Riemann-Rochov teorem i primjene

Varivoda, Marin

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Marin Varivoda

RIEMANN-ROCHOV TEOREM I PRIMJENE

Diplomski rad

Voditelj rada:
prof. dr. sc. Filip Najman

Zagreb, studeni 2024.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

Tema ovog rada je Riemann-Rochov teorem za algebarske krivulje i njegove primjene. Riemann-Rochov teorem je važan rezultat u kompleksnoj analizi i algebarskoj geometriji. Teorem je koristan za računanje dimenzije vektorskog prostora meromorfnih (ili racionalnih) funkcija sa zadanim nultočkama i polovima.

Riemann-Rochov teorem je prvi put dokazan u kontekstu kompleksne analize u obliku Riemannove nejednakosti (1857.) za kompaktne Riemannove plohe [5]. Kasnije ga je Gustav Roch poboljšao (1865.) tako što je okarakterizirao razliku između dvije strane nejednakosti (koja se naziva i *indeks specijalnosti*) [6]. Ispostavlja se da svaki član u Riemann-Rochovom teoremu ima prirodni analogon u algebarskoj geometriji, gdje umjesto Riemannovih ploha proučavamo glatke algebarske krivulje. U ovom radu dokazujemo teorem za algebarske krivulje i navodimo neke primjene.

Eliptičke krivulje su glatke algebarske krivulje genusa 1, s istaknutom racionalnom točkom. One su veoma aktualno područje istraživanja u teoriji brojeva. Dokazujemo da iz Riemann-Rochovog teorema slijedi da je svaka eliptička krivulja, do na izomorfizam, zadana s Weierstrassovom jednadžbom. Također demonstriramo kako se preko divizora definira grupni zakon na racionalnim točkama eliptičke krivulje. Nadalje, pomoću Riemann-Rochovog teorema potpuno klasificiramo do na izomorfizam glatke algebarske krivulje genusa 0 s racionalnom točkom, tako što dokazujemo da su izomorfne projektivnom pravcu. Navodimo i još neke primjene kao što su Cliffordov teorem koji je bitan rezultat za proučavanje specijalnih divizora.

U prvom poglavlju ovog rada definiramo algebarske i projektivne mnogostrukosti, te njihova osnovna svojstva. Također definiramo racionalna preslikavanja i morfizme između mnogostrukosti.

U drugom poglavlju se bavimo algebarskim krivuljama, tj. projektivnim mnogostrukostima dimenzije 1. Uvodimo funkcijska polja, te iskazujemo ekvivalenciju kategorija krivulja i funkcijskih polja. To nam omogućava da algebarskim pristupom, proučavajući funkcijska polja, dokažemo neke osnovne tvrdnje o krivuljama. Navodimo bitnu karakterizaciju racionalnih preslikavanja između glatkih krivulja, da je svako ili konstantno ili surjektivni morfizam. Uvodimo pojam divizora i Picardove grupe koja je pridružena svakoj krivulji.

U trećem poglavlju dokazujemo Riemann-Rochov teorem tako što uspostavimo nekoliko rezultata o Riemann-Rochovom prostoru. To je prostor racionalnih funkcija sa zadanim nultočkama i polovima, koji je definiran za svaki divizor. Definiramo genus glatke krivulje, koji je općenito važna invarijanta za klasifikaciju krivulja. Prvo dokazujemo Riemannovu nejednakost koja povezuje dimenziju Riemann-Rochovog prostora, stupanj divizora i genus krivulje. Onda pojačavamo taj rezultat karakterizirajući indeks specijalnosti. Za razumijevanje indeksa specijalnosti, uvodimo prstene adela i Weilove diferencijale. Pokazujemo kako divizori pridruženi Weilovim diferencijalima tvore kanonsku klasu divizora, koja nam je bitna u iskazu Riemann-Rochovog teorema. Na primjeru pokazujemo kako izračunati kanonsku klasu. Konačno iskazujemo Riemann-Rochov teorem i navodimo njegove posljedice.

Poglavlje 1

Osnovni pojmovi algebarske geometrije

Za početak uvedimo oznake, k će nam označavati savršeno (svako algebarsko proširenje od k je separabilno) polje, $\bar{k}$ je neko fiksno algebarsko zatvorenje od k, te $G_k := Gal(\bar{k}/k)$ je apsolutna Galoisova grupa.

1.1 Afine mnogostrukosti

Definicija 1.1.1. Za $n \in \mathbb{N}_0$, n-dimenzionalni *Afini prostor* nad k je skup

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

Slično, ako je $k \subseteq L \subseteq \bar{k}$, tada je *skup L-racionalnih točaka* od $\mathbb{A}^n$

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

Alternativno, $\mathbb{A}^n(L)$ su točno elementi od $\mathbb{A}^n_k$ fiksirani pri djelovanju G_k.

Definicija 1.1.2. Neka je $S \subseteq \bar{k}[x_1, \ldots, x_n]$ skup polinoma. Tada se skup točaka

$$Z_S = \{P \in \mathbb{A}^n : f(P) = 0, \ \forall f \in S\}$$

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

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

Kada S ima jedan element $S = \{f\}$, pišemo skraćeno $Z_f = Z_{\{f\}}$.

Napomena 1.1.3. Ako je $I = (S) \subseteq \bar{k}[x_1, \ldots, x_n]$ ideal generiran s S, tada vrijedi $Z_I = Z_S$. To znači da uvijek možemo zamijeniti S s idealom (S) kojeg taj skup generira.

Definicija 1.1.4. Ako je $Z \subseteq \mathbb{A}^n$ algebarski skup, ideal $I(Z)$ od Z je

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

Propozicija 1.1.5. *Vrijedi*

1. $Z_{I_1} \cup Z_{I_2} = Z_{I_1 I_2}$ *(unija dva algebarska skupa je algebarski skup),*
2. $\cap_{j \in J} Z_{I_j} = Z_{\cup_{j \in J} I_j}$ *(presjek familije alg. skupova je alg. skup),*
3. $Z_{(0)} = \mathbb{A}^n$*, te* $Z_{(1)} = \emptyset$ *(*$\mathbb{A}^n$ *i* $\emptyset$ *su algebarski skupovi),*
4. $S \subseteq T \implies Z_T \subseteq Z_S$ *(Z obrće inkluzije),*
5. $Z_{I(Y)} = Y$ *za algebarski skup* $Y \subseteq \mathbb{A}^n$*,*
6. $Z_{I(W)} = \overline{W}$ *za proizvoljni skup* $W \subseteq \mathbb{A}^n$*.*

Definicija 1.1.6. *Topologija Zariskog* na $\mathbb{A}^n$ je topologija u kojoj su zatvoreni skupovi točno svi algebarski skupovi.

Iz Propozicije 1.1.5, vidimo da je ovo uistinu dobra definicija topologije. Alternativno možemo definirati i topologiju Zariskog preko otvorenih podskupova. Za $f \in \bar{k}[x_1, \ldots, x_n]$ definiramo *osnovni otvoreni skup* $D(f) := \mathbb{A}^n \setminus Z_f$.

Propozicija 1.1.7. *Osnovni otvoreni skupovi* $D(f)$ *čine bazu za topologiju Zariskog na* $\mathbb{A}^n$*. Štoviše za sve* $f \neq 0$*,* $D(f)$ *je gust.*

Dokaz. Očito je svaki $D(f)$ otvoren jer mu je komplement Z_f zatvoren. Vrijedi $\mathbb{A}^n \setminus Z_I = \cup_{f \in I} D(f)$ tj. svaki otvoreni podskup je unija osnovnih. Zaključujemo da osnovni otvoreni podskupovi čine bazu. Neka je sada $f \in \bar{k}[x_1, \ldots, x_n]$, $f \neq 0$. Tada postoji ideal I takav da $\overline{D(f)} = Z_I$. Ako je $g \in I$, tada je $D(f) \subseteq Z_I \subseteq Z_g$ što znači da

$$f(P) \neq 0 \implies P \in D(f) \implies P \in Z_g \implies g(P) = 0.$$

Zaključujemo da je $(f \cdot g)(P) = 0, \ \forall P \in \mathbb{A}^n$. Općenito vrijedi sljedeće:

(1) Ako je L beskonačno polje i $f \in L[x_1, \ldots, x_n]$ takav da $f(P) = 0, \ \forall P \in \mathbb{A}^n(L)$ onda je $f = 0$.

(2) Ako je L algebarski zatvoreno polje, onda je L beskonačno.

Dokažimo prvo (1). Ako je $n = 1$ tvrdnja je očita. Inače zapišemo $f(x_1, \ldots, x_n) = \sum_i g_i(x_1, \ldots, x_{n-1}) x_n^i$. Za fiksne $x_1, \ldots, x_{n-1}$ imamo polinom u jednoj varijabli x_n sa konstantnim koeficijentima. Varirajući x_n zaključimo da taj polinom ima beskonačno nultočaka pa su svi koeficijenti $g_i(x_1, \ldots, x_{n-1}) = 0$. Tada je $g_i(Q) = 0,\ \forall Q \in \mathbb{A}^{n-1}(L)$. Indukcijom su svi $g_i = 0$, dakle $f = 0$. Napomenimo još da ovo ne mora vrijedit ako polje L nije beskonačno. Primjerice za $L = \mathbb{F}_7$ i $f(x) = x^7 - x$ imamo $f(P) = 0$ za sve $P \in \mathbb{A}^1(\mathbb{F}_7) = \mathbb{F}_7$, ali $f \neq 0$.

Za (2) ako je L konačno i algebarski zatvoreno, onda možemo konstruirati polinom $f(x) := \prod_{l \in L}(x - l) + 1 \in L[x]$ koji je nekonstantan, ali nema nultočku u L što je kontradikcija.

Vratimo se na dokaz propozicije. Imali smo $(f \cdot g)(P) = 0,\ \forall P$ za polinom $f \cdot g \in \bar{k}[x_1, \ldots, x_n]$. Koristeći (1) i (2) zaključujemo da $f \cdot g = 0$. S obzirom da je $f \neq 0$ i $\bar{k}[x_1, \ldots, x_n]$ je integralna domena slijedi $g = 0$. To znači da je nužno $I = (0)$, tj. $\overline{D(f)} = Z_I = \mathbb{A}^n$. □

Korolar 1.1.8. *Svi neprazni otvoreni skupovi u $\mathbb{A}^n$ su gusti.*

Da bolje shvatimo algebarske skupove, možemo ih konkretno karakterizirati kao skup nultočaka od nekog konačnog skupa polinoma. Za to će nam biti koristan Hilbertov teorem o bazi.

Definicija 1.1.9. Komutativni prsten s jedinicom R koji zadovoljava sljedeća 3 međusobno ekvivalentna uvjeta

(1) Svaki ideal u R je konačno generiran.

(2) Svaki rastući niz ideala
$$I_1 \subseteq I_2 \subseteq \ldots$$
se od nekog elementa stabilizira, tj. $\exists n \in \mathbb{N}$ takav da $I_m = I_n,\ \forall m \geq n$.

(3) Svaki neprazan skup ideala iz R sadrži maksimalan element s obzirom na inkluziju.

nazivamo *Noetherin* prsten.

Teorem 1.1.10 (Hilbertov teorem o bazi)**.** *Ako je R Noetherin prsten, tada je i $R[x]$ Noetherin.*

Dokaz. Vidi [1] za dokaz. □

Korolar 1.1.11. *$\bar{k}[x_1, \ldots, x_n]$ i $k[x_1, \ldots, x_n]$ su oba Noetherini prstenovi, te su svi pripadni ideali konačno generirani.*

Dokaz. Uzmemo niz proširenja

$$\bar{k} \subseteq \bar{k}[x_1] \subseteq \bar{k}[x_1, x_2] \subseteq \ldots \subseteq \bar{k}[x_1, \ldots, x_n]$$

i na njih uzastopno primjenjujemo Hilbertov teorem. □

Ako je Z algebarski skup, koristeći prethodni korolar zaključujemo da je pridruženi ideal $I(Z)$ konačno generiran nekim polinomima $f_1, \ldots, f_k \in \bar{k}[x_1, \ldots, x_n]$, tj. $I(Z) = (f_1, \ldots, f_k)$. Tada su točke $P \in Z$ točno one koje zadovoljavaju konačan niz uvjeta $f_i(P) = 0$ za $i = 1, \ldots, k$. Dakle vrijedi

$$P \in Z \iff f_i(P) = 0, \ \forall i = 1, \ldots, m.$$

Možemo ovo zapisati i kao

$$Z = \bigcap_{j=1}^{m} Z_{f_j}.$$

Definicija 1.1.12. Neka je R komutativni 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*.

Općenito vrijedi da je $J \subseteq \sqrt{J}$ i $\sqrt{\sqrt{J}} = \sqrt{J}$.

Teorem 1.1.13 (Hilbertov Nullstellensatz)**.** *Za svaki pravi ideal $I \subseteq \bar{k}[x_1, \ldots, x_n]$ vrijedi*

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

Dokaz. Poglavlje 4 u [1]. □

Korolar 1.1.14. *Neka je $R = \bar{k}[x_1, \ldots, x_n]$. Vrijedi*

(i) $Z_{J_1} = Z_{J_2} \iff \sqrt{J_1} = \sqrt{J_2}$,

(ii) $Z_J = \emptyset \iff J = R$,

(iii) $Z(J) = \mathbb{A}^n \iff J = (0)$,

gdje su J_1, J_2, J ideali u R.

Dokaz. Dokažimo (*i*). Očito $Z_{J_1} = Z_{J_2} \implies I(Z_{J_1}) = I(Z_{J_2})$. Primjenom Nullstellensatza dobivamo $\sqrt{J_1} = \sqrt{J_2}$.

Za drugi smjer, pokažimo prvo da vrijedi $Z_J = Z_{\sqrt{J}}$ za svaki ideal J u R. Vrijedi $J \subseteq \sqrt{J}$ pa zato imamo $Z_{\sqrt{J}} \subseteq Z_J$. Neka je sad $P \in Z_J$. To znači da je $f(P) = 0,\ \forall f \in J$. Ako je $g \in \sqrt{J}$, onda postoji $r \in \mathbb{N}$ takav da $g^r \in J$ dakle $g^r(P) = 0$, iz čega slijedi $g(P) = 0$. Dakle $g(P) = 0,\ \forall g \in \sqrt{J}$ što znači da je $P \in Z_{\sqrt{J}}$. S time smo pokazali da $Z_J \subseteq Z_{\sqrt{J}}$ pa konačno imamo $Z_J = Z_{\sqrt{J}}$.

Pretpostavimo sada $\sqrt{J_1} = \sqrt{J_2}$. Imamo $Z_{J_1} = Z_{\sqrt{J_1}} = Z_{\sqrt{J_2}} = Z_{J_1}$ kao što je traženo. Tvrdnje (*ii*), (*iii*) slijede direktno iz (*i*). □

Korolar 1.1.15 (Slabi Nullstellensatz)**.** *Za svaki pravi ideal $I \subseteq \bar{k}[x_1, \ldots, x_n]$, algebarski skup Z_I je neprazan.*

Dokaz. Napomenimo da je poznat rezultat komutativne algebre da je $\sqrt{I}$ presjek svih prostih ideala koji sadrže I tj. $\sqrt{I} = \bigcap_{I \subseteq P} P$ gdje su P prosti. To znači da je $\sqrt{I}$ također pravi ideal pa tvrdnja slijedi iz (*ii*) u Korolaru 1.1.14. □

Korolar 1.1.16. *Postoji* 1*-na-*1 *korespondencija između radikalnih ideala u prstenu $\bar{k}[x_1, \ldots, x_n]$ i algebarskih skupova u $\mathbb{A}^n$ koja je dana sa*

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

Ova korespondencija je izrazito važna jer nam dopušta da proučavamo algebarske skupove preko ideala u odgovarajućem prstenu, koji su nam u praksi puno pristupačniji.

Korolar 1.1.17. *Svi maksimalni ideali u $\bar{k}[x_1, \ldots, x_n]$ su oblika*

$$\mathfrak{m}_P = (x_1 - p_1, \ldots, x_n - p_n)$$

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

Dokaz. Ako je M maksimalni ideal, iz Nullstellensatza dobivamo da je zkup Z_M neprazan. Ako je $P \in Z_M$, tada je $M \subseteq I(\{P\})$ iz čega slijedi $M = I(\{P\}) = \mathfrak{m}_P$. S druge strane, ako je $\mathfrak{m}_P \subseteq I$ za neki pravi ideal I, tada je $\emptyset \neq Z_I \subseteq Z_{\mathfrak{m}_P} = \{P\} \implies Z_I = \{P\}$. Iz Nullstellensatza dobivamo $\sqrt{I} = I(\{P\}) = \mathfrak{m}_P$. Dakle $I \subseteq \sqrt{I} = \mathfrak{m}_P \subseteq I$. Zaključujemo da je $\mathfrak{m}_P = I$, dakle za proizvoljnu $P \in \mathbb{A}^n$, ideal $\mathfrak{m}_P$ je maksimalan. □

Definicija 1.1.18. U topološkom prostoru X, neprazan podskup $Y \subseteq X$ je *ireducibilan* ako nije unija 2 prava relativno zatvorena (u induciranoj topologiji na Y) podskupa. Podskup Y je *ireducibilna komponenta* ako je maksimalan ireducibilan podskup od X (s obzirom na inkluziju).

Propozicija 1.1.19. *Označimo $R = \bar{k}[x_1, \ldots, x_n]$. Neprazan podskup $Y \subseteq \mathbb{A}^n$ je ireducibilan ako i samo ako je $R(Y) = R/I(Y)$ integralna domena.*

Dokaz. Smjer " $\Longrightarrow$ ": Ako $R(Y)$ nije integralna domena tada $I(Y)$ nije prost ideal, pa postoje $f_1, f_2 \in R$ takvi da $f_1 f_2 \in I(Y)$, ali f_1, f_2 nisu u $I(Y)$. To znači da za svaki $P \in Y$ vrijedi $f_1(P) = 0$ ili $f_2(P) = 0$, dakle $Y \subseteq Z_{f_1} \cup Z_{f_2}$. Primijetimo da Z_{f_1} ne sadrži Y jer bi to značilo da je f_1 u $I(Y)$ što ne vrijedi. Također $Z_{f_1} \cap X \neq \emptyset$ jer bi inače bilo $f_1(P) \neq 0 \implies f_2(P) = 0$ za sve P u Y, tj. $f_2 \in I(Y)$ što također ne vrijedi. Dakle $Z_{f_1} \cap Y$ je pravi, relativno zatvoreni podskup od Y. Analogno, isto vrijedi i za $Z_{f_2} \cap Y$. Pošto je $Y = (Z_{f_1} \cap Y) \cup (Z_{f_2} \cap Y)$, slijedi da je Y reducibilan.

Smjer " $\Longleftarrow$: Pretpostavimo da je Y reducibilan, tada $Y = (Z_1 \cap Y) \cup (Z_2 \cap Y)$ gdje su Z_1, Z_2 zatvoreni u $\mathbb{A}^n$ i $(Z_j \cap Y)$, $j = 1, 2$ su pravi podskupovi od Y. Označimo $I_j := I(Z_j)$, $j = 1, 2$. Tada je $Z_1 \cup Z_2 = Z_{I_1 I_2} \implies I_1 I_2 \subseteq I(Z_1 \cup Z_2)$. $Y \subseteq Z_1 \cup Z_2$ sad daje $I(Z_1 \cup Z_2) \subseteq I(Y)$ pa zaključujemo $I_1 I_2 \subseteq I(Y)$. Ciljajući na kontradikciju, pretpostavimo da je $I(Y)$ prost. Tada je nužno $I_1 \subseteq I(Y)$ ili $I_2 \subseteq I(Y)$. Bez smanjenja općenitosti pretpostavimo da je $I_1 \subseteq I(Y)$. Tada $Y \subseteq Z_{I(Y)} \subseteq Z_{I_1} \subseteq Z_1$ što znači da $Z_1 \cap Y$ nije pravi podskup od Y, dakle došli smo do kontradikcije. Zaključujemo da $I(Y)$ nije prost i ekvivalentno $R(Y)$ nije integralna domena. □

Definicija 1.1.20. Topološki prostor X je *Noetherin* ako se svaki padajući niz zatvorenih podskupova stabilizira od nekog elementa, tj. za niz zatvorenih skupova

$$F_1 \supseteq F_2 \supseteq F_3 \supseteq \ldots$$

postoji $n \in \mathbb{N}$ takav da $F_m = F_n$, $\forall m \geq n$.

Primijetimo da je $\mathbb{A}^n$ Noetherin topološki prostor, kao posljedica činjenice da je $\bar{k}[x_1, \ldots, x_n]$ Noetherin i korespondencije između zatvorenih skupova i ideala koju smo uspostavili.

Teorem 1.1.21. *Neka je X Noetherin topološki prostor. Tada*

(i) X sadrži konačno mnogo ireducibilnih komponenti.

(ii) Nijedna ireducibilna komponenta od X nije sadržana u uniji ostalih ireducibilnih komponenti.

Dokaz. Vidi Propoziciju 2.14. u [3]. □

Korolar 1.1.22. *Svaki algebarski skup u $\mathbb{A}^n$ se može na jedinstven način prikazati kao konačna unija mnogostrukosti, gdje nijedna ne sadrži drugu.*

Ovaj teorem dokazuje da se svaki algebarski skup može jedinstveno zapisati kao unija ireducibilnih komponenti.

Definicija 1.1.23. *Afina mnogostrukost V* je ireducibilan algebarski skup u $\mathbb{A}^n$.

Definicija 1.1.24. Algebarski skup $Z \subseteq \mathbb{A}^n$ je *definiran nad k* ako je $I(Z)$ generiran s polinomima iz $k[x_1, \ldots, x_n]$. Pišemo Z/k da bi naznačili da je Z definiran nad k. Također definiramo

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

Ako je Z definiran nad k, uočimo da apsolutna Galoisova grupa $G_k = Gal(\bar{k}/k)$ djeluje na Z zato što za sve $f \in k[x_1, \ldots, x_n]$, $P \in Z$ vrijedi $f(\sigma(P)) = \sigma(f(P))$ gdje $\sigma \in G_k$. Primijetimo da je

$$Z(k) = Z \cap \mathbb{A}^n(k) = \{P \in Z : \sigma(P) = P,\ \forall \sigma \in G_k\}.$$

Definicija 1.1.25. Neka je Z algebarski skup definiran nad k. *Afin koordinatni prsten* ili samo *koordinatni prsten* od Z/k je prsten

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

Također definiramo

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

Primijetimo da ako je Z/k algebarska mnogostrukost definirana nad k, tada su $I(Z)$ i $I(Z/k)$ prosti ideali ili ekvivalentno $k[Z]$ i $\bar{k}[Z]$ su integralne domene.

Primjer 1.1.26. Potencijalno je moguće da je $I(Z/k)$ prost ideal dok $I(Z)$ nije. Neka je $k = \mathbb{Q}$ i $f(x) = x^2 + 1$. Tada je $Z_f = \{i, -i\} \subseteq \mathbb{A}^1(\overline{\mathbb{Q}})$. Primijetimo daje $Z_f(\mathbb{Q}) = \emptyset$. Imamo da je $I(Z/\mathbb{Q}) = (x^2 + 1)\mathbb{Q}[x]$ prost ideal u $\mathbb{Q}[x]$ dok $I(Z) = (x + i)(x - i)$ nije prost ideal u $\overline{\mathbb{Q}}[x]$. To konkretno znači da Z nije afina mnogostrukost.

Definicija 1.1.27. neka je V/k afina mnogostrukost definirana nad k. *Funkcijsko polje* $k(V)$ od V je polje razlomaka od $k[V]$. Slično, $\bar{k}(V)$ je polje razlomaka od $\bar{k}[V]$.

Primjer 1.1.28. Za afinu mnogostrukost $V = \mathbb{A}^n$ imamo $k(V) = k(x_1, \ldots, x_n)$. Za afinu mnogostrukost $\{P\}$ koja je sačinjena od jedne točke $P \in \mathbb{A}^n$ imamo $k(\{P\}) = k$.

Definicija 1.1.29. Za afinu mnogostrukost V, *dimenzija* $\dim V$ do V je stupanj transcendentnosti od polja $\bar{k}(V)$ nad $\bar{k}$.

Dimenzije mnogostrukosti iz prethodnog primjera su $\dim \mathbb{A}^n = n$ i $\dim\{P\} = 0$. Napomenimo da dimenziju možemo alternativno definirati kao duljinu najdužeg lanca prostih ideala u koordinatnom prstenu $\bar{k}[V]$. Tu podrazumijevamo da lanac prostih ideala oblika $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ ima *duljinu n*. Općenito supremum duljina lanaca prostih ideala

u komutativnom prstenu R nazivamo *Krullova dimenzija*. Ona ne mora biti konačna za proizvoljni prsten, ali u slučaju koordinatnih prstenova $\bar{k}[V]$ koji su pridruženi afinim mnogostrukostima, ona je konačna i jednaka $\dim V$. Inspirirani Krullovom dimenzijom i korespondencijom između zatvorenih skupova i ideala, za općeniti topološki prostor X možemo definirati $\dim X$ kao supremum duljina lanaca ireducibilnih zatvorenih podskupova. Hilbertov nullstellensatz sad implicira da je Krullova dimenzija od $\bar{k}[V]$ jednaka dimenziji topološkog prostora V s topologijom Zariskog. Konkretno, to znači da je $\dim V$ jednaka duljini najdužeg lanca afinih mnogostrukosti sadržanih u V.

Primjer 1.1.30. Za $\mathbb{V} = \mathbb{A}^3$ imamo da je $\dim V = 3$. Primijetimo da je

$$\{(0,0,0)\} \subsetneq \mathbb{A}^1 \times \{(0,0)\} \subsetneq \mathbb{A}^2 \times \{0\} \subsetneq \mathbb{A}^3 = V$$

primjer lanca afinih mnogostrukosti strogo sadržanih u $\mathbb{A}^3$ duljine 3. Može se pokazati da je to ujedno i najdulji mogući takav lanac.

Definicija 1.1.31. Neka je V afina mnogostrukost, $P \in V$ točka, i $f_1, \ldots, f_m \in \bar{k}[x_1, \ldots, x_m]$ skup generatora za $I(V)$. Kažemo da je V *nesingularna* (ili *glatka*) *u* P ako $m \times n$ Jacobijeva matrica

$$\left[\frac{\partial f_i}{\partial x_j}(P)\right]_{\substack{1 \le i \le m \\ 1 \le j \le n}}$$

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

Napomena 1.1.32. Neka je V zadana jednom nekonstantnom polinomijalnom jednadžbom

$$V : f(x_1, \ldots, x_n) = 0.$$

Tada je po prethodnoj definiciji točka $P \in V$ singularna ako i samo ako

$$\frac{\partial f}{\partial x_1}(P) = \ldots = \frac{\partial f}{\partial x_n}(P) = 0.$$

1.2 Projektivne mnogostrukosti

Definicija 1.2.1. Za $n \in \mathbb{N}_0$ definiramo relaciju ekvivalencije $\sim$ na $\mathbb{A}^{n+1} \setminus \{(0, \ldots, 0)\}$ sa

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \iff \exists \lambda \in k^\times \text{ takav da } (a_0, \ldots, a_n) = \lambda \cdot (b_0, \ldots, b_n).$$

Definiramo n-dimenzionalni *projektivni prostor* $\mathbb{P}^n := \mathbb{A}^{n+1}/\sim$ kao skup klasa ekvivalencije relacije $\sim$. Klasu ekvivalencije kojoj pripada točka $(a_0, \ldots, a_n)$ nazivamo *projektivna točka* i označavamo sa $(a_0 : \ldots : a_n)$. Za polje $k \subseteq L \subseteq \bar{k}$, skup *L-racionalnih točaka* od $\mathbb{P}^n$ je

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

Uočimo da apsolutna Galoisova grupa G_k na prirodan način djeluje na $\mathbb{P}^n$ sa

$$\sigma((a_0, \ldots, a_n)) = (\sigma(a_0), \ldots, \sigma(a_n)).$$

Slično kao u afinom slučaju, skup k-racionalnih točaka $\mathbb{P}^n(k)$ je ponovno skup točaka iz $\mathbb{P}^n$ koje djelovanje G_k fiksira.

Definicija 1.2.2. Polinom $f \in \bar{k}[x_0, \ldots, x_n]$ je *homogen stupnja d* ako je

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n), \ \forall \lambda \in \bar{k}.$$

Kažemo da je f *homogen* ako je homogen stupnja d za neki cijeli broj d.

Definicija 1.2.3. Ideal I u $\bar{k}[x_0, \ldots, x_n]$ je *homogen* ako je generiran homogenim polinomima.

Uočimo da ako je $f \in \bar{k}[x_0, \ldots, x_n]$ homogeni polinom, ima smisla pitati je li $f(P) = 0$ za neku projektivnu točku $P \in \mathbb{P}^n$ jer to ne ovisi o izboru reprezenta iz $\mathbb{A}^{n+1}$ od P u kojem biramo evaluirati f.

Definicija 1.2.4. *Projektivni algebarski skup* je svaki skup oblika Z_I za neki homogeni ideal I gdje

$$Z_I := \{P \in \mathbb{P}^n : f(P) = 0, \ \forall f \in I\}.$$

Ako je Z projektivni algebarski skup, *homogeni ideal* od Z koji označavamo sa $I(Z)$ je ideal u $\bar{k}[x_0, \ldots, x_n]$ generiran sa

$$I(Z) := \left(\{f \in \bar{k}[x_0, \ldots, x_n] : f \text{ je homogen i } f(P) = 0, \ \forall P \in Z\}\right).$$

Kažemo da je projektivni algebarski skup Z *definiran nad k* ako je $I(Z)$ generiran s homogenim polinomima iz $k[x_0, \ldots, x_n]$ i tada pišemo Z/k. Ako je Z definiran nad k, tada je skup *k-racionalnih točaka od Z* skup

$$Z(k) := Z \cap \mathbb{P}^n(k).$$

Kao i u afinom slučaju, $Z(k)$ se sastoji od točaka iz Z koje su fiksirane pri djelovanju apsolutne Galoisove grupe G_k.

Definicija 1.2.5. *Topologija Zariskog* na $\mathbb{P}^n$ je topologija u kojoj su zatvoreni skupovi upravo projektivni algebarski skupovi.

Lako se provjeri da svojstva iz Propozicije 1.1.5 vrijede i za projektivne algebarske skupove pa je zato Topologija Zariskog na $\mathbb{P}^n$ dobro definirana.

Definicija 1.2.6. Projektivni algebarski skup $V \subseteq \mathbb{P}^n$ nazivamo *projektivna mnogostrukost* ako je pridruženi homogeni ideal $I(V)$ prost u $\bar{k}[x_0, \ldots, x_n]$. Ekvivalentno, V je projektivna mnogostrukost ako je ireducibilan s obzirom na topološki prostor $\mathbb{P}^n$.

Ako je $f \in \bar{k}[x_0, \ldots, x_n]$ homogeni polinom stupnja 1, skup njegovih nultočaka Z_f nazivamo *hiperravnina*. Konkretno, označimo skup nultočaka od x_i sa

$$H_i := Z_{x_i} = \{(a_0 : \ldots : a_n) \in \mathbb{P}^n : a_i = 0\}$$

za $i = 0, \ldots, n$. Neka je U_i otvoreni skup $\mathbb{P}^n \setminus H_i$. Možemo definirati preslikavanje sa

$$\begin{aligned} \phi_i : U_i &\to \mathbb{A}^n \\ (a_0 : \ldots : a_n) &\mapsto \left(\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots \frac{a_n}{a_i}\right) \end{aligned}$$

Par (U_i, ϕ_i) nazivamo *afina karta*. Lako je provjeriti da je ϕ_i bijekcija i zato skup U_i možemo smatrati kopijom od $\mathbb{A}^n$ koja je uložena u $\mathbb{P}^n$. Uočimo i da ja projektivni n-prostor prekriven afinim kartama, tj. $\mathbb{P}^n = U_0 \cup \ldots \cup U_n$.

Propozicija 1.2.7. *Preslikavanje $\varphi_i : U_i \to \mathbb{A}^n$ je homeomorfizam, gdje je topologija na U_i inducirana iz $\mathbb{P}^n$.*

Prije nego što dokažemo propoziciju, opisat ćemo preslikavanje između homogenih polinoma u $\bar{k}[x_0, \ldots, x_n]$ i polinoma u $\bar{k}[y_1, \ldots, y_n]$ (koordinatni prsten od $\mathbb{A}^n$). Prvo fiksirajmo neki indeks $0 \leq i \leq n$. Za polinom $f \in \bar{k}[y_1, \ldots, y_n]$ stupnja d definiramo njegovu *homogenizaciju* $F \in \bar{k}[x_0, \ldots, x_n]$ kao homogeni polinom

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

Obrnuto, za neki homogeni polinom $F \in \bar{k}[x_0, \ldots, x_n]$ kažemo da je $f \in \bar{k}[y_1, \ldots, y_n]$ definiran sa

$$f(y_1, \ldots, y_n) = F(y_1, \ldots, y_i, 1, y_{i+1}, \ldots, y_n)$$

dehomogenizacija od F. Označavat ćemo dehomogenizaciju od F sa $\alpha(F) = f$ i obratno homogenizaciju od f sa $\beta(f) = F$. Sada smo spremni dokazati tvrdnju.

Dokaz. S obzirom da je φ bijekcija, dovoljno je provjeriti da preslikava zatvorene podskupove 1-na-1. Prvo pretpostavimo da je Y relativno zatvoren u U_i. Neka je $\overline{Y}$ zatvorenje od Y u $\mathbb{P}^n$. Imamo da je $Y = \overline{Y} \cap U_i$. Nadalje $\overline{Y}$ je projektivni algebarski skup što znači da ima pridružen homogeni ideal $I = I(Y)$. Neka je $\{F_a\}_{a \in A}$ neki skup homogenih polinoma koji generira I. Za svaki $a \in A$ neka je f_a dehomogenizacija od F_a i neka je J ideal u $\bar{k}[y_1, \ldots, y_n]$ generiran sa $\{f_a\}_{a \in A}$. Tvrdimo da je $\varphi(Y) = Z_J$. Za $P \in U_i$ možemo izabrati

reprezent $(a_0, \ldots, a_n)$ za P takav da je $a_i = 1$. Sada vidimo da je $f_a(\varphi(P)) = F_a(a_0, \ldots, a_n)$ dakle $f_a(\varphi(P)) = 0 \iff F_a(P) = 0,\ \forall a \in A$ ili $\varphi(P) \in Z_J \iff P \in Z_I$. S obzirom da je $Z_I \cap U_i = Y$ zaključujemo da je $\varphi(Y) = Z_J$. Dakle φ preslikava zatvorene podskupove u zatvorene podskupove.

Obratno, neka je sada $W = Z_{J'}$ zatvoren podskup od $\mathbb{A}^n$. Neka je I homogeni ideal u $\bar{k}[x_0, \ldots, x_n]$ generiran sa $\{\beta(f) : f \in J'\}$. Sada je $Y := Z_I \cap U_i$ relativno zatvoren u U_i. Ako sada krenuvši od I definiramo J isto kao u prethodnom slučaju, onda imamo $\varphi(Y) = Z_J$. Nije teško vidjeti da je $J' = J$ dakle $\varphi^{-1}(W) = Y$. Zaključujemo da φ^{-1} također preslikava zatvorene podskupove u zatvorene podskupove i konačno φ je homeomorfizam. □

S obzirom na prethodni teorem, za neki fiksni i (npr. $i = 0$) ćemo poistovjetiti $\mathbb{A}^n$ sa skupom U_i u $\mathbb{P}^n$. Tako ćemo primjerice za projektivnu mnogostrukost $V \subseteq \mathbb{P}^n$ umjesto $\varphi(V \cap U_i)$ pisati $V \cap \mathbb{A}^n$.

Definicija 1.2.8. Neka je $Z \subseteq \mathbb{A}^n$ afini algebarski skup s idealom $I(Z)$. Ako poistovjetimo Z sa podskupom $\varphi_i^{-1}(Z)$ od $\mathbb{P}^n$, *projektivno zatvorenje* od Z je zatvorenje od $\varphi_i^{-1}(Z)$ u topologiji Zariskog na $\mathbb{P}^n$. Projektivno zatvorenje označavamo sa $\overline{Z} := \overline{\varphi_i^{-1}(Z)}$.

Napomena 1.2.9. Za projektivno zatvorenje $\overline{Z}$, homogeni ideal $I(\overline{Z})$ je generiran sa $\{\beta(f) : f \in I(Z)\}$.

Propozicija 1.2.10. *(i) Neka je Z afini algebraski skup. Tada je $\overline{Z}$ projektivni algebarski skup i*

$$Z = \overline{Z} \cap \mathbb{A}^n.$$

Štoviše ako je Z afina mnogostrukost, onda je projektivno zatvorenje $\overline{Z}$ projektivna mnogostrukost.

(ii) Neka je Y projektivna mnogostrukost. Ako je $Y \cap \mathbb{A}^n \neq \emptyset$ onda je $Y \cap \mathbb{A}^n$ afina mnogostrukost i

$$Y = \overline{Y \cap \mathbb{A}^n}.$$

(iii) Ako je afina mnogostrukost Z definirana nad k, onda je projektivna mnogostrukost $\overline{Z}$ definirana nad k. Obratno, ako je projektivna mnogostrukost Y definirana nad k i $Y \cap \mathbb{A}^n \neq \emptyset$, onda je afina mnogostrukost $Y \cap \mathbb{A}^n$ definirana nad k.

Dokaz. Precizan iskaz od (i) je da ako je $Z \subseteq \mathbb{A}^n$ algebarski skup, onda je $\varphi^{-1}(Z) = \overline{\varphi^{-1}(Z)} \cap U_i$. To vrijedi jer je φ homeomorfizam pa je zato $\varphi^{-1}(Z)$ relativno zatvoren u U_i. Pretpostavimo sada da je Z afina mnogostrukost. Ako je $\overline{Z} = \overline{\varphi^{-1}(Z)} = F_1 \cup F_2$ za zatvorene podskupove F_1, F_2, imamo $Z = \varphi(F_1 \cap U_i) \cup \varphi(F_2 \cap U_i)$. Z je ireducibilan, a $\varphi(F_j \cap U_i)$ su zatvoreni u $\mathbb{A}^n$ dakle neki od njih nije pravi podskup. Recimo da je to $j = 1$

ili $Z = \varphi(F_1 \cap U_i)$. Slijedi da je $\varphi^{-1}(Z) \subseteq F_1 \implies \overline{\varphi^{-1}(Z)} \subseteq F_1$ dakle F_1 nije pravi podskup od $\overline{\varphi^{-1}(Z)}$. Zaključujemo da je $\overline{Z} = \overline{\varphi^{-1}(Z)}$ ireducibilan.

Za (*ii*), neka je I homogeni ideal pridružen Y, te neka je $\{F_a\}_{a\in A}$ neki skup homogenih polinoma koji generiraju I. Pretpostavimo da je $Y \cap \mathbb{A}^n \neq \emptyset$. To znači da $x_i \notin I$ jer bi inače imali $Y = Z_I \subseteq H_i = \mathbb{P}^n \setminus \mathbb{A}^n$ što nije istina. Ako je neki od F_a djeljiv sa x_i ($\bar{k}[x_0, \ldots, x_n]$ je domena jedinstvene faktorizacije), npr. $F_a = x_i G_a$, tada vrijedi $x_i \in I$ ili $G_a \in I$ jer je ideal I prost. Zaključujemo $G_a \in I$. To znači da možemo iz svakog F_a izbaciti faktore x_i na način da $\{F_a\}_{a\in A}$ ostaje generirajući skup za ideal I. Dakle bez smanjenja općenitosti pretpostavimo da je $\{F_a\}_{a\in A}$ generirajući skup za ideal I takav da su svi F_a homogeni polinomi, nedjeljivi s x_i. Ako je f_a dehomogenizacija od F_a, uočimo da nedjeljivost sa x_i znači da je homogenizacija od f_a ponovno jednaka F_a! Ako je $J := (\{f_a\}_{a\in A})$ ideal u $\bar{k}[y_1, \ldots, y_n]$, ponovno imamo kao u dokazu Propozicije 1.2.7 da je $\varphi_i(Y \cap U_i) = Z_J$ i nadalje ideal $I(Y \cap U_i)$ je generiran sa $\{\beta(f_a)\}_{a\in A}) = \{F_a\}_{a\in A}$. Dakle $I(Y \cap U_i) = I(Y)$ što implicira da je $\overline{Y \cap U_i} = Y$. Provjerimo još da je afini algebarski skup $Y \cap \mathbb{A}^n$ uistinu mnogostrukost. Naime ako taj skup nije ireducibilan, onda postoje pravi relativno zatvoreni podskupovi F_1, F_2 od $Y \cap U_i$ takvi da $Y \cap U_i = F_1 \cup F_2$. Tada je $Y = \overline{Y \cap U_i} = \overline{F_1 \cup F_2} = \overline{F_1} \cup \overline{F_2}$. Nadalje $\overline{F_j} \cap U_i = F_j \neq Y \cap U_i$ za $j = 1, 2$ pa zaključujemo da su $\overline{F_1}, \overline{F_2}$ pravi podskupovi od Y što znači da Y nije ireducibilan. To je kontradikcija dakle $Y \cap \mathbb{A}^n$ mora biti ireducibilan pa je algebarska mnogostrukost.

Za (*iii*) uočimo da je homogeni polinom F definiran nad k ako i samo je dehomogenizacija f definirana nad k. Tvrdnja slijedi iz $I(\overline{Z}) = (\{\beta(f) : f \in I(Z)\})$ te $I(Y \cap \mathbb{A}^n) = (\{\alpha(F) : F \in I(Y)\})$. □

Ako je V projektivna mnogostrukost, uvijek možemo uzeti neku afinu kartu $\mathbb{A}^n \simeq U_i$ za koju $V \cap U_i \neq \emptyset$. Tako dobijemo afinu mnogostrukost koju samo označavamo sa $V \cap \mathbb{A}^n$. S obzirom na dokazanu tvrdnju (*ii*), iz $V \cap \mathbb{A}^n$ možemo rekonstruirati V tako što uzmemo projektivno zatvorenje i zato pri ovom postupku ne gubimo informacije o V. Sada ima smisla definirati neka svojstva od V koristeći već definirana svojstva za afine mnogostrukosti.

Definicija 1.2.11. Neka je V/k projektivna mnogostrukost i $\mathbb{A}^n \subseteq \mathbb{P}^n$ projektivna karta za koju $V \cap \mathbb{A}^n \neq \emptyset$. Definiramo *dimenziju* od V sa $\dim V := \dim(V \cap \mathbb{A}^n)$.

Funkcijsko polje od V je $k(V) := k(V \cap \mathbb{A}^n)$. Napomenimo da je ta definicija dobra jer su za različite izbore $\mathbb{A}^n \subseteq \mathbb{P}^n$, polja $k(V \cap \mathbb{A}^n)$ kanonski izomorfna.

Definicija 1.2.12. Neka je V projektivna mnogostrukost i $P \in V$. Odaberimo $\mathbb{A}^n \subseteq \mathbb{P}^n$ tako da je $P \in \mathbb{A}^n$. Kažemo da je V *nesingularna* (ili *glatka*) u P ako je $V \cap \mathbb{A}^n$ nesingularna u P.

Podsjetimo se da smo za svaki projektivni algebarski skup Z definirali pridruženi homogeni ideal $I(Z)$ kao ideal generiran sa homogenim polinomima f sa svojstvom da je f nula na cijelom Z. Ispostavlja se da možemo alternativno definirati $I(Z)$ kao ideal generiran

nekim afinim algebarskim skupom koristeći uobičajenu definiciju 1.1.4 koja ne spominje homogene polinome.

Definicija 1.2.13. Neka je $Y \subseteq \mathbb{P}^n$ neprazan projektivni algebarski skup. Definiramo *afini konus* nad Y kao skup

$$C(Y) := \left\{(a_0, \ldots, a_n) \in \mathbb{A}^{n+1} \setminus (0, \ldots, 0) \ : \ (a_0 : \ldots : a_n) \in Y\right\} \cup \{(0, \ldots, 0)\}.$$

Primjer 1.2.14. Za projektivnu mnogostrukost $V : X^2 + Y^2 = Z^2$, $V \subseteq \mathbb{P}^2(\bar{\mathbb{Q}})$ definiranu nad $\mathbb{Q}$, imamo da je $C(V) \subseteq \mathbb{A}^3(\bar{\mathbb{Q}})$ afina mnogostrukost

$$C(V) = \{(x, y, z) : x^2 + y^2 = z^2, x, y, z \in \bar{\mathbb{Q}}\}.$$

Nije teško dokazati da vrijedi sljedeća propozicija.

Propozicija 1.2.15. *Neka je $Y \subseteq \mathbb{P}^n$ neprazan projektivni algebarski skup. Afini konus $C(Y)$ je afini algebarski skup i njegov ideal $I(C(Y))$ (Definicija 1.1.4) u $\bar{k}[x_0, \ldots, x_n]$ je jednak homogenom idealu $I(Y)$ (Definicija 1.2.4).*

Primijetimo također da je Y projektivna mnogostrukost ako i samo ako je $C(Y)$ afina mnogostrukost. Naime oboje je ekvivalentno s time da je $I(Y) = I(C(Y))$ prosti ideal.

Napomena 1.2.16. Ako je V/k projektivna mnogostrukost, onda je funkcijsko polje $k(C(V))$ polje razlomaka od $k[x_0, \ldots, x_n]/I(V)$. Funkcijsko polje $k(V)$ se može alternativno opisati kao potpolje od $k(C(V))$ koje se sastoji od elemenata $F = [f]/[g]$, $[g] \neq 0$ gdje su $f, g \in k[x_0, \ldots, x_n]$ homogeni polinomi istog stupnja. Tu nam je $[\cdot] : k[x_0, \ldots, x_n] \to k[C(V)]$ kanonsko preslikavanje $[h] = h + I(V)$.

Nadalje koristeći koncept afinog konusa možemo iskazati *projektivni Nullstellensatz* kao posljedicu afinog.

Teorem 1.2.17 (Projektivni Nullstellensatz)**.** *Za svaki homogeni ideal $I \subseteq \bar{k}[x_0, \ldots, x_n]$ vrijedi:*

(i) $Z_I = \emptyset$ *ako i samo ako* $\sqrt{I} \supseteq (x_0, \ldots, x_n)$,

(ii) ako $Z_I \neq \emptyset$ *onda* $I(Z_I) = \sqrt{I}$.

Dokaz. Dokažimo prvo (*ii*). Ako je $Y := Z(I)$, onda iz Propozicije 1.2.15 imamo da je $I(Y) = I(C(Y))$. Uočimo da za $I = (0)$ tvrdnja trivijalno vrijedi pa možemo pretpostaviti da je $I \neq (0)$. Osim toga $Z_I \neq \emptyset$ povlači da je $I \neq \bar{k}[x_0, \ldots, x_n]$ što znači da je I pravi nenul ideal. Označimo sa Z_J^A afini algebarski skup u $\mathbb{A}^{n+1}$ pridružen idealu J od $\bar{k}[x_0, \ldots, x_n]$. Tvrdimo da je $Z_{I(Y)}^A = C(Y)$. Neka je $\{F_a\}_{a \in A}$ neki skup homogenih polinoma koji generiraju $I(Y)$. Svi F_a su tada homogeni stupnja ≥ 1, jer bi inače imali $F_a \in \bar{k}^\times = \bar{k}[x_0, \ldots, x_n]^\times$ za

neki $a \in A$ što bi značilo $I(Y) = \bar{k}[x_0, \ldots, x_n]^\times$, a pokazali smo da to nije slučaj. Uočimo da je

$$Z^A_{I(Y)} = \{P \in \mathbb{A}^{n+1} : F_a(P) = 0,\ \forall a \in A\}.$$

S obzirom da su svi F_a homogeni stupnja ≥ 1, vidimo da je $F_a((0, \ldots, 0)) = 0,\ \forall a \in A$, dakle $(0, \ldots, 0) \in Z^A_{I(Y)}$. Ako je sada $P = (a_0, \ldots, a_n) \in \mathbb{A}^{n+1}$, $P \neq (0, \ldots, 0)$, vidimo da je $F_a(P) = 0 \iff F_a(\lambda P) = 0,\ \forall \lambda \in \bar{k}$. Zaključujemo da je

$$P \in Z^A_{I(Y)} \iff \lambda P \in Z^A_{I(Y)},\ \forall \lambda \in \bar{k}^\times \iff (a_0 : \ldots : a_n) \in I(Y),$$

što dokazuje da je $Z^A_{I(Y)} = C(Y)$. Iz Hilbertovog Nullstellensatza sada je $I(Z^A_{I(Y)}) = \sqrt{I(Y)}$. S obzirom da je $I(Y) = I(C(Y)) = I(Z^A_{I(Y)})$, to povlači (*ii*).

Sada pređimo na (*i*). Jasno je da za $I = \bar{k}[x_0, \ldots, x_n]$ imamo da su obe tvrdnje (s lijeve i desne strane ekvivalencije) istinite i za $I = (0)$ imamo da obe tvrdnje nisu istinite. Dakle možemo pretpostaviti da je I pravi ne-nul ideal. Iz Nullstellensatza (afinog) sada znamo da $Z^A_I \neq \emptyset$ i $I(Z^A_I) = \sqrt{I}$. Ako postoji $P \in Z^A_I$ takva da $P = (a_0, \ldots, a_n) \neq (0, \ldots, 0)$, slično kao u prethodnom slučaju imamo da je onda $(a_0, \ldots, a_n) \in Z_I \subseteq \mathbb{P}^n$. Dakle $Z_I \neq \emptyset$. Nadalje postoji i takav da $a_i \neq 0$ što znači da $x_i \notin I(Z^A_I) = \sqrt{I}$ dakle $\sqrt{I} \not\supset (x_0, \ldots, x_n)$. Inače, ako takva P ne postoji, onda je $Z^A_I = \{(0, \ldots, 0)\}$. Tada još jače od $\supseteq$, vrijedi jednakost $\sqrt{I} = \mathfrak{m}_{(0,\ldots,0)} = (x_0, \ldots, x_n)$. □

Napomena 1.2.18. U ostatku rada ćemo se uglavnom fokusirati na glatke projektivne mnogostrukosti dimenzije 1, tj. *algebarske krivulje*. Uzmimo za primjer $V : Y^2Z = X^3 + 17Z^3$. S obzirom na Propoziciju 1.2.10, smisleno je zadati takve mnogostrukosti s nehomogenom jednadžbom ili u ovom primjeru $V : y^2 = x^3 + 17$. To će nam olakšati računanje, ali bitno je napomenuti da pritom podrazumijevamo da je V zapravo projektivno zatvorenje zadane afine mnogostrukosti.

1.3 Preslikavanja između mnogostrukosti

Morfizmi i racionalna preslikavanja afinih mnogostrukosti

Definicija 1.3.1. Neka su $X \subseteq \mathbb{A}^m$ i $Y \subseteq \mathbb{A}^n$ afine mnogostrukosti definirane nad k. *Morfizam* $\phi : X \to Y$ je preslikavanje $\phi(P) := (f_1(P), \ldots, f_n(P))$ gdje su $f_1, \ldots, f_n$ polinomi u $\bar{k}[X]$ takvi da je $\phi(P) \in Y,\ \forall P \in X$. Ako su $f_1, \ldots, f_n \in k[X]$, onda kažemo da je morfizam *f definiran nad k*.

Uočimo da je za morfizme $\phi : X \to Y$, $\psi : X \to Z$, njihova kompozicija $\psi \circ \phi : X \to Z$ također morfizam.

Definicija 1.3.2. Dvije afine mnogostrukosti X, Y su *izomorfne* ako postoji par morfizama $\phi : X \to Y$, $\psi : Y \to X$ takvih da $\psi \circ \phi = Id_X$ i $\phi \circ \psi = Id_Y$. Tada kažemo da su ϕ, ψ *izomorfizmi*.

Propozicija 1.3.3. *Morfizam afinih algebri $\phi : X \to Y$ inducira homomorfizam prstenova $\phi^* : \bar{k}[Y] \to \bar{k}[X]$ definiran s $\phi^*(g) = g \circ \phi$. Nadalje ako je $\psi : Y \to Z$ također homomorfizam prstenova, onda $(\psi \circ \phi)^* = \phi^* \circ \psi^*$.*

Propozicija 1.3.4. *Morfizam afinih mnogostrukosti $\phi : X \to Y$ je neprekidan.*

Dokaz. Neka je Z_J neki zatvoren podskup od Y, dovoljno je pokazati da je $\phi^{-1}(Z_J)$ algebarski skup. Neka je I ideal generiran sa $\{\phi^*(g) : g \in J\}$. Konačno

$$\begin{aligned} P \in Z_I &\iff \phi^*(g)(P) = 0,\ \forall g \in J \iff g(\phi(P)) = 0,\ \forall g \in J \\ &\iff \phi(P) \in Z_J \iff P \in \phi^{-1}(Z_J), \end{aligned}$$

dakle $Z_I = \phi^{-1}(Z_J)$ je uistinu algebarski skup. □

Uočimo da koordinatni prsteni $\bar{k}[X]$ imaju dodatnu strukturu da sadrže polje $\bar{k}$ i konačan skup generatora nad $\bar{k}$. Općenito, *afina algebra* R je integralna domena koja je ujedno i konačno generirana asocijativna $\bar{k}$-algebra za neko polje k. Vidimo da je $\bar{k}[X]$ afina algebra i inducirano preslikavanje ϕ^* je zapravo homomorfizam afinih algebri. Naime ϕ^* fiksira $\bar{k}$.

Teorem 1.3.5. *Kategorija afinih mnogostrukosti i kategorija asocijativnih algebri su kontravarijantno ekvivalentne.*

Dokaz. Označimo sa `Aff` kategoriju afinih mnogostrukosti definiranih nad $\bar{k}$ s morfizmima mnogostrukosti i sa `AsAlg` kategoriju asocijativnih algebri nad $\bar{k}$. Nećemo provjeriti sve detalje, ali ćemo pokazati kako definirati funktore $F : \texttt{Aff}^{op} \to \texttt{AsAlg}$ i $G : \texttt{AsAlg} \to \texttt{Aff}^{op}$ koji realiziraju ekvivalenciju kategorija. Prvo funktor F šalje objekte V u koordinatne prstene $\bar{k}[V]$ te morfizme afinih mnogostrukosti $\phi : X \to Y$ u morfizme afinih algebri $\phi^* : \bar{k}[Y] \to \bar{k}[X]$. Obratno, neka je sada R asocijativna algebra. Cilj nam je konstruirati $G(R)$. Neka su $r_1, \ldots, r_n$ neki generatori algebre R nad $\bar{k}$. Tada možemo definirati surjektivni homomorfizam asocijativnih algebri $\phi : \bar{k}[x_1, \ldots, x_n] \to R$ sa

$$\phi(f) := f(r_1, \ldots, r_n).$$

Neka je sada $I := \ker \phi$ te $V := Z_I$. Konačno definiramo $G(R) := V$. Uočimo i da je I prost zato što je R integralna domena. To znači da je V afina mnogostrukost, te iz Nullstellensatza slijedi $I = I(V)$. Imamo dakle

$$\bar{k}[V] = \bar{k}[x_1, \ldots, x_n]/I = \bar{k}[x_1, \ldots, x_n]/\ker \phi \cong R. \tag{1.1}$$

Neka je sada $\theta : R \to S$ neki homomorfizam afinih algebri. Ako sada kao i prethodno izaberemo surjektivne homomorfizme $\phi : \bar{k}[x_1, \ldots, x_n] \to R$ i $\psi : \bar{k}[y_1, \ldots, y_m] \to S$ te stavimo $I := \ker \phi$, $J := \ker \psi$, na temelju (1.1) imamo da $\theta : R \to S$ inducira homomorfizam

$$\tilde{\theta} : \bar{k}[x_1, \ldots, x_n]/I \to \bar{k}[y_1, \ldots, y_m]/J.$$

Za svaki x_i, neka je $f_i \in \bar{k}[y_1, \ldots, y_m]$ neki reprezent od $\tilde{\theta}(x_i)$. Tada možemo definirati morfizam $\eta : \mathbb{A}^m \mapsto \mathbb{A}^n$ sa

$$\nu(P) := (f_1(P), \ldots, f_n(P)).$$

Označimo $X := Z_I = G(R)$ i $Y := Z_J = G(S)$. Tada je restrikcija $\nu|_Y$ morfizam afinih mnogostrukosti $\nu|_Y : Y \to X$ i konačno definiramo $G(\theta) := \nu|_Y$. Uočimo još i da $G(\theta)$ ne ovisi o izboru reprezentanata f_i od $\tilde{\theta}(x_i)$. □

Definicija 1.3.6. Neka je X afina mnogostrukost. Funkcija $r \in \bar{k}(X)$ je *regularna* ili *definirana* u točki $P \in X$ ako postoji $g \in \bar{k}[X]$ takav da $gr \in \bar{k}[X]$ i $g(P) \neq 0$. Skup točaka u kojima je r regularna označavamo sa $\mathrm{dom}(r)$.

U biti $\mathrm{dom}(r)$ shvaćamo kao skup točaka u kojima možemo evaluirati r.

Propozicija 1.3.7. *Neka je X afina mnogostrukost i $r \in \bar{k}(X)$. Tada je* $\mathrm{dom}(r)$ *gusti otvoreni podskup od X.*

Dokaz. Primijetimo da je $I = \{g \in \bar{k}[X] : gr \in \bar{k}[X]\}$ ideal i štoviše $X \setminus \mathrm{dom}(r) = Z_I$ dakle $\mathrm{dom}(r)$ je otvoren skup. Nadalje $I \neq (0)$ pa iz Nullstellensatza $Z_I \neq X$, što znači da $\mathrm{dom}(r) \neq \emptyset$. Po Korolaru 1.1.8 neprazni otvoreni skupovi su gusti pa zaključujemo da je $\mathrm{dom}(r)$ gust u topologiji Zariskog. □

Propozicija 1.3.8. *Neka je $r \in \bar{k}(X)$. Tada je $r \in \bar{k}[X]$ ako i samo ako je* $\mathrm{dom}(r) = X$.

Dokaz. Za $r \in \bar{k}[X]$ očito je $\mathrm{dom}(r) = X$. S druge strane ako je $\mathrm{dom}(r) = X$, imamo da je $Z_I = \emptyset$ za ideal $I = \{g \in \bar{k}[X] : gr \in \bar{k}[X]\}$. Iz Korolara 1.1.14 slijedi da je $I = \bar{k}[X]$. Dakle $1 \in I \implies 1 \cdot r = r \in \bar{k}[x]$. □

Definicija 1.3.9. Neka su $X \subseteq \mathbb{A}^n$ i $Y \subseteq \mathbb{A}^m$ afine mnogostrukosti. Kažemo da je m-torka $(\phi_1, \ldots, \phi_m)$ funkcija $\phi_i \in \bar{K}(X)$ *regularna* u $P \in X$ ako su sve ϕ_i regularne u P. *Racionalno preslikavanje* $\phi : X \to Y$ je m-torka $(\phi_1, \ldots, \phi_n)$ funkcija $\phi_i \in \bar{K}(X)$ takvih da za sve P u kojima je ϕ regularno, vrijedi $\phi(P) := (\phi_1(P), \ldots, \phi_n(P)) \in Y$. Ako je racionalno preslikavanje ϕ regularno u svim točkama $P \in X$, tada kažemo da je ϕ *regularno*.

Također definiramo *domenu* racionalnog preslikavanja kao skup svih točaka P u kojima je ϕ regularno, ili ekvivalentno $\mathrm{dom}(\phi) := \mathrm{dom}(\phi_1) \cap \ldots \cap \mathrm{dom}(\phi_n)$.

Teorem 1.3.10. *Racionalno preslikavanje afinih mnogostrukosti je morfizam ako i samo ako je regularno.*

Dokaz. Iz definicije vidimo da je svaki morfizam ujedno i regularno racionalno preslikavanje. Obratno ako je $\phi = (\phi_1, \ldots, \phi_n)$ racionlano preslikavanje koje je regularno u svim točkama, tada su sve funkcije $\phi_i \in \bar{K}(X)$ također regularne u svim točkama. Iz Propozicije 1.3.8 slijedi da je $\phi_i \in \bar{K}[X]$ za sve i. Dakle ϕ je morfizam. □

Htjeli bismo definirati kategoriju u kojoj imamo racionalna preslikavanja ujestu morfizama afinih mnogostrukosti. Problem je što ne možemo nužno komponirati racionalna preslikavanja.

Primjer 1.3.11. Neka su $X = Y = Z = \mathbb{A}^2$ afine mnogostrukosti, te neka su $\phi_1 : X \ni (x_1, x_2) \mapsto (1/x_1, 0) \in Y$ i $\phi_2 : Y \ni (x_1, x_2) \mapsto (0, 1/x_2) \in Z$ racionalna preslikavanja. Vidimo da su slika od ϕ_1 i domena od ϕ_2 disjunktne pa ih nema smisla komponirati.

Propozicija 1.3.12. *Racionalno preslikavanje afinih mnogostrukosti $\phi : X \to Y$ je neprekidno kao preslikavanje iz topološkog prostora* $\mathrm{dom}(\phi)$ *s induciranom topologijom u topološki prostor Y.*

Dokaz. Skiciramo dokaz. Svaka točka P u $\mathrm{dom}\,\phi$ ima otvorenu okolinu U_P na kojoj sve komponente ϕ_i imaju reprezentaciju $\phi_i = f_i/g_i$ takvu da g_i nije 0 na okolini. Ako je F zatvoren u Y, može se pokazati da je $\phi^{-1}(F) \cap U_P = Z_{P,F} \cap U_P$ za neki $Z_{P,F}$ koji je zatvoren u X (zadamo ga kao skup nultočaka nekih polinoma koje biramo na temelju ϕ i F). $\{U_P\}$ je otvoren pokrivač od $\mathrm{dom}\,\phi$, sve zajedno to implicira da je $\phi^{-1}(F) \subseteq \mathrm{dom}\,\phi$ relativno zatvoren. Tada imamo da je ϕ neprekidno. □

Propozicija 1.3.13. *Neka je $\phi : X \to Y$ racionalno preslikavanje afinih mnogostrukosti. Tada je $\overline{\mathrm{Im}\,\phi}$ afina mnogostrukost.*

Dokaz. Prvo primijetimo da je $\mathrm{dom}\,\phi$ ireducibilan skup. Naime ako je $\mathrm{dom}\,\phi = F_1 \cup F_2$ za relativno zatvorene F_1, F_2 imamo da je $X = \overline{\mathrm{dom}\,\phi} = \overline{F_1} \cup \overline{F_2}$. Dakle neki od $\overline{F_j}$ nije pravi podskup, recimo $\overline{F_1} = X$. Tada $F_1 = \overline{F_1} \cap \mathrm{dom}\,\phi = \mathrm{dom}\,\phi$. Dakle $\mathrm{dom}\,\phi$ nije unija dva prava zatvorena skupa. Općenito je slika ireducibilnog skupa preko neprekidnog preslikavanja također ireducibilna pa zaključujemo da je $\mathrm{Im}\,\phi$ ireducibilan. Također, zatvorenje ireducibilnog skupa je ireducibilno pa slijedi da je $\overline{\mathrm{Im}\,\phi}$ ireducibilan. □

Definicija 1.3.14. Racionalno preslikavanje $\phi : X \to Y$ je *dominantno* ako mu je slika gusta u Y, ili ekvivalentno ako vrijedi $\overline{\mathrm{Im}\,\phi} = \overline{\phi(\mathrm{dom}(\phi))} = Y$.

Propozicija 1.3.15. *Neka su X, Y, Z afine mnogostrukosti i $\phi : X \to Y$, $\psi : Y \to Z$ racionalna preslikavanja. Tada je $\psi \circ \phi : X \to Z$ dobro definirano racionalno preslikavanje koje je također dominantno.*

Dokaz. Pokažimo da je kompozicija dominantna. Slika $\operatorname{Im}\phi$ je gusta u Y te je $\operatorname{dom}(\psi)$ otvoren, dakle $\operatorname{Im}\phi \cap \operatorname{dom}(\psi)$ je gust u $\operatorname{dom}(\psi)$. Imamo da je ψ neprekidna pa dobijemo da je $\psi(\operatorname{Im}\phi \cap \operatorname{dom}(\psi))$ gust u $\operatorname{Im}\psi$, koji je opet gust u Z. To dokazuje da je $\operatorname{Im}\psi \circ \phi$ gusta u Z. Što se tiče domene, imamo da $\operatorname{dom}(\psi \circ \phi)$ barem sadrži $\phi^{-1}(\operatorname{dom}(\psi))$ što je otvoren i gust podskup od X. □

Uočimo da su identitete 1_X na afinim mnogostrukostima X također dominantna racionalna preslikavanja. Sve to enkapsuliramo sa sljedećim korolarom.

Korolar 1.3.16. *Afine mnogostrukosti zajedno s dominantnim racionalnim preslikavanjima čine kategoriju.*

Sad možemo iskazati analog Teorema 1.3.5 koristeći dominantna racionalna preslikavanja umjesto morfizama i funkcijska polja $\bar{k}(X)$ umjesto koordinatnih prstenova. Općenito, definiramo *funkcijsko polje* kao konačno generirano proširenje od $\bar{k}$.

Propozicija 1.3.17. *Dominantno racionalno preslikavanje $\phi : X \to Y$ inducira homomorfizam funkcijskih polja $\phi^* : \bar{k}(Y) \to \bar{k}$ definiran s $\phi^*(r) = r \circ \phi$. Nadalje ako je $\psi : Y \to Z$ također dominantno racionalno preslikavanje, onda $(\psi \circ \phi)^* = \phi^* \circ \psi^*$.*

Teorem 1.3.18. *Kategorija afinih mnogostrukosti s dominantnim racionalnim preslikavanjima i kategorija općenitih funkcijskih polja su kontravarijantno ekvivalentne.*

Dokaz. Postupamo slično kao u dokazu Teorema 1.3.5. Jedan funktor je očito zadan sa $V \mapsto \bar{k}(V)$, tj. mnogostrukosti pridružuje njeno funkcijsko polje. Drugi konstruiramo kao u ekvialenciji za asocijativne algebre. Naime neka su $r_1, \ldots, r_n$ generatori od funkcijskog polja F nad $\bar{k}$. Neka je R asocijativna algebra nad $\bar{k}$ koja je sadržana u F i generirana sa $r_1, \ldots, r_n$. To nas navodi da prirodno definiramo homomorfizam asocijativnih algebri $\phi : \bar{k}[x_1, \ldots, x_n] \mapsto R$ koji djeluje kao evaluacija u $(r_1, \ldots, r_n)$. Sad je $\bar{k}[x_, \ldots, x_n]/I \cong R$ za prosti ideal $I = \ker\phi$. Kao i prije definiramo $V := Z_I$ i tada imamo da je $K[V] \cong R$. Jednostavno funktorom pridružimo polju F afinu algebarsku mnogostrukost V, i tada imamo da je $K(V)$ izomorfno s F jer je F polje razlomaka od R. Slično, ako imamo homomorfizam funkcijskih polja $\theta : F_1 \to F_2$, imamo inducirani homomorfizam $\tilde{\theta} : k(X_1) \to k(X_2)$ gdje su X_1, X_2 afine mnogostrukosti pridružene funkcijskim poljima F_1, F_2. Za svaki x_j uzmemo neke funkcije f_j, g_j takve da je $\tilde{\theta}(x_j) = [f_j]/[g_j]$. Sada

$$\nu(P) := ((f_1/g_1)(P), \ldots, (f_n/g_n)(P)) .$$

definira racionalno preslikavanje. Za dominantnost dovoljno je provjeriti da je 0 jedini element iz $\bar{k}[X_1]$ koji iščezava na $\operatorname{Im}\nu$. □

Definicija 1.3.19. 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 $P \in \mathrm{dom}(\phi \circ \psi)$ i $(\psi \circ \phi)(P) = P$ za sve $P \in \mathrm{dom}(\psi \circ \phi)$.

Korolar 1.3.20. *Dvije afine mnogostrukosti su biracionalno ekvivalentne ako i samo ako su im funkcijska polja izomorfna.*

Morfizmi i racionalna preslikavanja projektivnih mnogostrukosti

Cilj nam je pojmove uvedene u prethodnoj sekciji iskazati u kontekstu projektivnih mnogostrukosti.

Definicija 1.3.21. Neka je X projektivna mnogostrukost i neka je $P \in X$. Odaberimo $\mathbb{A}^n \subseteq \mathbb{P}^n$ tako da je $P \in \mathbb{A}^n$. Tada je $X \cap \mathbb{A}^n$ afina mnogostrukost i X je njeno projektivno zatvorenje. Po definiciji imamo da je $\bar{k}(X) \cong \bar{k}(X \cap \mathbb{A}^n)$. Kažemo da je $r \in \bar{k}(X)$ *regularna* u P ako je korespondirajuća funkcija $\tilde{r} \in \bar{k}(X \cap \mathbb{A}^n)$ regularna u P. Skup regularnih točaka od r ponovno označavamo sa $\mathrm{dom}(r)$.

Primijetimo odmah da je $\mathrm{dom}(r)$ otvoren u X jer je za svaku afinu kopiju $\mathbb{A}^n$ u $\mathbb{P}^n$ takvu da $\mathbb{A}^n \cap X \neq \emptyset$, skup $\mathrm{dom}(r) \cap \mathbb{A}^n = \mathrm{dom}(\tilde{r})$ relativno otvoren u $X \cap \mathbb{A}^n$, a X ima otvoreni pokrivač koji se sastoji od afinih kopija.

Napomena 1.3.22. Podsjetimo se da $\bar{k}(X)$ također možemo realizirati kao potpolje od $\bar{k}(C(X))$ ($C(X)$ je afini konus nad X, iz Definicije 1.2.13) koje se sastoji do funkcija oblika $[f]/[g]$ gdje su $f, g \in \bar{k}[x_0, \ldots, x_n]$ homogeni polinomi istog stupnja, a $[f], [g]$ su njihove pripadajuće klase u $\bar{k}[x_0, \ldots, x_n]/I(X)$. Za $r = [f]/[g] \in \bar{k}(X)$ funkcija $\hat{r} := f/g \in \bar{k}(x_0, \ldots, x_n)$ je neki njen *reprezent*. Tada je r regularna u P ako i samo ako ima neki reprezent $\hat{r}$ koji je definiran u P, u smislu da nazivnik nije 0.

Napomena 1.3.23. Uočimo i da ako je $r \in \bar{k}(X)$ regularna u P, tada ima smisla evaluirati r u P. Naime definiramo $r(P) := f(a_0, \ldots, a_n)/g(a_0, \ldots, a_n)$ gdje je $\hat{r}$ reprezent od r (takav da $g(P) \neq 0$) i $(a_0 : \ldots : a_n)$ reprezent od P. Ova definicija je dobra jer ne ovisi o izboru konrektnih reprezenata za r i za P.

Definicija 1.3.24. Neka su $X \subseteq \mathbb{P}^n$ i $Y \subseteq \mathbb{P}^m$ projektivne mnogostrukosti. Za $(m+1)$-torke funkcija $(\phi_0, \ldots, \phi_m)$, $\phi_i \in \bar{k}(X)$ definiramo relaciju ekvivalencije sa

$$(\phi_0, \ldots, \phi_m) \sim (\psi_0, \ldots, \psi_m) \iff \exists \lambda \in \bar{k}(X)^\times : \phi_i = \lambda \psi_i \text{ za } i = 0, \ldots, m$$

Klasu kojoj $(\phi_0, \ldots, \phi_m)$ pripada tada označavamo sa $(\phi_0 : \ldots : \phi_m)$.

Kažemo da je klasa $(\phi_0 : \ldots : \phi_m)$, $\phi_i \in \bar{k}(X)$ *regularna* u $P \in X$ ako postoji $g \in \bar{k}(X)$ takva da

(i) svaka $g\phi_i$ je regularna u P,

(ii) postoji i za koji $(g\phi_i)(P) \neq 0$.

Racionalno preslikavanje $\phi : X \to Y$ je klasa ekvivalencije $(\phi_0 : \ldots : \phi_m)$, $\phi_i \in \bar{k}(X)$ takva da je $\phi(P) := (\phi_0(P) : \ldots : \phi_m(P)) \in Y$ za sve točke P u kojima je ϕ regularno. Skup točaka od X u kojima je ϕ regularno opet čini otvoren podskup i označavamo ga sa $\mathrm{dom}(\phi)$.

Napomena 1.3.25. Alternativno možemo prikazati racionalno preslikavanje $\phi : X \to Y$ kao $(m+1)$-torku homogenih polinoma iz $\bar{k}[x_0, \ldots, x_m]$ koji su svi istog stupnja i ne pripadaju svi u $I(X)$. To jednostavno postignemo tako da u racionalnom preslikavanju $\phi = (\phi_0 : \ldots : \phi_m)$ pomnožimo svaku komponentu ϕ_i nekom funkcijom koja svim ϕ_i "krati nazivnike".

Definicija 1.3.26. Racionalno preslikavanje projektivnih mnogostrukosti $\phi : X \to Y$ koje je regularno u svim točkama od X se naziva *morfizam*. Racionalno preslikavanje je *dominantno* ako mu je slika gusta u kodomeni.

Prisjetimo se da i za afine mnogostrukosti po Teoremu 1.3.10 također vrijedi da je racionalno preslikavanje morfizam ako i samo ako je regularno. Racionalno preslikavanje projektivnih mnogostrukosti $\phi : X \to Y$ ponovno na očit način inducira homomorfizam funkcijskih polja $\phi^* : \bar{k}(Y) \to \bar{k}(X)$. Kao i za afine mnogostrukosti imamo analog Teorema 1.3.18. Dokaz nije bitno različit od afinog.

Teorem 1.3.27. *Kategorija projektivnih mnogostrukosti s dominantnim racionalnim preslikavanjima i kategorija općenitih funkcijskih polja su kontravarijantno ekvivalentne.*

Primjer 1.3.28. Neka je $V/\mathbb{Q}$ je projektivna mnogostrukost definirana sa

$$V : X^2 + Y^2 = Z^2 \tag{1.2}$$

Neka je $\phi : V \to \mathbb{P}^1$ racionalno preslikavanje $\left(\frac{X+Z}{Y} : 1\right)$ dakle

$$\phi((X : Y : Z)) = \left(\frac{X+Z}{Y} : 1\right)$$

za $P = (X : Y : Z) \in \mathrm{dom}(\phi)$. Očito je ϕ regularno u svim točkama gdje $Y \neq 0$. Ako uvrstimo $Y = 0$ u jednadžbu (1.2) dobijemo da je ϕ može jedino biti neregularna u $(1 : 0 : 1)$ i $(1 : 0 : -1)$. Uočimo sada da je

$$\left(\frac{X+Z}{Y} : 1\right) = \left(\frac{X+Z}{Y} \cdot \frac{Y}{X} : \frac{Y}{X}\right) = \left(\frac{X+Z}{X} : \frac{Y}{X}\right).$$

Dakle $\phi((1 : 0 : 1)) = (2 : 0) = (1 : 0)$ je dobro definirano. Uočimo također

$$\left(\frac{X+Z}{Y} : 1\right) = \left(\frac{X^2 - Z^2}{Y(X-Z)} : 1\right) = \left(\frac{-Y^2}{Y(X-Z)} : 1\right) = \left(\frac{-Y}{X-Z} : 1\right).$$

Dakle $\phi((1 : 0 : -1)) = (0 : 1)$. Zaključujemo da je ϕ regularno svugdje što znači da je morfizam projektivnih mnogostrukosti. Lako se provjeri i da je preslikavanje

$$\psi : \mathbb{P}^1 \to V, \quad \psi = \left(\frac{S^2 - T^2}{S^2 + T^2} : \frac{2ST}{S^2 + T^2}, 1 \right)$$

također morfizam koji je i inverz od ϕ. Dakle V i $\mathbb{P}^1$ su izomorfne.

Primjer 1.3.29. Racionalno preslikavanje $\phi : \mathbb{P}^2 \to \mathbb{P}^2$ zadano sa $\phi = (X^2 : XY : Z^2)$ je regularno svugdje osim u $(0 : 1 : 0)$.

Definicija 1.3.30. Neka su X/k i Y/k projektivne mnogostrukosti definirane nad k. Racionalno preslikavanje $\phi : X \to Y$ između projektivnih/afinih mnogostrukosti je *definirano nad k* ako su komponente $\phi_i \in k(X)$ (u projektivnom slučaju, precizno je reći da postoji reprezent $(\phi_0 : \ldots : \phi_m)$ sa $\phi_i \in k(X)$ za sve i).

Projektivne/afine mnogostrukosti definirane nad k zajedno sa dominantnim racionalnim preslikavanjima definiranima nad k također čine kategoriju.

Funkcijsko polje definirano nad k je konačno generirano proširenje $F \supseteq k$ takvo da je k algebarski zatvoreno u F, pišemo F/k. Slično kao i ostale navedene ekvivalencije kategorija, možemo dokazati.

Teorem 1.3.31. *Kategorija projektivnih/afinih mnogostrukosti definiranih nad k s dominantnim racionalnim preslikavanjima definiranima nad k i kategorija općenitih funkcijskih polja definiranih nad k su kontravarijantno ekvivalentne.*

Podsjetimo se da sa k označavamo savršeno polje.

Poglavlje 2

Algebarske krivulje

2.1 Funkcijska polja

Definicija 2.1.1. *Algebarska krivulja* je 1-dimenzionalna algebarska mnogostrukost.

Napomena 2.1.2. U budućnosti ćemo pisati samo *krivulja* pod čim podrazumijevamo glatku projektivnu algebarsku krivulju.

Kao što smo vidjeli u prethodnoj sekciji, prirodno je proučavati mnogostrukosti preko njihovih funkcijskih polja. Za krivulju C/k, $k(C)$ je polje stupnja transcendentnosti 1 koje je konačno generirano nad k. Da bi općenito opisali takva polja uvodimo sljedeću definiciju.

Definicija 2.1.3. *Funkcijsko polje F/k* je konačno generirano proširenje od k stupnja transcendentnosti 1, takvo da je k algebarski zatvoreno u F.

Napomena 2.1.4. Uočimo da nam Teorem 1.3.31 zapravo daje ekvivalenciju kategorije algebarskih krivulja s dominantnim racionalnim preslikavanjima i kategorije funkcijskih polja iz Definicije 2.1.3. Naime ekvivalenciju mnogostrukosti i općenitih funkcijskih polja možemo restringirati na mnogstrukosti dimenzije 1 i funkcijska polja stupnja transcendentnosti 1.

Problem u uspostavljenoj ekvivalenciji kategorija je što te algebarske krivulje ne moraju biti glatke. Ispostavlja se da za svaku algebarsku krivulju C postoji **desingularizacija** $\tilde{C}$ tj. glatka algebarska krivulja koja je biracionalno ekvivalentna s C. Postojanje desingularizacije povlači da je kategorija algebarskih krivulja ekvivalentna s kategorijom glatkih algebarskih krivulja. To nam konačno daje sljedeći teorem.

Teorem 2.1.5. *Kategorija krivulja s dominantnim racionalnim preslikavanjima je kontravarijantno ekvivalentna s kategorijom funkcijskih polja (Definicija 2.1.3).*

Napomenimo da gornji teorem vrijedi za krivulje i funkcijska polja definirana nad poljem k, koje ne mora biti algebraski zatvoreno. Za proizvoljno funkcijsko polje F/k, pridruženu krivulju ćemo označavati sa X_F. Dakle vrijedi $k(X_F) \cong F$.

Sad nam je cilj iskazati neka osnovna svojstva funkcijskih polja.

Definicija 2.1.6. *Prsten valuacije* funkcijskog polja F/k je prsten $\mathcal{O} \subseteq F$ sa svojstvima:

(1) $k \subsetneq \mathcal{O} \subsetneq F$ i

(2) za sve $r \in F$ vrijedi $r \in F$ ili $r^{-1} \in F$.

Primjer 2.1.7. Neka je p ireduciblni normirani polinom u $k[x]$. Tada je skup

$$\mathcal{O}_p := \{f/g : f, g \in k[x], p \nmid g\}$$

prsten valuacije u funkcijskom polju $k(x)/k$. Štoviše za neki drugi ireduciblni normirani polinom q imamo $\mathcal{O}_p \neq \mathcal{O}_q$.

Propozicija 2.1.8. *Neka je $\mathcal{O}$ prsten valuacije u funkcijskom polju F/k. Vrijedi*

(i) $\mathcal{O}$ je lokalni prsten, tj. ima jedinstven maksimalni ideal P.

(ii) Neka je $r \in F^\times$. Tada $r \in P \iff r^{-1} \notin \mathcal{O}$.

Dokaz. Definirajmo $P := \mathcal{O} \setminus \mathcal{O}^\times$. Tvrdimo da je P pravi ideal od $\mathcal{O}$. Iz definicije valuacijskog prstena jasno je da $1 \in \mathcal{O}$, dakle $1 \notin P$ što znači $P \neq \mathcal{O}$. Također vrijedi $P \neq (0)$ jer inače, ako $P = (0)$, to znači da su svi nenul elementi u $\mathcal{O}$ invertibilni, što čini $\mathcal{O}$ poljem. Tada je $F/\mathcal{O}$ proširenje polja i znamo da postoji element $\alpha \in F \setminus \mathcal{O}$. Očito je tada $\alpha \notin \mathcal{O}$ i $\alpha^{-1} \notin \mathcal{O}$ što je kontradikcija. Dakle $P \neq (0), \mathcal{O}$. Pokažimo sada da je P zatvoren na zbrajanje. Neka su $\alpha, \beta \in \mathcal{O} \setminus \mathcal{O}^\times$. Ako je $\alpha = 0$ ili $\beta = 0$, očito je $\alpha + \beta \in P$, dakle možemo pretpostaviti da $\alpha \neq 0$ i $\beta \neq 0$. Sad $\alpha, \beta \notin \mathcal{O}^\times \implies \alpha^{-1}, \beta^{-1} \notin \mathcal{O}$. Dovoljno je pokazati $\alpha + \beta \notin \mathcal{O}^\times$. Pretpostavimo suprotno, tj. $\alpha + \beta \in \mathcal{O}^\times \implies 1/(\alpha + \beta) \in \mathcal{O}$. Imamo

$$\frac{1}{\alpha} = \left(\frac{\beta}{\alpha} + 1\right) \frac{1}{\alpha + \beta}.$$

S obzirom da je $1/(\alpha + \beta) \in \mathcal{O}$ i $1/\alpha \notin \mathcal{O}$, zaključujemo $\beta/\alpha + 1 \notin \mathcal{O} \implies \beta/\alpha \notin \mathcal{O}$. Analogno dobijemo da je $\alpha/\beta \notin \mathcal{O}$ što je kontradikcija jer barem jedan od $\alpha/\beta, \beta/\alpha$ mora biti u $\mathcal{O}$. Pokažimo sada da je P zatvoren na množenje elementima iz $\mathcal{O}$. Neka je $\alpha \in \mathcal{O}$ i $\beta \in P$. Dovoljno je pokazati da $\alpha\beta \notin \mathcal{O}^\times$, stoga pretpostavimo suprotno da $(\alpha\beta)^{-1}$ postoji i sadržan je u $\mathcal{O}$. Množenjem s α dobijemo $\beta^{-1} \in \mathcal{O} \implies \beta \in \mathcal{O}^\times$ što je kontradikcija jer $\beta \in P \implies \beta \notin \mathcal{O}^\times$. To dokazuje da je P pravi, nenul ideal u $\mathcal{O}$.

Nadalje svaki pravi ideal I u $\mathcal{O}$ je sadržan u komplementu od $\mathcal{O}^\times$ (inače ne bi bio pravi) pa stoga $I \subseteq P$. Iz toga zaključujemo da je P jedinstveni maksimalni ideal.

Za (*ii*) uočimo za smjer "⇒" da ako je $r \in P$ i $r^{-1} \in \mathcal{O}$ imali bi $1 = r^{-1} \cdot r \in P$ što bi značilo da P nije pravi ideal, kontradikcija. Obratno ako $r^{-1} \notin \mathcal{O}$, tada je $r \in \mathcal{O}$ jer barem jedan od r^{-1}, r mora biti sadržan u valuacijskom prstenu. Očito i $r \notin \mathcal{O}^\times$ dakle $r \in P$. □

Teorem 2.1.9. *Neka je $\mathcal{O}$ prsten valuacije u funkcijskom polju F/k i neka je P njegov jedinstveni maksimalni ideal. Tada vrijedi:*

(i) P je glavni ideal.

(ii) Ako je $P = t\mathcal{O}$, tada svaki $r \in F^\times$ ima jedinstvenu reprezentaciju oblika $r = t^n u$ za neki $n \in \mathbb{Z}$ i $u \in \mathcal{O}^\times$.

(iii) $\mathcal{O}$ je domena glavnih ideala. Konkretno, ako je $P = t\mathcal{O}$, svi pravi nenul ideali su oblika $I = t^n\mathcal{O}$ za neki $n \in \mathbb{N}$.

Definicija 2.1.10. Prsten koji je ujedno lokalni prsten i domena glavnih ideala se naziva *prsten diskretne valuacije*.

Dakle Teorem 2.1.9 zapravo tvrdi da je svaki prsten valuacije od F/k ujedno i prsten diskretne valuacije. Za dokaz nam treba sljedeća lema.

Lema 2.1.11. *Neka je $\mathcal{O}$ prsten valuacije funkcijskog polja F/k i neka je P njegov maksimalni ideal, te $0 \neq x \in P$. Neka su $x_1 \ldots, x_n \in P$ takvi da $x_1 = x$ i $x_i \in x_{i+1}P$ za $i = 1, \ldots, n-1$. Tada*

$$n \leq [F : K(x)] < \infty.$$

Dokaz. Općenito vrijedi da ako je x transcendentan nad k, onda je $[F : k(x)] < \infty$. U ovom slučaju x mora biti transcendentan nad k jer bi inače vrijedilo $x \in k^\times \subseteq \mathcal{O}^\times$ što je nemoguće jer bi to značilo da $P = \mathcal{O}$, a imamo da je P pravi ideal.

Dovoljno je dakle dokazati da su $x_1, \ldots, x_n$ linearno nezavisni nad $k(x)$. Pretpostavimo suprotno da je $\sum_{i=1}^n f_i(x)x_i = 0$ za neke $f_i \in k(x)$ koji nisu svi 0. Možemo pretpostaviti da su f_i elementi od $k[x]$ (množimo sve s nazivnikom) i da nisu svi djeljivi s x. Primijetimo i da su $f_i(x) \in \mathcal{O}$ jer je $x = x_1 \in \mathcal{O}$ te $k \subseteq \mathcal{O}$. Neka je j najveći indeks takav da $f_j(x)$ nije djeljiv s x. Dakle imamo $f_i(0) = 0$ za sve $i > j$. Sada je $-f_j(x) = \sum_{i \neq j} f_i(x)x_i$. Ako zapišemo $f_i(x) = xg_i(x)$ za $i > j$ gdje $g_i \in k[x]$. Dobijemo

$$-f_j(x) = \sum_{i<j} f_i(x)\frac{x_i}{x_j} + \sum_{i>j} g_i(x)x_i\frac{x_1}{x_j}. \tag{2.1}$$

Uočimo da iz uvjeta $x_i \in x_{i+1}P$ slijedi da je zapravo $x_s \in x_tP$ kad god $s < t$. U (2.1) zato imamo da je $x_i/x_j \in P$ za $i < j$ i $x_1/x_j \in P$ za $i > j$. Zaključujemo da je desna strana jednadžbe sadržana u P što povlači da je $f_j(x) \in P$. Sada iz $x \in P$ slijedi da je $f_j(0) \in P$. To je kontradikcija jer $f_j(0) \in k^\times \subseteq \mathcal{O}^\times$. □

Dokaz Teorema 2.1.9. (*i*) Pretpostavimo da P nije glavni ideal i odaberimo element $x_1 \in P$, $x_1 \neq 0$. Tada $x_1\mathcal{O} \subsetneq P \implies \exists x_2 \in P \setminus x_1\mathcal{O}$. Vrijedi dakle $x_2x_1^{-1} \notin \mathcal{O}$. Iz Propozicije 2.1.8 zaključujemo $x_2^{-1}x_1 \in P \implies x_1 \in x_2P$. Nastavljajući postupak konstruiramo beskonačan niz (x_i) takav da $x_i \in x_{i+1} \in P$ za sve i. Postojanje takvog niza je kontradikcija s Lemom 2.1.11.

(*ii*) Jedinstvenost reprezentacije je očita pa nam preostaje dokazati postojanje. Kako je r ili r^{-1} u $\mathcal{O}$ možemo pretpostaviti da je $r \in \mathcal{O}$. Ako je $r \in \mathcal{O}^\times$ tada $r = t^0r$. Preostaje slučaj kada $r \in P$. Tada postoji maksimalan $m \geq 1$ takav da $r \in t^m\mathcal{O}$, zato što je duljina niza

$$x_1 = r,\ x_2 = t^{m-1},\ x_3 = t^{m-2},\ \ldots,\ x_m = t$$

ograničena Lemom 2.1.11. Za taj maksimalan m imamo $r = t^mu$ gdje $u \in \mathcal{O}$. Iz $r \notin t^{m+1}\mathcal{O}$ slijedi da $u \notin P = t\mathcal{O}$. Dakle $u \in \mathcal{O}^\times = \mathcal{O} \setminus P$.

(*iii*) Ako je I pravi nenul ideal u $\mathcal{O}$, može se pokazati da je $I = t^n\mathcal{O}$, gdje je $n \in \mathbb{N}$ najmanji prirodan broj takav da $t^n \in I$.

□

Definicija 2.1.12. *Mjesto* P u funkcijskom polju F/k je maksimalni ideal nekog prstena valuacije $\mathcal{O}$ od F/k. Svaki element $t \in P$ koji generira P se naziva *uniformizator* ili *uniformizirajući parametar* od P. Definiramo $\mathbb{P}_F := \{P : P \text{ je mjesto od } F/k\}$.

Primijetimo da svaki prsten valuacije $\mathcal{O}$ jedinstveno zadaje mjesto P kao njegov maksimalni ideal. Obratno, iz P možemo rekonstruirati $\mathcal{O}$ sa $\mathcal{O} = \{r \in F : r^{-1} \notin P\}$ (slijedi iz Propozicije 2.1.8). Dakle postoji 1-na-1 korespondencija između mjesta i prstena valuacije u funkcijskom polju. Zato uvodimo oznaku $\mathcal{O}_P := \mathcal{O}$ i nazivamo to *prsten valuacije mjesta* P.

Definicija 2.1.13. *Diskretna valuacija* od F/k je funkcija $v : F \to \mathbb{Z} \cup \{\infty\}$ sa sljedećim svojstvima:

(1) $v(x) = \infty \iff x = 0$.

(2) $v(xy) = v(x) + v(y)$ za sve $x, y \in F$.

(3) $v(x + y) \geq \min\{v(x), v(y)\}$ za sve $x, y \in F$.

(4) $\exists r \in F$ takav da $v(r) = 1$.

(5) $v(a) = 0$ za sve $a \in k^\times$.

Lema 2.1.14. *Neka je v diskretna valuacija od F/k i $v(x) \neq v(y)$ za neke $x, y \in F$. Tada $v(x + y) = \min\{v(x), v(y)\}$.*

Definicija 2.1.15. Mjestu $P \in \mathbb{P}_F$ pridružimo funkciju $v_P : F \to \mathbb{Z} \cup \infty$ na sljedeči način. Odaberemo neki uniformizator t_P. Tada svaki element $r \in F^\times$ ima jedinstvenu reprezentaciju $r = t_P^n u$ sa $u \in \mathcal{O}_P^\times$ i $n \in \mathbb{Z}$. Definiramo $v_P(r) := n$ i $v_P(0) := \infty$.

Napomenimo da definicija od v_P ne ovisi o izboru uniformizatora t_P nego samo o P.

Propozicija 2.1.16. *Neka je F/k funkcijsko polje.*

(i) Za mjesto $P \in \mathbb{P}_F$, gore definirana v_P je diskretna valuacija. Nadalje imamo

$$\begin{aligned} \mathcal{O}_P &= \{r \in F : v_P(r) \geq 0\}, \\ \mathcal{O}_P^\times &= \{r \in F : v_P(r) = 0\}, \\ P &= \{r \in F : v_P(r) > 0\}. \end{aligned}$$

(ii) Element $t \in F$ je uniformizator od P ako i samo ako $v_P(t) = 1$.

(iii) Obratno, pretpostavimo da je v diskretna valuacija od F/k. Tada je $P := \{r \in F : v(r) > 0\}$ mjesto od F/k i $\mathcal{O}_P = \{r \in F : v(r) \geq 0\}$ je pridruženi prsten valuacije.

Dokaz. Tvrdnje (*i*) i (*ii*) slijede iz Teorema 2.1.9. Dakle oslanjamo se na činjenicu da postoji neki uniformizator t_P od P i svaki element $r \in F^\times$ ima jedinstvenu reprezentaciju $r = t_P^n u$ sa $n \in \mathbb{Z}$ i $u \in \mathcal{O}^\times$. Za (*iii*), iz svojstva diskretne valuacije lako se provjeri da je definirani prsten $\mathcal{O}_P$ uistinu prsten valuacije od F/k (stoga i prsten diskretne valuacije). Nadalje P je prost ideal jer $v(r_1 r_2) > 0 \implies v(r_1) > 0$ ili $v(r_2) > 0$. Iz toga vidimo da je P ujedno i jedinstveni maksimalni ideal od $\mathcal{O}_p$ pa i mjesto od F. □

Vidimo da diskretne valuacije, prsteni valuacije i mjesta međusobno prirodno korespondiraju, u biti možemo ih poistovjetiti. Postoji čak i četvrta interpretacija. Neka je F/k funkcijsko polje i C/k korespondirajuća krivulja (dakle $k(C) \cong F$). Apsolutna Galoisova grupa G_k djeluje na $C(\bar{k})$ i orbite tog djelovanja nazivamo *zatvorene točke* od C. Preslikavanje

$$\{\text{zatv. točke od } C/k\} \ni P \mapsto \mathfrak{m}_P \in \mathbb{P}_F$$

gdje je $\mathfrak{m}_P$ maksimalni ideal lokalnog prstena $\mathcal{O}_P := \{r \in k(C) : P \text{ je regularna u } r\}$ je zapravo bijekcija između zatvorenih točaka od C i mjesta od F. Fiksirajmo neku zatvorenu točku P i neka je $P = \{P_1, \ldots, P_N\}$ gdje $P_j \in C(\bar{k})$. Uočimo da je funkcija $f \in k(V)$ regularna u P_j za neki j ako i samo ako je regularna u P_j za sve j. Zato ima smisla reći da je funkcija f *regularna* u zatvorenoj točki P. Konkretno $\mathfrak{m}_P$ se sastoji od funkcija f koje su regularne u P i $f(P_1) = \ldots = f(P_n) = 0$. Ponovno imamo $f(P_j) = 0$ za neki indeks j ako i samo ako isto vrijedi za sve j.

Korespondencija između zatvorenih točaka od C i mjesta u F nam omogućava da prevodimo tvrdnje o krivuljama u tvrdnje o funkcijskim poljima i obrnuto.

Definicija 2.1.17. Neka je $P \in \mathbb{P}_F$. $F_P := \mathcal{O}/P$ je *polje ostataka* od P. Definiramo *stupanj* od P sa $\deg P := [F_P : k]$.

Ako je C/k neka krivulja kojoj je F/k polje ostataka i P je zatvorena točka od C/k, tada ćemo još označavati $k(P)$ za polje ostataka od P (dakle $k(P) = F_P = F_{\mathfrak{m}_P}$ gdje je $\mathfrak{m}_P \in \mathbb{P}_F$ mjesto koje korespondira zatvorenoj točki P).

Propozicija 2.1.18. *Ako je $x \in P$, $x \neq 0$, imamo da je* $\deg P \leq [F : K(x)]$. *Nadalje* $\deg P$ *je točno jednak duljini G_k-orbite korespondirajuće zatvorene točke.*

Definicija 2.1.19. Neka je $r \in F$ i $P \in \mathbb{P}_F$. Kažemo da r ima *nultočku reda m u P* ako je $v_P(f) = m > 0$, i *pol reda m u P* ako je $v_P(f) = -m < 0$.

S obzirom da zatvorene točke i mjesta funkcijskog polja korespondiraju, ima smisla govoriti o uniformizatoru pridruženom nekoj točki. Ovdje navodimo jedan koristan kriterij koji nam pomaže naći uniformizator u praksi.

Napomena 2.1.20. Neka je C krivulja zadana afinom jednadžbom

$$C : f(x, y) = 0.$$

Za točku $P = (a, b) \in C(k)$, iz glatkoće imamo da je $\nabla f(a, b) \neq 0$. Vrijedi

- Ako je $\partial_y f(a, b) \neq 0$, tada je $x - a$ uniformizator.
- Ako je $\partial_x f(a, b) \neq 0$, tada je $y - b$ uniformizator.

Primjer 2.1.21. Neka je $C : y^2 = x^3 - x$ i $P = (0, 0)$. Za $f(x, y) = x^3 - x - y^2$ računamo $\partial_x f(0, 0) = -1$ dakle iz gornje napomene slijedi da je y je uniformizator od P. Pokažimo sad istu tvrdnju bez napomene. Imamo da je ideal $\mathfrak{m}_P$ u $\mathcal{O}_P$ generiran sa $\mathfrak{m}_P = (x, y)$. Vrijedi $y^2 = (x^2 - 1)x$ te $(x^2 - 1) = -1 \neq 0$ u $P = (0, 0)$, dakle $x^2 - 1 \in \mathcal{O}^\times$. Imamo $x = \frac{1}{x^2-1} y^2 \in (y) \implies (x, y) = (y)$ kao ideal u $\mathcal{O}_P$. Dakle y generira ideal $\mathfrak{m}_P$ pa zaključujemo da je uniformizator od P. Imamo i $v_P(x) = v_P(1/(x^2 - 1)) + 2v_P(y) = 0 + 2 = 2$.

Preslikavanja između krivulja

Propozicija 2.1.22. *Neka je C krivulja i $\phi : C \to Y$ racionalno preslikavanje. Tada je ϕ morfizam.*

Dokaz. Neka $\phi = (\phi_0 : \ldots : \phi_n)$ i izaberimo neku $P \in C$. Neka je t_P uniformizator od P i $m := \min\{v_P(\phi_i) : i = 0, \ldots, n\}$. Tada je $\phi = (t_P^{-m}\phi_0 : \ldots : t_P^{-m}\phi_n)$ očito regularno u P. To vrijedi za sve $P \in C$ dakle ϕ je morfizam. □

Propozicija 2.1.23. *Neka je $\phi : C_1 \to C_2$ morfizam između krivulja. Tada je ili konstantan ili dominantan.*

Dokaz. Lako se pokaže da Propozicija 1.3.13 vrijedi i za projektivne mnogostrukosti, dakle $\overline{\operatorname{Im}\phi} \subseteq C_2$ je projektivna mnogostrukost. Imamo da je

$$\dim \overline{\operatorname{Im}\phi} \leq \dim C_2 = 1.$$

Ako je $\overline{\operatorname{Im}\phi} \neq C_2$, vrijedi stroga nejednakost za dimenziju dakle $\dim \overline{\operatorname{Im}\phi} = 0$. Tada je $\overline{\operatorname{Im}\phi}$ točka i ϕ je konstantno. Inače $\overline{\operatorname{Im}\phi} = C_2$ znači da je morfizam dominantan. □

Naime, vrijedi još i jači rezultat.

Teorem 2.1.24. *Nekonstantan morfizam $C_1 \to C_2$ je surjektivan.*

Dokaz. Vidi Teorem 8.2.7 u [2]. □

Korolar 2.1.25. *Ako su dvije krivulje biracionalno ekvivalentne, tada su one izomorfne.*

Uočimo da nam ovi rezultati pokazuju da su dominantna racionalna preslikavanja između krivulja zapravo surjektivni morfizmi. Zato možemo iskazati Teorem 2.1.5 u sljedećem obliku.

Korolar 2.1.26. *Kategorija krivulja s nekonstantnim morfizmima je kontravarijantno ekvivalentna kategoriji funkcijskih polja.*

Lema 2.1.27. *Neka su C_1/k i C_2/k krivulje, te neka je $\phi : C_1 \to C_2$ morfizam definiran nad k. Ako je P zatvorena točka od C_1, onda je $\phi(P)$ zatvorena točka od C_2.*

Dokaz. Neka je $P = \{P_1, \ldots, P_N\}$. Imamo $\phi(P) = \{\phi(P_1), \ldots, \phi(P_N)\}$. Pogledajmo kako G_k djeluje na $\phi(P)$. Naime imamo

$$\sigma(\phi(P_j)) = \phi(\sigma(P_j)) = \phi(P_{j'}) \in \phi(P)$$

za sve j i $\sigma \in G_k$. Iz toga vidimo da je $\{\phi(P_1), \ldots, \phi(P_N)\}$ neka orbita djelovanja G_k na $C_2(\bar{k})$, dakle $\phi(P)$ je zatvorena točka. □

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

Definicija 2.1.28. Neka su C_1/k i C_2/k krivulje, te $\phi : C_1 \to C_2$ nekonstantan morfizam definiran nad k. Neka je P zatvorena točka od C_1/k. *Indeks grananja* od ϕ u P je

$$e_\phi(P) := v_P(\phi^*(t_Q)),$$

gdje je t_Q uniformizator u $Q = \phi(P)$. Ako je $e_\phi(P) = 1$, kažemo da je ϕ *nerazgranat* u P. Ako je $e_\phi(P) = 1$ za sve zatvorene točke P od C_2/k, tada kažemo da je ϕ *nerazgranat*.

Lema 2.1.29. *Neka su C_1/k i C_2/k krivulje, te $\phi : C_1 \to C_2$ nekonstantan morfizam definiran nad k. Neka je P zatvorena točka od C_1/k, $Q = \phi(P)$ je zatvorena točka od C_2/k. Tada*

$$v_P(\phi^*(r)) = e_\phi(P)v_Q(r), \quad \forall r \in k(C_2).$$

Dokaz. Neka je $v_Q(r) = n$ i zapišimo $r = t_Q^n u$ gdje je t_Q uniformizator od Q i $u \in \mathcal{O}_Q^\times$. Podsjetimo se da to znači da je funkcija u regularna u Q te $u(Q) \neq 0$. Dakle $\phi^*(u)(P) = u(\phi(P)) \neq 0$, tj. $\phi^*(u) \in \mathcal{O}_P^\times$. Imamo $\phi^*(r) = \phi^*(t_Q)^n \phi^*(u)$ i stoga

$$v_P(\phi^*(r)) = nv_P(\phi^*(t_Q)) + v_P(\phi^*(u)) = ne_\phi(P) + 0 = nv_Q(r).$$

□

Definicija 2.1.30. Neka su C_1/k i C_2/k krivulje, te $\phi : C_1 \to C_2$ nekonstantan morfizam definiran nad k. *Stupanj* morfizma definiramo sa

$$\deg \phi := [k(C_1) : \phi^*(k(C_2))].$$

Uočimo da je gore definiran stupanj konačan. Naime ϕ^* je injektivno i $k(C_2) \neq k$ pa je $\phi^*(k(C_2))/k$ transcendentno proširenje (svako proširenje od k sadržano u $k(C_1)$ je transcendentno). S obzirom da je $k(C_1)/k$ stupnja transcendentnosti 1 i konačno generirano, imamo da je $k(C_1)/\phi^*(k(C_2))$ konačno generirano algebarsko proširenje.

Sljedeći bitan teorem navodimo bez dokaza.

Teorem 2.1.31. *Neka su C_1/k i C_2/k krivulje, te $\phi : C_1 \to C_2$ nekonstantan morfizam definiran nad k. Tada za sve $Q \in C_2(\bar{k})$ imamo*

$$\sum_{P \in C_1(\bar{k}) : \phi(P) = Q} e_\phi(P) = \deg(\phi).$$

Dokaz. Vidi Teorem 8.2.12. u [2]. □

Napomena 2.1.32. Teorem možemo alternativno formulirati za zatvorene točke. Naime za sve *zatvorene točke* Q od C_2/k imamo

$$\sum_{P : \phi(P) = Q} e_\phi(P) \frac{\deg P}{\deg Q} = \deg(\phi),$$

gdje suma ide po zatvorenim točkama P od C_1/k. Nije teško provjeriti da je ova tvrdnja ekvivalentna s originalnom formulacijom teorema.

Primjer 2.1.33. Neka je $\phi : \mathbb{P}^1 \mapsto \mathbb{P}^1$ morfizam krivulja nad algebarski zatvorenim poljem k, koji je zadan sa $\phi((a : 1)) = (a^5 : 1)$ i $\phi((1 : 0)) = (1 : 0)$. To je surjektivni morfizam i imamo da je $\deg \phi = [k(x) : \operatorname{Im} \phi^*] = [k(x) : k(x^5)] = 5$.

2.2 Divizori

Definicija 2.2.1. 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 $n_P \neq 0$ za najviše konačno mnogo P. Skup točaka P za koje $n_P \neq 0$ naziva se *podrška* divizora D. Divizori krivulje C s operacijom zbrajanja tvore slobodnu Abelovu grupu, koju nazivamo *grupa divizora od C* i označavamo s $\operatorname{Div} C$.

Definicija 2.2.2. Neka je F/k funkcijsko polje nad algebarski zatvorenim poljem. Divizor od F je formalna suma

$$D := \sum_{P \in \mathbb{P}_F} n_P P.$$

gdje je $n_P \in \mathbb{Z}$, te $n_P \neq 0$ za najviše konačno mnogo P. Divizori od F sa zbrajanjem tvore slobodnu abelovu grupu $\operatorname{Div} F$. Vidimo da je po ovoj definiciji $\operatorname{Div} F \cong \operatorname{Div} X_F$ gdje je X_F krivulja pridružena F (vidi 2.1.26).

Sada želimo definirati divizore nad općim poljima, dakle i onima koja nisu algebarski zatvorena. Definicija divizora preko funkcijskih polja nam sugerira kako to napraviti jer su mjesta uvijek definirana i korespondiraju zatvorenim točkama.

Definicija 2.2.3. Neka je k polje, $\bar{k}$ algebarsko zatvorenje i G_k apsolutna Galoisova grupa. Divizor $D = \sum n_P P \in \operatorname{Div} C$ je *definiran nad k* ako je fiksiran pri djelovanju G_k gdje

$$\sigma(D) = \sum n_P \sigma(P),\ \sigma \in G_k.$$

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

Primijetimo da G_k fiksira D ako i samo ako za svaku točku $P \in C(\bar{k})$ vrijedi $n_P = n_{\sigma(P)}$ za sve $\sigma \in G_k$. To znači da divizor D koji je definiran nad k možemo promatrati kao formalnu sumu po orbitama od G_k tj. zatvorenim točkama. Dakle alternativno definiramo

Definicija 2.2.4. Neka je C/k krivulja. *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.

Napomena 2.2.5. S obzirom da su mjesta funkcijskog polja u bijekciji s zatvorenim točkama, mogli smo ekvivalentno definirati divizor od C kao formalnu sumu $D := \sum_{P \in \mathbb{P}_{k(C)}} n_P P$ po mjestima funkcijskog polja $k(C)$.

Definicija 2.2.6. 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 2.2.7. 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*.

Teorem 2.2.8. *Neka je F/k funkcijsko polje i $f \in F^\times$. Tada je $v_P(f) = 0$ za sve osim konačno mnogo P.*

Dokaz. Neka je C/k krivulja s $k(C) \cong F$. Neka je $f \in k(C)$ neka funkcija takva da $f \neq 0$. Imamo da je $k(C) = k(C \cap \mathbb{A}^n)$, dakle $f = g/h$ za neke $g, h \in k[C \cap \mathbb{A}^n]$. Vrijedi da su skupovi nultočaka $Z_g, Z_h \subseteq (C \cap \mathbb{A}^n)(\bar{k})$ konačni. To je zato što se zatvoreni skupovi u topologiji Zariskog općenito mogu prikazati kao konačna unija ireducibilnih (Korolar 1.1.22), a u ovom konkretnom slučaju mnogostrukosti koje su sadržane u $Z_g \cup Z_h$ moraju biti dimenzije 0 dakle točke. Primijetimo da je

$$\{P \in C \cap \mathbb{A}^n : v_P(f) \neq 0\} \subseteq Z_g \cup Z_h$$

dakle taj skup je konačan. Iz činjenice da se C može pokriti s konačno afinih mnogostrukosti $C \cap U_i \cong C \cap \mathbb{A}^n$, slijedi da je $v_P(f) \neq 0$ za najviše konačno točaka $P \in C(\bar{k})$.

Iz toga imamo i da je $v_P(f) \neq 0$ za najviše konačno zatvorenih točaka P od C/k. □

Definicija 2.2.9. Neka je C/k krivulja i F/k odgovarajuće funkcijsko polje. *Stupanj* divizora se definira sa

$$\deg D := \sum n_P \deg P \quad \text{gdje} \quad D = \sum n_P P.$$

Definicija 2.2.10. Neka je C/k krivulja. Glavne divizore u $\operatorname{Div}_k C$ označavamo sa $\operatorname{Gl}_k C$. Nije teško provjeriti da je to podgrupa. Nadalje kvocijentna grupa

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

se naziva *Picardova grupa* od C. Za divizore D_1, D_2 koji pripadaju istoj klasi u $\operatorname{Pic}_k C$ (ili ekvivalentno $D_2 - D_1 = \operatorname{div} f$ za neki $f \in k(C)^\times$) kažemo da su *linearno ekvivalentni*, te označavamo to s $D_1 \sim D_2$.

Teorem 2.2.11. *Niz*

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

je egzaktan.

Dokaz. Jedino je potencijalno nejasno da $\ker \mathrm{div} = k^\times$. Očito je $k^\times \subseteq \ker \mathrm{div}$, pa dokažimo sada obrnutu inkluziju. Neka je $f \in \ker \mathrm{div} \subseteq k(C)^\times$. Možemo f shvatiti kao racionalno preslikavanje $\phi : C \to \mathbb{P}^1$. Vidjeli smo da je svako racionalno preslikavanje između krivulja morfizam koji je ili surjektivan ili konstantan. Ako je ϕ konstantan morfizam, to znači da je $f \in k^\times$. Inače ako je ϕ surjektivan, onda $\exists P_1 \in C(\bar{k})$ takva da $\phi(P_1) = 0 = (0 : 1)$, pa je i $f(P_1) = 0$ tj. $v_{P_1}(f) > 0$. Očito ako je P zatvorena točka koja sadrži P_1, isto vrijedi $v_P(f) = v_{P_1}(f) > 0$. Zaključujemo $\mathrm{div}\, f \neq 0$ što je kontradikcija pa ϕ ne može biti surjektivan. □

Definicija 2.2.12. Neka su C_1/k i C_2/k krivulje, te $\phi : C_1 \to C_2$ nekonstantan morfizam definiran nad k. *Preslikavanje povlačenja* ϕ^* na divizorima je homomorfizam $\phi^* : \mathrm{Div}_k C_2 \to \mathrm{Div}_k C_1$ definiran s

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

gdje je Q divizor koji se sastoji od jedne točke, tj. $\mathrm{div}\, Q = Q$. *Preslikavanje guranja* ϕ_* je homomorfizam $\phi_* : \mathrm{Div}_k C_1 \to \mathrm{Div}_k C_2$ definiran s

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

Uočimo da divizori koji se sastoje od jedne zatvorene točke ($\mathrm{div}\, Q = Q$) općenito generiraju grupu k-racionalnih divizora $\mathrm{Div}_k C$. Dakle dovoljno je definirati homomorfizme na zatvorenim točkama, kao što smo gore i napravili.

Propozicija 2.2.13. *Vrijedi da je* $\phi_*(\phi^*(D)) = \deg(\phi)D$, *tj.* $\phi_* \circ \phi^*$ *je množenje s* $\deg \phi$ *u* $\mathrm{Div}_k C_2$.

Dokaz. Dovoljno je dokazati da se homomorfizmi $\phi_* \circ \phi^*$ i $\deg \phi \cdot *$ podudaraju na divizorima koji se sastoje od jedne točke. Neka je dakle Q zatvorena točka od C_2/k koju promatramo kao divizor, tj. $\mathrm{div}\, Q = Q$. Računamo

$$(\phi_* \circ \phi^*)(Q) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)\phi_*(P) = \left(\sum_{P \in \phi^{-1}(Q)} e_\phi(P) \frac{\deg P}{\deg \phi(P)} \right) Q = \deg \phi Q$$

gdje zadnja jednakost slijedi iz Teorema 2.1.31. □

Propozicija 2.2.14. *Neka je $\phi : C_1 \to C_2$ nekonstantan morfizam krivulja definiranih nad k. Tada za svaki divizor $D \in \mathrm{Div}_k C_2$, vrijedi*

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

Dokaz. Dokazat ćemo jednakost za točke. Neka je Q zatvorena točka od C_2/k. Imamo

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

gdje zadnja jednakost slijedi iz Teorema 2.1.31. □

Posljedica je sljedeći bitan teorem.

Teorem 2.2.15. *Neka je $f \in k(C)^\times$ za krivulju C/k. Tada je* $\deg \mathrm{div}\, f = 0$*, te ako je $f \notin k^\times$, tada*

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

Dokaz. Funkciju $f \in k(C)^\times$ možemo shvatiti kao racionalno preslikavanje $\phi : C \to \mathbb{P}^1$. Vidjeli smo da je racionalno preslikavanje krivulja ili konstantan ili surjektivan morfizam. Iz $f \notin k^\times$ dobijemo da ϕ nije konstantan morfizam, dakle surjektivan je. Funkcijsko polje od $\mathbb{P}^1$ je $k(x)$ i $\phi^* : k(x) \to k(C)$ djeluje sa $\phi^*(r) = r \circ f$. Dakle

$$\deg \phi = [k(C) : \phi^*(k(x))] = [k(C) : k(f)].$$

Nadalje imamo iz Propozicije 2.2.14

$$\deg \phi^*((0:1)) = \sum_{P:\phi(P)=(0:1)} e_\phi(P) \deg P = \deg \phi.$$

Uočimo da je $t = x$ uniformizator u točki $0 = (0 : 1)$ od $\mathbb{P}^1$. Dakle $e_\phi(P) = v_P(\phi^*(t)) = v_P(f)$. Kada uvrstimo to u gornju jednadžbu dobijemo

$$\deg \mathrm{div}_0 f = \sum_{P:\phi(P)=(0:1)} v_P(f) \deg P = \deg \phi = [k(C) : k(f)].$$

Ako umjesto f uvrstimo $1/f$ dobijemo slično

$$\deg \mathrm{div}_\infty f = \deg \mathrm{div}_0 1/f = [k(C) : k(1/f)] = [k(C) : k(f)].$$

□

Korolar 2.2.16. *Za sve glavne divizore $D \in \mathrm{Gl}_k C$, vrijedi* $\deg D = 0$.

Divizori stupnja 0

Definicija 2.2.17. Neka je C/k krivulja. Divizori stupnja 0 čine podgrupu od $\mathrm{Div}_k C$ koju označavamo sa $\mathrm{Div}_k^0 C$.

Tada je $\mathrm{Gl}_k C \subseteq \mathrm{Div}_k^0 C$ pa dodatno definiramo $\mathrm{Pic}_k^0 C := \mathrm{Div}_k^0 C / \mathrm{Gl}_k C$.

Uočimo sada da je

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

egzaktan niz.

Općenito, ako je k algebarski zatvoreno polje, očekujemo da $\mathrm{Pic}_k^0 C$ nije trivijalna. Naime, to se dogodi ako i samo ako je C izomorfna projektivnom pravcu.

Teorem 2.2.18. *Neka je C/k krivulja nad algebarski zatvorenim poljem k. Tada je $C \simeq \mathbb{P}^1$ ako i samo ako je* $\mathrm{Pic}_k^0(C) = \{0\}$.

Dokaz. Neka je $C \simeq \mathbb{P}^1$. Svaka točka $P = (a_0 : a_1) \in \mathbb{P}^1$ je nultočka homogenog polinoma $f_P(x_0, x_1) = a_1 x_0 - a_0 x_1$. Za svaki divizor $D = \sum n_P P$, definiramo funkciju $f_D := \Pi f_P^{n_P}$. Ako je D stupnja 0, tada su brojnik i nazivnik od f_D homogeni polinomi istog stupnja, pa $f_D \in k(\mathbb{P}^1) \simeq k(C)$. Nadalje $D = \mathrm{div}\, f_D$ što znači da je svaki divizor stupnja 0 ujedno i glavni.

Obratno, pretpostavimo da je $\mathrm{Pic}_k^0(C) = \{0\}$ i neka su P i Q različite točke od $C(k)$. Divizor $D := P - Q$ je stupnja 0 pa je zato glavni i imamo $D = \mathrm{div}\, f$ za neki $f \in k(C)^\times$. Očito $f \notin k^\times$ jer $\mathrm{div}\, f \neq 0$. Iz Teorema 2.2.15 slijedi da je $[k(C) : k(f)] = \deg \mathrm{div}_0 f = 1$. Dakle $k(C) = k(f) \simeq k(\mathbb{P}^1)$. Iz ekvivalencije kategorija funkcijskih polja i krivulja s morfizmima, sada slijedi da su C i $\mathbb{P}^1$ izomorfne. □

Napomena 2.2.19. Primijetimo da ako je C/k krivulja nad poljem k koje nije nužno algebarski zatvoreno, i dalje imamo da $C \simeq \mathbb{P}^1 \implies \mathrm{Pic}_k^0(C) = \{0\}$. Međutim, obrat ne vrijedi jer postoje krivulje C/k takve da $\mathrm{Pic}_k^0(C) = \{0\}$ koje nisu izomorfne s $\mathbb{P}^1$. Navedeni dokaz ne radi za njih jer trebamo da su P i Q "prave" točke, ne samo zatvorene. To je potrebno da osiguramo $\deg D_0 = 1$ gdje $D = P - Q = D_0 - D_\infty$. Ako postoje barem dvije različite točke u $C(k)$ onda obrat vrijedi.

Korolar 2.2.20. *Neka je C/k krivulja s barem dvije k-racionalne točke. Tada je $C/k \simeq \mathbb{P}^1/k \iff \mathrm{Pic}_k^0 C = \{0\}$.*

Poglavlje 3

Riemann-Rochov teorem

3.1 Riemannov teorem

Definicija 3.1.1. Neka je C/k krivulja. Za $D \in \mathrm{Div}_k C$, definiramo *linearni sustav* ili *Rimeann-Rochov prostor*

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

Navedimo osnovna svojstva Riemann-Rochovih prostora.

Propozicija 3.1.2. *Neka je C/k krivulja i $D \in \mathrm{Div}_k C$ divizor. Tada*

1. *$L(D)$ je vektorski potrpstor (nad k) od $k(C)$.*
2. *$D \leq D' \implies L(D) \subseteq L(D')$.*
3. *$L(0) = k$.*
4. *$L(D) = \{0\}$ ako $\deg D < 0$.*
5. *Ako je $D \sim D'$ tada su $L(D) \simeq L(D')$ izomorfni vektorski prostori.*
6. *$L(D) \neq \{0\} \iff D \sim D'$ za neki divizor $D' \geq 0$.*

Dokaz.

1. Neka $D = \sum n_P P$. Za zatvorenu točku P definiramo $V_P := \{f \in k(C) : v_P(f) \geq -n_P\}$. Iz svojstva diskretne valuacije v_P (Definicija 2.1.13) lako provjerimo da V_P sadrži 0 i da je zatvoren na zbrajanje i množenje skalarima iz k, dakle V_P je vektorski prostor. Tada je i $L(D) = \cap_P V_P$ vektorski potprostor nad k.

2. Neka je $D = \sum n_P P$ i $D' = \sum n'_P P$. Tada $n_P \leq n'_P$, $\forall P$. Imamo da $f \in L(D) \implies v_P(f) \geq -n_P$, $\forall P \implies v_P(f) \geq -n'_P$, $\forall P \implies f \in L(D')$.

3. $L(0)$ je skup funkcija $f \in k(C)$ takvih da $\operatorname{div} f \geq 0$. Iz $\deg \operatorname{div} f = 0$ dobivamo $\operatorname{div} f = 0$ što je istina samo za $f \in k^\times$. Dakle $L(0) = k$.

4. Ako je $0 \neq f \in L(D)$ tada je $\operatorname{div} f + D \geq 0 \implies \deg \operatorname{div} f + \deg D = \deg D \geq 0$.

5. Neka je $D' = D + \operatorname{div} h$ za neki $h \in k(C)^\times$. Tvrdimo da je linearno preslikavanje $\phi : L(D') \to L(D)$ definirano sa $\phi(f) := fh$ izomorfizam. Dovoljno je uočiti da za $f \in k(C)^\times$ imamo

$$\begin{aligned} f \in L(D') &\iff \operatorname{div} f \geq -D' \iff \operatorname{div} f \geq -D' - \operatorname{div} h \\ &\iff \operatorname{div}(fh) \geq -D \iff fh \in L(D). \end{aligned}$$

   Dakle ϕ je dobro definirano, očito je injekcija i za $0 \neq g \in L(D)$ imamo $g/h \in L(D')$ te $\phi(g/h) = h$ pa je i surjekcija.

6. Ako postoji $0 \neq f \in L(D)$, tada za $D' := \operatorname{div} f + D$ imamo $D' \geq 0$ i $D \sim D'$. Obratno, ako je $D' \geq 0$ i $D' = \operatorname{div} f + D$ za neki $f \in k(C)^\times$, to znači da je $f \in L(D)$ pa $L(D) \neq \{0\}$.

□

Primjer 3.1.3. Neka je $C = \mathbb{P}^1/k$. Afine točke su oblika $(a : 1) \in \mathbb{A}^1 \subseteq \mathbb{P}^1$. Dakle *točka u beskonačnosti* $\infty = (1 : 0) \in \mathbb{P}^1(k)$ je jedinstvena točka izvan $\mathbb{A}^1$. Za funkciju $x \in k[x] \subseteq k(x) = k(C)$ imamo

$$\operatorname{div} x = (0 : 1) - \infty.$$

Naime, znamo da je $P = (0 : 1) = 0$ jedina afina točka za koju je $v_P(x) \neq 0$ i x je uniformizator u P. Iz $\deg \operatorname{div} x = 0$ sada slijedi da x ima pol reda 1 u ∞ što potpuno određuje $\operatorname{div} x$. Općenitije, za sve polinome $p \in k[X]$, $p \neq 0$ imamo da je $v_\infty(p) = -\deg p$.

Kako izgleda $L(4\infty)$? Ako je $0 \neq f \in L(4\infty)$, vidimo da je $v_P(f) \geq 0$ za sve zatvorene točke iz $\mathbb{A}^1$. Dakle f je regularna u svim afinim točkama. Iz Propozicije 1.3.8 sada slijedi $f \in k[x]$. Vidjeli smo da onda $v_\infty(f) = -\deg f$ što znači da se $L(4\infty)$ sastoji od polinoma stupnja ≤ 4. Vektorski prostor $L(4\infty)$ ima bazu $\{1, x, x^2, x^3, x^4\}$ nad k dakle $\dim_k L(4\infty) = 5$.

Lema 3.1.4. *Za bilo koja dva divizora $A \leq B$, imamo $L(A) \subseteq L(B)$ i*

$$\dim(L(B)/L(A)) \leq \deg B - \deg A.$$

Dokaz. Dovoljno je dokazati tvrdnju u slučaju da je $B = A + P$, tj. divizori $A \leq B$ se razlikuju za jednu zatvorenu točku P. Cilj nam je dakle dokazati $\dim(L(B)/L(A)) \leq \deg P$. Primijetimo da je $\deg P = \dim_k k(P)$ gdje je $k(P) = \mathcal{O}_P/\mathfrak{m}_P$ polje ostataka od P. Neka je $m := v_P(A)$. Tada je $v_P(B) = m + 1$ i $v_P(f) \geq -m - 1$, $\forall f \in L(B)$. Neka je t uniformizator u točki P. Definirajmo linearno preslikavanje $\phi : L(B) \to k(P)$ sa $\phi(f) := t^{m+1} f \mod P$. Imamo da je $L(A) = \ker \phi$, dakle prvi teorem o izomorfizmu kaže

$$L(B)/L(A) = L(B)/\ker \phi \cong \operatorname{Im} \phi \subseteq k(P).$$

Zaključujemo $\dim_k L(B)/L(A) \leq \dim_k k(P) = \deg P$. □

Teorem 3.1.5. *Za svaki divizor $D \in \operatorname{Div}_k C$ takav da $D \geq 0$, vrijedi* $\dim L(D) \leq \deg D + 1$.

Dokaz. Koristimo Lemu 3.1.4 za $A = 0$ i $B = D$. To daje $\dim L(D)/L(0) \leq \deg D$. Vrijedi $\dim L(D)/L(0) = \dim L(D) - \dim L(0) = \dim L(D) - 1$, dakle $\dim L(D) \leq \deg D + 1$. □

Definicija 3.1.6. Za $D \in \operatorname{Div}_k C$ definiramo $l(D) := \dim_k L(D) \in \mathbb{N}_0$.

Podsjetimo se dakle da je $l(D) \geq \deg D + 1$ za divizore sa $D \geq 0$. Ako su $D \sim D'$ imamo iz Propozicije 3.1.2 (5.) da $l(D) = l(D')$. Nadalje $l(0) = 1$.

Lema 3.1.7. *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 glavni divizor, onda je $D \sim 0$ pa $l(D) = l(0) = 1$. Inače pretpostavimo da D nije glavni divizor. Ciljajući na kontradikciju, pretpostavimo da je $l(D) \neq 0$. Tada po Propoziciji 3.1.2 (6.), $D \sim D'$ za neki $D' \geq 0$. Vrijedi da je $\deg D' = \deg D = 0$, pa je nužno $D' = 0$. To znači da je D glavni divizor što je kontradikcija. □

Teorem 3.1.8. *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 $f \in k(C)$ transcendentna nad k i neka je $A := \operatorname{div}_\infty f > 0$. Iz Teorema 2.2.15 slijedi $d = \deg A = [k(C) : k(f)]$. Izaberimo bazu $v_1, \ldots, v_d$ za vektorski prostor $k(C)$ nad $k(f)$. Primijetimo da je za $n \in \mathbb{N}$ skup

$$S_n = \{v_i f^j : 1 \leq i \leq d, 0 \leq j \leq n\}$$

linearno nezavisan nad k. Naime v_i su linearno nezavisni nad $k(f)$ i f je transcendentan nad k. Primijetimo da je $\operatorname{div} f \geq -A \implies \operatorname{div} f^j \geq -jA \geq -nA$. Stoga, ako izaberemo $B \geq 0$

tako da div $v_i \geq -B$ za sve v_i, dobivamo div $v_i f^j \geq -nA - B$. To znači da je $S_n \subseteq L(nA + B)$ dakle $l(nA + B) \geq (n + 1)d$. Računamo

$$\begin{aligned}\deg nA + 1 - l(nA) &= \deg(nA + B) + 1 - l(nA + B) + (l(nA + B) - l(nA) - \deg B) \\ &\leq \deg(nA + B) + 1 - l(nA + B) \\ &\leq nd + \deg B + 1 - (n + 1)d = \deg B - \deg A + 1,\end{aligned}$$

gdje smo u prvoj nejednakosti koristili Lemu 3.1.4. Definiramo $g := \deg B - \deg A + 1$ pa imamo

$$\deg nA + 1 - l(nA) \leq g, \quad \forall n \geq 0. \tag{3.1}$$

Sada ćemo dokazati da (3.1) i dalje vrijedi ako umjesto nA stavimo proizvoljan divizor D. To ćemo napraviti u dva koraka:

1. Ako je $D_1 \leq D_2$, tada $\deg D_1 + 1 - l(D_1) \leq \deg D_2 + 1 - l(D_2)$.
2. Za divizor $D \geq 0$ postoje $n \in \mathbb{N}$ i divizor $D' \sim D$ takvi da $D' \leq nA$.

Primijetimo da su ove dvije tvrdnje dovoljne. Naime, ako je D proizvoljan divizor, imamo $D = D_0 - D_\infty$. Tada je $D \leq D_0$ pa je iz (1.) dovoljno dokazati $\deg D_0 + 1 - l(D_0) \leq g$. Vrijedi $D_0 \geq 0$ pa iz (2.) sad dobivamo da $D_0 \sim D'$, $D' \leq nA$. Konačno

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

Dokažimo sada te dvije tvrdnje.

1. Iz Leme 3.1.4 slijedi $l(D_2) - l(D_1) \leq \deg(D_2 - D_1)$. To povlači da je $\deg D_1 + 1 - l(D_1) \leq \deg D_2 + 1 - l(D_2)$.
2. Neka je $D \geq 0$. Tada je $nA - D \leq nA$ pa iz tvrdnje (1.) i nejednakosti (3.1) dobivamo $\deg(nA - D) + 1 - l(nA - D) \leq g \implies l(nA - D) \geq nd - \deg D + 1 - g$. Dakle za veliki n imamo $l(nA - D) \neq 0$ pa postoji $0 \neq f \in L(nA - D)$. Tada je div $f \geq D - nA$, dakle za divizor $D' := D - \text{div } f$ imamo $nA \geq D'$.

□

Vidimo da je vrijednost $\deg D - l(D)$ uniformno omeđena za divizore $D \in \text{Div}_k C$ pa uvodimo oznaku:

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

Pokazali smo da postoji g za koji

$$r(D) \leq g - 1, \quad \forall D \in \text{Div}_k C.$$

Iz Leme 3.1.4 slijedi da ako je $A \leq B$, onda $r(A) \leq r(B)$. Nadalje, ako je $A \sim B$, očito imamo $r(A) = r(B)$.

Definicija 3.1.9. Označimo $r(D) := \deg D - l(D)$. *Genus* krivulje C/k se definira kao

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

Teorem 3.1.10 (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 dovoljnog stupnja.*

Dokaz. Neka je A neki divizor takav da $r(A) = g - 1$ (dakle r postiže maksimum u A). Dokazat ćemo

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

Naime, ako je $\deg D \geq \deg A + g$, onda $r(D - A) = \deg(D - A) - l(D - A) \leq g - 1 \implies l(D - A) \geq 1 + (\deg D - \deg A - g) \geq 1$. Dakle postoji $0 \neq f \in L(D - A)$ pa vrijedi $\mathrm{div}\, f \geq A - D$. Za divizor $A' := A - \mathrm{div}\, f$ sada imamo $D \geq A'$ i $A' \sim A$. Dakle $r(D) \geq r(A') = r(A) = g - 1$. S obzirom da je $r(D) \leq g - 1$, dobivamo $r(D) = g - 1$. □

Riemann-Rochov teorem pojačava Riemannov teorem tako što točno karakterizira koliko je $r(D)$ udaljen od $g - 1$. Ispostavlja se da postoji posebna klasa divizora u $\mathrm{Pic}_k C$ koju ćemo nazivati kanonska klasa. Divizore W koji pripadaju kanonskoj klasi nazivamo kanonski divizori i Riemann-Rochov teorem tvrdi da za njih vrijedi

$$(g - 1) - r(D) = l(W - D).$$

U sljedećim sekcijama, cilj nam je definirati kanonski divizor i precizno iskazati Riemann-Rochov teorem. Sljedeća oznaka će nam biti korisna.

Definicija 3.1.11. Neka je C/k krivulja genusa g. Za $D \in \mathrm{Div}_k C$ definiramo *indeks specijalnosti* sa

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

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

3.2 Prsten adela

Prsten adela nam je koristan za bolje razumijevanje indeksa specijalnosti.

Definicija 3.2.1. *Prsten adela* od funkcijskog polja F/k s oznakom $\mathcal{A}_F$ ili samo $\mathcal{A}$, je potprsten direktnog produkta $\Pi_P F$ (gdje produkt ide po mjestima $P \in \mathbb{P}_F$ čiji su elementi $\alpha = (\alpha_P)$ takvi da je $\alpha_P \in \mathcal{O}_P$ za sve osim konačno mnogo P-ova). Elementi od $\mathcal{A}$ se zovu *adeli*.

Postoji kanonsko ulaganje $F/k \to \mathcal{A}$ zadano sa

$$f \mapsto (\alpha_P)_{P\in\mathbb{P}_F} = (f)_{P\in\mathbb{P}_F}.$$

Uistinu imamo da je $v_P(f) = 0$ za sve osim konačno P pa $v_P(f) = 0 \implies f \in \mathcal{O}_P$. Adele koji se nalaze u slici ovog ulaganja nazivamo *glavni adeli*. Proširujemo definiciju valuacije v_P na adele sa $v_P(\alpha) := v_P(\alpha_P)$.

Definicija 3.2.2. Neka je $D \in \mathrm{Div}_k C$. *Prostor adela* od D je

$$\mathcal{A}(D) := \{\alpha \in \mathcal{A} : v_P(\alpha) \geq -v_P(D),\ \forall P \in C\}.$$

Uočimo da je $\mathcal{A}(D)$ vektorski prostor nad k.

Sljedeću tvrdnju navodimo bez dokaza, ali je dokaz srodan dokazu Leme 3.1.4.

Propozicija 3.2.3. *Za svaka dva divizora $A \leq B$ vrijedi $\mathcal{A}(A) \subseteq \mathcal{A}(B)$ i $\mathcal{A}(A)+F \subseteq \mathcal{A}(B)+F$ gdje gledamo kopiju od F u $\mathcal{A}$, te*

$$\dim_k(\mathcal{A}(B)/\mathcal{A}(A)) = \deg B - \deg A \tag{3.2}$$

$$\dim_k \frac{\mathcal{A}(B)+F}{\mathcal{A}(A)+F} = r(B) - r(A). \tag{3.3}$$

Dokaz. Poglavlje 6 u [4]. □

Propozicija 3.2.4. *Za svaki divizor D za koji $r(D) = g - 1$ imamo $\mathcal{A} = \mathcal{A}(D) + F$.*

Dokaz. Neka je $\alpha \in \mathcal{A}$. Za divizor $\tilde{D} := \sum_{P:v_P(\alpha)<0} -v_P(\alpha)P$ imamo da je $\alpha \in \mathcal{A}(\tilde{D}) \subseteq \mathcal{A}(\tilde{D}) + F$. Neka je D' divizor takav da $D' \geq D$ i $D' \geq \tilde{D}$. Tada je $\mathcal{A}(\tilde{D}) + F \subseteq \mathcal{A}(D') + F$ pa imamo $\alpha \in \mathcal{A}(D') + F$. Nadalje $r(D') \geq r(D) \implies r(D') = g - 1$. Iz (3.3) zaključujemo $\mathcal{A}(D') + F = \mathcal{A}(D) + F$. Dakle vrijedi $\alpha \in \mathcal{A}(D) + F$ za sve $\alpha \in \mathcal{A}$. □

Teorem 3.2.5. *Neka je F/k funkcijsko polje. Za svaki $D \in \mathrm{Div}_k C$ imamo*

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

Dokaz. Neka je $D \in \mathrm{Div}_k C$. Iz Riemannovog teorema (3.1.10) postoji $D' \geq D$ takav da $r(D') = g - 1$. Tada

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

□

3.3 Diferencijali

Neka je F/k funkcijsko polje i $\mathcal{A}$ njegov prsten adela. Teorem 3.2.5 nam kaže da je $\dim_k \frac{\mathcal{A}}{\mathcal{A}(D)+F}$ konačna. Da bi još sažetije okarakterizirali indeks specijalnosti $i(D)$, prirodno je promatrati anihilator od $\mathcal{A}(D) + F$. Označimo ga sa

$$\Omega(D) := (\mathcal{A}(D) + F)^0 = \{\varphi \in \mathcal{A}' : \mathcal{A}(D) + F \subseteq \ker \varphi\},$$

gdje je $\mathcal{A}'$ dualni vektorski prostor od $\mathcal{A}$. Iz linearne algebre imamo da je

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

Definicija 3.3.1. Skup

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

nazivamo prostor *Weilovih diferencijala* za F/k.

Propozicija 3.3.2. *Neka je F/k funkcijsko polje. Prostor Weilovih diferencijala Ω_F je vektorski prostor nad k.*

Dokaz. Neka su $\omega_1 \in \Omega(D_1)$, $\omega_2 \in \Omega(D_2)$. Postoji divizor D takav da $D \leq D_1$ i $D \leq D_2$. Tada je $\Omega(D_1) \cup \Omega(D_2) \subseteq \Omega(D)$ pa je $\omega_1, \omega_2 \in \Omega(D) \implies \omega_1 + \omega_2 \in D$. Svaki individualni $\Omega(D)$ je vektorski prostor nad k, pa imamo za $\omega \in \Omega(D)$ da je $a\omega \in \Omega(D)$ za skalare $a \in k$. Dakle Ω_F je zatvoren na množenje elementima iz k. Zaključujemo da je Ω_F vektorski potprostor od $\mathcal{A}'$ nad k. □

Ispada da je Ω također i vektorski prostor nad F! Ako je $f \in F, \omega \in \Omega$, $f \cdot \omega$ je definiran kao funkcional iz $\mathcal{A}'$ koji djeluje na $\mathcal{A}$ sa $(f \cdot \omega)(\alpha) = \omega(f\alpha)$. Uistinu je $1 \cdot \omega = \omega$ i vrijede potrebni aksiomi vektorskih prostora:

$$\begin{aligned}
(f(\omega_1 + \omega_2))(\alpha) &= (\omega_1 + \omega_2)(f\alpha) = \omega_1(f\alpha) + \omega_2(f\alpha) = (f\omega_1)(\alpha) + (f\omega_2)(\alpha),\\
((f_1 + f_2)\omega)(\alpha) &= \omega((f_1 + f_2)\alpha) = \omega(f_1\alpha) + \omega(f_2\alpha) = (f_1\omega)(\alpha) + (f_2\omega)(\alpha),\\
((f_1 f_2)\omega)(\alpha) &= \omega(f_1 f_2\alpha) = (f_1\omega)(f_2\alpha) = (f_2(f_1\omega))(\alpha).
\end{aligned}$$

Teorem 3.3.3. *Neka je F/k funkcijsko polje i Ω_F prostor Weilovih diferencijala. Tada je* $\dim_F \Omega = 1$.

Dokaz. Vidi Teorem 85 u [4]. □

Po definiciji je $\Omega = \bigcup_{D \in \mathrm{Div}_k F} \Omega(D)$. Za neki $\omega \in \Omega$, $\omega \neq 0$ imamo da je $\omega \in \Omega(D) \iff \mathcal{A}(D) + F \subseteq \ker \omega$. Ako definiramo

$$M(\omega) := \{D \in \mathrm{Div}_k(F) : \mathcal{A}(D) + F \subseteq \ker \omega\},$$

ispostavlja se da vrijedi:

Lema 3.3.4. *Postoji jedinstven divizor $D_\omega \in M(\omega)$ takav da $D \leq D_\omega$ za sve $D \in M(\omega)$.*

Dokaz. Fiksirajmo neki $\omega \in \Omega$, $\omega \neq 0$. Tada je $\omega \in \Omega(D)$ za neki D, pa $D \in M(\omega)$ što znači $M(\omega) \neq \emptyset$. Dokazat ćemo da $M(\omega)$ ima jedinstven maksimalni element s obzirom na parcijalni uređaj $\leq$ (definiran na divizorima). To je dovoljno jer je jedinstveni maksimalni element nužno i najveći ako postoji.

Prvo pokažimo da maksimalni element postoji. Riemannov teorem nam kaže da $\exists c \in \mathbb{N}$ takav da $\deg D \geq c \implies i(D) = 0$. Za takav D je $\mathcal{A}(D) + F = \mathcal{A}$. S obzirom da $\omega \neq 0$, imamo da $\mathcal{A} \nsubseteq \ker\omega$ pa $\mathcal{A}(D) + F \nsubseteq \ker\omega \implies D \notin M(\omega)$. Dakle c je gornja ograda na skup $\{\deg D : D \in M(\omega)\}$. To znači da postoji $D \in M(\omega)$ koji maksimizira $\deg D$ i taj element je očito maksimalan u $M(\omega)$ s obzirom na $\leq$.

Sada dokažimo jedinstvenost. Pretpostavimo da postoje različiti maksimalni elementi $D_1, D_2 \in M(\omega)$. Tada $D_2 \not\leq D_1$ povlači da postoji Q za koji $v_Q(D_2) > v_Q(D_1)$. Tvrdimo da je $D_1 + Q \in M(\omega)$. Neka je dakle $\alpha \in \mathcal{A}(D_1 + Q)$. Definiramo $\alpha', \alpha'' \in \mathcal{A}$ sa

$$\alpha'_P := \begin{cases} \alpha_P & \text{za } P \neq Q \\ 0 & \text{za } P = Q \end{cases} \quad \text{i} \quad \alpha''_P = \begin{cases} 0 & \text{za } P \neq Q \\ \alpha_P & \text{za } P = Q \end{cases}.$$

Vidimo da su $\alpha' \in \mathcal{A}(D_1)$, $\alpha'' \in \mathcal{A}(D_2)$ i $\alpha = \alpha_1 + \alpha_2$. Sada je $\omega(\alpha) = \omega(\alpha_1) + \omega(\alpha_2) = 0$. Dakle $\mathcal{A}(D_1 + Q) \subseteq \ker\omega$. S obzirom da je $F \subseteq \ker\omega$, imamo i $\mathcal{A}(D_1 + Q) + F \subseteq \ker\omega \implies D_1 + Q \in M(\omega)$. To je kontradikcija s maksimalnošću od D_1. □

Gornji teorem nam pokazuje da postoji prirodan način da svakom nenul diferencijalu ω pridružimo divizor. Označimo to sa $\operatorname{div}\omega := D_\omega$.

Definicija 3.3.5. Neka je C/k krivulja i F/k njeno funkcijsko polje. Divizore $D \in Div_k C$ koji su oblika $D = \operatorname{div}\omega$ za neki $\omega \in \Omega_F$ nazivamo *kanonski divizori*.

Lema 3.3.6. *Za $0 \neq f \in F$ i $0 \neq \omega \in \Omega_F$ imamo*

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

Dokaz. Uočimo prvo da je $\alpha \in \mathcal{A}(D) \iff f\alpha \in \mathcal{A}(D - \operatorname{div} f)$.

Zaista $\alpha \in \mathcal{A}(D) \iff v_P(\alpha_P) \geq -v_P(D),\ \forall P \iff v_P(f\alpha) \geq -v_P(D) + v_P(F),\ \forall P \iff f\alpha \in \mathcal{A}(D - \operatorname{div} f)$. Sada imamo

$$\begin{aligned} D \in M(f\omega) &\iff (f\omega)(\alpha) = \omega(f\alpha) = 0,\ \forall \alpha \in \mathcal{A}(D) \\ &\iff \omega(\beta) = 0,\ \forall \beta \in \mathcal{A}(D - \operatorname{div} f) \\ &\iff D - \operatorname{div} f \in M(\omega). \end{aligned}$$

Napomenimo da se $\operatorname{div}\omega$ i $\operatorname{div} f\omega$ mogu redom okarakterizirati kao elementi najvećeg stupnja u $M(\omega)$ i $M(f\omega)$. Nadalje $\deg(D - \operatorname{div} f) = \deg D$. Zato imamo $\operatorname{div}\omega = \operatorname{div} f\omega - \operatorname{div} f \implies \operatorname{div}(f\omega) = \operatorname{div} f + \operatorname{div}\omega$. □

Teorem 3.3.3 i Lema 3.3.6 pokazuju da kanonski divizori čine klasu ekvivalencije u $\mathrm{Div}_k C$ s obzirom na $\sim$. Odgovarajući element u $\mathrm{Pic}_k C$ koji se sastoji od kanonskih divizora nazivamo *kanonska klasa*.

Računanje kanonskog divizora

Za krivulju C/k možemo na njoj definirati diferencijalne forme. One su srodne Weilovim diferencijalima Ω_F, a nama su korisne jer pružaju način da eksplicitno izračunamo kanonski divizor. Sljedeće tvrdnje navodimo iz $II.4$ [7].

Sljedeća definicija je formalna i simbol dx neće imati nikakvo drugo značenje.

Definicija 3.3.7. Neka je C krivulja. *Prostor diferencijalnih formi* na C, s oznakom Ω_C je $\bar{k}$-vektorski prostor generiran simbolima dx za $x \in \bar{k}(C)$ koji zadovoljavaju relacije:

1. $d(x+y) = dx + dy, \quad \forall x, y \in \bar{k}(C)$
2. $d(xy) = xdy + ydx, \quad \forall x, y \in \bar{k}(C)$
3. $da = 0, \quad \forall a \in \bar{k}.$

Propozicija 3.3.8. *Neka je C krivulja, $P \in C(\bar{k})$ i $t \in \bar{k}(C)$ je uniformizator u P. Vrijedi:*

(i) Ω_C *je* 1*-dimenzionalni* $\bar{k}$*-vektorski prostor.*

(ii) Za sve $\omega \in \Omega_C$ *postoji jedinstvena funkcija* $g \in \bar{k}(C)$ *takva da*

$$\omega = gdt.$$

Označavamo g *sa* ω/dt*.*

(iii) $v_P(\omega/dt)$ *ne ovisi o izboru uniformizatora, pa označavamo* $v_P(\omega) := v_P(\omega/dt)$*.*

(iv) Ako je $f \in \bar{k}(C)$ *regularna u* P*, onda je* df/dt *regularna u* P*.*

(v) Ako je $v_P(f) \neq 0$*, onda* $v_P(df) = v_P(f) - 1$*.*

(vi) Za $\omega \in \Omega_C$*,* $\omega \neq 0$ *vrijedi* $v_P(\omega) = 0$ *za sve osim konačno* $P \in C(\bar{k})$*. Dakle ima smisla definirati* $\operatorname{div}\omega := \sum v_P(\omega)P$*. Tada je* $\operatorname{div}\omega$ *kanonski divizor (isti kao u Definiciji 3.3.5).*

Upravo ovo zadnje svojstvo ćemo upotrijebiti za računanje kanonskog divizora. Pogledajmo primjer.

Primjer 3.3.9. Neka je krivulja C projektivno zatvorenje afine krivulje $C_a : y^2 = x^3 - 4x$ definirane nad $\bar{\mathbb{Q}}$. C ima točno jednu točku $(0 : 1 : 0)$ koja nije prikaziva u afinim koordinatama i nju označimo sa ∞. Označimo i $P_1 := (-2, 0)$, $P_2 := (0, 0)$, $P_3 := (2, 0)$. Izračunajmo prvo $\operatorname{div} y$. Za $F(x, y) := y^2 - x^3 + 4x$ imamo $\nabla F = \left[-3x^2 + 4, 2y\right]$, dakle $\partial_x F \neq 0$ u P_1, P_2, P_3 pa je y uniformizator u tim točkama. Očito su to sve nultočke od y, pa iz $\deg \operatorname{div} y = 0$ zaključujemo da y ima pol stupnja 3 u ∞. Dakle

$$\operatorname{div} y = P_1 + P_2 + P_3 - 3\infty.$$

Izračunajmo $\operatorname{div} x$. Jedina afina nultočka od x je očito P_2, te $x = \frac{1}{x^2-4} y^2$ gdje $\frac{1}{x^2-4} \in \mathcal{O}_{P_2}^\times$ dakle $v_{P_2}(x) = v_{P_2}(y^2) = 2$. Ponovno $\deg \operatorname{div} f$ dakle

$$\operatorname{div} x = 2P_2 - 2\infty.$$

Neka je sada $\omega := dx$. Izračunat ćemo njegov diferencijal. Imamo dakle $v_P(\omega) = v_P(x) - 1$ za $P = \infty$ i $P = P_2$, pa $v_{P_2}(\omega) = 1$ i $v_\infty(\omega) = -3$. Neka je $P = (x_0, y_0)$ afina točka sa $y_0 \neq 0$. Tada je $\partial_y F(P) \neq 0$ pa je $x - x_0$ uniformizator u P. Iz svojstva diferencijala je $\omega = dx = d(x - x_0)$. Dakle $v_P(\omega) = 0$. Preostaje odrediti valuaciju za točke P_1, P_3 (imaju y koordinatu 0). Imamo

$$2ydy = d(y^2) = d(x^3 - 4x) = (3x^2 - 4)dx \implies \omega = \frac{2y}{3x^2 - 4} dy.$$

Sad je $v_{P_1}(\omega) = v_{P_1}(\frac{2y}{3x^2-4}) = 1$ gdje smo koristili da je y uniformizator u P_1. Potpuno analogno $v_{P_2}(\omega) = 1$. Konačno, zaključujemo

$$\operatorname{div} \omega = P_1 + P_2 + P_3 - 3\infty.$$

Dakle u ovom slučaju je $\operatorname{div} dx = \operatorname{div} y$ što znači da su kanonski divizori točno jednaki glavnim divizorima (ili 0 u $\operatorname{Pic}_k C$).

Ispostavlja se da je C iz gornjeg primjera krivulja genusa 1, i za takve općenito vrijedi da se kanonski divizori podudaraju s glavnim divizorima. To ćemo precizno dokazati kasnije u Propoziciji 3.5.10.

Primjer 3.3.10. Neka je $\mathbb{P}^1/\bar{\mathbb{Q}}$ projektivni pravac. Imamo $\mathbb{P}^1 = \mathbb{A}^1 \cup (1 : 0)$. Označimo $\infty := (1 : 0)$. Nije teško provjeriti da funkcija $x \in k(\mathbb{P}^1) = k(x)$ ima divizor

$$\operatorname{div} x = (0 : 1) - \infty.$$

Neka je $\omega := dx$. Zaključujemo da je $v_0(\omega) = v_0(x) - 1 = 0$ i $v_\infty(\omega) = v_\infty(x) - 1 = -2$. Ako je $P = (a : 1)$ točka sa $a \neq 0$, imamo da je $x - a$ uniformizator u P. Tada je $\omega = dx = d(x - a)$ i stoga je $v_P(\omega) = 0$. Zaključujemo

$$\operatorname{div} \omega = \operatorname{div} dx = -2\infty.$$

U ovom slučaju kanonski divizor nije glavni, uistinu imamo $\deg \operatorname{div} \omega = -2$.

3.4 Riemann-Rochov teorem

Teorem 3.4.1 (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. Imamo da je $\operatorname{div}(f\omega) = \operatorname{div} f + \operatorname{div}\omega \geq D - W + \operatorname{div}\omega = D$. Iz $D \leq \operatorname{div}(f\omega)$, slijedi da je $f\omega \in \Omega(D)$. Naime, imamo da je $\mathcal{A}(D) + F \subseteq \mathcal{A}(\operatorname{div}(f\omega)) + F \subseteq \ker(f\omega) \implies f\omega \in \Omega(D)$. Zaključujemo da je linearno preslikavanje ϕ dobro definirano. Nadalje, ϕ je injektivno zato što je Ω vektorski prostor nad F, pa imamo $f_1\omega = f_2\omega \implies f_1 = f_2$. Pokažimo da je ϕ surjekcija. Ako je $0 \neq \omega' \in \Omega(D)$, iz Teorema 3.3.3 slijedi da je $\omega' = f\omega$ za neki $f \in F$. Sada računamo

$$\operatorname{div}(f\omega) = \operatorname{div} f + W = \operatorname{div}(\omega') \geq D$$

gdje zadnja nejednakost vrijedi zbog $\omega' \in \Omega(D)$. Odmah dobivamo $\operatorname{div} f \geq D - W \implies f \in L(W - D)$. Konačno $\phi(f) = \omega'$, dakle ϕ je surjekcija.

Zaključujemo da je ϕ izomorfizam. Za kraj $l(W - D) = \dim_k \Omega(D) = i(D)$. □

Teorem 3.4.2 (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. Po definiciji od i imamo $l(D) = \deg D + 1 - g + i(D)$. Konačno, prethodni teorem nam daje $i(D) = l(W - D)$. □

3.5 Posljedice Riemann-Rochovog teorema

Korolar 3.5.1 (Svojstva kanonskog divizora)**.** *Neka je C/k krivulja. Vrijedi*

1. *Za kanonski divizor W je $\deg W = 2g - 2$, $l(W) = g$, $i(W) = 1$.*

2. *Ako je $D \in \operatorname{Div}_k C$ takav da $\deg D = 2g - 2$ i $l(D) \geq g$, tada je D kanonski divizor.*

Dokaz.

1. Uvrštavanjem $D = 0$ u Teorem 3.4.2, dobijemo $l(0) = \deg 0 + 1 - g + l(W) \implies l(W) = g$. Sada uvrštavanjem $D = W$, dobijemo $l(W) = \deg W + 1 - g + l(0) \implies \deg W = 2g - 2$. Konačno $i(W) = g - 1 - \deg W + l(W) = 1$.

2. Teorem 3.4.2 nam daje $l(W-D) = g - 1 - \deg D + l(D) \geq g - 1 - 2g + 2 + g = 1$. Imamo da je $\deg W - D = 0$, pa iz Leme 3.1.7 slijedi da je $W - D$ glavni divizor. To znači da je $D \sim W$ kanonski.

□

Podsjetimo se da Riemannov teorem tvrdi da svi divizori dovoljno velikog stupnja imaju indeks specijalnosti 0. Riemann-Rochov teorem nam daje precizno koliko velik taj stupanj mora biti. Nadalje, ograda u sljedećem teoremu je oštra jer za kanonski divizor W imamo $i(W) = 1 \neq 0$ i $\deg W = 2g - 2$.

Teorem 3.5.2. *Neka je C/k krivulja i $D \in \mathrm{Div}_k C$ takav da $\deg D \geq 2g - 1$. Vrijedi*

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

Ekvivalentno, vrijedi $i(D) = 0$.

Dokaz. Riemann-Rochov teorem nam daje $l(D) = \deg D + 1 - g + l(W - D)$. Imamo $\deg W - D \leq 2g - 2 - 2g + 1 < 0$, dakle $l(W - D) = 0$. □

Propozicija 3.5.3. *Neka je P zatvorena točka na krivulji C/k. Za svaki $n \geq 2g$, postoji funkcija $f \in k(C)$ takva da je $\mathrm{div}_\infty f = nP$.*

Dokaz. Primijetimo da se $L(mP)$ općenito sastoji od funkcija koje su regularne svugdje osim što u P mogu imati pol reda najviše m. Zato je dovoljno pokazati da postoji neka funkcija $f \in L(nP) \setminus L((n-1)P)$, ili ekvivalentno $L((n-1)P) \subsetneq L(nP)$. Vrijedi $\deg(n-1)P = (n-1)\deg P \geq 2g - 1$, dakle po prethodnom teoremu je $l((n-1)P) = \deg(n-1)P + 1 - g$. Slično $\deg nP \geq 2g-1 \implies l(nP) = \deg P + 1 - g$. Zaključujemo da je $l(nP) - l((n-1)P) = \deg P > 0$. Dakle stvarno $L((n-1)P) \neq L(nP)$. □

Teorem 3.5.4. *Neka je C/k krivulja koja ima k-racionalnu točku. Tada C ima genus 0 ako i samo ako je izomorfna s $\mathbb{P}^1/k$.*

Dokaz. Neka je $P \in C(k)$. Ako C ima genus 0, iz Propozicije 3.5.3 slijedi da $\exists f \in k(C)$ takva da $\mathrm{div}_\infty f = P$. Teorem 2.2.15 nam sada daje $[k(C) : k(f)] = \deg \mathrm{div}_\infty f = 1$, dakle $k(C) = k(f) \simeq k(\mathbb{P}^1)$. S obzirom da je kategorija funkcijskih polja ekvivalentna kategoriji krivulja (nad k), slijedi da je $C/k \simeq \mathbb{P}^1/k$.

Obratno, neka je $C/k \simeq \mathbb{P}^1/k$. Tada je $k(C) \simeq k(x)$. Funkcija x je regularna svugdje osim u ∞, gdje ima pol reda 1. Za $n \in \mathbb{N}$ su $1, x, \ldots, x^n \in L(n\infty)$ i nadalje $1, \ldots, x^n$ su nezavisni nad k. Dakle

$$n + 1 \leq l(n\infty) = \deg n\infty + 1 - g + l(W - n\infty) = n + 1 - g + l(W - n\infty).$$

Zaključujemo da je $g \leq l(W - n\infty)$. Za dovoljno velike n je $\deg W - n\infty < 0$ i stoga imamo $l(W - n\infty) = 0$. Konačno $g \leq 0 \implies g = 0$. □

Lema 3.5.5. *Neka je ϕ automorfizam od $\mathbb{P}^1$ koji fiksira barem 3 točke u $\mathbb{P}^1(\bar{k})$. Tada je ϕ identiteta.*

Dokaz. Bez gubitka općenitosti pretpostavimo da ϕ fiksira točku ∞ (inače linearnom transformacijom možemo premjestiti neku fiksnu točku od ϕ u ∞). Restrikcija od ϕ na $\mathbb{A}^1 = \mathbb{P}^1 \setminus \{\infty\}$ je bijekcija i ujedno morfizam afinih krivulja. Tu restrikciju označimo sa ϕ_a, onda je $\phi_a \in k[x]$, te $\deg \phi_a = 1$ jer je ϕ_a automorfizam. Dakle $\phi_a(x) = x$ ima barem dva različita rješenja. S obe strane su linearni polinomi što znači da se podudaraju, tj. ϕ_a je identiteta. Tada je i ϕ identiteta. □

Eliptičke krivulje

Teorem 3.5.6. *Neka je C/k krivulja koja ima k-racionalnu točku. Tada C ima genus 1 ako i samo ako je izomorfna glatkoj krivulji oblika*

$$C' : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{3.4}$$

Dokaz. Neka je C/k genusa 1 i $P \in C(k)$. Za $n \in \mathbb{N}$, imamo $\deg nP = n \geq 2g - 1 = 1$. Dakle iz Teorema 3.5.2 slijedi da je $l(nP) = \deg nP + 1 - g = n$.

Imamo da je $l(P) = l(0) = 1$, dakle $\{1\}$ je baza za vektorski prostor $L(P) = L(0) = k$.

Vrijedi $l(2P) = 2$ pa postoji $x \in L(2P) \setminus L(P)$. Sada je $\{1, x\}$ baza za $L(2P)$. Slično je $l(3P) = 3$ dakle $\exists y \in L(3P) \setminus L(2P)$, te je $\{1, x, y\}$ baza za $L(3P)$. Očito je $v_P(x) = 2$ i $v_P(y) = 3$. Sada

$$x^2 \in L(4P) \setminus L(3P) \implies \{1, x, y, x^2\} \text{ je baza za } L(4P)$$
$$xy \in L(5P) \setminus L(4P) \implies \{1, x, y, x^2, xy\} \text{ je baza za } L(5P)$$

Nastavljajući postupak, dobijemo dvije različite baze za $L(6P)$. Naime x^3 i y^2 su oboje u $L(6P) \setminus L(5P)$, stoga su $\{1, x, y, x^2, xy, x^3\}$ i $\{1, x, y, x^2, xy, y^2\}$ dvije baze. Zaključujemo da su $1, x, y, x^2, xy, x^3, y^2$ linearno zavisne nad k pa imamo

$$ax^3 + by^2 + cxy + dx^2 + ey + fx + g = 0 \tag{3.5}$$

za neke koeficijente $a, \ldots, g$ iz k koji nisu svi 0. Ako je $a = 0$, onda su svi ostali koeficijenti također jednaki 0 zbog linearne nezavisnosti. Zaključujemo da je $a \neq 0$ i slično $b \neq 0$. Ako sad zamijenimo x sa abx i y sa a^2by, jednadžba (3.5) nakon dijeljenja s a^4b^3 prelazi u oblik (3.4).

Obratno, neka je C/k glatka krivulja zadana jednadžbom (3.4). Tada je $P := (0 : 1 : 0) \in C(k)$. Funkcija $X := (x : y : z) \mapsto (x : z)$ za $z \neq 0$, $P \mapsto \infty$ je funkcija stupnja $[k(C) : k(x)]$. U afinim koordinatam, y je nultočka polinoma stupnja 2 nad $k(x)$ tj.

$$y^2 + (a_1x + a_3)y - (x^3 + a_2x^2 + a_4x + a_6) = 0.$$

Po definiciji, krivulja je mnogostrukost pa ta jednadžba mora biti ireducibilna nad $k(x)$ i stoga je $[k(C) : k(x)] = 2$. Iz Teorema 2.2.15, dobivamo $\deg \mathrm{div}_\infty X = 2$. Uočimo da X ima pol samo u P, pa je $\mathrm{div}_\infty X = 2P$. Analognim argumentom, za funkciju $Y := (x : y : z) \mapsto (y : z)$ zaključujemo $\mathrm{div}_\infty Y = 3P$. Sada je $v_P(X^iY^j) = 2i + 3j$. Za $n \geq 2$ je moguće odabrati $i, j \in \mathbb{N}_0$ takve da $2i + 3j = n$. Tada $X^iY^j \in L(nP) \setminus L((n-1)P) \implies l(nP) \geq l((n-1)P) + 1$. Indukcijom slijedi da je $l(nP) \geq (n-1) + l(P)$ za sve $n \geq 2$. Vrijedi $l(P) \geq l(0) = 1$, dakle $l(nP) \geq n$. Iz Riemannovog teorema slijedi da za dovoljno velike n, vrijedi $i(nP) = 0$. Dakle

$$n \leq l(nP) = \deg nP + 1 - g = n + 1 - g \implies g \leq 1.$$

Preostaje provjeriti da genus od C nije 0. Pokazat ćemo dokaz u slučaju kada je $\mathrm{char}\, k \neq 2$. Pretpostavimo suprotno da je $g = 0$. Iz Teorema 3.5.4 imamo da je $C \simeq \mathbb{P}^1/k$. Definirajmo morfizam $\phi : C \mapsto C$ sa

$$(x : y : z) \mapsto (x : -y - a_1x - a_3z : z).$$

Tada je ϕ definiran nad k, te je ϕ očito involucija pa je sam sebi inverz, iz čega slijedi da je automorfizam. Za $\mathbb{A}^2 = \{(* : * : 1)\} \subseteq \mathbb{P}^2$, lako provjerimo (uvrstimo $z = 0$ u (3.4)) da je $P = (0 : 1 : 0)$ jedina točka u skupu $C(\bar{k}) \setminus (C \cap \mathbb{A}^2)(\bar{k})$. Automorfizam ϕ fiksira P, pa je restrikcija $\phi_a : C \cap \mathbb{A}^2 \to C \cap \mathbb{A}^2$ također automorfizam. U afinim koordinatama imamo:

$$C \cap \mathbb{A}^2 : F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0, \tag{3.6}$$

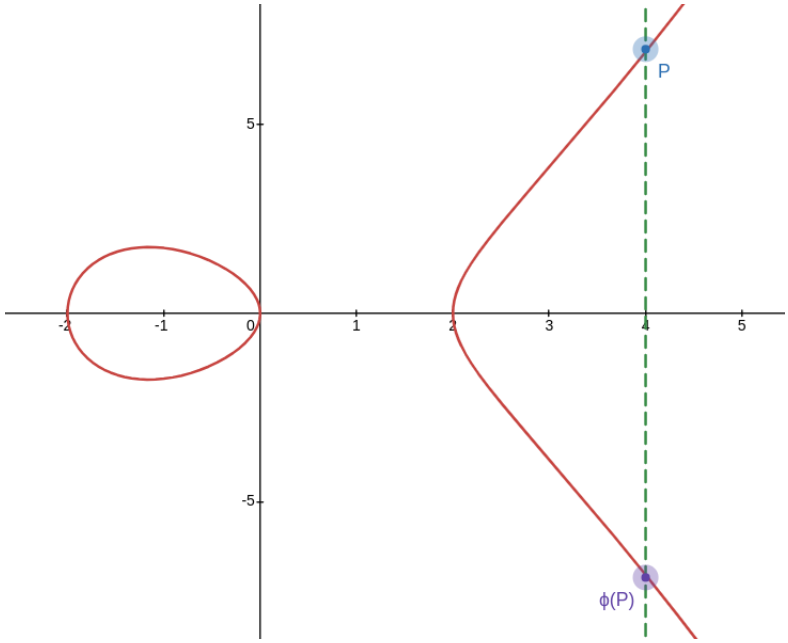
$$\phi_a(x, y) = (x, -y - a_1x - a_3). \tag{3.7}$$

Cilj nam je pronaći fiksne točke od ϕ_a, zato uvrstimo $y = (-a_1x - a_3)/2$ u (3.6). To nam daje kubnu jednadžbu

$$p(x) := x^3 + a_2x^2 + a_4x + a_6 + \frac{(a_1x + a_3)^2}{4} = 0. \tag{3.8}$$

Lako se provjeri da za $y = (-a_1x - a_3)/2$, vrijedi $\partial_y F(x, y) = 0$. Nadalje $\partial_x F(x, y) = -p'(x)$, pa iz glatkoće od C, imamo da je $p'(x) \neq 0$ (Napomena 1.1.32) za sve $(x, y) \in (C \cap \mathbb{A}^2)(\bar{k})$ takve da $y = (-a_1x - a_3)/2$. To znači da p nema ponovljene nultočke, tj. ima tri različite nultočke u $\bar{k}$. Zaključujemo da ϕ fiksira točno 4 točke: jedna je $P = (0 : 1 : 0)$, ostale 3 su u $C \cap \mathbb{A}^2$ i x koordinate im zadovoljavaju (3.8). Iz Leme 3.5.5 slijedi da je ϕ identiteta dakle fiksira sve točke iz $C(\bar{k})$. To je kontradikcija s činjenicom da fiksira točno 4. Zaključujemo da C nije genusa 0. □

Definicija 3.5.7. Krivulju C/k genusa 1 zajedno s istaknutom k-racionalnom točkom od C nazivamo *eliptička krivulja*.



Slika 3.1: Vizualizacija automorfizma ϕ za krivulju $C : y^2 = x^3 - 4x$ nad $\mathbb{R}$. U ovom slučaju automorfizam je refleksija preko x osi i fiksne točke su $(0,0), (-2,0), (2,0), \infty$.

Jednadžba (3.4) se naziva *Weierstrassova jednadžba eliptičke krivulje*. Teorem 3.5.6 tada tvrdi da je svaka eliptička krivulja izomorfna nekoj krivulji koja je zadana Weierstrassovom jednadžbom. Bitna činjenica je da k-racionalne točke eliptičke krivulje čine abelovu grupu. Sljedeći teorem precizno opisuje grupovnu operaciju.

Teorem 3.5.8. *Neka je E/k eliptička krivulja i $O \in E(k)$ istaknuta k-racionalna točka. Preslikavanje*

$$\begin{aligned} \Phi : E(k) &\to \mathrm{Pic}^0_k E \\ P &\mapsto [P - O] \end{aligned}$$

inducira 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. Dovoljno je dokazati:

1. Preslikavanje Φ je injektivno.

2. Slika preslikavanje $\operatorname{Im}\Phi$ je podgrupa od $\operatorname{Pic}_k^0 E$.

Za injektivnost, pretpostavimo da je $\Phi(P) = \Phi(Q)$. Tada je $[P] = [P - O] + [O] = [Q - O] + [O] = [Q] \implies P \sim Q$ kao divizori. Dakle za neki $f \in k(E)^\times$ je $Q = \operatorname{div} f + P$ ili ekvivalentno $\operatorname{div} f = Q - P$. Pretpostavimo da je $P \neq Q$. Iz Teorema 2.2.15 imamo $[k(E) : k(f)] = \deg \operatorname{div}_\infty f = 1$ pa $k(E) = k(f) \simeq k(\mathbb{P}^1) \implies E/k \simeq \mathbb{P}^1/k$. To je kontradikcija jer je $\mathbb{P}^1$ genusa 0, a E genusa 1, dakle ne mogu biti izomorfne. Zaključujemo $P = Q$, tj. Φ je injektivno.

Neka su $P_1, P_2 \in E(k)$. Definiramo $D := P_1 + P_2 - O$. Tada je $\deg D = 1 \geq 2g - 1$, pa Teorem 3.5.2 daje $l(D) = \deg(D) + 1 - g = 1$. Sada $l(D) \neq 0 \implies D \sim D'$ za neki divizor $D' \geq 0$. Vrijedi $\deg D' = \deg D = 1$, stoga je D' nužno oblika $\deg D' = Q$ za neku točku $Q \in E(k)$. Sada

$$P_1 + P_2 - O \sim Q \implies [P_1 + P_2 - O] = [Q] \implies [P_1 - O] + [P_2 - O] = [Q - O].$$

To znači $\Phi(P_1) + \Phi(P_2) = \Phi(Q)$, dakle $\operatorname{Im}\Phi$ je zatvorena na zbrajanje, pa je podgrupa od $\operatorname{Pic}_k^0 E$. □

Napomena 3.5.9. Neka je eliptička krivulja dana sa Weierstrassovom jednadžbom $E/k : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ i neka je $O = \infty = (0 : 1 : 0) \in E(k)$ istaknuta. Za točke $P_1 = (x_1, y_1) \in E(k)$ i $P_2 = (x_2, y_2) \in E(k)$, njihov zbroj $P_3 = P_1 + P_2 = (x_3, y_3)$ je određen s:

$$\lambda := \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} - a_1, & \text{ako } P_1 \neq P_2 \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & \text{ako } P_1 = P_2 \end{cases}$$

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \quad y_3 = -y_1 - a_1x_3 - a_3 + \lambda(x_1 - x_3)$$

Specijalno, ako je P_1 ili P_2 jednaka O, tada je $P_1 + P_2$ jednaka drugoj točki, a ako je $P_2 = (x_1, -y_1 - a_1x_1 - a_3)$, tada je $P_1 + P_2 = O$.

Propozicija 3.5.10. *Neka je C/k krivulja genusa* 1. *Tada je kanonski divizor W ujedno i glavni divizor.*

Dokaz. Ustanovili smo da je $l(W) = g = 1$ i $\deg W = 2g - 2 = 0$. Iz Leme 3.1.7 slijedi da je W glavni divizor. □

Specijalni divizori

Podsjetimo se da su specijalni divizori oni za koje je $i(D) \neq 0$. Posljedica Riemann-Rochovog teorema je da $\deg D \geq 2g - 1 \implies i(D) = 0$. Dakle svi specijalni divizori su stupnja najviše $2g - 2$. Konkretno, ako je C/k krivulja i $P \in C(k)$ neka točka, imamo

$l(nP) = n+1-g$ za $n \geq 2g-1$. Tada, ako je $n \geq 2g$ uvijek postoji neka $f \in L(nP)\backslash L((n-1)P)$ i za nju je $\mathrm{div}_\infty f = nP$, kao što smo dokazali u Propoziciji 3.5.3.

Vrijednosti $n \in \mathbb{N}$ takve da $\exists f \in k(C)^\times$ za koju $\mathrm{div}_\infty f = nP$ nazivamo *polni brojevi* od P. U suprotnom, ako za n takva funkcija ne postoji, kažemo da je *broj raskoraka* od P.

Teorem 3.5.11 (Weierstrassov teorem o brojevima raskoraka)**.** *Neka je C/k krivulja genusa $g > 0$, te $P \in C$ točka. Tada postoji točno g brojeva raskoraka $i_1 < i_2 < \ldots < i_g$ od P, te je*

$$i_1 = 1, \quad i_g \leq 2g - 1.$$

Dokaz. Uočimo da je n broj raskoraka od P ako i samo ako $l(nP) = l((n-1)P)$. Jer inače, ako je $l(nP) > l((n-1)P)$, onda za funkcije $f \in L(nP) \setminus L((n-1)P)$ vrijedi $\mathrm{div}_\infty f = nP$. Vrijedi $l((2g-1)P) = g$ jer je $\deg(2g-1)P \geq 2g-1$, pa je po Teoremu 3.5.2 $i((2g-1)P) = 0$, iz čega lako izračunamo $l((2g-1)P) = g$. Sad je

$$g - 1 = l((2g-1)P) - l(0) = \sum_{n=1}^{2g-1} l(nP) - l((n-1)P).$$

Iz Leme 3.1.4 imamo da je $l(nP) - l((n-1)P) \leq \deg P = 1$, dakle svaki sumand desno ima vrijednost $l(nP) - l((n-1)P) \in \{0, 1\}$. Zaključujemo da je $l(nP) - l((n-1)P) = 1$ za točno $g-1$ različitih sumanada, pa je $l(nP) - l((n-1)P) = 0$ za ostalih $2g - 1 - (g-1) = g$ vrijednosti od n. Tih g vrijednosti su točno brojevi raskoraka od P. □

Napomenimo još da se "tipično" brojevi raskoraka nalaze najviše lijevo. Tj. niz $l(P), l(2P), \ldots$ je oblika

$$\underbrace{1, 1, \ldots, 1}_{g \text{ puta}}, 2, 3, \ldots$$

Takve P za koje $i_k = k$, $k = 1, \ldots, g$ nazivamo *ne-Weierstrassove* točke od C. Točke koje nisu ne-Weierstrassove su *Weierstrassove*.

Sljedeći teorem nam daje dodatnu restrikciju na pozicije brojeva raskoraka.

Teorem 3.5.12 (Cliffordov teorem o specijalnim divizorima)**.** *Za svaki divizor D takav da je $0 \leq \deg D \leq 2g - 2$ vrijedi*

$$l(D) \leq 1 + \frac{1}{2} \deg D \tag{3.9}$$

Dokaz. Dokazat ćemo teorem u slučaju kada je k beskonačno polje. Primijetimo prvo da vrijedi

$$l(D) \leq 1 + \frac{1}{2} \deg D \iff l(W - D) \leq 1 + \frac{1}{2} \deg(W - D). \tag{3.10}$$

Pokažimo "⇐", drugi smjer je analogan. Iz Riemann-Rocha imamo

$$l(D) = \deg D + 1 - g + l(W - D) \leq \deg D + 1 - g + 1 + \frac{1}{2}\deg(W - D) = 1 + \frac{1}{2}\deg D,$$

gdje smo koristili $l(W - D) \leq 1 + \frac{1}{2}\deg(W - D)$ za nejednakost, i u zadnjoj jednakosti smo upotrijebili $\deg(W - D) = 2g - 2 - \deg D$ (jer $\deg W = 2g - 2$). To dokazuje (3.10).

Dokažimo teorem indukcijom po $\deg D$. Za $\deg D = 0$, imamo $l(D) \in \{0, 1\}$ gdje vrijednost ovisi o tome je li D glavni divizor ili nije, pa je nejednakost očito istinita. Pretpostavimo sada da nejednakost (3.9) vrijedi za sve $\deg D < d$. Fiksirajmo neki $D \in \mathrm{Div}_k C$ takav da $\deg D = d \leq 2g - 2$. Ako je $l(D) = 0$ teorem očito vrijedi pa pretpostavimo $l(D) \neq 0$. Na temelju (3.10) pretpostavimo i $l(W - D) \neq 0$. Sada je $D \sim A$ i $(W - D) \sim B$ za neke efektivne divizore $A, B \geq 0$. Divizor $W' := A + B$ je kanonski ($W' \sim W$). Ako za neku zatvorenu točku P vrijedi $L(A) = L(A - P)$, onda iz pretpostavke indukcije dobijemo još bolju ogradu nego što je traženo na $l(D) = l(A) = l(A - P)$ jer je $\deg(A - P) < d$. Pretpostavimo dakle $L(A) \neq L(A - P),\ \forall P$. Postoji funkcija $g \in L(A)$ takva da $g \notin L(A - P)$ za sve $P \leq B$. Tu smo iskoristili pretpostavku da je k beskonačno polje, jer u tom slučaju vektorski prostor nad k nije konačna unija pravih potprostora. Definiramo linearno preslikavanje

$$\begin{aligned} \varphi : L(B) &\to L(W')/L(A) \\ f &\mapsto [fg]. \end{aligned}$$

Uočimo da $\mathrm{div}\, f \geq -B$ i $\mathrm{div}\, g \geq -A$ povlači $\mathrm{div}(fg) \geq -A - B = -W'$, pa je $fg \in L(W')$ i linearno preslikavanje φ je dobro definirano. Odredimo mu sada jezgru. Ako je $\varphi(f) = 0$, $f \neq 0$, onda $fg \in L(A) \implies v_P(f) + v_P(g) \geq -v_P(A),\ \forall P$. Specifično za P takve da $P \leq B$, po definiciji od g imamo $v_P(g) = -v_P(A) \implies v_P(f) \geq 0$. Za sve ostale P, iz $f \in L(B)$ slijedi $v_P(f) \geq -v_P(B) = 0$. Zaključujemo da je $\mathrm{div}\, f \geq 0 \implies \mathrm{div}\, f = 0 \implies f \in k^\times$. Konačno $\ker\varphi = L(0)$. Iz prvog teorema o izomorfizmu imamo

$$L(B)/L(0) \cong \mathrm{Im}\,\varphi \subseteq L(W')/L(A).$$

To nam daje $l(B) - 1 \leq l(W') - l(A)$ ili ekvivalentno $l(A) + l(B) \leq g + 1$. Iz Riemann-Rocha slijedi

$$l(A) = \deg A + 1 - g + l(B) \leq \deg A + 1 - g + g + 1 - l(A) \implies 2l(A) \leq 2 + \deg A.$$

S obzirom da $D \sim A$, zadnja nejednakost je ekvivalentna s $l(D) \leq 1 + \frac{1}{2}\deg D$. □

Bibliografija

[1] David Cox, John Little i Donal O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 4. izd., Springer, 2015, ISBN 978-3-319-16720-6.

[2] S.D. Galbraith, *Mathematics of Public Key Cryptography*, Cambridge University Press, 2012, ISBN 9781107013926.

[3] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Modern Birkhäuser Classics, Springer New York, 2012, ISBN 9781461459873.

[4] Filip Najman, *Aritmetička Geometrija*, https://web.math.pmf.unizg.hr/~fnajman/ag.pdf, Skripta.

[5] Georg Friedrich Bernhard Riemann, *Theorie der Abel'schen Functionen.*, Journal für die reine und angewandte Mathematik (Crelles Journal) **1857**, 115 – 155, https://api.semanticscholar.org/CorpusID:16593204.

[6] G. Roch, *Ueber die Anzahl der willkürlichen Constanten in algebraischen Functionen.*, Journal für die reine und angewandte Mathematik (Crelles Journal) **1865**, 372 – 376, https://api.semanticscholar.org/CorpusID:120178388.

[7] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer New York, 2009, ISBN 9780387094946.

[8] H. Stichtenoth, *Algebraic Function: Fields and Codes*, Universitext (Berlin. Print), Springer-Verlag, 1993, ISBN 9783540564898.

Sažetak

U ovom radu bavili smo se Riemann-Rochovim teoremom za algebarske krivulje. Uveli smo nužne pojmove iz algebarske geometrije, dokazali teorem i naveli neke njegove primjene.

Prvo smo dali kratki uvod u algebarsku geometriju gdje smo definirali afine i projektivne mnogostrukosti, te preslikavanja između njih. Dalje smo se fokusirali specifično na glatke krivulje, tj. nesingularne projektivne mnogostrukosti dimenzije 1.

Uveli smo funkcijska polja koja čine kategoriju koja je ekvivalentna kategoriji glatkih krivulja. Pokazali smo kako se tvrdnje o funkcijskim poljima i o krivuljama prevode iz jednog konteksta u drugi. Definirali smo grupu divizora koja je pridružena krivulji i ustanovili osnovna svojstva divizora.

Svakom divizoru je pridružen Riemann-Rochov prostor koji je sačinjen od racionalnih funkcija sa zadanim nultočkama i polovima. Definirali smo genus krivulje i ustanovili nekoliko rezultata o Riemann-Rochovim prostorima. Dokazali smo Riemannovu nejednakost koja nam daje relaciju između dimenzije Riemann-Rochovog prostora, stupnja divizora i genusa krivulje. Onda smo uveli prstene adela i Weilove diferencijale da okarakteriziramo indeks specijalnosti i dokažemo Riemann-Rochov teorem koji pojačava Riemannovu nejednakost. Naveli smo primjene Riemann-Rochovog teorema: odredili smo svojstva kanonskog divizora, karakterizirali krivulje genusa 0 s racionalnom točkom do na izomorfizam, dokazali da je svaka eliptička krivulja izomorfna nekoj krivulji zadanoj Weierstrassovom jednadžbom, definirali smo grupni zakon na eliptičkoj krivulji, dokazali smo neke tvrdnje o specijalnim divizorima uključujući Cliffordov teorem.

Summary

In this thesis, we explore the Riemann-Roch theorem for algebraic curves. We introduced the necessary notions from algebraic geometry, proved the Riemann-Roch theorem, and stated some of its applications.

We started with a brief introduction to algebraic geometry, in which we defined affine and projective varieties, and the maps between them. Later we focused specifically on smooth curves, i.e. nonsingular projective varieties of dimension 1.

We introduced function fields that form a category, that is equivalent to the category of smooth curves. We demonstrated how statements about function fields and curves can be translated from one context to another. For each curve, we defined the associated divisor group and established some of the basic properties of divisors.

To each divisor, there is an associated Riemann-Roch space. It is made up of rational functions with prescribed zeros and poles. We defined the genus of a curve and proved a couple of results about Riemann-Roch spaces. We proved the Riemann inequality, which relates the dimension of a Rimeann-Roch space, the degree of a divisor, and the curve genus. Then, we introduced adele rings and Weil differentials to characterize the index of speciality and prove the Riemann-Roch theorem which improves the Riemann inequality. We stated some applications of the Riemann-Roch theorem: we determined the properties of the canonical divisor, we characterized smooth curves of genus 0 containing a rational point up to isomorphism, we proved that each elliptic curve is isomorphic to a curve defined by Weierstrass equation, we defined the group law on the elliptic curve, and we proved some results about special divisors, including Clifford's theorem.

Životopis

Marin Varivoda rođen je 24. 9. 2000. u Zadru, gdje je pohađao Osnovnu školu Šime Budinića i kasnije Gimnaziju Franje Petrića. Za vrijeme osnovnog i srednjoškolskog obrazovanja, sudjelovao je na brojnim natjecanjima iz matematike i srodnih područja kao što su informatika i fizika. Na 58. Međunarodnoj matematičkoj olimpijadi održanoj u Brazilu osvojio je brončanu, a na 59. olimpijadi u Rumunjskoj srebrnu medalju.

Započeo je 2019. preddiplomski studij matematike na Jagielonskom sveučilištu u Krakovu u sklopu Mertensove stipendije za strane studente, a 2021. se prebacio na Prirodoslovno-matematički fakultet Sveučilišta u Zagrebu. Upisao je diplomski studij teorijske matematike.

Tijekom studija je sudjelovao na studentskim natjecanjima. Na međunarodnim natjecanjima iz matematike IMC 2022. i IMC 2023. je dvaput osvojio prvu nagradu.

Koautor je članaka:

- *Convexity of Chebyshev Sets Revisited* (Deka & Varivoda, 2022), *The American Mathematical Monthly*, 129(8), 763–774.
- *On the Banach–Mazur Distance in Small Dimensions* (Kobos & Varivoda, 2024), *Discrete & Computational Geometry*.