Eliptičke krivulje i Mordell-Weilov teorem

Dražić, Goran

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Goran Dražić

ELIPTIČKE KRIVULJE I MORDELL-WEILOV TEOREM

Diplomski rad

Voditelj rada:
doc. dr. sc. Matija Kazalicki

Zagreb, lipanj 2015.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Obitelji i prijateljima

Sadržaj

Uvod

Eliptička krivulja je glatka projektivna krivulja genusa jedan sa istaknutom baznom točkom. Eliptičke krivulje imaju važnu primjenu u modernoj matematici. Igrale su veliku ulogu u dokazu velikog Fermatovog teorema (Taniyama-Shimura-Weilova hipoteza), Birch i Swinerton-Dyerova hipoteza(jedan od milenijskih problema) je tvrdnja o aritmetici eliptičkih krivulja. Koriste se u mnogim algoritmima za faktorizaciju te kriptiranje podataka.
Na eliptičkoj krivulji možemo definirati zbrajanje koje ju čini grupom. Dvije točke zbrajamo tako da kroz njih povučemo pravac, gledamo treću presječnu točku s krivuljom, odnosno njenu simetričnu točku u odnosu na x-os koju definiramo kao zbroj početnih točaka.

Teorem 0.0.1 (Mordell-Weil)**.** *Neka je E/K eliptička krivulja nad poljem algebarskih brojeva K. Grupa K-racionalnih točaka $E(K)$ je konačno generirana Abelova grupa.*

Posebno, ako promatramo polje $\mathbb{Q}$, definiramo rang kao broj kopija $\mathbb{Z}$ u $E(\mathbb{Q})$. Trenutno je otvoreno pitanje o konačnosti ranga, najveći znani rang neke eliptičke krivulje je 19, a postoje i krivulje ranga barem 28, ali se ne zna koliko im je točan rang.
Jedan od najbitnijih teorema za eliptičke krivulje je Mazurov teorem koji kaže da torzijska grupa od $E(\mathbb{Q})$ može biti samo jedna od 15 slijedećih grupa: $\mathbb{Z}/n\mathbb{Z}$ za $n = 1, \ldots, 10$ ili 12 te $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ za $n = 1, 2, 3, 4$.

U prvom poglavlju definiramo pojmove krivulje i divizora te iskazujemo Riemann-Rochov teorem. Drugo poglavlje definira eliptičku krivulju preko Weierstrassovih jednadžbi, opisuje zbrajanje točaka na krivulji te definira pojam redukcije. U trećem poglavlju promatramo eliptičke krivulje nad $\mathbb{C}$, za koje vrijedi da se mogu poistovjetiti sa torusom. Slijedeća dva poglavlja služe da pojednostavnimo račune i dokaze nekih rezultata za eliptičke krivulje. U zadnjem poglavlju dokazujemo početni teorem, čiji je dokaz podijeljen na dva dijela: Dokaz da je $E(K)/mE(K)$ konačna grupa te proceduru spusta, koja koristi konačnost grupe $E(K)/mE(K)$.

Poglavlje 1

Uvod u algebarsku geometriju

1.1 Mnogostrukosti

Budući da želimo proučavati krivulje, potrebno je uvesti jezik algebarske geometrije. $K[X] = K[X_1, \ldots, X_n]$ zovemo *prsten polinoma* u n varijabli s *poljem razlomaka* $K(X)$ racionalnih funkcija na K (analogno za $\bar{K}$). Neka je $I \subset \bar{K}[X]$ ideal. Svakom takvom I pridružimo podskup od $\mathbb{A}^n$

$$V_I = \{P \in \mathbb{A}^n \colon f(P) = 0, \quad \forall f \in I\} \tag{1.1}$$

Definicija 1.1.1. *Afini algebarski skup je bilo koji skup oblika V_I. Ako je V algebarski skup,* ideal od *V je dan sa*

$$I(V) = \{f \in \bar{K}[X] \colon f(P) = 0, \quad \forall P \in V\}. \tag{1.2}$$

Algebarski skup je definiran nad *K ako se njegov ideal $I(V)$ može generirati polinomima iz $K[X]$. Ovo označavamo sa V/K.*

Definicija 1.1.2. *Afini algebarski skup V zovemo* (afina) mnogostrukost *ako je $I(V)$ prost ideal u $\bar{K}[X]$*

Za mnogostrukost V/K definiramo *afini koordinatni prsten od V/K*

$$K[V] = \frac{K[X]}{I(V/K)}. \tag{1.3}$$

$K[V]$ je integralna domena, njeno polje razlomaka označavamo $K(V)$ i nazivamo *polje funkcija od V/K.*

Definicija 1.1.3. Dimenzija od *V, označena sa* $\dim(V)$*, je stupanj transcedentnosti od $\bar{K}[V]$ nad $\bar{K}$.*

Definicija 1.1.4. *Neka je V mnogostrukost, $P \in V$ te $f_1, \ldots, f_m \in \bar{K}[X]$ skup generatora za $I(V)$. Tada je V* nesingularna *ili* glatka u *P ako je $m \times n$ matrica*

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{1\leq i\leq m, 1\leq j\leq n} \tag{1.4}$$

ranga $n = \dim V$. Ako je V glatka u svakoj točki, kažemo da je V nesingularna *ili* glatka.

Ideal u $\bar{K}(V)$ dan sa

$$M_P = \{f \in \bar{K}(V) \colon f(P) = 0\} \tag{1.5}$$

je maksimalni ideal funkcija koje P poništava. Neka je $\bar{K}[V]_P$ lokalizacija u M_P. Generator ideala M_P zovemo *uniformizator u P*, a $f \in \bar{K}(V)$ zovemo *regularnom u P* ako je $f \in \bar{K}[V]_P$.

Propozicija 1.1.5. *Za mnogostrukost V, točka P je glatka ako i samo ako*

$$\dim_{\bar{K}} M_P/M_P^2 = \dim V, \tag{1.6}$$

Dokaz. [1, str. 32, teorem 5.1.] □

Definicija 1.1.6. Projektivni *n*-prostor *(nad K), označen sa $\mathbb{P}^n$ ili $\mathbb{P}^n(\bar{K})$ je skup svih $(n+1)$-orki*

$$(x_0, \ldots, x_n) \in \mathbb{A}^{n+1} \tag{1.7}$$

takvih da je barem jedan x_i nenul, modulo slijedeća relacija ekvivalencije:

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \tag{1.8}$$

ako postoji $\lambda \in \bar{K}^*$ t.d. $x_i = \lambda y_i$ za svaki i. Klasa ekvivalencije

$$\left\{(\lambda x_0, \ldots, \lambda x_n) \colon \lambda \in \bar{K}^*\right\} \tag{1.9}$$

se označava $[x_0, \ldots, x_n]$, a pojedinačne vrijednosti $x_0, \ldots, x_n$ zovemo homogene koordinate.

Definicija 1.1.7. *Polinom $f \in \bar{K}[X] = \bar{K}[X_0, \ldots, X_n]$ je* homogen stupnja *d ako*

$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n) \quad \forall \lambda \in \bar{K}. \tag{1.10}$$

Ideal $I \in \bar{K}[X]$ zovemo homogenim *ako je generiran homogenim polinomima.*

Za homogen polinom f ima smisla pitati je li $f(P) = 0$, jer je odgovor neovisan o izboru homogenih koordinata. Svakom homogenom idealu I pridružujemo podskup od $\mathbb{P}^n$ na sljedeći način

$$V_I = \{P \in \mathbb{P}^n \colon f(P) = 0 \quad \text{za sve homogene } f \in I\}. \tag{1.11}$$

Definicija 1.1.8. Projektivni algebarski skup *je bilo koji skup oblika V_I za homogeni ideal I. Ako je V projektivni algebarski skup,* (homogeni) ideal od *V, označen sa I(V), je ideal u* $\bar{K}[X]$ *generiran sa*

$$\{f \in \bar{K}[X] \colon f \text{ je homogen i } f(P) = 0 \quad \forall P \in V\}. \tag{1.12}$$

Takav V je definiran nad K, *označeno sa V/K, ako mu se ideal I(V) može generirati homogenim polinomima u K[X]*

Definicija 1.1.9. *Projektivni algebarski skup zovemo* (projektivna) mnogostrukost *ako je njegov homogeni ideal I(V) prost ideal u* $\bar{K}[X]$. Polje funkcija od *V,označeno sa K(V) je polje funkcija od* $V \cap \mathbb{A}^n$, lokalni prsten od *V* u *P, označen sa* $\bar{K}[V]_P$ *je lokalni prsten od* $V \cap \mathbb{A}^n$ *u P.*

Definicija 1.1.10. *Za projektivnu mnogostrukost V/K odaberimo* $\mathbb{A}^n \subset \mathbb{P}^n$ *t.d.* $V \cap \mathbb{A}^n \neq \emptyset$. Dimenzija od *V je dimenzija od* $V \cap \mathbb{A}^n$.

Definicija 1.1.11. Krivulja *C je projektivna mnogostrukost dimenzije jedan.*

Propozicija 1.1.12. *Neka je* $P \in C$ *glatka točka. Tada je* $\bar{K}[C]_P$ *prsten diskretne valuacije. Valuacija je dana sa*

$$\mathrm{ord}_P \colon \bar{K}[C]_P \to \mathbb{N} \cup \{\infty\}, \quad \mathrm{ord}_P(f) = \sup\{d \in \mathbb{Z} \mid f \in M_P^d\}. \tag{1.13}$$

Dokaz. Znamo da je $\dim_{\bar{K}} M_P/M_P^2 = 1$ pa rezultat dolazi iz leme 4.1.4. □

1.2 Divizori na krivulji

Promatrajmo polje K s apsolutnom Galoisovom grupom $G(\bar{K}/K)$. Neka je C/K glatka krivulja. Primjetimo da G djeluje na točke u C prirodno po svakoj koordinati.

Definicija 1.2.1. Divizor na *C je konačna formalna suma*

$$D = \sum_{P \in C} n_P(P), n_p \in \mathbb{Z} \tag{1.14}$$

točaka iz $\bar{K}$ *na C.* Stupanj *divizora D je*

$$\deg(D) = \sum_{P \in C} n_P. \tag{1.15}$$

Grupa divizora od *C je slobodna Abelova grupa generirana s* $\bar{K}$*-točkama na C te ju označavamo* $\mathrm{Div}(C)$. *Skup divizora stupnja* 0 *čini podgrupu te se označava* $\mathrm{Div}^0(C)$.

Očito je prirodno djelovanje grupe G na $\mathrm{Div}(C)$ dano sa

$$\sigma\left(\sum_{P\in C} n_P(P)\right) = \sum_{P\in C} n_P(\sigma P). \tag{1.16}$$

Divizori koje G fiksira čine podgrupu koju označavamo $\mathrm{Div}_K(C)$, posebno njena podgrupa su divizori stupnja 0 (fiksirani s G) koju označavamo $\mathrm{Div}_K^0(C)$.

Svaka funkcija $f \in \bar{K}(C)^\times$ ima pridružen divizor

$$\mathrm{div}(f) = \sum_{P\in C} ord_P(f)(P). \tag{1.17}$$

Za dva divizora D_1, D_2 kažemo da su *linearno ekvivalentni* ako je $D_1 - D_2 = \mathrm{div}(f)$ za neki $f \in \bar{K}(C)^\times$ te pišemo $D_1 \sim D_2$. Svaki divizor $D = \mathrm{div}(f)$ za neki $f \in \bar{K}(C)^\times$ zovemo *glavni*. *Picardova grupa*

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\sim \tag{1.18}$$

je grupa klasa ekvivalencije.

Propozicija 1.2.2. *Neka je C glatka krivulja te neka je $f \in \bar{K}(C)^\times$. Tada*

(a) $\mathrm{div}(f) = 0$ *ako i samo ako* $f \in \bar{K}^\times$

(b) $\deg(\mathrm{div}(f)) = 0$.

Dokaz. Za (a), ako je $\mathrm{div}(f) = 0$ onda f nema polove ni nultočke pa mora biti konstantna. Za (b), vidi [1, str. 138, kor 6.10.] □

Teorem 1.2.3. *Sljedeći niz je egzaktan*

$$1 \to \bar{K}^\times \to \bar{K}^\times(C) \to \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0.$$

Dokaz. Jasno je iz definicija i prethodne propozicije. □

Definicija 1.2.4. *Neka je C krivulja. Prostor (meromorfnih) diferencijalnih formi na C, označen s Ω_C, je $\bar{K}$-vektorski prostor generiran simbolima oblika dx, za $x \in \bar{K}(C)$, modulo sljedeće relacije:*

1. $d(x + y) = dx + dy$ *za sve* $x, y \in \bar{K}(C)$
2. $d(xy) = ydx + xdy$ *za sve* $x, y \in \bar{K}(C)$
3. $da = 0$ *za svaki* $a \in \bar{K}$.

Napomena 1.2.5. *Za dano nekonstantno preslikavanje* $\phi\colon C_1 \to C_2$*, imamo pridruženo sljedeće preslikavanje polja funkcija*

$$\phi\colon \bar{K}[C_2] \to \bar{K}[C_1], \quad [f] \mapsto [f \circ \phi] \tag{1.19}$$

koje inducira preslikavanje na diferencijalima

$$\phi^*\colon \Omega_{C_2} \to \Omega_{C_1}, \quad \sum f_i dx_i \mapsto \sum (\phi f_i) d(\phi x_i). \tag{1.20}$$

Propozicija 1.2.6. *Neka je* C *krivulja,* $P \in C$*,* $t \in \bar{K}(C)$ *uniformizator u točki* P*. Tada*

(a) Za svaki diferencijal $\omega \in \Omega_C$ *postoji jedinstvena* $g \in \bar{K}(C)$ *koja zadovoljava* $\omega = g\,dt$*. Označavamo* g *s* ω/dt

(b) Neka je $f \in \bar{K}(C)$ *regularna u* P*. Tada je* df/dt *regularna u* P*.*

(c) Neka je $0 \neq \omega \in \Omega_C$*. Tada* $\operatorname{ord}_P(\omega)$ *ovisi samo o* ω *i* P*:*

$$\operatorname{ord}_P(\omega) := \operatorname{ord}_P(\omega/dt). \tag{1.21}$$

(d) Neka su $x, f \in \bar{K}(C)$ *sa* $x(P) = 0$*,* $p = \operatorname{char} K$*. Tada je*

$$\operatorname{ord}_P(f\,dx) = \operatorname{ord}_P(f) + \operatorname{ord}_P(x) - 1 \quad \text{ako je } p = 0 \text{ ili } p \nmid \operatorname{ord}_P(x) \tag{1.22}$$

$$\operatorname{ord}_P(f\,dx) \geq \operatorname{ord}_P(f) + \operatorname{ord}_P(x) \quad \text{ako je } p > 0 \text{ te } p \mid \operatorname{ord}_P(x) \tag{1.23}$$

(e) Neka je $0 \neq \omega \in \Omega_C$*. Tada je* $\operatorname{ord}_P(\omega) = 0$ *za sve osim konačno mnogo* $P \in C$*.*

Dokaz. [3, str. 31] □

Definicija 1.2.7. *Ako je* $\omega \in \Omega_C$*, tada definiramo* $\operatorname{div}(\omega) = \sum_{P \in C} \operatorname{ord}_P(\omega)$*.*

Propozicija 1.2.8.

(a) Ω_C *je* 1*-dimenzionalan* $\bar{K}(C)$*-vektorski prostor.*

(b) Neka je $x \in \bar{K}(C)$*. Tada je* dx *baza nad* $\bar{K}(C)$ *za* Ω_C *ako i samo ako je* $\bar{K}(C)/\bar{K}(x)$ *konačno separabilno proširenje.*

(c) Neka je $\phi\colon C_1 \to C_2$ *nekonstantno preslikavanje, tada je* ϕ *separabilno ako i samo ako je* $\phi^*\colon \Omega_{C_2} \to \Omega_{C_1}$ *injekcija.*

Napomena 1.2.9. *Za svake nenul* $\omega_1, \omega_2 \in \Omega_C$*, postoji neka* $f \in \bar{K}(C)^*$ *takva da je* $\omega_1 = f\omega_2$*. Zato je* $\operatorname{div}(\omega_1) = \operatorname{div}(f) + \operatorname{div}(\omega_2)$*.*

Definicija 1.2.10. *Za svaki nenul diferencijal* $\omega \in \Omega_C$, $\mathrm{div}(\omega)$ *zovemo* kanonskim divizorom*, a njegovu sliku u* $\mathrm{Pic}(C)$ klasa kanonskog divizora u C.

Definicija 1.2.11. *Pretpostavimo da je*

$$D = \sum_{P \in C} n_P(P), \quad D' = \sum_{P \in C} n'_P(P). \tag{1.24}$$

Tada pišemo $D \geq D'$ *ako je* $n_p \geq n'_p$ *za svaki* $P \in C$. *Danom divizoru* $D \in \mathrm{Div}(C)$ *pridružujemo skup funkcija*

$$\mathcal{L}(D) = \{f \in \bar{K}(C)^* \mid \mathrm{div}(f) \geq -D\} \cup \{0\}, \tag{1.25}$$

koji je očito $\bar{K}$*-vektorski prostor čiju dimenziju označavamo s*

$$l(D) = \dim_{\bar{K}} \mathcal{L}(D). \tag{1.26}$$

Teorem 1.2.12 (Riemann-Roch)**.** *Neka je C glatka krivulja, a* K_C *kanonski divizor na C. Tada postoji cijeli broj* $g \geq 0$*, koji zovemo genus krivulje C, takav da za svaki divizor* $D \in \mathrm{Div}(C)$ *vrijedi*

$$l(D) - l(K_C - D) = \deg D - g + 1. \tag{1.27}$$

Dokaz. Vidi [1, str. 295, teorem 1.3.] □

Poglavlje 2

Uvod u eliptičke krivulje

2.1 Weierstrassove jednadžbe

Fiksirajmo neko polje K s algebarskim zatvaračem $\bar{K}$. *Eliptička krivulja nad* $\bar{K}$ je nesingularna krivulja nad $\bar{K}$ genusa 1 s istaknutom baznom točkom. Koristeći Riemann-Rochov teorem, može se pokazati da se svaka takva krivulja može uložiti u $\mathbb{P}^2$ kao skup rješenja kubne jednadžbe sa samo jednom točkom, baznom točkom, na pravcu u beskonačnosti. Tako je svaka eliptička krivulja skup rješenja pripadajuće *Weierstrassove jednadžbe*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.1}$$

s baznom točkom $O = [0, 1, 0]$ i koeficijentima $a_i \in \bar{K}$. Često pišemo Weierstrassovu jednadžbu u nehomogenim koordinatama $x = X/Z$, $y = Y/Z$

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

imajući u vidu dodatnu točku O u beskonačnosti. Ako je svaki $a_i \in K$ tada kažemo da je E *definirana nad* K i označavamo to sa E/K. Za bilo koje proširenje L/K promatramo

$$E(L) = \{O\} \cup \{(x, y) \in L^2 \mid x, y \text{ zadovoljavaju Weierstrassovu jednadžbu}\}. \tag{2.3}$$

Pretpostavimo da je E/K eliptička krivulja uz $\operatorname{char} K \neq 2$, tada kroz promjenu koordinata možemo pojednostaviti Weierstrassovu jednadžbu u oblik

$$E\colon y^2 = f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{2.4}$$

gdje su

$$b_2 = a_1^2 + 4a_4, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6, \quad b_8 = b_2b_6 - b_4^2. \tag{2.5}$$

Ovdje definiramo dvije osnovne konstante koje vežemo uz takve eliptičke krivulje i Weierstrassovu jednadžbu.

Definicija 2.1.1. Diskriminanta Δ *Weierstrassove jednadžbe te* j-invarijanta eliptičke krivulje *dane su sa*

$$\Delta = \Delta(E) = 16\,\mathrm{Disc}(f) = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6, \tag{2.6}$$

$$j = j(E) = \frac{(b_2^2 - 24b_4)^3}{\Delta}. \tag{2.7}$$

Ako dodatno pretpostavimo da $\mathrm{char}\, K \neq 2, 3$, onda Weierstrassovu jednadžbu možemo pojednostaviti u oblik

$$E\colon y^2 = f(x) = x^3 + Ax + B. \tag{2.8}$$

Uz Weierstrassovu jednadžbu ovog oblika, lako se provjeri da vrijedi

$$\Delta = -16(4A^3 + 27B^2) \quad \text{te} \quad j = -1728\frac{(4A)^3}{\Delta}. \tag{2.9}$$

Propozicija 2.1.2. *Neka su E i E' dvije eliptičke krivulje definirane nad $\bar{K}$.*

(a) Neka je $E/\bar{K}$ dana Weierstrassovom jednadžbom (2.2)*. Tada je E* nesingularna *ako i samo ako je $\Delta = 0$.*

(b) Dvije eliptičke krivulje E, E' su izomorfne ako i samo ako je $j(E) = j(E')$.

(c) Za bilo koji $j_0 \in \bar{K}$ postoji eliptička krivulja $E''/K(j_0)$ sa $j(E'') = j_0$.

Dokaz. [3, str. 45, prop. 1.4.] □

Opišimo zbrajanje točaka na eliptičkim krivuljama. Neka je E/K eliptička krivulja, L/K bilo koje proširenje te $P, Q \in E(L)$. Neka je l jedinstveni pravac kroz P, Q. Zbog Bezoutovog teorema l siječe E u jedinstvenoj trećoj točki (brojeći kratnost) $R \in \mathbb{P}^2(L)$. Neka je v_R jedinstveni pravac kroz R, O i konačno definiramo $P+Q$ kao treću točku presjeka $E(L)$ i v_R.

Ova konstrukcija zapravo daje komutativnu strukturu grupi $E(L)$. Jasno je da je $O + P = P + O = P$ za bilo koju $P \in E(L)$ pa je O neutralni element. Nadalje, za bilo koji $P \in E(L)$ je $v_P \cap E(L) = \{O, P, -P\}$ pa je $-P$ inverz točke P. Jedini netrivijalni aksiom je asocijativnost, koja se može provjeriti direktnim, ali kompliciranim računom. Umjesto toga dajemo alternativni dokaz u sljedećem poglavlju.
Pogledajmo još eksplicitne jednadžbe za zbrajanje točaka na eliptičnim krivuljama.

Teorem 2.1.3. *Neka je E dana Weierstrassovom jednadžbom*

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.10}$$

(a) Ako je $P_0 = (x_0, y_0)$ onda je $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$.

(b) Neka je sada $P_i = (x_i, y_i) \in E$ *te* $P_1 + P_2 = P_3$
Ako je $x_1 = x_2$ *te* $y_1 + y_2 + a_1x_2 + a_3 = 0$ *onda je* $P_1 + P_2 = O$.
Inače, definiramo λ *i* ν *sljedećim formulama:*

	λ	ν
$x_1 \neq x_2$	$\dfrac{y_2 - y_1}{x_2 - x_1}$	$\dfrac{y_1x_2 - x_1y_2}{x_2 - x_1}$
$x_1 = x_2$	$\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$	$\dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$

Tada je ili $y = \lambda x + \nu$ *pravac kroz* P_1, P_2 *ili tangenta na* E *ako su točke* P_1 *i* P_2 *jednake.*

(c) Koristeći notaciju iz (b), $P_3 = P_1 + P_2$ *ima koordinate*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \tag{2.11}$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3 \tag{2.12}$$

(d) Kao poseban slučaj od (c) navodimo formulu duplikacije, za $P = (x, y) \in E$

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4 + b_6} \tag{2.13}$$

gdje su b_2, b_4, b_6, b_8 *polinomi u* a_i*-ovima dani ranije u* (2.5).

Dokaz. [3, str. 53/54] □

Sada dajemo bez dokaza uvid u formule množenja s $[m]$ na eliptičkoj krivulji E. Za eliptičku krivulju E danu Weierstrassovom jednadžbom

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.14}$$

te b_2, b_4, b_6, b_8 definiranima kao i ranije, definiramo *divizijske polinome* $\psi_m \in \mathbb{Z}[a_1, \ldots, a_6, x, y]$

$$\begin{aligned}
\psi_1 &= 1,\\
\psi_2 &= 2y + a_1x + a_3,\\
\psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\\
\psi_4 &= \psi_2 \cdot (2x^6 + b_2x^5 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)),
\end{aligned}$$

te dalje rekurzivno formulama

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \qquad \text{za } m \geq 2,$$
$$\psi_2\psi_{2m} = \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^2 \qquad \text{za } m \geq 3.$$

Lako se provjeri da je ψ_{2m} polinom za svaki $m \geq 1$ pa dalje definiramo polinome ϕ_m te ω_m sa

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \tag{2.15}$$

$$4y\omega_m = \psi_{m-1}^2\psi_{m+2} + \psi_{m-2}\psi_{m+1}^2. \tag{2.16}$$

Može se pokazati da su za neparne m funkcije ψ_m, ϕ_m te $y^{-1}\omega_m$ polinomi u $\mathbb{Z}[a_1, \ldots, a_6, x, (2y+a_1x+a_3)^2]$, te slično za $(2y)^{-1}\psi_m, \phi_m, \omega_m$ ako je m paran. Ako sad zamijenimo $(2y+a_1x+a_3)^2$ s $4x^3 + b_2x^2 + 2b_4x + b_6$ vidimo da je svaka od prethodno navedenih funkcija polinom u $\mathbb{Z}[a_1, \ldots, a_6, x]$.

Formula množenja s $[m]$ točke $P = (x_0, y_0) \in E$ dana je sa

$$[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right). \tag{2.17}$$

Korolar 2.1.4. *Svaka $[m]$-praslika algebarske točke je opet algebarska točka.*

2.2 Redukcija eliptičkih krivulja

Neka je K lokalno polje, potpuno u odnosu na diskretnu valuaciju v, skupa s prstenom cijelih $R = \{x \in K | v(x) \geq 0\}$, čiji je maksimalni ideal $\mathfrak{m}$, uniformizator π te polje ostataka $k = R/\mathfrak{m}$ karakteristike p. Redukciju modulo $\mathfrak{m}$ označavamo tildom.

Primjer 2.2.1. *Postoji prirodno redukcijsko preslikavanje*

$$R \twoheadrightarrow R/\mathfrak{m}$$

dano sa $t \mapsto \tilde{t}$. Ovo preslikavanje lako proširimo do preslikavanja prstena polinoma

$$R[X] \twoheadrightarrow R/\mathfrak{m}[X]$$

dano sa $\sum a_iX^i \mapsto \sum \tilde{a}_iX^i$.

Primjer 2.2.2. *Još jedan primjer je redukcija projektivne ravnine*

$$\mathbb{P}^2(K) \twoheadrightarrow \mathbb{P}^2(k) \tag{2.18}$$

na sljedeći način. Uzmimo neki $[a, b, c] \in \mathbb{P}^2(K)$. Množeći dobro izabranim elementom iz R možemo pretpostaviti da su $a, b, c \in R$, a nakon toga dijeleći prikladnom potencijom uniformizatora π možemo pretpostaviti

$$\min\{v(a), v(b), v(c)\} = 0. \tag{2.19}$$

Sada koristimo prirodnu redukciju na R kao u primjeru 2.2.1, $[\widetilde{a, b, c}] = [\tilde{a}, \tilde{b}, \tilde{c}]$ je dobro definirano jer je situacija $\tilde{a} = \tilde{b} = \tilde{c} = 0$ nemoguća zbog jednadžbe (2.19).

Neka je E/K eliptička krivulja nad K, tj. neka je E skup rješenja Weierstrassove jednadžbe $f(X, Y, Z) = 0$ s diskriminantom Δ. Redukcijom kao u primjeru 2.2.1 $\tilde{f}(X, Y, Z) = \tilde{0}$ definira novu krivulju $\tilde{E}/k$ nad poljem k s diskriminantom $\tilde{\Delta}$. Sada je $\tilde{E}$ eliptička krivulja ako $\tilde{\Delta} \neq \tilde{0}$ (ako $\Delta \notin \mathfrak{m}$). U tom slučaju postoji prirodno redukcijsko preslikavanje eliptičkih krivulja $\rho\colon E/K \to \tilde{E}/k$ dano redukcijom projektivnih prostora iz primjera 2.2.2.

Definicija 2.2.3. $[m]$-torzija *eliptičke krivulje je*

$$E[m] = \{P \in E\colon [m]P = O\}. \tag{2.20}$$

Teorem 2.2.4. *Neka je m prirodan broj relativno prost s $p = \operatorname{char} K$. Restrikcija redukcije na $E[m]$ je injektivna.*

Dokaz. [3, str. 192, prop. 3.1.b)] □

2.3 Primjena divizora na eliptičke krivulje

Lema 2.3.1. *Neka je C krivulja genusa 1 te neka su $P, Q \in C$. Tada je $(P) \sim (Q)$ ako i samo ako $(P) = (Q)$.*

Dokaz. Pretpostavimo $(P) \sim (Q)$. Tada postoji $f \in \bar{K}(C)$ t.d. $\operatorname{div}(f) = (P) - (Q)$. Vidimo da je $f \in \mathcal{L}(Q)$ po definiciji, a po Riemann-Rochu $\mathcal{L}(Q)$ ima dimenziju 1. $\mathcal{L}(Q)$ očito sadržava konstantne funkcije pa je $f \in \bar{K}$ te je $P = Q$. Drugi smjer je očit. □

Propozicija 2.3.2. *Neka je E/K eliptička krivulja.*

(a) Za svaki divizor $D \in \operatorname{Div}^0(E)$ (stupnja 0) postoji jedinstvena točka $P \in E$ koja zadovoljava $D \sim (P) - (O)$.Definirajmo preslikavanje

$$\psi\colon \operatorname{Div}^0(E) \to E$$

koje šalje D u njemu asociranu točku P.

(b) ψ je surjektivna.

(c) Neka su $D_1, D_2 \in \operatorname{Div}^0(E)$. Tada je $\psi(D_1) = \psi(D_2)$ ako i samo ako je $D_1 \sim D_2$, posebno

$$\psi\colon \operatorname{Pic}^0(E) \to E \tag{2.21}$$

je bijekcija.

(d) Inverz funkcije ψ je

$$\kappa\colon E \to \operatorname{Pic}^0(E), \quad P \mapsto (P) - (O). \tag{2.22}$$

(e) Grupovni zakon induciran na E preko ψ je zbrajanje opisano ranije. Posebno, zbrajanje na eliptičkim krivuljama je asocijativno.

Dokaz.

(a) E ima genus 1 pa je $l(D + (O)) = 1$ po Riemann-Rochu. Neka je f bilo koji nenul element od $\mathcal{L}(D + (O))$, posebno f je baza za taj $\bar{K}$-vektorski prostor. Budući je

$$\operatorname{div}(f) \geq -D - (O) \quad \text{te} \quad \deg(\operatorname{div}(f)) = 0,$$

imamo da je $\operatorname{div}(f) = -D + (O) + (P)$ za neki $P \in E$. Posebno, vrijedi $D \sim (P) - (O)$ što nam daje točku s traženim svojstvom. Ako točka P' ima isto svojstvo, onda je $(P) \sim D + (O) \sim (P')$, ali sada po lemi 2.3.1 imamo $P = P'$. Zato je P jedinstvena.

(b) Neka je $P \in E$. Tada je $\psi((P) - (O)) = P$.

(c) Neka su $D_1, D_2 \in \operatorname{Div}^0(E)$ te neka su $P_1 = \psi(D_1), P_2 = \psi(D_2)$. Imamo $(P_1) - (P_2) \sim D_1 - D_2$ pa je jedan smjer očit, a drugi opet slijedi iz leme 2.3.1.

(d) Očito.

(e) Dovoljno je pokazati $\kappa(P+Q) = \kappa(P)+\kappa(Q)$. (Napomena: Zbrajanje na lijevoj strani je geometrijsko zbrajanje točaka na eliptičkoj krivulji, dok je zbrajanje na desnoj zbrajanje klasa divizora u $\operatorname{Pic}^0(E)$).
Neka je $f(X, Y, Z) = \alpha X + \beta Y + \gamma Z = 0$ pravac L u $\mathbb{P}^2$ koji prolazi kroz P, Q te neka je R treća točka presjeka L sa E. Neka je $f'(X, Y, Z) = \alpha' X + \beta' Y + \gamma' Z = 0$ pravac L' koji prolazi kroz R, O. Iz geometrijske definicije zbrajanja znamo da L' prolazi kroz $P + Q$, a znamo da pravac $Z = 0$ tri puta "prolazi" kroz točku O. Sada imamo

$$\operatorname{div}(f/Z) = (P) + (Q) + (R) - 3(O), \tag{2.23}$$
$$\operatorname{div}(f'/Z) = (R) + (O) + (P + Q) - 3(O). \tag{2.24}$$

Zato je redom

$$(P + Q) - (P) - (Q) + (O) = \operatorname{div}(f'/Z) - \operatorname{div}(f/Z) = \operatorname{div}(f'/f) \sim 0 \tag{2.25}$$
$$((P + Q) - (O)) - ((P) - (O)) - ((Q) - (O)) = \operatorname{div}(f'/f) \sim 0 \tag{2.26}$$
$$\kappa(P + Q) - \kappa(P) - \kappa(Q) = 0 \tag{2.27}$$

što dokazuje da je κ homomorfizam grupa.

□

Teorem 2.3.3. *Divizor* $D = \sum_P n_P(P) \in \mathrm{Div}(E)$ *je glavni ako i samo ako*

$$\sum_P n_P = 0 \quad te \quad \sum_P n_P P = O \tag{2.28}$$

Dokaz. Po propoziciji 2.3.3 znamo da svaki glavni divizor ima stupanj 0. Neka je $D \in \mathrm{Div}^0(E)$. Sada je

$$D \sim 0 \iff \psi(D) = O \iff \psi(D - \sum_{P\in E} n_P(O)) \iff \sum_{P\in E} [n_P]\psi((P) - (O)) = O \tag{2.29}$$

što daje traženu tvrdnju jer je $\psi((P) - (O)) = P$ □

Poglavlje 3

Eliptičke krivulje nad $\mathbb{C}$

3.1 Weierstrassova $\wp$-funkcija

Definicija 3.1.1. Rešetka $\Lambda = \langle \omega_1, \omega_2 \rangle \subset \mathbb{C}$ *je slobodna podgrupa od* $\mathbb{C}$ *ranga* 2*, gdje zahtjevamo da* ω_1 *i* ω_2 *nisu linearno zavisni nad* $\mathbb{R}$*.* Fundamentalni paralelogram za Λ *je skup oblika*

$$\Pi = \{\alpha + a\omega_1 + b\omega_2 \mid 0 \leq a, b < 1\} \tag{3.1}$$

za neki $\alpha \in \mathbb{C}$ *te* $\{\omega_1, \omega_2\}$ *generatore za* Λ *. Meromorfnu funkciju* $f \colon \mathbb{C} \to \mathbb{C}$ *zovemo* eliptička funkcija u odnosu na Λ *ako je* $f(z) = f(z+\lambda)$ *za sve* $z \in \mathbb{C}, \lambda \in \Lambda$*. Označimo skup svih takvih funkcija s* $\mathbb{C}_\Lambda$*.*

Propozicija 3.1.2. *Ako je* $f \in \mathbb{C}_\Lambda$ *holomorfna funkcija ili funkcija koja nema nultočke, onda je konstanta.*

Dokaz. Ako je f holomorfna funkcija, onda je zbog periodičnosti

$$\sup_{z \in \mathbb{C}} |f(z)| = \sup_{z \in \bar{\Pi}} |f(z)|. \tag{3.2}$$

$\bar{\Pi}$ je kompakt, f je neprekidna pa je i ograničena na $\bar{\Pi}$ te zbog periodičnosti i na $\mathbb{C}$. Sada po Liouviellovom teoremu znamo da je konstantna. Ako f nema nulu onda je $1/f$ holomorfna. □

Propozicija 3.1.3. *Pretpostavimo da* f *nema polova niti nultočki na* $\partial\Pi$[1]*. Tada je*

$$\sum_{\omega \in \Pi} \mathrm{res}_\omega(f) = 0. \tag{3.3}$$

[1] Ovo možemo pretpostaviti pametnim izborom α u definiciji fundamentalnog paralelograma. Smatramo da je ovo svojstvo zadovoljeno za sve f koje dalje promatramo.

Dokaz. Po teoremu o reziduumu

$$\sum_{\omega\in\Pi} \mathrm{res}_\omega(f) = \frac{1}{2\pi i}\int_{\partial\Pi} f dz. \tag{3.4}$$

f poprima iste vrijednosti na suprotnim stranama ruba paralelograma pa se ti dijelovi ponište u integralu te je integral jednak 0. □

Korolar 3.1.4. *Svaka nekonstantna eliptička funkcija ima barem dva pola (brojeći kratnosti) u* Π.

Dokaz. Ako postoji točno jedan pol kratnosti 1 u točki $\omega_0 \in \Pi$, onda je $\mathrm{res}_{\omega_0}(f) = \sum_{\omega\in\Pi} \mathrm{res}_\omega(f) = 0$ po prethodnoj propoziciji pa f nema polova. Sada znamo da je f konstantna. □

Dokazi nekoliko narednih propozicija mogu se pronaći u [3, str. 165-171]

Definicija 3.1.5. Weierstrassovu $\wp$-funkciju *definiramo kao*

$$\wp(z,\Lambda) = \frac{1}{z^2} + \sum_{0\neq\lambda\in\Lambda}\left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right). \tag{3.5}$$

Propozicija 3.1.6. *Weierstrassova $\wp$-funkcija konvergira apsolutno te uniformno na bilo kojem kompaktu $K \subset \mathbb{C}\setminus\Lambda$.*

Propozicija 3.1.7. *$\wp(z,\Lambda) \in \mathbb{C}(\Lambda)$, a njeni polovi su točno dvostruki polovi u svakom $\lambda \in \Lambda$.*

Propozicija 3.1.8. *$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp')$, tj. $\mathbb{C}(\Lambda)$ je kao polje nad $\mathbb{C}$ generirano s $\wp$ i njenom derivacijom.*

Teorem 3.1.9. *Promotrimo eliptičku krivulju $E\colon y^2 = 4x^3 - g_2x - g_3$ gdje su $g_2 = 60\sum_{0\neq\lambda\in\Lambda}\lambda^{-4}$ te $g_3 = 140\sum_{0\neq\lambda\in\Lambda}\lambda^{-6}$. Tada je*

$$\begin{aligned}\mathbb{C}/\Lambda &\to E(\mathbb{C})\\ z &\mapsto (\wp(z,\Lambda), \wp'(z,\Lambda))\end{aligned}$$

kompleksno analitički izomorfizam. Nadalje, za svaku eliptičku krivulju $E/\mathbb{C}$ postoji Λ takva da je $E(\mathbb{C}) = \mathbb{C}/\Lambda$.

Dva korolara ovog vrlo važnog teorema su

Korolar 3.1.10. *Neka je $E/\mathbb{C}$ eliptička krivulja. Tada je grupa m-torzije $E[m] \cong (\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z})$.*

Dokaz. Postoji rešetka Λ takva da je $E(\mathbb{C}) = \mathbb{C}/\Lambda$. Sada je

$$E[m] \cong (\mathbb{C}/\Lambda)[m] \cong \frac{\frac{1}{m}\Lambda}{\Lambda} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}). \tag{3.6}$$

□

Korolar 3.1.11. *Množenje s* $[m]$ *na* $E(\mathbb{C})$ *je surjektivno.*

Poglavlje 4

Uvod u algebarsku teoriju brojeva

4.1 Definicije i teoremi

Definicija 4.1.1. *Prsten R zovemo* prsten diskretne valuacije *ako je R domena glavnih ideala s jedinstvenim nenul prostim idealom* $\mathfrak{m}$. Rezidualno polje od R *je* $k = R/\mathfrak{m}$.

Definicija 4.1.2. *Integralnu domenu A zovemo* Dedekindova domena *ako A zadovoljava bilo koji od ova dva ekvivalentna uvjeta*

1. *A je Noetherin, cijelo zatvoren i ima Krullovu dimenziju 1.*

2. *A je Noetherin i lokalizacija $A_{\mathfrak{p}}$ je prsten diskretne valuacije za sve proste* $\mathfrak{p}$.

Neka je K polje razlomaka od A. *Razlomljeni ideal od K* je konačno generirani A-podmodul od K.

Definicija 4.1.3. Polje algebarskih brojeva K *je konačno proširenje od* $\mathbb{Q}$.
Prsten cijelih od K *je*

$$O_K = \{x \in K \mid f(x) = 0 \text{ za neki normirani } f \in \mathbb{Z}[X]\}. \tag{4.1}$$

Iskazujemo neke rezultate bez dokaza, za više informacija pogledajte [2]

Lema 4.1.4. *Neka je R Noetherina lokalna domena koja nije polje, neka je* $\mathfrak{m}$ *njen maksimalni ideal te neka je $k = R/\mathfrak{m}$ njeno rezidualno polje. Sljedeće tvrdnje su ekvivalentne:*

(i) *R je prsten diskretne valuacije.*

(ii) $\mathfrak{m}$ *je glavni ideal.*

(iii) $dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$.

Teorem 4.1.5. *Neka je A Dedekindova domena s poljem razlomaka K. Skup nenul razlomljenih ideala Id(A) tvori grupu u odnosu na množenje. Dedekindove domene imaju jedinstvenu faktorizaciju ideala na proste ideale pa je zbog toga Id(A) slobodna grupa čiji su generatori prosti ideali.*

Propozicija 4.1.6. *Ako je K polje algebarskih brojeva, onda je $\mathcal{O}_K$ Dedekindova domena.*

Definicija 4.1.7. *Neka je L/K proširenje stupnja n polja algebarskih brojeva i neka je $\mathfrak{p}$ prost u $\mathcal{O}_K$. Po teoremu 4.1.5 imamo*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g} \tag{4.2}$$

za jedinstvene proste $\mathfrak{q}_i \subset \mathcal{O}_L$. Kažemo da $\mathfrak{q}_i$ dijeli $\mathfrak{p}$ *ili* leži iznad $\mathfrak{p}$ *i to označavamo $\mathfrak{q}_i \mid \mathfrak{p}$. Kažemo da je L/K* neramificirano u $\mathfrak{q}_i$ *ako je $e_i = 1$, a* neramificirano nad $\mathfrak{p}$ *ako je $e_i = 1$ za svaki i, inače kažemo da je L/K* ramificiran nad $\mathfrak{p}$. *Ako je $g = 1$ i $e_1 = n$ kažemo da je L/K* potpuno ramificirano nad $\mathfrak{p}$.

Po definiciji 4.1.2, za dani prost $\mathfrak{p}$ u Dedekindovoj domeni A s poljem razlomaka K, $A_\mathfrak{p}$ je prsten diskretne valuacije pa slijedeća definicija ima smisla.

Definicija 4.1.8. Rezidualno polje od K u odnosu na $\mathfrak{p}$ *je rezidualno polje od $A_\mathfrak{p}$.* Upotpunjenje od K u odnosu na $\mathfrak{p}$ *je polje razlomaka upotpunjenja od $A_\mathfrak{p}$ u odnosu na (jedinstveni) maksimalni ideal $\mathfrak{p}$ i označavamo ga $K_\mathfrak{p}$.*

Propozicija 4.1.9. *Neka je L/K konačno Galoisovo proširenje i neka je $\mathfrak{p} \subset \mathcal{O}_K$ prost ideal. Tada $G(L/K)$ djeluje tranzitivno na S, skup prostih ideala $\mathfrak{q} \subset \mathcal{O}_L$ nad $\mathfrak{p}$.*

Definicija 4.1.10. *Koristeći oznake iz prethodne propozicije, za $\mathfrak{q} \in S$* dekompozicijska grupa od $\mathfrak{q}$ *je*

$$D_\mathfrak{q}(L/K) = \mathrm{Stab}(\mathfrak{q}) \leq G(L/K). \tag{4.3}$$

Propozicija 4.1.11. *$D_\mathfrak{q}(L/K)$ je Galoisova grupa pripadajućeg proširenja upotpunjenja, tj.*

$$G(L_\mathfrak{q}/K_\mathfrak{p}) = D_\mathfrak{q}(L/K). \tag{4.4}$$

Propozicija 4.1.12. *Koristeći oznake prethodnih propozicija, neka je k (odn. l) rezidualno polje od K (odn. L) u odnosu na $\mathfrak{p}$ (odn. $\mathfrak{q}$). Prelaskom na kvocijent, preslikavanje*

$$\varepsilon\colon D_\mathfrak{q}(L/K) \to G(l/k) \tag{4.5}$$

je surjekcija.

Definicija 4.1.13. Inercijska podgrupa od $\mathfrak{q}$ *je*

$$I_{\mathfrak{q}}(L/K) = \mathrm{Ker}(\varepsilon) \tag{4.6}$$

gdje je ε definirano u prethodnoj propoziciji.

Lema 4.1.14. *Neka je K polje algebarskih brojeva. Ako za $\mathfrak{p} \in O_K$ vrijedi da se $\mathfrak{p} \mid p$ grana u $K/\mathbb{Q}$ tada $p \mid \mathrm{Disc}(K)$.*

Dokaz. Neka je $pO_K = \mathfrak{p} \cdot \mathfrak{p} \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_{n-2}$. Definiramo $I := \mathfrak{p} \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_{n-2} \neq (0)$. Iz definicije ideala I vidimo da ako je $\mathfrak{q}$ neki prost ideal u O_K nad p, tada $\mathfrak{q} \mid I$. Posebno, I je sadržan u svim takvim idealima. Za $n := [K : \mathbb{Q}]$ neka su $\sigma_1', \ldots, \sigma_n' : K \to \mathbb{C}$ ulaganja. Neka je L normalno proširenje od $\mathbb{Q}$ konačnog stupnja koje sadrži K te $\sigma_1, \ldots, \sigma_n : L \to \mathbb{C}$ neka proširenja od $\sigma_1', \ldots, \sigma_n'$. Odaberimo neku cijelu bazu $\alpha_1, \ldots, \alpha_n$ od O_K te $\alpha \in I \backslash pO_K$. Vrijedi $\alpha = \sum_{i=1}^{n} b_i \alpha_i$. Budući da $p \nmid \alpha$ BSO možemo pretpostaviti da $p \nmid b_1$. Iz jednakosti

$$\det\left[\begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \ldots & \sigma_n(\alpha_n) \end{pmatrix} \cdot \begin{pmatrix} b_1 & 0 & \ldots & 0 \\ b_2 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ b_n & 0 & \ldots & 1 \end{pmatrix}\right]^2 = \det \begin{pmatrix} \sigma_1(\alpha) & \ldots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}^2$$

imamo $\Delta_K \cdot b_1^2 = D$ gdje je D desna strana jednakosti. Sada je dovoljno pokazati $p \mid D$. Uzmimo neki prost ideal $\mathfrak{s} \subset O_L$ iznad p. Sada je $\sigma_i^{-1}(\mathfrak{s})$ prost u O_L iznad p za svaki $i \in \{1, \ldots, n\}$. Znamo da α leži u svakom prostom idealu u O_L koji se nalazi iznad p pa je zato $\alpha \in \sigma_i^{-1}(\mathfrak{s})$ tj $\sigma_i(\alpha) \in \mathfrak{s}\ \forall i$. Ako razvijemo determinantu desne matrice po prvom stupcu imamo $D \in \mathfrak{s}$. Znamo da je $D \in \mathbb{Z}$ pa jer je $\mathfrak{s} \cap \mathbb{Z} = p\mathbb{Z}$ imamo $p \mid D$ što daje $p \mid \Delta_K$ □

Teorem 4.1.15. *Postoji* konačan *skup (razlomljenih) ideala u $O_K, I_1, \ldots, I_n$, takvih da za bilo koji (razlomljeni) ideal $I \in O_K$ postoji $k \in \{1, 2, \ldots, n\}$ takav da je II_k glavni ideal.*

Teorem 4.1.16 (Dirichletov teorem o jedinicama)**.** *Grupa jedinica od K^* je konačno generirana.*

Dokaz. Za dokaze ova dva teorema pogledaj [2]

□

Teorem 4.1.17. *Neka je K polje algebarskih brojeva koje sadržava m-te korijene iz jedinice. Promatramo C_m, skup cikličkih proširenja od K stupnja koji dijeli m. Za konačan skup S prostih ideala u O_K definiramo $C_{m,S} \subset C_m$, takav da je svako polje $L \in C_{m,S}$ neramificirano nad svakim $\mathfrak{p} \notin S$. Tvrdimo da je $C_{m,S}$ konačan skup.*

Dokaz. Po teoremu 5.3.4 znamo da postoji surjekcija

$$\Phi\colon K^\times/K^{\times m} \to C_m, \text{ dana sa } aK^{\times m} \mapsto K(\sqrt[m]{a})$$

Zato za svako polje $L \in C_{m,S} \subset C_m$ postoji $a \in K$ takav da je $L = K(\sqrt[m]{a})$. Neka je $(a) = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ jedinstvena faktorizacija u O_K. Ako $\mathfrak{p} \notin S$, onda $m | e_{\mathfrak{p}}$, posebno neka je $e_{\mathfrak{p}} = ma_{\mathfrak{p}}$. Za svaki $\mathfrak{p} \in S$ neka je $e_{\mathfrak{p}} = \alpha_{\mathfrak{p}} + mb_{\mathfrak{p}}$, gdje je $\alpha_{\mathfrak{p}}$ ostatak od $e_{\mathfrak{p}}$ pri dijeljenju s m. Imamo

$$(a) = (\prod_{\mathfrak{p}\in S} \mathfrak{p}^{\alpha_{\mathfrak{p}}})\Big((\prod_{\mathfrak{p}\in S} \mathfrak{p}^{b_{\mathfrak{p}}})(\prod_{\mathfrak{p}\notin S} \mathfrak{p}^{a_{\mathfrak{p}}})\Big)^m. \tag{4.7}$$

Definiramo $I := (\prod_{\mathfrak{p}\in S} \mathfrak{p}^{b_{\mathfrak{p}}})(\prod_{\mathfrak{p}\notin S} \mathfrak{p}^{a_{\mathfrak{p}}})$. Ideal I, kao razlomljeni ideal, ima pridružen ideal I_k t.d. $I^{-1}I_k = (b)$ za neki $k \in \{1, \ldots, n\}, b \in K^*$. Sada je

$$(ab^m) = (\prod_{\mathfrak{p}\in S} \mathfrak{p}^{\alpha_{\mathfrak{p}}})I^m(I^{-m}I_k^m) = (\prod_{\mathfrak{p}\in S} \mathfrak{p}^{\alpha_{\mathfrak{p}}})I_k^m. \tag{4.8}$$

Trenutni zaključak je da za svako polje $L \in C_{m,S}$ postoji element polja $ab^m \in K$ t.d. $L = K(\sqrt[m]{a}) = K(\sqrt[m]{ab^m})$ te $(ab^m) = (\prod_{\mathfrak{p}\in S} \mathfrak{p}^{\alpha_{\mathfrak{p}}})I_k^m$.

Ako pogledamo desnu stranu jednakosti ideala, vidimo da takvih ideala ima samo konačno mnogo (m je fiksan broj, postoji konačno ideala I_k, S je konačan skup, a svaki $\alpha_{\mathfrak{p}} \leq m$). Za svaki takav fiksan ideal J (oblika $(\prod_{\mathfrak{p}\in S} \mathfrak{p}^{\alpha_{\mathfrak{p}}})I_k^m$) promatramo sve $a \in K^*/K^{*m}$ t.d. je $(a) = J$ i za sve takve a promatramo broj različitih proširenja polja oblika $K(\sqrt[m]{a})$. Želimo pokazati da njih(različitih proširenja) ima konačno mnogo!

Krenimo, dakle, od dva elementa polja a_1, a_2 za koje vrijedi $(a_1) = (a_2)$. Sada je $(a_1a_2^{-1}) = O_K$ tj. $a_1a_2^{-1}$ je jedinica. Po teoremu 4.1.16 grupa jedinica u O_K je konačno generirana, neka su ti generatori $s_1, \ldots, s_r$. Sada je $a_1a_2^{-1} = \prod_{i=1}^{r} s_i^{d_i}$. Dovoljno je gledati modulo s_i^m za svaki i jer polja koja generiramo s a su oblika $K(\sqrt[m]{a})$. Vidimo da postoji konačno[1] mnogo klasa elemenata a koji generiraju isti ideal J, a generiraju različito polje $K(\sqrt[m]{a})$. Proširenja L traženog tipa ima konačno mnogo te je teorem dokazan.

□

[1] te klase su točno $a\prod_{i=1}^{r} s_i^{d_i}$ gdje su $d_i \in \{0, 1, \ldots, m-1\}$.

Poglavlje 5

Kohomologija

5.1 Definicije kohomoloških grupa

Neka je G grupa.

Definicija 5.1.1. *(Lijevi)* G-modul *je Abelova grupa M zajedno s djelovanjem grupe G dano homomorfizmom*

$$G \to AutM, g \mapsto (m \mapsto m^g) \tag{5.1}$$

*(posebno $m^1 = m$ te $(m^g)^h = m^{hg}$). G-*invarijante *su*

$$M^G := \{m \in M : m^g = m, \forall g \in G\}. \tag{5.2}$$

Funktor iz G-modula u G-module, koji šalje M u M^G je lijevo egzaktan, ali ne i desno. Neka je

$$0 \to A \to B \xrightarrow{\psi} C \to 0 \tag{5.3}$$

egzaktan niz G-modula. Iz njega možemo dobiti egzaktan niz

$$0 \to A^G \to B^G \xrightarrow{\psi} C^G. \tag{5.4}$$

Za dani $c \in C^G$. Budući da $B \twoheadrightarrow C$, postoji $b \in B$ t.d. je $\psi(b) = c$. Preslikavanje

$$\xi : G \to B, g \mapsto b^g - b \tag{5.5}$$

ima sliku u $A \subset B$[1]. Ovo preslikavanje je nul-preslikavanje ako i samo ako $b \in B^G$, a samo preslikavanje ξ zadovoljava

$$\xi(gh) = b^{gh} - b^g + b^g - b = \xi(h)^g + \xi(g).$$

[1] $\psi(b^g - b) = \psi(b)^g - \psi(b) = c^g - c = 0$ jer je $c \in C^G$ po pretpostavci, pa je $\xi(g) \in \ker\psi = A$

Svako takvo preslikavanje zovemo 1-*kociklus* $G \to A$. Birajući neku drugu prasliku $b' \in \psi^{-1}(c)$, tj. $b' = b + a$ za neki $a \in A$, mijenjamo ξ u $\xi' = \xi +$ (preslikavanje$g \mapsto a^g - a$). Preslikavanja oblika $g \mapsto a^g - a$ zovemo 1-*korub* $G \to A$.

Definicija 5.1.2. *Neka je M G-modul.* Nulta kohomologija *od M je*

$$H^0(G, M) := M^G. \tag{5.6}$$

Prva kohomologija *od M je*

$$H^1(G, M) := \frac{\textit{1-kociklusi}}{\textit{1-korubovi}} = \frac{\{\textit{preslikavanja } \xi\colon G \to M \mid \xi(gh) = \xi(g) + \xi(h)^g\}}{\{\textit{preslikavanja oblika } m \mapsto m^g - m \textit{ za neki } m \in M\}}. \tag{5.7}$$

Kohomološke grupe su komutativne. Morfizam G-modula $\phi\colon M \to N$ inducira homomorfizam $H^1(G, M) \to H^1(G, N)$ (komponiranjem preslikavanja).

Napomena 5.1.3. *Ako G djeluje trivijalno na M ($m^g = m, \forall g, m$), tada*

$$H^1(G, M) = \frac{\{\xi\colon\ \xi(gh) = \xi(g) + \xi(h)\}}{\{0\}} = \mathrm{Hom}(G, M). \tag{5.8}$$

Konstruirali smo preslikavanje $C^G \xrightarrow{\delta} H^1(G, A)$. Trivijalno je vidjeti da se $\psi(B^G)$ nalazi u $\ker\delta$. Pretpostavimo da se $c \in C^G$ nalazi u $\ker\delta$. Tada po definiciji preslikavanja δ, za b t.d. $\psi(b) = c$, postoji $a \in A$ t.d. vrijedi $b^g - b = a^g - a, \forall g \in G \iff (b-a)^g = b - a, \forall g \in G$. Sada je $b - a \in B^G$, a vrijedi i $\psi(b - a) = \psi(b) = c \implies c \in \psi(B^G)$ Općenito vrijedi:

Propozicija 5.1.4. *Svaki kratki egzaktni niz G-modula*

$$0 \to A \to B \to C \to 0 \tag{5.9}$$

inducira dugi egzaktni niz[2]

$$0 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C). \tag{5.10}$$

Dokaz. Upravo smo pokazali egzaktnost u C^G, jedino mjesto koje još može predstavljati problem je $H^1(G, A)$. Iz definicije preslikavanja δ se vidi da je $\delta(C^G) \subset \ker(H^1(G, A) \to H^1(G, B))$, a ako pretpostavimo da je $\xi_A \in \ker(H^1(G, A) \to H^1(G, B)) \iff i \circ \xi_A = b^g - b$, tada je $0 = \psi \circ i \circ \xi_A = \psi(b^g - b) = c^g - c, \forall g \in G$ pa je $\psi(b) = c \in C^G$. Lako se vidi da je $\delta(\psi(b)) = \xi_A$ pa je $\mathrm{Im}(\delta) = \ker(H^1(G, A) \to H^1(G, B))$ i naš niz je egzaktan. □

[2]Niz se zapravo nastavlja, ali nama nije potrebno

5.2 Weilovo sparivanje

Neka je K polje algebarskih brojeva te E/K eliptička krivulja nad K. Korolar iz prethodnog poglavlja kaže kako je m-torzija $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ slobodni $\mathbb{Z}/m\mathbb{Z}$ modul ranga 2. Znamo da na $E[m]$ postoji prirodno nedegenerirano multilinearno preslikavanje, determinanta. Za neku bazu $\{T_1, T_2\}$ od $E[m]$ determinanta je dana s

$$det\colon E[m] \times E[m] \to \mathbb{Z}/m\mathbb{Z}, \tag{5.11}$$

$$(aT_1 + bT_2, cT_1 + dT_2) \mapsto ad - bc. \tag{5.12}$$

Ovo sparivanje nije nužno Galois invarijantno, što je naš cilj. Htjeli bi preslikavanje oblika $\zeta^{det(P,Q)}$ gdje je ζ primitivni m-ti korijen jedinice. Za neki $T \in E[m]$ po teoremu 2.3.3 postoji $f_T \in \bar{K}(E)^*$ t.d.

$$\mathrm{div}(f_T) = m(T) - m(O). \tag{5.13}$$

Uzmimo neki $T' \in E(\bar{K})$ takav da je $mT' = T$. Koristeći nanovo teorem 2.3.3 postoji funkcija $g_T \in \bar{K}(E)^*$ t.d.

$$\mathrm{div}(g_T) = \sum_{R \in E[m]} (T' + R) - (R).^3 \tag{5.14}$$

Izračunajmo $\mathrm{div}(f_T \circ [m])$. f_T ima m-struku nulu u T i m-struki pol u O. Točke koje $[m]$ preslika u T su točno točke oblika $T' + R$ za $R \in E[m]$ pa za svaku takvu i samo za svaku takvu točku funkcija $\mathrm{div}(f_T \circ [m])$ ima m-struku nulu. Isto vrijedi za polove u točkama R, $R \in E[m]$. Zato je

$$\mathrm{div}(f_T \circ [m]) = \sum_{R \in E[m]} m(T' + R) - m(R) = m \cdot \mathrm{div}(g_T) = \mathrm{div}(g_T^m) \tag{5.15}$$

pa je $f_T \circ [m] = C \cdot g_T^m$, ali konstantu C možemo "ubaciti" u funkciju f_T[4] pa imamo $f_T \circ [m] = g_T^m$. Sada za neki $S \in E[m]$ imamo

$$g_T^m(X + S) = f_T(m(X + S)) = f_T(mX) = g_T^m(X) \tag{5.16}$$

pa je $g_T(X + S)/g_T(X)$ $m-$ti korijen jedinice za svaki $X \in E$. Preslikavanje

$$E(\bar{K}) \to \mathbb{P}^1 \tag{5.17}$$

$$X \mapsto g_T(X + S)/g_T(X) \tag{5.18}$$

[3] divizor na desnoj strani zadovoljava uvjete teorema. $\sum_P n_P = 0$ jer se koeficijenti 1 i -1 pojavljuju svaki po m^2 puta, a $\sum_{R \in E[m]} [1](T' + R) - [1](R) = \sum_{R \in E[m]} T' = [m^2]T' = [m]T = O$.

[4] jer možemo manipulirati njima do na množenje konstantom

je morfizam krivulja, koji mora biti surjektivan ili konstanta[5]. Surjektivan očito nije pa je slika ovog preslikavanja neki m-ti korijen jedinice.
Sada možemo definirati preslikavanje

$$\langle \cdot, \cdot \rangle_m \colon E[m] \times E[m] \to \mu_m, \tag{5.19}$$
$$(S, T) \mapsto g_T(X + S)/g_T(X) \tag{5.20}$$

gdje je $X \in E$ bilo koja točka takva da $g_T(X+S)$, $g_T(X)$ postoje i nisu nula.[6] Ovo sparivanje naziva se *Weilovo sparivanje* i ima sljedeća svojstva:

Propozicija 5.2.1. *Weilovo sparivanje $\langle \cdot, \cdot \rangle_m$ je*

1. *Bilinearno, tj. $\langle S_1 + S_2, T \rangle_m = \langle S_1, T \rangle_m \langle S_2, T \rangle_m$ te $\langle S, T_1 + T_2 \rangle_m = \langle S, T_1 \rangle_m \langle S, T_2 \rangle_m$.*
2. *Alternirajuće, tj. $\langle T, T \rangle_m = 1$ za svaki $T \in E[m]$. Posebno, $\langle S, T \rangle_m = \langle T, S \rangle_m^{-1}$.*
3. *Nedegenerirano, tj. ($\langle S, T \rangle_m = 1$ za svaki $S \in E[m]$) ako i samo ako ($T = O$).*
4. *Galois invarijantno, tj. $\sigma \langle S, T \rangle_m = \langle \sigma S, \sigma T \rangle_m$ za sve $S, T \in E[m], \sigma \in G(\bar{K}/K)$.*
5. *Kompatibilno, tj. $\langle S, T \rangle_{mm'} = \langle m'S, T \rangle_m$ za sve $m, m' \in \mathbb{N}$ te $S \in E[mm'], T \in E[m]$*

Dokaz. [3, str. 94, prop. 8.1.] □

Korolar 5.2.2. *Ako je $E[m] \subset E(K)$, onda je $\mu_m \subset E(K)$.*

Dokaz. Neka je $E[m] \subset E(K)$. Tvrdimo da postoje $S, T \in E[m]$ t.d. $\langle S, T \rangle_m = \zeta$, primitivni $m-$ti korijen jedinice. Neka je $Im(\langle \cdot, \cdot \rangle_m) = \mu_d \leq \mu_m$. [7] Tada je $1 = \langle S, T \rangle_m^d = \langle dS, T \rangle_m$ zbog bilinearnosti, za sve $S, T \in E[m]$. Sada zbog trećeg svojstva prethodne propozicije imamo $dS = O$ za svaki $S \in E[m]$, što povlači $E[m] \subset E[d]$ pa je $d = m$. Neka je sada $\langle S, T \rangle_m = \zeta$. Koristimo Galoisovu invarijantnost $\langle \cdot, \cdot \rangle_m$ te činjenicu da je $E[m] \subset E(K)$. $\sigma\zeta = \sigma \langle S, T \rangle_m = \langle \sigma S, \sigma T \rangle_m = \langle S, T \rangle_m = \zeta$ za sve $\sigma \in G(\bar{K}/K)$, što povlači $\zeta \in K$ pa je $\mu_m = \langle \zeta \rangle \subset K$. □

[5] [3, str. 20, Teorem II.2.3.]
[6] μ_m označava grupu m-tih korijena jedinice.
[7] znamo da je slika neka podgrupa od μ_m

5.3 Hilbertov teorem 90 i Kummerova teorija

Lema 5.3.1. *Neka je E polje i neka su $\sigma_1, \ldots, \sigma_n$ različiti automorfizmi polja E. Tada, ako su $c_1, \ldots, c_n \in E$ te*

$$c_1\sigma_1(x) + \cdots + c_n\sigma_n(x) = 0 \tag{5.21}$$

vrijedi za svaki $x \in E$, onda je $c_1 = \cdots = c_n = 0$.

Dokaz. Pretpostavimo da postoji netrivijalna relacija koja povezuje σ_i, neka je u njoj r nenul koeficijenata te neka je r najmanji prirodni broj za koji to vrijedi. Očito je $r > 1$. Možemo BSO pretpostaviti da su prvih r koeficijenata nenul, tj. da je

$$c_1\sigma_1(x) + \cdots + c_r\sigma_r(x) = 0 \tag{5.22}$$

za svaki $x \in E$, gdje nijedan c_i nije nula. Uvrstimo sad ax u jednadžbu umjesto x. Imamo

$$c_1\sigma_1(a)\sigma_1(x) + \cdots + c_r\sigma_r(a)\sigma_r(x) = 0. \tag{5.23}$$

Množenjem prve jednadžbe sa $\sigma_r(a)$ i oduzimanjem od druge imamo

$$c_1[\sigma_1(a) - \sigma_r(a)]\sigma_1(x) + \cdots + c_{r-1}[\sigma_{r-1}(a) - \sigma_r(a)]\sigma_{r-1}(x) = 0. \tag{5.24}$$

Ova jednadžba je kraća ($r - 1 < r$) od prve pa ako pokažemo da je netrivijalna, dobili smo kontradikciju. Po pretpostavci, funkcije σ_i su sve različite, zato možemo odabrati početni $a \in E$ t.d. je $\sigma_1(a) \neq \sigma_r(a)$. Sada je, jer je $c_1 \neq 0$, prvi koeficijent $c_1[\sigma_1(a) - \sigma_r(a)] \neq 0$ pa imamo kraću netrivijalnu relaciju što je kontradikcija. □

Teorem 5.3.2 (Kohomološki Hilbertov teorem 90)**.** *Neka je E/F Galoisovo proširenje s Galoisovom grupom G. Tada je $H^1(G, E^*)$ trivijalno, tj. svaki* 1*-kociklus od G u E^* je* 1*-korub.*

Dokaz. Neka je $\{\alpha_\sigma\}_{\sigma\in G}$ 1-kociklus od G u E^*. U multiplikativnoj notaciji to znači da je

$$\alpha_{\sigma\tau} = \alpha_\sigma \cdot \sigma(\alpha_\tau) \tag{5.25}$$

za sve $\sigma, \tau \in G$. Želimo pokazati (po definiciji 1-koruba) da postoji neki $\gamma \in E^*$ t.d. $\alpha_\sigma = \frac{\sigma\gamma}{\gamma}$ za sve $\sigma \in G$. Budući da su α_τ nenul (jer su u E^*) lema 5.3.1 kaže da sljedeća konačna (jer je E/F Galoisovo, dakle konačno) linearna kombinacija

$$\sum_{\tau\in G} \alpha_\tau\tau \colon E \to E \tag{5.26}$$

nije nul preslikavanje. Zato postoji neki $\theta \in E$ t.d.

$$\beta := \sum_{\tau\in G} \alpha_\tau\tau(\theta) \neq 0. \tag{5.27}$$

Sada za svaki $\sigma \in G$ imamo

$$\sigma\beta = \sum_{\tau\in G} \sigma(\alpha_\tau)\sigma\tau(\theta) = \sum_{\tau\in G} \alpha_\sigma^{-1}\alpha_{\sigma\tau}\sigma\tau(\theta) = \alpha_\sigma^{-1}\sum_{\tau\in G}\alpha_{\sigma\tau}\sigma\tau(\theta) = \alpha_\sigma^{-1}\beta \tag{5.28}$$

jer suma prolazi po cijelom G. Sada je $\alpha_\sigma = \frac{\beta}{\sigma(\beta)}$, a uz supstituciju $\gamma := \beta^{-1}$ imamo $\alpha_\sigma = \frac{\sigma\gamma}{\gamma}$ što smo i htjeli dokazati. □

Teorem 5.3.3 (Klasična verzija Hilbertovog teorema 90)**.** *Neka je E/F konačno cikličko proširenje s generatorom Galoisove grupe σ. Za bilo koji $\alpha \in E$ norme 1 postoji $\beta \in E$ t.d. $\alpha = \frac{\beta}{\sigma(\beta)}$*

Dokaz. Norma od α je 1 je ekvivalentno sa $\alpha \cdot \sigma\alpha \cdots \sigma^{m-1}\alpha = 1$, lako se vidi da je sa $\alpha_\sigma = \alpha$ dan 1-kociklus od $\langle\sigma\rangle$ u E^*. Iz teorema 5.3.2 znamo da je to ujedno i korub te vrijedi $\alpha_\sigma = \frac{\sigma(\gamma)}{\gamma}$. Supstitucijom $\beta := \gamma^{-1}$ imamo $\alpha = \alpha_\sigma = \frac{\beta}{\sigma\beta}$ što smo i htjeli. □

Teorem 5.3.4 (Kummerova teorija)**.** *Za svako cikličko proširenje L/K stupnja n, t.d. $\mu_n \subset K$, postoji $a \in K$, t.d. $L = K(\sqrt[n]{a})$.*

Dokaz. Neka je ζ primitivni n-ti korijen jedinice, očito je $N(\zeta) = 1$. Zato je po 5.3.3 $\zeta = \frac{\sigma(\beta)}{\beta}$ za neki $\beta \in L$. β nije u K jer bi ga σ fiksirao pa bi imali $\zeta = 1$, očitu kontradikciju. Dalje je $\beta^n = \zeta^n\beta^n = (\sigma(\beta))^n = \sigma(\beta^n)$. Element β^n je fiksiran generatorom Galoisove grupe, shodno tome i cijelom Galoisovom grupom pa zaključujemo da je $\beta^n = a \in K$. Zadnji argument koji imamo je da $\beta^k \notin K$ za bilo koji $k < n$ jer bi tada bilo $\zeta^k = (\frac{\sigma(\beta)}{\beta})^k = \frac{(\sigma(\beta))^k}{\beta^k} = \frac{\sigma(\beta^k)}{\beta^k} = \frac{\beta^k}{\beta^k} = 1$. Zato je $K(\beta)$ proširenje stupnja n koje se nalazi u L (koje je i samo proširenje stupnja n) pa vrijedi $L = K(\beta) = K(\sqrt[n]{a})$. □

5.4 Kummerovo sparivanje

Neka je $E(K)$ eliptička krivulja te $m \in \mathbb{Z}$.

Lema 5.4.1. *Neka je L/K konačno Galoisovo proširenje. Pretpostavimo da je $E[m] \subset E(L)$ te $|E(L)/mE(L)| < \infty$. Tada je $|E(K)/mE(K)| < \infty$.*

Dokaz. Krenimo s kratkim egzaktnim nizom

$$0 \to E[m] \hookrightarrow E(L) \xrightarrow{m\cdot} mE(L) \to 0 \tag{5.29}$$

Koristeći Galoisovu kohomologiju za $G = \mathrm{Gal}(L/K)$ imamo dugi egzaktni niz

$$0 \to E(K)[m] \to E(K) \to mE(L) \cap E(K) \to H^1(G, E(K)[m]) \to \dots. \tag{5.30}$$

Iz definicije egzaktnosti vidimo da postoji ulaganje

$$mE(L) \cap E(K)/mE(K) \hookrightarrow H^1(G, E(K)[m]). \tag{5.31}$$

Budući da je djelovanje grupe G na $E(K)$ trivijalno imamo $H^1(G, E(K)[m]) = \mathrm{Hom}(G, E(K)[m])$. Desni skup je konačan jer su G i $E[m]$ konačni skupovi pa je i $mE(L) \cap E(K)/mE(K)$ konačno.

$$0 \to \frac{mE(L) \cap E(K)}{mE(K)} \to \frac{E(K)}{mE(K)} \to \frac{E(L)}{mE(L)} \tag{5.32}$$

je egzaktan niz pa je $\frac{E(K)}{mE(K)}$ konačno. □

Ova lema pokazuje da nam je dovoljno dokazati glavni teorem za konačno proširenje L/K koje sadrži $[m]$-torziju. Budući da postoji samo konačno mnogo točaka u $[m]$-torziji, dovoljno je promatrati Galoisovo proširenje $L/K(E[m])$. Zato odsad smatramo da $E[m] \subset E(K)$. Definirajmo preslikavanje $\kappa\colon E(K) \times \mathrm{Gal}(\bar{K}/K) \to E[m]$ tako što $\forall P \in E(K)$ izaberemo $Q \in E(\bar{K})$ t.d. $[m]Q = P$ te definiramo $\kappa(P, \sigma) := Q^\sigma - Q$. Dokažimo da je ovo preslikavanje dobro definirano.[8] Pretpostavimo da je Q' neka druga $[m]$-praslika od P. Tada je $[m](Q - Q') = 0 \implies Q - Q' \in E[m] \subset E(K)$(po pretpostavci). $\mathrm{Gal}(\bar{K}/K)$ fiksira sve točke u $E(K)$ pa je $(Q - Q')^\sigma = Q - Q' \iff Q^\sigma - Q = Q'^\sigma - Q'$.
Promatrajmo jednadžbu $[m]Q = P$. Preslikavanje $[m]$ je racionalna funkcija s koeficijentima u K pa je

$$[m]Q^\sigma = ([m]Q)^\sigma = P^\sigma = P = [m]Q \implies [m](Q^\sigma - Q) = 0 \iff \kappa(P, \sigma) \in E[m] \tag{5.33}$$

Propozicija 5.4.2. *Lijeva jezgra preslikavanja κ je $mE(K)$.*

Dokaz. Jasno je da se $mE(K)$ nalazi u jezgri jer $P \in mE(K) \implies P = mQ$ za neki $Q \in E(K)$ što implicira $Q^\sigma = Q$.
Ako je P u jezgri, onda je po definiciji $Q = Q^\sigma, \forall \sigma \in \mathrm{Gal}(\bar{K}/K)$. Sada po definiciji Galoisove grupe mora biti $Q \in E(K) \implies P \in mE(K)$. □

Propozicija 5.4.3. *Desna jezgra preslikavanja κ je $\mathrm{Gal}(\bar{K}/L)$, gdje je $L = K(m^{-1}E(K))$ proširenje od K koje sadrži sve koordinate točaka Q za koje vrijedi $[m]Q \in E(K)$. Posebno, L je Galoisovo proširenje od K.*

Dokaz. Očito je svaki element $\sigma \in \mathrm{Gal}(\bar{K}/L)$ u jezgri jer σ po definiciji fiksira sve $[m]$-praslike točaka iz $E(K)$. Ako se $\sigma \in \mathrm{Gal}(\bar{K}/K)$ nalazi u desnoj jezgri, onda je $Q^\sigma = Q$ za svaki Q koji je $[m]$-praslika neke točke $P \in E(K)$. Posebno, to znači da σ fiksira sve generatore polja L pa je $\sigma \in \mathrm{Gal}(\bar{K}/L)$. L/K je Galoisovo jer je $\mathrm{Gal}(\bar{K}/L)$ jezgra homomorfizma, dakle normalna podgrupa od $\mathrm{Gal}(\bar{K}/K)$. □

[8] moramo pokazati neovisnost o izboru praslike te činjenicu da je slika stvarno sadržana u torziji

Definicija 5.4.4. Savršeno sparivanje $f\colon G\times H \to A$ *je homomorfizam t.d. je* $f(g,\cdot)\colon H \to A$ *trivijalan ako i samo ako je* g *identiteta u* G *te* $f(\cdot,h)\colon G \to A$ *trivijalan ako i samo ako je* h *identiteta u* H.

Lema 5.4.5. *Neka je* $f\colon G \times H \to A$ *savršeno sparivanje, gdje je* A *konačna Abelova grupa. Tada su ili obje* G, H *konačne ili su obje beskonačne.*

Dokaz. Bez smanjenja općenitosti pretpostavimo da je G konačna te H beskonačna. Primjetimo da je $\mathrm{Hom}(G,A) \subset \mathrm{Maps}(G,A)$ konačno jer su obje G, A konačne. Preslikavanje iz beskonačne grupe H u konačnu grupu $\mathrm{Hom}(G,A)$ dano sa $h \mapsto f(\cdot,h)$ ima netrivijalnu jezgru, ali to je u kontradikciji s činjenicom da je f savršeno sparivanje. □

Propozicija 5.4.6. *Preslikavanja* $\kappa(P,\cdot)\colon \mathrm{Gal}(\bar{K}/K) \to E[m]$ *te* $\kappa(\cdot,\sigma)\colon E(K) \to E[m]$ *su homomorfizmi.*

Dokaz. Želimo dokazati $(Q^{\sigma_1}-Q)+(Q^{\sigma_2}-Q) = Q^{\sigma_1\circ\sigma_2}-Q \iff Q^{\sigma_1}-Q = (Q^{\sigma_2})^{\sigma_1}-Q^{\sigma_2}$. Budući da je κ dobro definirano(slika je u $E[m]$), znamo da je $[m]\kappa(P,\sigma_2) = [m](Q^{\sigma_2}-Q) = 0 \implies mQ^{\sigma_2} = mQ = P$ tj. Q^{σ_2} je m-praslika od P. Zato je zbog neovisnosti o izboru praslike $\kappa(P,\sigma_1) = (Q^{\sigma_2})^{\sigma_1} - Q^{\sigma_2} = Q^{\sigma_1} - Q$.
S druge strane, želimo dokazati $(Q_1^\sigma - Q_1) + (Q_2^\sigma - Q_2) = (Q_1+Q_2)^\sigma - (Q_1+Q_2)) \iff Q_1^\sigma + Q_2^\sigma = (Q_1+Q_2)^\sigma$. Zbrajanje je racionalna funkcija s koeficijentima u K pa jer je σ automorfizam polja imamo traženu tvrdnju. □

Propozicija 5.4.7. *Kummerovo sparivanje inducira savršeno sparivanje* $\kappa\colon E(K)/mE(K)\times \mathrm{Gal}(L/K) \to E[m]$

Dokaz. Lako se vidi iz prethodnih propozicija. □

Naša motivacija je sada očita. $E(K)/mE(K)$ je konačno ako i samo ako je $\mathrm{Gal}(L/K)$ konačno, dakle dovoljno je pokazati da je L/K konačno proširenje.

Poglavlje 6

Mordell-Weilov teorem

6.1 Slabi Mordell-Weilov teorem

Dokaz glavnog teorema ćemo podijeliti na dva dijela. Prvi dio je

Teorem 6.1.1 (Slabi Mordell-Weilov teorem)**.** *Za polje algebarskih brojeva K, kvocijent $E(K)/mE(K)$ je konačan.*

Drugi dio je procedura spusta o kojoj ćemo u sljedećem poglavlju. Vratimo se na slabi Mordell-Weilov teorem.

Neka je K lokalno polje, potpuno u odnosu na diskretnu valuaciju v, zajedno s prstenom cijelih R te maksimalnim idealom $\mathcal{M} \subset R$.

Definicija 6.1.2. *Neka je E/K Eliptička krivulja i neka je $\tilde{E}$ redukcija modulo $\mathcal{M}$ minimalne Weierstrassove jednadžbe za E. Kažemo da E ima* dobru *redukciju ako je $\tilde{E}$ nesingularna, inače ima* lošu *redukciju.*

Propozicija 6.1.3. *E ima dobru redukciju ako i samo ako diskriminanta Δ Weierstrassove jednadžbe krivulje E zadovoljava $v(\Delta) = 0$*

Dokaz. [3, str. 196, prop. 5.1.a)] □

Definicija 6.1.4. *Neka je K polje algebarskih brojeva i neka je E/K eliptička krivulja. Neka je $v \in M_K^0$ (gdje je M_K^0 skup diskretnih valuacija na K). Kažemo da E ima* dobru *(odn.* lošu*)* redukciju u *v ako E ima dobru (odn. lošu) redukciju promatrana nad K_v. Uzimajući minimalnu Weierstrassovu jednadžbu za E nad K_v, reduciranu krivulju nad rezidualnim poljem označavamo sa $\tilde{E}_v/k_v$.*

Propozicija 6.1.5 (nanovo iskazan teorem 2.2.4)**.** *Neka je $v \in M_K^0$ diskretna valuacija takva da je $v(m) = 0$ i takva da E ima dobru redukciju u v. Tada je redukcija*

$$E(K)[m] \to \tilde{E}_v(k_v) \tag{6.1}$$

injektivna.

Propozicija 6.1.6. *Neka je $L_P = K([m]^{-1}P)$*

$$S = \{v \in M_K^0 \colon E \text{ ima lošu redukciju u } v\} \cup \{v \in M_K^0 \colon v(m) \neq 0\} \cup M_K^\infty. \tag{6.2}$$

tada je L_P/K neramificirano za sve $v \notin S$, tj. ako je $v \in M_K$ i $v \notin S$ onda je L_P/K neramificiran u v. Ovo vrijedi za svaku točku $P \in E(K)$.

Dokaz. Neka $v' \in M_{K'}^0$ leži nad v i neka je $k'_{v'}/k_v$ pripadajuće proširenje rezidualnih polja. Pretpostavka da $v \notin S$ osigurava da E ima dobru redukciju u v pa ima i dobru redukciju u v' jer možemo uzeti istu Weierstrassovu jednadžbu. Zato imamo standardnu redukciju

$$E(K') \to \tilde{E}(k'_{v'}), \tag{6.3}$$

koje označavamo sa tildom. Neka je $I_{v'/v} \leq G_{\bar{K}/K}$ inercijska grupa za v'/v i uzmimo bilo koji $\sigma \in I_{v'/v}$. Po definiciji, element inercijske grupe djeluje trivijalno na $\tilde{E}(k'_{v'})$ pa je

$$\widetilde{Q^\sigma - Q} = \tilde{Q}^\sigma - \tilde{Q} = \tilde{O}. \tag{6.4}$$

S druge strane, činjenica da je $[m]Q \in E(K)$ nam daje

$$[m](Q^\sigma - Q) = ([m]Q)^\sigma - [m]Q = O. \tag{6.5}$$

Zato je točka $Q^\sigma - Q \in mE(K)$, ali i u jezgri redukcije modulo v'. Sada propozicija 6.1.5 daje $Q^\sigma - Q = O$. Ovo vrijedi za svaki element inercije σ pa je inercija trivijalna i L_P je neramificiran nad K u v'. Budući da ovo vrijedi za svaki v' nad v i za svaki $v \notin S$, tvrdnja je dokazana. □

Polje $L = K([m]^{-1}E(K))$ je kompozicija polja oblika $L_P = K([m]^{-1}P)$ koja sva zadovoljavaju prethodnu propoziciju.

Lema 6.1.7. *Svako proširenje L_P je kompozicija dva ciklička proširenja od K stupnja najviše m.*

Dokaz. Neka je $G = G(\bar{\mathbb{Q}}/K)$. Korolar 2.1.4 u kombinaciji sa korolarom 3.1.11 daje kratki egzaktni niz

$$0 \to E[m] \to E(\bar{\mathbb{Q}}) \xrightarrow{[m]} E(\bar{\mathbb{Q}}) \to 0. \tag{6.6}$$

Galoisova kohomologija inducira dugi egzaktni niz

$$0 \to E[m] \to E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta} H^1(G, E[m]) \to \dots \tag{6.7}$$

Budući je $E[m] \subset E(K)$, djelovanje grupe G na $E[m]$ je trivijalno pa je $H^1(G, E[m]) = \mathrm{Hom}(G, E[m])$. Posebno, imamo injekciju

$$E(K)/mE(K) \xrightarrow{\delta} \mathrm{Hom}(G, E[m]) \tag{6.8}$$

danu sa $\delta(P)(\sigma) = \sigma Q - Q$ za bilo koji $P \in E(K)/mE(K), \sigma \in G$ gdje je $Q \in [m]^{-1}P$. (Ovo je zapravo preslikavanje κ iz 5. poglavlja).
Uzmimo $f \in \mathrm{Hom}(G, E[m])$. Budući je $\ker(f) \trianglelefteq G$, Galoisova teorija daje pridruženo fiksno polje $L = \bar{\mathbb{Q}}^{\ker(f)}$. Vrijedi

$$G(L/K) \cong G/G(\bar{\mathbb{Q}}/L) \cong G/\ker(f) \cong Im(f) \leq E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2 \tag{6.9}$$

pa je L/K kompozicija najviše dva ciklička proširenja stupnja koji dijeli m. Po definiciji preslikavanja δ imamo $L_P = K([m]^{-1}P) = \bar{Q}^{\ker(\delta(P))}$ te je lema dokazana. □

Svaki L_P (tj. svako od najviše dva proširenja od kojih je L_P kompozicija) zadovoljava uvjete teorema 4.1.17. Zato postoji konačno mnogo različitih polja L_P te je L kao njihova kompozicija konačno proširenje od K. Lema 5.4.5 u kombinaciji sa propozicijom 5.4.7 daje $E(K)/mE(K) < \infty$.

6.2 Procedura spusta

Ovdje opisujemo proceduru spusta, koja nam omogućuje da izvedemo Mordell-Weilov teorem iz slabog Mordell-Weilovog teorema. Proces je opisan u sljedećem teoremu, jedino što preostaje je pronaći zadovoljavajuću visinu na krivulji.

Teorem 6.2.1. *Neka je A Abelova grupa zajedno s visinskom funkcijom $h\colon A \to R$ koja zadovoljava*

(i) Za fiksni $Q \in A$ postoji konstanta C_Q takva da $h(P+Q) \leq 2h(P) + C_Q$ za svaki $P \in A$.

(ii) Postoje prirodni broj $m \geq 2$ i konstanta C t.d. $h(mP) \geq m^2 h(P) - C$ za svaki $P \in A$.

(iii) Za svaki $D \in \mathbb{R}$, skup $\{P \in A \mid h(P) \leq D\}$ je konačan.

Ako je A/mA konačna, onda je A konačno generirana.

Dokaz. Neka su $Q_1, \ldots, Q_r \in A$ predstavnici klasa kvocijenta A/mA. Neka je $P \in A$. Klase čine particiju skupa A pa postoji $1 \leq i_1 \leq r$ t.d. je $P - Q_{i_1} \in mA$. Označimo $P = P_0 = mP_1 + Q_{i_1}$. Slično, možemo rekurzivno konstruirati niz točaka $P_{j-1} = mP_j + Q_{i_j}$ za $P_j \in A, i_j \in \{1, \ldots, r\}$. Tada za svaki j, koristeći redom (ii) te (i)

$$h(P_j) \leq \frac{1}{m^2}(h(mP_j) + C) = \frac{1}{m^2}(h(P_{j-1} - Q_{i_j}) + C) \leq \frac{1}{m^2}(2h(P_j - 1) + C' + C) \tag{6.10}$$

gdje je $C' = \max\{C_{-Q_1}, \ldots, C_{-Q_r}\}$. Iterirana upotreba ove nejednakosti nam daje vezu između $h(P_n)$ i $h(P)$.

$$h(P_n) \leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \cdots + \frac{2^{n-1}}{m^{2n}}\right)(C' + C) \tag{6.11}$$

$$< \left(\frac{2}{m^2}\right)^n h(P) + \frac{1}{m^2 - 2}(C' + C) \tag{6.12}$$

$$\leq \left(\frac{1}{2}\right)^n h(P) + \frac{1}{2}(C' + C) \quad \text{jer je } m \geq 2 \tag{6.13}$$

$$\leq 1 + \frac{1}{2}(C' + C) \quad \text{za dovoljno veliki } n. \tag{6.14}$$

Sada je

$$P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j} \tag{6.15}$$

pa je A generirana sa

$$\{Q_1, \ldots, \mathbb{Q}_r\} \cup \{P \in A \mid h(P) \leq 1 + (C' + C)/2\}$$

što je konačno zbog (iii) □

Radi jednostavnosti, dati ćemo samo primjer visinske funkcije za $E/\mathbb{Q}$. Postoji kompliciranija visinska funkcija na $E(K)$ koja daje Mordell-Weilov teorem na E/K. (vidi [3, str. 234, VIII.6.])

Definicija 6.2.2. *Neka je $t \in \mathbb{Q}$ sa $t = p/q$, $(p, q) = 1$.* Visina *od t dana je sa*

$$H(t) = \max\{|p|, |q|\}. \tag{6.16}$$

Definicija 6.2.3. Logaritamska visina na $E(\mathbb{Q})$ *je funkcija*

$$h_x \colon E(\mathbb{Q}) \to \mathbb{R} \tag{6.17}$$

dana s $h_x(x, 0) = 0$ te $h_x(x, y) = \log H(x(P))$.

Lema 6.2.4. *Neka je $E/\mathbb{Q}$ eliptička krivulja dana Weierstrassovom jednadžbom*

$$E\colon y^2 = x^3 + Ax + B \quad A, B \in \mathbb{Z} \tag{6.18}$$

(i) Fiksirajmo $P_0 \in E(\mathbb{Q})$. Postoji konstanta C_1 ovisna o P_0, A, B t.d. $h(P + P_0) \leq 2h(P) + C_1$ za svaki $P \in E(\mathbb{Q})$

(ii) Postoji konstanta C_2 ovisna o A, B t.d. $h(2P) \geq 4h(P) - C_2$ za svaki $P \in E(\mathbb{Q})$

(iii) Za svaki $C_3 \in E(\mathbb{R})$, skup $\{P \in E(\mathbb{Q}) \mid h(P) \leq C_3\}$ je konačan.

Dokaz. (i) Pretpostavljamo da je $C_1 > \max\{h_x(P_0), h_x([2]P_0)\}$, što osigurava tvrdnju u slučajevima $P_0 = O$ ili $P \in \{O, \pm P_0\}$. Inače je

$$P = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \quad \text{te} \quad P = (x_0, y_0) = \left(\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3}\right). \tag{6.19}$$

gdje su svi razlomci skraćeni koliko je moguće. Jednadžbe zbrajanja točaka na $E(\mathbb{Q})$ nam daju

$$x(P + P_0) = \left(\frac{y - y_0}{x - x_0}\right)^2 - x - x_0. \tag{6.20}$$

Koristeći činjenicu da P, P_0 zadovoljavaju 6.18 imamo

$$x(P + P_0) = \frac{(xx_0 + A)(x + x_0) + 2B - 2yy_0}{(x - x_0)^2} \tag{6.21}$$

$$= \frac{(aa_0 + Ad^2d_0^2)(ad_0^2 + a_0d^2) + 2Bd^4d_0^4 - 2bdb_0d_0}{(ad_0^2 - a_0d^2)^2}. \tag{6.22}$$

Kada računamo visinu racionalnog broja, kraćenje razlomka može samo smanjiti visinu. Lako se dolazi do ocjene

$$H(x(P + P_0)) \leq C_1' \max\{|a|^2, |d|^4, |bd|\}, \tag{6.23}$$

gdje je C_1' jednostavan izraz ovisan o A, B, a_0, b_0, d_0. Budući da je $H(x(P)) = \max\{|a|^2, |d|^4\}$ skoro smo gotovi, jedino se moramo "rješiti" izraza $|bd|$. Koristimo činjenicu da P leži na krivulji E pa vrijedi

$$b^2 = a^3 + Aad^4 + Bd^6 \tag{6.24}$$

Zato je

$$|b| \leq C_1'' \max\{|a|^{3/2}, |d|^3\}, \tag{6.25}$$

što u kombinaciji s gornjom ocjenom za $H(x(P + P_0))$ daje

$$H(x(P + P_0)) \leq C_1 \max\{|a|^2, |d|^4\} = C_1 H(x(P))^2. \tag{6.26}$$

Logaritmiranjem dobivamo željeni rezultat.

(ii) Dokaz ovog dijela leme je tehnički zahtjevan, ali ne koristi ništa osim jednostavnih ocjena. Dokaz možete naći u [3, str. 222,lema 4.1.b)]

(iii) Za svaku konstantu C, skup

$$\{t \in \mathbb{Q} \colon H(T) \leq C\} \tag{6.27}$$

ima najviše $(2C+1)^2$ elemenata, jer brojnik i nazivnik broja t moraju biti cijeli brojevi između $-C$ i C. Nadalje, za svaki x postoje najviše dvije vrijednosti za y takve da je $(x, y) \in E$. Zato je skup

$$\{P \in E(\mathbb{Q}) \colon h_x(P) \leq C_3\} \tag{6.28}$$

konačan.

□

Teorem 6.2.5 (Mordell-Weilov teorem)**.** *$E(\mathbb{Q})$ je konačno generirana Abelova grupa.*

Dokaz. Po teoremu 6.1.1 i lemi 6.2.4, $E(\mathbb{Q})$ i h_x zadovoljavaju uvjete teorema 6.2.1 pa je $E(\mathbb{Q})$ konačno generirana. □

Bibliografija

[1] R. Hartshorne, *Algebraic Geometry*, Encyclopaedia of mathematical sciences, Springer, 1977, ISBN 9780387902449, https://books.google.hr/books?id=3rtX9t-nnvwC.

[2] James S. Milne, *Algebraic Number Theory (v3.06)*, 2014, Available at www.jmilne.org/math/, str. 164.

[3] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer, 2009, ISBN 9780387094946, https://books.google.hr/books?id=Z90CA_EUCCkC.

Sažetak

Mordell-Weilov teorem kaže da je za algebarsku mnogostrukost A nad poljem brojeva K, grupa K-racionalnih točaka $A(K)$ konačno generirana Abelova grupa, koju zovemo Mordell-Weilova grupa. Poseban slučaj, kad je A eliptička krivulja E te K polje racionalnih brojeva $\mathbb{Q}$ je Mordellov teorem. On odgovara na pitanje koje je navodno postavio Poincare oko 1908. Teorem je dokazao Louis Mordell 1922. U ovom radu dokazujemo Mordellov teorem za eliptičke krivulje nad algebarskim poljima brojeva K.

Summary

The Mordell–Weil theorem states that for an abelian variety A over a number field K, the group $A(K)$ of K-rational points of A is a finitely-generated abelian group, called the Mordell-Weil group. The case with A an elliptic curve E and K the rational number field $\mathbb{Q}$ is Mordell's theorem, answering a question apparently posed by Poincaré around 1908; it was proved by Louis Mordell in 1922. In this paper we prove Mordell's theorem for elliptic curves on number fields K.

Životopis

Rođen sam 27.11.1987. godine u Zagrebu, gdje sam pohađao Osnovnu školu Nikole Tesle do 2002. kada sam upisao V. gimnaziju u Zagrebu. Kroz osnovnu i srednju školu ostvario sam zapažene rezultate na raznim natjecanjima iz matematike i fizike. Preddiplomski studij matematike na PMF-u sam upisao 2006. te ga završio odličnim uspjehom. Integrirani doktorski studij matematike na Jacobs University Bremen započeo sam 2009. godine kao stipendist fakulteta, da bi isti prekinuo zbog osobnih razloga 2012. Tada sam se vratio u Zagreb te upisao diplomski studij teorijske matematike na PMF-u.