# Eliptičke krivulje nad poljima algebarskih brojeva

Filip Najman

Prirodoslovno matematički fakultet, Matematički odsjek
2013.

# Sadržaj


**1 Uvod** **3**

**2 Grupovni zakon** **10**

**3 Funkcijska polja (afinih) krivulja** **16**

**4 Preslikavanja eliptičkih krivulja** **17**

**5 Izogenije** **21**

**6 Eliptičke krivulje nad $\mathbb{C}$** **24**

**7 Dualna izogenija** **28**

**8 Eliptičke krivulje nad $\mathbb{F}_p$** **30**

**9 Polja algebarskih brojeva** **36**
9.1 Kvadratna polja . . . . . 38
9.2 Kubna polja . . . . . 38
9.3 Kvartična polja . . . . . 39
9.4 Ciklotomska polja . . . . . 39
9.5 Grupa jedinica . . . . . 39
9.6 Faktorizacija u prstenovima cijelih brojeva PAB . . . . . 40
9.7 Eksplicitna faktorizacija . . . . . 40

**10 Galoisove reprezentacije pridružene eliptičkim krivuljama** **43**
10.1 Djelidbeni polinomi . . . . . 48

**11 Dokaz Mordell-Weilovog teorema** **50**
11.1 Slabi Mordell-Weilov teorem . . . . . 50
11.2 Spust . . . . . 54

**12 Weilovo sparivanje** **57**

**13 Galoisova kohomologija** **59**

**14 Twistovi** **69**

**15 Torzori** **71**

**16 Selmerova i Tate-Šafarevičeva grupa** **74**

**17 Spust pomoću 2-izogenija** **79**

**18 $L$-funkcije pridružene eliptičkim krivuljama i Birch–Swinnerton-Dyerova slutnja** **83**

**19 Modularne krivulje** **86**

**20 Eliptičke krivulje u Magmi** **92**

**21 Eliptičke krivulje nad kvadratnim poljima** **101**

**22 Eliptičke krivulje nad poljima algebarskih brojeva stupnja većeg od 2** **109**

**23 Torzijske grupe racionalnih eliptičkih krivulja nad poljima algebarskih brojeva** **112**
23.1 Racionalne eliptičke krivulje nad kubnim poljima . . . . . 115

**24 Upotreba eliptičkih krivulja u rješavanju diofantskih jednadžbi** **118**
24.1 Problem kongruentnih brojeva . . . . . 121
24.2 Modularna metoda za rješavanje diofantskih jednadžbi . . . . . 123

# Poglavlje 1

# Uvod

Diofantske jednadžbe tj. polinomijalne jednadžbe (u više varijabli) nad $\mathbb{Z}$ i nad $\mathbb{Q}$ (ili nad nekim drugim nama zanimljivim prstenovima) imaju dugačku povijest, još od stare Grčke.

Preciznije, neka je $R$ neki komutativni prsten, te neka su $f_1, \ldots, f_n \in R[x_1, \ldots, x_m]$. Neka je $V(R)$ skup riješenja

$$\begin{aligned} f_1(x_1, \ldots, x_m) &= 0, \\ &\vdots \\ f_n(x_1, \ldots, x_m) &= 0, \end{aligned} \tag{1.1}$$

to jest,

$$V(R) = \{P \in R^m | f_i(P) = 0\}.$$

Nas će na ovom predmetu zanimati prvenstveno krivulje, tj. rješenja polinomijalnih jednadžbi u dvije varijabl, npr. $x^2 - 2y^4 = 1$.

Najpoznatiji diofantski problem je posljednji Fermatov teorem koji kaže da

$$x^n + y^n = z^n$$

ima samo trivijalna rješenja (ona za koje je $xyz = 0$) u $\mathbb{Z}$ za $n \geq 3$, ili ekvivalentno

$$x^n + y^n = 1$$

ima samo trivijalna rješenja u $\mathbb{Q}$, za $n \geq 3$. Primjetimo da je ovo zapravo tvrdnja u skupu diofantskih jednadžbi (za svaki fiksni $n$, dana je tvrdnja diofantska jednadžba). Teorem je dokazao Wiles 1995., te su ključnu ulogu u dokazu igrale upravo eliptičke krivulje.

Neka pitanja koja se možemo pitati o $V(R)$ su

1. $V(R) =?$
2. $V(R) = \emptyset?$

3. $\#V(R) = \infty$?

4. Ako je $\#V(R) = \infty$, definiramo $N_V(B) = \#\{P \in V(R) | h(P) < B\}$ - broj rješenja "manjih"(mjereno funkcijom $h$) od neke vrijednosti $B$. Kako raste $N_v(B)$ kada $B \to \infty$?

5. Postoji li algoritam za odrediti je li $V(R) = \emptyset$?

Recimo nešto više o problemu (5) - problem određivanja postoji li algoritam za provjeravanje ima li općenita diofantska jednadžba $V$ nad $\mathbb{Z}$ rješenja, tj. je li $V(\mathbb{Z}) = \emptyset$, poznat je kao Hilbertov 10. problem. Ovo ime dolazi od činjenice da je ovaj problem bio na listi od 23 najvažnija problema 1900. godine koju je sastavio David Hilbert. Matijaševič je, koristeći rezultate od Davis, Putnam i Robinson, 1970. dokazao da takav algoritam ne postoji. Isti problem nad $\mathbb{Q}$ je još uvijek otvoren.

Aritmetička[1] (algebarska) geometrija ili diofantska geometrija proučava diofantske jednadžbe koristeći metode iz algebarske teorije brojeva i algebarske geometrije. To i nije iznenađujuće pošto polinomijalne jednadžbe opisuju neke geometrijske objekte (krivulje, plohe, itd.) nad $\mathbb{C}$.

Krenimo od najjednostavnijih diofantskih jednadžbi, tj. jednadžbi oblika

$$ax + by = c, \text{ gdje su } a, b, c \in \mathbb{Q}.$$

Bez smanjenja općenitosti može se pretpostaviti da su $a, b, c \in \mathbb{Z}$. Ova jednadžba ima racionalna rješenja rješenja ako i samo ako $(a, b)|c$ (gdje s $(a, b)$ označavamo najveći zajednički djelitelj od $a$ i $b$), te ako rješenja postoje, tada se sva rješenja mogu naći Euklidovim algoritmom (ima ih $\infty$).

Sljedeće po težini su *konike* tj. jednadžbe oblika

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, a, b, c, d, e, f \in \mathbb{Z}, a, b \text{ ili } c \neq 0,$$

gdje je polinom s lijeve strane ireducibilan. Geometrijski, ove jednadžbe opisuju presjek konusa i ravnine. Linearnim promjenama koordinata, ove jednadžbe se mogu svesti na jedan od sljedeća tri oblika

$$Ax^2 + By^2 = C, \ B > 0 \text{ - elipsa,}$$

$$Ax^2 - By^2 = C, \ B > 0 \text{ - hiperbola,}$$

$$Ax + By^2 = C \text{ - parabola,}$$

gdje su sada $A, B, C \in \mathbb{Q}$.

Kada ove jednadžbe imaju rješenja? Promotrimo

$$T_1 : x^2 + 3y^2 = 2$$

$$T_2 : x^2 + y^2 = -1$$

$$T_3 : x^2 + y^2 = 1$$

[1] Aritmetika je stara riječ za teoriju brojeva

Pitamo se $\#T_i(\mathbb{Q}) = ?$.

S $F_q$ označavamo konačno polje s $q$ elemenata, gdje je $q$ potencija nekog prostog broja $p$. S $Q_p$ označavamo $p$-adsko upotpunjenje od $\mathbb{Q}$ korištenjem $p$-adske valuacije (vidi [13, Chapter II] za detalje).

Lako se vidi da je $T_1(\mathbb{Q}) = \emptyset$ jer $x^2 + 3y^2 \equiv 2 \pmod 3$ nema rješenja. Tj. $T_1(\mathbb{F}_3) = \emptyset$ pa $T_1(\mathbb{Q}_3) = \emptyset$.

Također $T_1(\mathbb{Q}) \subset T_1(\mathbb{Q}_3) \Longrightarrow T_1(\mathbb{Q}) = \emptyset$. Vrijedi $T_2(\mathbb{Q}) = \emptyset$ jer je $T_2(\mathbb{R}) = \emptyset$.

Može se pokazati da su ovi nužni uvjeti za postojanje rješenja i dovoljni - ako ima rješenja nad $\mathbb{Q}_p$ za sve proste $p$ i nad $\mathbb{R}$, tada ima i nad $\mathbb{Q}$!

O tome nam govori tzv. lokalno-globalni princip. Prije nego što iskažemo sljedeći teorem, primjetimo da kvadratni i linearni polinomi opisuju krivulje genusa 0.

**Teorem 1** (Hasse-Minkowski)**.** *Krivulja genusa 0 ima točke nad $\mathbb{Q}$ ako i samo ako ima točke nad $\mathbb{Q}_p$ za sve proste brojeve $p$ i nad $\mathbb{R}$.*

Lokalno-globalni princip se često naziva i Hasseov princip. Provjeriti ima li krivulja točke nad $\mathbb{Q}_p$ za sve proste $p$ je "lagano", tj. može se napraviti u konačno vremena (treba provjeriti samo da ima rješenja modulo $p^k$ za konačno mnogo $p$-ova i $k$-ova, tj. ne treba provjeravati za sve $p$-ove) - dakle postoji algoritam za određivanje ima li krivulja genusa 0 konačno mnogo točaka nad $\mathbb{Q}$.

Također, ako krivulja genusa 0 ima jednu točku, imat će ih beskonačno mnogo. Neka znamo jednu točku $P$ na krivulji genusa 0. Tada možemo dobiti sve točke na krivulji tako da iz $P$ vučemo pravce s racionalnim nagibom, te uzmemo da je nova točka presjek tog pravca s konikom.

Tako ćemo dobiti sve točke.

Npr. pogledajmo najjednostavniji primjer kružnice $x^2 + y^2 = 1$ (i za druge konike je procedura ista, iako je račun malo kompliciraniji).

Uzmimo očitu točku $P = (-1, 0)$. Uzmimo sada neki racionalan $t \in \mathbb{Q}$. Tada vučemo pravac $y = t(x + 1)$ s nagibom $t$ kroz $P$. On sječe kružnicu u točki

$$\left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right).$$

Primjetimo da je nagib pravca $QP$, za bilo koju drugu racionalnu točku na kružnici $Q$ također racionalan. Dakle na ovaj način smo dobili sve racionalne točke na kružnici (ako dodamo samu točku $P$), te one ovise samo o parametru $t$, tj. *parametrizirali* smo kružnicu.

Spomenuli smo genus, zašto? Pokazuje se da je genus najbolji način sortiranja krivulja po "kompliciranosti", puno bolji od možda intuitivnijeg sortiranja po stupnju polinoma koji određuje krivulju.

Npr. krivulja

$$3x^4y^2 + 5x^2y + 11xy + 23x + 14 = 0,$$

je puno složenija od

$$y - x^8 = 0,$$

iako druga ima veći stupanj. Sva rješenja druge jednadžbe se mogu lako naći tako da se uzme $x = t, y = t^8$, tj. ona se može parametrizirati.

Ovo je primjer principa "geometrija određuje aritmetiku", tj. geometrijska svojstva krivulje (genus u ovom slučaju) određuju neka aritmetička svojstva (broj točaka nad $\mathbb{Q}$).

Dakle, krivulje genusa 0 su nam nezanimljive s aritmetičkog stajališta. S druge strane za krivulje genusa $\geq 2$, imamo sljedeći važan rezultat koji je Mordell 1922. formulirao kao slutnju, te ga je dokazao Faltings 1983. (za što je, između ostalog, dobio Fieldsovu medalju 1986).

**Teorem 2** (Faltings)**.** *Krivulja genusa $\geq 2$ ima samo konačno mnogo točaka nad bilo kojim poljem algebarskih brojeva.*

**Definicija.** Polje algebarskih brojeva $K$ je konačno proširenje od $\mathbb{Q}$, tj. $[K : \mathbb{Q}] < \infty$.

Postoji slutnja da je broj racionalnih točaka koji može imati nesingularna krivulja fiksiranog genusa $\geq 2$ omeđen. Nesingularna krivulja genusa 2 s najviše poznatih racionalnih točaka je

$$y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 + 567207969x^2$$
$$-985905640x + 247747600,$$

koju je pronašao Stoll 2008. godine, te koja ima 642 točke. Postoji slutnja da "nasumično odabrana" krivulja genusa $\geq 2$ ima 0 racionalnih točaka.

Ako pustimo da genus varira, tada broj točaka koji krivulja može imati nije ograničen. Na primjer možemo odabrati $n$ točaka na $x$ osi (tj. oblika $(x, 0)$), te interpolirati ih polinomom $f(x)$. Tada će krivulja $y^2 = f(x)$ biti genusa $\geq 2$, te imati barem $n$ točaka. Međutim kako povećavamo $n$, tako će rasti i genus ove krivulje.

Eliptičke krivulje će biti u zlatnoj sredini, tj. imat će dovoljno, ali ne previše strukture.

**Definicija. Eliptička krivulja** nad poljem $k$ je glatka, projektivna krivulja genusa 1 sa specificiranom točkom $\mathcal{O} \in k$.

Objasnimo ovu definiciju. **Afini pravac** je $\mathbb{A}^1(k) = k$. **Afina ravnina** je $\mathbb{A}^2(k) = k \times k$.

**Definicija. Projektivni pravac** $\mathbb{P}^1(k)$ je

$$\mathbb{P}^1(k) = \{(a, b) \in k^2 | (a, b) \neq (0, 0)\}/\sim$$

gdje je $(a, b) \sim (c, d)$ ako i samo ako postoji $0 \neq \lambda \in k$ takav da je $a = \lambda c$ i $b = \lambda d$.

Analogno, **projektivna ravnina** $\mathbb{P}^2(k)$ je

$$\mathbb{P}^2(k) = \{(a, b, c) \in k^3 | (a, b, c) \neq (0, 0, 0)\}/\sim$$

gdje je $(a,b,c) \sim (d,e,f)$ ako i samo ako postoji $0 \neq \lambda \in k$ takav da je $a = \lambda d$ i $b = \lambda e$ i $c = \lambda f$. Klasu ekvivalencije čije je $(a,b,c)$ reprezent, označavamo s $(a : b : c)$.

Točke projektivnog pravca $\mathbb{P}^1(k)$ možemo zamišljati kao nagib nekog pravca u ravnini ili alternativno kao $A^1(k) \cup \{\infty\}$, gdje $\infty$ "predstavlja" okomiti pravac. Pošto je preslikavanje

$$(a : b : c) \to \begin{cases} (a/c, b/c) & \text{ako je } c \neq 0 \\ (a : b) & \text{ako je } c \neq 0 \end{cases}$$

bijekcija, vrijedi da je $\mathbb{P}^2(k) = A^2(k) \cup \mathbb{P}^1(k)$.

**Definicija.** Neka je $k$ savršeno polje, $f \in k[x,y]$ polinom, te $\overline{k}$ algebarsko zatvorneje od $k$. Tada je **afina krivulja** $C_f$ skup točaka

$$C_f = \{P \in A^2(\overline{k}) | f(P) = 0\}.$$

**Definicija.** Neka je $F \in k[X,Y,Z]$ homogeni polinom. Tada je **projektivna krivulja** $C_F$ skup točaka

$$C_F = \{P \in \mathbb{P}^2(\overline{k}) | F(P) = 0\}.$$

Stupanj od krivulje $C_F$ je stupanj od $F$.

S $C_f(k)$ i $C_F(k)$ označavamo skupove $k$-racionalnih točaka od $C_f$ i $C_F$.

Ako je krivulja $C$ definirana nad $k$ (tj. $F \in k[X,Y,Z]$ za projektivnu krivulju, ili $f \in k[x,y]$), tada pišemo $C/k$.

**Definicija.** Projektivna krivulja $C_F/k$ je nesingularna ako ne postoji $P \in C_F(k)$ takva da je

$$\frac{dF}{dX}(P) = \frac{dF}{dY}(P) = \frac{dF}{dZ}(P) = 0.$$

Na primjer, krivulja

$$Y^2Z = X^3 + X^2Z$$

ima sve parcijalne derivacije jednake 0 u $P = (0 : 1 : 0)$, dakle nije glatka.

Bitno je i da eliptička krivulja ima $k$-racionalnu točku. Npr. krivulja

$$S : 3X^3 + 4Y^3 + 5Z^3 = 0$$

nema točaka (sjetimo se da $(0 : 0 : 0)$ nije točka!), tako da $S$ nije eliptička krivulja, iako je glatka projektivna krivulja genusa 1.

Krivulja $S$, poznata kao Selmerova krivulja, je primjer kršenja lokalno-globalnog principa: $S$ ima točke nad $\mathbb{Q}_p$ za svaki prosti proj $p$ i ima realne točke ali nema $\mathbb{Q}$-racionalne točke. Dakle, ima točke "lokalno" (tj. nad svim lokalnim poljima, tj. $\mathbb{Q}_p$ i $\mathbb{R}$ ), ali nema "globalno" (nad $\mathbb{Q}$).

Svaka afina krivulja se može upotpuniti do projektivne krivulje dodavanjem odgovarajuće potencije od $z$ u svakom sumandu. Na primjer,

$$x^4 + xy = y^3 + 2x$$

se može upotpuniti tako da se napiše kao

$$x^4 + xyz^2 = y^3z + 2xz^3.$$

Projektivne krivulje se često pretvaraju u afine krivulje (između ostalog zbog lakše notacije) tako da se uzme $z = 1$. Mi ćemo često, zbog lakše notacije pisati (eliptičke) krivulje kao da su afine krivulje, iako ćemo ih zapravo zauvijek smatrati projektivnim krivuljama.

Prije nego što krenemo promatrati svojstva eliptičkih krivulja, uvest ćemo standardni oblik zapisivanja krivulja.

**Lema 3.** *Svaka eliptička krivulja $E$ nad poljem $k$ se može zapisati u* ***Weierstrassovoj formi***

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

Eliptička krivulja $E$, zapisana u projektivnom obliku je zapravo

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

ali mi možemo zbog jednostovanosti $E(k)$ zamišljati kao skup točaka koje zadovoljavaju jednadžbu (1.2) plus "točka u beskonačnosti $\mathcal{O}$", koja je $(0 : 1 : 0)$ u projektivnim koordinatama.

Ako je karakteristika polja $k$, *char* $k \neq 2, 3$, tada se eliptička krivulja može zapisati u **kratkoj Weierstrassovoj formi**

$$y^2 = x^3 + ax + b.$$

Neka je

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

eliptička krivulja u kratkoj Weierstrtassovoj formi. Tada je **diskriminata eliptičke krivulje**

$$\Delta(E) = \Delta = -16(4a^3 + 27b^2).$$

Primjetimo da je $\Delta(E) = 16\times$diskriminanta od $x^3 + ax + b$, te vrijedi da je $\Delta \neq 0$ ekvivalentno tome da je $E$ glatka. Zaista ako je $F = y^2 - x^3 - ax - b$, tada je

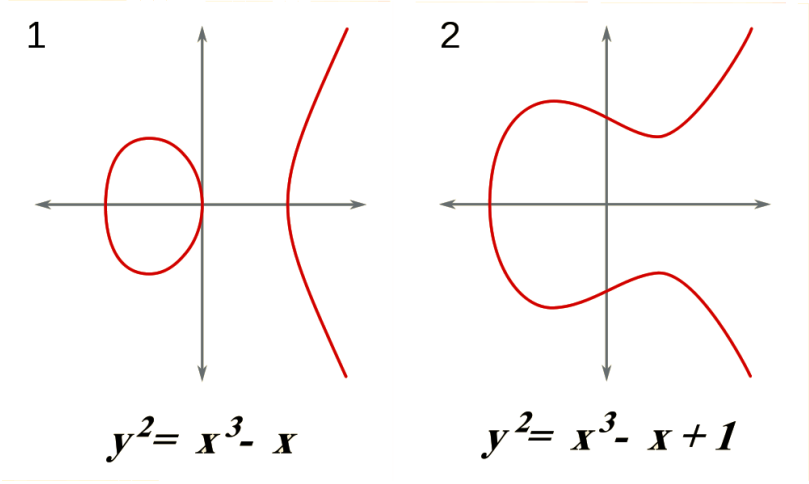
$$\frac{dF}{dy}(P) = 0 \Longleftrightarrow y(P) = 0,$$

te je

$$\frac{dF}{dy}(P) = 0 \text{ i } \frac{dF}{dx}(P) = 0 \Longleftrightarrow x^3 + ax + b \text{ ima višestruke nultočke}$$

$\iff$ diskriminanta od $x^3 + ax + b$ je $0 \iff \Delta(E) = 0$.

Ako je $E$ definirana nad potpoljem od $\mathbb{R}$, tada ovisno o tome je li $\Delta$ pozitivna ili negativna, $x^3+ax+b$ će imati ili 1 ili 3 nultočke nad $\mathbb{R}$. Možemo sada skicirati $E(\mathbb{R})$, ovisno o tome je li diskriminanta pozitivna (slika 1) ili negativna (slika 2).



# Poglavlje 2

# Grupovni zakon

Krivulje genusa 1, kao što smo vidjeli, mogu imati 0 točaka (tada nisu eliptičke krivulje). Mogu imati i pozitivan konačan broj točaka, te mogu i imati beskonačno mnogo točaka. Štoviše, skup točaka $E(K)$ čini Abelovu grupu, pod sljedećom definicijom. Pretpostavimo da je $E$ zadana ravninskom kubikom. Neka je $\mathcal{O}$ (točka u beskonačnosti) neutralni element, te definiramo operaciju $+$ tako da za svake 3 kolinearne točke $P, Q, R \neq \mathcal{O}$ vrijedi $P + Q + R = \mathcal{O}$.

Pretpostavimo zbog jednostavnosti da je eliptička krivulja $E/k$ zadana u kratkoj Weierstrassovoj formi. Trebat će nam Bezoutov teorem:

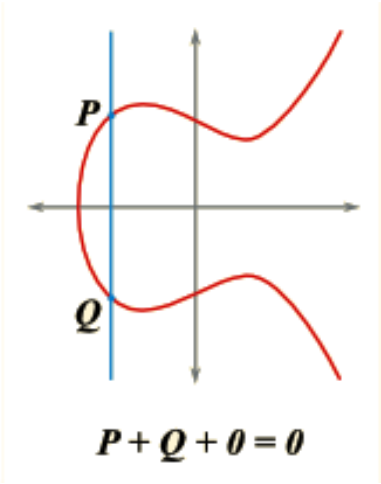
**Teorem 4** (Bezout)**.** *Dvije algebarske krivulje definirane nad poljem $k$ stupnjeva $m$ i $n$, koje nemaju zajedničku komponentu, sijeku se u $mn$ točaka, ako brojimo kratnost svake točke presjeka nad algebarskim zatvorenjem $\overline{k}$ od $k$.*

Uzmimo prvo da su točke $\mathcal{O} \neq P, Q \in E(k)$ dvije različite točke s istim $x$-koordinatama, tj. $y(P) = -y(Q) \neq 0$. Sada ćemo se nakratko prebaciti u projektivne koordinate

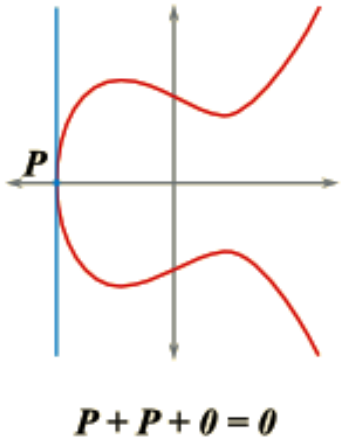
$$y^2 z = x^3 + axz^2 + bz^3,$$

te se sjetimo da je $\mathcal{O} = (0 : 1 : 0)$ točka u beskonačnosti. Neka je $P = (x : y : 1)$, $Q = (x : -y : 1)$, tada je pravac koji prolazi kroz $P$ i $Q$ $u(x : y : 1)+v(x : -y : 1)$. Za $u = -v = 1$ dobivamo da pravac siječe $(0 : 2y : 0) = (0 : 1 : 0)$, tj. točku u beskonačnosti.

Skicirat ćemo sve što radimo nad $\mathbb{R}$, tj. za $E(\mathbb{R})$, iako sve što radimo vrijedi i nad općenitim poljem $k$.




Dakle $P + Q + \mathcal{O} = \mathcal{O}$, tj. $P = -Q$.
Ako je $y(P) = 0$, tada će okomiti pravac biti tangenta na $E$ u $P$ ,




pa je $P + P + \mathcal{O} = \mathcal{O}$, tj. $2P = \mathcal{O}$, tj. $P$ će biti točka reda 2 u našoj grupi.

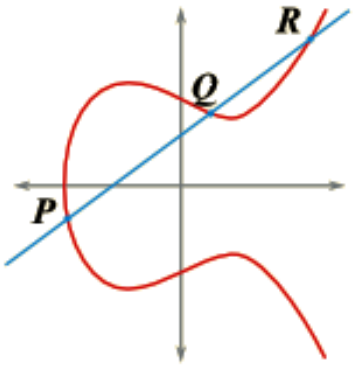
Uzmimo sada da su $P, Q \in E(k)$ dvije točke s različitim $x$-koordinatama, te neka pravac $p$ kroz njih siječe svaku od točaka s multiplicitetom 1 (dakle nije ni tangenta ni infleksijska točka). Tada po Bezoutovom teoremu slijedi da pravac kroz $P$ i $Q$, nad $\overline{k}$, siječe $E$ u nekoj trećoj točki $R \in E(\overline{k})$. Međutim $x(R)$ je rješenje sustava jednadžbi

$$y^2 = x^3 + ax + b$$
$$p : y = cx + d,$$

gdje su $c$ i $d$ $k$-racionalni. Dakle, pošto

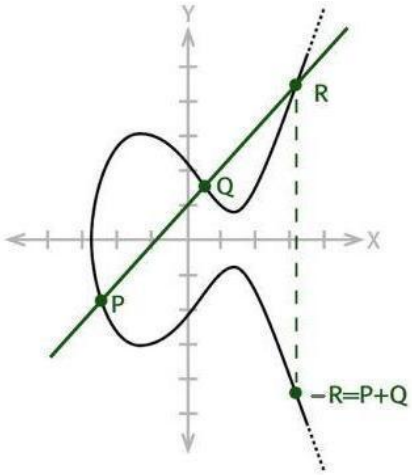
$$(cx + d)^2 = x^3 + ax + b$$

ima 2 rješenja ($x(P)$ i $x(Q)$), tada i treća nultočka mora biti definirana nad $k$. Također mora biti različita od $x(P)$ i $x(Q)$ pošto smo pretpostavili da se $p$ i $E$ sijeku u točkama multipliciteta 1. Iz jednadžbe za $p$ slijedi da je $y(R)$ također $k$-racionalan, pa je $R \in E(K)$.

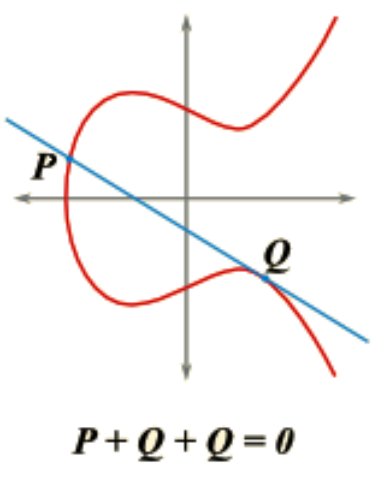



$$P + Q + R = 0$$

Pošto je $P + Q + R = 0$ slijedi da je $R = -(P + Q)$ pa je $P + Q$ prema ranije dokazanoj točka $-R$, tj. točka koju dobijemo zrcaljenjem s obzirom na $x$-os. Ovaj postupak nam zapravo daje pravilo zbrajanja točaka: povuci pravac kroz točke krivulje, nađi treću točku na pravcu (koja može biti jedna od već odabranih), te zrcali s obziron na $x$-os.




Pogledajmo za kraj što dobijemo ako pravac $p$ prolazi kroz različite točke $P$ i $Q$, te taj pravac siječe neku točku s multiplicitetom 2 (ne može više zbog Bezoutovog teorema).




tj. vrijedi $P + Q = -Q$.

Ako je točka $P$ točka infleksije, tj. tangenta siječe eliptičku krivulju s multiplicitetom 3, tada je $P + P + P = 0$, odnosno $P$ je točka reda 3.

Pogledajmo formule za zbrajanje točaka. Neka je $P = (x_1, y_1)$, $Q = (x_2, y_2)$.

1. $-\mathcal{O} = \mathcal{O}$.
2. $-P = (x_1, -y_1)$.
3. $\mathcal{O} + P = P$.
4. ako je $Q = -P$, tada je $P + Q = \mathcal{O}$.
5. ako je $Q \neq -P$, tada je $P + Q = (x_3, y_3)$, gdje je

$$x = \lambda^2 - x_1 - x_2, \;\; y_3 = -y_1 + \lambda(x_1 - x_3),$$

gdje je $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, ako je $x_2 \neq x_1$, te
$\lambda = \frac{3x_1^2 + a}{2y_1}$, ako je $x_2 = x_1$.

Vidimo da je operacija $+$ dobro definirana, ima neutralni element $\mathcal{O}$, te svaki element ima svoj inverz. Da bi $(E(k), +)$ bila grupa, trebalo bi još dokazati asocijativnost. Taj dokaz je (tehnički) kompliciraniji, te ćemo ga preskočiti.

Lako se vidi po definiciji grupovnog zakona da je $(E(k), +)$ komutativna grupa. Štoviše, vrijedi i više.

**Teorem 5** (Mordell-Weil)**.** *Neka je $E$ eliptička krivulja nad poljem algebarskih brojeva $k$. Tada je $E(k)$ konačno generirana Abelova grupa.*

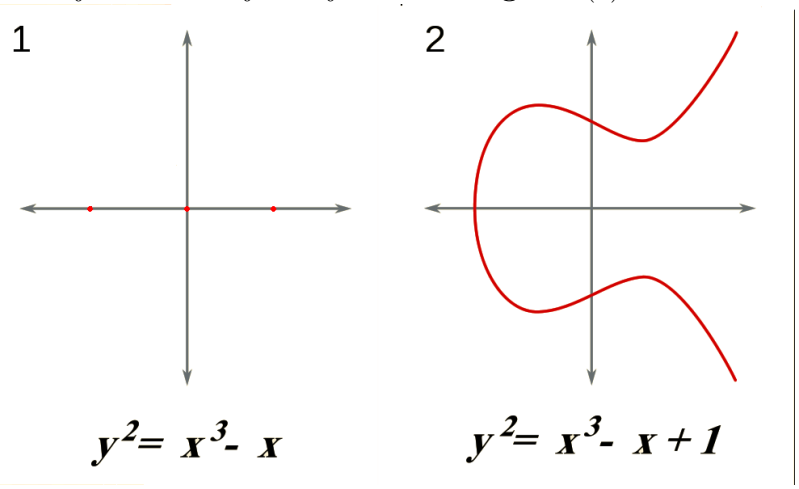
Ovaj teorem ćemo dokazati kasnije u kolegiju.

Teorem je za eliptičke krivulje nad $\mathbb{Q}$ dokazao Mordell, te ga je poopćio Weil za Abelove mnogostrukosti (algebarske mnogostrukosti koje su ujedno i Abelove grupe) nad poljima algebarskih brojeva.

Po Mordell-Weilovom teoremu i teoremu o klasifikaciji konačno generiranih Abelovih grupa, slijedi da je

$$E(k) \simeq T \oplus \mathbb{Z}^r,$$

gdje je $r \geq 0$, te je $T$, **torzijska podgrupa** od $E(k)$, podgrupa elemenata konačnog reda u $E(k)$. Primjetimo da pošto je $T$ konačno generirana grupa, slijedi i da je konačna. Cijeli broj $r$ se zove **rang** od $E(k)$.




$E_1(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ $E_2(\mathbb{Q}) \simeq \mathbb{Z}$.

Rang od $E_1(\mathbb{Q})$ je 0, a od $E_2(\mathbb{Q})$ je 1. Torzija od $E_1(\mathbb{Q})$ je $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ a od $E_2(\mathbb{Q})$ je trivijalna.

**Teorem 6** (Mazur 1978.)**.** *$E(\mathbb{Q})_{tors}$ je jedna od sljedećih 15 grupa*

$$\mathbb{Z}/n\mathbb{Z}, \ n = 1, \ldots, 10, 12,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, \ m = 1, \ldots, 4.$$

Za zadanu eliptičku krivulju se lako izračuna torzija, tj. postoje algoritmi za njeno računanje, te su oni i u praksi vrlo efikasni.

S druge strane, o rangu (nad $\mathbb{Q}$) se puno manje zna. Nije poznato ni može li biti proizvoljno velik ili postoji apsolutna gornja ograda za rang eliptičkih krivulja nad $\mathbb{Q}$.

Najveći poznati rang eliptičke krivulje nad $\mathbb{Q}$ je 28 (Elkies 2006).

**Slutnja 7** (Goldfeld)**.** *Ako poredamo eliptičke krivulje po veličini koeficijenata, asimptotski 50% krivulja ima rang 0, a 50% ih ima rang 1.*

Dakle, Goldfeldova slutnja predviđa da je prosječni rang jednak 0.5.

**Teorem 8** (Bhargava & Shanakar (2011))**.** *Ako poredamo eliptičke krivulje po veličini koeficijenata, prosječni rang je* $< 0.99$.

Računanje ranga je teško (i u praksi i u teoriji): postoji "postupak", za računanje ranga - u praksi često funkcionira, ali nema garancije da će proces ikada završiti.

Postoji slutnja (Tate-Šafarevič) čija bi istinitost povlačila da je gornji postupak zaista algoritam.

**Primjer 1.** Za zadani prirodan broj $n$ postoji li pravokutan trokut s racionalnim stranicama i površinom $n$? Brojevi za koje to vrijedi, zovu se *kongruentni brojevi*.

Vrijedi da je $n$ kongruentan $\iff E : y^2 = x^3 - n^2x$ ima pozitivan rang.

Npr. $n = 157$ je kongruentan, jer postoji trokut sa stranicama

$$\frac{157841 \cdot 4947203 \cdot 526771095761}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441},$$

$$\frac{2^2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 157 \cdot 17401 \cdot 46997 \cdot 356441}{157841 \cdot 4947203 \cdot 526771095761},$$

$$\frac{20085078913 \cdot 1185369214457 \cdot 942545825502442041907480 1}{2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 37 \cdot 101 \cdot 17401 \cdot 46997 \cdot 356441 \cdot 157841 \cdot 4947203 \cdot 526771095761}.$$

# Poglavlje 3

# Funkcijska polja (afinih) krivulja

U ovom i sljedećem poglavlju ćemo navoditi mnoge tvrdnje bez dokaza. Dokazi se mogu naći u [14].

**Definicija.** Neka je $R$ integralna domena. Tada je $\mathrm{Frac}(R) = \{\frac{a}{b}, a, b \in R, b \neq 0\}/\sim$, gdje je $\sim$ standardna relacija ekvivalencije, **polje razlomaka** od $R$.

**Primjer 2.** $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q},\ \mathrm{Frac}(k[x]) = k(x)$.

**Definicija. Racionalna funkcija** na $\mathbb{A}^n(k)$ je $f \in k(x_1, \ldots, x_n) =: k(A^n)$.

Mi ćemo promatrati samo slučaj $n = 2$.

**Definicija.** Neka je $C/k$ afina krivulja, te $f = \frac{g}{h} \in k(\mathbb{A}^2)$, gdje je $h \neq 0$ na $C(k)$. Restrikcija od $f$ na $C$

$$f : C - \{\text{konačan skup gdje je } h = 0\} \to \overline{k}$$

je **racionalna funkcija na** $C$. Skup svih racionalnih funkcija na $C$ čini polje, koje označavamo s $k(C)$.

**Činjenica.** Neka je $C_f$ afina krivulja definirana s $f \in k[x, y]$. Tada je

$$k(C) \simeq \mathrm{Frac}\left(\frac{k[x,y]}{(f)}\right).$$

**Primjer 3.** Neka je $D : y = 0$ u afinoj ravnini.

$$k(C) \simeq \mathrm{Frac}\left(\frac{k[x,y]}{(y)}\right) \simeq \mathrm{Frac}(k[x]) = k(x).$$

**Primjer 4.** Neka je $C : y^2 = x^3 + 1$ u afinoj ravnini. Tada je

$$k(C) \simeq \mathrm{Frac}\left(\frac{k[x,y]}{(y^2 - x^3 - 1)}\right) \simeq k(x, \sqrt{x^3 + 1}).$$

# Poglavlje 4

# Preslikavanja eliptičkih krivulja

**Definicija.** Neka su $C/k$ i $D/k$ krivulje. **Racionalno preslikavanje** (nad $k$) $\phi : C \to D$ je preslikavanje definirano s racionalnim funkcijama $\phi = (u, v),\ u, v \in k(C)$, takvo da $u$ i $v$ nisu oboje 0. Tj, $\phi(P) = (u(P), v(P))$ za $P \in C(k)$.

Primjetimo sljedeće: Neka su $C_f$ i $D_g$ krivulje, te neka je $\phi : C \to D$ preslikavanje. Ako je $a$ racionalna funkcija $\in k(D)$, tada je $a \circ \phi$ racionalna funkcija $\in k(C)$. Dakle, racionalna funkcija $\phi : C \to D$ inducira injekciju polja

$$\phi^* : k(D) \hookrightarrow k(C),$$

$$a \mapsto a \circ \phi = \phi^* a.$$

**Definicija.** Stupanj od $\phi$ je $[k(C) : \phi^* k(D)]$, ako $\phi$ nekonstantna, a definiramo da je stupanj od $\phi$ jednak 0 ako je $\phi$ konstantna.

**Primjer 5.** Neka su $C$ i $D$ kao u primjerima 3 i 4. Tada je

$$\phi : C \to D,\ \ \phi(x, y) = (x, 0)$$

racionalno preslikavanje, te vrijedi da ako je $a(x, 0) = x$ racionalna funkcija na $k(D)$, tada je

$$a \circ \phi(x, y) = \phi^* a(x, y) = x$$

Dakle $\phi^* k(D) = k(x)$, te je

$$[k(C) : \phi^* k(D)] = [k(x, \sqrt{x^3 + 1}) : k(x)] = 2,$$

pa slijedi da je ovo preslikavanje stupnja 2.

**Činjenica.** Neka je $k$ polje algebarskih brojeva, te neka je $K$ konačno proširenje od $k(x)$. Tada postoji krivulja $C$ takva da je $k(C) = K$.

**Činjenica.** Neka je $i : k(C_2) \hookrightarrow k(C_1)$ ulaganje funkcijskih polja koje fiksira $k$. Tada postoji jedinstveno ne-konstantno racionalno preslikavanje $\phi : C_1 \to C_2$ takvo da je $\phi^* = i$.

**Definicija.** Kažemo da je $\phi : C \to D$ **definirano** u točki $P$ ako postoji $g \in k(C)^*$ takav da su $ug, vg$ definirani u $P$. Ako je $\phi$ definiran na cijeloj $C$, tada je $\phi$ **morfizam**.

**Definicija.** Ako je $\phi : C \to D$ morfizam takav da postoji morfizam $\psi : D \to C$ takav da su $\psi \circ \phi$ i $\phi \circ \psi$ identiteta na $C$ i $D$, tada je $\phi$ **izomorfizam**.

**Činjenica.** Ako je $\phi : C \to D$ racionalno preslikavanje takvo da je $C$ glatka, tada je $\phi$ morfizam.

**Činjenica.** Ako je $\phi : C \to D$ racionalno preslikavanje stupnja 1, te su $C$ i $D$ glatke, tada je $\phi$ izomorfizam.

Imamo sljedeću ekvivalenciju kategorija:

$$\text{glatke krivulje nad } k \leftrightarrow \text{proširenja polja } K/k(x)$$

$$\text{racionalna preslikavanja (morfizmi)} \leftrightarrow \text{ulaganja polja}$$
$$C \to k(C).$$

**Činjenica.** Ako su dvije eliptičke krivulje

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$$E' : y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6$$

u Weierstrassovoj formi izomorfne, tada postoji preslikavanje $(x_E, y_E) \mapsto (x_{E'}, y_{E'})$,

$$x_{E'} = u^2x_E + r,$$

$$y_{E'} = u^3y_E + sx_E + t, \text{ gdje } u \in k^*, r, s, t \in k.$$

Također, ako su dvije eliptičke krivulje

$$E : y^2 = x^3 + ax + b, \tag{4.1}$$

$$E' : y^2 = x^3 + a'x + b' \tag{4.2}$$

u kratkoj Weierstrassovoj formi (nad poljem karakteristike $\neq 2, 3$) izomorfne, tada postoji pomjena varijabli

$$x_{E'} = u^2x_{E,}$$

$$y_{E'} = u^3y_E, \text{ gdje } u \in k^*.$$

Dakle za eliptičke krivulje $E$ i $E'$ u kratkoj Weierstrassovoj formi vrijedi

$$E \simeq E' \iff (u^3y_E)^2 = (u^2x_E)^3 + a'(u^2x_E) + b',$$

$$\iff a' = u^4a,\ b' = u^6b$$

$$\Delta(E') = -16(4a'^3 + 27b'^2) = u^{12}\Delta(E)$$

**Definicija.** ***j*-invarijanta** eliptičke krivulje $y^2 = x^3 + ax + b$ je

$$j = j(E) = \frac{1728(-4a)^3}{\Delta}.$$

Za eliptičku krivulju u (općoj) Weierstrassovoj formi

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

diskriminanta i $j$-invarijanta se računaju na sljedeći način:

$$b_2 = a_1^2 + 4a_2,\ b_4 = a_1a_3 + 2a_4,\ b_6 = a_3^2 + 4a_6,\ b_8 = b_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4,\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6,\ \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b^2b^4b^6,\ j = c_4^3/\Delta.$$

**Propozicija 9.** *Neka je $k$ polje karakteristike $\neq 2, 3$.*

1. *Eliptičke krivulje $E$ i $E'$ su izomorfne nad $\overline{k}$ ako i samo ako je $j(E) = j(E')$.*
2. *Za svaki $j \in k$, postoji eliptička krivulja $E/k$ takva da je $j(E) = j$.*

*Dokaz.* 1. Pretpostavimo da su $E$ i $E'$ kao u (4.1) i (4.2), to sigurno možemo pošto se svaka eliptička krivulja nad poljem karakteristike $\neq 2, 3$ može zapisati u kratkoj Weierstrassovoj formi.

$$\text{Ako } a, b \neq 0,\ a' = u^4a,\ b' = u^6b, u \in \overline{k}^*, \iff \sqrt[4]{a/a'} = \sqrt[6]{b/b'} \iff$$

$$(a'/a)^3 = (b'/b)^2 \iff \frac{4a^3 + 27b^2}{a^3} = \frac{4a'^3 + 27b'^2}{a'^3} \iff j(E) = j(E').$$

Ako je $a = 0$, tada je $a' = 0$ i $b, b' \neq 0$, pa dobivamo izomorfizam uzimanjem $u = \sqrt[6]{b'/b}$. Ako je $b = 0$, tada je $b' = 0$, te $a, a' \neq 0$. Dobivamo izomorfizam uzimanjem $u = \sqrt[4]{a'/a}$.

2. Za $j \neq 0, 1728$ eliptička krivulja

$$E : y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728}$$

ima

$$j(E) = j,\ \Delta(E) = \frac{j^2}{(j - 1728)^3}.$$

Za

$$E_1 : y^2 = x^3 + ax,\ j(E_1) = 1728,$$
$$E_2 : y^2 = x^3 + b,\ j(E_2) = 0.$$

□

**Korolar 10.** *Postoji bijekcija između $\{$eliptičke krivulje $/k$ do na $\overline{k}$-izomorfizam$\}$ i $k$.*

**Korolar 11.** *Grupa automorfizama eliptičke krivulje (nad $\overline{k}$)*

$$\operatorname{Aut} E = \{izomorfizmi : E \to E\}$$

*je*

$$\mathbb{Z}/2\mathbb{Z} \text{ za } y^2 = x^3 + ax + b, a, b \neq 0$$
$$\mathbb{Z}/4\mathbb{Z} \text{ za } y^2 = x^3 + ax,$$
$$\mathbb{Z}/6\mathbb{Z} \text{ za } y^2 = x^3 + b.$$

*Dokaz.* $\operatorname{Aut} E = \{u \in k^* : u^4 a = a,\ u^6 b = b\}$, pa slijedi da je

$$\operatorname{Aut} E = \langle -1 \rangle, \text{ ako } a, b \neq 0,$$
$$\operatorname{Aut} E = \langle i \rangle, \text{ ako } b = 0,$$
$$\operatorname{Aut} E = \langle \zeta_6 \rangle, \text{ ako } a = 0,$$

gdje je $\zeta_6$ primitivni šesti korijen iz jedinice (npr. $\frac{1-\sqrt{-3}}{2}$). □

# Poglavlje 5

# Izogenije

Pretpostavimo u ovom poglavlju da je $\operatorname{char} k \neq 2, 3$.

**Definicija. Izogenija** između dvije eliptičke krivulje je morfizam $\phi : E \to E'$ koji preslikava $\mathcal{O} \in E$ u $\mathcal{O}' \in E'$.

**Činjenica.** Svaka izogenija je homomorfizam grupa.

$[0] : E \to E$ je nul-izogenija. Definiraimo $\operatorname{st}[0] = 0$, tako da bi vrijedilo

$$\operatorname{st} \phi \circ \psi = \operatorname{st} \phi \operatorname{st} \cdot \psi$$

za sve izogenije $\phi : E \to E'$, $\psi : E' \to E$.

**Primjer 6.** Neka je $E : y^2 = x^3 + ax + b$. Promotrimo množenje s 2 na $E$, $[2] : E \to E$,

$$[2] : (x, y) \to \left( \frac{x^4 - 2ax^2 + a^2 - 8b}{4(x^3 + ax + b)}, \dots \right).$$

Preslikavanje [2] je definirano racionalnim funkcijama, te je $[2]\mathcal{O} = \mathcal{O}$, tako da je [2] izogenija.

**Primjer 7.** Množenje s $m$ na eliptičkoj krivulji $[m]$ je za svaki $m \geq 1$ izogenija.

Neka su $E_1$ i $E_2$ eliptičke krivulje. Tada je

$$\operatorname{Hom}(E_1, E_2) = \{izogenije : E_1 \to E_2\}$$

grupa uz operaciju zbrajanja.

Nadalje, $\operatorname{End} E = \operatorname{Hom}(E, E)$ je prsten s jedinicom (s operacijama zbrajanja i kompozicije) koji sadrži $\mathbb{Z}$, pošto je množenje s $m$ izogenija za svaki $m \in \mathbb{Z}$.

Zapravo, za eliptičke krivulje definirane nad poljima algebarskih brojeva, skoro uvijek će vrijediti $\operatorname{End} E = \mathbb{Z}$.

*Napomena.* Ako u subskriptu imamo polje, npr. $\operatorname{End}_k(E)$ ili $\operatorname{Hom}_k(E_1, E_2)$, tada to označava skup morfizama tog tipa nad $k$. Ako ne piše ništa u subskriptu, onda se uvijek misli na preslikavanja definirana nad $\overline{k}$.

**Primjer 8.** Neka je $E : y^2 = x^3 - x$, te $[i] \in \operatorname{End} E$, $[i] : (x, y) = (-x, iy)$. Primjetimo $[i]([i][-1]) = [1]$, te je $[i]$ automorfizam. Slijedi $\operatorname{End} E \supset \mathbb{Z}[i]$. Međutim, $\operatorname{End}_{\mathbb{Q}} E = \mathbb{Z}$.

Neka su $C$ i $D$ glatke projektivne krivulje. Sjetimo se da je stupanj nekog nekonstantnog racionalnog preslikavanja krivulja $\phi : C \to D$ jednak maksimalnom broju točaka $\in C$ u praslici od $\phi(P)$ za neki $P \in D$. Ako je preslikavanje stupnja $n$, tada će $|\phi^{-1}(P)| = n$ za sve osim konačno mnogo $P$-ova. Ako je $|\phi^{-1}(P)| < n$ tada je $\phi$ **razgranato** u $P$, ako je $|\phi^{-1}(P)| = n$ onda je **nerazgranato** u $P$.

Ako je $\phi : E_1 \to E_2$ ne-nul izogenija, tada je $\operatorname{Ker} \phi = \phi^{-1}(\mathcal{O})$ konačna podgrupa (od $E(\overline{k})$).

**Primjer 9.** Neka je $E : y^2 = (x - a_1)(x - a_2)(x - a_3), a_i \in \mathbb{Q}$, $T_i = (a_i, 0)$. Tada je

$$\operatorname{Ker}[2] = \{\mathcal{O}, T_1, T_2, T_3\} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Neka je $E$ eliptička krivulja, $\mathcal{O} \neq P \in E$. Definiramo

$$\tau_P : E \to E,$$

$$\tau_P(Q) = P + Q$$

tj. $\tau_p$ je translacija s $P$. Preslikavanje $\tau_p$ je morfizam (ali nije homomorfizam grupa).

**Teorem 12.** *Neka su $E_1, E_2$ eliptičke krivulje nad poljem algebarskih brojeva $k$, te $\phi : E_1 \to E_2$ izogenija stupnja $n \neq 0$.*

1. *$\phi$ je nerazgranato preslikavanje, tj. $|\phi^{-1}(P)| = n$ za svaki $P \in D$.*
2. *Neka je $K_1 = \overline{k}(E_1)$, $K_2 = \phi^*(\overline{k}(E_2))$. Tada je $K_1$ Galoisovo proširenje od $K_2$, te je $\operatorname{Gal}(K_1/K_2) \simeq \operatorname{Ker} \phi$.*
3. *Ako je $\psi : E_1 \to E_3$ izogenija i $\operatorname{Ker} \psi \supset \operatorname{Ker} \phi$, tada postoji jedinstvena izogenija $\chi : E_2 \to E_3$ takva da je $\psi = \chi \circ \phi$.*

*Dokaz.* 1. Pošto je $\phi$ preslikavanje stupnja $n$, vrijedi da postoji točka $P \in E_2$, t.d. $|\phi^{-1}(P)| = n$. Definirajmo $\phi^{-1}(P) = \{Q_i, i = 1, \ldots, n\}$. Neka je sada $P'$ proizvoljna točka $\in E_2$, te neka je $Q' \in \phi^{-1}(P')$. Tada su $Q' + Q_i - Q_1$, $i = 1, \ldots n$ različite točke te pošto je $\phi$ homomorfizam grupa, vrijedi da je $\phi(Q' + Q_i - Q_1) = P$, $i = 1, \ldots n$.

2. Neka je $\Phi = \operatorname{Ker} \phi = \{T_1, \ldots, T_n\}$. Promotrimo $\tau_{T_i} : E_1 \to E_1$. To preslikavanje je izomorfizam, pa inducira automorfizam $\tau^*_{T_i}$ funkcijskog polja $K_1$. Neka je $P \in E_1$, te neka je $\phi^* f \in K_2$. Tada je

$$\tau^*_{T_i}\phi^* f(P) = (\phi^* f)\tau_{T_i}(P) = f(\phi(P + T_i)) = f(\phi(P) + \phi(T_i)) = f\phi(P) =$$

$$= \phi^* f(P).$$

Slijedi da je $\tau^*_{T_i}$ automorfizam od $K_1$ koji fiksira $K_2$, tj. $|Aut(K_1/K_2)| \geq n$. Pošto je $[K_1 : K_2] = n$ slijedi da je $|Aut(K_1/K_2)| = n$, te $K_1/K_2$ Galoisovo, te

$$\mathrm{Gal}(K_1/K_2) \simeq \mathrm{Ker}\,\phi.$$

Primjetimo da slijedi i da će $\mathrm{Gal}(K_1/K_2)$ biti Abelova grupa.

3. Neka je $K_3 = \psi^*\overline{k}(E_3)$. Tada je kao i prije $K_3$ fiksiran sa svim $\mathrm{Gal}(K_1/K_3) = \{\tau^*_P : P \in \mathrm{Ker}\,\psi\} \leq \{\tau^*_P : P \in \mathrm{Ker}\,\phi\} = \mathrm{Gal}(K_1/K_2)$. Po Fundamentalnom teoremu Galoisove teorije

$$K_3 = K_1^{\mathrm{Gal}(K_1/K_3)} \subset K_1^{\mathrm{Gal}(K_1/K_2)} = K_2,$$

tj. $K_3$ je potpolje od $K_2$. Dakle, postoji jedinstveni $\chi : E_2 \to E_3$ koji inducira ovu inkluziju funkcijskih polja. Pošto je (po konstrukciji koju smo upravo napravili) $\phi^*(\chi^* K_3) = \psi^* K_3$, vrijedi $\psi = \chi\phi$. Da bi završili dokaz da je ovo izogenija, treba primjetiti

$$\chi(\mathcal{O}) = \chi(\phi(\mathcal{O})) = \psi(\mathcal{O}) = \mathcal{O}.$$

□

Na sličan način uz korištenje Riemann-Hurwitzove formule za genus, dobiva se sljedeća važna činjenica.

**Činjenica.** Ako je $\Phi$ podgrupa od $E$, tada postoji jedinstvena eliptička krivulja $E'$ i izogenija

$$\phi : E \to E'$$

takva da je $\ker\phi = \Phi$.

# Poglavlje 6

# Eliptičke krivulje nad $\mathbb{C}$

Sjetimo se da kažemo da je kompleksna funkcija $f$ **meromorfna** ako je holomorfna osim na skupu izoliranih točaka, u kojima ima polove. U ovom poglavlju ćemo također izreći neke tvrdnje bez dokaza (pogledajte [14] za detalje).

**Definicija.** Rešetka $\Lambda \subset \mathbb{C}$ je diskretna podgrupa ranga 2, tj.

$$\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2,\ w_1, w_2 \in \mathbb{C},$$

takva da su $w_1$ i $w_2$ linearno nezavisni nad $\mathbb{R}$.

Baza $w_1, w_2$ je jedinstvena do na $\mathrm{GL}_2(\mathbb{Z})$.

**Definicija. Eliptička funkcija** (s obzirom na $\Lambda$) je meromorfna funkcija $f$ za koju vrijedi

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

**Definicija. Fundamentalni paralelogram** za $\Lambda$ je skup

$$D = \{a + t_1 w_1 + t_2 w_2 : 0 \leq t_1, t_2 < 1\},$$

gdje je $a \in \mathbb{C}$, te su $w_1, w_2$ baza za $\Lambda$.

**Propozicija 13.** *Eliptička funkcija koja nema nultočke ili nema polove je konstanta.*

*Dokaz.* Pretpostavimo da je $f$ holomorfna. Pošto je $f$ eliptička vrijedi da je

$$\sup_{z \in \mathbb{C}} |f(z)| = \sup_{z \in \overline{D}} |f(z)|,$$

pa pošto je $f$ neprekidna i $\overline{D}$ je kompaktan skup slijedi da je $\sup_{z\in\mathbb{C}} |f(z)|$ omeđen, pa je po Liouvilleovom teoremu $f$ konstanta. Ako $f$ nema nultočaka, isti argument za $1/f$ dokazuje tvrdnju. □

**Definicija. Eisensteinov red** težine $2k$ s obzirom na $\Lambda$ je

$$G_{2k} = G_{2k(\Lambda)} = \sum_{w \in \Lambda \setminus \{0\}} w^{-2k}, \quad k \geq 2.$$

**Teorem 14.** *Postoji jedinstvena eliptička funkcija $\wp(z)$ (s obzirom na fiksiranu rešetku $\Lambda$) takva da je*

$$\wp(z) = \frac{1}{z^2} + O(z) \text{ oko } z = 0.$$

*Funkcija $\wp$ je holomorfna na $\mathbb{C}\setminus\Lambda$.*

Točnije, vrijedi

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

Funkcija $\wp(z)$ se zove "Weierstrasssova p-funkcija".

**Teorem 15.** *Napišimo $g_2 = g_2(\Lambda) = 60G_4$ i $g_3 = g_3(\Lambda) = 140G_6$. Tada je $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$.*

*Dokaz.* Vrijedi (oko $z = 0$)

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + \cdots$$

$$\wp(z)^3 = \frac{1}{z^6} + 9G_4 \frac{1}{z^2} + 15G_6 + \cdots$$

$$\wp'(z)^2 = \frac{1}{4z^6} - 14G_4 \frac{1}{z^2} - 80G_6 + \cdots$$

pa je $\wp'(z)^2 - (4\wp(z)^3 - g_2\wp(z) - g_3)$ funkcija koja je holomorfna u 0, pa pošto je eliptička, onda je holomorfna i na $\Lambda$. Također iz prošlog teorema znamo da je holorfna na $\mathbb{C}\setminus\Lambda$. Po Liouvilleovom teoremu slijedi da je funkcija 0. □

**Definicija.** Neka je $\Lambda$ rešetka. Tada definiramo

$$E_\Lambda : y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda).$$

**Teorem 16.** *Preslikavanje*

$$\phi : \mathbb{C}/\Lambda \to E_\Lambda, \quad z \to (\wp(z), \wp'(z))$$

*je izomorfizam (kompleksnih Liejevih) grupa.*

*Napomena.* Točnije, izomorfizam je $z \to (\wp(z) : \wp'(z) : 1) \in \mathbb{P}^2(\mathbb{C})$ za $z \neq 0 \in \mathbb{C}/\Lambda$, te $\Lambda \to (0 : 1 : 0)$.

*Napomena.* Vrijedi i obrat teorema 16, tj, svaka eliptička krivulja nad $\mathbb{C}$ je izomorfna $\mathbb{C}/\Lambda$, za neku rešetku $\Lambda$.

**Definicija.** Neka je $E/k$ eliptička krivulja nad poljem algebarskih brojeva $k$. Tada je

$$E[m] = \mathrm{Ker}[m] = \{P \in E(\overline{k}) : mP = \mathcal{O}\},$$
$$E(k)[m] = \{P \in E(k) : mP = \mathcal{O}\}.$$

**Korolar 17.** *Vrijedi* $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$.

*Dokaz.* $E \simeq \mathbb{C}/\Lambda \simeq (\mathbb{R}/\mathbb{Z})^2$, pa vrijedi $E[m] \simeq (\frac{1}{m}\mathbb{Z}/\mathbb{Z})^2 \simeq (\mathbb{Z}/m\mathbb{Z})^2$. □

Sljedeće što nas zanima su izogenije

$$E = \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda' = E'$$

nad $\mathbb{C}$.

Ako je $\alpha \in \mathbb{C}$ takav da $\alpha\Lambda \subset \Lambda'$, tada je

$$\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda', z \to \alpha z$$

dobro definirano, holomorfno preslikavanje $E \to E'$ takvo da je $\mathcal{O} \to \mathcal{O}$, dano sa

$$\phi_\alpha : (\wp_\Lambda(z), \wp'_\Lambda(z)) \to (\wp_{\Lambda'}(\alpha z), \wp'_{\Lambda'}(\alpha z)).$$

Također, preslikavanje $z \to \wp_{\Lambda'}(\alpha z)$ je eliptičko s obzirom na $\Lambda$:

$$\wp_{\Lambda'}(\alpha(z+w)) = \wp_{\Lambda'}(\alpha z + \alpha w) = \wp_{\Lambda'}(\alpha z) \text{ za } w \in \Lambda,$$

jer je $\alpha w \in \Lambda$, dakle $z \to \wp_{\Lambda'}(\alpha z)$ je funkcija $\in \mathbb{C}(E)$. Isto se može dokazati i za $\wp'_{\Lambda'}(\alpha z)$.

Obrnuto, ako je $\phi : E \to E'$ holomorfno preslikavanje takvo da je $\phi(\mathcal{O}) = \mathcal{O}$, tada se $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ može "podignuti" ili proširiti do holomorfnog preslikavanja $f : \mathbb{C} \to \mathbb{C}$, takvo da je $f(0) = 0$.

Za svaki

$$w \in \Lambda, f(z+w) \equiv f(z) \pmod{\Lambda'},$$

tj. $f(z+w) - f(z)$ ne ovisi o $z$, tj. $(f(z+w) - f(z))' = 0$, odnosno

$$f'(z+w) = f'(z),\ \forall z \in \mathbb{C},\ \forall w \in \Lambda.$$

Dakle $f'$ je holomorfna eliptička funkcija, dakle kostanta je po Propoziciji 13. Slijedi da je $f(z) = \alpha z + \beta$, s tim da je $\beta = 0$ jer $f(0) = 0$.

Imamo i sljedeću lemu

**Lema 18.** *Neka su $E$ i $E'$ eliptičke krivulje koje odgovaraju rešetkama $\Lambda$ i $\Lambda'$. Tada postoji bijekcija*

$$\{\textit{izogenije } \phi : E \to E'\} \leftrightarrow \{\textit{holomorfna preslikavanja } \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'\}.$$

**Teorem 19.** *Postoji bijekcija između sljedećih skupova*

$$\{\textit{izogenije } \phi : E \to E'\} \leftrightarrow \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda'\}.$$

*Napomena.* Ako su elementi iz $\operatorname{Ker}\phi$ $\operatorname{Gal}(\overline{k}/k)$-invarijantni za neko PAB (polje algebarskih brojeva) $k$, tada $\phi$ mora biti definirana nad $k$.

**Definicija.** Rešetke $\Lambda$ i $\Lambda'$ su **homotetične** ako postoji $\alpha \in \mathbb{C}$ takav da $\alpha\Lambda = \Lambda'$.

**Korolar 20.** *$E \simeq E'$ ako i samo ako $\Lambda = \alpha\Lambda'$ za neki $\alpha \in \mathbb{C}^*$. Dakle, nad $\mathbb{C}$,*

$$\{\textit{eliptičke krivulje}/\simeq\} \leftrightarrow \{\textit{rešetke}/\textit{homotetija}\}.$$

Očito je svaka rešetka homotetična rešetci $\mathbb{Z} + \mathbb{Z}\tau$, za neki $\tau$ (npr. $\tau = w_2/w_1$). Izbor elementa $\tau$ je jedinstven do na djelovanje $\mathrm{SL}_2(\mathbb{Z})$ na bazu $\{1, \tau\}$. Npr. ako je $\{1, \tau\}$ baza za $\Lambda$, tada je i $\{1, 1+\tau\}$ također baza za rešetku $\Lambda$.

**Definicija.** Neka je $k$ polje algebarskih brojeva. Tada je **red** $O$ od $k$ potprsten od $k$ koji je konačno generiran kao $\mathbb{Z}$-modul i zadovoljava $O \otimes \mathbb{Q} = k$.

**Teorem 21.** *Neka je $E/\mathbb{C}$ eliptička krivulja, te neka je $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$ rešetka koja odgovora krivulji $E$. Tada postoje 2 slučaja:*

1. $\operatorname{End} E = \mathbb{Z}$.
2. *$\mathbb{Q}(\tau)$ je kvadratno imaginarno proširenje od $\mathbb{Q}$, te je $\operatorname{End} E$ izomorfno redu od $\mathbb{Q}(\tau)$.*

*Dokaz.* Neka je $R = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$. Slijedi $R \simeq \operatorname{End} E$. Tada za svaki $\alpha \in R$, postoje $a, b, c, d \in \mathbb{Z}$ takvi da

$$\alpha 1 = a + b\tau \text{ i } \alpha\tau = c + d\tau. \tag{6.1}$$

Eliminirajući $\tau$ dobijemo

$$\alpha^2 - (a+d)\alpha + bc = 0.$$

Dakle, $\alpha$ je element prstena cijelih brojeva kvadratnog polja ili od $\mathbb{Q}$.

Pretpostavimo da je $R \neq \mathbb{Z}$ i neka je $\alpha \in R$, $\alpha \notin \mathbb{Z}$. Eliminirajući $\alpha$ iz (6.1) dobijemo ($b \neq 0$)

$$b\tau^2 - (a-d)\tau + c = 0.$$

Dakle $\mathbb{Q}(\tau)$ je kvadratno imaginarno polje. Konačno, pošto je $R$ sadržan u prstenu cijelih brojeva kvadratnog polja, slijedi da je $R$ red u $\mathbb{Q}(\tau)$. □

**Definicija.** Neka je $E/k$ eliptička krivulja nad poljem algebarskih brojeva $k$. Ako je $\operatorname{End} E \supsetneq \mathbb{Z}$ tada kažemo da $E$ ima **kompleksno množenje**.

# Poglavlje 7

# Dualna izogenija

**Definicija.** Dvije krivulje $E_1$ i $E_2$ su izogene (nad $k$) ako postoji izogenija $0 \neq \phi : E_1 \to E_2$ (definirana nad $k$).

**Propozicija 22.** *Ako je $\phi : E_1 \to E_2$ izogenija stupnja $m \neq 0$, tada postoji jedinstvena izogenija $\widehat{\phi} : E_2 \to E_1$ takva da je $\widehat{\phi}\phi = [m]$. $\widehat{\phi}$ se zove **dualna izogenija**.*

*Dokaz.* Pošto po Teoremu 12, 1. vrijedi $|\operatorname{Ker}\phi| = m$, slijedi po Korolaru 17 da $\operatorname{Ker}\phi \subset \operatorname{Ker}[m]$, pa nadalje po Teoremu 12, 3. postoji preslikavanje $\widehat{\phi} : E_2 \to E_1$ takvo da je $\widehat{\phi}\phi = [m]$.

Da bi dokazali jedinstvenost, pretpostavimo da je $\psi$ neko drugo takvo preslikavanje; slijedi da je $\psi\phi = \widehat{\phi}\phi$, pa je $(\psi - \widehat{\phi})\phi = [0]$, te pošto je $\phi \neq 0$ slijedi (pošto $\operatorname{End}(E)$ nema torzije) da je $\psi = \widehat{\phi}$. □

**Korolar 23.** *Biti izogen je relacija ekvivalencije, tj. postoje klase izogenija eliptičkih krivulja.*

Sljedeći teorem nam daje neka svojstva dualne izogenije

**Teorem 24.** *Neka je $\phi : E_1 \to E_2$ izogenija. Tada vrijedi sljedeće:*

1. $\widehat{\phi}\phi = [m]$ *na* $E_1$ *i* $\phi\widehat{\phi}$ *na* $E_2$
2. $\widehat{\chi \circ \phi} = \widehat{\phi} \circ \widehat{\chi}$ *za sve* $\chi : E_2 \to E_3$.
3. $\widehat{[m]} = [m]$.
4. $\operatorname{st}\widehat{\phi} = \operatorname{st}\phi$.
5. $\widehat{\widehat{\phi}} = \phi$.

Neka je $P \in E, \sigma \in \operatorname{Gal}(\overline{k}/k)$. Tada pišemo $P^\sigma = (x^\sigma, y^\sigma) = (\sigma(x), \sigma(y))$.

**Činjenica.** Neka je $\phi$ izogenija definirana nad $k$, te neka je $\sigma \in \mathrm{Gal}(\overline{k}/k)$. Tada $\sigma$ permutira $\mathrm{Ker}\,\phi$.

**Primjer 10** (2-izogenija)**.** Dokažimo da ako $E_1$ ima 2-izogeniju nad $k$ (tj. koeficijenti su definirani nad $k$) na drugu eliptičku krivulju, tada $E$ ima točku reda 2. Neka je $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Tada $\sigma$ permutira $\mathrm{Ker}\,\phi = \{\mathcal{O}, T\}$. Pošto je $\mathcal{O}$ racionalna točka, tada je $\mathcal{O}^\sigma = \mathcal{O}$. Pošto je $\sigma$ permutacija od $\mathrm{Ker}\,\phi$, slijedi da je $T^\sigma = T$. Pošto to vrijedi za svaki $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, slijedi da je $T \in E(k)$.

Neka je $E_1/k$ eliptička krivulja nad poljem algebarskih brojeva, te neka je $\phi : E_1 \to E_2$ 2-izogenija (tj. izogenija stupnja 2), gdje su

$$E_1 : y^2 = x^3 + ax^2 + bx,$$

$$E_2 : Y^2 = X^3 - 2aX^2 + rX,$$

gdje je $r = a^2 - 4ab \neq 0$. Tada je

$$\phi : E_1 \to E_2, \quad \phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(b-x)}{x^2}\right), \text{ ako } x \neq 0, \ \phi(0,0) = \mathcal{O},$$

$$\widehat{\phi} : E_2 \to E_1, \quad \widehat{\phi}(X,Y) = \left(\frac{Y^2}{4X^2}, \frac{Y(r-X^2)}{8X^2}\right), \text{ ako } X \neq 0, \ \widehat{\phi}(0,0) = \mathcal{O}.$$

# Poglavlje 8

# Eliptičke krivulje nad $\mathbb{F}_p$ i računanje torzijskih točaka

"Redukcija modulo $p$" (homomorfizam $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$) je jedan od osnovnih alata u teoriji brojeva. Prednosti projektivnog prostora je da se cijeli prostor $\mathbb{P}^n(\mathbb{Q})$ može reducirati u $\mathbb{P}^n(\mathbb{F}_p)$. Ideja - eliptičke krivulje reduciramo mod $p$ tako da reduciramo mod $p$ njezine koeficijente.

Pretpostavimo da imamo eliptičku krivulju $E$ nad $\mathbb{Q}$. Da bi reducirali eliptičke krivulje modulo $p$, prvo treba dovesti eliptičku krivulju u pogodan oblik za to. Prvo primjetimo da je svaka eliptička krivulja nad $\mathbb{Q}$ izomorfna nekoj eliptičkoj krivulji nad $\mathbb{Q}$ oblika

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}.$$

To se lako vidi jer ako krenemo od $Y^2 = X^3 + a'X + b'$, tada možemo uzeti da je $u$ najmanji zajednički višekratnik od nazivnika od $a'$ i $b'$, te uz $a = u^4a'$, $b = u^6b'$ imamo da je naša početna jednadžba izomorfna nekoj sa cjelobrojnim koeficijentima.

Međutim, postoji puno izomorfnih eliptičkih krivulja s cjelobrojnim koeficijentima, te njihove redukcije nisu nužno iste. Npr.

$$E_1 : y^2 = x^3 + x + 1, \quad \text{i}$$

$$E_2 : y^2 = x^2 + 81x + 729$$

su izomorfne nad $\mathbb{Q}$, međutim njihove redukcije mod 3 su

$$\overline{E}_1 : y^2 = x^3 + x + 1$$

$$\overline{E}_2 : y^2 = x^3,$$

gdje prva jednadžba opisuje eliptičku krivulju, a druga ne (singularna je). Primjetimo

$$\Delta(E_1) = 2^4 \cdot 31, \quad \Delta(E_2) = 2^4 \cdot 3^{12} \cdot 31.$$

Dakle, $\Delta(E_1) \equiv 1 \pmod 3$, a $\Delta(E_2) \equiv 0 \pmod 3$, pa $\overline{E}_2$ nije eliptička krivulja nad $\mathbb{F}_3$.

Dakle, da bi smisleno reducirali eliptičku krivulju, treba izabrati *minimalni* model u klasi izomorfizma eliptičke krivulje nad $\mathbb{Q}$.

**Definicija.** Kažemo da je model od $E/\mathbb{Q}$

$$E : y^2 + a_1xy + a_3y = x^3 + a_4x^2 + a_4x + a_6,$$

**minimalan**, ako su $a_i \in \mathbb{Z}$ i ako je $|\Delta(E)|$ minimalan u klasi izomorfizma od $E$.

**Definicija.** Neka je $n \in \mathbb{Z}$, te zapišimo $n = p^k \cdot m$, gdje $(p, m) = 1$, $k \geq 0$. Tada je **$p$-adska valuacija** od $n$, $\nu_p(n) = k$. Tj. $p$-adska valuacija od $n$ je najveća potencija od $p$ koja dijeli $n$.

**Propozicija 25.** *Neka je*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}.$$

*Ako je* $0 \leq \nu_p(\Delta(E)) < 12$*, za sve proste brojeve* $p$*, tada je* $E$ *minimalan model.*

*Dokaz.* Kada bi postojao izomorfizam $E \to E'$ za neki drugi model $E'$, tada bi bilo $\Delta(E') = u^{12}\Delta(E)$ za neki $u \in \mathbb{Q}^*$. Pošto je po pretpostavci $\nu_p(\Delta(E)) < 12$ za sve proste brojeve $p$, te $\Delta(E')$ mora biti cjelobrojan, zaključujemo da $u \in \mathbb{Z}^*$. Dakle $|\Delta(E')| \geq |\Delta(E)|$. □

*Napomena.* Postojanje minimalnog modela je jedno od rijetkih svojstava eliptičkih krivulja koje se ne prenosi iz $\mathbb{Q}$ u polja algebarskih brojeva, tj. u pravilu nad poljima algebarskih brojeva ne postoji minimalni model. To je posljedica toga da prstenovi cijelih brojeva PAB nisu domene jedinstvene faktorizacije (ili ekvivalentno domene glavnih ideala).

Do kraja poglavlja pretpostavljamo da je $E/\mathbb{Q}$ zadana u minimalnom modelu.

**Definicija.** Neka je $E/\mathbb{Q}$ zadana sa (minimalnim modelom)

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}.$$

Tada, definiramo $\overline{E}/\mathbb{F}_p$ kao

$$\overline{E} : y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6,$$

gdje su $\overline{a}_i$ slike od $a_i$ od homomorfizma $\mathbb{Z} \to \mathbb{F}_p$ redukcija mod $p$.

Primjetimo da je $\overline{E}$ eliptička krivulja $\iff \Delta(\overline{E}) \neq 0$ (u $\mathbb{F}_p$) $\iff p \nmid \Delta(E)$.

**Definicija.** Ako $p \nmid \Delta(E)$, tj. da je redukcija mod $p$ od $E$ eliptička krivulja, tada kažemo da $E$ ima **dobru redukciju u** $p$. Ako $E$ nema dobru redukciju u $p$, tada ima **lošu redukciju** u $p$.

Ima više vrsta loše redukcije. Neka je eliptička krivulja zadana modelom $E : y^2 = f(x)$, gdje je $f$ polinom stupnja 3, te neka je $\overline{E} : y^2 = \overline{f}(x)$, gdje je $\overline{f} \in \mathbb{F}_p[x]$ polinom $f$ modulo $p$ (sve koeficijente reduciramo modulo $p$). Tada $E$ ima lošu redukciju ako i samo ako $\overline{f}$ ima višestruki korijen. Ako $\overline{f}$ ima dvostruki korijen, tada $E$ ima **multiplikativnu redukciju** u $p$. Dakle $\overline{E}$ ima model $y^2 = x^2(x + a)$. Ako je $a$ kvadratni ostatak modulo $p$, tad kažemo da $E$ ima **rascjepibu multiplikativnu redukciju**, a inače kažemo da ima **nerascjepivu multiplikativnu redukciju**.

Ako $\overline{f}$ ima trostruki korijen, tada kažemo da $E$ ima **aditivnu redukciju** modulo $p$.

*Napomena.* Pošto diskriminanta eliptičke krivulje ima samo konačno mnogo prostih faktora, slijedi da svaka eliptička krivulja ima lošu redukciju u samo konačno mnogo $p$-ova.

**Primjer 11.** Neka je $E : y^2 = x^3 - x^2 - 86x + 240$. Vrijedi $\Delta(E) = -2^6 3^4 5^2 13^2$, dakle $E$ ima lošu redukciju u $2, 3, 5, 13$. Redukcija mod 3 je

$$y^2 = x^3 - x^2 + x = x(x + 1)^2.$$

Promjenom varijabli $x \to x - 1$ dobivamo

$$y^2 = x^2(x + 2),$$

te pošto 2 nije kvadratni ostatak modulo 3, $E$ ima nerascjepivu multiplikativnu redukciju mod 3.

**Propozicija 26.** *Neka je $E$ eliptička krivulja s dobrom redukcijom u $p$. Tada je redukcija mod $p$,*

$$E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$$
$$P = (x : y : z) \in \mathbb{P}^2(\mathbb{Z}) \to (\overline{x} : \overline{y} : \overline{z}) \in \mathbb{P}^2(\mathbb{F}_p)$$

*homomorfizam grupa.*

U prethodnoj propoziciji uzimamo točku $P = (x : y : z)$ takvu da su $x, y, z \in \mathbb{Z}$, da je barem jedan $\neq 0$, te da nisu svi djeljivi s $p$.

Zbog jednostavnost ćemo za grupu točaka redukciju mod $p$ neke $E/\mathbb{Q}$ pisati $E(\mathbb{F}_p)$ umjesto $\overline{E}(\mathbb{F}_p)$.

*Napomena.* Redukcija modulo $p$ preslikava $\mathcal{O} \in E(\mathbb{Q})$ u $\mathcal{O} \in E(\mathbb{F}_p)$.

*Napomena.* Grupovni zakon nad $\mathbb{F}_p$ je potpuno jednak kao nad $\mathbb{Q}$ - koristimo iste formule, samo sve reduciramo mod $p$. Pošto nad $\mathbb{F}_2$ i $\mathbb{F}_3$ nekad treba koristiti dugu Weierstrassovu formu, grupovni zakon ima drukčije jednadžbe - one se mogu naći u [14, p. 58-59].

**Propozicija 27.** *Neka je $E$ eliptička krivulja s dobrom redukcijom u $p$. Tada je redukcija mod $p$ injekcija na $p$-slobodnom dijelu torzije od $E(\mathbb{Q})$, tj. podgrupi točaka čiji red je relativno prost s $p$.*

Prethodna propozicija nam zapravo daje postupak za računanje torzije eliptičkih krivulja - ovaj postupak je često vrlo efikasan.

Kako odrediti $E(\mathbb{F}_p)$? Vrijedi

$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2$ koji zadovoljavaju jednadžbu eliptičke krivulje $\overline{E}\} \cup \{\mathcal{O}\}$.

**Primjer 12.** Neka je $E : y^2 = x^3 - x$. Diskriminanta $\Delta(E) = 64$, dakle ovo je minimalni model za ovu eliptičku krivulju, te $E$ ima dobru redukciju u svim $p \neq 2$. Također, primjetimo da su $(0, 0),\ (1, 0), (-1, 0)$, racionalne točke reda 2. Dakle, sve točke reda 2 od $E$ su definirane nad $\mathbb{Q}$, tj.

$$E(\mathbb{Q})[2] = E[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Nađimo $E(\mathbb{F}_3)$. Uvrštavanjem redom $x = 0, 1, 2$ dobivamo točke (nad $\mathbb{F}_3$)

$$(0, 0), (1, 0), (2, 0),$$

tako da je

$$E(\mathbb{F}_3) = \{\mathcal{O}, (0, 0), (1, 0), (2, 0)\},$$

pa pošto je 3-slobodni dio od $E(\mathbb{Q})_{tors}$ injektivno ulazi u $E(\mathbb{F}_3)$. Zaključujemo $E(\mathbb{F}_3) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, te po Mazurovom teoremu,

$$E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \text{ ili } \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Uvrštavanjem redom $x = 0, 1, 2, 3, 4$ dobivamo

$$E(\mathbb{F}_5) = \{\mathcal{O}, (0, 0), (1, 0), (2, 1), (2, 4), (3, 2), (3, 2), (4, 0)\}.$$

Pošto je $|E(\mathbb{F}_5)| = 8$, te $E(\mathbb{Q})[3]$ injektivno ulazi u $E(\mathbb{F}_5)$, slijedi da je

$$E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Iako je metoda koju smo sada demonstrirali u praksi vrlo djelotvorna, ona nam ne daje algoritam. Sljedeći teorem nam daje algoritam za računanje torzije eliptičke krivulje nad $\mathbb{Q}$.

**Teorem 28** (Lutz-Nagell)**.** *Neka je*

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z},$$

*te neka je $\mathcal{O} \neq P \in E(\mathbb{Q})$ točka konačnog reda (torzijska točka). Tada je*

1. $x(P), y(P) \in \mathbb{Z}$.
2. $y(P) = 0$ *ili* $y(P)^2 | 4a^3 + 27b^2 = \frac{-\Delta(E)}{16}$.

Lutz-Nagellov teorem nam pokazuje da imamo samo konačno mnogo kandidata $y$ za provjeriti za torzijske točke.

**Primjer 13.** Neka je

$$E : y^2 = x^3 - 4x + 4.$$

Odredimo $E(\mathbb{Q})_{tors}$. Vrijedi $\Delta(E) = -2816 = -2^8 \cdot 11$. Po Lutz-Nagellovom teoremu ako je $P = (x, y)$ točka konačnog reda, tada $y = 0$ ili $y^2 | \frac{\Delta(E)}{16}$, tj. jedine mogućnosti su $\pm y = 0, 1, 2, 4$. Uvrštavanjem $y = 0$ dobijemo $x^3 - 4x + 4 = 0$, što nema racionalna rješenja. Za $y = 1$ dobijemo $x = 1$. Promotrimo kojeg je reda $Q = (1, 1)$. Računamo

$$2Q = Q + Q = \left(\frac{-7}{4}, \frac{-19}{8}\right).$$

Kad bi $Q$ bio konačnog reda, tada bi morao biti i $2Q$, međutim pošto $2Q$ nema cjelobrojne koordinate, pa po Lutz-Nagellovom teoremu slijedi da je $2Q$, pa onda i $Q$ beskonačnog reda. Primjetimo da $(1, -1) = -Q$, pa je i $(1, -1)$ beskonačnog reda. Za $y = \pm 4$, dobivamo da je $x^3 - 4x + 4 - y^2$ ireducibilan, tako da $y = \pm 4$ ne daje točke na $E(\mathbb{Q})$. Neka je $y = \pm 2$ sada slijedi da može biti $x = 0, \pm 2$. Neka je $R = (2, 2)$. Sada je $2R = (0, 2)$, te $-R = (2, -2)$. Dakle samo treba provjeriti je li $R$ konačnog ili beskonačnog reda. Računamo da je $4R = (1, -1) = -Q$, što smo već pokazali da je beskonačnog reda. Dakle $E(\mathbb{Q})$ ima trivijalnu torziju.

Može se pokazati da je $E(\mathbb{Q}) \simeq \mathbb{Z}$, te $E(\mathbb{Q}) = \langle (2, 2) \rangle$.

**Primjer 14.** Neka je $E : y^2 = x^3 + 4$. Vrijedi $\Delta(E) = -2^8 \cdot 3^3$. Ako je $P = (x, y)$ točka konačnog reda, slijedi $\pm y = 0, 1, 2, 4, 3, 6, 12$. Za $y = 0, \pm 1, \pm 4, \pm 3, \pm 6, \pm 12$, lako vidimo da je $x^3 + 4 - y^2$ ireducibilan nad $\mathbb{Q}$. Za $y = 2$ dobivamo točku $Q = (0, 2)$. Računamo $2Q = (0, -2) = -Q$. Slijedi da je $3Q = Q + 2Q = Q - Q = \mathcal{O}$, dakle $\mathbb{Q}$ je točka reda 3 i to iscrpljuje moguće $y$-eve iz Lutz-Nagellovog Teorema.

Štoviše, može se pokazati da je $E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, $E(\mathbb{Q}) = \langle (0, 2) \rangle$.

Koliki može biti $|E(\mathbb{F}_p)|$? Lako vidimo da ako je $E : y^2 = x^3 + ax + b$, tada za svaki $x \in \mathbb{F}_p$, imamo 0 točaka ako $x^3 + ax + b$ nije kvadratni ostatak modulo $p$, 1 točku ako je $x^3 + ax + b$ djeljivo s $p$, te 2 točke ako je $x^3 + ax + b$ kvadratni ostatak modulo $p$ (i nije djeljivo s $p$). Dakle,

$$|E(\mathbb{F}_p)| = 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p}\right),$$

gdje 1 dolazi od točke $\mathcal{O}$. Heuristički očekujemo da će za pola $x$-eva $x^3 + ax + b$ biti kvadratni ostatak modulo $p$, a da pola neće biti kvadratni ostatci modulo $p$. Dakle očekujemo da će u prosjeku biti $|E(\mathbb{F}_p)| = 2 \cdot \frac{p}{2} + 0 \cdot \frac{p}{2} + 1 = p + 1$.

Sljedeći teorem nam kaže da $|E(\mathbb{F}_p)|$ ne može biti previše daleko od $p + 1$.

**Teorem 29** (Hasse)**.** *Neka je $E/\mathbb{F}_q$ eliptička krivulja nad konačnim poljem $\mathbb{F}_q$. Tada je*

$$||E(\mathbb{F}_q)| - (q + 1)| \leq 2\sqrt{q}.$$

Vrijedi i generalizacija, koju je dokazao Weil

**Teorem 30** (Hasse-Weil)**.** *Neka je $C$ nesingularna krivulja genusa $g$ nad $\mathbb{F}_q$, tada je*

$$||E(\mathbb{F}_q)| - (q+1)| \leq 2g\sqrt{q}.$$

# Poglavlje 9

# Polja algebarskih brojeva

U ovom poglavlju ćemo ponoviti neke činjenice iz algebarske teorije brojeva koje ćemo dalje korisiti. Samo ćemo izreći činjenice, bez dokaza i to dosta šturo. Za više detalja, može se pogledati [8] ili još bolje [15].

Ranije smo već spomenuli da su polja algebarskih brojeva konačna proširenja od $\mathbb{Q}$. Svako PAB je izomorfno s $\mathbb{Q}[x]/(f)$, gdje je $f$ ireducibilan polinom iz $\mathbb{Q}[x]$, te je stupanj od $f$ jednak stupnju od $K$.

Neka je $\phi : K \to K'$ homomorfizam PAB. Tada $\phi$ mora fiksirati $\mathbb{Z}$ zbog aditivnosti, te onda i $\mathbb{Q}$ zbog multiplikativnosti. Također, sjetimo se da homomorfizam između polja mora biti injekcija. Homomorfizme polja zovemo ulaganjima.

**Definicija.** Neka su $\alpha_i$, algebarski brojevi stupnja $n_i$, $i = 1, \ldots, k$. Tada označavamo s

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_k) = \{\sum_j (c_j \prod_{i=1}^{k} \alpha_i^{t_i}), 0 \leq t_i \leq n_i - 1,\ c_j \in \mathbb{Q}\}$$

najmanje polje koje sadrži $\mathbb{Q}$ i $\alpha_1, \ldots, \alpha_k$.

Po teoremu o primitivnom elementu, svako PAB $K$ se može generirati jednim elementom (tzv. primitivnim elementom), tj. oblika je

$$K = \mathbb{Q}(\alpha) = \{\sum_{i=0}^{n-1} c_i \alpha^i,\ c_i \in \mathbb{Q}\},$$

gdje je $n$ stupanj od $K$.

Nama će biti zgodnije promatrati PAB kao potpolja od $\mathbb{C}$ nego kao $\mathbb{Q}[x]/(f)$.

**Propozicija 31.** *PAB stupnja $n$ ima $n$ ulaganja u $\mathbb{C}$.*

Međutim neće slika ulaganja $\mathbb{Q}[x]/(f)$ u $\mathbb{C}$ uvijek biti neovisna o ulaganju.

**Primjer 15.** Promotrimo polje $\mathbb{Q}[x]/(x^2-2)$. Tada postoje 2 ulaganja tog polja u $\mathbb{C}$, $x \to \sqrt{2}$ i $x \to -\sqrt{2}$, gdje je $\sqrt{2}$ pozitivni korijen iz 2. Slika od $\mathbb{Q}[x]/(x^2-2)$ je u oba slučaja

$$\{a + b\sqrt{2},\ a, b \in \mathbb{Q}\},$$

tj. $\mathbb{Q}(\sqrt{2})$.

Međutim, ako promotrimo ulaganja od $\mathbb{Q}[x]/(x^3-2)$, tada postoje 3 ulaganja u $\mathbb{C}$, gdje se $x$ može preslikavati u $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$ ili $\zeta^2\sqrt[3]{2}$, gdje je $\zeta$ neki fiksni treći korijen iz 1. U ovom slučaju slike ulaganja su 3 različita polja - jedno je potpolje od $\mathbb{R}$, dok druga dva nisu.

Ako je ulaganje PAB potpolje od $\mathbb{R}$, tada kažemo da je to ulaganje realno, u suprotnom kažemo da je ulaganje kompleksno.

Npr. kvadratno polje $\mathbb{Q}(\sqrt{d})$ ima 2 realna ulaganja ako je $d > 0$, te 2 kompleksna ulaganja ako je $d < 0$. Polje $\mathbb{Q}[x]/(x^3-2)$ ima 1 realno i 2 kompleksna ulaganja.

Ako su sva ulaganja od PAB realna, tada kažemo da je PAB **potpuno realno polje**. Ako su sva ulaganja od PAB kompleksna, tada kažemo da je $PAB$ **potpuno kompleksno polje**.

**Činjenica.** Sva ulaganja PAB daju isto potpolje od $\mathbb{C}$ ako i samo ako je $K$ Galoisovo proširenje od $\mathbb{Q}$.

Kada je $K$ Galoisovo proširenje od $\mathbb{Q}$, tada možemo jednoznačno opisati $K$ kao potpolje od $\mathbb{C}$ zadano nekim polinomom.

Neka je $\alpha$ proizvoljan element od PAB $K$ s minimalnim polinomom $f \in \mathbb{Q}[x]$ stupnja $d$. Tada definiramo da su $d$ korijena od $f$ **konjugati od** $\alpha$.

Neka je $K$ Galoisovo proširenje od $\mathbb{Q}$, te neka su $\sigma_i,\ i = 1, \ldots, n$ ulaganja od $K$ u $\mathbb{C}$. Tada $\sigma_i$ induciraju $n$ automorfizama od $K$ (točnije, ti automorfizmi su definirani s $\sigma_1^{-1} \circ \sigma_i$), tj. $\mathrm{Gal}(K/\mathbb{Q})$. **Trag** nekog elementa $\alpha \in K$, $Tr_{K/\mathbb{Q}}(\alpha)$ je

$$Tr_{K/\mathbb{Q}} = \sum_{i=1}^{n} \sigma_i(\alpha).$$

**Norma** nekog elementa $\alpha \in K$, $N_{K/\mathbb{Q}}(\alpha)$ je

$$N_{K/\mathbb{Q}} = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Prsten cijelih brojeva $O_K$ nekog PAB $K$ je skup elemenata iz $K$ čiji minimalni polinom (tj. normirani polinom najmanjeg stupnja koji poništava element) ima cjelobrojne koeficijente. **Diskriminanta** polja $\Delta_K$ se definira na sljedeći način: uzmimo bazu $\{b_1, \ldots, b_n\}$ za $O_K$ (kao $\mathbb{Z}$-modul) te je tada

$$\Delta_K = \det \begin{pmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \cdots & \sigma_1(b_n) \\ \sigma_2(b_1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_n(b_1) & \cdots & \cdots & \sigma_n(b_n) \end{pmatrix},$$

Napomenimo da postoje različita (neizomorfna) polja algebarskih brojeva s istim diskriminantama (i istim stupnjem). Npr. postoje 2 kubna polja s diskriminantom -1836, te 3 s diskriminantom -1228.

## 9.1 Kvadratna polja

Kvadratna polja su proširenja od $\mathbb{Q}$ stupnja 2. Svako kvadratno polje $K$ je Galoisovo s $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.

**Činjenica.** Svako kvadratno polje se može zapisati u obliku $\mathbb{Q}(\sqrt{d})$, gdje je $d$ neki kvadratno slobodan cijeli broj.

**Činjenica.** $O_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{d}] & \text{inače} \end{cases}$

**Činjenica.** $\Delta_{\mathbb{Q}(\sqrt{d})} = \begin{cases} d & d \equiv 1 \pmod 4 \\ 4d & \text{inače} \end{cases}$

Za kvadratna polja, diskriminanta jednoznačno određuje kvadratno polje.

## 9.2 Kubna polja

Za razliku od kvadratnih polja, kubna polja nisu uvijek Galoisova - vidjeli smo primjer $\mathbb{Q}(\sqrt[3]{2})$.

Kubna polja generirana s $\sqrt[3]{n}$, za neki prirodan broj $n$ se zovu **čista kubna polja**.

Neka je $f$ ireducibilan polinom koji generira kubno polje $K$. Ako su sva 3 korijena od $f$ realna, tada je $K$ **potpuno realno kubno polje**, a u suprotnom je **kompleksno kubno polje**. Ako su sva 3 korijena od $f$ u $K$, tada je $K$ Galoisovo proširenje od $\mathbb{Q}$ i kažemo da je $K$ **cikličko kubno polje**; naziv dolazi jer je $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$. Ako $K$ nije cikličko kubno polje, tada je Galoisovo zatvorenje od $K$ proširenje od $K$ s Galoisovom grupom $S_3$, koja nije ciklička.

Neka je $\Delta_K$ diskriminanta kubnog polja $K$. Tada će $\sqrt{\Delta_K}$ biti sadržan u Galoisovom zatvorenju od $K$, te je predznak od $\Delta_K$ jednak $(-1)^{r_2}$, gdje je $r_2$ broj parova kompleksnih ulaganja od $K$. Cikličko kubno polje mora nužno biti potpuno realno (u suprotnom bi kompleksna konjugacija, koja je automorfizam reda 2, bila automorfizam od $K$), te $\Delta_K$ mora biti kvadrat u $\mathbb{Q}$.

## 9.3 Kvartična polja

Galoisova grupa (Galoisovog zatvorenja) kvartičnog polja $K$ može biti $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, Dihedralna grupa s 8 elemenata $D_4$ ili $S_4$. U prva dva slučaja je $K$ Galoisovo, a u druga dva nije.

Ako je Galoisova grupa od $K$ jednaka $\mathbb{Z}/4\mathbb{Z}$, tada kažemo da je $K$ **cikličko kvartično polje**, a ako je Galoisova grupa od $K$ jednaka $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, tada kažemo da je $K$ **bikvadratno polje**: ovaj naziv dolazi jer se tada $K$ može prikazati kao

$$K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}),$$

za neka 2 cijela broja $d_1$ i $d_2$.

## 9.4 Ciklotomska polja

Promotrimo sada **ciklotomska polja**, tj. polja generirana korijenima jedinice. Neka je $\zeta_m$ primitivni $m$-ti korijen jedinice, tj. $m$ je najmanji prirodan broj $n$ za koji vrijedi da je $\zeta_m^n = 1$.

**Činjenica.** $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$, gdje je $\phi$ Eulerova $\phi$-funkcija. Slijedi da su $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, te $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$ jedina ciklotomska polja stupnja 2, te da ne postoje ciklotomska polja stupnja 3.

**Činjenica.** Konjugati od $\zeta_m$ su $\phi(m)$ primitivnih $m$-tih korijena iz jedinice.

**Činjenica.** Ako $m$ dijeli $n$, tada je $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$.

## 9.5 Grupa jedinica

Invertibilni elementi u $O_K$ se zovu jedinice (nekad se kaže da su to jedinice od $K$). O strukturi grupe jedinica nam govori sljedeći važan teorem.

**Teorem 32** (Dirichletov teorem o jedinicama)**.** *Neka je $K$ PAB, te neka je $r_1$ broj realnih ulaganja od $K$, te $r_2$ broj parova kompleksnih ulaganja. Tada je grupa jedinica od $O_k$ izomorfna s*

$$T \oplus \mathbb{Z}^{r_1+r_2-1},$$

*gdje je $T$ grupa korijena jedinice sadržana u $K$.*

Slijedi da sva realna kvadratna polja imaju grupu jedinica $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$, te da kompleksna kvadratna polja imaju grupu jedinica ili $\mathbb{Z}/6\mathbb{Z}$ ($\mathbb{Q}(\sqrt{-3})$), ili $\mathbb{Z}/4\mathbb{Z}$ ($\mathbb{Q}(\sqrt{-1})$) ili $\mathbb{Z}/2\mathbb{Z}$ (sva ostala). Na primjer grupa jedinica od $\mathbb{Q}(\sqrt{2})$ je generirana s $-1$ i $1 - \sqrt{2}$, tj. svaka jedinica je oblika $\pm(1 - \sqrt{2})^n,\ n \in \mathbb{N}$.

Npr. $\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(\sqrt{-1}, \sqrt{-3})$ ima četiri kompleksna ulaganja, pa je $r_1 = 0,\ r_2 = 2$, pa je grupa jedinica izomorfna s $\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}$.

## 9.6 Faktorizacija u prstenovima cijelih brojeva PAB

Jedna od ključnih činjenica u teoriji brojeva je osnovni teorem aritmetike koji kaže da postoji jedinstvena faktorizacija na proste faktore svakog cijelog broja. Ta tvrdnja ne vrijedi općenito u PAB. Npr, u prstenu cijelih brojeva od $\mathbb{Q}(\sqrt{-5})$ vrijedi $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{5})$, što pokazuje da 6 ima 2 različita rastava na ireducibilne elemente.

Međutim vrijedi donekle slično svojstvo, tj. faktorizacija ideala na proste ideale u $O_K$ je jedinstvena. Npr. za primjer koji smo uzeli, neka je

$$a_1 = (2, 1 + \sqrt{-5}),\ a_2 = (3, 1 + \sqrt{-5}),\ a_3 = (3, 1 - \sqrt{5}).$$

Vrijedi da je

$$a_1^2 = (2),\ a_1 a_2 = (1 + \sqrt{-5}), a_1 a_3 = (1 - \sqrt{-5}), a_2 a_3 = (3),$$

$$(6) = a_1^2 a_2 a_3 = (a_1 a_2)(a_1 a_3) = (a_1 a_1)(a_2 a_3),$$

te od tuda dolaze dvije različite faktorizacije elementa 6 koje smo ranije vidjeli.

**Činjenica.** Prstenovi cijelih brojeva od PAB su **Dedekindove domene**, tj. postoji jedinstvena faktorizacija u proste ideale.

Neka su $\gamma_1, \ldots, \gamma_k \in K$. Skup

$$I = \{\alpha_1 \gamma_1 + \ldots + \alpha_k \gamma_k | \alpha_i \in O_K\}$$

zovemo **razlomljeni ideal** od $O_K$. Razlomljene ideale se može definirati i kao skupove $I$ takve da postoji $n \in \mathbb{N}$ takve da je $nI$ ideal u $O_K$. Razlomljeni ideali čine Abelovu grupu (s obzirom na množenje ideala), koja se označava s $I_K$. Skup $P_K$ glavnih razlomljenih ideala čini podgrupu od $I_K$, te je kvocijent

$$C_K = I_K / P_K$$

**grupa klasa ideala**. Broj elemenata $|C_K|$ se zove **broj klasa** od $K$, te se označava s $h_K$. Broj klasa mjeri stupanj neuspjeha jedinstvene faktorizacije u $O_K$. Primjetimo da je $O_K$ domena glavnih ideala ako i samo ako $I_K = P_K$, tj. $C_K$ je trivijalna grupa i $h_K = 1$.

## 9.7 Eksplicitna faktorizacija

Definirajmo prvo nekoliko pojmova. Neka je $\mathcal{P}$ prost ideal u $O_K$. Tada postoji jedinstveni prost cijeli broj $p$ takav da je $\mathcal{P}|(p) = pO_K$. Kažemo da $\mathcal{P}$ **leži iznad** $(p)$ (ili jednostavnije iznad $p$), te da $(p)$ (tj. $p$) **leži ispod** $\mathcal{P}$. Kažemo da je stupanj proširenja $O_K/\mathcal{P}$ od $\mathbb{F}_p$ **stupanj inertnosti** od $p$. Kažemo da je najveća potencija od $\mathcal{P}$ koja dijeli $(p)$ **stupanj grananja** od $\mathcal{P}$.

Neka je

$$(p) = \mathcal{P}_1^{e_1} \dots \mathcal{P}_k^{e_k}$$

faktorizacija od $(p)$ u $O_K$, gdje su $e_i$ i $f_i$ stupnjevi grananja i inertnosti od $\mathcal{P}_i$, te neka je $K$ polje stupnja $n$. Tada vrijedi

$$\sum_{i=1}^{k} e_i f_i = n.$$

Ako je u gornjoj notaciji $k = 1$, $e_1 = 1$, $f_1 = n$, tada kažemo da je $p$ **inertan** u $O_K$. Ako je $e_i > 1$ za bilo koji $i$, kažemo da je $p$ **razgranat** u $O_K$. Ako je $k = 1$, $e_1 = n$, $f_1 = 1$, kažemo da je $p$ **potpuno razgranat**. Ako je $k \geq 2$ kažemo da se $p$ **cijepa** u $O_K$. Ako je $k = n$ kažemo da se $p$ **potpuno cijepa** u $O_K$.

Ima samo konačno mnogo prostih brojeva koji su razgranati u $O_K$. Točnije, to su samo prosti brojevi $p$ koji dijele $\Delta_K$.

Ako je $K$ Galoisovo proširenje od $\mathbb{Q}$, tada je $e_1 = e_2 = \ldots = e_k$, te $f_1 = f_2 = \ldots = f_k$.

Kako eksplicitno odrediti faktorizira li se $p$ u $O_K$? Mi ćemo pokazati jednostavan potupak, uz pretpostavku da je $O_K = \mathbb{Z}[\alpha]$, što je na primjer sluăj za sva kvadratna polja (uz dobar izbor od $\alpha$). Postupak je sljedeći: neka je $f$ polinom koji generira polje $K$, te $\alpha$ primitivni element od $K$.

Tada faktorizacija od $f \pmod p$ odgovara fakrtorizaciji od $p$ u $O_K$. Neka je $f = f_1^{e_1} f_2^{e_2} \dots f_k^{e_k} \pmod p$; tada je

$$p = \mathcal{P}_1^{e_1} \dots \mathcal{P}_k^{e_k},$$

gdje je $\mathcal{P}_i = (p, f_i(\alpha))$, te je stupanj inertnosti od $\mathcal{P}_i$ jednak stupnju od $f_i$.

**Primjer 16.** Promotrimo faktorizaciju u kubnom polju $K$ generiranom sa $x^3 + 2x + 1$, te neka je $\alpha$ korijen ovog polinoma, tj. $\mathbb{Q}(\alpha) = K$. Ovo polje nije Galoisovo. Vrijedi

$$x^3 + 2x + 1 \equiv (x+1)(x^2 + x + 1) \pmod 2,$$

$$2O_K = (2, \alpha + 1)(2, \alpha^2 + \alpha + 1),$$

dakle 2 se cijepa u $O_K$ na 2 ideala stupnja inertnosti 1 i 2. Vrijedi

$$x^3 + 2x + 1 \equiv (x-3)(x-5)(x-9) \pmod{17},$$

$$17O_K = (17, \alpha - 3)(17, \alpha - 5)(17, \alpha - 9),$$

tj. 17 se potpuno cijepa u $O_K$.

Pošto je diskriminanta od $K$ jednaka $-59$, vrijedi da je 59 jedini prost broj koji se grana u $K$;

$$x^3 + 2x + 1 \equiv (x - 14)^2 (x - 31) \pmod{59},$$

$$59O_K = (59, \alpha - 14)^2 (59, \alpha - 31).$$

**Primjer 17.** Promotrimo sada faktorizaciju u kvadratnom polju $K = \mathbb{Q}(\sqrt{d})$. Lako se vidi da su jedini prosti brojevi $p$ koji se granaju u $K$ oni koji dijele $d$ ako je $d \equiv 1 \pmod 4$, te 2 i oni koji dijele $d$ ako je $d \equiv 2, 3 \pmod 4$. U $K$ se cijepaju oni prosti brojevi za koje $x^2 - d$ ima noltočke modulo $p$, što je ekvivalentno tome da je $d$ kvadrat modulo $p$. Dakle

$$p \text{ se cijepa ako } \left(\frac{d}{p}\right) = 1,$$

$$p \text{ je inertan ako } \left(\frac{d}{p}\right) = -1,$$

$$p \text{ je razgranat ako } \left(\frac{d}{p}\right) = 0.$$

Npr. u $\mathbb{Q}(i)$ je $\left(\frac{-1}{p}\right) = 1$ ako i samo ako $p \equiv 1 \pmod 4$, te $\left(\frac{-1}{p}\right) = -1$ ako i samo ako $p \equiv 3 \pmod 4$. Vrijedi

$$x^2 + 1 = (x+1)^2 \pmod 2,$$

te je $(2) = (1+i)^2$, te pošto je $\Delta_{\mathbb{Q}(i)} = -4$, slijedi da je 2 jedini razgranati prost broj u $\mathbb{Q}(i)$.

**Primjer 18.** Neka je $E : y^2 = x^3 - x$ eliptička krivulja definirana nad $\mathbb{Q}(i)$. Sjetimo se da $E$ ima kompleksno množenje s $\mathbb{Z}[i]$. Vrijedi da $E$ ima izogenije stupnja $p^2$ za svaki prost broj $p$ - to je množenje s $p$. Međutim ako se $p = \mathcal{P}_1\mathcal{P}_2$ cijepa u $\mathbb{Z}[i]$, tada koristeći činjenicu da je $\mathbb{Q}(i)$ domena glavnih ideala, tj. $h_{\mathbb{Q}(i)} = 1$, vrijedi da su $\mathcal{P}_1$ i $\mathcal{P}_2$ glavni ideali, generirani nekim elementima $p_1$ i $p_2$. Tada je množenje s generatorima od $\mathcal{P}_1$ i $\mathcal{P}_2$ izogenija stupnja $p$ na $E$.

Na primjer, $5 = (2+i)(2-1)$. Dakle izogeniju $[5]$ faktoriziramo kao $[2+i] \circ [2-i]$. Slijedi da je stupanj od $[2+i]$ i $[2-i]$ jednak 5.

# Poglavlje 10

# Galoisove reprezentacije pridružene eliptičkim krivuljama

Cilj ovoga poglavlja je razumjeti kako elementi Galoisove grupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ djeluju na $E[n]$, za neki $n \in \mathbb{N}$. Bit će nam bitan pojam djelovanja grupe.

**Definicija.** Neka je $G$ grupa, te $X$ skup. Tada je (desno) **djelovanje grupe** od $G$ na $X$ funkcija

$$G \times X \to X,\ (g, x) \to x^g$$

gdje vrijedi asocijativnost tj.

$$x^{gh} = (x^g)^h\ \forall x \in X, g, h \in G,$$

te

$$x^e = x, \text{ gdje je } e \text{ identitet u } G.$$

Npr. $S_n$ kanonski djeluje na skup $\{1, \ldots, n\}$, svaka grupa $G$ djeluje na samu sebe množenjem, $\mathrm{Gal}(K/\mathbb{Q})$ djeluje na $K$, za neko Galoisovo proširenje polja $K$ od $\mathbb{Q}$.

**Definicija.** Neka grupa $G$ djeluje na skup $X$, te $x \in X$. **Orbita** $Gx$ elementa $x$ je skup elementa iz $X$ u koje se $x$ može pomaknuti djelovanjem nekih elemenata $g \in G$, tj.

$$Gx = \{x^g | g \in G\}.$$

**Definicija.** Ako je $g \in G$ i $x \in X$ takvi da je $x^g = x$ kažemo da je $x$ fiksna točka od $g$, te da $g$ fiksira $x$.

Za svaki $x \in X$, definiramo **stabilizatorsku podgrupu od** $x$ (ili izotropsku grupu) $G_x$ kao skup svih elemenata iz $G$ koji fiksiraju $x$:

$$G_x = \{g \in G | x^g = x\}.$$

Može se pokazati da je $G_x$ podgrupa od $G$, te po Lagrangevom teoremu slijedi

**Teorem 33** (Teorem o orbiti i stabilizatoru)**.** *Neka su $G$ i $X$ konačni. Tada vrijedi*

$$|Gx| = [G : G_x] = \frac{|G|}{|G_x|}.$$

Lako se vidi da je "biti u istoj orbiti" relacija ekvivalencije, te da na ovaj način dobivamo particiju od $X$.

**Definicija.** Ako grupa $G$ djeluje na $X$ tako da ima samo 1 orbitu, tj. da postoji $x \in X$ takav da je $Gx = X$, kažemo da je grupovna akcija **tranzitivna**.

Ako grupa $G$ djeluje na $X$ tako da za $\forall g, h \in G$, ako postoji $x \in X$ sa svojstvom da $x^g = x^h$, onda slijedi $g = h$, tada kažemo da je $G$ djeluje **vjerno** na $X$. Ekvivalentno je da ako $x^g = x$ za neki $x \in X$, tada slijedi $g = id$.

Općenito, grupovne akcije grupe $G$ se promatraju najčešće kako bi razumjeli samu grupu $G$. Sjajni primjeri korištenja grupovnih akcija se mogu naći na
`http://gowers.wordpress.com/2011/11/06/group-actions-i/`
`http://gowers.wordpress.com/2011/11/09/group-actions-ii-the-orbit-stabilizer-theorem/`

Međutim, kod nas je situacija nešto drukčija, pošto nas zanimaju činjenice o $E[n]$, npr. koja su minimalna polja definicije elemenata iz $E[n]$. Tu će nam biti korisne reprezentacije grupa.

**Definicija.** Reprezentacija grupe $G$ na vektorskom prostoru $V$ je homomorfizam grupa iz $G$ u $GL(V)$. Tj. reprezentacija je preslikavanje

$$\rho : G \to \mathrm{GL}(V) \text{ takvo da je } \rho(g_1 g_2) = \rho(g_1)\rho(g_2),\ \forall g_1, g_2 \in G.$$

Neka je $E/\mathbb{Q}$. Sjetimo se da je $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, te da $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ djeluje na $E[n]$, tj. automorfizam je od $E[n]$. Dakle dobivamo preslikavanje

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

te na taj način dobivamo reprezentaciju grupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Spomenuta reprezentacija, koja je inducirana s $E[n]$ se obično označava s $\rho_n$. Eliptičku krivulju ne pišemo u subskriptu, jer će uvijek biti jasno o kojoj krivulji se radi. Reprezentacija $\rho_n$ se često naziva i **mod $n$ Galoisova reprezentacija**.

Prvo što možemo primjetiti je da su koordinate svih točaka u $E[n]$ elementi nekih polja algebarskih brojeva. Najmanje polje koje sadrži eve elemente iz $E[n]$ se označava s $\mathbb{Q}(E[n])$ i zove se **$n$-to djelidbeno polje od $E$**.

Primjetimo da za svaki $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[n]))$, tj. $\sigma$ koji fiksira $\mathbb{Q}(E[n])$ nužno i fiksira eve elemente iz $E[n]$, tj. djeluje trivijalno na $E[n]$. Dakle $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ se može promatrati jednostavno kroz svoju restrikciju na $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$, tj. samo promatramo kako neki $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ djeluje na $\mathbb{Q}(E[n])$.

Pogledajmo eksplicitno kako se dobije spomenuta reprezentacija. Krenimo prvo od najjednostavnijeg slučaja gdje nam je $n = p$ prost broj. Neka je $\sigma \in$

$\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$. Dakle, $E[p]$ je generiran s neka 2 elementa reda $p$, $P_1$ i $P_2$. Tada je $P_1^\sigma \in E[p]$, tj.

$$P_1^\sigma = \alpha P_1 + \beta P_2, \text{ gdje } \alpha \neq 0 \text{ ili } \beta \neq 0.$$

Isto tako je

$$P_2^\sigma = \gamma P_1 + \delta P_2 \text{ gdje } \gamma \neq 0 \text{ ili } \delta \neq 0.$$

Dakle

$$\rho_p(\sigma) = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p).$$

Činjenica da je $\rho_p(\sigma) \in \mathrm{GL}_2(\mathbb{F}_p)$, tj. invertibilna matrica slijedi iz činjenice da je $\sigma$ automorfizam, tj. ima inverz. Analogno, ako je $n$ općeniti prirodan broj, ne nužno prost, dobivamo da je $\rho_n$ preslikavanje iz $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ u $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

**Činjenica.** Neka je $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, slijedi da je $\rho_n(G)$ podgrupa od $\mathrm{GL}_2(\mathbb{F}_p)$. Vrijedi da je $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ izomorfno s $\rho_n(G)$.

Drugim riječima $\rho_n$ je injekcija na $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$.

**Primjer 19.** Neka je $E : y^2 = x^3+ax+b$ eliptička krivulja nad $\mathbb{Q}$, te promotrimo $\rho_2$. Primjetimo da je $\mathbb{Q}(E[2])$, polje dobiveno pridruživanjem svih koordinata točaka reda 2, zapravo polje dobiveno pridruživanjem svih korijena od $x^3+ax+b$, tj. polje razlaganja od $x^3 + ax + b$.

Po prethodno navedenoj činjenici, $\rho_2(\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}))$ je podgrupa od $\mathrm{GL}_2(\mathbb{F}_2)$, za koju nadalje znamo da je izomorfna s $S_3$. Dakle, $\rho_2(\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}))$ može biti ili trivijalna grupa, ciklička grupa reda 2, ciklička grupa reda 3, te $S_3$.

Ako je $\rho_2(\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}))$ trivijalna grupa, tada svaki automorfizam od $\overline{\mathbb{Q}}$ djeluje trivijalno na elemente od $E[2]$, pa slijedi da su svi elementi iz $E[2]$ racionalni, tj. $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Primjetimo da je to ekvivalentno tome da se $x^3 + ax + b$ faktorizira kao umnožak 3 linearna polinoma.

Ako je $\rho_2(\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}))$ ciklička grupa reda 2, slijedi da je BSO

$$\rho_2(\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})) = \left\{ \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Dakle, za svaki $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ vrijedi $P_2^\sigma = P_2$, tj. $P_2 \in E(\mathbb{Q})$. Kako postoji $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ takav da je $P_1^\sigma = P_1+P_2$, slijedi da $P_1 \notin E(\mathbb{Q})$. Dakle $E(\mathbb{Q})[2] = \{O, P_2\} \simeq \mathbb{Z}/2\mathbb{Z}$. Ovaj slučaj odgovara slučaju kada se $x^3 + ax + b$ faktorizira kao produkt linearnog i kvadratnog polinoma. Lako vidimo da će $\mathbb{Q}(E[2])$ u ovom slučaju biti kvadratno polje.

Ako je $\rho_2(\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}))$ ciklička grupa reda 3, vrijedit će da je $x^3+ax+b$ ireducibilan, tj. da je $E(\mathbb{Q})[2]$ trivijalna grupa. Također, polje razlaganja će biti cikličko kubno polje, te će diskriminanta eliptičke krivulje biti kvadrat.

Ako je $\rho_2(\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}))$ izomorfna sa $S_3$, tada , vrijedit će da je $x^3+ax+b$ ireducibilan, tj. da je $E(\mathbb{Q})[2]$ trivijalna grupa. Također, polje razlaganja od $x^3 + ax + b$ će biti polje stupnja 6 s Galoisovom grupom $S_3$.

**Primjer 20.** Pogledajmo sada jedan potpuno eksplicitan primjer; neka je $E : y^2 = x^3 - 2$. Sada je

$$E[2] = \{O, (\sqrt[3]{2}, 0), (\rho\sqrt[3]{2}, 0)(\rho\sqrt[3]{2}, 0)\},$$

gdje je $\rho = \frac{-1+\sqrt{-3}}{2}$ treći korijen iz jedinice, te je

$$\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt[3]{2}, \rho) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}).$$

Vrijedi da je

$$\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) = \langle \sigma, \tau \rangle,$$

gdje

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

Primjetimo da je $\sigma(\rho) = \rho^2$, te $\sigma(\rho^2) = \rho^4 = \rho$.

Uzmimo za bazu od $E[2]$ točke

$$P_1 = (\sqrt[3]{2}, 0) \text{ i } P_2 = (\rho\sqrt[3]{2}, 0),$$

Tada je

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

Dakle imamo da je

$$\rho_2(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Analogno dobivamo da je

$$P_1^\tau = P_2 \text{ i } P_2^\tau = P_1 + P_2,$$

pa je

$$\rho_2(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Neka je $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Prirodno je pitanje što je $\rho_n(G)$, tj. kolika je slika mod $n$ Galoisove reprezentacije u $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. O tome nam govori jedan od najbitnijih teorema u teoriji eliptičkih krivulja, tzv. Serreov teorem o otvorenoj slici. Da bi iskazali teorem u punoj generalnosti morat ćemo uvesti neke pojmove (koje nećemo kasnije koristiti na predmetu, te će nam biti bitni samo za iskaz Serreovog teorema).

Neka je $l$ fiksan prost broj. Primjetimo da postoji prirodni homomorfizam $E[l^{n+1}] \to E[l^n]$ (tj. množenje s $l$). Definiramo **Tateov modul** $T_l(E)$ kao

$$T_l = \varprojlim E[l^n].$$

Vrijedi da je $T_l$ slobodan $\mathbb{Z}_l$-modul ranga 2. Neka je $V_l = \mathbb{Q} \otimes T_l$. Primjetimo da $V_l$ daje reprezentaciju

$$\hat{\rho}_l : G \to \mathrm{GL}_2(\mathbb{Q}_l)$$

koja se naziva $l$-adska Galoisova reprezentacija.

**Teorem 34** (Serre)**.** *Neka je $E$ eliptička krivulja bez kompleksnog množenja.*

- *Slika $\hat{\rho}_l(G)$ je jednaka $GL_2(\mathbb{Z}_l)$ za sve osim konačno mnogo $l$-ova.*
- *Slika $\hat{\rho}_l(G)$ je u $l$-adskoj topologiji otvorena u $GL_2(\mathbb{Z}_l)$ (tj. $[GL_2(\mathbb{Z}_l) : \rho_l(G)]$ je konačan).*

Što nam govori ovaj teorem o mod $n$ reprezentacijama (koje će nas prvenstveno zanimati)? Prvi dio povlači da će $\rho_p(G)$ biti jednak $\mathrm{GL}_2(\mathbb{F}_p)$ za sve osim konačno mnogo $p$-ova, tj. drugim rječima $[\mathbb{Q}(E[p]) : \mathbb{Q}]$ će biti najveći mogući.

Drugi dio teorema nam govori da ako $\rho_p(G)$ nije surjekcija, tada postoji $m$ takav da je $\rho_{p^{n+1}}(G)$ najveći mogući koji mu dopušta $\rho_{p^n}(G)$ za svaki $n \geq m$. Štoviše, ako je $p > 3$, tada je $m = 1$, a ako je $p = 2$, tada je $m = 1, 2$ ili 3, a ako je $p = 3$, tada je $m = 1$ ili 2 (tj. mod 9 reprezentacija ne mora biti najveća moguća s obzirom na mod 3 reprezentaciju, ali već mod 27 reprezentcija mora biti najveća moguća koja je dopuštena s obzirom na mod 9 reprezentaciju).

Nama će Galoisove reprezentacija biti vrlo korisne kod određivanja $[\mathbb{Q}(E[n]) : \mathbb{Q}]$.

**Primjer 21.** Neka je $p$ prost broj i $E$ eliptička krivulja takva da je $\rho_p$ surjekcija. Koliki je $[\mathbb{Q}(E[p]) : \mathbb{Q}]$?

Znamo da je $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \simeq \rho_p(G)$, tj. $[\mathbb{Q}(E[p]) : \mathbb{Q}] = |\rho_p(G)| = |\mathrm{GL}_2(\mathbb{F}_p)| = (p^2-1)(p^2-p)$. Sjetimo se da $|\mathrm{GL}_2(\mathbb{F}_p)|$ dobijemo tako da prvo brojimo broj izbora za prvi stupac - bilo što osim nul-vektor - $p^2 - 1$ izbora, dok za drugi stupac imamo bilo što osim višekratnik prvog stupca- dakle $p^2 - p$ izbora.

Dakle u surjektivnom slučaju je $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 6$, te $[\mathbb{Q}(E[3]) : \mathbb{Q}] = 48$.

Možemo se i pitati kako izgledaju Galoisove reprezentacije eliptičkih krivulja s torzijom ili izogenijom.

Neka je $E/\mathbb{Q}$ eliptička krivulja s točkom $P_1$ reda $n$. Tada postoji $P_2$ takav da je $E[n] = \langle P_1, P_2 \rangle$. Kako svaki element od $G$ fiksira $P_1$, vrijedi da je

$$\rho_n(\sigma) = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}, \ \forall \sigma \in G.$$

Ako je $E$ eliptička krivulja sa cikiličkom izogenijom $\phi$ stupnja $n$, tj. $\mathrm{Ker}\,\phi \simeq \mathbb{Z}/n\mathbb{Z}$, prisjetimo se da tada svaki $\sigma \in G$ djeluje na $\mathrm{Ker}\,\phi$, tj. vrijedi $P^\sigma \in \mathrm{Ker}\,\phi$ za svaki $P \in \mathrm{Ker}\,\phi$, tj. $P^\sigma = \alpha P$. Neka je $P_2$ neki generator od $\mathrm{Ker}\,\phi$; tada postoji neki $P_1$ takav da je $E[n] = \langle P_1, P_2 \rangle$. Tada je

$$\rho_n(\sigma) = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, \ \forall \sigma \in G,$$

tj. slika mod $n$ Galoisove reprezentacije je sadržana u skupu gornje-trokutastih matrica.

## 10.1 Djelidbeni polinomi

Djelidbeni polinomi nam daju jednostavniji i eksplicitniji način baratanja s torzijskim točkama u proširenjima nego Galoisove reprezentacije, iako nam često daju manje informacija.

Neka je

$$E : y^2 = x^3 + Ax + B.$$

Definiramo

$\psi_0 = 0$,
$\psi_1 = 1$,
$\psi_2 = 2y$,
$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$,
$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$,
$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$ za $m \geq 2$,
$\psi_{2m} = (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$ za $m \geq 2$,

te polinome

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

**Propozicija 35.** *Neka je $P = (x, y)$ točka na eliptičkoj krivulji $y^2 = x^3+Ax+B$ (nad nekim poljem karakteristike različite od 2), te neka je $n$ prirodan broj. Tada je*

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3}\right). \tag{10.1}$$

Vrijedi da je $\psi_{2n+1}(x, y)$ zapravo polinom u varijablalama $x$ i $y^2$, te se uvrštavanjem $y^2 = x^3 + Ax + B$ dobiva samo polinom u varijabli $x$, tj. $\psi_{2n+1}(x)$. Isto vrijedi i za

$$\frac{\psi_{2n}(x,y)}{y}.$$

Neka je $n > 2$ neparan. Primjetimo da je $nP = O$ ako i samo ako je $\psi_n(x) = 0$ - ovo je vrlo bitna činjenica koja nam daje metodu nalaženja $x$-koordinata točaka iz $E[n]$ - to je upravo $\frac{n^2-1}{2}$ nultočaka polinoma $\psi_n(x)$. Primjetimo da ako je $K$ polje nad kojim $\psi_n(x)$ ima nultočku $\alpha$, to ne znači odmah da postoji točka $P$ takva da je $nP = O$, to znači samo da postoji takav $P$ s $x$-koordinatom iz $K$. Da bi i $y(P)$ bio u $K$, tada $\alpha^3 + A\alpha + B$ mora biti kvadrat u $K$. Drugim rječima, $P$ će biti definiran nad $\mathbb{Q}(\alpha, \sqrt{\alpha^3 + A\alpha + B})$. Primjetimo da ako je $P$ definiran nad $K$, onda su i svi višekratnici od $P$ definirani nad $K$. Pošto je $\psi_n(x)$ stupnja $(n^2-1)/2$, znači da će $x(P)$ biti definiran u najgorem slučaju nad poljem stupnja $(n^2-1)/2$, dok će onda $y(P)$ biti definiran ili nad tim poljem ili nad proširenjem stupnja 2 od tog polja; dakle postoji polje $K$ stupnja $\leq n^2 - 1$ takvo da je $E[n] \neq \{0\}$.

**Primjer 22.** Neka je $E : y^2 = x^3 + x + 2$. Dobivamo da je $\psi_3(x) = 3 \cdot (x^4 + 2x^2 + 8x - 1/3)$ ireducibilan polinom. Neka je $\alpha$ korijen od $x^4 + 2x^2 + 8x - 1/3$, te $K = \mathbb{Q}(\alpha)$. Računom dobijemo da je $E[3](\mathbb{Q}(\alpha)) = \{O\}$, te da je $E[3](\mathbb{Q}(\alpha, \sqrt{\alpha^3 + \alpha + 2})) \simeq \mathbb{Z}/3\mathbb{Z}$. Primjetimo da činjenica da je $\psi_3(x)$ ireducibilan povlači da ne postoje točke reda 3 na $E$ ni nad jednim kvadratnim ni kubnim poljem.

# Poglavlje 11

# Dokaz Mordell-Weilovog teorema

Cilj sljedećeg poglavlja će biti dokaz Mordell-Weilovog teorema. Već smo vidjeli da je torzija eliptičkih krivulja nad PAB konačno generirana (tj. ili je ciklička grupa ili produkt dvije cikličke). Mordell-Weilov teorem nam govori da je cijeli $E(K)$ konačno generiran, gdje je $K$ neko PAB.

Pratit ćemo [14, VIII], te ćemo neke dijelove dokaza izostaviti, tj. navest ćemo neke tvrdnje bez dokaza (kompletni dokazi se mogu naći u [14]). Dokaz se dijeli na dva dijela. Prvi dio je tzv. slabi Mordell-Weilov teorem.

## 11.1 Slabi Mordell-Weilov teorem

**Teorem 36** (Slabi Mordell-Weilov teorem)**.** *Neka je $K$ polje algebarskih brojeva, te $E/K$ eliptička krivulja i $m \geq 2$ cijeli broj. Tada je $E(K)/mE(K)$ konačna grupa.*

Prvo dokazujemo sljedeću lemu.

**Lema 37.** *Neka je $L/K$ konačno Galoisovo proširenje. Ako je $E(L)/mE(L)$ konačna grupa, tada je i $E(K)/mE(K)$ konačna grupa*

*Dokaz.* Inkluzija $E(K) \hookrightarrow E(L)$ prirodno inducira preslikavanje kvocijentnih grupa

$$E(K)/mE(K) \to E(L)/mE(L).$$

Neka je $\Phi$ jezgra ovog preslikavanja. Imamo

$$\Phi = \frac{E(K) \cap mE(L)}{mE(K)}.$$

Primjetimo da za svaki $P \pmod{mE(K)} \in \Phi$, možemo odabrati točku $Q_P \in E(L)$ koja zadovoljava $[m]Q_p = P$. Primjetimo da ovaj izbor nije jedinstven. Definirajmo sada preslikavanje skupova (koje općenito nije homomorfizam

grupa)

$$\lambda_P : \mathrm{Gal}(L/K) \to E[m],\ \ \lambda_P(\sigma) = Q_P^\sigma - Q_P.$$

Primjetimo da je

$$[m](Q_P^\sigma - Q_P) = ([m]Q_P)^\sigma - [m]Q_P = P^\sigma - P = O,$$

pošto je $P \in E(K)$. Iz gore navedene jednadžbe zaključujemo da je $Q_P^\sigma - Q_P \in E[m]$.

Dokažimo sada da je $\Phi$ konačna grupa. To ćemo dokazati tako da pokažemo da postoji injekcija s $\Phi$ u drugi konačan skup. Neka su $P, P' \in E(K) \cap mE(L)$ koji zadovoljavaju $\lambda_P = \lambda'_P$. Tada je

$$(Q_P - Q_{P'})^\sigma = (Q_P - Q_{P'}) \text{ za sve } \sigma \in \mathrm{Gal}(L/K),$$

pa je $Q_P - Q_{P'} \in E(K)$. Slijedi da je

$$P - P' = [m]Q_P - [m]Q_{P'} \in mE(K),$$

te je $P \equiv P' \pmod{mE(K)}$. Dakle preslikavanje

$$\Phi \mapsto \{\text{Preslikavanja} : \mathrm{Gal}(L/K) \to E[m]\},\ \ P \mapsto \lambda_P$$

je injekcija. Primjetimo da su $\mathrm{Gal}(L/K)$ i $E[m]$ konačne grupe, pa je i broj preslikavanja među njima konačan. Slijedi po prvom teoremu o izomorfizmu grupa da je $(E(K)/mE(K))/\Phi$ podgrupa od $E(L)/mE(L)$, koja je konačna grupa. Slijedi da je $(E(K)/mE(K))$ konačna. □

Glavna korist ove leme je da možemo pretpostaviti da je $E[m] \subset K$. U suprotnom proširimo polje $K$, te dokazujemo Slabi Mordell-Weilov teorem za prošireno polje. Do kraja poglavlja, bez spominjanja, pretpostavljamo $E[m] \subset K$.

**Definicija. Kummerovo sparivanje**

$$\kappa : E(K) \times \mathrm{Gal}(\overline{K}/K) \to E[m]$$

se definira na sljedeći način. Neka je $P \in E(K)$ i izaberimo bilo koji $Q \in E(\overline{K})$ takav da je $[m]Q = P$. Tada je

$$\kappa(P, \sigma) = Q^\sigma - Q.$$

Sljedeće propozicija nam daje osnovna svojstva Kummerovog sparivanja.

**Propozicija 38.** *(a) Kummerovo sparivanje je dobro definirano.*

*(b) Kummerovo sparivanje je bilinearno.*

*(c) Jezgra Kummerovog sparivanja s lijeva je $mE(K)$.*

*(d) Jezgra Kummerovog sparivanja s desna je* $\mathrm{Gal}(\overline{K}/L)$*, gdje je*

$$L = K([m]^{-1}E(K)), \tag{11.1}$$

*kompozitum svih polja* $K(Q)$ *(polje dobiveno pridruživanju polju* $K$ *koordinate točke* $Q$*) gdje* $Q$ *varira po svim točkama iz* $E(\overline{K})$ *koja zadovoljavaju* $[m]Q \in E(K)$*.*

*Dokaz.* (a) Moramo dokazati da je $\kappa(P,\sigma) \in E[m]$, te da njegova vrijednost ne ovisi o izboru $Q$. Da bi dokazali prvu tvrdnju, primjetimo da je

$$[m]\kappa(P,\sigma) = [m]Q^\sigma - [m]Q = P^\sigma - P = O,$$

pošto je $P \in E(K)$, a $\sigma$ fiksira $K$. Za drugu tvrdnju, neka je $Q'$ neka druga točka takva da je $[m]Q' = P$. Tada je $Q' = Q + T$ za neki $T \in E[m]$. Vrijedi

$$(Q')^\sigma - Q' = (Q+T)^\sigma - (Q+T) = Q^\sigma + T^\sigma - Q - T = Q^\sigma - Q,$$

pošto smo pretpostavili da je $E[m] \subset E(K)$ (a time i $T \in E(K)$), te zato što $\sigma$ fiksira $K$.

(b) Linearnost u prvoj varijabli je očita. Za linearnost u drugoj varijabli, neka su $\sigma, \tau \in \mathrm{Gal}(\overline{K}/K)$. Vrijedi

$$\kappa(P,\sigma\tau) = Q^{\sigma\tau} - Q = (Q^\sigma - Q)^\tau + (Q^\tau - Q) = \kappa(P,\sigma)^\tau + \kappa(P,\tau).$$

Međutim $\kappa(P,\sigma) \in E[m] \subset E(K)$, pa je $\kappa(P,\sigma)^\tau = \kappa(P,\sigma)$.

(c) Neka je $P \in mE(K)$, recimo $P = [m]Q$ za neki $Q \in E(K)$. Tada svaki $\sigma \in \mathrm{Gal}(\overline{K}/K)$ fiksira $Q$, te je

$$\kappa(P,\sigma) = Q^\sigma - Q = O.$$

Obrnuto, pretpostavimo da je $\kappa(P,\sigma) = O$ za sve $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Uzmimo $Q \in E(\overline{K})$ takav da je $[m]Q = P$. Imamo

$$Q^\sigma = Q \text{ za sve } \sigma \in \mathrm{Gal}(\overline{K}/K).$$

Slijedi da je $Q \in E(K)$, pa je $P = [m]Q \in mE(K)$.

(d) Ako je $\sigma \in \mathrm{Gal}(\overline{K}/L)$, tada je

$$\kappa(P,\sigma) = Q^\sigma - Q = O,$$

pošto je $Q \in E(L)$ po definiciji od $L$. Obrnuto, pretpostavimo da $\sigma \in \mathrm{Gal}(\overline{K}/K)$ zadovoljava $\kappa(P,\sigma) = O$ za sve $P \in E(K)$. Tada za svaki $Q \in E(\overline{K})$ koji zadovoljava $[m]Q \in E(K)$ imamo

$$O = \kappa([m]Q,\sigma) = Q^\sigma - Q.$$

Pošto je $L$ kompozitum svih $K(Q)$ gdje variramo po svim $Q$-ovima, slijedi da $\sigma$ fiksira $L$. Dakle $\sigma \in \mathrm{Gal}(\overline{K}/L)$. □

Kažemo da je bilinearno sparivanje $B$ **nedegenerirano** ako $B(x,y)=0$ za sve $x$ povlači da je $y=0$, te ako $B(x,y)=0$ za sve $y$ povlači da je $x=0$.

**Propozicija 39.** *Kummerovo sparivanje inducira nedegenerirano sparivanje*

$$E(K)/mE(K) \times \mathrm{Gal}(L/K) \to E[m]$$

*gdje je $L$ polje iz* (11.1). *Ako je $L/K$ konačno proširenje, tada slijedi da je $E(K)/mE(K)$ konačno.*

*Dokaz.* Prvo treba dokazati da je $L$ definiran u (11.1) Galoisovo proširenje. To slijedi iz činjenice da je $\mathrm{Gal}(\overline{K}/L)$ jezgra homomorfizma

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Hom}(E(K), E[m]), \quad \sigma \to \kappa(\cdot, \sigma),$$

pa slijedi da je $\mathrm{Gal}(\overline{K}/L)$ normalna podgrupa od $\mathrm{Gal}(\overline{K}/K)$ i po Galoisovoj teoriji da je $L/K$ Galoisovo, te da je

$$\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\overline{K}/K)/\,\mathrm{Gal}(\overline{K}/L).$$

Prva tvrdnja zatim slijedi iz Propozicije 38 (b) i (c).

Da bi dokazali drugu tvrdnju pretpostavimo da je $L$ konačno proširenje od $K$. Slijedi da je $\mathrm{Gal}(L/K)$ konačna. Pretpostavimo suprotno tj. da je $E(K)/mE(K)$ beskonačna grupa. Tada bi, pošto su $\mathrm{Gal}(L/K)$ i $E[m]$ konačne grupe morali postojati $P, Q \in E(K)/mE(K)$, $P \neq Q$ takvi da je $\kappa(P,\sigma) = \kappa(Q,\sigma)$ za sve $\sigma \in \mathrm{Gal}(L/K)$. To jest, $\kappa(P-Q,\sigma) = O$ za sve $\sigma \in \mathrm{Gal}(L/K)$, što je kontradikcija sa činjenicom da je ovo sparivanje nedegenerirano. □

Dakle, dokaz slabog Mordell-Weilovog teorema se sada svodi na dokazivanje konačnosti proširenja $L/K$. To je tehnički najzahtjevniji dio dokaza Slabog Mordell-Weilovog teorema, koji se dokazuje u dvije propozicije - jedna koristi svojstva eliptičkih krivulja nad lokalnim poljima, a druga algebarsku teoriju brojeva i Kummerovu teoriju (proučava proširenja oblika $K(\sqrt[n]{n})$).

Sjetimo se da je **eksponent grupe** G najmanji $n$, ako takav postoji, takav da je $nx = 0$ za svaki $x \in G$. Npr. eksponent od $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ je 8.

Sada ćemo uvesti i pojam prostih ideala u beskonačnosti. U algebarskoj teoriji brojeva postoji ekvivalencija između prostih ideala i diskretnih valuacija. Kao što u $\mathbb{Q}$ imamo uobičajenu absolutnu vrijednost $|\cdot| : \mathbb{Q} \to \mathbb{R}$, imamo i absolutne vrijednosti $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$, definirane za svaki prost broj $p$ u $\mathbb{Z}$, tj. $p$-adske apsolutne vrijednosti. Teorem Ostrowskog kaže da su to sve absolutne vrijednosti na $\mathbb{Q}$, do na ekvivalenciju.

Analogno se za PAB $K$ može za svaki prost ideal $\mathcal{P}$ (od $O_K$) definiranti $\mathcal{P}$-adska valuacija, te se još mogu definirati i absolutne vrijednosti dobivene ulaganjem $K$ u $\mathbb{C}$ te onda uzimanjem standardne absolutne vrijednosti $|\cdot| : \mathbb{C} \to \mathbb{R}$. Ako je $r_1 + 2r_2$ broj ulaganja $K$ u $\mathbb{C}$, gdje je $r_1$ broj relanih ulaganja, a $r_2$ broj parova kompleksnih ulaganja, tada dobivamo na ovaj način $r_1+r_2$ različitih absolutnih vrijednosti. Proste ideale u $K$, koji definiraju $\mathcal{P}$-adske valuacije, nazivamo **konačni prosti ideali** ili **konačna mjesta**. Absolutne

vrijednosti dobivene preko ulaganja u $\mathbb{C}$ se zovu **beskonačni prosti ideali** ili **beskonačna mjesta**. Beskonačna mjesta mogu biti realna (ako su dobivena preko ulaganja u $\mathbb{R}$), te kompleksna (inače).

Dakle, možemo mjesta od $\mathbb{Q}$ zapisati kao $\{2, 3, 5, \ldots, \infty\}$. Standardna absolutna vrijednost se često piše sa $|\cdot|_\infty$.

Definirajmo s $M_K^0$ konačna mjesta od $K$, te s $M_K^\infty$ beskonačna mjesta od $K$.

**Propozicija 40** ([14], Proposition VIII.1.5.)**.** *Neka je $L = K([m]^{-1}E(K))$ polje iz* (11.1).

*(a) Proširenje $L/K$ je Abelovo (tj.* $\mathrm{Gal}(L/K)$ *je Abelova) s eksponentom $m$.*

*(b) Neka je*

$$S = \{v \in M_K^0 : E \text{ ima lošu redukciju u } v\} \cup \{v \in M_K^0,\ v|m\} \cup M_K^\infty. \tag{11.2}$$

*Tada je $L/K$ nerazgranat izvan $S$, tj. ako je $v \in M_K$ takav da je $v \notin S$, tada je $L/K$ nerazgranato u $v$.*

**Propozicija 41** ([1], Theorem 25)**.** *Proširenje sa svojstvima iz Propozicije 40 je konačno.*

Time je dokazan Slabi Mordell-Weilov teorem.

*Napomena.* Prvo napomenimo (što ćemo kasnije i pokazati) da ako imamo $E(K)/mE(K)$, tada možemo dobiti i $E(K)$.

Pitanje koje se prirodno nameće je koliko je ovaj dokaz efektivan, tj. možemo li iskoristiti dokaz da bi izračunali $E(K)/mE(K)$? Kummerovo sparivanje nam daje injekciju

$$E(K)/mE(K) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L/K), E[m]).$$

Moguće je eksplicitno izračunati $\mathrm{Gal}(L/K)$ te time i desnu stranu. Međutim, ono što je problem i što se ne može uvijek napravaiti je izračunati koji elementi desne strane su u slici od $E(K)/mE(K)$.

## 11.2 Spust

Sada moramo dokazati da konačnost od $E(K)/mE(K)$ povlači da je $E(K)$ konačno generirana. Primjetimo da ta tvrdnja ne vrijedi općenito za Abelove grupe, pošto npr. $\mathbb{R}/m\mathbb{R} = 0$ za sve $m$, ali $R$ nije konačno generirana.

Ključne ideja u dokazu će nam biti da množenje s $m$ "povećava" koordinate točaka na eliptičkoj krivulji, te da postoji konačno mnogo točaka "manjih" od neke veličine. Kao što vidimo, bit će nam bitno na neki način mjeriti "veličinu" točaka. To će nam raditi tzv. *funkcija visine*.

**Teorem 42** (Teorem o spustu)**.** *Neka je $A$ Abelova grupa. Pretpostavimo da postoji* ***funkcija visine***

$$h : A \to \mathbb{R}$$

*takva da ima sljedeća tri svojstva*

*(i) Neka je $Q \in A$. Postoji konstanta $C_1$, ovisna o $A$ i $Q$, takva da*

$$h(P+Q) \leq 2h(P) + C_1 \text{ za sve } P \in A.$$

*(ii) Postoji cijeli broj $m \geq 2$ i konstanta $C_2$, ovisna o $A$, takva da*

$$h(mP) \geq m^2 h(P) - C_2 \text{ za sve } P \in A.$$

*(iii) Za svaku konstantu $C_3$, skup*

$$\{P \in A : h(P) \leq C_3\}$$

*je konačan.*

*Pretpostavimo da je za $m$ iz (ii) kvocijentna grupa $A/mA$ konačna. Tada je $A$ konačno generirana.*

*Dokaz.* Izaberimo $Q_1, \ldots, Q_r \in A$ za reprezente koskupova iz $A/mA$, te neka je $P \in A$. Cilj nam je dokazati da je razlika između $P$ i neke linearne kombinacije $Q_1, \ldots, Q_r$ višekratnik neke točke čija je visina manja od konstante koja je neovisna od $P$, tada $Q_1, \ldots, Q_r$ i skup od konačno mnogo točaka čija je visina manja od te konstante generiraju $A$.

Pošto skupovi $Q_i + mA$ čine particiju od $A$, vrijedi da je $P \in Q_{i_1} + mA$ za neki $i_1$, tj.

$$P = mP_1 + Q_{i_1}.$$

Isto vrijedi i za $P_1$, tj.

$$P_1 = mP_2 + Q_{i_2}$$

$$\vdots$$

$$P_{n-1} = mP_n + Q_{i_n}.$$

Za svaki indeks $j$ imamo

$$h(P_j) \leq \frac{1}{m^2}(h(mP_j) + C_2) = \frac{1}{m^2}(h(P_{j-1} - Q_{i_j}) + C_2)$$

$$\leq \frac{1}{m^2}(2h(P_{j-1}) + C_1' + C_2),$$

gdje je $C_1'$ maksimum konstanti iz (i) za $Q \in \{-Q_1, \ldots, -Q_r\}$. Primjetimo da $C_1'$ i $C_2$ ne ovise o $P$. Višestrukom primjenom ove nejednakosti dobivamo

$$h(P_n) \leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} \cdots \frac{2^{n-1}}{m^{2n}}\right)(C_1' + C_2)$$

$$< \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_1' + C_2}{m^2 - 2}$$

$$\leq \frac{h(P)}{2^n} + \frac{C_1' + C_2}{2} \text{ pošto je } m \geq 2.$$

Ako izaberemo $n$ dovoljno velik, dobit ćemo $h(P_n) \leq 1 + (C_1' + C_2)/2$. Primjetimo da vrijedi

$$P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j},$$

te slijedi da je svaki $P$ in $A$ linearna kombinacija točaka iz skupa

$$\{Q_1, \dots Q_r\} \cup \left\{ Q \in A : h(Q) \leq 1 + \frac{C_1' + C_2}{2} \right\},$$

koji je po pretpostavci konačan. □

Sljedeći teorem ostavljamo bez dokaza (vidite [14, VIII.4 -VIII.6] za dokaze).

**Teorem 43.** *Funkcija visine postoji za $E(K)$.*

To završava dokaz Mordell-Weilovog teorema.

Primjetimo da funkcija visine nije jedinstvena. Završimo s primjerom najjednostavnije visine za $E(\mathbb{Q})$. Neka je $t = \frac{p}{q} \in \mathbb{Q}$, gdje su $p$ i $q$ relativno prosti. **Visina** od $t$, $H(t)$ je definirana s

$$H(t) = \max\{|p|, |q|\}.$$

**Definicija. Logaritamska visina** na $E(\mathbb{Q})$, s obzirom na danu Weierstrassovu jednadžbu, je funkcija

$$h : E(\mathbb{Q}) \to \mathbb{R}, \quad h(P) = \begin{cases} \log H(x(P)) & \text{ako } P \neq O \\ 0 & \text{ako } P = 0 \end{cases}.$$

# Poglavlje 12

# Weilovo sparivanje

Neka je u ovom poglavlju $E/K$ eliptička krivulja nad poljem algebarskih brojeva. Sjetimo se da je $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$, tj. $E[m]$ je slobodan $\mathbb{Z}/m\mathbb{Z}$-modul ranga 2, te je općenita činjenica da svaki slobodan modul dolazi s prirodnim alternirajućim nedegeneriranim sparivanjem, determinantom. Konkretno, neka je $\{T_1, T_2\}$ baza za $E[m]$; tada je spomenuto sparivanje na $E[m]$ dano sa

$$\det : E[m] \to \mathbb{Z}/m\mathbb{Z}, \;\; \det(aT_1 + bT_2, cT_1 + dT_2) = ad - bc.$$

Vrijednost ovog sparivanja je neovisna o izboru baze, međutim nije Galois-invarijantna, tj. $\det(P^\sigma, Q^\sigma)$ ne mora nužno biti jednako $\det(P, Q)^\sigma$.

Međutim, može se postići Galois-invarijantnost, tako da se sparivanje definira kao $\zeta^{\det(P,Q)}$, gdje je $\zeta$ neki fiksni $m$-ti korijen iz jedinice. Postoji i (teoretski bolji, međutim kompliciraniji) način definicije ovog sparivanja (vidi [14, III.8]), međutim nama će biti samo važna svojstva ovog sparivanja.

Weilovo sparivanje $e_m$, koje je definirano na $E[m]$, tj.

$$e_m : E[m] \times E[m] \to \mu_m,$$

gdje je $\mu_m$ grupa $m$-tih korijena iz jedinice.

**Propozicija 44.** *Weilovo sparivanje $e_m$ ima sljedeća svojstva.*

*(a) Bilinearno je, tj.*

$$e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T),$$

$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2).$$

*(b) Alternirajuće je, tj.*

$$e_m(T, T) = 1.$$

*Slijedi da je $e_m(S, T) = e_m(T, S)^{-1}$.*

*(c) Nedegenerirano je, tj. ako je*

$$e_m(S,T) = 0 \text{ za sve } S \in E[m],$$

*tada je* $T = O$.

*(d) Galois-invarijantno je, tj.*

$$e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma) \text{ za sve } \sigma \in \mathrm{Gal}(\overline{K}/K).$$

*(e) Kompatibilno je, tj.*

$$e_{mm'}(S,T) = e_m([m']S,T) \text{ za sve } S \in E[mm'] \text{ i } T \in E[m].$$

*Navedena svojstva Weilovog sparivanja impliciraju njegovu surjektivnost, tj. imamo sljedeći važan korolar.*

**Korolar 45.** *Postoje točke* $S,T \in E[m]$ *takve da je* $e_m(S,T)$ *primitivni* $m$*-ti korijen iz jedinice. Nadalje, ako je* $E[m] \subset E(K)$*, tada je* $\mu_m \subset K^*$.

*Dokaz.* Slika od $e_m(S,T)$, kada $S$ i $T$ variraju po svim elementima od $E[m]$ je podgupa od $\mu_m$. Neka je to $\mu_d$, gdje $d|m$. Slijedi da je

$$1 = e_m(S,T)^d = e_m([d]S,T) \text{ za sve } S,T \in E[m].$$

Zbog nedegeneriranosti od $E_m$ slijedi da je $[d]S = O$, pa pošto je $S$ proizvoljan, mora biti $d = m$.

Zbog Galois-invarijantnosti od $E_m$ vrijedi da $e_m(S,T)$ mora biti u $K$ za sve $S,T \in E[m]$. Slijedi $\mu_m \subset K^*$. □

Dajmo jedan primjer primjene Weilovog sparivanja.

**Primjer 23.** Neka je $E/K$ eliptička krivulja, te $\mathbb{Q}(\zeta_3) \subset K$, te neka je $Q \in E(K)$ točka reda 3. Neka je $P \in E[3]$ takva da $P$ nije višekratnik od $Q$. Dokažimo da ako je $x(P) \in K$, onda je i $P \in K$.

Pretpostavimo suprotno, tj. $y(P) \in L$, gdje je $[L : K] = 2$. Neka je $\sigma$ generator od $\mathrm{Gal}(L/K)$. Pošto je $2P = -P$, slijedi da je $x(P) = x(2P)$, te da je $P^\sigma = -P$ (ne može biti $P^\sigma = P$, jer bi tada bilo $P \in E(K)$).

Neka je sada $e_3(P,Q) = \zeta$, gdje je $\zeta$ neki primitivni treći korijen iz jedinice. No $\sigma(\zeta) = \zeta$, te

$$\zeta = e_3(P,Q)^\sigma = e_3(P^\sigma, Q^\sigma) = e_3(2P,Q) = e_3(P,Q)^2 = \zeta^2,$$

što je kontradikcija.

# Poglavlje 13

# Galoisova kohomologija

Već smo vidjeli da nam je bitno razumjeti djelovanje grupa na skupove. Međutim, u našim primjerima neće grupa djelovati samo na skup, nego na neku drugu grupu, te tada vrijede i neki jači rezultati. Reference za ovo poglavlje su [14, Appendix B i VIII.2], te [3, Chapter 7].

**Definicija.** Neka je $A$ abelova grupa na koju djeluje konačna grupa $G$. Tada definiramo podgrupu od $A$ **$G$-invarijantnih elemenata** (ili $G$-invarijanti) $A^G$

$$A^G = \{a \in A : a^g = a \ \forall g \in G\}.$$

Podgrupa $A^G$ se još naziva i **nulta kohomološka grupa** i označava s $H^0(G, A)$.

Zašto nas zanima skup $G$-invarijanti? U našim primjenama će $G$ biti Galoisova grupa. Ako je $K/k$ Galoisovo proširenje, te ako je $A = E(K)$, te $G = \mathrm{Gal}(K/k)$, tada je $A^G = E(k)$. Također je $K^G = k$.

Neka su $A, B, C$ grupe (ili $G$-moduli), te neka je

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

egzaktan niz. Sjetimo, se to znači da je $A \to B$ injekcija, $B \to C$ je surjekcija, te $\mathrm{Im}(A \to B) = \mathrm{Ker}(B \to C)$, tj. slijedi $C \simeq B/A$.

Što kada uzmemo $G$-invarijante ovog niza? O tome nam govori sljedeća propozicija:

**Propozicija 46.** *Neka je $G$ grupa, $A$ i $B$ grupe na koje djeluje $G$, gdje je $A \leq B$. Tada uzimanjem $G$-invarijanti na egzaktnom nizu*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

*dobivamo*

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G.$$

*Dokaz.* Pošto je je $A^G \to B^G$ restrikcija injekcije $A \to B$, jasno je da je injekcija. Nadalje

$$\mathrm{Ker}(B^G \to C^G) = \mathrm{Ker}(B \to C) \cap B^G = \mathrm{Im}(A \to B) \cup B^G = \mathrm{Im}(A^G \to B^G),$$

što dokazuje propoziciju. □

Prirodno se nameće pitanje surjektivnosti od $B^G \to C^G$. Nažalost, to ne mora uvijek biti surjekcija. Sjetimo se da je $C \simeq B/A$. Tada je $(B/A)^G$ skup $a+A$ takav da je $(a+A)^g = a+A$ za sve $g \in G$. Međutim, ne mora svaki takav koskup dolaziti od nekog $a \in A^G$. Može se dogoditi da je koskup $(a+B)^g = a+A$ za sve $g \in G$, a da nijedan $x \in a + A$ nije $G$-invarijantan.

Kohomologija grupa nam daje odgovor na pitanje u kojoj mjeri to nije surjekcija.

**Definicija.** Neka je $M$ $G$-modul. Tada je **grupa 1-kolanaca** (iz $G$ u $M$) definirana s

$$C^1(G, M) = \{\text{preslikavanja } \xi : G \to M\}.$$

**Definicija. Grupa 1-kociklusa** (iz $G$ u $M$) je dana s

$$Z^1(G, M) = \{\xi \in C^1(G, M) : \xi(\sigma\tau) = \xi(\sigma)^\tau + \xi(\tau) \text{ za sve } \sigma, \tau \in G\}.$$

Primjetimo da postoje određeni "trivijalni" kociklusi. Izaberimo neki $P \in M$, te definirajmo funkciju $\xi : G \to M$ s $\xi(\sigma) = P^\sigma - P$. Tada je

$$\xi(\sigma\tau) = P^{\sigma\tau} - P = (P^\sigma - P)^\tau + (P^\tau - P) = \xi(\sigma)^\tau + \xi(\tau).$$

**Definicija. Grupa 1-korubova** (iz $G$ u $M$) se definira sa

$$B^1(G, M) = \left\{\xi \in C^1(G, M) : \exists P \in M \text{ takav da } \xi(\sigma) = P^\sigma - P,\ \forall \sigma \in G\right\}.$$

Lako se provjeri da je $B^1(G, M)$ grupa, te da je podgrupa od $Z^1(G, M)$.

**Definicija. Prva kohomološka grupa** ($G$-modula $M$) se definira sa

$$H^1(G, M) = \frac{Z^1(G, M)}{B^1(G, M)}.$$

*Napomena.* Ako $G$ djeluje trivijalno na $M$, tada je $H^0(G, M) = M$ i $H^1(G, M) = \mathrm{Hom}(G, M)$. Druga tvrdnja se lako provjeri - kociklusi su homomorfizmi, a sve kogranice su 0.

Glavna propozicija (općenite) kohomologije grupa je

**Propozicija 47.** *Neka je*

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0$$

*egzatan niz $G$-modula, gdje je $A$ podmodul od $B$. Tada postoji dugi egzaktni niz*

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \xrightarrow{\delta} H^1(G, A) \to H^1(G, B) \to H^1(G, C).$$

*Dokaz.* Jedino što nije lako pokazati je postojanje preslikavanja $\delta$. Preslikavanje $\delta$ se definira na sljedeći način. Neka je $c \in C^G$, te izaberimo $b \in B$ takav da je $\psi(b) = c$, te definirajmo kolanac $\xi \in C^1(G, B)$ s

$$\xi(\sigma) = b^\sigma - b.$$

Sada je

$$\psi(\xi(\sigma)) = \psi(b^\sigma) - \psi(b) = \psi(b)^\sigma - \psi(b) = c^\sigma - c = 0,$$

pošto je $c \in C^G$. Dakle $\xi(\sigma) \in \operatorname{Ker}\psi = \operatorname{Im}\phi$, tj. $\xi(\sigma) \in A$. Dakle $\xi$ je kociklus u $H^1(G, A)$. □

Prije nego što krenemo na primjenu kohomologije grupa na teoriju eliptičkih krivulja, dajmo jedan primjer eksplicitnog računa s Galoisovom kohomologijom.

**Primjer 24.** Neka je $E/\mathbb{Q}$ eliptička krivulja takva da je $E(\mathbb{Q})[2] = 0$, te neka je $K/\mathbb{Q}$ cikličko kubno polje i $E(K)[2] \neq 0$.

Pogledajmo sada kako $G$ djeluje na $E(K)[2]$. Pošto je $E(\mathbb{Q})[2] = 0$, slijedi da je $O$ jedina fiksna točka od $G$.

Prvo primjetimo da mora biti $E(K) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, pošto kad bi bilo $E(K) \simeq \mathbb{Z}/2\mathbb{Z}$, tada pošto $\mathrm{Gal}(K/\mathbb{Q})$ fiksira $O$, morao bi fiksirati i jedinu točku reda 2, iz čega bi slijedilo $E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Dakle 3 točke reda 2 iz $E(K)[2]$ čine jednu orbitu. Neka je $G = \{id, \sigma, \sigma^2\}$, te neka je $\{P, Q\}$ baza od $E[2]$ takva da je $P^\sigma = Q$ i $Q^\sigma = P + Q$.

Neka je $\xi \in Z^1(G, E(K)[2]) = 0$. Ako je $\xi(\sigma) = O$ tada je $\xi(\sigma^2) = \xi(\sigma)^\sigma - \xi(\sigma) = O$, te je analogno $\xi(id) = O$. Možemo i napisati da je $\xi(\sigma) = O^\sigma - O$ tj. $\xi \in B^1(G, M)$.

Pretpostavimo sada da je $\xi(\sigma) \neq O$. Neka je BSO $\xi(\sigma) = P = Q^\sigma - Q$. Tada je $\xi(\sigma^2) = P^\sigma - P = P + Q = Q^{\sigma\,2} - Q$. Analogno je $\xi(id) = O$.

Dakle $\xi \in B^1(G, E(K)[2])$. Dakle $B^1(G, E(K)[2]) = Z^1(G, E(K)[2])$, tj. $H^1(G, E(K)[2]) = 0$.

**Primjer 25. Hilbertov teorem 90** kaže da za (ne nužno konačno) Galoisovo proširenje $L/K$, vrijedi

$$H^1(\mathrm{Gal}(L/K), L^\times) = 0,$$

gdje je $L^\times$ multiplikativna grupa elemenata od $L$. Uzmimo $L = \mathbb{Q}(i)$ i $K = \mathbb{Q}$ i izvedimo parametrizaciju kružnice iz ovog teorema.

Elementi iz $L^\times$ su elementi s normom 1, tj. oni oblika $a+bi$, gdje je $a^2+b^2 = 1$.

Neka je $\alpha \in \mathbb{Q}(i)$ norme 1, $\sigma$ kompleksno konjugiranje, i neka $\xi$ 1-kociklus iz $H^1(\mathrm{Gal}(L/K), L^\times)$, takav da $\xi(\sigma) = \alpha$. To je zaista kociklus jer je $\xi(id) = \xi(\sigma^2) = \alpha^\sigma \cdot \alpha = 1$. Kako je $H^1(\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}), \mathbb{Q}(i)^\times) = 0$, slijedi da je taj kociklus korub, te je $\alpha = \frac{\beta^\sigma}{\beta}$ za neki $\beta \in \mathbb{Q}(i)^\times$. Neka je $\beta = x + yi$. Vrijedi da je

$$\alpha = \frac{x - yi}{x + yi} = \frac{x^2 - y^2}{x^2 + y^2} - i\frac{2xy}{x^2 + y^2}.$$

Tj. svaki element na jediničnoj kružnici je kao u jednadžbi iznad, tj. dobili smo parametrizaciju jedinične kružnice.

Neka je $E/K$ eliptička krivulja. Nas će zanimati sljedeći egzaktan niz $G$-modula, gdje je $G := \mathrm{Gal}(\overline{K}/K)$:

$$0 \longrightarrow E[m] \longrightarrow E(\overline{K}) \xrightarrow{[m]} E(\overline{K}) \longrightarrow 0.$$

Uzimanjem $G$-invarijanti, tj. primjenom Propozicije 47, dobivamo

$$0 \longrightarrow E(K)[m] \longrightarrow E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta}$$

$$H^1(G, E[m]) \xrightarrow{\psi} H^1(G, E(\overline{K})) \xrightarrow{[m]} H^1(G, E(\overline{K})).$$

Pogledajmo sada $\delta$. Imamo da je $\mathrm{Ker}\,\delta = \mathrm{Im}([m]E(K)) = mE(K)$. Nadalje, imamo da je $\mathrm{Im}\,\psi = \ker[m] = H^1(G, E(\overline{K}))[m]$. Iz ovoga dobivamo kratki egzaktni niz

$$0 \longrightarrow \tfrac{E(K)}{mE(K)} \xrightarrow{\delta} H^1(G, E[m]) \xrightarrow{[m]} H^1(G, E(\overline{K}))[m] \longrightarrow 0.$$

Ovo je **Kummerov niz** za $E/K$. Homomorfizam $\delta$ je po Propoziciji 47 definiran na sljedeći način: neka je $P \in E(K)$ i izaberimo $Q \in E(\overline{K})$ takvog da je $[m]Q = P$. Tada je 1-kociklus koji predstavlja $\delta(P)$ dan s

$$c : \mathrm{Gal}(\overline{K}/K) \to E[m], \quad c(\sigma) = Q^\sigma - Q.$$

Uočavamo da je ovo upravo Kummerovo sparivanje iz prošlog poglavlja, tj.

$$c(\sigma) = \kappa(P, \sigma).$$

U prošlom poglavlju smo i vidjeli da ako je $E[m] \subseteq E(K)$, tada je svaki kociklus homomorfizam, tj.

$$H^1(\mathrm{Gal}(\overline{K}/K), E[m]) = \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), E[m])),$$

pa dobivamo injektivni homomorfizam

$$E(K)/mE(K) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), E[m])), \quad P \to \kappa(P, \cdot).$$

Postoji također Kummerov niz i za polja. Krećemo od sljedećeg egzaktnog niza

$$1 \longrightarrow \mu_m \longrightarrow \overline{K}^* \xrightarrow{z \to z^m} \overline{K}^* \longrightarrow 1,$$

neka je $G = \mathrm{Gal}(\overline{K}/K)$, te uzmimo $G$-invarijante. Dobivamo

$$1 \longrightarrow \mu_m^G \longrightarrow K^* \xrightarrow{z \to z^m} K^* \longrightarrow$$

$$H^1(G, \mu_m) \longrightarrow H^1(G, \overline{K}^*) \xrightarrow{z \to z^m} H^1(G, \overline{K}^*).$$

Iz ovog niza, na analogan način kao i za eliptičke krivulje, dobivamo

$$1 \longrightarrow (K^*)/(K^*)^m \longrightarrow H^1(G, \mu_m) \longrightarrow H^1(G, \overline{K}^*)[m] \longrightarrow 0.$$

Znamo iz Hilbertovog teorema 90 da je $H^1(G, \overline{K}^*) = 0$, pa dobivamo sljedeću propoziciju

**Propozicija 48.** *Postoji izomorfizam*

$$\delta : (K^*)/(K^*)^m \xrightarrow{\sim} H^1(G, \mu_m)$$

*definiran s*

$$\delta(a) = \text{ klasa kohomologije od preslikavanja } \sigma \to \frac{\alpha^\sigma}{\alpha},$$

*gdje je* $\alpha \in \overline{K}^*$ *takav da je* $\alpha^m = a$.

Neka je $E/K$ i $m \geq 2$, takvi da je $E[m] \subset E(K)$. Označimo povezujući homomorfizam iz Kummerovog niza za eliptičke krivulje s $\delta_E$, tj.

$$\delta_E : E(K)/mE(K) \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), E[m]),$$

$$\delta_E(P) = (\sigma \to \kappa(P, \sigma)).$$

Označimo povezujući homomorfizam iz Kummerovog niza za polje $K$ s $\delta_K$, tj.

$$\delta_K : (K^*)/(K^*)^m \to H^1(\mathrm{Gal}(\overline{K}/K), \mu_m) = (\mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_m),$$

$$\delta_K(c) = (\sigma \to \beta^\sigma/\beta),$$

gdje je $\beta^m = c$.

Ključan teorem za eksplicitno računanje Mordell-Weilovog ranga će biti sljedeći teorem.

**Teorem 49.** *(a) Uz gornju notaciju, postoji bilinearno sparivanje*

$$b : E(K)/mE(K) \times E[m] \to K^*/(K^*)^m$$

*koje zadovoljava*

$$e_m(\delta_E(P)(\sigma), T) = \delta_K(b(P,T))(\sigma) \text{ za sve } \sigma \in \mathrm{Gal}(\overline{K}/K).$$

*(b) Sparivanje iz (a) je nedegenerirano s lijeva.*

*(c) Neka je $S \subset M_K$ unija beskonačnih mjesta, konačnih prostih elemenata (od $K$) u kojima $E$ ima lošu redukciju, i konačnih prostih ideala koji dijele $m$. Tada slika sparivanja iz (a) leži u sljedećoj podgrupi od $K^*/(K^*)^m$:*

$$K(S, m) = \{d \in K^*/(K^*)^m : ord_v(d) \equiv 0 \pmod{m},\ \forall v \notin S\}.$$

*(d) Sparivanje iz (a) se može eksplicitno izračunati: za svaki $T \in E[m]$ izaberemo funkcije $f_T, g_T \in K(E)$, takve da $f_T$ ima nultočku reda $m$ u $T$ i pol reda $m$ u $O$, te je*

$$f_T \circ [m] = g_T^m.$$

*Tada za svaki $P \neq T$ vrijedi*

$$b(P, T) \equiv f_T(P) \pmod{(K^*)^m}.$$

*Napomena.* Primjetimo da se u (d) $b(T,T)$ može izračunati iz linearnosti. Uzmimo proizvoljan $Q \in E(K)$, te je onda

$$b(T+Q,T) = b(T,T)b(Q,T),$$

pa je

$$b(T,T) = b(T+Q,T)/b(Q,T) \equiv f_T(T+Q)f_T(Q)^{-1} \pmod{(K^*)^m}.$$

*Napomena.* Ovaj teorem nam zapravo daje postupak za računanje ranga od $E(K)$. Prvo primjetimo da je grupa $K(S,m)$ konačna i jednostavna za izračunati. Funkcije $f_T$ je također jednostavno izračunati iz jednadžbe krivulje. Pošto je preslikavanje nedegenerirano s lijeva, zapravo jedino što preostaje je napraviti sljedeće:

Fiksirajmo generatore $\{T_1, T_2\}$ od $E[m]$. Za svaki od konačno mnogo parova $(b_1, b_2) \in K(S,m) \times K(S,m)$, provjeravamo je li jednadžbe

$$b_1 z_1^m = f_{T_1}(P) \text{ i } b_2 z_2^m = f_{T_2}(P)$$

imaju rješenje $(P, z_1, z_2) \in E(K) \times K^* \times K^*$. Konkretnije, ako je jednadžba od $E/K$ jednaka

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

tada tražimo rješenja $(x, y, z_1, z_2)$ jednadžbi

$$b_1 z_1^m = f_{T_1}(x,y), \;\; b_2 z_2^m = f_{T_2}(x,y).$$

Ove dvije jednakosti definiraju novu krivulju, *glavni homogeni prostor* ili *torzor* za $E/K$. Dakle sveli smo problem dobivanja $E(K)/mE(K)$ na problem određivanja postojanja racionalnih točaka na eksplicitno zadanom skupu krivulja.

Mnoge od tih krivulja možemo eliminirati tako da vidimo da krivulje nemaju lokalnih točaka, tj. nad $K_v$, što je vrlo jednostavno provjeriti. S druge strane često je lako uočiti ili naći pomoću računala neke trivijalne racionalne točke na tim krivuljama.

Problem nastaje kada torzor ima točke nad svim upotpunjenjima $K_v$, a ne možemo naći $K$-racionalne točke. Može se dogodi da zaista nema točaka, pošto ove krivulje ne zadovoljavaju općenito Hasseov princip.

Provedimo eksplicitno ovaj postupak za $m = 2$, što se u praksi daleko najčešće koristi. Krećemo, kao i u dokazu, s pretpostavkom da je $E[2] \subset E(K)$. Tako da možemo BSO pretpostavljati da je $E$ zadana sa sljedećom Weierstrassovom jednadžbom:

$$y^2 = (x-e_1)(x-e_2)(x-e_3), \;\; e_1, e_2, e_3 \in K.$$

Torzijske točke reda 2 su

$$T_1 = (e_1, 0), \quad T_2 = (e_2, 0), \quad T_3 = (e_3, 0).$$

Neka je $T = (e, 0)$ jedna od ove tri točke. Tada je funkcija iz Teorema 49 (d) $f_T = x - e$ (ovo zahtijeva malo računa, koji ćemo preskočiti, da bi se provjerilo da zadovoljava tražena svojstva).

Neka je sada $(b_1, b_2) \in K(S, m) \times K(S, m)$. Želimo odrediti postoji li $P \in E(K)/2E(K)$ takav da zadovoljava

$$b(P, T_1) = b_1 \text{ i } b(P, T_2) = b_2.$$

Takva točka postoji ako i samo ako postoji $(x, y, z_1, z_2) \in K \times K \times K^* \times K^*$ takav da sustav jednadžbi

$$y^2 = (x - e_1)(x - e_2)(x - e_3),\ b_1 z_1^2 = x - e_1,\ b_2 z_2^2 = x - e_2,$$

ima rješenje.

Tada $y$ mora biti oblika $y = b_1 b_2 z_1 z_2 z_3$ za neki $z_3$, te nadalje vrijedi $x - e_3 = b_1 b_2 z_3^2$. Sada eliminiranjem varijable $x$ dobivamo sustav jednadžbi

$$b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1,\ \ b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1.$$

Sada treba odrediti ima li ovaj sustav jednadžbi rješenje. Tu možemo koristiti razne metode - lokalne, potragu korištenjem računala, itd. Primjetimo također da ako nađemo rješenje $(z_1, z_2, z_3)$, tada možemo naći odgovarajuću točku $P \in E(K)/2E(K)$:

$$x = b_1 z_1^2 + e_1,\ \ y = b_1 b_2 z_1 z_2 z_3.$$

Konačno trebamo uzeti u obzir da ako je $T = P$, tada ne možemo koristiti $b(P, T) = f_T(P)$. Dakle postoje 2 para $(b_1, b_2)$ koji se ne dobivaju ovim postupkom, tj. parovi $(b(T_1, T_1), b(T_1, T_2))$ i $(b(T_2, T_1), b(T_2, T_2))$. Njih možemo izračunati korištenjem linearnosti:

$$b(T_1, T_1) = b(T_1, T_1 + T_2) b(T_1, T_2)^{-1} = b(T_1, T_3) b(T_1, T_2) = \frac{e_1 - e_3}{e_1 - e_2}.$$

Analogno dobivamo $b(T_2, T_2) = \frac{e_2 - e_3}{e_2 - e_1}$.

Sljedeća propozicija rezimira dobivene rezultate:

**Propozicija 50** (Potpuni 2-spust)**.** *Neka je $E/K$ eliptička krivulja dana jednadžbom*

$$y^2 = (x - e_1)(x - e_2)(x - e_3),\ e_1, e_2, e_3 \in K.$$

*Neka je $S \subset M_K$ konačan skup mjesta od $K$ koji uključuje sva arhimedska (tj. beskonačna) mjesta, sva mjesta koja dijele 2, i sva mjesta u kojima $E$ ima lošu redukciju. Nadalje, neka je*

$$K(S, 2) = \{b \in K^*/(K^*)^2 : ord_v b \equiv 0 \pmod 2 \ \text{ za sve } v \notin S\}.$$

*Tada postoji injektivni homomorfizam*

$$E(K)/2E(K) \to K(S, 2) \times K(S, 2)$$

*definiran s*

$$P=(x,y)\to\begin{cases}(x-e_1,x-e_2) & \text{ako } x\neq e_1,e_2,\\ \left(\frac{e_1-e_3}{e_1-e_2},e_1-e_2\right) & \text{ako } x=e_1,\\ \left(e_2-e_1,\frac{e_2-e_3}{e_2-e_1}\right) & \text{ako } x=e_2,\\ (1,1) & \text{ako } P=O.\end{cases}$$

*Neka je* $(b_1,b_2)\in K(S,2)\times K(S,2)$ *par koji nije u slici jedne od točaka* $O,(e_1,0),(e_2,0)$. *Tada je* $(b_1,b_2)$ *slika točke*

$$P=(x,y)\in E(K)/2E(K)$$

*ako i samo ako jednadžbe*

$$b_1z_1^2-b_2z_2^2=e_2-e_1,$$
$$b_1z_1^2-b_1b_2z_3^2=e_3-e_1,$$

*imaju rješenje* $(z_1,z_2,z_3)\in K^*\times K^*\times K$. *Ako takvo rješenje postoji, tada možemo uzeti*

$$P=(x,y)=(b_1z_1^2+e_1,b_1b_2z_1z_2z_3).$$

**Primjer 26.** Prikažimo sada primjenu propozicije o 2-spustu na eliptičkoj krivulji

$$y^2=x^3-12x^2+20x=x(x-2)(x-10).$$

Ova eliptička krivulja ima diskriminatnu $\Delta=409600=2^{14}5^2$, te ima dobru redukciju u svim mjestima osim u 2 i 5. Odredimo torziju od $E(\mathbb{Q})$. Prvo izračunamo da je $|E(\mathbb{F}_3)|=4$, te provjerimo da nema točke reda 3, (npr. korištenjem djelidbenih polinoma) i dobijemo da je $E(\mathbb{Q})_{tors}\simeq\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$, tj. $E(\mathbb{Q})_{tors}=E[2]$.

Neka je $S=\{2,5,\infty\}\subset M_{\mathbb{Q}}$. Potpuni skup reprezenata od

$$\mathbb{Q}(S,2)=\{b\in\mathbb{Q}^*/(\mathbb{Q}^*)^2:ord_pb\equiv 0 \pmod 2 \text{ za sve } p\notin S\}$$

je skup $\{\pm1,\pm2,\pm5,\pm10\}$. Ovaj skup ćemo poistovjećivati sa $\mathbb{Q}(S,2)$. Promotrimo sada preslikavanje iz propozicije o 2-spustu

$$E(\mathbb{Q})/2E(\mathbb{Q})\to\mathbb{Q}(S,2)\times\mathbb{Q}(S,2),$$

recimo sa $e_1=0,\ e_2=2,\ e_3=10$.

Postoje 64 para $(b_1,b_2)\in\mathbb{Q}(S,2)\times\mathbb{Q}(S,2)$, te moramo odrediti koji od njih dolaze od elemenata $E(\mathbb{Q})/2E(\mathbb{Q})$. Pogledajmo prvo gdje se preslikava $E[2]$. Vrijedi:

$$O\to(1,1),\quad(0,0)\to(5,-2),\quad(2,0)\to(2,-1),\quad(10,0)\to(10,2).$$

Još treba za sve preostale parove $(b_1,b_2)$ odrediti imaju li jednadžbe

$$b_1z_1^2-b_2z_2^2=2,\ \ b_1z_1^2-b_1b_2z_3^2=10, \tag{13.1}$$

rješenja $z_1,z_2,z_3\in\mathbb{Q}$.

1. Ako je $b_1 < 0$ i $b_2 > 0$, tada prva jednadžba u (13.1) nema rješenja u $\mathbb{R}$. Time eliminiramo 16 parova.

2. Ako je $b_1 < 0$ i $b_2 < 0$, tada druga jednadžba u (13.1) nema rješenja u $\mathbb{R}$. Time eliminiramo 16 parova.

3. Promotrimo par $(b_1, b_2) = (1, -1)$. On odgovara jednadžbama

$$z_1^2 + z_2^2 = 2 \text{ i } z_1^2 + z_3^2 = 10.$$

   Lako uočavamo da ovaj sustav ima rješenje $(1, 1, 3)$. To nam dalje daje točku $(1, -3)$ na $E(\mathbb{Q})$.

4. Primjetimo da je slika našeg preslikavanja u $\mathbb{Q}(S,2)\times\mathbb{Q}(S,2)$ grupa. Dakle vrijedi da su

$$(1,-1)\cdot(5,-2) = (5,2),$$
$$(1,-1)\cdot(2,-1) = (2,1),$$
$$(1,-1)\cdot(10,2) = (10,-2).$$

   u slici.

5. Ako je $b_1 \not\equiv 0 \pmod 5$ i $b_2 \equiv 0 \pmod 5$, tada prvo iz prve jednadžbe možemo zaključiti da nazivnici od $z_1$ i $z_2$ ne mogu biti djeljivi s 5. Nadalje, druga jednadžba u (13.1) pokazuje da je $z_1$ djeljiv s 5. Tada nam prva jednadžba daje kontradikciju $0 \equiv 2 \pmod 5$. Ovime eliminiramo 8 od preostalih parova (tj. parove $(a, b)$, gdje $a \in \{1, 2\},\ b \in \{\pm 5, \pm 10\}$).

6. Koristeći slučaj 5. i svojstvo da je slika u $\mathbb{Q}(S,2)\times\mathbb{Q}(S,2)$ grupa, možemo eliminirati parove oblika $(a, b)$, gdje $a \in \{5, 10\},\ b \in \{\pm 5, \pm 10\}$. Na primjer kada bi $(5, 5)$ bio u slici tada bi i $(5, 5)\cdot(5, 2) = (1, 10)$ bio u slici, što je u kontradikciji s 5. Ovime eliminiramo 8 od preostalih parova.

7. Promotrimo par $(b_1, b_2) = (1, 2)$. Tada sustav (13.1) postaje

$$z_1^2 - 2z_2^2 = 2 \text{ i } z_1^2 - 2z_3^2 = 10.$$

   Pošto 2 nije kvadratni ostatak $\pmod 5$, slijedi da $z_1 \equiv z_3 \equiv 0 \pmod 5$. Ali tada ta ista jednadžba daje $0 \equiv 10 \pmod{25}$, što je kontradikcija.

8. Kao i prije, korištenjem svojstva da je slika grupa, možemo eliminirati parove oblika $(a, b)$, gdje $a \in \{1, 2\},\ b \in \{\pm 2\}$, te parove $(c, d)$, gdje je $c \in \{5, 10\},\ b \in \{\pm 1\}$. Time smo iscrpili sve parove.

Zaključujemo da je $|E(\mathbb{Q})/2E(\mathbb{Q})| = 8$, te pošto je $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$, slijedi da je $E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$.

*Napomena.* U ovom slučaju se za sve torzore može ili trivijalno naći racionalna točka ili dokazati da nemaju lokalna rješenja, tj. nemaju rješenja nad nekim $\mathbb{Q}_p$ (sjetimo se da je $\mathbb{Q}_\infty = \mathbb{R}$).

Skup svugdje rješivih parova $(b_1, b_2)$ čini *Selmerovu grupu* ili točnije *2-Selmerovu grupu*. Slika od $E(K)/2E(K)$ je sadržana u Selmerovoj grupi. Međutim slika i Selmerova grupa ne moraju biti jednake - razlika se sastoji od svugdje lokalno rješivih torzora koji nemaju racionalnu točku, tj. od torzora koji krše Hasseov princip. Ova grupa (koja je zapravo kvocijent Selmerove grupe i slike od $E(K)/2E(K)$) je dio *Tate-Šafarevičeve grupe* tj. točnije 2-torzija te grupe.

# Poglavlje 14

# Twistovi

Tvrdnje u ovom poglavlju vrijede i za općenite krivulje nad općenitim poljima, međutim, mi ćemo se zadržati samo na eliptičkim krivuljama nad poljima algebarskih brojeva.

**Definicija.** Neka je $E/K$ eliptička krivulja nad PAB. *Grupa izomorfizama od* $E$, koju ćemo označavati sa $\mathrm{Isom}(E)$, je grupa $\overline{K}$-izomorfizama (krivulja genusa 1, ne nužno eliptičkih krivulja) iz $E$ u $E$. Izomorfizmi definirani nad $K$ će se označavati s $\mathrm{Isom}_K(E)$.

*Napomena.* Primjetimo da su nama izomorfizmi ono što se obično naziva automorfizmom neke grupe. Međutim, mi koristimo naziv automorfizam za izomorfizam koji šalje $O$ u $O$. Primjetimo da općenito $\mathrm{Aut}(E) \neq \mathrm{Isom}(E)$, jer npr. translacija s nekom točkom $O \neq P \in E(\overline{K})$ je izomorfizam, ali nije automorfizam.

**Definicija.** Twist (ili zakret) od $E/K$ je glatka krivulja $C/K$ koja je izomorfna s $E$ nad $\overline{K}$. Dva twista smatramo ekvivalentnima ako su izomorfni nad $K$. Skup twistova od $E/K$, modulo $K$-izomorfizam, označavamo sa $\mathrm{Twist}(E/K)$.

*Napomena.* Definicija twista eliptičke krivulje u ovom poglavlju je nešto općenitija od uobičajene, - obično se twist eliptičke krivulje $E/K$ definira kao eliptička krivulja (a ne krivulja genusa 1) koja je $\overline{K}$-izomorfna sa $E$.

Neka je $C/K$ twist od $E/K$. Tada postoji izomorfizam $\phi : C \to E$, koji je definiran nad $\overline{K}$. Da mi izmjerili koliko je "daleko" $\phi$ od toga da bude definiran nad $K$, promatramo preslikavanje

$$\xi : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Isom}(E), \;\; \xi(\sigma) = \phi^\sigma \phi^{-1}.$$

**Teorem 51.** *Neka je $E$ eliptička krivulja. Za svaki twist $C/K$ od $E/K$, izaberimo $\overline{K}$-izomorfizam $\phi : C \to E$ i preslikavanje $\xi(\sigma) = \phi^\sigma \phi^{-1} \in \mathrm{Isom}(E)$ kao iznad.*

(a) *Preslikavanje $\xi$ je 1-kociklus, tj.*

$$\xi(\sigma\tau) = \xi(\sigma)^\tau \xi(\tau) \text{ za sve } \sigma, \tau \in \mathrm{Gal}(\overline{K}/K).$$

*Pripadajuću kohomološku klasu u $H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{Isom}(E))$ označavamo s $\{\xi\}$.*

(b) *Kohomološka klasa $\{\xi\}$ je određena s $K$-izomorfizam klasom od $C$ i neovisna je o izboru izomorfizma $\phi$. Drugim rječima prirodno dobivamo preslikavanje*

$$\mathrm{Twist}(E/K) \to H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{Isom}(E)).$$

(c) *Preslikavanje iz (b) je bijekcija.*

Mi ćemo dokazati samo (a). Dokazi od (b) i (c) se mogu naći u [14, X.2.3].

*Dokaz.* (a) Vrijedi

$$\xi(\sigma\tau) = \phi^{\sigma\tau}\phi^{-1} = (\phi^\sigma\phi^{-1})^\tau(\phi^\tau\phi^{-1}) = \xi(\sigma)^\tau\xi(\tau).$$

□

*Napomena.* Primjetimo da $H^1(\mathrm{Gal}(\overline{K}/K))$ nije grupa, te da je preslikavanje u b) najobičnije preslikavanje skupova.

**Primjer 27.** Neka je $E/K$ eliptička krivulja zadana Weierstrassovom jednadžbom

$$E : y^2 = f(x),$$

te neka je $K(\sqrt{d})$ kvadratno proširenje od $K$, te neka je

$$\chi : \mathrm{Gal}(\overline{K}/K) \to \{\pm 1\}, \quad \chi(\sigma) = \frac{\sqrt{d}^\sigma}{\sqrt{d}}$$

*kvadratni karakter* pridružen $K(\sqrt{d})/K$. Lako se provjeri da je $\chi$ kociklus. Twist $C/K$ od $E/K$ koji odgovara ovom kociklusu, tada ima jednadžbu

$$C : dy^2 = f(x),$$

te je $\phi \in \mathrm{Isom}(E)$ sa $C$ u $E$ zadan sa $\phi(x, y) = (x, y\sqrt{d})$. Kažemo da je $C$ twist od $E$ sa $d$ ili twist sa $\chi$. Taj twist se označava sa $E^d$ (ili nekad u literaturi $E^\chi$).

Ovakvi twistovi se zovu kvadratni twistovi.

# Poglavlje 15

# Torzori

Neka je $G = \mathrm{Gal}(\overline{K}/K)$. Sjetimo se Kummerovog niza za $E/K$:

$$0 \longrightarrow \tfrac{E(K)}{mE(K)} \xrightarrow{\delta} H^1(G, E[m]) \xrightarrow{[m]} H^1(G, E(\overline{K}))[m] \longrightarrow 0.$$

Sada nam je cilj razumjeti treći član ovog egzaktnog niza; u tu svrhu ćemo svakom elementu iz $H^1(G, E(\overline{K}))$ pridružiti twist (definiran kao u prošlom poglavlju) od $E$ koji se naziva *torzor* ili *(glavni) homogeni prostor*.

Počet ćemo tako da definiramo torzore i njihova svojstva, te ćemo onda uspostaviti njihovu kohomološku interpretaciju.

**Definicija.** Neka je $E/K$ eliptička krivulja. *Torzor* od $E/K$ (ili $E$-torzor) je glatka krivulja $C/K$ zajedno sa slobodnom tranzitivnom (desnom) grupovnom akcijom od $E$ na $C$ koja je definirana nad $K$. Drugim rječima, $E$-torzor je par $(C, \mu)$, gdje je $C/K$ glatka krivulja i

$$\mu : C \times E \to C$$

je morfizam definiran nad $K$ koji ima sljedeća svojstva

1. $\mu(p, O) = p$ za sve $p \in C$;
2. $\mu(\mu(p, P), Q) = \mu(p, P + Q)$ za sve $p \in C$ i $P, Q \in E$;
3. Za sve $p, q \in C$, postoji jedinstveni $P \in E$ takav da je $\mu(p, P) = q$.

Iako se iz definicije torzora ovo može činiti kao neprirodna konstrukcija, sjetimo se da je $E(\overline{K})$ grupa, a da grupe vole djelovati na druge objekte. Prirodno je pisati $\mu(p, P)$ kao $p+P$. Iako ćemo za dvije različite binarne operacije koristiti $+$, ovisno o domeni (i kodomeni) bit, će jasno o kojoj se operaciji radi.

Drugo je svojstvo jednostavno "asocijativnost":

$$(p + P) + Q = p + (P + Q).$$

*Napomena.* Primjetimo da je $E$ također $E$-torzor, gdje je operacija $+$ uobičajeno zbrajanje na eliptičkim krivuljama.

Koristeći svojstvo 3. možemo definirati "minus operaciju" na $C$

$$- : C \times C \to E,$$

koja šalje $(q, p)$ u jedinstveni $P \in E$ takav da je $p + P = q$.

Operacije $+$ i $-$ imaju sljedeća svojstva.

**Lema 52.** *Vrijedi:*

1. $- : C \times C \to E$ *je morfizam definiran nad* $K$.
2. $p + O = p \;\; i \;\; p - p = O$.
3. $p + (q - p) = q \;\; i \;\; (p + P) - p = P$.
4. $(q + Q) - (p + P) = (q - p) + Q - P$

Sada ćemo pokazati da je $C/K$ twist od $E/K$.

**Propozicija 53.** *Neka je $E/K$ eliptička krivulja, i neka je $C/K$ $E$-torzor. Fiksirajmo točku $p_0 \in C$, te definirajmo*

$$\Phi : E \to C, \quad \Phi(P) = p_0 + P.$$

*Tada je $\phi$ izomorfizam krivulja genusa 1 definiran nad $K(p_0)$. Drugim rječima, $C/K$ je twist od $E/K$.*

*Dokaz.* Prvo primjetimo da je djelovanje od $E$ na $C$ definirano nad $K$. Neka je $\sigma \in \mathrm{Gal}(\overline{K}/K)$ takav da $p_0^\sigma = p_0$. Imamo

$$\Phi(P)^\sigma = (p_0 + P)^\sigma = p_0^\sigma + P^\sigma = p_0 + P^\sigma = \Phi(P^\sigma),$$

iz čega slijedi da je $\Phi$ definiran nad $K(p_0)$. Iz svojstava torzora se lako vidi da je $\Phi$ stupnja 1, a morfizam stupnja 1 je izomorfizam. □

**Definicija.** Dva $E$-torzora $C/K$ i $C'/K$ su *ekvivalentna* ako postoji izomorfizam $\Phi : C \to C'$ koji je definiran nad $K$, te koji je kompatibilan s djelovanjem od $E$ na $C$ i na $C'$, tj.

$$\Phi(p + P) = \Phi(p) + P \text{ za sve } p \in C,\ P \in E.$$

Klasa ekvivalencije od $E/K$ (koja djeluje na $E$ translacijom) je *trivijalna klasa*. Skup klasa ekvivalencija $E$-torzora se zove *Weil-Châteletova grupa za $E/K$* i označava se s $\mathrm{WC}(E/K)$.

Nameće se prirodno pitanje: koji su torzori trivijalni? Odgovor daje sljedeća propozicija.

**Propozicija 54.** *Neka je $C/K$ $E$-torzor. Tada je $C/K$ u trivijalnoj klasi ako i samo ako je $C(K) \neq \emptyset$.*

*Dokaz.* Pretpostavimo da je $C/K$ u trivijalnoj klasi. Tada postoji $K$-izomorfizam $\Phi : E \to C$, pa je $\Phi(O) \in C(K)$.

Obrnuto pretpostavimo da je $p_0 \in C(K)$. Tada je iz Propozicije 53

$$\Phi : E \to C, \quad \Phi(P) = p_0 + P$$

izomorfizam koji je definiran nad $K(p_0) = K$. Traženi uvjet kompatibilnosti u $\Phi$ je

$$p_0 + (P + Q) = (p_0 + P) + Q,$$

koji slijedi iz definicije torzora. □

Glavni razlog zašto proučavamo torzore je sljedeći teorem.

**Teorem 55.** *Neka je $E/K$ eliptička krivulja. Tada postoji bijekcija*

$$\mathrm{WC}(E/K) \to H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K}))$$

*definirana na sljedeći način:*

*Neka je $C/K$ $E$-torzor, te izabreimo proizvoljnu točku $p_0 \in C$. Tada preslikavamo*

$$[C/K] \to [\sigma \mapsto p_0^\sigma - p_0],$$

*gdje uglate zagrade označavaju klasu ekvivalencije.*

*Napomena.* Primjetimo da iz ovog teorema slijedi da je $\mathrm{WC}(E/K)$ grupa - pošto znamo da je $H^1(\mathrm{Gal}(\overline{K}/K), E(\overline{K}))$ grupa.

# Poglavlje 16

# Selmerova i Tate-Šafarevičeva grupa

U ovom poglavlju ćemo preciznije definirati dvije gore navedene grupe, koje su vrlo bitne u razumijevanju ranga.

Ranije smo pokušavali dobiti informacije preko $E(K)/mE(K)$ (gdje smo ulagali $E(K)/mE(K)$ u neku kohomološku grupu). Možemo umjesto izogenije $[m] : E \to E$ koristiti izogeniju $\phi : E \to E'$, gdje je $E'$ neka izogena krivulja. Tako ćemo doći do informacija o rangu preko grupe $E'(K)/\phi(E(K))$ (sjetimo se da izogene krivulje imaju isti rang).

Označimo s $E[\phi] = \operatorname{Ker}\phi$, u skladu s $E[m] = \operatorname{Ker}[m]$. Sjetimo se da kada pišemo $E$, bez polja, mislimo na grupu $E(\overline{K})$. Sada imamo egzaktni niz

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0\cdot$$

Uzimanjem $\mathrm{Gal}(\overline{K}/K)$-invarijanti, dobivamo dugi egzaktni niz

$$0 \longrightarrow E(K)[\phi] \longrightarrow E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta}$$

$$H^1(\mathrm{Gal}(\overline{K}/K), E[\phi]) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), E) \xrightarrow{\phi} H^1(\mathrm{Gal}(\overline{K}/K), E'),$$

gdje je u ovom nizu $\phi$ induciran iz prethodnog egzaktnog niza.

Iz ovog egzaktnog niza, kao i prije, dobivamo kratki egzaktan niz

$$0 \to E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(\mathrm{Gal}(\overline{K}/K), E[\phi]) \to H^1(\mathrm{Gal}(\overline{K}/K), E)[\phi] \to 0.$$

Sve grupe iznad, koje su definirane nad poljem $K$, možemo uložiti u analognu grupu definiranu nad lokalnim poljem $K_v$ za sva mjesta $v \in M_K$. Primjetimo na primjer da ako $E(K)$ ima neku točku, tada je ta točka definirana i nad $\prod_{v\in M_K} E(K_v)$. Analogno vrijedi i za kohomološke grupe iz navedenih egzaktnih nizova. S $G_v$ ćemo označavati podgrupu od $\mathrm{Gal}(\overline{K}/K)$ koja fiksira $v$, pa onda djeluje na $K_v$ i $E(K_v)$.

Prebacivanjem iz $K$ u $K_v$ dobivamo kratki egzaktni niz:

$$0 \to E'(K_v)/\phi(E(K_v)) \xrightarrow{\delta} H^1(G_v, E[\phi]) \to H^1(G_v, E)[\phi] \to 0.$$

Jedan od ključnih koraka (koji mi nismo dokazivali) u dokazu Slabog Mordell-Weilovog teorema je da je druga grupa u ovom nizu tj. $H^1(G_v, E[\phi])$ konačna, te da se $H^1(\mathrm{Gal}(\overline{K}/K), E[\phi])$ ulaže u nju.

Označimo $G := \mathrm{Gal}(\overline{K}/K)$. Sada se može spajanjem egzaktnih nizova nad $K$ i nad $K_v$ može dobiti sljedeći komutativni dijagram.

$$\begin{array}{ccccccc}
0 \to E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(G, E[\phi]) & \longrightarrow & \mathrm{WC}(E/K)[\phi] \to 0 \\
\downarrow & & \downarrow & & \downarrow \\
0 \to \prod\limits_{v\in M_K} E'(K_v)/\phi(E(K_v)) & \xrightarrow{\delta} & \prod\limits_{v\in M_K} H^1(G_v, E[\phi]) & \longrightarrow & \prod\limits_{v\in M_K} \mathrm{WC}(E/K_v)[\phi] \to 0,
\end{array}$$

gdje smo zamijenili $H^1(G, E)$ sa $\mathrm{WC}(E/K)$, te gdje su retci egzaktni.

Naš konačni cilje je razumjeti sliku od $E'(K)/\phi(E(K))$ u $H^1(G, E[\phi])$ ili ekvivalentno jezgru od

$$H^1(G, E[\phi]) \to \mathrm{WC}(E/K)[\phi].$$

To je ekvivalentno određivanju imaju li određeni $E$-torzori $K$-racionalnu točku ili ne. Primjetimo da je to zapravo ono što smo radili u primjeru 26. Međutim, kao što smo više puta spomenuli, u općem slučaju to može biti teško. Ono što sigurno možemo izračunati je

$$\mathrm{Ker}\left(H^1(G_v, E[\phi]) \to \mathrm{WC}(E/K_v)[\phi]\right);$$

pošto zbog Henselove leme potrebno je samo provjeriti ima li torzor točku nad konačnim poljem.

**Definicija.** Neka je $\phi : E/K \to E'/K$ izogenija. Tada je *$\phi$-Selmerova grupa od $E/K$* podgrupa od $H^1(\mathrm{Gal}(\overline{K}/K), E[\phi])$ definirana s

$$S^{\phi}(E/K) = \mathrm{Ker}\left\{H^1(\mathrm{Gal}(\overline{K}/K), E[\phi]) \to \prod_{v\in M_K} \mathrm{WC}(E/K_v)\right\}.$$

*Tate-Šafarevičeva grupa od $E/K$* je podgrupa od $\mathrm{WC}(E/K)$ definirana s

$$Ш(E/K) = \mathrm{Ker}\left\{\mathrm{WC}(E/K) \to \prod_{v\in M_K} \mathrm{WC}(E/K_v)\right\}.$$

*Napomena.* Selmerovu grupu je dobro zamišljati kao svugdje lokalno rješive torzore. Točnije, to su 1-kociklusi koji se preslikaju u takve torzore.

Netrivijalne elemente od $Ш(E/K)$ je dobro zamišljati kao $E$-torzore koji imaju lokalno točku svuda, a nemaju globalnu (modulo ekvivalencija).

Iz argumentacije iznad slijedi.

**Teorem 56.** *Neka je $\phi : E/K \to E/K$ izogenija definirana nad $K$. Tada postoji egzaktan niz*

$$0 \longrightarrow E'(K)/\phi(E(K)) \longrightarrow S^{(\phi)}(E/K) \longrightarrow Ш(E/K)[\Phi] \longrightarrow 0.$$

*Napomena.* Slabi Mordell-Weilov teorem nam zapravo kaže da je $S^{(\phi)}(E/K)$ konačna grupa.

Primjetimo da smo u primjeru 26 zapravo dobili

$$S^{(2)}(E/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \quad \text{i} \quad Ш(E/\mathbb{Q})[2] = 0.$$

Kako dobiti eksplicitno elemente $Ш(E/K)[\phi]$? Dajmo skicu jednog primjera.

**Propozicija 57.** *Neka je $p \equiv 1 \pmod 8$ takav da 2 nije četvrta potencija modulo $p$, te neka je $E$ eliptička krivulja*

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

*Tada je rang od $E(\mathbb{Q})$ jednak 0, te je $Ш(E/\mathbb{Q})[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$.*

Za dokaz ćemo koristiti sljedeću lemu čiji dokaz ostavljamo za vježbu.

**Lema 58.** *Neka je $E$ kao u prethodnoj propoziciji. Tada je $S^{(2)}(E/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^3$.*

Trebat će nam i sljedeća lema iz algebarske geometrije, koja nam kaže da krivulje genusa 1 imaju točke nad $\mathbb{F}_p$ gdje je $p$ prost broj u kojem uimaju dobru redukciju.

**Lema 59** ([10], Corollary 9.3.)**.** *Nesingularna projektivna krivulja $C$ genusa 1 nad $\mathbb{F}_p$ ima točku s koordinatama u $\mathbb{F}_p$.*

Treba nam i sljedeći poznati rezultat iz teorije brojeva.

**Teorem 60** (Gaussov zakon kvadratnog reciprociteta)**.** *Neka su $p$, $q$ neparni prosti brojevi. Tada je*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

*Također,*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

*Dokaz Propozicije 57.* Kako je $S^{(2)} \simeq (\mathbb{Z}/2\mathbb{Z})^3$, te kako jedna kopija $\mathbb{Z}/2\mathbb{Z}$ dolazi od torzije od $E$, da bi dokazali da je $Ш(E/\mathbb{Q})[2]$ kao u tvrdnji propozicije, mi ćemo konstruirati njene elemente.

To će biti torzori

$$y^2 = 4px^4 - 1 \text{ i } \pm y^2 = 2px^4 - 2.$$

Lako se provjeri da su to $E$-torzori.

Mi ćemo skicirati dokaz da

$$C : y^2 = 2 - 2px^4$$

nema točke u $\mathbb{Q}$, a ima lokalno točke svuda. Pretpostavimo suprotno, tj. neka je $(x, y)$ točka na ovoj krivulji i neka je $x = r/t$, gdje su $r, t$ relativno prosti cijeli brojevi. Tada je

$$y^2 = \frac{2t^4 - 2pr^4}{t^4}.$$

Brojnik i nazivnik na desnoj strani nemaju zajednički faktor, pa $2t^4 - 2pr^4$ mora biti kvadrat (parnog) cijelog broja. Dakle postoji cijeli broj $s$ takav da je

$$2s^2 = t^4 - pr^4.$$

Neka je $q$ prost broj koji djeli $s$. Tada je $t^4 \equiv pr^4 \pmod{q}$, pa je $\left(\frac{p}{q}\right) = 1$. Po Gaussovom zakonu o reciprocitetu, slijedi da je $\left(\frac{q}{p}\right) = 1$, te da je $\left(\frac{2}{p}\right) = 1$, dakle svi prosti faktori od $s$ su kvadrati modulo $p$. Dakle $s^2$ je četvrta potencija modulo $p$. Jednadžba

$$2s^2 \equiv t^4 \pmod{p}$$

dalje pokazuje da je 2 četvrta potencija modulo $p$, što je kontradikcija s početnom hipotezom. Trebalo bi još provjeriti da ova krivulja nema $\mathbb{Q}$ racionalnu točku u beskonačnosti, te to ostavljamo za vježbu.

Ostaje dokazati da krivulja ima lokalne točke svuda. Očito je da ima točaka nad $\mathbb{R}$, te iz leme 59 i Henselove leme slijedi da ima točke nad $\mathbb{F}_q$ za $q \neq 2, p$, pošto krivulja ima dobru redukciju u $q$. Za $q = 2, p$ dokaz zahtijeva malo finiju upotrebu Henselove leme, koju također ostavljamo za vježbu. □

Recimo još nekoliko činjenica o $Ш(E/\mathbb{Q})$. Jedna od najvažnijih slutnji u teoriji eliptičkih krivulja je sljedeća.

**Slutnja 61.** *Neka je $E/K$ eliptička krivulja. Tada je $Ш(E/\mathbb{Q})$ konačna.*

Smatra se da je ova slutnja najveća zapreka u dokazivanju Birch–Swinnerton-Dyerove slutnje (o kojoj će biti više riječi poslije). Svi dokazani slučajevi BSD slutnje se baziraju na dokazivanju činjenice da je $Ш(E/\mathbb{Q})$ konačna za te krivulje.

Element $g$ grupe $G$ je *djeljiv* ako za svaki $n \in \mathbb{N}$ postoji $a_n \in G$ takav da je $n \cdot a_n = g$. Iskažimo sada za kraj sljedeći teorem.

**Teorem 62.** *Neka je $E/K$ eliptička krivulja. Tada postoji alternirajuće bilinearno sparivanje*

$$\Gamma : Ш(E/\mathbb{Q}) \times Ш(E/\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z},$$

*čija su lijeva i desna jezgra podgrupa djeljivih elemenata od $Ш(E/\mathbb{Q})$.*

Iz ovog teorema slijedi da ako je $Ш(E/\mathbb{Q})$ konačna, tada je red od $Ш(E/\mathbb{Q})$ kvadrat pa je i svaki $Ш(E/\mathbb{Q})[n]$ kvadrat, što povlači da se rang $E/K$ i rang $n$-Selmerove grupe razlikuju za paran broj.

**Slutnja 63** (Slutnja o parnosti)**.** *Selmerov rang i rang eliptičke krivulje su iste parnosti.*

Braća Dokchitser su 2010. dokazali da Slutnja o parnosti slijedi iz slabije pretpostavke da su 2-dio i 3-dio (tj. elementi čiji je red djeljiv samo s 2 ili 3) od $Ш(E/\mathbb{Q})$ konačni.

# Poglavlje 17

# Spust pomoću 2-izogenija

Na analogan način kao i za običan 2-spust može se napraviti i spust pomoću 2-izogenija (ili tzv. 2-izogenija spust). Detalji se mogu naći u [14, X.3. i X.4.]; mi ćemo samo iskazati rezultat te demonstrirati njegovu primjenu. Primjetimo da nam je 2-izogenija spust u praksi često korisniji od običnog 2-spusta. Ako je $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, tada se nad poljem $K$ može provesti 2-izogenija spust, dok se 2-spust ne može (za njega bi se trebalo raditi nad poljem $L/K$ takvim da je $E[2] \subset E(L)$).

Također, općenito je postpuak spusta pomoću 2-izogenija jednostavniji i zahtijeva promatranje puno manje torzora.

**Propozicija 64** (Spust pomoću 2-izogenija)**.** *Neka je $E/K$ dana s*

$$E : y^2 = x^3 + ax^2 + bx,$$

*te neka je njoj 2-izogena krivulja $E'/K$ dana s*

$$E' : y^2 = x^3 - 2ax^2 + (a^2 - b)x$$

*i neka je*

$$\phi : E \to E', \;\; \phi(x, y) = \left( \frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right),$$

*izogenija stupnja 2 s jezgrom $E[\phi] = \{O, (0, 0)\}$. Neka je*

$$S = M_K^\infty \cup \left\{ v \in M_K^0 : \mathrm{ord}_v(2) \neq 0 \text{ \textit{ili} } \mathrm{ord}_v(b) \neq 0 \text{ \textit{ili} } \mathrm{ord}_v(a^2 - 4b) \neq 0 \right\}.$$

*Za svaki $d \in K^*$, neka je $C_d/K$ $E$-torzor dan s jednadžbom*

$$C_d : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

*Tada postoji egzaktan niz*

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} K(S, 2) \xrightarrow{\lambda} \mathrm{WC}(E/K)[\phi],$$

*gdje je*

$$\delta(x,y) = \begin{cases} x & (x,y) \neq O,(0,0), \\ 1 & (x,y) = O, \\ a^2 - 4b & (x,y) = (0,0), \end{cases}$$

$$\lambda(d) = C_d.$$

*Tada je $\phi$-Selmerova grupa*

$$S^{(\phi)}(E/K) \simeq \{d \in K(S,2) : C_d(K_v) \neq 0 \text{ za sve } v \in S\}.$$

*Preslikavanje*

$$\psi : C_d \to E', \psi(z,w) = \left(\frac{d}{z^2}, \frac{-dw}{z^3}\right),$$

*ima svojstvo da ako je $P \in C_d(K)$, tada je*

$$\delta(\psi(p)) \equiv d \pmod{(K^*)^2}.$$

*Napomena.* Za dobiti $E(K)/2E(K)$ neće nam biti dosta promotriti samo $E'(K)/\phi(E(K))$, već će trebati i pogledati i $E(K)/\hat{\phi}(E'(K))$. Promotrimo egzaktan niz

$$0 \longrightarrow \frac{E'(K)[\hat{\phi}]}{\phi(E(K)[2])} \longrightarrow \frac{E'(K)}{\phi(E(K))} \xrightarrow{\hat{\phi}} \frac{E(K)}{2(E(K))} \longrightarrow \frac{E(K)}{\hat{\phi}(E'(K))} \longrightarrow 0. \tag{17.1}$$

Drugi i četvrti član niza se mogu izračunati pomoću propozicije 64, dok je $E'(K)[\hat{\phi}] \simeq \mathbb{Z}/2\mathbb{Z}$, te je $\phi(E(K)[2]) \simeq 0$ ako je $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z}$, dok je $\phi(E(K)[2]) \simeq \mathbb{Z}/2\mathbb{Z}$ ako je $E(K)[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

**Primjer 28.** Neka je

$$E : y^2 = x^3 - 6x^2 + 17x.$$

Diskriminanta $\Delta(E) = -147968 = -2^9 17^2$, pa je $S = \{\infty, 2, 17\}$, te definiramo $\mathbb{Q}(S,2) := \{\pm 1, \pm 2, \pm 17, \pm 34\}$. Ova krivulja je 2-izogena s

$$E' : y^2 = x^3 + 12x^2 - 32x,$$

te je za $d \in \mathbb{Q}(S,2)$, odgovarajući homogeni prostor

$$C_d : dw^2 = d^2 + 12dz^2 - 32z^4.$$

1. Odredimo prvo torziju od $E(\mathbb{Q})$ i $E'(\mathbb{Q})$. Standardnim metodama dobivamo
$$E(\mathbb{Q})_{tors} \simeq E'(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z}.$$

2. Iz propozicije 64 znamo da se točka $\delta(O) = 1$, te da $\delta$ preslikava $(0,0) \in E'(\mathbb{Q})$ preslikava u
$$\delta(0,0) \equiv -32 \equiv -2 \pmod{(\mathbb{Q}^*)^2},$$
pa je $-2 \in S^{(\phi)}(E/\mathbb{Q})$.

3. Slučaj $d = 2$: Imamo

$$C_2 : 2w^2 = 4 + 24z^2 - 32z^4,$$

te nakon dijeljenja s 2 dobivamo

$$C_2 : w^2 = 2 + 12z^2 - 16z^4,$$

te normiramo polinom s lijeve strane i uzimanjem $u = 2z$ dobivamo

$$w^2 = 2 + 3u^2 - u^4,$$

te ova krivulja ima očitu točku $(u, w) = (1, 2)$, pa je točka $\left(\frac{1}{2}, 2\right) \in C_2(\mathbb{Q})$. Vrijedi $\psi\left(\frac{1}{2}, 2\right) = (8, -32) \in E'(\mathbb{Q})$. Također, lako provjerimo da je $\delta(8, -32) = 8 \equiv 2 \pmod{(\mathbb{Q}^*)^2}$.

4. Slučaj $d = 17$ Imamo

$$C_{17} : 17w^2 = 17^2 + 12 \cdot 17z^2 - 32z^4.$$

Dokazat ćemo da je $C_{17}(\mathbb{Q}_{17}) = \emptyset$ tako da dokažemo da najveće potencije od 17 koje dijeli lijevu i desnu strana moraju biti različite. Kako je $\mathrm{ord}_{17}(17w^2)$ neparan, a $\mathrm{ord}_{17}(32z^4)$ paran, vidimo da kada bi nazivnik od $z$ bio djeljiv sa 17, tada bi došli do kontradikcije. Dakle, dobivamo da nazivnik od $z$ nije djeljiv s 17, pa onda lako vidimo da je $z \equiv 0 \pmod{17}$, iz čega nadalje slijedi da je $w \equiv 0 \pmod{17}$. Sada imamo da je lijeva strana $\equiv 0 \pmod{17^3}$, a desna strana je $\equiv 17^2 \pmod{17^3}$. Dakle, $17 \notin S^{(\phi)}(E/\mathbb{Q})$.

5. Kao i u 2-spustu, koristimo svojstvo da je $S^{(\phi)}$ grupa. Pošto su $1, -2, 2 \in S^{(\phi)}$ slijedi da je $-2 \cdot 2 = -1 \in S^{(\phi)}$, te pošto je $17 \notin S^{(\phi)}$, imamo da je $17 \cdot a \notin S^{(\phi)}$, gdje je $a \in \{\pm 1, \pm 2\}$. Time smo dokazali da je

$$S^{(\phi)} = \{\pm 1, \pm 2\}.$$

6. Sada treba izračunati $S^{(\hat{\phi})}$; to radimo tako da samo zamijenimo $E$ i $E'$. Sada za $d \in \mathbb{Q}(S, 2)$ promotramo torzore

$$C'_d : dw^2 = d^2 - 24dz^2 + 272z^4.$$

Kao i prije $\delta(O) = 1$, $\delta(0, 0) = 272 \equiv 17 \pmod{(\mathbb{Q}^*)^2}$.

7. Ako je $d < 0$, tada je očito $C'_d(\mathbb{R}) = \emptyset$, te $d \notin S^{(\hat{\phi})}$.

8. Promotrimo $d = 2$. Sada je

$$C'_2 : 2w^2 = 4 - 12z^2 + 17z^4.$$

Dokazat ćemo da je $C'_2(\mathbb{Q}_2) = \emptyset$ tako da dokažemo da su 2-adske valuacije lijeve i desne strane različite. Pretpostavimo da $C'_2$ ima racionalnu točku. Prvo primjetimo da je $\mathrm{ord}_2(2w^2)$ neparna, a da je 2-adska valuacija desne strane parna. Iz toga zaključujemo da nazivnici od $z$ i $w$ nisu djeljivi s 2. Sada prvo zaključimo da je $z$ djeljiv s 2, pa onda iz toga da je $w \equiv 0 \pmod 2$. Sada imamo kongruenciju $0 \equiv 4 \pmod 8$.

9. Kao i prije, iz činjenice da je $S^{(\hat{\phi})}$ grupa, zaključujemo da je $S^{(\hat{\phi})} = \{1, 17\}$.

Također primjetimo da smo za sve elemente od $S^{(\phi)}$ i $S^{(\hat{\phi})}$ našli točku koja se preslika u odgovarajući torzor, te iz toga zaključujemo da je $Ш(E/\mathbb{Q})[\phi] = \emptyset$ i $Ш(E'/\mathbb{Q})[\hat{\phi}] = \emptyset$.

Iz toga zaključujemo da je

$$E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \simeq S^{(\phi)} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \text{ i } E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q})) \simeq S^{(\hat{\phi})} \simeq \mathbb{Z}/2\mathbb{Z}.$$

Sada uvrštavamo dobiveno u egzaktan niz (17.1), za $E/\mathbb{Q}$:

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow \tfrac{E(K)}{2(E(K))} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

i za $E'/\mathbb{Q}$:

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \tfrac{E'(K)}{2(E'(K))} \longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow 0.$$

U oba slučaja dobivamo

$$E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \text{ i } E'(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}.$$

# Poglavlje 18

# $L$-funkcije pridružene eliptičkim krivuljama i Birch–Swinnerton-Dyerova slutnja

$L$-funkcija eliptičke krivulje je funkcija koje prikuplja "globalne" informacije o eliptičkoj krivulji iz lokalnih informacija.

Neka je $E/\mathbb{Q}$ eliptička krivulja (definicija se lako generalizira na općenita PAB) s minimalnim modelom. Neka je $\Delta$ (minimalna) diskriminata od $E$. Definirajmo $a_p$ na sljedeći način:

$$a_p = \begin{cases} p+1-|E(\mathbb{F}_p)| & \text{ako } p \nmid \Delta, \\ 1 & \text{ako } E \text{ ima rascjepivu multiplikativnu redukciju u } p, \\ -1 & \text{ako } E \text{ ima nerascjepivu multiplikativnu redukciju u } p, \\ 0 & \text{ako } E \text{ ima aditivnu redukciju u } p. \end{cases}$$

Uz notaciju kao gore i uz pretpostavku da je $E$ zadana u minimalnom modelu, imamo sljedeću definiciju.

**Definicija.** $L$-funkcija eliptičke krivulje $E/\mathbb{Q}$ je dana sa

$$L_E(s) = \prod_{p \nmid \Delta} \frac{1}{1 - a_p \cdot p^{-s} + p^{1-2s}} \cdot \prod_{p \mid \Delta} \frac{1}{1 - a_p \cdot p^{-s}}. \tag{18.1}$$

Produkt u (18.1) se može zapisati i kao red

$$L_E(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}. \tag{18.2}$$

Lako je vidjeti da ovaj red konvergira kada je realan dio od $s$ veći od $\frac{3}{2}$. Jedna od posljedića *Teorema o modularnosti* kojeg ćemo kasnije spomenuti je da postoji analitičko proširenje od $L_E(s)$ na cijeli $\mathbb{C}$.

Posebno je bitna vrijednost od $L_E$ u točki $s = 1$.

**Definicija.** Red nultočke $L$-funkcije $L_E$ eliptičke krivulje $E/\mathbb{Q}$ u točki $s = 1$ se naziva *analitički rang od* $E/\mathbb{Q}$.

Vrijednost koju smo mi nazivali rang se često naziva i algebarski rang od $E/\mathbb{Q}$. Kao što se može i naslutiti, očekuje se da su algebarski i analitički rang jednaki, i o tome nam govori jedna od najvažnijih slutnji u teoriji eliptičkih krivulja, Birch–Swinnerton-Dyerova slutnja. BSD slutnja je jedan od "Milenijskih problema" za čije se rješenje nudi milijun dolara nagrade. U svojoj najjednostavniji formulaciji (u kojoj se i pojavljuje na listi Milenijskih problema) glasi

**Slutnja 65** (Birch–Swinnerton-Dyer)**.** *Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada su njezini algebarski i analitički rang jednaki.*

Primjetimo da slutnja povlači da je

$$L(E, 1) \neq 0 \iff \mathrm{rk}(E/\mathbb{Q}) = 0,$$

gdje $\mathrm{rk}(E/\mathbb{Q})$ označava (algebarski) rang od $E/\mathbb{Q}$. S $\mathrm{rk}_{an}$ ćemo označavati analitički rang.

Otkuda je uopće došla BSD-slutnja? Primjetimo iz (18.1) da $L$-funkcija broji koliko točaka imaju redukcije eliptičkih krivulja. Na jednom od uopće prvih računa rađenima na računalima (u 1960-ima) su Birch i Swinnerton–Dyer primjetili da eliptičke krivulje s većim rangom u pravilu imaju više točaka u svojim redukcijama. Točnije primjetili su da

$$\prod_{p \leq x} \frac{|E(\mathbb{F}_p)|}{p} \sim C \log(x)^{\mathrm{rk}(E/\mathbb{Q})} \text{ kada } x \to \infty.$$

Najjači rezultat (koji je zapravo sastavljen od 2 zasebna teorema) je

**Teorem 66** (Gross-Zagier; Kolyvagin)**.** *Ako je* $\mathrm{rk}_{an}(E/\mathbb{Q}) \leq 1$*, tada je*

$$\mathrm{rk}(E/\mathbb{Q}) = \mathrm{rk}_{an}(E/\mathbb{Q}).$$

Sjetimo se da očekujemo da 100% krivulja (kad poredamo po veličini koeficijenata) ima (algebarski) rang 0 ili 1, pa (pošto očekujemo da je BSD slutnja istinita) onda Gross-Zagierov i Kolyvaginov teorem nam zapravo kažu da očekujemo da će 100% krivulja zadovoljavati BSD slutnju.

Spomenimo da bi BSD slutnja imala mnoge direktne posljedice, npr. da bi tada odmah bio riješen i dva tisućljeća star problem kongruentnih brojeva.

Postoji i jača verzija Birch–Swinnerton-Dyerove slutnje, koja predviđa koliki je vodeći koeficijent u razvoju od $L_E(s)$ oko $s = 1$.

**Slutnja 67** (Birch-Swinnerton–Dyerova slutnja, jača verzija)**.** *Uz notaciju kao i prije vrijedi* $r = \mathrm{rk}_{an}(E/\mathbb{Q})$*, te*

$$\frac{L_E(1)^{(r)}}{r!} = \frac{|Ш(E/\mathbb{Q})|\Omega_E R_E \prod_{p|\Delta} c_p}{|E(\mathbb{Q})_{tors}|^2}, \tag{18.3}$$

*gdje je* $\Omega_E$ *realni period,* $R_E$ *regulator, te su* $c_p$ *Tamagawini brojevi.*

Vrijednosti $\Omega_E$, $R_E$, $\prod_{p|\Delta} c_p$ nećemo definirati; recimo samo da su to vrijednosti koje dobro razumijemo, kao i $|E_(\mathbb{Q})_{tors}|$. Dakle (18.3) se može i zapisati kao

$$\frac{L_E(1)^r}{r!} = C(E)|Ш(E/\mathbb{Q})|,$$

gdje je $C(E)$ neka konstanta, ovisna o eliptičkoj krivulji. Primjetimo da je tek prije par godina dokazano da $L_E(s)$ uopće konvergira u $s = 1$, te da se ne zna da je $Ш(E/\mathbb{Q})$ konačna grupa, što je ponukalo Johna Tatea da (prije dvadesetak godina) o ovoj slutnji kaže: *Ova izuzetna slutnja povezuje ponašanje funkcije* $L$ *u točki u kojoj nije poznato da je* $L$ *definirana s redom grupe za koju nije poznato da je konačna.*

# Poglavlje 19

# Modularne krivulje

U ovom poglavlju ćemo slijediti [2, Chapter 1]. Cilj poglavlja je uvesti *modularne krivulje* koje će istovremeno biti kvocijent gornje poluravnine i neke matrične grupe i *prostor parametara* (moduli space na engleskom) klasa izomorfizama eliptičkih krivulja skupa s nekim (torzijskim) svojstvom.

**Modularna grupa** $\mathrm{SL}_2(\mathbb{Z})$ je

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

Modularna grupa je generirana matricama

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ i } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Prisjetimo se da je Riemannova sfera $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. Svaki element modularne grupe se može promatrati i kao automorfizam Riemannove sfere na sljedeći način: neka je $\tau \in \hat{\mathbb{C}}$, tada je

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \frac{a\tau + b}{c\tau + d}.$$

Treba u gornjoj definiciji još napomenuti i da ako $c \neq 0$, tada ovaj automorfizam šalje $-d/c$ u $\infty$, te $\infty$ šalje u $a/c$. Ako je $c = 0$, onda se $\infty$ šalje u $\infty$.

Pošto je modularna grupa generirana sa 2 ranije spomenute matrice, slijedi da se sve transformacije $\hat{\mathbb{C}}$ definirane elementima iz modularne grupe mogu dobiti kompozicijama funkcija

$$\tau \to \tau + 1 \text{ i } \tau \to -1/\tau.$$

**Gornja poluravnina** je

$$\mathcal{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}.$$

Primjetimo da je

$$\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}, \text{ gdje je } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

dakle modularna grupa šalje gornju poluravninu u gornju poluravninu.

Sada ćemo napraviti malu digresiju i definirati što je modularna forma kako bismo mogli izreći Teorem o modularnosti, koji je jedan od najčuvenijih matematičkih rezultata u 21. stoljeću.

**Definicija.** Neka je $k \in \mathbb{Z}$. Meromorfna funkcija $f : \mathcal{H} \to \mathbb{C}$ je **slabo modularna težine** $k$ ako

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau) \text{ za sve } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ i } \tau \in \mathcal{H}.$$

**Definicija.** Neka je $k \in \mathbb{Z}$. Funkcija $f : \mathcal{H} \to \mathbb{C}$ je **modularna forma težine** $k$ ako je

1. $f$ holomorfna na $\mathcal{H}$.
2. $f$ je slabo modularna težine $k$,
3. $f$ je holomorfna u $\infty$, tj. ima Fourierov razvoj

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2i\pi nz}.$$

Često se piše $q = e^{2i\pi z}$, pa zadnji uvjet postaje

$$f(z) = \sum_{n=0}^{\infty} a_n q^n.$$

Spomenimo još da ako modularna forma ima nultočku u $z = \infty$ (ili ekvivalentno u $q = 0$), tada takvu modularna formu nazivamo **kusp formom**.

Izrecimo sada slabu verziju Teorema o modularnosti (postoji i bolja verzija koja daje više informacija).

**Teorem 68** (Teorem o modularnosti)**.** *Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada su koefincijenti $a_n$ u $L_E(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ jednaki koeficijentima u Fourierovom razvoju neke modularne (kusp) forme $f = \sum_{n=1}^{\infty} a_n q^n$.*

Teorem o modularnosti je dokazao 1995. Andrew Wiles (uz pomoć Richarda Taylora) za polustabilne eliptičke krivulje (dakle one koje imaju multiplikativnu redukciju na mjestima gdje imaju lošu redukciju, tj. nigdje nemaju aditivnu redukciju). Posljedica toga je bio Posljednji Fermatov teorem. Teorem o modularnosti za sve eliptičke krivulje su dokazali Cristophe Breuil, Brian Conrad, Fred Diamond i Richard Taylor 2001. godine. Puni teorem o modularnosti je

za posljedicu imao činjenicu da $L$-funkcija eliptičke krivulje nužno konvergira u 1 (dakle jedna strana jednakosti u Birch–Swinnerton-Dyerovoj slutnji sigurno ima smisla).

Nas će zanimati podgrupe modularne grupe.

**Definicija.** Neka je $N$ prirodan broj. Tada je **glavna kongruencijska podgrupa nivoa** $N$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

**Definicija.** Podgrupa $\Gamma$ od $\mathrm{SL}_2(\mathbb{Z})$ je **kongruencijska podgrupa** ako je $\Gamma(N) \leq \Gamma$ za neki $N \in \mathbb{N}$. Neka je $N$ najmanji takav; u tom slučaju kažemo da je $\Gamma$ kongruencijska podgrupa nivoa $N$.

Primjetimo da je svaka $\Gamma(N)$ konačnog indeksa u $\mathrm{SL}_2(\mathbb{Z})$, pa slijedi da je svaka kongruencijska podgrupa također konačnog indeksa.

Osim glavne kongruencijske grupe, bit će nam vrlo bitne i dvije sljedeće kongruencijske podgrupe.

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Vrijedi

$$\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_0(N) \leq \mathrm{SL}_2(\mathbb{Z}).$$

Prisjetimo se sada da je svakoj eliptičkoj krivulji pridružena rešetka $\Lambda \subset \mathbb{C}$, te se može bez smanjenja općenitosti uzeti da je $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$, za neki $\tau \in \mathbb{C}$. Također, možemo bez smanjenja općenitosti uzeti $\tau \in \mathcal{H}$. Također, vrijedi da za $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ vrijedi da su $\Lambda$ i $\mathbb{Z} + \gamma(\tau)\mathbb{Z}$ iste rešetke (vrijedi i obrat). Označimo s

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} = \{\mathrm{SL}_2(\mathbb{Z})\tau : \tau \in \mathcal{H}\}.$$

Zapravo ovdje poistovjećujemo sve elemente $a$ i $b$ takve da je $\gamma(a) = b$ za neki $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Dakle imamo bijekciju između

$$\{ \text{ eliptičke krivulje nad } \mathbb{C} \text{ do na izomorfizam } \} \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}.$$

Kažemo da je $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$ **prostor parametara** za eliptičke krivulje. Vidjet ćemo da na sličan način grupe $\Gamma(N)$, $\Gamma_0(N)$ i $\Gamma_1(N)$ generiraju prostor parametara eliptičkih krivulja s nekim svojstvom.

**Definicija.** Za kongruencijsku podgrupu $\Gamma$ od $\mathrm{SL}_2(\mathbb{Z})$ definiramo **modularnu krivulju** kao kvocijentni prostor orbita od $\Gamma$, to jest

$$Y(\Gamma) = \Gamma\backslash\mathcal{H} = \{\Gamma\tau : \tau \in \mathcal{H}\}.$$

Definirajmo $S_0(N)$ kao skup čiji su elementi $[E, C]$ (uglate zagrade svuda označavaju klasu izomorfizma, gdje je $E$ eliptička krivulja, a $C$ je podgrupa reda $N$ (sve je za sada definirano nad $\mathbb{C}$, nešto kasnije ćemo reći što znače točke nad nekim PAB $K$). Objasnimo što mislimo pod klasa izomorfizma od $[E, C]$; smatramo da su $(E, C)$ i $(E', C')$ izomorfni ako postoji izomorfizam eliptičkih krivulja $f : E \to E'$ takav da je $f(C) = C'$.

Isto tako definirajmo skup $S_1(N)$ kao skup čiji su elementi $[E, Q]$, gdje je $Q$ točka reda $N$, te gdje su $(E, Q)$ i $(E', Q')$ izomorfni ako postoji izomorfizam eliptičkih krivulja $f : E \to E'$ takav da je $f(Q) = Q'$.

Skup $S(N)$ definiramo kao skup klasa izomorfizama od $[E, (P, Q)]$, gdje je $\langle P, Q\rangle \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ i gdje je $e_N(P, Q) = e^{2\pi i/N}$ ($e_N$ je Weilovo sparivanje), te gdje su $(E, Q)$ i $(E', Q')$ izomorfni ako postoji izomorfizam eliptičkih krivulja $f : E \to E'$ takav da je $f(P) = P'$ i $f(Q) = Q'$.

Modularne krivulje za $\Gamma_0(N)$, $\Gamma_1(N)$ i $\Gamma(N)$ se označavaju sa

$$Y_0(N) = \Gamma_0(N)\backslash\mathcal{H},\ Y_1(N) = \Gamma_1(N)\backslash\mathcal{H},\ Y(N) = \Gamma(N)\backslash\mathcal{H}.$$

Sljedeći važan teorem će nam reći što točno parametrizira svaka od ovih modularnih krivulja.

**Teorem 69.** *Neka je $N$ prirodan broj.*

*a) Prostor parametara za $\Gamma_0(N)$ je*

$$S_0(N) = \{[E_\tau, \langle 1/N + \Lambda_\tau\rangle] : \tau \in \mathcal{H}\}.$$

*Dvije točke $[E_\tau, \langle 1/N + \Lambda_\tau\rangle]$ i $[E_{\tau'}, \langle 1/N + \Lambda_{\tau'}\rangle]$ su jednake ako i samo ako je $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. Dakle, postoji bijekcija*

$$\psi_0 : S_0(N) \xrightarrow{\sim} Y_0(N), \quad [\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle] \to \Gamma_0(N)\tau.$$

*b) Prostor parametara za $\Gamma_1(N)$ je*

$$S_1(N) = \{[E_\tau, 1/N + \Lambda_\tau] : \tau \in \mathcal{H}\}.$$

*Dvije točke $[E_\tau, 1/N + \Lambda_\tau]$ i $[E_{\tau'}, 1/N + \Lambda_{\tau'}]$ su jednake ako i samo ako je $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. Dakle, postoji bijekcija*

$$\psi_1 : S_1(N) \xrightarrow{\sim} Y_1(N), \quad [\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] \to \Gamma_1(N)\tau.$$

*c) Prostor parametara za $\Gamma(N)$ je*

$$S(N) = \{[E_\tau, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)] : \tau \in \mathcal{H}\}.$$

*Dvije točke $[E_\tau, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)]$ i $[E_{\tau'}, (\tau'/N + \Lambda_{\tau'}, 1/N + \Lambda_{\tau'})]$ su jednake ako i samo ako je $\Gamma(N)\tau = \Gamma(N)\tau'$. Dakle, postoji bijekcija*

$$\psi : S(N) \xrightarrow{\sim} Y_0(N), \quad [\mathbb{C}/\Lambda_\tau, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)] \to \Gamma_0(N)\tau.$$

*Dokaz.* Dokazat ćemo samo tvrdnju b); tvrdnje a) i c) se dokazuju slično. Prvo uzmimo proizvoljnu točku $[E, Q]$ iz $S_1(N)$. Sjetimo se da je $E$ izomorfan s $\mathbb{C}/\Lambda_{\tau'}$ za neki $\tau' \in \mathcal{H}$; pišemo $E = \mathbb{C}/\Lambda_{\tau'}$. Pošto je $Q$ točka reda $N$, vrijedi da je $Q = (c\tau' + d)/N + \Lambda_{\tau'}$ za neke $c, d \in \mathbb{Z}$. Tada je $(c, d, N) = 1$, pošto je $Q$ točno reda $N$, pa postoje $a, b, k \in \mathbb{Z}$ takvi da je $ad - bc - kN = 1$, pa se matrica $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ reducira modulo $N$ u $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Ako dodajemo višekratnike od $N$ vrijednostima od $c, d$ ne mijenjamo točku $Q$, te pošto $\mathrm{SL}_2(\mathbb{Z})$ trivijalno surjektira na $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, možemo uzeti da je $\gamma$ element od $\mathrm{SL}_2(\mathbb{Z})$. Neka je $\tau = \gamma(\tau')$, te neka je $m = c\tau' + d$. Tada je $m\tau = a\tau' + b$, pa je

$$m\Lambda_\tau = m(\tau\mathbb{Z} \oplus \mathbb{Z}) = (a\tau' + b)\mathbb{Z} \oplus (c\tau' + d)\mathbb{Z} = \Lambda_{\tau'}.$$

Predzadnja jednakost slijedi iz činjenice (koju ostavljamo za vježbu) da je rešetka $\alpha\mathbb{Z} \oplus \beta\mathbb{Z}$ ista kao i $\alpha'\mathbb{Z} \oplus \beta'\mathbb{Z}$ ako i samo ako postoji $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ takva da je

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix}.$$

Također vrijedi da je

$$m\left(\frac{1}{N} + \Lambda_{\tau'}\right) = \frac{c\tau' + d}{N} + \Lambda_{\tau'} = Q.$$

Sjetimo se da homotetične rešetke definiraju iste eliptičke krivulje; slijedi da je $[E, Q] = [\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau]$, kao što smo i htjeli.

Pretpostavimo sada da su $\tau, \tau' \in \mathcal{H}$ takvi da je $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. Dakle, vrijedi da je $\tau = \gamma(\tau')$ za neki $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$. Neka je opet $m = c\tau' + d$. Tada je kao i prije

$$m\Lambda_\tau = \Lambda_{\tau'}, \quad m\left(\frac{1}{N} + \Lambda_\tau\right) = \frac{c\tau' + d}{N} + \Lambda_{\tau'}.$$

Međutim, pošto je $(c, d) \equiv (0, 1) \pmod{N}$ po pretpostavci, dobivamo da je $m(1/N + \Lambda_\tau) = 1/N + \Lambda_{\tau'}$. Dakle, imamo da je $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] = [\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}]$.

Obratno, pretpostavimo sada da je $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] = [\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}]$, gdje su $\tau, \tau' \in \mathcal{H}$. Tada za neki $m \in \mathbb{C}$ vrijedi da je $m\Lambda_\tau = \Lambda_{\tau'}$ i $m(1/N + \Lambda_\tau) = 1/N + \Lambda_{\tau'}$. Kao što smo i prije spomenuli, vrijedi da je

$$\begin{pmatrix} m\tau \\ m \end{pmatrix} = \gamma \begin{pmatrix} \tau' \\ 1 \end{pmatrix} \text{ za neki } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

pa slijedi da je $m = c\tau' + d$. Sada zbog drugog uvjeta imamo

$$\frac{c\tau' + d}{N} + \Lambda_{\tau'} = \frac{1}{N} + \Lambda_{\tau'},$$

pa nadalje slijedi da je $(c,d) \equiv (0,1) \pmod{N}$, te je $\gamma \in \Gamma_1(N)$. Pošto je $\tau = \gamma(\tau')$, slijedi da je $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. □

Primjetimo da ako specijaliziramo $N = 1$, dobivamo da je $Y_0(1) = Y_1(1) = Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$, te da svaka od ovih modularnih krivulja zapravo predstavlja jednostavno skup klasa izomorfizama eliptičkih krivulja.

**Činjenica.** Skupovi $Y_0(N)$, $Y_1(N)$ i $Y(N)$ nisu kompaktni. Da bi ih se kompaktificiralo, prvo uzmimo $\mathcal{H}^* = \mathcal{H} \cup \{\infty\} \cup \mathbb{Q}$, te definriajmo $X(\Gamma) = \Gamma\backslash\mathcal{H}^*$, za neku kongrunecijsku grupu $\Gamma$. Dakle $X(\Gamma)$ je jednak uniji od $\mathcal{H}$ i konačnom skupu klasa elemenata od $\mathbb{Q} \cup \{\infty\}$ koji se zovu kuspovi.

Može se pokazati da $X_0(N)$, $X_1(N)$ i $X(N)$ imaju strukturu Riemannove plohe, te su i algebarske krivulje, iz čega slijedi da su i $Y_0(N)$, $Y_1(N)$ i $Y(N)$ algebraske krivulje. Štoviše, $Y_0(N)$ i $Y_1(N)$ se mogu definirati nad $\mathbb{Q}$, dok se $Y(N)$ može definirati nad $\mathbb{Q}(\zeta_N)$. Dokaze i više o ovoj temi se može naći [2, Chapter 2].

*Napomena.* Točke u $S_0(N)$, $S_1(N)$ i $S(N)$ određuju krivulje skupa s nekom strukturom "do na izomorfizam". Ako zanemarimo na trenutak tu strukturu i promatramo samo eliptičku krivulju, možemo se pitati nad kojim poljem je taj izomorfizam definiran? Odgovor je da $K$-racionalna točka definira $E$ do na $\overline{K}$-izomorfizam za točke iz $S_0(N)$, dok je $E$ dobivena iz $K$-racionalne točke na $S(N)$ i $S_1(N)$ određena do na $K$-izomorfizam.

Prostor parametara $S_0(N)$ je primjer grubog prostora parametara (coarse moduli space), koji razaznaju elemente do na izomorfizam nad algebarskim zatvorenjem, dok su $S_1(N)$ (za $N \geq 5$) i $S(N)$ (za $N \geq 3$), primjeri finih prostora parametara (fine moduli space), koji razaznaju elemete do na izomorfizam definiran nad tim poljem.

# Poglavlje 20

# Eliptičke krivulje u Magmi

Magma `http://magma.maths.usyd.edu.au/magma/` je najnapredniji programski paket s ugrađenim funkcijama za eliptičke krivulje i općenitije teoriju brojeva, algebru i algebarsku geometriju. Nije besplatan, ali postoji online aplikacija `http://magma.maths.usyd.edu.au/calc/` koja ograničava izračune na 120 sekundi, što nam je za većinu primjena dovoljno. Spomenimo i SAGE `http://www.sagemath.org/` koji ima prednost da je besplatan i open source. On je također dobar, međutim Magma ima puno više korisnih funkcija.

U ovom poglavlju ćemo opisati kako koristiti Magmu. Magma nudi korisniku dosta fleksibilnosti, ali je često kod kompliciran. Sve naredbe završavaju s ";", te je operacija pridruživanja ":=".

Prvo što se razlikuje od većine drugih sličnih programa je da treba definirati varijablu (ako ćemo je koristiti); to se radi sa
Q<x>:=PolynomialRing(Rationals());
Sada nam je $Q$ prsten polinoma $\mathbb{Q}[x]$. Eliptičke krivulje možemo definirati na više načina. Ako želimo definirati eliptičku krivulju $E$ u (dugoj) Weierstrassovoj formi,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

to se radi sa E:=EllipticCurve([$a_1, a_2, a_3, a_4, a_6$]); Na primjer, kod
E:=EllipticCurve([3,4,5,7,8]);
E;
vraća

```
Elliptic Curve defined by y^2 + 3*x*y + 5*y = x^3 + 4*x^2 + 7*x
+ 8 over Rational Field
```

Možemo i definirati eliptičku krivulju u kratkoj Weierstrassovoj formi

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

sa

```
E:=EllipticCurve([a,b])
```

Na primjer, kod

```
E:=EllipticCurve([3,4]);
E;
```

vraća

```
Elliptic Curve defined by y^2 = x^3 + 3*x + 4 over Rational Field
```

Može se konstruirati i eliptička krivulja sa zadanom $j$-invarijantom, te sa moničnim kubnim polinomom $f$, gdje se konstruira krivulja $y^2 = f(x)$;

```
E:=EllipticCurve(x^3+2*x^2+4*x-1);
E;
E1:=EllipticCurveFromjInvariant(43);
E1;
```

Ovaj kod vraća

```
Elliptic Curve defined by y^2 = x^3 + 2*x^2 + 4*x - 1 over Rational Field
Elliptic Curve defined by y^2 + x*y = x^3 + 36/1685*x + 1/1685 over Rational
Field
```

Spomenimo da postoji i vrlo korištena baza eliptičkih krivulja, takozvana Cremonina baza (po tvorcu Johnu Cremoni)
`http://homepages.warwick.ac.uk/~masgaj/ftp/data/`. Magma može i pozivati krivulje po nazivu iz te baze.

```
E:=EllipticCurve("11a1");
E;
```

vraća

```
Elliptic Curve defined by y^2 + y = x^3 - x^2 - 10*x - 20 over Rational Field
```

Mogu se i konsturirati kvadratni twistovi zadane krivulje. Zadajmo sada krivulju $E$, te njezin twist s $-2$, tj. $E^{-2}$.

```
E:=EllipticCurve([3,7]);
QuadraticTwist(E,-2);
```

Ovaj kod vraća

```
Elliptic Curve defined by y^2 = x^3 + 12*x - 56 over Rational Field
```

Točke na eliptičkim krivuljama definiramo u afininim koordinatama u uglatim zagradama, iako ih Magma vrraća u projektivnim i pridružujemo ih na eliptičku krivulju sa "!". Naredbe

```
E:=EllipticCurve([3,0]);
E;
P:=E![1,2];
2*P;
P+2*P;
Order(P);
}
```

vraćaju

```
Elliptic Curve defined by y^2 = x^3 + 3*x over Rational Field
(1/4 : -7/8 : 1)
(121/9 : -1342/27 : 1)
0
```

Dakle, zbrajanje i množenje točaka na eliptičkim krivuljama je točno kao očekivano. Funkcija Order() određuje red točke. Ako funkcija vrati 0, kao u ovom slučaju, to znači da je red točke beskonačan.

Možemo računati diskriminantu, $j$-invariantu, konduktor, naći minimalni model, kratki Werierstrassov model, model sa cjelobrojnim korrdinatama:

```
E:=EllipticCurve([3,4,7/5,-4,0]);
Discriminant(E);
Conductor(E);
jInvariant(E);
IsMinimalModel(E);
MinimalModel(E);
WeierstrassModel(E);
IntegralModel(E);
```

Ove nardebe vraćaju

```
-4212842/625
105321050
-229605859705/4212842
false
Elliptic Curve defined by y^2 + x*y + y = x^3 - 9326*x + 351298 over
Rational Field
Elliptic Curve defined by y^2 = x^3 - 96687/5*x + 26282286/25 over
Rational Field
Elliptic Curve defined by y^2 + 15*x*y + 175*y = x^3 + 100*x^2 - 2500*x
over Rational Field
```

Torziju eliptičke krivulje računamo sa

```
E:=EllipticCurve([-4,0]);
TorsionSubgroup(E);
```

što vraća

```
Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2*$.1 = 0
    2*$.2 = 0
```

dakle dobili smo samo torziju kao abstraktu grupu. Međutim, funkcija TorsionGroup() vraća dvije vrijednosti (druga je skrivena), dakle abstraktnu grupu, te preslikavanje iz te abstraktne grupe na eliptičku krivulju. Ako nas zanimaju torzijske točke, tada to treba napraviti na sljedeći način:

```
E:=EllipticCurve([-4,0]);
G,m:=TorsionSubgroup(E);
G;
m;
m(G.1);
m(G.2);
m(G.1)+m(G.2);
```

Ovdje je $G$ abstraktna grupa ($\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ u ovom slučaju), a $m$ je izomorfizam s $G$ na $E(\mathbb{Q})$. Nadalje, $G.1$ je prvi generator grupe, a $G.2$ drugi, pa su $m(G.1)$ i $m(G.2)$ generatori od $E(\mathbb{Q})_{tors}$. Kao što vidimo, možemo te točke i zbrajati. Magma vraća:

```
Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2*G.1 = 0
    2*G.2 = 0
Mapping from: GrpAb: G to Set of points of E with coordinates
in Rational Field
(-2 : 0 : 1)
(0 : 0 : 1)
(2 : 0 : 1)
```

Možemo i mijenjati polje ili prsten nad kojim je $E$ definirana. Polja algebarskih brojeva definiramo minimalnim polinomom, te onda s funkcijom BaseChange() ili ChangeRing() mijenjamo polje nad kojim je definirana eliptička krivulja.

Pogledajmo kod

```
E:=EllipticCurve([1,1]);
E2:=EllipticCurve([4,8]);
IsQuadraticTwist(E,E2);
Q<x>:=PolynomialRing(Rationals());
K<w>:=NumberField(x^2-2);
Ek:=BaseChange(E,K);
```

```
Ek2:=BaseChange(E2,K);
IsIsomorphic(Ek,Ek2);
```

koji vraća

```
true 2
true
```

Prvo definiramo dvije eliptičke krivulje. Magma automatski pretpostavlja da je svaka krivulja definirana nad najmanjim poljem iz kojeg su koeficijenti koje smo zadali. Sada pretpostavlja da su $E$ i $E_2$ definirane nad $\mathbb{Q}$. Zatim provjeravom jesu li te dvije eliptičke krivulje kvadratni twistovi - jesu i to "za 2". To znači da te krivulje nisu izomrfne nad $\mathbb{Q}$, ali postaju izomorfne nad $\mathbb{Q}(\sqrt{2})$. Zatim definiramo $\mathbb{Q}(\sqrt{2})$, te definiramo da je $w$ korijen polinoma $x^2-2$, te promjenimo polje definicije od $E$ i $E_2$. Tada krivulje postaju izomorfne.

Najbolje funkcije za računanje ranga (koje se razlikuju samo u imenu) su DescentInformation() i MordellWeilShaInformation().

```
E:=EllipticCurve([1,1]);
rank, gens, sha:=DescentInformation(E);
rank;
gens;
sha;
```

Kod vraća:

```
Torsion Subgroup is trivial
Analytic rank = 1
     ==> Rank(E) = 1
The 2-Selmer group has rank 1
Found a point of infinite order.
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 100 on the 2-coverings.)

[ 1, 1 ]
[ (0 : -1 : 1) ]
[
    <2, [ 0, 0 ]>
]
```

Dakle, ovdje se analitičkim metodama može dokazati da je analitički rang jednak 1. Po Kolyvaginovom teoremu, slijedi da je rang jednak 1. Također 2-spust pokazuje da je rang omeđen odozdo i odozgo s 1, tj. on je točno 1. Prvu vrijednost koju vraća funkcija je upravo to, uređeni par donje i gornje ograde, koji je $(1,1)$ u ovom slučaju. Donja ograda je dobivena tako da je nađena točka beskonačnog reda. Gornja ograda je dobivena tako da je pokazano da je

$Sel^{(2)}(E/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$. Dakle, pošto je torzija trivijalna, imamo da je $E(\mathbb{Q}) \simeq \mathbb{Z}$. Druga vrijednost koju vraća funkcija je točka $(0, -1)$, koja je generator od $E(\mathbb{Q})$. Treća funkcija vraća informacije o $Ш(E/\mathbb{Q})$. U ovom slučaju informacija koja je vraćena je $Ш(E/\mathbb{Q})[2] = \{0\}$.

Pogledajmo sada

```
E:=EllipticCurve([15,132,14,17,118]);
DescentInformation(E);
```

koji vraća

```
Torsion Subgroup is trivial
The 2-Selmer group has rank 2
After 2-descent:
    0 <= Rank(E) <= 2
    Sha(E)[2] <= (Z/2)^2
(Searched up to height 10000 on the 2-coverings.)
The Cassels-Tate pairing on Sel(2,E)/E[2] is
    [0 1]
    [1 0]
After using Cassels-Tate:
    0 <= Rank(E) <= 0
    (Z/2)^2 <= Sha(E)[4] <= (Z/2)^2

[ 0, 0 ]
[]
[
    <2, [ 2, 2 ]>,
    <4, [ 0, 0 ]>
]
```

U ovom slučaju je opet torzija trivijalna, te imamo da je $Sel^{(2)}(E/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, te nije nađena ni jedna točka beskonačnog reda. Naprednije metode (koje nećemo objašnjavati) pokazuju da svi elementi Selmerove grupe dolaze od Tate-Šafarevičeve grupe, te da je $Ш(E/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Pokažimo na sljedećem primjeru kako koristiti djelidbene polinome i konstruirati izogenije iz njih.

```
_<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([1,-1,0,-2,-1]);
p:=Factorization(DivisionPolynomial(E,7))[1][1];
p;
E1,f:=IsogenyFromKernel(E,p);
E1;
f;
G,m:=TorsionSubgroup(E);
Q:=m(G.1);
f(Q);
```

Objasnimo što kod radi. Eliptička krivulja koju promatramo ima izogeniju stupnja 7. Prvo izračunamo sedmi djelidbeni polinom - njega nećemo ispisivati jer je stupnja 24. Faktoriziramo taj polinom, te uzmemo faktor najmanjeg stupnja - on je točno stupnja 3. Nultočke tog faktora stupnja 3 su $x$-koordinate jezgre izogenije stupnja 7. Svakoj $x$-koordinati odgovaraju 2 točke na eliptičkoj krivulji, te tih 6 točka skupa s točkom u beskonačnosti čine podgrupu od $E$ reda 7. Kao što smo dokazivali, svakoj podgupi od $E$ odgovara izogenija. Upravo to radi naredba IsogenyFromKernel() stvara izogeniju iz te podgrupe reda 7. Funkcija vraća krivulju $E_1$ i 7-izogeniju $f : E \to E'$. Zatim uzimamo 2-torzijsku točku $Q$ na $E(\mathbb{Q})$ te ju šaljemu u $f(Q) \in E_1(\mathbb{Q})$.

Ove naredbe vraćaju

```
x^3 + x^2 - 2*x - 1
Elliptic Curve defined by y^2 + x*y = x^3 - x^2 - 107*x + 552 over
Rational Field
Elliptic curve isogeny from: CrvEll: E to CrvEll: E1
taking (x : y : 1) to ((x^7 + 2*x^6 + 18*x^5 - 34*x^4 - 75*x^3
 - 52*x^2 - 27*x - 14) / (x^6 + 2*x^5 - 3*x^4 - 6*x^3 + 2*x^2
  + 4*x + 1) : (x^9*y + 3*x^8*y - 21*x^8 - 24*x^7*y + 42*x^7
   + 63*x^6*y + 126*x^6 + 105*x^5*y + 203*x^5 + 329*x^4*y +
   210*x^4 + 525*x^3*y + 126*x^3 + 390*x^2*y + 7*x^2 + 106*x*y -
 42*x - 29*y - 7) / (x^9 + 3*x^8 - 3*x^7 - 14*x^6 + 21*x^4 + 7*x^3
 - 9*x^2 - 6*x - 1) : 1)
(-12 : 6 : 1)
```

Nastavimo sada ovaj primjer te nađimo polje nad kojim je definirana ta podgrupa reda 7 od $E$. Upisujemo dalje sljedeći kod:

```
K<w>:=NumberField(p);
E2:=BaseChange(E,K);
G:=TorsionSubgroup(E2);
G;
ZZ<y>:=PolynomialRing(K);
E;
L:=ext<K|y^2 + w*y - (w^3 - w^2 - 2*w - 1)>;
;
E3:=BaseChange(E,L);
G:=TorsionSubgroup(E3);
G;
```

koji vraća

```
Abelian Group isomorphic to Z/2
Defined on 1 generator
Relations:
    2*G.1 = 0
Elliptic Curve defined by y^2 + x*y = x^3 - x^2 - 2*x - 1
over Rational Field
```

```
Abelian Group isomorphic to Z/2 + Z/14
Defined on 2 generators
Relations:
    2*G.1 = 0
    14*G.2 = 0
```

Dakle prvo definiramo kubno polje $K$ nad kojim je definiran barem jedan korijen od polinoma $p$ (faktora stupnja 3 koji odgovara 7-izogeniji). Znamo da je $x$-koordinata točke reda 7 definirana nad $K$. Provjerimo torziju - dobivamo da je torzija $\mathbb{Z}/2\mathbb{Z}$, dakle nema točaka reda 7, tj. $y$-koordianta točke reda 7 nije definirana nad $K$. U sljedećem koraku moramo definirati prsten polinoma $K[y]$, te računamo $y$-koordiantu točke na $E$ čija je $x$-koordianta $w$ ($w$ je nultočka od $p$). Zatim definiramo da je $L$ proširenje od $K$ kojem pripada $y$ - znamo da je to kvadratno proširenje. Računamo torziju od $E(L)$- to je $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$, dakle našli smo polje nad kojim je grupa reda 7 definirana.

Možemo i reducirati krivulje (mod $p$) tako da promijenimo prsten nad kojim je definirana krivulja u konačno polje s $p$ elemenata. Zatim možemo pobrojati broj elemenata, te naći i grupovnu strukturu od $E(\mathbb{F}_p)$.

```
E:=EllipticCurve([3,7]);
E2:=ChangeRing(E,FiniteField(7));
#E2;
AbelianGroup(E2);
```

Ovaj kod vraća

```
8
Abelian Group isomorphic to Z/2 + Z/4
Defined on 2 generators
Relations:
    2*$.1 = 0
    4*$.2 = 0
```

Često Magma ne može izračunati rang eliptičke krivulje, pogotovo nad poljima algebarskih brojeva. Tada ako nas zanima samo neka točka beskonačnog reda možemo koristiti primitivnu funkciju Points() koja jednostavno traži točke na eliptičkoj krivulji. Za ovu funkciju treba odrediti gornju ogradu "veličine" (tj. visine) točaka koje se pretražuje.

```
E:=EllipticCurve([4,19]);
Q<x>:=PolynomialRing(Rationals());
E1:=BaseChange(E,NumberField(x^3+2));
pts:=Points(E1:Bound:=30);
pts;
Order(pts[2]);
Order(pts[4]);
IsLinearlyIndependent(pts[2],pts[4]);
RootNumber(E1);
```

Ovaj kod vraća:

```
{@ (0 : 1 : 0), (1/4*($.1^2 + 4*$.1 - 4) : 1/4*(5*$.1^2 - 8*$.1 - 9)
: 1), (1/4*($.1^2 + 4*$.1 - 4) : 1/4*(-5*$.1^2 + 8*$.1 + 9) : 1),
(2*$.1 + 1 : -$.1^2- 2*$.1 - 4 : 1),(2*$.1 + 1 : $.1^2 + 2*$.1 + 4
: 1),(9 : 28 : 1), (9 :-28 : 1) @}
0
0
true
1
```

Ovdje smo pronašli dvije točke beskonačnog reda, te pokazali da nisu linearno zavisne - dakle rang ove eliptičke krivulje nad $\mathbb{Q}(\sqrt[3]{2})$ je barem 2. Na kraju koristimo funkciju RootNumber() - ona nam vraća parnost ranga eliptičke krivulje pod pretpostavkom da je BSD slutnja točna. Ako je rang paran, onda vraća 1, ako je neparan onda vraća $-1$, te je vrlo brza. Napomenimo da za ovu krivulju (nad $\mathbb{Q}(\sqrt[3]{2})$) Magma ne može direktno izračunati rang.

# Poglavlje 21

# Eliptičke krivulje nad kvadratnim poljima

Prvo ćemo dokazati sljedeću propoziciju.

**Propozicija 70.** *Neka je $K$ PAB, $L$ kvadratno proširenje od $K$, $L = K(\sqrt{d})$, te $E$ eliptička krivulja definirana na $K$. Tada je*

$$\mathrm{rk}(E(L)) = \mathrm{rk}(E(K)) + \mathrm{rk}(E^d(K)).$$

*Dokaz.* Neka je $E$ eliptička krivulja u kratkoj Weierstrassovoj formi

$$E : y^2 = x^3 + ax + b,$$

te neka je twist $E^d$ zapisan u obliku

$$E^d : dy^2 = x^3 + ax + b,$$

gdje su $a, b \in K$. Neka je $\sigma$ generator od $\mathrm{Gal}(L/K)$. Prvo primjetimo da točke na $(x, y) \in E^d(K)$ odgovaraju točkama $(x, y\sqrt{d}) \in E(L)$, gdje su $x, y \in K$.

Prvo dokazujemo da je $\mathrm{rk}(E(L)) \geq \mathrm{rk}(E(K)) + \mathrm{rk}(E^d(K))$. Ako je $\mathrm{rk}(E(K)) = 0$ ili $\mathrm{rk}(E^d(K)) = 0$, tada smo gotovi. Ako $E$ i $E^d$ imaju pozitivan rang nad $K$, tada trebamo dokazati da će dvije točke beskonačnog reda, od kojih jedna dolazi od $E(K)$, a druga od $E^d(K)$, nužno biti nezavisne. Neka su $P_1 \in E(K)$ i $P_2 \in E^d(K)$ točke beskonačnog reda. Pretpostavimo da su linearno zavisne. Tada postoje $\alpha, \beta \in \mathbb{Z}$, gdje nisu i $\alpha = 0$ i $\beta = 0$, takvi da vrijedi

$$\alpha P_1 + \beta P_2 = O.$$

Djelujemo sa $\sigma$ na ovu jednadžbu, te pošto je $\sigma P_2 = -P_2$, dobivamo

$$\alpha P_1 - \beta P_2 = O.$$

Zbrajajući ove dvije jednadžbe, dobivamo $\alpha = 0$ i $\beta = 0$, što je kontradikcija.

Sada dokazujemo da je $\mathrm{rk}(E(L)) \leq \mathrm{rk}(E(K)) + \mathrm{rk}(E^d(K))$. Neka je

$$\mathrm{rk}(E(K)) = r_1,\ \mathrm{rk}(E^d(K)) = r_2,\ \mathrm{rk}(E(L)) = r,$$

$$< P_1, \ldots, P_{r_1} >= E(K)/E(K)_{tors},$$

$$< P_{r_1+1}, \ldots, P_{r_1+r_2} >= E^d(K))/E^d(K)_{tors}$$

i

$$< T_1, \ldots, T_r >= E(L)/E(L)_{tors}.$$

Pretpostavimo da je $P = (x_1 + x_2\sqrt{d}, y_1 + y_2\sqrt{d}) \in E(L)$ točka beskonačnog reda. Pošto je $E$ definirana nad $K$, zaključujemo da je $\sigma P \in E(L)$. Tada, direktnim računom, možemo provjeriti da je

$$P + \sigma P \in E(K),\ P - \sigma P \in E^d(K),$$

te je

$$2P \in E(K) + E^d(K).$$

Zaključujemo da je

$$< 2T_1, \ldots, 2T_r > /E(L)_{tors} \text{ je podgrupa od } < P_1, \ldots, P_{r_1+r_2} > /E(L)_{tors}.$$

Dakle $< P_1, \ldots, P_{r_1+r_2} >$ je konačnog indeksa u $E(L)/E(L)_{tors}$, što dokazuje $\mathrm{rk}(E(L)) \leq \mathrm{rk}(E(K)) + \mathrm{rk}(E^d(K))$.

□

Ova propozicija nam omogućava, ako je eliptička krivulja definirana nad $\mathbb{Q}$, problem računanja ranga od $E(K)$ riješiti računanjem ranga $E(\mathbb{Q})$ i $E^d(\mathbb{Q})$.

Primjetimo da se dokaz prošle propozicije može adaptirati na način da se točke beskonačnog reda u dokazu zamijene s točkama neparnog reda. Definirajmo $E(K)_{(2')}$ podgrupu od $E(K)$ točaka neparnog reda. Dobije se sljedeća tvrdnja (dokaz ostavljamo za vježbu).

**Propozicija 71.** *Neka je $E/\mathbb{Q}$ eliptička krivulja, $L/K$ kvadratno proširenje, $L = K(\sqrt{d})$. Tada je*

$$E(L)_{(2')} \simeq E(K)_{(2')} \oplus E^d(K)_{(2')}.$$

S druge strane, 2-torzija eliptičke krivulje se ne mijenja pri uzimanju kvadratnih twistova.

**Propozicija 72.** *Neka je $E/K$ eliptička krivulja, te neka $d \in K$ nije kvadrat. Tada je*

$$E(K)[2] \simeq E^d(K)[2].$$

*Dokaz.* Neka je

$$E : y^2 = x^3 + ax + b,$$

te neka je kvadratni twist zapisan kao

$$E^d : y^2 = x^3 + ad^2x + bd^3.$$

Sjetimo se da je $P \in E(K)$ točka reda 2 ako i samo ako je $y(P) = 0$. Tj. $P = (t, 0)$, gdje je $t \in K$ korijen od $x^3 + ax + b$.

Međutim, $t$ je korijen od $x^3 + ax + b$ ako i samo ako je $td$ korijen od $x^3 + ad^2x + bd^3$. Dakle, broj nultočaka od $x^3 + ax + b$ i $x^3 + ad^2x + bd^3$ se poklapa, pa je

$$E(K)[2] \simeq E^d(K)[2].$$

□

**Činjenica.** Modularne krivulje $X_1(11)$, $X_1(14)$, $X_1(15)$ su jedine modularne krivulje oblika $X_1(N)$, $N \in \mathbb{N}$ koje su genusa 1. Primjetimo da su te krivulje nužno eliptičke krivulje (nad $\mathbb{Q}$) pošto postoje kuspovi na njima (dakle nemoguće je da nemaju točku). Također, sjetimo se da svaka točka na $X_1(N)$ odgovara paru koji se sastoji od eliptičke krivulja i točke na $E$ reda $n$. Zapisat ćemo jednadžbe od $X_1(N)$ za gore navedene $n$, te za točku $(t, s) \in X_1(N)(K)$ odgovarajući par $(E, P)$, eliptičke krivulje $E/K$, te točke $P \in E(K)$ reda $n$. Za sve dolje navedene krivulje će $(0, 0)$ biti točka reda $n$.

| |
|---|
| $X_1(11) : s^2 - s = t^3 - t^2,$ |
| $E_{11} : y^2 + (st + t - s^2)xy + s(s-1)(s-t)t^2y = x^3 + st(s-1)(s-t)x^2$ |
| $X_1(14) : s^2 + st + s = t^3 - t$ |
| $a = \frac{t^4 - st^3 + (2s-4)t^2 - st + 1}{(t+1)(t^3 - 2t^2 - t + 1)}$ |
| $b = \frac{-t^7 + 2t^6 + (2s-1)t^5 + (-2s-1)t^4 + (-2s+2)t^3 + (3s-1)t^2 - st}{(t+1)^2(t^3 - 2t^2 - t + 1)^2}$ |
| $E_{14} : y^2 + axy + by = x^3 + bx^2.$ |
| $X_1(15) : s^2 + st + s = t^3 + t^2.$ |
| $a = \frac{(t^2 - t)s + (t^5 + 5t^4 + 9t^3 + 7t^2 + 4t + 1)}{(t+1)^3(t^2 + t + 1)}$ |
| $b = \frac{t(t^4 - 2t^2 - t - 1)s + t^3(t+1)(t^3 + 3t^2 + t + 1)}{(t+1)^6(t^2 + t + 1)}$ |
| $E_{15} : y^2 + axy + by = x^3 + bx^2.$ |

*Napomena.* Modeli $X_1(n)$ za druge vrijednosti $n$ se mogu naći npr. u [16]. Postoje i modularne krivulje $X_1(m, n)$ koje parametriziraju eliptičke krivulje s torzijom $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, gdje $m$ dijeli $n$.

Primjetimo da ako je za neku $P \in X_1(n)$ diskriminanta jednaka 0, to znači da je $P \notin Y_1(n)$, tj. $P$ je kusp.

Sljedeći teorem nam daje analogon Mazurovog teorema za kvadratna polja, tj. on nam daje sve moguće torzijske grupe eliptičkih krivulja nad svim kvadratnim poljima.

**Teorem 73** (Kamienny, Kenku-Momose)**.** *Neka $E$ varira po svim eliptičkim krivuljama nad svim kvadratnim poljima $K$. Tada će $E(K)_{tors}$ biti jedna od sljedećih grupa:*

$$\mathbb{Z}/n\mathbb{Z}, \text{ gdje } n = 1, \ldots, 16 \text{ ili } 18,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ gdje } n = 1, \ldots, 6,$$

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, \text{ gdje } n = 1 \text{ or } 2,$$
$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Također sjetimo se da iz svojstava Weilovog sparivanja slijedi da $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \subset E(K)$ samo ako $\mathbb{Q}(\zeta_n) \subset K$. Slijedi da $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \subset E(K)$, gdje $n = 1$ or 2, samo kada je $K = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, te $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \subset E(K)$ samo kada je $K = \mathbb{Q}(i)$.

**Činjenica.** Ako variramo po svim kvadratnim poljima (tj. ako promatramo sve eliptičke krivulje nad svim kvadratnim poljima), za svaku torzijsku grupu iz teorema Kamienny-Kenku-Momose, postoji beskonačno mnogo (do na $\overline{\mathbb{Q}}$-izomorfizam) eliptičkih krivulja $E/K$ takvih da je $E(K) \supset T$.

Teorem Kamienny-Kenku-Momose nam daje torzije nad svim kvadratnim poljima. Međutim, ako fiksiramo jedno kvadratno polje, tada se ne moraju pojaviti sve grupe sa liste (štoviše ni nad jednim poljem se neće pojaviti sve grupe sa liste).

Pogledajmo javljaju li se grupe $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{5})$. Ovo polje smo izabrali jer je to polje oblika $\mathbb{Q}(\sqrt{d})$, $d > 0$ s najmanjom diskriminantom.

**Propozicija 74.** *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/11\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{5})$.

*Dokaz.* Da bi ovo dokazali, treba samo pokazati da je $Y_1(11)(\mathbb{Q}(\sqrt{5})) = \emptyset$, tj. drugim rječima da je $X_1(11)(\mathbb{Q}(\sqrt{5})) = \{\text{kuspovi}\}$. Točka $P = (t, s) \in X_1(11)$ je kusp ako i samo ako je

$$\Delta(E_{11}) = t(t-1)(t^5 - 18t^4 + 35t^3 - 16t^2 - 2t + 1) = 0.$$

Lako vidimo da su $t = 0, 1$ jedine nultočke ovog polinoma nad $\mathbb{Q}(\sqrt{5})$. Dakle kuspovi nad $\mathbb{Q}(\sqrt{5})$ su

$$X_1(11)(\mathbb{Q}(\sqrt{-5}))\backslash Y_1(11)(\mathbb{Q}(\sqrt{-5})) = \{\mathcal{O}, (0,0), (1,0), (0,1), (1,1)\}.$$

Sada trebamo izračunati $X_1(11)(\mathbb{Q}(\sqrt{-5}))$. Standardnim (ranije opisanim) metodama za računanje ranga i torzije eliptičkih krivulja nad $\mathbb{Q}$, dobivamo

$$\text{rk}(X_1(11)(\mathbb{Q})) = 0$$
$$\text{rk}(X_1^{(5)}(11)(\mathbb{Q})) = 0$$
$$X_1(11)(\mathbb{Q})_{tors} \simeq \mathbb{Z}/5\mathbb{Z},$$
$$X_1^{(5)}(11)(\mathbb{Q})_{tors} = \{\mathcal{O}\},$$

pa iz propozicija 70 i 71 dobivamo

$$X_1(11)(\mathbb{Q}(\sqrt{5})) \simeq \mathbb{Z}/5\mathbb{Z}.$$

Nadalje, pošto postoji 5 kuspova na $X_1(11)$, zaključujemo da

$$X_1(11)(\mathbb{Q}(\sqrt{5})) = \{\textit{kuspovi}\},$$

to jest

$$Y_1(11)(\mathbb{Q}(\sqrt{5})) = \emptyset.$$

□

Sada gledamo postoje li eliptičke krivulje s točkama reda 14.

**Propozicija 75.** *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/14\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{5})$.

*Dokaz.* Dokaz ide kao i dokaz propozicije 74. Ako je $P = (t, s) \in X_1(14)$ kusp, tada je

$$\Delta(E_{14}) = t(t-1)(t+1)(t^3 - 9t^2 - t + 1)(t^3 - 2t^2 - t + 1) = 0.$$

Zaključujemo da je

$$X_1(14)(\mathbb{Q}(\sqrt{5}))\backslash Y_1(14)(\mathbb{Q}(\sqrt{5})) = \{\mathcal{O}, (1,0), (0,0), (-1,0), (0,-1), (1,-2)\}.$$

Računamo

$$\mathrm{rk}(X_1(14)(\mathbb{Q})) = 0$$

$$\mathrm{rk}(X_1^{(5)}(14)(\mathbb{Q})) = 0$$

$$X_1(14)(\mathbb{Q})_{tors} \simeq \mathbb{Z}/6\mathbb{Z},$$

$$X_1^{(5)}(14)(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z}.$$

Odavdje još nije jasno što je $X_1(14)(\mathbb{Q}(\sqrt{5}))_{tors}$; mogućnosti iz ovoga što je za sada izračunato (i teorema Kamienny-Kenku-Momose) su $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$. Mogućnost da je torzija $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ možemo eliminirati tako da prebacimo $X_1(15)$ u kratku Weierstrassovu formu $y^2 = f(x)$, te izračunamo da $f$ ima samo jedan korijen nad $\mathbb{Q}(\sqrt{5})$.

Mogućnost da je torzija $\mathbb{Z}/12\mathbb{Z}$ možemo eliminirati na sljedeći način: faktoriziramo (13) u $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ kao $(13) = (2+\sqrt{5})(2-\sqrt{5})$. Označimo $(2+\sqrt{5}) = \rho$, pa je $(13) = \rho\overline{\rho}$, gdje je $\overline{\rho} = (2-\sqrt{5})$ Galoisov konjugat od $\rho$. Pošto su jedini faktori diskriminante od $X_1(14)$ 2 i 7, slijedi da $X_1(14)/\mathbb{Q}(\sqrt{5})$ ima dobru redukciju u $\rho$. Reduciramo mod $\rho$ i dobivamo

$$X_1(14)(O_{\mathbb{Q}(\sqrt{5})}/\rho) = X_1(14)(\mathbb{F}_{13}) \simeq \mathbb{Z}/18\mathbb{Z}.$$

Pošto se 13-slobodan dio od $X_1(14)(\mathbb{Q}(\sqrt{5}))_{tors}$ ulaže u $X_1(14)(\mathbb{F}_{13})$, slijedi $X_1(14)(\mathbb{Q}(\sqrt{5}))_{tors} \simeq \mathbb{Z}/6\mathbb{Z}$, te nadalje

$$Y_1(14)(\mathbb{Q}(\sqrt{5})) = \emptyset.$$

□

Za razliku od eliptičkih krivulja s torzijom reda 11 i 14, postoji eliptička krivulja s torzijom reda 15 nad $\mathbb{Q}(\sqrt{5})$.

**Propozicija 76.** *Postoji točno jedna eliptička krivulja s torzijom reda 15 nad* $\mathbb{Q}(\sqrt{5})$ *i to je*

$$E_{15} : y^2 + \frac{\sqrt{5}}{2}xy + \frac{-11\sqrt{5}+25}{4}y = x^3 + \frac{-11\sqrt{5}+25}{4}x^2$$

*Dokaz.* Da bi ovo dokazali, treba odrediti $Y_1(15)(\mathbb{Q}(\sqrt{5}))$ Lako vidimo da je $P = (t, s) \in X_1(15)$ kusp ako i samo ako je

$$\Delta(E_{15}) = t(t+1)(t^2+t+1)(t^4+3t^3+4t^2+2t+1)(t^4-7t^3-6t^2+2t+1) = 0.$$

Lako vidimo da su $t = 0, -1$ jedine nultočke ovog polinoma nad $\mathbb{Q}(\sqrt{5})$, te je

$$X_1(15)(\mathbb{Q}(\sqrt{5}))\backslash Y_1(15)(\mathbb{Q}(\sqrt{5})) = \{\mathcal{O}, (0,0), (-1,0), (0,-1)\}$$

Istim metodama kao i ranije izračunamo da je

$$X_1(15)(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z},$$

$$X_1^{(d)}(15)(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z},$$

iz čega zaključujemo da $X_1(15)(\mathbb{Q}(\sqrt{5}))$ ima samo točke parnog reda. Lako provjerimo da $X_1(15)(\mathbb{Q}(\sqrt{5}))[2] \simeq \mathbb{Z}/2\mathbb{Z}$. Dakle, jedina mogućnost da $X_1(15)$ ima veću torziju nad $\mathbb{Q}(\sqrt{5})$ nego nad $\mathbb{Q}$ je da sadrži $\mathbb{Z}/8\mathbb{Z}$.

Sada faktoriziramo osmi djelidbeni polinom od $X_1(15)$ nad $\mathbb{Q}(\sqrt{5})$, te dobivamo da ima sljedeće nultočke: $x = 0, -1, -2, -(1\pm\sqrt{5})/2$. Znamo da $x = 0, -1$ odgovaraju točkama reda 2 i 4. Izračunamo da točka s $x$-koordinatom 2 ima $y$-koordinatu koja nije definirana nad $\mathbb{Q}(\sqrt{5})$, dok nam $x = -(1 \pm \sqrt{5})/2$ daju sljedeće točke reda 8:

$$\left(\frac{-\sqrt{5}+1}{2}, \frac{-\sqrt{5}+1}{2}\right), \left(\frac{-\sqrt{5}+1}{2}, \sqrt{5}-2\right), \left(\frac{\sqrt{5}+1}{2}, \frac{\sqrt{5}+1}{2}\right),$$

$$\left(\frac{\sqrt{5}+1}{2}, -\sqrt{5}-2\right).$$

Uzimajući prvu od ovih točaka dobivamo eliptičku krivulju $E_{15}$ iz iskaza propozicije.

Može se provjeriti da i ostale 3 točke daju izomorfnu eliptičku krivulju. □

*Napomena.* Zašto 4 točke na $X_1(15)$ daju istu eliptičku krivulju? To je zato jer svaka točka na $X_1(15)$ odgovara paru $(E, P)$, gdje je $P$ točka reda 15, do na izomorfizam. Pošto je $[-1]$ automorfizam od $E$ slijedi da je $(E, P) = (E, -P)$. Međutim, $\pm 2P$, $\pm 4P, \pm 7P$ su također točke reda 15, te pošto množenje s $n \neq \pm 1$ nije izomorfizam, slijedi da su $(E, P)$, $(E, 2P)$, $(E, 4P)$ i $(E, 7P)$ različite točke na $X_1(15)$. To su točno 4 točke koje se pojavljuju u dokazu prethodne propozicije.

Vidjeli smo da postoji točno jedna eliptička krivulja s torzijom reda 15 nad $\mathbb{Q}(\sqrt{5})$. Sjetimo se da nad $\mathbb{Q}$ postoji beskonačno mnogo eliptičkih krivulja sa zadanom torzijskom grupom $T$, gdje je $T$ grupa sa liste iz Mazurovog teorema. Pa se prirodno možemo pitati je li slučaj kao u $\mathbb{Q}(\sqrt{5})$ da postoji samo jedna eliptička krivulja sa zadanom torzijom tipičan ili je to iznimka.

Vidjet ćemo da je slučaj koji smo imali sa $\mathbb{Q}(\sqrt{5})$ ipak jedna od iznimaka (za kvadratna polja).

**Teorem 77.** *Polja $\mathbb{Q}(\sqrt{5})$ i $\mathbb{Q}(\sqrt{-15})$ su jedina kvadratna polja takva da nad njima postoji pozitivan konačan broj eliptičkih krivulja s torzijom $\mathbb{Z}/15\mathbb{Z}$. Nad svim ostalim kvadratnim poljima postoji ili 0 ili beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/15\mathbb{Z}$.*

*Dokaz.* Prvo primjetimo da ako je $\mathrm{rk}(X_1(15)(K)) > 0$, za neko kvadratno polje $K$, slijedi da će biti beskonačno eliptičkih krivulja s torzijom $\mathbb{Z}/15\mathbb{Z}$ nad $K$.

Dakle jedina mogućnost da postoji konačno mnogo, ali više od 0 eliptičkih krivulja, je da je $\mathrm{rk}(X_1(15)(K)) = 0$, te da je

$$X_1(15)(\mathbb{Q})_{tors} \subsetneq X_1(15)(K)_{tors}.$$

Pošto od ranije znamo da je $X_1(15)(\mathbb{Q})_{tors} \simeq \mathbb{Z}/4\mathbb{Z}$, promatramo mogućnosti za $X_1(15)(K)_{tors}$. Prvo primjetimo da pošto $X_1(15)(\mathbb{Q})$ ima samo jednu točku reda 2, on se može napisati kao

$$y^2 = (x - \alpha)f(x),$$

gdje je $f$ ireducibilni (nad $\mathbb{Q}$) kvadratni polinom. Krivulja $X_1(15)(K)$ će imati punu 2-torziju ako i samo ako su korijeni od $f$ definirani nad $K$, tj. $X_1(15)$ će imati punu 2-torziju samo nad poljem definiranima sa $f$. Računajući, dobivamo da je

$$X_1(15) : y^2 = (x + 21)(x^2 - 21x + 414),$$

te lako izračunamo da $x^2 - 21x + 414$ generira kvadratno polje $\mathbb{Q}(\sqrt{-3})$.

Nadalje, računamo $X_1(15)(\mathbb{Q}(\sqrt{-3})) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, te provjerimo da su točke koje su definirane nad $\mathbb{Q}(\sqrt{-3})$, a nisu nad $\mathbb{Q}$, zapravo kuspovi. Dakle,

$$Y_1(15)(\mathbb{Q}(\sqrt{-3})) = \emptyset.$$

Sljedeće, trebamo vidjeti postoje li točke reda 3 na $X_1(15)$ nad nekim kvadratnim poljem $K$. Izračunamo treći djelidbeni polinom $\psi_3$ od $X_1(15)$, vidimo da je ireducibilan nad $\mathbb{Q}$, te pošto je četvrtog stupnja zaključujemo da $X_1(15)$ neće imati točku reda 3 ni nad jednim kvadratnim (a ni kubnim) poljem. Ostaje još mogućnost da je $X_1(15)(K) \supset \mathbb{Z}/8\mathbb{Z}$ za neka kvadratna polja $K$ (vidjeli smo da se to događa za $K = \mathbb{Q}(\sqrt{5})$). Računanjem 8-djelidbenog polinoma, dobivamo da $X_1(15)$ ima još točke reda 8 samo nad $\mathbb{Q}(\sqrt{-15})$.

Računamo da je

$$X_1(15)(\mathbb{Q}(\sqrt{-15})_{tors} \simeq \mathbb{Z}/8\mathbb{Z},$$

$$\mathrm{rk}(X_1(15)(\mathbb{Q}(\sqrt{-15})) = \mathrm{rk}(X_1(15)(\mathbb{Q})) + \mathrm{rk}(X_1^{-15}(15)(\mathbb{Q})) = 0 + 0 = 0,$$

te na analogan način kao u napomeni nakon propozicije 76, zaključujemo da postoji točno jedna eliptička krivulja s torzijom $\mathbb{Z}/15\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{-15})$.

Promatranjem mogućnosti za torziju eliptičke krivulje nad kvadratni poljem iz Teorema Kamienny-Kenku-Momose, vidimo da je teorem dokazan. □

*Napomena.* Kao i u propoziciji 76, može se eksplicitino izračunati tu jedinstvenu eliptičku krivulju s torzijom $\mathbb{Z}/15\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{-15})$, to je:

$$y^2 + \frac{145 + 7\sqrt{-15}}{128}xy + \frac{265 + 79\sqrt{-15}}{4096}y = x^3 + \frac{265 + 79\sqrt{-15}}{4096}x^2.$$

Pogledajmo anologne rezultate za grupe $\mathbb{Z}/11\mathbb{Z}$ i $\mathbb{Z}/14\mathbb{Z}$.

**Teorem 78.** *Nad kvadratnim poljem $K$ postoji ili 0 ili beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/11\mathbb{Z}$.*

**Teorem 79.** *Postoji točno dvije eliptičke krivulje s torzijom $\mathbb{Z}/14\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{-7})$. Nad svakim drugim kvadratnim poljem $K$, postoji ili 0 ili beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/14\mathbb{Z}$.*

Dokaze ovih teorema ostavljamo za zadaću.

Što je s ostalim cikličkim grupama koje se pojavljuju kao torzija eliptičkih krivulja nad kvadratnim poljima, točnije s grupama $\mathbb{Z}/n\mathbb{Z}$, za $n = 13, 16, 18$? Bitna je činjenica da su to sve krivulje genusa 2.

Sjetimo se da Faltingsov teorem kaže da će svaka krivulja genusa $> 2$ imati samo konačno mnogo točaka nad bilo kojim poljem algebarskih brojeva.

**Korolar 80.** *Neka je $K$ polje algebarskih brojeva. Postoji konačno mnogo (do na izomorfizam) eliptičkih krivulja s torzijom $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$ i $\mathbb{Z}/18\mathbb{Z}$.*

Dakle koliko god proširivali i povećavali naše polje, uvijek imamo samo konačno mnogo takvih krivulja.

# Poglavlje 22

# Eliptičke krivulje nad poljima algebarskih brojeva stupnja većeg od 2

U ovom poglavlju ćemo promotriti koliko postoji eliptičkih krivulja s torzijom $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$ i $\mathbb{Z}/15\mathbb{Z}$, nad poljima algebarskih brojeva viših stupnjeva.

Pogledajmo grupu $\mathbb{Z}/11\mathbb{Z}$. Iskoristit ćemo sljedeću lemu.

**Lema 81.** *Galoisove reprezentacije $\rho_p$, za $p$ prost, pridružene eliptičkoj krivulji $X_1(11)$ su surjektivne za sve $p$ osim za $p = 5$.*

Inače, za zadanu eliptičku krivulju, u kompjuterskom programu Sage mogu se izračunati svi prosti brojevi za koju ta eliptička krivulja nema surjektivnu Galoisovu reprezentaciju.

Dokažimo sada sljedeći teorem.

**Teorem 82.** *Postoji ili 0 ili beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/11\mathbb{Z}$ nad PAB $K$ koje je prostog stupnja $p > 5$.*

*Dokaz.* Neka je $K$ PAB takvo da je $[K : \mathbb{Q}] = p$, gdje je $p > 5$ prost broj. Dokazat ćemo da je $X_1(11)(K)_{tors} = X_1(11)(\mathbb{Q})_{tors}$. Također primjetimo da $K$ nema pravo potpolje, tj. jedina potpolja od $K$ su samo polje $K$ i $\mathbb{Q}$ (pošto stupanj potpolja dijeli stupanj polja).

Sljedeću činjenicu koju koristimo je da ako je Galoisova reprezentacija $\rho_l$ surjekcija, tada je djelidbeni polinom $\psi_l$ ireducibilan nad $\mathbb{Q}$ (jer kada bi bio reducibilan, tada bi reprezentacija bila reducibilna, a surjektivna Galoisova reprezentacija je uvijek ireducibilna).

Neka je sada $l \neq 2, 5$ prost broj. Dakle $\psi_l$ je polinom stupnja $\frac{l^2-1}{2}$, tj. stupanj je djeljiv sa 4. Dakle polje najmanjeg stupnja nad kojim postoji točka reda $l$ je stupnja koji je višekratnik od 4. Dakle nad $K$ ne postoji točka reda $l$.

Još treba pogledati slučajeve $l = 2, 5$. Za $l = 2$, pošto je reporezentacija $\rho_l$ surjektivna, slijedi da je

$$\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_2) \simeq S_3,$$

dakle ne postoje točke reda 2 nad $K$.

Ostaje slučaj $l = 5$. Pošto je $X_1(11)(\mathbb{Q})_{tors} \simeq \mathbb{Z}/5\mathbb{Z}$, te pošto PAB koje sadrži punu 5-torziju mora sadržavati $\mathbb{Q}(\zeta_5)$, vrijedi da je $X_1(11)(K)[5] = X_1(11)(\mathbb{Q})[5]$. Dakle treba provjeriti još ima li $X_1(11)(K)$ točke reda 25. Faktoriziramo

$$\psi_{25} = \psi_5 f_5 g_5 f_{20} g_{20} f_{250}, \tag{22.1}$$

gdje $f_n$ i $g_n$ ireducibilni polinomi stupnja $n$, a $\psi_5$ je 5-djelidbeni polinom. Dakle ne postoji točka reda 25 nad $K$ (pošto je po pretpostavci $[K : \mathbb{Q}] > 5$). □

U prošlom teoremu smo promotrili broj krivulja sa 11-torzijom nad svim poljima prostog stupnja $> 5$, a ranije smo odredili broj krivulja s 11-torzijom nad kvadratnim poljima. Sada ćemo promotriti broj krivulja nad poljima stupnja 3 i stupnja 5.

Neka je $\mathbb{Q}(\zeta_n)$ $n$-to ciklotomsko polje. Tada sa $\mathbb{Q}(\zeta_n)^+$ označavmo *maksimalno realno potpolje* od $\mathbb{Q}(\zeta_n)$. Vrijedi $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)^+] = 2$, te $[\mathbb{Q}(\zeta_n)^+ : \mathbb{Q}] = \frac{\phi(n)}{2}$.

Također, $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

**Teorem 83.** *Postoje točno* 3 *eliptičke krivulje s torzijom* $\mathbb{Z}/11\mathbb{Z}$ *nad* $\mathbb{Q}(\zeta_{11})^+$, *te točno jedna nad kubnim poljem generiranim s polinomom* $x^3 - x^2 + x + 1$.

*Nad svim ostalim poljima stupnja 3 i 5 postoji ili 0 ili beskonačno mnogo eliptičkih krivulja koje sadrže* 11*-torziju.*

*Dokaz.* Iz dokaza teorema 82, vidimo da nad poljima stupnja 3 i 5 ne može biti točaka prostog reda $\neq 2, 5$ na $X_1(11)$.

Postoji točno jedna točka reda 2 nad poljem generiranim polinomom $f$, gdje $X_1(11)$ zapišemo kao

$$X_1(11) : y^2 = f(x),$$

te 3 točke reda 2 nad poljem cijepanja od $f$ (koje će u ovom slučaju biti stupnja 6). Izračunamo da $f$ generira upravo kubno polje iz iskaza teorema. Nazovimo to polje $K$.

Računamo da je $X_1(11)(K) \simeq \mathbb{Z}/10\mathbb{Z}$, te da nijedna od 5 točaka koje su definirane nad $K$, a nisu nad $\mathbb{Q}$, nije kusp.

Također izračunamo $\mathrm{rk}(X_1(11)(K)) = 0$.

Dakle imamo 5 točka na $Y_1(11)(K)$. One odgovaraju jednoj eliptičkoj krivulji. To vidimo jer grupa $(\mathbb{Z}/11\mathbb{Z})^\times/\langle -1\rangle$ ima 5 generatora. Drugim riječima, tih 5 točaka odgovara parovima

$$(E, \pm P), (E, \pm 2P), (E, \pm 3P), (E, \pm 4P), (E, \pm 5P),$$

gdje je $\alpha$ korijen od $x^3 - x^2 + x + 1$, a $E/K$ je

$$E : y^2 + (3\alpha^2 - 5\alpha - 3)xy + (8\alpha^2 + 8\alpha + 2)y = x^3 + (2\alpha^2 - 10\alpha - 6)x^2,$$

te gdje je $P \in E(K)$ neka točka reda 11.

Pogledajmo sada točke čiji je red potencija od 5. Kao što je rečeno u dokazu teorema 82, jedina mogućnost je da postoje točke reda 25 nad nekim poljem stupnja 5 koje je generirano polinomima $f_5$ ili $g_5$ iz (22.1).

Direktim računom provjeravamo da $X_1(11)$ ima veću torziju jedino nad $\mathbb{Q}(\zeta_{11})^+$ i da vrijedi $X_1(11)(\mathbb{Q}(\zeta_{11})^+) \simeq \mathbb{Z}/25\mathbb{Z}$ (dakle osim što je torzija veća, vrijedi i $\mathrm{rk}(X_1(11)(\mathbb{Q}(\zeta_{11})^+)) = 0$).

Nadalje dobivamo da od tih dodatnih 20 točaka, njih 5 su kuspovi, a 15 nisu. Kako znamo od prije da 5 točaka odgovara jednoj eliptičkoj krivulji, znači da imamo 3 nove eliptičke krivulje.

Nećemo ispisivati te 3 eliptičke krivulje, ali napomenimo da se mogu pronaći u [12]. □

Iskažimo sada slične rezultate za torzijsku grupu $\mathbb{Z}/14\mathbb{Z}$ i $\mathbb{Z}/15\mathbb{Z}$.

**Teorem 84.** *Postoje točno* 2 *eliptičke krivulje s torzijom* $\mathbb{Z}/14\mathbb{Z}$ *nad* $\mathbb{Q}(\zeta_7)^+$. *Nad svim ostalim poljima prostog stupnja* $\geq 3$ *postoji ili* 0 *ili beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/14\mathbb{Z}$.

**Teorem 85.** *Nad svim poljima prostog stupnja* $\geq 3$ *postoji ili* 0 *ili beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/15\mathbb{Z}$.

# Poglavlje 23

# Torzijske grupe racionalnih eliptičkih krivulja nad poljima algebarskih brojeva

U prošlom poglavlju smo promatrali moguće torzije eliptičkih krivulja nad kvadratnim i kubnim poljima. U ovom poglavlju ćemo promatrati moguće torzijske grupe racionalnih eliptičkih krivulja. To jest, krenut ćemo od eliptičke krivulje nad $\mathbb{Q}$, te ćemo onda promatrati koje su moguće torzijske grupe te eliptičke krivulje nad kvadratnim i nad kubnim poljima.

Prije nego što krenemo iskazivati prve rezultate u ovom smjeru, prvo ćemo iskazati vrlo važan teorem koji će nam biti i kasnije koristan, a to je teorem koji govori o mogućim $n$-izogenijama nad $\mathbb{Q}$. Teorem je sličan Mazurovom torzijskom teoremu, a i najveći dio sljedećeg teorema je dokazao sam Mazur u [9]. On je tu našao sve moguće izogenije osim što je bila ostala mogućnost da postoje još $n$-izogenije za par $n$-ova (npr. $n = 125$). Preostale slučajeve je u seriji članaka eliminirao Kenku [4, 5, 6].

U tablici ispod, za svaki $n$ za koji postoji $n$-izogenija nad $\mathbb{Q}$, zapisali smo genus $g$ od $X_0(n)$, te broj klasa $m$ (do na $\overline{\mathbb{Q}}$-izomorfizam) eliptičkih krivulja sa $n$-izogenijom.

| $n$ | $g$ | $m$ | $n$ | $g$ | $m$ | $n$ | $g$ | $m$ |
|---|---|---|---|---|---|---|---|---|
| $\leq 10$ | 0 | $\infty$ | 11 | 1 | 3 | 27 | 1 | 1 |
| 12 | 0 | $\infty$ | 14 | 1 | 2 | 37 | 2 | 2 |
| 13 | 0 | $\infty$ | 15 | 1 | 4 | 43 | 3 | 1 |
| 16 | 0 | $\infty$ | 17 | 1 | 2 | 67 | 5 | 1 |
| 18 | 0 | $\infty$ | 19 | 1 | 1 | 163 | 13 | 1 |
| 25 | 0 | $\infty$ | 21 | 1 | 4 | | | |

Jasno je da će skup mogućih torzija racionalnih eliptičkih krivulja nad kvadratnim poljima biti podskup (i to strogi, kao što ćemo vidjeti), od skupa grupa

koje se pojavljuju u KMK (Kamienny-Kenku-Momose) teoremu.

**Teorem 86.** *Neka je $E/\mathbb{Q}$ racionalna eliptička krivulja i neka je $K$ kvadratno polje.*

*a) Torzija od $E(K)$ je izomorfna jednoj od sljedećih grupa*

$$\begin{gathered}\mathbb{Z}/m\mathbb{Z},\ m=1,\dots,10,12,15,16,\\ \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2m\mathbb{Z},\ 1\le m\le 6.\\ \mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3m\mathbb{Z},\ m=1,2,\\ \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}.\end{gathered} \tag{23.1}$$

*b) Svaka od ovih grupa, osim $\mathbb{Z}/15\mathbb{Z}$, se pojavljuje kao torzijska podgrupa od $E(K)$ za beskonačno mnogo parova $(E,K)$, gdje je $E$ racionalna eliptička krivulja, a $K$ kvadratno polje.*

*Dokaz.* Eliminirajmo grupe koje se pojavljuju u $KMK$ teoremu a koje nisu u iskazu teorema. Neka je $K=\mathbb{Q}(\sqrt{d})$ proizvoljno kvadratno polje.

Prvo iz propozicije 71 zkaljučujemo da je

$$E(K)[n]=E(\mathbb{Q})[n]+E^d(\mathbb{Q})[n],$$

za $n=11,13$. Zaključujemo da pošto ne postoje eliptičke krivulje s $n$-torzijom nad $\mathbb{Q}$, da ne postoje ni racionalne eliptičke krivulje s takvom torzijom ni nad kvadratnim poljima. Dakle eliminirali smo grupe $\mathbb{Z}/11\mathbb{Z}$ i $\mathbb{Z}/13\mathbb{Z}$.

Primjetimo da je broj točaka reda 2 nad $K$ eliptičke krivulje

$$E: y^2=f(x)=x^3+ax+b$$

jednak broju korijena od $f$ nad $K$. Dakle, kad bi $E(K)$ imao $n$-torziju, za $n=14,18$, slijedilo bi da postoji eliptička krivulja sa $n$-torzijom nad $\mathbb{Q}$ (jer ako $E(\mathbb{Q})$ ima netrivijalnu 2-torziju, tada ima i svaki twist, vidi propoziciju 72), što je po Mazurovom teoremu nemoguće.

Svaka eliptička krivulja $E/\mathbb{Q}$ koja ima torziju nad $\mathbb{Q}$ oblika $\mathbb{Z}/n\mathbb{Z}$, gdje je $n=10,12$ se može zapisati u obliku

$$E: y^2=(x-\alpha)f(x),$$

gdje je $f$ ireducibilan kvadratni polinom. Ako promotrimo $E$ nad kvadratnim poljem $K$ definiranim s $f$, tada ćemo dobiti $E(K)\simeq\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}$.

Dokaz da postoji beskonačno mnogo eliptičkih krivulja definiranih nad $\mathbb{Q}$ s torzijom $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$ i $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$ ćemo preskočiti (on je konstruktivan tj. eksplicitno se nađu beskonačne familije eliptičkih krivulja definiranih and $\mathbb{Q}$ s traženom torzijom nad odgovarajućim kvadratnim poljem).

Također, dokaz da postoji beskonačno mnogo eliptičkih krivulja sa svakom od torzija iz Mazurovog teorema ostavljamo za (poučnu) vježbu.

Nadalje želimo naći sve racionalne eliptičke krivulje s 15-torzijom nad kvadratnim poljima. Neka je $E/\mathbb{Q}$ eliptička krivulja koja ima 15-torziju nad nekim kvadratnim poljem. Po propoziciji 71 ovo povlači da je

$$E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/3\mathbb{Z} \text{ i } E^d(\mathbb{Q})_{tors} \simeq \mathbb{Z}/5\mathbb{Z} \tag{23.2}$$

ili obrnuto. Pretpostavimo bez gubitka općenitosti da je ovako kako smo zapisali. Također, pošto ako $E$ ima $p$-izogeniju, tada imaju i svi twistovi $E^d$ od $E$, pa slijedi da $E$ mora imati 15-izogeniju.

Ali kao što smo vidjeli postoje samo 4 familije twistova racionalnih eliptičkih krivulja sa 15-izogenijom, te je poznato (vidi npr. [11, p.78–80]), da su to eliptičke krivulje s $j$-invariantama

$$-25/2,\ -349938025/8,\ -121945/32,\ 46969655/32768.$$

To su twistovi eliptičkih krivulja sa oznakama 50A1, 50A2, 50B1 and 50B2 u Cremonim tablicama.

Promatranjem djelidbenih polinoma (detalji za vježbu) dobivamo da 50B1 ima 15-torziju samo nad $\mathbb{Q}(\sqrt{5})$ i da 50B2 ima 15-torziju samo nad $\mathbb{Q}(\sqrt{-15})$, te da 50A1 and 50A2 nemaju twistove sa 5-torzijom.

Ostaje samo dokazati da postoji beskonačno racionalnih eliptičkih krivulja s torzijom $\mathbb{Z}/16\mathbb{Z}$ nad kvadratnim poljima. Njih ćemo konstruirati na sljedeći način. Prvo krenimo od eliptičke krivulje $E$ s torzijom $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ nad $\mathbb{Q}$. Možemo $E(\mathbb{Q})_{tors}$ napisati kao $G \oplus H$, gdje je $G \simeq \mathbb{Z}/2\mathbb{Z}$, a $H \simeq \mathbb{Z}/8\mathbb{Z}$.

Sada možemo promotriti $E/G$ i $E/H$, gdje $E$ promatramo kao $\mathbb{C}/\Lambda$. Pošto postoji bijekcija između konačnih podgrupa od $E$ i izogenija iz $E$, slijedi da nad $\mathbb{Q}$ postoje izogenije $f : E \to E' = E/G$ i $g : E \to E'' = E/H$, gdje je $f$ izogenija stupnja 2, a $g$ je ciklička izogenija stupnja 8. Promatranjem rešetki $\Lambda'$ i $\Lambda''$ vidimo da $f$ nije faktor od $g$ tj. $g$ se ne može napisati kao $g = h \circ f$. Drugim rječima postoji ciklička izogenija $k = \hat{f} \circ g : E' \to E''$. Također $f(G \oplus H) \subset E'(\mathbb{Q}) \simeq \mathbb{Z}/8\mathbb{Z}$, tj. u $\operatorname{Ker} k \simeq \mathbb{Z}/16\mathbb{Z}$ postoji podgrupa $F \simeq \mathbb{Z}/8\mathbb{Z}$.

Iz elementarne teorije grupa zaključujemo da ako je $\operatorname{Ker} k = \langle P \rangle$, tada je $F = \langle 2P \rangle$. Sada promatramo djelovanje od $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ na $\operatorname{Ker} k$. Pošto je $F$ definirana nad $\mathbb{Q}$, ona je fiksna. Dakle pošto je $\sigma(2P) = 2P$, slijedi da je $\sigma(P) = P$ ili $9P$ za svaki $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Ako je $F$ definirana nad nekim poljem $K$, slijedi da $\mathrm{Gal}(K/\mathbb{Q})$ djeluje na $\operatorname{Ker} k$ (kažemo da se $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ faktorizira kroz $\mathrm{Gal}(K/\mathbb{Q})$). Zaključujemo, pa Galoisovoj teoriji da je $\mathrm{Gal}(K/\mathbb{Q})$ grupa reda 2, te da je $K$ kvadratno polje.

Pošto eliptičkih krivulja s torzijom $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ nad $\mathbb{Q}$ ima beskonačno mnogo, zaključujemo da se i traženih krivulja može konstruirati beskonačno mnogo.

□

*Napomena.* Primjetimo da su krivulje 50B1 i 50B2 upravo krivulje iz teorema 77 i napomeni nakon njega. Iako su te krivulje zadane u modelu koji ima koeficijente koji nisu iz $\mathbb{Q}$, one imaju model s koeficijentima nad $\mathbb{Q}$.

**Primjer 29.** Pokažimo eksplicitno kako konstruirati eliptičku krivulju s torzijom $\mathbb{Z}/16\mathbb{Z}$ nad kvadratnim poljem krećući od racionalne eliptičke krivulje. Uzmimo npr. eliptičku krivulju 210E2 iz Cremoninih tablica. To je

$$E : y^2 + xy = x^3 - 1070x + 7812.$$

To je prva krivulja s torzijom $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ koja se pojavljuje u Cremoninim tablicama.

Sada računamo 2-izogenu krivulju $E'$ - to je 210E1

$$E' : y^2 + xy = x^3 + 210x + 900.$$

Nju možemo identificirati tako da je ona 2-izogena s $E$, a nije 2-izogena s ni jednom drugom krivuljom. Primjetimo da 210E4 također ima to svojstvo, dok 210E3 nema. Također, torzija od 210E3 nad $\mathbb{Q}$ je $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Sada računamo (u Magmi) kvocijent 16-djelidbenog i 8-djelidbenog polinoma $\frac{\psi_{16}}{\psi_8}$ od $E'$, te dobivamo da je prvi faktor od tog kvocijenta $x^2 - 240x - 720$, koji generira polje $\mathbb{Q}(\sqrt{105})$. Provjeravamo

$$E'(\mathbb{Q}(\sqrt{105})) \simeq \mathbb{Z}/16\mathbb{Z}.$$

## 23.1 Racionalne eliptičke krivulje nad kubnim poljima

Prije nego krenemo promatrati racionalne eliptičke krivulje nad kubnim poljima, možemo se pitati je li postoji analogon KMK teorema (i Mazurovog teorema) nad kubnim poljima. Na žalost još ne postoji. Postoji sljedeći rezultat Pierrea Parenta iz 2003.

**Teorem 87** (Parent)**.** *Neka je $K$ kubno polje i $E/K$ eliptička krivulja, te neka je $p$ prost broj takav da $p$ dijeli $E(K)_{tors}$. Tada je $p \leq 13$.*

Postoji i rezultat Jeona, Kima i Schweizera iz 2004. godine, koji nam daje grupe koje se pojavljuju kao torzija beskonačno mnogo eliptičkih krivulja (kada idemo kroz sve eliptičke krivulje nad svim kubnim poljima).

**Teorem 88** (Jeona, Kim i Schweizer)**.** *Ako prođemo kroz sve eliptičke krivulje nad svim kubnim poljima, torzijske podgrupe na koje ćemo naići beskonačno puta su sljedeće:*

$$\mathbb{Z}/n\mathbb{Z}, \text{ gdje je } n = 1, \ldots, 16, \ 18, \text{ or } 20$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ gdje je } n = 1, \ldots, 7.$$

Ovo je slabiji rezultat od KMK teorema za kvadratna polja, pošto postoji mogućnost da postoje neke druge grupe koje se pojavljuju konačno mnogo puta. Vidjet ćemo da postoje takve grupe.

Sada ćemo dokazati nekoliko lema o tome kako $E(\mathbb{Q})_{tors}$ može rasti u $E(K)_{tors}$, gdje je $K/\mathbb{Q}$ neko PAB. Nas će zanimati prvenstveno podgrupe neparnog reda - podgrupe parnog reda su puno teže.

**Lema 89.** *Neka su $p, q$ neparni različiti prosti brojevi, $F_2/F_1$ Galoisovo proširenje polja algebarskih brojeva takvo da je $\mathrm{Gal}(F_2/F_1) \simeq \mathbb{Z}/q\mathbb{Z}$, i neka je $E/F_1$ eliptička krivulja bez $p$-torzije nad $F_1$. Tada ako $q$ ne dijeli $p-1$ i $\mathbb{Q}(\zeta_p) \not\subset F_2$, tada je $E(F_2)[p] = 0$.*

*Dokaz.* Pošto ako je jedna točka reda $p$ definirana nad $F_2$, tada su svi višekratnici također definirani nad $F_2$, slijedi da je ili $p-1$ ili $p^2-1$ točaka reda $p$ definirano nad $F_2$, a nije nad $F_1$. Međutim, zbog Weilovog sparivanja, nemoguće je da ih je $p^2-1$ pošto $\mathbb{Q}(\zeta_p) \not\subset F_2$.

Neka je $\langle\sigma\rangle = \mathrm{Gal}(F_2/F_1)$, $P$ točka reda $p$ u $E(F_2)$ i primjetimo da je $P^\sigma \neq P$, te pošto $\mathrm{Gal}(F_2/F_1)$ djeluje na $\langle P\rangle$, slijedi da orbite od $P$ s obzirom na djelovanje od $\mathrm{Gal}(F_2/F_1)$ imaju duljinu $q$, što povlači da se $\langle P\rangle$ razlaže u jednu orbitu duljine 1 (tj. $\mathcal{O} \in E(F_2)$), i oribte duljina $q$, što je kontradikcija, po Teoremu o orbiti i stabilizatoru, s činjenicom da $q$ ne dijeli $p-1$. □

Pošto ćemo promatrati eliptičke krivulje nad kubnim poljima, uvedimo notaciju za polja koja će nam trebati. Polje $K$ će biti kubno polje, $L$ će biti njegovo normalno (tj. Galoisovo) zatvorenje nad $\mathbb{Q}$. Sjetimo se da $K$ može biti ili Galoisovo (tj. $K = L$ i $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$) ili je $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$.

S $M$ označavamo jedinstveno PAB sa svojstvom da je $M$ potpolje od $L$ takvo da je $[L:M] = 3$ (iz čega slijedi da je $\mathrm{Gal}(L/M) \simeq \mathbb{Z}/3\mathbb{Z}$). Ako je $K$ normalno nad $\mathbb{Q}$, ovo znači da je $M = \mathbb{Q}$.

**Lema 90.** *Ako $E(M)$ nema točku reda 3, nema ni $E(L)$.*

*Dokaz.* Neka je $G = \mathrm{Gal}(L/M)$. Tada $G$ djeluje na $E(M)$. Pošto $E(L)[3]$ može imati 3 ili 9 točaka, a $G$ fiksira samo $\mathcal{O} \in E(M)[3]$, slijedi da se $E(L)[3]$ razlaže u orbite duljine 3. To je kontradikcija po Teoremu o orbiti i stabilizatoru. □

Bit će nam bitna i sljedeća lema.

**Lema 91.** *Neka je $n$ neparan cijeli broj koji nije djeljiv sa 3 i pretpostavimo da $E(K)$ ima točku reda $n$. Tada $E/\mathbb{Q}$ ima izogeniju stupnja $n$.*

*Dokaz.* Prvo primjetimo da $E(L)$ ima točku $P$ reda $n$. Neka je

$$\langle\sigma\rangle = \mathrm{Gal}(L/M),\ \langle\tau\rangle = \mathrm{Gal}(L/K),\ \langle\sigma,\tau\rangle = \mathrm{Gal}(L/\mathbb{Q}).$$

Pošto je $P$ $K$-racionalna (tj. definirana nad $K$), slijedi da je $P^\tau = P$. Neka je $E[n] = \langle P, Q\rangle$ i neka je $P^\sigma = \alpha P + \beta Q \in E(L)$. Ali pošto je $(n-\alpha)P + P^\sigma = \beta Q \in E(L)$, slijedi da je $\beta = 0$ jer bi u suprotnome $E(L)$ imala punu $l$-torziju, za neki $l|n$, što je nemoguće pošto $L$ nema $l$-tih korijena iz jedinice.

Dakle

$$P^\mu = kP \text{ za sve } \mu \in \mathrm{Gal}(L/\mathbb{Q}),$$

te pošto se djelovanje od $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ na $\langle P\rangle$ faktorizira kroz $\mathrm{Gal}(L/\mathbb{Q})$, slijedi da je

$$P^\mu = kP \text{ za sve } \mu \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),$$

što znači da $E/\mathbb{Q}$ ima $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ invarijantnu cikličku grupu reda $n$, iz čega slijedi da ima $n$-izogeniju. □

Bit će nam bitna i sljedeća lema.

**Lema 92.** *Neka je $F/\mathbb{Q}$ kvadratno proširenje, $n$ neparan prirodan broj, i $E/\mathbb{Q}$ eliptička krivulja takva da $E(F)$ sadrži $\mathbb{Z}/n\mathbb{Z}$. Tada $E/\mathbb{Q}$ ima $n$-izogeniju.*

*Dokaz.* Kao što smo puno puta već spominjali, ako je $F = \mathbb{Q}(\sqrt{d})$, tada je

$$E(F)[n] = E(\mathbb{Q})[n] \oplus E^d(\mathbb{Q})[n].$$

Tada ili $E(\mathbb{Q})$ ili $E^d(\mathbb{Q})$ imaju netrivijalnu $n$-torziju. Ako eliptička krivulja ima $n$-torziju, tada također ima i $n$-izogeniju $\phi$ (gdje je grupa generirana s točkom reda $n$ jezgra $n$-izogenije), te ako eliptička krivulja ima $n$-izogeniju, tada imaju i svi twistovi od $E$. Tvrdnja leme slijedi iz ove dvije činjenice. □

Sada ćemo pokazati da postoji jedinstvena racionalna eliptička krivulja s torzijom $\mathbb{Z}/21\mathbb{Z}$ nad kubnim poljem $\mathbb{Q}(\zeta_9)^+$. Dakle to je jedina racionalna eliptička krivulja s takvom torzijom nad nekim kubnim poljem, međutim teoretski mogu postojati i eliptičke krivulje koje su definirane nad nekim kubnim poljem (dakle ne mogu se definirati nad $\mathbb{Q}$) s tom torzijom.

Primjetimo i da ova torzijska grupa nije na listi 88. Dakle za razliku od $\mathbb{Q}$ i od kvadratnih polja, nad kubnim poljima postoje "sporadične torzijske grupe", dakle one koje se javljaju kao torzija samo konačno mnogo eliptičkih krivulja.

**Propozicija 93.** *Eliptička krivulja 162$B$1 ima torziju izomorfnu s $\mathbb{Z}/21\mathbb{Z}$ nad $\mathbb{Q}(\zeta_9)^+$. Ovo je jedinstveni par $(E, K)$ racionalne eliptičke krivulje $E$ i kubnog polja takvih da $E(K)$ ima točku reda* 21.

*Dokaz.* Po Lemi 90, ako $E(M)_{tors} = 0$, ili $\mathbb{Z}/7\mathbb{Z}$, tada je $E(L)[3] = 0$. Dakle zaključujemo da $E(M)[3] \neq 0$. Nadalje ako je $M = \mathbb{Q}(\sqrt{d})$ kvadratno polje, tada je ili $E(\mathbb{Q})[3] \neq 0$ ili $E^d(\mathbb{Q})[3] \neq 0$ po Lemi 71. Možemo bez smanjenja općenitosti pretpostaviti da je $E(\mathbb{Q})[3] \neq 0$.

Pretpostavimo sada da je $E(K)[21] \supset \mathbb{Z}/21\mathbb{Z}$. Po Lemi 91, slijedi da $E/\mathbb{Q}$ ima izogeniju stupnja 7, i pošto ima 3-torzijsku točku, mora imati i 21-izogeniju. Postoje 4 krivulje (do na $\overline{\mathbb{Q}}$-izomorfizam) s 21-izogenijom (vidi tablicu). To su krivulje u klasama izogenija 162B i 162C. Primjetimo da je klasa izogenija 162B $-3$ twist od klase 162C.

Korištenjem djelidbenih polinoma dobivamo da među twistovima u klasama izogenija 162B i 162C jedine krivulje koje imaju netrivjalnu 3-torziju su krivulje 162C1, 162C3, 162B1 i 162B3. Korištenjem djelidbenih polinoma dobivamo da 162B1 ima 7-torzijsku točku nad kubnim poljem $\mathbb{Q}(\zeta_9)^+$, koje je generirano polinomom $x^3 - 3x^2 + 3$. □

# Poglavlje 24

# Upotreba eliptičkih krivulja u rješavanju diofantskih jednadžbi

U ovom poglavlju ćemo pokazati kako se eliptičke krivulje mogu koristiti za rješavanje diofantskih jednadžbi.

Krenimo sa sljedećim jednostavnim primjerom, gdje ćemo rješiti dva specijalna slučaja Fermatovog posljednjeg teorema, za $n = 3, 4$, i to za $\mathbb{Q}(i)$, a ne samo za $\mathbb{Q}$. Također, primjetimo da ćemo mi naći i sva racionalna, a ne samo rješenja iz nekog potprstena.

Rješenja Fermatove jednadžbe

$$x^n + y^n = z^n \tag{24.1}$$

ćemo zvati **trivijalnima** ako je $xyz = 0$.

Rješimo najprije problem za $n = 3$ nad $\mathbb{Q}(i)$.

**Teorem 94.** *Jednadžba $x^3 + y^3 = z^3$ nema netrivijalna rješenja nad $\mathbb{Q}(i)$.*

*Dokaz.* Dovedimo prvo jednadžbu $x^3 + y^3 = z^3$, koja opisuje projektivnu krivulju, u afine koordinate te u Weierstrassovu formu za eliptičke krivulje. Ovo je krivulja genusa 1, te ima očitu (trivijalnu) točku $(1, -1, 0)$, tako da lako zaključujemo da je to eliptička krivulja.

Napravimo zamjenu varijabli

$$x = 3u, \;\; y = -v \;\; z = 9 - v,$$

te dobivamo

$$27u^3 - v^3 = 9^3 - 3 \cdot 9^2 v + 27v^2 - v^3,$$

te nakon kraćenja i dijeljenja sa 27 dobivamo eliptičku krivulju u Weierstrassovoj formi

$$E : v^2 - 9v = u^3 - 27,$$

te izračunamo da je $E(\mathbb{Q}(i)) \simeq \mathbb{Z}/3\mathbb{Z}$, te da torzijske točke odgovaraju točkama $(-1:0:1),\ (-1:1:0)$ i $(0:-1:1)$ na početnoj krivulji. □

Sada ćemo dokazati jaču tvrdnju od Fermatovog teorema za $n = 4$, tj. pokazat ćemo da $x^4 \pm y^4 = z^2$ nema rješenja. Primjetimo da ako $x^4 \pm y^4 = z^2$ nema rješenja tada nema očito nema ni $x^4 \pm y^4 = z^4$.

**Teorem 95.** *Diofantska jednadžba $x^4 + y^4 = z^2$ nema netrivijalna rješenja u $\mathbb{Q}(i)$.*

*Dokaz.* Pretpostavimo da je $(x, y, z)$ netrivijalno rješenje. Djeleći jednadžbu s $y^4$ te nakon zamjene varijabli $s = x/y,\ t = z/y^2$, dobivamo jednadžbu $s^4 \pm 1 = t^2$, gdje su $s, t \in \mathbb{Q}(i)$. Možemo ovu jednadžbu zapisati kao

$$r = s^2, \tag{24.2}$$

$$r^2 \pm 1 = t^2, \tag{24.3}$$

te množenjem ove dvije jednadžbe, te zamjenom varijabli $a = st$, dobivamo dvije eliptičke krivulje

$$a^2 = r^3 \pm r.$$

Te dvije krivulje su izomorfne nad $\mathbb{Q}(i)$, te imaju rang 0, te torziju $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ nad $\mathbb{Q}(i)$. Lako se provjeri da sve torzijske točke daju trivijalna rješenja u početnoj jednadžbi. □

Pogledajmo sada drukčiju primjenu eliptičkih krivulja u rješavanju diofantskih jednadžbi, tj. u određivanju racionalnih točaka na krivuljama višeg genusa.

Prvo ćemo imati jedan vrlo jednostavan primjer.

**Primjer 30.** Nađimo sve racionalne brojeve $x$ i $y$ koji zadovoljavaju

$$y^2 = x^6 + 1. \tag{24.4}$$

Neka je $u = x^2$. Tada svako rješenje od (24.4) daje (barem jednu) racionalnu točku na eliptičkoj krivulji

$$E : y^2 = x^3 + 1.$$

Međutim računamo da je $E(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$, te da je

$$E(\mathbb{Q}) = \{\mathcal{O},\ (-1, 0),\ (0, \pm 1),\ (2, \pm 3)\}.$$

Vidimo da će na početnoj krivulji rješenja davati samo $x = 0$, pa su $(0, \pm 1)$ jedina rješenja početnog problema.

Promotrimo sličan, ali složeniji primjer.

**Primjer 31.** Nađimo sve racionalne brojeve $x$ i $y$ koji zadovoljavaju

$$C : 2y^2 = x^6 + 1. \tag{24.5}$$

Prvo što nam može pasti na pamet je postupiti kao u prošlom slučaju, međutim eliptička krivulja $2y^2 = x^3 + 1$ ima beskonačno rješenja, tako da nam taj pristup neće proći.

Ono što smo u prošlom primjeru zapravo radili je da smo našli eliptičku krivulju $E$ koju je naša početna krivulja $C$ natkrivala. Tj. u prošlom primjeru smo našli $E$ takav da je

$$C \xrightarrow{2} E$$

*natkrivanje* stupnja 2. Zatim smo uspjeli naći $E(\mathbb{Q})$, te onda naći sve točke na $C(\mathbb{Q})$.

U ovom primjeru ćemo postuputu suprotno, tj. konstruirat ćemo familiju natkrivanja $D_\delta$ od $C$, te odrediti sve točke na tim natkrivanjima.

Prvo raspišimo

$$2y^2 = x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1).$$

Definiramo

$$D_\delta = \begin{cases} x^2 + 1 = 2\delta y_1^2 \\ x^4 - x^2 + 1 = \delta y_2^2 \\ y = \delta y_1 y_2 \end{cases} \tag{24.6}$$

Može se pokazati da je $D_\delta \longrightarrow C$ natkrivanje stupnja 2, za svaki $\delta \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Također, lako se vidi da za svaku racionalnu točku na $C$, postoji racionalna točka na $D_\delta$, za neki $\delta$.

Međutim, prvi očiti problem je da krivulja $D_\delta$ ima beskonačno mnogo. Pokažimo prvo da sve osim konačno mnogo $D_\delta$ nema racionalnih točaka.

Neka je prvo $p$ prost neparan broj koji dijeli $\delta$. Tada prvo primjetimo da nazivnik od $x$ ne može biti djeljiv sa $p$ iz prve jednadžbe, pošto bi lijeva strana imala parnu, a desna neparnu $p$-adsku valuaciju. Dakle, možemo pretpostaviti da je $x$ cijeli $p$-adski broj, tj. $x \in \mathbb{Z}_p$. Nadalje zaključujemo da $p$ dijeli $x^2 + 1$ (u $\mathbb{Z}_p$), te analogo $p|x^4 - x^2 + 1$. Sada se vrlo lako dobije da vrijedi da $p|3$.

Zaključujemo da je $\delta \in \pm 1, \pm 2, \pm 3, \pm 6$. Iz prve jednadžbe odmah zaključujemo da je $\delta > 0$. Pokažimo sada da 3 ne može dijeliti $\delta$. Kad bi se to dogodilo, tada bi u prvoj jednadžbi imali (sjetimo se $x \in \mathbb{Z}_3$) $x^2 + 1 \equiv 0 \pmod 3$, što je nemogu će.

Promotrimo još sada što kada je $\delta = 2$. Iz druge jednadžbe zaključujemo da je $x \in \mathbb{Z}_2$, međutim slijedi da će lijeva strana uvijek imati parnu, a desna stranu neparnu 2-adsku valuaciju.

Dakle zaključujemo da je $D_\delta(\mathbb{Q}) = \emptyset$ za sve $\delta \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Osim možda za $\delta = 1$. Odredimo $D_1(\mathbb{Q})$. Imamo $y_2^2 = x^4 - x^2 + 1$, te lako dobijemo da je ova krivulja izomorfna sa

$$E : v^2 = u^3 - u^2 - 4u + 4,$$

te dobivamo da je $E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Ostaje provjeriti koje racionalne točke na $E$ daju točke na $C(\mathbb{Q})$. Dobivamo da su to samo $(\pm 1, \pm 1)$.

## 24.1 Problem kongruentnih brojeva

Kažemo da je prirodan broj $n$ kongruentan ako je on površina nekog pravokutnog trokuta čije su sve stranice racionalne duljine. Ovaj problem potječe još iz stare Grčke, a još nije u potpunosti riješen.

Pokažimo sada vezu kongruentnih brojeva i eliptičkih krivulja. Pretpostavimo da su $a$ i $b$ katete, a $c$ hipotenuza pravokutnog trokuta s površinom $n$. Tada je

$$a^2 + b^2 = c^2,$$
$$\frac{ab}{2} = n.$$

Neka je

$$E_n : y^2 = x^3 - n^2 x.$$

Sljedeća propozicija će nam dovesti u vezu određene točke na $E_n(\mathbb{Q})$ i trojke $(a, b, c)$ koje su stranice pravokutnog trokuta s površinom $n$.

**Propozicija 96.** *Neka je $n$ fiksan pozitivan broj. Postoji bijekcija između pravokutnih trokuta sa stranicama $a, b, c \in \mathbb{Q}^+$, $a < b < c$ i površinom $n$, i $x \in \mathbb{Q}^+$ takvih da su $x, x + n, x - n \in \mathbb{Q}^2$. Bijekcija je dana sa*

$$x = (c/2)^2,$$
$$a = \sqrt{x+n} - \sqrt{x-n},\ b = \sqrt{x+n} + \sqrt{x-n},\ c = 2\sqrt{x}.$$

*Dokaz.* Neka je $a^2 + b^2 = c^2$ i $ab/2 = n$. Dodajmo i oduzmimo 4 puta drugu jednadžbu prvoj. Dobivamo

$$(a \pm b)^2 = c^2 \pm 4n.$$

Podijelimo li obje strane sa 4, dobivamo da broj $x = (c/2)^2$ ima svojstvo da su i $x \pm n$ kvadrati od $(a \pm b)/2$.

Obrnuto, za dani $x$ s traženim svojstvima, lako je vidjeti da racionalni brojevi $a < b < c$ zadovoljavaju $ab/2 = n$, te $a^2 + b^2 = c^2$. Još bi trebalo provjeriti da dvije različite trojke $(a, b, c)$ ne mogu dati isti $x$; ovo ostavljamo za vježbu. □

Pošto tražimo $x$-eve takve da su $x, x - n, x + n$ svi kvadrati, prirodno je pomnožiti ih i dobiti eliptičku krivulju $E_n$. Međutim, jasno je da neće svaka točka na $E_n(\mathbb{Q})$ davati traženu trojku.

Preciznije nam govori o tome sljedeća propozicija.

**Propozicija 97.** *Neka je $(x, y) \in E_n(\mathbb{Q})$ takvi da je $x \in \mathbb{Q}^2$, nazivnik od $x$ je paran, te je brojnik od $x$ relativno prost sa $n$. Tada postoji trojka $(a, b, c)$ koja odgovara $x$-u kao u propoziciji 96.*

*Dokaz.* Neka je $u = \sqrt{x} \in \mathbb{Q}^+$. Stavimo $v = y/u$, dakle $v^2 = y^2/x = x^2 - n^2$ (iz definicije $E_n$). Dakle $v^2 + n^2 = x^2$. Neka je sada $t$ nazivnik od $u$, dakle $tu \in \mathbb{Z}$. Po pretpostavci je $t$ paran. Primjetimo, također, da su nazivnici od $v^2$

i od $x^2$ jednaki. Dakle imamo da je $t^2v, t^2n, t^2x$ primitivna Pitagorina trojka, te da postoje $a, b \in \mathbb{N}$ takvi da je

$$t^2n = 2ab,\ t^2v = a^2 - b^2,\ t^2x = a^2 + b^2.$$

Tada trokut sa stranicama $2a/t, 2b/t, 2c/t$ ima površinu $2ab/t^2 = n$, kao što smo i tražili. □

Sljedeći korak koji trebamo napraviti je odrediti $E_n(\mathbb{Q})_{tors}$. Prvo primjetimo da je $E_n : y^2 = x(x-n)(x+n)$, tj. imamo da je $E[2] \subset E(\mathbb{Q})$. Nadalje, trebat ćemo odrediti broj točaka koje ima $E_n(\mathbb{F}_p)$ za $p \equiv 3 \pmod 4$, $p \nmid n$.

**Propozicija 98.** *Neka je $p$ prost broj, $p \equiv 3 \pmod 4$, $p \nmid 2n$. Tada je $|E(\mathbb{F}_p)| = p + 1$.*

*Dokaz.* Prvo primjetimo da se cijeli $E[2]$ ulaže u $E(\mathbb{F}_p)$ - to su točka u beskonačnosti, $(0,0)$ i $(\pm n, 0)$. Sada posložimo preostalih $p-3$ $x$-eva ($x \neq 0, \pm n$) u $(p-3)/2$ parova $\{x, -x\}$. Primjetimo da je $x^3 - n^2x$ neparna funkcija, te da $-1$ nije kvadratni ostatak modulo $q$, te slijedi da je za točno jedan od $x$ i $-x$, vrijednost $x^3 - n^2x$ kvadrat. Dakle, dobivamo da traženih parova $(x, y)$, ne brojeći točke iz $E[2]$ ima točno $p-3$, dakle $E_n(\mathbb{F}_p)$ ima $p+1$ točaka. □

Sada možemo dokazati da je torzija od $E_n(\mathbb{Q})$ jednaka $E[2]$.

**Propozicija 99.** *Vrijedi*

$$E_n(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

*Dokaz.* Primjetimo prvo da $E(n)$ ima dobru redukciju za svaki $p \nmid 2n$. Pretpostavimo da $E_n(\mathbb{Q})_{tors}$ ima točku reda $k$ za neki $k > 2$. Tada za svaki prost $p$, takav da je $p \equiv 3 \pmod 4$ i $p \nmid 2nk$, slijedi da $E_n(\mathbb{F}_p)$ ima točku reda $k$, dakle da po prethodnoj propoziciji $k | p+1$ za skoro sve proste brojeve $p \equiv 3 \pmod 4$. To je očita kontradikcija.

□

Trebat će nam još jedna općenita propozicija koju nećemo dokazivati. Želimo vidjeti kako algebarski opisati točke na eliptičkoj krvulji $E_n(\mathbb{Q})$ koje zadovoljavanju uvjete iz propozicije 96.

**Propozicija 100.** *Neka je $E$ eliptička krivulja*

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3),\ e_1, e_2, e_3 \in \mathbb{Q}.$$

*Neka je $P \in E(\mathbb{Q}) \backslash \{\mathcal{O}\}$. Tada je $P \in 2E(\mathbb{Q}) \backslash \{\mathcal{O}\}$ ako i samo ako su $x - e_1, x - e_2, x - e_3$ svi kvadrati racionalnih brojeva.*

*Dokaz.* Dokaz je elementaran, ali dosta dug; vidi [7, Proposition 20, pp. 47]. □

Treba nam također sljedeća jednostavna lema, koju također ne dokazujemo.

**Lema 101.** *Neka je* $(x, y) \in 2E_n(\mathbb{Q})\backslash\{\mathcal{O}\}$. *Tada je nazivnik od* $x$ *paran i brojnik od* $x$ *je realtivno prost sa* $n$.

Sada vidimo da mi zapravo tražimo točke $\neq \mathcal{O}$ koje su 2 puta neka druga točka. Kako to ne mogu biti torzijske točke, dokazali smo zapravo sljedeći teorem.

**Teorem 102.** *Broj* $n$ *je kongruentan ako i samo ako* $E_n(\mathbb{Q})$ *ima pozitivan rang.*

*Napomena.* Možemo zaključiti da ako je $n$ kongruentan, tada ima beskonačno točaka u $2E_n(\mathbb{Q})$, te time i beskonačno različitih pravokutnih trokuta sa racionalnim stranicama čija je površina jednaka $n$.

Iskažimo za kraj neke poznate rezultate o kongruentnim brojevima.

**Teorem 103.** *Neka je* $p$ *prost cijeli broj. Tada vrijedi:*

1. *Ako je* $p \equiv 3 \pmod 8$, *tada* $p$ *nije kongruentan broj, a* $2p$ *je.*
2. *Ako je* $p \equiv 5 \pmod 8$, *tada je* $p$ *kongruentan broj.*
3. *Ako je* $p \equiv 7 \pmod 8$, *tada su i* $p$ *i* $2p$ *kongruentni brojevi.*

**Teorem 104** (Tian, 2012.)**.** *Neka je* $k$ *cijeli broj. Postoji beskonačno mnogo kvadratno slobodnih* $n$*-ova u svakoj klasi kongruencija* $n \equiv 5, 6, 7 \pmod 8$ *takvih da* $n$ *ima* $k$ *prostih faktora i da je* $n$ *kongruentan broj.*

Spomenimo i da je Fermat dokazao da 1 nije kongruentan broj (ovaj teorem je poznat kao Fermatov teorem o pravokutnom trokutu), što je u našoj terminologiji ekvivalentno tome činjenici da eliptička krivulja

$$E_{-1} : y^2 = x^3 - x$$

ima rang 0 nad $\mathbb{Q}$.

## 24.2 Modularna metoda za rješavanje diofantskih jednadžbi

Sada ćemo prikazati tzv. modularnu metodu za rješavanje diofantskih jednadžbi. To je metoda s kojom je Andrew Wiles 1995. riješio posljednji Fermatov teorem. Rezultate koje ćemo koristit ćemo uglavnom iskazivati bez dokaza. Sve ćemo rezultate iskazivati u što manjoj generalnosti, i na najnižoj mogućoj razini, takvoj da možemo koristiti. Slijedit ćemo bilješke Samira Sikseka, koje se mogu naći na `http://temple.birs.ca/~12ss131/samirnotes.pdf`.

Prvo će nam trebati koncept **newforme**. To je vrsta modularne forme koja ima razvoj u Fourierov red, tj. $q$-razvoj oblika

$$f = q + \sum_{n \geq 2} c_n q^n,$$

gdje su $c_i$ elementi nekog potpuno realnog polja algebarskih brojeva $K$ (postoje i druge modularn forme za koje to vrijedi, međutim nama je jedino bitno da newforme to zadovoljavaju). Štoviše, oni su elementi prstena cijelih brojeva $\mathcal{O}_K$ polja $K$. Također, ako je $l$ prost broj tada vrijedi

$$|c_l^\sigma| \leq 2\sqrt{l}.$$

Svaka newforma ima težinu (koju smo ranije definirali) te nivo $N$. Nećemo precizno definirati nivo - otprilike nivo newforme $N$ je najmanji $N$ takav da je djelovanje newforme invarijantno s obzirom na djelovanje grupe $\Gamma_0(N)$ na gornju poluravninu.

**Činjenica.** Za svaki prirodan broj $N$, postoji konačno mnogo newformi nivoa $N$. One se daju eksplicitno odrediti u Magmi s kodom

```
Newforms(CuspForms(N));
```

Na primjer za $N = 110$, imamo sljedeće newforme

$$q - q^2 + q^3 + q^4 - q^5 - q^6 + 5q^7 + \dots$$
$$q + q^2 + q^3 + q^4 - q^5 + q^6 - q^7 + \dots$$
$$q + q^2 - q^3 + q^4 + q^5 - q^6 + 3q^7 + \dots$$
$$q - q^2 + \theta q^3 + q^4 + q^5 - \theta q^6 - \theta q^7 + \dots$$
$$q - q^2 + \theta^\sigma q^3 + q^4 + q^5 - \theta^\sigma q^6 - \theta^\sigma q^7 + \dots,$$

gdje je $\theta = (-1 + \sqrt{33})/2$, a $\sigma$ je netrivijalni automorfizam od $\mathbb{Q}(\sqrt{33})$.

Sjetimo se još jednom teorema o modularnosti

**Teorem 105** (Teorem o modularnosti (drugi iskaz))**.** *Svakoj* ***racionalnoj*** *newformi (tj. onoj kojoj su svi koeficijenti iz $\mathbb{Q}$) $f$ nivoa $N$ je pridružena eliptička krivulja $E_f/\mathbb{Q}$ konduktora $N$ takva da za sve proste brojeve $l \nmid N$*

$$c_l = a_l(E_f),$$

*gdje je $c_l$ $l$-ti koeficijent u $q$-razvoju od $f$ i $a_l(E_f) = l + 1 - |E_f(\mathbb{F}_l)|$. Za svaki prirodan broj $N$, pridruživanje $f \to E_f$ je bijekcija između racionalnih newformi nivoa $N$ i klasa izogenija eliptičkih krivulja konduktora $N$.*

Pridruživanje $f \to E_f$ je dokazao Shimura, dok je obrat dokazao za kvadratno slobodne $N$-ove Wiles, te su zatim dokaz završili za sve $N$-ove Breuil, Conrad, Diamond i Taylor.

Možemo se pitati postoji li prirodni $N$-ovi za koje ne postoje newforme nivoa $N$. O tome nam govori sljecdeći teorem.

**Teorem 106.** *Ne postoje newforme nivoa*

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60.$$

**Definicija.** Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je

$$f = q + \sum_{n\geq 2} c_n q^n \quad K = \mathbb{Q}(c_2, c_3, \ldots)$$

newforma. Kažemo da krivulja $E$ **nastaje modulo** $p$ **iz newforme** $f$ ako postoji neki prosti ideal $\mathfrak{P}|p$ od $\mathcal{O}_K$ takav da je

$$a_l(E) \equiv c_l \pmod{\mathfrak{P}} \text{ za skoro sve proste brojeve } l.$$

Koristimo notaciju $E \sim_p f$.

Iskažimo sada malo preciznije uvjete za "nastajati iz":

**Propozicija 107.** *Neka je $E/\mathbb{Q}$ eliptička krivulja sa konduktorom $N$, te neka $f$ ima nivo $N'$. Pretpostavimo da je $E \sim_p f$. Tada postoji ideal $\mathfrak{P}|p$ takav da za sve proste brojeve $l$ vrijedi*

1. *ako $l \nmid pNN'$, tada $a_l(E) \equiv c_l \pmod{\mathfrak{P}}$,*
2. *ako $l \nmid pN'$ i $l\|N$ tada $l+1 \equiv \pm c_l \pmod{\mathfrak{P}}$.*

*Ako $E \sim_p f$ i $f$ je racionalna, tada pišemo $E \sim_p E_f$.*

Sljedeća propozicija je vrlo slična, međutim ona je ipak malo jača, pošto miče uvjet $l \neq p$.

**Propozicija 108.** *Neka $E$ i $E'$ imaju konduktore $N$ i $N'$. Ako $E \sim_p E'$, tada za sve proste brojeve $l$ vrijedi*

1. *ako $l \nmid NN'$ tada $a_l(E) \equiv a_l(E') \pmod{p}$,*
2. *alo $l \nmid N'$ i $l\|$ tada $l+1 \equiv \pm a_l(E') \pmod{p}$.*

Primjetimo da u gore navedenim propozicijama $l \nmid NN'$ znači da $E$ i $E'$ imaju dobru redukciju u $l$ (sjetimo se da su prosti faktori od $N$ upravo prosti brojevi u kojima $N$ ima lošu redukciju).

Neka je $E/\mathbb{Q}$ eliptička krivulja nad $\mathbb{Q}$ u minimalnom modelu, s minimalnom diskriminantom (tj. diskriminantom minimalnog modela) $\Delta$ i s konduktorom $N$. Pretpostavimo da je $p$ prost broj, te neka je

$$N_p = N/\prod_{\substack{q\|N,\\ p|\operatorname{ord}_q \Delta}} q.$$

Sada ćemo iskazati jednostavnu verziju tzv. Ribetovog teorema o snižavanju nivoa.

**Teorem 109** (Ribet)**.** *Pretpostavimo da je $E/\mathbb{Q}$ eliptička krivulja i da je $p \geq 5$ prost takav da $E$ nema izogeniju stupnja $p$ nad $\mathbb{Q}$. Tada postoji newforma $f$ nivoa $N_p$ takva da je $E \sim_p f$.*

*Napomena.* Primjetimo da newforma iz Ribetovog teorema ne mora biti racionalna!

Ribetov teorem je puno općenitiji od iskazanog, međutim ovo je jedini slučaj koji će nama trebati.

**Primjer 32.** Promotrimo eliptičku krivulju

$$E : y^2 = x^3 - x^2 - 77x + 330;$$

to je eliptička krivulja s oznakom $132B1$ u Cremoninim tablicama. Minimalna diskriminanta i konduktor su

$$\Delta = 2^4 \times 3^{10} \times 11, \quad N = 2^2 \times 3 \times 11.$$

Jedina izogenija koju ova krivulja ima je 2-izogenija. Primjenimo Ribetov teorem na za $p = 5$. Dobivamo da je $N_5 = 44$. Postoji samo jedna newforma nivoa 44 i ona odgovara eliptičkoj krivulji

$$E' : y^2 = x^3 + x^2 + 3x - 1$$

koja ima oznaku $44A1$ u Cremoninim tablicama. Dakle $E \sim_5 E'$. Provjerimo to - računamo $a_l(E)$ i $a_l(E')$ za $2 \leq l \leq 19$.

| $l$ | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 |
|---|---|---|---|---|---|---|---|---|
| $a_l(E)$ | 0 | $-1$ | 2 | 2 | $-1$ | 6 | $-4$ | $-2$ |
| $a_l(E')$ | 0 | 1 | $-3$ | 2 | $-1$ | $-4$ | 6 | 8 |

Vidimo da je u Ribetovom teoremu bitno da eliptička krivulja nema izogenija stupnja $p$. Najlakši način provjeravanja te činjenice je faktorizacijom $p$-tog djelidbenog polinoma - ako dobijemo da $\psi_p(E)$ nema faktora stupnja $d|p-1$, tada nema ni $p$-izogeniju.

Druga mogućnost je primjeniti sljedeći teorem.

**Definicija.** Eliptička krivulja $E/\mathbb{Q}$ je polustabilna ako nema aditivnu redukciju ni u jednnom prostom broju $p$.

Eliptička krivulja je polustabilna ako i samo ako joj je konduktor kvadratno slobodan.

**Teorem 110.** *Neka je $E/\mathbb{Q}$ eliptička krivulja koja zadovoljava barem jedan od sljedećih uvjeta.*

1. *$p \geq 17$ i $j(E) \notin \mathbb{Z}[\frac{1}{2}] = \{a/b : a, b \in \mathbb{Z}, (a, b) = 1, b = 2^k\}$.*
2. *$p \geq 11$ i $E$ je polustabilna eliptička krivulja*
3. *$p \geq 5$, $|E(\mathbb{Q})[2]| = 4$ i $E$ je polustabilna*

*Tada $E$ nema $p$-izogeniju.*

Drugi koristan teorem je sljedeći.

**Teorem 111** (Diamond i Kramer)**.** *Pretpostavimo da je $E$ eliptička krivulja s konduktorom $N$. Ako je* $\operatorname{ord}_2 N = 3, 5$ *ili* $7$*, tada $E$ nema izogenija neparnog stupnja.*

Pokažimo sada kako korisiti Ribetovo teorem za rješavanje diofantskih jednadžbi. Za to ćemo trebati konstruirati **Freyove krivulje**. Pretpostavimo da zadana diofantska jednadžba ima rješenje.

Freyova krivulja $E$ je eliptička krivulja sa sljedećim svojstvima.

1. Koeficijenti od $E$ ovise o rješenju zadane diofantske jednadžbe.
2. Minimalna diskriminanta dobivene eliptičke krivulje se može napisati kao $\Delta = C \cdot D^p$, gdje je $D$ vrijednost koja ovisi o rješenju Diofanstske jednadžbe. Vrijednost $C$ ne ovisi o rješenju diofanstske jednadžbe.
3. $E$ ima multiplikativnu redukciju u prostim brojevima koji dijele $D$.

Konduktor $N$ od $E$ će dijeliti prosti brojevi koji dijele $C$ i $D$, te će oni koji dijele $D$ biti maknuti kada snizimo nivo i dobijemo $N_p$. Tako možemo zapravo dobiti konačnu listu mogućih $N_p$-ova koji ovise o početnoj jednadžbi.

Dakle, možemo eksplicitno izračunati konačnu listu newformi $f$ takvih da je $E \sim_p f$, te iz podataka o $f$ možemo zaključiti neke činjenice o rješenjima diofantske jednadžbe.

Sada smo spremni upotrijebiti mašineriju koju smo razvili za dokaz posljedenjeg Fermatovog teorema.

**Teorem 112** (Wiles)**.** *Neka je $p \geq 5$ prost broj. Jednadžba*

$$x^p + y^p + z^p = 0 \tag{24.7}$$

*nema rješenja takvih da je $xyz \neq 0$.*

*Dokaz.* Pretpostavimo da je $xyz \neq 0$. Bez smanjenja općenitosti možemo pretpostaviti da su $x, y$ i $z$ (u parovima) relativno prosti. Nadalje možemo pretpostaviti da

$$2|y, \quad x^p \equiv -1 \pmod 4, \quad z^p \equiv 1 \pmod 4.$$

Sljedeći korak koji trebamo napraviti je konstruirati Freyovu krivulju. To će nam biti

$$E : Y^2 = X(X - x^p)(X + y^p).$$

Diskriminanta ove eliptičke krivulje je

$$\Delta = 16x^{2p}y^{2p}(x^p + y^p)^2 = 16(xyz)^{2p}.$$

Ovo je diskriminata, međutim ona nije minimalna. Postoji tzv. Tateov algoritam (kojeg nećemo opisivati) za računanje minimalne diskriminante eliptičke krivulje, te se on može primjeniti i u ovakvim slučajevima, gdje imamo "varijable". Dobivamo

$$\Delta_{min} = 2^{-8}(xyz)^{2p}$$

te dobivamo da je konduktor

$$N = \prod_{l|xyz} l.$$

Sada računamo

$$N/ \prod_{\substack{q\|N,\\ p|\operatorname{ord}_q \Delta}} q,$$

te dobivamo $N_p = 2$. Također, $|E(\mathbb{Q})[2]| = 4$ i $N$ je kvadratno slobodan (tj. eliptička krivulja je polustabilna), pa po Teoremu 110 imamo da ona nema $p$-izogeniju.

Sada po Ribetovom teoremu o snižavanju nivoa imamo $E \sim_p f$, gdje je $f$ newforma nivoa 2. Međutim, po Teoremu 106, takva newforma ne postoji. Došli smo do kontradikcije, dakle rješenje ne postoji. □

# Bibliografija


[1] E. Artin, Galois Theory, Dover Publications Inc. Mineola, NY, second edition, 1998.

[2] F. Diamond and J. Shurman, A First Course in Modular Forms, Springer, 2005.

[3] D. Hüsemoller, Elliptic Curves, Second Edition, Springer, 2004.

[4] M. A. Kenku, *The modular curves* $X_0(65)$ *and* $X_0(91)$ *and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20.

[5] M. A. Kenku, *The modular curve* $X_0(169)$ *and rational isogeny*, J. London Math. Soc. (2) **22** (1980), 239–244.

[6] M. A. Kenku, *On the modular curves* $X_0(125)$, $X_1(25)$ *and* $X_1(49)$, J. London Math. Soc. (2) **23** (1981), 415–427.

[7] N. Koblitz, Introduction to Elliptic Curves and Modular Forms, Second Edition, Springer, New York, 1993.

[8] D. Marcus, Number Fields, Springer, 1977.

[9] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[10] J. S. Milne, Elliptic Curves, 2006. `http://www.jmilne.org/math/Books/ectext5.pdf`

[11] Modular functions of one variable IV, Edited by B. J. Birch and W. Kuyk. Lecture Notes in Mathematics, Vol. 476. Springer-Verlag, Berlin-New York, 1975.

[12] F. Najman, *Torsion of elliptic curves over cubic fields,* J. Number Theory, **132** (2012), 26–36.

[13] J. P. Serre, A Course in Arithmetic, Sprimger, 1973.

[14] J. Silverman, Arithmetic of Elliptic Curves, 2nd edition, Springer, 2009.

[15] T. Weston, Algebraic Number Theory, `https://www.math.umass.edu/~weston/cn/notes.pdf`

[16] Y. Yang, *Defining equations of modular curves*, Adv. Math. **204** (2006), 481.–508.