo analize, može se pokazati da vrijedi tvrdnja niže.

Teorem 2.2.5. *Neka je $\Lambda \in \mathbb{C}$ rešetka. Tada pripadni Eisensteinov red apsolutno konvergira za svaki $k > 1$. Red koji definira Weierstrassovu funkciju konvergira apsolutno i uniformno na svakom kompaktnom podskupu od $\mathbb{C} \setminus \Lambda$. Red definira meromorfnu funkciju koja ima polove točno u točkama iz Λ i oni su reda 2. Dodatno, Weierstrassova funkcija je parna eliptička funkcija.*

Igranjem s poretkom sumacije pokazuje se da vrijedi propozicija:

Propozicija 2.2.6. *Laurentov red za $\wp(z)$ oko $z = 0$ je dan s:*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k}.$$

Koristeći prethodnu propoziciju promatranjem Laurentovog reda se može dobiti ovaj važan rezultat:

Teorem 2.2.7. *Za sve $z \in \mathbb{C} \setminus \Lambda$, Weierstrassova funkcija zadovoljava relaciju*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Ako uvedemo oznake

$$g_2 = g_2(\Lambda) = 60G_4, \quad g_3 = g_3(\Lambda) = 140G_6,$$

dobijamo relaciju

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

Ovo sada podsjeća na oblik jednadžbe eliptičke krivulje kojeg smo naveli na početku ove diskusije. Zasad znamo da ako imamo rešetku $\Lambda \subseteq \mathbb{C}$, tada ona određuje Weierstrassovu funkciju i vrijednosti g_2 i g_3. Iz gornje relacije vidi se da je za svaki $z \in \mathbb{C} \setminus \Lambda$ točka $P = (\wp(z), \wp'(z))$ na krivulji $y^2 = 4x^3 - g_2x - g_3$. Ipak, još uvijek nije jasno da je to eliptička krivulja jer nismo još garantirali regularnost. To pitanje rješava ova propozicija:

Propozicija 2.2.8. *Neka je $\Lambda \subseteq \mathbb{C}$ i neka su g_2, g_3 definirani kao maloprije. Tada polinom $f(x) = 4x^3 - g_2x - g_3$ ima tri različite nultočke.*

Ovime smo dobili da svaka rešetka daje jednu eliptičku krivulju. Ključno je da vrijedi i obrat u obliku takozvanog uniformizacijskog teorema za eliptičke krivulje:

Teorem 2.2.9. *Za proizvoljne $A, B \in \mathbb{C}$ takve da polinom $f(x) = 4x^3 - Ax - B$ ima tri različite nultočke postoji jedinstvena rešetka $\Lambda \subseteq \mathbb{C}$ koja zadovoljava*

$$g_2(\Lambda) = A, \quad g_3(\Lambda) = B.$$

Ako promatramo eliptičke krivulje do na izomorfizam, rešetka je jedinstvena do na homotetiju tj. do na množenje kompleksnim brojem različitim od 0*.*

Dosadašnje tvrdnje su dovoljne da se dokaže teorem koji će razriješiti pitanje grupovne strukture kompleksnih točaka na eliptičkoj krivulji.

Teorem 2.2.10. *Neka je eliptička krivulja dana jednadžbom $y^2 = 4x^3 - g_2x - g_3$ za neke kompleksne g_2 i g_3 i neka je Λ pripadna rešetka. Tada je preslikavanje $\phi : \mathbb{C} \to E(\mathbb{C})$ dano s*

$$\phi(z) = \begin{cases} (\wp(z), \wp'(z)), & z \notin \Lambda \\ O, & z \in \Lambda \end{cases}$$

surjektivni homomorfizam grupa. Promatramo li pripadno kvocijentno preslikavanje na $\mathbb{C}/\Lambda$, dobijamo izomorfizam pa vrijedi $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$.

Sada je jasno koje su točke konačnog reda. Vrijedi da je $\mathbb{C}/\Lambda \cong \mathbb{R}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Z} \cong S^1 \oplus S^1$ (torus), pa je $E(\mathbb{C})_{tors}$ izomorfna direktnom produktu dviju kopija grupa kompleksnih korijena iz jedinice.
Za proizvoljni $n \in \mathbb{N}$, promatrajmo skup $E[n] = \{P \in E(\mathbb{C}) : nP = O\}$. Jasno je da je on podgrupa grupe svih kompleksnih točaka na E. Pomoću informacija koje zasad imamo, nije nam teško odrediti izgled te podgrupe. To će nam biti korisno kasnije.

Korolar 2.2.11. *Uz oznake kao do sada,*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Dokaz. Jasno je da su elementi grupe $\mathbb{R}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Z}$ koji pomnoženi s n daju 0 upravo $\left(\frac{a}{n} + \mathbb{Z}, \frac{b}{n} + \mathbb{Z}\right)$ za $a, b \in \mathbb{Z}$. Jasno je da oni tvore grupu izomorfnu grupi $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, pa sada zbog $E(\mathbb{C}) \cong \mathbb{R}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Z}$ slijedi tvrdnja. □

2.3 Grupa realnih točaka

Koristeći prethodne rezultate, možemo odrediti grupu realnih točaka eliptičke krivulje. Jasno je iz formula zbrajanja točaka da ako je eliptička krivulja definirana nad $\mathbb{R}$ ili $\mathbb{Q}$ da njene realne točke čine grupu. Prvo ćemo odrediti kako izgleda rešetka Λ koja odgovara eliptičkoj krivulji s realnim koeficijentima i zatim ćemo zaključiti kojim sve standardnim grupama i pod kojim uvjetima može biti izomorfna grupa realnih točaka. Nakon toga, slično kao u kompleksnom slučaju, torzijsku grupu će biti lako odrediti.

Propozicija 2.3.1. *Neka je $E/\mathbb{R}$ eliptička krivulja dana u obliku $y^2 = 4x^3 - Ax - B$ i Λ pripadna rešetka. Tada je Λ invarijantna na kompleksno konjugiranje.*

Dokaz. Pretpostavimo suprotno i promotrimo konjugiranu rešetku Λ'. Tada je iz ranije danih formula za g_2 i g_3 jasno da je $g_2(\Lambda') = \overline{g_2(\Lambda)} = \overline{A} = A$, analogno za B. To je sada u kontradikciji s teoremom 2.2.9 jer su Λ i Λ' različite rešetke. □

Jasno je iz formule kojom je dana Weierstrassova funkcija da u slučaju kad je Λ invarijantna na konjugiranje vrijedi

$$\wp(\overline{z}) = \overline{\wp(z)}, \quad \wp'(\overline{z}) = \overline{\wp'(z)}.$$

To znači da konjugirani kompleksni brojevi odgovaraju konjugiranim točkama na krivulji. Tražimo realne točke, pa nas zanimaju $z \in \mathbb{C}$ takvi da z i $\overline{z}$ odgovaraju istim točkama. Jasno je da svi članovi rešetke imaju to svojstvo, oni odgovaraju točki O koju računamo kao realnu (i racionalnu) točku na E. Ako z nije član rešetke, kako je $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, mora biti $z = \overline{z}$, gledano modulo Λ. Prije nego što pronađemo takve z, malo ćemo više saznati o strukturi rešetke koja je invarijantna na konjugiranje.

Propozicija 2.3.2. *Neka je $\Lambda \subseteq \mathbb{C}$ rešetka invarijantna na konjugiranje. Tada možemo uzeti da je jedan od generatora $r \in \mathbb{R}$, a drugi $v \in \mathbb{C}$ koji zadovoljava $\overline{v} = -v + kr$ za neki $k \in \mathbb{Z}$.*

Dokaz. Neka je su ω_1, ω_2 generatori za Λ i neka bez smanjenja općenitosti ω_1 nije čisto imaginaran. Tada je $\overline{\omega_1} \in \Lambda$, pa je i $\omega_1 + \overline{\omega_1} \in \Lambda$, no jasno je da je $\omega_1 + \overline{\omega_1} \in \mathbb{R}$. Imamo dakle da je $\omega_1 + \overline{\omega_1} = a\omega_1 + b\omega_2$ za neke cijele a i b. Kako ω_1 nije čisto imaginaran, a i b nisu oba 0, pa možemo pretpostaviti da su relativno prosti (inače samo podijelimo s najvećim zajedničkim djeliteljem). Stavimo $r = a\omega_1 + b\omega_2$. Kako su a i b relativno prosti, postoje cijeli brojevi c i d takvi da $A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ ima determinantu 1. Stavimo $v = c\omega_1 + d\omega_2$. Sada je lako dobiti da se svaki član rešetke Λ može dobiti kao cjelobrojna kombinacija r i v, npr. tražimo cijele k i l takve da je

$$kr + lv = m\omega_1 + n\omega_2.$$

Uvrštavanjem se dobije da je to ekvivalentno s

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} k \\ l \end{bmatrix} = \begin{bmatrix} m \\ n \end{bmatrix}.$$

Kako je determinanta matrice sustava 1, rješenje je cjelobrojno pa r i v zaista generiraju Λ. Znamo da mora biti $\overline{v} \in \Lambda$, pa je $\overline{v} = lv + kr$, za neke cijele k i l. Nužno je $l = -1$ jer r utječe samo na realni dio, a v nikako nije realan jer je nezavisan s r. Ovime je tvrdnja dokazana. □

Sada možemo odrediti koji su članovi grupe $\mathbb{C}/\Lambda$ invarijantni na konjugiranje.

Propozicija 2.3.3. *Neka je $\Lambda \subseteq \mathbb{C}$ rešetka invarijantna na konjugiranje i neka su v, r, k kao u prethodnoj propoziciji. Ako je k neparan, tada su točno članovi skupa $S = \{ar : 0 \leq a < 1\} \subseteq \mathbb{C}/\Lambda$ invarijantni na konugiranje. Ako je k paran, to su točno članovi skupa $T = \{ar + bv : 0 \leq a < 1, b \in \{0, \frac{1}{2}\}\} \subseteq \mathbb{C}/\Lambda$.*

Dokaz. Neka je $z \in \mathbb{C}/\Lambda$. Tada je $z = ar + bv$ za $0 \leq a, b < 1$. Imamo $\overline{z} = ar + b\overline{v} = ar + bkr - bv$. Da bi u $\mathbb{C}/\Lambda$ vrijedilo $z = \overline{z}$ mora biti $b = -b$ i $a = a + kb$, gledano modulo 1. Slijedi da je $b = \frac{1}{2}$ ili $b = 0$. Ako je $b = 0$, a može biti bilo što između 0 i 1. Ako je k neparan, $b = \frac{1}{2}$ ne dolazi u obzir, pa je tada traženi skup elemenata invarijantnih na konjugiranje upravo S iz iskaza. Slično zaključimo za paran k da je traženi skup upravo T iz iskaza. □

Kao što smo prije zaključili, elementi $\mathbb{C}/\Lambda$ invarijantni na konjugiranje čine podrupu koja odgovara grupi realnih točkaka krivulje. Iz prethodne propozicije vidimo da postoje

dvije mogućnosti. U prvom slučaju (k neparan), grupa realnih točaka je izomorfna s $\mathbb{R}/\mathbb{Z} \cong S^1$, a u drugom slučaju s $(\mathbb{R}/\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) \cong S^1 \oplus (\mathbb{Z}/2\mathbb{Z})$. Jasno je da se oba slučaja mogu dogoditi (samo odaberemo rešetku s parnim ili neparnim k i odredimo pripadne g_2 i g_3), ali još nismo dali jasan odgovor kad nastupa koji slučaj. Karakterizacija preko parnosti k nije dovoljno korisna.
Sjetimo se preslikavanja ϕ iz teorema 2.2.10. Ono je izomorfizam ako mu za domenu uzmemo $\mathbb{C}/\Lambda$, pa ako su r i v generatori za Λ kao i do sada, on točke $\frac{r}{2}, \frac{v}{2}, \frac{r+v}{2}$ šalje u točke reda 2 na krivulji. Znamo od ranije da je y-koordinata tih točaka 0, pa imamo da su $\wp\left(\frac{r}{2}\right), \wp\left(\frac{v}{2}\right), \wp\left(\frac{r+v}{2}\right)$ sve različite nultočke polinoma $f(x) = 4x^3 - g_2x - g_3$. Točno oni od $\frac{r}{2}, \frac{v}{2}, \frac{r+v}{2}$ koji odgovaraju realnim nultočkama su invarijantni na konjugiranje. Ako je samo $\frac{r}{2}$, imamo slučaj koji je nastupio za neparan k, inače onaj koji je nastupio za paran k. Sve ovo možemo sumirati ovim teoremom:

Teorem 2.3.4. *Neka je $E/\mathbb{Q}$ eliptička krivulja dana jednadžbom $y^2 = f(x) = 4x^3 - g_2x - g_3$. Tada je $E(\mathbb{R}) \cong S^1$ kada f ima jednu realnu nultočku, a $E(\mathbb{R}) \cong S^1 \oplus (\mathbb{Z}/2\mathbb{Z})$ kada f ima tri realne nultočke.*

Poglavlje 3

Grupa racionalnih točaka

3.1 Nagell-Lutzov teorem

Neka je kao i do sada $E/\mathbb{Q}$ eliptička krivulja zadana jednadžbom

$$y^2 = f(x) = x^3 + bx + c.$$

Promatrat ćemo racionalne točke na E (koje očito tvore grupu) i dokazati neke važne činjenice o racionalnim točkama konačnog reda, s naglaskom na Nagell-Lutzov teorem i leme koje su potrebne u njegovom dokazu, ali i korisne same po sebi. Razmatrat ćemo i pitanje strukture torzijske grupe racionalnih točaka, koje će se pokazati znatno težim nego u kompleksnom i realnom slučaju.
Uočimo da ako jednadžbu kojom je zadana krivulja pomnožimo s d^6, za neki $d \in \mathbb{Z}$, a zatim uvedemo zamjenu $X = d^2x$, $Y = d^3y$, jednadžba postaje:

$$Y^2 = X^3 + d^4bX + d^6c.$$

Jasno je da možemo odabrati d tako da nova jednadžba ima cjelobrojne koeficijente. Zato ćemo u ovom poglavlju pretpostaviti da su b i c cijeli. Označimo s $D = -4b^3 - 27c^2$ diskriminantu polinoma f. Ona je različita od 0 jer f ima različite nultočke (regularnost). Nije teško dokazati ovu pomoćnu tvrdnju:

Lema 3.1.1. *Neka je $P = (x, y)$ točka na E takva da P i $2P$ imaju cjelobrojne koordinate. Tada je $y = 0$ ili $y^2|D$.*

Dokaz. Pretpostavimo da je $y \neq 0$. Tada je $2P \neq O$, pa je prema duplikacijskoj formuli

$$x(2P) = \frac{\phi(x)}{4f(x)} = \frac{x^4 - 2bx^2 - 8cx + b^2}{4(x^3 + bx + c)}.$$

Kako je $x(2P)$ cijeli broj, vrijedi $4y^2|x^4 - 2bx^2 - 8cx + b^2$, pa bi bilo dobro prikazati D kao

$$\phi(X)F(X) + f(X)G(X)$$

za neke $F, G \in \mathbb{Z}[x]$. Računanjem možemo dobiti da vrijedi

$$(X^4 - 2bX^2 - 8cX + b^2)(3X^2 + 4b) + (X^3 + bX + c)(-3X^3 + 5bX + 27c) = -D.$$

Imamo da je $f(x) = y^2$ i ranije smo komentirali da $y^2|\phi(x)$, pa slijedi $y^2|D$. □

Sada ćemo pokazati tvrdnju koja će u kombinaciji s prethodnom lemom dati Nagell-Lutzov teorem koji daje jednostavan i očit način kako odrediti torzijsku grupu specifične eliptičke krivulje $E/\mathbb{Q}$.

Teorem 3.1.2. *Neka je $P = (x, y)$ racionalna točka na E konačnog reda. Tada P ima cjelobrojne koordinate ili je $P = O$.*

Dokaz. Neka je p prost broj i $q \in \mathbb{Q}$, q promatramo kao do kraja skraćen razlomak. Promatrajmo najveću potenciju od p koja dijeli q, u oznaci $v_p(q)$. Ako je brojnik od q djeljiv s p, tada je $v_p(q)$ jednak najvećoj potenciji od p koja dijeli brojnik (preciznije, njenom eksponentu). Ako je nazivnik djeljiv s p, tada je $v_p(q)$ jednak negativnoj najvećoj potenciji od p koja dijeli nazivnik. Inače, $v_p(q) = 0$. Npr. $v_3\left(\frac{9}{2}\right) = 2$, $v_5\left(\frac{3}{5}\right) = -1$, $v_7\left(\frac{9}{2}\right) = 0$.
Slučaj $P = O$ je trivijalan, pa neka je $P \neq O$. Jasno je da će tvrdnja biti dokazana ako dokažemo da je za proizvoljan prost p vrijedi $v_p(x), v_p(y) \geq 0$. Pretpostavimo suprotno. Riješimo najprije slučaj kad je neka od koordinata od P jednaka 0. Ako je $x = 0$, onda je $y^2 \in \mathbb{Z}$, a kako je $y \in \mathbb{Q}$, znamo i $y \in \mathbb{Z}$. Ako je $x \neq 0, y = 0$, tada je x nultočka normiranog polinoma s cjelobrojnim koeficijantima i slijedi $x \in \mathbb{Z}$.
Neka je sada $x, y \neq 0$. Zato možemo staviti $v_p(x) = v_1$, $v_p(y) = v_2$. Tada je $x = mp^{v_1}$, $y = np^{v_2}$, gdje su m i n racionalni brojevi kojima ni brojnik ni nazivnik nisu djeljivi s p. Ako uvrstimo to u jednadžbu za E, imamo da je

$$n^2p^{2v_2} = m^3p^{3v_1} + bmp^{v_1} + c.$$

Ako je barem jedan od v_1, v_2 negativan, onda je i drugi. Zaista, ako je v_1 negativan, lako je provjeriti da je $v_p(m^3p^{3v_1} + bmp^{v_1} + c) = 3v_1$, a jasno je $v_p(n^2p^{2v_2}) = 2v_2$, pa su tada oba negativni i vrijedi $3v_1 = 2v_2$. Obratno, ako je v_2 negativan, a v_1 pozitivan, tada nazivnik desne strane nije djeljiv s p, ali lijeve jest. Dakle, v_1 i v_2 su oba negativni i vrijedi $3v_1 = 2v_2$ pa postoji $v \in \mathbb{N}$ takav da je $v_1 = -2v$, $v_2 = -3v$.
Promotrimo sada supstituciju $t = \frac{x}{y}$, $s = \frac{1}{y}$. Ona nije definirana ako je $y = 0$, no tada je $x^3 + bx + c = 0$ pa ako je $x \in \mathbb{Q}$, sigurno je i $x \in \mathbb{Z}$ jer imamo normirani polinom. Dakle, slučaj $y = 0$ je dokazan. Ako izuzmemo točke reda 2, lako se provjeri da je ovo bijektivno preslikavanje skupa točaka na krivulji u samog sebe. Možemo staviti da se točka

u beskonačnosti preslikava u $(0, 0)$. Uočimo da se pravci oblika $x = k$ preslikavaju u pravce $t = ks$ i da se pravci oblika $y = kx + l$ preslikavaju u pravce $1 = kt + ls$ (samo podijelimo prvu jednadžbu s y). Također uočimo da se točke koje su međusobno inverzne s obzirom na grupovnu operaciju na prvoj krivulji preslikavaju u točke centralnosimetrične s obzirom na ishodište na drugoj krivulji. Zato je grupovna operacija očuvana. Lako se dobije da je jednadžba nove krivulje:

$$s = t^3 + bts^2 + cs^3.$$

Iz $v_p(x) = -2v$, $v_p(y) = -3v$ lako dobijemo $v_p(t) = v$, $v_p(s) = 3v$. Neka je sada $C(p^v)$ skup svih točaka krivulje takav da je $v_p(s) \geq 3v, v_p(t) \geq v$. Neka su $P_1 = (t_1, s_1)$ i $P_2 = (t_2, s_2)$ dvije različite točke iz $C(p^v)$. One obje zadovoljavaju jednadžbu krivulje, pa kada ih oduzmemo, dobijemo da vrijedi:

$$s_2 - s_1 = (t_2^3 - t_1^3) + b(t_2 s_2^2 - t_1 s_1^2) + c(s_2^3 - s_1^3).$$

Cilj nam je dobiti izraz za nagib pravca kroz P_1 i P_2, pa ima smisla preurediti izraz na ovaj način:

$$s_2 - s_1 = (t_2^3 - t_1^3) + b((t_2 - t_1)s_2^2 + t_1(s_2^2 - s_1^2)) + c(s_2^3 - s_1^3).$$

Kad bi bilo $t_1 = t_2$, taj izraz bi nam dao:

$$(s_2 - s_1)(1 - bt_1(s_1 + s_2) - c(s_1^2 + s_1 s_2 + s_2^2)) = 0.$$

Pošto su P_1 i P_2 različite, a $t_1 = t_2$, mora biti $1 - bt_1(s_1 + s_2) - c(s_1^2 + s_1 s_2 + s_2^2) = 0$, no lako se vidi da je $v_p(1 - bt_1(s_1 + s_2) - c(s_1^2 + s_1 s_2 + s_2^2)) = 0$. Dakle, $t_1 \neq t_2$, pa možemo grupirati članove u preuređenom izrazu i sve podijeliti s $t_2 - t_1$. dobijamo:

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1 t_2 + t_1^2 + bs_2^2}{1 - bt_1(s_1 + s_2) - c(s_1^2 + s_1 s_2 + s_2^2)}.$$

Ako je $P_1 = P_2$, nagib pravca koji spaja P_1 i P_2 je upravo nagib tangente u P_1 kojeg lako dobijemo deriviranjem po t i uvrštavanjem:

$$\alpha = \frac{3t_1^2 + bs_1^2}{1 - 2bt_1 s_1 - 3cs_1^2}.$$

Uočimo da kada bismo u izraz za nagib u slučaju $P_1 \neq P_2$ uvrstili $t_1 = t_2$ i $s_1 = s_2$, dobili bismo upravo formulu iz drugog slučaja, pa možemo cijelo vrijeme koristiti prvu formulu. Već smo komentirali da nazivnik u formuli za α nikako nije 0, pa je jednadžba pravca kroz P_1 i P_2 dana s $s = \alpha t + \beta$. Zato vrijedi $s_1 = \alpha t_1 + \beta$. Trivijalno je provjeriti iz izraza za α da je $v_p(\alpha) \geq 2v$. Kako znamo da je $v_p(s_1) \geq 3v$ i $v_p(t_1) \geq v$, lagano dobijamo $v_p(\beta) \geq 3v$.

Neka je $P_3 = (t_3, s_3)$ treće sjecište pravca $s = \alpha t + \beta$ s krivuljom. Tada su t_1,t_2, t_3 rješenja jednadžbe

$$\alpha t + \beta = t^3 + bt(\alpha t + \beta)^2 + c(\alpha t + \beta)^3,$$

odnosno, nakon sređivanja, to su rješenja jednadžbe

$$(1 + b\alpha^2 + c\alpha^3)t^3 + (\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta)t^2 + (b\beta^2 + 3c\alpha\beta^2 - \alpha)t + c\beta^3 - \beta = 0.$$

Bitno je uočiti da ovo zaista jest jednadžba trećeg stupnja jer je $v_p(1 + b\alpha^2 + c\alpha^3)$ pa P_3 zaista postoji. Vieteove formule sada kažu da vrijedi:

$$t_1 + t_2 + t_3 = -\frac{\alpha\beta + 2b\alpha\beta + 3c\alpha^2 + \beta}{1 + b\alpha^2 + c\alpha^3}.$$

Jasno je da je $v_p(t_1 + t_2 + t_3) \geq 3v$. Zbog načina na koji je grupovna operacija na krivulji očuvana, imamo da je $P_1 + P_2 = (-t_3, -s_3)$, pa slijedi da za proizvoljne P_1, P_2 $inC(p^v)$ vrijedi da p^{3v} dijeli brojnik od

$$t(P_1) + t(P_2) - t(P_1 + P_2)$$

. Ono što još možemo uočiti iz Vieteovih formula od maloprije je da možemo zaključiti da je $v_p(t_3) \geq v$, pa kada to ubacimo u jednadžbu pravca $s = \alpha t + \beta$, dobijamo da je $v_p(s_3) \geq 3v$ pa je $P_1 + P_2 \in C(p^v)$ tj. $C(p^v)$ je grupa.
Vratimo se sada na tvrdnju teorema. Neka je $P = (x, y)$ racionalna točka reda $m \geq 2$. Neka $p \nmid m$. Pokazali smo da ako ona nije cjelobrojna, tada postoji prost broj p i $v \in \mathbb{N}$ takav da je $v_p(x) = -2v$ i $v_p(y) = -3v$. Tada je slika točke P pri promatranoj supstituciji u $C(p^v)$, ali nije u $C(p^{v+1})$. Primijenimo li ranije dokazanu tvrdnju da je za $P_1, P_2 \in C(p^v)$

$$t(P_1) + t(P_2) \equiv t(P_1 + P_2) \pmod{p^{3v}},$$

dobijamo da je:

$$0 \equiv t(mP) \equiv mt(P) \pmod{p^{3v}}.$$

Kako $p \nmid m$, imamo da je $t(P) \equiv 0 \pmod{p^{3v}}$, no iz $v_p(x) = -2v$ i $v_p(y) = -3v$ slijedi $v_p(t(P)) = v$, kontradikcija.
Neka sada $p|m$ pa je $m = pn$. Promotrimo točku $P' = nP$. Jasno je da je ona reda p. Uočimo da je svakako slika točke P u $C(p)$, pa je tamo i slika točke P'. Sada slično kao ranije odaberemo $v \in \mathbb{N}$ takav da je $v_p(x(P')) = -2v$ i $v_p(y(P')) = -3v$ pa je slika točke P' u $C(p^v)$, ali ne u $C(p^{v+1})$. Sada je kao i ranije:

$$0 \equiv t(pP') \equiv pt(P') \pmod{p^{3v}}.$$

To znači da je $v_p(t(P')) \geq 3v - 1$. No, imamo da je $v_p(t(P')) = v$ i jasno je da je $3v - 1 > v$ za $v \in \mathbb{N}$. Ovo je kontradikcija. Zaključujemo da P ima cjelobrojne koordinate. □

Sada je lako zaključiti da vrijedi Nagell-Lutzov teorem:

Teorem 3.1.3 (Nagell-Lutz)**.** *Neka je E eliptička krivulja dana jednadžbom $y^2 = x^3+bx+c$ gdje su $b, c \in \mathbb{Z}$. Neka je $D = -4b^3 - 27c^2$ diskriminanta pripadnog polinoma i $P = (x, y)$ racionalna točka na E konačnog reda. Tada P ima cjelobrojne koordinate i vrijedi $y = 0$ ili $y^2|D$.*

Dokaz. Ako je P konačnog reda, onda je i $2P$ konačnog reda, pa obje imaju cjelobrojne koordinate. Sada iz leme 2.4.1 slijedi $y = 0$ ili $y^2|D$. □

3.2 Mordell-Weilov i Mazurov teorem

Svakako je važno spomenuti Mordell-Weilov i Mazurov teorem. Ta dva teorema se bave pitanjem grupovne strukture racionalnih točaka na $E/\mathbb{Q}$, kao i pitanjem mogućih torzijskih grupa. Dokazi ova dva teorema su nešto složeniji, pogotovo Mazurovog teorema, pa ih ne uključujemo u ovaj rad. Već iz Nagell-Lutzovog teorema je jasno da je $E(\mathbb{Q})_{tors}$ konačna. Ipak, vrijedi i mnogo više od toga i to nam govori Mordell-Weilov teorem.

Teorem 3.2.1 (Mordell-Weil)**.** *Neka je $K \subseteq \mathbb{C}$ konačnodimenzionalno proširenje od $\mathbb{Q}$ i E/K eliptička krivulja. Tada je $E(K)$ konačno generirana.*

Dokaz ze može naći u ([5], VIII). Iz Mordell-Weilovog teorema i teorema o strukturi konačno generiranih Abelovih grupa možemo lagano zaključiti da vrijede ove dvije relacije:

$$E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r,$$

$$E(K)_{tors} \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}, \quad m_1|m_2|\ldots|m_k.$$

Broj r iz gornje relacije zovemo rang eliptičke krivulje. Već s tim informacijama možemo naslutiti kako izgleda $E(K)_{tors}$. Posebno, zaključci će vrijediti i za $K = \mathbb{Q}$.

Propozicija 3.2.2. *Neka je $K \subseteq \mathbb{C}$ konačnodimenzionalno proširenje od $\mathbb{Q}$ i E/K eliptička krivulja. Tada je $E(K)_{tors} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$ za neke $m, n \in \mathbb{N}$.*

Dokaz. Znamo da je $E(K)_{tors} \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}, \quad m_1|m_2|\ldots|m_k$ i možemo pretpostaviti $m_1 > 1$. Sjetimo se da smo dok smo promatrali kompleksne točke na krivulji pokazali da je $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Kad bi bilo $k \geq 3$ bilo bi $E[m_1] \geq \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_1\mathbb{Z}$ pa slijedi tvrdnja propozicije. □

Ipak, vrijedi mnogo jača tvrdnja. Mazur je 1978. pokazao da je lista kandidata za $E(\mathbb{Q})_{tors}$ mnogo kraća.

Teorem 3.2.3 (Mazur)**.** *Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada je $E(\mathbb{Q})_{tors}$ izomorfna jednoj od ovih grupa:*

$$\mathbb{Z}/n\mathbb{Z}, \quad n \in \{1,2,3,4,5,6,7,8,9,10,12\},$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad n \in \{1,2,3,4\}.$$

3.3 Određivanje torzijske grupe specifične eliptičke krivulje

Jasno je da nam Nagell-Lutzov teorem daje jednostavan način određivanja torzijske grupe specifične eliptičke krivulje. Ipak, ako je D prevelik, taj pristup možda nije dovoljno brz. Postoje mnoge napredne metode za to, ovdje ćemo prikazati jednu jednostavnu koja će koristiti eliptičke krivulje nad konačnim poljima. Sjetimo se da smo za transformaciju krivulje u kratku Weierstrassovu formu morali prepostaviti da je karakteristika promatranog polja različita od 2 i 3. Do sada je to uvijek bila istina. Promatrat ćemo polja $\mathbb{F}_p$ za $p \geq 5$ prost. Neka je eliptička krivulja E zadana jednadžbom

$$y^2 = x^3 + bx + c,$$

pri čemu su b i c cijeli. Ako je $P = (x, y)$ točka konačnog reda na njoj, onda su x i y cijeli i vrijedi

$$\widetilde{y}^2 = \widetilde{x}^3 + \widetilde{b}\widetilde{x} + \widetilde{c},$$

gdje $\widetilde{x}$ označava ostatak koji x daje pri dijeljenju s p. Ima smisla promatrati krivulju E' definiranu nad $\mathbb{F}_p$ danu jednadžbom

$$y^2 = x^3 + \widetilde{b}x + \widetilde{c}.$$

Ostaje pitanje regularnosti tj. definira li ta jednadžba zaista eliptičku krivulju nad $\mathbb{F}_p$. Dovoljan uvjet za to je da diskriminanta polinoma $x^3 + \widetilde{b}x + \widetilde{c}$ nije 0 u polju $\mathbb{F}_p$ tj. da diskriminanta polinoma $x^3 + bx + c$ nije djeljiva s p. Tada ako na $E'/\mathbb{F}_p$ promatramo skup $E'(\mathbb{F}_p)$, dobijamo grupovnu strukturu s istim formulama za zbrajanje točaka koje smo naveli na samom početku.
Promotrimo preslikavanje $\rho_p : E(\mathbb{Q})_{tors} \to E'(\mathbb{F}_p)$ zadano s:

$$\rho_p(P) = \begin{cases} (\widetilde{x}, \widetilde{y}), & P = (x, y) \\ \widetilde{O}, & P = O. \end{cases}$$

Propozicija 3.3.1. *Neka su $E/\mathbb{Q}$ i $E'/\mathbb{F}_p$ i $\rho_p : E(\mathbb{Q})_{tors} \to E'(\mathbb{F}_p)$ dani kao ranije, uz $p \geq 5$ i $p \nmid D$. Tada je ρ_p homomorfizam.*

Dokaz. Trivijalno je vidjeti da vrijedi

$$\widetilde{-P} = (\widetilde{x}, -\widetilde{y}) = -\widetilde{(P)}$$

pa se inverzne točke šalju u inverzne.
Neka je $P_1 + P_2 + P_3 = O$. Ako pokažemo da je tada $\widetilde{P_1} + \widetilde{P_2} + \widetilde{P_3} = \widetilde{O}$, bit ćemo gotovi jer smo provjerili da se inverzi šalju u inverze (samo prebacimo P_3 na drugu stranu). Ako je neka od P_1, P_2, P_3 jednaka O, tvrdnja slijedi iz dokazane tvrdnje za inverzne točke. Inače, možemo tim točkama pridijeliti koordinate:

$$P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_3 = (x_3, y_3).$$

Kako je $P_1 + P_2 = -P_3$, zbog pravila zbrajanja točaka na E, one su kolinearne i leže na pravcu $y = kx + l$. Ako to kombiniramo s formulom zbrajanja točaka P_1 i P_2, dobijamo da vrijedi:

$$x_3 = k^2 - x_1 - x_2, \quad y_3 = kx_3 + l.$$

Sjetimo se da P_1, P_2, P_3 imaju cjelobrojne koordinate pa su $k, l \in \mathbb{Q}$. Iz gornjih jednakosti je jasno da je $k^2 \in \mathbb{Z}$, pa je $k \in \mathbb{Z}$ pa je trivijalno i $l \in \mathbb{Z}$. Sada imamo da vrijedi

$$x^3 + bx + c - (kx + l)^2 = (x - x_1)(x - x_2)(x - x_3)$$

jer P_1, P_2, P_3 leže i na E i na $y = kx + l$ pa su upravo to nultočke polinoma na lijevoj strani. Sada, kako su svi brojevi koji nam se pojavljuju cijeli, možemo napraviti redukciju modulo p i dobiti:

$$x^3 + \widetilde{b}x + \widetilde{c} - (\widetilde{k}x + \widetilde{l})^2 = (x - \widetilde{x_1})(x - \widetilde{x_2})(x - \widetilde{x_3}), \quad \widetilde{y_i} = \widetilde{k}\widetilde{x_i} + \widetilde{l}, \quad i = 1, 2, 3.$$

Dakle, pravac $y = \widetilde{k}x + \widetilde{l}$ siječe E' upravo u $\widetilde{P_1}, \widetilde{P_2}, \widetilde{P_3}$, pa zbog pravila zbrajanja točaka na E' (iste formule kao i za E) slijedi $\widetilde{P_1} + \widetilde{P_2} + \widetilde{P_3} = \widetilde{O}$. Dakle, ρ_p je homomorfizam. □

Propozicija 3.3.2. *Uz oznake kao do sada i uz $p \nmid D$, $\rho_p : E(\mathbb{Q})_{tors} \to E'(\mathbb{F}_p)$ je injekcija.*

Dokaz. Neka je $P \in E(\mathbb{Q})_{tors}$ i $P \neq O$. Tada je $P = (x, y)$ za neke cijele x, y. Zato je $\widetilde{P} = (\widetilde{x}, \widetilde{y}) \neq O$. Zato je $\mathrm{Ker}(\rho_p) = O$ pa je ρ_p injekcija. □

Sada direktno iz ovoga dobijamo novu tvrdnju.

Propozicija 3.3.3. *Neka je $E/\mathbb{Q}$ eliptička krivulja dana jednadžbom $y^2 = x^3 + bx + c$ gdje su $b, c \in \mathbb{Z}$. Neka je $p \geq 5$ prost takav da $p \nmid D$. Neka je $E'/\mathbb{F}_p$ eliptička krivulja dana jednadžbom $y^2 = x^3 + \widetilde{b}x + \widetilde{c}$. Tada je $E(\mathbb{Q})_{tors}$ izomorfna podgrupi grupe $E'(\mathbb{F}_p)$ i posebno vrijedi $|E(\mathbb{Q})_{tors}| \mid |E'(\mathbb{F}_p)|$.*

Imajmo na umu da relacija $|E(\mathbb{Q})_{tors}| \mid |E'(\mathbb{F}_p)|$ ima smisla jer znamo da je $E(\mathbb{Q})_{tors}$ konačna. Da bi ova propozicija bila primjenjiva, treba nam način određivanja $|E'(\mathbb{F}_p)|$. Lako je naći formulu za red te grupe preko Legendreovih simbola.

Propozicija 3.3.4. *Neka je p prost i $E/\mathbb{F}_p$ eliptička krivulja dana jednadžbom $y^2 = x^3 + bx + c$. Tada je:*

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + bx + c}{p} \right).$$

Dokaz. Svaki $x \in \mathbb{F}_p$ daje $\left(\frac{x^3+bx+c}{p}\right)+1$ točaka u $E(\mathbb{F}_p)$. Zbrajanjem tih brojeva i dodavanjem točke O dobijamo traženu formulu. □

Primjer 3.3.5. *Odredimo $E(\mathbb{Q})_{tors}$ za $E/\mathbb{Q}$ danu s:*

$$y^2 = x^3 + 18x + 72.$$

Rješenje. Imamo da je pripadna diskriminanta $D = 4 \cdot 18^3 + 27 \cdot 72^2 = 163296$ pa bi nam trebalo malo više vremena da torzijsku grupu odredimo pomoću Nagell-Lutzova teorema. Ako reduciramo krivulju modulo 5 i 11, što možemo, jer to nisu djelitelji diskriminante, koristeći gornju formulu dobijemo $|E(\mathbb{F}_5)| = 5$ i $|E(\mathbb{F}_{11})| = 8$. Sada slijedi

$$|E(\mathbb{Q})_{tors}| \mid M(5, 8)$$

pa je $E(\mathbb{Q})_{tors}$ trivijalna. □

Poglavlje 4

Torzija nad poljima algebarskih brojeva

Promatrali smo situaciju za kompleksne, realne i racionalne točke pa je svakako prirodno pitati se kako može izgledati torzijska grupa racionalne eliptičke krivulje nad nekim poljem algebarskih brojeva. Može nas zanimati odgovor na to pitanje za neko specifično polje ili možda za sva polja određenog stupnja proširenja nad $\mathbb{Q}$. Kad već razmišljamo o algebarskim brojevima, prirodno je razmisliti i o transcendentnim i možda se pitati kako može izgledati $E(\mathbb{Q}(\pi))_{tors}$. Tim i sličnim pitanjima bavimo se u ovom poglavlju.

4.1 Eliptičke krivulje i Galoisova proširenja

U ovoj kratkoj sekciji, za $K \subseteq \mathbb{C}$, gdje je K konačnodimenzionalno proširenje od $\mathbb{Q}$, definirat ćemo djelovanje Galoisove grupe $Gal(K/\mathbb{Q})$ na točke iz $E(K)$ i dokazati neka njegova svojstva koja će nam biti vrlo bitna uskoro. Također se možemo pitati kakve koordinate mogu imati točke konačnog reda na E. Ovdje ćemo pokazati da koordinate moraju biti algebarski brojevi.

Propozicija 4.1.1. *Neka je $E/\mathbb{Q}$ eliptička krivulja i K Galoisovo proširenje od $\mathbb{Q}$. Za svaku $P \in E(K)$ i $\sigma \in Gal(K/\mathbb{Q})$ definirajmo:*

$$P^\sigma = \sigma(P) = \begin{cases} (\sigma(x), \sigma(y)), & P = (x, y) \\ O, & P = O. \end{cases}$$

Tada je gornjom definicijom dano djelovanje $Gal(K/\mathbb{Q})$ na $E(K)$ i dodatno vrijedi:

$$\sigma(P + Q) = \sigma(P) + \sigma(Q), \quad \sigma(-P) = -\sigma(P),$$

za sve $P, Q \in E(K)$ i $\sigma \in Gal(K/\mathbb{Q})$.

Dokaz. Da je $P^\sigma \in E(K)$ se vidi trivijalno djelovanjem sa σ na jednakost $y^2 = x^3 + bx + c$ i iz činjenise da σ fiksira $\mathbb{Q}$. Također je jasno da je $(\sigma\tau)(P) = \sigma(\tau(P))$ i da identiteta fiksira svaku točku P pa zaista imamo djelovanje.
$\sigma(P + Q) = \sigma(P) + \sigma(Q)$ i $\sigma(-P) = -\sigma(P)$ se može provjeriti lagano pomoću formula za zbrajanje točaka. □

Propozicija 4.1.2. *Djelovanje definirano u prethodnoj propoziciji čuva red točaka iz $E(K)$.*

Dokaz. Neka je $P \in E(K)$ reda n. Tada je za $\sigma \in Gal(K/\mathbb{Q})$:

$$O = \sigma(O) = \sigma(nP) = n\sigma(P).$$

Zato je red od $\sigma(P)$ djelitelj od n. Pretpostavimo da je taj red m. Tada je $m\sigma(P) = \sigma(mP) = O$, no zbog definicije djelovanja to znači da je $mP = O$ pa je $m = n$. □

Propozicija 4.1.3. *Neka je $E/\mathbb{Q}$ eliptička krivulja i $P \in E[n]$. Tada su koordinate od P algebarski brojevi nad $\mathbb{Q}$ i proširenje $\mathbb{Q}(E[n])/\mathbb{Q}$ je Galoisovo.*

Dokaz. Promatrajmo $\mathbb{Q}$-ulaganja od $\mathbb{Q}(E[n])$ u $\mathbb{C}$. Pošto fiksiraju $\mathbb{Q}$, analogno kao u gornjim propoziciji vrijedi $\sigma(P + Q) = \sigma(P) + \sigma(Q)$ pa svako takvo ulaganje čuva red točke (iako još ne znamo da je proširenje Galoisovo). Dakle, ako je $\sigma : \mathbb{Q}(E[n]) \to \mathbb{C}$ neko $\mathbb{Q}$-ulaganje i $P \in E[n]$, tada je i $P^\sigma \in E[n]$. Ovo znači da svaki σ permutira točke iz $E[n]$ pa ih ima najviše konačno mnogo, što znači da je dano proširenje konačnodimenzionalno, pa i algebarsko. Zato su koordinate točaka iz $E[n]$ algebarski brojevi nad $\mathbb{Q}$. Dodatno, kako svaki σ permutira točke, to svaki σ šalje generatore proširenja u generatore pa je $\sigma(\mathbb{Q}(E[n]) \subseteq \mathbb{Q}(E[n])$, što je dovoljno da zaključimo da je proširenje Galoisovo. □

4.2 Weilovo sparivanje

Slično kao i ranije, neka je $K \subseteq \mathbb{C}$ konačnodimenzionalno proširenje od $\mathbb{Q}$ i E/K eliptička krivulja. Vidjeli smo ranije da smo promatranjem grupa $E[m]$ došli do nekih manjih zaključaka o mogućem izgledu grupe $E(K)_{tors}$. Označimo s $\boldsymbol{\mu}_m$ grupu$m$-tih korijena iz jedinice. Ispostavlja se da je korištenjem alata algebarske geometrije moguće konstruirati preslikavanje $e_m : E[m] \times E[m] \to \mu_m$ koje zovemo Weilovim e_m-sparivanjem. Pokazuje se da tako konstruirano preslikavanje zadovoljava neka važna svojstva.

Propozicija 4.2.1. *Weilovo e_m-sparivanje na E/K zadovoljava sljedeća svojstva:*

(a)

$$e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T), \quad (\forall\ S_1, S_2, T \in E[m])$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2), \quad (\forall\ S, T_1, T_2 \in E[m])$$

(b)

$$e_m(T,T) = 1, \quad (\forall\ T \in E[m])$$

(c)

$$(\forall S \in E[m])(e_m(S,T) = 1) \Rightarrow T = O$$

(d)

$$e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma), \quad (\forall\ \sigma \in Gal(\overline{K}/K))$$

(e)

$$e_{mk}(S,T) = e_m(kS,T), \quad (\forall\ S \in E[mk], T \in E[m]).$$

Napomena 4.2.2. *$\overline{K}$ označava algebarski zatvarač od K. Vrijedi da je proširenje $\overline{K}/K$ Galoisovo ako i samo ako je K savršeno polje. U našem slučaju je $char(K) = 0$ pa je to zadovoljeno i oznaka $Gal(\overline{K}/K)$ ima smisla.*

Propozicija 4.2.3. *Uz oznake kao i do sada, e_m je surjektivno. Dodatno, ako je $E[m] \subseteq E(K)$, onda je i $\boldsymbol{\mu}_m \subseteq K$.*

Dokaz. Svojstva $(a), (b)$ impliciraju da vrijedi

$$1 = e_m(S+T, S+T) = e_m(S,S)e_m(T,T)e_m(S,T)e_m(T,S) = e_m(S,T)e_m(T,S),$$

odnosno vrijedi $e_m(S,T) = e_m(T,S)^{-1}$. Uzmimo bazu za $E[m]$ S_1, T_1 i neka je $e_m(S_1,T_1) = \mu$. Tada je $e_m([a]S_1 + [b]T_1, [c]S_1 + [d]T_1) = \mu^{ad-bc}$. Sada lako slijedi da je slika preslikavanja e_m podgrupa od $\boldsymbol{\mu}_m$. Neka je ta slika $\boldsymbol{\mu}_d$, gdje $d|m$. Tada imamo za proizvoljne $S, T \in E[m]$:

$$1 = e_m(S,T)^d = e_m([d]S, T).$$

T je proizvoljan pa zbog svojstva (c) slijedi da je $[d]S = O$ za svaki S. Iz toga slijedi $d = m$ pa je surjektivnost dokazana.
Ako je $E[m] \subseteq E(K)$, onda imamo:

$$e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma) = e_m(S,T).$$

Kako gornje vrijedi za sve $\sigma \in Gal(\overline{K}/K)$, slijedi $e_m(S,T) \in K$ tj. $\boldsymbol{\mu}_m \subseteq K$. □

Ova tvrdnja može pomoći u eliminaciji mnogih kandidata za $E(K)_{tors}$. Npr. već s ovim možemo značajno suziti izbor kandidata za $E(\mathbb{Q})_{tors}$ kad je E definirana nad $\mathbb{Q}$, iako se ne možemo približiti Mazurovom teoremu.

Korolar 4.2.4. *Neka je $E/\mathbb{Q}$ eliptička krivulja definirana nad $\mathbb{Q}$. Tada je $E(\mathbb{Q})_{tors}$ izomorfna jednoj od ovih grupa:*

$$\mathbb{Z}/n\mathbb{Z}, \quad n \in \mathbb{N},$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad n \in \mathbb{N}.$$

Dokaz. Ranije smo pokazali da je

$$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}, \quad m, n \in \mathbb{N}.$$

Slijedi da je $E[m] \subseteq E(\mathbb{Q})$ pa je $\boldsymbol{\mu}_m \subseteq \mathbb{Q}$. Kako su jedini racionalni korijeni jedinice 1 i -1, zaključujemo $m \in \{1, 2\}$. □

Cilj nam je pokazati još jednu tvrdnju koja može biti od velike koristi u eliminaciji potencijalnih kandidata za $E(K)_{tors}$. Prije nego što dođemo do nje, morat ćemo definirati Galoisovu reprezentaciju.

Definicija 4.2.5. *Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je $\{P, Q\}$ baza za $E[n]$, gdje je $n \in \mathbb{N}$. Za svaki $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ stavimo:*

$$P^\sigma = \alpha_\sigma P + \beta_\sigma Q, \quad Q^\sigma = \gamma_\sigma P + \delta_\sigma Q.$$

Tada preslikavanje $\rho_{E,n} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z})$ dano s:

$$\rho(\sigma) = \begin{pmatrix} \alpha_\sigma & \gamma_\sigma \\ \beta_\sigma & \delta_\sigma \end{pmatrix}$$

zovemo modulo n Galoisova reprezentacija pridružena E.

Direktnom provjerom se lako pokazuje da je Galoisova reprezentacija homomorfizam grupa. Galoisova reprezentacija je u direktnoj vezi s Weilovim sparivanjem, što se vidi kroz ovu propoziciju:

Propozicija 4.2.6. *Neka je $E/\mathbb{Q}$ eliptička krivulja, $n \in N$ i ζ n-ti korijen iz jedinice. Tada za svaki $\sigma \in Gal(Q(E[n]/\mathbb{Q})$ vrijedi*

$$\sigma(\zeta) = \zeta^{det\rho_{E,n}(\sigma)},$$

gdje je $\rho_{E,n}$ modulo n Galoisova reprezentacija pridružena E.

Dokaz. Neka je $\{P, Q\}$ baza za $E[n]$. Jasno je iz dokaza prethodne propozicije da je slika Weilovog sparivanja e_n generirana s $e_n(P, Q)$. Tada je $e_n(P, Q) = \zeta_n$ primitivni n-ti korijen iz jedinice zbog surjektivnosti Weilovog sparivanja. Sada za proizvoljni $\sigma \in Gal(\mathbb{Q}(E[n]/\mathbb{Q})$ imamo:

$$P^\sigma = aP + bQ, \quad Q^\sigma = cP + dQ.$$

Identično kao u prethodnoj propoziciji imamo

$$e_n(P^\sigma, Q^\sigma) = e_n([a]P + [b]Q, [c]P + [d]Q) = \zeta_n^{ad-bc} = \zeta_n^{det\rho_{E,n}(\sigma)}.$$

Zbog Galois-invarijantnosti Weilovog preslikavanja je:

$$e_n(P^\sigma, Q^\sigma) = e_n(P, Q)^\sigma = \sigma(\zeta_n),$$

što je i trebalo pokazati. □

Sada imamo dovoljno sredstava da dokažemo sljedeću propoziciju:

Propozicija 4.2.7. *Neka je $E/\mathbb{Q}$ eliptička krivulja, $n \in \mathbb{N}$ i $K \subseteq \mathbb{C}$ konačnodimenzionalno Galoisovo proširenje od $\mathbb{Q}$. Neka je $E(K)[n] \cong \mathbb{Z}/n\mathbb{Z}$ i $P \in E(K)$ točka reda n.*
Tada vrijedi:

$$[\mathbb{Q}(P) : \mathbb{Q}] \mid M(\phi(n), [K : \mathbb{Q}]),$$

gdje $M(\cdot, \cdot)$ označava najveću zajedničku mjeru, a ϕ je Eulerova funkcija.

Dokaz. Neka je P točka reda n s koordinatama iz K. Tada možemo uzeti $Q \in E[n]$ takvu da je $\{P, Q\}$ baza za $E[n]$. Promotrimo Galoisovu reprezentaciju modulo n pridruženu E:

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z}).$$

Neka je $\sigma \in Gal(K/\mathbb{Q})$. Tada je $P^\sigma = \alpha P + \beta Q$ za neke $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$ jer djelovanje sa σ na P čuva red točke. Jasno je da je $P^\sigma - \alpha P = \beta Q$ iz čega slijedi $\beta Q \in E(K)$. Kad bi bilo $\beta \neq 0$, grupa $E(K)[n]$ bi bila veća od $\mathbb{Z}/n\mathbb{Z}$. Dakle, $\beta = 0$, pa je $P^\sigma \in \langle P \rangle$ za sve $\sigma \in Gal(K/\mathbb{Q})$. Dodatno, zbog očuvanja reda, gornji α mora biti iz $(\mathbb{Z}/n\mathbb{Z})^\times$.
Kako se restrikcijskim preslikavanjem dobije da vrijedi $Gal(K/\mathbb{Q}) \cong Gal(\overline{\mathbb{Q}}/\mathbb{Q})/Gal(\overline{\mathbb{Q}}/K)$, imamo da je $P^\sigma \in \langle P \rangle$ za sve $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Zato je za svaki $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$:

$$\rho(\sigma) = \begin{pmatrix} \varphi(\sigma) & \tau(\sigma) \\ 0 & \psi(\sigma) \end{pmatrix},$$

pri čemu su $\varphi, \psi, \tau : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}/n\mathbb{Z}$, a φ, ψ su homomorfizmi sa slikom u $(\mathbb{Z}/n\mathbb{Z})^\times$. Znamo da je $P^\sigma = gP \Leftrightarrow \varphi(\sigma) = g$, za sve $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Zato imamo da je:

$$|\operatorname{Im}(\varphi)| = |\{P^\sigma : \sigma \in Gal(K/\mathbb{Q})\}| = |Orb(P)|.$$

Jasno je da je $\operatorname{Stab}(P) = Gal(K/\mathbb{Q}(P))$, pa je po teoremu o orbiti i stabilizatoru:

$$|\operatorname{Im}(\varphi)| = \frac{|Gal(K/\mathbb{Q})|}{|Gal(K/\mathbb{Q}(P))|} = [\mathbb{Q}(P) : \mathbb{Q}].$$

S druge strane, jasno je da je $\operatorname{Im}(\varphi) \leq (\mathbb{Z}/n\mathbb{Z})^\times$ pa vrijedi:

$$[\mathbb{Q}(P) : \mathbb{Q}] \mid \phi(n).$$

$[\mathbb{Q}(P) : \mathbb{Q}] \mid [K : \mathbb{Q}]$ je trivijalno pa je tvrdnja dokazana. □

4.3 Torzija nad jednim ciklotomskim poljem

Neki korisni rezultati

Nedavno su određene sve moguće strukture torzijske grupe racionalne eliptičke krivulje nad $\mathbb{Q}^{ab}$, gdje je $\mathbb{Q}^{ab} = \mathbb{Q}(\{\zeta_n : n \in \mathbb{N}\})$ maksimalno Abelovo proširenje od $\mathbb{Q}$ (ζ_n označava primitivni n-ti korijen iz jedinice). Također je poznato kako može izgledati torzijska grupa racionalne eliptičke krivulje nad proširenjima od $\mathbb{Q}$ malog stupnja. Već s tim rezultatima i nekim tvrdnjama dokazanim u ovom radu možemo pokušati dati odgovor na pitanje o strukturi torzijske grupe nad nekim specifičnim poljima. Iskažimo najprije spomenute teoreme.

Teorem 4.3.1. *Neka je $E/\mathbb{Q}$ racionalna eliptička krivulja i $K/\mathbb{Q}$ proširenje stupnja 2. Tada je $E(K)_{tors}$ izomorfno jednoj od sljedećih grupa:*

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 1, 2, \ldots, 9, 10, 12, 15, 16$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, \quad m = 1, 2, 3, 4, 5, 6$$
$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}, \quad m = 1, 2$$
$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Dodatno, svaka od danih grupa se zaista pojavi u beskonačno mnogo slučajeva, osim $\mathbb{Z}/15\mathbb{Z}$ koja se javlja u samo konačno mnogo slučajeva i to samo nad kvadratnim proširenjima $\mathbb{Q}(\sqrt{5})$ i $\mathbb{Q}(\sqrt{-15})$.

Dokaz. Dokaz se nalazi u ([4], teorem 2). □

Teorem 4.3.2. *Neka je $E/\mathbb{Q}$ racionalna eliptička krivulja i $K/\mathbb{Q}$ proširenje stupnja 2. Tada je $E(\mathbb{Q}^{ab})_{tors}$ izomorfno jednoj od sljedećih grupa:*

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 37, 43, 67, 163$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, \quad m = 1, 2, \ldots, 8, 9$$
$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}, \quad m = 1, 3$$
$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4m\mathbb{Z}, \quad m = 1, 2, 3, 4$$
$$\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$$
$$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$$
$$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

Dokaz. Dokaz je iznesen u [1]. □

Glavne tvrdnje koje se koriste u dokazu teorema 4.3.2. se tiču izogenija na eliptičkim krivuljama i te tvrdnje same za sebe mogu biti vrlo korisne pa ćemo ih navesti.

Definicija 4.3.3. *Neka su E_1 i E_2 eliptičke krivulje. Izogenija s E_1 na E_2 je morfizam $\psi : E_1 \to E_2$ koji zadovoljava $\psi(O_1) = O_2$, gdje su O_1 i O_2 pripadni neutralni elementi. Ako je ψ netrivijalan, kažemo da su E_1 i E_2 izogene eliptičke krivulje.*

Definicija 4.3.4. *Neka su E_1 i E_2 eliptičke krivulje i ψ izogenija između njih. Za ψ kažemo da je $\mathbb{Q}$-racionalna ciklična n-izogenija ako joj je jezgra ciklička grupa reda n i ako je definirana nad $\mathbb{Q}$ kao morfizam. Tada ćemo u nastavku skraćeno govoriti da E_1 ima n-izogeniju nad $\mathbb{Q}$.*

Vrijedi sljedeća tvrdnja:

Propozicija 4.3.5. *Neka je E eliptička krivulja i G bilo koja njena konačna podgrupa. Tada postoji eliptička krivulja E' i izogenija $\psi : E \to E'$ čija je jezgra G. Posebno, ako je E definirana nad nekim poljem K i G je stabilan pod djelovanjem $Gal(\overline{K}/K)$, može se uzeti da su i E' i ψ definirani nad K.*

Dodatni materijali o izogenijama, kao i dokaz ove tvrdnje, mogu se naći u ([5], III.4). Sada možemo dokazati ovu tvrdnju:

Propozicija 4.3.6. *Neka je $K \subseteq \mathbb{C}$ Galoisovo proširenje od $\mathbb{Q}$ i neka je $E/\mathbb{Q}$ eliptička krivulja za koju vrijedi $E(K)_{tors} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$. Tada E ima n-izogeniju nad $\mathbb{Q}$.*

Dokaz. Prema prethodnoj propoziciji, dovoljno je pronaći cikličku podgrupu točaka koja će biti stabilna pod djelovanjem $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Uzmimo točku $P \in E(K)$ reda mn i neka je $\{P, Q\}$ baza za $E[mn]$. Za $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ tada zbog očuvanja reda vrijedi:

$$P^\sigma = aP + bQ.$$

Kako je K Galoisovo proširenje, vrijedi $\sigma(K) = K$. Sada je slično kao u propoziciji 4.2.7:

$$P^\sigma - aP = bQ \in E(K).$$

Pomnožimo li to s m, na desnoj strani dobijemo O jer je nužno $bQ \in E[m]$ zbog strukture $E(K)_{tors}$. Dakle, za $P \in E(K)$ reda mn vrijedi $(mP)^\sigma = (ma)P = a(mP)$. Ovo znači da je grupa $\langle mP \rangle$ stabilna pri djelovanju $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, a jasno je da je reda n pa je tvrdnja dokazana. □

Također vrijedi i ovaj teorem koji se na očit način može kombinirati s upravo dokazanom tvrdnjom kako bi se eliminirali neki kandidati za torzijsku grupu:

Teorem 4.3.7. *Neka je $E/\mathbb{Q}$ eliptička krivulja i neka ona ima n-izogeniju nad $\mathbb{Q}$. Tada je $n \leq 19$ ili $n \in \{21, 25, 27, 37, 43, 67, 163\}$.*

Više o ovom teoremu se može naći u [2]. Korisnost propozicije 4.3.6 leži u činjenici da čak i kad se pojavi izogenija koja nije isključena gornjim teoremom, ona može značajno smanjiti skup eliptičkih krivulja koje potencijalno mogu dati određenu torzijsku grupu nad K.

Torzija nad $\mathbb{Q}(\zeta_{11})$

Možemo se npr. pitati čemu može biti izomorfno $E(\mathbb{Q}(\zeta_{11}))_{tors}$ za eliptičku krivulju $E/\mathbb{Q}$. Imajmo na umu da je to proširenje Galoisovo i stupnja 10. Vidjet ćemo da ćemo kombinacijom dosadašnjih rezultata brzo eliminirati većinu kandidata. Jasno je da su kandidati za torzijsku grupu u ovom slučaju sve podgrupe grupa iz upravo iskazanog teorema. Korak po korak ćemo pokušati eliminirati što više kandidata.

Propozicija 4.3.8. *Neka je $E/\mathbb{Q}$ eilptička krivulja. Tada je $E(\mathbb{Q}(\zeta_{11}))_{tors}$ izomorfna jednoj od sljedećih grupa (ne pojavljuju se nužno sve):*

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 1, 2, 3, \ldots 18, 19, 21, 25, 27, 37, 43, 67, 163$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, \quad m = 1, 2, \ldots, 8, 9.$$

Dokaz. Pretpostavimo da je $E(\mathbb{Q}(\zeta_{11}))_{tors} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$. Tada je $E[n] \subseteq E(\mathbb{Q}(\zeta_{11}))$ pa zbog egzistencije Weilovog sparivanja slijedi $\zeta_n \in \mathbb{Q}(\zeta_{11})$. No, jedini korijeni iz jedinice u $\mathbb{Q}(\zeta_{11})$ su 22. korijeni iz jedinice, pa je $n \in \{1, 2, 11, 22\}$. Promatranjem popisa iz teorema 4.3.2. i uzimajući u obzir dobivene mogučnosti za n, jasno je da su jedine preostale grupe kandidati upravo one iz iskaza. □

Weilovo sparivanje značajno je suzilo izbor. Pokušajmo upotrijebiti neku drugu ranije dokazanu tvrdnju kako bismo dodatno smanjili popis kandidata.

Propozicija 4.3.9. *Neka je $E/\mathbb{Q}$ eilptička krivulja. Tada je $E(\mathbb{Q}(\zeta_{11}))_{tors}$ nije izomorfna nijednoj od sljedećih grupa:*

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 13, 14, 15, 17, 18, 19, 21, 27, 37, 43, 67, 163.$$

Dokaz. Pretpostavimo suprotno tj. $E(\mathbb{Q}(\zeta_{11}))_{tors} \cong \mathbb{Z}/m\mathbb{Z}$ za neki m iz iskaza. Tada je $E(\mathbb{Q}(\zeta_{11}))[m] \cong \mathbb{Z}/m\mathbb{Z}$ pa možemo iskoristiti propoziciju 4.2.7. Ako je P točka reda m, tada imamo (jer je stupanj proširenja 10):

$$[\mathbb{Q}(P) : \mathbb{Q}] \mid M(\phi(m), 10),$$

gdje ϕ označava Eulerovu funkciju. Lako je provjeriti uvrštavanjem da za sve m iz iskaza ovo daje relaciju:

$$[\mathbb{Q}(P) : \mathbb{Q}] \mid 2.$$

Dakle, pripadna torzijska grupa se postiže već nad kvadratnim proširenjem, što je nemoguće prema teoremu 4.3.1., osim za $m = 15$. No, u tom istom teoremu smo vidjeli da bi tada moralo biti $\mathbb{Q}(P) = \mathbb{Q}(\sqrt{5})$ ili $\mathbb{Q}(P) = \mathbb{Q}(\sqrt{-15})$. Kako je jedino kvadratno međuproširenje od $\mathbb{Q}(\zeta_{11})$ polje $\mathbb{Q}(\sqrt{-11})$, slučaj $m = 15$ je također nemoguć. □

Napomena 4.3.10. *Neka je p prost broj i $\mathbb{Q}(\zeta_p)$ p-to ciklotomsko polje. $\mathbb{Q}(\zeta_p)$ ima jedinstveno međuproširenje svakog stupnja koji dijeli $p-1$ jer je $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Dodatno, jedinstveno kvadratno proširenje je upravo $\mathbb{Q}(\sqrt{\pm p})$, gdje $'+'$ znak stoji ako i samo ako je p oblika $4k+1$. Detaljnije o ovome se može naći u ([3], poglavlje 2).*

Propozicija 4.3.11. *Neka je $E/\mathbb{Q}$ eilptička krivulja. Tada je $E(\mathbb{Q}(\zeta_{11}))_{tors}$ nije izomorfna nijednoj od grupa:*

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}.$$

Dokaz. Dokazat ćemo tvrdnju za $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$, ostale se dokazuju potpuno analogno. Donekle ćemo imitirati dokaz propozicije 4.2.7. Pretpostavimo suprotno. Neka je $P \in E(\mathbb{Q}(\zeta_{11}))$ reda 16 i neka je $\{P, Q\}$ baza za $E[16]$. Uzmimo $\sigma \in Gal(\mathbb{Q}(\zeta_{11})/\mathbb{Q})$. Zbog čuvanja reda imamo $P^\sigma = aP + bQ$, odnosno vrijedi $P^\sigma - aP = bQ \in E(\mathbb{Q}(\zeta_{11}))$. Iz toga slijedi da je $b \in \{0, 8\}$. Množenjem svega s 2 (u smislu zbrajanja točaka), dobijamo da je $(2P)^\sigma = a(2P)$.
Stavimo $R = 2P, S = 2Q$. Tada je $\{R, S\}$ baza za $E[8]$ i vrijedi $R^\sigma = aR$. Sada možemo nastaviti kao i u dokazu propozicije 4.2.7. i zaključiti:

$$[\mathbb{Q}(2P) : \mathbb{Q}] \mid \phi(8) = 4.$$

To znači da je $\mathbb{Q}(2P)$ trivijalno ili kvadratno proširenje od $\mathbb{Q}$, jer mora dijeliti i 10. Dokažimo da iz toga slijedi da je i $\mathbb{Q}(P)$ trivijalno ili kvadratno proširenje od $\mathbb{Q}$.
Sjetimo se duplikacijske formule i stavimo $x(P) = x$ i neka je krivulja dana jednadžbom $y^2 = x^3 + bx + c$. Kako je $2P \neq O$, nemamo nulu u nazivniku duplikacijske formule pa možemo pomnožiti s njim i dobiti relaciju:

$$x^4 - 4x(2P)x^3 - 2bx^2 - (8c + 4bx(2P))x + b^2 - 4cx(2P) = 0.$$

jasno je da je $\mathbb{Q}(x(2P))$ potpolje od $\mathbb{Q}(x(P))$. Ovo je polinom četvrtog stupnja s koeficijentima iz $\mathbb{Q}(x(2P))$ i jedna njegova nultočka je $x(P)$, pa je $[\mathbb{Q}(x(P)) : \mathbb{Q}(x(2P))] \leq 4$. Jasno je prema ranije pokazanome da je $[\mathbb{Q}(x(2P)) : \mathbb{Q}] \leq 2$, pa je $[\mathbb{Q}(x(P)) : \mathbb{Q}] \leq 8$, ali je vidljivo da ne može biti djeljivo s 5, pa je $\mathbb{Q}(x(P))$ trivijalno ili kvadratno proširenje od $\mathbb{Q}$. Znamo i da vrijedi:

$$y(P)^2 - x(P)^3 - bx(P) - c = 0,$$

pa je $[\mathbb{Q}(P) : \mathbb{Q}(x(P))] \leq 2$. Zato je $[\mathbb{Q}(P) : \mathbb{Q}] \leq 4$, ali kako mora dijeliti 10, slijedi da je $\mathbb{Q}(P)$ proširenje stupnja najviše 2.
Uočimo da još uvijek nismo gotovi jer P generira torzijsku podgrupu $\mathbb{Z}/16\mathbb{Z}$ koja se može

pojaviti nad kvadratnim proširenjima. Ipak, $E(\mathbb{Q}(\zeta_{11}))$ ima još jednu točku S reda 2 koja nije u $\langle P \rangle$. Njena y-kooradinata je 0, a x-koordinata je nultočka polinoma trećeg stupnja s racionalnim koeficijentima, pa je $[\mathbb{Q}(S) : \mathbb{Q}] \leq 3$. Jasno je da ne može vrijediti jednakost jer $3 \nmid 10$ pa je $[\mathbb{Q}(S) : \mathbb{Q}] \leq 2$. Dakle, i P i S su ili racionalne ili imaju koordinate iz $\mathbb{Q}(\sqrt{-11})$ (jedinstveno kvadratno međuproširenje od $\mathbb{Q}(\zeta_{11})$). Ovo je kontradikcija s teoremom 4.3.1. □

Propozicija 4.3.12. *Za svaku od sljedećih grupa, postoji eliptička krivulja $E/\mathbb{Q}$ takva da joj je $E(\mathbb{Q}(\zeta_{11}))_{tors}$ izomorfna:*

$$\mathbb{Z}/11\mathbb{Z},$$
$$\mathbb{Z}/25\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}.$$

Dokaz. Krivulja E s Cremona oznakom $11a3$ zadovoljava $E(\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1}))_{tors} \cong \mathbb{Z}/25\mathbb{Z}$. Ta torzija ne može narasti nad poljem $\mathbb{Q}(\zeta_{11})$ jer onda torzijska grupa ne bi bila podgrupa neke od grupa iz teorema 4.3.2.
Krivulja E s Cremona oznakom $121b2$ zadovoljava $E(\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1}))_{tors} \cong \mathbb{Z}/11\mathbb{Z}$. Tada je i $E(\mathbb{Q}(\zeta_{11}))_{tors} \cong \mathbb{Z}/11\mathbb{Z}$ iz istog razloga kao ranije.
Krivulja E s Cremona oznakom $10230bg2$ zadovoljava $E(\mathbb{Q}(\sqrt{-11}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$. Opet je i $E(\mathbb{Q}(\zeta_{11}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$. □

Sve ove propozicije se sada mogu objediniti u jednu:

Propozicija 4.3.13. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada je $E(\mathbb{Q}(\zeta_{11}))_{tors}$ izomorfna jednoj od grupa iz Mazurovog teorema ili jednoj od sljedećih grupa:*

$$\mathbb{Z}/11\mathbb{Z},$$
$$\mathbb{Z}/25\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z},$$
$$\mathbb{Z}/16\mathbb{Z},$$

gdje za zadnje dvije grupe slutimo da se ne mogu pojaviti, ali ih nismo uspjeli eliminirati.

Bibliografija

[1] Michael Chou, *Torsion of rational elliptic curves over the maximal abelian extension of* $\mathbb{Q}$, (2017), https://arxiv.org/abs/1711.00412v2.

[2] A. Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Mathematische Annalen **357** (2013), br. 1, 279–305.

[3] Daniel A. Marcus, *Number fields*, Springer-Verlag, New York, 1977.

[4] Filip Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$, (2012), https://arxiv.org/abs/1211.2188v4.

[5] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

Sažetak

U ovom radu promatrali smo torzijske grupe elitpičkih krivulja. Nakon uvodnih definicija i malih rezultata o točkama malog reda, promatrali smo situaciju najprije za polje kompleksnih brojeva. Prateći ranije dokazane rezultate, odredili smo kako može izgledati grupa kompleksnih točaka i zaključili smo da je za svaku racionalnu eliptičku krivulju $E(\mathbb{C})_{tors}$ uvijek ista, točnije, izomorfna je torusu u aditivnom smislu. Koristeći taj zaključak, promatrali smo kako može izgledati grupa realnih točaka racionalne eliptičke krivulje i zaključili da postoje dvije mogućnosti te smo odredili uz koji uvjet se dešava koji slučaj. Samim time, odredili smo i kako može izgledati $E(\mathbb{R})_{tors}$.

Dokazali smo Nagell-Lutzov teorem koji se može na očit način koristiti za određivanje torzijske grupe specifične eliptičke krivulje. Uz tu očitu metodu, obradili smo još jednu koja koristi eliptičke krivulje nad poljem $\mathbb{F}_p$, za p prikladno odabran prost broj. Također smo iskazali i Mordell-Weilov i Mazurov teorem.

Nakon toga, prešli smo na polja algebarskih brojeva. Najprije smo pokazali da točke konačnog reda na racionalnoj eliptičkoj krivulji zaista imaju algebarske brojeve za svoje koordinate. Definirali smo Weilovo sparivanje i Galoisovu reprezentaciju i dokazali nekoliko važnih rezultata koji se povezuju s njima, a mogu biti od velike pomoći pri klasifikaciji torzijskih grupa nad Galoisovim proširenjima. Dotaknuli smo se i izogenija eliptičkih krivulja i pokazali jednu značajnu tvrdnju koja ih povezuje s torzijom. Također smo naveli neke bitne, ranije pokazane poznate rezultate vezane za torziju nad nekim specifičnim poljima.

Na kraju, upotrijebili smo sve razvijene alate, iskazane i dokazane tvrdnje kako bismo (djelomično) klasificirali torzijske grupe racionalnih eliptičkih krivulja nad $(\mathbb{Q}(\zeta_{11}))$.

Summary

In this paper we considered torsion groups of elliptic curves. After some introductory definitions and some results for points of small order, we considered the situation for the field of complex numbers. Following known results, we determined the group of complex points and concluded that for every rational elliptic curve $E(\mathbb{C})_{tors}$ is always the same. More precisely, it is isomorphic to a torus as an additive group. Using that conclusion, we considered the group of real points on a rational elliptic curve and concluded that there are only two options. We also determined the conditions under which each of the two options arises. With that, we have determined the structure of $E(\mathbb{R})_{tors}$.

We proved the Nagell-Lutz theorem which can help in determining the torsion group structure for some specific elliptic curve. In addition to that obvious method, we gave one more method which uses elliptic curves over $\mathbb{F}_p$, for a suitable prime p. We also stated the Mordell-Weil theorem and Mazur's theorem.

After that, we moved on to number fields. First we proved that the coordinates of points of finite order on rational elliptic curves are algebraic numbers. We defined the Weil pairing and Galois representation and proved several results which can be helpful in classifying torsion groups of elliptic curves over Galois extensions. We also considered isogenies of elliptic curves and proved one important proposition which connects them to torsion groups. Additionally, we stated several important well-known results concerning torsion over some specific fields.

Finally, we used all the developed tools and results we quoted and/or proved to (partially) classify torsion groups of rational elliptic curves over $\mathbb{Q}(\zeta_{11})$.

Životopis

Borna Vukorepa je rođen 16. 10. 1994. u Zagrebu. Pohađao je XV. gimnaziju i za vrijeme srednjoškolskog obrazovanja sudjelovao na brojnim natjecanjima iz matematike i srodnih znanosti. Na 54. Međunarodnoj matematičkoj olimpijadi održanoj u Kolumbiji osvojio je zlatnu medalju.
2013. godine upisao je preddiplomski studij matematike na Prirodoslovno-matematičkom fakultetu Sveučilišta u Zagrebu, a 2016. upisao je diplomski studij teorijske matematike. Tokom studija sudjelovao je na brojnim studentskim matematičkim natjecanjima, od čega najviše vrijedi spomenuti prvu nagradu na Međunarodnom matematičkom studenstskom natjecanju *IMC* 2014. i drugo mjesto na Međunarodnom matematičkom natjecanju *Vojtech Jarnik* 2018.
Odradio je tri ljetne studentske prakse u Microsoftu (2015. - 2017.), a 2017. je dobio *Microsoft patent award* za prototip vezan za područje strojnog učenja i *metalearninga*.