Aritmetička geometrija

Filip Najman

Prirodoslovno matematički fakultet, Matematički odsjek
2015/2016

Sadržaj

Poglavlje 1

Uvod

Poglavlje 2

Racionalne točke na konikama

Ovo poglavlje bi se moglo nazvati i "racionalne točke na krivuljama genusa 0", međutim, kako još nismo definirali genus, te kako će nam trebati Riemann-Rochov teorem da bismo pokazali da su sve krivulje genusa 0 konike, sadašnji naslov je prikladniji.

Definicija. *Konika* je ravninska projektivna krivulja definirana polinomom stupnja 2, tj. krivulja definirana s

$$C/k : ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0, \text{ za neke } a, b, c, d, e, f \in k. \quad (2.1)$$

Sjetimo se da projektivna krivulja mora biti definirana polinomima stupnaj 2, pa su zato svi monomi stupnja 2.

Geometrijski, afin dio ove jednadžbe opisuje presjek konusa i ravnine. Linearnim promjenama koordinata, ove jednadžbe se mogu svesti na jedan od sljedeća tri oblika

$$ax^2 + by^2 = c, \ a, b > 0 \text{ - elipsa},$$
$$ax^2 - by^2 = c, \ a, b > 0 \text{ - hiperbola},$$
$$ax + by^2 = c \text{ - parabola},$$

gdje su $a, b, c \in \mathbb{Q}$.

Promotrimo broj točaka u beskonačnosti ovih (projektivne) krivulja. Elipsa ima 0 točaka u beskonačnosti nad $\mathbb{Q}$, te 2 nad $\mathbb{C}$. Parabola ima jednu točku u beskonačnosti i nad $\mathbb{Q}$ i nad $\mathbb{C}$. Hiperbola ima 2 točke u beskonačnosti nad $\mathbb{C}$ - to su $(1 : \pm\sqrt{\frac{a}{b}} : 0)$, te ovisno o tome je li $\sqrt{\frac{a}{b}}$ racionalan broj, ima 0 ili 2 točke u beskonačnosti nad $\mathbb{Q}$.

Kada ove jednadžbe imaju rješenja i kako izgledaju ta rješenja kada postoje.

Primjer 1. Promotrimo

$$T_1 : x^2 + y^2 = -1,$$
$$T_2 : x^2 + 3y^2 = 2,$$
$$T_3 : x^2 + y^2 = 1.$$

Promatramo $\mathbb{Q}$-racionalne točke na ovim krivuljama.

Očito vrijedi $T_1(\mathbb{Q}) = \emptyset$ jer je $T_1(\mathbb{R}) = \emptyset$.

Dokažimo sada da je $T_2(\mathbb{Q}) = \emptyset$. Pretpostavimo da postoje $x = \frac{u}{v}$ i $y = \frac{z}{v}$, gdje su $u, z, v \in \mathbb{Z}$, te su $(u, z) = 1$ i $(v, z) = 1$, koji zadovoljavaju ovu jednadžbu. Prvo primjetimo da moraju u i v biti relativno prosti, jer bi u suprotnom i z imao taj isti prosti faktor, te bi došli do kontradikcije.

Tada je $u^2 + 3v^2 = 2z^2$. Promatrajući jednadžbu modulo 3, imamo

$$u^2 \equiv 2z^2 \pmod 3,$$

što je moguće samo ako je $u \equiv z \equiv 0 \pmod 3$, što je kontradickija s tim da su u i z relativno prosti.

$T_3(\mathbb{Q})$ je očito neprazan, pa sada želimo opisati sva rješenja ove jednadžbe.

Uzmimo očitu točku $P = (-1, 0)$ i promotrimo pravac $x = 0$. Za svaku racionalnu točku na tom pravcu $P_t = (0, t)$, povucimo pravac $y = t(x + 1)$ kroz P i P_t. Sada rješavamo sustav jednadžbi

$$y = t(x + 1),$$
$$x^2 + y^2 = 1,$$

te dobijemo $x(x^2 + tx^2 + 2t) = 0$, tj.

$$x = \frac{-2t}{1 + t^2}, \quad y = \frac{1 - t^2}{1 + t^2}.$$

Lako se vidi da svakom izboru točke na kružnici (osim P) odgovara neka racionalna točka na pravcu $x = 0$. Obrnuto, svakoj vrijednosti t odgovara neka točka na kružnici.

Treba još samo riješiti problem s točkom P, to se napravi tako da se promatra projektivni pravac $xy = 0$, te tada točki P odgovara točka u beskonačnosti $(1 : 0)$. Dakle dobili smo da je kružnica izomorfna s $\mathbb{P}^1$ nad $\mathbb{Q}$.

Napomena. Još nismo definirali što to znači da "je C izomorfna nad k s projektivnim pravcem $\mathbb{P}^1$". To otprilike znači da postoje racionalna funkcije definirane u svim točkama s C u $\mathbb{P}^1$ koja ima inverz koji je također racionalna funkcija.

Isti postupak koji smo u prethodnom primjeru proveli za kružnicu, se može provesti za svaku koniku.

Teorem 1. *Neka je C/k geometrijski ireducibilna konika s k-racionalnom točkom i pretpostavimo da je* $\operatorname{char} k \neq 2$. *Tada je C izomorfna nad k s projektivnim pravcem $\mathbb{P}^1$.*

Ovaj teorem bi se mogao dokazati računski, međutim, mi ćemo ga kasnije dokazati algebarski.

Dakle, imali smo 2 slučaja, ili konika nema točaka, ili ih ima beskonačno mnogo, te ih sve možemo parametrizirati. Kako odrediti u kojoj smo situaciji? Očito ako nema točaka "mod p^n" ili ako nema točaka u $\mathbb{R}$, tada konika neće imati ni točaka nad $\mathbb{Q}$. Ono pto vrijedi je i obrat ove tvrdnje, da ako ima točaka "mod p^n" (preciznije ćemo definirati ovu tvrdnju uskoro) za sve p i ima točaka nad $\mathbb{R}$, tada ima točaka i nad $\mathbb{Q}$.

Poglavlje 3

p-adski brojevi

3.1 Inverzni limes

Definicija. *Inverzni sistem* je niz objekata (npr. skupova/grupa/prstena) (A_n) skupa sa nizom morfizmama (npr. funkcija/homomorfizama) (f_n)

$$\cdots \to A_{n+1} \xrightarrow{f_n} A_n \to \cdots \xrightarrow{f_2} A_2 \xrightarrow{f_1} A_1.$$

Definicija. *Inverzni limes* $A = \varprojlim A_n$ inverznog sistema skupova (A_n), (f_n) definiranog kao gore je skup A čiji elementi su besklonačni nizovi (a_n), gdje je $a_n \in A_n$ za svaki $n \geq 0$, te koji zadovoljavaju $f_n(a_{n+1}) = a_n$ za svaki $n \geq 0$.

Napomena. Ako su A_n grupe i f_n su homomorfizmi grupa, tada je inverzni limes također grupa. Ako su A_n prsteni i f_n homomorfizmi prstenova, tada je A_n prsten.

3.2 Prsten cijelih p-adskih brojeva

Definicija. Neka je p fiksan prost broj. *Prsten cijelih p-adskih brojeva* $\mathbb{Z}_p$ je inverzni limes

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

inverznog sistema prstenova $(\mathbb{Z}/p^n\mathbb{Z})$ s homomorfizmima prstenova (f_n), gdje je f_n redukcija modulo p^n.

Napomena. Multiplikativna jedinica u prstenu je $1 = (\overline{1}, \overline{1}, \ldots)$, gdje je n-ta $\overline{1}$ označava $1 + p^n\mathbb{Z}$. Preslikavanje koje šalje $x \in \mathbb{Z}$ u $(\overline{x}, \overline{x}, \ldots)$, je homomorfizam prstenova koji očito ima trivijalnu jezgru. Dakle vidimo da se $\mathbb{Z}$ ulaže u $\mathbb{Z}_p$, pa vidimo da $\mathbb{Z}_p$ ima karakteristiku 0, te možemo smatrati $\mathbb{Z}$ potprstenom od $\mathbb{Z}_p$. Međutim, prsten $\mathbb{Z}_p$ je puno veći od $\mathbb{Z}$.

Elemente prstena $\mathbb{Z}_p$ ćemo neformalno pisati kao nizove $(a_1, a_2, \ldots)$, gdje cijeli broj $a_i \in [0, p^i - 1]$ reprezntira $1 + p^i\mathbb{Z}$.

Primjer 2. U $\mathbb{Z}_7$ imamo

$$\begin{aligned}
2 &= (2,2,2,2,2\ldots),\\
2002 &= (0,42,287,2002,2002,\ldots),\\
-2 &= (5,47,341,23999,16805,\ldots),\\
\frac{1}{2} &= (4,25,172,1201,8304,\ldots),\\
\sqrt{2} &= \begin{cases}(3,10,108,2166,4567,\ldots)\\(4,39,235,235,12240,\ldots)\end{cases}\\
\sqrt[5]{2} &= (4,46,95,1124,15530,\ldots)
\end{aligned}$$

Zadatak 1. Dokažite da postoji $\sqrt[p]{2}$ u $\mathbb{Z}_7$ za svaki $p > 7$.

Definicija. Sjetimo se da je niz homomorfizama grupa *egzaktan* ako je za svaku grupu u nizu slika ulaznog homomorfizma jednaka jezgri izlaznog homomorfizma. Za *kratki egzaktan niz*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0,$$

to znači da je f injektivan, g surjektivan, te da je $\operatorname{im} f = \ker g$. Po prvom teoremu o izomorfizmu grupa, također vrijedi $B/\operatorname{im} f \simeq C$.

Propozicija 2. *Za svaki cijeli broj m, niz*

$$0 \to \mathbb{Z}_p \xrightarrow{[p^m]} \mathbb{Z}_p \xrightarrow{\pi_m} \mathbb{Z}/p^m\mathbb{Z} \to 0$$

je egzaktan, gdje je $[p^m]$ množenje s p^m, te je π_m projekcija na $\mathbb{Z}/p^m\mathbb{Z}$, tj. preslikavanje koje šalje niz (a_n) u a_m.

Dokaz. Dokažimo prvo da je množenje s p u $\mathbb{Z}_p$ injektivno. Pretpostavimo suprotno, tj. da je $a = (a_n)$ u jezgri. Tada je $pa = 0$, pa je $pa_n = 0$ za svaki n. Posebno, $pa_{n+1} = 0$ u $\mathbb{Z}/p^{n+1}\mathbb{Z}$. To sada znači da je $a_{n+1} = p^n y_{n+1}$ u $\mathbb{Z}/p^{n+1}\mathbb{Z}$ za neki $y_{n+1} \in \mathbb{Z}/p^{n+1}\mathbb{Z}$. Sada slijedi da je $a_n = f(a_{n+1}) = p^n f(y_{n+1}) = 0$ u $\mathbb{Z}/p^n\mathbb{Z}$. Kako ovo vrijedi za sve n, slijedi $a = 0$.

Egzaktnost s lijeva: Pošto je množenje s p injektivno, vrijedi da je kompozicija tog preslikavanja sa samim sobom m puta (tj. množenje s p^m) injektivno.

Egzaktnost s desna: Zapišimo $\beta \in \mathbb{Z}/p^m\mathbb{Z}$ kao $b + p^m\mathbb{Z}$. Tada će π_m preslikati element $(b,b,b,b,\ldots)$ u β.

Egzaktnost u sredini: Ako je $a \in \mathbb{Z}_p$, tada je $\pi_m(p^m a) = p^m \pi_m(a) = 0$ u $\mathbb{Z}/p^m\mathbb{Z}$. Dakle slika ulaznog preslikavanja je u jezgri izlaznog preslikavanja. Dokažimo suprotnu inkluziju. Neka je $a = (a_n)$ u jezgri od π_m. Dakle vrijedi da je $a_m = 0$. Dakle za svaki $n \geq m$, imamo $a_n \in p^m\mathbb{Z}/p^n\mathbb{Z}$. Dakle postoji jedinstveni b_{n-m} koji se preslikava u a_n pod djelovanjem izomorfizma

$$\mathbb{Z}/p^{n-m}\mathbb{Z} \xrightarrow{p^m} p^m\mathbb{Z}/p^n\mathbb{Z}.$$

Niz tih b_{n-m}-ova je kompatibilan, pošto su a_n-ovi kompatibilni, te postoji element $b = (b_n)$ takav da je $p^m b = a$, dakle a je u slici od množenja s p^m.

□

Korolar 3. *Za svaki prirodan broj m vrijedi $\mathbb{Z}_p/p^m\mathbb{Z}_p \simeq \mathbb{Z}/p^m\mathbb{Z}$.*

Propozicija 4. *Element $x \in \mathbb{Z}_p$ je invertibilan ako i samo ako $x \notin p\mathbb{Z}_p$. Drugim rječima, $\mathbb{Z}_p^\times$ je $\mathbb{Z}_p \backslash p\mathbb{Z}_p$.*

Dokaz. Ako je $a = (a_n) \in \mathbb{Z}_p$ djeljiv s p, tada je $a_1 = 0$, pa a očito ne može biti invertibilan. Ako a nije djeljiv s p tada za svaki n vrijedi $a_n = b_n + p^n\mathbb{Z}$ za neki $b_n \in \mathbb{Z}$, te taj b_n nije djeljiv s p. Slijedi da a_n ima inverz c_n u $\mathbb{Z}/p^n\mathbb{Z}$ Također, niz (c_n) mora biti kompatibilan, te je $c = (c_n)$ inverz od a. □

Propozicija 5. *Svaki elemnt $x \in \mathbb{Z}_p$ se može na jedinstven način zapisati kao $p^n u$, gdje je $u \in \mathbb{Z}_p^\times$.*

Dokaz. Postojanje zapisa: Ako je $0 \neq a = (a_n)$, tada postoji najveći n takav da je $a_n = 0$. Za taj n, po Propoziciji 2 vrijedi $a = p^n u$ za neki $u \in \mathbb{Z}_p$. Štoviše, u ne može biti djeljiv s p, pošto bi tada bilo $u_{n+1} = 0$, pa je po prethodnoj propoziciji u invertibilan.

Jedinstvenost zapisa: Pretpostavimo $p^n u_1 = p^m u_2$. Ako je $m = n$, tada zbog injektivnosti množenja s p^m imamo $u_1 = u_2$. U suprotnom možemo BSO pretpostaviti da je $n > m$. Tada je $u_2 = p^{n-m} u_2$ invertibilan, što je kontradikcija s prethodnom propozicijom. □

Korolar 6. *Prsten $\mathbb{Z}_p$ je integralna domena.*

Dokaz. Množenjem dva ne-nul elementa $p^n u_1$ i $p_m u_2$ dobivamo $p^{n+m} u_1 u_2$, čija je $(n + m + 1)$-ta komponenta različita od nule. □

Definicija. Neka je $a = (a_n) \in \mathbb{Z}_p$, gdje je po običaju a_n cijeli broj iz $[0, p^n - 1]$. Niz $(b_0, b_1, \ldots)$ za kojeg vrijedi $b_0 = a_1$ i $b_n = (a_{n+1} - a_n)/p^n$ se zove p-adska ekspanzija od a.

Dakle svaki $a \in \mathbb{Z}_p$ se može zapisati kao formalni red

$$a = \sum_{i=0}^{\infty} b_i p^i.$$

Iz defincije odmah slijedi:

Propozicija 7. *Svaki element u $\mathbb{Z}_p$ ima jedinstvenu p-adsku ekspanziju i svaki niz $(b_0, b_1, \ldots)$, gdje je $b_i \in [0, p-1]$ je p-adska ekspanzija nekog elementa iz $\mathbb{Z}_p$.*

Dakle postoji bijekcija između $\mathbb{Z}_p$ i nizova cijelih brojeva s elementima iz $[0, p-1]$.

Definicija. Za svaki $0 \neq a \in \mathbb{Z}_p$, *p-adska valuacija* od a, s oznakom $v_p(a)$ je najveći cijeli broj m za koji je a u $p^m\mathbb{Z}_p$. Ekvivalentno $v_p(a)$ je za $a = \sum_{i=0}^{\infty} b_i p^i$ najmanji prirodan broj m takav da je $b_m \neq 0$. Također ekivivalentno, ako zapišemo $a = p^m u$, gdje je $u \in \mathbb{Z}_p^\times$ tada je $v_p(a) = m$. Definiramo $v_p(0) = +\infty$.

Propozicija 8. *Svaki ne-nul ideal u $\mathbb{Z}_p$ je oblika (p^m) za neki prirodan broj m.*

Dokaz. Neka je I ne-nul ideal u $\mathbb{Z}_p$ i neka je $m = inf\{v_p(a) : a \in I\}$. Pošto je $I \neq (0)$, tada je $m < \infty$, te za svaki $a \in I$ vrijedi $a \in p^m\mathbb{Z}_p = (p^m)$. S druge strane, postoji $a \in I$ takav da je $a = p^m u$. Slijedi da je $u^{-1}a = p^m \in I$, iz čega slijedi da je $(p^m) \subset I$. □

Korolar 9. *Prsten $\mathbb{Z}_p$ je domena glavnih ideala (a time i prsten jedinstvene faktorizacije) s jedinstvenim prostim idealom (p) (te jednim prostim elementom p).*

Propozicija 10. *Uz konvenciju da je $n+\infty = \infty$ za svaki cijeli broj n, p-adska valuacija zadovoljava sljedeća svojstva:*

1. *$v_p(a) = \infty$ ako i samo ako je $a = 0$.*
2. *$v_p(ab) = v_p(a) + v_p(b)$.*
3. *$v_p(a + b) \geq \min(v_p(a), v_p(b))$.*

Dokaz. Prvo svojstvo slijedi iz definicije. Drugo i treće svojstvo su očito zadovoljena ako su a ili b jednaki 0. Pretpostavimo $a, b \neq 0$. Neka je $v_p(a) = m$ i $v_p(b) = n$.

Da bi dokazali drugu tvrdnju zapišimo $a = p^m u_1$ i $b = p^n u_2$, gdje su $u_1, u_2 \in \mathbb{Z}_p^\times$. Tada je $ab = p^{m+n}u_1u_2$, pa je $v_p(ab) = m + n$.

U trećoj tvrdnji možemo BSO pretpostaviti da je $m \leq n$. Slijedi da je $p^n\mathbb{Z}_p \subseteq p^m\mathbb{Z}_p$, pa su i $a, b \in p^m\mathbb{Z}_p$, iz čega slijedi da je $a + b \in p^m\mathbb{Z}_p$, te je $v_p(a + b) \geq \min(v_p(a), v_p(b))$.

□

p-adska valuacija je primjer *diskretne valuacije*.

Definicija. Neka je R komutativni prsten. *Diskretna valuacija* (na R) je funkcija $v : R \to \mathbb{Z} \cup \{\infty\}$ koja zadovoljava svojstva iz propozicije 10.

Definicija. *Prsten diskretne valuacije* je domena glavnih ideala koja sadrži jedinstveni maksimalan ideal, te nije polje.

Možda je ova definicija na prvi pogled neobična, pošto se ne spominje valuacija, međutim za svaki prsten diskretne valuacije se može na analogan način definirati diskretna valuacija.

Prsten diskretne valuacije je "najbliže" što komutativni prsten može biti polje, a bez da zaista je polje.

3.3 Polje p-adskih brojeva

Sjetimo da se polje razlomaka nekog prstena R definira kao skup uređenih parova $(a, b) \in R^2$, koji se obično zapisuje kao a/b gdje vrijedi da je $a/b \sim c/d$ kad god je $ad = bc$.

Definicija. *Polje p-adskih brojeva* $\mathbb{Q}_p$ je polje razlomaka od $\mathbb{Z}_p$.

Pošto je $a \in \mathbb{Q}_p$ po definiciji $a = (p^m u_1)/(p^n u_2) = p^{m-n} u_1 u_2^{-1}$, možemo svaki element iz $\mathbb{Q}_p$ zapisati kao up^k za $u \in \mathbb{Z}_p^\times,\ k \in \mathbb{Z}$. Sada možemo proširiti definiciju od v_p na $\mathbb{Q}_p$ tako da za $a = up^k$, $u \in \mathbb{Z}_p^\times,\ k \in \mathbb{Z}$ vrijedi $v_p(up^k) = k$, te je kao i prije $v_p(0) := +\infty$.

Napomena. Primjetimo da sada možemo $\mathbb{Z}_p$ identificirati kao podskup od $\mathbb{Q}_p$ sa elementima ne-negativne valuacije, te $\mathbb{Z}_p^\times$ možemo definirati kao podskup $\mathbb{Q}_p$ elemenata s valuacijom 0.

Vrijedi $\mathbb{Q} \subset \mathbb{Q}_p$, te vrijedi za svaki $x \in \mathbb{Q}_p$ je ili $x \in \mathbb{Z}_p$ ili je $x^{-1} \in \mathbb{Z}_p$.

Ovo je jedan od dva načina definiranja polja $\mathbb{Q}_p$. Promotrimo sada drugi način, preko apsolutnih vrijednosti.

3.4 Apsolutne vrijednosti

Definicija. Neka je k polje. *Apsolutna vrijednost* na k je funkcija $\|\| : k \to \mathbb{R}_{\geq 0}$ sa sljedećim svojstvima:

(1) $\|x\| = 0$ ako i samo ako je $x = 0$,

(2) $\|xy\| = \|x\| \cdot \|y\|$.

(3) $\|x + y\| \leq \|x\| + \|y\|$.

Absloutne vrijednosti se nekada nazivaju i "norme", ali mi 'cemo koristiti izraz norme za nešto drugo, te ćemo koristiti naziv "apsolutna vrijednost" kako bi izbjegli zabunu.

Neke norme zadovoljavaju jače svojstvno

(3') $\|x + y\| \leq \max\{\|x\|, \|y\|\}$.

se zovu *nearhimedske* apsolutne vrijednosti, a one koje ne zadovoljavaju se zovu *arhimedske*.

Definicija. Definiramo p-adsku apsolutnu vrijednost $|\ |_p$ na $\mathbb{Q}_p$ s

$$|x|_p = p^{-v_p(x)}.$$

Napomena. Primjetimo da pošto je $\mathbb{Q} \subset \mathbb{Q}_p$, ovo daje definiciju apsolutne vrijednosti $|\ |_p$ na $\mathbb{Q}$. Spomenuti alternativni način definicije od $\mathbb{Q}_p$ je da definiramo $\mathbb{Q}_p$ kao upotpunjenje od $\mathbb{Q}$ (tj. $\mathbb{Q}$ skupa s svim limesima nizova iz $\mathbb{Q}$) s obzirom

na apsolutnu vrijednost $|\ |_p$. Dosta knjiga definira $\mathbb{Q}_p$ upravo na ovaj način. Tada se $\mathbb{Z}_p$ definira kao

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\},$$

ili kao upotpunjenje od $\mathbb{Z}$ s obzirom na $|\ |_p$.

Napomena. Naziv *prsten cijelih brojeva* u $\mathbb{Q}_p$ može biti zbunjujuć. Naime, $\mathbb{Z}_p$ *nije* integralno zatvorenje od $\mathbb{Z}$ u $\mathbb{Q}_p$. To možemo vidjeti promatranjem karidnaliteta tih skupova. Integralno zatvorenje od $\mathbb{Z}$ u $\mathbb{Q}_p$ je prebrojiv skup, (pošto postoj prebrojivo mnogo polinoma s cjelobrojnim koeficijentima) dok je $\mathbb{Z}_p$ očito neprebrojiv skup. Međutim, istina je da je $\mathbb{Z}_p$ integralno zatvoren u $\mathbb{Q}_p$, te $\mathbb{Z}_p$ sadrži integralno zatvorenje od $\mathbb{Z}$ u $\mathbb{Q}$.

Definicija. Dvije apsolutne vrijednosti $\|\ \|$ i $\|\ \|'$ na polju k su ekvivalentne ako postoji $\alpha \in \mathbb{R}$ takav da je

$$\|x\|' = \|x\|^\alpha$$

za svaki $x \in k$.

Sljedeći teorem, koji nećemo dokazivati, nam govori koje su sve apsolutne vrijednosti, do na ekvivalenciju, na $\mathbb{Q}$. Označimo s $|\ |_\infty$ uobičajenu apsolutnu vrijednost.

Općenito u p-adskoj apsolutnoj vriejdnosti, "mali" su brojevi koji su djeljivi velikim potencijama broja p.

Teorem 11 (Ostrowski)**.** *Svaka ne-trivijalna apsolutna vrijednost na $\mathbb{Q}$ je ekvivalentna s $|\ |_p$ za neki prost broj p ili $|\ |_\infty$.*

Na $\mathbb{Z}_p$ i $\mathbb{Q}_p$ se može definirati *p-adska topologija* preko apsolutne vrijednosti. U p-adskim brojevima su $a, b \in \mathbb{Q}$, promatrani kao elementi od $\mathbb{Q}_p$ "blizu", ako je u brojniku od $a-b$ velika potencija od p. Npr niz $2, 4, 8, 16, 32, \ldots$ konvergira u 0 u $\mathbb{Z}_2$.

p-adska analiza nam je često vrlo korisna, međutim trebamo biti vrlo pažljivi s intuicijom kada radimo s p-adskim brojevima.

Primjer 3. Neka su $b, c \in \mathbb{Q}$, te neka je p prost broj. Tada postoji niz racionalnih brojeva a_i koji konvergira u b u standardnoj (realnoj) topologiji, te konvergira u c u p-adskoj topologiji. Dokažimo ovu tvrdnju. Neka je

$$d_n = \frac{p^n}{p^n+1} \quad e_n = \frac{1}{p^n+1}.$$

U standardnoj topologiji d_n konvergir au 1, a e_n konvergira u 0, dok u p-adskoj topologiji d_n konvergira u 0, a $e_n = 1 - \frac{p^n}{p^n+1}$ kovergira u 1. Dakle vidimo da će niz $(a_n) = (bd_n + ce_n)$ konvergirati u b u standardnoj toppologiji, te u c u p-adskoj.

Prikažimo sada jednu primjenu p-adskih brojeva i jednostavne p-adske analize.

Primjer 4. Peromtrimo razvoj ;

$$(1+t)^{\frac{1}{6}} = 1 + \frac{1}{6}t - \frac{5}{2^2 3^2}t^2 + \frac{55}{2^4 3^4}t^3 - \frac{935}{2^7 3^5}t^4 + \dots.$$

Vidimo da se u nazivnicima nalaze samo potencije od 2 i 3, tj. prostih djelitelja od 6. Tvrdimo da, za $a \in \mathbb{Q}$, $k \in \mathbb{N}$, se u nazivniku od

$$\binom{a}{k} = \frac{a(a-1)(a-2)\dots(a-k+1))}{k!}$$

nalaze samo potencije prostih projeva koje dijele nazivnik od a.

Dokažimo tvrdnju obratom po kontrapoziciji: ako p ne dijeli nazivnik od a, tada p ne dijeli nazivnik od $\binom{a}{k}$. Pošto a nema faktore od p u nazivniku, tada je $a \in \mathbb{Z}_p$. Dakle, zaključujemo da je $a = (a_n)$ limes niza (b_n), gdje je $b_n \in \mathbb{Z}$, npr. uzmimo da je b_i i-ti član p-adske ekspanzije $b_i = \sum_{k=0}^{i} a_k p^k$. Općenitije $\mathbb{Z}_p$ je upotpunjenje od $\mathbb{Z}$ u p-adskoj topologiji, pa ova tvrdnja vrijedi za svaki $r \in \mathbb{Z}_p$.

S druge strane, polinomijalna funkcija $x \mapsto \binom{x}{k} \in \mathbb{Q}[x]$ je neprekidna u p-adskoj topologiji, pa zbog $a = \lim_{i\to\infty} b_i$, imamo

$$\binom{a}{k} = \lim_{i\to\infty} \binom{b_i}{k}.$$

Pošto je $b_i \in \mathbb{Z}$, slijedi da je $\binom{b_i}{k} \in \mathbb{Z}$. Pošto je $\binom{a}{k}$ limes elemenata iz $\mathbb{Z}$, slijedi da je $\binom{a}{k} \in \mathbb{Z}_p$, tj. p ne dijeli nazivnik od $\binom{a}{k}$.

3.5 Rješenja polinomijalnih jednadžbi

Lema 12. *Neka je (S_n) inverzni sistem konačnih nepraznih skupova s kompatibilnim preslikavanjem $f_n : S_{n+1} \to S_n$. Tada je $\varprojlim S_n$ neprazan.*

Dokaz. Ako su svi f_n surjektivni, tada lako konstuiramo element (s_n): izaberemo bilo koji $s_1 \in S_1$, te za $n \geq 1$ izaberemo $s_{n+1} \in f_n^{-1}(s_n)$. sada nam je cilj opći slučaj reducirati na ovaj.

Neka je $T_{n,n} = S_n$ i za $m > n$ neka je $T_{m,n}$ slika od S_m u S_n, tj.

$$T_{m,n} = f_n(f_{n+1}(\cdots f_{m-1}(S_m)\cdots)).$$

Tada za svaki n imamo niz inkluzija

$$\cdots, \subseteq T_{m,n} \subseteq T_{m-1,n} \subseteq \cdots T_{n,n} \subseteq S_n.$$

Svaki $T_{m,n}$ je konačan neprazan skup, pa slijedi da je za sve osim konačno mnogo inkluzija, ta inkluzija zapravo jednakost. Dakle za svaki n, je $E_n = \cap_m T_{m,n}$ neprazan podskup od S_n. Restringirajući prselikavanje f_n tako da definira preslikavanje $E_{n+1} \to E_n$ dobivamo inverzni sistem (E_n) nepraznih skupova takvih da su sva preslikavanja surjekcija, kao što smo i htjeli. □

Propozicija 13. *Neka je $f \in \mathbb{Z}_p[x]$. Tada su sljedeće tvrdnje ekvivalentne:*

(1) Jednadžba $f(x) = 0$ ima rješenja u $\mathbb{Z}_p$.

(2) Jednadžba $f(x) = 0$ ima rješenja u $\mathbb{Z}/p^n\mathbb{Z}$ za svaki $n \in \mathbb{N}$

Dokaz. Neka je S_n skup rješenja u $\mathbb{Z}/p^n\mathbb{Z}$. Tada je $\varprojlim S_n \subseteq \varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$ skup rješenja u $\mathbb{Z}_p$. Sada imamo $\varprojlim S_n \neq \emptyset$ ako i samo ako su svi S_n neprazni po Lemi 12. □

Henselova lema će nam reći da je nešto što je "blizu" rješenja polinomijalne jednadžbe može "popraviti" do egzaktnog rješenja.

Teorem 14 (Henselova lema)**.** *Neka je $f_p \in \mathbb{Z}_p[x]$. Pretpostavimo da je $f(a) \equiv 0 \pmod{p}$ i $f'(a) \not\equiv 0 \pmod{p}$. Tada postoji jedinstveni $b \in \mathbb{Z}_p$, $b \equiv a \pmod{b}$ takav da je $f(b) = 0$.*

Dokaz. Neka $a_1 = a$ i definiramo za $n \geq 1$

$$a_{n+1} = a_n - f(a_n)/f'(a_n).$$

Dokazujemo indukcijom da za svaki $n \geq 1$ vrijedi

$$f'(a_n) \not\equiv 0 \pmod{p}, \tag{3.1}$$

$$f(a_n) \equiv 0 \pmod{p^n}. \tag{3.2}$$

Primjetimo da (3.1) osigurava da je $f'(a_n) \in \mathbb{Z}_p^\times$, pa je a_{n+1} dobro definiran element iz $\mathbb{Z}_p$. Definicija od a_{n+1} skupa s (3.1) i (3.2) osiguravaju da je $a_{n+1} \equiv a_n \pmod{p^n}$, što znači da niz $(a_n \mod p^n)$ definira element $b \in \mathbb{Z}_p$ za koji vrijedi $f(b) = 0$ i $b \equiv a_1 \equiv a \pmod{p}$.

Za $n = 1$ tvrdnja očito vrijedi, pa pretpostavimo da (3.1) i (3.2) vrijede za a_n. Tada $a_{n+1} \equiv a_n \pmod{p^n}$, pa je $f'(a_{n+1}) \equiv f'(a_n) \not\equiv 0 \pmod{p}$. Dakle (3.1) je zadovoljen za sve $n \in \mathbb{N}$. Da bi pokazali (3.2), napravimo Taylorov razvoj od f oko a_n:

$$f(x) = f(a_n) + f'(a_n)(x - a_n) + (x - a_n)^2 g(x),$$

za neki $g(x) \in \mathbb{Z}_p[x]$. Uvrštavajući $x = a_{n+1}$, dobivamo

$$f(a_{n+1}) = f(a_n) + f'(a_n)(a_{n+1} - a_n) + (a_{n+1} - a_n)^2 g(a_n + 1).$$

Iz definicije a_{n+1} imamo $f'(a_n)(a_{n+1} - a_n) = -f(a_n)$, pa je

$$f(a_{n+1}) = (a_{n+1} - a_n)^2 g(a_{n+1}).$$

Pošto je $a_{n+1} \equiv a_n \pmod{p^n}$, slijedi da je $f(a_{n+1}) \equiv 0 \pmod{p^{n+1}}$, pa (3.2) vrijedi za a_{n+1}.

Pošto $f(x) = 0$ ima jedinstveno rješenje u $\mathbb{Z}/p^n\mathbb{Z}$ konguentno s a modulo p (jer (3.1) povlači da je $f'(a_n) \not\equiv 0 \pmod{p^n}$, pa je a_n jednostruka nul-točka od $f \pmod{p}^n$.), slijedi da niz (a_n) definira jedinstveno rješenje u $\mathbb{Z}_p$. □

3.6 Stuktura od $\mathbb{Z}_p^\times$

Restrikcija projekcije $\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ na $\mathbb{Z}_p^\times$ definira surjektivni homomorfizam

$$\mathbb{Z}_p^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Jezgra ovog preslikavanja je $U_n := 1 + p^n\mathbb{Z}_p$. Dakle vrijedi

$$\mathbb{Z}_p^\times/U_n \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times,$$

pa je

$$\mathbb{Z}_p^\times \simeq \varprojlim(\mathbb{Z}_p^\times/U_n) \simeq \varprojlim(\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Primjetimo da je (U_n) padajući niz podgrupa od $\mathbb{Z}_p^\times$:

$$\cdots \subset U_3 \subset U_2 \subset U_1 \subset \mathbb{Z}_p^\times.$$

Lema 15. *Vrijedi:*

(1) $\mathbb{Z}_p^\times/U_1 \simeq (\mathbb{Z}/p\mathbb{Z})^\times$.

(2) $U_n/U_{n+1} \simeq \mathbb{Z}/p\mathbb{Z}$.

Dokaz. Prvu tvrdnju smo već dokazali. Za drugu, promotrimo preslikavanje

$$U_n \to \mathbb{Z}/p\mathbb{Z},$$
$$1 + p^n z \mapsto (z \bmod p).$$

To preslikavanje je surjekcija, te je jezgra U_{n+1}. □

Korolar 16. *Grupa U_1/U_n ima p^{n-1} elemenata.*

Propozicija 17. *Neka je μ_{p-1} skup rješenja jednadžbe $x^{p-1} = 1$ u $\mathbb{Z}_p^\times$. Tada je μ_{p-1} s opercaijom množenja grupa izomorfna s $(\mathbb{Z}/p\mathbb{Z})^\times$, te je $\mathbb{Z}_p^\times = U_1 \times \mu_{p-1}$.*

Dokaz. Skup μ_{p-1} je jezgra homomorfizam potenciranja na $(p-1)$-vu potenciju sa $\mathbb{Z}_p^\times$ u $\mathbb{Z}_p^\times$, pa je grupa. Neka je $f(x) = x^{p-1} - 1$. Po Malom Fermatovom teoremu, svaki element $\neq 0$ iz $\mathbb{Z}/p\mathbb{Z}$ je korijen ovog polinoma, te vrijedi $f'(x) \not\equiv 0 \pmod p$ za sve $x \in \{1, 2, \ldots, p-1\}$. Sada po Henselovoj lemi, za svaki $x \in \{1, 2, \ldots, p-1\}$ postoji jedinstveni $a \in \mathbb{Z}_p$ takav da je $f(a) = 0$. Također, ne postoji element is μ_{p-1} koji je kongruentan 0 modulo p. Slijedi da je redukcija modulo p izomorfizam $\mu_{p-1} \to (\mathbb{Z}/p\mathbb{Z})^\times$.

Primjetimo sada da je $U_1 \cap \mu_{p-1} = \{1\}$, pošto je 1 očito rješenje, a po Henselovoj lemi, rješenje kongruentno 1 mod p je jedinstveno. Također, vrijedi da je $U_1 \cdot \mu_{p-1} = \mathbb{Z}_p^\times$, pošto se bilo koji element $a \in \mathbb{Z}_p^\times$ može podijeliti s elementom iz μ_{p-1} koji je kongruentan s a modulo p da bi dobio element iz U_1. Slijedi da je direktan produkt $U_1 \times \mu_{p-1}$ izomorfan $\mathbb{Z}_p^\times$. □

Lema 18. *Neka je p prost broj. Ako je $p \neq 2$, neka je $n \geq 1$, a ako je $p = 2$, neka je $n \geq 2$. Ako je $x \in U_n \backslash U_{n+1}$, tada je $x^p = U_{n+1} \backslash U_{n+2}$.*

Dokaz. Neka je $x \in U_n \backslash U_{n+1}$, dakle $x = 1 + p^n k$, za neki k koji nije djeliv s p. Tada je

$$x^p = 1 + \binom{p}{1} kp^n + \binom{p}{2} k^2 p^{2n} + \cdots k^p p^{np} \equiv 1 + kp^{n+1} \pmod{p^{n+2}}.$$

Slijedi da je $x^p \in U_{n+1} \backslash U_{n+2}$. □

Propozicija 19. *Ako je $p \neq 2$, tada je $U_1 \simeq \mathbb{Z}_p$. Ako je $p = 2$, tada je $U_1 = \{\pm 1\} \times U_2$, te je $U_2 \simeq \mathbb{Z}_2$.*

Dokaz. Neka je prvo $p \neq 2$, te neka je $\alpha = 1 + p \in U_1 \backslash U_2$. Koristeći prethodnu lemu, zaključujemo da je $\alpha^{p^i} \in U_{i+1} \backslash U_{i+2}$. Neka je α_n slika od α u U_1/U_n. Tada je $\alpha_n^{p^{n-2}} \neq 1$, ali je $\alpha_n^{p^{n-1}} = 1$, pa onda α ima red točno p^{n-1}. Dakle U_1/U_n je ciklička grupa generirana s α. Slijedi da imamo izomorfizam inverznih sistema

$$\begin{array}{ccccccc} \cdots & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^{n-1}\mathbb{Z} & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & U_1/U_{n+1} & \longrightarrow & U_1/U_n & \longrightarrow & \cdots \end{array}$$

Nakon što primjetimo da je $\varprojlim(U_1/U_n) = U_1$, slijedi da je $U_1 \simeq \mathbb{Z}_p$.

Za $p = 2$, isti argument s izborom $\alpha = 1 + 4$ dokazuje da je $U_2 \simeq \mathbb{Z}_2$. Koristeći da $\{\pm 1\}$ i U_2 imaju trivijalan presjek (tj. $-1 \notin U_2$, te pošto njihov produkt generira U_1 (jer je $[U_1 : U_2] = 2$), slijedi da je $\{\pm 1\} \times U_2$. □

Teorem 20. *Vrijedi:*

(1) Grupa $\mathbb{Z}_p^\times$ je izomorfna s $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ za $p \neq 2$, te s $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ za $p = 2$.

(2) Grupa $\mathbb{Q}_p^\times$ je izomorfna s $\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ ako je $p \neq 2$, te s $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ ako je $p = 2$.

Dokaz. Tvrdnja (1) slijedi iz Propozicija 17 i 19.
Da bi dokazali (2), promotimo preslikavanje

$$\begin{aligned} \mathbb{Z} \times \mathbb{Z}_p^\times &\to \mathbb{Q}_p^\times \\ (n, u) &\mapsto p^n u, \end{aligned}$$

te primjetimo da je to izomorfizam grupa. Korištnjem (1), tvrdnja slijedi. □

Propozicija 21. *Za $p \neq 2$ i prirodan broj m postoji primtivni m-ti korijen iz jedinice u $\mathbb{Q}_p^\times$ (tj. element reda m) ako i samo ako $m|p-1$, te su u $\mathbb{Q}_2^\times$ elementi -1 i 1 jedini korijeni iz jedinice.*

Dokaz. Neka je prvo $p \neq 2$. Da postoje m-ti korijeni iz jedinice kada $m|p-1$ smo vidjeli u korolaru 17. S druge strane kada bi za $m \not| p-1$ postojao m-ti korijen iz jedinice ζ_m, tada bi $\mu_m = \{1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{n-1} q\}$ činili podgrupu reda m od $\mathbb{Z}_p^\times$, što je u kontradikciji s Teoremom 20, (2).

U $\mathbb{Z}_2$ je očito da su ± 1 korijeni iz jedinice. Iz strukture od $\mathbb{Z}_2^\times$ opisane u Teoremom 20, vidimo da su to jedini elementi konačnog reda u $\mathbb{Q}_2^\times$.

□

Korolar 22. *Neka su p i q različiti prosti brojevi. Tada polja $\mathbb{Q}_p$ i $\mathbb{Q}_q$ nisu izomorfna.*

Dokaz. Tvrdnja direktno slijedi iz prošle propozicije, pošto polja imaju korijene jedinice različitog reda. □

Napomena. Neka je p neparan. Tada će se element -1 nalaziti u podgrupi μ_{p-1}, koja je ciklička reda $p-1$, te je -1 reda 2. Element -1 će dakle biti kvadrat u $\mathbb{Q}_p^\times$ ako i samo ako u μ_{p-1} postoji element reda 4, tj. kada je $p \equiv 1 \pmod 4$.

3.7 Kvadrati u $\mathbb{Q}_p^\times$

3.7.1 Slučaj $p \neq 2$

Teorem 23. *Vrijedi:*

(1) Element $p^n u \in \mathbb{Q}_p^\times$ (s $n \in \mathbb{Z}$ i $u \in \mathbb{Z}_p^\times$) je kvadrat ako i samo ako je n paran i $u \mod p$ je kvadrat u $\mathbb{F}_p^\times$.

(2) Vrijedi $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

(3) Za svaki $c \in \mathbb{Z}_p^\times$ s $c \mod p \notin (\mathbb{F}_p^\times)$, slike od p i c generiraju $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.

Dokaz. (1) Zapisujući $\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{F}_p^\times \times \mathbb{Z}_p$. Primjetimo da je $2\mathbb{Z}_p = \mathbb{Z}_p$, pa je

$$(\mathbb{Q}_p^\times)^2 = p^{2\mathbb{Z}} \times (\mathbb{F}_p^\times)^2 \times \mathbb{Z}_p.$$

Dakle elemnt $p^n u$ je kvadrat ako i samo ako je n paran u $u \mod p \in (\mathbb{F}_p^\times)^2$.

(2) Koristeći sti zapisa kao u (1), imamo

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \times \{0\} \simeq (\mathbb{Z}/2\mathbb{Z})^2,$$

pošto je $[\mathbb{F}_p^\times : (\mathbb{F}_p^\times)^2] = 2$.

(3) Očito je da je slika od p generator od $p^{\mathbb{Z}}/p^{2\mathbb{Z}}$, te da je slika od c generator od $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$.

□

3.7.2 Slučaj $p = 2$

Teorem 24. *Vrijedi:*

(1) Element $2^n u \in \mathbb{Q}_2^\times$ (s $n \in \mathbb{Z}$ i $u \in \mathbb{Z}_2^\times$) je kvadrat ako i samo ako je n paran i $u \equiv 1 \mod 8$.

(2) Vrijedi $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^3$.

(3) Slike od $2, -1$ i 5 generiraju $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$.

Dokaz. (1) Zapišimo

$$\mathbb{Q}_2^\times \simeq 2^{\mathbb{Z}} \times \mathbb{Z}_2^\times \simeq 2^{\mathbb{Z}} \times U_1.$$

Dokažimo sada da je $U_1^2 \simeq U_3$. Da bi dokazali $U_1^2 \supseteq U_3$, moramo pokazati da za svaki $t \in \mathbb{Z}_2$ postoji $x \in \mathbb{Z}_2$ takav da je $(1+2x)^2 = 1 + 4x + 4x^2 = 8t + 1$, tj. da jednadžba $f(x) = x + x^2 - 2t = 0$ ima rješenje u $\mathbb{Z}_2$. Lako se vidi da je $f(1) \equiv 0 \pmod 2$, te da je $f'(1) \equiv 1 \pmod 2$, pa po Henselovoj lemi, ta jednadžba ima rješenje u $\mathbb{Z}_2$. S druge strane, vidimo da za $1 + 2x \in U_1$, $x \in \mathbb{Z}_2$ vrijedi da je $(1+2x)^2 = 1 + 4x + 4x^2$, a pošto je $x + x^2 \equiv 0 \pmod 2$ za sve $x \in \mathbb{Z}_2$, slijedi da je $x + x^2 \in 2\mathbb{Z}_2$, pa je i $(1+2x)^2 \in 1 + 8\mathbb{Z}_2 = U_3$.

Sada imamo da je $\mathbb{Q}_2^\times \simeq 2^{2\mathbb{Z}} \times U_3$, te slijedi da je element $2^n u \in \mathbb{Q}_2^\times$ kvadrat ako i samo ako je n paran i $u \equiv 1 \pmod 8$.

(2) Koristći (1) dobivamo

$$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times U_1/U_3.$$

Po korolaru 16 vrijedi da je U_1/U_3 grupa reda 4, te se lako provjeri da je svaki element u njoj reda 2.

(3) Očito je da je slika od 2 generator od $2^{\mathbb{Z}}/2^{2\mathbb{Z}}$, te se lako provjeri da slike od -1 i 5 generiraju U_1/U_3.

□

3.8 Dekompozicijska i inercijska grupa

Neka je K polje algebarskih brojeva, te neka je L/K konačno Galoisovo proširenje od K stupnja n. Neka je $\mathfrak{p}$ fiksan prost ideal od $\mathcal{O}_K$ i neka je njegova faktorizacija u $\mathcal{O}_L$

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e,$$

gdje svi $\mathfrak{P}_i$-ovi imaju isti stupanj inercije f. Sjetimo se da vrijedi $ref = n$, te da grupa $\mathrm{Gal}(L/K)$ djeluje na skup $\{\mathfrak{P}_1, \cdots, \mathfrak{P}_r\}$. To djelovanje je tranzitivno, tj. za svaki $\mathfrak{P}_i$ i $\mathfrak{P}_j$ postoji $\sigma \in \mathrm{Gal}(L/K)$ takav da je $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$.

Kada grupa djeluje na skup, tada se često promatra stabilizatorska podgrupa nekog elementa, tj. podgrupa elemenata u grupi koji trivijalno djeluje na taj element skupa.

Definicija. Uz notaciju kao i prije, definiramo *dekompozicijsku grupu* $D(\mathfrak{P}_i/\mathfrak{p})$ elementa $\mathfrak{P}_i$

$$D(\mathfrak{P}_i/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\} \leq \mathrm{Gal}(L/K).$$

Primjetimo sljedeće neka su $\mathfrak{P}_i$ i $\mathfrak{P}_j$ takvi da je $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Tada se lako provjeri da je

$$D(\mathfrak{P}_j/\mathfrak{p}) = \sigma D(\mathfrak{P}_i/\mathfrak{p})\sigma^{-1}.$$

Dakle sve dekompozicijske grupe su konjugirane. Pošto je $D(\mathfrak{P}_i)$ po definiciji stabilizatorska podgrupa elementa $\mathfrak{P}_i$, te je djelovanje grupe tranzitivno (tj. orbita od $\mathfrak{P}_i$ je duljine r), po teoremu o Orbiti i stabilizatoru da je

$$\#D(\mathfrak{P}_i/\mathfrak{p}) = n/r = ef.$$

Primjer 5. Promotrimo proširenje $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$; to je proširenje stupnja $\phi(15) = 8$, vrijedi $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q}) \simeq (\mathbb{Z}/15\mathbb{Z})^\times$. Elemente $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q})$ prikazujemo kao $\sigma_i(\zeta_{15}) = \zeta_{15}^i$, gdje je $i \in (\mathbb{Z}/15\mathbb{Z})^\times$. Također, vrijedi da je prsten cijelih brojeva u $\mathbb{Q}(\zeta_{15})$ jednak $\mathbb{Z}[\zeta_{15}]$.

Promotrimo faktorizaciju elemenata $2, 3, 5$ i 31 u $\mathbb{Z}(\zeta_{15})$. Neka su

$$\begin{aligned}
\mathfrak{p}_2 &= (2, \zeta_{15}^4 + \zeta_{15} + 1),\\
\mathfrak{p}_3 &= (3, \zeta_{15}^4 + \zeta_{15}^3 + \zeta_{15}^2 + \zeta_{15} + 1),\\
\mathfrak{p}_5 &= (5, \zeta_{15}^2 + \zeta_{15} + 1)\\
\mathfrak{p}_{31} &= (31, \zeta_{15} + 3)
\end{aligned}$$

Prikažimo u sljedećoj tablici vrijednosti r, e i f za navedene proste brojeve.

	r	e	f
$\mathfrak{p}_2$	2	1	4
$\mathfrak{p}_3$	1	2	4
$\mathfrak{p}_5$	1	4	2
$\mathfrak{p}_{31}$	8	1	1

Izračunajmo sada dekompozicijsku grupu svakog od ovih prostih elemenata. Očito je $D(\mathfrak{p}_3/3) = D(\mathfrak{p}_5/5) = \mathrm{Gal}(L/K)$, pošto su $\mathfrak{p}_3$ i $\mathfrak{p}_5$ jedini prosti brojevi iznad 3 i 5. Također, očito vrijedi $\#D(\mathfrak{p}_{31}/31) = n/r = 1$.

Dakle jedini zanimljivi slučaj je $D(\mathfrak{p}_2/2)$. To je grupa reda $ef = 4$. Promotrimo preslikavanje

$$\mathbb{Z}[\zeta_{15}] \to \mathbb{Z}[\zeta_{15}]/\mathfrak{p}_2 = \mathbb{F}_2[x]/(x^4 + x + 1),$$

koji šalje ζ_{15} u x. Vrijedi

$$\sigma_i((2, \zeta_{15}^4 + \zeta_{15} + 1)) = (2, \sigma(\zeta_{15}^4 + \zeta_{15} + 1)) = (2, \zeta_{15}^{4i} + \zeta_{15}^i + 1).$$

Zaključujemo da će σ biti u $D(\mathfrak{p}_2/2)$ ako i samo ako je $\zeta_{15}^{4i}+\zeta_{15}^{i}+1$ u $\mathfrak{p}_2$, ili ekvivalentno, da x^4+x+1 dijeli $x^{4i}+x+1$ u $\mathbb{F}_2[x]$. Sada eksplicitnim računom možemo provjeriti da je

$$D(\mathfrak{p}_2/2)=\{\sigma_1,\sigma_2,\sigma_4,\sigma_8\}.$$

Dekompozicijska grupa nam je važna jer fiksira polje ostataka. Neka je $\mathfrak{P}$ prost broj iznad $\mathfrak{p}$, te neka je $\sigma\in D(\mathfrak{P}/\mathfrak{p})$. Pošto je $\sigma(\mathfrak{P})=\mathfrak{P}$, slijedi da σ inducira automorfizam polja $\mathcal{O}_L/\mathfrak{P}$. Ovaj automorfizham svakako fiksira $\mathcal{O}_K/\mathfrak{p}$, te slijedi da smo dobili preslikavanje

$$D(\mathfrak{P}/\mathfrak{p})\to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})), \tag{3.3}$$

koje lako provjerimo da je homomorfizam.

Definicija. *Inercijska grupa* $I(\mathfrak{P}/\mathfrak{p})$ je jezgra preslikavanja (3.3), tj.

$$I(\mathfrak{P}/\mathfrak{p})=\ker\left(D(\mathfrak{P}/\mathfrak{p})\to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))\right).$$

Eksplicitnije, vrijedi da je

$$I(\mathfrak{P}/\mathfrak{p})=\{\sigma\in D(\mathfrak{P}/\mathfrak{p})|\sigma(\alpha)\equiv\alpha \pmod{\mathfrak{P}} \text{ za sve } \alpha\in\mathcal{O}_L\}.$$

Po definiciji inercijske grupe i prvom teoremu o izomorfizmu grupa, slijedi da je

$$D(\mathfrak{P}/\mathfrak{p})/I(\mathfrak{P}/\mathfrak{p})\simeq \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})).$$

Kao i za dekompozicijske grupe, inercijske grupe konjugiranih prostih idela su međusobno konjugirane, te se lako vidie da je $\#I(\mathfrak{P}/\mathfrak{p})=e$. Drugim riječima, inercijska grupa $I(\mathfrak{P}/\mathfrak{p})$ je trivijalna ako i samo ako je $\mathfrak{P}/\mathfrak{p}$ nerazgranat.

Primjer 6. Izračunajmo inercijske grupe iz prethodnog primjera. Očito su $I(\mathfrak{p}_2/2)$ i $I(\mathfrak{p}_{31}/31)$ trivijalne. Grupa $I(\mathfrak{p}_3/3)$ je reda 2. Promotrimo preslikavanje

$$\mathbb{Z}[\zeta_{15}]/\mathfrak{p}_3\simeq\mathbb{F}_3[x]/(x^4+x^3+x^2+x+1).$$

Element σ_i iz $D(\mathfrak{p}_3/3)$ će biti u $I(\mathfrak{p}_3/3)$ ako i samo ako je $\sigma_i(\zeta_{15})=\zeta_{15}$ pošto je očito $\sigma_i(1)=1$, a 1 i ζ_{15} su generatori od $\mathbb{Z}[\zeta_{15}]$, pa time i $\mathbb{Z}[\zeta_{15}]/\mathfrak{p}_3$. To je ekvivalentno da je

$$\sigma_i(x)=x^i\equiv x \pmod{x^4+x^3+x^2+x+1}.$$

Drugim rječima, pitamo se kada $x^4+x^3+x^2+x+1$ dijeli x^i-x. Vidimo da je to istina za $i=11$, te onda pošto je $I(\mathfrak{p}_3/3)$ grupa reda 2, zaključujemo da je

$$I(\mathfrak{p}_3/3)=\{\sigma_1,\sigma_{11}\}.$$

Analogno možemo izračunati

$$I(\mathfrak{p}_5/5)=\{\sigma_1,\sigma_4,\sigma_7,\sigma_{13}\}.$$

Definicija. Pretpostavimo da je $\mathrm{Gal}(L/K)$ Abelova. Definiramo *inercijsko polje* L^I od $\mathfrak{P}/\mathfrak{p}$ kao fiksno polje od $I(\mathfrak{P}/\mathfrak{p})$, te *dekompozicijsko polje* L^D od $\mathfrak{P}/\mathfrak{p}$ kao fiksno polje od $D(\mathfrak{P}/\mathfrak{p})$.

3.9 Proširenja od $\mathbb{Q}_p$

Vratimo se sada na lokalna polja.

Definicija. Neka je $K/\mathbb{Q}_p$ konačno proširenje polja $\mathbb{Q}_p$. Definiramo *prsten cijelih brojeva* $\mathcal{O}_K$ od K kao integralno zatvorneje od $\mathbb{Z}_p$ u K.

Sljedeća propozicije (koju ostavljamo bez dokaza), nam govore da postoji jedinstveno proširenje apsolutne vrijednosti i izgledaju takvi prsteni cijelih brojeva.

Propozicija 25. *Neka je K konačno proširenje od $\mathbb{Q}_p$. Tada postoji jedinstveno ne-arhimedska apsolutna vrijednost na K, koja proširuje p-adsku apsolutnu vrijednost na $\mathbb{Q}_p$.*

Tu apsolutnu vrijednost ćemo također označavati sa $|\cdot|_p$.

Propozicija 26. *Neka je K konačno proširenje od $\mathbb{Q}_p$. Tada je*

$$\mathcal{O}_K = \{x \in K : |x|_p \leq 1\}.$$

Za proširenja od $\mathbb{Q}_p$, kao i za $\mathbb{Q}_p$ vrijedi da imaju jedinstveni maksimalni ideal u svom prstenu cijelih.

Propozicija 27. *Neka je K konačno proširenje od $\mathbb{Q}_p$. Tada $\mathcal{O}_K$ ima jedinstveni maksimalni ideal M,*

$$M = \{x \in K : |x|_p < 1\}.$$

Dokaz. Tvrdnja slijedi odmah iz činjenice da se svaki neinvertibilni element iz $\mathcal{O}_K$ nalazi u M. □

Neka je sada L/K Galoisovo proširenje, $\sigma \in \mathrm{Gal}(L/K)$, gdje su L i K konačna proširenja od $\mathbb{Q}_p$, dakle L je polje cijepanja nekog polinoma iz $K[x]$. Neka je $\mathfrak{p}$ maksimalni ideal od K, a $\mathfrak{P}$ maksimalni ideal od L. Tada je očito $\sigma(\mathfrak{P}) = \mathfrak{P}$. Dakle σ inducira automorfizam od $\mathcal{O}_L/\mathfrak{P}$ koji fiksira $\mathcal{O}_K/\mathfrak{p}$ (lako se dokaže da je $\mathcal{O}_K/\mathfrak{p}$ izomorfno potpolju od $\mathcal{O}_L/\mathfrak{P}$), te nam time daje homomorfizam

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})). \tag{3.4}$$

Propozicija 28. *Preslikavanje* (3.4) *je surjekcija.*

Dokaz. Pošto je $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ konačno proširenje polja, slijedi da postoji primitivni element, tj. da je $\mathcal{O}_L/\mathfrak{P} \simeq (\mathcal{O}_K/\mathfrak{p})[a]$. Neka je $f(x)$ njegov minimalni polinom; slijedi da je minimalni polinom proširenja $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ jednak

$$f(x) = \prod_{s \in \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))} (x - s(a)).$$

Izaberimo $\alpha \in \mathcal{O}_L$ takvog da se preslikava u a pri redukciji $\mod \mathfrak{P}$. Neka je S podskup od $\mathrm{Gal}(L/K)$ takv da se svi konjugati od α pojavljuju točno jednom u skupu $\{\sigma(\alpha)|\alpha \in S\}$. Tada je minimalni polinom od α jednak

$$g(x) = \prod_{\sigma \in S} (x - \sigma(\alpha)).$$

Promotrimo redukciju $\overline{g}(x)$ od $g(x)$. Pošto je α korijen od $g(x)$, tada je i a korijen od $\overline{g}(x)$. Zaključujemo da $f(x)$, pošto je minimalni polinom od a, dijeli $\overline{g}(x)$ u $(\mathcal{O}_K/\mathfrak{p})[x]$. Isto vrijedi i za sve konjugate od a. To znači da za svaki $s \in \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ postoji $\sigma \in \mathrm{Gal}(L/K)$ takav da je $s(a) \equiv \sigma(a) \pmod{\mathfrak{P}}$. Pošto je a primitivni element proširenja, djelovanje $s : \mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}$ je u potpunosti određeno djelovanjem na a. Dakle, vidimo da σ inducira s, tj. s je slika od σ s obzirom na preslikavanje (3.4), te slijedi da je preslikavanje surjektivno. □

Definicija. *Inercijska podgrupa* $I(L/K)$ od $\mathrm{Gal}(L/K)$ je jezgra preslikavanja (3.4).

Drugim rječima, $I(L/K)$ je normalna podgrupa od $\mathrm{Gal}(L/K)$ koju možemo zapisati kao

$$I(L/K) = \{\sigma \in \mathrm{Gal}(L/K)|\sigma(\alpha) \equiv \alpha \text{ za sve } \alpha \in \mathcal{O}_L\}.$$

Iz definicije slijedi da je

$$\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})) \simeq \mathrm{Gal}(L/K)/I(L/K).$$

Definicija. Kažemo da je L/K *nerazgranato* proširenje ako je $I(L/K) = \{1\}$. Kažemo da je L/K *potpuno razgranato* ako je $I(L/K) = \mathrm{Gal}(L/K)$.

Vidimo da je po definiciji proširenje nerazgranato ako i samo ako je

$$\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})) \simeq \mathrm{Gal}(L/K).$$

Primjetimo da će nerazgranato proširenje onda biti uvijek cikličko, pošto je proširenje konačnih polja cikličko (generirano Frobeniusom). U takvoj situaciji ćemo generator od $\mathrm{Gal}(L/K)$ koji odgovara Frobeniusu u $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ također zvati Frobeniusom. Dakle, to je preslikavanje koje zadovoljava

$$\phi(\alpha) = \alpha^q \pmod{\mathfrak{P}},$$

za $q = \#(\mathcal{O}_L/\mathfrak{P})$ i za sve $\alpha \in \mathcal{O}_L$.

Sljedeću činjenicu nećemo dokazivati.

Teorem 29. *Neka je K konačno proširenje od $\mathbb{Q}_p$, neka je k polje ostataka od K, te neka je l/k neko konačno proširenje. Tada postoji jedinstveno nerazgranato proširenje L/K, takvo da je l polje ostataka od L.*

Promotirimo sada opći slučaj - neka je $I(L/K)$ inercijska podgrupa. Neka je K^{nr} fiksno polje od $I(L/K)$ vidimo da tada po Galoisovoj teoriji slijedi da je K^{nr}/K nerazgranato, a da je L/K^{nr} potpuno razgranato.

Sada pogledajmo kako primijeniti teoriju p-adskih polja na proširenja polja algebarskih brojeva. Na isti način na koji smo konstruirali $\mathbb{Z}_p$ i $\mathbb{Q}_p$ možemo za polje algebarskih brojeva i prosti ideal $\mathfrak{p}$ u $\mathcal{O}_K$ konstruirati

$$\mathcal{O}_{K,\mathfrak{p}} = \varprojlim \mathcal{O}_K/\mathfrak{p}^n,$$

te $K_\mathfrak{p}$ kao polje razlomaka od $\mathcal{O}_{K,\mathfrak{p}}$.

Definicija. Neka je $\mathfrak{p}$ jedinstveni maksimalni ideal u $\mathcal{O}_{K,\mathfrak{p}}$. Generator od π od $\mathfrak{p}$ se zove *uniformizator*.

Neka je L/K Galoisovo proširenja polja algebarskih brojeva, te neka je $\mathfrak{P}$ prost ideal u $\mathcal{O}_L$ iznad prostog ideala $\mathfrak{p}$ u $\mathcal{O}_K$. Može se dokazati da postoji prirodno ulaganje $\mathcal{O}_{K,\mathfrak{p}} \hookrightarrow \mathcal{O}_{L,\mathfrak{P}}$. Slijedi da postoji i ulaganje $K_\mathfrak{p} \hookrightarrow L_\mathfrak{P}$. Zapravo iz ove činjenice možemo vidjeti da su $K_\mathfrak{p}$ i $L_\mathfrak{P}$ poširenja od $\mathbb{Q}_p$. Vrijedi također da je $L_\mathfrak{P}/K_\mathfrak{p}$ također Galoisovo proširenje.

Odredimo sada $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$. Očito za svaki $\sigma \in \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$, možemo restringirati σ na L, te će σ fiksirati K, pa smo dobili element u $\mathrm{Gal}(L/K)$. Dakle dobili smo preslikavanje $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \to \mathrm{Gal}(L/K)$ za koje lako vidimo da je homomorfizam. Nadalje, pošto je $\sigma(\mathfrak{P}\mathcal{O}_{L,\mathfrak{P}}) = \mathfrak{P}\mathcal{O}_{L,\mathfrak{P}}$ (jer je $\mathfrak{P}\mathcal{O}_{L,\mathfrak{P}}$ jedini prost ideal u $\mathcal{O}_{L,\mathfrak{P}}$), vidimo da je slika takve σ zapravo u dekompozicijskokj grupi $D(\mathfrak{P}/\mathfrak{p})$. S druge strane za svaki $\sigma \in \mathrm{Gal}(L/K)$ koji je u $D(\mathfrak{P}/\mathfrak{p})$, vrijedi da je $\sigma(\mathfrak{P}^i) = \mathfrak{P}^i$. Zaključujemo da je σ automorfizam od $\mathcal{O}_L/\mathfrak{P}^i$, pa time i automorfizam od $\mathcal{O}_{L,\mathfrak{P}}$. Dakle, sada imamo homomorfizam $D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$.

Komponiranjem navedena dva preslikavanja

$$D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \to \mathrm{Gal}(L/K),$$

iz njihovih dfinincija vidimo da je $D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(L/K)$ prirodno ulaganje (identiteta), te iz toga slijedi da je

$$\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \to \mathrm{Gal}(L/K)$$

također injekcija sa slikom $D(\mathfrak{P}/\mathfrak{p})$. Dakle,

$$\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \simeq D(\mathfrak{P}/\mathfrak{p}).$$

Ova konstrukcija je vrlo korisna u Galoisovoj teorija polja algebarskih brojeva, jer nam dopušta da promatramo Galoisovu grupu proširenja tako da proučavamo "jedan po jedan" prost ideal.

3.10 Kvadratne forme i teorem Hasse-Minkowskog

Neka je u ovom poglavlju k polje karakteristike različite od 2.

Definicija. *Kvadratna forma* nad poljem k je homogeni polinom $q(x_1, \dots x_n) \in k[x_1, \dots, x_n]$ stupnja 2.

Primjer 7. Npr. $q(x, y) = 2x^2 + 5xy - 6y^2$ je kvadratna forma.

Kvadratna forma očito definira funkciju $q : V \to k$, gdje je $V = k^n$. Pošto $\#k > 2$, funkcija u potpunosti određuje kvadratnu formu, te ćemo funkciju i kvadratnu formu nadalje poistovjećivati.

Definicija. *Bilinearna forma* na vektorskom prostoru V nad k je funkcija $B : V \times V \to k$ za koju vrijedi

1. $B(v_1 + v_2, w) = B(v_1, w) + B(v_2, w)$, za sve $v_1, v_2, w \in V$,
2. $B(\lambda v, w) = \lambda B(v, w) = B(v, \lambda w)$, za sve $v, w \in V$, $\lambda \in k$,
3. $B(v, w_1 + w_2) = B(v, w_1) + B(v, w_2)$, za sve $v, w_1, w_2 \in V$.

Definicija. Bilinearna forma je *simetrična* ako je $B(v, w) = B(w, v)$ za sve $v, w \in V$.

Za sve vektorske prostore V, postoji bijekcija

$$\{\text{kvadratne forme na } V\} \longleftrightarrow \{\text{simetrične bilinearne forme na } V\}$$
$$q \mapsto B(x, y) := \frac{q(x + y) - q(x) - q(y)}{2}$$
$$q(x) := B(x, x) \hookleftarrow B.$$

Iz ovoga slijedi da kvadratnoj formi možemo pridružiti jedinstvenu simetričnu matricu A tako da vrijedi $q(x) = x^t Ax$ i $B(x, y) = x^t Ay$.

Definicija. *Rang* kvadratne forme q je rang pridružene simetričen matrice A.

Definicija. Kvadratna forma $q \in k[x_1, \dots, x_n]$ je *nedegenerirana* ako vrijedi bilo koji od sljedećih ekvivalentnih uvjeta:

- Asocirana matrica A je invertibilna.
- Za svaki $0 \neq x \in V$, linearno presliakvanje $y \to B(x, y)$ nije nul-presliakvanje.
- Rang on q je n.

Definicija. Dvije kvadratne forme $q(x_1, \dots, x_n)$ i $q'(x_1, \dots, x_n)$ su *ekvivalentne* nad k ako se raztlikuju za linearnu promjenu varijabli, tj. vrijedi $q'(x) = q(Tx)$ za neku invertibilnu matricu $T \in GL_n(k)$.

Primjer 8. Kvadratna forma $x^2 + y^2$ je ekvivalentna kvadratnoj formi $5x^2 + 5y^2$ nad $\mathbb{Q}$ jer je

$$5x^2 + 5y^2 = (2x + y)^2 + (x - 2y)^2,$$

te je matrica $A = \begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix}$ *invertibilna*. Međutim $x^2 + y^2$ i $3x^2 + 3y^2$ nisu ekvivalentne nad $\mathbb{Q}$.

Iz prethodnog primjera vidimo da nije trivijalno odrediti jesu li dane kvadratne forme ekvivalentne.

Propozicija 30. *Svaka kvadratna forma $q \in k[x_1, \ldots, x_n]$ nad k je ekvialentna nad k nekoj dijagonalnoj kvadratnoj formi*

$$a_1x_1^2 + a_2x_2^2 + \ldots a_nx_n^2.$$

Dokaz. Dokaz provodimo indukcijom po $\dim V$. Kada je $\dim V = 1$, tvrdnja očito sijedi. Ako je $q = 0$, tada također tvrdnja slijedi uz izbor $a_i = 0$ za sve i. U suprotnom, postoji $v \in V$ takav da je $q(v) \neq 0$. Pošto je $x \mapsto B(x, v)$ netrivijalno linearno preslikavanje vektorskih prostora $V \to k$, slijedi da je surjektivno, pa mu je jezgra $v^\perp := \{x \in V : B(x, v) = 0\}$ dimenzije $\dim V - 1$. Pošto $v \notin v^\perp$, siljedi da je $V \simeq kv \oplus v^\perp$. Ako je $y = y_1 + y_2$, gdje je $y_1 \in kv$ i $y_2 \in v^\perp$, slijedi da je $q(y) = q(y_1) + q(y_2) + 2B(y_1, y_2) = q(y_1) + q(y_2)$. Po pretpostavci indukcije, q se može dijagonailizirati na $v^\perp$ (dimenzije $\dim V - 1$), te je $q(x_1v)$ oblika $q(v)x_1^2$, gdje $q(v)$ možemo smatrati konstantom. □

Primjetimo da ako je q ekvivalentna s $a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2$, tada je rang od q jednak broju ne-nul a_i-ova.

Sada ćemo promatrati koji su brojevi u slici kvadratnih formi.

Definicija. Neka je q kvadrana forma na V i neka je $a \in k$. Kažemo da q reprezentira a ako postoji $0 \neq x \in V$ takav da je $q(x) = a$.

Uvjet da je $x \neq 0$ je bitan samo ako je $a = 0$ (jer bi u tomslučaju sve kvadratne forme reprezentirale 0), a to je upravo slučaj koji će mama biti posebno zanimljiv.

Primjer 9. Kvadratna forma $x^2 - 2y^2$ reprezentira -7 nad $\mathbb{Q}$, ali ne reprezentira 0.

Propozicija 31. *Ako nedegenerirana kvadratna forma reprezentira* 0*, tada reprezentira svaki element od k.*

Dokaz. Pretpostavimo da postoji $e \in V$ takav da $q(e) = 0$. Pošto je q nedegenerirana, postoji $f \in V$ takav da je $B(e, f) \neq 0$. Primjetimo da e i f moraju biti linearno nezavisini, jer bi u suprotnom bilo $B(e, f) = 0$. Sada imamo da je za $x, y \in k$

$$xyB(e, f) = B(xe, yf) = \frac{q(xe + yf) - q(xe) - q(yf)}{2} = \frac{q(xe + yf) - y^2q(f)}{2},$$

pa imamo da je $q(xe + yf) = axy + by^2$ za $a = 2B(e, f)$, te $b = q(f)$.

Neka je sada $c \in k$, te u jednadžbu

$$q(xe + yf) = axy + by^2 = (ax + by)y = c$$

uvrstimo $y = 1$, pa dobivamo $ax + b = c$, tj. $x = a^{-1}(c - b)$. □

Pri kraju dokazu vidimo da q reprezentira c već i na vektorskom potprostoru $\langle e, f\rangle$.

Sljedeći cilj nam je dokazati lokalno-globalni princip za kvadratne forme.

Teorem 32 (Hasse-Minkowski)**.** *Neka je $q \in \mathbb{Q}[x_1, \ldots, x_n]$ kvadratna forma nad $\mathbb{Q}$. Tada q reprezentira 0 nad $\mathbb{Q}$ ako i samo ako reprezentira 0 nad $\mathbb{Q}_p$ za sve $p \leq \infty$.*

Mi nećemo dokazati teorem u potpunosti, već ćemo ga samo dokazati kada je $n = 2$ i 3 (pošto će nam slučaj $n = 3$ odgovarati konikama). Napomenimo da je analogon gore navedenog oblika teorema (kojeg je u ovom obliku dokazao sam Minkowski) vrijedi i nad svim poljima algebarskih brojeva (generalizaciju je dokazao Hasse).

Evo još nekih varijanti teorema Hasse-Minkowski:

Teorem 33. *Za $a \in \mathbb{Q}$, kvadratna forma nad $\mathbb{Q}$ reprezentira a ako i samo ako reprezentira a nad $\mathbb{Q}_p$ za sve $p \leq \infty$.*

Teorem 34. *Dvije kvadratne forme nad $\mathbb{Q}$ su ekvivalentne ako i samo ako reprezentira a ako i samo ako su ekvivalentne nad $\mathbb{Q}_p$ za sve $p \leq \infty$.*

Poslejdica će biti i lokalno-globalni princip za konike.

Korolar 35. *Neka je X glatka geometrijski ireducibilna projektivna ravninska konika nad $\mathbb{Q}$. Tada je ekvivalentno:*

(i) X ima $\mathbb{Q}$-racionalnu točku.

(ii) X ima $\mathbb{Q}_p$-racionalnu točku za sve $p \leq \infty$.

(iii) $X \simeq \mathbb{P}^1(\mathbb{Q})$.

Dokaz. Ekvivalencija od (i) i (ii) slijedi iz teorema Hasse-Minkowski. Tvrdnja (i) slijedi trivijalno iz (iii), a (iii) se dokaže iz (i), na isti način na koji smo dokazali tvrdnju za kružnicu. □

Definicija. Kažemo da algebarska mnogostrukost X zadovoljava *lokalno-globalni princip* ili *Hasseov princip* ako vrijedi

$$X \text{ ima } \mathbb{Q}_p\text{-racionalnu točku za sve } p \leq \infty \Longrightarrow X \text{ ima } \mathbb{Q}\text{-racionalnu točku.}$$

Danas je tema od velikog interesa određivanje koje klase algebarskih mnogostrukosti zadovoljavaju lokalno-globalni princip.

Dokaz Hasse-Minkowski teorema za $n = 2, 3$. Prvo primjetimo da možemo pretpostaviti da je kvadratna forma zapisana u dijagonalnoj formi te da je prvi koeficijent $a_1 = 1$. Očito je da opstajanje $\mathbb{Q}$-točke povlači postojanje $\mathbb{Q}_p$-točke.

Slučaj $n = 2$:
Dakle promatramo $x^2 - ay^2$ za neki $a \in \mathbb{Q}$. Lako se vidi da ova kvadratna forma

reprezentira 0 ako i samo ako je $a \in \mathbb{Q}^{\times 2}$, tj. to želimo dokazati. Neka je $a \neq 0$. Pošto q reprezentira 0 nad $\mathbb{R}$, imamo da je $a > 0$. Zapišimo a kao

$$a = \prod_{p \text{ prost broj}} p^{n_p}.$$

Pošto q reprezentira 0 nad $\mathbb{Q}_p$, sve valuacije n_p moraju biti parne. Pošto ovo vrijedi za sve p, slijedi da je a kvadrat u $\mathbb{Q}$, pa q reprezentira 0 u $\mathbb{Q}$.

Slučaj $n = 3$:
Da bi dokazali ovaj slučaj, prvo će nam trebati sljedeća lema.

Lema 36. *Neka su $a, b \in k$, gdje je $\operatorname{char} k \neq 2$. Neka je $N : k(\sqrt{a}) \to k$ funkcija norme, tj. ako je a kvadrat u k tada je $N(x) = x$, te ako a nije kvadrat u k, tada je $N(x + y\sqrt{a}) = x^2 - ay^2$. Tada kvadratna forma $x^2 - ay^2 - bz^2$ reprezentira 0 nad k ako i samo ako je $b = N(\alpha)$ za neki $\alpha \in k(\sqrt{a})$.*

Dokaz. Slučaj a je kvadrat:
Neka je $a = c^2$. Tada je $x^2 - ay^2 = (x + cy)(x - cy)$, što je ekvivalentno kvadratnoj formi xy koja reprezentira 0, pa time i sve elemente od k, pa onda i $x^2 - ay^2 - bz^2 = 0$ ima rješenje s npr. $z = 1$. Također vrijedi i $b = N(b)$, dakle u ovom slučaju obje strane ekvivalencije su uvijek istinite.

Slučaj a nije kvadrat:
Ako je b norma, npr. $b = N(x+y\sqrt{a})$, tada je $x^2-ay^2-b\cdot 1^2 = 0$. Obrnuto, ako $x^2 - ay^2 - bz^2 = 0$ reprezentira 0, tada ne-trivijalno rješenje mora zadovoljavati $z \neq 0$ (zbog pretpostavke da a nije kvadrat). Dijeljenjem s z^2, vidimo da je b norma nekog elementa iz $k(\sqrt{a})$. □

Pretpostavimo, dakle, da je $q(x, y, z) = x^2 - ay^2 - bz^2$, gdje su $a, b \neq 0$. Možemo također, bez smanjenja općenitosti pretpostaviti da su a i b kvadratno slobodni cijeli brojevi. Dokazujemo tvrdnju po indukciji po $m := |a| + |b|$.

Slučaj $m \leq 2$:
U ovom slučaju postoje 4 mogućnosti,

$$q(x, y, z) = x^2 \pm y^2 \pm z^2,$$

gdje slučaj kada su oba znaka + odbacujemo jer tada q ne reprezentira 0 nad $\mathbb{R}$. U svim ostalim slučajevima, q očito reprezenira 0.

Slučaj $m > 2$:
Bez smanjenja općenitosti, pretpostavimo da je $|b| \geq |a|$, pa je $|b| \geq 2$. Neka je $b = \pm p_1 \dots p_k$, gdje su svi p_i-ovi međusobno različiti prosti brojevi. Neka je p jedan od p_i-ova. Po pretpostavci, jednadžba $x^2 - ay^2 - bz^2 = 0$ ima rješenja u $\mathbb{Q}_p$ i možemo pretpostaviti da su $x, y, z \in \mathbb{Z}_p$ i da nisu svi u $p\mathbb{Z}_p$.

Tvrdimo da je a kvadrat modulo p. Kada ne bi bio tada bi jednadžba $x^2 - ay^2 - bz^2 = 0$ modulo p imala jedino rješenje $x \equiv y \equiv 0 \pmod{p}$, ali tada p^2 dijeli x^2 i ay^2, pa mora i bz^2, pa mora dijeliti i z. To je kontradickija s pretpostavkom da nisu svi $x, y, z \in p\mathbb{Z}_p$.

Dakle imamo da je a kvadrat mod p_i, te je $\mathbb{Z}/b\mathbb{Z} \simeq \prod \mathbb{Z}/p_i\mathbb{Z}$, pa je a kvadrat modulo b. Dakle, postoji $t \in \mathbb{Z}$ takav da je $t^2 \equiv a \pmod{b}$ i možemo pretpostaviti da je $|t| \leq |b|/2$. Dakle, $t^2 - a = bb'$ za neki $b' \in \mathbb{Z}$. Imamo

$$|b'| = \left|\frac{t^2 - a}{b}\right| \leq \frac{|t|^2}{|b|} + \frac{|a|}{|b|} \leq \frac{|b|}{4} + 1 < |b|,$$

pošto je $|b| \geq 2$.

Također, vidimo da je bb' norma elementa iz $\mathbb{Q}(\sqrt{a})$. Po lemi 36, pošto $x^2 - ay^2 - bz^2$ reprezentira 0 u $\mathbb{Q}_p$, slijedi da je i b norma u $\mathbb{Q}_p(\sqrt{a})$. Dakle, vrijedi i da je $b' = (bb')/b$ norma elementa iz $\mathbb{Q}_p(\sqrt{a})$ po multiplikativnosti norme. Sada imamo da

$$x^2 - ay^2 - b'z^2 = 0$$

reprezentira 0 nad $\mathbb{Q}_{p_i}$, za sve i-ove. Međutim, imamo da je $|a| + |b'| < |a| + |b|$, te po pretpostavci indukcije vrijedi da ova forma reprezentira 0 nad $\mathbb{Q}$. Slijedi da je b' norma u $\mathbb{Q}(\sqrt{a})$. Ako je $b' = 0$, onda slijedi da je a kvadrat, te smo gotovi (jer tada $x^2 - ay^2$ reprezentira 0, tj. možemo uzeti $z = 0$). Ako $b' \neq 0$, tada je $b = (bb')/b'$ norma elementa iz $\mathbb{Q}(\sqrt{a})$, pa nam lema 36 kaže da $x^2 - ay^2 - bz^2$ reprezentira 0. □

Primjer 10. Pokažimo primjere krivulja koja krši lokalno-globalni princip. Možda najpoznatiji je Selmerov primjer, krivulja

$$3x^3 + 4y^3 + 5y^3 = 0.$$

Pokažimo još jedan primjer. Neka je $p \equiv 1 \pmod{16}$ takav da 2 nije četvrta potencija mod p i neka je

$$C : y^2 = 2 - 2px^4$$

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. Za to možemo koristit sljedeći rezultat (naša krivulja ima genus 1) koji za sada nećemo dokazivati

Lema 37 ([3], Corollary 9.3.)**.** *Nesingularna projektivna krivulja C genusa* 1 *nad $\mathbb{F}_p$ ima točku s koordinatama u $\mathbb{F}_p$.*

Očito je da ima točaka nad $\mathbb{R}$, te iz leme 37 i Henselove leme slijedi da ima točke nad $\mathbb{F}_q$ za $q \neq 2, p$, pošto krivulja ima dobru redukciju u q. Za $q = p$ uzmimo $y = \sqrt{2} \in \mathbb{Z}_p$ (iz Henselova leme se lako vidi da je $\sqrt{2} \in \mathbb{Z}_p$) te $x = 0$.

Za $p = 2$, uzmimo x takav da je $x^4 = \frac{1}{p}$ u $\mathbb{Z}_2$ (ostavljamo za vježbu dokazati da je taj $x \in \mathbb{Z}_2$).

3.11 Racionalne točke na konikama II

Promotrimo prvo konike nad konačnim poljima. Promotimo sada konike nad konačnim poljem $\mathbb{F}_q$ (gdje je $q = p^k$ za neki prirodan broj k).

Propozicija 38. *Projektivna konika X nad $\mathbb{F}_q$ ima $\mathbb{F}_q$-racionalnu točku.*

Dokaz. Mi ćemo dokazati propoziciju u slučaju da q nije potencija od 2 (iako teorem vrijedi i u tom slučaju). Svaka projektivna konika se može zapisati kao $ax^2 + by^2 + cz^2 = 0$. Ako je $abc = 0$ (tada konika neće biti ireducibilna!), bez smanjenja općenitosti pretpostavimo da je $c = 0$. Tada je $(0 : 0 : 1)$ točka na X. Ako je $abc \neq 0$ uzmimo da je $z = 1$. Sada skupovi

$$\{ax^2 : x \in \mathbb{F}_q\} \quad i \quad \{-by^2 - c : y \in \mathbb{F}_q\}$$

imaju oboje po $(q+1)/2$ elemenata u $\mathbb{F}_q$. To vidimo jer je $\mathbb{F}_q^\times$ ciklička grupa reda $q-1$, te $\mathbb{F}_q$ ima $(q-1)/2$ kvadrata elemenata in $\mathbb{F}_q - \{0\}$, tj. $(q+1)/2$ kvadrata elemenata iz $\mathbb{F}_q$. Dakle za neki $x, y \in \mathbb{F}_q$ mora vrijediti $ax^2 = -by^2 - c$. □

Korolar 39. *Za glatku projektivnu geometrijski ireducibilnu koniku nad $\mathbb{F}_q$ vrijedi $X \simeq \mathbb{P}^1(\mathbb{F}_q)$, te $\#X(\mathbb{F}_q) = q + 1$.*

Vidjeli smo da sve konike možemo zapisati kao $ax^2 + by^2 + cz^2 = 0$ u projektivnoj ravnini. Bez smanjenja općenitosti možemo pretpostaviti da su $a, b, c \in \mathbb{Z}$. Sljedeća propozicija nam daje jednostavan kriterij za provjeravanje imaju li konike p-adskih točaka.

Propozicija 40. *Ako su $a, b, c \in \mathbb{Z}$ sve ne-nul, i p je konačan prost broj ($p \neq \infty$) takav da je $p \nmid 2abc$, tada $ax^2 + by^2 + cz^2 = 0$ ima netrivijalno rješenje u $\mathbb{Q}_p$.*

Dokaz. Po Propoziciji 38, postoji netrivijalno rješenje ove jednadžbe nad $\mathbb{F}_p$. Možemo podignuti ovo rješenje na proizvoljan način u neko rješenje $(x_0, y_0, z_0) \in \mathbb{Z}_p^3$, takvi da nisu svi x_0, y_0, z_0 u $p\mathbb{Z}_p$ koje zadovoljava $ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{p}$. Bez smanjenja općenitosti možemo pretpostaviti da je $x_0 \notin p\mathbb{Z}_p$. Tada je x_0 aproksimacija nultočke polinoma $f(x) = ax^2 + by_0^2 + cz_0^2 \in \mathbb{Z}_p[x]$, te $p \nmid f'(x_0) = 2ax_0$, pa po Henselovoj lemi postoji egzaktno rješenje $x_1 \in \mathbb{Z}_p$ takvo da je $f(x_1) = 0$, te je $x_1 \equiv x_0 \not\equiv 0 \pmod{p\mathbb{Z}_p}$. Dakle (x_1, y_0, z_0) je rješenje od $ax^2 + by^2 + cz^2 = 0$ u $\mathbb{Q}_p$ (a također i u $\mathbb{Z}_p$. □

Primjer 11. Već smo pokazali da konika $x^2 + y^2 = 3z^2$ nema točaka nad $\mathbb{Q}_3$. Na isti način se može pokazati da nema točaka ni nad $\mathbb{Q}_2$.

Napomena. Može se pokazati da je broj $p \leq \infty$ takvih da neka fiksna konika nema $\mathbb{Q}_p$-točaka uvijek paran! To se može dokazati korištenjem kvadratne recipročnosti.

Pokažimo sada primjene ovih rezultata na neke klasične rezultate iz teorije brojeva.

Propozicija 41. *Racionalan broj a se može prikazati kao $x^2 + y^2 + z^2$ za racionalne x, y, z ako i samo ako je $a > 0$ i nije oblika $a = 4^m u$, gdje je $u \in 7 + 8\mathbb{Z}_2$, $u > 0$.*

Dokaz. Po Propoziciji 40, $x^2 + y^2 + z^2$ reprezentira 0 nad $\mathbb{Q}_p$ za sve neparne p-ove, pa time i sve $\mathbb{Q}_p$-racionalne brojeve. Dakle, treba provjeriti tvrdnju samo za $p = 2$.

Pogledajmo prvo koje vriejdnosti može poprimiti $x^2+y^2+z^2$ uz pretopstavku da je $x \in \mathbb{Z}_2^\times$, $y, z \in \mathbb{Z}_2$. Ako x poprima sve vrijednosti iz $\mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2$, tada x^2 poprima sve vrijednosti iz $\mathbb{Z}_2^{\times 2}$. Po dokazu teorema 24 (1), vrijedi da je $\mathbb{Z}_2^{\times 2}$ upravo $1 + 8\mathbb{Z}_2$. Kako su y^2 i z^2 poprimaju vrijednosti $0, 1, 4$ modulo 8, vidimo da u ovom slučaju $x^2 + y^2 + z^2$ poprima upravo vrijednosti $b + 8\mathbb{Z}_2$, gdje je $b \in \{0, 1, 2, 3, 5, 6\}$. Vrijednosti $x^2+y^2+z^2$ u $\mathbb{Q}_2$ opće trojke $(x, y, z) \in \mathbb{Q}_2^3 - (0, 0, 0)$ se tada dobiju množenjem potencijom (x, y, z) od 2, dakle množenjem $x^2+y^2+z^2$ s potnecijom od 4. □

Teorem 42 (Gauss)**.** *Prirodan broj a se može prikazati kao suma tri kvadrata prirodnih brojeva ako i samo ako nije oblika $4^m(8k + 7)$, za neke $m, k \in \mathbb{N}_0$.*

Da bi dokazali ovaj teorem treba nam sljedeće (općenitija) lema:

Lema 43 (Cassels- Davenport)**.** *Neka je $q(x) = f(x_1, \ldots, x_n) = \sum_{i,j=1}^n a_{ij} x_i x_j$ kvadratna forma takva da je $a_{ji} = a_{ij} \in \mathbb{Z}$. Pretpostavimo da vrijedi svostvo (DC): za svaki $y = (y_1, \ldots, y_n) \in \mathbb{Q}^n - \mathbb{Z}^n$, postoji $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ takav da je*

$$0 < |q(x - y)| < 1.$$

Tada, za svaki cijeli broj d, kvadratna forma repreznetira d u cijelim brojevima ako i samo ako q reprezentira d u racionalnim brojevima.

Dokaz. Za $x, y \in \mathbb{Q}^n$, definirajmo $x \cdot y := \frac{1}{2}(q(x + y) - q(x) - q(y))$. Tada je $(x, y) \to x \cdot y$ bilinearno preslikavanje i $x \cdot x = q(x)$. Također primjetimo da za $x, y \in \mathbb{Z}^n$ vrijedi $2(x \cdot y) \in \mathbb{Z}$.

Neka je sada $d \in \mathbb{Z}$, i pretpostavimo da postoji $x \in \mathbb{Q}^n$ takav da je $q(x) = d$. Ekvivalentno tome, postoji $t \in \mathbb{Z}$ i $x' \in \mathbb{Z}^n$ takav da je $t^2 d = x' \cdot x'$. Izaberimo t i x' takve da je $|t|$ minimalan takav. Zapravo trbamo doazati da je $|t| = 1$.

Pretpostavimo da je $|t| > 1$ i neka je sada $v = x'/t$. Po pretpostavci (DC) za v, postoji $y \in \mathbb{Z}^n$ takav da ako je $z = v - y$, tada imamo $0 < |q(z)| < 1$.

Definirajmo sada

$$\begin{aligned} a &:= y \cdot y - d \\ b &:= 2(dt - x' \cdot y) \\ T &:= at + b \\ X &:= ax' + by. \end{aligned}$$

Uz ove definicije je $a, b, T \in \mathbb{Z}$ i $X \in \mathbb{Z}^n$.

Sada vrijedi

$$X \cdot X = (ax'+by)\cdot(ax'+by) = ax'\cdot(ax'+by)+by\cdot(ax'+by) = a^2(x'\cdot x')+2ab(x'\cdot y)+b^2(y\cdot y)$$

$$= a^2t^d + ab(2dt - b) + b^2(a + d) = d(a^2t^2 + 2abt + b^2) = T^2d.$$

Nadalje, imamo

$$tT = at^2 + bt = t^2(y \cdot y) - dt^2 + 2dt^2 - t(2x' \cdot y)$$

$$= t^2(y \cdot y) - t(2x' \cdot y) + x' \cdot x' = (ty - x') \cdot (ty - x') = (-tz) \cdot (-tz) = t^2(z \cdot z).$$

Zaključujemo da vrijedi da je $T = t(z \cdot z)$. Pošto je po pretpostavci $0 < |z \cdot z| < 1$, imamo da je $0 < |T| < |t|$, te da je $(X/T) \cdot (X/T) = q(X/T) = d$, te smo dobili kontradikciju s minimalnošću od $|t|$.

□

Napomena. Primjetimo da je u uvjetima nužno da je $|q(x - y)| > 0$. Primjer je $q(x, y) = x^2 - y^2$, koji reprezentira 2 u racionalnim brojevima, ali ne i u cijelim.

Napomena. Primjetimo da nam pretpostavke Cassels-Davenportove leme nisu zadovoljene za

$$q(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2;$$

tako da nam ova lema ne pomaže pri određivanju koji se cijeli brojevi mogu prikazati kao zbrojevi 4 kvadrata.

Dokaz Gaussovog teorema 42. Kvadratna forma $q(x, y, z) = x^2 + y^2 + z^2$ zadovoljava uvjet (DC) iz leme 43, te onda rezultat slijedi iz propozicije 41. □

Iz Gaussovog teorema, imamo odmah dvije zanimljive posljedice.

Korolar 44 (Lagrange)**.** *Svaki prirodan broj a se može prikazati kao $x^2 + y^2 + z^2 + w^2$, gdje su $x, y, z, w \in \mathbb{Z}$.*

Dokaz. Ako a nije oblika $4^m(8k + 7)$, tada ga možemo prikazati kao sumu tri kvadrata, te uzeti $w = 0$. Ako je a oblika $8k + 7$, tada, pošto se $8k + 6$ može prikazati kao suma tri kvadrata $x^2 + y^2 + z^2$, te možemo uzeti $w = 1$. Sada još pomnožimo x, y, z, w s 2^m, te imamo da je $x^2+y^2+z^2+w^2 = 4^m(8k+7) = a$. □

Korolar 45 (Gauss)**.** *Svaki prirodan broj a se može prikazati kao suma tri trokutasta broja (trokutasti broj je broj oblika $(m(m + 1))/2$).*

Dokaz. Primjetimo da ako je $x = 2m + 1$, imamo da je

$$\frac{x^2 - 1}{8} = \frac{m(m+1)}{2}.$$

Nadalje pošto se $8a+3$ može prikazati kao suma tri kvadrata $8a+3 = x_1^2+x_2^2+x_3^2$. Primjetimo da x_1, x_2, x_3 trebaju svi biti neparni. Zapišimo $x_i = 2m_i + 1$. Sada je

$$\begin{aligned} a &= \frac{x_1^2 + x_2^2 + x_3^2 - 3}{8} = \frac{x_1^2 - 1}{8} + \frac{x_2^2 - 1}{8} + \frac{x_3^2 - 1}{8} \\ &= \frac{m_1(m_1+1)}{2} + \frac{m_2(m_2+1)}{2} + \frac{m_3(m_3+1)}{2}. \end{aligned}$$

□

Poglavlje 4

Osnove algebarske geometrije

4.1 Algebarski skupovi

Neka je k savršeno polje, $\overline{k}$ neko njegovo fiksno algebarski zatvoreno polje, te neka je $G_k = \mathrm{Gal}(\overline{k}/k)$.

Definicija. Neka je $n \in \mathbb{N}_0$. Definiramo n-dimenzionalni *afin prostor* nad k

$$\mathbb{A}_k^n := \{(x_1, \ldots, x_n) \in \overline{k}^n\}.$$

Kada je k jasan iz konteksta, često ćemo pisati samo $\mathbb{A}^n$. Ako je $k \subseteq L \subseteq \overline{k}$, tada je skup L-racionalnih točaka na $\mathbb{A}^n$

$$\mathbb{A}^n(L) = \{(x_1, \ldots, x_n) \in L^n\} = \mathbb{A}^n(\overline{k})^{G_L}.$$

Definicija. Neka je S skup polinoma u $\overline{k}[x_1, \ldots, x_n]$, tada se skup točaka

$$Z_S = \{P \in \mathbb{A}^n : f(P) = 0 \text{ za sve } f \in S\}$$

zove *algebarski skup*. Ako je $k \subseteq L \subseteq \overline{k}$, tada je skup L-racionalnih točaka u Z_S jednak

$$Z_S(L) = Z_S \cap \mathbb{A}^n(L).$$

Kada se S sastoji od samo jednog polinoma f, pišemo Z_f (umjesto $Z_{\{f\}}$).

Primjetimo da ako je I ideal generiran s S, da će tada vrijediti $Z_I = Z_S$. Dakle, možemo uvijek zamijeniti S s idealom (S) kojeg taj skup generira.

Primjer 12. Imamo $Z_{(0)} = \mathbb{A}^n$, te $Z_{\{1\}} = Z_{(1)} = \emptyset$.

Primjetimo da ako je $S \subseteq T$, da je tada $Z_S \supseteq Z_S$, ali obrat tvrdnje ne vrijedi.

Definicija. Komutativan prsten je *Noetherin* ako je svaki ideal u R konačno generiran.

Teorem 46 (Hilbertov teorem o bazi)**.** *Ako je R Noetherin prsten, tada je i $R[x]$ Noetherin.*

Definicija. Ako je $Z \subseteq \mathbb{A}^n$ algebarski skup, ideal $I(Z)$ od Z je

$$I(Z) := \{f \in \bar{k}[x_1, \ldots, x_n] : f(P) = 0 \text{ za sve } P \in Z\}.$$

Primjetimo sada da ako je $Y \subseteq Z$, tada je $I(Y) \supseteq I(Z)$ i $I(Y \cup Z) = I(Y) \cap I(Z)$. Također, imamo da je $Z = Z_{I(Z)}$ za svaki algebarski skup Z, ali ne vrijedi da je $I = Z(I_Z)$ za svaki ideal I. Npr. za $f \in k[x_1, \ldots, x_n]$, imamo

$$I(Z_{(f^2)}) = (f).$$

Definicija. Neka je R komutativan prsten. Za svaki ideal I u R, definiramo *radikal* $\sqrt{I}$ ideala I

$$\sqrt{I} = \{x \in R : x^r \in I, \text{ za neki } r > 0\}.$$

Ako je $I = \sqrt{I}$, kažemo da je ideal radikalan.

Lema 47. *Za svkai ideal I u komutativnom prstenu R, skup $\sqrt{I}$ je ideal.*

Teorem 48 (Hilbertov Nullstellensatz)**.** *Za svkai ideal $I \subseteq \overline{k}[x_1, \ldots, x_n]$, vrijedi*

$$I(Z_I) = \sqrt{I}.$$

Iz Hilbertovog Nullstellensatza direktno slijedi Slabi Nullstellensatz.

Teorem 49 (Slabi Nullstellensatz)**.** *Za svkai pravi ideal $I \subseteq \overline{k}[x_1, \ldots, x_n]$, mnogostrukost Z_I je neprazna.*

Dokaz. Pretostavimo da je I ideal takav da je $I(Z_I)$ prazan; tada je $I(Z_I) = (1)$, pa je po Nullstellensatzu $\sqrt{I} = (1)$. Slijei da za neki $r \in \mathbb{N}$ vrijedi $1^r = 1 \in I$, pa ideal I nije pravi. □

Primjetimo da je vrlo bitno da se radi nad algebarskim zatvorenim poljem, u suprotnom teorem nije istinit.

Korolar 50. *Maksimalni ideali prstena $\overline{k}[x_1, \ldots, x_n]$ su svi oblika*

$$m_P = (x_1 - p_1, \ldots, x_n - p_n),$$

za neki $P = (p_1, \ldots, p_n) \in \mathbb{A}^n$.

Sada imamo i sljedeći vrlo bitni korolar jakog Hilbertovog Nullstellensatza:

Korolar 51. *Postoji $1-1$ korespondencija koja obrće relaciju inkluzije između radikalnih ideala $I \subseteq \overline{k}[x_1, \ldots, x_n]$ i algebarskih skupova $Z \subseteq \mathbb{A}^n$ u kojoj je*

$$I \leftrightarrow Z_I \text{ tj. } I(Z) \leftrightarrow Z.$$

Ovaj korolar je izrazito važan, te on čini temelje algebarske geometrije. On dopušta proučavanje algebarskih mnogostrukosti kroz proučavanje ideala u prstenim polinoma, za koje se puno lakše "uhvatiti".

Definicija. Algebarski skup je *ireducibilan* ako je neprazan i ako nije unija dva manja neprazna algebarska skupa.

Teorem 52. *Algebarski skup je ireducibilan ako i samo ako je njemu odgovarajući ideal prost.*

Dokaz. ($\Longrightarrow$) Neka je Y ireducibilan algebarski skup i neka je $fg \in I(Y)$ za neke $f, g \in \overline{k}[x_1, \ldots, x_n]$. Vrijedi

$$Y \subseteq Z_{fg} = Z_f \cup Z_g$$

Dakle, imamo

$$Y = (Y \cap Z_f) \cup (Y \cap Z_g),$$

pa pošto je Y ireducibilan je $Y = (Y \cap Z_f)$ ili $Y = (Y \cap Z_g)$, pa je ili $f \in I(Y)$ ili je $g \in I(Y)$. Slijedi da je ideal $I(Y)$ prost. ($\Longleftarrow$) Pretpostavimo da je $I(Y)$ prost i da je $Y = Y_1 \cup Y_2$. Imamo da je

$$I(Y) = I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2) \supseteq I(Y_1)I(Y_2),$$

pa onda $I(Y)$ (pošto je prost) sadrži ili $I(Y_1)$ ili $I(Y_2)$. S druge strane, $I(Y)$ je sadržan i u $I(Y_1)$ i u $I(Y_2)$, pa onda slijedi da je $I(Y)$ jednak ili $I(Y_1)$ ili $I(Y_2)$. Sada slijedi da je $Y = Y_1$ ili $Y = Y_2$ (pošto su skupovi s istim idealom su jednaki), pa slijedi da je Y ireducibilan.

□

4.2 Afine mnogostrukosti

Definicija. Algebarski skup $Z \subseteq \mathbb{A}^n$ je *definiran nad* k ako je $I(Z)$ generiran polinomima iz $k[x_1, \ldots, x_n]$. Pišemo Z/k da bi naznačili da je Z definiran nad k. Također definiramo

$$I(Z/k) = I(Z) \cap k[x_1, \ldots, x_n].$$

Neka je $G_k := \mathrm{Gal}(\overline{k}/k)$ *absolutna Galoisova grupa od* k. Primjetimo da ako je Z definiran nad k, tada G_k djeluje na Z, pošto za svaki $\sigma \in G_k$ i za svaki $k[x_1, \ldots x_n]$, te svaki $P \in \mathbb{A}^n$ vrijedi $f(P^\sigma) = f(P)^\sigma$. Tada imamo da je

$$Z(k) = \{P \in Z : P^\sigma = P \text{ za sve } \sigma \in G_k\} = Z^{G_k}.$$

Definicija. Neka je Z algebarski skup definiran nad k. *Afin koordinatni prsten* ili samo *koordinatni prsten* od Z/k je prsten

$$k[Z] = \frac{k[x_1, \ldots, x_n]}{I(Z/k)},$$

te definiramo

$$\overline{k}[Z] = \frac{\overline{k}[x_1, \ldots, x_n]}{I(Z)}.$$

Primjetimo da je koordinatni prsten $k[Z]$ integralna domena ako i samo ako je $I(Z/k)$ prosti ideal. Također, ako $k[Z]$ nema djelitelja nule, to ne znači nužno da $\overline{k}[Z]$ nema djelitlja nule, npr. uzmimo $k = \mathbb{Q}$, te $Z = Z_{x^2+1}$.

Sjetimo se da je $I(Z)$ prost ideal ako i samo ako je Z ireducibilan.

Definicija. *Afina mnogostrukost* V je ireducibilan algebarski skup u $\mathbb{A}^n$.

Primjetimo da imamo ranije spomenutu $1-1$ korespondenciju između afinih mnogostrukosti i prostih ideala.

Definicija. Neka je V/k afina mnogostrukost nad k. *Funkcijsko polje* $k(V)$ od V je polje razlomaka od $k[V]$.

Primjer 13. Vrijedi $k(\mathbb{A}^n) = k(x_1, \ldots, x_n)$. Neka je $P \in \mathbb{A}^n$ neka točka. Tada je $k(P) = k$.

Definicija. *Dimenzija* $\dim V$ od V je stupanj transcedentnosti od $\overline{k}(V)/\overline{k}$.

Primjer 14. Vrijedi $\dim \mathbb{A}^n = n$, $\dim P = 0$ za svaki $P \in \mathbb{A}^n$.

Definicija. Neka je V afina mnogostrukost i neka su $f_1, \ldots, f_m \in \overline{k}[x_1, \ldots, x_m]$ skup generatora za $I(V)$. Točka $P \in C$ je *nesingularna* (ili V je *gladak u* P) ako $m \times n$ Jacobijeva matrica $M(P)$ s koeficijentima

$$M_{ij}(P) = \frac{\partial f_i}{\partial x_j}(P)$$

ima rang $n - \dim V$. U suprotnom kažemo da je P *singularna točka*. Ako V nema singularnih točaka, kažemo da je V *glatka*.

4.3 Projektivne mnogostrukosti

Definicija. n-dimenzionalno *projektivni prostor* $\mathbb{P}^n$ je skup svih točaka u $\mathbb{A}^{n+1} - \{0\}$ modulo ekvivalencija

$$(a_0, \ldots, a_n) \sim (\lambda a_0, \ldots, \lambda a_n)$$

za sve $\lambda \in k^\times$. Obično koristimo notaciju $(a_0 : \ldots : a_n)$ da označimo klasu ekvivalencije od $(a_0, \ldots, a_n)$, te takvu klasu nazivamo *projektivna točka* ili samo *točka* od $\mathbb{P}^n$. Skup k-racionalnih točaka od $\mathbb{P}^n$ je

$$\mathbb{P}^n(k) = \{(a_0 : \ldots : a_n) \in \mathbb{P}^n : a_0, \ldots, \in k\}.$$

Apsolutna Galoisova grupa G_k djeluje na $\mathbb{P}^n$ s

$$(a_0 : \ldots : a_n)^\sigma = (a_0^\sigma : \ldots : a_n^\sigma).$$

Ovo djelovanje je dobro definirano jer je $(\lambda P)^\sigma = \lambda^\sigma P^\sigma \sim P^\sigma$ za sve $\lambda \in \overline{k}^\times$ i $P \in \mathbb{A}^{n+1} \backslash \{0\}$. Dakle imamo

$$\mathbb{P}^n(k) = (\mathbb{P}^n)^{G_k}.$$

Definicija. Polinom $f \in \overline{k}[x_0, \ldots, x_n]$ je *homogen stupnja d* ako je

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$$

za sve $\lambda \in \overline{k}$. Ekvivalenton, svi monomi su stupnja d. Kažemo da je f *homogen* ako je homogen stupnja d za neki cijeli broj d.

Definicija. Za polinom $f \in \overline{k}[x_0, \ldots, x_{n-1}]$ u n varijabli stupnja d, definiramo homogenizaciju $F \in \overline{k}[x_0, \ldots, x_n]$ da je

$$F(x_0, \ldots, x_n) = x_n^d f\left(\frac{x_0}{x_n}, \ldots, \frac{x_{n-1}}{x_n}\right).$$

Obrnuto, za neki homogeni polinom $F \in \overline{k}[x_0, \ldots, x_n]$, te neki $i \in [0, n]$ kažemo da je

$$f(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots x_n) = F(x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots x_n)$$

dehomogenizacija od F (s obzirom na x_i).

Primjetimo da za homogene polinome (i samo za njih) ima smisla govoriti o vrijednosti $f(P)$, gdje je $P \in \mathbb{P}^n$, pošto vrijednost ne ovisi o izboru reprezenta.

Neka je $i \in [0, n]$; tada je skup nultočaka x_i hiperravnina

$$H_i = \{(a_0 : \ldots : a_{i-1} : 0 : a_{i+1} : \ldots : a_n) \in \mathbb{P}^n\},$$

koji odgovara kopiji $\mathbb{P}^{n-1}$ u $\mathbb{P}^n$.

Definicija. Komplement od H_i u $\mathbb{P}^n$ je *afina karta*

$$U_i = \{(a_0 : \ldots : a_{i-1} : 1 : a_{i+1} : \ldots : a_n) \in \mathbb{P}^n\},$$

koji odgovara kopiji $\mathbb{A}^n$ uloženoj u $\mathbb{P}^n$.

Primjetimo da izbor $a_i = 1$ u prethodnoj definciji fiksira izbor reprezenta projektivne točke $(a_0 : \ldots : a_{i-1} : 1 : a_{i+1} : \ldots : a_n)$.

Dakle za neku hiperravninu H_i imamo

$$\mathbb{P}^n = H_i \cup U_i \simeq \mathbb{A}^n \cup \mathbb{P}^{n-1},$$

gdje je svaka od unija u ovoj jednakosti zapravo disjunktna unija. Sada možemo ponoviti istu stvar za $H_i \simeq \mathbb{P}^{n-1}$, te onda višestrukom primjene istog principa dobivamo

$$\mathbb{P}^n \simeq \mathbb{A}^n \cup A^{n-1} \cup A^{n-2} \cup \ldots \cup A^1 \cup \mathbb{P}^0,$$

gdje je $\mathbb{P}^0$ projektivna točka u $\mathbb{P}^n$. Također možemo promatrati i $\mathbb{P}^n$ kao uniju $n+1$ (ne međusobno dijskunktnih) afinih karti U_i, za $i = 1, \ldots, n+1$.

Definicija. Za svaki skup polinoma S, iz $\overline{k}[x_0, \ldots, x_n]$, definiramo *projektivni algebarski skup*

$$\mathbb{Z}_S = \{P \in \mathbb{P}^n : f(P) = 0 \text{ za sve homogene } f \in S\}.$$

Homogeni ideal u $\overline{k}[x_0, \ldots, x_n]$ je ideal generiran s skupom homogenih polinoma.

Primjetimo da nisu svi polinomi u homogenom idealu homogeni; međutim to za našu definiciju nije bitno, pošto promatramo samo nultočke homogenih polinoma.

Definicija. Neka je Z algebarski skup u $\mathbb{P}^n$. Tada je *ideal od* Z ideal $I(Z)$ generiran s svim homogenim polinomima iz $\overline{k}[x_0, \ldots, x_n]$ koji poprimaju vrijednost 0 na svim točkama od Z.

Definicija. Kažemo da je Z *definiran nad* k ako se njegov ideal može generirati homogenim polinomima u $k[x_0, \ldots, x_n]$, te pišemo Z/k ako je Z definiran nad k, tada je skup *k-racionalnih točaka* na Z jednak

$$Z(k) = Z \cap \mathbb{P}^n(k) = Z^{G_k},$$

te slično za sva proširenja od k.

Definicija ireducibilnosti za projektivne algebarske skupove je jednaka kao i za (afine) algebrske skupove.

Definicija. *Projektivna mnogostrukost* je ireducibilan algebarski skup u $\mathbb{P}^n$.

Kao i u afinom slučaju, $Z \subseteq \mathbb{P}^n$ je ireducibilan ako i samo ako je $I(Z)$ prost.

Definicija. Koordinatni prsten projektivne mnogostrukosti V/k je $k[x_0, \ldots, x_n]/I$, gdje je I ideal koji definira mnogostrukosti V.

4.3.1 Topologija Zariskog

Definicija. *Topologija Zariskog* na $\mathbb{A}^n$ (ili na $\mathbb{P}^n$) je definirana tako da definiramo da su algebarski skupovi zatvoreni.

Primjetimo da nam korespondencija između algebarskih skupova i ideala u prstenima polinoma inducira topologiju Zariskog na $k[x_1, \ldots, x_n]$.

Primjetimo da su prazan skup i $\mathbb{A}^n$ (ili $\mathbb{P}^n$) zatvoreni, pošto su oni algebarski skupovi definirani idealima (1) i (0). Topologija Zariskog nije Hausdorffova, štoviše presjek svaka 2 otvorena skupa je otvoren, te je svaki otvoreni skup gust.

4.4 Morfizmi mnogostrukosti

Pogledajmo prvo morfizme afinih mnogostrukosti.

Definicija. Neka su $X \subseteq \mathbb{A}^m$ i $Y \subseteq \mathbb{A}^n$ afine mnogostrukosti definirane nad k. *Morfizam* $f : X \to Y$ je preslikavanje $f(P) := (f_1(P), \ldots, f_n(P))$ definirano s polinomima $f_1, \ldots, f_n \in \overline{k}[X]$ takvo da je $f(P) \in Y$ za svaki $P \in X$.

Kompozicija 2 morfizma je također morfizam.

Teorem 53. *Morfizam afinih mnogostrukosti $f : X \to Y$ je neprekidan, tj. praslika $f^{-1}(Z)$ od algebarskog skup $Z \subseteq Y$ je algebarski skup.*

Napomena. Primjetimo da slika morfizma nije nužno afina mnogostrukost, štoviše, ne mora čak biti ni algebarski skup. Promotrimo npr. $f : \mathbb{A}^2 \to \mathbb{A}^2$ (nad neim beskonačnim poljem, recimo PAB) definiran s $f(x_1, x_2) = (x_1, x_1x_2)$. Lako se vidi da je $\operatorname{im} f$ cijeli $\mathbb{A}^2$ osim točaka oblika $(0, c)$, gdje je $c \neq 0$. Pokažimo da ovo nije algebarski skup. Pretpostavimo da polinom $g(y_1, y_2)$ poprima 0 na cijelom $\operatorname{im} f$. Tada za svaki $k \neq 0$, polinom $h(t) = g(t, k)$ ima beskonačmno mnogo nultočaka, te je nul-polinom, pa slijedi da je g nul-polinom. Dakle $I(\operatorname{im} f) = (0)$, te je $\mathbb{A}^2$ jedini algebarski skup koji sadrži $\operatorname{im} f$.

Definicija. Dvije mnogostrukosti X i Y su *izomorfne* ako postoji morfizam $f : X \to Y$ i $g : Y \to X$ takve da su $f \circ g$ i $g \circ f$ identiteta na X i Y. U tom slučaju kažemo da su f i g izomorfizmi.

Definicija. *Afina algebra* R je integralna domena, koja je ujedno i konačno generirana asocijativna $\overline{k}$-algebra za neko polje k.

Teorem 54. *Vrijedi:*

1. *Svaki morfizam $\phi : X \to Y$ afinih mnogostrukosti inducira morfizam $\phi^* : \overline{k}[Y] \to \overline{k}[X]$ afinih algebri definiran s $\phi^*(g) = g \circ \phi$.*
2. *Svaki morfizam $\theta : R \to S$ afinih algebri inducira morfizam $\phi^* : X \to Y$ afinih mnogostrukosti takvih da je $R \simeq \overline{k}[Y]$ i da je $S \simeq \overline{k}[X]$ takvih da je slika od $\theta(g)$ u $\overline{k}[X]$ jednaka $g \circ \theta^*$.*

Korolar 55. *Svi neprazni afini djelovi (karte) projektivne mnogostrukosti su izomorfni.*

Dokaz. Ovo slijedi iz činjenice da projektivna mnogostrukost i svaki njezin afin dio imaju isti prsten koordinata. □

Korolar 56. *Kategorije afinih mnogostrukosti i afinih algebri (s morfizmima) su kontravarijantno izomorfne.*

Prirodno je gledati može li se u prethodnoj konstrukciji $\overline{k}[X]$ zamijeniti s $\overline{k}(X)$. Međutim problem nastaje da ako $r \in \overline{k}(X)$ zapišemo kao $r = f/g$, gdje su $f, g \in \overline{k}[X]$, taj zapis nije nužno jedinstven. Pošto je $\overline{k}(X)$ polje razlomaka od $\overline{k}[X]$, vrijedi da je i $r = p/q$ za $p, q \in \overline{k}[X]$ za p, q takve da je $pq = fg$. Vrijedi da su za sve $P \in X$ vrijednosti $f(P)/g(P)$ i $p(P)/q(P)$ nužno jednake kada su definirane, ali može biti da je $q(P) = 0$,a $g(P) \neq 0$ ili obrnuto. Pokažimo to na primjeru.

Primjer 15. Pogledajmo skup nultočaka od $x_1x_2 - x_3x_4$ u $\mathbb{A}^4$, te racionalnu funkciju $r = x_1/x_3 = x_4/x_2$. Vidimo da ju $P = (0, 1, 0, 0) \in X$, x_1/x_3 nije definirana u P, dok je $(x_4/x_2)(P) = 0$.

Definicija. Funkcija $r \in \overline{k}(X)$ je *regularna* ili *je definirana* u točki $P \in X$ ako je $gr \in \overline{k}[x]$ za neki $g \in \overline{k}[x]$ za koji je $g(P) \neq 0$ (drugim rječima, možemo je prikazati kao $r = f/g$, za neki $g(P) \neq 0$.)

Ako definiramo domenu $dom(r)$ od r kao skup točaka na X na kojima je r regularna, može se lako pokazati da je to otvoren, a time i gust podskup od X. Komplement od $dom(r)$ je definiran *idealom razlomaka* $\{g(x) \in \overline{k}[X] : gr \in \overline{k}[X]\}$.

Primjetimo da ako je $r \in \overline{k}[X]$, tada je domena $dom(r)$ od r jednak cijelom X. Vrijedi i obrat.

Propozicija 57. *Neka je $r \in \overline{k}(X)$. Tada je $r \in \overline{k}[X]$ ako i samo ako je $dom(r) = X$.*

Dokaz. "Samo ako" dio propopozicije je očit. S druge strane ako je $dom(r) = X$, tada je komplement od $dom(r)$ prazan skup, te je ideal razlomaka jednak (1), pa je $r \in k[X]$. □

Definicija. Neka je $X \subseteq \mathbb{A}^m$ i $Y \subseteq \mathbb{A}^n$ afine mnogostrukosti. Kažemo da je n-torka $(\phi_1, \ldots, \phi_n)$ s $\phi_i \in \overline{k}(X)$ *regularna* u $P \in X$ ako su svi ϕ-ovi regularni u P. Racionalno preslikavanje $\Phi : X \to Y$ je n-torka $(\phi_1, \ldots, \phi_n)$ funkcija $\phi_i \in \overline{k}(X)$ takvih da je $\phi(P) := (\phi_1, \ldots, \phi_n) \in Y$ za sve točke u kojima je ϕ regularno. Ako je ϕ regularna u svim točkama $P \in X$, tada kažemo da je ϕ regularna.

Na isti način kao i prethodnu propoziciju, možemo dokazati sljedeći teorem.

Teorem 58. *Racionalno preslikavanje afinih mnogostrukosti je morfizam ako i samo ako je regularan.*

Htjeli bismo imati ekvivalenciju kategorija u kojoj je pojam morfizma zamijenjen pojmom racionalnih funkcija. Međutim, problem je što ne možemo uvijek komponirati racionlne funkcije.

Primjer 16. Neka je $X = Y = Z = \mathbb{A}^2$, te neka je $\phi_1 : X \to Y$ zadan s $(1/x_1, 0)$, te neka je $\phi_2 : Y \to Z$ zadan s $(0, 1/x_2)$. Vidimo da je slika od ϕ_1 disjunktna s domenom od ϕ_2.

Nameće se zaključak da trebamo promatrati određeni podskup racionalnih preslikavanja.

Definicija. Racionalno preslikavanje $\phi : X \to Y$ je dominatno ako je zatvorenje od $\overline{\phi(dom(\phi))} = Y$.

Primjetimo da ako su $\phi_1 : X \to Y$ i $\phi_2 : y \to Z$ dominatna preslikavanja, tada je komplement od $\phi(dom(\phi_1))$ pravi zatvoreni podskup od Y, te ne može sadržati otvoreni (i gusti) skup $dom(\phi_2)$. Slijedi da uvijek možemo komponirati dominantna racionalna preslikavanja.

Imamo

Teorem 59. *Vrijedi:*

(i) Svako dominatno racionalno preslikavanje afinih mnogostrukosti $\phi : X \to Y$ inducira morfizam funkcijskih polja $\phi^* : \overline{k}(Y) \to \overline{k}(X)$ takvih da je $\phi^*(r) = r \circ \phi$.

(ii) Svaki morfizam $\theta : K \to L$ funkcijskih polja inducira dominantno racionalno preslikavanje afinih mnogostrukosti $\theta^* : X \to Y$, takvo da je $K \simeq \overline{k}(Y)$ i $L \simeq \overline{k}(X)$, takvo da je $\theta(r) = r \circ \theta^*$ za $r \in \overline{k}(Y)$.

(iii) Ako su $\phi : X \to Y$ i $\psi : Y \to Z$ dominantna racionalna preslikavanja afinih mnogostrukosti, tada je $(\psi \circ \phi)^* = \phi^* \circ \psi^*$.

Korolar 60. *Kategorija afinih mnogostrukosti i dominantnih racionalnih preslikavanja je kontravarijantno ekvivalentna kategoriji funkcijskih polja.*

Definicija. Dvije afine mnogostrukosti X i Y su biracionalno ekvivalentne ako postoje dominantna racionalna preslikavanja $\phi : X \to Y$ i $\psi : Y \to X$ takva da je $(\phi \circ \psi)(P) = P$ za sve $P \in dom(\phi \circ \psi)$ i $(\psi \circ \phi)(P) = P$ za sve $P \in dom(\psi \circ \phi)$.

Korolar 61. *Dvije afine mnogostrukosti su biracionalno ekvivalentne ako i samo ako su im funkcijska polja izomorfna.*

Analogni rezultati vrijede i za projektivne mnogostrukosti, te ih mi ovdje nećemo navoditi. Napomenimo samo da (analogoni) Teorem 59 i Korolar 60 vrijede i za projektivne mnogostrukosti.

Primjer 17. Neka je $X \subseteq \mathbb{A}^2_{\mathbb{Q}}$ afina mnogostrukost definirana s $x^2 + y^2 - 1 = 0$, te neka je $P = (-1, 0) \in X$. Racionalno preslikavanje $\phi : X \to \mathbb{A}^1$ definirano s

$$\phi(x, y) = \frac{y}{x+1} = \frac{1-x}{y}$$

nije morfizam pošto nije regulanro u P. Međutim, to preslikavanje šalje točku kružnice Q u koeficijent smjera od $\overline{PQ}$, te je dominatno preslikavanje (štoviše i surjektivno). Preslikavanje $\psi : \mathbb{A}^1 \to X$ definirano s

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

nije regularno (nije definirano u i), i nije surjektivno (P nije u slici), međutim dominatno je. Primjetimo da je ψ inverz od ϕ u točkama gdje su obje funckije definirane. Dakle, X je biracionalno ekvivalentan s $\mathbb{A}^1$, ali nije izomorfan. Primjetimo da je $\mathbb{Q}(X) \simeq \mathbb{Q}(t)$ (D.Z. -dokažite), te da je $\mathbb{Q}(\mathbb{A}^1) \simeq \mathbb{Q}(t)$, dakle kao što smo očekivali, vidimo da su ta 2 funkcijska polja izomorfna.

Pogledajmo sada projektivno zatvorenje $\overline{X}$ od X u $\mathbb{P}^2$, definirano s $x^2 + y^2 = z^2$. Definirajmo preslikavanje $\phi : \overline{X} \to \mathbb{P}^1$ s

$$\phi(x : y : z) = (y : x + z) = (z - x : y).$$

Prvi oblik je definiran svugdje osim u $(1:0:-1)$, dok je drugi definiran svugdje osim u $(1:0:1)$, dakle ϕ je regularna funkcija. Definirajmo $\psi : \mathbb{P}^1 \to \overline{X}$ sa

$$\psi(s:t) = (s^2 - t^2 : 2st : s^2 + t^2).$$

Preslikavanje ψ je definirano svugdje, te je morfizam, te možemo provjeriti da su $\phi \circ \psi$ i $\psi \circ \phi$ identiteta, dakle imamo da je $\overline{X}$ izomorfan s $\mathbb{P}^1$.

Definicija. Neka je $\phi : C_1 \to C_2$ racionalno preslikavanje krivulja. Tada se *stupanj* od ϕ definira kao stupanj proširenja funkcijskih polja $\deg \phi = [k(C_1) : \phi^* k(C_2)]$.

Napomena. Treba biti oprezan da se ne poistovjećuje $k(C_2)$ sa svojom slikom u $k(C_1)$. Npr. promotrimo morfizam $\phi : X = \mathbb{A}^1 \to Y = \mathbb{A}^1$, $\phi(x) = x^2$. Tada ϕ^* šalje $f(x) \in k(x) = k(Y)$ u $f(x^2)$, te je $\phi^*(k(Y)) = k(x^2)$, te je $[k(X) : \phi^*(k(Y))] = 2$. Međutim kada bi $k(Y) = k(x)$ poistovjetili s svojom slikom $\phi^*(k(Y))$, imali bi da je $k(X) = k(Y)$. Poanta je da bitno kako se $\phi^*(k(Y))$ ulaže u $k(X)$.

4.5 Valuacije na funkcijskom polju krivulje

Definicija. Algebarska krivulja (ili samo krivulja, kako ćemo dalje pisati) je 1-dimenzionalnan algebarska mnogostrukost.

Neka je C/k krivulja, te neka je $k(C)$ funkcijsko polje od C.

Definicija. Neka je $P \in C(k)$. Pretpostavimo da je C glatka u P. *Lokalni prsten* $\mathcal{O}_P$ od C u P je skup funkcija $f \in k(C)$ koje su regularne u P.

Neka je $\mathfrak{m}_P := \{f \in \mathcal{O}_P : f(P) = 0\}$. Lako se provjeri da je $\mathfrak{m}_p$ maksimalan ideal u $\mathcal{O}_P$.

Definicija. Definiramo *(normaliziranu) valuaciju* na $\mathcal{O}_P$

$$v_p : k(C) \to \mathbb{Z} \cup \{+\infty\}$$

koji $f \in \mathcal{O}_P$ pridružuje najveći broj d takav da je $f \in \mathfrak{m}_P^d$.

Teorem 62. *Neka je C glatkja krivulja i $P \in C(k)$. Tada vrijedi*

$$\mathcal{O}_P = \{f \in k(C) : v_P(f) \geq 0\}$$

$$\mathfrak{m}_p = \{f \in k(C) : v_P(f) > 0\}$$

$$\mathcal{O}_P^\times = \{f \in k(C) : v_P(f) = 0\}.$$

Definicija. Kažemo da f ima *nultočku reda m* u P ako je $v_P(f) = m > 0$, i *pol reda m* u P ako je $v_P(f) = -m < 0$.

Definicija. Element $t \in k(C)$ takav da t generira $\mathfrak{m}_p$ (ili ekvivalentno $v_P(t) = 1$) se zove *uniformizator* ili *uniformizirajući parametar*.

Ako je t uniformizator, tada se svaka $f \in k(C)^\times$ može jedinstveno zapisati kao $t^n u$, gdje je $u \in \mathcal{O}_P^\times$. Tada je $n = v_P(f)$.

Napomena. Neka je C krivulja zadana s $f(x,y) = 0$ u $\mathbb{A}^2$, i neka je $(a,b) \in C(k)$ točka u kojoj je C glatka, pa je $\frac{\partial f}{\partial y}(a,b) \neq 0$ ili $\frac{\partial f}{\partial x}(a,b) \neq 0$.

- Ako je $\frac{\partial f}{\partial y}(a,b) \neq 0$, tada je $x - a$ uniformizator.
- Ako je $\frac{\partial f}{\partial x}(a,b) \neq 0$, tada je $y - b$ uniformizator.

Primjer 18. Neka je $C : y^2 = x^3 - x$ i neka je $P = (0,0)$. Dokažimo prvo da je y uniformizator u P (bez korištenja gornje napomene). Imamo $\mathfrak{m}_p = (x,y)$, $y^2 = x(x^2-1)$, te je $x^2 - 1 \neq 0$ u $(0,0)$ pa je $x^2 - 1 \in \mathcal{O}_P^\times$. Slijedi da je $x = \frac{y^2}{x^2-1} \in (y)$. Dakle imamo $(x,y) = (y)$, pa je y uniformizator u P, tj. $v_P(y) = 1$. Zbog $x = \frac{y^2}{x^2-1}$, te $\frac{1}{x^2-1} \in \mathcal{O}_P^\times$, slijedi $v_P(x) = 2$.

Poglavlje 5

Divizori

Mogu se promatrati divizori općenitih n-dimenzionalnih algebarskih mnogostrukosti, međutim, mi ćemo u ovom poglavlju samo promatrati krivulje. U cijelom poglavlju će nam krivulje biti **glatke projektivne algebarske** krivulje.

Definicija. *Funkcijsko polje* F/k je konačno generirano proširenje od k stupnja transcendentnosti 1, takvo da je k algebarski zatvoreno u F.

Napomena. Primjetite da je $\mathbb{Q}$ algebarski zatvoren u $\mathbb{Q}(x)$, tj. $\mathbb{Q}(x)$ je polje funkcija nad $\mathbb{Q}$.

Definicija. Neka je C/k krivulja nad algebarski zatvorenim poljem. *Divizor* je formalna suma

$$D := \sum_{P \in C} n_P P,$$

gdje je $n_P \in \mathbb{Z}$, te gdje je samo konačno mnogo $n_P \neq 0$. Skup točaka P za koje je $n_P \neq 0$ se zove *podrška* divizora D. Divizori krivulje C s operacijom zbrajanja (na prirodan način) tvore slobodnu Abelovu grupu, *grupu divizora* od C, koju označavamo s $\operatorname{Div} C$.

Primjer 19. Neka je C projektivna krivulja $x^2 + y^2 = z^2$ nad $\mathbb{Q}$. Neka je $P = (0 : 1 : 1)$, $Q = (1 : 0 : 1)$. Tada je $2P - 3Q$ divizor.

Za funkcijsko polje F/k definiramo X_F kao abstraktnu krivulju s funkcijskim poljem F/k. Sjetimo se da funkcijsko polje određuje algebarsku mnogostrukost do na biracionalnu ekvivalenciju. Za projektivne krivulje, vrijedi i više zahvaljujući sljedećem teoremu.

Teorem 63. *Ako su dvije nesingularne projektivne krvulje biracionalno ekvivalentne, tada su one izomorfne.*

Dokaz. Vidi npr. [2, Chapter 1, Section 6]. □

Dakle svakom funkcijskom polju jednoznačno pridružujemo krivulju.

Definicija. Neka je F/k polje funkcija nad algebarski zatvorenim poljem. *Divizor* od F je formalna suma

$$D := \sum_{P \in X_F} n_P P,$$

s $n_P \in \mathbb{Z}$ i sve osim konačno $n_P = 0$, gdje ovdje X_F označava abstraktnu krivulju pridruženu F. Divizori od F s obzirom na zbrajanje tvore slobdnu Abelovu grupu $\operatorname{Div} F$.

Po definiciji, ako je X glatka projektivna krivulja s funkcijskim poljem F, tada je $\operatorname{Div} F \simeq \operatorname{Div} C$.

Sada želimo definirati divizore nad općim poljima, dakle i nad onima koja nisu algebarski zatvorena.

Definicija. Neka je k polje, te $\overline{k}$ negovo algebarsko zatvorenje, te neka je $G_k = \operatorname{Gal}(\overline{k}/k)$. Divizor $D = \sum n_P P \in \operatorname{Div} C$ je *definiran nad* k ako za sve G_k vrijedi $D^\sigma = D$, gdje je

$$D^\sigma = \sum n_P P^\sigma.$$

Podskup od $\operatorname{Div} C$ divizora definiranih nad k čini podgrupu *k-racionalnih divizora.*

Primjetimo da $D^\sigma = D$ *ne znači* da je $P = P^\sigma$ za sve P u podršci od D, već to znači da je $n_{P^\sigma} = n_P$ za sve $\sigma \in G_k$. Dakle možemo k-racional ni divizor pramatrati kao sumu G_k orbita točaka iz $C(k)$. Dakle dobivamo alternativnu definiciju k-racionalnih divizora:

Definicija. Neka je C/k krivulja. Tada se G_k-orbite od $C(\bar{k})$ zovu *zatvorene točke*. k-racionalni divizor ili samo *racionalni divizor* od C/k je formalna suma

$$D := \sum n_P P,$$

gdje P varira po svim zatvorenim točkama od C/k, $n_P \in \mathbb{Z}$ i $n_P = 0$ za sve osim konačno mnogo P-ova.

Proste ideale od F/k zovemo *mjestima* od F/k. Mjesta od F/k su u bijekiciji s zatvorenim točkama odgovarajuće krivulje X_F/k.

Grupu k-racionalnih divizora od C/k se označava s $\operatorname{Div}_k C$. Za funkcijska polja F/k, nad poljima koja nisu algebarski zatvorena, grupa divizora se definira na isti način kao i kad je polje algebarski zatvoreno.

Napomena. Treba uvijek paziti da radimo razliku između točaka $C(k)$ i zatvorenih točaka od C/k, gdje je prvi skup podskup drugoga. Također primjetimo da je svaka točka iz $C(\bar{k})$ sadržana u nekoj zatvorenoj točki. Također primjetimo da zatvorene točke ovise o polju k, te ćemo zato uvijek pisati C/k kako bilo jasno nad kojim se poljem radi.

Definicija. Neka je $D = \sum n_P P \in \operatorname{Div} C$. Kažemo da je D *efektivan* divizor ako je $n_P \geq 0$ za sve P, te pišemo $D \geq 0$. Ako za divizore D_1, D_2 vrijedi $D_1 - D_2 \geq 0$, tada pišemo $D_1 \geq D_2$.

Definicija. Neka je $f \neq 0$ element funkcijskog polja F/k. *Divizor od* f je

$$\operatorname{div} f := \sum_{P \in X_F} v_P(f)P.$$

Takvi divizori se zovu *glavni divizori*.

Da bi ova definicija bila u skladu s prethodnima, trebamo još pokazati da je $v_P(f) = 0$ osim za konačno mnogo vrijednosti P. Primjetimo da ako je P nultočka od f, tada je svaka točka u orbiti od G_k nultočka od f, tako da ima smisla govoriti je li zatvorena točka nultočka od f.

Teorem 64. *Neka je F funkcijsko polje i neka je $f \in F^\times$. Tada je $v_P(f) = 0$ za sve osim konačno mnogo P.*

Dokaz. Neka je C/k glatka projektivna krivulja s $k(C) \simeq F$, te identificirajmo ta dva polja. Neka je $0 \neq f \in k[C]$. Tada imamo $v_P(f) = 0$ osim ako je zatvorena točka P nultočka od f. Ali skup nultočaka od f je zatvoren skup koji nije jednak cijeloj krivulji C (jer $f \neq 0$ na C). Iz toga slijedi da je taj skup nultočaka konačan (pošto je C ireducibilna svaki zatvoreni pravi podskup je manje dimenzije). Opći slučaj $f = g/h \in k(C)$ se dokazuje analogno jer slijedi da je $v_P(f) = 0$ osim ako P nije nultočka od f ili g. □

Definicija. Neka je C/k krivulja i neka je F/k odgovarajuće funkcijsko polje. Ako je P zatvorena točka od C/k, ili mjesto od F/k, tada je *stupanj* od P dimenzija *polja ostataka* $k(P) = \mathcal{O}_P/\mathfrak{m}_p$ nad k, tj. $\deg P := [k(P) : k]$. Drugim riječima $\deg P$ je za zatvorenu točku P duljina G_K-orbite točaka iz $C(\overline{k})$ sadržanih u P. Neka je $D = \sum n_P P$. Tada se *stupanj* od D definira kao $\deg D := \sum n_P(\deg P)$.

Primjer 20. Primjetimo da ako je k algebarski zatvoren, tada je $\deg D := \sum n_P$. Također, koristeći notaciju iz prethodnog primjera, imamo $\deg(2P - 3Q) = -1$.

Suma glavnih divizora je glavni divizor, pošto je $\operatorname{div} f + \operatorname{div} g = \operatorname{div} fg$. Također $\operatorname{div} 1 = 0$, te je preslikavanje $k(C)^\times \to \operatorname{Div}_k C$ defnirano s $f \mapsto \operatorname{div} f$ homomorfizam grupa. Njegova slika je $\operatorname{Gl}_k C$, grupa k-racionalnih glavnih divizora.

Definicija. Neka je C/k krivulja. Kvocijentna grupa

$$\operatorname{Pic}_k C := \operatorname{Div}_k C / \operatorname{Gl}_k C$$

se naziva *Picardova grupa* od C ili *grupa klasa divizora* od C. Kažemo da su divizori $D_1, D_2 \in \operatorname{Div}_k C$ koji su istoj klasi modulo $\operatorname{Gl}_k C$ *linearno ekvivalentni,* te označavamo to s $D_1 \sim D_2$.

Primjer 21. Neka je E projektivno zatvorenje afine krivulje

$$E_0 : y^2 = x(x-1)(x-7).$$

Dakle E ima model

$$E : y^2z = x(x-z)(x-7z).$$

Prmjetimo da ako je $x = 0$, da to povlači $z = 0$. Promatrajući točke koje su na E a nisu na afinoj karti E_0, presjecamo E s "hiperravninom u beskonačnosti" $z = 0$. Tada slijedi da je $x = 0$, te je $\infty := (0 : 1 : 0)$ jedina točka u E koja nije u E_0. Odredimo divizor funkcije $x \in k(E_0) = k(E)$. Na E_0 funckija x nestaje samo u $P := (0, 0)$. Ali pošto $\operatorname{div} x$ mora iamti stupanj 0, slijedi da je $\operatorname{div} x = nP - n\infty$. Dakle treba odrediti $v_P(x)$. Pošto je

$$\frac{\partial}{\partial x}(y^2 - x(x-1)(x-7)) \neq 0$$

imamo da je y uniformizator u P. Sada imamo da je

$$x = \frac{y^2}{(x-1)(x-7)},$$

pa pošto je $\frac{1}{(x-1)(x-7)} \neq 0$, te time i invertibilan, slijedi da je $v_P(x) = 2$, te je $(x) = 2P - 2\infty$.

Dokažimo sada da postoji točka reda 2 u $\operatorname{Pic} E$. Neka je $D = P - \infty$. Slijedi da je $2P$ glavni divizor, te da je on 0 u $\operatorname{Pic} E$. Da bi dokazali da je E reda 2 u $\operatorname{Pic} E$, treba pokazati da on nije 0, tj. da ne postoji funkcija čiji je divizor D.

Pretpostavimo da je $D = \operatorname{div} f$ za neku funkciju f. Slijedi da je f stupnja 1 (ima 1 nultočku), dakle $[k(E) : k(\mathbb{P}^1)] = 1$, pa je E biracionalan s $\mathbb{P}^1$, pa je $E \simeq \mathbb{P}^1$, po ranije spomenutom teoremu. Ali $E(\mathbb{R})$ ima 2 komponente, a $\mathbb{P}^1(\mathbb{R})$ jednu.

Teorem 65. *Niz*

$$1 \to k^\times \to k(C)^\times \xrightarrow{\text{div}} \operatorname{Div}_k C \to \operatorname{Pic}_k C \to 0$$

je egzaktan.

Dokaz. Jedina tvrdnja koju ostaje dokazati je da je $\ker \operatorname{div} = k^\times$. Jasno je da je $\ker \operatorname{div} \supseteq k^\times$, dokažimo sada obrnutu inkluziju. Ako je $f \in \ker \operatorname{div}$, tada f nema nultočaka ni polova na svim zatvorenim točkama C/k, te tada slijedi da je f invertibilan u koordinatnom prstenu $k[C]$ od C/k. Pošto je $k[C]^\times = k^\times$, tvrdnja slijedi. □

Definicija. Za glavni divizor $\operatorname{div} f = \sum n_P P$, divizor

$$\operatorname{div}_0 f = \sum_{n_P > 0} n_P P \ i \ \operatorname{div}_\infty f = \sum_{n_P < 0} -n_P P$$

se zovu *divizor nula* i divizor polova, tim redoslijedom. Imamo

$$\operatorname{div} f = \operatorname{div}_0 f - \operatorname{div}_\infty f.$$

Definicija. Kažemo da je morfizam $\phi : C_1 \to C_2$ *definiran nad* k ako su C_1, C_2 i funkcija ϕ definirani nad k (tj. svi njezini koeficijenti su definirani nad k).

Lema 66. *Neka je $\phi : C_1 \to C_2$ morfizam definiran nad k i neka je P zatvorena točka od C_1/k. Tada je $\phi(P)$ zatvorena točka od C_2/k.*

Dokaz. Po definiciji, zatvorena točka P je G_k-orbita $\{P_1, \ldots, P_d\}$, gdje je $d = \deg P$. Pošto je po pretpostavci ϕ definiran nad k, vrijedi da je $\phi(P_i)^\sigma = \phi(P_i^\sigma)$ za sve $\sigma \in G_k$. Slijedi da svaki $\sigma \in G_k$ fiksira skup $\{\phi(P_1), \ldots, \phi(P_d)\}$, dakle taj skup je unija G_k orbita. Pošto je $\{P_1, \ldots, P_d\}$ jedna G_k orbita, za svaki i, postoji $\sigma \in G_k$ takav da $P_i = P_1^\sigma$, pa je onda i $\phi(P_i) = \phi(P_1)^\sigma$, te onda slijedi da je skup $\{\phi(P_1), \ldots, \phi(P_d)\}$ jedna G_k-orbita. □

Dakle, sada možemo morfizam $\phi : C_1 \to C_2$ definiran nad k smatrati preslikavanjem zatvorenih točaka.

Definicija. Neka je $\phi : C_1 \to C_2$ morfizam definiran nad k i neka je $\phi^* : k(C_2) \to k(C_1)$ odgovarajući morfizam funkcijskih polja. Indeks grananja (ili stupanj grananja) od ϕ u zatvorenoj točki $P \in C_1$ je $e_\phi := v_P(\phi^* t_Q)$, gdje je t_Q uniformizator u $Q = \phi(P)$. Ako je $e_\phi(P) = 1$, tada je ϕ nerazgranat u P, te ako je $e_\phi(P) = 1$ za sve zatvorene točke P od C_1/k, tada kažemo da je ϕ *nerazgranato.*

Definicija. Neka je $\phi : C_1 \to C_2$ morfizam definiran nad k. *Preslikavanje povlačenja* ϕ^* na divizorima je homomorfizam $\phi^* : \mathrm{Div}_k C_2 \to \mathrm{Div}_k C_1$ definirano s

$$\phi^*(Q) := \sum_{P \in \phi^{-1}(Q)} e_\phi(P) P,$$

gdje je Q divizor koji se sastoji od jedne točke Q, tj $\operatorname{div} Q = Q$.

Peslikavanje guranja ϕ_* je homomorfizam $\phi_* : \mathrm{Div}\, C_1 \to \mathrm{Div}\, C_2$ koje je definirano s

$$\phi_*(P) = [k(P) : \phi^*(k(\phi(P)))]\phi(P) = \frac{\deg P}{\deg \phi(P)}\phi(P).$$

Vrijedi da je $\phi_*(\phi^*(D)) = \deg(\phi) D$, tj. $\phi_* \circ \phi^*$ je množenje s $\deg \phi$ u $\mathrm{Div}_k C_2$.

Napomena. Primjetimo da ϕ^* označava i dualni morfizam $k(C_2) \to k(C_1)$; to je zato što vrijedi

$$\phi^* \operatorname{div} f = \phi^* \operatorname{div} g \iff \phi^* f = \lambda \phi^* g, \text{ za neki } \lambda \in k^\times.$$

Primjer 22. Neka je $C_1 : x^2 + y^2 - 1 = 0$, te neka je $C_2 = \mathbb{A}^1$, te neka je $\phi : C_1 \to C_2$ definirana s $\Phi(x, y) = x^2$. Primjetimo da je u svakoj točki $c \in \mathbb{A}^1$ uniformizator $t_c = x - c$. Sada je funkcija $\Phi^* : k(C_2) \to k(C_1)$ funkcija koja pridružuje funkciji $f(x)$ funkciju $f(x^2) \in k(C_1)$. Primjetimo prvo da je funkcija stupnja 4. Neka je $P = (0, 1)$. Pošto je $x^2 = 1 - y^2 = (1 - y)(-1 - y)$, vidimo da je x uniformizator u P. Vidimo da je $\phi(P) = 0$, pa je $e_\phi(P) = v_P(x^2) = 2$ (jer je uniformizator u $0 \in C_2$ funkcija x). Neka je sada $t_1 \in < 0, 1 >$, te neka je $P_1 = (t_1, t_2)$. Pošto je

$$x^2 + y^2 - 1 = x^2 - (y^2 - t_2^2) + t_2^2 - 1 = x^2 - t_1^2 + (y - t_2)(y + t_2) = 0,$$

pa slijedi da je $(y - t_2) = (x^2 - t_1^2)/(y + t_2)$, pa vidimo da je $y - t_2 \in (x - t_1)$, pa je $x - t_1$ uniformizator.

Vidimo da je $\phi(P_1) = t_1^2$, te je uniformizator u $\phi(P_1)$ jednak $x - t_1^2$, dakle sada se pitamo koliko je $e_\phi(P) = v_{P_1}(x^2 - t_1^2)$, te odmah vidimo da je to 1. Lako provjerimo i da je $e_\phi(\pm 1, 0) = e_\phi(\pm 0, 1) = 2$.

Dakle

Sljedeći teorem ćemo ostaviti bez dokaza.

Teorem 67. *Neka je $\Phi : C_1 \to C_2$ morfizam krivulja definiranih nad k. Tada za svaku zatvorenu točku Q od C_2/k, vrijedi*

$$\deg \phi^*(Q) = \deg \phi \deg Q.$$

Posljedica je sljedeći teorem, koji ostavljamo također bez dokaza.

Teorem 68. *Neka je $f \in k(C)^\times$ za krivulju C/k. Tada je* $\deg \operatorname{div} f = 0$*, te ako je $f \notin k^\times$, tada*

$$\deg \operatorname{div}_0 f = \deg \operatorname{div}_\infty f = [k(C) : k(f)].$$

5.1 Divizori stupnja 0

Očito je da za krivulju C/k divizori stupnja 0 čine podgrupu $\operatorname{Div}_k^0 C$ od $\operatorname{Div}_k C$, te da je $\operatorname{Gl}_k C$ podgrupa od $\operatorname{Div}_k^0 C$.

Definicija. Definiramo $\operatorname{Pic}_k^0 C := \operatorname{Div}_k^0 C / \operatorname{Gl}_k C$.

Dakle vidimo da imamo egzaktan niz

$$1 \to k^\times \to k(C)^\times \to \operatorname{Div}_k^0 C \to \operatorname{Pic}_k^0 C \to 0.$$

Sve grupe divizora koje smo promatrali do sada su bile bekonačne, međutim $\operatorname{Pic}_k^0 C$ ne mora biti beskonačan. Promtrimo slučaj kada je trivijalan.

Teorem 69. *Pretpostavimo da je k algebarski zatvoreno polje, te neka je C/k krivulja. Tada je $C \simeq \mathbb{P}^1$ ako i samo ako je* $\operatorname{Pic}_k^0 C = \{0\}$.

Dokaz. Neka je $C \simeq \mathbb{P}^1$. Tada je svaka točka $P = (a_0 : a_1) \in \mathbb{P}^1$ nultočka polinoma $f_P(x_0, x_1) = a_1 x_0 - a_0 x_1$, te za svaki divizor $D = \sum n_p P$, možemo konstruirati odgovarajuću homogenu racionalnu funkciju funkciju $f = \prod f_P^{n_P}$. Ako D ima stupanj 0, tada brojnik i nazivnik od f imaju isti stupanj i f je element od $k(\mathbb{P}^1) \simeq k(C)$, da je $D = \operatorname{div} f$. Dakle, $\operatorname{div}_k C = \operatorname{Gl}_k C$ i $\operatorname{Pic}_k^0 C = 0$.

Neka su sada P i Q različite točke na $C(k)$ - takve točke sigurno postoje pošto je k algebarski zatvoreno polje. Tada je $f = f_P/f_Q$ ne-konstantna funkcija na $C(k)$, koja definira morfizam $\phi : C \to \mathbb{P}^1$

$$\phi(T) = (f_P(T) : f_Q(T)).$$

Morfizam f je stupnja 1, te je izomorfizam (DZ). □

Primjetimo sada da je "samo ako" implikacija istinita i ako ne pretpostavimo da je k algebarski zatvoreno polje. Međutim, obrat ne vrijedi - postoje krivulje C/k takve da je $\mathrm{Pic}_k^0 C = \{0\}$, koje nisu izomorfne $\mathbb{P}^1$. Primjetimo da ne možemo uzeti da su P i Q zatvorene točke (koje nisu obične točke) jer će tada dobiveno preslikavanje f biti stupnja većeg od 1.

Kao primjer možemo uzeti neku eliptičku krivulju nad $\mathbb{Q}$ sa samo jednom točkom u beskonačnosti (slutnja je da je ovo istina za pola eliptičkih krivulja).

Međutim iz dokaza teorema slijedi da je obrat istina ako postoje barem 2 točke na $C(k)$. Dakle, imamo:

Korolar 70. *Neka je $C(k)$ krivulja s barem 2 k-racionalne točke. Tada je C/k izomorfno nad k s $\mathbb{P}^1/k$ ako i samo ako je $\mathrm{Pic}_k^0 C = \{0\}$.*

Kao posljedica, krivulja genusa > 0 s barem 2 točke u k ne može imati trivijalan $\mathrm{Pic}_k^0 C$.

Poglavlje 6

Riemann-Rochov teorem

Definicija. Za $D \in \operatorname{Div} C$, definiramo *linearni sustav* ili *Riemann-Rochov prostor*

$$L(D) := \{f \in k(C)^\times : \operatorname{div} f + D \geq 0\} \cup \{0\}.$$

Propozicija 71. *Skup $L(D)$ je vektorski potprostor (nad k) od $k(C)$.*

Dokaz. Pretpostavimo da je $D = \sum n_P P$. Ako je $f \in L(D)$, tada je $v_P(f) \geq -n_P$ za sve P. Za fiksan P neka je V_P skup funckija koje zadovoljavaju $v_P(f) \geq -n_P$; taj skup sadrži 0 te je zatvoren s obzirom na zbrajanje i množenje konstantam iz k, te je vektorski prostor. Tada je i $L(D) = \bigcap_P V_P$ vektorski prostor nad k. □

Primjer 23. Ako je $D = 0$, tada je $L(D)$ skup funkcija $f \in k(C)$ takvih da je $\operatorname{div} f \geq 0$. Pošto $\deg \operatorname{div} f = 0$, slijedi da je $\operatorname{div} f = 0$, što je istina samo za $f \in k^\times$. Dakle $L(D) = k$.

Primjer 24. Neka je $D = 2P$ za zatvorenu točku P. Sada je $L(D)$ skup funkcija koje imaju najviše dvostruki pol (dakle ili nemaju pol, ili imaju jednostruki ili dvostruki pol) u P i nemaju pol u nijednoj drugoj zatvorenoj točki od C. Ako je $D = 3P - 2Q$, tada je $L(D)$ skup $f \in k(C)$ takvih da f ima najviše trostruki pol, te barem dvostruku nultočku (dakle možda i nultočku višeg reda) u Q.

Primjetimo da ako je $D_1 \leq D_2$, tada je $L(D_1) \subseteq L(D_2)$.

Primjer 25. Neka je $C = \mathbb{P}^1 \supset \mathbb{A}^1$. Tada je $k(C) = k[x]$. Neka je $\infty \in \mathbb{P}^1(k)$ jedinstven točka izvan $\mathbb{A}^1$. Dakle imamo $\operatorname{ord}_\infty(x) = -1$,te općenitije $\operatorname{ord}_\infty(p) = -\deg p$ za svaki $p \in k[x]$. Neka je $D = 3\infty$.

Što je $L(3\infty)$? Ako je $f = \frac{p(x)}{q(x)} \in L(3\infty)$, tada su p i q relativno mprosti polinomi u $k[x]$, te q nema zatvorenu nultočku P u $\mathbb{A}^1$, pa zaključujemo da je q konstanta, te možemo pretpostaviti da je $q = 1$. Dakle $f = p$ je polinom u x. Pošto je $f \in L(3\infty)$, slijedi $\operatorname{div} f + 3\infty \geq 0$, pa je $-\deg p \geq -3$, tj. $\deg p \leq 3$. Dakle $L(3\infty)$ je k-vektorski prostor polinoma u $k[x]$ stupnja ≤ 3. Taj vektorski prostor ima bazu $\{1, t, t^2, t^3\}$, pa je $\dim_k L(3\infty) = 4$.

Neka je sada $P \in \mathbb{A}^1(k)$ vrijednost u kojoj x poprima vrijednost 7. Što je $L(3\infty - P)$? To je potprostor od $L(3\infty)$ koji se sastoji od polinoma koji imaju barem jednostruku nultočku u P, tj. da su djeljivi s $x - 7$. Dakle

$$L(3\infty - P) = \{(x-7)g(x) : g \in k[x],\ \deg g \leq 2\}.$$

Lema 72. *Vrijedi $L(D) \neq \{0\}$ ako i samo ako je $D \sim D'$ za neki divizor $D' \geq 0$.*

Dokaz. Ako je $0 \neq f \in L(D)$, tada je $\operatorname{div} f \geq -D$ i $D \sim D' = D + \operatorname{div} f \geq 0$. Obrnuto, ako je $D \sim D' \geq 0$, tada je $D + \operatorname{div} f \geq 0$, tj. $\operatorname{div} f \geq -D$, za neki $f \in k(C)^\times$, dakle $L(D) \neq \{0\}$. □

Lema 73. *Za bilo koja dva divizora $A \leq B$, imamo $L(A) \subseteq L(B)$ i*

$$\dim(L(B)/L(A)) \leq \deg B - \deg A. \tag{6.1}$$

Dokaz. Jasno je da $L(A) \subseteq L(B)$ i da nejednakost (6.1) vrijedi ako je $A = B$. Pretpostavimo sada da je $B = A + P$ za neku zatvorenu točku P. Neka je t uniformizator u P i neka je $k(P) = \mathcal{O}_P/\mathfrak{m}_P$ polje ostataka u P i neka je $n = v_P(B)$. Sada definirajmo linearnu transformaciju $\phi : L(B) \to k(P)$ s $\phi(f) = t^n f \mod m_P$. Vrijedi $v_P(t^n f) = n + v_P f \geq 0$ za $f \in L(B)$. Dakle imamo $t^n f \in \mathcal{O}_P$, pa je ϕ dobro definirano. Jezgra ovog preslikavanja sastoji od funkcija za koje je $v_P(t^n f) \geq 1$, tj. $v_P(f) \geq 1 - n = -v_P(A)$, a taj potprostor je upravo $L(A)$. Dakle imamo $L(B)/L(A) \simeq L(B)/\ker\phi \simeq \operatorname{im}\phi$, pa je

$$\dim(L(B)/L(A)) = \dim(\operatorname{im}\phi) \leq \dim k(P) = \deg P = \deg B - \deg A.$$

Sada se opći rezultat dokazuje višestrukom primjenom dobivenog rezultata. □

Teorem 74. *Za svaki divizor D, imamo da je $\dim L(D) \leq \deg D + 1$.*

Dokaz. Koristeći lemu 73 s $B = D$ i $A = 0$, imamo

$$\dim(L(D)/L(0)) \leq \deg D - \deg 0 = \deg D.$$

S druge strane, znamo da je $L(0) = k$, pa je

$$\dim L(D) = \dim(L(D)/L(0)) + 1 \leq \deg D + 1.$$

□

Iz ovog teorema slijedi da je dimenzija od $L(D)$ konačna za svaki divizor D.

Definicija. Za svaki $D \in \operatorname{Div}_k C$, definiramo $l(D) := \dim_k L(D) \in \mathbb{N}_0$.

Primjer 26. Ako je $D = 0$, tada je $L(D) = k$, pa je $l(D) = 1$.

Propozicija 75. *Ako je $\deg D < 0$, tada je $L(D) = \{0\}$ i $l(D) = 0$.*

Dokaz. Neka je $\deg D < 0$, te neka je $0 \neq f \in L(D)$. Dakle $\operatorname{div} f + D \geq 0$. Međutim, po pretpostavci je $\deg(\operatorname{div} f + D) = \deg D < 0$, što daje kontradikciju. □

Propozicija 76. *Ako su D i D' linearno ekvivlentni, tada je $l(D) = l(D')$.*

Dokaz. Neka je $D = D' + \operatorname{div} g$ za neki $g \in k(C)^\times$. Ako je $0 \neq f \in L(D)$, tada je $\operatorname{div} f + D \geq 0$, pa je $\operatorname{div} f + \operatorname{div} g + D' \geq 0$, pa je $\operatorname{div} fg + D' \geq 0$, tj. $fg \in L(D')$. Dakle množenje s g preslikava injektivno $L(D)$ u $L(D')$ pošto je množenje s g injektivno u $k(C)^\times$. Analogno množenje s g^{-1} injektivno preslikava $L(D')$ u $L(D)$. Dakle ova 2 preslikavanja su (međusobno inverzni) izomorfizmi vektorskih prostora, pa su i dimenzije tih vektorskih prostora jednake. □

Lema 77. *Ako je $\deg D = 0$, tada je $l(D) = 1$ ako je D glavni divizor, te $l(D) = 0$ ako nije.*

Dokaz. Ako je $D = \operatorname{div} f$ glavni, tada je $f \in L(D)$, pa je $l(D) \geq 1$, te po Lemi 72, potoji neki $D' \geq 0$, takav da je $D \sim D'$. Ali pošto je $\deg D' = \deg D = 0$, slijedi da je $D' = 0$, pa je $l(D) = l(0) = 1$.

Sada ćemo dokazati da ako je $l(D) > 0$, da D mora biti glavni divizor; pretpostavimo dakle da je $l(D) \geq 1$. Istim argumentom kao i prije zaključujemo da je $D \sim D' = 0$, pa je $l(D) = 1$. Dakle postoji $0 \neq f \in L(D)$, pa pošto je $\operatorname{div} f \geq -D$, imamo da je $D + \operatorname{div} f \geq 0$. Međutim, vrijedi da je $\deg(D + \operatorname{div} f) = 0$, pa je $D + \operatorname{div} f = 0$, te je $D = -\operatorname{div} f = \operatorname{div}(1/f)$, te smo dobili da je D glavni divizor. □

Teorem 78. *Postoji $g \in \mathbb{N}_0$ takav da je*

$$\deg D + 1 - l(D) \leq g$$

za sve $D \in \operatorname{Div}_k C$.

Dokaz. Neka je $f \in k(C)$ transcedentna nad k, i neka je $A = \operatorname{div}_\infty f \geq 0$. Neka su $v_1, \ldots, v_d$ baza za $k(C)/k(f)$, gdje je $d = \deg A = [k(C) : k(f)]$ (po Teoremu 68). Neka je $B \geq 0$ takav da je $\operatorname{div} v_i \geq -B$ za sve v_i.

Sada primjetimo da je skup $S = \{v_i f^j : 1 \leq i \leq d, 0 \leq j \leq n\}$ linearno nezavisan nad k, pošto je f transcedentan nad k, te su v_i linearno nezavisni nad $k(f)$. Također imamo $S \subseteq L(nA + B)$, pošto je $\operatorname{div}(v_i f^j) \geq -nA - B$, za sve $v_i f^j \in S$. Imamo

$$l(nA + B) \geq d(n + 1) = (n + 1) \deg A \tag{6.2}$$

za sve $n \geq 0$. S druge strane imamo $nA \leq nA + B$, te po lemi 73 slijedi

$$\dim_k(L(nA+B)/L(nA)) = l(nA+B) - l(nA) \leq \deg(nA+B) - \deg(nA) = \deg B. \tag{6.3}$$

Kombiniranjem (6.2) i (6.3) dobivamo

$$l(nA) \geq l(nA+B) - \deg B \geq (n+1)\deg A - \deg B = \deg(nA) + (\deg A - \deg B).$$

Slijedi da je

$$\deg(nA) + 1 - l(nA) \leq \deg B - \deg A + 1$$

za sve $n \geq 0$. Stavimo sada $g = \deg B - \deg A + 1$. Dakle imamo

$$\deg nA + 1 - l(nA) \leq g. \tag{6.4}$$

Sada želimo ovu tvrdnju dokazati za proizvoljni divizor u $\mathrm{Div}_k C$, te neka je $D = D_0 - D_\infty$, $D_0, D_\infty \geq 0$. Tvrdimo da je $D_0 \sim D'$, za neki efektivni divizor $D' \leq nA$, za neki n. Po lemi 73 imamo

$$\dim_k(L(nA)/L(nA-D_0)) = l(nA)-l(nA-D_0) \leq \deg(nA)-\deg(nA-D_0) = \deg D_0,$$

te primjenom (6.4) dobivamo

$$l(nA - D_0) \geq l(nA) - \deg D_0 \geq \deg(nA) + 1 - g + \deg D_0.$$

Očito je desna strana pozitivna za dovoljno velik n, pa izaberimo n takav da je $l(nA-D_0) > 0$ i neka je $0 \neq f \in L(nA-D_0)$. Definirajmo sada $D' := D_0 - \mathrm{div}\, f$; vrijedi

$$D' = D_0 - \mathrm{div}\, f \leq D_0 - (D_0 - nA) = nA,$$

kao što smo i tvrdili. Imamo da je $D \leq D_0$, pa je $l(D_0) - l(D) \leq \deg D_0 - \deg D$, te je

$$\begin{aligned} \deg D + 1 - l(D) &\leq \deg D_0 + 1 - l(D_0) = \deg D' + 1 - l(D') \\ &\leq \deg nA + 1 - l(nA) \leq g, \end{aligned}$$

gdje smo drugu nejednakost dobili na isti način kao i prvu. □

Sada smo dokazali da je vrijednost $\deg D - l(D)$ omeđena za sve $D \in \mathrm{Div}_k C$. To motivira sljedeću oznaku:

$$r(D) := \deg D - l(D),$$

za koju očito vrijedi

$$r(D) \leq g - 1. \tag{6.5}$$

Vrijedi da ako je $A \leq B$, tada je $r(A) \leq r(B)$, te ako je $A \sim B$, tada je $r(A) = r(B)$.

Imamo sljedeću definiciju.

Definicija. *Genus* krivulje C/k se definira kao

$$g := max\{r(D) + 1 : D \in \mathrm{Div}_k C\}.$$

Upravo definirani genus se nekada naziva i geometrijski genus. Postoji i aritmetički genus, međutim za glatke projektivne krivulje se te dvije vrijednosti poklapaju.

Teorem 79 (Riemannov teorem)**.** *Neka je C/k krivulja genusa g. Tada je $r(D) \leq g - 1$ za sve $D \in \mathrm{Div}_k C$, te jednakost vrijedi za sve divizore dovljno velikog stupnja.*

Dokaz. Neka je A divizor takav da je $r(A) = g-1$, takav A postoji po definiciji genusa. Pokazat ćemo da je $r(D) = g-1$ kad god je $\deg D \geq \deg A + g$. Pretpostavimo da je $\deg D \geq \deg A + g$; tada imamo $r(D-A) = \deg(D-A) - l(D-A) \leq g-1$, pa je

$$l(D-A) \geq \deg(D-A) + 1 - g \geq \deg A + g - \deg A + 1 - g = 1.$$

Dakle postoji $0 \neq f \in L(D-A)$, te neka je $D' = D + \operatorname{div} f \geq D + A - D = A$. Sada je

$$r(D) = r(D') \geq r(A) = g - 1.$$

S druge strane znamo po definiciji genusa da je $r(D) \leq g-1$, dakle imamo $r(D) = g-1$. □

Riemann-Rochov teorem će nam biti preciznija formulacija Riemannovog teorema, on će nam točno reći koliko je $r(D)$ daleko od $g-1$ za neki dani divizor.

Definicija. Neka je C/k krivulja genusa g. Za $D \in \operatorname{Div}_k C$, definiramo *indeks specijalnosti* od D kao

$$i(D) := g - 1 - r(D).$$

Divizori za koje vrijedi $i(D) > 0$ se zovu *specijalni divizori*.

Po Riemannovom teoremu znamo da je $i(D) = 0$ za sve D-ove dovoljno velikog stupnja $i(D) = 0$, te da je $i(0) = g$.

6.1 Prsten adela

Sada ćemo definirati prsten adela koji će nam omogućiti bolje razumijevanje indeksa specijalnosti.

Definicija. *Prsten adela* od funkcijskog polja F/k s oznakom $\mathcal{A}_F$ ili samo $\mathcal{A}$, je potprsten direktnog produkta $\prod_P F$, čiji su svi elementi $\alpha = (\alpha_P)$ za koje je $\alpha_P \in \mathcal{O}_P$ za sve osim konačno mnogo P-ova. Elementi od $\mathcal{A}$ se zovu *adeli*.

Primjetimo da možemo kanonski uložiti funkcijsko polje F/k u $\mathcal{A}$:

$$f \mapsto (f, f, f, \ldots).$$

Adeli koji su dobiveni na ovaj način se zovu *glavni adeli*. Primjetimo da je prsten adela $\mathcal{A}$ vektorski prostor nad k. Proširujemo valuaciju $v_P(\alpha) = v_P(\alpha_P)$ za $\alpha_P \neq 0$ te $v_P(0) = \infty$.

Definicija. Za divizor $D \in \operatorname{Div}_k C$, *prostor adela* od D je sljedeći vektorski prostor nad k

$$\mathcal{A}(D) := \{\alpha \in \mathcal{A} : v_P(\alpha) \geq -v_P(D) \text{ za sve } P \in C\}.$$

Primjetimo da je po definiciji $L(D) = \mathcal{A}(D) \cap F$, te je očito $\mathcal{A}(D)$ potprostor od $\mathcal{A}$. Dokažimo sada 3 leme.

Lema 80. *Za svaka dva divizora $A \leq B$ imamo $\mathcal{A}(A) \subseteq \mathcal{A}(B)$ i*

$$\dim_k(\mathcal{A}(B)/\mathcal{A}(A)) = \deg B - \deg A. \tag{6.6}$$

Dokaz. Inkluzija $\mathcal{A}(A) \subseteq \mathcal{A}(B)$ očito vrijedi. Kao i prije, dokazat ćemo (6.6), tako da promotrimo slučaj $B = A + P$ za neko mjesto P, te iz tog slučaja zaključimo opći slučaj.

Izaberimo uniformizator t u P i definirajmo linearno preslikavanje $\phi : \mathcal{A}(B) \to k(P)$ s $\phi(f) = (t^n f_P)(P)$, gdje je $n = v_P(B)$. Preslikavanje ϕ je surjektivno i jezgra mu je $\mathcal{A}(A)$, dakle

$$\dim_k(\mathcal{A}(B)/\mathcal{A}(A)) = \dim k(P) = \deg P = \deg B - \deg A.$$

□

Lema 81. *Za bilo koja dva divizora $A \leq B$, imamo $\mathcal{A}(A) + F \subseteq \mathcal{A}(B) + F$ i*

$$\dim_k \frac{\mathcal{A}(B) + F}{\mathcal{A}(A) + F} = r(B) - r(A),$$

gdje je F uložen u $\mathcal{A}$.

Dokaz. Neka je $S = \mathcal{A}(B)$, te $N = \mathcal{A}(A) + F$. Tada je po drugom teoremu o izomorfizmu

$$\frac{\mathcal{A}(B) + F}{\mathcal{A}(A) + F} = \frac{S + N}{N} \simeq \frac{S}{S \cap N} = \frac{\mathcal{A}(B)}{\mathcal{A}(B) \cap (\mathcal{A}(A) + F)} = \frac{\mathcal{A}(B)}{\mathcal{A}(A) + L(B)},$$

te je po trećem teoremu o izomorfizmu

$$\frac{\mathcal{A}(B)}{\mathcal{A}(A) + L(B)} \simeq \frac{\mathcal{A}(B)/\mathcal{A}(A)}{(\mathcal{A}(A) + L(B))/\mathcal{A}(A)}.$$

Sada je po lemi 80

$$\dim_k \frac{\mathcal{A}(B) + F}{\mathcal{A}(A) + F} = \deg B - \deg A - \dim_k \frac{(\mathcal{A}(A) + L(B))}{\mathcal{A}(A)}.$$

S druge strane, opet po drugom teoremu o izomorfizmu vrijedi

$$\dim_k \frac{\mathcal{A}(A) + L(B)}{\mathcal{A}(A)} = \dim_k \frac{L(B)}{\mathcal{A}(A) \cap L(B)} = \dim_k \frac{L(B)}{\mathcal{A}(A) \cap \mathcal{A}(B) \cap F}$$
$$= \dim_k \frac{L(B)}{\mathcal{A}(A) \cap F} = \dim_k \frac{L(B)}{L(A)} = l(B) - l(A).$$

Dakle imamo

$$\dim_k \frac{\mathcal{A}(B) + F}{\mathcal{A}(A) + F} = \deg B - \deg A - (l(B) - l(A)) = r(B) - r(A).$$

□

Lema 82. *Za svaki divizor D za koji je $r(D) = g - 1$ imamo $\mathcal{A} = \mathcal{A}(D) + F$.*

Dokaz. Neka je $\alpha \in \mathcal{A}$. Neka je $D' \geq D$ takav da je $\alpha \in \mathcal{A}(D') + F$ - ovo je očito moguće. Imamo da je

$$g - 1 = r(D) \leq r(D') \leq g - 1,$$

po Riemannovom teoremu, pa je $r(D') = g - 1$. Sada po lemi 81 imamo

$$\dim_k \frac{\mathcal{A}(D') + F}{\mathcal{A}(D) + F} = r(D') - r(D) = 0,$$

pa je $\mathcal{A}(D') + F = \mathcal{A}(D) + F$, pa slijedi da je $\alpha \in \mathcal{A}(D) + F$. □

Sada dobivene rezultate možemo primjeniti tako da izrazimo indeks specijalnosti nekog divizora kroz njegov prostor adela.

Teorem 83. *Neka je F/k funkcijsko polje. Za svaki $D \in \mathrm{Div}_k F$ imamo*

$$i(D) = \dim_k \frac{\mathcal{A}}{\mathcal{A}(D) + F}.$$

Dokaz. Po Riemannovom teoremu, postoji divizor $D' \geq D$ za koji je $r(D') = g - 1$. Po prethodnoj lemi imamo $\mathcal{A} = \mathcal{A}(D') + F$, pa je

$$\dim_k \frac{\mathcal{A}}{\mathcal{A}(D) + F} = \dim_k \frac{\mathcal{A}(D') + F}{\mathcal{A}(D) + F} = r(D') - r(D) = g - 1 - r(D) = i(D).$$

□

6.2 Diferencijali

Definicija. Neka je F/k funkcijsko polje i neka je $\mathcal{A}$ njegov prsten adela. Za divizor $D \in \mathrm{Div}_k F$, definiramo prostor *Weilovih diferencijala* $\Omega(D)$ kao ortogonalni komplement od $\mathcal{A}(D) + F$ u $\mathcal{A}$. Drugim riječima to je skup svih linearnih funkcionala $w : \mathcal{A} \to k$ čija jezgra sadrži $\mathcal{A}(D) + F$. Vektorski prostor nad k

$$\Omega = \Omega_F := \bigcup_{D \in \mathrm{Div}_k F} \Omega(D)$$

je prostor *Weilovih diferencijala* za F/k.

Jasno je da je Ω vektorski prostor nad k: za $\omega_1 \in \Omega(D_1)$ i $\omega_2 \in \Omega(D_2)$, vrijedi da je $\omega_1 + \omega_2 \in D_3$, gdje je $D_3 = D_1 \wedge D_2$ je definiran s $v_P(D) = \min(v_P(D_1), v_P(D_2))$.

Lema 84. *Za svaki $D \in \mathrm{Div}_k F$, imamo* $\dim \Omega(D) = i(D)$.

Dokaz. Po teoremu 83, imamo $i(D) = \dim_k \mathcal{A}/(\mathcal{A}(D) + F)$, te je ta dimenzija konačna, iz čega slijedi da je dimenzija ovog vektorskog prostora jednaka dimenziji dualnog vektorskog prostora. Dakle $\mathcal{A}/(\mathcal{A}(D) + F)$ je kanonski izomorfno, po prvom teoremu o izomorfizmu, s $(\mathcal{A}(D) + F)^{\perp} = \Omega(D)$. Dakle $\dim_k \Omega(D) = i(D)$. □

Osim što je $\Omega(D)$ vektorski prostor nad k, on će biti i vektorski prostor nad F, uz definciju da, za $f \in F$, $\omega \in \Omega$ je $f\omega$ linearni funkcijonal koji šalje α u $\omega(f\alpha)$, za sve $\alpha \in \mathcal{A}$. Zaista, pošto su $\omega_1, \omega_2 \in \Omega_D$ linearni funkcijonali, za $f, g \in F$ vrijedi

$$(f(\omega_1 + \omega_2))(\alpha) = (\omega_1 + \omega_2)(f\alpha) = \omega_1(f\alpha) + \omega_2(f\alpha),$$

$$(fg)\omega_1(\alpha) = \omega_1(fg\alpha) = f(\omega_1(g\alpha)) = f(g\omega_1(\alpha)).$$

Teorem 85. *Neka je F/k funkcijsko polje i neka je Ω prostor Weilovih diferencijala; tada je* $\dim_F \Omega = 1$.

Dokaz. Neka su $\omega_1, \omega_2 \in \Omega$. Primjetimo da je $\Omega \neq 0$, jer ako uzmemo divizor D koji je "dovoljno" negativnog stupnja, tada će $i(D) > 0$, te će omega biti pozitivne dimenzije (nad k). Dokazat ćemo da je $\omega_1/\omega_2 \in F$.

Neka je $\omega_1 \in \Omega(D_1)$, $\omega_2 \in \Omega(D_2)$, te definirajmo za fiksni divizor D koji ćemo tek odrediti, k-linearno preslikavanje

$$\begin{aligned} \phi_{\omega_i, D} : L(D_i + D) &\to \Omega(-D) \\ f &\mapsto f\omega_i \end{aligned}$$

Za svaki $\alpha + g \in \mathcal{A}(-D) + F$, imamo

$$(f\omega_i)(\alpha + g) = \omega_i(f\alpha) + \omega_i(fg) = 0 + 0 = 0,$$

pošto je $fg \in F$ (pa je zato $\omega_i(fg) = 0$) te je

$$v_P(f\alpha) = v_P(f) + v_P(\alpha) \geq v_P(-D_i - D) + v_P(D) = v_P(-D_i),$$

za sve P-ove, pa je $\omega_i(f\alpha) = 0$. Sada smo dokazali da je $\phi_{\omega_i, D}$ dobro definiran, te je očito injektivan jer je $\Omega(-D)$ vektorski prostor nad F.

Sada tvrdimo da je za odgovarjaući $D \in \mathrm{Div}_k F$,

$$\phi_{\omega_1, D}(L(D_1 + D)) \cap \phi_{\omega_2, D}(L(D_2 + D)) \neq \{0\}. \tag{6.7}$$

Po Riemannovom teoremu, možemo izabrati $D > 0$ dovoljno velikog stupnja, takvog da je $r(D_i + D) = g - 1$ za $i = 1, 2$. Neka je $U_i := \phi_{\omega_i, D}(L(D_i + D))$. Imamo

$$\dim_k \Omega(-D) = i(-D) = g - 1 - r(-D) = g - 1 - \deg(-D) - l(-D) = g - 1 + \deg D,$$

jer je $l(-D) = 0$ za $D > 0$. Imamo da je $U_1 + U_2 \subseteq \Omega(-D)$, te je

$$\dim_k \Omega(-D) \geq \dim(U_1 + U_2) = \dim_k U_1 + \dim_k U_2 - \dim_k(U_1 \cap U_2),$$

pa je

$$\begin{aligned}
&\dim_k(U_1 \cap U_2) \geq \dim_k U_1 + \dim_k U_2 - \dim_k \Omega(-D) \\
&= l(D_1 + D) + l(D_2 + D) - g + 1 - \deg D \\
&= \deg(D_1 + D) - r(D_1 + D) + \deg(D_2 + D) - r_2(D_2 + D) - g + 1 - \deg D \\
&= \deg(D_1 + D) - g + 1 + \deg(D_2 + D) - g + 1 - g + 1 - \deg D \\
&= \deg D + \deg D_1 + \deg D_2 - 3g + 3,
\end{aligned}$$

pa očito izborom D dovoljno velikog stupnja možemo napraviti desnu stranu pozitivnom. Iz toga zaključujemo da za taj D vrijedi $U_1 \cap U_2 \neq \{0\}$.

Dakle, sada postoje $f_1 \in L(D_1+D)$ i $f_2 \in L(D_2+D)$ takvi da je $\phi_{\omega_1,D}(f_1) = \phi_{\omega_2,D}(f_2)$, što znači da je $f_1\omega_1 = f_2\omega_2 \neq 0$, pa je $\omega_1/\omega_2 = f_2/f_1 \in F$, što smo i htjeli dokazati. □

Sada želimo svakom diferencijalu pridružiti divizor. Definirajmo sada za diferencijal $\omega \in \Omega$

$$M(\omega) := \{D \in \mathrm{Div}_k(F) | \omega(\alpha) = 0 \text{ za sve } \alpha \in \mathcal{A}(D) + F\}.$$

Lema 86. *Za svaki $0 \neq \omega \in \Omega$ postoji jedinstveni divizor $D_\omega \in M(\omega)$ takav da je $D \leq D_\omega$ za sve $D \in M(\omega)$.*

Dokaz. Fiksirajmo diferencijal $0 \neq \omega \in \Omega$. Po Riemannovom teoremu postoji konstanta c, koja ovisi samo o F/k sa svojstvom da je $i(D) = 0$ kada je $\deg D \geq c$. Pošto je $\dim_k(\mathcal{A}/(\mathcal{A}(D) + F)) = i(D)$, vidimo da ako je $\deg D \geq c$, tada je $\mathcal{A} = (\mathcal{A}(D) + F)$. Kada bi takav D bio u $M(\omega)$, to bi značilo da je ω nestaje na cijelom $\mathcal{A}$, što je kontradikcija. Zaključujemo da je $\deg D < c$ za svaki $D \in M(\omega)$. Dakle skup $\{\deg D | D \in M(\omega)\}$ je omeđen odozgo, pa možemo izabrati divizor D_ω minimalnog stupnja.

Pretpostavimo sada da postoje D_1 i D_2 takvi da su maksimalni uz pretpostavku te da je $\omega \in \Omega(D_1)$ i $\omega \in \Omega(D_2)$. Tada postoji točka P_1 takva da je $v_{P_1}(D_1) > v_{P_1}(D_2)$ za neki P_1. Isto tako, mora vrijediti da potoji neki P_2 takav da je $v_{P_2}(D_1) < v_{P_2}(D_2)$, inače smo dobili kontradikciju s maksimalnošću od D_ω.

Sada tvrdimo da je

$$D_1 + P_2 \in M(\omega) \tag{6.8}$$

što bi bila kontradikcija s maksimalnošću od $\deg D_\omega$. Promotimo $\alpha = (\alpha_P) \in \mathcal{A}(D_1 + P_2)$. Zapišimo $\alpha = \alpha_1 + \alpha_2$, gdje je

$$\alpha' = \begin{cases} \alpha & \text{za } P \neq P_2 \\ 0 & \text{za } P = P_2 \end{cases} \quad \text{i} \quad \alpha'' = \begin{cases} 0 & \text{za } P \neq P_2 \\ \alpha & \text{za } P = P_2 \end{cases}$$

Sada imamo da je $\alpha' \in \mathcal{A}(D_1)$ i $\alpha'' \in \mathcal{A}(D_2)$, te je $\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$, pošto je $\omega \in \Omega(D_1)$ i $\omega \in \Omega(D_2)$. Dakle, $\omega \in \Omega(D_1 + P_2)$, što je kontradikcija. □

Definicija. Za Weilov deiferncijal $\omega \in \Omega$ definiramo *divizor od* ω da je jedinstveni divizor $\operatorname{div} w := D_\omega$ dan prethodnom lemom. Divizor D je *kanonski divizor* ako je $D = \operatorname{div}\omega$ za neki $\omega \in \Omega$. Definiramo $v_P(w) := v_P(\operatorname{div} w)$.

Definicija. Kažemo da je diferencijal $\omega \in \Omega$ *regularan u* P ako je $v_P(\omega) \geq 0$ te da je *regularan* (ili *holomorfan*) ako je $\operatorname{div}\omega \geq 0$.

Napomena. Primjetimo da iz definicije vrijedi da je

$$\Omega(D) = \{\omega \in \Omega | \omega = 0 \text{ ili } \operatorname{div}\omega \geq D\}.$$

Također, vrijedi da ω nestaje na $\mathcal{A}(D) + F$ ako i samo ako je $\mathcal{A}(D) + F \subseteq \mathcal{A}(\operatorname{div}\omega) + F$ što je istina ako $\operatorname{div} D \leq \operatorname{div}\omega$. S druge strane, ako ω nestaje na $\mathcal{A}(D) + F$, onda po defnciji od defnciji od $\operatorname{div}\omega$, vrijedi $\operatorname{div} D \leq \operatorname{div}\omega$.

$$\Omega(0) = \{\omega \in \Omega | \omega \text{ je regularan}\}.$$

Primjetimo da vrijedi $\dim_k \Omega(0) = g$.

Lema 87. *Za svaki* $0 \neq f \in F$ *i* $0 \neq \omega \in \Omega$ *imamo*

$$\operatorname{div}(f\omega) = \operatorname{div} f + \operatorname{div}\omega.$$

Dokaz. Dokažimo $f\omega \in \Omega(\operatorname{div} f + \operatorname{div}\omega)$. Uzmimo $\alpha + g \in \mathcal{A}(\operatorname{div} f + \operatorname{div}\omega) + F$. Vrijedi

$$(f\omega)(\alpha + g) = \omega(f\alpha + fg) = \omega(fg) + \omega(f\alpha).$$

Pošto je $fg \in F$ a ω nestaje na F, imamo da je $\omega(fg) = 0$. Također, imamo

$$v_P(f\alpha) = v_P(f) + v_P(\alpha) \geq v_P(\operatorname{div} f) + v_P(-\operatorname{div} f - D_\omega) = v_P(-D_\omega),$$

te slijedi da je $f\alpha \in \mathcal{A}(D_\omega)$, a iz definicije D_ω slijedi da ω nestaje na $\mathcal{A}(D_\omega)$, pa je $\omega(f\alpha) = 0$, te slijedi

$$(f\omega)(\alpha + g) = 0.$$

Sada po defnciji $\operatorname{div}(f\omega) = D_{f\omega}$, pošto $f\omega$ nestaje na $\mathcal{A}(\operatorname{div} f + \operatorname{div}\omega) + F$, a $\operatorname{div}(f\omega)$ je maksimalni element za koji to vrijedi, slijedi da je $\operatorname{div} f + \operatorname{div}\omega \leq \operatorname{div}(f\omega)$.

Da bi dokazali obrat, pokažemo da je

$$\operatorname{div}\omega = \operatorname{div}(f^{-1}f\omega) \geq \operatorname{div} f^{-1} + \operatorname{div}(f\omega) = \operatorname{div}(f\omega) - \operatorname{div} f,$$

pa je $\operatorname{div}(f\omega) \leq \operatorname{div} f + \operatorname{div}\omega$, što smo i htjeli dokazati. □

Iz ove leme slijedi da postoji jedinstveni element u $\operatorname{Pic}_k C$ koji odgovara kanonskim divizorima, koji se zove *kanonska klasa*. Pokažimo još da su diferencijali u potpunosti određeni, do na množenje s skalarima iz $k^\times$, svojim divizorima.

Propozicija 88. *Dva ne-nul diferencijala* $\omega_1, \omega_2 \in \Omega$ *imaju isti divizor ako i samo ako je* $\omega_2 = c\omega_1$ *za neki* $c \in k^\times$.

Dokaz. Pošto je $\omega_1 \neq 0$ i $\dim_F \Omega = 1$, svakako možemo napisati $\omega_2 = f\omega_1$ za neki $f \in F^\times$. Sada je $\operatorname{div}\omega_2 = \operatorname{div} f\omega_1 = \operatorname{div} f + \operatorname{div}\omega_1$, pa ako je $\operatorname{div}\omega_1 = \operatorname{div}\omega_2$, tada je $\operatorname{div} f = 0$, te je $f \in k^\times$. Obrnuto $\operatorname{div}\omega_2 = \operatorname{div} c\omega_1 = \operatorname{div} c + \operatorname{div}\omega_1 = \operatorname{div}\omega_1$ za sve $c \in k^\times$. □

Pokažimo sada kako eksplicitno izračunati neki kanonski divizor (a time i odrediti kanonsku klasu). Način računanja kanonskih divizora je preuzet iz [9, II.4], te se u [6, Chapter 6] može naći više o diferencijalima. Za krivulju C/k za svaki $f \in \overline{k}(C)$, postoji diferencijalna forma df, te će diferencijalne forme tog oblika činiti vektorski prostor Ω_C nad $\overline{k}(C)$ te vrijede sljedeće relacije među diferencijalnim formama:

1) $d(f+g) = df + dg$ za sve $f, g \in \overline{k}(C)$.

2) $d(fg) = fdg + gdf$ za sve $f, g \in \overline{k}(C)$.

3) $da = 0$ za sve $a \in \overline{k}$.

Vrijedi da je Ω_C 1-dimenzijonalni vektorski prostor nad $\overline{k}(C)$, te se svaki uniformizator t u $P \in C$, može svaka diferencijalna forma ω napisati kao $\omega = gdt$, za neki $g \in \overline{k}(C)$. Sada označavamo g s ω/dt. Vrijednost $v_P(\omega)$ definiramo kao

$$v_P(\omega) := v_P\left(\frac{\omega}{dt}\right) = v_P(g),$$

gdje se g odredi korištenjem svojstava 1).

Sada je

$$\operatorname{div}(\omega) = \sum_{P \in C} v_p(\omega)P$$

neki kanonski divizor.

Također je korisna jednakost (vidi [9, Proposition II.4.3 (d), p.36]), za $f \in \overline{k}(C)$ i $P \in C$, takve da je $f(P) = 0$, te za $g \in \overline{k}(C)$ vrijedi

4) $v_P(gdf) = v_P(g) + v_P(f) - 1$.

Primjer 27. Neka je x funkcija na $y^2 = x^3 - x$. Sjetimo se da x ima nultočku reda 2 u $P_1 = (0,0)$ te pol reda 2 u ∞. Odredimo sada $\operatorname{div}(dx)$. Primjetimo da je po 1) i 3) $dx = d(x-1) = d(x+1)$, te da funkcije $(x-1)$ i $(x+1)$ imaju nultočke reda 2 u $P_2 = (1,0)$ i $P_3 = (-1,0)$. Neka je $P_0 = (x_0, y_0)$, takva da je $x_0 \neq 0, \pm 1$, tada je $dx = d(x - x_0)$, gdje je $(x - x_0)$ uniformizator u P_0. Dakle $g = 1$, pa je $v_{P_0}(dx) = v_{P_0}(1) = 0$.

Sada imamo da je za $v_{P_1}(dx) = v_{P_1}(x) - 1 = 1$, te je $v_{P_2}(dx) = v_{P_2}(d(x-1)) = 2 - 1 = 1$. Analogno je $v_{P_3}(dx) = 1$. Ostaje odrediti $v_\infty(dx)$. Primjetimo da je po 2)

$$0 = d(x \cdot (1/x)) = \frac{1}{x}dx + xd\left(\frac{1}{x}\right),$$

te je $dx = -x^2 d\left(\frac{1}{x}\right)$. Po 4) slijedi da je

$$v_\infty(dx) = v_\infty(-x^2 d\left(\frac{1}{x}\right)) = v_\infty(-x^2) + v_\infty(1/x) - 1 = -4 + 2 - 1 = -3.$$

Dakle imamo

$$\operatorname{div}(dx) = P_1 + P_2 + P_3 - 3\infty,$$

te je to kanonski divizor. Primjetimo također da je i $\frac{dx}{y}$ također neka diferencijalna forma, iz čeka slijedi da je 0 kanonski divizor na ovoj krivulji.

6.3 Riemann-Rochov Teorem

Teorem 89 (Dualnost)**.** *Za svaki divizor D i kanonski divizor $W = \operatorname{div}\omega$, linearno preslikavanje $\phi : L(W-D) \to \Omega(D)$ definirano s $\phi(f) = f\omega$ je izomorfizam vektorskih prostora. Nadalje, $i(D) = l(W - D)$.*

Dokaz. Za $f \in L(W - D)$ imamo

$$\operatorname{div} f\omega = \operatorname{div} f + \operatorname{div}\omega \geq -(W - D) + W = D,$$

pa iz napomene u prethodnom poglavlju vrijedi da je $f\omega \in \Omega(D)$. Preslikavanje ϕ ima trvijalnu jezgru, pa je injektivno. Također, ϕ je očito linearan.

Dokažimo surjektivnost. Neka je $0 \neq \omega_1 \in \Omega(D)$. Po teoremu 85, možemo napisati $\omega_1 = f\omega$ za neki $f \in F^\times$, te pošto je

$$\operatorname{div} f + W = \operatorname{div} f + \operatorname{div}\omega = \operatorname{div} f\omega = \operatorname{div}\omega_1 \geq D,$$

dobivamo $\operatorname{div} f \geq -(W - D)$, pa je taj f iz $L(W - D)$, pa je $omega_1 = \phi(f)$. Dakle imamo $\dim_k(\Omega(D)) = l(W - D)$, pa je po lemi 84 $i(D) = l(W - D)$. □

Konačno možemo iskazati Riemann-Rochov teorem.

Teorem 90 (Riemann-Roch)**.** *Neka je W kanonski divizor krivulje C/k genusa g. Tada za svaki divizor $D \in \operatorname{Div} C$ vrijedi*

$$l(D) = \deg D + 1 - g + l(W - D).$$

Dokaz. Tvrdnja slijedi ditektno iz prehodnog teorema i iz definicije $i(D)$. □

6.4 Posljedice Riemann-Rochovog teorema.

Sada ćemo pokazati niz posljedica ovog teorema.

Korolar 91. *Za kanonski divizor W vrijedi*

$$\deg W = 2g - 2, \quad l(W) = g, \quad i(W) = 1.$$

Dokaz. Uvrstimo $D = 0$ u Riemann-Rochhov teorem; dobijemo

$$1 = l(0) = \deg 0 + 1 - g + l(W - 0),$$

tj. $l(W) = g$. Ako stavimo $D = W$, dobijemo

$$g = l(W) = \deg W + 1 - g + l(W - W) = \deg W + 2 - g,$$

tj. $\deg W = 2g - 2$. Odmah slijedi i $i(W) = 1$. □

Pokažimo još jednu karakterizaciju kanonskih divizora.

Propozicija 92. *Divizor D je kanonski divizor ako i samo ako je* $\deg D = 2g-2$ *i* $l(D) \geq g$.

Dokaz. Pretpostavimo da je $\deg D = 2g-2$ i $l(D) \geq g$, te neka je W neki kanonski divizor. Tada je

$$g \leq l(D) = \deg D + 1 - g + l(W - D) = g - 1 + l(W - D),$$

dakle $l(W - D) \geq 1$. Kako je $W - D$ stupnja 0, te time i $l(W - D) \leq 1$, slijedi da je $l(W - D) = 1$. Sada po lemi 77 slijedi da je $W - D$ glavni divizor, tj. $W \sim D$. □

Sjetimo se da nam Riemannov teorem kaže da za divizor D "dovoljno velikog" stupnja vrijedi $i(D) = 0$. Slejdeći teorem nam daj precizniju tvrdnju što to znači "dovoljno velik" stupanj.

Teorem 93. *Za C/k i divizor $D \in \operatorname{Div} C$ takav da je* $\deg D \geq 2g - 1$ *vrijedi*

$$l(D) = \deg A + 1 - g.$$

Dokaz. Prema korolaru 91 znamo da je $\deg W = 2g-2$, pa onda ako je $\deg D \geq 2g - 1$, tada imamo da je $\deg(W - D) < 0$, pa po propoziciji 75 vrijedi da je $l(W - D) = 0$. Sada tvrdnja slijedi po Riemann-Rochovom teoremu. □

Primjetimo da je ova ograda najbolja moguće, jer za kanonski divizor W, po korolaru 91 vrijedi

$$l(W) > \deg W + 1 - g = g - 1.$$

Sada ćemo pokazati kako Riemann-Rochov teorem karakterizira i genus i klasu kanonskih divizora.

Propozicija 94. *Pretpostavimo da je $g_0 \in \mathbb{Z}$ i $W_0 \in \operatorname{Div} C$, te da oni zadovoljavaju*

$$l(D) = \deg D + 1 - g_0 + l(W_0 - D) \tag{6.9}$$

za sve $D \in \operatorname{Div} C$. Tada je $g_0 = g$ i W_0 je kanonski divizor.

Dokaz. Ako stavimo $D = 0$, dobivamo $l(W_0) = g_0$, te ako stavimo $D = W_0$, dobivamo $\deg W_0 = 2g_0 - 2$. Neka je sada W kanonski divizor od C/k. Uzmimo neki divizor D, takav da je $\deg D > \max\{2g - 2, 2g_0 - 2\}$. Tada je po teoremu 93 $l(D) = \deg D + 1 - g$ i $l(D) = \deg D + 1 - g_0$ po (6.9). Dakle $g = g_0$. Sada uvrštavanjem $D = W$ u (6.9) dobivamo

$$g = l(W) = 2g - 2 + 1 - g + l(W_0 - W),$$

pa je $l(W_0 - W) = 1$. Pošto je $\deg(W_0 - W) = 0$, slijedi da je $W_0 - W$ glavni divizor, tj. $W_0 \sim W$. □

Propozicija 95. *Neka je P neka točka na krivulji C/k. Za svaki $n \geq 2g$, postoji funkcija $f \in k(C)$ takva da je* $\operatorname{div} f_\infty = nP$.

Dokaz. Po teoremu 93 vrijedi $l((n-1)P) = (n-1)\deg P + 1 - g$ i $l(nP) = n\deg P + 1 - g$, dakle $L((n-1)P) \subsetneq L(nP)$, tj. postoji element koji ima samo pol u P, te je taj pol točno reda n. □

Primjenimo dobivene alate i na krivulje.

Teorem 96. *Neka je C/k krivulja koja ima k-racionalnu točku. Tada C ima genus 0 ako i samo ako je izomorfna s $\mathbb{P}^1$ (nad k).*

Dokaz. Neka je C krivulja genusa 0 s racionalnom točkom P. Sada Riemann-Rochov teorem implicira da je

$$l(P) = \deg P + 1 - g = 2,$$

pošto je $\deg(W - P) = 2g - 2 + 1 = -1$. Dakle slijedi da postoji nekonstanta funkcija f koja ima jednostruki pol u P i nema drugih polova. Dakle $\deg \operatorname{div}_\infty f = \deg P = 1$, dakle f je morfizam stupnja 1 iz C u $\mathbb{P}^1$ definiran nad k, pošto je $f \in k(C)$, dakle f je izomorfizam.

Dokažimo sada obrat: neka ke $C \simeq \mathbb{P}^1$, pa je dakle $k(C) \simeq k(x)$. Promotrimo funkciju x; ona ima pol samo u ∞. Promotrimo vektorski prostor $L(r\infty)$. Očito su $1, x, \ldots, x^r \in L(r\infty)$, te su očito linearno nezavisni nad k. Dakle imamo

$$r + 1 \leq l(r\infty) = \deg(r\infty) + 1 - g + l(W - r\infty) = r + 1 - g + l(W - r\infty).$$

Pošto je $l(W - r\infty) \geq 0$, slijedi $g = 0$. □

Zbog ovog teorema se krivulje genusa 0 obično nazivaju *racionalne krivulje* (pošto im je funkcijsko polje izomrofno s poljem racionalnih funkcija $k(x)$).

Napomena. Dokaz se može probati provesti i tako da uzemo da je P neka zatvorena točka; međutim tada će $\deg P$ biti veći od 1 pa nećemo dobiti izomorfizam. Međutim, ako proširimpo bazu od C/k na polje nad kojim se točka P cijepa u točke stupnja 1, nad tim poljem ćemo sigurno dobiti izomorfizam. Dakle svaka krivulja C/k genusa 0 je izomorfna s $\mathbb{P}^1$ nad konačnim proširenjema od k.

Lema 97. *Neka je ϕ automorfizam od $\mathbb{P}^1$ koji fiksira više od 2 točke u $\mathbb{P}^1(\overline{k})$. Tada je ϕ identiteta.*

Dokaz. Možemo bez smanjenja općenitosti pretpostaviti da ϕ fiksira $\infty = (1 : 0)$ (u suprotnom upotrijebimo linearnu transformaciju koja prmejesti tu točku u beskonačnost). Ako restringiramo ϕ na $\mathbb{A}^1(\overline{k}) = \mathbb{P}^1(\overline{k}) - \infty$, nazovimo to preslikavanja ϕ_a, dobivamo bijekciju koja je isto morfizam afinih krivulja. Dakle $\phi_a \in k[x]$, te je $\deg \phi_a = 1$, pošto je bijekcija. Ako jednadžba $\phi_a(x) = x$ ima više od jednog rješenja, onda se obje strane moraju poklapati kao polinomi (jer su obje strane stupnja 1). Dakle, tada je $\phi_a(x)$ upravo jednako x, tj. ϕ je identiteta. □

Napomena. Može se pokazati da su svi automorfizmi od $\mathbb{P}^1$ racionlen funkcije oblika $(ax+by)/(cx+dy)$, gdje je $ad-bc\neq 0$. Ovakva preslikavanj se zovu *Möbusove transformacije*.

Primjenimo sada Riemann-Rochov teorem na krivulje genusa 1.

Teorem 98. *Neka je C/k krivulja s k-racinalnom točkom. Tada C ima genus 1 ako i samo ako je izomorfna glatkoj krivulji oblika*

$$C' : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \tag{6.10}$$

gdje su $a_1, a_2, a_3, a_4, a_6 \in k$.

Dokaz. Neka je C/k krivulja genusa 1 s racionalnom točkom P. Primjetimo da za svaki $n \in N$ vrijedi $\deg nP > 2g-2 = 0$, pa je po Riemann-Rochovom teoremu

$$l(nP) = \deg(nP) + 1 - g = n.$$

Dakle, imamo da je $l(2P) = 2$. Pošto je očito $k \in L(2P)$, opstoji funkcija x takva da je $\{1, x\}$ baza za $L(2P)$. Primjetimo da x nužno ima opl reda 2, jer kada bi imao pol manjeg reda, tada bi i x^2 bilo u $L(2P)$.

Isto tako, $L(3P)$ sadrži $L(2P)$, pa ima bazu $\{1, x, y\}$ za neku funkciju $y \in k(C)^\times$; ta funkcija mora očito imati pol reda 3 u P.

Primjetimo da su $1, x, y, x^2$ svi u $L(4P)$, te pošto su njihovi polovi u P reda $0, 2, 3, 4$, oni su nezavisni nad k, te čine bazu za $L(4P)$.

Analogno, $1, x, y, x^2, xy$ su elementi od $L(5P)$ čiji su polovi u P reda $0, 2, 3, 4, 5$, te čine bazu od $L(5P)$ nad k

Promtrimo sada $L(6P)$: unutra se očito nalaze $1, x, y, x^2, xy, y^2, x^3$. Ovih 7 elemenata očito ne može biti linearno nezavisno nad k, pošto leže u 6-dimenzionalnom prostoru $L(6P)$. Dakle tih 7 funkcija zadovoljavaju neku linearnu jednadžbu. Ta jednadžba mora nužno sadržati ax^3 i by^2, jer bui u suprotnom imali 6 funkcija različitih reda polova (te bi činili bazu). Pa zamjenom x s ax/b, y s by/a, te množenjem s b^3/a^4 dobijamo jednadžbu oblika (6.10).

Dokažimo sada obrat; neka je C/k projektivizacija afine krivulje definirana jednadžbom (6.10). Tada je očito $P := (0:1:0)$ k-racionalna točka na C.

Funkcija $X := (x:y:z) \mapsto (x:z)$ za $z \neq 0$, $P \mapsto \infty$ je funckija stupnja $[k(C) : k(x)]$ (sjetimo se $k(\mathbb{P}^1) \simeq k(t)$). Lako se vidi da je $[k(C) : k(x)] = 2$, pošto je y stupnja 2 nad $k(x)$ (promotimo u afinim koordinatama i primjetimo da mora biti stupnja 2, jer jednadžba (6.10) po definiciji krivulje mora biti ireducibilna nad $k(x)$). Sada slijedi da je $\deg \mathrm{div}_\infty X = 2$, te funkcija ima pol samo kada je $z = 0$, dakle samo u točki P. Dakle X ima dvostruki pol u P. Istom argumentacijom zaključujemo da je $Y := (x:y:z) \mapsto (y:z)$ funkcija stupnja 3 s polom samo u P. Dakle, funkcije oblika x^iy^j imaju polove samo u P i to stupnja $2i+3j$. Primjetimo da svaki elemtet od $\mathbb{N}_0$ osim 1 možemo prikazati kao $2i+3j$. Dakle, možemo konstruirati skup od n linearno nezavisnih elemenata s polovima stupnja $0, 2, 3 \ldots n$, koji svi leže u $L(nP)$, te to napraviti za svaki n. Dakle za dovoljno veliki n upotrebom Riemann-Rochovog teorema (ili zapravo Riemannove nejednakosti) dobijemo

$$n \leq l(nP) = \deg(nP) + 1 - g = n + 1 - g,$$

pa je genus od C najviše 1.

Treba dokazati još da je $g \neq 0$. Mi ćemo to napraviti uz pretpostavku da je $\operatorname{char} k \neq 2$. Promotrimo preslikavanje i definirano s

$$(x : y : z) \mapsto (x : -y - a_1x - a_3z : z).$$

Desna strana ostaje ista, dok se računom pokazuje da lijeva strane također ostaje ista. Dakle i je morfizam C u samog sebe. Vrijedi da je i invertibilan (sam je sebi inverz, tj. involucija je), pa je automorfizam. Pronađimo fiksne točke: $(0 : 1 : 0)$ je očito fiksna, te je točka s $z \neq 0$ fiksna ako i samo ako je $y = -y - a_1x - a_3z$. Uz pretpostavku da je $\operatorname{char} k \neq 2$, imamo da je $y = -(a_1x + a_3z)/2$. Sada postoje tri mogućnosti za x; to su nultočke kubičnog polinoma

$$x^3 - a_2x^2 + a_4x + a_6z + (a_1x + a_3z)^2/4.$$

Pretpostavili smo da je krivulja glatka, te vidimo da zato ova kubična jednadžba mora imati različite nultočke, jer bi dvostruka nultočka odgovarala singularitetu na krivulji C'. Dakle imamo da i fiksira 4 točke na krivulji $C'(\overline{k})$. Međutim, i očito nije identiteta na $k(C')$. Po lemi 97 slijedi da C' ne može biti genusa 0. □

6.4.1 Specijalni divizori

Sjetimo se da smo po propoziciji 95 imali da za krivulju X i za svaki $P \in X$ i za sve n-ove dovoljno velikog stupnja, vrijedi da postoji funkcija f takva da je $\operatorname{div}_\infty f = nP$.

Definicija. Neka je X/k krivulja, te neka je $P \in X$. Ako postoji funkcija f takva da je $\operatorname{div}_\infty f = nP$, kažemo da je *$n$ polni broj od P*, a u suprotnom kažemo da je *broj raskoraka od P*.

Primjetimo da skup polnih brojeva s operacijom zbrajanja čine pod-polugrupu od polugrupe $\mathbb{N}$. To vidimo jer ako je $\operatorname{div}_\infty f_1 = n_1P$ i $\operatorname{div}_\infty f_2 = n_2P$, tada je i $\operatorname{div}_\infty f_1f_2 = (n_1 + n_2)P$.

Teorem 99 (Weierstrassov teorem o brojevima raskoraka)**.** *Neka je C/k krivulja genusa $g > 0$, te $P \in C$ točka. Tada postoji točno g brojeva raskoraka $i_1 < i_2 < i_g$ od P, te je*

$$i_1 = 1 \quad i \quad i_g \leq 2g - 1.$$

Dokaz. Vrijedi da za svaki broj raskoraka od P vrijedi da je $\leq 2g - 1$ po Propoziciji 95. Očito je da je 0 polni broj za svaku točku P, pošto je $\operatorname{div}_\infty a = 0P$ za svaku točku P i za svaki $a \in k^\times$. Također, vrijedi da je

$$i \text{ je broj raskoraka } \iff L((i-1)P) = L(iP).$$

Dakle, vrijedi

$$k = L(0) \subseteq L(P) \subseteq L(2P) \subseteq \cdots \subseteq L((2g-1)P) \tag{6.11}$$

, te je $l(0) = 1$ i $l((2g-1)P) = g$ po Riemann-Rochovom teoremu. Sjetimo se da je po Lemi 73 vrijedi da ako je $L(A) \subseteq L(B)$, tada je $L(B)/L(A) \leq \deg B - \deg A$. Primijenjeno na $A = (i-1)P$ i $B = iP$, dobivamo da je

$$l(iP) \leq l((i-1))) + 1.$$

Slijedi da postoji točno $g-1$ brojeva k, $1 \leq k \leq 2g-1$ takvih da je u nizu 6.11 $L((k-1)P) \subsetneq L(kP)$. Preostalih g brojeva su brojevi raskoraka.

Ostaje za dokazati da je 1 broj raskoraka. Pretpostavimo suprotno, da je 1 polni broj od P. Pošto su polni brojevi od P aditivna polugrupa, slijedi da je svaki prirodan broj polni broj, što je kontradikcija s ranije dokazanim. □

Sjetimo se da je

$$i(D) = l(W - D) = g - 1 - r(D) = g - 1 + l(D) - \deg D,$$

te da je $i(D) = 0$ za sve D takve da je $\deg D \geq 2g - 1$.

Definicija. Kažemo da je divizor D *specijalan* ako je $i(D) \neq 0$, a u suprotnom kažemo da je *ne-specijalan.*

Sada možemo promotriti niz

$$l(P),\ l(2P), \ldots,\ l((2g-1)P), l(2gP), \ldots$$

Znamo da je on oblika

$$1,\ ?,\ ?,\ \ldots, g,\ g+1,\ \ldots.$$

Ono što se tipično događa da su svi brojevi raskoraka najviše lijevo moguće, tj. da ovaj niz izgleda ovako:

$$1, 1, \ldots, 1, 2, 3, 4, \ldots, g, g+1, \ldots.$$

Definicija. Kažemo da je točka $P \in C$ *ne-Weierstrassova* ako je $i_k = k$ za $k = 1, \ldots, g$. Kažemo da je točka *Weierstrassova* ako nije ne-Weierstrassova.

Iskažimo u sljedećoj propoziciji što znamo o specijalnim deivizorima:

Propozicija 100. *a) Je li divizor specijalan ili ne ovisi samo o klasi divizora u* $\operatorname{Pic} C$.

b) Kanonski divizori su specijalni.

c) Svaki divizor D takav da je $l(D) > 0$ i $\deg D < g$ je specijalan.

d) Ako je A ne-specijalan i $B \geq A$, tada je i B ne-specijalan.

Dokaz. a) Tvrdnja slijedi direktno iz definicije od $i(D)$, te iz činjenice da $\deg D$ i $l(D)$ ovise samo o klasi divizora.

b) Za kanonski divizor W vrijedi $i(W) = l(W - W) = l(0) = 1$, pa je W specijalan, što dokazuje b).

c) Vrijedi $1 \leq l(D) = \deg D + 1 - g + i(D)$, pa je $i(D) \geq g - \deg A > 0$, po pretpostavci.

d) Ako je A ne-specijalan ako i samo ako je $i(A) = 0$, iz čega slijedi $\mathcal{A} = \mathcal{A}(A) + F$ po Teoremu 83. Pošto je $B \geq A$, vrijedi $\mathcal{A}(A) \subseteq \mathcal{A}(B)$, iz čega slijedi $\mathcal{A} = \mathcal{A}(B) + F$, tj. $i(B) = 0$. □

Sada želimo dokazati sljedeći važan rezultat o specijalnim divizorima.

Teorem 101 (Cliffordov teorem o specijalnim divizorima)**.** *Za svaki divizor D takav da je $0 \leq \deg D \leq 2g - 2$, vrijedi*

$$l(D) \leq 1 + \frac{1}{2} \deg D.$$

Da bi dokazali Cliffordov teorem, trebat će nam sljedeća lema.

Lema 102. *Neka su $A, B \in \operatorname{Div} C$, gdje je C/k krivulja nad beskonačnim poljem k, takvi da je $l(A) > 0$ i $l(B) > 0$. Tada je*

$$l(A) + l(B) \leq 1 + l(A + B).$$

Dokaz. Pošto je $l(A) > 0$ i $l(B) > 0$, možemo po Lemi 72 naći divizore $A_0, B_0 \geq 0$, takve da je $A_0 \sim A$ i $B_0 \sim B$. Neka je

$$X = \{D \in \operatorname{Div} C | D \leq A_0 \text{ i } L(D) = L(A_0)\}.$$

Očito je X neprazan pošto je $A_0 \in X$. Pošto je $\deg D \geq 0$ za sve $D \in X$, postoji neki divizor D_0 minimalnog stupnja. Slijedi da je

$$l(D_0 - P) < l(D_0) \text{ za sve } P \in C.$$

Želimo pokazati da je

$$l(D_0) + l(B_0) \leq 1 + l(D_0 + B_0). \tag{6.12}$$

Kada bismo to dokazali, slijedilo bi

$$l(A) + l(B) = l(A_0) + l(B_0) = l(D_0) + l(B_0)$$

$$\leq 1 + l(D_0 + B_0) \leq 1 + l(A_0 + B_0) = 1 + l(A + B).$$

Dokažimo sada (6.12). Neka je $\{P_1, \ldots, P_r\}$ podrška od B_0. Vrijedi da je $L(D_0 - P_i)$ prvi potprostor od D_0, za sve $i = 1, \ldots r$.

Pošto vrijedi da ni jedan vektorski prostor nad beskonačnim poljem nije unija svojih pravih potprostora, vrijedi da postoji

$$z \in L(D_0) \setminus \bigcup_{i=1}^{r} L(D_0 - P_i).$$

Promotrimo k-linearno preslikavanje

$$\phi : \begin{cases} L(B_0) & \longrightarrow L(D_0 + B_0)/L(A_0), \\ x & \longmapsto xz \mod L(A_0). \end{cases}$$

Pošto je $z \geq -D_0$, te $x \geq -B_0$, slijedi da je $xz \geq -B_0 - D_0$, pa je $xz \in L(D_0 + B_0)$. Tvrdimo da je $\ker \phi = k$. Kada bi $x \notin K$ bio u jezgri od ϕ, slijedilo bi da x ima pol u nekom P_i (pošto je $x \in L(B_0)$). Dakle $\operatorname{div} x = D' - P_i$ za neki $D' \in \operatorname{Div} C$ takav da je $v_{P_i}(D') \leq 0$. Pošto je po pretpostavci $xz \in L(A_0) = L(D_0)$, vrijedi da je $\operatorname{div} x + \operatorname{div} z \geq -D_0$, pa je

$$\operatorname{div} x + \operatorname{div} z = D' - P_i + \operatorname{div} z \geq -D_0,$$

pa vrijedi da je $v_{P_i}(z) > -v_{P_i}(D_0)$, tj. $z \in L(D_0 - P_i)$, što je kontradikcija.

Sada imamo po prvom teoremu o izomorfizmu

$$l(B_0) - 1 \leq l(D_0 + B_0) - l(A_0),$$

što dokazuje (6.12) □

Dokaz Cliffordovog teorema o specijalnim divizorima. Ako je $l(D) = 0$, tvrdnja trivijalno vrijedi. Također, ako je $l(W - D) = 0$ za kanonski divizor W, tada slijedi da je

$$l(D) = \deg D + 1 - g = 1 + \frac{1}{2} \deg D + \frac{1}{2}(\deg D - 2g) < 1 + \frac{1}{2} \deg D.$$

Promotimo slučaj kada je $l(D) > 0$ i $l(W - D) > 0$. Sada je po Lemi 102

$$l(D) + l(W - D) \leq 1 + l(W) = 1 + g,$$

dok je s druge strane, po Riemann-Rochovom teoremu

$$l(D) - l(W - D) = \deg A + 1 - g.$$

Zbrajanjem ove dvije jednakosti dobivamo traženi rezultat. □

Poglavlje 7

Eliptičke krivulje

Definicija. Glatka projektivna krivulja genusa 1 and nekim poljem k zajedno s jednom k-racionalnom točkom se zove *eliptička krivulja.*

Teorem 103. *Neka je E/k krivulja genusa 1 s nekom fiksiranom k-racionalnom točkom O. Preslikavanje*

$$\begin{aligned}\Phi : E(K) &\to \mathrm{Pic}_k^0(E)\\ P &\mapsto [P-O]\end{aligned}$$

inducira (pošto je $\mathrm{Pic}_k^0(E)$ grupa) grupovnu operaciju na $E(k)$ definiranu s

$$P_1 + P_2 := \phi^{-1}(\phi(P_1) + \phi(P_2)),$$

u kojoj je O neutralni element.

Dokaz. Dokažimo prvo injektivnost. Primjetimo da ako je $P-O \sim Q-O$, tada je $P-O+\mathrm{div}\, f = Q-O$ za neki $f \in k(E)$, pa je $P+\mathrm{div}\, f = Q$, tj. $\mathrm{div}\, f = P-Q$. Ako je $f \neq 0$, tada je f izomorfizam s E u $\mathbb{P}^1$, što je kontradikcija s činjenicom da je genus od E jednak 1. Dakle $P = Q$ i ϕ je injekcija.

Neka je sada D neki divizor srupnja 0. Tada $D+O$ je stupnja $1 \leq 2g-1 = 1$, pa je po teoremu 93

$$l(D+O) = \deg(D+O) + 1 - g = 1,$$

dakle postoji $f \in L(D+O)$ takav da je $\mathrm{div}\, f + D + O \geq 0$. Pošto je $\deg(\mathrm{div}\, f + D + O) = 1$, imamo da je $\mathrm{div}\, f + D + O = P$ za neki $P \in E(k)$. Dakle

$$D \sim P - O = \phi(P).$$

□

Vidjeli smo u Teoremu 98 da se svaka eliptička krivulja E/k može zapisati u *(dugom) Weierstrassovom modelu*:

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

gdje su $a_i \in k$.

Pokažimo da se nad poljem k karakteristike $chark \neq 2, 3$ prikazati i jednostavnije.

Propozicija 104. *Neka je E/k (projektivna) krivulja definirana s (projektivizacijom od)*

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

te neka je $chark \neq 2, 3$, tada je E izomorfna (nad k) krivulji

$$E' : u^2 = v^3 + av + b \tag{7.1}$$

Dokaz. Pošto je $chark \neq 2$, lijevu stranu možemo zapisati kao

$$y + (a_1x + a_3)/2)^2 - (a_1x + a_3)^2/4,$$

te zamjenom varijabli $u = y + (a_1x + a_3)/2$, dobivamo jednadžbu oblika

$$u^2 = x^3 + b_2x^2 + b_4x + b_6,$$

za neke $b_2, b_4, b_6 \in k$. Pošto je $chark \neq 3$, zamjenom varijabli $v = x + b_2/3$ dobivamo

$$u^2 = v^3 + av + b,$$

za neke $a, b \in k$. □

Napomena. Eliptičke krivulje koje su po definiciji projektivne krivulje, se često zapisuju u afinom obliku (kao u prethodnoj propoziciji), tj. kao afina karta eliptičke krivulje. Imajmo na umu da se *uvijek* zapravo radi o projektivnim krivuljama.

Također, vidjeli smo iz Teorema 103 da je skup točaka $E(k)$ pretvoriti u Abelovu grupu preko bijekcije s grupom $\mathrm{Pic}^0_k E$, dakle dobiva strukturu grupe. Ta struktura grupe se može eksplicitno opisati (vidi npr. [9] ili [4]), ali mi nećemo to sada raditi.

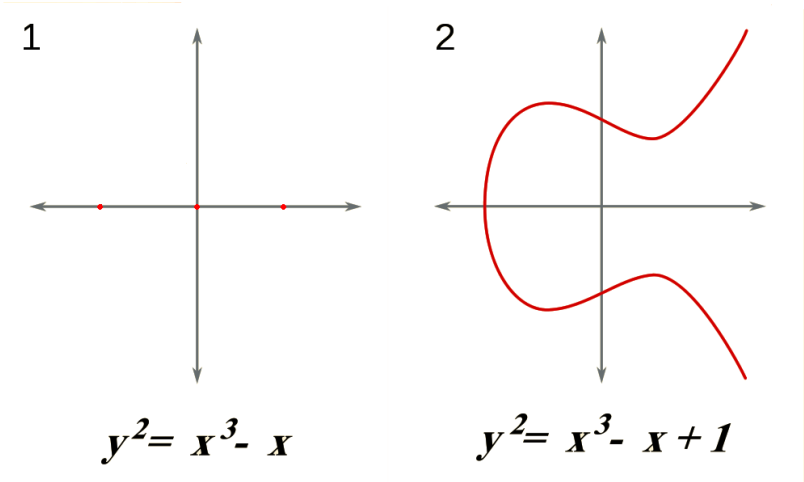
Najvažniji rezultat o eliptičkim krivuljama nad poljima algebarskih brojeva je Mordell-Weilov teorem.

Teorem 105 (Mordell-Weil)**.** *Neka je E eliptička krivulja nad poljem algebarskih brojeva k. Tada je $E(k)$ konačno generirana Abelova grupa.*

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

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

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

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 107 (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 108 (Bhargava & Shanakar (2013))**.** *Ako poredamo eliptičke krivulje po veličini koeficijenata, prosječni rang je* < 0.85.

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.

7.1 Galoisove reprezentacije pridružene eliptičkim krivuljama

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

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

Sljedeći teorem ostavljamo bez dokaza.

Teorem 109. *Za svaku eliptičku krivulju $E/\mathbb{C}$, postoji (jedinstvena do na homotetiju) rešetka $\Lambda \subseteq C$ i izomorfizam (kompleksnih Liejevih) grupa*

$$\phi : \mathbb{C}/\Lambda \to E.$$

Korolar 110. *Vrijedi $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$.*

Dokaz. $E \simeq \mathbb{C}/\Lambda \simeq (\mathbb{R}/\mathbb{Z})^2$, pa vrijedi $E[m] \simeq (\frac{1}{m}\mathbb{Z}/\mathbb{Z})^2 \simeq (\mathbb{Z}/m\mathbb{Z})^2$. Lako se vidi da su sve točke u $E[m]$ algebarske, pošto su im koordinate rješenja algebarskih jednadžbi. □

Cilj ovoga poglavlja je razumjeti kako, za eliptičku krivulju definiranu nad $\mathbb{Q}$, 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 111 (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 ρ_n. Eliptičku krivulju ne pišemo u subskriptu, jer će uvijek biti jasno o kojoj krivulji se radi. Reprezentacija ρ_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. σ 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 σ automorfizam, tj. ima inverz. Analogno, ako je n općeniti prirodan broj, ne nužno prost, dobivamo da je ρ_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 $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Vrijedi da je $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ izomorfno s $\rho_n(G)$.

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

Primjer 28. Neka je $E : y^2 = x^3+ax+b$ eliptička krivulja nad $\mathbb{Q}$, te promotrimo ρ_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 29. 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

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

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.

Možemo i enkapsulirati sve reprezentacije odjednom: neka je $E_{tors} = E(\overline{k})_{tors}$, tada je očito

$$\mathrm{Aut}(E_{\mathrm{tors}}) = \varprojlim_n \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) = \mathrm{GL}_2(\hat{\mathbb{Z}}).$$

Analogno kao i prije, dobivamo reprezentaciju

$$\rho : G \to \mathrm{GL}_2(\hat{\mathbb{Z}}),$$

koja se naziva adelička reprezentacija pridružena eliptičkoj krivulji.

Jedan od ključnih rezultata u teoriji eliptičkih krivulja je da adelička reprezentacija eliptičkih krivulja bez kompleksnog množenja ne može biti prevelika.

Teorem 112 (Serreov teorem o otvorenoj slici)**.** *Neka je E eliptička krivulja bez kompleksnog množenja. Tada je slika pridružene adeličke reprezentacije konačnog indeksa u $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Drugim riječima,*

- *Slika $\hat{\rho}_l(G)$ je jednaka $\mathrm{GL}_2(\mathbb{Z}_l)$ za sve osim konačno mnogo l-ova.*
- *Slika $\hat{\rho}_l(G)$ je u l-adskoj topologiji otvorena u $\mathrm{GL}_2(\mathbb{Z}_l)$ (tj. $[\mathrm{GL}_2(\mathbb{Z}_l) : \rho_l(G)]$ 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 30. Neka je p prost broj i E eliptička krivulja takva da je ρ_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 ϕ stupnja n, tj. $\operatorname{Ker}\phi \simeq \mathbb{Z}/n\mathbb{Z}$, prisjetimo se da tada svaki $\sigma \in G$ djeluje na $\operatorname{Ker}\phi$, tj. vrijedi $P^\sigma \in \operatorname{Ker}\phi$ za svaki $P \in \operatorname{Ker}\phi$, tj. $P^\sigma = \alpha P$. Neka je P_2 neki generator od $\operatorname{Ker}\phi$; 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.

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 31. 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 32. 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 $m \in \mathbb{Z}$.

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

Primjer 33. 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, $\operatorname{End}_{\mathbb{Q}} E = \mathbb{Z}$.

Činjenica. Ako je Φ podgrupa od E, tada postoji jedinstvena eliptička krivulja E' i izogenija

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

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

Ako je izogenija $\phi : E \to E'$ definirana nad nekim poljem $\mathbb{Q}$ (sjetimo se to znači da su svi koeficijenti morfizma definirani nad $\mathbb{Q}$), tada očito jezgra mora biti $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invarijantna. Posebno nas zanimaju cikličke izogenije, tj. one s cikličkom jezgrom. Primjetimo da ako je jezgra ciklička reda p tada za svaki $\sigma \in G_{\mathbb{Q}}$ vrijedi da je $P^\sigma = \alpha P$. U tom slučaju vrijedi da je reprezentacija oblika

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

7.2 Modularne krivulje

U ovom poglavlju ćemo slijediti [1, 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 ∞, te ∞ šalje u a/c. Ako je $c = 0$, onda se ∞ šalje u ∞.

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.

Definicija. Neka je N prirodan broj. Tada je **glavna kongruencijska podgrupa nivoa** N

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Grupa $\Gamma(N)$ se može i definirati kao jezgra "redukcije modulo n"

$$\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Definicija. Podgrupa Γ 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 Γ 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 Λ 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 Γ od $\mathrm{SL}_2(\mathbb{Z})$ definiramo **modularnu krivulju** kao kvocijentni prostor orbita od Γ, 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 113. *Neka je N prirodan broj.*

a) Skup $Y_0(n)$ je prostor parametara za

$$S_0(N) = \{[E_\tau, \langle 1/N + \Lambda_\tau\rangle] : \tau \in \mathcal{H}\}.$$

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) Skup $Y_1(n)$ je prostor parametara za

$$S_1(N) = \{[E_\tau, 1/N + \Lambda_\tau] : \tau \in \mathcal{H}\}.$$

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 $Y(N)$ 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 definicije $S_1(N)$. Pokažimo prvo da je

$$S_1(N) = \{[E_\tau, 1/N + \Lambda_\tau] : \tau \in \mathcal{H}\}.$$

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 γ 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 Γ. 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 [1, 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.

Prikažimo i način kako možemo dobiti eksplicitni model za modularne krivulje.

Neka je P točka reda $n > 3$ u $E(k)$. Promjenom koordinata, možemo staviti da je $P = (0,0)$ i da E ima sljedeći oblik, koji se naziva (*Tateova normalna forma*).

$$y^2 + (1-c)xy - by = x^3 - bx^2 \tag{7.2}$$

$$-P = (0, b),\ \ 2P = (b, bc),\ \ -2P = (b, 0),\ \ 3P = (c, b - c),\ \ -3P = (c, c^2),$$

$$4P = \left(\frac{b(b-c)}{c^2}, \frac{-b^2(b-c-c^2)}{c^3}\right), \quad -4P = \left(\frac{b(b-c)}{c^2}, \frac{b(b-c)^2}{c^3}\right),$$

$$5P = \left(\frac{-bc(b-c-c^2)}{(b-c)^2}, \frac{bc^2(b^2-bc-c^3)}{(b-c)^3}\right),$$

$$-5P = \left(\frac{-bc(b-c-c^2)}{(b-c)^2}, \frac{b^2(b-c-c^2)^2}{(b-c)^3}\right),$$

$$6P = \left(\frac{(c-b)(c^3+bc-b^2)}{(c-b+c^2)^2}, \frac{c(c-b)^2(bc^2-c^2+3bc-2b^2)}{(c-b+c^2)^3}\right),$$

$$-6P = \left(\frac{(c-b)(c^3+bc-b^2)}{(c-b+c^2)^2}, \frac{c(c^3+bc-b^2)^2}{(c-b+c^2)^3}\right).$$

Slijedi da na primjer, eliptička krivulja s točkomk reda 7 mora zadovoljavati $4P = -3P$, to jest $b^2 - bc = c^3$. Dakle eliptička krivulja ima točku reda 7 ako i samo ako je $b^2 - bc = c^3$.

To je zapravo modularna krivulja $X_1(7)$.

Krivulja $b^2 - bc = c^3$ je singularna kubična krivulja i ima singularitet u $(0, 0)$. Ona je krivulja genusa 0. Zamjenom varijabli $b = cd$ dobivamo parametrizaciju $b = d^3 - d^2$ i $c = d^2 - d$.

Slijedi da eliptičke krivulje s točkom reda 7 čine jedno-parametarsku familiju. Primjetimo da neke vrijednosti od d daju singularne krivulje - to su kuspovi od $X_1(7)$. Sjetimo se da je krivulja $Y_1(7)$ zapravo $X_1(7)$ bez kuspova.

Neka sada E u normalnoj Tateovoj formi ima točju reda 11, tj. neka zadovoljava $6P = -5P$. Dobivamo da mora vrijediti $b^2 - b = c^3 - c$ - ovo je $X_1(11)$. Standardnim metodama možemo izračunati torziu i rang od $X_1(11)(\mathbb{Q})$ dobijemo da $X_1(11)(\mathbb{Q})$ ima 5 racionalnih točaka i da su svi kuspovi.

Na taj način smo zapravo dokazali da ne postoje eliptičke krivulje s točkom reda 11 nad $\mathbb{Q}$!

Poglavlje 8

Krivulje genusa 2

8.0.1 Riemnann-Hurwitzov teorem

Definicija. Kažemo da je morfizam krivulja $\phi : X \to Y$ separabilno/Galoisovo ako je $k(X)$ separabilno/Galoisovo proširenje od $\phi^*(k(Y))$.

Iskažimo sada rezultat o preslikavanjima diferencijala. Za više detalja, vidi [8, Chapter 3.6.1].

Propozicija 114. *Neka je $\phi : X \to Y$ separabilan morfizam krivulja nad poljem k. Tada je $\phi^* : \Omega(Y) \to \Omega(X)$ definirano s $\phi^*(df) = d(\phi \circ f)$ ulaganje polja. Za uniformizator t u točki P, vrijedi $v_P(\phi^* dt) \geq e_\phi(P) - 1$, gdje jednakost vrijedi ako i samo ako je $\operatorname{char} k = 0$ ili je $\operatorname{char} k = p$ i p ne dijeli $e_\phi(P)$.*

Teorem 115. *Neka su X/k, Y/k krivulje, neka je $\phi : X \to Y$ separabilan morfizam krivulja stupnja d, te neka su g_X i g_Y genusi krivulja X i Y. Tada imamo*

$$2g_X - 2 \geq d(2g_Y - 2) + \sum_{P \in X} (e_\phi(P) - 1)P \tag{8.1}$$

Jednakost vrijedi ako i samo ako je ili $\operatorname{char} K = 0$ *ili* $\operatorname{char} K = p > 0$ *i p ne dijeli $e_\phi(P)$ ni za jedan $P \in X$.*

Dokaz. Neka je $P \in X$, te neka je s uniformizator u P, t uniformizator u $\phi(P)$, te neka je $\omega = ft^n dt$ za neki $f \in \mathcal{O}^\times_{\phi(P),Y}$, gdje je $n = v_P(\omega)$. Tada je

$$v_P(\phi^*\omega) = v_P(\phi^* f t^n) + v_P(\phi^* dt).$$

Znamo da je $v_P(\phi^* f t^n) = n v_P(\phi^* t) = n e_\phi(P) = e_\phi(P) v_P(\omega)$, po definiciji divizora diferencijala. Također vrijedi da je $v_P(\phi^*(dt)) \geq e_\phi(P) - 1$ po Propoziciji 114 (jednakost vrijedi ovisno o tome je li $\operatorname{char} k$ dijeli $e_\phi(P)$). Suminjarem po svim točkama i uzimanjem stupnja dobivamo

$$\deg(\operatorname{div} \phi^*(\omega)) \geq \deg \phi^*(\operatorname{div}(\omega)) + \sum_{P \in X} (e_\phi(P) - 1).$$

Sada koristimo činjenicu da je $\deg \phi^*(\operatorname{div}(\omega)) = d \deg \operatorname{div} \omega$, pa pošto je $\deg \operatorname{div} \omega = 2g_Y - 2$ i $\deg \operatorname{div}(\phi^*\omega) = 2g_X - 2$, vrijedi

$$2g_X - 2 \geq d(2g_Y - 2) + \sum_{P \in X} (e_\phi(P) - 1).$$

□

Korolar 116. *Neka su X/k, Y/k krivulje, neka je $\phi : X \to Y$ separabilan morfizam krivulja nad poljem karakteristike 0. Tada je broj $\sum_{P \in X}(e_\phi(P) - 1)$ paran.*

Korolar 117. *Neka je $\phi : X \to Y$ separabilan morfizam krivulja genusa g_X i g_Y. Tada je $g_X \geq g_Y$ te jednakost vrijedi samo ako je $g_Y = 0, 1$ ili je $d = 1$.*

Dokaz. Ako je $g_Y = 0$, tada se nema što dokazivati. Ako je $g_Y = 1$, tada je desna strana u jednadžbi 8.1 očto nenegativna, pa je onda i lijeva strana, što povlači da je $g_X \geq 2$. Ako je $g_Y > 1$, tada je $g_X - 1 \geq d(g_Y - 1) \geq g_Y - 1$, te jednakosti očito vrijede samo ako je $d = 1$. □

Korolar 118. *Ne postoji separabilan nerazgranat morfizam krivulja $f : X \to Y$ nad poljem karkateristike 0 takav da je $g_Y = 0$ i $g_X > 0$.*

Dokaz. Direktno iz Riemann-Hurwitzovog teorema. □

8.0.2 Hipereliptičke krivulje

Definicija. Kažemo da je krivulja C hipereliptička (nad k) ako postoji morfizam (nad k) $\phi : C \to \mathbb{P}^1$ stupnja 2 koji se zove hipereliptičko preslikavanje.

Teorem 119. *Svaka krivulja genusa 2 je hipereliptička.*

Dokaz. Sjetimo se da je $\dim_k(\Omega(0)) = g = 2$, dakle postoje 2 regularna, linearno nezavisna nad k, diferencijala ω_1, ω_2. Sada je $\deg \operatorname{div} \omega_1 = \deg \operatorname{div} \omega_2 = 2g - 2 = 2$. Pošto je $\omega_1/\omega_2 \neq k$, siljedi $\operatorname{div} \omega_1 \neq \operatorname{div} \omega_2$. S druge strane, znamo da je $\dim_{k(C)} \Omega = 1$, pa postoji $f \in k(C)^\times$ takva da je $f = \omega_1/\omega_2$, tj. $\operatorname{div} f = \operatorname{div} \omega_1 - \operatorname{div} \omega_2$. Pošto su $\operatorname{div} \omega_1$ i $\operatorname{div} \omega_2$ efektivni divizori supnja 2, slijedi da je $\deg f \leq 2$. Međutim, nemoguće je da je $\deg f = 1$, jer bi tada C bio genusa 0. □

Dakle postoji kanonska involucija $i : C \to C$ koja mijenja elemente $\phi^{-1}(P)$, za sve $P \in \mathbb{P}^1$. Ona se zove *hipereliptička involucija.* Ta involucija se može promatrati i kao generator Galoisove grupe od $k(C)/\phi^*(k(\mathbb{P}^1))$. Ako je $y^2 = f(x)$, tada hipereliptička involucija djeluje na sljedeći način $i(x, y) = (x, -y)$.

Propozicija 120. *Svaka hipereliptička krivulja C/k, nad poljem k karakteristike različite od 2, genusa g se može zapisati kao*

$$y^2 = \prod_{i=1}^{2g+2} (x - x_i),$$

gdje su $x_i \in \overline{k}$ međusobno različiti.

Dokaz. Prvo primjetimo da je po teoremu 119, $[k(C) : k(x)] = 2$, pa postoji funkcija y koja je kvadratna nad $k(x)$, pa se C može zapisati kao $y^2 = f(x)$. Funkcija y se grana samo u točkama za koje je $y = 0$, te po Riemann-Hurwitzovoj formuli ima

$$\sum_{P \in X} (e_\phi(P) - 1) = 2g_X - 2 - d(2g_Y - 2) = 2g - 2 - (-4) = 2g + 2.$$

Pošto je $e_\phi(P) \leq \deg \phi$, slijedi da postoji točno $2g + 2$ točaka grananja, tj. polinom $f(x)$ ima točno $2g + 2$ nultočaka nad $\overline{k}$. □

8.0.3 Jacobijani krivulja

Definicija. *Abelova mnogostrukost* je projektivna algebarska mnogostrukost na kojima postoji struktura grupe koja se može definirati s regularnim funkcijama.

Teorem 121 (Abel-Jacobijev teorem)**.** *Neka je C/k genusa g. Postoji Abelova mnogostrukost J/k dimenzije g, takva da postoji izomorfizam G_k-modula* $\mathrm{Pic}^0_k C \simeq J(\overline{k})$.

Definicija. Abelova mnogostrukost J iz prethodnog teorema se naziva Jacobijeva mnogostrukost ili samo Jacobijan od C.

Primjer 34. Vidjeli smo da ako je C krivulja genusa 0 tada je $J(\overline{k}) = \{0\}$, te ako je E eliptička krivulja, tada je $E \simeq J$.

Obično poistovjećujemo $J(\overline{k})$ s Pic^0_k; iako je J projektivna mnogostrukost, nije poučno razmišljati o J kao mnogostrukosti. To je zato što ih je izrazito teško realizirati. Npr. Jacobijan krivulje genusa 2 se može prirodno opisati s 72 kvadratne jednadžbe u $\mathbb{P}^{15}$, te ne postoje eksplicitne jednadžbe Jakobijana ni jedne krivulje genusa ≥ 3.

Razlog zašto su nam Jacobijani toliko korisni je sljedeći:

Korolar 122. *Neka je C/k krivulja genusa $g \geq 1$ s Jacobijanom J i neka je $[D_0]$ k-racionalna klasa divizora stupnja 1. Tada je*

$$i_{[D_0]} : C \to J, \quad P \mapsto [P - D_0]$$

ulaganje mnogostrukosti nad k.

Dokaz. Neka je $[P - D_0] = [Q - D_0]$; slijedi da postoji $f \in k(C)$ takav da je $P - D_0 + \operatorname{div} f = Q - D_0$, pa je $\operatorname{div} f = P - Q$. Slijedi da je $P = Q$, jer bi u suprotnom f bio morfizam $f : C \to \mathbb{P}^1$ stupnja 1, pa bi C bio genusa 0. □

Primjetimo sada da hipereliptička krivulja

$$C : y^2 = f(x),$$

definirana nad k, ne mora imati točku nad poljem k, ali mora imati nad nekim kvadratnim proširenjem. To je npr. $(x_0, \sqrt{f(x_0)})$, za bilo koji $x_0 \in k$. Tada je $D_0 = (x_0, \sqrt{f(x_0)}) + (x_0, -\sqrt{f(x_0)})$ k-racionalni divizor stupnja 2.

Lema 123. *Divizor D_0 je kanonski.*

Dokaz. DZ. □

Propozicija 124. *Neka su C i D_0 definirani kao iznad, s tim da pretpostavljamo da je C genusa 2. Tada se svaka točka $0 \neq Y \in J_C(k)$ može prikazati kao $[D] - [D_0]$, za neki jedinstveni efektivni divizor $D \in \mathrm{Div}_k^2 C$.*

Dokaz. Neka je $0 \neq Y \in \mathrm{Div}_k^0 C$, te X neki divizor u klasi od Y, tj. $[X] = Y$, i neka je K neki fiksni kanonski divizor. Tada je po Riemann-Rochu

$$l(X + D_0) = 2 - 1 + l(K - X - D_0) \geq 1.$$

Prvo primjetimo da je $l(K - X - D_0) = 0$ ili 1.

Prvo primjetimo da ako je $l(K-X-D_0) = 1$, to znači da je $X+D_0$ kanonski divizor, tj. X je glavni divizor tj. $[X] = 0$, što je kontradikcija s pretpostavkom.

Ako je $l(K-X-D_0) = 0$, tada je $l(X+D_0) = 1$, dakle postoji jedinstveni, do na množenje s $k^\times$, $f \in k(C)^\times$ takva da je $\mathrm{div}\, f \geq -X-D_0$, tj. $\mathrm{div}\, f+x+D_0 \geq 0$. Pošto je $\deg(\mathrm{div}\, f + X + D_0) = 2$, te je $\mathrm{div}\, f + x + D_0$ efektivan, slijedi da je $\mathrm{div}\, f = -X - D_0 + D$, tj. $D = X + D_0 + \mathrm{div}\, f$ za neki jedinstveni (efektivan) divizor D stupnja 2.

Uzimajući klase, imamo

$$[X] = [D - D_0],$$

dakle traženi divizor D postoji, te je jedinstven. □

Definirajmo $\mathrm{Sym}^2 C$ kao skup neuređenih parova točaka na C (to je zapravo ista stvar kao i $\mathrm{Div}^2 C$). Primjetimo da nam prethodna propozicija govori jako puno o geometriji preslikavanja

$$\begin{aligned} \phi : \mathrm{Sym}^2 C &\longrightarrow J_C \\ \{P, Q\} &\longmapsto [P + Q - D_0]. \end{aligned}$$

Vrijedi sljedeće:

Lema 125. *Preslikavanje ϕ preslikava točke oblika $\{P, i(P)\}$ (gdje je i hipereliptička involucija)u $0 \in J_C$, a na ostatku $\mathrm{Sym}^2 C$ je bijekcija.*

Dokaz. DZ. □

To nam daje jednu zanimljivu posljedicu:

Propozicija 126. *Neka je C/k hipereliptička krivulja nad nekim poljem k dana jednadžbom $y^2 = f(x)$ takva da je $J_C(k) = \{0\}$. Tada su sve kvadratne točke na C oblika $(x, \pm\sqrt{f(x)})$, za neki $x \in k$.*

Dokaz. Neka je $P \in C(F)$ gdje je F neko kvadratno proširenje od k, te neka je σ netrivijalni element u $\mathrm{Gal}(F/k)$. Tada je $\{P, P^\sigma\}$ racionalna točka na $\mathrm{Sym}^2 C$, te je $\phi(\{P, P^\sigma\}) \in J_C(k) = \{0\}$, tj. $\{P, P^\sigma\}$ je fiksiran s hipereliptičkom involucijom, tj. $\{P, P^\sigma\} = \{P, i(P)\}$, tj. $i(P) = P^\sigma$. Ako je sada $P = (x, y)$, tada imamo

$$(x, -y) = i(P) = P^\sigma = (x^\sigma, y^\sigma),$$

dakle $x = x^\sigma$, tj. $x \in k$. □

Bibliografija

[1] F. Diamond and J. Shurman, A First Course in Modular Forms, Springer, 2005.

[2] R. Hartshorne, Algebraic Geometry, Springer

[3] J. S. Milne, Elliptic Curves, 2006. http://www.jmilne.org/math/Books/ectext5.pdf

[4] F. Najman, Eliptičke krivulje nad poljima algebarskih brojeva, 2012. https://web.math.pmf.unizg.hr/~fnajman/elipticke.pdf

[5] B. Poonen, Introduction to Arithmetic Geometry, math.mit.edu/~poonen/782/782notes.pdf

[6] M. Rosen, Number Theory in Function Fields, Springer, 2002.

[7] T. Weston, A brief introduction to local fields, people.math.umass.edu/~weston/oldpapers/local.pdf

[8] I. R. Shafarevich, Basic Algebraic Geometry 1, Third Edition, Springer, 2013.

[9] J. H. Silverman, The arithmetic of elliptic curves, Second Edition, Springer, 2009.

[10] H.Stichtenoth, Algebraic function fields and codes, Springer, 2009.

[11] A. V. Sutherland, Introduction to Arithmetic Geometry, online course notes, http://ocw.mit.edu/courses/mathematics/18-782-introduction-to-arithmetic-geometry-fall-2013/