SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Ivan Krijan, Sara Muhvić

MULTIPLICITETI PRESJEKA I RACIONALNOST RAVNINSKIH KRIVULJA

Zagreb, 2013.

Ovaj rad izrađen je na Zavodu za algebru i osnove matematike na Matematičkom odsjeku Prirodoslovno–matematičkog fakulteta, pod vodstvom prof. dr. sc. Gorana Muića i predan je na natječaj za dodjelu Rektorove nagrade u akademskoj godini 2012./2013.

Sadržaj

Uvod **1**

1 Algebarski skupovi u afinom prostoru **5**

1.1 Osnovni pojmovi iz algebre 5

1.2 Faktorizacija i derivacija polinoma 11

Dodatni pojmovi iz algebre 11

Faktorizacija polinoma 15

Derivacija polinoma 18

1.3 Hilbertov teorem o bazi 22

1.4 Algebarski skupovi 24

1.5 Hilbertov teorem o nulama 29

1.6 Rastav u ireducibilne komponente 42

Ravninski algebarski skupovi 45

2 Afine mnogostrukosti **47**

2.1 Osnovni pojmovi 47

2.2 Racionalne funkcije i lokalni prsteni 54

2.3 Dodatni algebarski pojmovi i rezultati 57

2.4 Ravninske krivulje 73

Regularne i singularne točke 74

2.5 Multipliciteti presjeka 78
2.6 Algoritam za računanje multipliciteta presjeka 86
Posebne klase krivulja 98
2.7 Drukčija definicija multipliciteta presjeka 100
Osnovno o formalnim redovima 100
Multipliciteti presjeka i formalni redovi 103
Primjer primjene 107

3 Projektivne mnogostrukosti **109**
3.1 Osnovni pojmovi 109
Veza afinih i projektivnih mnogostrukosti 118
3.2 Ravninske krivulje i Bézoutov teorem 122

4 Afine i projektivne krivulje **128**
4.1 Projektivni i afini prostori 128
Dualnost 132
Afini prostori 134
4.2 Afine krivulje 135
4.3 Krivulje u projektivnoj ravnini 137
Veza između algebarskih i afinih krivulja 138
4.4 Rezultanta dvaju polinoma 139
4.5 Singulariteti 141
4.6 Sjecišta krivulja 142

5 Racionalne krivulje **150**
5.1 Definicija i karakterizacije 150
5.2 Dovoljan uvjet za racionalnost krivulje 156
5.3 Kvadratne transformacije 160

5.4 Algoritam za određivanje racionalnosti ravninske krivulje 168
5.5 Primjeri 170

Bibliografija **176**

Sažetak **179**

Summary **181**

Uvod

Ovaj rad počinje s detaljnim pregledom pojmova i rezultata iz opće algebre koji su nam potrebni u razvoju pojmova iz algebarske geometrije ključnih za proučavanje multipliciteta presjeka dviju afinih ravninskih krivulja. To se sve nalazi u poglavlju 1 te je većina napravljena prema uzoru na tipičnu knjigu iz algebre, [12] te predavanja [23]. U poglavlju 2 najprije definiramo najosnovnije algebarsko–geometrijske pojmove kao što su **mnogostrukost**, **racionalna funkcija**, **lokalni prsten** i sam pojam **krivulje**. Dakle, to su sekcije 2.1, 2.2, 2.3 te 2.4, uglavnom su korištene moderne knjige algebarske geometrije, kao što su [3], [6], [9], [21] te [22], naravno, uz predavanja [18]. Zanimljivih stvari o tome ima također i u člancima [14] i [15].

Sada dolazimo na prvu ključnu (od tri) točku u ovome radu, to su sekcije 2.5, 2.6 te 2.7. Sekcija 2.5 je u potpunosti napravljena prema izvrsnoj knjizi [8] te je u njoj dana algebarska definicija **multipliciteta presjeka dviju afinih ravninskih krivulja** F i G u točki P, u oznaci:

$$I\left(P,\, F \cap G\right).$$

Za još apstraktniji pristup istoj temi te objašnjenja čemu nam uopće služi pojam multipliciteta valja pogledati knjige [7] i [13], u drugoj su navedena neka pitanja koja su ljude dovela do pojma multipliciteta. Ključan dio te sekcije je teorem 2.5.5 koji nam daje eksplicitnu formulu za definirani multiplicitet:

$$I\left(P,\, F \cap G\right) = \dim_K \left(\mathcal{O}_P\left(\mathbb{A}^2\right)/\left(F,\, G\right)\right).$$

No, sam dokaz tog teorema je još plodonosniji jer u njemu nailazimo na postupak koji nam daje **algoritam za računanje multipliciteta** koji se svodi na elementarne aritmetičke operacije nad polinomima. O načinu izračunavanja multipliciteta postoji mnošto literature, navodimo samo dio. Knjige [10] i [11], članci [2] i [19], a zanimljive stvari se mogu naći i na [1], [5] i [16]. Cijela sekcija 2.6 je posvećena upravo tom algoritmu. U njoj se nalazi prvi značajniji **originalni doprinos** ovoj temi. Ključne stvari su algoritam (2.6) napisan u programskom jeziku C te teorem 2.6.6. Odmah nakon algoritma su navedeni primjeri na kojima je on testiran, njegova valjanost je, jasno, precizno objašnjenja tokom procesa dolaska do samog algoritma. Spomenuti teorem 2.6.6 nam daje svojevrsnu motivaciju za ono što slijedi u sekciji 2.7. Tu dajemo drugu definiciju multipliciteta presjeka, onu koja je više geometrijske prirode, nju možemo naći u knjizi [24]. Spomenimo da u [4] možemo naći ponešto o računanju takozvanih Serreovih multipliciteta, no mi se ovdje time nećemo baviti. Ono što slijedi je prvi **centralni originalni razultat** u ovome radu, a to je dokaz teorema 2.7.9 koji nam govori da su dvije definicije multipliciteta presjeka (algebarska i geometrijska) koje smo obradili, jednake. Preciznije, teorem kaže da za multiplicitet presjeka krivulja F i G u točki $P = (0, 0)$, pri čemu je barem jedna od krivulja dovoljno "lijepa" (što znači da o njoj možemo reći sve samo na osnovu geometrijskih svojstava) vrijedi:

$$\dim_K \left(\mathcal{O}_{(0,0)}\left(\mathbb{A}^2\right)/ (F, G)\right) = \nu\left(G\left(X, \sum_{k=1}^{\infty} a_k X^k\right)\right),$$

pri čemu je $f(X) = \sum_{k=1}^{\infty} a_k X^k$ jedinstven takav da je $F(X, f(X)) = 0$ te $\nu(g) = +\infty$ ako je $g = 0$, a ako je $g \neq 0$, onda je to najveći $n \in \mathbb{Z}_{\geq 0}$ takav da $X^n \mid g$, u $K[[X]]$, za $g \in K[[X]]$. Spomenimo još kako je sve potkrijepljeno mnoštvom primjera, od kojih je većina vezana uz algoritam, ključan je primjer 2.6.1. Podsekcija 2.7 nam prikazuje lijep primjer u kojemu se očitava korisnost teorema 2.7.9, tj. činjenice da su algebarska i geometrijska definicija multipliciteta presjeka međusobno jednake (kada god geometrijska ima smisla).

Poglavlje 3 služi kao uvod u teoriju projektivnih mnogostukosti. Njihova glavna svrha (ona radi koje su uvedene) je da se u projektivnoj ravnini krivulje ponašaju puno bolje nego u afinoj. Preciznije, projektivnu ravninu možemo gledati kao globalnu situaciju, dok je afina lokalna. One krivulje koje se ne sijeku u afinoj ravnini, ali se asimptotski približavaju jedna drugoj, u projektivnoj ravnini se sijeku i za njih kažemo da se sijeku "u beskonačnosti". Uz većinu do sada navedene literature, ovdje je još dobro istaknuti knjigu [17]. Ključni dio ovog poglavlja je Bézoutov teorem (3.2.6), koji je svojevrsno poopćenje osnovnog teorema algebre.

U nastavku rada se fokus stavlja na pojam racionalnih krivulja te metoda za određivanje racionalnosti. U poglavlju 4 ponavljamo osnovne definicije iz algebarske geometrije, poput pojmova projektivnog i afinog prostora, afine i projektivne krivulje te dajemo neke osnovne rezultate. Većina rezultata iz ovog poglavlja se može naći u knjizi [24], predavanjima [18], te neke osnovne algebarske činjenice u [12]. Treba istaknuti kako se u sekciji 4.6 daju dokazi dvaju teorema o sjecištima krivulje i pravaca kroz određenu točku koji omogućuju efikasnu upotrebu algoritma koji se predstavlja u poglavlju 5.

U petom poglavlju definiramo racionalnu krivulju u afinoj ravnini kao ireducibilnu krivulju koja se može parametrizirati racionalnim funkcijama. Preciznije, zahtjev je da postoje racionalne funkcije φ, ψ takve da se definirajući polinom ove krivulje poništava u $(\varphi(t),\ \psi(t))$. Definicija je uzeta iz [21], no treba napomenuti da se poopćenje ove definicije na algebarsku mnogostrukost proizvoljne dimenzije ne uzima za definiciju racionalnosti, već za takve mnogostrukosti kažemo da su uniracionalne, a racionalne mnogostrukosti su one koje su biracionalno ekvivalentne projektivnom prostoru iste dimenzije. Zbog toga dajemo dokaz Lürothovog teorema koji povlači da su definicije racionalnosti i uniracionalnosti u slučaju krivulja u ravnini ekvivalentne. Štoviše, ova ekvivalencija vrijedi isključivo za mnogostrukosti dimenzija 1. Više o tom, tzv. Lürothovom problemu se može naći u [21].

Dalje u radu dolazimo do još jedne karakterizacije racionalnih krivulja, izuzetno važne za primjene. Teorem iz [24] kaže da je krivulja stupnja n koja nema složenih singulariteta racionalna ako i samo ako je

$$(n-1)(n-2) = \sum r_i (r_i - 1),$$

pri čemu su r_i multipliciteti singularnih točaka krivulje. Dokaz dovoljnosti je konstruktivan, i iako su metode nalaženja parametrizacija racionalnih krivulja od golemog značenja, u ovom radu smo se ograničili na određivanje racionalnosti. Više o nalaženju parametrizacija se može naći npr. u članku [20].

Sada kada imamo praktičan kriterij za određivanje racionalnosti krivulje, prirodno se postavlja pitanje, možemo li na sličan način odrediti racionalnost ukoliko krivulja ima složeni singularitet i ovdje dolazimo do posljednjeg ključnog dijela rada. Odgovor je da postoji metoda kojom krivulju sa složenim singularitetima možemo izmijeniti tako da nova krivulja nema složenih singulariteta, a da sam postupak transformacije ne mijenja racionalnost. Pred kraj poglavlja predstavljamo algoritam koji to čini. Algoritam je temeljen na Walkerovom dokazu tvrdnje da se svaka krivulja može nizom kvadratnih transformacija prevesti u krivulju koja ima samo jednostavne singularitete. Na samom kraju, u dva primjera provodimo algoritam na konkretnim racionalnim krivuljama.

Poglavlje 1

Algebarski skupovi u afinom prostoru

1.1 Osnovni pojmovi iz algebre

Definicija 1.1.1. ***Prsten*** *je neprazan skup R snabdjeven s dvije binarne operacije, $+$ (zbrajanje) i $\cdot$ (množenje), takve da vrijedi:*

(i) $(R, +)$ *je* ***Abelova grupa****, tj. vrijedi:*

(a) *(asocijativnost)* $a + (b + c) = (a + b) + c,\ \forall a, b, c \in R$,

(b) *postoji element* $0_R \in R$ *takav da je* $a + 0_R = 0_R + a = a,\ \forall a \in R$,

(c) *za svaki* $a \in R$ *postoji* $-a \in R$ *takav da je* $a + (-a) = -a + a = 0$,

(d) *(komutativnost, tj. Abelovo svojstvo)* $a + b = b + a,\ \forall a, b \in R$,

(ii) *(asocijativnost)* $a \cdot (b \cdot c) = (a \cdot b) \cdot c,\ \forall a, b, c \in R$,

(iii) *(distributivnost)* $a \cdot (b + c) = a \cdot b + a \cdot c$ *i* $(a + b) \cdot c = a \cdot c + b \cdot c,\ \forall a, b, c \in R$.

Potprsten *prstena R je svaki podskup prstena R koji je zatvoren s obzirom na operacije zbrajanje i množenja te je i sam prsten, uz iste operacije.*

Napomena 1.1.2. *U ovom radu smatrati ćemo da je prsten uvijek komutativan i da ima jedinicu (različitu od nule). Odnosno,*

$$a \cdot b = b \cdot a,\ \forall a, b \in R \quad te \quad \exists 1_R \in R,\ a \cdot 1_R = 1_R \cdot a = a,\ \forall a \in R,\ 1_R \neq 0_R.$$

Također, kraće ćemo pisati $0 = 0_R$ *i* $1 = 1_R$*. Nadalje, znak za množenje će uglavnom biti izostavljen, tj. pisati ćemo* ab *umjesto* $a \cdot b$*.*

Za $r \in R$ i cijeli broj n uvedimo oznaku nr takvu da je $nr = \underbrace{r + r + \ldots + r}_{n \text{ puta}}$, ako je $n > 0$, $nr = 0$, ako je $n = 0$ te $nr = -((-n)\, r)$, ako je $n < 0$. Također, neka je $r^0 = 1$ te, za $n > 0$, $r^n = \underbrace{r \cdot r \cdot \ldots \cdot r}_{n \text{ puta}}$. U prstenu R vrijedi sljedeće:

- $0 \cdot a = 0,\ \forall a \in R$,
- $(-a)\, b = a\, (-b) = -(ab),\ \forall a, b \in R$,
- $(-a)\, (-b) = ab,\ \forall a, b \in R$,
- $(na)\, b = n\, (ab),\ \forall n \in \mathbb{Z},\ \forall a, b \in R$,
- (binomni teorem) $(a + b)^n = \sum_{k=0}^{n} a^k b^{n-k},\ \forall n \in \mathbb{Z},\ n \geq 0,\ \forall a, b \in R$,

ovdje je sa $\mathbb{Z}$ označen skup cijelih brojeva.

Definicija 1.1.3. *Neka je* R *prsten. Pretpostavimo da postoji prirodan broj* n *takav da je* $nr = 0$*, za svaki* $r \in R$*. Najmanji takav prirodan broj* n *nazivamo* ***karakteristika*** *prstena* R *i pišemo* $\mathrm{char}\,(R) = n$*. Ukoliko takav prirodan broj ne postoji, onda je* $\mathrm{char}\,(R) = 0$*.*

Primijetimo da je karakteristika prstena R zapravo najmanji prirodan broj n (Ukoliko takav postoji.) takav da je $n \cdot 1 = 0$.

Definicija 1.1.4. *Neka su R i S prsteni. Funkcija $f : R \to S$ je* ***homomorfizam*** *prstenova (R i S) ako:*

$$f(a+b) = f(a) + f(b) \quad i \quad f(ab) = f(a)\, f(b)\,, \ \forall a, b \in R.$$

Napomena 1.1.5. *Za gore definirani homomorfizam (Često će biti ispuštena riječ "prstenova".) ćemo dodatno podrazumijevati da vrijedi $f(1_R) = 1_S$.*

Ukoliko je homomorfizam injektivan (surjektivan, bijektivan) nazivati ćemo ga monomorfizam (epimorfizam, izomorfizam). Za monomorfizam $f : R \to S$ ćemo reći da je ulaganje prstena R u prsten S, a za izomorfizam $f : R \to R$ ćemo reći da je automorfizam prstena R. Ukoliko postoji izomorfizam između prstena R i S, onda ćemo reći da su oni izomorfni i to ćemo označavati s $R \cong S$.

Definicija 1.1.6.

- *Element $0 \neq a \in R$ se zove* ***djelitelj nule*** *ako postoji $0 \neq b \in R$ takav da je $ab = 0$.*
- *Element $a \in R$ je* ***invertibilan*** *ako postoji $b \in R$ takav da je $ab = 1$.*

Definicija 1.1.7. ***Integralna domena*** *je prsten koji nema djelitelja nule.* ***Polje*** *je integralna domena u kojoj je svaki element različit od nule invertibilan.*

Primijetimo da u integralnoj domeni vrijedi "zakon kraćenja", tj. ako za a, b, $c \in R$ vrijedi $ac = bc$ i $c \neq 0$, tada je $a = b$. Nadalje, jednostavnosti radi, standardno ćemo označavati skup cijelih brojeva (To je primjer integralne domene.) sa $\mathbb{Z}$, skup nenegativnih cijelih brojeva sa $\mathbb{Z}_{\geq 0}$, skup prirodnih brojeva s $\mathbb{N}$, skupove racionalnih, realnih i kompleksnih brojeva (Što su sve primjeri polja.) redom s $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$.

Definicija 1.1.8. ***Polje razlomaka*** *K integralne domene D jest polje čiji elementi su klase ekvivalencije elemenata iz $D \times (D \setminus \{0\})$ inducirane relacijom:*

$$(a', b') \sim (a, b) \iff a'b = ab',$$

stavljamo $\frac{a}{b} = \{(a', b') \in D \times (D \setminus \{0\}) \ : \ (a', b') \sim (a, b)\}$, *uz zbrajanje i množenje:*

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + b_1 a_2}{b_1 b_2}, \qquad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}.$$

Napomena 1.1.9. *Gornja definicija je dobra za svaku integralnu domenu R, diskusije i dokaz te činjenice se mogu naći u [12].*

U smislu gornje definicije, D je potprsten od K, jednostavno $a \in D$ identificiramo s $\frac{a}{1}$. Stavimo li $D = \mathbb{Z}$ vidimo da je $K = \mathbb{Q}$.

Definicija 1.1.10. *Neka je R prsten.* ***Prsten polinoma*** *u varijabli X je prsten* $R[X]$ *koji se sastoji od svih nizova u R koji imaju najviše konačno mnogo članova različitih od* 0 *uz operacije, za polinome* $f = (a_0, a_1, a_2, \ldots)$ *i* $g = (b_0, b_1, b_2, \ldots)$, *dane s:*

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots), \quad f \cdot g = (a_0 b_0, a_0 b_1 + a_1 b_0, \ldots, \underbrace{\sum_{k=0}^{n} a_k b_{n-k}}_{n\text{-to mjesto}}, \ldots).$$

Nadalje, $X := (0, 1, 0, 0, \ldots)$ *te* $X^0 := (1, 0, 0, \ldots)$. *Brojeve* $a_0, a_1, a_2, \ldots$ *nazivamo* ***koeficijentima*** *polinoma* f.

Napomena 1.1.11. *Vrijedi da je* $0_{R[X]} = (0, 0, 0, \ldots)$ *te* $1_{R[X]} = (1, 0, 0, \ldots)$. *Za* $a \in R$ *identificiramo* $(a, 0, 0, \ldots) = a$ *te time dobivamo da je R potprsten od* $R[X]$. *Nadalje, skup svih invertibilnih elemenata u* $R[X]$ *jednak je skupu svih invertibilnih elemenata u R.*

Definicija 1.1.12. *Neka je* f *polinom kao gore. Ukoliko postoji* $d \in \mathbb{Z}_{\geq 0}$ *takav da je* $a_d \neq 0$, *najveći takav* d *nazivamo* ***stupanj*** *polinoma* f *i pišemo* $d = \deg(f)$. *Ukoliko takav* d *ne postoji onda taj polinom nazivamo nul–polinomom i za njega stupanj ne definiramo.*

Polinomi iz definicije 1.1.10 su jednaki ako i samo ako je $a_k = b_k$, za svaki $k \in \mathbb{Z}_{\geq 0}$. Nadalje, nul–polinom označavamo jednostavno s 0, neka f nije nul–polinom i neka je $d = \deg(f)$. Lako se vidi da za $n \in \mathbb{Z}_{\geq 0}$ vrijedi da je $X^n = (0, \ldots, 0, \underbrace{1}_{n\text{-to mjesto}}, 0, \ldots)$. Sada

"standardno" pišemo $f = (a_0, a_1, a_2, \ldots) = a_0 + a_1X + a_2X^2 + \ldots + a_dX^d = f(X)$. Ukoliko je R integralna domena, tada je i $R[X]$ integralna domena te vrijedi da je $\deg(f \cdot g) = \deg(f) + \deg(g)$, za sve polinome f i g, različite od nul–polinoma.

Napomena 1.1.13. *Pomoću definicije 1.1.10 sada lako induktivno definiramo prsten polinoma u više varijabli:*

$$R[X_1, X_2] = R[X_1][X_2], \ldots, R[X_1, X_2, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n], \ \forall n \in \mathbb{N}, n \geq 3.$$

Neka je $f = f(X_1, X_2, \ldots, X_n) \in R[X_1, X_2, \ldots, X_n]$. Neka je $k \in \{1, 2, \ldots, n\}$, promatrajmo $R[X_1, X_2, \ldots, X_n]$ kao $R[X_1, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n][X_k]$. U smislu definicije 1.1.10, f možemo napisati kao $(f_0, f_1, f_2, \ldots)$. Sada, kao u definiciji 1.1.12 definiramo $\deg_{X_k}(f)$, stupanj polinoma f u varijabli X_k. Konačno dolazimo do standardnog načina zapisivanja polinoma, ukoliko je f nul–polinom označavamo ga s 0. Ako f nije nul–polinom, neka je $d = \deg_{X_k}(f)$, tada pišemo:

$$f(X_1, X_2, \ldots, X_n) = \sum_{l=0}^{d} f_l(X_1, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n) X_k^l.$$

Opet, ukoliko je R integralna domena, tada je i $R[X_1, X_2, \ldots, X_n]$ integralna domena. Pripadajuće polje razlomaka označavamo s $R(X_1, X_2, \ldots, X_n)$ i nazivamo polje racionalnih funkcija.

Propozicija 1.1.14 (Univerzalno svojstvo)**.** *Neka su R i S prsteni, $\varphi : R \to S$ homomorfizam prstenova te $n \in \mathbb{N}$. Nadalje, neka su $s_1, s_2, \ldots, s_n \in S$, tada postoji jedinstveni homomorfizam $\overline{\varphi} : R[X_1, X_2, \ldots, X_n] \to S$ takav da je*

$$\overline{\varphi}|_R = \varphi \quad \textit{(U smislu napomene 1.1.11.)} \qquad i \qquad \overline{\varphi}(X_k) = s_k, \ \forall k \in \{1, 2, \ldots, n\}.$$

Dokaz. Može se naći u [12] na stranici 152, Theorem 5.5. Q.E.D.

Neka je $f(X_1, X_2, \ldots, X_n) \in R[X_1, X_2, \ldots, X_n]$. Stavimo da je $S = R$ te pogledajmo što je $\overline{\varphi}(f)$. Dobiti ćemo da je to jednako vrijednosti polinoma f (shvaćenog kao funkcije s R^n u R) u točki $(s_1, s_2, \ldots, s_n)$, u oznaci $f(s_1, s_2, \ldots, s_n)$.

Definicija 1.1.15. *Upravo opisani homomorfizam nazivamo* ***evaluacija*** *polinoma u točki* $r = (s_1, s_2, \ldots, s_n)$ *te označavamo s* φ_r.

Definicija 1.1.16. *Polinomi oblika* $X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}$, *gdje su* $k_1, k_2, \ldots, k_n$ *nenegativni cijeli brojevi, u prstenu* $R[X_1, X_2, \ldots, X_n]$ *nazivaju se* ***monomi****. Stupanj monoma definiramo kao* $k_1 + k_2 + \ldots + k_n$.

Neka su $k_1, k_2, \ldots, k_n$ nenegativni cijeli brojevi, uvodimo oznake $X^{(k)} = X_1^{k_1} X_2^{k_2} \cdots X_n^{k_n}$ te $|k| = k_1 + k_2 + \ldots + k_n$. Lako se vidi da svaki polinom $f \in R[X_1, X_2, \ldots, X_n]$ ima jedinstven zapis u obliku $f = \sum_{|k|=0}^{\infty} a_{(k)} X^{(k)}$, gdje su $a_{(k)} \in R$ i $X^{(k)}$ monomi. Kako je $\deg_{X_k}(f)$ konačan za sve $k = 1, 2, \ldots, n$ vidimo da je gornja suma zapravo konačna.

Definicija 1.1.17. *Reći ćemo da je polinom* f ***homogen****, stupnja (homogenosti)* $d \in \mathbb{Z}_{\geq 0}$, *ako su u gornjem prikazu svi koeficijenti* $a_{(k)}$ *jednaki nula, osim eventualno onih gdje je* $|k| = d$.

Napomena 1.1.18. *Primijetimo da je prema gornjoj definiciji nul–polinom homogen bilo kojeg stupnja. Nadalje, svaki polinom* f *ima jedinstven prikaz* $f = f_0 + f_1 + \ldots + f_d$, *gdje je* f_k *homogen polinom stupnja* k. *Najveći* $d \in \mathbb{Z}_{\geq 0}$ *takav da je* $f_d \neq 0$ *(Takav uvijek postoji, osim za nul polinom, ali za njega stupanj ne definiramo.) nazivamo stupnjem polinoma* f *i pišemo* $\deg(f) = d$. *Ukoliko je* R *integralna domena, vidimo da je i* $R[X_1, X_2, \ldots, X_n]$ *integralna domena te da je* $\deg(fg) = \deg(f) + \deg(g)$, *gdje su* f *i* g *polinomi, različiti od nul–polinoma.*

1.2 Faktorizacija i derivacija polinoma

Imajmo na umu da nama prsten uvijek predstavlja komutativan prsten s jedinicom, koja je različita od nule. Neke od sljedećih definicija su za "obični" prsten (Dakle, onaj koji možda nije komutativan ili nema jedinicu ili je ima, ali je ona jednaka nuli.) nešto drukčije ili čak uopće nemaju smisla. Uvedimo dodatnu oznaku za skup invertibilnih elemenata prstena R, neka to bude R^*.

Dodatni pojmovi iz algebre

Definicija 1.2.1. *Element a u prstenu R je **ireducibilan** ako je različit od nule, nije invertibilan te za svaku faktorizaciju $a = bc$, gdje su $b, c \in R$ slijedi da je ili $b \in R^*$ ili $c \in R^*$.*

Definicija 1.2.2. *Neka je R prsten te neka su $a, b \in R$ i $b \neq 0$. Kažemo da element b **dijeli** element a, to označavamo s $b \mid a$, ako postoji $c \in R$ takav da je $a = bc$.*

Definicija 1.2.3. *Neka je R prsten. Kažemo da su elementi $a, b \in R \setminus \{0\}$ **asocirani** ako postoji $c \in R^*$ takav da je $a = bc$.*

Neka je D integralna domena. Primijetimo da su $a, b \in D \setminus \{0\}$ asocirani ako i samo ako $a \mid b$ i $b \mid a$. Naime, $a \mid b$ i $b \mid a$ ako i samo ako postoje $c, d \in D$ takvi da je $b = ac$ i $a = bd$. Sada imamo da je $a = bd = acd$, a to je ako i samo ako je $a(1 - cd) = 0$, a pošto smo u integralnoj domeni i $a \neq 0$, zaključujemo da je $cd = 1$, dakle, $c, d \in D^*$.

Definicija 1.2.4. *Integralna domena D je **domena jedinstvene faktorizacije (faktorijalna domena)**, kraće DJF, ako za svaki $a \in D$, takav da je $a \neq 0$ i $a \notin D^*$, postoje $n \in \mathbb{N}$ te $a_1, a_2 \ldots, a_n$ ireducibilni elementi iz D takvi da je $a = a_1 a_2 \cdots a_n$. Nadalje, vrijedi jedinstvenost prikaza, tj. ako su $m \in \mathbb{N}$ i $b_1, b_2, \ldots, b_m$ ireducibilni elementi iz D takvi da je $a = b_1 b_2 \cdots b_m$, tada je $m = n$ i postoji permutacija π skupa $\{1, 2, \ldots, n\}$ takva da su, za svaki $k \in \{1, 2, \ldots, n\}$, a_k i $b_{\pi(k)}$ asocirani.*

Lema 1.2.5. *Neka je R faktorijalna domena i neka je K njezino polje razlomaka. Tada se svaki element $z \in K$ može prikazati u obliku $z = \frac{a}{b}$, gdje su $a, b \in R$, $b \neq 0$ i koji nemaju zajedničkih faktora. Tj. ne postoji $c \in R \setminus R^*$, $c \neq 0$ takav da $c \mid a$ i $c \mid b$. Takav prikaz je jedinstven do na množenje invertibilnim elementima iz R.*

Dokaz. Neka je $\frac{a'}{b'}$, gdje su $a', b' \in R$, $b' \neq 0$, bilo koji reprezentant klase $z \in K$. Ukoliko je $b' \in R^*$ tvrdnja je očita, kao što je očita i ako je $a' = 0$ ili $a' \in R^*$. Pretpostavimo da je $a' \neq 0$ i $a', b' \notin R^*$. Tada postoje jedinstveni $m, n \in \mathbb{N}$ i ireducibilni, jedinstveni do na poredak i množenje invertibilnim elementima, $a_1, a_2, \ldots, a_m \in R$ te $b_1, b_2, \ldots, b_n \in R$ takvi da je $a' = a_1 a_2 \cdots a_m$ i $b' = b_1 b_2 \cdots b_n$. Konačno, dobivamo tražene a i b iz a' i b' tako da iz prikaza a', odnosno b' "izbacimo" sve parove (a_k, b_l), gdje su $k \in \{1, 2, \ldots, m\}$, $l \in \{1, 2, \ldots, n\}$, koji su asocirani. $\mathfrak{Q.E.D.}$

Definicija 1.2.6. *Neka je R prsten i I njegov potprsten. Kažemo da je I **ideal** u R ako je, za svaki $r \in R$ i za svaki $x \in I$, $rx \in I$. Ideal I je **pravi** ideal u R ako je $I \neq R$. Pravi ideal I u R je **maksimalan** ideal ako nije sadržan u niti jednom većem pravom idealu. Pravi ideal I u R je **prost** ideal ako vrijedi: ako su $a, b \in R$ takvi da je $ab \in I$, tada je $a \in I$ ili $b \in I$.*

Primijetimo da je pravi ideal I u prstenu R maksimalan ako i samo ako za svaki ideal J u prstenu R, takav da je $I \subseteq J \subseteq R$, vrijedi da je $J = I$ ili $J = R$. Nadalje, primijetimo da je ideal I pravi ako i samo ako je $I \cap R^* = \emptyset$.

Definicija 1.2.7. *Neka su R i S prsteni te $\varphi : R \to S$ homomorfizam. **Slika** homomorfizma φ, u oznaci $\mathrm{Im}(\varphi)$, je skup $\{\varphi(r) : r \in R\} \subseteq S$. **Jezgra** homomorfizma φ, $\mathrm{Ker}(\varphi)$, je skup $\varphi^{-1}(0) = \{r \in R : \varphi(r) = 0\} \subseteq R$.*

Napomena 1.2.8. *Lako se vidi da je $\mathrm{Ker}(\varphi)$ ideal u R. Također, φ je monomorfizam ako i samo ako je $\mathrm{Ker}(\varphi) = \{0\}$.*

Neka je S bilo koji podskup prstena R, sa $\langle S \rangle$ označavamo najmanji ideal u R koji sadrži S. On uvijek postoji i jednak je presjeku svih ideala u R koji sadrže S (R je uvijek primjer jednog takvog). Jasno je da je presjek bilo koje (neprazne) familije ideala u R ponovno ideal u R. Nadalje, znamo točno kako izgleda taj ideal:

$$\langle S \rangle = \left\{ \sum_{k=1}^{n} r_k s_k \ : \ n \in \mathbb{N},\ r_1, \ldots, r_n \in R,\ s_1, \ldots, s_n \in S \right\}.$$

Definicija 1.2.9. *Ideal I u prstenu R je* ***konačno generiran****, ako postoji konačan podskup $S \subseteq R$ takav da je $I = \langle S \rangle$. U tom slučaju, ako je, za $n \in \mathbb{N}$, $S = \{r_1, r_2, \ldots, r_n\}$, pišemo $I = (r_1, r_2, \ldots, r_n)$. Ideal je* ***glavni*** *ako je generiran s jednim elementom. Integralna domena u kojoj je svaki ideal glavni naziva se* ***domena glavnih ideala****, kraće DGI.*

Napomena 1.2.10. *Svaka domena glavnih ideala je faktorijalna domena. Skup $\mathbb{Z}$ je DGI, također, ako je K polje, prsten polinoma u jednoj varijabli nad poljem K, $K[X]$ je DGI. Glavni ideal $I = (r)$ u DJF R je prost ako i samo ako je r ireducibilan (ili nula) element u DJF R.*

Definicija 1.2.11. *Element p u prstenu R je* ***prost*** *ako je različit od nule, nije invertibilan te ako za neke $a, b \in R$ vrijedi da $p \mid ab$ onda $p \mid a$ ili $p \mid b$.*

Napomena 1.2.12. *U prstenu R, svaki prost element je ireducibilan. Ako je R DGI, onda vrijedi i obratno, tj. svaki ireducibilan element u R je prost.*

Definicija 1.2.13. *Neka je R prsten. Za $a, b \in R$ kažemo da su* ***relativno prosti*** *ako ne postoji $c \in R$ takav da je $c \neq 0$, $c \notin R^*$, $c \mid a$ i $c \mid b$.*

Definicija 1.2.14. *Neka je I ideal u prstenu R.* ***Kvocijentni prsten*** *je skup R/I čiji elementi su klase ekvivalencije skupa R, inducirane relacijom: $a \sim b \iff a - b \in I$, $a, b \in R$. Njegove elemente označavamo sa, za $r \in R$, $r + I$, ili kraće $\overline{r}$, a operacije su, za $r, r' \in R$:*

$$(r + I) + (r' + I) = (r + r') + I \qquad i \qquad (r + I)(r' + I) = rr' + I.$$

Napomena 1.2.15. *Gornja definicija je dobra, što se može naći u [12]. Ukoliko je R komutativan prsten s jedinicom (Što u ovom radu uvijek jest!) i I ideal u R, onda je i R/I komutativan prsten s jedinicom. Pravi ideal I u R je prost ako i samo ako je R/I integralna domena, odnosno maksimalan ako i samo ako je R/I polje. Iz ovoga zaključujemo: svaki maksimalni ideal u prstenu R je prost.*

Primijetimo da ukoliko je R komutativan prsten s jedinicom, različitom od nule (U ovom radu je to uvijek tako!) i I ideal u R, onda je i R/I komutativan prsten s jedinicom, no ona sada ne mora biti različita od nule. Uzmimo npr. $I = R$.

Definicija 1.2.16. *Neka je R prsten i I ideal u R.* ***Kanonski epimorfizam*** *prstena R u kvocijentni prsten R/I je preslikavanje $\pi : R \to R/I$ dano s $\pi(r) = r + I$, za svaki $r \in R$.*

Lako se vidi da kanonski epimorfizam uistinu jest epimorfizam s prstena R na prsten R/I.

Propozicija 1.2.17 (Prvi teorem o izomorfizmu)**.** *Neka su R i S prsteni te $\varphi : R \to S$ homomorfizam. Neka je I ideal u R takav da je $I \subseteq \operatorname{Ker}(\varphi)$. Tada postoji jedinstven homomorfizam $\overline{\varphi} : R/I \to S$ takav da je $\varphi = \overline{\varphi} \circ \pi$. Nadalje, $\operatorname{Im}(\overline{\varphi}) = \operatorname{Im}(\varphi)$ i $\operatorname{Ker}(\overline{\varphi}) = \operatorname{Ker}(\varphi)/I$. $\overline{\varphi}$ je izomorfizam ako i samo ako je φ epimorfizam i $I = \operatorname{Ker}(\varphi)$.*

Dokaz. U [12], stranica 125, Theorem 2.9. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Neka je D integralna domena i neka je $p = \operatorname{char}(D)$. Neka je $\varphi : \mathbb{Z} \to D$ jedinstven homomorfizam. On postoji i jedinstven je, zato što mora biti $\varphi(1) = 1$. Sada lako vidimo da je $\operatorname{Ker}(\varphi) = (p)$. No, D je integralna domena, iz čega zaključujemo da je ideal (p) prost u $\mathbb{Z}$. Odnosno, karakteristika integralne domene može biti samo prost broj ili nula.

Neka je K polje te $n \in \mathbb{N}$ i I pravi ideal u $K[X_1, X_2, \ldots, X_n]$. Kako je I pravi ideal, vidimo da I ne sadrži niti jedan element polja K, u suprotnom I ne bi bio pravi ideal.

Promatrajmo kanonski epimorfizam $\pi : K[X_1, X_2, \ldots, X_n] \to K[X_1, X_2, \ldots, X_n]/I$ i njegovu restrikciju na polje K, $\pi|_K$. Jasno je da je $\pi|_K$ ulaganje polja K u $K[X_1, X_2, \ldots, X_n]/I$. Dakle, polje K je potprsten prstena $K[X_1, X_2, \ldots, X_n]/I$. Konačno, $K[X_1, X_2, \ldots, X_n]/I$ je vektorski prostor nad poljem K.

Definicija 1.2.18. *Neka je D integralna domena i neka je $f \in D[X]$. Za polinom f kažemo da je primitivan ako, za $a \in D$ takav da a dijeli sve koeficijente od f slijedi da je $a \in D^*$.*

Faktorizacija polinoma

Teorem 1.2.19 (Faktorizacija u prstenu polinoma)**.** *Neka je R domena jedinstvene faktorizacije, tada je, za svaki $n \in \mathbb{N}$, $R[X_1, X_2, \ldots, X_n]$ također domena jedinstvene faktorizacije. Nadalje, neka je K pripadajuće polje razlomaka od R i f primitivan polinom pozitivnog stupnja u $R[X]$. Tada je f ireducibilan u $R[X]$ ako i samo ako je ireducibilan u $K[X]$.*

Dokaz. Sve tvrdnje teorema su posljedice Gaussove leme čiji se iskaz i dokaz mogu naći u [12] na stranici 162, Lemma 6.11. Konkretan dokaz tvrdnji teorema se nalaze u istoj knjizi na stranicama 163 i 164, riječ je o: Lemma 6.12., Lemma 6.13. i Theorem 6.14. $\mathfrak{Q.E.D.}$

Korolar 1.2.20. *Neka je R domena jedinstvene faktorizacije i K pripadajuće polje razlomaka. Neka su f, $g \in R[X]$. Polinomi f i g imaju zajednički faktor u $R[X]$ ako i samo ako ga imaju u $K[X]$.*

Dokaz. Direktna posljedica prethodnog teorema. Naime, f i g imaju zajednički faktor ako i samo ako imaju ireducibilni zajednički faktor, zato jer su R i K, a time i $R[X]$ i $K[X]$ DJF. $\mathfrak{Q.E.D.}$

Definicija 1.2.21. *Neka je R prsten i neka je $f \in R[X]$. $\alpha \in R$ je* ***nultočka*** *polinoma f ako je $f(\alpha) = 0$.*

Definicija 1.2.22. *Neka je R prsten i $f \in R[X]$ takav da f nije nul–polinom. Koeficijent polinoma f uz $X^{\deg(f)}$ nazivamo* ***vodeći koeficijent*** *polinoma f. Nul–polinom ima vodeći koeficijent jednak 0. Polinom je* ***normiran*** *ukoliko mu je vodeći koeficijent jednak 1.*

Teorem 1.2.23 (o dijeljenju polinoma)**.** *Neka je R prsten i $f, g \in R[X]$ različiti od nul–polinoma. Nadalje, neka je vodeći koeficijent polinoma g invertibilan u R. Tada postoje jedinstveni polinomi $q, r \in R[X]$ takvi da*

$$f = qg + r \qquad i \qquad r = 0 \quad ili \quad \deg(r) < \deg(g).$$

Dokaz. Pogledati u [12], stranica 158, Theorem 6.2. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Korolar 1.2.24. *Neka je D integralna domena i $f, g \in D[X]$. Nadalje, neka je $g \neq 0$. Tada postoje $a \in D \setminus \{0\}$ i polinomi $q, r \in D[X]$ takvi da*

$$af = qg + r \qquad i \qquad r = 0 \quad ili \quad \deg(r) < \deg(g).$$

Dokaz. Slično kao dokaz prethodnog teorema, samo malo "pazimo" na vodeći koeficijent polinoma g. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Korolar 1.2.25. *Neka je R prsten i neka je $f \in R[X]$. $\alpha \in R$ je nultočka polinoma f ako i samo ako polinom $X - \alpha$ dijeli polinom f u $R[X]$.*

Dokaz. Ako je f nul–polinom tvrdnja je očita. Pretpostavimo da f nije nul–polinom. Neka je $g = X - \alpha$. Prema teremu o dijeljenju polinoma znamo da postoje jedinstveni polinomi $q, r \in R[X]$ takvi da je $f = qg + r$ i $r = 0$ ili $\deg(r) < \deg(g)$. Vidimo da je $\deg(g) = 1$. Stoga je ili $r = 0$ ili $\deg(r) = 0$, u svakom slučaju je $r \in R$. Pretpostavimo da je $f(\alpha) = 0$. Evaulacijom jednadže $f = qg + r$ u točki α tada dobivamo da je $0 = r$, tj. $f = qg$, odnosno $X - \alpha = g \mid f$. Obratno, ako $X - \alpha \mid f$, to znači da je $r = 0$. Opet, evaulacijom iste jednadžbe u točki α dobivamo da je $f(\alpha) = r = 0$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Korolar 1.2.26. *Neka je D integralna domena i $f \in D[X]$ različit od nul–polinoma. Tada f ima najviše* $\deg(f)$ *nultočaka u D.*

Dokaz. Indukcija po $\deg(f)$. Ukoliko je $\deg(f) = 0$, polinom f nema niti jednu nultočku jer je jednak nekoj konstanti iz D koja je različita od nule. Dakle, tvrdnja vrijedi. Pretpostavimo da tvrdnja vrijedi za sve polinome stupnja n, za neki $n \in \mathbb{Z}_{\geq 0}$. Neka je $\deg(f) = n + 1$. Ukoliko f nema nultočaka u D gotovi smo. Neka je $\alpha \in D$ nultočka polinoma f. Prema prethodnom korolaru tada znamo da $X - \alpha \mid f$. Neka je $f = (X - \alpha)\, g$, gdje je $g \in D[X]$. Kako je D integralna domena i $\deg(X - \alpha) = 1$ znamo da je $\deg(g) = n$. No, prema pretpostavci, polinom g ima najviše n nultočaka u D, zaključujemo da polinom f ima najviše $n + 1$ nultočaka u D. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Korolar 1.2.27. *Neka je K polje s beskonačno mnogo elemenata te neka je F polinom u $K[X_1, X_2, \ldots, X_n]$. Ukoliko je $F(a_1, a_2, \ldots, a_n) = 0$, za sve $a_1, a_2, \ldots, a_n \in K$, onda je $F = 0$.*

Dokaz. Ukoliko je $n = 1$ tvrdnja je direktna posljedica prethodnog korolara. Neka je $n > 1$ te neka tvrdnja vrijedi za $n - 1$. Pretpostavimo suprotno, tj. da je $F \neq 0$. Tada je polinom F pozitivnog stupnja u barem jednom varijabli, bez smanjenja općenitosti pretpostavimo da je to varijabla X_n. Tada postoje $m \in \mathbb{N}$ i $F_0, F_1, \ldots, F_m \in K[X_1, X_2, \ldots, X_{n-1}]$, $F_m \neq 0$, takvi da je $F = \sum_{i=0}^{m} F_i X_n^i$. Kako je $F_m \neq 0$ i tvrdnja vrijedi za $n - 1$ vidimo da postoje $a_1, a_2, \ldots, a_{n-1} \in K$ takvi da je $F_m(a_1, a_2, \ldots, a_{n-1}) \neq 0$. Sada smo dobili ne–nul–polinom $F(a_1, a_2, \ldots, a_{n-1}, X_n)$, u jednoj varijabli, X_n, koji ima beskonačno mnogo nultočaka, što je kontradikcija. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Definicija 1.2.28. *Polje K je* ***algebarski zatvoreno*** *ako svaki ne–konstantni polinom iz $K[X]$ ima nultočku u K.*

Propozicija 1.2.29. *Svako algebarski zatvoreno polje ima beskonačno mnogo elemenata.*

Dokaz. Neka je K algebarski zatvoreno polje. Pretpostavimo da K ima konačno mnogo elemenata, tj. neka su, za $n \in \mathbb{N}$, $k_1, k_2 \ldots, k_n$ svi elementi polja K. Promotrimo polinom $(X - k_1)(X - k_2) \cdots (X - k_n) + 1$. On se nalazi u $K[X]$, no očito nema nultočku u K jer nije djeljiv s niti jednim od polinoma $X - k_1$, $X - k_2$, $\ldots$, $X - k_n$. Kontradikcija! Dakle, polje K ima beskonačno mnogo elemenata. $\mathfrak{Q.E.D.}$

Polje kompleksnih brojeva, $\mathbb{C}$, je primjer algebarski zatvorenog polja.

Definicija 1.2.30. *Neka je R prsten i $f \in R[X]$ različit od nul–polinoma. Neka je $\alpha \in R$ takav da je $f(\alpha) = 0$.* ***Multiplicitet*** *nultočke α polinoma f je najmanji prirodan broj n takav da $(X - \alpha)^n$ dijeli f i $(X - \alpha)^{n+1}$ ne dijeli f.*

Napomena 1.2.31. *Sada lako vidimo da u algebarski zatvorenom polju K, svaki polinom f iz $K[X]$ ima jedinstven prikaz u obliku $f = \alpha \prod_{k=1}^{m} (X - \alpha_k)^{n_k}$. Pri tome je $m \in \mathbb{N}$, α je vodeći koeficijent polinoma f, $\alpha_1, \alpha_2, \ldots, \alpha_m$ su sve međusobno različite nultočke polinoma f, redom s multiplicitetima $n_1, n_2, \ldots, n_m$. Primijetimo još da je $n_1 + n_2 + \ldots + n_m = \deg(f)$.*

Derivacija polinoma

Definicija 1.2.32. *Neka je R prsten i neka je $f \in R[X]$. Promatrajmo polinom f u obliku $f = \sum_{k \geq 0} r_k X^k$. (Jasno, ako je f nul–polinom suma je prazna, inače suma ide do $\deg(f)$.)* ***Derivacija*** *polinoma f, u oznaci $\frac{\partial f}{\partial X}$, kraće f_X ili f', je polinom $\sum_{k \geq 1} k r_k X^{k-1}$. Ako je $n \in \mathbb{N}$ i $f \in R[X_1, X_2, \ldots, X_n]$ tada, za $k \in \{1, 2, \ldots, n\}$, definiramo $\frac{\partial f}{\partial X_k}$, odnosno f_{X_k}, kao derivaciju polinoma f u varijabli X_k nad prstenom $R[X_1, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n]$. To je* ***parcijalna derivacija*** *polinoma f po varijabli X_k.*

Propozicija 1.2.33. *Neka je R prsten i neka su $f, g, h \in R[X]$. Tada vrijedi:*

(1) $(\alpha)_X = 0, \ \forall \alpha \in R,$

(2) $(\alpha f + \beta g)_X = \alpha f_X + \beta g_X,\ \forall \alpha, \beta \in R,$

(3) $(fg)_X = f_X g + f g_X,$

(4) $(f^m)_X = m f^{m-1} f_X,\ \forall m \in N,$

(5) ako je $h(X) = g(f(X))$, *onda je* $h_X(X) = g_X(f(X))\, f_X(X)$.

Neka je $n \in \mathbb{N}$, $F \in R[X_1, X_2, \ldots X_n]$ *te* $G_1, G_2, \ldots, G_n \in R[X]$, *tada:*

(6) $F(G_1, G_2, \ldots, G_n)_X = \sum_{k=1}^{n} F_{X_k}(G_1, G_2, \ldots, G_n)(G_k)_X,$

(7) $(F_{X_k})_{X_l} = (F_{X_l})_{X_k},\ \forall k, l \in \{1, 2, \ldots, n\}.$

Konačno, ako je F *homogen polinom stupnja* d, *vrijedi tkzv.* ***Eulerov teorem****:*

(8) $dF = \sum_{k=1}^{n} X_i F_{X_i}.$

Dokaz. Sve tvrdnje slijede direktno iz definicije, uz elementarni račun. Q.E.D.

Definicija 1.2.34. *Neka je* R *prsten i* $f \in R[X]$. *Definiramo* ***derivacije višeg reda*** *i to kako sljedi:*

$$f^{(0)} := f \qquad te \qquad \frac{\partial^m}{X^m} f = f^{(m)} := \left(f^{(m-1)}\right)',\ \forall m \in \mathbb{N}.$$

Nadalje, za $n \in \mathbb{N}$ *te* $F \in R[X_1, X_2, \ldots, X_n]$, *neka je* $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$, *definiramo:*

$$\frac{\partial^{|\alpha|}}{\partial X^\alpha} F = \frac{\partial^{\alpha_1+\alpha_2+\ldots+\alpha_n}}{\partial X_1^{\alpha_1} \partial X_2^{\alpha_2} \cdots \partial X_n^{\alpha_n}} F := \frac{\partial^{\alpha_1}}{\partial X_1^{\alpha_1}} \left(\frac{\partial^{\alpha_2}}{\partial X_2^{\alpha_2}} \left(\cdots \left(\frac{\partial^{\alpha_n}}{\partial X_n^{\alpha_n}} F \right) \right) \right).$$

Poredak u zadnjemu je nebitan, radi prethodne propozicije, tj. tvrdnje (7).

Propozicija 1.2.35 (Taylorov razvoj)**.** *Neka je* D *integralna domena karakteristike* 0 *i neka je* K *pripadajuće polje razlomaka. Tada je* $\operatorname{char}(K) = 0$. *Neka je* $f \in D[X]$ *različit od nul–polinoma te neka je* $d = \deg(f)$. *Za svaki* $a \in D$ *tada, gledajući u* $K[X]$, *vrijedi:*

$$f(X) = \sum_{k=0}^{d} \frac{f^{(k)}(a)}{k!} (X - a)^k.$$

Analogno, neka je $n \in \mathbb{N}$ *te neka je* $F \in D[X_1, X_2, \ldots, X_n]$ *i* $(a_1, a_2, \ldots, a_n) \in D^n$*, tada:*

$$F = \sum_{\alpha=(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}} b_\alpha (X_1 - a_1)^{\alpha_1} (X_2 - a_2)^{\alpha_2} \cdots (X_n - a_n)^{\alpha_n},$$

gdje je

$$b_\alpha = \frac{1}{\alpha_1! \alpha_2! \cdots \alpha_n!} \frac{\partial^{|\alpha|}}{\partial X_1^{\alpha_1} \partial X_2^{\alpha_2} \cdots \partial X_n^{\alpha_n}} F(a_1, a_2, \ldots, a_n).$$

Jasno, u gornjoj sumi, samo je konačno mnogo članova b_α *različito od nule.*

Dokaz. Činjenica da iz $\operatorname{char}(D) = 0$ slijedi da je $\operatorname{char}(K) = 0$ je očita. Naime, vrijedi i više, ako je $\operatorname{char}(D) = p$, za neki $p \in \mathbb{Z}_{\geq 0}$, onda je i $\operatorname{char}(K) = p$, jer je u svakom prstenu njegova karakteristika (ako nije nula) jednaka najmanjem prirodnom broju p takvom da je $p \cdot 1 = 0$. Taylorov razvoj za polinome u jednoj varijabli se vidi direktno deriviranjem, dok za n varijabli jednostavno primijenimo činjenicu za jednu varijablu n puta, nad odgovarajućom integralnom domenom. Q.E.D.

Lema 1.2.36. *Neka je* D *domena jedinstvene faktorizacije, karakteristike* 0*. Neka je* $g \in D[X]$ *ireducibilan polinom pozitivnog stupnja i neka je* $f \in D[X]$*. Tada:*

$$g^2 \mid f \qquad \Longleftrightarrow \qquad g \mid f \quad i \quad g \mid f'.$$

Dokaz. Pretpostavimo da $g \mid f$ i $g \mid f'$. Dakle, postoje h, $h_1 \in D[X]$ takvi da je $f = hg$ i $f' = h_1 g$. Deriviranjem prve jednadžbe dobivamo da je $f' = h'g + hg'$, uvrštavanjem druge slijedi $h_1 g = h'g + hg' \Longrightarrow (h_1 - h')\, g = hg'$. Dakle, $g \mid hg'$. Kako je D integralna domena dobivamo da je $g' \neq 0$, nadalje, jer je $\operatorname{char}(D) = 0$ vidimo da je $\deg(g') = \deg(g) - 1 \geq 0$. Polinom g je ireducibilan i g' je ne–nul–polinom manjeg stupnja od stupnja polinoma g. Zaključujemo da su polinomi g i g' relativno prosti, tj. nemaju zajedničkih faktora u $D[X]$. Dakle, iz $g \mid hg'$, slijedi $g \mid h$, a kako je $f = hg$, imamo da $g^2 \mid f$. Obratno, $g^2 \mid f$, to znači da postoji $h_2 \in D[X]$ takav da je $f = h_2 g^2$, deriviranjem dobivamo da je $f' = h_2' g^2 + 2h_2 gg'$. Konačno, $g \mid f'$. Q.E.D.

Lema 1.2.37. *Neka je R prsten i neka su $f, g \in R[X]$ te neka je $m \in \mathbb{N}$. Tada:*

$$(fg)^{(m)} = \sum_{k=0}^{m} \binom{m}{k} f^{(k)} g^{(m-k)}.$$

Dokaz. Matematičkom indukcijom, uz elementarni račun. Q.E.D.

Teorem 1.2.38. *Neka je D domena jedinstvene faktorizacije, karakteristike 0. Neka je $g \in D[X]$ ireducibilan polinom pozitivnog stupnja i neka je $f \in D[X]$. Tada, za svaki $m \in \mathbb{N}$ vrijedi:*

$$g^m \mid f \qquad \Longleftrightarrow \qquad g \mid f,\ g \mid f',\ \ldots,\ g \mid f^{(m-1)}.$$

Dokaz. Pretpostavimo najprije da $g^m \mid f$, tada postoji $h \in D[X]$ takav da je $f = g^m h$. No, sada možemo primijeniti lemu 1.2.37 na polinome g^m i h pa odmah vidimo da $g \mid f^{(k)}$, za svaki $k \in \{0, 1, \ldots, m-1\}$. Obratno, dokaz provodimo matematičkom indukcijom. Za $m = 1$ tvrdnja je očita, za $m = 2$ tvrdnja je dokazana u lemi 1.2.36. Pretpostavimo da tvrdnja vrijedi za neki $m \in \mathbb{N}$, $m \geq 2$, želimo ju dokazati za $m + 1$. Dakle, znamo da $g \mid f^{(k)}$, za sve $k \in \{0, 1, \ldots, m\}$, prema pretpostavci tada znamo da $g^m \mid f$. Dakle, dovoljno nam je (a i nužno) pokazati da iz $g^m \mid f$ i $g \mid f^{(m)}$ slijedi da $g^{m+1} \mid f$. Neka su, slično kao u dokazu leme 1.2.36, $h, h_1 \in D[X]$ takvi da je $f = hg^m$ i $f^{(m)} = h_1 g$. Sada, deriviranjem prve jednadže m puta, uvrštavanjem druge te primjenom leme 1.2.37 dobivamo:

$$h_1 g = \sum_{k=0}^{m} \binom{m}{k} h^{(k)} \left(g^m\right)^{(m-k)}.$$

Lijeva strana gornje jednakosti je djeljiva s g, svi članovi sume gornje jednakosti, osim eventualnog onog za $k = 0$ su djeljivi s g, dakle, on je isto djeljiv s g. Odnosno, zaključujemo da $g \mid h\left(g^m\right)^{(m)}$. Primijenimo sada lemu 1.2.37 na polinome g^{m-1} i g, slijedi:

$$\left(g^{m-1} g\right)^{(m)} = \sum_{k=0}^{m} \binom{m}{k} \left(g^{m-1}\right)^{(k)} g^{(m-k)}.$$

Za $k \in \{0, 1, \ldots, m-2\}$ imamo da $g \mid \left(g^{m-1}\right)^{(k)}$, a za $k = m$ imamo da $g \mid g^{(0)} = g$. Dakle, dobili smo da $g \mid h\left(g^{m-1}\right)^{(m-1)} g'$. Kao u dokazu leme 1.2.36 znamo da su g i g' relativno

prosti. Pretpostavimo da g i $\left(g^{m-1}\right)^{(m-1)}$ nisu relativno prosti. Kako je g ireducibilan polinom pozitivnog stupnja zaključujemo da tada $g \mid \left(g^{m-1}\right)^{(m-1)}$, no prema pretpostavci indukcije tada dobivamo da $g^m \mid g^{m-1}$, što je kontradikcija. Dakle, g i $\left(g^{m-1}\right)^{(m-1)} g'$ su relativno prosti pa mora $g \mid h$. Odnosno, konačno imamo da $g^{m+1} \mid f$. Q.E.D.

Korolar 1.2.39. *Neka je D domena jedinstvene faktorizacije, karakteristike 0. Neka je $f \in D[X]$ i $m \in N$. Vrijedi da je $a \in D$ nultočka polinoma f, multipliciteta m ako i samo ako je $f(a) = f'(a) = \ldots = f^{(m-1)}(a) = 0$ i $f^{(m)}(a) \neq 0$.*

Dokaz. Slijedi direktno primjenom prethodnog teorema i korolara 1.2.25. Q.E.D.

Primjer 1.2.40. Neka je R prsten i neka je $\text{char}(R) = p$, gdje je p prost broj. Primijetimo da je $\mathbb{Z}/p\mathbb{Z}$ primjer takvog prstena, štoviše, polja. Stupanj polinoma $f = X^p \in R[X]$ je jednak p. No, $f' = p \cdot X^{p-1} = 0$, jer je $\text{char}(R) = p$. Dakle, da bismo mogli zaključit da je derivacija polinoma pozitivnog stupnja ne–nul–polinom, nužno nam je da se nalazimo u prstenu karakteristike nula.

1.3 Hilbertov teorem o bazi

Definicija 1.3.1. *Za prsten R kažemo da je **Noetherin prsten** ako je svaki ideal u R konačno generiran.*

Polja i domene glavnih ideala su primjeri Noetherinih prstenova.

Teorem 1.3.2 (Hilbertov teorem o bazi)**.** *Neka je R Noetherin prsten, tada je, za svaki $n \in \mathbb{N}$, $R[X_1, X_2, \ldots, X_n]$ Noetherin prsten.*

Dokaz. Dovoljno je dokazati da ako je R Noetherin prsten da je tada i $R[X]$ Noetherin prsten. Tvrdnja će tada za prsten polinoma u $n \in \mathbb{N}$ varijabli slijediti po principu matematičke indukcije. Dakle, neka je R Noetherin prsten. Neka je $I \subseteq R[X]$ ideal. Ukoliko

je $I = (0)$ tvrdnja je očita, stoga pretpostavimo da je $I \neq (0)$. Za polinom $f \in R[X]$ uvedimo oznaku $\langle f \rangle$, za vodeći koeficijent polinoma f. Neka je $J \subseteq R$ skup svih vodećih koeficijenata svih polinoma iz I. J je ideal u R. Naime, neka je $a \in J$ te neka je $r \in R$. Postoji $f \in I$ takav da je $\langle f \rangle = a$, sada, pošto je I ideal u $R[X]$ zaključujemo da je i $rf \in I$, odnosno $ra = \langle rf \rangle \in J$. R je Noetherin prsten pa postoje $d \in \mathbb{N}$ i $f_1, f_2, \ldots, f_d \in I$ takvi da je $J = (\langle f_1 \rangle, \langle f_2 \rangle, \ldots, \langle f_d \rangle)$, naravno, možemo pretpostaviti da su svi ovi polinomi različiti od nul–polinoma. Neka je $M = \max\{\deg(f_1), \deg(f_2), \ldots, \deg(f_d)\}$. Za svaki $k \in \mathbb{Z}_{\geq 0}$, takav da je $k \leq M$, neka je $J_k \subseteq R$ skup svih vodećih koeficijenata svih polinoma iz I, stupnja najviše k. Kao i ranije, zaključujemo da je J_k ideal u R. Primijetimo da je $J_0 \subseteq J_1 \subseteq \ldots \subseteq J_M$. Neka je $m \in \mathbb{Z}_{\geq 0}$ najmanji takav da je $J_m \neq (0)$, primijetimo tada da je $J_k = (0)$, za svaki $k \in \mathbb{Z}_{\geq 0}$, $k < m$. Neka je, za $k \in \mathbb{Z}_{\geq 0}$, $m \leq k \leq M$, $d_k \in \mathbb{N}$ te $f_{k1}, f_{k2}, \ldots, f_{kd_k} \in R[X]$ takvi da je $J_k = (\langle f_{k1} \rangle, \langle f_{k2} \rangle, \ldots, \langle f_{kd_k} \rangle)$. Tvrdimo da je:

$$I = (f_1, f_2, \ldots, f_d, f_{m1}, f_{m2}, \ldots, f_{md_m}, \ldots, f_{M1}, f_{M2}, \ldots, f_{Md_M}).$$

Označimo desni ideal s I'. Neka je $g \in I$, dovoljno je pokazati da stupanj polinoma g možemo po volji smanjiti oduzimajući od njega polinome iz I'. Time dobivamo da je $I \subseteq I'$, dok je očito $I' \subseteq I$, tj. $I = I'$. No, to je očito. Ako je $g = 0$ gotovi smo. Neka je $g \neq 0$. Ukoliko je $\deg(g) > M$, jasno je da možemo izabrati polinom $q_1, q_2, \ldots, q_d \in R[X]$ takve da polinom $\sum_{l=1}^{d} q_l f_l$ ima vodeći koeficijent jednak $\langle g \rangle$ te da je istog stupnja kao polinom g. Oduzimanjem toga polinoma od polinoma g smanjili smo stupanj polinomu g. Ponavljamo opisani proces sve dok nije $g = 0$ ili $\deg(g) \leq M$. Ako je $g = 0$ gotovi smo, a ako nije, neka je $\deg(g) = k$. Tada je $m \leq k \leq M$, radi definicije skupova J_k. No, sada jednostavno na već opisani način "poništimo" vodeći koeficijent polinoma g, tako da ga promatramo u idealu J_k (Ranije smo to napravili u idealu J). Jasno je da ćemo ovim postupkom nakon najviše $\deg(g) + 1$ koraka dobiti da je $g = 0$. $\mathfrak{Q.E.D.}$

Napomena 1.3.3. *Primijetimo da je za svako polje K i svaki $n \in \mathbb{N}$, $K[X_1, X_2, \ldots, X_n]$ Noetherin prsten.*

1.4 Algebarski skupovi

Neka je K polje te neka je $n \in \mathbb{N}$. S $\mathbb{A}^n(K)$ ili kraće, kada se polje K podrazumijeva, $\mathbb{A}^n$, ćemo označavati Kartezijev produkt polja K sa samim sobom, n puta. Dakle, $\mathbb{A}^n$ je skup svih uređenih n-torki elemenata polja K.

Definicija 1.4.1. ***Afini n-dimenzionalni prostor nad poljem*** *K jest $\mathbb{A}^n(K)$. Elemente toga prostora zvati ćemo točkama. Specijalno, $\mathbb{A}^1$ je afini pravac, $\mathbb{A}^2$ je afina ravnina.*

Prisjetimo se, neka je $f \in K[X_1, X_2, \ldots, X_n]$. Točka $x = (x_1, x_2, \ldots, x_n) \in \mathbb{A}^n(K)$ je nultočka polinoma f, ako je $f(x) = f(x_1, x_2, \ldots, x_n) = 0$.

Definicija 1.4.2. *Ako f nije konstanta (tj. ako je pozitivnog stupnja) onda skup svih nultočaka polinoma f nazivamo* ***afina hiperploha*** *određena polinomom f, to označavamo s $V(f)$.*

Napomena 1.4.3. *Ako je f konstanta i $f \neq 0$, onda je $V(f) = \emptyset$, a ako je $f = 0$, onda je $V(f) = \mathbb{A}^n$. Za $n = 2$ hiperplohe nazivamo afine (ravninske) krivulje.*

Definicija 1.4.4. *Neka je K polje, $n \in \mathbb{N}$ te $S \subseteq K[X_1, X_2, \ldots, X_n]$ bilo koji skup polinoma.* ***(Afini) algebarski skup*** *određen sa S je $V(S) := \{x \in \mathbb{A}^n(K) \,:\, f(x) = 0, \forall f \in S\}$.*

Primijetimo da je $V(S) = \bigcap_{f \in S} V(f)$. Ukoliko je skup S konačan, tj. postoji $k \in \mathbb{N}$ takav da je $S = \{f_1, f_2, \ldots, f_k\}$, za neke $f_1, f_2, \ldots, f_k \in K[X_1, X_2, \ldots, X_n]$, onda jednostavno pišemo $V(S) = V(f_1, f_2, \ldots, f_k)$.

Lema 1.4.5. *Uz oznake iz prethodne definicije, neka je $I = \langle S \rangle$ (Ideal u $K[X_1, X_2, \ldots, X_n]$ generiran skupom S, ako je $S = \emptyset$, stavimo da je $I = (0)$.), tada je $V(I) = V(S)$.*

Dokaz. Očito je $S \subseteq I$, stoga, ako je $x \in V(I)$, tj. $f(x) = 0,\ \forall f \in I$, onda je i $f(x) = 0$, za sve $f \in S$, tj. $x \in V(S)$. Dakle, imamo da je $V(I) \subseteq V(S)$. Obratno, znamo da je svaki element iz I oblika $\sum_{k=1}^{m} f_k g_k$, gdje su $m \in \mathbb{N}$, $f_1, f_2, \ldots, f_m \in S$ te $g_1, g_2, \ldots, g_m$ polinomi iz $K[X_1, X_2, \ldots, X_n]$. Konačno, vidimo da ako je $x \in V(S)$ onda je i $x \in V(I)$, radi oblika elemenata skupa I. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Upravo dokazana lema nam govori da je svaki algebarski skup zapravo jednak skupu $V(I)$, gdje je I neki ideal u $K[X_1, X_2, \ldots, X_n]$.

Definicija 1.4.6. *Neka je K polje, $n \in \mathbb{N}$ te $V \subseteq \mathbb{A}^n(K)$ bilo koji skup točaka. Definiramo* $I(V) := \{f \in K[X_1, X_2, \ldots, X_n] \ :\ f(x) = 0,\ \forall x \in V\}$.

Primijetimo da je $I(V)$ ideal u $K[X_1, X_2, \ldots, X_n]$, za svaki skup točaka V iz $\mathbb{A}^n$.

Definicija 1.4.7. *Neka je R prsten i neka je $I \subseteq R$ ideal. Definiramo* ***radikal*** *ideala I kao skup* $\mathrm{Rad}(I) := \left\{a \in R \ :\ \exists k \in \mathbb{N},\ a^k \in I\right\}$. *Kažemo da je ideal I* ***radikalan ideal*** *ako je* $\mathrm{Rad}(I) = I$.

Primijetimo da je $\mathrm{Rad}(I)$ ideal u R. Naime, ako su $a, b \in R$ i $k, l \in \mathbb{N}$ takvi da je $a^k, b^l \in I$, onda je $(a+b)^{k+l} \in I$, što se vidi direktno primjenom binomnog teorema i toga da je I ideal. Također, jasno je da je uvijek $I \subseteq \mathrm{Rad}(I)$. Nadalje, $\mathrm{Rad}(I)$ je radikalan ideal, što se vidi direktno iz definicije. Primijetimo još i da ako je I prost ideal da je on radikalan, to se također vidi direktno iz definicije prostog i radikalnog ideala.

Propozicija 1.4.8. *Neka je K polje i $n \in \mathbb{N}$.*

(1) Ako su I i J ideali u $K[X_1, X_2, \ldots, X_n]$ takvi da je $I \subseteq J$, onda je $V(I) \supseteq V(J)$.

(2) Ako su V i W skupovi točaka u $\mathbb{A}^n(K)$ takvi da je $V \subseteq W$, onda je $I(V) \supseteq I(W)$.

(3) Presjek proizvoljne (neprazne) familije algebarskih skupova jest algebarski skup.

(4) Konačna unija algebarskih skupova jest algebarski skup.

(5) $V(0) = \mathbb{A}^n(K)$, $V(1) = \emptyset$, $V(X_1 - x_1, X_2 - x_2, \ldots, X_n - x_n) = \{(x_1, x_2, \ldots, x_n)\}$, *pri čemu su* $x_1, x_2, \ldots, x_n \in K$.

(6) Svaki konačni skup točaka u $\mathbb{A}^n(K)$ *je algebarski skup.*

(7) $I(\emptyset) = K[X_1, X_2, \ldots, X_n]$, $I(\{(x_1, x_2, \ldots, x_n)\}) = (X_1 - x_1, X_2 - x_2, \ldots, X_n - x_n)$, *za* $x_1, x_2, \ldots, x_n \in K$. *Ukoliko je polje* K *beskonačno, onda je* $I(\mathbb{A}^n(K)) = (0)$.

(8) $I(V(S)) \supseteq S$, *za svaki skup polinoma,* S. $V(I(W)) \supseteq W$, *za svaki skup točaka,* W. *Također,* $V(I(V(S))) = V(S)$ *te* $I(V(I(W))) = I(W)$, *za svaki skup polinoma,* S *i za svaki skup točaka,* W.

(9) Ideal $I(V)$ *je radikalan za svaki skup točaka* $V \subseteq \mathbb{A}^n(K)$.

(10) Svaki algebarski skup, različit od praznog skupa i cijelog afinog prostora, jednak je presjeku konačnog broja afinih hiperploha.

Dokaz.

(1) Očito, ako je točka nultočka svim polinomima nekog skupa, onda je ona nultočka i svim polinomima svakog podskupa tog skupa.

(2) Također očito, ako se polinom poništava na nekom skupu, onda se poništava i na svakom njegovom podskupu. Pri tome podrazumijevamo da se polinom poništava na skupu, ako je jednak nuli u svakoj točki toga skupa.

(3) Neka je $\{I_\lambda\}_{\lambda\in\Lambda}$ neprazna familija ideala u $K[X_1, X_2, \ldots, X_n]$, gdje je Λ neki indeksni skup. Tada je

$$\bigcap_{\lambda\in\Lambda} V(I_\lambda) = V\left(\sum_{\lambda\in\Lambda} I_\lambda\right),$$

gdje je $\sum_{\lambda\in\Lambda} I_\lambda = \left\{ \sum_{k=1}^{m} f_k \ : \ f_k \in I_{\lambda_k},\ \lambda_k \in \Lambda,\ k \in \{1, 2, \ldots, m\},\ m \in \mathbb{N} \right\}$ ideal generiran skupom $\bigcup_{\lambda\in\Lambda} I_\lambda$.

(4) Dovoljno je pokazati da je unija dva algebarska skupa opet algebarski skup. Neka su I i J ideali u $K[X_1, X_2, \ldots, X_n]$. Tvrdimo da je $V(I) \cup V(J) = V(IJ)$, gdje je $IJ = \left\{ \sum_{k=1}^{m} f_k g_k \ : \ f_k \in I,\ g_k \in J,\ k \in \{1, 2, \ldots, m\},\ m \in \mathbb{N} \right\}$ umnožak ideala I i J, što je također ideal. Neka je $x \in V(IJ)$, ako je $x \in V(I)$ gotovi smo. Pretpostavimo da $x \notin V(I)$. Tada postoji $f \in I$ takav da je $f(x) \neq 0$. No, sada, kako je $fg \in IJ$, za sve $g \in J$, $x \in V(IJ)$ i kako je K polje, a time specijalno i integralna domena, dobivamo da je $g(x) = 0$, za sve $g \in J$. Dakle, $x \in V(J)$. Ovime smo dobili da je $V(IJ) \subseteq V(I) \cup V(J)$. Obratno, neka je $x \in V(I) \cup V(J)$. Očito je tada $x \in V(IJ)$, to se vidi iz oblika elemenata ideala IJ. Dakle, $V(I) \cup V(J) = V(IJ)$.

(5) Očito.

(6) Iz (5) vidimo da je prazan skup algebarski skup i da je svaka točka algebarski skup. Također, iz (4) znamo da je konačna unija algebarskih skupova također algebarski skup. Dakle, svaki konačni skup točaka je algebarski skup.

(7) Prva tvrdnja je očita. Nadalje, jednostavnosti radi, označimo $x = (x_1, x_2, \ldots, x_n)$ te $I_x = (X_1 - x_1, X_2 - x_2, \ldots, X_n - x_n)$. Želimo pokazati da je $I(\{x\}) = I_x$. Jasno je da ako je $f \in I_x$ da je onda $f(x) = 0$, tj. $f \in I(\{x\})$. Obratno, neka je $f \in I(\{x\})$. No, sada napravimo Taylorov razvoj polinoma f oko točke x i odmah vidimo da on mora biti u I_x. Ovime je i druga tvrdnja pokazana. Neka je sada polje K beskonačno i neka je $f \in I(\mathbb{A}^n(K))$. Želimo pokazati da je $f = 0$. No, to je upravo tvrdnja korolara 1.2.27.

(8) Prva dva svojstva su očita, dok druga dva slijede primjenom prva dva i već pokazanih svojstava u (1) i (2).

(9) Očito, ako je $f^k(x) = 0$, za neki $k \in \mathbb{N}$ i neku točku $x \in V$, onda je i $f(x) = 0$, zato jer je K polje, a time i integralna domena.

(10) Neka je I ideal u $K[X_1, X_2, \ldots, X_n]$ takav da je $V(I)$ neprazan i različit od cijelog afinog prostora $\mathbb{A}^n(K)$. Prema Hilbertovom teoremu o bazi, tj. prema napomeni 1.3.3, znamo da postoje $m \in \mathbb{N}$ i $f_1, f_2, \ldots, f_m \in K[X_1, X_2, \ldots, X_n]$ takvi da je $I = (f_1, f_2, \ldots, f_m)$. Sada prema lemi 1.4.5 i dokazu točke (3) vidimo da je $V(I) = V(f_1, f_2, \ldots, f_m) = \bigcap_{k=1}^{m} V(f_k)$. Radi uvjeta na skup $V(I)$ lako vidimo da među polinomima $f_1, f_2, \ldots, f_m$ nema konstantnih. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Napomena 1.4.9. *Svojstva (3) i (4) nam govore da postoji (jedinstvena) topologija na prostoru $\mathbb{A}^n(K)$ čija familija zatvorenih skupova je jednaka familiji algebarskih skupova. Tu topologiju nazivamo topologijom Zariskoga.*

Propozicija 1.4.10. *Neka je I ideal u prstenu R i neka je $\pi : R \to R/I$ kanonski epimorfizam.*

(a) Neka je J' ideal u R/I, tada je $J = \pi^{-1}(J')$ ideal u R koji sadrži I. Obratno, neka je J ideal u R koji sadrži I, tada je $J' = \pi(J)$ ideal u R/I.

(b) Neka je J' ideal u R/I i neka je $J = \pi^{-1}(J')$. Ideal J' je radikalan (odnosno prost, odnosno maksimalan) ako i samo ako je ideal J radikalan (odnosno prost, odnosno maksimalan).

(c) Neka je J konačno generiran ideal u R koji sadrži I. Tada je $J' = \pi(J)$ konačno generiran ideal u R/I.

Dokaz.

(a) Tvrdnja da su J i J' ideali je očita, također, kako je $\pi^{-1}(0_{R/I}) = I$, očita je i tvrdnja da ideal J sadrži I.

(b) Pretpostavimo da je J' radikalan ideal, to znači da za svaki $a \in R$, ako postoji $n \in \mathbb{N}$ takav da je $(a+I)^n \in J'$, onda je $a + I \in J'$. No, sada je jasno da to vrijedi ako i samo ako je za svaki $a \in R$ za koji postoji $n \in \mathbb{N}$ takav da je $a^n \in J$, da je onda $a \in J$. Tvrdnja za proste ideale se dokazuje slično. Ukoliko je J' maksimalan ideal, znamo da je J' neprazan, nije jednak R/I te ne postoji pravi ideal u R/I kojemo je J' pravi podskup. Lako se vidi da to vrijedi ako i samo ako iste tvrdnje vrijede za ideal J, tj. J je maksimalan ideal u R.

(c) Tvrdnja je očita, naime, ako je $k \in \mathbb{N}$ i $r_1, r_2, \ldots, r_k \in R$ generatori za J, jasno je da su onda $r_1 + I, r_2 + I, \ldots, r_k + I$ generatori za J'. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Napomena 1.4.11. *Prema prethodnoj propoziciji lako vidimo sljedeće, ako je R Noetherin prsten i I ideal u R, tada je R/I Noetherin prsten. Također, za polje K, $n \in \mathbb{N}$, I ideal u $K[X_1, X_2, \ldots, X_n]$, $K[X_1, X_2, \ldots, X_n]/I$ je Noetherin prsten.*

1.5 Hilbertov teorem o nulama

Prije glavnog rezultata, tj. Hilbertovog teorema o nulama, odnosno Nullstellensatz teorema, uvesti ćemo algebarski aparat potreban za dokaz istoga. Također, iskazati ćemo i dokazati nekoliko pomoćnih tvrdnji, među kojima će biti i tkzv. slabi Nullstellensatz. Prije uvođenja novih pojmova, iskažimo i dokažimo neke (pomoćne) tvrdnje koje će nam biti od koristi, a za koje već imamo na raspolaganju potrebnu algebru.

Lema 1.5.1. *Neka je R domena glavnih ideala i neka je P neprazan, prost ideal u R. Tada je P generiran ireducibilnim elementom u R i P je maksimalan ideal u R.*

Dokaz. Kako je R DGI, postoji $a \in R$ takav da je $P = (a)$. Znamo da je $a \neq 0$, jer je $P \neq (0)$. Nadalje, pretpostavimo da je Q ideal u R takav da je $P \subseteq Q \subseteq R$. Moramo dokazati da je a ireducibilan u R i da je $Q = R$ ili $Q = P$. Neka je $b \in R$ takav da je $Q = (b)$. Jasno je, $b \neq 0$. Neka je $a = cd$ za neke $c, d \in R$. $cd = a \in (a)$ i (a) je prost, dakle, ili je $c \in (a)$ ili je $d \in (a)$. Bez smanjenja općenitosti pretpostavimo da je $c \in (a)$, tada postoji $e \in R$ takav da je $c = ae$. Sada je $a = cd = aed$, R je DGI, tj. specijalno je R integralna domena pa vrijedi zakon kraćenja, dakle $ed = 1$, tj. $d \in R^*$. Zaključujemo, a je ireducibilan, jer a ne može biti invertibilan, pošto je $P = (a)$ prost ideal u R i samim time različit od R. Nadalje, kako je $(a) \subseteq (b)$ zaključujemo da je $a \in (b)$ pa postoji $f \in R$ takav da je $a = bf$. Već znamo da je a ireducibilan, dakle, ili $b \in R^*$ ili $f \in R^*$. Ako je $b \in R^*$, onda je $Q = (b) = R$, a ako je $f \in R^*$, onda je $b = af^{-1}$ pa je $b \in (a)$, odnosno $Q = (b) = (a) = P$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Lema 1.5.2. *Neka je K polje. Tada $K[X]$ sadrži beskonačno mnogo ireducibilnih, normiranih polinoma.*

Dokaz. Kako je $K[X]$ DJF (Teorem 1.2.19.) i $K[X]$ nije polje (Npr. X nije invertibilan.), zaključujemo da $K[X]$ sadrži barem jedan ireducibilan, normiran polinom. Pretpostavimo da postoji $m \in \mathbb{N}$ takav da su $f_1, f_2, \ldots, f_m$ svi ireducibilni, normirani polinomi u $K[X]$. No, tada je $f_1 f_2 \cdots f_m + 1$ polinom u $K[X]$ koji nije djeljiv niti jednim od njih, što je kontradikcija, jer je $K[X]$ DJF. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Lema 1.5.3. *Neka je K polje, neka je $n \in \mathbb{N}$ i neka je V algebarski skup u $\mathbb{A}^n(K)$. Neka je $m \in \mathbb{N}$ i neka su $x_1, x_2, \ldots, x_m$ različite točke iz $\mathbb{A}^n(K)$ koje nisu u V. Tada, za svaki odabir $a_{kl} \in K$, $k, l \in \{1, 2, \ldots, m\}$, postoje polinomi $f_1, f_2, \ldots, f_m \in I(V)$ takvi da je $f_k(x_l) = a_{kl}$, za sve $k, l \in \{1, 2, \ldots, m\}$.*

Dokaz. Neka je W također algebarski skup u $\mathbb{A}^n$. Tvrdimo da je $I(V) = I(W)$ ako i samo ako je $V = W$. Ako je $V = W$, jasno je da je $I(V) = I(W)$. Obratno, ako je $I(V) = I(W)$, tada, prema propoziciji 1.4.8, točki (8) i činjenici da su V i W algebarski skupovi direktno

dobivamo da je $V = V(I(V)) = V(I(W)) = W$. Prema istoj propoziciji, ali prema točki (5) znamo da je $\{x_1\}$ algebarski skup, dok prema točki (4) znamo da je i $V \cup \{x_1\}$ algebarski skup. Sada, prema dokazanom znamo da je, jer $x_1 \notin V$, $I(V) \neq I(V \cup \{x_1\})$. Očito je $V \cup \{x_1\} \supseteq V$ pa je prema već spomenutoj propoziciji, točki (2), $I(V) \supseteq I(V \cup \{x_1\})$, točnije, $I(V) \supsetneq I(V \cup \{x_1\})$. Dakle, postoji polinom $g_1 \in I(V)$ takav da je $g_1(x_1) \neq 0$. Kako je K polje, možemo pomnožiti s $(g_1(x_1))^{-1}$ pa dobivamo da je $g_1 \in I(V)$ i $g_1(x_1) = 1$. Označimo sa S skup točaka $x_1, x_2, \ldots, x_m$. Primijenimo li gornji postupak na algebarski skup $V \cup S \setminus \{x_l\}$ (Za koji znamo da je algebarski po istoj propoziciji, točki (6).) i točku x_l, redom za $l = 1, 2, \ldots, m$, nalazimo polinome $g_1, g_2, \ldots, g_m$, koji se svi nalaze u $I(V)$ i za koje je $g_k(x_l) = \delta_{kl}$. Ovdje je δ_{kl} Kroneckerova delta, tj.

$$\delta_{kl} = \begin{cases} 0, & l \neq k, \\ 1, & l = k. \end{cases}$$

Konačno, stavimo li, za svaki $k \in \{1, 2, \ldots, m\}$, da je $f_k = \sum_{l=1}^{m} a_{kl} g_l$, vidimo da je $f_k \in I(V)$ i da je $f_k(x_l) = a_{kl}$, za sve $k, l \in \{1, 2, \ldots, m\}$. Q.E.D.

Lema 1.5.4. *Neka je K polje, $n \in \mathbb{N}$ i neka je I ideal u $K[X_1, X_2, \ldots, X_n]$. Tada je $V(I) = V(\mathrm{Rad}(I))$ i $\mathrm{Rad}(I) \subseteq I(V(I))$.*

Dokaz. Kako je $I \subseteq \mathrm{Rad}(I)$, prema propoziciji 1.4.8, točki (1), slijedi $V(I) \supseteq V(\mathrm{Rad}(I))$. Obratno, neka je $x \in V(I)$. Neka je $f \in \mathrm{Rad}(I)$, tada postoji $m \in \mathbb{N}$ takav da je $f^m \in I$, no to znači da je $f^m(x) = 0$, a kako je to jednakost u polju K, tj. u integralnoj domeni, zaključujemo da je $f(x) = 0$. Dakle, $x \in V(\mathrm{Rad}(I))$, tj. $V(I) \subseteq V(\mathrm{Rad}(I))$. Konačno, $V(I) = V(\mathrm{Rad}(I))$. Nadalje, prema već spomenutoj propoziciji, točki (8), dobivamo da je $\mathrm{Rad}(I) \subseteq I(V(\mathrm{Rad}(I))) = I(V(I))$. Q.E.D.

Lema 1.5.5. *Neka je K polje, neka je $n \in \mathbb{N}$ i neka su $x_1, x_2, \ldots, x_n \in K$. Tada je ideal $I = (X_1 - x_1, X_2 - x_2, \ldots, X_n - x_n)$ maksimalan ideal u prstenu $K[X_1, X_2, \ldots, X_n]$ i postoji izomorfizam $\overline{\varphi} : K[X_1, X_2, \ldots, X_n]/I \to K$.*

Dokaz. Općenito, znamo da je ideal J u prstenu R maksimalan ako i samo ako je R/J polje. Dakle, kako bismo dokazali da je ideal I maksimalan u prstenu $K[X_1, X_2, \ldots, X_n]$, dovoljno je pokazati da je $K[X_1, X_2, \ldots, X_n]/I$ polje, a to ćemo imati odmah ako pokažemo da postoji izomorfizam $\overline{\varphi} : K[X_1, X_2, \ldots, X_n]/I \to K$. No, za to je, prema prvom teoremu o izomorfizmu, tj. propoziciji 1.2.17, dovoljno pokazati da postoji epimorfizam $\varphi : K[X_1, X_2, \ldots, X_n] \to K$ takav da je $\mathrm{Ker}(\varphi) = I$. Neka je $x = (x_1, x_2, \ldots, x_n)$ i stavimo da je $\varphi = \varphi_x$, evaluacija polinoma u točki x. Konkretnije, za svaki $f \in K[X_1, X_2, \ldots, X_n]$, $\varphi(f) = f(x)$. Znamo da je ovako definirano preslikavanje φ, homomorfizam. Neka je $y \in K$, stavimo li da je f konstanta jednaka upravo y dobivamo da je $\varphi(f) = y$, što znači da je φ epimorfizam. Konačno, prema propoziciji 1.4.8, točki (7) znamo da je $I(\{x\}) = I$, dok je očito, prema samoj definiciji jezgre, $\mathrm{Ker}(\varphi) = I(\{x\})$, tj. $\mathrm{Ker}(\varphi) = I$. Q.E.D.

Propozicija 1.5.6. *Neka je R Noetherin prsten i neka je $\mathcal{S}$ neprazna familija ideala u R. Tada $\mathcal{S}$ sadrži maksimalni element, tj. postoji ideal $I \in \mathcal{S}$ koji nije sadržan u niti jednom drugom idealu u $\mathcal{S}$.*

Dokaz. Pretpostavimo suprotno. Neka je $I_1 \in \mathcal{S}$ bilo koji ideal, on postoji jer je familija $\mathcal{S}$ neprazna. Kako, prema pretpostavci, familija ideala $\mathcal{S}$ nema maksimalni element, postoji $I_2 \in \mathcal{S}$ takav da je $I_1 \subsetneq I_2$. Analogno, postoji $I_3 \in \mathcal{S}$ takav da je $I_2 \subsetneq I_3$. Tako postupimo za svaki $m \in \mathbb{N}$ i dobivamo niz ideala $\{I_m\}_{m\in\mathbb{N}}$ u $\mathcal{S}$ takav da je $I_m \subsetneq I_{m+1}$, za svaki $m \in \mathbb{N}$. $I := \bigcup_{m=1}^{\infty} I_m$ je očito ideal u R. Kako je R Noetherin prsten, ideal I je konačno generiran, tj. postoje $k \in \mathbb{N}$ i $a_1, a_2, \ldots, a_k \in I$ takvi da je $I = (a_1, a_2, \ldots, a_k)$. No, sada to znači da postoji $M \in \mathbb{N}$ (dovoljno velik) takav da je $a_1, a_2, \ldots, a_k \in I_M$, što onda znači da je $I_M = I$, tj. $I_M = I_{M+1}$, a to je kontradikcija. Q.E.D.

Korolar 1.5.7. *Svaki pravi ideal I u Noetherinom prstenu R je sadržan u nekom maksimalnom idealu prstena R.*

Dokaz. Direktno primjenom prethodne propozicije na familiju svih pravih ideala prstena R koji sadrže ideal I, ta familija je neprazna jer uvijek sadrži sam ideal I. Q.E.D.

Sada uvodimo dodatne stvari iz algebre koje će nam biti potrebne.

Definicija 1.5.8. *Neka je R prsten. Neka je A skup, snabdjeven s binarnom operacijom $+$, takav da je $(A, +)$ Abelova grupa.* ***R–modul*** *je aditivna Abelova grupa A zajedno s preslikavanjem*

$$\begin{aligned} R \times A &\to A \\ (r, a) &\mapsto r \cdot a = ra \end{aligned}$$

takvim da vrijedi:

(i) $r(a + b) = ra + rb,\ \forall r \in R,\ \forall a, b \in A,$

(ii) $(r + s)a = ra + sa,\ \forall r, s \in R,\ \forall a \in A,$

(iii) $(rs)a = r(sa),\ \forall r, s \in R,\ \forall a \in A,$

(iv) $1 \cdot a = a,\ \forall a \in A.$

Primjer 1.5.9.

(1) $0 \cdot a = 0,\ \forall a \in A.$ To se lako vidi, naime, $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, dakle, neka je $b \in A$ takav da je $b = 0 \cdot a$. Imamo da je $b = 2b$, dodavanjem $-b$ na obje strane dobivamo da je $b = 0$.

(2) Svaka Abelova grupa je zapravo $\mathbb{Z}$–modul. Naime, neka je A Abelova grupa, tada za $m \in \mathbb{Z}_{\geq 0}$ i $a \in A$ jednostavno stavimo $(\pm m)\, a = \pm(\underbrace{a + a + \ldots + a}_{m \text{ puta}})$.

(3) Neka je R prsten, uz množenje u prstenu, svaki ideal u R je R–modul.

(4) Ako je R polje, onda je R–modul zapravo vektorski prostor nad poljem R.

(5) Ako je R potprsten prstena S, onda S možemo smatrati R–modulom.

Definicija 1.5.10. *Neka je $(A, +)$ Abelova grupa, $B \subseteq A$ je (Abelova)* ***podgrupa*** *od A ako je B zatvoren na operaciju $+$ i ako je $(B, +)$ Abelova grupa.*

Definicija 1.5.11. *Neka je R prsten i neka je A R–modul. R***–podmodul** *ili samo podmodul modula A je podgrupa $B \subseteq A$ za koju vrijedi da je $rb \in B$, za sve $r \in R$ i $b \in B$. B je tada također R–modul.*

Definicija 1.5.12. *Neka je R prsten i A R–modul. Neka je $S \subseteq A$.* ***Podmodul*** *modula A* ***generiran skupom*** *S je najmanji podmodul modula A koji sadrži skup S. Eksplicitno ga možemo zapisati kao:*

$$\left\{ \sum_{k=1}^{m} r_k a_k \ : \ m \in \mathbb{N},\ r_1, r_2, \ldots, r_m \in R,\ a_1, a_2, \ldots, a_m \in S \right\}.$$

Ako je S konačan skup, tj. ako je $m \in \mathbb{N}$ i $S = \{a_1, a_2, \ldots, a_m\}$, onda podmodul generiran skupom S označavamo sa $\sum_{k=1}^{m} Ra_k$. Za modul A kažemo da je ***konačno generiran*** *ako je $A = \sum_{k=1}^{m} Ra_k$, za neke $a_1, a_2, \ldots, a_m \in A$.*

Definicija 1.5.13.

- *Neka je R potprsten prstena S. Promatramo S kao R–modul. Kažemo da je S* ***modul–konačan*** *nad R ako je S konačno generiran kao R–modul.*

- *Neka je R potprsten prstena S. Neka je $n \in \mathbb{N}$ i neka je $s = (s_1, s_2, \ldots, s_n) \in S^n$. Neka je $\varphi : R[X_1, X_2, \ldots, X_n] \to S$ evaluacija u točki s. $\mathrm{Im}(\varphi)$ je najmanji potprsten od S koji sadrži R i $s_1, s_2, \ldots, s_n$, označavamo ga s $R[s_1, s_2, \ldots, s_n]$. Eksplicitno ga možemo zapisati kao: $\left\{ \sum_{k=(k_1,k_2,\ldots,k_n)\in\mathbb{Z}^n_{\geq 0}}^{|k|=k_1+k_2+\ldots+k_n\leq m} r_{(k)} s_1^{k_1} s_2^{k_2} \cdots s_n^{k_n} \ : \ m \in \mathbb{Z}_{\geq 0},\ r_{(k)} \in R \right\}$. Kažemo da je prsten S* ***prsten–konačan*** *nad R ako je $S = R[s_1, s_2, \ldots, s_n]$.*

- *Neka je K potpolje polja L te neka je $K(l_1, l_2, \ldots, l_n)$ polje razlomaka prstena $K[l_1, l_2, \ldots, l_n]$, gdje su $n \in \mathbb{N}$ i $l_1, l_2, \ldots, l_n \in L$. $K(l_1, l_2, \ldots, l_n)$ je najmanje potpolje polja L koje sadrži polje K i $l_1, l_2, \ldots, l_n$. Kažemo da je polje L* ***konačno generirano proširenje polja*** *K ako je $L = K(l_1, l_2, \ldots, l_n)$.*

Lema 1.5.14. *Neka je R potprsten prstena S i S potprsten prstena T. Tada:*

(a) Ako su $m, k \in \mathbb{N}$ i $s_1, s_2, \ldots, s_m \in S$ te $t_1, t_2, \ldots, t_k \in T$ takvi da je $S = \sum_{j=1}^{m} Rs_j$ i $T = \sum_{l=1}^{k} St_l$, onda je $T = \sum_{j=1}^{m}\sum_{l=1}^{k} Rs_jt_l$.

(b) Ako su $m, k \in \mathbb{N}$, $s_1, s_2, \ldots, s_m \in S$, $t_1, t_2, \ldots, t_k \in T$ i ako je $S = R[s_1, s_2, \ldots, s_m]$ i $T = S[t_1, t_2, \ldots, t_l]$, onda je $T = R[s_1, s_2, \ldots, s_m, t_1, t_2, \ldots, t_l]$.

(c) Neka su R, S i T polja takva da je R potpolje od S i S potpolje od T. Ako su $m, k \in \mathbb{N}$, $s_1, s_2, \ldots, s_m \in S$ te $t_1, t_2, \ldots, t_k \in T$ takvi da je $S = R(s_1, s_2, \ldots, s_m)$ i $T = S(t_1, t_2, \ldots, t_l)$, onda je $T = R(s_1, s_2, \ldots, s_m, t_1, t_2, \ldots, t_l)$.

Dokaz. Sve tvrdnje slijede direktno iz prethodne definicije. Q.E.D.

Definicija 1.5.15. *Neka je R potprsten prstena S. Kažemo da je element $s \in S$* ***integralan*** *nad R ako postoji normiran polinom $f \in R[X]$ takav da je $f(s) = 0$. Ako su R i S polja, za $s \in S$ kažemo da je* ***algebarski*** *nad R ako je s integralan nad R.*

Propozicija 1.5.16. *Neka je R potprsten integralne domene S i neka je $s \in S$. Tada je s integralan nad R ako i samo ako je $R[s]$ modul–konačan nad R. Točnije, ako i samo ako postoji potprsten od S koji je modul–konačan nad R i koji sadrži $R[s]$.*

Dokaz. Pretpostavimo da je s integralan nad R, prema definiciji tada postoji $d \in \mathbb{N}$ te normiran polinom $f(X) = X^d + r_1X^{d-1} + \ldots + r_{d-1}X + r_d \in R[X]$, takav da je $f(s) = 0$. Iz ovoga odmah zaključujemo da je $s^d \in \sum_{k=0}^{d-1} Rs^k$, a time i da je $s^m \in \sum_{k=0}^{d-1} Rs^k$, za sve $m \in \mathbb{N}$.

Dakle, $R[s]$ je modul–konačan, točnije, $R[s] = \sum_{k=0}^{d-1} Rs^k$. Obratno, pretpostavimo da postoje $m \in \mathbb{N}$ i $s_1, s_2, \ldots, s_m \in S$ takvi da je $R[s] = \sum_{k=1}^{m} Rs_k$. Dakle, $ss_l = \sum_{k=1}^{m} r_{lk}s_k$, gdje su $r_{lk} \in R$ i $l \in \{1, 2, \ldots, m\}$. Promatrajmo sada, u polju razlomaka integralne domene S sljedeći sustav, u varijablama $x_1, x_2, \ldots, x_m$:

$$\begin{array}{ccccccccc} (r_{11}-s)\,x_1 & + & r_{12}x_2 & + & \ldots & + & r_{1m}x_m & = & 0 \\ r_{21}x_1 & + & (r_{22}-s)\,x_2 & + & \ldots & + & r_{2m}x_m & = & 0 \\ \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\ r_{m1}x_1 & + & r_{m2}x_2 & + & \ldots & + & (r_{mm}-s)\,x_m & = & 0 \end{array}.$$

On ima netrivijalno rješenje $s_1, s_2, \ldots, s_m$. Ukoliko je $s_1 = s_2 = \ldots = s_m = 0$, onda je $R = (0)$, a mi takve prstene ne promatramo. Dakle, determinanta matrice toga sustava jednaka je 0. No, ona je jednaka:

$$M = \begin{bmatrix} r_{11}-s & r_{12} & \ldots & r_{1m} \\ r_{21} & r_{22}-s & \ldots & r_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ r_{m1} & r_{m2} & \ldots & r_{mm}-s \end{bmatrix},$$

vidimo da se s pojavljuje samo na dijagonali te matrice pa postoje $r_1, r_2, \ldots, r_m \in R$ takvi da je $0 = \det M = s^m + r_1 s^{m-1} + \ldots + r_{m-1}s + r_m$. Dakle, s je integralan nad R. Vidimo da nam isto vrijedi i ako je $R[s] \subseteq \sum_{k=1}^{m} Rs_k$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Korolar 1.5.17. *Neka je R potprsten integralne domene S. Skup elemenata skupa S koji su integralni nad R je potprsten prstena S koji sadrži prsten R.*

Dokaz. Neka su $s_1, s_2 \in S$ integralni nad R, dovoljno je pokazati da su i $s_1 \pm s_2$ i $s_1 s_2$ integralni nad R. Kako je s_1 integralan nad R, prema prethodnoj propoziciji znamo da je $R[s_1]$ modul–konačan nad R. s_2 je integralan nad R pa je onda integralan i nad $R[s_1]$, jer je

$R \subseteq R[s_1]$. Dakle, $R[s_1][s_2]$ je modul–konačan nad $R[s_1]$, a prema lemi 1.5.14 tada znamo da je $R[s_1, s_2]$ modul–konačan nad R. Kako su $s_1 \pm s_2 \in R[s_1, s_2]$ i $s_1 s_2 \in R[s_1, s_2]$, prema prethodnoj propoziciji zaključujemo da su $s_1 \pm s_2$ i $s_1 s_2$ integralni nad R. $\mathfrak{Q.E.D.}$

Lema 1.5.18. *Algebarski zatvoreno polje K nema modul–konačnih proširenja polja, osim samoga sebe.*

Dokaz. Pretpostavimo suprotno, neka je L modul–konačno proširenje polja K takvo da je $L \supsetneq K$. Neka je $l \in L \setminus K$, kako je $K[l] \subseteq L$, prema propoziciji 1.5.16 tada zaključujemo da je l algebarski nad K. Dakle, kako bismo došli do kontradikcije, dovoljno je dokazati da se svi elementi algebarski nad K, nalaze u K. No, to je očito, jer su sve nultočke svakog polinoma nad algebarski zatvorenim poljem, sadržane u tom polju. $\mathfrak{Q.E.D.}$

Lema 1.5.19. *Neka je K polje i neka je $L = K(X)$.*

(a) Ako je $l \in L$ integralan nad $K[X]$, onda je $l \in K[X]$.

(b) Ne postoji $f \in K[X]$, $f \neq 0$, takav da, za svaki $l \in L$, vrijedi da je, za neki $m \in \mathbb{N}$, $f^m l$ integralan nad $K[X]$.

Dokaz.

(a) Neka su $f, g \in K[X]$ relativno prosti, takvi da je $l = \frac{f}{g}$. l je integralan nad $K[X]$ pa postoje $k \in \mathbb{N}$ i $h_1, h_2, \ldots, h_k \in K[X]$ takvi da je $l^k + h_1 l^{k-1} + \ldots + h_{k-1} l + h_k = 0$. Pomnožimo dobivenu jednadžbu s g^k i dobivamo da je $f^k + h_1 f^{k-1} g + \ldots + h_{k-1} f g^{k-1} + h_k g^k = 0$. Sada vidimo da $g \mid f$, a f i g su relativno prosti, iz čega zaključujemo da je $g \in K[X]^*$, odnosno, $l \in K[X]$.

(b) Pretpostavimo suprotno. Prema (a) tada zaključujemo da postoji $f \in L[K]$, $f \neq 0$, takav da, za svaki $l \in L$, vrijedi da je, za neki $m \in \mathbb{N}$, $f^m l \in K[X]$. No ovo sada znači da je f djeljiv sa svakim ireducibilnim polinomom iz $K[X]$, a to je nemoguće jer ih, prema lemi 1.5.2, postoji beskonačno mnogo. $\mathfrak{Q.E.D.}$

Propozicija 1.5.20. *Neka je K algebarski zatvoreno polje i neka je L proširenje polja K koje je prsten–konačno nad poljem K. Tada je $L = K$.*

Dokaz. Iz leme 1.5.18 vidimo da je dovoljno dokazati da je L modul–konačno nad K. Neka je $L = K[l_1, l_2, \ldots, l_n]$ za neke $n \in \mathbb{N}$ i $l_1, l_2, \ldots, l_n \in L$. Dokaz ćemo provesti matematičkom indukcijom po n. Neka je $n = 1$ i neka je $\varphi : K[X_1] \to L$ odgovarajući epimorfizam, točnije, evaluacija polinoma iz $K[X_1]$ u točki l_1. Znamo da je $K[X_1]$ DGI, stoga postoji $f \in K[X_1]$ takav da je $\mathrm{Ker}(\varphi) = (f)$. Sada je $L = K[l_1] \cong K[X_1]/(f)$. Dakle, $K[X_1]/(f)$ je polje, stoga je (f) maksimalan ideal u $K[X_1]$. $K[X_1]$ nije polje, jer npr. element X_1 nije invertibilan, stoga je $(f) \neq 0$, odnosno, $f \neq 0$. Nadalje, svaki maksimalan ideal je prost pa prema lemi 1.5.1, zaključujemo da je f ireducibilan polinom, dodatno, kako je K polje, možemo ga normirati. Konačno, f je normirani polinom u $K[X_1]$ za kojeg je $f(l_1) = 0$, dakle, l_1 je algebarski nad K, odnosno, prema propoziciji 1.5.16, $L = K[l_1]$ je modul–konačno nad K. Neka je $n \in \mathbb{N}$, $n \geq 2$, pretpostavimo da tvrdnja vrijedi za $n - 1$. Neka je $K_1 = K(l_n)$. L je najmanji prsten koji sadrži K i $l_1, l_2, \ldots, l_n$, no L i K su polja pa je zato $K(l_1, l_2, \ldots, l_n) = L$. Prema lemi 1.5.14 i sličnim zaključivanjem vidimo da je $L = K(l_1, l_2, \ldots, l_n) = K(l_n)(l_1, l_2, \ldots, l_{n-1}) = K_1[l_1, l_2, \ldots, l_{n-1}]$. Prema induktivnoj pretpostavci sada znamo da je L modul–konačno nad K_1, a prema propoziciji 1.5.16 znamo da su tada $l_1, l_2, \ldots, l_{n-1}$ algebarski nad K_1. Kako bismo pokazali da je L modul–konačno nad K vidimo da je, prema lemi 1.5.14, dovoljno pokazati da je K_1 modul–konačno nad K, odnosno, prema propoziciji 1.5.16, da je l_n algebarski nad K. Pretpostavimo suprotno. Tada je $K[l_n] \cong K[X]$, odnosno, $K(l_n) \cong K(X)$. Nadalje, za svaki $k \in \{1, 2, \ldots, n-1\}$, postoje $m_k \in \mathbb{N}$ i $a_{k,1}, a_{k,2}, \ldots, a_{k,m_k} \in K_1$ takvi da je $l_k^{m_k} + a_{k,1} l_k^{m_k - 1} + \ldots + a_{k,m_k - 1} l_k + a_{k,m_k} = 0$. Neka je $a \in K[l_n]$ jednak umnošku svih nazivnika elemenata $a_{k,m}$, $k \in \{1, 2, \ldots, n-1\}$ i $m \in \{1, 2, \ldots, m_k\}$, očito je $a \neq 0$. Množeći dobivene jednadžbe, svaku s odgovarajućim, a^{m_k}, dobivamo da je $(al_k)^{m_k} + a a_{k,1} (al_k)^{m_k - 1} + \ldots + a^{m_k - 1} a_{k,m_k - 1} (al_k) + a^{m_k} a_{k,m_k} = 0$. Dakle, dobili smo da je al_k integralan nad $K[l_n]$, za svaki $k \in \{1, 2, \ldots, n-1\}$, dok je al_n očito

integralan nad $K[l_n]$, jer je $al_n \in K[l_n]$. Prema korolaru 1.5.17 sada direktno dobivamo da je $K[al_1, al_2, \ldots, al_{n-1}, al_n]$ integralan nad $K[l_n]$. To nam zapravo govori da za svaki $l \in L = K[l_1, l_2, \ldots, l_{n-1}, l_n]$ postoji $m \in \mathbb{N}$ takav da je $a^m l$ integralan nad $K[l_n]$. Znamo da je $K_1 \subseteq L$, stoga, za svaki $l \in K_1$ postoji $m \in \mathbb{N}$ takav da je $a^m l$ integralan nad $K[l_n]$. No to je kontradikcija s lemom 1.5.19, dio (b), jer je $K[l_n] \cong K[X]$ i $K(l_n) \cong K(X)$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Napokon dolazimo do samog dokaza Hilbertovog teorema o nulama. Kao što je već napisano, najprije ćemo dokazati tkzv. slabi Nullstellensatz, pomoću kojega ćemo zatim dokazati Nullstellensatz.

Teorem 1.5.21 (Slabi Nullstellensatz)**.** *Neka je K algebarski zatvoreno polje i neka je $n \in \mathbb{N}$. Ako je I pravi ideal u $K[X_1, X_2, \ldots, X_n]$, tada je $V(I) \neq \emptyset$.*

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti da je I maksimalan ideal, jer je prema korolaru 1.5.7, I sadržan u nekom maksimalnom idealu J, a prema propoziciji 1.4.8, dio (1), znamo da je $V(J) \subseteq V(I)$. Dakle, $L = K[X_1, X_2, \ldots, X_n]/I$ je polje, a kao što je već spomenuto, polje K možemo smatrati njegovim potpoljem. Dakle, L je proširenje polja K koje je prsten–konačno nad poljem K, prema lemi 1.5.20 slijedi da je $L = K$. Neka je $k \in \{1, 2, \ldots, n\}$, znamo da je $X_k + I \in L$, zaključujemo (Imajmo na umu da promatramo K kao potpolje od $L = K[X_1, X_2, \ldots, X_n]/I$ i da je $K = L$.) da postoji $x_k \in K$ takav da je $X_k - x_k \in I$. Nadalje, prema lemi 1.5.5 znamo da je $(X_1 - x_1, X_2 - x_2, \ldots, X_n - x_n)$ maksimalan ideal u $K[X_1, X_2, \ldots, X_n]$, stoga je $I = (X_1 - x_1, X_2 - x_2, \ldots, X_n - x_n)$. Konačno, prema propoziciji 1.4.8, dio (5), znamo je $V(I) = \{(x_1, x_2, \ldots, x_n)\} \neq \emptyset$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

U dokazu Hilbertovog teorema u nulama služit ćemo se Rabinowitschevim trikom. Pomoću kojega, uvođenjem jedne dodatne varijable, relativno lako i zgodno dolazimo do općenite tvrdnje Nullstellensatza.

Teorem 1.5.22 (Hilbertov teorem o nulama)**.** *Neka je K algebarski zatvoreno polje i neka je $n \in \mathbb{N}$. Ako je I ideal u $K[X_1, X_2, \ldots, X_n]$, tada je $I(V(I)) = \mathrm{Rad}(I)$.*

Dokaz. Prema lemi 1.5.4 znamo da je $\mathrm{Rad}(I) \subseteq I(V(I))$. Dakle, potrebno je dokazati obratnu inkluziju. Prema Hilbertovom teoremu o bazi, tj. prema napomeni 1.3.3, znamo da postoje $m \in \mathbb{N}$ i $f_1, f_2, \ldots, f_m \in K[X_1, X_2, \ldots, X_n]$ takvi da je $I = (f_1, f_2, \ldots, f_m)$. Neka je $g \in I(V(I))$. Promatrajmo $J = (f_1, f_2, \ldots, f_m, X_{n+1}g - 1) \subseteq K[X_1, X_2, \ldots, X_n, X_{n+1}]$. Pretpostavimo da je $J \neq K[X_1, X_2, \ldots, X_n, X_{n+1}]$, prema teoremu 1.5.21 je tada $V(J) \neq \emptyset$, no, to je nemoguće, jer kada god su polinomi $f_1, f_2, \ldots, f_m$ jednaki 0, polinom g je također jednak 0. Dakle, $J = K[X_1, X_2, \ldots, X_n, X_{n+1}]$. Zaključujemo da postoje polinomi $a_1, a_2, \ldots, a_m$ i b iz $K[X_1, X_2, \ldots, X_n, X_{n+1}]$ takvi da je $\sum_{k=1}^{m} a_k f_k + b(X_{n+1}g - 1) = 1$. Promatrajmo dobivenu jednakost u polju $K(X_1, X_2, \ldots, X_n, X_{n+1})$. Pomnožimo ju s $\frac{1}{X_{n+1}^N}$, gdje je $N - 1 \in \mathbb{Z}_{\geq 0}$ najveći eksponent na varijabli X_{n+1} koji se pojavljuje među polinomima $a_1, a_2, \ldots, a_m$ i b. Označimo li $Y = \frac{1}{X_{n+1}}$, vidimo da su $c_k = \frac{a_k}{X_{n+1}^N}$, $k = 1, 2, \ldots, m$ i $d = \frac{b}{X_{n+1}^{N-1}}$ polinomi u $K[X_1, X_2, \ldots, X_n, Y]$. Dakle, dobivamo da u tom prstenu, kojeg ćemo promatrati kao $K[X_1, X_2, \ldots, X_n][Y]$, vrijedi jednakost:

$$Y^N = f_1c_1 + f_2c_2 + \ldots + f_mc_m + gd - Yd.$$

Možemo uvrstiti da je $Y = g$ pa dobivamo da je $g^N = c_1(g) f_1 + c_2(g) f_2 + \ldots + c_m(g) f_m$. Kako je $g \in K[X_1, X_2, \ldots, X_n]$, vidimo da su $c_k(g)$, gdje je $k \in \{1, 2, \ldots, m\}$, polinomi iz $K[X_1, X_2, \ldots, X_n]$. Konačno, dobili smo da je $g^N \in I$, što znači da je $g \in \mathrm{Rad}(I)$. Q.E.D.

Korolar 1.5.23. *Neka je K algebarski zatvoreno polje i neka je $n \in \mathbb{N}$. Ako je I radikalan ideal u $K[X_1, X_2, \ldots, X_n]$, onda je $I(V(I)) = I$. Dakle, svakim radikalnim idealom je jedinstveno određen algebarski skup, a i obratno.*

Dokaz. Direktna posljedica Hilbertovog teorema o nulama. Q.E.D.

Korolar 1.5.24. *Neka je K algebarski zatvoreno polje, neka je $n \in \mathbb{N}$ i neka je I ideal u $K[X_1, X_2, \ldots, X_n]$. Tada je $V(I)$ konačan skup ako i samo ako je $K[X_1, X_2, \ldots, X_n]/I$*

konačno dimenzionalni vektorski prostor nad K. *U tom slučaju je broj točaka u skupu* $V(I)$ *najviše* $\dim_K(K[X_1, X_2, \ldots, X_n]/I)$.

Dokaz. Pretpostavimo najprije da je $K[X_1, X_2, \ldots, X_n]/I$ konačno dimenzionalni vektorski prostor nad K. Neka su $m \in \mathbb{N}$ i $x_1, x_2, \ldots, x_m \in V(I)$ međusobno različite točke. Primijenimo li sada lemu 1.5.3 na algebarski skup $W = \emptyset$, dobivamo da postoje polinomi $f_1, f_2, \ldots, f_m \in I(W) = K[X_1, X_2, \ldots, X_n]$ takvi da je $f_k(x_l) = \delta_{kl}$, $k, l \in \{1, 2, \ldots, m\}$. Promatrajmo sada odgovarajuće elemente (tj. klase ekvivalencije) u kvocijentnom prstenu $K[X_1, X_2, \ldots, X_n]/I$, $\overline{f_1}, \overline{f_2}, \ldots, \overline{f_m}$. Neka su $a_1, a_2, \ldots, a_m \in K$ takvi da je $\sum_{k=1}^{m} a_k \overline{f_k} = \overline{0}$, odnosno takvi da je $\sum_{k=1}^{m} a_k f_k \in I$. Za svaki $l \in \{1, 2, \ldots, m\}$ je očito $\sum_{k=1}^{m} a_k f_k(x_l) = a_l$, a kako je $x_l \in V(I)$, imamo da je $\left(\sum_{k=1}^{m} a_k f_k\right)(x_l) = 0$. Dakle, $a_l = 0$, za sve $l \in \{1, 2, \ldots, m\}$. Zaključujemo da je $\overline{f_1}, \overline{f_2}, \ldots, \overline{f_m}$ linearno nezavisan skup u $K[X_1, X_2, \ldots, X_n]/I$, stoga je $m \leq \dim_K(K[X_1, X_2, \ldots, X_n]/I)$. Obratno, neka je $V(I)$ konačan. Ukoliko je $V(I) = \emptyset$, prema slabom Nullstellensatzu (teorem 1.5.21) znamo da je tada $I = K[X_1, X_2, \ldots, X_n]$ pa je $K[X_1, X_2, \ldots, X_n]/I = \{0\}$, tj. tvrdnja je trivijalna. Nadalje, pretpostavimo da je $m \in \mathbb{N}$ i da su $x_1, x_2, \ldots, x_m$ sve točke skupa $V(I)$. Neka je $x_l = (x_{l1}, x_{l2}, \ldots, x_{ln})$, za svaki $l \in \{1, 2, \ldots, m\}$. Definirajmo polinome $f_k = \prod_{l=1}^{m} (X_k - x_{lk})$, za svaki $k \in \{1, 2, \ldots, n\}$. Očito je $f_k \in I(V(I))$, $\forall k \in \{1, 2, \ldots, n\}$, prema Hilbertovom teoremu o nulama (teorem 1.5.22) znamo da, za svaki $k \in \{1, 2, \ldots, n\}$, postoji $N_k \in \mathbb{N}$ takav da je $f_k^{N_k} \in I$. Neka je $N = \max\{N_1, N_2, \ldots, N_n\}$. Sada, opet gledajući odgovarajuće elemente dobivamo da je $\overline{f_k}^N = \overline{0}$ u $K[X_1, X_2, \ldots, X_n]/I$, za svaki $k \in \{1, 2, \ldots, n\}$. Konačno zaključujemo da je $\overline{X_k}^{mN}$ jednak nekoj linearnoj kombinaciji (Jasno, s koeficijentima iz K.) elemenata $1, \overline{X_k}, \ldots, \overline{X_k}^{mN-1}$, a onda indukcijom da isto vrijedi i za $\overline{X_k}^M$, za svaki $M \in \mathbb{N}$ i za svaki $k \in \{1, 2, \ldots, n\}$. Dakle, $K[X_1, X_2, \ldots, X_n]/I$ je konačno generiran vektorski prostor nad K, tj. on je konačno dimenzionalan vektorski prostor nad K. Sada lako dobijemo, kao u

prvom dijelu dokaza, da je $m \leq \dim_K (K[X_1, X_2, \ldots, X_n]/I)$. Q.E.D.

1.6 Rastav u ireducibilne komponente

Definicija 1.6.1. *Neka je K polje i $n \in \mathbb{N}$. Algebarski skup $V \subseteq \mathbb{A}^n(K)$ je* ***reducibilan*** *ako je $V = V_1 \cup V_2$, za neke algebarske skupove V_1, V_2 iz $\mathbb{A}^n(K)$ takve da je $V_1 \neq V$ i $V_2 \neq V$. V je* ***ireducibilan*** *ako nije reducibilan.*

Propozicija 1.6.2. *Neka je K polje i $n \in \mathbb{N}$. Neka je V algebarski skup u $\mathbb{A}^n(K)$ te neka je I prost ideal u $K[X_1, X_2, \ldots, X_n]$. V je ireducibilan ako i samo ako je $I(V)$ prost ideal u $K[X_1, X_2, \ldots, X_n]$, $V(I)$ je ireducibilan algebarski skup u $\mathbb{A}^n(K)$. Dakle, svakim prostim idealom je jedinstveno određen ireducibilan algebarski skup, a i obratno. Primijetimo također da su točke iz $\mathbb{A}^n(K)$ u 1—1 korespodenciji s maksimalnim idealima u $K[X_1, X_2, \ldots, X_n]$.*

Dokaz. Dokazati ćemo da je V ireducibilan ako i samo ako je $I(V)$ prost ideal, ostale tvrdnje tada slijede direktno iz Hilbertovog teorema (1.5.22) o nulama. Pretpostavimo da je V reducibilan, tada postoje algebarski skupovi V_1, V_2 takvi da je $V_1 \cup V_2 = V$ i $V_1 \neq V$, $V_2 \neq V$. Sada odmah zaključujemo da je, za $k \in \{1, 2\}$, $V_k \subsetneq V$, a iz ovoga, kao u dokazu leme 1.5.3, vidimo da je $I(V_k) \supsetneq I(V)$. Dakle, postoji $f_k \in I(V_k)$ takav da $f_k \notin I(V)$, za $k = 1, 2$. No, kako je $V = V_1 \cup V_2$, zaključujemo da je $f_1 f_2 \in I(V)$, dakle, $I(V)$ nije prost ideal u $K[X_1, X_2, \ldots, X_n]$. Obratno, ako $I(V)$ nije prost ideal u $K[X_1, X_2, \ldots, X_n]$, onda postoje polinomi f_1 i f_2 iz $K[X_1, X_2, \ldots, X_n]$, koji nisu u $I(V)$, ali $f_1 f_2 \in I(V)$. Tada je $V = (V \cap V(f_1)) \cup (V \cap V(f_2))$ i očito je $V \cap V(f_k) \supsetneq V$, za $k = 1, 2$, jer $f_k \notin I(V)$. Dakle, V je reducibilan algebarski skup u $\mathbb{A}^n(K)$. Q.E.D.

Teorem 1.6.3. *Neka je K polje, $n \in \mathbb{N}$ i V algebarski skup u $\mathbb{A}^n(K)$. Tada postoje jedinstveni $m \in \mathbb{N}$ i ireducibilni algebarski skupovi $V_1, V_2, \ldots, V_m$ (Jedinstveni do na poredak.)*

u $\mathbb{A}^n(K)$ *takvi da je* $V = V_1 \cup V_2 \cup \ldots \cup V_m$ *i* $V_k \not\subseteq V_l$*, za sve* $k, l \in \{1, 2, \ldots, m\}$, $l \neq k$.

Dokaz. Neka je $\mathcal{S}$ familija algebarskih skupova u $\mathbb{A}^n(K)$ koji se ne mogu prikazati kao konačna unija ireducibilnih algebarskih skupova. Želimo pokazati da je $\mathcal{S}$ prazna familija. Pretpostavimo suprotno. Nadalje, pretpostavimo da $\mathcal{S}$ nema minimalni element (U smislu inkluzije.), tj. da za svaki $V \in \mathcal{S}$ postoji $W \in \mathcal{S}$ takav da je $W \subsetneq V$. No, pogledamo li sada familiju $\mathcal{S}' = \{I(V) : V \in \mathcal{S}\}$, dobivamo da ona nema maksimalni element, a to je u kontradikciji s propozicijom 1.5.6. Dakle, $\mathcal{S}$ ima minimalni element. Neka je $V \in \mathcal{S}$ jedan takav. Kako je $V \in \mathcal{S}$, V je reducibilan pa postoje algebarski skupovi V_1 i V_2 koji nisu jednaki V takvi da je $V = V_1 \cup V_2$. Kako je V minimalan element od $\mathcal{S}$ zaključujemo da je $V_1, V_2 \notin \mathcal{S}$. Dakle, V_1 i V_2 su prikazivi kao konačna unija ireducibilnih algebarskih skupova. No, to sada znači da je i V prikaziv kao konačna unija ireducibilnih algebarskih skupova, jer je $V = V_1 \cup V_2$. To je kontradikcija, dakle, familija $\mathcal{S}$ je prazna, tj. svaki algebarski skup se može prikazati kao konačna unija ireducibilnih algebarskih skupova. Preostaje nam dokazati jedinstvenost prikaza. Neka je V algebarski skup i neka je $V = V_1 \cup V_2 \cup \ldots V_m$, $m \in \mathbb{N}$, njegov prikaz kao konačne unije ireducibilnih algebarskih skupova. Ukoliko je, za neke $k, l \in \{1, 2, \ldots, m\}$, $l \neq k$, $V_l \subseteq V_k$, izbacimo V_l. Neka je $M \in \mathbb{N}$ i $V = W_1 \cup W_2 \cup \ldots \cup W_M$ neki drugi prikaz algebarskog skupa V kao konačne unije ireducibilnih algebarskih skupova za koje ne postoje $K, L \in \{1, 2, \ldots, M\}$, $L \neq K$, takvi da je $W_L \subseteq W_K$. Neka je $k \in \{1, 2, \ldots, m\}$, vrijedi: $V_k = V_k \cap V = \bigcup_{K=1}^{M} (V_k \cap W_K)$. Kako je V_k ireducibilan, vidimo da postoji $K \in \{1, 2, \ldots, M\}$ takav da je $V_k = V_k \cap W_K$, odnosno, $V_k \subseteq W_K$. Slično, postoji $l \in \{1, 2, \ldots, m\}$ takav da je $W_K \subseteq V_l$, slijedi $V_k \subseteq V_l$ pa je $l = k$. Dakle, $V_k = W_K$. Analogno dobijemo da za svaki $L \in \{1, 2, \ldots, M\}$ postoji $l \in \{1, 2, \ldots, m\}$ takav da je $W_L = V_l$. Dakle, dobili smo da je $M = m$ i da su pripadajući ireducibilni algebarski skupovi jedinstveni, do na poredak. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Definicija 1.6.4. *Uz oznake iz prethodnog teorema,* $V = V_1 \cup V_2 \cup \ldots \cup V_m$ *je* ***rastav*** *al-*

gebarskog skupa V ***u ireducibilne komponente****, a V_k, $k = 1, 2, \ldots, m$, su njegove* ***ireducibilne komponente****.*

Teorem 1.6.5. *Neka je K algebarski zatvoreno polje, $n \in \mathbb{N}$ i neka je f nekonstantni polinom u $K[X_1, X_2, \ldots, X_n]$. Neka su $m \in \mathbb{N}$, $k_1, k_2, \ldots, k_m \in \mathbb{N}$ i $f_1, f_2, \ldots, f_m$ ireducibilni polinomi u $K[X_1, X_2, \ldots, X_n]$ takvi da je $f = f_1^{k_1} f_2^{k_2} \cdots f_m^{k_m}$. Oni postoje i jedinstveni su (do na poredak i množenje konstantama), jer je, prema teoremu 1.2.19, $K[X_1, X_2, \ldots, X_n]$ domena jedinstvene faktorizacije. Tada je $V(f) = V(f_1) \cup V(f_2) \cup \ldots \cup V(f_m)$ rastav od $V(f)$ u ireducibilne komponente i $I(V(F)) = (f_1 f_2 \cdots f_m)$. Dakle, postoji 1—1 korespodencija između normiranih ireducibilnih polinoma $g \in K[X_1, X_2, \ldots, X_n]$ i ireducibilnih hiperploha u $\mathbb{A}^n(K)$.*

Dokaz. Za svaki $l \in \{1, 2, \ldots, m\}$, je $V(f_l) = V\left(f_l^{k_l}\right)$. Sada, kao u dokazu točke (4) propozicije 1.4.8, vidimo da je $V\left(f_1^{k_1}\right) \cup V\left(f_2^{k_2}\right) \cup \ldots \cup V\left(f_m^{k_m}\right) = V\left(f_1^{k_1} f_2^{k_2} \cdots f_m^{k_m}\right) = V(f)$. Nadalje, $f_1, f_2, \ldots, f_m$ su ireducibilni i međusobno neasocirani pa ne postoje, $k \neq l$ iz skupa $\{1, 2, \ldots, m\}$, takvi da $f_l \mid f_k$, tj. takvi da je $V(f_l) \subseteq V(f_k)$. Ovime smo pokazali da je $V(f) = V(f_1) \cup V(f_2) \cup \ldots \cup V(f_m)$ rastav od $V(f)$ rastav skupa $V(f)$ u ireducibilne komponente. Dalje, prema Hilbertovom teoremu (1.5.22) o nulama i činjenici da je (f_k) prost (time i radikalan) ideal u $K[X_1, X_2, \ldots]$, za svaki $k \in \{1, 2, \ldots, m\}$, dobivamo da je $I(V(f_k)) = (f_k)$. Konačno je

$$I(V(F)) = I\left(\bigcup_{k=1}^{m} V(f_k)\right) = \bigcap_{k=1}^{m} I(V(f_k)) = \bigcap_{k=1}^{m} (f_k) = (f_1 f_2 \cdots f_m).$$

Posljednja jednakost slijedi iz činjenice da za polinom $h \in K[X_1, X_2, \ldots, X_n]$ vrijedi da $f_k \mid h$, za svaki $k \in \{1, 2, \ldots, m\}$, ako i samo ako $f_1 f_2 \cdots f_m \mid h$, jer su $f_1, f_2, \ldots, f_m$ ireducibilni, međusobno neasocirani polinomi iz $K[X_1, X_2, \ldots, X_n]$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Propozicija 1.6.6. *Neka je $I \subseteq K[X_1, X_2, \ldots, X_n]$ ideal, gdje je K algebarski zatvoreno polje i $n \in \mathbb{N}$. Neka je $V = V(I)$, tada postoji 1—1 korespodencija između algebarskih*

podskupova od V i radikalnih ideala u $K[X_1, X_2, \ldots, X_n]/I$, također, ireducibilni algebarski skupovi su u korespodenciji s prostim idealima, dok su točke u korespodenciji s maksimalnim idealima.

Dokaz. Tvrdnja direktno slijedi iz propozicija 1.4.10 i 1.6.2. Q.E.D.

Ravninski algebarski skupovi

Ovdje ćemo pronaći, tj. opisati sve algebarske skupove u ravnini. Prema teoremu 1.6.3 vidimo da je za to dovoljno pronaći sve ireducibilne algebarske skupove.

Propozicija 1.6.7. *Neka je K polje. Neka su f i g relativno prosti polinomi u $K[X, Y]$. Tada je $V(f, g) = V(f) \cap V(g)$ konačan skup točaka.*

Dokaz. Prema korolaru 1.2.20 vidimo da su f i g relativno prosti i u $K(X)[Y]$. Nadalje, $K(X)[Y]$ je, kao prsten polinoma u jednoj varijabli nad poljem $K(X)$, domena glavnih ideala. Stoga postoji $h \in K(X)[Y]$ takav da je $(f, g) = (h)$, no f i g su relativno prosti pa je $h \in (K(X)[Y])^*$. Dakle, $(f, g) = (1) = K(X)[Y]$. Stoga postoje $d, e \in K(X)[Y]$ takvi da je $df + eg = 1$. Neka je $c \in K[X]$ jednak umnošku svih nazivnika koji se pojavljuju u d i e, tada su $a = cd$ i $b = ce$ iz $K[X, Y]$. Dakle, imamo da je $af + bf = c$, u $K[X, Y]$ i očito je $c \neq 0$. Imajmo na umu da desna strana jednakosti "ovisi" samo o varijabli X. Neka je $(a, b) \in V(f, g)$, tada je $c(a) = 0$. Dakle, samo konačno mnogo različitih "X-koordinata" ima među točkama iz $V(f, g)$. Isto zaključujemo za Y-koordinate. Konačno, $V(f, g)$ je konačan skup točaka. Q.E.D.

Korolar 1.6.8. *Neka je K polje s beskonačno mnogo elemenata. Tada su svi ireducibilni algebarski skupovi u ravnini $\mathbb{A}^2(K)$:*

- $\mathbb{A}^2(K)$,
- $\emptyset$,

- $\{x\}\,,\ x \in \mathbb{A}^2(K)$,
- *ireducibilne ravninske krivulje* $V(f)$, *gdje je* $f \in K[X, Y]$ *ireducibilan polinom takav da je* $V(f)$ *beskonačan skup točaka.*

Dokaz. Neka je V ireducibilan algebarski skup u ravnini $\mathbb{A}^2(K)$. Ako je V konačan, jasno je da je $V = \emptyset$ ili $V = \{x\}$, za neki $x \in \mathbb{A}^2(K)$. Pretpostavimo da je V beskonačan skup točaka i da nije $V = \mathbb{A}^2(K)$. Tada $I(V)$ sadrži neki polinom $f \in K[X, Y]$ koji nije konstantan, također, prema propoziciji 1.6.2 znamo da je $I(V)$ prost ideal. Stoga, bez smanjenja općenitosti možemo pretpostaviti da je f ireducibilan polinom. Tada je $I(V) = (f)$. U suprotnom postoji $g \in I(V)$ takav da $g \notin (f)$, ali tada je $V \subseteq V(f, g)$ konačan, prema prethodnoj propoziciji. Dakle, $I(V) = (f)$, odnosno, $V = V(f)$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Poglavlje 2

Afine mnogostrukosti

2.1 Osnovni pojmovi

U cijelom ovom poglavlju, neka je K algebarski zatvoreno polje (Osim ako ne bude naglašeno drukčije.) te neka je $\mathbb{A}^n = \mathbb{A}^n(K)$, gdje je $n \in \mathbb{N}$.

Definicija 2.1.1. *Ireducibilni afini algebarski skup u $\mathbb{A}^n$ naziva se* ***afina mnogostrukost****.*

Kada je to iz konteksta jasno, afine mnogostrukosti (Kasnije ćemo se upoznati i s projektivnim.) ćemo nazivati, jednostavno, mnogostrukostima. Tako će to biti u cijelom ovom poglavlju.

Definicija 2.1.2. *Neka je $V \subseteq \mathbb{A}^n$ neprazna mnogostrukost. Prsten*

$$\Gamma(V) = K[X_1, X_2, \ldots, X_n] / I(V)$$

nazivamo ***koordinatni prsten od*** *V.*

Primijetimo da je $\Gamma(V)$ integralna domena, zato jer je, prema propoziciji 1.6.2, $I(V)$ prost ideal.

Definicija 2.1.3. *Neka je* $\emptyset \neq V \subseteq \mathbb{A}^n$. $\mathcal{F}(V, K)$ *je skup svih funkcija* $V \to K$. *Taj skup smatramo prstenom s uobičajenim zbrajanjem i množenjem funkcija po točkama. Ukoliko je* V *mnogostrukost,* $f \in \mathcal{F}(V, K)$ *je* ***polinomijalna funkcija*** *ako postoji polinom* $F \in K[X_1, X_2, \ldots, X_n]$ *takav da je*

$$f(a_1, a_2, \ldots, a_n) = F(a_1, a_2, \ldots, a_n), \ \forall (a_1, a_2, \ldots, a_n) \in V.$$

Napomena 2.1.4. *Polje* K *smatramo potprstenom prstena* $\mathcal{F}(V, K)$ *tako što ga identificiramo s konstantnim funkcijama. Vidimo da skup polinomijalnih funkcija tvori potprsten prstena* $\mathcal{F}(V, K)$ *koji sadrži* K. *Nadalje, vidimo da polinomi* $F, G \in K[X_1, X_2, \ldots, X_n]$ *određuju istu polinomijalnu funkciju ako i samo ako je* $F - G \in I(V)$. *Dakle,* $\Gamma(V)$ *je potprsten prstena* $\mathcal{F}(V, K)$ *(Zapravo prsten svih polinomijalnih funkcija.), tako što svaku klasu polinoma prikažemo odgovarajućom (jedinstvenom) polinomijalnom funkcijom.*

Definicija 2.1.5. *Neka je* $V \subseteq \mathbb{A}^n$ *mnogostrukost. Mnogostrukost* $W \subseteq \mathbb{A}^n$ *naziva se* ***podmnogostrukost*** *od* V *ako je* $W \subseteq V$.

Propozicija 2.1.6. *Neka je* $V \subseteq \mathbb{A}^n$ *mnogostrukost. Postoji 1—1 korespodencija između algebarskih podskupova od* V *i radikalnih ideala u* $\Gamma(V)$. *Dodatno, podmnogostrukosti od* V *odgovaraju prostim, dok točke u* V *odgovaraju radikalnim idealima u* $\Gamma(V)$.

Dokaz. Direktna posljedica propozicije 1.6.6. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Definicija 2.1.7. *Neka su* $V \subseteq \mathbb{A}^n$ *i* $W \subseteq \mathbb{A}^m$ *mnogostrukosti. Preslikavanje* $\varphi : V \to W$ *je* ***polinomijalno preslikavanje*** *ako postoje polinomi* $P_1, P_2, \ldots, P_m \in K[X_1, X_2, \ldots, X_n]$ *takvi da je*

$$\varphi(a_1, a_2, \ldots, a_n) = (P_1(a_1, a_2, \ldots, a_n), P_2(a_1, a_2, \ldots, a_n), \ldots, P_m(a_1, a_2, \ldots, a_n)),$$

za sve $(a_1, a_2, \ldots, a_n) \in V$.

Svako preslikavanje $\varphi : V \to W$ inducira homomorfizam $\tilde{\varphi} : \mathcal{F}(W, K) \to \mathcal{F}(V, K)$, djelovanjem $\tilde{\varphi}(f) = f \circ \varphi,\ f \in \mathcal{F}(W, K)$. Ukoliko je φ polinomijalno preslikavanje, jasno je da je $\tilde{\varphi}(\Gamma(W)) \subseteq \Gamma(V)$, tj. $\tilde{\varphi}|_{\Gamma(W)}$ je homomorfizam s $\Gamma(W)$ u $\Gamma(V)$. Ukoliko je $V = \mathbb{A}^n$ i $W = \mathbb{A}^m$ te $P_1, P_2, \ldots, P_m \in K[X_1, X_2, \ldots, X_n]$ određuju polinomijalno preslikavanje $\varphi : \mathbb{A}^n \to \mathbb{A}^m$, onda su $P_1, P_2, \ldots, P_m$ jedinstveno određeni s φ (To slijedi iz korolara 1.2.27.). Stoga možemo pisati da je $\varphi = (P_1, P_2, \ldots, P_m)$.

Propozicija 2.1.8. *Neka su $V \subseteq \mathbb{A}^n$ i $W \subseteq \mathbb{A}^m$ mnogostrukosti. Svakom polinomijalnom preslikavanju $\varphi : V \to W$ odgovara jedan i samo jedan homomorfizam $\tilde{\varphi} : \Gamma(W) \to \Gamma(V)$ i obratno.*

Dokaz. Za dano polinomijalno preslikavanje $\varphi : V \to W$ smo već opisali kako izgleda homomorfizam $\tilde{\varphi} : \Gamma(W) \to \Gamma(V)$. Obratno, neka je $\psi : \Gamma(W) \to \Gamma(V)$ homomorfizam. Za svaki $k \in \{1, 2, \ldots, m\}$ odaberimo $P_k \in K[X_1, X_2, \ldots, X_n]$ takav da je $\psi(X_k + I(W)) = P_k + I(V)$. Ovime smo dobili polinomijalno preslikavanje $P = (P_1, P_2, \ldots, P_m)$ s $\mathbb{A}^n$ u $\mathbb{A}^m$ koje inducira homomorfizam

$$\tilde{P} : \Gamma(\mathbb{A}^m) (= K[X_1, X_2, \ldots, X_m]) \to \Gamma(\mathbb{A}^n) (= K[X_1, X_2, \ldots, X_n]).$$

Neka je $f \in I(W)$, tada je $f + I(W) = 0 + I(W)$ pa je $\psi(f + I(W)) = 0 + I(V)$, zato je $\tilde{P}(f) \in I(V)$, tj. $\tilde{P}(I(W)) \subseteq I(V)$, iz ovoga pak zaključujemo da je $P(V) \subseteq W$. Dakle, možemo promatrati polinomijalno preslikavanje $P|_V : V \to W$. Kako je očito da je $\tilde{P|_V} = \psi$ dobili smo i traženu obratnu tvrdnju. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Definicija 2.1.9. *Uz oznake iz propozicije 2.1.8, polinomijalno preslikavanje $\varphi : V \to W$ je* ***izomorfizam*** *ako postoji polinomijalno preslikavanje $\psi : W \to V$ tako da je $\psi \circ \varphi = id_V$ i $\varphi \circ \psi = id_W$.*

Napomena 2.1.10. *U prethodnoj definiciji, id_X je oznaka za identitetu na skupu X. Propozicija 2.1.8 nam pokazuje da su dvije mnogostrukosti izomorfne ako i samo ako su njihovi koordinatni prsteni izomorfni, nad K.*

Neka je $P = (P_1, P_2, \ldots, P_m)$ polinomijalno preslikavanje $\mathbb{A}^n \to \mathbb{A}^m$, neka je F polinom, a I ideal u $K[X_1, X_2, \ldots, X_m]$ te neka je V algebarski skup u $\mathbb{A}^m$. Uvodimo oznake:

$$F^P = \tilde{P}(F) = F(P_1, P_2, \ldots, P_m),$$

$$I^P = \text{ideal u } K[X_1, X_2, \ldots, X_n] \text{ generiran s } \left\{F^P \ : \ F \in I\right\},$$

$$V^P = P^{-1}(V) = V\left(I(V)^P\right).$$

Definicija 2.1.11. *Polinomijalno preslikavanje $P = (P_1, P_2, \ldots, P_n) : \mathbb{A}^n \to \mathbb{A}^n$ je **afina zamjena koordinata** na $\mathbb{A}^n$ ako je P_k polinom stupnja 1, za svaki $k \in \{1, 2, \ldots, n\}$ te ako je P bijekcija.*

Uz gornje oznake, neka je P_k polinom stupnja 1 za svaki $k \in \{1, 2, \ldots, n\}$. Tada je $P_k = \sum_{l=1}^{n} a_{kl}X_l + a_{k0}$, gdje su $a_{k0}, a_{k1}, \ldots, a_{kn} \in K$ i barem jedan od $a_{k1}, \ldots, a_{kn}$ je različit od 0. Vidimo da je $P = P'' \circ P'$, gdje je P' linearno preslikavanje, tj. $P'_k = \sum_{l=1}^{n} a_{kl}X_l$, a P'' je translacija, tj. $P''_k = X_k + a_{k0}$. Jasno je da svaka translacija ima inverz, zaključujemo da je P bijekcija ako i samo ako je P' bijekcija. Ako su P i Q afine zamjene koordinata na $\mathbb{A}^n$ onda su to i P^{-1} te $P \circ Q$, također, P je izomorfizam mnogostrukosti $\mathbb{A}^n$ sa samom sobom.

Definicija 2.1.12. *$V \subseteq \mathbb{A}^n$ je **linearna mnogostrukost** ako je $V = V(f_1, f_2, \ldots, f_k)$ za neki $k \in \mathbb{N}$ i polinome $f_1, f_2, \ldots, f_k \in K[X_1, X_2, \ldots, X_n]$ stupnja 1.*

Propozicija 2.1.13. *Neka je $V \subseteq \mathbb{A}^n$ linearna mnogostrukost.*

(a) Neka je P afina zamjena koordinata na $\mathbb{A}^n$, tada je V^P također linearna mnogostrukost u $\mathbb{A}^n$.

(b) Ako je $V \neq \emptyset$, tada postoje $m \in \{1, 2, \ldots, n\}$ i afina zamjena koordinata P na $\mathbb{A}^n$ takva da je $V^P = V(X_{m+1}, X_{m+2}, \ldots, X_n)$, takav $m \in \{1, 2, \ldots, n\}$ je jedinstven, tj. ne ovisi o zamjeni koordinata P.

Dokaz. Neka je $k \in \mathbb{N}$ i $f_1, f_2, \ldots, f_k \in K[X_1, X_2, \ldots, X_n]$ polinomi stupnja 1 takvi da je $V = V(f_1, f_2, \ldots, f_k)$.

(a) Želimo pokazati da je $V^P = P^{-1}(V)$ linearna mnogostrukost. Pokažemo li da je $V^P = V\left(\tilde{P}(f_1), \tilde{P}(f_2), \ldots, \tilde{P}(f_k)\right)$ gotovi smo, jer je jasno da je $\tilde{P}(f_l)$ polinom stupnja 1 za svaki $l \in \{1, 2, \ldots, k\}$. No, ta činjenica slijedi lako na skupovnoj razini:

$$a \in V^P \iff P(a) \in V \iff f_l(P(a)) = 0,\ \forall l \in \{1, 2, \ldots, k\}$$

$$\iff a \in V\left(\tilde{P}(f_1), \tilde{P}(f_2), \ldots, \tilde{P}(f_k)\right).$$

(b) Dokažimo najprije, indukcijom po broju k, da takva zamjena koordinata P i broj $m \in \{1, 2, \ldots, n\}$ postoje. Neka je $k = 1$, tj. $V = V(f_1)$, f_1 je polinom stupnja 1 pa postoje $a_0, a_1, \ldots, a_n \in K$, od kojih je barem jedan od $a_1, a_2, \ldots, a_n$ različiti od 0, takvi da je $f_1 = \sum_{l=1}^{n} a_l X_l + a_0$. Neka je $h \in \{1, 2, \ldots, n\}$ takav da je $a_h \neq 0$. Definirajmo afinu zamjenu koordinata, za $(b_1, b_2, \ldots, b_n) \in \mathbb{A}^n$, neka je:

$$P_1(b_1, b_2, \ldots, b_{h-1}, b_h, b_{h+1}, \ldots, b_n) =$$

$$= (b_1, b_2, \ldots, b_{h-1}, \frac{1}{a_h}(b_h - \sum_{\substack{l=1 \\ l \neq h}}^{n} a_l b_l - a_0), b_{h+1}, \ldots, b_n),$$

vidimo da je, $P_1^{-1}(c_1, c_2, \ldots, c_{h-1}, c_h, c_{h+1}, \ldots, c_n) =$

$$= (c_1, c_2, \ldots, c_{h-1}, \sum_{l=1}^{n} a_l c_l + a_0, c_{h+1}, \ldots, c_n),$$

za $(c_1, c_2, \ldots, c_n) \in \mathbb{A}^n$. Dakle, $V^{P_1} = V(X_h)$, definirajmo još jednu afinu zamjenu koordinata, za $(b_1, b_1, \ldots, b_n) \in \mathbb{A}^n$, neka je

$$P_2(b_1, b_2, \ldots, b_{h-1}, b_h, b_{h+1}, \ldots, b_n) = (b_1, b_2, \ldots, b_{h-1}, b_n, b_{h+1}, \ldots, b_h),$$

lako se vidi da je $P_2^{-1} = P_2$. Neka je $P = P_2 \circ P_1$, lako vidimo da je $V^P = V(X_n)$, čime je tvrdnja za $k = 1$ pokazana. Pretpostavimo da je $k > 1$ i da tvrdnja vrijedi

za $k-1$. Znamo da je $V = V(f_1, f_2, \ldots, f_k) = V(f_k) \cap V(f_1, f_2, \ldots, f_{k-1})$. Prema pretpostavci indukcije znamo da postoje afina zamjena koordinata P_1, na $\mathbb{A}^n$ i broj $m \in \{1, 2, \ldots, n\}$ takvi da je $V(f_1, f_2, \ldots, f_{k-1})^{P_1} = V(X_{m+1}, X_{m+2}, \ldots, X_n)$, sada je $V^{P_1} = V(f_k(P_1), X_{m+1}, X_{m+2}, \ldots, X_n)$. Vidimo da su varijable $X_{m+1}, X_{m+2}, \ldots X_n$ irelevantne u polinomu $f_k(P_1)$ pa ga možemo smatrati polinomom u varijablama $X_1, X_2, \ldots, X_m$. Kako je $V \neq \emptyset$, to je i $V^{P_1} \neq \emptyset$ pa je polinom $f_k(P_1)$ ili jednak nul–polinomu pa smo gotovi ili je jednak polinomu stupnja 1, jasno, u varijablama $X_1, X_2, \ldots, X_m$. U tom slučaju primijenimo već dokazanu tvrdnju za $k = 1$, tj. postoji afina zamjena koordinata P_2, koja fiksira varijable $X_{m+1}, X_{m+2}, \ldots, X_n$, takva da je $V(f_k(P_1))^{P_2} = V(X_m)$. Konačno, stavimo li da je $P = P_2 \circ P_1$, dobivamo da je $V^P = V(X_m, X_{m+1}, \ldots, X_n)$. Ovime je dokazana egzistencija tražene zamjene koordinata i broja $m \in \{1, 2, \ldots, n\}$. Pokažimo još da je taj broj m jedinstven. Pretpostavimo da postoje afine zamjene koordinata P_1, P_2 na $\mathbb{A}^n$ i brojevi m, $s \in \{1, 2, \ldots, n\}$ takvi da je

$$V^{P_1} = V(X_{m+1}, X_{m+2}, \ldots, X_n) \quad \text{te} \quad V^{P_2} = V(X_{s+1}, X_{s+2}, \ldots, X_n).$$

Dakle, $V(X_{m+1}, X_{m+2}, \ldots, X_n)^P = V(X_{s+1}, X_{s+2}, \ldots, X_n)$, pri čemu je $P = P_1^{-1} \circ P_2$. Možemo, bez smanjenja općenitosti, uzeti da je $m \leq s$. Pretpostavimo da je $m < s$. Znamo da je $V(P_{m+1}, P_{m+2}, \ldots, P_n) = V(X_{s+1}, X_{s+2}, \ldots, X_n)$, no, to sada znači da su $P_{m+1}, P_{m+2}, \ldots, P_n$ međusobno zavisne, što je kontradikcija. Dakle, pokazali smo i jedinstvenost broja m. Q.E.D.

Definicija 2.1.14. *Broj m iz dijela (b) propozicije 2.1.13 naziva se* ***dimenzija*** *linearne mnogostrukosti $V \subseteq \mathbb{A}^n$.*

Definicija 2.1.15. *Neka su $a = (a_1, a_2, \ldots, a_n)$ i $b = (b_1, b_2, \ldots, b_n)$ dvije različite točke iz $\mathbb{A}^n$.* ***Pravac*** *kroz a i b je:*

$$L = \{(a_1 + t(b_1 - a_1), a_2 + t(b_2 - a_2), \ldots, a_n + t(b_n - a_n)) \ : \ t \in K\}.$$

Lema 2.1.16.

(a) Neka su $a = (a_1, a_2, \ldots, a_n)$ *i* $b = (b_1, b_2, \ldots, b_n)$ *dvije različite točke iz* $\mathbb{A}^n$ *te neka je* L *pravac kroz* a *i* b*. Ako je* P *afina zamjena koordinata na* $\mathbb{A}^n$*, onda je* $P(L)$ *pravac kroz* $P(a)$ *i* $P(b)$*.*

(b) Svaki pravac u $\mathbb{A}^n$ *je linearna mnogostrukost dimenzije* 1 *u* $\mathbb{A}^n$ *te je svaka linearna mnogostrukost dimenzije* 1 *u* $\mathbb{A}^n$ *jednaka pravcu kroz bilo koje dvije svoje različite točke.*

(c) U $\mathbb{A}^2$ *pravac je isto što i afina hiperploha* $V(f)$*, za neki polinom* $f \in K[X, Y]$*, stupnja* 1*.*

(d) Neka su $a, b \in \mathbb{A}^2$*,* A_1, A_2 *dva različita pravca kroz* a *te* B_1, B_2 *dva različita pravca kroz* b*. Tada postoji afina zamjena koordinata* P *na* $\mathbb{A}^2$ *takva da je* $P(a) = b$ *i* $P(A_k) = B_k$*, za* $k = 1, 2$*.*

Dokaz.

(a) Neka je $P = (P_1, P_2, \ldots, P_n)$, kako je P afina zamjena koordinata, znamo da je za svaki $k \in \{1, 2, \ldots, n\}$, P_k polinom stupnja 1, tj. linearni funkcional $\mathbb{A}^n \to K$. Dakle, vidimo da je $P_k(a_k + t(b_k - a_k)) = P_k(a_k) + t(P_k(b_k) - P_k(a_k))$, iz čega odmah dobivamo traženu tvrdnju.

(b) Uz oznake iz definicije 2.1.15, zato jer je $a \neq b$, postoji $k \in \{1, 2, \ldots, n\}$ takav da je $b_k - a_k \neq 0$. Sada lako vidimo da je $L = V(f_1, f_2, \ldots, f_{k-1}, f_{k+1}, \ldots, f_n)$, gdje je

$$f_l = X_l - \frac{b_l - a_l}{b_k - a_k}(X_k - a_k) - a_l,\ l \in \{1, 2, \ldots, n\},\ l \neq k.$$

Očito je da je to linearna mnogostrukost dimenzije 1. Obratno, svaka linearna mnogostrukost dimenzije 1 je, prema dijelu (b) propozicije 2.1.13 izomorfna, preko neke

afine zamjene koordinata, P na $\mathbb{A}^n$, s $V(X_2, X_3, \ldots, X_n)$. Jasno je da to zapravo pravac $\{(k, 0, \ldots, 0) : k \in K\}$, a jasno je da je pravac jednak pravcu kroz svake dvije svoje točke. Prema (a) dijelu sada dobivamo traženu tvrdnju.

(c) Ova tvrdnja slijedi direktno iz dokaza dijela (b).

(d) Prema dijelu (c) vidimo da postoje polinomi $f_1, f_2, g_1, g_2 \in K[X, Y]$ stupnja 1 takvi da je $A_k = V(f_k)$ i $B_k = V(g_k)$, za $k = 1, 2$. Pokažemo li da postoji afina zamjena koordinata P na $\mathbb{A}^2$ takva da je $f_k(P) = g_k$, za $k = 1, 2$ gotovi smo, činjenica da je $P(a) = P(b)$ će slijediti direktno, jer, kao što smo već vidjeli, P prebacuje točke pravca na sliku tog pravca, a a je jedina zajednička točka pravaca A_1 i A_2, dok je b jedina zajednička točka pravaca B_1 i B_2. No, ta činjenice je očita, jer kao u dokazu dijela (b) propozicije 2.1.13 možemo konstruirati zamjene koordinata takve da je A_1 i B_1 izomorfno s $V(X)$, dok je A_2 i B_2 izomorfno s $V(Y)$. Odgovarajuća kompozicija tih zamjena dati će nam upravo zamjenu koja nam treba $\mathfrak{Q.E.D.}$

2.2 Racionalne funkcije i lokalni prsteni

Neka je V neprazna mnogostrukost u $\mathbb{A}^n$, znamo da je $\Gamma(V)$ integralna domena, stoga ima smisla promatrati polje razlomaka prstena $\Gamma(V)$, shvaćenog u smislu napomene 2.1.4.

Definicija 2.2.1. *Neka je V neprazna mnogostrukost u $\mathbb{A}^n$, $K(V)$ je* ***polje racionalnih funkcija na*** *V i definira se kao polje razlomaka prstena $\Gamma(V)$. Za $f \in K(V)$ kažemo da je* ***definirana*** *u točki $P \in V$ ako postoje $a, b \in \Gamma(V)$ takve da je $f = \frac{a}{b}$ i $b(P) \neq 0$.*

Primijetimo da je $f \in K(V)$ općenito moguće prikazati na puno načina, no, ako je $\Gamma(V)$ domena jedinstvene faktorizacije, prema lemi 1.2.5 taj prikaz $f = \frac{a}{b}$, gdje su a i b relativno prosti je jedinstven do na množenje brojnika i nazivnika konstantnom pa vidimo da je f definirana u $P \in V$ ako i samo ako je $b(P) \neq 0$.

Definicija 2.2.2. *Neka je $V \subseteq \mathbb{A}^n$ neprazna mnogostrukost i neka je $P \in V$.* ***Lokalni prsten od** V **u** P, $\mathcal{O}_P(V)$, je skup racionalnih funkcija na V koje su definirane u točki P. Skup točaka $P \in V$ u kojima racionalna funkcija $f \in K(V)$ nije definirana naziva se* ***skup polova funkcije** f.*

Lako se vidi da vrijede sljedeće inkluzije među prstenima:

$$K \subseteq \Gamma(V) \subseteq \mathcal{O}_P(V) \subseteq K(V).$$

Propozicija 2.2.3. *Neka je $V \subseteq \mathbb{A}^n$ neprazna mnogostrukost.*

(a) Skup polova racionalne funkcije $f \in K(V)$ je algebarski podskup od V.

(b) $\Gamma(V) = \bigcap_{P \in V} \mathcal{O}_P(V)$.

Dokaz.

(a) Neka je $J_f = \{g \in K[X_1, X_2, \ldots, X_n] : (g + I(V))\, f \in \Gamma(V)\}$, jasno je da je J_f ideal u $K[X_1, X_2, \ldots, X_n]$ koji sadrži $I(V)$. $P \in V$ je točka u kojoj f nije definirana ako ne postoje $a, b \in \Gamma(V)$ takvi da je $f = \dfrac{a}{b}$ i $b(P) \neq 0$ pa vidimo da je skup polova racionalne funkcije f upravo skup $V\left(J_f\right)$.

(b) Jasno je da je dovoljno dokazati da je $\bigcap_{P \in V} \mathcal{O}_P(V) \subseteq \Gamma(V)$. Neka je $f \in \bigcap_{P \in V} \mathcal{O}_P(V)$, to znači da je $V\left(J_f\right) = \emptyset$ iz čega po Nullstellensatz teoremu (1.5.22) dobivamo da je $J_f = K[X_1, X_2, \ldots, X_n]$, tj. $1 \in J_f$ pa je $f = 1 \cdot f \in \Gamma(V)$. Q.E.D.

Definicija 2.2.4. *Neka je $V \subseteq \mathbb{A}^n$ neprazna mnogostrukost i neka je $P \in V$. Neka je f racionalna funkcija na V koja je definirana u točki P. Definiramo* ***vrijednost od** f **u točki** P, $f(P) = \dfrac{a(P)}{b(P)}$, gdje su $a, b \in \Gamma(V)$ takve da $f = \dfrac{a}{b}$ i $b(P) \neq 0$.*

Jasno je da gornja definicija ne ovisi o odabranom prikazu racionalne funkcije f.

Definicija 2.2.5. *Ideal* $\mathfrak{m}_P(V) = \{f \in \mathcal{O}_P(V) \ : \ f(P) = 0\}$ *se naziva* ***maksimalni ideal od*** V ***u*** P.

Jasno je da je $\mathfrak{m}_P(V)$ jezgra evaluacijskog homomorfizma s $\mathcal{O}_P(V)$ na K, stoga je $\mathcal{O}_P(V)/\mathfrak{m}_P(V) \cong K$. Jasno je da je $f \in \mathcal{O}_P(V)$ invertibilna ako i samo ako je $f(P) \neq 0$, iz čega vidimo da je zapravo $\mathfrak{m}_P(V) = \{f \in \mathcal{O}_P(V) \ : \ f$ nije invertibilna$\}$ pa zaključujemo da je $\mathfrak{m}_P(V)$ uistinu maksimalan ideal u $\mathcal{O}_P(V)$, a i više, on je jedini maksimalan ideal u $\mathcal{O}_P(V)$.

Lema 2.2.6. *Neka je R prsten, tada je skup elemenata od R koji nisu invertibilni ideal ako i samo ako R ima jedinstveni maksimalni ideal koji sadrži svaki pravi ideal u R.*

Dokaz. Neka je $\mathfrak{m}$ skup svih elemenata od R koji nisu invertibilni. Ako je $\mathfrak{m}$ ideal onda je odmah jasno da je on maksimalan i jedinstven takav. Obratno, jasno je da je svaki pravi ideal u R sadržan u $\mathfrak{m}$, prsten R ima jedinstven maksimalan ideal koji sadrži svaki pravi ideal u R. Zaključujemo da taj maksimalni ideal sadrži $\mathfrak{m}$ pa može biti samo jednak $\mathfrak{m}$, dakle, $\mathfrak{m}$ je ideal. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Definicija 2.2.7. *Svaki prsten R koji zadovoljava uvjete leme 2.2.6 naziva se* ***lokalni prsten****.*

Vidimo da su elementi koji nisu invertibilni u lokalnom prstenu u pravo oni koji ne pripadaju jedinstvenom maksimalnom idealu. Također, vidimo da je $\mathcal{O}_P(V)$ lokalni prsten i $\mathfrak{m}_P(V)$ njegov maksimalni ideal, gdje je $V \subseteq \mathbb{A}^n$ neprazna mnogostrukost i $P \in V$.

Propozicija 2.2.8. *Neka je* $V \subseteq \mathbb{A}^n$ *neprazna mnogostrukost i neka je* $P \in V$. $\mathcal{O}_P(V)$ *je Noetherina lokalna integralna domena.*

Dokaz. Činjenica da je $\mathcal{O}_P(V)$ lokalna integralna domena je trivijalna. Preostaje nam dokazati da je svaki ideal I u $\mathcal{O}_P(V)$ konačno generiran. Prema napomeni 1.4.11 znamo

da je $\Gamma(V)$ Noetherin prsten pa postoje $k \in \mathbb{N}$ i $f_1, f_2, \ldots, f_k \in \Gamma(V)$ koji generiraju ideal $I \cap \Gamma(V)$ u $\Gamma(V)$. Neka je $f \in I \subseteq O_P(V)$, tada postoji $b \in \Gamma(V)$ takav da je $b(P) \neq 0$ i $bf \in \Gamma(V)$, no, kako je $f \in I$, zaključujemo da je $bf \in I \cap \Gamma(V)$ pa postoje $a_1, a_2, \ldots, a_k \in \Gamma(V)$ takvi da je $bf = \sum_{l=1}^{k} a_l f_l$, konačno, vidimo da je $f = \sum_{l=1}^{n} \frac{a_l}{b} f_l$, tj. I je generiran isto s funkcijama $f_1, f_2, \ldots, f_k$ kao ideal u $O_P(V)$. Q.E.D.

Propozicija 2.2.9. *Neka je $O_P(V)$ lokalni prsten neprazne mnogostrukosti $V \subseteq \mathbb{A}^n$ u točki $P \in V$. Tada postoji 1—1 korespodencija između prostih ideala u $O_P(V)$ i podmnogostrukosti od V koje sadrže točku P.*

Dokaz. Neka je I prost ideal u $O_P(V)$, tada je $I \cap \Gamma(V)$ prost ideal u $\Gamma(V)$. Iz dokaza propozicije 2.2.8 vidimo da $I \cap \Gamma(V)$ generira ideal I u $O_P(V)$, dok prema propoziciji 2.1.6 znamo da postoji 1—1 korespodencija između prostih ideala u $\Gamma(V)$ i podmnogostrukosti od V. Kako je $I \subseteq O_P(V)$ vidimo da sve dobivene mnogostrukosti sadrže točku P. Ovime je dokaz završen. Q.E.D.

Propozicija 2.2.10. *Neka je T afina zamjena koordinata na $\mathbb{A}^n$ i neka je $P \in \mathbb{A}^n$. Neka je $T(P) = Q$, tada je $\tilde{T} : O_Q(\mathbb{A}^n) \to O_P(\mathbb{A}^n)$ izmorfizam. Ako je $V \subseteq \mathbb{A}^n$ neprazna mnogostrukost i $P \in V^T$, onda $\tilde{T}$ inducira izomorfizam $O_Q(V) \to O_P\left(V^T\right)$.*

Dokaz. Primijetimo da drugi dio tvrdnje slijedi direktno iz prvog. Neka su $f, g \in O_Q(\mathbb{A}^n)$ takve da je $\tilde{T}(f) = \tilde{T}(g)$. To znači da je $f(T) = g(T)$, a kako je T bijekcija, zaključujemo da je $f = g$. Dakle, $\tilde{T}$ je injekcija. Neka je $g \in O_P(\mathbb{A}^n)$, ali tada je jasno da je $f = g\left(T^{-1}\right) \in O_Q(\mathbb{A}^n)$ i da je $\tilde{T}(f) = g$, dakle, $\tilde{T}$ je i bijekcija. Q.E.D.

2.3 Dodatni algebarski pojmovi i rezultati

Lema 2.3.1. *Neka je R integralna domena koja nije polje, tada je sljedeće ekvivalentno:*

(1) R je Noetherin lokalni prsten i maksimalni ideal je glavni.

(2) Postoji ireducibilni element $t \in R$ takav da se svaki $z \in R$, $z \neq 0$ može, na jedinstven način, prikazati kao $z = ut^n$, gdje je u invertibilan element u R, a $n \in \mathbb{Z}_{\geq 0}$.

Dokaz. Dokažimo najprije da (1) povlači (2). Neka je $\mathfrak{m}$ maksimalni ideal u R i neka je $t \in R$ njegov generator. Neka su u, $v \in R^*$ i neka su m, $n \in \mathbb{Z}_{\geq 0}$, $m \leq n$ takvi da je $ut^n = vt^m$. Tada je $ut^{n-m} = v$, dakle, ut^{n-m} je invertibilan element, kako t to nije, zaključujemo da je $n = m$ pa iz toga i $u = v$. Dakle, imamo jedinstvenost zapisa, preostaje dokazati da svaki $z \in R$, $z \neq 0$ ima takav prikaz. Ukoliko je $z \in R^*$ gotovi smo. Neka z nije invertibilan, to znači da je $z \in \mathfrak{m}$, tj. $z = z_1 t$ za neki $z_1 \in R$. Ako je $z_1 \in R^*$ gotovi smo, ako nije nastavljamo jednako dalje i dobivamo da je $z_n = z_{n+1} t$ za neki $z_{n+1} \in R$, gdje je $n \in \mathbb{N}$. Ukoliko je $z_n \in R^*$ za neki $n \in \mathbb{N}$ gotovi smo, pretpostavimo suprotno. Vidimo da dobivamo rastući niz ideala $(z_1) \subseteq (z_2) \subseteq \ldots$, prema propoziciji 1.5.6 taj niz se u nekom koraku stabilizira, tj. postoji $n \in \mathbb{N}$ takav da je $(z_n) = (z_{n+1})$ pa je $z_{n+1} = az_n$ za neki $a \in R$, tj. $z_n = atz_n$, što znači da je $at = 1$, što je kontradikcija jer t nije invertibilan. Obratno, (2) povlači (1). To je očito, jer je jasno da je $\mathfrak{m} = (t)$ skup elemenata u R koji nisu invertibilni i to je jedinstveni maksimalni ideal u R. Jasno je da je R Noetherin i da su svi pravi ideali u R oblika (t^n), za neki $n \in \mathbb{N}$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Definicija 2.3.2. *Prsten R koji zadovoljava uvjete leme 2.3.1 naziva se* ***prsten diskretne valuacije****, element t iz dijela (2) iste leme naziva se* ***uniformizirajući parametar*** *za R.*

Vidimo da svaki uniformizirajući parametar za R ima oblik ut, gdje je $u \in R^*$. Neka je K polje razlomaka od R i fiksirajmo neki uniformizirajući parametar t za R. Tada se svaki element $z \in K$, $z \neq 0$, prema lemi 1.2.5, može na jedinstven način prikazati kao $z = ut^n$, gdje je $u \in R^*$ i $n \in \mathbb{Z}$.

Definicija 2.3.3. *Eksponent $n \in \mathbb{Z}$ iz gornje diskusije nazivamo* ***red*** *elementa z i pišemo $n = \operatorname{ord}(z)$, dodatno, definiramo $\operatorname{ord}(0) = +\infty$.*

Primijetimo da je $R = \{z \in K \ : \ \mathrm{ord}\,(z) \geq 0\}$ te $\mathfrak{m} = \{z \in K \ : \ \mathrm{ord}\,(z) > 0\}$ je maksimalni ideal u R.

Lema 2.3.4. *Neka je R prsten diskretne valuacije i neka je K njegovo polje razlomaka.*

(a) Za $a, b \in K$, ako je $\mathrm{ord}\,(a) < \mathrm{ord}\,(b)$, onda je $\mathrm{ord}\,(a+b) = \mathrm{ord}\,(a)$.

(b) Neka su $k \in \mathbb{N}$ i $a_1, a_2, \ldots, a_k \in K$ te $l \in \{1, 2, \ldots, k\}$ takav da je $\mathrm{ord}\,(a_l) < \mathrm{ord}\,(a_h)$, za sve $h \in \{1, 2, \ldots, k\}$, $h \neq l$. Tada je $a_1 + a_2 + \ldots + a_k \neq 0$.

Dokaz. Neka je $t \in R$ uniformizirajući parametar za R te neka je $\mathfrak{m} = (t)$ jedinstveni maksimalni ideal u R.

(a) Jasno je da je $a \neq 0$, ukoliko je $b = 0$ tvrdnja je očita. Neka je $b \neq 0$ i neka su $u_1, u_2 \in R^*$ i $m, n \in \mathbb{Z}_{\geq 0}$ takvi da je $a = u_1 t^n$ i $b = u_2 t^m$, iz uvjeta $\mathrm{ord}\,(a) < \mathrm{ord}\,(b)$ dobivamo da je $n < m$. Sada je $a + b = \left(u_1 + u_2 t^{m-n}\right) t^n$. Kako je $n < m$ dobivamo da je $u_1 + u_2 t^{m-n} \in R$. Kada bi bilo $u_1 + u_2 t^{m-n} \in \mathfrak{m}$, pošto je $u_2 t^{m-n} \in \mathfrak{m}$ bilo bi $u_1 \in \mathfrak{m}$, a to je nemoguće jer je $u_1 \in R^*$. Dakle, $v = u_1 + u_2 t^{m-n} \in R^*$, tj. $a + b = v t^n$ i $v \in R^*$ pa je $\mathrm{ord}\,(a+b) = n = \mathrm{ord}\,(a)$.

(b) Jasno je da je $\mathrm{ord}\,(a_l) < +\infty$ pa je $a_l \neq 0$. Iz niza $a_1, a_2, \ldots, a_k$ izbacimo sve one koji su jednaki 0, tj. pretpostavimo da su svi različiti od 0, tada istim postupkom kao u (a) dobivamo da je $\mathrm{ord}\,(a_1 + a_2 + \ldots + a_k) = \mathrm{ord}\,(a_l) < +\infty$ iz čega vidimo da je $a_1 + a_2 + \ldots + a_k \neq 0$. Q.E.D.

Propozicija 2.3.5. *Neka je R prsten diskretne valuacije s uniformizirajućim parametrom t, neka je $\mathfrak{m} = (t)$ jedinstveni maksimalni ideal u R. Pretpostavimo da je polje K potprsten od R takav da je $\pi \circ \iota$ izomorfizam s K na $R/\mathfrak{m}$, gdje je $K \xrightarrow{\iota} R \xrightarrow{\pi} R/\mathfrak{m}$, ι ulaganje i π kanonski epimorfizam.*

(a) Za svaki $z \in R$ postoji jedinstven $\lambda \in K$ takav da je $z - \lambda \in \mathfrak{m}$.

(b) Za svaki $z \in R$ i za svaki $n \in \mathbb{Z}_{\geq 0}$ postoje jedinstveni $\lambda_0, \lambda_1, \ldots, \lambda_n \in K$ i $z_{n+1} \in R$ takvi da je $z = \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \ldots + \lambda_n t^n + z_{n+1} t^{n+1}$.

Dokaz.

(a) Ova tvrdnja je očita jer postoji jedinstven $\lambda \in K$ takav da je $\lambda + \mathfrak{m} = z + \mathfrak{m}$ u $R/\mathfrak{m}$ te točno za taj i samo taj $\lambda \in K$ vrijedi da je $z - \lambda \in \mathfrak{m}$.

(b) Neka je $z \in R$ i $n \in \mathbb{Z}_{\geq 0}$. Dokazati ćemo tvrdnju indukcijom po n. Prema dijelu (a) vidimo da tvrdnja vrijedi za $n = 0$. Neka je $n > 0$ i pretpostavimo da tvrdnja vrijedi za $n - 1$. To znači da postoje jedinstveni $\lambda_0, \lambda_1, \ldots, \lambda_{n-1} \in K$ i $z_n \in R$ takvi da je $z = \lambda_0 + \lambda_1 t + \lambda_2 t^2 + \ldots + \lambda_{n-1} t^{n-1} + z_n t^n$, no, kao što je pokazano, tvrdnja vrijedi za za $n = 0$ pa postoje jedinstveni $\lambda_n \in K$ i $z_{n+1} \in R$ takvi da je $z_n = \lambda_n + z_{n+1} t$, dakle, tvrdnja vrijedi i za n. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Neka je R integralna domena. Neka je $F \in R[X_1, X_2, \ldots, X_{n+1}]$ homogen polinom. Definiramo "dehomogenizaciju" polinoma F kao $F_* = F(X_1, X_2, \ldots, X_n, 1)$, vidimo da je $F_* \in R[X_1, X_2, \ldots, X_n]$. Obratno, za svaki polinom $f \in R[X_1, X_2, \ldots, X_n]$, različit od nul–polinoma, stupnja $d \in \mathbb{Z}_{\geq 0}$, neka je $f = f_0 + f_1 + \ldots + f_d$, gdje je f_k homogen polinom stupnja k, $k \in \{0, 1, \ldots, d\}$. Definiramo "homogenizaciju" polinoma f kao polinom $f^* \in R[X_1, X_2, \ldots, X_{n+1}]$,

$$f^* = X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + \ldots + f_d = X_{n+1}^d f\left(\frac{X_1}{X_{n+1}}, \frac{X_2}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right),$$

vidimo da je f^* homogen polinom stupnja d.

Propozicija 2.3.6. *Uz gornje oznake, neka su $F, G \in R[X_1, X_2, \ldots, X_{n+1}]$ homogeni polinomi, neka su $f, g \in R[X_1, X_2, \ldots, X_n]$ različiti od nul–polinoma i neka je $r = \deg(f)$ i $s = \deg(g)$.*

(1) $(FG)_* = F_* G_*$, $(fg)^* = f^* g^*$.

(2) Ako je $F \neq 0$ *i* $d \in \mathbb{Z}_{\geq 0}$ *je najveća potencija od* X_{n+1} *koja dijeli* F*, onda je* $X_{n+1}^{d} (F_*)^* = F$*, također je* $(f^*)_* = f$*.*

(3) $(F + G)_* = F_* + G_*$*, ako je* $f + g \neq 0$*, onda* $X_{n+1}^{t} (f + g)^* = X_{n+1}^{s} f^* + X_{n+1}^{r} g^*$*, gdje je* $t = r + s - \deg(f + g)$*.*

Dokaz. Sve tvrdnje slijede direktnim računom. Q.E.D.

Korolar 2.3.7. *Uz iste oznake, do na potencije od* X_{n+1}*, faktoriziranje homogenog polinoma* $F \in R[X_1, X_2, \ldots, X_{n+1}]$ *je isto što i faktoriziranje polinoma* F_* *u prstenu polinoma* $R[X_1, X_2, \ldots, X_n]$*. Specijalno, ako je* K *algebarski zatvoreno polje i* $F \in K[X, Y]$*, onda se* F *razlaže na produkt linearnih faktora.*

Dokaz. Prva tvrdnja je direktna posljedica propozicije 2.3.6, dok druga tvrdnja slijedi direktno iz prve i činjenice da je K algebarski zatvoreno polje. Q.E.D.

Propozicija 2.3.8. *Neka je* K *polje. Neka je, za* $n \in \mathbb{N}$, $d \in \mathbb{Z}_{\geq 0}$*:*

$$V(d, n) = \{f \in K[X_1, X_2, \ldots, X_n] \ : \ f \text{ je homogen polinom stupnja } d\}.$$

(a) $V(d, n)$ *je vektorski prostor nad* K *čiju bazu čine monomi stupnja* d*.*

(b) $\dim V(d, n) = \binom{d + n - 1}{n - 1}$.

(c) Neka su $L_1, L_2, \ldots$ $M_1, M_2, \ldots$ *nizovi linearnih (stupnja 1) homogenih polinoma u* $K[X, Y]$*. Pretpostavimo da za sve* $l, m \in \mathbb{N}$ *ne postoji* $\lambda \in K$ *takav da je* $L_l = \lambda M_m$*. Neka je, za sve* $l, m \in \mathbb{N}$, $A_{lm} = L_1 L_2 \cdots L_l \cdot M_1 M_2 \cdots M_m$*, dodatno, za* l *ili* $m = 0$*, neka je* $A_{l0} = L_1 L_2 \cdots L_l$, $A_{0m} = M_1 M_2 \cdots M_m$ *te* $A_{00} = 1$*. Tada je skup*

$$\{A_{lm} \ : \ l, m \in \mathbb{Z}_{\geq 0}, \ l + m = d\}$$

baza za $V(d, 2)$*.*

Dokaz.

(a) Ova tvrdnja je očita.

(b) Prema (a) vidimo da treba pokazati da je u prstenu $K[X_1, X_2, \ldots, X_n]$ broj monoma stupnja d jednak $\binom{d+n-1}{n-1}$, a to je jasno, jer je to upravo broj nenegativnih cjelobrojnih rješenja jednadžbe $x_1 + x_2 + \ldots + x_n = d$.

(c) Prema (b) vidimo da je dovoljno pokazati da je dani skup polinoma linearno nezavisan nad K, zato jer je broj polinoma u tom skupu jednak upravo $\binom{d+2-1}{2-1} = d+1$. Ovu tvrdnju ćemo dokazati indukcijom po $d \in \mathbb{Z}_{\geq 0}$. Za $d = 0$ tvrdnja je očita, za $d = 1$ tvrdnja direktno slijedi iz danog uvjeta. Neka je $d > 1$ i pretpostavimo da tvrdnja vrijedi za $d-1$. Neka su $\alpha_0, \alpha_1, \ldots, \alpha_d \in K$ takvi da je

$$\alpha_0 A_{0d} + \alpha_1 A_{1(d-1)} + \ldots + \alpha_d A_{d0} = 0.$$

Sada vidimo da je $\alpha_0 A_{0d} + L_1(\alpha_1 A_{0(d-1)} + \alpha_2 A_{1(d-2)} + \ldots + \alpha_d A_{(d-1)0}) = 0$. Prvi sumand je jednak $\alpha_0 M_1 M_2 \cdots M_d$, dok je drugi sadržan u idealu (L_1). Iz danog uvjeta na polinome L_1 i $M_1, M_2, \ldots, M_d$ direktno slijedi da je $\alpha_0 M_1 M_2 \cdots M_d \notin (L_1)$ pa mora biti $\alpha_0 = 0$ i $\alpha_1 A_{0(d-1)} + \alpha_2 A_{1(d-2)} + \ldots + \alpha_d A_{(d-1)0} = 0$. Konačno, iz induktivne pretpostavke slijedi da je $\alpha_1 = \alpha_2 = \ldots = \alpha_d = 0$. Q.E.D.

Neka je $n \in \mathbb{N}$ i neka su $R_1, R_2, \ldots, R_n$ prsteni. $R = R_1 \times R_2 \times \ldots \times R_n$ smatramo prstenom s uobičajenim zbrajanjem i množenjem po koordinatama.

Definicija 2.3.9. *R nazivamo **direktnim produktom prstenova** $R_1, R_2, \ldots, R_n$ i pišemo* $R = \prod_{k=1}^{n} R_k$.

Jasno je da su projekcije $\pi_k : R \to R_k$, $\pi_k(a_1, a_2, \ldots, a_n) = a_k$, $k \in \{1, 2, \ldots, n\}$ homomorfizmi prstenova. Direktni produkt prstenova karakteriziramo tako da za svaki prsten S i homomorfizme $\varphi_k : S \to R_k$, $k \in \{1, 2, \ldots, n\}$ postoji jedinstven homomorfizam

$\varphi : S \to R$ takav da je $\pi_k \circ \varphi = \varphi_k$, za sve $k \in \{1, 2, \ldots, n\}$. Specijalno, ako je K polje koje je sadržano, kao potprsten, u svakom prstenu R_k, $k = 1, 2, \ldots, n$, onda K možemo smatrati i potprstenom prstena R.

Definicija 2.3.10. *Neka su I i J ideali u prstenu R.* ***Produkt ideala*** *I i J, u oznaci IJ je ideal u R generiran skupom $\{ab \ : \ a \in I, b \in J\}$.*

Slično, za $n \in \mathbb{N}$ i $I_1, I_2, \ldots, I_n$ ideale u R definiramo $I_1 I_2 \cdots I_n$ kao ideal u R generiran skupom $\{a_1 a_2 \cdots a_n \ : \ a_1 \in I_1, a_2 \in I_2, \ldots, a_n \in I_n\}$. Za svaki ideal I u R definiramo da je $I^0 = R$, $I^1 = I$ te $I^n = II^{n-1}$, za sve $n \in \mathbb{N}$, $n > 1$. Imajmo na umu da I^n sadrži sve n-te potencije elemenata od I, ali nije nužno generiran njima. Jasno je da je $R = I^0 \supseteq I^1 \supseteq I^2 \supseteq \ldots$. Pretpostavimo li da je I generiran s $a_1, a_2, \ldots, a_k$ za neki $k \in \mathbb{N}$, onda je I^n generiran skupom $\left\{a_1^{l_1} a_2^{l_2} \cdots a_k^{l_k} \ : \ l_1, l_2, \ldots, l_k \in \mathbb{Z}_{\geq 0}, \ l_1 + l_2 + \ldots + l_k = n\right\}$.

Primjer 2.3.11. Neka je $R = K[X_1, X_2, \ldots, X_n]$ i $I = (X_1, X_2, \ldots, X_n)$. Tada je, za $d \in \mathbb{N}$, I^d generiran monomima stupnja d, tj. u I^d se nalaze oni i samo oni polinomi u kojima je svaki monom stupnja barem d. Zaključujemo da monomi stupnja manjeg od d, točnije, njihove slike pri kanonskom epimorfizmu u R/I^d tvore bazu za R/I^d, nad poljem K.

Neka je R potprsten prstena S i neka je I ideal u R. Tada je IS ideal u S generiran elementima od I. Lako se vidi da je $I^n S = (IS)^n$, za svaki $n \in \mathbb{N}$.

Definicija 2.3.12. *Neka su I i J ideali u prstenu R.* ***Suma ideala*** *I i J, u oznaci $I + J$ je jednaka $\{a + b \ : \ a \in I, b \in J\}$.*

Lako se vidi da je $I + J$ ideal u S, štoviše, to je najmanji ideal koji sadrži I i J.

Definicija 2.3.13. *Neka su I i J ideali u prstenu R. Kažemo da su I i J* ***relativno prosti ideali*** *ako je $I + J = R$.*

Primijetimo da su I i J relativno prosti ako i samo ako postoje $a \in I$ i $b \in J$ takvi da je $a + b = 1_R$. Ukoliko je $\mathfrak{m}$ maksimalni ideal u R i I ideal u R koji nije sadržan u $\mathfrak{m}$, jasno je da je $\mathfrak{m} + I = R$.

Lema 2.3.14. *Neka su I i J ideali u prstenu R. Tada je $IJ \subseteq I \cap J$, ukoliko su I i J relativno prosti, onda vrijedi jednakost.*

Dokaz. Tvrdnja da je $IJ \subseteq I \cap J$ je očita. Pretpostavimo da su I i J relativno prosti ideali, tada je

$$I \cap J = (I \cap J) R = (I \cap J)(I + J) = (I \cap J) I + (I \cap J) J \subseteq JI + IJ = IJ.$$

Dakle, vrijedi jednakost. $\mathfrak{Q.E.D.}$

Lema 2.3.15. *Neka je $N \in \mathbb{N}$ te neka su $I_1, I_2, \ldots, I_N$ i J ideali u prstenu R. Tada vrijedi da je $(I_1 + I_2 + \ldots + I_N) J = I_1 J + I_2 J + \ldots + I_N J$ te $(I_1 I_2 \cdots I_N)^n = I_1^n I_2^n \cdots I_N^n$, za svaki $n \in \mathbb{Z}_{\geq 0}$.*

Dokaz. Obje tvrdnje je dovoljno dokazati samo za $N = 2$, općenito onda lako slijedi indukcijom. No, to lako vidimo, naime:

$$\begin{aligned} (I_1 + I_2) J &= \langle \{(a_1 + a_2) b \,:\, a_1 \in I_1,\, a_2 \in I_2,\, b \in J\} \rangle \\ &= \langle \{a_1 b + a_2 b \,:\, a_1 \in I_1,\, a_2 \in I_2,\, b \in J\} \rangle = I_1 J + I_2 J. \end{aligned}$$

Za $n = 0$ tvrdnja je očita. Neka je $n > 0$, imamo

$$\begin{aligned} (I_1 I_2)^n &= \langle \{(a_{11} a_{21})(a_{12} a_{22}) \cdots (a_{1n} a_{2n}) \,:\, a_{1k} \in I_1,\, a_{2k} \in I_2,\, k \in \{1, 2, \ldots, n\}\} \rangle \\ &= \langle \{(a_{11} a_{12} \cdots a_{1n}) \cdot (a_{21} a_{22} \cdots a_{2n}) \,:\, a_{1k} \in I_1,\, a_{2k} \in I_2,\, k \in \{1, 2, \ldots, n\}\} \rangle \\ &= I_1^n I_2^n. \end{aligned}$$

$\mathfrak{Q.E.D.}$

Lema 2.3.16.

(a) *Neka su I i J relativno prosti ideali u prstenu R, tada su I^m i J^n relativno prosti ideali za sve $m, n \in \mathbb{Z}_{\geq 0}$.*

(b) *Neka je $N \in \mathbb{N}$ i neka su $I_1, I_2, \ldots, I_N$ ideali u R. Pretpostavimo da su ideali I_k i $\bigcap_{l=1,\, l\neq k}^{N} I_l$ relativno prosti, za svaki $k \in \{1, 2, \ldots, N\}$. Tada je*

$$I_1^n \cap I_2^n \cap \ldots \cap I_N^n = (I_1 I_2 \cdots I_N)^n = (I_1 \cap I_2 \cap \ldots \cap I_N)^n\,,\ \forall n \in \mathbb{N}.$$

Dokaz.

(a) Ako je $m = 0$ ili $n = 0$ tvrdnja je očita pa neka je $m > 0$ i $n > 0$. I i J su relativno prosti pa onda postoje $a \in I$ i $b \in J$ takvi da je $a + b = 1_R$. No, to znači da je $(a + b)^{m+n} = 1_R$, konačno

$$1_R = (a+b)^{m+n} = \underbrace{\sum_{k=0}^{n-1} a^m a^{n-k} b^k}_{\in I^m} + \underbrace{\sum_{k=n}^{m+n} a^{m+n-k} b^{k-n} b^n}_{\in J^n}.$$

Dakle, I^m i J^n su relativno prosti ideali u R.

(b) Ovu tvrdnju ćemo dokazati matematičkom indukcijom po N. Za $N = 1$ tvrdnja je očita. Pretpostavimo da tvrdnja vrijedi za neki $N \in \mathbb{N}$, dokažimo ju za $N + 1$. Prema pretpostavci odmah dobivamo da je

$$J = I_1^n \cap I_2^n \cap \ldots \cap I_{N+1}^n = I_1^n \cap I_2^n \cap \ldots \cap I_N^n \cap I_{N+1}^n = (I_1 \cap I_2 \cap \ldots \cap I_N)^n \cap I_{N+1}^n.$$

Ideali $I_1 \cap I_2 \cap \ldots \cap I_N$ i I_{N+1} su relativno prosti pa su prema dijelu (a) relativno prosti i ideali $(I_1 \cap I_2 \cap \ldots \cap I_N)^n$ i I_{N+1}^n, zato je, prema lemi 2.3.14,

$$(I_1 \cap I_2 \cap \ldots \cap I_N)^n \cap I_{N+1}^n = (I_1 \cap I_2 \cap \ldots \cap I_N)^n\, I_{N+1}^n,$$

a prema lemi 2.3.15 imamo $(I_1 \cap I_2 \cap \ldots \cap I_N)^n I_{N+1}^n = [(I_1 \cap I_2 \cap \ldots \cap I_N) I_{N+1}]^n$. Konačno, primijenimo li lemu 2.3.14 dobivamo $J = (I_1 \cap I_2 \cap \ldots \cap I_{N+1})^n$, a iskoristimo li pretpostavku indukcije za $n = 1$ imamo i $J = (I_1 I_2 \cdots I_{N+1})^n$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Lema 2.3.17. *Neka su I i J ideali u prstenu R. Neka je I konačno generiran i neka je $I \subseteq \mathrm{Rad}\,(J)$. Tada postoji $n \in \mathbb{N}$ takav da je $I^n \subseteq J$.*

Dokaz. Neka su $k \in \mathbb{N}$ i $a_1, a_2, \ldots, a_k \in R$ takvi da je $I = (a_1, a_2, \ldots, a_k)$. $I \subseteq \mathrm{Rad}\,(J)$ pa postoje $n_1, n_2, \ldots, n_k \in \mathbb{N}$ takvi da je $a_1^{n_1}, a_2^{n_2}, \ldots, a_k^{n_k} \in J$. Stavimo $n = n_1 + n_2 + \ldots + n_k$. Znamo, $I^n = \left\langle \left\{ a_1^{l_1} a_2^{l_2} \cdots a_k^{l_k} \,:\, l_1, l_2, \ldots, l_k \in \mathbb{Z}_{\geq 0},\ l_1 + l_2 + \ldots + l_k = n \right\} \right\rangle$, no, to znači da postoji $h \in \{1, 2, \ldots, k\}$ takav da je $l_h \geq n_h$, u suprotnom bi bilo $l_1 + l_2 + \ldots + l_k < n$. Tj. imamo da je $a_h^{l_h} = a_h^{l_h - n_h} a_h^{n_h} \in J$, konačno vidimo da je $I^n \subseteq J$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Lema 2.3.18.

(a) Neka su $I \subseteq J$ ideali u prstenu R. Postoji prirodni epimorfizam $R/I \to R/J$.

(b) Neka je I ideal u prstenu R koji je potprsten prstena S. Postoji prirodni homomorfizam $R/I \to S/IS$.

Dokaz.

(a) Tvrdnja je očita, za $r \in R$ stavimo da je $\varphi(r + I) = r + J$. φ je traženi epimorfizam, dobro je definiran jer je $I \subseteq J$, a činjenica da je riječ o surjektivnom homomorfizmu je očita.

(b) Jednostavno stavimo $\psi(r + I) = r + IS$, jasno je da je to homomorfizam, a dobro je definiran jer je $I \subseteq IS$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Lema 2.3.19. *Neka je $P = (0, 0, \ldots, 0) \in \mathbb{A}^n$, $\mathcal{O} = \mathcal{O}_P(\mathbb{A}^n)$, $\mathfrak{m} = \mathfrak{m}_P(\mathbb{A}^n)$ te neka je I ideal u $K[X_1, X_2, \ldots, X_n]$ koji je jednak $(X_1, X_2, \ldots, X_n)$. Tada je $I^k \mathcal{O} = \mathfrak{m}^k$, za sve $k \in \mathbb{N}$.*

Dokaz. Jasno je da je dovoljno dokazati da je $I\mathcal{O} = \mathfrak{m}$. No, $\frac{f}{g} \in \mathcal{O}$ je u $\mathfrak{m}$ ako i samo ako je $f(0, 0, \ldots, 0) = 0$, a iz toga zaključujemo $X_k \mid f$ (u $K[X_1, X_2, \ldots, X_n]$), za sve $k \in \{1, 2, \ldots, n\}$. No to točno znači da $X_k \mid \frac{f}{g}$ (u $\mathcal{O}$). Zaključujemo da je $I\mathcal{O} = \mathfrak{m}$. Q.E.D.

Lema 2.3.20. *Neka je V neprazna mnogostrukost u $\mathbb{A}^n$, $I = I(V) \subseteq K[X_1, X_2, \ldots, X_n]$ te $P \in V$. Neka je J ideal u $K[X_1, X_2, \ldots, X_n]$ koji sadrži I te neka je J' slika ideala J u $\Gamma(V)$. Postoji prirodni izomorfizam $\varphi : \mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n) \to \mathcal{O}_P(V)/J'\mathcal{O}_P(V)$. Specijalno, $\mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_P(\mathbb{A}^n)$ je izomorfno s $\mathcal{O}_P(V)$.*

Dokaz. U slučaju kada je $J = I$ i uz pretpostavku da vrijedi prva tvrdnja, odmah vidimo da vrijedi druga tvrdnja, zato jer je u tom slučaju $J' = J/I = I/I = \{0\}$, stoga smo gotovi dokažemo li prvu tvrdnju. Svaku funkciju $\frac{f}{g} \in \mathcal{O}_P(\mathbb{A}^n)$ možemo smatrati i kao funkciju u $\mathcal{O}_P(V)$, tako da jednostavno gledamo odgovarajuće klase od f, odnosno g u $\Gamma(V)$. Stoga je prirodno da definiramo preslikavanje $\varphi\left(\frac{f}{g} + J\mathcal{O}_P(\mathbb{A}^n)\right) = \frac{f}{g} + J'\mathcal{O}_P(V)$. Dokažemo li da je to preslikavanje dobro definirana funkcija odmah vidimo da je riječ o homomorfizmu koji je surjektivan te nam ostaje još za dokazati injektivnost. Jasno je da je $\frac{f}{g} \in J\mathcal{O}_P(\mathbb{A}^n)$ ako i samo ako je $f \in J$. No, tada odmah vidimo da gledamo li $\frac{f}{g}$ kao funkciju u $J'\mathcal{O}_P(V)$ da je pripadna klasa od f zapravo u J', jer je $I \subseteq J$. Ovime smo dobili da je dano preslikavanje dobro definiramo. Ako je $\varphi\left(\frac{f}{g} + J\mathcal{O}_P(\mathbb{A}^n)\right) = 0 + J'\mathcal{O}_P(V)$, vidimo da je klasa od f u $\Gamma(V)$ zapravo u J', a to je moguće jedino ako je $f \in J$, zato jer je $I \subseteq J$. Dakle, $\frac{f}{g} + J\mathcal{O}_P(\mathbb{A}^n) = 0 + J\mathcal{O}_P(\mathbb{A}^n)$, tj. jezgra epimorfizma φ je trivijalna, konačno zaključujemo da je φ izomorfizam. Q.E.D.

Lema 2.3.21. *Ideali $I, J \subseteq K[X_1, X_2, \ldots, X_n]$ su relativno prosti ako i samo ako je $V(I) \cap V(J) = \emptyset$.*

Dokaz. Označimo $R = K[X_1, X_2, \ldots, X_n]$. Znamo da je $V(I) \cap V(J) = V(I + J)$. Ako je $I + J = R$ jasno je da je $V(I + J) = \emptyset$, dok nam obratnu tvrdnju daje Nullstellensatz, tj. teorem 1.5.22. Q.E.D.

Lema 2.3.22. *Neka je* $I = (X, Y) \subseteq K[X, Y]$. *Vrijedi:* $\dim_K (K[X, Y]/I^n) = \frac{n(n+1)}{2}$, *za svaki prirodni broj* n.

Dokaz. Tvrdnja slijedi direktno pomoću primjera 2.3.11 i činjenice da monoma stupnja manjeg od n u $K[X, Y]$ ima točno $\frac{n(n+1)}{2}$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Sljedeći teorem će nam biti koristan da povežemo lokalna svojstva (gdje ulogu igraju lokalni prsteni) s globalnim svojstvima (koordinatni prsteni).

Teorem 2.3.23. *Neka je* I *ideal u* $K[X_1, X_2, \ldots, X_n]$ *te neka je* $V(I) = \{P_1, P_2, \ldots, P_m\}$, *za neki* $m \in \mathbb{N}$, *konačan skup točaka iz* $\mathbb{A}^n$. *Neka je* $\mathcal{O}_k = \mathcal{O}_{P_k}(\mathbb{A}^n)$, *za sve* $k \in \{1, 2, \ldots, m\}$, *tada je*

$$K[X_1, X_2, \ldots, X_n]/I \cong \prod_{k=1}^{m} (\mathcal{O}_k/I\mathcal{O}_k).$$

Dokaz. Prema (b) dijelu leme 2.3.18 znamo da, za svaki $k \in \{1, 2, \ldots, m\}$, postoji prirodni homomorfizam $\varphi_k : R \to R_k$, gdje je $R = K[X_1, X_2, \ldots, X_n]/I$ i $R_k = \mathcal{O}_k/I\mathcal{O}_k$. Jasno je da ovime dobivamo homomorfizam $\varphi : R \to \prod_{k=1}^{m} R_k$, tako da stavimo $\varphi = (\varphi_1, \varphi_2, \ldots, \varphi_m)$. Tvrdimo da je taj homomorfizam zapravo izomorfizam. Dokažimo to. Neka je, za sve $k \in \{1, 2, \ldots, m\}$, $I_k = I(\{P_k\})$. Jasno je da je $I \subseteq I_k$, $\forall k \in \{1, 2, \ldots, m\}$. Prema Hilbertovom teoremu (1.5.22) o nulama znamo da je $\mathrm{Rad}(I) = I(\{P_1, P_2, \ldots, P_m\}) = \bigcap_{k=1}^{m} I_k$, prema lemi 2.3.17 sada vidimo da postoji $d \in \mathbb{N}$ takav da je $\left(\bigcap_{k=1}^{m} I_k\right)^d \in I$. Prema lemi 2.3.21 vidimo da su, za svaki $l \in \{1, 2, \ldots, m\}$, ideali $\bigcap_{k=1, k\neq l}^{m} I_k$ i I_l relativno prosti, stoga je, prema (b) dijelu leme 2.3.16, $\bigcap_{k=1}^{m} I_k^d = \left(\bigcap_{k=1}^{m} I_k\right)^d \subseteq I$. Prema lemi 1.5.3, za svaki $k \in \{1, 2, \ldots, m\}$, možemo odabrati $F_k \in K[X_1, X_2 \ldots, X_n]$ takav da je $F_k(P_l) = \delta_{kl}$ (Kroneckerova delta, tj. 1 ako je $l = k$, inače 0.), za sve $l \in \{1, 2, \ldots, m\}$. Neka je, za sve $k \in \{1, 2, \ldots, m\}$, $E_k = 1 - \left(1 - F_k^d\right)^d$, lako vidimo da postoji $D_k \in K[X_1, X_2, \ldots, X_n]$ takav da je $E_k = F_k^d D_k$.

Dakle je $E_k \in I_l^d$ ako i samo ako je $l \neq k$, za sve $l \in \{1, 2, \ldots, m\}$. Lako se vide sljedeće dvije činjenice:

$$1 - \sum_{k=1}^{m} E_k = (1 - E_l) - \sum_{k=1, k\neq l}^{m} E_k \ (\forall l \in \{1, 2, \ldots, m\}) \ \in \bigcap_{k=1}^{m} I_k^d \subseteq I,$$

$$E_k E_l \in \left(\bigcap_{h=1, h\neq k}^{m} I_h^d \right) I_k^d \subseteq \bigcap_{h=1}^{m} I_h^d \subseteq I, \ \forall k, \, l \in \{1, 2, \ldots, m\}, \ k \neq l.$$

Neka je e_k jednak odgovarajućoj klasi polinoma E_k u R, za $k \in \{1, 2, \ldots, m\}$. Tada je prema prethodnim činjenicama:

$$\sum_{h=1}^{m} e_h = 1, \ e_k e_l = 0, \ \forall k, \, l \in \{1, 2, \ldots, m\}, \ k \neq l.$$

Dokažimo pomoćnu tvrdnju. Neka je $G \in K[X_1, X_2, \ldots, X_n]$ takav da je $G(P_1) \neq 0$ tada postoji $T \in K[X_1, X_2, \ldots, X_n]$ takav da je $tg = e_1$, gdje su g i t odgovarajuće klase polinoma G i T u R. Jasno je da možemo pretpostaviti da je $G(P_1) = 1$. Neka je $Q = 1 - G$, jasno je da je $Q \in I_1$, odnosno $Q^d \in I_1^d$ pa je $Q^d E_1 \in \bigcap_{k=1}^{m} I_k^d \subseteq I$. Sada je jasno, stavimo li $T = E_1 + QE_1 + \ldots + Q^{d-1}E_1$, imamo $TG = E_1 - Q^d E_1$, odnosno $tg = e_1$. Konačno, uz sve do sada pokazano, dokazujemo da je φ injekcija i surjekcija. Neka je f odgovarajuća klasa polinoma $F \in K[X_1, X_2, \ldots, X_n]$ u R te neka je $\varphi(f) = 0$. To znači da je, za svaki $k \in \{1, 2, \ldots, m\}$, $\varphi_k(f) = 0$, odnosno, postoji $G_k \in K[X_1, X_2, \ldots, X_n]$ takav da je $G_k(P_k) \neq 0$ i $G_k F \in I$. Prema pomoćnoj tvrdnji, postoji $T_k \in K[X_1, X_2, \ldots, X_n]$ takav da je $t_k g_k = e_k$, gdje su t_k i g_k uobičajeno odgovarajuće klase polinoma T_k i G_k u R. Sada je $f = f \sum_{k=1}^{m} e_k = \sum_{k=1}^{m} t_k g_k f = 0$, jer je $g_k f_k = 0$, za sve $k \in \{1, 2, \ldots, m\}$. Dakle, φ je injekcija. Neka je $k \in \{1, 2, \ldots, m\}$. Kako je $E_k(P_k) = 1 \neq 0$ vidimo da je $\varphi_k(e_k) \neq 0$. Nadalje, $\varphi_k(e_k)\varphi_k(e_l) = \varphi_k(e_k e_l) = \varphi_k(0) = 0$, za svaki $l \in \{1, 2, \ldots, m\}$, $l \neq k$, iz toga je $\varphi_k(e_l) = 0$. Zaključujemo da je $\varphi_k(e_k) = \varphi_k\left(\sum_{h=1}^{m} e_h\right) = \varphi_k(1) = 1$. Konačno, pokazujemo da je φ surjekcija, neka je $z = \left(\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_m}{b_m}\right) \in \prod_{k=1}^{m} R_k$. Prema pomoćnoj tvrdnji znamo

da, za svaki $k \in \{1, 2, \ldots, m\}$, postoji (odgovarajuća klasa nekog polinoma) t_k takav da je $t_k b_k = e_k$, tj. $\dfrac{a_k}{b_k} = a_k t_k$. Konačno, vidimo da je $\varphi_k\left(\sum_{l=1}^{m} a_l t_l e_l\right) = \varphi_k(a_k t_k) = \dfrac{a_k}{b_k}$, odnosno, $\varphi\left(\sum_{l=1}^{m} a_l t_l e_l\right) = z$. Ovime smo dobili da je φ i surjekcija. $\mathfrak{Q.E.D.}$

Sljedeća dva korolara su direktna posljedica prethodnog teorema, stoga ih navodimo bez dokaza.

Korolar 2.3.24. *Neka je I ideal u $K[X_1, X_2, \ldots, X_n]$ te neka je $V(I) = \{P_1, P_2, \ldots, P_m\}$, za neki $m \in \mathbb{N}$, konačan skup točaka iz $\mathbb{A}^n$. Tada je*

$$\dim_K\left(K[X_1, X_2, \ldots, X_n]/I\right) = \sum_{k=1}^{m} \dim_K\left(\mathcal{O}_{P_k}(\mathbb{A}^n)/I\mathcal{O}_{P_k}(\mathbb{A}^n)\right).$$

Korolar 2.3.25. *Neka je I ideal u $K[X_1, X_2, \ldots, X_n]$ te neka je $V(I) = \{P\}$, gdje je $P \in \mathbb{A}^n$, tada je*

$$K[X_1, X_2, \ldots, X_n]/I \cong \mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_P(\mathbb{A}^n).$$

Reći ćemo još ponešto o kvocijentima modula i egzaktnim nizovima, zatim napokon dolazimo na ravninske krivulje i njihova osnovna (lokalna) svojstva.

Definicija 2.3.26. *Neka je R prsten i neka su M i M' R–moduli. Homomorfizam Abelovih grupa $\varphi : M \to M'$ se naziva* ***homomorfizam R–modula*** *ako je $\varphi(rm) = r\varphi(m)$, za sve $r \in R$ i $m \in M$.*

Jasno, ukoliko je φ injektivan, surjektivan, odnosno bijektivan kažemo da je on monomorfizam, epimorfizam, odnosno izomorfizam R–modula.

Neka je R prsten i neka je N R–podmodul R–modula M. Za svaki $m \in M$ i $r \in R$ stavljamo da je $r(m + N) = rm + N$. Lako vidimo da smo ovime kvocijentnu grupu M/N učinili R–modulom i to tako da je kanonski epimorfizam $M \to M/N$ zapravo epimorfizam R–modula.

Definicija 2.3.27. *Uz prethodne oznake i diskusiju, M/N se naziva* ***kvocijentni modul*** *modula M po podmodulu N.*

Definicija 2.3.28. *Neka je R prsten, neka su M, M', M'' R–moduli i neka su $\varphi : M' \to M$ i $\psi : M \to M''$ homomorfizmi R–modula. Kažemo da je niz (modula i homomorfizama)*

$$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M''$$

egzaktan *(u M) ako je* $\mathrm{Im}\,(\varphi) = \mathrm{Ker}\,(\psi)$.

Uz iste oznake, lako vidimo da su nizovi

$$0 \to M' \xrightarrow{\varphi} M \quad \text{i} \quad M \xrightarrow{\psi} M'' \to 0$$

egzaktni ako i samo ako je φ injekcija i ψ surjekcija. To slijedi iz činjenice što postoje jedinstveni homomorfizmi R–modula $0 \to M'$ i $M'' \to 0$, oba jednaka konstanti 0. Analogno, za prsten R, R–module $M_1, M_2, \ldots, M_{n+1}$ ($n \in \mathbb{N}$, $n \geq 2$) i homomorfizme R–modula $\varphi_k : M_k \to M_{k+1}$, za $k = 1, 2, \ldots, n$, reći ćemo da je niz

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} \ldots \xrightarrow{\varphi_n} M_{n+1}$$

egzaktan ako je $\mathrm{Im}\,(\varphi_k) = \mathrm{Ker}\,(\varphi_{k+1})$, za $k = 1, 2, \ldots, n-1$. Dakle, uz uobičajene oznake, niz

$$0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0$$

je egzaktan ako i samo ako je φ injekcija i ψ surjekcija te $\mathrm{Im}\,(\varphi) = \mathrm{Ker}\,(\psi)$.

Propozicija 2.3.29.

(a) Neka je $0 \to V' \xrightarrow{\varphi} V \xrightarrow{\psi} V'' \to 0$ egzaktni niz konačno dimenzionalnih vektorskih prostora (i linearnih preslikavanja) nad poljem K. Tada je $\dim V' + \dim V'' = \dim V$.

(b) Neka je $0 \to V_1 \xrightarrow{\varphi_1} V_2 \xrightarrow{\varphi_2} V_3 \xrightarrow{\varphi_3} V_4 \to 0$ *egzaktni niz konačno dimenzionalnih vektorskih prostora (i linearnih preslikavanja) nad poljem* K*. Tada je*

$$\dim V_1 - \dim V_2 + \dim V_3 - \dim V_4 = 0.$$

Dokaz.

(a) Ovo slijedi direktno iz teorema o rangu i defektu i činjenice da je $V' \cong \operatorname{Ker}(\psi)$ i $V'' = \operatorname{Im}(\psi)$.

(b) Označimo $W = \operatorname{Im}(\varphi_2) = \operatorname{Ker}(\varphi_3)$ te neka je $\psi : W \to V_3$ ulaganje, tada su nizovi

$$0 \to V_1 \xrightarrow{\varphi_1} V_2 \xrightarrow{\varphi_2} W \to 0 \quad \text{i} \quad 0 \to W \xrightarrow{\psi} V_3 \xrightarrow{\varphi_3} V_4 \to 0$$

egzaktni. Prema (a) dijelu tada vidimo da je $\dim V_1 + \dim W = \dim V_2$ te također $\dim W + \dim V_4 = \dim V_3$. Oduzimanjem ove dvije jednakosti dobivamo traženu tvrdnju. Q.E.D.

Lema 2.3.30. *Neka je* $\mathcal{O}$ *lokalni prsten i* $\mathfrak{m}$ *njegov jedinstveni maksimalni ideal, tada, za svaki* $n \in \mathbb{N}$*, postoji prirodni egzaktni niz* $\mathcal{O}$*–modula i homomorfizama* $\mathcal{O}$*–modula:*

$$0 \to \mathfrak{m}^n/\mathfrak{m}^{n+1} \xrightarrow{\varphi} \mathcal{O}/\mathfrak{m}^{n+1} \xrightarrow{\psi} \mathcal{O}/\mathfrak{m}^n \to 0.$$

Dokaz. Jednostavno stavimo da je φ ulaganje te $\psi\left(f + \mathfrak{m}^{n+1}\right) = f + \mathfrak{m}^n$, za svaki $f \in \mathcal{O}$. ψ je dobro definirano jer je $\mathfrak{m}^{n+1} \subseteq \mathfrak{m}^n$. Q.E.D.

Lema 2.3.31. *Neka je* R *prsten diskretne valuacije s uniformizirajućim parametrom* t *i maksimalnim idealom* $\mathfrak{m} = (t)$*. Pretpostavimo da je polje* K *potprsten od* R *takav da je* $\pi \circ \iota$ *izomorfizam s* K *na* $R/\mathfrak{m}$*, gdje je* $K \xrightarrow{\iota} R \xrightarrow{\pi} R/\mathfrak{m}$*,* ι *ulaganje i* π *kanonski epimorfizam.*

(a) Za svaki $n \in \mathbb{Z}_{\geq 0}$ *je* $\dim_K\left(\mathfrak{m}^n/\mathfrak{m}^{n+1}\right) = 1$ *i* $\dim_K(R/\mathfrak{m}^n) = n$*.*

(b) Neka su $z \in R$ *i* $n \in \mathbb{Z}_{\geq 0}$ *takvi da je* $(z) = \mathfrak{m}^n$*, tada je* $\operatorname{ord}(z) = n = \dim_K(R/(z))$*.*

Dokaz.

(a) Prva tvrdnja je očita, jasno je da je baza za $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ nad K jednaka $t^n + \mathfrak{m}^{n+1}$. Drugu tvrdnju dobivamo direktno iz (b) dijela propozicije 2.3.5.

(b) Jasno je da je dovoljno pokazati da je $\operatorname{ord}(z) = n$. No, to slijedi direktno iz činjenice da je $(z) = \mathfrak{m}^n = (t^n)$, što nam govori da se z i t^n razlikuju do na množenje invertibilnim elementom, a to točno znači da je $\operatorname{ord}(z) = n$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

2.4 Ravninske krivulje

Polje K nam je i dalje algebarski zatvoreno. Uvesti ćemo malo drukčiju definiciju pojma afine ravninske krivulje, no ona u suštini ostaje ista, samo je na ovaj način operativnija. Naime, iako su skupovi točaka u $\mathbb{A}^2$ koje zadovoljavaju jednadžbe $X = 0$ i $X^2 = 0$ geometrijski jednaki, mi ćemo te dvije krivulje smatrati (algebarski) različitima.

Definicija 2.4.1. *Za dva polinoma $F, G \in K[X, Y]$ kažemo da su* ***ekvivalentni*** *ako je $F = \lambda G$ za neki $0 \neq \lambda \in K$.* ***Afina ravninska krivulja*** *je odgovarajuća klasa ekvivalencije nekog nekonstantnog polinoma u $K[X, Y]$.*

Lako se vidi da imamo relaciju ekvivalencije. Govoriti ćemo naprosto "krivulja" kada god je iz konteskta jasno na što se točno misli. Nekonstantni polinom $F \in K[X, Y]$ ćemo smatrati i krivuljom, znajući da pri tome zapravo mislimo na cijelu klasu ekvivalencije.

Definicija 2.4.2. ***Stupanj*** *krivulje je stupanj definirajućeg polinoma. Krivulje stupnja* 1 *nazivamo* ***pravcima****.*

Ova definicija pravca se podudara s već spomenutom (2.1.15), što se lako vidi. Također, jasno je da definicija stupnja ne ovisi o izboru definirajućeg polinoma.

Definicija 2.4.3. *Neka je* $F \in K[X, Y]$ *te neka je* $F = \prod_{k=1}^{n} F_k^{r_k}$, *gdje su* $n, r_1, r_2, \ldots, r_n \in \mathbb{N}$ *i* $F_k \in K[X, Y]$ ($k \in \{1, 2, \ldots, n\}$) *ireducibilni polinomi, rastav polinoma* F *u ireducibilne faktore. Kažemo da su* F_k ***komponente*** *od* F, *a broj* r_k *je* ***kratnost*** *komponente* F_k. *Kažemo da je komponenta* F_k ***jednostruka*** *ako je* $r_k = 1$, *inače kažemo da je* ***višestruka***.

Primijetimo da komponente krivulje F možemo odrediti iz $V(F)$, no ne možemo znati njihove kratnosti. Ako je F ireducibilna krivulja (ireducibilni polinom), onda je $V(F)$ (neprazna) mnogostrukost u $\mathbb{A}^2$, kraće ćemo pisati $\Gamma(F)$, $K(F)$ i $\mathcal{O}_P(F)$, umjesto $\Gamma(V(F))$, $K(V(F))$ i $\mathcal{O}_P(V(F))$.

Regularne i singularne točke

U izrazu "neka je F krivulja" ćemo podrazumijevati da je krivulja zapravo odgovarajuća klasa ekvivalencije nekonstantnog polinoma $F \in K[X, Y]$. F_X i F_Y su, standardno, oznake za derivaciju polinoma F po varijabli X, odnosno Y.

Definicija 2.4.4. *Neka je* $P = (a, b)$ *točka krivulje* F. *Točka* P *je* ***regularna*** *točka krivulje* F *ako je* $F_X(P) \neq 0$ *ili* $F_Y(P) \neq 0$. ***Tangenta*** *na krivulju* F *u njenoj regularnoj točki* P *je pravac* $F_x(P)(X - a) + F_Y(P)(Y - b) = 0$. ***Singularna*** *točka je ona koja nije regularna, nazivamo ih još i višestrukima. Krivulja kojoj su sve točke regularne naziva se* ***glatka*** *(ili nesingularna ili regularna) krivulja.*

Definicija 2.4.5. *Neka je* F *kivulja i neka je* $P = (0, 0) \in \mathbb{A}^2$. *Neka je* $F = \sum_{k=0}^{n} F_k$, *gdje je* $n \in \mathbb{N}$ *i* F_k *homogen polinom stupnja* $k \in \{0, 1, \ldots, n\}$, $F_n \neq 0$, *jedinstven prikaz polinoma* F *kao sume homogenih polinoma. Definiramo* ***kratnost*** *(ili multiplicitet) točke* P *na krivulji* F *kao najmanji* $m \in \{0, 1, \ldots, n\}$ *takav da je* $F_m \neq 0$. *Označavamo* $m = m_P(F)$.

Primijetimo da je $P \in F$ ako i samo ako je $m_P(F) > 0$. Također, lako se vidi da je točka P regularna ako i samo ako je $m_P(F) = 1$, u tom slučaju je tangenta na krivulju F u točki P

jednaka upravo F_1. Prirodno ćemo u slučaju $m = 2$ reći da je riječ o dvostrukoj, u slučaju $m = 3$ trostrukoj, tj. općenito m-strukoj točki krivulje F. F_m je homogen polinom u dvije varijable pa se prema korolaru 2.3.7 razlaže u produkt linearnih faktora. Zato možemo pisati $F_m = \prod_{k=1}^{n} L_k^{r_k}$, gdje su $n \in \mathbb{N}$, L_k pravci i $r_k \in \mathbb{N}$, $k \in \{1, 2, \ldots, n\}$.

Definicija 2.4.6. *L_k, $k = 1, 2, \ldots, n$ su **tangente** na F u točki $P = (0, 0)$, r_k je **kratnost** odgovarajuće tangente. Ako je $r_k = 1$ kažemo da je pravac L_k jednostruka tangenta, ako je $r_k = 2$ kažemo da je dvostruka, i slično za ostale. Dodatno, za pravac točkom P koji nije tangenta krivulje F kažemo da je kratnosti* 0.

Definicija 2.4.7. *Ako krivulja F ima m (stupanj polinoma F_m) različitih (tada su, jasno, sve jednostruke) tangenti u točki P, kažemo da je P **jednostavna** m-struka točka krivulje F. Jednostavna dvostruka točka naziva se **čvor**.*

Neka je F krivulja, $n \in \mathbb{N}$ i $F = \prod_{k=1}^{n} F_k^{e_k}$ rastav na ireducibilne faktore. Tada je, za $P = (0, 0)$, $m_P(F) = \sum_{k=1}^{n} e_k m_P(F_k)$. Nadalje, ukoliko je pravac L tangenta na krivulju F_k (u točki P) kratnosti $r_k \in \mathbb{Z}_{\geq 0}$, za $k \in \{1, 2, \ldots, n\}$, onda je L tangenta na krivulju F kratnosti $\sum_{k=1}^{n} e_k r_k$. Dakle, vidimo da je točka P regularna točka krivulje F ako i samo ako P pripada točno jednoj komponenti, F_k, krivulje F te je $e_k = 1$ i P je regularna točka komponente F_k.

Preostaje nam proširiti sve uvedene definicije općenito na točku $P = (a, b) \neq (0, 0)$. Neka je F krivulja i neka je T translacija (Specijalno, afina zamjena koordinata.) koja prebacuje $(0, 0) \mapsto (a, b)$, tj. $T(x, y) = (x + a, y + b)$. Tada je $F^T = F(X + a, Y + b)$. Definiramo $m_P(F) = m_{(0,0)} F^T$. Neka je $F^T = F_m + F_{m+1} + \ldots$, prikaz u obliku sume homogenih polinoma, gdje je $F_m \neq 0$ i $m = m_P(F)$. Neka je $F_m = \prod_{k=1}^{n} L_k^{r_k}$, gdje su $L_k = \alpha_k X + \beta_k Y$ pravci, kao i prije. Definiramo da su $\alpha_k(X - a) + \beta_k(Y - b)$ tangente na krivulju F u točki P, a r_k odgovarajuće kratnosti. Primijetimo da T prebacuje točke krivulje F^T u točke krivulje F i da T prebacuje tangente na krivulju F^T u točki $(0, 0)$ u tangente na krivulju F

u točki P. Također, $F_X(P) = F_X^T(0, 0)$ i $F_Y(P) = F_Y^T(0, 0)$, stoga je P regularna točka krivulje F ako i samo ako je $m_p(F) = 1$ i definicija tangente na ovaj način se podudara s onom u definiciji 2.4.4. Sljedeća dva teorema će nam dati vezu između kratnosti točke P na ireducibilnoj krivulji F i lokalnog prstena $\mathcal{O}_P(F)$. Za svaki polinom $G \in K[X, Y]$, g će nam označavati sliku polinoma G u odgovarajućem koordinatnom prstenu krivulje F, $\Gamma(F) = K[X, Y]/(F)$. Slobodnije rečeno, polinome ćemo označavati "velikim" slovima, dok će nam njihove slike predstavljati odgovarajuća "mala" slova.

Teorem 2.4.8. *Neka je $P \in \mathbb{A}^2$ točka ireducibilne krivulje F. Tada za svaki dovoljno velik $n \in \mathbb{N}$, točnije $n \geq m_P(F)$, vrijedi*

$$m_P(F) = \dim_K \left(\mathfrak{m}_P(F)^n / \mathfrak{m}_P(F)^{n+1} \right).$$

Dokaz. Bez smanjenja općenitosti neka je $P = (0, 0)$. Neka je $\mathcal{O} = \mathcal{O}_P(F)$ i $\mathfrak{m} = \mathfrak{m}_P(F)$. Također, označimo $m = m_P(F)$. Prema lemi 2.3.30 postoji (prirodni) egzaktni niz

$$0 \to \mathfrak{m}^n/\mathfrak{m}^{n+1} \to \mathcal{O}/\mathfrak{m}^{n+1} \to \mathcal{O}/\mathfrak{m}^n \to 0.$$

Propozicija 2.3.29, tj. njen (a) dio nam govori da je

$$\dim_K \left(\mathfrak{m}^n/\mathfrak{m}^{n+1} \right) = \dim_K \left(\mathcal{O}/\mathfrak{m}^{n+1} \right) - \dim_K \left(\mathcal{O}/\mathfrak{m}^n \right),$$

iz čega vidimo da je dovoljno pokazati da je $\dim_K(\mathcal{O}/\mathfrak{m}^n) = nm + c$, gdje je $c \in \mathbb{Z}$ konstanta, za sve $n \in \mathbb{N}$, $n \geq m$. Neka je $I = (X, Y) \subseteq K[X, Y]$. Prema lemi 2.3.19 je $\mathfrak{m}^n = I^n\mathcal{O}$. Neka je (I^n, F) ideal u $K[X, Y]$ generiran skupom $I^n \cup \{F\}$. Prema korolaru 2.3.25 i činjenici da je $V(I^n, F) = \{(0, 0)\} = \{P\}$ vidimo da je

$$K[X, Y]/(I^n, F) \cong \mathcal{O}_P\left(\mathbb{A}^2\right)/(I^n, F)\,\mathcal{O}_P\left(\mathbb{A}^2\right).$$

Nadalje, jasno je da ideal (I^n, F) sadrži ideal I^n i da je slika tog ideala u $\Gamma(F)$ jednaka I^n, točnije, odgovarajućim slikama polinoma iz I^n, zato je prema lemi 2.3.20

$$K[X, Y]/(I^n, F) \cong \mathcal{O}_P(F)/I^n\mathcal{O}_P(F) = \mathcal{O}/\mathfrak{m}^n.$$

Dakle, moramo izračunati $\dim_K (K[X, Y] / (I^n, F))$. Promotrimo niz

$$0 \to K[X, Y]/I^{n-m} \xrightarrow{\varphi} K[X, Y]/I^n \xrightarrow{\psi} K[X, Y]/(I^n, F) \to 0,$$

gdje je $\psi(G + I^n) = G + (I^n, F)$ i $\varphi(G + I^{n-m}) = FG + I^n$, za svaki $G \in K[X, Y]$. Jasno je da je ψ dobro definiram homomorfizam, jer je $I^n \subseteq (I^n, F)$, dok je φ dobro definiran zato što je $F \in I^m$ pa onda, ako je $G \in I^{n-m}$ je $FG \in I^n$. Dakle, promatrani niz je egzaktan. Prema (a) dijelu propozicije 2.3.29 i lemi 2.3.22 sada konačno slijedi

$$\dim_K (K[X, Y] / (I^n, F)) = \frac{n(n+1)}{2} - \frac{(n-m)(n-m+1)}{2} = nm + \frac{m(1-m)}{2},$$

za sve $n \in \mathbb{N}$, $n \geq m$. Q.E.D.

Teorem 2.4.9. *Neka je F ireducibilna krivulja. Točka P je regularna točka krivulje F ako i samo ako je $\mathcal{O}_P(F)$ prsten diskretne valuacije. U tom slučaju, ako je L bilo koji pravac točkom P koji nije tangenta krivulje F u točki P, onda je slika l, pravca L u $\mathcal{O}_P(F)$ uniformizirajući parametar za $\mathcal{O}_P(F)$.*

Dokaz. Pretpostavimo da je $\mathcal{O}_P(F)$ prsten diskretne valuacije, tada iz prethodnog torema (2.4.8) i (a) dijela leme 2.3.31 vidimo da je $m_P(F) = 1$, tj. P je regularna točka krivulje F. Obratno, pretpostavimo da je P regularna točka krivulje F i da je L pravac točkom P koji nije tangenta na krivulju F u točki P. Prema (d) dijelu leme 2.1.16 i propoziciji 2.2.10 možemo, bez smanjenja općenitosti, (napravimo odgovarajuću afinu zamjenu koordinata) pretpostaviti da je $P = (0, 0)$, Y tangenta na F u točki P i $L = X$. Prema lemi 2.3.1 dovoljno je pokazati da je x (Podsjetimo se, prema dogovoru, x je oznaka za sliku polinoma X u $\Gamma(F)$.) generator za $\mathfrak{m}_P(F)$. Prema lemi 2.3.19 znamo da je $\mathfrak{m}_P(F) = (x, y)$. Prema pretpostavkama, možemo pisati $F = Y + (\text{homogeni polinomi stupnja} > 1)$. Grupirajmo zajedno sve one koji su djeljivi s Y pa vidimo da je $F = YG - X^2H$, gdje su G, $H \in K[X, Y]$ takvi da je $G = 1 + (\text{polinom bez konstantnog člana})$ (ili $G = 1$) i $\deg_Y(H) = 0$ (ili $H = 0$). Sada vidimo da je, u $\Gamma(F)$, $yg = x^2h$, a kako je $g(P) \neq 0$, jer je $G(P) = 1$, vidimo da je $y = x^2hg^{-1}$. Konačno, $y \in (x)$, iz čega zaključujemo da je $\mathfrak{m}_P(F) = (x)$. Q.E.D.

Definicija 2.4.10. *Neka je P regularna točka ireducibilne krivulje F. Definiramo funkciju* ord_P^F *koja svakom elementu iz $K(F)$ pridružuje red induciran prstenom diskretne valuacije $\mathcal{O}_P(F)$, kao u definiciji 2.3.3.*

Kada je jasno o kojoj se krivulji radi, pisati ćemo jednostavno ord_P. Za $G \in K[X, Y]$ pisati ćemo $\mathrm{ord}_P^F(G)$ umjesto $\mathrm{ord}_P^F(g)$ (g je slika polinoma G u $\Gamma(F)$). Ako je P regularna točka reducibilne krivulje F, onda, kako je P regularna, postoji jedna i samo jedna ireducibilna komponenta F_k krivulje F koja sadrži P. U tom slučaju ćemo isto pisati ord_P^F, umjesto preciznijeg $\mathrm{ord}_P^{F_k}$.

Napomena 2.4.11. *Neka je P regularna točka krivulje F i neka je L bilo koji pravac točkom P. Tada je* $\mathrm{ord}_P^F(L) = 1$ *ako L nije tangenta na krivulju F u točki P i* $\mathrm{ord}_P^F(L) \geq 2$ *ako L je tangenta na krivulju F u točki P. Zašto? Naime, pretpostavimo sve isto kao i u dokazu teorema 2.4.9, tj. Y je tangenta i $y = x^2hg^{-1}$, iz čega vidimo da je* $\mathrm{ord}_P(y) = \mathrm{ord}_P\left(x^2\right) + \mathrm{ord}_P\left(hg^{-1}\right) = 2 + \mathrm{ord}_P\left(hg^{-1}\right) \geq 2$.

2.5 Multipliciteti presjeka

Neka su F i G ravninske krivulje, definirati (pomoću svojstava koja prirodno želimo da ima) ćemo multiplicitet presjeka, u oznaci $I(P, F \cap G)$, krivulja F i G u točki $P \in \mathbb{A}^2$ i dati eksplicitnu formulu za njega i vrlo operativan algoritam za računanje istoga. Najprije dajemo jednu uvodnu definiciju, a zatim slijedi definicija multipliciteta presjeka. Ta definicija će zapravo sadržavati svojstva (neka se mogu lako izvesti iz preostalih) koja prirodno očekujemo od takvog broja, a nakon nje slijedi teorem (prije kojega će biti jedna pomoćna lema) koji nam daje eksplicitnu formulu broja $I(P, F \cap G)$ u čijem dokazu će biti opisan i algoritam za njegovo računanje.

Definicija 2.5.1. *Kažemo da se krivulje F i G sijeku* ***transverzalno*** *u točki $P \in \mathbb{A}^2$ ako je*

P regularna točka i krivulje F i krivulje G i ako je tangenta na krivulju F u točki P različita od tangente na krivulju G u točki P.

Definicija 2.5.2. *Neka su F i G ravninske krivulje i neka je* $P \in \mathbb{A}^2$. ***Multiplicitet presjeka*** *krivulja F i G u točki P je broj* $I(P, F \cap G)$ *koji zadovoljava sljedećih devet svojstava.*

(1) $I(P, F \cap G) \in \mathbb{Z}_{\geq 0}$ *ako F i G nemaju zajedničku komponentu koja sadrži točku P,* $I(P, F \cap G) = +\infty$ *u suprotnom.*

(2) $I(P, F \cap G) = 0$ *ako i samo ako* $P \notin F \cap G$. $I(P, F \cap G)$ *ovisi samo o komponentama krivulja F i G koje sadrže P.*

(3) $I(P, F \cap G) = I\left(Q, F^T \cap G^T\right)$, *gdje je je T afina zamjena koordinata na* $\mathbb{A}^2$ *takva da je* $T(Q) = P$.

(4) $I(P, F \cap G) = I(P, G \cap F)$.

(5) $I(P, F \cap G) = I(P, F \cap (G + AF))$, *za svaki* $A \in K[X, Y]$.

(6) $I(P, F \cap G) = \sum_{k=1}^{n_F} \sum_{l=1}^{n_G} r_k s_l I(P, F_k \cap G_l)$, *gdje su* $n_F, n_G \in \mathbb{N}$, F_k *i* G_l *krivulje te* r_k *i* s_l *prirodni brojevi, za sve* $k \in \{1, 2, \ldots, n_F\}$ *i sve* $l \in \{1, 2, \ldots, n_G\}$, *takvi da je* $F = \prod_{k=1}^{n_F} F_k^{r_k}$ *i* $G = \prod_{l=1}^{n_G} G_l^{s_l}$.

(7) $I(P, F \cap G) \geq m_P(F)\, m_P(G)$, *uz znak jednakosti ako i samo ako krivulje F i G nemaju zajedničkih tangenti u točki P.*

(8) $I(P, F \cap G) = \mathrm{ord}_P^F(G)$, *ako je P regularna točka krivulje F.*

(9) $\sum_{P \in \mathbb{A}^2} I(P, F \cap G) = \dim_K(K[X, Y] / (F, G))$, *ako krivulje F i G nemaju zajedničkih komponenti.*

Napomena 2.5.3. *Kao što ćemo vidjeti u teoremu 2.5.5, prethodna definicija je dobra, tj. $I(P, F \cap G)$ postoji za sve krivulje F i G i sve točke $P \in \mathbb{A}^2$ i jedinstven je za fiksne krivulje F, G i točku P. Štoviše, vidjeti ćemo i da je $I(P, F \cap G) = \dim_K \left(\mathcal{O}_P\left(\mathbb{A}^2\right)/(F, G)\right)$, gdje je (F, G) ideal u $\mathcal{O}_P\left(\mathbb{A}^2\right)$ generiran s F i G i to će proizlaziti samo iz svojstava (1)-(7). Dokažimo svojstva (8) i (9) uz tu informaciju. Svojstvo (9) je direktna posljedica propozicije 1.6.7 i korolara 2.3.24. Da bismo dokazali svojstvo (8) možemo pretpostaviti da je F ireducibilna krivulja, zato što je P njena regularna točka. Neka je g slika polinoma G u $\mathcal{O}_P(F)$, tada prema (b) dijelu leme 2.3.31 dobivamo da je $\operatorname{ord}_P^F(G) = \dim_K(\mathcal{O}_P(F)/(g))$. Prema lemi 2.3.20 je $\mathcal{O}_P(F)/(g) \cong \mathcal{O}_P\left(\mathbb{A}^2\right)/(F, G)$, a dimenzija tog vektorskog prostora nad poljem K je upravo $I(P, F \cap G)$. Napomenimo još, svojstvo (5) nam govori da ako je F ireducibilna krivulja, da $I(P, F \cap G)$ ovisi samo o slici polinoma G u $\Gamma(F)$. Svojstvo (6) kaže (što je dosta intuitivno) da se multipliciteti presjeka zbrajaju kada gledamo unije krivulja (umnožak polinoma je geometrijski interpretiran kao unija točaka na njima). (7) svojstvo nam kaže da će $I(P, F \cap G)$ biti jednak 1 ako i samo ako se krivulje F i G sijeku transverzalno u točki P.*

Lema 2.5.4. *Neka su F i G krivulje i $P = (0, 0) \in \mathbb{A}^2$. Neka je $m = m_P(F)$, $n = m_P(G)$ te $\mathcal{O} = \mathcal{O}_P\left(\mathbb{A}^2\right)$. Neka je $I = (X, Y) \subseteq K[X, Y]$.*

(a) Ako F i G nemaju zajedničkih tangenti točkom P, onda je $I^k \subseteq (F, G)\mathcal{O}$, za svaki $k \in \mathbb{N}$, $k \geq m + n - 1$.

(b) Preslikvanje $\varphi : (K[X, Y]/I^m) \times (K[X, Y]/I^n) \to K[X, Y]/I^{m+n}$, koje je dano s

$$\varphi\left(\overline{A}, \overline{B}\right) = \overline{AG + BF},$$

gdje je $\overline{A}$ slika polinoma $A \in K[X, Y]$ u odgovarajućem prostoru, je injekcija ako i samo ako krivulje F i G imaju različite tangente u točki P.

Dokaz.

(a) Neka su $L_1, L_2, \ldots, L_m$ i $M_1, M_2, \ldots, M_n$ tangente na krivulje F i G, redom, u točki P. Za svaki prirodni broj $r > m$ neka je $L_r = L_m$ i za svaki prirodni broj $s > n$ neka je $M_s = M_n$. Neka je skup $\{A_{rs} : r, s \in \mathbb{Z}_{\geq 0}\}$ definiran kao u (c) dijelu propozicije 2.3.8. Tj. skup $\{A_{rs} : r, s \in \mathbb{Z}_{\geq 0},\ r + s = k\}$ je tada baza za vektorski prostor svih homogenih polinoma stupnja k u $K[X, Y]$. Dakle, dovoljno je pokazati da je $A_{rs} \in (F, G)\mathcal{O}$, za sve $r, s \in \mathbb{Z}_{\geq 0}$ takve da je $r + s \geq m + n - 1$. No, to znači da je ili $r \geq m$ ili $s \geq n$. Neka je, bez smanjenja općenitosti, $r \geq m$. To znači da možemo pisati $A_{rs} = A_{m0}B$, gdje je B homogeni polinom stupnja $r + s - m$, također, znamo da je $F = A_{m0} + F_{\geq m+1}$, gdje je $F_{\geq m+1}$ polinom kojemu su svi monomi stupnja $\geq m + 1$. Sada je $A_{rs} = BF - BF_{\geq m+1}$, gdje je $BF_{\geq m+1}$ polinom kojemu svi monomi imaju stupanj $\geq r + s + 1$. Sada, ako pokažemo da postoji dovoljno velik $N \in \mathbb{N}$ takav da je $I^N \subseteq (F, G)\mathcal{O}$, onda vidimo da je i $A_{rs} \in (F, G)\mathcal{O}$, za sve $r, s \in \mathbb{Z}_{\geq 0}$ takve da je $r + s = N$. No, iz prethodne diskusije onda vidimo da ako je $N > m + n - 1$ da je onda i $A_{rs} \in (F, G)\mathcal{O}$, za sve $r, s \in \mathbb{Z}_{\geq 0}$ takve da je $r + s = N - 1$. Nastavljajući ovaj "spuštajući" postupak dalje dobivamo što želimo. Dakle, dovoljno je pokazati da postoji dovoljno velik $N \in \mathbb{N}$ takav da je $I^N \subseteq (F, G)\mathcal{O}$. Kako F i G nemaju zajedničkih tangenti u P, onda nemaju niti zajedničkih komponenti pa je prema propoziciji 1.6.7 $V(F, G)$ konačan skup točaka koji sadrži točku P. Prema lemi 1.5.3 znamo da postoji polinom $H \in K[X, Y]$ takav da je $H(Q) = 0$ za svaku točku $Q \neq P$ iz $V(F, G)$ i da je $H(P) = 1$. Sada je jasno da su polinomi HY i HX u idealu $I(V(F, G))$. Stoga, prema Nullstellensatzu (1.5.22) postoji $N \in \mathbb{N}$ takav da su $(HX)^N, (HY)^N \in (F, G) \subseteq K[X, Y]$. Kako je $H^N(P) = 1 \neq 0$, vidimo da je H^N invertibilan element u $\mathcal{O}$, iz čega konačno zaključujemo da su X^N i Y^N u $(F, G)\mathcal{O}$. Odnosno, $I^{2N} \subseteq (F, G)\mathcal{O}$.

(b) Pretpostavimo da je L zajednička tangenta krivulja F i G u točki P. Neka su F_m i G_n odgovarajući homogeni polinomi iz definicije 2.4.5. Tada postoje polinomi F_{m-1}

i G_{n-1} (oba različita od nul–polinoma) takvi da je $F_m = LF_{m-1}$ i $G_n = LG_{n-1}$. No, jasno je da je sada $\varphi\left(\overline{F_{m-1}},\, \overline{-G_{n-1}}\right) = 0$, tj. φ nije injekcija. Pretpostavimo sada da su tangente razlčite. Neka su $A,\, B \in K[X,\, Y]$ takvi da je $\varphi\left(\overline{A},\, \overline{B}\right) = \overline{AG + BF} = 0$. To znači da su svi monomi polinoma $AG + BF$ stupnja barem $m + n$. Neka su $A = A_r + \ldots$ i $B = B_s + \ldots$ zapisi polinoma A i B kao sume homogenih polinoma, pri čemu su A_r i B_s oni s najmanjim stupnjevima (Točno r i s.) u tim zapisima, F_m i G_n neka su kao i ranije. Tada je $AG + BF = A_rG_n + B_sF_m +$ (monomi višeg stupnja). Pretpostavimo li da je $r < m$ ili $s < n$ vidimo da mora biti $r + n = s + m$ te također $A_rG_n = -B_sF_m$. No, F_m i G_n nemaju zajedničkih faktora zato $F_m \mid A_r$ i $G_n \mid B_s$, što je kontradikcija s pretpostavkom $r < m$ ili $s < n$, dakle $r \geq m$ i $s \geq n$. Odnosno, konačno, $\left(\overline{A},\, \overline{B}\right) = (0,\, 0)$, tj. φ je injekcija. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Teorem 2.5.5. *Neka su F i G krivulje i neka je $P \in \mathbb{A}^2$. Postoji jedinstven multiplicitet presjeka $I(P,\, F \cap G)$ koji zadovoljava uvjete (1)-(7) definicije 2.5.2 i dan je formulom*

$$I(P,\, F \cap G) = \dim_K \left(O_P\left(\mathbb{A}^2\right)/\,(F,\, G)\right).$$

Dokaz. Provodimo ga u dva koraka, najprije pokazujemo jedinstvenost, a zatim i egzistenciju traženog broja. U dokazu jedinstvenosti ćemo zapravo provesti algoritam kojim ćemo izračunati $I(P,\, F \cap G)$ koristeći samo svojstva (1)-(7). To je i jači rezultat od same jedinstvenosti, zato jer ćemo dobiti efektivan način pronalaska broja $I(P,\, F \cap G)$.

Jedinstvenost. Prema svojstvu (3) možemo pretpostaviti da je $P = (0,\, 0)$, (1) nam govori da možemo uzeti da je $I(P,\, F \cap G) \in \mathbb{Z}_{\geq 0}$, dok primjenom svojstva (2) imamo jedinstvenost za $I(P,\, F \cap G) = 0$. Dalje nastavljamo indukcijom, pretpostavimo da je $n \in \mathbb{N}$ i $I(P,\, F \cap G) = n$ te da je $I(P,\, F \cap G)$ jedinstveno određen kada god je $I(P,\, F \cap G) < n$. Promotrimo polinome $F(X,\, 0)$ i $G(X,\, 0)$ te neka su $r,\, s \in \mathbb{Z}_{\geq 0}$ stupnjevi tih polinoma, redom, ako su oni različiti od nul–polinoma. Ako je neki od njih jednak nul–polinomu, u ovom slučaju ćemo dogovorno uzeti da mu je stupanj jednak 0. Svojstvo (4) nam govori da

bez smanjenja općenitosti možemo pretpostaviti da je $r \leq s$. Slijede dva koraka algoritma koja nas vode kraju.

(i) $r = 0$. To znači da $Y \mid F$ pa je $F = YH$ za neki polinom $H \in K[X, Y]$ pa nam onda (6) daje $I(P, F \cap G) = I(P, Y \cap G) + I(P, H \cap G)$. Znamo da je $P \in F \cap G$ pa je posebno $P \in G$, što znači da $X \mid G(X, 0)$ pa je $G(X, 0) = X^m L$, za neki $m \in \mathbb{N}$ i polinom $L \in K[X]$ takav da $X \nmid L$ (niže je objašnjeno zašto je $G(X, 0) \neq 0$). Prema svojstvu (5) znamo da je

$$I(P, Y \cap G) = I(P, Y \cap [G - (\text{dio od } G \text{ koji je djeljiv s } Y)]),$$

tj. vrijedi $I(P, Y \cap G) = I(P, Y \cap G(X, 0))$ (tu vidimo da je $G(X, 0) \neq 0$, inače bi bilo $I(P, F \cap G) = +\infty$). Prema (2) vidimo da je $I(P, Y \cap L) = 0$, jer $P \notin L$, dok prema (6) onda slijedi $I(P, Y \cap G) = I(P, Y \cap X^m) = mI(P, Y \cap X)$, a (7) nam daje $I(P, Y \cap X) = 1$, dakle, $I(P, Y \cap G) = m > 0$. To sada znači da je $I(P, H \cap G) < n$ pa je on prema induktivnoj pretpostavci jedinstveno određen i time smo gotovi.

(ii) $r > 0$. Možemo pretpostaviti da su polinomi $F(X, 0)$ i $G(X, 0)$ normirani (množimo ih konstantom ako je potrebno). Neka je $H = G - X^{s-r}F$, prema (5) vidimo da je $I(P, F \cap G) = I(P, F \cap H)$, dok je $t = \deg(H(X, 0)) < s = \deg(G(X, 0))$, pri čemu u slučaju da je $H(X, 0) = 0$ uzimamo, opet dogovorno, da je $t = 0$. Sada, ako je $r < t$ stavljamo $F = F$ i $G = H$, a ako je $t < r$ stavljamo $F = H$ i $G = F$, što smijemo prema svojstvu (4). Ponavljamo postupak, kako u svakom koraku smanjimo broj t (točnije, smanjimo ili broj r ili broj s), u nekom trenutku ćemo dobiti da je $t = 0$ i onda završavamo u koraku (i).

Egzistencija. Dokazujemo da broj $I(P, F \cap G) = \dim_K \left(\mathcal{O}_P\left(\mathbb{A}^2\right)/(F, G)\right)$ zadovoljava svojstva (1)-(7). Kako je $(F, G) = (G, F)$ odmah imamo (4), također, za svaki $A \in K[X, Y]$ je $(F, G) = (F, G + AF)$ pa imamo i (5). Ako $P \notin F \cap G$, onda je $F(P) \neq 0$ ili $G(P) \neq 0$ pa

je F ili G invertibilan element u $\mathcal{O}_P\left(\mathbb{A}^2\right)$, tj. $(F,\, G) = \mathcal{O}_P\left(\mathbb{A}^2\right)$ pa je $I\,(P,\, F \cap G) = 0$. Ako je $P \in F \cap G$ onda je $(F,\, G) \neq \mathcal{O}_P\left(\mathbb{A}^2\right)$ pa je $I\,(P,\, F \cap G) > 0$. One komponente od F i G koje ne sadrže P su invertibilni elementi u $\mathcal{O}_P\left(\mathbb{A}^2\right)$ pa one ne utječu na $(F,\, G)$. Iz svega ovoga imamo i svojstvo (2). Propozicija 2.2.10 nam govori da afina zamjena koordinata daje izomorfizam među lokalnim prstenima, stoga imamo i svojstvo (3). Iz do sada pokazanih svojstava vidimo da dalje možemo pretpostaviti da je $P = (0,\, 0)$ i da sve komponente od F i G sadrže točku P. Označimo $\mathcal{O} = \mathcal{O}_P\left(\mathbb{A}^2\right)$. Sada ćemo u tri koraka dokazati, redom, svojstva (1), (6) i (7).

Svojstvo (1). Ukoliko F i G nemaju zajedničkih komponenti, onda je $I\,(P,\, F \cap G)$ konačno prema propoziciji 1.6.7 i korolaru 2.3.24. Pretpostavimo da F i G imaju zajedničku komponentu H. Tada je $(F,\, G) \subseteq (H)$ pa postoji prirodni epimorfizam (lema 2.3.18, dio (a)) $\mathcal{O}/\,(F,\, G) \to \mathcal{O}/\,(H)$, zato je $I\,(P,\, F \cap G) \geq \dim_K\left(\mathcal{O}/\,(H)\right)$. Prema lemi 2.3.20 znamo da je $\mathcal{O}/\,(H) \cong \mathcal{O}_P(H)$. $\mathcal{O}_P(H) \supseteq \Gamma\,(H)$, a prema korolaru 1.5.24, pošto je $V\,(H)$ beskonačan skup točaka ($H \in K\,[X,\, Y]$ nekonstantan i K algebarski zatvoreno), je $\Gamma\,(H)$ beskonačno dimenzionalan vektorski prostor nad K. Zato je $I\,(P,\, F \cap G) = +\infty$.

Svojstvo (6). Dovoljno je pokazati da je $I\,(P,\, F \cap GH) = I\,(P,\, F \cap G) + I\,(P,\, F \cap H)$, za sve krivulje F, G i H. Tvrdnja je trivijalna ukoliko F i GH imaju zajedničku komponentu (radi svojstva (1)), stoga možemo pretpostaviti da nemaju. Kako je $(F,\, GH) \subseteq (F,\, G)$, postoji prirodni epimorfizam (lema 2.3.18, dio (a)) $\psi : \mathcal{O}/\,(F,\, GH) \to \mathcal{O}/\,(F,\, G)$. Nadalje, neka je $\varphi : \mathcal{O}/\,(F,\, H) \to \mathcal{O}/\,(F,\, GH)$ definirana kao $\varphi\,(\overline{z}) = \overline{Gz}$, za svaki $z \in \mathcal{O}$, ovdje $\overline{z}$ označava sliku funkcije z u odgovarajućem prostoru. (a) dio propozicije 2.3.29 nam govori da je sada dovoljno pokazati da je niz

$$0 \to \mathcal{O}/\,(F,\, H) \xrightarrow{\varphi} \mathcal{O}/\,(F,\, GH) \xrightarrow{\psi} \mathcal{O}/\,(F,\, G) \to 0$$

egzaktan. Već znamo da je ψ surjekcija. Neka je $a \in \mathcal{O}$ takva da je $\psi\,(\overline{a}) = 0$, to znači da je $a \in (F,\, G)$, što znači da postoje $b,\, c \in \mathcal{O}$ takve da je $a = bF + cG$. No, to znači da je $\overline{a} = \overline{cG}$ u $\mathcal{O}/\,(F,\, GH)$, tj. $\overline{a} \in \mathrm{Im}\,(\varphi)$. Očito je da je za svaki $\overline{a} \in \mathrm{Im}\,(\varphi)$, $\psi\,(\overline{a}) = 0$, dakle

$\mathrm{Im}(\varphi) = \mathrm{Ker}(\psi)$. Preostaje dokazati da je φ injekcija i gotovi smo. Neka je $z \in \mathcal{O}$ takva da je $\varphi(\overline{z}) = 0$, to znači da postoje $a,\ b \in \mathcal{O}$ takve da je $Gz = aF + bGH$. Postoji $S \in K[X,\ Y]$ takav da je $S\ (P) \neq 0$ i $Sz = Z$, $Sa = A$ i $Sb = B$, gdje su $A,\ B,\ Z \in K[X,\ Y]$. Dolazimo do jednakosti u $K[X,\ Y]$, $GZ = AF + BGH$. To je ekvivalentno s $G(Z - BH) = AF$, kako F i GH nemaju zajedničkih komponenti zaključujemo da $F \mid Z - BH$ pa postoji $D \in K[X,\ Y]$ takav da je $Z - BH = DF$, odnosno $Z = BH + DF$. Podijelimo li zadnju jednakost sa S (u $\mathcal{O}$) dobivamo da je $z = bH + \left(\frac{D}{S}\right)F$, odnosno $\overline{z} = 0$ u $\mathcal{O}/(F,\ H)$. Dakle, φ je injekcija.

Svojstvo (7). Neka je $m = m_P(F)$, $n = m_P(G)$ te neka je $I = (X,\ Y) \subseteq K[X,\ Y]$. Promotrimo niz

$$(K[X,\ Y]/I^m) \times (K[X,\ Y]/I^n) \xrightarrow{\varphi} K[X,\ Y]/I^{m+n} \xrightarrow{\psi} K[X,\ Y]/(I^{m+n},\ F,\ G) \to 0,$$

gdje je φ kao u (b) dijelu leme 2.5.4, a ψ je prirodni epimorfizam, opet kao u dijelu (a) leme 2.3.18. $(I^{m+n},\ F,\ G)$ nam označava ideal u $K[X,\ Y]$ generiran skupom $I^{m+n} \cup \{F,\ G\}$. Znamo da je ψ surjekcija, želimo vidjeti da je ovaj niz egzaktan, za to je još dovoljno pokazati da je $\mathrm{Im}(\varphi) = \mathrm{Ker}(\psi)$. Neka je $C \in K[X,\ Y]$ takav da je (potez nam i dalje označava sliku u odgovarajućem prostoru) $\overline{C} = \varphi\left(\overline{A},\ \overline{B}\right)$ za neke $A,\ B \in K[X,\ Y]$, tj. $\overline{C} \in \mathrm{Im}(\varphi)$. No, to znači da je $\overline{C} = \overline{AG + BF}$ pa je jasno da je $\psi\left(\overline{C}\right) = 0$. Obratno, neka je $C \in K[X,\ Y]$ takav da je $\psi\left(\overline{C}\right) = 0$, tada je $C \in (I^{m+n},\ F,\ G)$, odnosno $C = AG + BF + D$, gdje su $A,\ B$ polinomi iz $K[X,\ Y]$ i $D \in I^{m+n}$. Odmah vidimo da je $\overline{C} = \overline{AG + BF}$ u $K[X,\ Y]/I^{m+n}$, odnosno, $\overline{C} \in \mathrm{Im}(\varphi)$. Dakle, $\mathrm{Im}(\varphi) = \mathrm{Ker}(\psi)$, tj. dani niz je egzaktan. Iz toga zaključujemo da je (sve dimenzije gledamo nad poljem K)

$$\dim(K[X,\ Y]/I^m) + \dim(K[X,\ Y]/I^n) \geq \dim(\mathrm{Ker}(\psi)),$$

gdje jednakost vrijedi ako i samo ako je φ injekcija. Također, vidimo da je

$$\dim(K[X,\ Y]/(I^{m+n},\ F,\ G)) = \dim(K[X,\ Y]/I^{m+n}) - \dim(\mathrm{Ker}(\psi)).$$

Kako je $V(I^{m+n},\ F,\ G) = \{P\}$ (Jedina točka na kojoj se poništavaju svi polinomi iz I^{m+n} je upravo $(0,\ 0) = P$.), prema korolaru 2.3.25 je $K[X,\ Y]/(I^{m+n},\ F,\ G) \cong \mathcal{O}/(I^{m+n},\ F,\ G)$.

Prema (a) dijelu leme 2.3.18 postoji prirodni epimorfizam $\mathcal{O}/(F, G) \to \mathcal{O}/(I^{m+n}, F, G)$. Radi svega ovoga dobivamo da je

$$\begin{aligned} I(P, F \cap G) &= \dim(\mathcal{O}/(F, G)) \geq \dim(\mathcal{O}/(I^{m+n}, F, G)) \\ &= \dim(K[X, Y]/(I^{m+n}, F, G)) \\ &\geq \dim(K[X, Y]/I^{m+n}) - \dim(K[X, Y]/I^m) - \dim(K[X, Y]/I^n) \\ &= mn. \end{aligned}$$

Zadnja jednakost slijedi, uz račun, iz leme 2.3.22. Dakle, imamo da je $I(P, F \cap G) \geq mn$ i da jednakost vrijedi ako i samo ako su ispunjene obje nejednakosti u gornjem računu. Prva od njih je ispunjena ako je $\mathcal{O}/(F, G) \cong \mathcal{O}/(I^{m+n}, F, G)$, što će biti ako je $I^{m+n} \subseteq (F, G)\mathcal{O}$. Druga nejednakost će biti jednakost ako i samo ako je φ injekcija. Sada vidimo da svojstvo (7) konačno slijedi direktno iz leme 2.5.4. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Primjer 2.5.6. Neka je F krivulja i $P \in \mathbb{A}^2$ točka na njoj. Pravac L točkom P je tada tangenta na krivulju F ako i samo ako je $I(P, F \cap L) > m_P(F)$. Ova tvrdnja slijedi direktno iz svojstva (7) multipliciteta presjeka (definicija 2.5.2). Naime,

$$I(P, F \cap L) \geq m_P(F)\, m_P(L),$$

L je pravac točkom P pa je jasno da je $m_P(L) = 1$. Nadalje, jednakost vrijedi ako i samo ako F i L nemaju zajedničkih tangenata točkom P, ali L će biti tangenta na krivulju F u točki P ako i samo ako F i L imaju zajedničkih tangenata točkom P, upravo pravac L. To je zato što je tangenta na L u točki P jednaka upravo L. Dakle, L je tangenta na F u točki P ako i samo ako ne vrijedi jednakost, tj. ako i samo ako je $I(P, F \cap L) > m_P(F)$.

2.6 Algoritam za računanje multipliciteta presjeka

Sada ćemo "izolirati" algoritam opisan u dokazu jedinstvenosti multipliciteta presjeka u teoremu 2.5.5. Točnije, eksplicitno ćemo navesti korake tog algoritma koji će bit iznimno

operativan za računanje multipliciteta presjeka u bilo kojoj točki $P \in \mathbb{A}^2$ bilo kojih dviju krivulja F i G. Spomenuta operativnost algoritma će se odražavati u tom smislu da će nam za izračunavanje multipliciteta presjeka biti dovoljne tek elementarne aritmetičke operacije s polinomima. Opišimo najprije algoritam, zatim ćemo ukratko komentirati njegovu korektnost, a i dati nekoliko primjera u kojima ćemo ga primijeniti. Također, imajmo na umu da nam algoritam nije jedino oruđe, uvijek smijemo (a i poželjno je) koristiti se svojstvima multipliciteta presjeka. Napomenimo da ćemo u algoritmu nul–polinom smatrati polinomom stupnja 0. Koristiti ćemo pomoćne polinome H (high) i L (low). H ćemo uvijek održavati tako da ima veću potenciju od L, u smislu koji će biti jasan iz algoritma.

Neka su $F, G \in K[X, Y]$ krivulje (tj. polinomi, neki predstavnici odgovarajuće klase ekvivalencije) i neka je $P = (a, b) \in \mathbb{A}^2$. Slijedi algoritam za računanje $I(P, F \cap G)$:

Korak 0

- $I(P, F \cap G) = 0$.
- Neka je $H \in K[X, Y]$ takav da je $H(X, Y) = F(X + a, Y + b)$.
- Neka je $L \in K[X, Y]$ takav da je $L(X, Y) = G(X + a, Y + b)$.
- U svakom koraku algoritma, neka su $h, l \in \mathbb{Z}_{\geq 0}$ takvi da je $h = \deg(H(X, 0))$ te $l = \deg(L(X, 0))$. Prisjetimo se da tokom algoritma nul–polinom smatramo polinomom stupnja 0, kao i svaki drugi konstantni polinom.
- Ako je $h < l$, zamijeni H i L.
- Idi na ***Korak*** 1.

Korak 1

- Ako je $H(0, 0) \neq 0$ ili $L(0, 0) \neq 0$, **KRAJ**.
- Ako je $l > 0$ idi na ***Korak*** 2.
- Ako je $H(X, 0) = 0$ (u $K[X]$) ili $L = 0$, $I(P, F \cap G) = +\infty$, **KRAJ**.
- Povećaj $I(P, F \cap G)$ za mn, gdje su $m, n \in \mathbb{N}$ takvi da

$$X^m \mid H(X, 0),\ X^{m+1} \nmid H(X, 0) \quad \text{i} \quad Y^n \mid L,\ Y^{n+1} \nmid L.$$

- Neka je $L_0 \in K[X, Y]$ takav da je $L = Y^n L_0$, stavi $L = L_0$.
- Ako je $h < l$, zamijeni H i L.
- Idi na ***Korak*** 2.

Korak 2

- Pomnoži H i L odgovarajućim konstantama tako da su polinomi $H(X, 0)$ i $L(X, 0)$ normirani.
- Neka je $H_0 \in K[X, Y]$ takav da je $H_0 = H - X^{h-l}L$, stavi $H = H_0$.
- Ako je $h < l$, zamijeni H i L.
- Idi na ***Korak*** 1.

Zašto je dani algoritam korektan? Najprije, ***Korak*** 0 je jasan, u njemu koristimo svojstva multipliciteta presjeka (3) i (4) (definicija 2.5.2), da bismo vidjeli kako je

$$I(P, F \cap G) = I((0, 0), H \cap L) = I((0, 0), L \cap H).$$

Nadaje, algoritam će se "zaustaviti" u konačnom vremenu zato jer u svakom prolasku spustimo stupanj ili u varijabli X ili u varijabli Y barem jednog od polinoma, jasno je da to ne možemo ponavljati u nedogled. Algoritam je očito korektan (Što se vidi direktno iz dokaza jedinstvenosti u teoremu 2.5.5.) ako krivulje F i G nemaju zajedničkih komponenti koje sadrže točku P. Zanima nas hoće li algoritam "detektirati" da imaju takvu zajedničku komponentu ukoliko ju imaju? Odgovor je, jasno, da hoće. Naime, svi koraci algoritma su "legalni", tj. ispravni su nevezano za to imaju li ili ne krivulje F i G zajedničkih komponenti koje sadrže točku P. Promotrimo ***Korak*** 1, ukoliko je u svakom pristupu njemu $H(X, 0) \neq 0$ i $L \neq 0$ vidimo da će $I(P, F \cap G)$ nužno biti konačan broj. Dakle, ukoliko F i G imaju zajedničku komponentu koja sadrži točku P, algoritam će to prepoznati.

Imajmo na umu da u bilo kojem trenutku u algoritmu možemo primijeniti bilo koje od svojstava multipliciteta presjeka (definicija 2.5.2). "Pametna" kombinacija algoritma

sa svojstvima nam dodatno olakšava posao, kao što ćemo vidjeti u nekoliko sljedećih primjera. Također, ponekad je zgodno zamijeniti "ulogu varijable" X i varijable Y u algoritmu, tj. poništavati potencije varijable Y, umjesto varijable X.

Primjer 2.6.1. Neka su $F, G \in K[X, Y]$ definirani kao

$$F(X, Y) = \left[\left((X-1)^2 + (Y+1)^2\right)^2 + 3(X-1)^2(Y+1) - (Y+1)^3\right]\left(X^2 + 2Y^2\right),$$

$$G(X, Y) = \left[\left((X-1)^2 + (Y+1)^2\right)^3 - 4(X-1)^2(Y+1)^2\right]\left(X - i\sqrt{2}Y\right).$$

Odredimo multiplicitet presjeka tih dviju krivulja u točki $P \in \mathbb{A}^2$.

(a) $P = (0, -2)$. Vidimo da je $F(0, -2) = 16 \neq 0$. Dakle, $I((1, -1), F \cap G) = 0$.

(b) $P = \left(i, \dfrac{\sqrt{2}}{2}\right)$. Vidimo da je $i - i\sqrt{2} \cdot \dfrac{\sqrt{2}}{2} = 0$ i da $X - i\sqrt{2}Y \mid F$ i $X - i\sqrt{2}Y \mid G$. Zaključujemo da je $I\left(\left(i, \dfrac{\sqrt{2}}{2}\right), F \cap G\right) = +\infty$.

(c) $P = (1, -1)$. Kako je $1^2 + 2 \cdot (-1)^2 = 3 \neq 0$ i $1 - i\sqrt{2} \cdot (-1) \neq 0$, prema svojstvu (2) (ili primjenom svojstva (6)) multipliciteta presjeka (definicija 2.5.2) zaključujemo da možemo zanemariti faktor $X^2 + 2Y^2$ u F te faktor $X - i\sqrt{2}Y$ u G. Provedimo ***Korak*** 0 algoritma, dobivamo:

$$H(X, Y) = \left(X^2 + Y^2\right)^3 - 4X^2Y^2 \quad \text{i} \quad L(X, Y) = \left(X^2 + Y^2\right)^2 + 3X^2Y - Y^3.$$

Svojstvo (5) nam govori da možemo polinom H zamijeniti (što je super, riješimo se "najružnijeg" člana) polinomom $H - \left(X^2 + Y^2\right)L$, tj. L nam "ostaje isti", dok je "novi" $H(X, Y) = Y\left(Y^4 - 2X^2Y^2 - 4X^2Y - 3X^4\right)$, zamijenimo L i H te skočimo na ***Korak*** 1. Ovdje nam $I(P, F \cap G)$ postaje 4 te su nam "novi" H i L jednaki

$$H(X, Y) = \left(X^2 + Y^2\right)\left(Y^2 - 3X^2\right) - 4X^2Y, \quad L(X, Y) = \left(X^2 + Y^2\right)^2 + 3X^2Y - Y^3.$$

Opet, zamijenimo H s $H + 3L$ pa nam L ostaje isti, a novi H je

$$H(X, Y) = Y\left(4Y^3 + 4X^2Y + 5X^2 - 3Y^2\right).$$

Vidimo da sada $I(P, F \cap G)$ postaje 8 te mu moramo još dodati $I((0, 0), H \cap L)$, gdje je $H(X, Y) = \left(X^2 + Y^2\right)^2 + 3X^2Y - Y^3$, $\quad L(X, Y) = 4Y^3 + 4X^2Y + 5X^2 - 3Y^2$. Označimo $Q = (0, 0)$. Primijetimo da su tangente točkom Q na krivulju H linearni faktori polinoma $3X^2Y - Y^3$, dok su tangente točkom Q na krivulju L linearni faktori polinoma $5X^2 - 3Y^2$. Lako se vidi da ta dva polinoma nemaju zajedničkih linearnih faktora. Svojstvo (7) multipliciteta presjeka (definicija 2.5.2) nam sada govori da je $I(Q, H \cap L) = m_Q(H)\, m_Q(L) = 3 \cdot 2 = 6$. Konačno, zaključujemo da je

$$I((1, -1), F \cap G) = 14.$$

Sada ćemo dati primjer u kojem ćemo opisati direktniji pristup za posebne oblike krivulja (točnije, polinoma koje ih određuju).

Primjer 2.6.2. Odredimo $I(P, F \cap G)$, gdje je $P = (a, b) \in \mathbb{A}^2$ i $F, G \in K[X, Y]$ takvi da postoje polinomi $f_1, g_1 \in K[X]$ i $f_2, g_2 \in K[Y]$ takvi da je

$$F(X, Y) = f_1(X) + f_2(Y) \quad \text{te} \quad G(X, Y) = g_1(X) + g_2(Y).$$

Primijetimo da ako umjesto polinoma F i G promatramo polinome $F(X + a, Y + b)$ i $G(X + a, Y + b)$ da će oni biti istog oblika. Točnije, isto će biti jednaki sumi dva polinoma, jednog u varijabli X, drugog u varijabli Y. Stoga, bez smanjenja općenitosti možemo pretpostaviti da je $P = (0, 0)$. Nadalje, konstantni član iz polinoma f_2 i g_2 možemo prebaciti u polinom f_1, odnosno g_1. Dakle, vidimo da možemo pretpostaviti da je $f_2(0) = 0$ i $g_2(0) = 0$. Sada provodimo redukcije iz algoritma, napomenimo još jednom, ako je to zgodnije, možemo zamijeniti ulogu varijabli X i Y. Točnije, provoditi ***Korak*** 2 tako da smanjujemo potencije od Y, umjesto onih od X. Jasno, tada gledamo $\deg(H(0, Y))$ i

$\deg(L(0, Y))$. Uvijek ćemo nakon nekoliko koraka doći u neku od sljedećih situacija za koju direktno možemo reći koliko je $I(P, F \cap G)$. Navedimo te situacije.

(1) $f_1(0) \neq 0$ ili $g_1(0) \neq 0$. Tada je $I(P, F \cap G) = 0$.

(2) $f_1 = g_1 = 0$ ili $f_2 = g_2 = 0$ ili $F = 0$ ili $G = 0$. Tada je $I(P, F \cap G) = +\infty$.

(3) $f_1 = 0$, $f_2 \neq 0$ i $g_1 \neq 0$. Tada je $I(P, F \cap G) = mn$, gdje su $m, n \in \mathbb{Z}_{\geq 0}$ takvi da $X^m \mid g_1$ i $X^{m+1} \nmid g_1$ te $Y^n \mid f_2$ i $Y^{n+1} \nmid f_2$.

(4) $f_1 \neq 0$, $f_2 = 0$ i $g_2 \neq 0$. Tada je $I(P, F \cap G) = mn$, gdje su $m, n \in \mathbb{Z}_{\geq 0}$ takvi da $Y^m \mid g_2$ i $Y^{m+1} \nmid g_2$ te $X^n \mid f_1$ i $X^{n+1} \nmid f_2$. Ovo je primjer u kojemu smo zamijenili uloge varijablama X i Y u provođenju algoritma.

(5) $f_2(Y) = g_2(Y) = Y$. Točnije, $F(X, Y) = f(X) + Y$ i $G(X, Y) = g(X) + Y$, za neke $f, g \in K[X]$. Tada je $I(P, F \cap G) = 0$ ako je $f(0) \neq 0$ ili $g(0) \neq 0$. Inače, ako je $g - f = 0$, onda je $I(P, F \cap G) = +\infty$ te, ako je $g - f \neq 0$, onda je $I(P, F \cap G) = n$, gdje je $n \in \mathbb{N}$ takav da $X^n \mid g - f$ i $X^{n+1} \nmid g - f$. Zašto? Jednostavno promatramo polinome F i $G - F$ (svojstvo (5) iz definicije 2.5.2) i rezultat odmah slijedi iz algoritma, ali sa zamijenjenim ulogama varijabli X i Y.

(6) $f_1(X) = X$ i $g_2(Y) = Y$. Točnije, $F(X, Y) = X + f(Y)$ i $G(X, Y) = g(X) + Y$, za neke $f \in K[Y]$ i $g \in K[X]$. Neka je $f_0 \in K[Y]$ takav da je $f_0 = -f$. Znamo da

$$F = X + f(Y) = X - f_0(Y) \mid g(X) - g(f_0(Y)) = g(X) - g(-f(Y)).$$

Odnosno, postoji polinom $H \in K[X, Y]$ takav da je $HF = g(X) - g(-f(Y))$. Sada, umjesto polinoma G možemo promatrati polinom $G - HF = Y + g(-f(Y))$. Dakle, vidimo da je $I(P, F \cap G) = +\infty$, ako je $Y + g(-f(Y)) = 0$, inače, ako je $n \in \mathbb{Z}_{\geq 0}$ takav da $Y^n \mid Y + g(-f(Y))$ te $Y^{n+1} \nmid Y + g(-f(Y))$, onda je $I(P, F \cap G) = n$.

Napomena 2.6.3. *Posebno su nam važne točke (5) i (6) prethodnog primjera, zato jer iz njih vidimo kako vrlo lako možemo izračunati multiplicitet presjeka krivulje* $Y = f(X)$ *s krivuljama* $Y = g(X)$ *i* $X = h(Y)$*, gdje su* $f, g \in K[X]$ *i* $h \in K[Y]$*, u bilo kojoj točki* $P = (a, b) \in \mathbb{A}^2$*. Označimo te tri krivulje redom s* F, G *i* H*. Neka je npr.*

$$f = X^2 - X, \quad g = (X+1)^3 - 39(X+1)^2 - 3X - 1, \quad h = (Y-1)^2.$$

Neka je $P_1 = (1, 0)$ *i* $P_2 = (-1, 2)$*. Vidimo da* $P_1 \notin G$ *i* $P_2 \notin H$ *pa je* $I(P_1, F \cap G) = 0$*, kao i* $I(P_2, F \cap H) = 0$*. Računamo sada* $I(P_1, F \cap H)$*, to je isto što i* $I((0, 0), F_1 \cap H_1)$*, gdje su* F_1 *i* H_1 *krivulje dane, redom, s* $Y = X^2 + X$ *i* $X = Y^2$*. Dakle,* $I(P_1, F \cap H) = 1$*. Preostaje nam još izračunati* $I(P_2, F \cap G)$*, a to je isto što i* $I((0, 0), F_2 \cap G_2)$ *gdje su* F_2 *i* G_2 *redom dane s* $Y = X^2 - 3X$ *i* $Y = X^3 - 39X^2 - 3X$*. Dakle,* $I(P_2, F \cap G) = 2$*.*

Spomenuti algoritam ćemo sada još malo modificirati. Preciznije, u suštini će ostati isti, samo ćemo ga zapisati na način pogodniji za implementaciju, a zatim ćemo dati i konkretnu implementaciju u programskom jeziku C, uz nekoliko primjera. Za krivulje F i G s cjelobrojnim koeficijentima, računati ćemo njihov multiplicitet presjeka u točki $(0, 0)$. To je ograničenje koje uvodimo radi jednostavnije implementacije. Točnije, programu odmah šaljemo polinome H i L koje konstruiramo u algoritmu, ***Korak*** 0. Slijedi pseudokod:

- **ULAZ:** polinomi H i L
- **IZLAZ:** $ret = I((0, 0), H \cap L)$
- **INICIJALIZACIJA:** $ret = 0$, $h = \deg(H(X, 0))$, $l = \deg(L(X, 0))$
  //*u svakom koraku održavamo* $h = \deg(H(X, 0))$ *i* $l = \deg(L(X, 0))$
- **AKO:** $h < l$, **ONDA:** zamijeni H i L
- **RADI:**
  - **AKO:** $H(0, 0) \neq 0$ ili $L(0, 0) \neq 0$, **ONDA: KRAJ**

- **SVE DOK:** $l > 0$, **RADI:**
  - a = koeficijent uz monom X^h u polinomu H
  - b = koeficijent uz monom X^l u polinomu L
  - d = najveći zajednički djelitelj brojeva a i b
  - $H = \frac{1}{d}\left(bH - aX^{h-l}L\right)$
  - **AKO:** $h < l$, **ONDA:** zamijeni H i L
- **AKO:** $H(X, 0) = 0$ ili $L = 0$, **ONDA:** $ret = +\infty$, **KRAJ**
- nađi $n \in \mathbb{N}$ t.d. $Y^n \mid L$ i $Y^{n+1} \nmid L$
- povećaj ret za nm, gdje je $m \in \mathbb{N}$ t.d. $X^m \mid H(X, 0)$ i $X^{m+1} \nmid H(X, 0)$
- podijeli L s Y^n

Sada ćemo dati konkretnu implementaciju u programskom jeziku C. Dodatna ograničenja su da koeficijenti polinoma H i L moraju biti cjelobrojni i ne "preveliki", zato što će se međusobno množiti pa da bi rezultat mogao stati u tip podataka "int". Također, najveći eksponent na varijabli X u oba polinoma može biti 9, isto vrijedi i za varijablu Y. Ova ograničenja se lako mogu "oslabiti", ali onda raste složenost algoritma, a i njegova korektnost postaje upitna (ako koeficijenti mogu biti realni), radi grešaka u računalnoj aritmetici. Već i s ovim "jakim" ograničenjima ćemo od ovog algoritma dobiti mnoštvo konkretnih primjera, zato je za naše trenutne potrebe i više nego dostatan. Nakon samog koda programa ćemo opisati kako mu šaljemo podatke o polinomima te kako on nama vraća željeni rezultat. Zatim ćemo vidjeti nekoliko primjera.

```
1  #include <stdio.h>
2
3  #define MAX 10
4  //MAX - 1 je najveca moguca potencija
5  //na X, odnosno Y
6  #define oo 2123456789
7  //oo = +beskonacno
8
9  int H[MAX][MAX], L[MAX][MAX];
10 //H[i][j] je koeficijent uz X^iY^j
```

```
11 //u polinomu H, isto za L
12 int h, l;
13 //h i l su, redom, stupnjevi od
14 //H(X, 0) i L(X, 0)
15
16 int sadrze_0()
17 //provjera je li
18 //H(0, 0) = 0 i L(0, 0) = 0
19   {
20   if(H[0][0] != 0 || L[0][0] != 0)
21     return 0;
22   return 1;
23   }
24
25 int nula_H()
26 //provjera je li H(X, 0) = 0
27   {
28   int i;
29   for(i = 0; i < MAX; ++i)
30     if(H[i][0] != 0)
31       return 0;
32   return 1;
33   }
34
35 int nula_L()
36 //provjera je li L = 0
37   {
38   int i, j;
39   for(i = 0; i < MAX; ++i)
40     for(j = 0; j < MAX; ++j)
41       if(L[i][j] != 0)
42         return 0;
43   return 1;
44   }
45
46 int stupanj_u_X(int A[][MAX])
47 //vraca stupanj polinoma A(X, 0)
48   {
49   int i;
50   for(i = MAX - 1; i > 0; --i)
51     if(A[i][0] != 0)
52       return i;
53   return 0;
54   }
55
56 int pot_u_H()
57 //vraca najveci m iz N t.d.
58 //X^m | H(X, 0)
59   {
60   int i;
61   for(i = 1; i < MAX; ++i)
62     if(H[i][0] != 0)
63       return i;
64   }
65
66 int pot_u_L()
67 //vraca najveci n iz N t.d. Y^n | L
68   {
69   int i, j;
70   for(j = 1; j < MAX; ++j)
71     for(i = 0; i < MAX; ++i)
72       if(L[i][j] != 0)
73         return j;
74   }
75
76 void zamijeni()
77 //mijenja uloge polinomima H i L
78   {
79   int i, j, tmp;
80   tmp = h;
81   h = l;
82   l = tmp;
83   for(i = 0; i < MAX; ++i)
84     for(j = 0; j < MAX; ++j)
85       {
86       tmp = H[i][j];
```

```
87        H[i][j] = L[i][j];
88        L[i][j] = tmp;
89        }
90    }
91
92  void provjeri()
93  //provjerava treba li mijenjati H i L
94  //te ako treba, mijenja ih
95    {
96    h = stupanj_u_X(H);
97    l = stupanj_u_X(L);
98    if(h < l)
99      zamijeni();
100   }
101
102 void podijeli(int n)
103 //dijeli polinom L s Y^n
104 //te zatim izvrsi provjeru
105   {
106   int i, j;
107   for(j = 0; j < MAX - n; ++j)
108     for(i = 0; i < MAX; ++i)
109       L[i][j] = L[i][j + n];
110   for(j = MAX - n; j < MAX; ++j)
111     for(i = 0; i < MAX; ++i)
112       L[i][j] = 0;
113   provjeri();
114   }
115
116 int nzd(int a, int b)
117 //vraca najveci zajednicki djelitelj
118 //cijelih brojeva a i b
119   {
120   int tmp;
121   if(a < 0)
122     a *= (-1);
123   if(b < 0)
124     b *= (-1);
125   while(b != 0)
126     {
127     tmp = b;
128     b = a % tmp;
129     a = tmp;
130     }
131   return a;
132   }
133
134 void sredi()
135 //"uklanja" najvecu potenciju od X u
136 //polinomu H(X, 0) te izvrsi provjeru
137   {
138   int i, j, a, b, d;
139   d = nzd(H[h][0], L[l][0]);
140   a = H[h][0] / d;
141   b = L[l][0] / d;
142   d = h - l;
143   for(i = 0; i < d; ++i)
144     for(j = 0; j < MAX; ++j)
145       H[i][j] *= b;
146   for(i = d; i < MAX; ++i)
147     for(j = 0; j < MAX; ++j)
148       {
149       H[i][j] *= b;
150       H[i][j] -= (a*L[i - d][j]);
151       }
152   provjeri();
153   }
154
155 int main(void)
156 {
157 int m, n, i, j, ret = 0;
158 //ret je trazeni
159 //multiplicitet presjeka
160 scanf("%d %d", &m, &n);
161 //m - broj monoma u polinomu H,
162 //n - isto, ali u L
```

```
163 while(m--)
164 //unos monoma polinoma H
165   {
166   scanf("%d %d %d", &i, &j, &h);
167   H[i][j] = h;
168   }
169 while(n--)
170 //unos monoma polinoma L
171   {
172   scanf("%d %d %d", &i, &j, &l);
173   L[i][j] = l;
174   }
175 provjeri();
176 //inicijalna provjera
177 while(1)
178   {
179   if(!sadrze_0())
180   //algoritam staje ako
181   //H(0, 0) ili L(0, 0) nije 0
182     break;
183   while(l > 0)
184   //provodi se korak 2
185   //sve dok je potrebno
186     sredi();
187   if(nula_H() || nula_L())
188   //ako H i L imaju zajednicku
189   //komponentu, onda je
190   //ret = oo i gotovi smo
191     {
192     ret = oo;
193     break;
194     }
195   n = pot_u_L();
196   //najveci n iz N t.d. Y^n | L
197   ret += (n * pot_u_H());
198   //povecamo ret za nm, uz m iz N
199   //najveci t.d. X^m | H(X, 0)
200   podijeli(n);
201   //dijelimo polinom L s Y^n
202   }
203 if(ret == oo)
204   printf("+oo\n");
205 else
206   printf("%d\n", ret);
207 return 0;
208 }
```

Opišimo sada kako dani program prima, odnosno vraća podatke. Ulazni podaci se zadaju pomoću standardnog ulaza (stdin, tj. preko tipkovnice), izlaz će biti na standardnom izlazu (stdout, tj. preko ekrana).

- *Format **ulaznih** podataka:* U prvom retku se nalaze dva nenegativna cijela broja, m i n, broj monoma u, redom, polinomu H i polinomu L. Zatim slijedi m linija, u svakoj po tri cijela broja i, j, h (i, $j \geq 0$), oni opisuju monom hX^iY^j u kanonskom zapisu polinoma H. Zadnjih n linija unosa opisuje polinom L, na isti način.

- *Format **izlaznih** podataka:* U prvom i jedinom retku nalazi se ili nenegativni cijeli broj, traženi multiplicitet presjeka danih krivulja u točki (0, 0) ili $+\infty$.

Primjer 2.6.4. Sada dajemo nekoliko primjera na kojima smo testirali program. Prvi i drugi primjer su iz napomene 2.6.3, treći primjer je (c) dio primjera 2.6.1, ostali primjeri su oni gdje odmah vidimo koliki je multiplicitet. Lako vidimo koliki su iz osnovnih svojstava multipliciteta presjeka (definicija 2.5.2) ili iz napomene 2.6.3, odnosno iz teorema 2.6.6 i njegovog korolara, koji će biti iskazani i dokazani nakon navedenih primjera.

H	L	ULAZ	IZLAZ
$X^2 + X - Y$	$X - Y^2$	3 2 2 0 1 1 0 1 0 1 -1 1 0 1 0 2 -1	1
$X^3 - 39X^2 - 3X - Y$	$X^2 - 3X - Y$	4 3 3 0 1 2 0 -39 1 0 -3 0 1 -1 2 0 1 1 0 -3 0 1 -1	2
$\left(X^2 + Y^2\right)^3 - 4X^2Y^2$	$\left(X^2 + Y^2\right)^2 + 3X^2Y - Y^3$	5 5 6 0 1 4 2 3 2 4 3 2 2 -4 0 6 1 4 0 1 2 2 2 2 1 3 0 4 1 0 3 -1	14
$(X + Y)^2$	$X + Y$	3 2 2 0 1 1 1 2 0 2 1 1 0 1 0 1 1	$+\infty$
$X + Y + 1$	$X + Y$	3 2 1 0 1 0 1 1 0 0 1 1 0 1 0 1 1	0

H	L	ULAZ	IZLAZ
$X^9 - Y$	$X^7 + Y$	2 2 9 0 1 0 1 -1 7 0 1 0 1 1	7
$X^9 - 7Y^6$	$X + 13Y^5$	2 2 9 0 1 0 6 -7 1 0 1 0 5 13	6
$X^9 - Y$	$13X^8Y^3 + 4X^3Y^2 - Y^3$	2 3 9 0 1 0 1 -1 8 3 13 3 2 4 0 3 -1	21
$X^2 + Y^8$	$X + 17Y^7 - 14Y^5 + Y^3$	2 4 2 0 1 0 8 1 1 0 1 0 7 17 0 5 -14 0 3 1	6
$(X + Y)^2 Y^7$	$41X^9 - 32X^8 - Y$	3 3 2 7 1 1 8 2 0 9 1 9 0 41 8 0 -32 0 1 -1	58

Posebne klase krivulja

Najprije navodimo teorem koji je zapravo tvrdnja točaka (3) i (4) primjera 2.6.2 pa ga navodimo bez dokaza. Napomenimo da u teoremima 2.6.5, 2.6.6 i korolaru 2.6.7 uvijek možemo mijenjati uloge polinoma F i G kao i varijabli X i Y, sve to radi simetrije.

Teorem 2.6.5. *Neka su $F, G \in K[X, Y]$ i neka postoji $g \in K[Y]$ takav da je $G = g(Y)$. Tada, ako je $g = 0$ ili $F(X, 0) = 0$ (uz $g(0) = 0$), onda je $I((0, 0), F \cap G) = +\infty$, inače, ako su $m, n \in \mathbb{Z}_{\geq 0}$ takvi da $X^m \mid F(X, 0)$, $X^{m+1} \nmid F(X, 0)$ te $Y^n \mid g$, $Y^{n+1} \nmid g$, onda je*

$$I((0, 0), F \cap G) = mn.$$

Teorem koji slijedi reći će nam kako gotovo odmah možemo vidjeti koliki je multiplicitet presjeka krivulja u točki (0, 0), u posebnom slučaju kada je barem jedna od krivulja

zadana u obliku $Y = f(X)$ ili $X = f(Y)$. Teorem je motiviran činjenicom da ukoliko provodimo algoritam (uz zamijenjene uloge varijabli X i Y) nad krivuljama $F(X, Y) = f(X) - Y$ i $G(X, Y)$ dobivamo da nakon nekoliko koraka polinom G poprima oblik $G(X, f(X))$. Dokaz koji ćemo dati biti će nešto elegantniji od provođenja cijelog ovog računa. Tj. dokaz je motiviran postupkom u točki (6) primjera 2.6.2.

Teorem 2.6.6. *Neka su $f \in K[X]$ (takav da je $f(0) = 0$) i $F, G \in K[X, Y]$. Neka je $F(X, Y) = f(X) - Y$, tada je*

$$I((0, 0), F \cap G) = \begin{cases} +\infty, & G(X, f(X)) = 0 \\ n, & G(X, f(X)) \neq 0 \end{cases},$$

gdje je $n \in \mathbb{Z}_{\geq 0}$ takav da $X^n \mid G(X, f(X))$ i $X^{n+1} \nmid G(X, f(X))$.

Dokaz. Pretpostavimo da znamo da postoji polinom $H \in K[X, Y]$ takav da je

$$G(X, f(X)) = G + HF,$$

tada prema svojstvu (5) multipliciteta presjeka (definicija 2.5.2) znamo da je

$$I((0, 0), F \cap G) = I((0, 0), F \cap G(X, f(X))) = \begin{cases} +\infty, & G(X, f(X)) = 0 \\ n, & G(X, f(X)) \neq 0 \end{cases},$$

gdje je $n \in \mathbb{Z}_{\geq 0}$ takav da $X^n \mid G(X, f(X))$ i $X^{n+1} \nmid G(X, f(X))$. Naime, $G(X, f(X)) \neq 0$ nam govori da postoji takav $n \in \mathbb{Z}_{\geq 0}$ pa je $G(X, f(X)) = X^n L$, gdje je $L \in K[X]$ takav da $L(0) \neq 0$ pa tvrdnja slijedi odmah prema svojstvima (6) i (7) multipliciteta presjeka (u već spomenutoj definiciji). Preostaje nam, dakle, pokazati da postoji takav polinom $H \in K[X, Y]$. Znamo da postoji $N \in \mathbb{N}$ i brojevi $a_{kl} \in K$, gdje su $k, l \in \{0, 1, \ldots, N\}$, takvi da je $G(X, Y) = \sum_{k=0}^{N} \sum_{l=0}^{N} a_{kl} X^k Y^l$. Sada, trebamo pokazati da postoji $H \in K[X, Y]$ takav da je $HF = G(X, f(X)) - G(X, Y)$, za to je dovoljno pokazati da $F \mid G(X, f(X)) - G(X, Y)$. No, to je jasno jer je

$$G(X, f(X)) - G(X, Y) = \sum_{k=0}^{N} \sum_{l=0}^{N} a_{kl} X^k \left((f(X))^l - Y^l \right),$$

a $F = f(X) - Y \mid (f(X))^l - Y^l$, za sve $l \in \mathbb{Z}_{\geq 0}$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Sljedeći korolar je direktna posljedica prethodnog teorema pa ga navodimo bez dokaza.

Korolar 2.6.7. *Neka su m i n nenegativni cijeli brojevi, tada je multiplicitet presjeka krivulja $Y = X^m$ i $Y = X^n$ u točki $(0, 0)$ jednak*

$$\begin{aligned} +\infty, &\quad \text{ako je} \quad m = n, \\ \min\{m, n\}, &\quad \text{ako je} \quad m \neq n. \end{aligned}$$

Općenitije, neka su $f, g \in K[X]$ takvi da je $f(0) = g(0) = 0$, tada je multiplicitet presjeka krivulja $Y = f(X)$ i $Y = g(X)$ u točki $(0, 0)$ jednak $+\infty$ ako je $f = g$, odnosno k ako je $f \neq g$ i $k \in \mathbb{Z}_{\geq 0}$ takav da $X^k \mid f - g$ i $X^{k+1} \nmid f - g$.

2.7 Drukčija definicija multipliciteta presjeka

U ovoj sekciji ćemo dati definiciju multipliciteta presjeka krivulja pomoću teorije formalnih redova i teorema o implicitno zadanoj funkciji. Zatim ćemo pokazati da se takva definicija podudara s našom koju smo već izložili. Napomenimo da je već viđena definicija više algebarske prirode, dok će ova "nova" biti više geometrijska. Taj geometrijski pogled će se očitovati u tome što će nam, da bi definicija bila valjana, barem jedna krivulja morati biti ireducibilna. Uvedimo osnovne pojmove koji će nam biti potrebni iz teorije formalnih redova.

Osnovno o formalnim redovima

Prisjetimo se definicije polinoma u jednoj varijabli X, 1.1.10. Izbacimo li zahtjev da je najviše konačno mnogo članova različito od 0 dobivamo sljedeću definiciju.

Definicija 2.7.1. *Neka je R prsten.* ***Prsten formalnih redova nad prstenom*** *R je prsten $R[[X]]$ koji se sastoji od svih nizova u R, uz operacije, za nizove $f = (a_0, a_1, a_2, \ldots)$ i*

$g = (b_0, b_1, b_2, \ldots)$, *dane s:*

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots), \quad f \cdot g = (a_0 b_0, a_0 b_1 + a_1 b_0, \ldots, \underbrace{\sum_{k=0}^{n} a_k b_{n-k}}_{n\text{-to mjesto}}, \ldots).$$

Nadalje, $X := (0, 1, 0, 0, \ldots)$ *te* $X^0 := (1, 0, 0, \ldots)$.

Kao i u situaciji s polinomima, lako zaključujemo da uz gornje oznake, možemo pisati $f = \sum_{k=0}^{\infty} a_k X^k$. Napomenimo da se ovdje radi upravo u formalnim redovima, tj. nikakva konvergencija nas ne zanima. Pojam djeljivosti je isti kao u slučajnu polinoma. Ključna razlika između formalnih redova i polinoma se očituje u sljedećoj propoziciji.

Propozicija 2.7.2. *Uz iste oznake,* f *je invertibilan element u* $R[[X]]$ *ako i samo ako je* a_0 *invertibilan element u* R.

Dokaz. Pretpostavimo da je $f \in R[[X]]^*$, to znači da postoji $g = \sum_{l=0}^{\infty} b_l X^l \in R[[X]]$ takav da je $fg = 1$. No, to odmah znači da je $a_0 b_0 = 1$, iz čega vidimo da je $a_0 \in R^*$. Obratno, neka je $a_0 \in R^*$. Tražimo $g = \sum_{l=0}^{\infty} b_l X^l \in R[[X]]$ takav da je $fg = 1$, znamo da je

$$fg = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + \ldots + (a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0) X^n + \ldots.$$

Sada ćemo induktivno izračunati svaki koeficijent b_l, $l \in \mathbb{Z}_{\geq 0}$ formalnog reda g. Pretpostavimo da je $n \in \mathbb{N}$ i da znamo vrijednosti $b_0, b_1, \ldots, b_{n-1}$. Kako mora biti

$$a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0 = 0,$$

zaključujemo da je $b_n = -a_0^{-1} (a_1 b_{n-1} + \ldots + a_{n-1} b_1 + a_n b_0)$. Q.E.D.

Jasno je da je $R[X]$ potprsten prstena $R[[X]]$. Također, jasno je da ako je R integralna domena da je onda i $R[[X]]$ integralna domena, to se vidi naprosto množenjem vodećih koeficijenata. Sljedeći teorem je zapravo teorem o implicitno zadanoj funkciji, on nam je ključan za uvođenje nove definicije multipliciteta presjeka.

Teorem 2.7.3. *Neka je K polje i $F \in K[X, Y]$ takav da je $F(0, 0) = 0$ i $F_Y(0, 0) \neq 0$. Tada postoji jedinstven $\sum_{k=1}^{\infty} a_k X^k \in K[[X]]$ takav da je $F\left(X, \sum_{k=1}^{\infty} a_k X^k\right) = 0$.*

Napomena 2.7.4. *Zadnja jednakost je, jasno, jednakost u prstenu $K[[X]]$. Primijetimo da je navedeni red djeljiv s X, odnosno, nema slobodni koeficijent, tj. jednak mu je 0, prema propoziciji 2.7.2 to znači da nije invertibilan. Nadalje, uvjet $F_Y(0, 0) \neq 0$ nam zapravo govori da uz monom Y u polinomu F moramo imati koeficijent koji je različit od 0.*

Dokaz. Postoje $n \in \mathbb{N}$ i $f_0, f_1, \ldots, f_n \in K[X]$ takvi da je

$$F(X, Y) = f_0(X) + f_1(X)\, Y + \ldots + f_n(X)\, Y^n.$$

Kako je $F_Y(0, 0) \neq 0$ zaključujemo da je $f_1(0) \neq 0$, a kako je $F(0, 0) = 0$ zaključujemo da je $f_0(0) = 0$. Sada pomoću Taylorovog razvoja (propozicija 1.2.35) oko 0 vidimo da postoje $g_0, g_1 \in K[X]$ takvi da je

$$f_0(X) = X g_0(X) \qquad \text{i} \qquad f_1(X) = f_1(0) + X g_1(X).$$

Sada imamo sve što nam je potrebno da jednoznačno odredimo $\sum_{k=1}^{\infty} a_k X^k \in K[[X]]$ takav da je $F\left(X, \sum_{k=1}^{\infty} a_k X^k\right) = 0$. Želimo da nam u $K[[X]]$ vrijedi sljedeća jednakost.

$$0 = F\left(X, \sum_{k=1}^{\infty} a_k X^k\right) = X g_0(X) + (f_1(0) + X g_1(X))\left(\sum_{k=1}^{\infty} a_k X^k\right) + \sum_{l=2}^{n} f_l(X)\left(\sum_{k=1}^{\infty} a_k X^k\right)^l.$$

Odnosno, kako je $f_1(0) \neq 0$, možemo pisati:

$$\sum_{k=1}^{\infty} a_k X^k = \frac{-1}{f_1(0)}\left(X g_0(X) + X g_1(X)\left(\sum_{k=1}^{\infty} a_k X^k\right) + \sum_{l=2}^{n} f_l(X)\left(\sum_{k=1}^{\infty} a_k X^k\right)^l\right).$$

Sada redom računamo $a_1, a_2, \ldots$ izjednačavajući koeficijente uz $X, X^2, \ldots$, za X dobijemo $a_1 = \frac{-1}{f_1(0)} g_0(0)$. Zatim za X^2 imamo:

$$a_2 = \frac{-1}{f_1(0)}\left(\text{koeficijent uz } X \text{ u } g_0(X) + a_1 g_1(0) + f_2(0)\, a_1^2\right).$$

Slično nastavljamo dalje za sve $a_3, a_4, \ldots$, ovime smo gotovi. Q.E.D.

Multipliciteti presjeka i formalni redovi

Najprije uvedimo jednu novu oznaku.

Definicija 2.7.5. *Neka je* $0 \neq f = \sum_{k=0}^{\infty} a_k X^k \in K[[X]]$, *tada postoji najmanji* $n \in \mathbb{Z}_{\geq 0}$ *takav da je* $a_n \neq 0$. *Pisati ćemo* $\nu(f) = n$. *Dodatno, neka je* $\nu(0) = +\infty$.

Definirati ćemo multiplicitet presjeka dviju krivulja u točki $(0, 0)$ od kojih je barem jedna od njih ireducibilna i zadovoljava uvjete teorema 2.7.3. Najprije ćemo malo zlorabiti oznake pa ćemo za ovu, na prvi pogled, potpuno drukčiju definiciju koristiti istu oznaku za multiplicitet presjek kao i u definiciji 2.5.2. No, teorem 2.7.9 koji slijedi će nam pokazati da je takva notacija potpuno opravdana.

Definicija 2.7.6. *Neka su* $F, G \in K[X, Y]$. *Neka je* F *ireducibilna krivulja takva da je* $F(0, 0) = 0$ *i* $F_Y(0, 0) \neq 0$. *Definiramo* ***multiplicitet presjeka*** *krivulja* F *i* G *u točki* $(0, 0)$ *kao*

$$I((0, 0), F \cap G) = \nu\left(G\left(X, \sum_{k=1}^{\infty} a_k X^k\right)\right),$$

gdje je $\sum_{k=1}^{\infty} a_k X^k \in K[[X]]$ *jedinstven takav da je* $F\left(X, \sum_{k=1}^{\infty} a_k X^k\right) = 0$, *kao u teoremu 2.7.3.*

Napomena 2.7.7. *Prethodnu definiciju lako proširujemo na bilo koju točku iz* $\mathbb{A}^2$. *Naime, za* $P = (a, b) \in \mathbb{A}^2$, *jednostavno promatramo polinome* $F(X + a, Y + b)$ *i* $G(X + a, Y + b)$ *pa opet imamo situaciji u točki* $(0, 0)$. *Dodatno, ako je* $F_Y(P) \neq 0$, *onda je jasno i da je* $(F(X + a, Y + b))_Y(0, 0) \neq 0$, *kao i ako je* F *ireducibilan, onda je i njegova translacija ireducibilna, dakle, sve je dobro.*

Sada želimo pokazati da je ovakva definicija dobra, tj. da se ona podudara s onom od ranije, s definicijom 2.5.2. Time ćemo opravdati i korištenje iste oznake. Prema teoremu 2.5.5 vidimo da će ta činjenica slijediti direktno iz sljedećeg teorema. No, najprije iskažimo i dokažimo jednu pomoćnu tvrdnju.

Lema 2.7.8. *Neka su* $F, G \in K[X, Y]$ *relativno prosti polinomi. Tada postoje polinomi* $A, B \in K[X, Y]$ *i* $0 \neq H \in K[X]$ *takvi da je* $A(X, Y)F(X, Y) + B(X, Y)G(X, Y) = H(X)$.

Dokaz. Znamo da je $K[X]$ integralna domena, označimo njeno polje razlomaka s $K(X)$. Tada je očito $K[X, Y] = K[X][Y] \subseteq K(X)[Y]$. Nadalje, jasno je da su F i G relativno prosti i kao polinomi u prstenu $K(X)[Y]$. Dakle, postoje polinomi $A, B \in K[X, Y]$ i $H_1, H_2 \in K[X]$, oba različita od 0, takvi da je $\frac{A}{H_1}F + \frac{B}{H_2}G = 1$. Pomnožimo dobivenu jednakost s $H = H_1H_2 \neq 0$ i dobivamo što smo tražili. Q.E.D.

Teorem 2.7.9. *Neka su* $F, G \in K[X, Y]$. *Neka je* F *ireducibilna te neka je* $F(0, 0) = 0$ *i* $F_Y(0, 0) \neq 0$. *Tada, ako je* $\sum_{k=1}^{\infty} a_k X^k \in K[[X]]$ *jedinstven takav da je* $F\left(X, \sum_{k=1}^{\infty} a_k X^k\right) = 0$ *(kao u teoremu 2.7.3), onda je*

$$\dim_K \left(\mathcal{O}_{(0,0)}\left(\mathbb{A}^2\right)/(F, G)\right) = \nu\left(G\left(X, \sum_{k=1}^{\infty} a_k X^k\right)\right).$$

Dokaz. Označimo, $\mathcal{O} = \mathcal{O}_{(0,0)}\left(\mathbb{A}^2\right)$. Za polinom $A \in K[X, Y]$ uvodimo oznaku $\tilde{A} \in K[[X]]$, $\tilde{A} = A\left(X, \sum_{k=1}^{\infty} a_k X^k\right)$. Najprije pokažimo da krivulje F i G imaju zajedničku komponentu ako i samo ako je $\nu\left(\tilde{G}\right) = +\infty$. Kako je F ireducibilna krivulja zaključujemo da F i G imaju zajedničku komponentu ako i samo ako $F \mid G$. Dakle, moramo pokazati da je $\nu\left(\tilde{G}\right) = +\infty$ ako i samo ako $F \mid G$. Jasno je da ako $F \mid G$ da je $\tilde{G} = 0$, odnosno $\nu\left(\tilde{G}\right) = +\infty$. Obratno, ako je $\tilde{G} = 0$, tvrdimo da $F \mid G$. Pretpostavimo da $F \nmid G$. Kako je F ireducibilan, zaključujemo da su F i G relativno prosti polinomi. To znači, prema lemi 2.7.8, da postoje $A, B \in K[X, Y]$ i $0 \neq H \in K[X]$ takvi da je $AF + BG = H$, u $K[X, Y]$. No, to onda znači da je, u $K[[X]]$, $0 = \tilde{A}\tilde{F} + \tilde{B}\tilde{G} = \tilde{H} = H \neq 0$, što je očita kontradikcija. (Posljednja jednakost vrijedi zato što polinom H ne ovisi o varijabli Y.) Dakle, dalje radimo pod pretpostavkom da je $\nu\left(\tilde{G}\right) < +\infty$. Neka je $\nu\left(\tilde{G}\right) = n \in \mathbb{Z}_{\geq 0}$. Promatrajmo homomorfizam $\varphi : \mathcal{O} \to K[[X]]$, zadan kao

$$\varphi\left(\frac{A}{B}\right) = \frac{\tilde{A}}{\tilde{B}} = \tilde{A}\tilde{B}^{-1},$$

gdje su $A, B \in K[X, Y]$ i B takav da je $B(0, 0) \neq 0$. Iz toga odmah zaključujemo da B ima slobodni koeficijent različit od 0 pa je stoga, prema propoziciji 2.7.2, $\tilde{B}$ invertibilan u $K[[X]]$. Dakle, φ je dobro definiran homomorfizam. Neka je $\widetilde{O} = \mathrm{Im}(\varphi)$. Kako je (F, G), kao ideal u O, jednak $FO + GO$ vidimo da je

$$\varphi((F, G)) = \underbrace{\tilde{F}}_{=0}\widetilde{O} + \tilde{G}\widetilde{O} = \tilde{G}\widetilde{O}.$$

Označimo $\widetilde{I} = \tilde{G}\widetilde{O}$. Najveća potencija od X koja dijeli $\tilde{G}$ je X^n, stoga postoji invertibilni element $g \in K[[X]]$ (radi karakterizacije u propoziciji 2.7.2) takav da je $\tilde{G} = X^n g$, zato je $\widetilde{I} = X^n\widetilde{O}$. Označimo s (X^n) ideal u $K[[X]]$ generiran s X^n. Znamo da je

$$\dim_K(K[[X]] / (X^n)) = n,$$

zato jer bazu čine naprosto $1, X, X^2, \ldots, X^{n-1}$ (za $n = 0$ je to nul–prostor), tj. njihove slike, ovo je zapravo ista situacija kao s prstenom $K[X]$. Sada vidimo da ukoliko pokažemo da je

$$\dim_K(O/(F, G)) = \dim_K\left(\widetilde{O}/\widetilde{I}\right) = \dim_K(K[[X]] / (X^n))$$

da smo gotovi. Pokazati ćemo da su ta tri vektorska prostora međusobno izomorfna i time dokaz privesti kraju. To pokazujemo u dva koraka.

• $\widetilde{O}/\widetilde{I} \cong K[[X]] / (X^n)$. Definirajmo $\psi : \widetilde{O} \to K[[X]] / (X^n)$ kao kompoziciju prirodnog ulaganja $\left(\widetilde{O} \to K[[X]]\right)$ i kanonskog epimorfizma $(K[[X]] \to K[[X]] / (X^n))$. Jasno je da je dovoljno vidjeti da je ψ epimorfizam i da je $\mathrm{Ker}(\psi) = \widetilde{I}$. Činjenica da je epimorfizam slijedi iz očitog razloga što slike (po ψ) elemenata $1, X, X^2, \ldots, X^{n-1} \in \widetilde{O}$ čine bazu prostora $K[[X]] / (X^n)$. Nadalje, neka su $A, B \in K[X, Y]$, $B(0, 0) \neq 0$ takvi da je $\psi\left(\frac{\tilde{A}}{\tilde{B}}\right) = 0$. No, to onda znači da $X^n \mid \tilde{A}\tilde{B}^{-1}$, a kako $X \nmid \tilde{B}^{-1}$ (opet, radi propozicije 2.7.2), zaključujemo da $X^n \mid \tilde{A}$. Konačno zaključujemo da je $\frac{\tilde{A}}{\tilde{B}} \in \widetilde{I}$, odnosno, $\mathrm{Ker}(\psi) \subseteq \widetilde{I}$, obratna inkluzija je očita. Ovime smo pokazali da je $\widetilde{O}/\widetilde{I} \cong K[[X]] / (X^n)$.

• $O/(F, G) \cong \widetilde{O}/\widetilde{I}$. Definirajmo $\varphi_0 : O \to \widetilde{O}/\widetilde{I}$ kao kompoziciju već definiranog homomorfizma φ i kanonskog epimorfizma. Opet, moramo dokazati da je φ_0 epimorfizam

i da je $\mathrm{Ker}\,(\varphi_0) = (F, G)$. Iz definicije od φ i $\widetilde{O}$ je jasno da je φ_0 epimorfizam. Neka su $A, B \in K[X, Y]$, $B(0, 0) \neq 0$ takvi da je $\varphi_0\left(\frac{A}{B}\right) = 0$. Ovo znači da je $\tilde{A}\tilde{B}^{-1} \in \widetilde{I}$, odnosno, da je $\tilde{A} \in \widetilde{I}$. Dakle, postoje $C, D \in K[X, Y]$, $D(0, 0) \neq 0$ takvi da je $\tilde{A} = \tilde{G}\tilde{C}\tilde{D}^{-1}$. Točnije, imamo da je $\tilde{A}\tilde{D} - \tilde{G}\tilde{C} = 0$. Sada tvrdimo da $F \mid AD - GC$. Pretpostavimo suprotno, tj. $F \nmid AD - GC$, iz toga, kako je F ireducibilan, zaključujemo da su polinomi F i $AD - GC$ relativno prosti pa, prema lemi 2.7.8, postoje polinomi $L_1, L_2 \in K[X, Y]$ te polinom $0 \neq H \in K[X]$ takvi da je

$$L_1 F + L_2 (AD - GC) = H, \quad \text{u } K[X, Y].$$

Prebacimo li to u $K[[X]]$ vidimo da vrijedi $0 = \tilde{L_1}\tilde{F} + \tilde{L_2}\left(\tilde{A}\tilde{D} - \tilde{G}\tilde{C}\right) = \tilde{H} = H \neq 0$, što je kontradikcija. Dakle, postoji polinom $L \in K[X, Y]$ takav da je $AD = FL + CG$. Znamo da je $B(0, 0) \neq 0$ i $D(0, 0) \neq 0$ pa vidimo da je $\frac{A}{B} = \frac{L}{BD}F + \frac{C}{BD}G \in (F, G)$. Ovime smo pokazali da je $\mathrm{Ker}\,(\varphi_0) \subseteq (F, G)$, dok je obratna inkluzija jasna stvar. Dakle, imamo što smo željeli, tj. $O/(F, G) \cong \widetilde{O}/\widetilde{I}$. Q.E.D.

Napomenimo samo da uvijek možemo zamijeniti ulogu krivuljama F i G. Također, sve tvrdnje analogno vrijede zamijenimo li ulogu varijablama X i Y. Formalizirajmo rečeno, sljedeći korolar je direktna posljedica prethodnog teorema pa ga navodimo bez dokaza.

Korolar 2.7.10. *Neka su F i G afine ravninske krivulje. Neka je G ireducibilna i neka je $G(0, 0) = 0$ te $G_X(0, 0) \neq 0$. Tada, ako $G \mid F$, onda je $I((0, 0), F \cap G) = +\infty$, a ako $G \nmid F$ (tj. krivulje F i G nemaju zajedničkih komponenti), onda je $I((0, 0), F \cap G) = n$, gdje je $n \in \mathbb{Z}_{\geq 0}$ najveći takav da $Y^n \mid F\left(\sum_{k=1}^{\infty} b_k Y^k, Y\right)$. Pri tome je spomenuti red jedinstven takav da je $G\left(\sum_{k=1}^{\infty} b_k Y^k, Y\right) = 0$, u $K[[Y]]$, slično kao u teoremu 2.7.3.*

Primjer primjene

Ovdje ćemo dati primjer u kojem se multiplicitet presjeka izračuna lako pomoću ove nove definicije. Tražimo multiplicitet presjeka krivulje

$$F_n(X, Y) = (1 - X)(1 - Y)^n - 1,$$

gdje je $n \in \mathbb{N}$, s krivuljom $G(X, Y) = X^5 - 7X^3Y^5 + 3X^2Y^2 + Y^7$, jasno, u točki $(0, 0)$. U [12], strana 164, Theorem 6.15 nalazimo Eisensteinov kriterij. Prema njemu vidimo da je F_n ireducibilna krivulja $\left(Y \mid (1 - Y)^n - 1,\ Y^2 \nmid (1 - Y)^n - 1,\ Y \nmid (1 - Y)^n\right)$, jasno je da je $F(0, 0) = 0$ i da je $F_{nX}(0, 0) \neq 0$. Sada gledamo $F(X, Y) = 0$ i formalno provodimo račun u $K[[Y]]$:

$$X = 1 - \left(\frac{1}{1 - Y}\right)^n = 1 - \left(1 + \sum_{k=1}^{\infty} Y^k\right)^n = -\sum_{l=1}^{n} \binom{n}{l} \left(\sum_{k=1}^{\infty} Y^k\right)^l.$$

Sada nas zanima koja je najveća potencija od Y koja dijeli $G\left(-\sum_{l=1}^{n} \binom{n}{l} \left(\sum_{k=1}^{\infty} Y^k\right)^l,\ Y\right)$. Lako vidimo da je to Y^4, bez obzira na $n \in \mathbb{N}$. Naime, najveća potencija od Y koja dijeli $-\sum_{l=1}^{n} \binom{n}{l} \left(\sum_{k=1}^{\infty} Y^k\right)^l$ je Y, a u $G(X, Y)$ je monom najmanjeg stupnja jednak $3X^2Y^2$. Zaključujemo da je $I((0, 0), F_n \cap G) = 4$, za sve $n \in \mathbb{N}$. Ovo možemo, za male $n \in \mathbb{N}$, provjeriti i računalom, npr. programom iz sekcije 2.6. Dati ćemo primjer ulaznih podataka za $n = 1, 2, 3, 4, 5, 6$.

Napomena 2.7.11. *Primijetimo da nam je, uz gornje oznake, u krivulji G bio bitan jedino stupanj "najmanjeg" monoma. Dakle, za bilo koju krivulju G koja sadrži točku $(0, 0)$ i koja nije djeljiva krivuljom F_n (tj. F_n i G nemaju zajedničku komponentu) će vrijediti da je $I((0, 0), F \cap G)$ jednak stupnju najmanjeg monoma u polinomu G i to za svaki $n \in \mathbb{N}$.*

Sljedeća tablica sadrži spomenute ulazne podatke za $n = 1, 2, 3, 4, 5, 6$.

$n = 1$	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$
3 4 1 0 -1 1 1 1 0 1 -1 5 0 1 3 5 -7 2 2 3 0 7 1	5 4 1 0 -1 1 1 2 1 2 -1 0 1 -2 0 2 1 5 0 1 3 5 -7 2 2 3 0 7 1	7 4 1 0 -1 1 1 3 1 2 -3 1 3 1 0 1 -3 0 2 3 0 3 -1 5 0 1 3 5 -7 2 2 3 0 7 1	9 4 1 0 -1 1 1 4 1 2 -6 1 3 4 1 4 -1 0 1 -4 0 2 6 0 3 -4 0 4 1 5 0 1 3 5 -7 2 2 3 0 7 1	11 4 1 0 -1 1 1 5 1 2 -10 1 3 10 1 4 -5 1 5 1 0 1 -5 0 2 10 0 3 -10 0 4 5 0 5 -1 5 0 1 3 5 -7 2 2 3 0 7 1	13 4 1 0 -1 1 1 6 1 2 -15 1 3 20 1 4 -15 1 5 6 1 6 -1 0 1 -6 0 2 15 0 3 -20 0 4 15 0 5 -6 0 6 1 5 0 1 3 5 -7 2 2 3 0 7 1

Poglavlje 3

Projektivne mnogostrukosti

3.1 Osnovni pojmovi

Promotrimo krivulju $Y^2 = X^2 + 1$ i pravac $Y = X$, vidimo da se oni ne sijeku u $\mathbb{A}^2$, ali se krivulja asimptotski "približava" pravcu. Cilj nam je "povećati" afinu ravninu tako da se oni sijeku u "beskonačnosti". U tu svrhu, identificirajmo svaku točku $(x, y) \in \mathbb{A}^2$ točkom $(x, y, 1) \in \mathbb{A}^3$. Svaka točka $(x, y, 1) \in \mathbb{A}^3$ jedinstveno određuje pravac koji prolazi tom točkom i točkom $(0, 0, 0)$, obratno, svaki pravac točkom $(0, 0, 0)$ koji ne leži u ravnini $\{(x, y, 0) : x, y \in K\}$ (označavati ćemo ju jednostavno sa $z = 0$) jedinstveno određuje točku oblika $(x, y, 1)$. Pravce točkom $(0, 0, 0)$ koji leže u ravnini $z = 0$ ćemo smatrati "točkama u beskonačnosti".

Definicija 3.1.1. *Neka je K polje i $n \in \mathbb{Z}_{\geq 0}$.* ***Projektivni prostor*** *nad poljem K, u oznaci $\mathbb{P}^n(K)$ (tj. $\mathbb{P}^n$), je skup svih pravaca u $\mathbb{A}^{n+1}$ koji prolaze točkom $(0, 0, \ldots, 0)$.*

Napomena 3.1.2. *Primijetimo da svaka točka $0 \neq (x_1, x_2, \ldots, x_{n+1}) \in \mathbb{A}^{n+1}$ određuje jedan takav pravac točkom $0 = (0, 0, \ldots, 0)$. Obratno, primijetimo da točke*

$$x = (x_1, x_2, \ldots, x_{n+1}) \quad i \quad y = (y_1, y_2, \ldots, y_{n+1})$$

iz $\mathbb{A}^{n+1}$ *određuju isti pravac ako i samo ako postoji* $0 \neq \lambda \in K$ *takav da je* $y = \lambda x$.

Definicija 3.1.3. *Ako takav* λ *(iz prethodne napomene) postoji reći ćemo da su točke* x *i* y ***ekvivalentne***.

Dakle, vidimo da je projektivni prostor zapravo skup klasa navedene ekvivalencije točaka iz $\mathbb{A}^{n+1} \setminus \{(0, 0, \ldots, 0)\}$.

Definicija 3.1.4. *Elemente skupa* $\mathbb{P}^n$ *ćemo zvati* ***točke***. *Ako je točka* $P \in \mathbb{P}^n$ *određena nekom točkom* $0 \neq (x_1, x_2, \ldots, x_{n+1}) \in \mathbb{A}^{n+1}$, *reći ćemo da su* $(x_1, x_2, \ldots, x_{n+1})$ ***homogene koordinate*** *točke* P. *Kako bismo to naglasili, pisati ćemo* $P = (x_1 : x_2 : \ldots : x_{n+1})$.

Neka je $k \in \{1, 2, \ldots, n+1\}$, za vrijednost homogene koordinate x_k točke P iz prethodne definicije možemo samo reći je li $x_k = 0$ ili je $x_k \neq 0$. Ako je $x_k \neq 0$, onda je

$$P = \left(\frac{x_1}{x_k} : \frac{x_2}{x_k} : \ldots : \frac{x_{k-1}}{x_k} : 1 : \frac{x_{k+1}}{x_k} : \ldots : \frac{x_{n+1}}{x_k} \right).$$

Stavljamo $U_k = \{(x_1 : x_2 : \ldots : x_{n+1}) \in \mathbb{P}^n \ : \ x_k \neq 0\}$. Tada svaka točka $P \in U_k$ ima jedinstven zapis, kao gore, tj. s jedinicom na k-toj koordinati.

Definicija 3.1.5. $(x_1, x_2, \ldots, x_{k-1}, x_{k+1}, \ldots, x_{n+1})$ *iz gornje diskusije nazivamo* ***nehomogene koordinate*** *točke* P *u odnosu na* U_k, *ili kraće, u odnosu na* k.

Definirajmo $\varphi_k : \mathbb{A}^n \to U_k$ pomoću

$$\varphi_k (a_1, a_2, \ldots, a_n) = (a_1 : a_2 : \ldots : a_{k-1} : 1 : a_{k+1} : \ldots : a_n) .$$

Dakle, vidimo da postoji prirodna bijekcija između $\mathbb{A}^n$ i U_k. Kako je $\mathbb{P}^n = \bigcup_{k=1}^{n+1} U_k$ zaključujemo da je skup $\mathbb{P}^n$ "pokriven" s $n+1$ skupova od kojih svaki izgleda upravo kao afin prostor.

Definicija 3.1.6. *Definiramo* ***hiperplohu u beskonačnosti*** *kao*

$$H_\infty = \mathbb{P}^n \setminus U_{n+1} = \{(x_1 : x_2 : \ldots : x_{n+1}) \in \mathbb{P}^n \ : \ x_{n+1} = 0\} .$$

Lako vidimo da H_∞ možemo identificirati sa $\mathbb{P}^{n-1}$. Primijetimo također da je $\mathbb{P}^n = U_{n+1} \cup H_\infty$, tj. projektivni prostor je unija afinog prostora i hiperplohe u beskonačnosti.

Primjer 3.1.7.

(1) $\mathbb{P}^0$ je skup od samo jedne točke.

(2) $\mathbb{P}^1 = \{(x : 1) \ : \ x \in K\} \cup \{(1, 0)\}$, tj. $\mathbb{P}^1$ je afin pravac kojemu je dodana još jedna točka u beskonačnosti.

(3) $\mathbb{P}^2 = \left\{(x : y : 1) \ : \ (x, y) \in \mathbb{A}^2\right\} \cup \left\{(x : y : 0) \ : \ (x : y) \in \mathbb{P}^1\right\}$. $\mathbb{P}^2$ je afina ravnina kojoj je dodan pravac točaka u beskonačnosti.

(4) Neka su $a, b \in K$ i neka je $Y = aX + b$ pravac u $\mathbb{A}^2$. Identificirajmo $\mathbb{A}^2$ s $U_3 \subseteq \mathbb{P}^2$, tada točke pravca odgovaraju točkama $(x : y : z) \in \mathbb{P}^2$ koje zadovoljavaju $y = ax + bz$ i $z = 0$. Zašto? Morali smo uvesti dodatnu varijablu kako bismo homogenizirali jednadžbu. To smo učinili tako da smo umjesto X i Y promatrali $\frac{x}{z}$ i $\frac{y}{z}$ za dodatnu varijablu z. Jasno je da uz tu modifikaciju rješenja za $z = 0$ nemaju smisla. No, lako vidimo da ovom pravcu (kada ga promatramo u $\mathbb{P}^2$) pripada i jedna točka u beskonačnosti, tj. točka $(1 : a : 0)$. Ovo nam govori da svi međusobno paralelni (u $\mathbb{A}^2$), s istim koeficijentom smjera) pravci u $\mathbb{A}^2$, prolaze istom točkom u beskonačnosti.

(5) Prisjetimo se krivulje, $Y^2 = X^2 + 1$ i pravca, $Y = X$, s početka ovog poglavlja. Promatrajmo njihove homogene jednadžbe, to su $y^2 = x^2 + z^2$, $y = x$ i $z \neq 0$. Vidimo da se oni sijeku u beskonačnosti i to u točki $(1 : 1 : 0) \in H_\infty \subseteq \mathbb{P}^2$.

Definicija 3.1.8. $\mathbb{P}^1$ *nazivamo* ***projektivni pravac****, a* $\mathbb{P}^2$ ***projektivna ravnina****.*

Lema 3.1.9. *Neka je* $F \in K[X_1, X_2, \ldots, X_{n+1}]$*, gdje je* K *polje s beskonačno mnogo elemenata. Neka je* $m \in \mathbb{Z}_{\geq 0}$ *i neka je* $F = \sum_{k=0}^{m} F_k$*, gdje je* F_k *homogen polinom stupnja* k*, za sve* $k \in \{0, 1, \ldots, m\}$*. Neka je* $P \in \mathbb{P}^n(K)$ *te pretpostavimo da je* $F(x_1, x_2, \ldots, x_{n+1}) = 0$*,*

za svaki izbor homogenih koordinata $(x_1 : x_2 : \ldots : x_{n+1}) \in \mathbb{P}^n$ *točke* P*. Tada je, za svaki* $k \in \{0, 1, \ldots, m\}$, $F_k(x_1, x_2, \ldots, x_{n+1}) = 0$, *za svaki izbor* $(x_1 : x_2 : \ldots : x_{n+1}) \in \mathbb{P}^n$ *homogenih koordinata točke* P*.*

Dokaz. Fiksirajmo neki izbor homogenih koordinata točke P, $(x_1 : x_2 : \ldots : x_{n+1}) \in \mathbb{P}^n$. Promatrajmo polinom $G \in K[X]$ definiran kao

$$G(\lambda) = F(\lambda x_1, \lambda x_2, \ldots, \lambda x_{n+1}) = \sum_{k=0}^{m} \lambda^k F_k(x_1, x_2, \ldots, x_{n+1}),$$

za sve $\lambda \in K$. Vidimo da je to polinom m-tog stupnja u $K[X]$ koji je jednak 0 u svakoj točki $\lambda \in K \setminus \{0\}$. Kako polje K ima beskonačno mnogo elemenata zaključujemo da je $G = 0$. To znači da je $F_k(x_1, x_2, \ldots, x_{n+1}) = 0$, za sve $k = 0, 1, \ldots, m$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Sada nam je cilj razviti pojam projektivnog algebarskog skupa u $\mathbb{P}^n$. Većina ideja i rezultata se podudara s onima iz afinog slučaja, stoga imamo dosta manje posla.

Definicija 3.1.10. *Neka je* $P \in \mathbb{P}^n$ *i* $F \in K[X_1, X_2, \ldots, X_{n+1}]$*. Reći ćemo da je* P ***nultočka polinoma*** F *i to označavati s* $F(P) = 0$ *ako je* $F(x_1, x_2, \ldots, x_{n+1}) = 0$*, za svaki izbor homogenih koordinata* $(x_1 : x_2 : \ldots : x_{n+1}) \in \mathbb{P}^n$ *točke* P*.*

Ako je F homogen polinom, lako vidimo da ako je F jednak 0 za barem jedan odabir homogenih koordinata točke P, da je onda F jednak 0 u svima. Lema 3.1.9 nam govori da ako je točka P nultočka polinoma F, onda je P nultočka svakog homogenog dijela polinoma F, u smislu da F zapišemo, na standardni način, kao sumu homogenih polinoma. Neka je S bilo koji skup polinoma u $K[X_1, X_2, \ldots, X_{n+1}]$, stavljamo

$$V(S) = \{P \in \mathbb{P}^n \ : \ F(P) = 0, \ \forall F \in S\}.$$

Lako se vidi da ako je I ideal u $K[X_1, X_2, \ldots, X_{n+1}]$ generiran skupom S da je tada $V(I) = V(S)$. Neka je $m \in \mathbb{N}$ i neka je $I = \left(F^{(1)}, F^{(2)}, \ldots, F^{(m)}\right)$ te neka je, za svaki

$k \in \{1, 2, \ldots, m\}$, $F^{(k)} = \sum_{l=0}^{r_k} F_l^{(k)}$, gdje je $r_k \in \mathbb{Z}_{\geq 0}$ i $F_l^{(k)}$ homogen polinom stupnja l, za sve $l \in \{0, 1, \ldots, r_k\}$. Vidimo da je1 $V(I) = V\left(\left\{F_l^{(k)} \ : \ k \in \{1, 2, \ldots, m\}, \ l \in \{0, 1, \ldots, r_k\}\right\}\right)$. Dakle, zaključujemo da je, za svaki skup polinoma, S, $V(S)$ zapravo skup nultočaka konačnog skupa homogenih polinoma.

Definicija 3.1.11. *Skup $V(S)$, gdje je S bilo kakav skup polinoma iz, naziva se* ***projektivni algebarski skup****.*

Za svaki skup $W \subseteq \mathbb{P}^n$ definiramo

$$I(W) = \{F \in K[X_1, X_2, \ldots, X_{n+1}] \ : \ F(P) = 0, \ \forall P \in W\}$$

.

Definicija 3.1.12. *Ideal $I(W)$ se naziva* ***ideal skupa*** *$W \subseteq \mathbb{P}^n$.*

Definicija 3.1.13. *Ideal $I \subseteq K[X_1, X_2, \ldots, X_{n+1}]$ se naziva* ***homogeni ideal*** *ako za svaki $\sum_{k=0}^{m} F_k = F \in I$ vrijedi da je $F_k \in I$, za svaki $k \in \{0, 1, \ldots, m\}$. Ovdje je $m \in \mathbb{N}$ i F_k je homogeni polinom, za svaki $k \in \{0, 1, \ldots, m\}$, standardni zapis polinoma F kao sume homogenih polinoma.*

Lako se vidi da je, za svaki skup $W \subseteq \mathbb{P}^n$, ideal $I(W)$ homogen (lema 3.1.9).

Propozicija 3.1.14. *Ideal $I \subseteq K[X_1, X_2, \ldots, X_{n+1}]$ je homogen ako i samo ako je generiran (konačnim) skupom homogenih polinoma.*

Dokaz. Ako je I homogen ideal, iz prethodne diskusije dobivamo tvrdnju. Obratno, neka je $S = \left\{F^{(\alpha)} \ : \ \alpha \in A\right\}$ skup homogenih polinoma koji generira I te neka je $\deg\left(F^{(\alpha)}\right) = d_\alpha$, za svaki $\alpha \in A$ (ako je neki $F^{(\alpha)} = 0$, zanemarimo ga). Neka su $0 \leq r < r+1 < \ldots < s$ cijeli brojevi i neka su $F_r, F_{r+1}, \ldots, F_s$ homogeni polinomi odgovarajućeg stupnja (indeks), takvi da je $F_r + F_{r+1} + \ldots + F_s = F \in I$. Da bismo dokazali propoziciju dovoljno je

pokazati da je $F_r \in I$, jer je onda i $F - F_r \in I$ pa tvrdnja slijedi po principu matematičke indukcije. Postoje polinomi $G^{(\alpha)}$, $\alpha \in A$ (samo njih konačno različitih od 0) takvi da je $F = \sum_{\alpha \in A} G^{(\alpha)} F^{(\alpha)}$. Za svaki $m \in \mathbb{Z}_{\geq 0}$ neka je $G_m^{(\alpha)}$ homogeni polinom stupnja m iz jedinstvenog raspisa polinoma $G^{(\alpha)}$ kao sume homogenih polinoma, za svaki $\alpha \in A$. Za $m \in \mathbb{Z}$, $m < 0$, neka je $G_m^{(\alpha)} = 0$. Tada je jasno da je $F_r = \sum_{\alpha \in A} G_{r-d_\alpha}^{(\alpha)} F^{(\alpha)}$. Dakle, $F_r \in I$. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Lema 3.1.15. *Neka je $I \subseteq K[X_1, X_2, \ldots, X_{n+1}]$ homogeni ideal. I je prost ideal ako i samo ako za svaka dva homogena polinoma $F, G \in K[X_1, X_2, \ldots, Xn + 1]$ vrijedi: ako je $FG \in I$, onda je $F \in I$ ili $G \in I$.*

Dokaz. Jasno je da je dovoljno pokazati samo smjer $\boxed{\Leftarrow}$. Neka su F i G polinomi iz $K[X_1, X_2, \ldots, X_{n+1}]$ takvi da je $FG \in I$ i neka su $m_1, m_2 \in \mathbb{Z}_{\geq 0}$ takvi da su $F = \sum_{k=0}^{m_1} F_k$ i $G = \sum_{l=0}^{m_2} G_l$ raspisi polinoma F i G kao sume homogenih polinoma, odgovarajućeg stupnja, onog koji piše u indeksu. Pretpostavimo da je $FG \in I$. Kako je I homogen ideal, tada je, za sve $k \in \{0, 1, \ldots, m_1\}$ i $l \in \{0, 1, \ldots, m_2\}$, $F_k G_l \in I$. Ako je $F_k \in I$ za sve $k \in \{0, 1, \ldots, m_1\}$, onda je $F \in I$. Ako postoji neki $k \in \{0, 1, \ldots, m_1\}$ takav da $F_k \notin I$, onda vidimo da je nužno $G_l \in I$, za svaki $l \in \{0, 1, \ldots, m_2\}$ pa je $G \in I$. Dakle, svakako je $F \in I$ ili $G \in I$, tj. ideal I je prost. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Definicija 3.1.16. *Algebarski skup $V \subseteq \mathbb{P}^n$ je **ireducibilan** ako nije prikaziv kao unija dvaju nepraznih algebarskih skupova, od kojih niti jedan nije jednak V. Ireducibilni algebarski skup $V \subseteq \mathbb{P}^n$ naziva se **projektivna mnogostrukost**.*

Pomoću prethodne leme, kao u dokazu propozicije 1.6.2 vidimo:

Propozicija 3.1.17. *Algebarski skup $V \subseteq \mathbb{P}^n$ je ireducibilan ako i samo ako je $I(V)$ prost ideal.*

Također, slično kao teorem 1.6.3, imamo:

Teorem 3.1.18. *Svaki projektivni algebarski skup se može na jedinstven (do na poredak) način prikazati kao unija projektivnih mnogostrukosti od kojih niti jedna ne sadrži neku drugu.*

Preslikavanja V i I u "projektivnom svijetu" između skupova

$$\{\text{homogeni ideali u} K[X_1, X_2, \ldots, X_{n+1}]\} \quad \text{i} \quad \{\text{algebarski skupovi u} \mathbb{P}^n\}$$

zadovoljavaju gotovo jednaka svojstva kao i u afinom svijetu, propozicija 1.4.8.

Ukoliko postoji mogućnost zabune, pisati ćemo V_p i I_p te V_a i I_a da naglasimo nalazimo li se u projektivnom ili afinom prostoru.

Definicija 3.1.19. *Neka je V algebarski skup u $\mathbb{P}^n$, definiramo* ***konus*** *nad V kao*

$$C(V) = \left\{(x_1, x_2, \ldots, x_{n+1}) \in \mathbb{A}^{n+1} \ : \ (x_1, x_2, \ldots, x_{n+1}) = 0 \text{ ili } (x_1 : x_2 : \ldots : x_{n+1}) \in V\right\}.$$

Lako vidimo da vrijedi tvrdnja sljedeće leme (koja će nam pomoći u dokazu projektivnod Nullstellensatza):

Lema 3.1.20. *Neka je V neprazna projektivna mnogostrukost i neka je I homogeni ideal u $K[X_1, X_2, \ldots, X_{n+1}]$ takav da je $V_p(I) \neq \emptyset$. Tada je $I_a(C(V)) = I_p(V)$ i $C\left(V_p(I)\right) = V_a(I)$.*

Teorem 3.1.21 (Projektivni Nullstellensatz)**.** *Neka je $I \subseteq K[X_1, X_2, \ldots, X_{n+1}]$ homogeni ideal. Tada vrijedi sljedeće.*

(1) $V_p(I) = \emptyset$ ako i samo ako postoji cijeli broj N takav da I sadrži sve homogene polinome stupnja barem N.

(2) Ako je $V_p(I) \neq \emptyset$, onda je $I_p\left(V_p(I)\right) = \operatorname{Rad}(I)$.

Dokaz.

(1) Koristeći prethodnu lemu, svojstva (afina) (2) i (7) iz propozicije 1.4.8, "obični" (afini) Nullstellensatz (1.5.22) i lemu 2.3.17 dobivamo sljedeće niz ekvivalencija:

$$V_p(I) = \emptyset \Leftrightarrow V_a(I) \subseteq \{(0, 0, \ldots, 0)\} \Leftrightarrow \mathrm{Rad}(I) = I_a(V_a(I)) \supseteq (X_1, X_2, \ldots, X_{n+1})$$

$$\Longleftrightarrow \exists N \in \mathbb{N} \text{ t.d. } (X_1, X_2, \ldots, X_{n+1})^N \subseteq I.$$

(2) Ovo slijedi direktno iz prethodne leme i afinog Nullstellensatza (1.5.22), naime:
$I_p\left(V_p(I)\right) = I_a\left(C\left(V_p(I)\right)\right) = I_a(V_a(I)) = \mathrm{Rad}(I)$. Q.E.D.

Neka je V neprazna mnogostrukost u $\mathbb{P}^n$, tada je $I(V)$ prost ideal pa je

$$\Gamma_h(V) = K[X_1, X_2, \ldots X_{n+1}]/I(V)$$

integralna domena. Sada imamo definiciju (kao u afinom slučaju, 2.1.2):

Definicija 3.1.22. $\Gamma_h(V)$ *se naziva* ***homogeni koordinatni prsten*** *od* V*. Neka je* I *homogeni ideal u* $K[X_1, X_2, \ldots, X_{n+1}]$ *te neka je* $\Gamma = K[X_1, X_2, \ldots, X_{n+1}]/I$*. Za element* $f \in \Gamma$ *ćemo reći da je* ***homogen*** *stupnja* $d \in \mathbb{Z}_{\geq 0}$ *ako postoji homogen polinom* F *stupnja* d *u* $K[X_1, X_2, \ldots, X_{n+1}]$ *takav da je slika od* F *u* Γ *jednaka* f*.*

Propozicija 3.1.23. *Svaki element* $f \in \Gamma$ *može se, na jedinstven način, zapisati u obliku* $f = f_0 + f_1 + \ldots + f_m$*, gdje je* $m \in \mathbb{Z}_{\geq 0}$ *i* f_k *je homogen stupnja* k*, za svaki* $k = 0, 1, \ldots, m$*.*

Dokaz. Neka je $F \in K[X_1, X_2, \ldots, X_{n+1}]$ takav da je njegova slika u Γ jednaka f. Postoji $m \in \mathbb{Z}_{\geq 0}$ takav da je $F = F_0 + F_1 + \ldots + F_m$ standardni zapis polinoma F u obliku sume homogenih polinoma, jasno, F_k je stupnja k, za svaki $k \in \{0, 1, \ldots, m\}$. Odmah vidimo da je $f = f_0 + f_1 + \ldots + f_m$, gdje je f_k slika polinoma F_k u Γ, za $k = 0, 1, \ldots, m$. Kako bismo dobili i jedinstvenost, neka je $f = g_0 + g_1 + \ldots + g_l$, gdje je $l \in \mathbb{Z}_{\geq 0}$ i g_k je slika homogenog polinoma G_k stupnja k, za sve $k \in \{0, 1, \ldots, l\}$. No sada, kako je I homogeni ideal i kako je $F - (G_0 + G_1 + \ldots + G_l) \in I$ vidimo da je $l = m$ i $F_k - G_k \in I$, za svaki $k \in \{0, 1, \ldots, m\}$. Konačno, $g_k = f_k$, za $k = 0, 1, \ldots, m$. Q.E.D.

Definicija 3.1.24. *Kvocijentno polje homogenog koordinatnog prstena $\Gamma_h(V)$, u oznaci $K_h(V)$ nazivamo* ***homogeno polje funkcija*** *na V.*

Primijetimo, za razliku od afinog slučaja, samo konstante kao elementi od $\Gamma_h(V)$ definiraju (dobro) funkciju na V. Također, većina elemenata polja $K_h(V)$ ne definira (dobro) funkciju na V. No, ukoliko su $f,\ g \in \Gamma_h(V)$ homogeni, istog stupnja $d \in \mathbb{Z}_{\geq 0}$, onda $\dfrac{f}{g}$ dobro definira funkciju na V (tamo gdje je $g \neq 0$). To se vidi iz:

$$\frac{f(\lambda x)}{g(\lambda y)} = \frac{\lambda^d f(x)}{\lambda^d g(y)} = \frac{f(x)}{g(x)},$$

za sve $x \in \mathbb{A}^{n+1} \setminus \{0\}$ i za sve $\lambda \in K$. Dakle, vrijednost od $\dfrac{f}{g}$ ne ovisi o izboru homogenih koordinata.

Definicija 3.1.25. *Neka je V neprazna projektivna mnogostrukost.* ***Polje funkcija****, u oznaci $K(V)$ definiramo kao*

$$\left\{ z \in K_h(V) \ :\ z = \frac{f}{g},\ \textit{gdje su } f,\ g \in \Gamma_h(V)\ \textit{ homogeni istog stupnja} \right\}.$$

Elemente od $K(V)$ nazivamo ***racionalne funckije*** *na V.*

Lako se vidi da je $K \subseteq K(V) \subseteq K_h(V)$. No, primijetimo da $\Gamma_h(V) \nsubseteq K(V)$.

Definicija 3.1.26. *Neka je $P \in V$, gdje je V neprazna projektivna mnogostrukost. Kažemo da je $z \in K(V)$* ***definirana*** *u P ako postoje homogeni, istog stupnja, $f,\ g \in \Gamma_h(V)$ takvi da je $z = \dfrac{f}{g}$ i $g(P) \neq 0$.*

Sada uvodimo definicije lokalnog prste mnogostrukosti V u točki P i pripadajućeg maksimalnog ideala, kao u afinom slučaju.

Definicija 3.1.27. *Neka je V neprazna projektivna mnogostrukost i neka je $P \in V$, definiramo* ***lokalni prsten od*** *V u P kao*

$$\mathcal{O}_P(V) = \{ z \in K(V) \ :\ z \textit{ je definirana u } P \}.$$

Kao što vidimo, $\mathcal{O}_P(V)$ je potprsten od $K(V)$, to je lokalni prsten i pripadajući maksimalni ideal je jednak

$$\mathfrak{m}_P(V) = \left\{ z \in K(V) \ : \ z = \frac{f}{g},\ g(P) \neq 0,\ f(P) = 0 \right\}.$$

Primijetimo da je za svaki $z \in \mathcal{O}_P(V)$, vrijednost $z(P)$ dobro definirama.

Neka je $T : \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$ afina zamjena koordinata takva da je $T(0) = 0$ (tj. ima samo linerani dio). Tada vidimo da T prebacuje svaki pravac kroz ishodište u pravac kroz ishodište (lema 2.1.16, dio (a)). Dakle, T određuje preslikavanje s $\mathbb{P}^n$ u $\mathbb{P}^n$.

Definicija 3.1.28. *Uz prethodnu diskusiju, T nazivamo* ***projektivna zamjena koordinata****.*

Za projektivnu zamjenu koordinata vrijede iste (očekivane) stvari kao i za afinu. Ukoliko je $V \subseteq \mathbb{P}^n$ algebarski skup, onda je i $T^{-1}(V)$ algebarski skup, označavamo ga, kao i prije, s V^T. Neka je $V = V(F_1, F_2, \ldots, F_m)$, gdje je $m \in \mathbb{N}$ i F_k homogeni polinomi stupnja k, za sve $k = 1, 2, \ldots, m$. Neka je $T = (T_1, T_2, \ldots, T_{n+1})$, gdje je T_l homogeni polinom stupnja 1 za sve $l \in \{1, 2, \ldots, n+1\}$. Tada je $V^T = V\left(F_1^T, F_2^T, \ldots, F_m^T\right)$, gdje je $F_k^T = F_k(T_1, T_2, \ldots, T_{n+1})$, za sve $k \in \{1, 2, \ldots, m\}$. Tada je V mnogostrukost ako i samo ako je V^T mnogostrukost. Također, u tom slučaju T inducira izomorfizme među sljedećim skupovima

$$\Gamma_h(V) \to \Gamma_h\left(V^T\right), \quad K(V) \to K\left(V^T\right), \quad \mathcal{O}_P(V) \to \mathcal{O}_Q(V),$$

ako je $T(Q) = P$.

Veza afinih i projektivnih mnogostrukosti

Sada želimo povezati mnogostrukosti u $\mathbb{A}^n$ s onima u $\mathbb{P}^n$. U tu svrhu, smatrajmo $\mathbb{A}^n$ kao podskup od $\mathbb{P}^n$, to možemo realizirati, npr. preslikavanjem $\varphi_{n+1} : \mathbb{A}^n \to U_{n+1} \subseteq \mathbb{P}^n$. Podsjetimo se što je što u definiciji 3.1.5. Podsjetimo se i propozicije 2.3.6 i diskusije prije

nje, trebati će nam tamo uvedene oznake. Neka je V algebarski skup u $\mathbb{A}^n$ i neka je $I = I(V) \in K[X_1, X_2, \ldots, X_n]$. Definiramo I^* kao ideal u $K[X_1, X_2, \ldots, X_{n+1}]$ generiran skupom $\{F^* : F \in I\}$. Jasno je da je taj ideal homogen. Definiramo $V^* = V(I^*) \subseteq \mathbb{P}^n$. Obratno, ako je V algebarski skup u $\mathbb{P}^n$ i $I = I(V) \subseteq K[X_1, X_2, \ldots, X_{n+1}]$, definiramo I_*, ideal u $K[X_1, X_2, \ldots, X_n]$ generiran skupom $\{F_* : F \in I\}$. Također, $V_* = V(I_*) \subseteq \mathbb{A}^n$. Sada dolazimo do željenih svojstava u sljedećoj propoziciji.

Propozicija 3.1.29. *Uz oznake iz prethodne diskusije vrijedi.*

(1) Ako je $V \subseteq \mathbb{A}^n$, onda je $\varphi_{n+1}(V) = V^* \cap U_{n+1}$ i $(V^*)_* = V$.

(2) Ako je $V \subseteq W \subseteq \mathbb{A}^n$, onda je $V^* \subseteq W^* \subseteq \mathbb{P}^n$. Ako je $V \subseteq W \subseteq \mathbb{P}^n$, onda je $V_* \subseteq W_* \subseteq \mathbb{A}^n$.

(3) Ako je V ireducibilan u $\mathbb{A}^n$, onda je V^* ireducibilan u $\mathbb{P}^n$.

(4) Ako je $V \subseteq \mathbb{A}^n$, onda je V^* najmanji algebarski skup u $\mathbb{P}^n$ koji sadrži $\varphi_{n+1}(V)$.

(5) Ako je $V = \bigcup_{k=1}^{m} V_k$, $m \in \mathbb{N}$, rastav u ireducibilne komponente od $V \subseteq \mathbb{A}^n$, onda je $V^* = \bigcup_{k=1}^{n} V_k^*$ rastav u ireducibilne komponente od $V^* \subseteq \mathbb{P}^n$.

(6) Ako je $V \subsetneq \mathbb{A}^n$ neprazan algebarski skup, onda niti jedna ireducibilna komponenta od V^* ne leži u ili sadrži $H_\infty = \mathbb{P}^n \setminus U_{n+1}$.

(7) Ako je $V \subseteq \mathbb{P}^n$ i niti jedna komponenta od V ne leži u, niti sadrži H_∞, onda je $V_* \subsetneq \mathbb{A}^n$ i $(V_*)^* = V$.

Dokaz.

(1) Direktno iz propozicije 2.3.6.

(2) Očito.

(3) Znamo da je $I = I(V)$ prost. Želimo pokazati da je I^* prost. Prema lemi 3.1.15 vidimo da je dovoljno pokazati da ako su $F, G \in K[X_1, X_2, \ldots, X_{n+1}]$ homogeni polinomi takvi da je $FG \in I^*$ da je onda $F \in I^*$ ili $G \in I^*$. No, $FG \in I^*$, znači da je $F_* G_* \in I$ (propozicija 2.3.6), a kako je I prost, tvrdnja slijedi.

(4) Pretpostavimo da je $W \subseteq \mathbb{P}^n$ algebarski skup koji sadrži $\varphi_{n+1}(V)$. Neka je $F \in I(W)$, tada je $F_* \in I(V)$, a to znači da je $F = X_{n+1}^r (F_*)^* \in (I(V))^*$, za neki $r \in \mathbb{Z}_{\geq 0}$ (opet propozicija 2.3.6). Dakle, $I(W) \subseteq (I(V))^*$, iz čega slijedi $W \supseteq V^*$.

(5) Slijedi direktno iz prve četiri točke.

(6) Do sada pokazano nam govori da možemo pretpostaviti da je V ireducibilan. Prema (1) vidimo da $V^* \not\subseteq H_\infty$. Pretpostavimo da je $H_\infty \subseteq V^*$. Tada je

$$(I(V))^* \subseteq I(V^*) \subseteq I(H_\infty) = (X_{n+1}).$$

No, postoji $0 \neq F \in I(V)$, onda je $F^* \in (I(V))^*$ i $F^* \notin (X_{n+1})$, što je kontradikcija.

(7) Opet, možemo pretpostaviti da je V ireducibilan. Kako je $\varphi_{n+1}(V_*) \subseteq V$, jasno je da je dovoljno pokazati da je $V \subseteq (V_*)^*$, odnosno $(I(V_*))^* \subseteq I(V)$. Neka je $F \in I(V_*)$. Nullstellensatz (1.5.22) nam govori da postoji $N \in \mathbb{N}$ takav da je $F^N \in (I(V))_*$. Propozicija 2.3.6 nam govori da postoji $r \in \mathbb{Z}_{\geq 0}$ takav da je $X_{n+1}^r \left(F^N\right)^* \in I(V)$. Kako je $I(V)$ prost ideal i $X_{n+1} \notin I(V)$, jer $V \not\subseteq H_\infty$, zaključujemo da je $F^* \in I(V)$. Q.E.D.

Definicija 3.1.30. *Neka je $V \subseteq \mathbb{A}^n$, $V^* \subseteq \mathbb{P}^n$ nazivamo* ***projektivni zatvarač*** *od V.*

Propozicija 3.1.31. *Neka je $F \in K[X_1, X_2, \ldots, X_n]$ i $I = (F)$ te $V = V(I)$. Tada je*

$$I^* = (F^*) \quad i \quad V^* = V(I^*).$$

Dokaz. Obje tvrdnje su očite, slijede direktno iz definicija. Q.E.D.

Propozicija 3.1.32. *Neka je V mnogostrukost u $\mathbb{P}^n$ i neka je $H_\infty \subseteq V$. Tada je $V = \mathbb{P}^n$ ili $V = H_\infty$. Ako je $V = \mathbb{P}^n$ onda je $V_* = \mathbb{A}^n$, a ako je $V = H_\infty$, onda je $V_* = \emptyset$.*

Dokaz. Pretpostavimo da je $V \neq \mathbb{P}^n$. Tada je $\emptyset \neq I = I(V) \subseteq (X_{n+1})$. Dakle, dovoljno je pokazati da je $X_{n+1} \in I$. Za svaki $F \in I$ postoji $G \in K[X_1, X_2, \ldots, X_{n+1}]$ takav da je $F = X_{n+1}G$. Kako je I prost ideal, zaključujemo da je $G \in I$ ili $X_{n+1} \in I$. Odaberimo $F \neq 0$, tada vidimo da ćemo nakon konačno koraka dobiti da je $X_{n+1} \in I$, točnije polinom $F \neq 0$ ne možemo beskonačno dijeliti s X_{n+1}. Ovime je pokazana prva tvrdnja. Druga tvrdnja proizlazi direktno iz definicija. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Iz dijelova (1) i (7) propozicije 3.1.29, a i iz prethodne propozicije vidimo da postoji prirodna bijekcija između afinih mnogostrukosti i projektivnih mnogostrukosti koje nisu sadržane u H_∞.

Neka je V afina mnogostrukost i V^* njezin projektivni zatvarač. Neka je $f \in \Gamma_h(V^*)$ homogen stupnja $d \in \mathbb{Z}_{\geq 0}$. Definirajmo $f_* \in \Gamma(V)$ na sljedeći način. Neka je F homogen polinom, stupnja d, u $K[X_1, X_2, \ldots, X_{n+1}]$ takav da je njegova slika u $\Gamma_h(V^*)$ jednaka f te definirajmo f_* kao sliku polinoma F_* u $\Gamma(V)$. Lako se vidi da ovo ne ovisi o izboru predstavnika F, stoga je ovakva definicija dobra.

Definiramo prirodni izomorfizam $\alpha : K(V^*) \to K(V)$:

$$\alpha\left(\frac{f}{g}\right) = \frac{f_*}{g_*},$$

za bilo koja dva homogena, istog stupnja, $f, g \in K(V^*)$. Nadalje, svaku točku $P \in V$ možemo smatrati točkom u V^*, jednostavnu gledamo $\varphi_{n+1}(P)$. Tada vidimo da α inducira izomorfizam između $\mathcal{O}_P(V^*)$ i $\mathcal{O}_P(V)$.

Napomena 3.1.33. *Uvijek ćemo koristiti oznaku α za izomorfizam između $K(V^*)$ i $K(V)$, odnosno, između $\mathcal{O}_P(V^*)$ i $\mathcal{O}_P(V)$.*

Svaka projektivna mnogostrukost, V, je pokrivena s $n+1$ skupova oblika $V \cap U_k$, gdje je $k = 1, 2, \ldots, n+1$. Možemo konstruirati V_k u odnosu na U_k (kao što smo do sada to radili s U_{n+1}), tada će točke na $V \cap U_k$ biti u vezi s točkama u V_* te, također, lokalni prsteni će biti izomorfni. Dakle, sva pitanja (na koja se može dati odgovor samo gledajući $\mathcal{O}_P(V)$) o mnogostrukosti V u blizini neke njene točke P se svode na pitanja o afinoj mnogostrukosti V_* u blizini točke $P\left(=\varphi_k^{-1}(P)\right)$.

Za kraj iskažimo i dokažimo još jednu lemu koja će nam biti od koristi u nastavku.

Lema 3.1.34. *Za svaki konačan skup točaka u $\mathbb{P}^2$ postoji pravac koji ne prolaziti kroz niti jednu od tih točaka.*

Dokaz. Kako je samo konačno točaka, možemo pretpostaviti da niti jedna od njih nije jednaka $(0:0:1)$ (ako je potrebno napravimo projektivnu zamjenu koordinata). No, kako je polje beskonačno, to postoji beskonačno pravaca oblika $\left\{(x:y:z) \in \mathbb{P}^2 \ : \ x + ky = 0\right\}$, gdje je $k \in K$. Jasno je da možemo odabrati k tako da niti jedna točka iz danog (konačnog) skupa točaka ne zadovoljava jednadžbu. $\mathfrak{Q.E.D.}$

3.2 Ravninske krivulje i Bézoutov teorem

Definicija 3.2.1. *Za dva homogena polinoma $F, G \in K[X, Y, Z]$ kažemo da su* ***ekvivalentni*** *ako je $F = \lambda G$ za neki $0 \neq \lambda \in K$.* ***Projektivna ravninska krivulja*** *je odgovarajuća klasa ekvivalencije nekog nekonstantnog homogenog polinoma u $K[X, Y, Z]$.*

Definiramo analogno sve stvari kao u početku sekcije 2.4. Nadalje, znamo da ako je $P = (x : y : 1)$, onda je $\mathcal{O}_P(F)$ izomorfno s $\mathcal{O}_{(x,y)}(F_*)$, gdje je $F_* = F(X, Y, 1)$ odgovarajuća afina ravninska krivulja. Prisjetimo se skupova

$$U_k = \left\{(x_1 : x_2 : x_3) \in \mathbb{P}^2 \ : \ x_k \neq 0\right\}, \ k = 1, 2, 3.$$

Definicija 3.2.2. *Neka je F projektivna ravninska krivulja i neka je P točka iz $\mathbb{P}^2$ koja se nalazi u nekom U_k, $k = 1, 2$ ili 3. Dehomogeniziramo (prisjetimo se rasprave neposredno prije propozicije 2.3.6) polinom F u odnosu na varijablu X_k te definiramo* ***multiplicitet*** *krivulje F u točki P kao $m_P(F) = m_P(F_*)$.*

Primijetimo da nam teorem 2.4.8 govori da prethodna definicija ne ovisi o odabiru skupa U_k, također, invarijantna je u odnosu na projektivnu zamjenu koordinata. Promotrimo sada konačan skup točaka $P_1, P_2, \ldots, P_n \in \mathbb{P}^2$, gdje je $n \in \mathbb{N}$. Prema lemi 3.1.34 postoji pravac L koji ne prolazi niti jednom od tih točaka. Ako je F krivulja stupnja d, formalno stavljamo da je $F_* = \dfrac{F}{L^d} \in K\left(\mathbb{P}^2\right)$. Primijetimo da F_* ovisi o izboru pravca L. No, ako je L' neki drugi takav pravac, onda je $\dfrac{F}{L'^d} = \left(\dfrac{L}{L'}\right)^d F_*$, a $\dfrac{L}{L'}$ je invertibilni element u svakom od lokalnih prstena $\mathcal{O}_{P_k}\left(\mathbb{P}^2\right)$, gdje je $k \in \{1, 2, \ldots, n\}$. Nadalje, uvijek možemo napraviti projektivnu zamjenu koordinata tavku da niti jedna o točaka P_k ne leži na pravcu u beskonačnosti, točnije, možemo pretpostaviti da je $L = Z$. Sada vidimo da nam je F_*, uz prirodnu identifikaciju $K\left(\mathbb{A}^2\right)$ s $K\left(\mathbb{P}^2\right)$ (napomena 3.1.33) zapravo jednak "starom" $F_* = F(X, Y, 1)$.

Definicija 3.2.3. *Neka su F i G projektivne ravninske krivulje i neka je $P \in \mathbb{P}^2$. Definiramo* ***multiplicitet presjeka*** *$I(P, F \cap G)$ kao $\dim_K\left(\mathcal{O}_P\left(\mathbb{A}^2\right)/(F_*, G_*)\right)$.*

Iz diskusije prije definicije vidimo da je nebitno kako smo konstruirali F_* i G_*. Također, jasno je da su zadovoljena sva svojstva (1)-(7) iz definicije 2.5.2 uz sitne modifikacije. Naime, u točki (3), T mora biti projektivna zamjena koordinata, dok je u točki (5) bitno da je polinom A homogen stupnja $\deg(G) - \deg(F)$. Primjer 2.5.6 nam motivira sljedeću definiciju.

Definicija 3.2.4. *Definiramo da je pravac L* ***tangenta*** *na krivulju F u točki P ako je $I(P, F \cap L) > m_P(F)$. Točka P krivulje F je* ***jednostavna višestruka točka*** *krivulje F ako krivulja F ima $m_P(F)$ različitih tangenti u točki P.*

Za dvije projektivne ravninske krivulje F i G kažemo da su **projektivno ekvivalentne** ako postoji projektivna zamjena koordinata takva da je $G = F^T$. Jasno, sve što smo rekli i što ćemo još reći za krivulje će biti invarijantno u odnosu na projektivne zamjene koordinata. Sada ćemo navesti jednu lemu koja će nam zatim pomoći u dokazu Bézoutovog teorema.

Lema 3.2.5. *Projektivne ravninske krivulje F i G koje nemaju zajedničkih komponenti sijeku se u konačnom broju točaka.*

Dokaz. Neka je S skup točaka u kojima se sijeku krivulje F i G. Pretpostavimo da je S beskonačan. Tada je, barem za jedan $k \in \{1, 2, 3\}$, skup $S \cap U_k$ također beskonačan, zato što je $U_1 \cup U_2 \cup U_3 = \mathbb{P}^2$. Dehomogenizirajmo polinome F i G u odnosu na varijablu X_k. Dobivamo polinome F_* i G_* u dvije varijable koji se sijeku u beskonačno mnogo točaka. Prema propoziciji 1.6.7 to znači da oni nisu relativno prosti. No, onda nam propozicija 2.3.6 govori da ni polinomi F i G nisu relativno prosti, a to je kontradikcija. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Projektivnu ravninu smo konstruirali s ciljem da nam se svaka dva različita pravca sijeku u jednoj točki. Bézoutov teorem će nam reći još i puno više od toga.

Teorem 3.2.6 (Bézoutov teorem)**.** *Neka su F i G projektivne ravninske krivulje, stupnja m, odnosno n. Ako F i G nemaju zajedničkih komponenti, onda je*

$$\sum_{P \in \mathbb{P}^2} I(P, F \cap G) = mn.$$

Dokaz. Prema prethodnoj lemi znamo da je skup $F \cap G$ konačan, stoga možemo pretpostaviti (napravimo projektivnu zamjenu koordinata ako je potrebno) da niti jedna od zajedničkih točaka krivulja F i G ne leži na pravcu u beskonačnosti, $Z = 0$. Neka su F_* i G_* dehomogenizacije polinoma F i G u odnosu na varijablu Z. Tada, prema svojstvu (9) multipliciteta presjeka (definicija 2.5.2), znamo da je

$$\sum_{P \in \mathbb{P}^2} I(P, F \cap G) = \sum_{P \in \mathbb{A}^2} I(P, F_* \cap G_*) = \dim_K \left(K[X, Y] / (F_*, G_*)\right).$$

Uvedimo oznake

$$R = K[X, Y, Z], \qquad \Gamma = R/(F, G), \qquad \Gamma_* = K[X, Y]/(F_*, G_*).$$

Za $d \in \mathbb{Z}_{\geq 0}$ neka je R_d vektorskih prostor homogenih polinoma stupnja d u R, slično, u Γ neka je to Γ_d. Tvrdimo da vrijedi da je $\dim_K \Gamma_d = mn$ te $\dim_K \Gamma_* = \dim_K \Gamma_d$, za svaki $d \geq m + n$. Pokažemo li to jasno je da smo gotovi. Sada dokaz provodimo u dva koraka.

- $\dim_K \Gamma_d = mn$. Neka je $\pi : R \to \Gamma$ kanonski epimorfizam te neka su $\varphi : R \times R \to R$ i $\psi : R \to R \times R$ definirani kao

$$\varphi(A, B) = AF + BG, \qquad \psi(C) = (GC, -FC).$$

Pokažimo da je sljedeći niz egzaktan, $0 \to R \xrightarrow{\psi} R \times R \xrightarrow{\varphi} R \xrightarrow{\pi} \Gamma \to 0$. Kako F i G nemaju zajedničkih komponenti jasno je da je i $F \neq 0$ i $G \neq 0$, iz ovoga vidimo da je ψ injekcija. Ako su $A, B \in R$ takvi da je $\varphi(A, B) = 0$, vidimo da mora biti $BG = -AF$. Opet, kako F i G nemaju zajedničkih komponenti vidimo da $F \mid B$ i $G \mid A$, što znači da postoje $C_1, C_2 \in R$ takvi da je $A = GC_1$ i $B = -FC_2$. No, iz $-FC_2G = -GC_1F$ vidimo da je $C_1 = C_2 = C \in R$. Dakle, $\operatorname{Ker}(\varphi) = \operatorname{Im}(\psi)$. Jasno je da je, za $D \in R$, $\pi(D) = 0$ ako i samo ako je D oblika $AF + BG$, gdje su $A, B \in R$. Dakle, $\operatorname{Ker}(\pi) = \operatorname{Im}(\varphi)$, jasno je da je π surjekcija. Ovime smo pokazali da je niz egzaktan. Promatrajmo sada taj niz na odgovarajućim restrikcijama, točnije, promatrajmo

$$0 \to R_{d-m-n} \xrightarrow{\psi} R_{d-m} \times R_{d-n} \xrightarrow{\varphi} R_d \xrightarrow{\pi} \Gamma_d \to 0.$$

Iz dijela (b) propozicije 2.3.8 znamo da je $\dim_K R_d = \dfrac{(d+1)(d+2)}{2}$, sada pomoću (b) dijela propozicije 2.3.29 uz račun dobivamo da je $\dim_K \Gamma_d = mn$.

- $\dim_K \Gamma_* = \dim_K \Gamma_d$. Neka je $\alpha : \Gamma \to \Gamma$ definirana s $\alpha\left(\overline{H}\right) = \overline{ZH}$, za svaki $H \in R$. Ovdje je s $\overline{H}$ označena slika polinoma H u Γ. Tvrdimo da je α injekcija. Dakle, trebamo pokazati da ako je $ZH = AF + BG$, za neke $A, B \in R$ da je onda $H = A'F + B'G$ za neke $A', B' \in R$. Za bilo koji polinom $D \in K[X, Y, Z]$ neka je $D_0 = D(X, Y, 0)$. Dakle, imamo

da je $B_0G_0 = -A_0F_0$. Kako F, G i Z nemaju niti jednu zajedničku nultočku i F i G su relativno prosti, zaključujemo da su i F_0 i G_0 relativno prosti. Sada kao i u prethodnom koraku zaključujemo da postoji $C \in K[X, Y]$ takav da je $A_0 = G_0C$ i $B_0 = -F_0C$. Definirajmo $A_1 = A - CG$ i $B_1 = B + FC$. Vidimo da je $(A_1)_0 = (B_1)_0 = 0$ pa zaključujemo da postoje A', $B' \in R$ takvi da je $A_1 = ZA'$ i $B_1 = ZB'$. Konačno, kako je $ZH = A_1F + B_1G$, zaključujemo da je $H = A'F + B'G$. Dakle, α je injekcija. Nadalje, za $d \geq m + n$ znamo da Γ_d i Γ_{d+1} imaju jednaku dimenziju, stoga, ukoliko promatramo restrikciju od α na Γ_d vidimo da je $\alpha : \Gamma_d \to \Gamma_{d+1}$ izomorfizam (linearna injekcija između dva konačno dimenzionalna vektorska prostora jednakih dimenzija). Neka su $A_1, A_2, \ldots, A_{mn} \in R_d$ takvi da njihove slike u Γ_d čine bazu za Γ_d. Zaključujemo da slike od $Z^rA_1, Z^rA_2, \ldots, Z^rA_{mn}$ u Γ_{d+r} čine bazu za Γ_{d+r}, za svaki $r \in \mathbb{Z}_{\geq 0}$. Konačno, neka je, za svaki $k \in \{1, 2, \ldots, mn\}$,

$$A_{k*} = A_k(X, Y, 1) \in K[X, Y] \text{ i neka je } a_k \text{ slika od } A_{k*} \text{ u } \Gamma_*.$$

Tvrdimo da $a_1, a_2, \ldots, a_{mn}$ tvore bazu za Γ_*. Pokažemo li to, gotovi smo! Provedimo to u dva koraka.

Nezavisni su. Pretpostavimo da su $\lambda_1, \lambda_2, \ldots, \lambda_{mn} \in K$ takvi da je $\sum_{k=1}^{mn} \lambda_k a_k = 0$. To znači da je $\sum_{k=1}^{mn} \lambda_k A_{k*} = BF_* + CG_*$, za neke $B, C \in K[X, Y]$. Sada, prema propoziciji 2.3.6 vidimo da postoje $r, s, t \in \mathbb{Z}_{\geq 0}$ takvi da je $Z^r \sum_{k=1}^{mn} \lambda_k A_k = Z^sB^*F + Z^tC^*G$. Što znači da je $\sum_{k=1}^{mn} \lambda_k \overline{Z^rA_k} = 0$, u Γ_{d+r}, a kako je to linearna kombinacija vektora koji tvore bazu za Γ_{d+r}, zaključujemo da je $\lambda_1 = \lambda_2 = \ldots = \lambda_{mn} = 0$.

Generatori su. Neka je $h \in \Gamma_*$ i neka je $H \in K[X, Y]$ takav da je $\overline{H} = h$ u Γ_*. Postoji $N \in \mathbb{Z}_{\geq 0}$ takav da je Z^NH* homogen polinom stupnja $d + r$, za neki $r \in \mathbb{Z}_{\geq 0}$. No, to znači da postoje $\lambda_1, \lambda_2, \ldots, \lambda_{mn} \in K$ i $B, C \in R$ takvi da je $Z^NH^* = \sum_{k=1}^{mn} \lambda_k Z^rA_k + BF + CG$. No, $H = \left(Z^NH^*\right)_*$, tj. $H = \sum_{k=1}^{mn} \lambda_k A_{k*} + B_*F_* + C_*G_*$, tj. $h = \sum_{k=1}^{mn} \lambda_k a_k$. Q.E.D.

Sljedeći korolari slijede direktno iz Bézoutovog teorema, jedino u prvom treba još iskoristiti svojstvo (7) multipliciteta presjeka, iz definicije 2.5.2, stoga ih navodimo bez dokaza.

Korolar 3.2.7. *Ako projektivne ravninske krivulje F i G nemaju zajedničkih komponenti, onda je*

$$\sum_{P\in\mathbb{P}^2} m_P(F)\, m_P(G) \leq \deg(F)\cdot\deg(G).$$

Korolar 3.2.8. *Ako se projektivne ravninske krivulje F i G sijeku u točno mn različitih točki, gdje je $m = \deg(F)$ i $n = \deg(G)$, onda su sve te točke regularne točke i krivulje F i krivulje G.*

Korolar 3.2.9. *Ako dvije projektivne ravninske krivulje stupnjeva m i n imaju više od mn zajedničkih točaka, onda one imaju zajedničku komponentu.*

Poglavlje 4

Afine i projektivne krivulje

4.1 Projektivni i afini prostori

Iako su neki od pojmova iz ovog poglavlja već definirani ranije, radi konzistentnosti ćemo ponoviti definicije projektivnih i afinih prostora te dati neke osnovne rezultate.

Neka je dan skup P čije elemente ćemo zvati točkama i neka je K polje za koje do kraja pretpostavljamo da je algebarski zatvoreno.

Definicija 4.1.1. ***n-dimenzionalni projektivni koordinatni sustav*** *nad K u P jest odnos između točaka skupa P i uređenih $(n+1)$-torki elemenata polja K takvih da vrijedi:*

(i) svaka točka odgovara barem jednoj $(n+1)$-torci $(a_0, a_1, \ldots, a_n)$ takvoj da je $a_i \neq 0$ barem za jedan $i \in \{0, 1, \ldots, n\}$,

(ii) svaka $(n+1)$-torka $(a_0, a_1, \ldots, a_n)$ takva da barem za jedan $i \in \{0, 1, \ldots, n\}$ vrijedi $a_i \neq 0$, odgovara točno jednoj točki iz P,

(iii) $(a_0, a_1, \ldots, a_n)$ i $(b_0, b_1, \ldots, b_n)$ odgovaraju istoj točki ako i samo ako postoji $\lambda \in K \setminus \{0\}$ takva da je $a_i = \lambda b_i$, za sve $i \in \{0, 1, \ldots, n\}$.

Kako bi naglasili svojstvo (iii) prethodne definicije, koordinate točaka u projektivnom koordinatnom sustavu u daljnjem označavamo s $(a_0 : a_1 : \ldots : a_n)$, gdje $(a_0, a_1, \ldots, a_n)$ odgovara danoj točki.

Definicija 4.1.2. *Dva su projektivna koordinatna sustava* ***ekvivalentna*** *ukoliko postoji regularna matrica $A = [a_{ij}]_{0\leq i,j\leq n}$ takva da za svaku točku $x \in P$ vrijedi:*

$$y_j = a_{ij}x_i, \quad i \in \{0, 1, \ldots, n\},$$

gdje su $(x_0 : x_1 : \ldots : x_n)$ i $(y_0 : y_1 : \ldots : y_n)$ koordinate točke x u prvom, odnosno drugom koordinatnom sustavu.

Uočimo da je definicija dobra. Naime, lako se provjeri da se, ukoliko imamo jedan projektivni koordinatni sustav u P i regularnu matricu A, relacijom $y_j = a_{ij}x_i$ opet dobiva projektivni koordinatni sustav u P.

Direktnom provjerom po definiciji se vidi da vrijedi sljedeća lema.

Lema 4.1.3. *Ekvivalentnost projektivnih koordinatnih sustava je relacija ekvivalencije.*

Definicija 4.1.4. ***n-dimenzionalni projektivni prostor*** *nad K, u oznaci $\mathbb{P}^n$, je skup P zajedno sa klasom ekvivalencije n-dimenzionalnih koordinatnih sustava u P nad K.*

Kako se točke projektivne ravnine u danom koordinatnom sustavu označavaju kao $(n + 1)$-torke, možemo definirati linearnu zavisnost točaka na intuitivan način. Reći ćemo da je skup točaka projektivne ravnine linearno zavisan ako i samo ako su koordinate tih točaka linearno zavisne. Definicija ne ovisi o izboru koordinatnog sustava, jer množenje matrica stupaca regularnom matricom, ne mijenja linearnu nezavisnost.

Teorem 4.1.5. *Neka su dane $n + 2$ točke u projektivnoj ravnini $\mathbb{P}^n$ takve da nijednih $n + 1$ točaka nisu linearno nezavisne. Tada postoji jedinstveni koordinatni sustav u kojem te točke redom imaju koordinate*

$$(1 : 0 : \ldots : 0), (0 : 1 : \ldots : 0), \ldots, (0 : 0 : \ldots : 1), (1 : 1 : \ldots : 1).$$

Dokaz. Neka točke $P_0, \dots P_{n+1}$, imaju koordinate $\left(a_0^j : a_1^j : \dots : a_n^j\right)$. Definiramo matricu $A = \left[a_i^j\right]_{0\le i,j\le n}$. Kako su stupci matrice A koordinate prvih $n+1$ točaka, a one su linearno nezavisne, slijedi da je A regularna. Označimo s $B = \left[b_{ij}\right]_{0\le i,j\le n}$ njen inverz. Jasno je da je B također regularna. Tada zamjenom koordinata $y_j = \sum_{i=0}^{n} b_{ij}x^i$ dobivamo ekvivalentan koordinatni sustav u kojem točke $P_0, \dots, P_n$ imaju koordinate

$$(1 : 0 : \dots : 0), (0 : 1 : \dots : 0), \dots, (0 : 0 : \dots : 1).$$

Neka u novom koordinatnom sustavu točka P_{n+1} ima koordinate $(c_0 : c_1 : \dots : c_n)$. Kako P_{n+1} nije linearno zavisna niti o jednom n-članom podskupu prvih $n+1$ točaka, mora vrijediti $c_i \neq 0$ za sve $0 \le i \le n$. Definiramo matricu $C = \left[c_{ij}\right]_{0\le i,j\le n}$, takvu da je $c_{ii} = 1/c_i$, a $c_{ij} = 0$ ako je $i \neq j$, te novu zamjenu koordinata $z_j = \sum_{i=0}^{n} c_{ij}y_i$.

C je regularna pa je novi koordinatni sustav ekvivalentan prethodnom, a zbog tranzitivnosti relacija ekvialencije, i polaznom koordinatnom sustavu. Jasno je da točka P_{n+1} ima koordinate $(1 : 1 : \dots : 1)$, a jer se koordinate točaka P_i samo množe faktorima $1/c_i$, iz definicije projektivnog koordinatnog sustava slijedi da koordinate točaka $P_0, \dots, P_n$ ostaju iste. Time je teorem dokazan. Q.E.D.

Napomena 4.1.6. *$(n+2)$-torku točaka kao iz prethodnog teorema zove se* ***referentni okvir****, a prvih $n+1$ točaka* ***referentni vrhovi****. Posebno, u $\mathbb{P}^2$ skup referentnih vrhova ćemo zvati* ***fundamentalni trovrh****.*

Promotrimo sada sljedeću situaciju. Neka je P' podskup od $\mathbb{P}^n$ čije su sve točke linearno zavisne o točkama $P_0, P_1, \dots, P_r$. Tada postoje točke $P_{r+1}, \dots, P_n$ takve da su $P_0, P_1, \dots, P_n$ linearno nezavisne. Definiramo koordinatni sustav kojemu te točke čine referentni okvir i tada je jasno da sve točke iz P' imaju koordinate $(x_0 : x_1 : \dots : x_n)$ takve da je $x_{r+1} = \dots = x_n = 0$. Time je definirana relacija između P' i skupa svih $r+1$ torki za koju vrijede sva svojstva iz definicije 4.1.1 pa prema tome ona definira r-dimenzionalni projektivni prostor $\mathbb{P}^r$ čije točke su točke skupa P'.

Definicija 4.1.7. *Gore opisani projektivni prostor $\mathbb{P}^r$ zovemo* ***r-dimenzionalni linearni potprostor*** *ili samo* ***potprostor*** *od $\mathbb{P}^n$.*

Koristeći gornju konstrukciju, lako se dokazuje sljedeća lema i njena direktna posljedica:

Lema 4.1.8. *Neka je $\mathbb{P}^r$ potprostor projektivnog prostora $\mathbb{P}^n$. Tada za svaki koordinatni sustav od $\mathbb{P}^r$ postoji koordinatni sustav od $\mathbb{P}^n$ u kojem se koordinate točaka potprostora sastoje od koordinata u polaznom koordinatnom sustavu popraćenih s $n - r$ nula.*

Lema 4.1.9. *Ukoliko je $\mathbb{P}^r$ potprostor projektivnog prostora $\mathbb{P}^n$, tada su točke potprostora $\mathbb{P}^r$ linearno nezavisne u $\mathbb{P}^r$ ako i samo ako su nezavisne u $\mathbb{P}^n$.*

Teorem 4.1.10. *$r + 1$ linearno nezavisnih točaka leže u jednom i samo jednom potprostoru od $\mathbb{P}^n$ dimenzije r.*

Dokaz. Neka su $P_0, \ldots, P_r$ linearno nezavisne točke. Po definiciji slijedi da postoji barem jedan potprostor $\mathbb{P}^r$ koji sadrži svih $r + 1$ točaka. Ukoliko je $\tilde{\mathbb{P}}^n$ neki drugi potprostor koji sadrži točke $P_0, \ldots, P_r$, tada on sadrži i sve njhove linearne kombinacije, pa sadrži i cijeli $\mathbb{P}^r$. Analogno vrijedi i obratna inkluzija.

Provjerimo još da su koordinatni sustavi ovih dviju prostora ekvivalentni. Neka je x točka koja u $\mathbb{P}^n$ ima koordinate $(x_0 : x_1 : \ldots : x_r)$, a u $\tilde{\mathbb{P}}^n$ koordinate $(y_0 : y_1 : \ldots : y_r)$. Tada lema 4.1.8 osigurava da postoje koordinatni sustavi projektivnog prostora $\mathbb{P}^n$ u kojima x ima koordinate $(x_0 : \ldots : x_r : 0 : \ldots : 0)$, odnosno $(y_0 : \ldots : y_r : 0 : \ldots : 0)$. Kako se radi o ekvivalentnim koordinatnim sustavima, vrijedi $y_j = \sum_{i=0}^{n} a_{ij} x_i$, za sve $0 \leq j \leq n$, tj.

$$y_j = \sum_{i=0}^{r} a_{ij} x_i, \quad 0 \leq j \leq r$$

jer su zadnjih $n - r$ koordinata jednake nula u oba koordinatna sustava. Još ostaje primjetiti da je matrica $A = \left[a_{ij}\right]_{0 \leq i,j \leq r}$ regularna, jer bi u suprotnom točke $P_0, \ldots, P_r$ bile zavisne u y-koordinatama a to je kontradikcija. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Dualnost

Definicija 4.1.11. *$(n-1)$-dimenzionalni potprostor projektivnog prostora $\mathbb{P}^n$ zovemo **hiperravnina**.*

Neka je hiperravnina π u projektivnom prostoru $\mathbb{P}^n$ dana linearno nezavisnim točkama P_i, $i \in \{0, 1, \ldots, n-1\}$ s koordinatama $\left(a_0^i : a_1^i : \ldots : a_n^i\right)$. Tada sustav jednadžbi

$$\sum_{j=0}^{n} a_j^i x_j = 0$$

ima jedinstveno (do na množenje ne–nul skalarom) netrivijalno rješenje $(b_0, b_1, \ldots, b_n)$.

Kako je svaka točka $Q = (c_0 : c_1 : \ldots : c_n)$ hiperravnine π linearna kombinacija točaka P_i, vrijedi $\sum_{j=0}^{n} b_j c_j = 0$. S druge strane, jednadžba $\sum_{j=0}^{n} b_j x_j = 0$ ima $n-1$ linearno nezavisnih rješenja, a sva ostala rješenja su linearne kombinacije tih rješenja. Kako točke P_i zadovoljavaju jednadžbu, zadovoljavaju ju i sve linearne kombinacije tih točaka, dakle sve točke hiperravnine π.

Prema tome, uz zadani projektivni koordinatni sustav, svakoj hiperravnini π pridružena je do na konstantan faktor različit od nula, jedinstvena $n+1$-torka $(b_0, b_1, \ldots, b_n)$ takva da je skup točaka hiperravnine jednak skupu netrivijalnih rješenja jednadžbe

$$\sum_{i_0}^{n} b_i x_i = 0.$$

Tu jednadžbu zovemo **jednadžba hiperravnine**.

Lako se provjeri da odnos između skupa svih hiperravnina danog projektivnog prostora i koordinata hiperravnina zadovoljava definiciona svojstva iz 4.1.1. Prema tome, klase ekvivalencije ovako definiranih projektivnih koordinatnih sustava zajedno sa skupom hiperravnina čine n-dimenzionalni projektivni prostor.

Definicija 4.1.12. *Projektivni prostor definiran kao u gornjem odjeljku se zove **dualni** projektivni prostor prostora $\mathbb{P}^n$ i označava s $\mathbb{P}^{n*}$.*

Napomena 4.1.13. *Direktno se provjeri da je definicija dobra, tj. da se isti dualni projektivni prostor dobije neovisno o polaznom projektivnom koordinatnom sustavu.*

Često je korisno hiperravnine promatrati kao elemente dualnog projektivnog prostora, umjesto kao podskupove projektivnog prostora. Zato uvodimo još nekoliko pojmova.

Definicija 4.1.14. *Ako je projektivni koordinatni sustav u $\mathbb{P}^{n*}$ dobiven iz projektivnog koordinatnog sustava u $\mathbb{P}^n$ na gore opisani način, reći ćemo da su ti koordinatni sustavi* ***odgovarajući****.*

Definicija 4.1.15. *Neka točka P ima koordinate $(a_0 : a_1 : \ldots : a_n)$ u $\mathbb{P}^n$, a hiperravnina π koordinate $(b_0 : b_1 : \ldots : b_n)$ u odgovarajućem koordinatnom sustavu u $\mathbb{P}^{n*}$. Kažemo da su P i π* ***incidentni*** *ako vrijedi $\sum_{i=0}^{n} a_i b_i = 0$.*

Teorem 4.1.16. *Skup hiperravnina projektivnog prostora $\mathbb{P}^n$ koje sadrže potprostor $\mathbb{P}^r$ odgovara potprostoru $\mathbb{P}^{(n-r-1)*}$.*

Dokaz. Neka nezavisne točke $P_i = \left(a_0^i : a_1^i : \ldots : a_n^i\right)$, $i \in \{0, 1, \ldots r\}$ razapinju $\mathbb{P}^r$. Hiperravnina s koordinatama $(b_0,\ b_1,\ \ldots,\ b_n)$ sadrži $\mathbb{P}^r$ ako i samo ako je incidentna s $P_0, \ldots, P_r$, a to je ako i samo ako vrijede jednakosti

$$\sum_{j_0}^{n} a_j^i b_j = 0 \quad 0 \leq i \leq r.$$

Zbog nezavisnosti točaka P_i, ovaj sustav ima točno $n - r - 1$ linearno nezavisnih rješenja $\pi_0, \ldots \pi_{n-r}$ pa primjenom teorema 4.1.10 slijedi tvrdnja. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Koristan je sljedeći teorem, dual teorema 4.1.5

Teorem 4.1.17. *Neka je dano $n + 2$ hiperravnina projektivne ravnine $\mathbb{P}^n$ takvih da nijednih $n + 1$ nisu nezavisne. Tada postoji jedinstveni koordinatni sustav u kojem te hiperravnine redom imaju jednadžbe $x_0 = 0$, $x_1 = 0$, …, $x_n = 0, x_0 + x_1 = \ldots + x_n = 0$.*

Afini prostori

Neka je dan projektivni prostor $\mathbb{P}^n$ nad skupom S. Odaberemo jednu hiperravninu π u tom prostoru, te projektivne koordinate u kojima je π dana jednadžbom $x_0 = 0$.

Definicija 4.1.18. *n-dimenzionalni afini koordinatni sustav nad S je bijekcija između točaka skupa $\mathbb{P}^n \setminus \pi$ i svih n-torki takva da vrijedi:*

- *ako su $(a_0 : a_1 : \ldots : a_n)$ projektivne koordinate točke P, njene afine koordinate su $(a_1/a_0,\ a_2/a_0,\ \ldots,\ a_n/a_0)$.*

Hiperravninu π zovemo ***hiperravnina u beskonačnosti****.*

Definicija 4.1.19. *Kažemo da su dva afina koordinatna sustava* ***ekvivalentna*** *ako postoji regularna matrica $A_{ij} = \left[a_{ij}\right]_{1\le i,j\le n}$ i vektor $[b_1, \ldots b_n]^T$ takvi da su za svaku točku projektivne ravnine, njene afine koordinate u dva sustava $(x_1,\ x_2,\ \ldots,\ x_n)$ i $(y_1,\ y_2,\ \ldots,\ y_n)$ vezane jednakostima*

$$y_i = \sum_{j=1}^{n} a_{ij}x_j + b_i, \quad 1 \le i \le n.$$

Ekvivalentno, dva afina koordinatna sustava su ekvivalentna ako su dobivena od dvaju ekvivalentnih projektivnih sustava sa istom hiperravninom u beskonačnosti. Ova tvrdnja se direktno provjerava iz definicija.

Definicija 4.1.20. *Točke projektivne ravnine $\mathbb{P}^n$ koje ne leže u hiperravnini π zajedno sa klasom ekvivalencije afinih koordinatnih sustava tvore n-**dimenzionalni afini prostor** $\mathbb{A}^n$ nad K.*

Neka je $\mathbb{A}^n$ afini prostor u $\mathbb{P}^n$ sa hiperravninom u beskonačnosti π, te neka je $\mathbb{P}^r$ linearni potprostor od $\mathbb{P}^n$ koji ne leži u π. Odaberemo projektivni koordinatni sustavi u $\mathbb{P}^n$ kao u lemi 4.1.8, i kako hiperravnina ima jednadžbu oblika $\sum_{i=0}^{n} a_i x_i$ za neke $a_0, \ldots, a_n$ ne sve jednake nula, vidi se da točke potprostora $\mathbb{P}^r$ koje leže na π čine hiperravninu π' u $\mathbb{P}^r$.

Prema tome, točke od $\mathbb{P}^r$ koje leže u $\mathbb{A}^n$ su samo točke skupa $\mathbb{P}^r \setminus \pi'$ pa mogu biti shvaćene kao poseban afini prostor koji označavamo s $\mathbb{A}^r$ i nazivamo **linearni potprostor** ili samo potprostor afinog prostora $\mathbb{A}^n$.

Direktna posljedica odnosa između projektivnih i afinih koordinata je da hiperravnina u afinom prostoru također ima linearnu jednadžbu, no ona općenito nije homogena.

4.2 Afine krivulje

Definicija 4.2.1. ***Afina krivulja*** *u ravnini (dalje u tekstu samo krivulja) je skup svih točaka afine ravnine koje zadovoljavaju jednadžbu*

$$f(x, y) = 0,$$

gdje je $f \in K[x, y]$. *Takvu afinu krivulju označavamo s* $V(f)$.

Dakle, afina krivulja je zapravo hiperploha u afinoj ravnini (a to je afini prostor dimenzije 2).

Promotrimo sada proizvoljnu krivulju $V(f)$, $f \in K[x, y]$. Kako je $K[x, y]$ domena jedinstvene faktorizacije, polinom f možemo (na jedinstven način) rastaviti na produkt ireducibilnih polinoma: $f = f_1^{n_1} f_2^{n_2} \dots f_k^{n_k}$.

Napomena 4.2.2. *U gornjem zapisu, polinomi* f_i, $i \in \{1, 2, \dots, k\}$ *su međusobno različiti i broj* n_i *zovemo* ***multiplicitetom*** *ireducibilnog faktora* f_i *polinoma* f.

Lako se vidi da vrijedi

$$V(f) = V(f_1) \cup V(f_2) \cup \dots \cup V(f_k) = V(f_1 \dots f_k).$$

Prema tome, svakoj afinoj krivulji C pridružen je jedinstven polinom f_C oblika $f_C = f_1 \cdots f_k$, gdje su f_i, $i \in \{1, 2, \dots, k\}$, međusobno različiti ireducibilni polinomi.

Definicija 4.2.3. *Reći ćemo da je polinom $f \in K[x, y]$* ***pridružen*** *afinoj krivulji ako za svaku točku (x, y) te krivulje vrijedi $f(x, y) = 0$, te ako je f polinom čiji su svi ireducibilni faktori multipliciteta 1.*

Definicija 4.2.4. ***Stupanj afine krivulje*** *se definira kao stupanj polinoma koji je pridružen danoj krivulji.*

Posebno, krivulja stupnja 2 naziva se **konika**, a krivulja stupnja 3 **kubika**.

Definicija 4.2.5. *Afina krivulja je* ***ireducibilna*** *ukoliko je polinom kojim je zadana ireducibilan.*

Lema 4.2.6. *Neka je K polje, $f \in K[x, y]$ ireducibilni polinom, te $g \in K[x, y]$ bilo koji polinom. Ako f ne dijeli g, tada sustav jednadžbi*

$$f(x, y) = g(x, y) = 0$$

ima najviše konačno mnogo rješenja.

Dokaz. Pretpostavimo da je x u raspisu polinoma f pozitivnog stupnja. Naime, nemoguće je da su i x i y stupnja nula, jer tada f ne bi bio ireducibilan. Promatramo polinome f i g kao elemente prstena $K(y)[x]$. Po teoremu 1.2.19 slijedi da je f ireducibilan u $K(y)[x]$, te po korolaru 1.2.20 da u istom prstenu vrijedi i $f \nmid g$. Dakle, po [12], strana 140, Theorem 3.11. (ii), postoje $u', v' \in K(y)[x]$ takvi da vrijedi $u'f + v'g = 1$. Neka je sada $a \in K[y]$ najmanji zajednički višekratnik nazivnika racionalnih funkcija u' i g'. Dobivamo jednakost u $K[x, y]$

$$uf + vg = a,$$

gdje je $u = au'$ i $v = av'$, $u, v \in K[x, y]$. Ukoliko je (α, β) neko rješenje danog sustava, tj. ako vrijedi $f(\alpha, \beta) = g(\alpha, \beta) = 0$, tada je i $a(\beta) = 0$, što (jer polinom u jednoj varijabli ima najviše konačno nultočaka) znači da postoji samo konačno mnogo mogućnosti za β. Sada

za svaki takav β promatramo polinom $b \in K[x]$ definiran s $b(x) = f(x, \beta)$. Ako bi b bio identički jednak nuli, tada bi f bio djeljiv s $y - \beta$, što je u kontradikciji s ireducibilnošću te početnom pretpostavkom (da je x pozitivnog stupnja). Zaključujemo da postoji samo konačno mogućnosti i za α. Q.E.D.

4.3 Krivulje u projektivnoj ravnini

Definicija 4.3.1. *Neka je F ireducibilan homogen polinom stupnja n u $K[x_0, x_1, x_2]$. Skup točaka*

$$C = \left\{(a) = (a_0 : a_1 : a_n) \in \mathbb{P}^2 \mid F(a_0, a_1, a_2) = 0\right\}$$

zovemo ***ireducibilna algebarska krivulja*** *stupnja n određena polinomom F, a polinom F* ***polinom pridružen*** *toj krivulji.*

Za algebarsku krivulju C iz definicije često ćemo reći da je krivulja određena polinomom F, odnosno da je polinom F pridružen danoj krivulji.

Primjetimo da je definicija dobra. Naime, koordinate iste točke se razlikuju do na faktor različit od nule pa ukoliko su $(a_0 : a_1 : a_2)$ i $(\lambda a_0 : \lambda a_1 : \lambda a_2)$ dvoje koordinate iste točke, tada je $F(\lambda a_0, \lambda a_1, \lambda a_2) = \lambda^n F(a_0, a_1, a_2)$.

Napomenimo još da se polinomi pridruženi istoj krivulji razlikuju do na konstantan faktor, i obratno, ukoliko se polinomi razlikuju na konstantan faktor, tada definiraju istu algebarsku krivulju.

Nadalje, napravimo li zamjenu koordinatnog sustava takvu da vrijedi $x_i = \sum_{j=0}^{2} a_j i y_j$, gdje je $i \in \{0, 1, 2\}$, a matrica $\left[a_{ij}\right]_{0 \le i,j \le 2}$, tada je polinom

$$G(y_0, y_1, y_2) = F\left(\sum_{j=0}^{2} a_{j0} y_j, \sum_{j=0}^{2} a_{j1} y_j, \sum_{j=0}^{2} a_{j2} y_j\right)$$

pridružen istoj krivulji u novom koordinatnom sustavu.

Opet, kako je $K[x_0, x_1, x_2]$ domena jedinstvene faktorizacije, proizvoljan homogeni polinom F se, do na poredak jedinstven način, rastavlja na produkt ireducibilnih polinoma $F = F_1 F_2 \dots F_m$. Netrivijalna je činjenica da su tada i $F_1, \dots, F_m$ također homogeni i dokaz se može naći u [24], strana 28, Theorem 10.5. Neka su $C_1, \dots C_m$ ireducibilne algebarske krivulje određene polinomima $F_1, \dots F_m$.

Definicija 4.3.2. *Uz oznake iz gornjeg odjeljka, skup točaka određen jednadžbom $F = 0$, ili ekvivalentno, uniju ireducibilnih krivulja $C_1, \dots C_m$ nazivamo* ***algebarska krivulja*** *određena polinomom F, a ireducibilne krivulje $C_1, \dots, C_n$* ***komponentama*** *krivulje C.*

Veza između algebarskih i afinih krivulja

Neka je dana algebarska krivulja C određena polinomom F. Odaberemo projektivni koordinatni sustav takav da $x_0 = 0$ nije komponenta od F, te definiramo afini koordinatni sustav kojemu je $x_0 = 0$ pravac u beskonačnosti. Stavimo $x = \dfrac{x_1}{x_0}$ i $y = \dfrac{x_2}{x_0}$ i definiramo $f(x, y) := F(1, x, y)$. Afinu krivulju definiranu polinomom f nazivamo **afinom reprezentacijom** krivulje C.

Nultočke jednadžbe $f(x, y) = 0$ odgovaraju svim točkama krivulje C osim točaka u beskonačnosti. Dakle, afina reprezentacija krivulje je nepotpuna u odnosu na početnu krivulju jer ne sadrži točke u beskonačnosti. Sloboda izbora pravca u beskonačnosti omogućuje postojanje afine reprezentacije svake algebarske krivulje.

Obratno, ukoliko je jednandžbom $f(x, y) = 0$, gdje je $f \in K[x, y]$ stupnja n, zadana afina krivulja, definiramo homogeni polinom $F \in K[x_0, x_1, x_2]$

$$F(x_0, x_1, x_2) = x_0^n f\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right).$$

Za algebarsku krivulju $F(x_0, x_1, x_2) = 0$ kažemo da je **projektivizacija** dane afine krivulje.

4.4 Rezultanta dvaju polinoma

Prije nastavka, uvodimo pojam rezultante polinoma, koji će biti intenzivno korišten u nastavku.

Definicija 4.4.1. *Neka je D faktorijalan prsten karakteristike nula i neka su $f, g \in D[x]$ oblika*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0.$$

Rezultanta *polinoma f i g se definira kao determinanta $(m+n) \times (m+n)$ matrice tj.*

$$Res(f,g) = \begin{vmatrix} a_0 & a_1 & a_2 & . & . & . & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & . & . & 0 & 0 \\ \vdots & \vdots & \vdots & & & & \vdots & \vdots \\ 0 & 0 & 0 & . & . & . & a_{n-1} & a_n \\ b_0 & b_1 & b_2 & . & . & . & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & . & . & 0 & 0 \\ \vdots & \vdots & \vdots & & & & \vdots & \vdots \\ 0 & 0 & 0 & . & . & . & b_{m-1} & b_m \end{vmatrix}$$

Uz ove oznake vrijedi teorem koji dajemo bez dokaza.

Teorem 4.4.2. *Polinomi f i g imaju zajednički faktor stupnja većeg od 0 ako i samo ako je $Res(f,g) = 0$.*

Dokaz. Dokaz se može naći u [18]. Q.E.D.

Ovaj teorem najveću primjenu ima u situaciji kada je K algebarski zatvoreno polje, a $D = K[x_1, \ldots x_{r-1}]$. Tada je, za polinome $f, g \in D[x_r] = K[x_1, \ldots, x_r]$, njihova rezultanta polinom nad K u varijablama $x_1, \ldots, x_{r-1}$.

Definicija 4.4.3. ***Rezultanta polinoma*** $f, g \in K[x_1, \ldots, x_r]$ ***u odnosu na varijablu*** x_i, *u oznaci* $Res_{x_i}(f, g)$, *jest rezultanta polinoma* f *i* g *promatranih kao elementi prstena* $K[x_1, \ldots x_{i-1}, x_{i+1}, \ldots, x_r][x_i]$.

Tada teorem 4.4.2 povlači da f i g imaju zajednički faktor pozitivnog stupnja u x_r ako i samo ako je $Res_{x_r}(f, g) = 0$ u $K[x_1, \ldots, x_{r-1}]$. Ovo ima jednostavnu posljedicu koja će nam biti potrebna. Ako su $\alpha_1, \ldots, \alpha_{r-1} \in K$ i polinomi $f, g \in K[x_1, \ldots, x_r]$ koji su pozitivnih stupnjeva u x_r, onda jednostavnim računom slijedi da vrijedi jednakost

$$Res\left(f(\alpha_1, \ldots, \alpha_{r-1}, x_r), g(\alpha_1, \ldots, \alpha_{r-1}, x_r)\right) = Res_{x_r}(f, g)(\alpha_1, \ldots, \alpha_{r-1}).$$

Iskoristimo li sada teorem 4.4.2, vidimo da ako su $\alpha_1, \ldots, \alpha_{r-1} \in K$ i vrijedi

$$Res_{x_r}(f, g)(\alpha_1, \ldots, \alpha_{r-1}) = 0,$$

tada (zbog algebarske zatvorenosti polja K) slijedi da postoji $\alpha_r \in K$ takav da je

$$f(\alpha_1, \ldots, \alpha_r) = g(\alpha_1, \ldots, \alpha_r) = 0.$$

Definicija 4.4.4. ***Diskriminanta*** *polinoma* $f \in D[x]$ *se definira kao* $Res(f, f') \in D$.

Korolar 4.4.5. *Polinom* $f \in D[x]$ *ima ireducibilan faktor pozitivnog stupnja multipliciteta većeg ili jednakog* 2 *ako i samo ako je diskriminanta polinoma* f *jednaka nula.*

Primjetimo da je, u slučaju da je D polje, zahtjev teorema o faktoru pozitivnog stupnja suvišan jer u polju nema ireducibilnih elemenata, pa su svi ireducibilni elementi u $D[x]$ nužno pozitivnog stupnja.

4.5 Singulariteti

Neka je afina krivulja C zadana polinomom $f \in K(x, y)$ stupnja n. Promatramo točku P s afinim koordinatama (a, b). Za $i \in \{0, 1, \ldots, n+1\}$ definiramo polinome

$$f_i(x, y) = \sum_{j=0}^{i} \frac{\delta^i f}{\delta x^j y^{i-j}}(a, b) \cdot (x-a)^j (y-b)^{i-j}.$$

Tada je Taylorov razvoj polinoma f oko točke (a, b) jednak:

$$f(x, y) = \sum_{i=0}^{n} f_i(x, y).$$

Suma je konačna jer zbog stupnja polinoma f vrijedi $f_i = 0$, za sve $i \geq n+1$.

Definicija 4.5.1. *Kažemo da je točka (a, b) krivulje C **multipliciteta** r ili r**-terostruka**, ukoliko vrijedi $f_0 = f_1 = \ldots = f_{r-1} = 0$ u $K[x, y]$, ali $f_r \neq 0$. Točke multipliciteta većeg od 1 zovu se **singularne** točke.*

Kako je f_r homogen stupnja r, točno r točaka $(x-a : y-b)$ zadovoljava jednakost $f_r = 0$, pa se, jer je K algebarski zatvoreno, taj polinom može rastaviti na linearne faktore.

Definicija 4.5.2. *Ukoliko je (a, b) r-terostruka točka krivulje $f(x, y) = 0$ i $r \geq 2$, linearne faktore polinoma f_r definiranog kao gore nazivamo **tangentama** te krivulje u točki (a, b).*

Iz definicije je jasno da vrijedi sljedeći teorem.

Teorem 4.5.3. *Ako polinom $f \in K[x, y]$ nema članove stupnja manjeg od r, ali ima one stupnja r, tada je ishodište r-terostruka točka krivulje zadane polinomom f. Nadalje, tangente te krivulje u ishodištu su komponente krivulje definirane polinomom koji se sastoji samo od članova polinoma r koji su stupnja r.*

Definicija 4.5.4. *Ukoliko su tangente u singularnoj točki dane krivulje međusobno različite, kažemo da je singularitet **jednostavan**. U suprotnom ćemo reći da je singularitet **složen**.*

4.6 Sjecišta krivulja

Teorem 4.6.1. *Neka je dana algebarska krivulja C stupnja n. Tada za svaki pravac vrijedi da je ili komponenta krivulje C ili siječe C u točno n točaka, brojeći multiplicitete.*

Napomena 4.6.2. *U iskazu gornjeg teorema, ne moraju sve točke presjeka biti međusobno različite. Na primjer, ukoliko krivulja ima dvostruku komponentu, sjecište pravca s tom komponentom se broji dva puta.*

Dokaz. Neka je krivulja C dana polinomom $F \in K[x_0, x_1, x_2]$. Odaberimo pravac i dvije njegove različite točke $(a) = (a_0 : a_1 : a_2)$ i $(b) = (b_0 : b_1 : b_2)$. Tada svaka točka pravca ima koordinate $x_i = sa_i + tb_i \quad i \in \{0, 1, 2\}$, za neke $s, t \in K$. Primjetimo da su $(s : t)$ zapravo projektivne koordinate točke u projektivnom prostoru u danom pravcu (zadovoljena su sva tri definiciona svojstva).

Promotrimo polinom $G(s, t) := F(sa + tb)$. G je homogen polinom stupnja n. Ukoliko je G identički jednak nuli, tada sve točke danog pravca leže u C, tj. taj je pravac komponenta od C.

U suprotnom, G ima točno n nultočaka ([24], strana 29, Theorem 10.8) $(s : t)$, pri čemu r-terostruke nultočke brojimo kao r nultočaka. Svaki par $(s : t)$ odgovara točno jednoj točki danog pravca pa slijedi da pravac ima n zajedničkih točaka s C. $\mathfrak{Q.E.D.}$

Ukoliko krivulja nema višestrukih komponenata, prethodni teorem se može poboljšati.

Teorem 4.6.3. *Ako krivulja C stupnja n nema višestrukih komponenata, tada se kroz svaku točku P koja ne leži na C može povući pravac koji siječe C u n* različitih *točaka.*

Dokaz. Neka P ima koordinate $(0 : 0 : 1)$. Za pravac u beskonačnosti uzmemo $x_0 = 0$, te neka u pripadnom afinom prostoru krivulja C ima reprezentaciju $f(x, y) = 0$. Za svaki $\alpha \in K$ definiramo pravce L_α jednadžbama

$$x_1 = \alpha x_0,$$

te uočimo da točka P leži na svim L_α. Jednadžbe tih pravaca u pripadnim afinim koordinatama su $x = \alpha$.

Za svaki $\alpha \in K$ sjecišta pravca L_α i krivulje su nultočke polinoma $f(\alpha, y) \in K[y]$ koji je, jer točka $(0:0:1)$ ne leži na C, stupnja n. Pretpostavimo sada da za svaki $\alpha \in K$ taj polinom ima višestruki korijen. Označimo s $D = Res_y\left(f, \frac{\delta f}{\delta y}\right)$, tj. $D \in K[x]$ je diskriminanta polinoma f s obzirom na y. Onda je $D(\alpha)$ diskriminanta polinoma $f(\alpha, y)$ s obzirom na y, pa zbog pretpostavke, vrijedi $D(\alpha) = 0$ za svaki $\alpha \in K$. Zbog toga je $D = 0$ u $K[x]$, a to povlači da f ima višestruki faktor, što je kontradikcija.

Zaključimo, ako $\alpha \in K$ nije nultočka polinoma $D = Res_y\left(f, \frac{\delta f}{\delta y}\right) \in K[x]$, tada pravac L_α siječe krivulju C u n međusobno različitih točaka. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Teorem 4.6.4. *Neka krivulja C stupnja n nema višestrukih komponenata. Tada se kroz r-terostruku točku P te krivulje mogu provući pravci koji sijeku C u još $n - r$ međusobno različitih točaka.*

Dokaz. Neka je $P = (1:0:0)$ i za pravac u beskonačnosti uzmemo $x_0 = 0$. Tada je definirajući polinom za C u afinim koordinatama oblika:

$$f(x, y) = f_r(x, y) + f_{r+1}(x, y) + \ldots + f_n(x, y),$$

gdje su f_i homogeni polinomi stupnja i u $K[x, y]$, za $i \in \{r, r+1, \ldots, n\}$. U gornjem zapisu polinoma f nema članova f_i za $i < r$ jer je ishodište r-terostruka točka pa to slijedi direktno iz definicije singulariteta. Tada za $i \in \{r, \ldots, n\}$ postoje $a^i_j \in K$, $j \in \{0, \ldots, i\}$ takvi da je

$$f_i(x, y) = \sum_{j=0}^{i} a^i_j x^{i-j} y^j.$$

Projektivizacijom dobivamo polinom $F(x_0, x_1, x_2) = x_0^n f(x_1/x_0, x_2/x_0)$ tj.

$$F(x_0, x_1, x_2) = x_0^{n-r} \sum_{j=0}^{r} a^r_j x_1^{r-j} x_2^j + x_0^{n-r-1} \sum_{j=0}^{r+1} a^{r+1}_j x_1^{r+1-j} x_2^j + \ldots + \sum_{j=0}^{n} a^n_j x_1^{n-j} x_2^j.$$

Promatramo sada pravce oblika $y = \lambda x$ za $\lambda \in K$, koji u projektivnim koordinatama imaju oblik $x_2 = \lambda x_1$. Zanimaju nas sjecišta tih pravaca s krivuljom C, a njih ćemo dobiti uvrštavanjem:

$$F(x_0, x_1, \lambda x_1) = \left(\sum_{j=0}^{r} a_j^r \lambda^j\right) x_0^{n-r} x_1^r + \left(\sum_{j=0}^{r+1} a_j^{r+1} \lambda^j\right) x_0^{n-r-1} x_1^{r+1} + \ldots \left(\sum_{j=0}^{n} a_j^n \lambda^j\right) x_1^n =$$

$$x_0^n \left[\left(\sum_{j=0}^{r} a_j^r \lambda^j\right)\left(\frac{x_1}{x_0}\right)^r + \left(\sum_{j=0}^{r+1} a_j^{r+1} \lambda^j\right)\left(\frac{x_1}{x_0}\right)^{r+1} + \ldots \left(\sum_{j=0}^{n} a_j^n \lambda^j\right)\left(\frac{x_1}{x_0}\right)^n\right].$$

Prebacivanjem natrag u afine koordinate, uz $x = x_1/x_0$ kao i ranije, dobivamo

$$f(x, \lambda x) = F(1, x, \lambda x) = \left(\sum_{j=0}^{r} a_j^r \lambda^j\right) x^r + \left(\sum_{j=0}^{r+1} a_j^{r+1} \lambda^j\right) x^{r+1} + \ldots \left(\sum_{j=0}^{n} a_j^n \lambda^j\right) x^n = x^r g(x, \lambda),$$

gdje je

$$g(x, \lambda) = \left(\sum_{j=0}^{r} a_j^r \lambda^j\right) + \left(\sum_{j=0}^{r+1} a_j^{r+1} \lambda^j\right) x + \ldots \left(\sum_{j=0}^{n} a_j^n \lambda^j\right) x^{n-r}.$$

Kako faktor x^r određuje ishodište, tj. točku P, mi želimo dobiti $n - r$ međusobno različitih točaka presjeka koje su sve različite od P, tražimo λ takav da je polinom g stupnja $n - r$ koji nema višestrukih faktora u x i nije djeljiv s x. Ti su zahtjevi redom ekvivalentni sljedećim:

(i) $\displaystyle\sum_{j=0}^{n} a_j^n \lambda^j = f_n(1, \lambda) \neq 0$

(ii) $Res_x\left(g, \dfrac{\delta g}{\delta x}\right) \neq 0$

(iii) $\displaystyle\sum_{j=0}^{r} a_j^r \lambda^j = f_r(1, \lambda) \neq 0$

$Res_x\left(g, \dfrac{\delta g}{\delta x}\right)$ je polinom u λ pa se postavlja pitanje je li drugi zahtjev opravdan. Pretpostavimo da je rezultanta identički jednaka nuli. Tada polinom g ima višestruki faktor

koji ovisi o x pa postoje polinomi $h, k \in K[x, \lambda]$ takvi da vrijedi $g(x, \lambda) = h^2(x, \lambda)\, k(x, \lambda)$. No onda uz $x = x_1/x_0$ vrijedi

$$F\left(1, \frac{x_1}{x_0}, \lambda\frac{x_1}{x_0}\right) = \left(\frac{x_1}{x_0}\right)^r h^2\left(\frac{x_1}{x_0}, \lambda\right) k\left(\frac{x_1}{x_0}, \lambda\right),$$

iz čega slijedi jednakost

$$F(x_0, x_1, \lambda x_1) = x_1^r x_0^{n-r} h^2\left(\frac{x_1}{x_0}, \lambda\right) k\left(\frac{x_1}{x_0}, \lambda\right).$$

Zbog $\lambda = \dfrac{x_2}{x_1}$ sada konačno vrijedi

$$F(x_0, x_1, x_2) = x_1^r x_0^{n-r} h^2\left(\frac{x_1}{x_0}, \frac{x_2}{x_1}\right) k\left(\frac{x_1}{x_0}, \frac{x_2}{x_1}\right) = x_1^r x_0^{n-r} g\left(\frac{x_1}{x_0}, \frac{x_2}{x_1}\right),$$

a to je polinom u varijablama x_0, x_1, x_2 jer najviši stupanj koji varijabla x_0 poprima u nazivniku od $g\left(\dfrac{x_1}{x_0}\right)$ je $n - r$, a najviši stupanj od x_1 u nazivniku iste racionalne funkcije je manji ili jednak n. Slijedi da F ima višestruki faktor, a to je kontradikcija. Dakle, $Res_x\left(g, \dfrac{\delta g}{\delta x}\right)$ nije identički jednaka nuli.

Konačno, zaključujemo da ukoliko $\lambda \in K$ nije nultočka polinoma

$$f_r(1, \lambda)\, f_n(1, \lambda)\, Res_x\left(g, \frac{\delta g}{\delta x}\right),$$

gdje je $g(x, \lambda) = x^{-r} f(x, \lambda x)$, tada pravac $x_2 = \lambda x_1$ siječe krivulju u $n - r$ točaka različitih od P i različitih međusobno.

$\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Teoremi 4.6.3 i 4.6.4 su nam od velike važnosti. Zbog konstruktivnosti njihovih dokaza, imamo sada precizne uvijete koje pravci moraju zadovoljavati da bi sjekli danu krivulju u međusobno različitim točkama, što će se pokazati vrlo korisno u prvim koracima algoritma predstavljenog u radu. Prethodni teoremi su dali neke tvrdnje o presjeku krivulje i pravca, a u nastavku dajemo nekoliko rezultata o presjecima dviju krivulja.

Teorem 4.6.5 (Bezout)**.** *Ako dvije krivulje, redova m i n imaju više od mn zajedničkih točaka, onda imaju zajedničku komponentu.*

Dokaz. Neka je krivulja reda n dana polinomom F, a krivulja reda m polinomom G. Odaberimo bilo kojih $mn+1$ zajedničkih točaka tih krivulja, i svaki par tih točaka spojimo pravcem. Tih spojnica ima konačno mnogo pa postoji točka P takva da ne leži niti na jednoj, i ne leži ni na krivuljama F i G. Odaberimo koordinatni sustav u kojem P ima koordinate $(0:0:1)$. Tada je

$$F(x_0, x_1, x_2) = A_n x_2^n + \sum_{i=0}^{n-1} A_i(x_0, x_1)\, x_2^i$$

$$G(x_0, x_1, x_2) = B_m x_2^m + \sum_{i=0}^{m-1} B_i(x_0, x_1)\, x_2^i,$$

gdje su A_n i B_m konstante različite od nula, A_i, $i \in \{0, \ldots, n-1\}$ homogeni polinomi stupnja $n-i$, a B_i, $i \in \{0, \ldots, m-1\}$ homogeni polinomi stupnja $m-i$. Rezultanta polinoma F i G s obzirom na varijablu x_2 je ili nula ili polinom u x_0 i x_1 stupnja mn.

$Res_{x_2}(c_0, c_1) = 0$ ako i samo ako postoji c_2 takav da je $F(c_0, c_1, c_2) = G(c_0, c_1, c_2) = 0$. Ukoliko bi postojale dvije različite točke zajedničke danim dvjema krivuljama, s koordinatama $(c_0 : c_1 : c_2)$ i $(d_0 : d_1 : d_2)$ takvima da vrijedi $c_0 = \lambda d_0$ i $c_1 = \lambda d_1$, za neki $\lambda \in K$, tada bi točka P ležala na njihovoj spojnici, a to je nemoguće. Prema tome, $Res_{x_2}(x_0, x_1)$ se poništava u barem $mn+1$ različitih točaka, što znači da je identički jednaka nuli, a to opet povlači da F i G imaju zajednički faktor. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Teorem 4.6.6. *Neka su dvije krivulje dane polinomima oblika:*

$$F(x_0, x_1, x_2) = A_n x_2^n + \sum_{i=0}^{n-1} A_i(x_0, x_1)\, x_2^i$$

$$G(x_0, x_1, x_2) = B_m x_2^m + \sum_{i=0}^{m-1} B_i(x_0, x_1)\, x_2^i,$$

gdje su A_n i B_m konstante različite od nula, A_i, $i \in \{0, \ldots, n-1\}$ homogeni polinomi stupnjeva $n-i$, a B_i, $i \in \{0, \ldots, m-1\}$ homogeni polinomi stupnjeva $m-i$. Neka je $P = (a_0 : a_1 : a_2)$ točka multipliciteta r za krivulju danu s F, a multipliciteta s za krivulju danu s G. Pretpostavimo još da rezultanta $Res_{x_2}(x_0, x_1)$ s obzirom na varijablu x_2 nije identički jednaka nuli. Tada je $(a_0 : a_1)$ nultočka te rezultante multipliciteta barem rs.

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti da P ima koordinate $(1 : 0 : 0)$. Pokažimo to. Kako točka $(0, 0, 1)$ ne leži na danim krivuljama, ne može biti $a_0 = a_1 = 0$, pa možemo pretpostaviti da je na primjer $a_0 \neq 0$. Definiramo zamjenu koordinata

$$x_0' = x_0/a_0 \quad x_1' = x_1 - a_1 x_0/a_0 \quad x_2' = x_2.$$

U novim koordinatama točka P postaje $(1 : 0 : a_2)$, polinomi F i G zadržavaju isti oblik, u smislu da se mijenjaju samo polinomi A_i, $i \in \{0, \ldots, n-1\}$ i B_j, $j \in \{0, \ldots, m-1\}$. Nadalje, rezultanta u novim koordinatama postaje $Res_{x_2'}(a_0 x_0', x_1' + a_1 x_0')$ i $(1 : 0)$ je nultočka istog multipliciteta kao nultočka $(a_0 : a_1)$ polinoma $Res_{x_2}(x_0,\ x_1)$.

Promotrimo sada rezultantu s obzirom na varijablu x_2 polinoma $F(x_0, x_1, x_2 + \lambda x_0)$ i $G(x_0, x_1, x_2 + \lambda x_0)$. Dobivamo polinom

$$Res_{x_2}(x_0, x_1, \lambda) = \sum_{i=0}^{N} C_i(x_0, x_1)\, \lambda^i.$$

Primjetimo da je $C_0(x_0, x_1) = R(x_0, x_1, 0) = Res_{x_2}(F, G) \neq 0$. Pretpostavimo da je $N > 0$ i $C_n \neq 0$. Tada postoje konstante b_0, b_1 takve da je $C_0(b_0, b_1)\, C_N(b_0, b_1) \neq 0$. Kako je K algebarski zatvoreno, postoji $\lambda_0 \in K$ takva da je $R(b_0, b_1, \lambda_0) = 0$. Slijedi da polinomi $F(b_0, b_1, x_2 + \lambda_0 b_0)$ i $G(b_0, b_1, x_2 + \lambda_0 b_0)$ imaju zajedničku nultočku b_2. No onda polinomi $F(b_0, b_1, x_2)$ i $G(b_0, b_1, x_2)$ imaju zajednučku nultočku $b_2 + \lambda_0 b_0$, što je nemoguće jer je $Res_{x_2}(b_0, b_1, 0) = C_0(b_0, b_1 \neq 0)$. Zaključujemo da je $N = 0$, pa uz zamjenu koordinata

$$x_0' = x_0 \quad x_1' = x_1 \quad x_2' = x_2 - a_2 x_0,$$

točka P mijenja koordinate u $(1 : 0 : 0)$, a rezultanta novih polinoma ostaje ista kao i stara.

Prelaskom na afine koordinate (za pravac u beskonačnosti uzimamo $x_0 = 0$), polinomi F i G postaju

$$f(x, y) = \sum_{i=0}^{r} f_i(x) x^{r-i} y^i + f_{r+1}(x) y^{r+1} + \dots$$

$$g(x, y) = \sum_{i=0}^{r} g_i(x) x^{r-i} y^i + g_{r+1}(x) y^{r+1} + \dots$$

Ishodište je r-terostruka, odnosno s-terostruka nultočka polinoma f i g redom, pa su zato ti polinomi oblika danog u gornjim jednakostima.

Promotrimo rezultantu $Res_y(f, g)$. Pomnožimo li njen prvi redak sa x^s, drugi s x^{s-1} i tako dalje, zatim $(s+1)$-ti redak s x^r, $(s+2)$-ti s x^{r-1}, moći ćemo iz i-tog stupca izlučiti $x^{r+s+1-i}$, za $1 \leq i \leq r+s$.

$$\sum_{i=1}^{r+s} i - \sum_{i=1}^{r} i - \sum_{i=1}^{s} i = \dots = rs$$

Prema tome, $Res_y(f, g)$ je djeljiva s x^{rs}. Q.E.D.

Teorem 4.6.7. *Ako dvije krivulje reda m i n nemaju zajedničkih komponenata, no imaju zajedničke točke P_i multipliciteta r_i, odnosno s_i, tada vrijedi $\sum r_i s_i \leq mn$.*

Dokaz. Odaberemo koordinate potpuno jednako kao i u dokazu teorema 4.6.5. Tada su danim krivuljama pridruženi polinomi

$$F(x_0, x_1, x_2) = A_n x_2^n + \sum_{i=0}^{n-1} A_i(x_0, x_1) x_2^i$$

$$G(x_0, x_1, x_2) = B_m x_2^m + \sum_{i=0}^{m-1} B_i(x_0, x_1) x_2^i.$$

Po prethodnom teoremu, ako je $P_i = (a_0 : a_1 : a_2)$, tada je $(a_0 : a_1)$ nultočka rezultante $Res_{x_2}(F, G)$ multipliciteta barem $r_i s_i$. Zbog izbora koordinatnog sustava, različite točke zajedničke objema krivuljama, daju i različite $(a_0 : a_1)$ pa rezultanta ima barem

$\sum r_i s_i$ nultočaka, brojeći multiplicitete. S druge strane, po teoremu 4.6.5, ima najviše mn nultočaka. Time je teorem dokazan.

$\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Poglavlje 5

Racionalne krivulje

5.1 Definicija i karakterizacije

Definicija 5.1.1. *Ireducibilna afina krivulja* $V(f) = \left\{(x, y) \in \mathbb{A}^2 \ : \ f(x, y) = 0\right\}$ *je* ***racionalna*** *ukoliko postoje racionalne funkcije* $\varphi(t)$ *i* $\psi(t)$*, od kojih je barem jedna nekonstantna, takve da vrijedi*

$$f(\varphi(t), \psi(t)) = 0$$

u prstenu polinoma $K(t)$*.*

Često ćemo reći da je racionalna krivulja V **parametrizirana** racionalnim funkcijama φ i ψ.

Napomena 5.1.2. *Primjetimo da, ukoliko je* t_0 *takav da se niti jedan od nazivnika funkcija* φ *i* ψ *ne poništava u* t_0*, te ako vrijedi* $f(\varphi(t_0), \psi(t_0)) = 0$*, tada je točka* $(\varphi(t_0), \psi(t_0))$ *sadržana u krivulji* $V(f)$*.*

Neka je sada V ireducibilna krivulja i $f \in K[x, y]$ njoj pridružen (ireducibilan) polinom. Definiramo nekoliko novih pojmova:

Definicija 5.1.3. *Za racionalnu funkciju* $u(x,y) = \dfrac{p(x,y)}{q(x,y)}$, *gdje su* $p, q \in K[x,y]$ *kažemo da je* ***definirana na*** V *ako* q *nije djeljiv s* f.

Definicija 5.1.4. *Za dvije racionalne funkcije* $\dfrac{p_1}{q_1}$ *i* $\dfrac{p_2}{q_2}$ *definirane na* V *kažemo da su* ***jednake na*** V *ako* f *dijeli polinom* $p_1q_2 - q_1p_2$ *u* $K[x,y]$

Lako je provjeriti kako je jednakost na V relacija ekvivalencije. Nadalje, klase ekvivalencije koje ova relacija tvori čine polje.

Definicija 5.1.5. *Polje čiji su elementi klase ekvivalencije relacije jednakosti na* V *zovemo* ***polje racionalnih funkcija*** *ili* ***polje razlomaka na*** V *i označavat ćemo ga s* $K(V)$.

Racionalna funkcija $u(x,y) = \dfrac{p(x,y)}{q(x,y)}$ je definirana na svim točkama krivulje V, osim točaka koje su rješenja sustava $f(x,y) = q(x,y) = 0$, a po lemi 4.2.6 takvih točaka ima najviše konačno mnogo. Prema tome, elemente polja $K(V)$ možemo promatrati kao funkcije na V, definirane svuda, osim možda na konačnom skupu.

Definicija 5.1.6. *Za racionalnu funkciju na* V *kažemo da je regularna u točki* (x_0, y_0) *ukoliko postoje* $p, q \in K[x,y]$ *takvi da je* $u = \dfrac{p}{q}$ *i* $q(x_0, y_0) \neq 0$.

Kako bismo mogli dokazati Lürothov teorem koji će za posljedicu dati jednu važnu karakterizaciju pojma racionalne krivulje, nedostaje nam nekoliko pojmova.

Definicija 5.1.7. *Neka je dano polje* F. *Kažemo da je* α ***transcedentan*** *nad* F *ukoliko nije nultočka niti jednog ne-nul polinoma* $f \in F[x]$.

Definicija 5.1.8. *Za* L *kažemo da je* ***proširenje polja*** F, *u oznaci* $F \subset L$ *ukoliko je* F *potpolje od* L, *tj. ukoliko je* F *polje takvo da vrijedi* $F \subseteq L$.

Definicija 5.1.9. *Neka je* $F \subset L$. *Za podskup* $\{\alpha_1, \ldots, \alpha_n\} \subseteq L$ *kažemo da je* ***algebarski nezavisan*** *ako ne postoji nenul polinom* $g \in F[x_1, \ldots, x_n]$ *takav da je* $g(\alpha_1, \ldots, \alpha_n) = 0$.

Definicija 5.1.10. *Neka je $F \subset L$.* ***Baza transcedencije*** *je podskup L, algebarski nezavisan nad K, koji je maksimalan (u smislu inkluzije) u skupu svih algebarski nezavisnih podskupova od L.*

Napomena 5.1.11. *Da takav skup postoji slijedi direktno iz Zornove leme.*

Teorem 5.1.12 (**Lüroth**). *Neka je t transcedentan nad poljem K, te neka je L pravo proširenje polja K, sadržano u $K(t)$. Tada postoji u transcedentan nad K takav da je $L = K(u)$.*

Dokaz. Neka je $l = \dfrac{g(t)}{h(t)} \in L$ nekonstantan. Tada vrijedi $g(t) - lh(t) = 0$, tj. t je nultočka polinoma $g(x) - lh(x) = 0$ s koeficijentima u L. Prema tome, t je algebarski nad L pa postoji ireducibilan polinom $f \in L[x]$ takav da je $f(t) = 0$. Postoje racionalne funkcije u t takve da je $a_0(t), a_1(t), \ldots, a_r(t) \in L$, $r \in \mathbb{N}$, te da je

$$f(x) = a_0(t) + a_1(t)x + \ldots + a_r(t)x^r.$$

Označimo s $v(t)$ najmanji zajednički višekratnik nazivnika funkcija $a_0(t), a_1(t), \ldots, a_r(t)$, a s $d(t)$ najveći zajednički djelitelj njihovih brojnika. Imamo sljedeću jednadžbu:

$$\tilde{f}(t, x) = b_0(t) + b_1(t)x + \ldots + b_r(t)x^r,$$

uz $b_i = \dfrac{va_i}{d} \in K[t]$ za svaki $0 \leq i \leq r$. Kada bi $\tilde{f}$ imao faktor koji ovisi samo o t, to bi bilo u kontradikciji s izborom v i t.

Neka je $s \in \{0, 1, \ldots, r\}$ takav da $\dfrac{b_s(t)}{b_r(t)} \notin K$ (takav postoji iz konstrukcije koeficijenata $b_0, \ldots, b_r$) i definirajmo $u = \dfrac{b_s(t)}{b_r(t)} = \dfrac{a_s(t)}{a_r(t)} \in L$. Imamo jednakost

$$b_s(t) - ub_r(t) = 0,$$

što povlači da se polinom $b_s(x) - ub_r(x)$ poništava u t. Prema tome, f dijeli taj polinom u $L[x]$. Za neki $g \in L[x]$ imamo jednakost

$$b_s(x) - ub_r(x) = f(x)\, g(x).$$

Množenjem ove jednakosti s $b_r(t)$ dobivamo

$$b_s(x)\,b_r(t) - b_r(x)\,b_s(t) = a_r(t)g(x)\,\tilde{f}(x) = \tilde{g}(x)\,\tilde{f}(x),$$

gdje je $\tilde{g}(x) = \dfrac{b_r(t)\,d(t)}{v(t)}g(x) \in K(t)[x]$. No, kako je lijeva strana polinom, a $\tilde{f}$ nije djeljiv niti jednim polinomom u t, mora vrijediti da je i $\tilde{g}$ polinom.

Kako su $b_s(t)$ i $b_r(t)$ koeficijenti polinoma $\tilde{f}$, gledanog nad x, stupanj od t u svakom od njih je manji ili jednak stupnju t u $\tilde{f}$. No to dalje povlači da se t ne pojavljuje u $\tilde{g}$. Zbog simetrije lijeve strane posljednje jednakosti, $\tilde{g}$ mora biti konstantan. Zaključujemo da je $b_s(x) - ub_r(x)$ polinom nad $K(u)$ stupnja r, čija je t nultočka, tj. t je stupnja najviše r nad poljem $K(u)$.

Konačno, jasno je da vrijedi $K(u) \subseteq L$. Kada ne bi vrijedila jednakost, postojao bi neki $s \in L$, $s \notin K(u)$. Taj s je ujedno i element od $K(t)$, a prema prethodnom paragrafu je t stupnja manjeg ili jednakog r nad $K(u)$ pa postoji zapis

$$s = c_0 + c_1 t + \ldots + c_{r-1}t^{r-1},$$

gdje su $c_i \in K(u)$. Ova jednakost dalje povlači da je t stupnja manjeg od r nad L što je kontradikcija. Prema tome $L = K(u)$. Q.E.D.

Korolar 5.1.13. *Krivulja V je racionalna ako i samo ako su polja racionalnih funkcija na V i na $\mathbb{P}^1$ izomorfna nad K.*

Dokaz. Jasno je iz definicije da je polje racionalnih funkcija na $\mathbb{P}^1$ jednako polju racionalnih funkcija u jednoj varijabli. Neka je V ireducibilna krivulja s pridruženim polinomom u dvije varijable f i neka je parametrizirana s $\varphi, \psi \in K(t)$. Definirajmo preslikavanje s $K(V)$ u $K(t)$ koje racionalnoj funkciji na V $u(x,y)$ pridružuje racionalnu funkciju jedne varijable $u(\varphi(t), \psi(t))$. Provjerimo dobru definiranost pridruživanja.

Neka je $u = \dfrac{p}{q}$, $p, q \in K[x,y]$. i pretpostavimo da je $q(\varphi(t), \psi(t)) = 0$ u $K(t)$. Kako je polje K algebarski zatvoreno, jednadžba $\varphi(t) = x$ ima konačno mnogo rješenja za svaki

x iz K. Analogno jednadžba $\psi(t) = y$ ima konačno mnogo rješenja za svaki y iz K. Prema tome, uvrštavanjem beskonačno vrijednosti za t u jednadžbu $q(\varphi(t), \psi(t)) = 0$, uz činjenicu $f(\varphi(t), \psi(t)) \equiv 0$, lema 4.2.6 povlači da f dijeli q u $K[x, y]$, što je kontradikcija. Nadalje, ukoliko su racionalne funkcije $\frac{p_1}{q_1}$ i $\frac{p_2}{q_2}$ jednake, tada postoji polinom $g \in K[x, y]$ takav da vrijedi $p_1 q_2 - p_2 q_1 = fg$. Sada se jednostavno vidi da ovo pridruživanje racionalnim funkcijama jednakim na V pridružuje iste vrijednosti.

Očito je ovo preslikavanje monomorfizam sa polja racionalnih funkcija na krivulji V u polje $K[t]$, tj. $K(V)$ je izomorfno nekom potpolju od $K(t)$. Lürathov teorem sada daje dovoljnost.

Obratno, neko je $K(V)$ izomorfno nad K polju racionalnih funkcija $K(t)$. Neka taj izomorfizam varijablama x i $y$pridružuje $\varphi(t)$, odnosno $\psi(t)$. Izomorfizam čuva jednadžbu $f(x, y) = 0$, tj. vrijedi $f(\varphi(t), \psi(t)) = 0$. Dakle, V je racionalna. $\mathfrak{Q.E.D.}$

Napomena 5.1.14. *Karakterizacija iz prethodnog korolara je zapravo standardna definicija racionalnih krivulja u algebarskoj geometriji. Općenito, za algebarsku mnogostrukost dimenzije d kažemo da je racionalna ako joj je polje racionalnih funkcija izomorfno nad K polju racionalnih funkcija na $\mathbb{P}^d$. U sluč aju $d = 1$ korolar 5.1.13 sada povlači da su definicija 5.1.1 i ova standardna definicija ekvivalentne pa je upotreba definicije 5.1.1 u ovom radu opravdana.*

Napomenimo još da u slučaju $d \geq 2$ ekvivalencije između definicije racionalnih funkcija i poopćenja definicije 5.1.1 iz ovog rada nema. Problem ekvivalencije ovih dviju definicija naziva se Lürothov problem.

Neka je V racionalna krivulja i neka je $f \in K(x, y)$ njoj pridružen polinom. Prema prethodnom korolaru, njezino polje razlomaka $K(V)$ izomorfno je polju $K(t)$. Neka ovaj izomorfizam pridružuje $x \to \varphi(t)$, te $y \to \psi(t)$. Time je dana jedna parametrizacija.

Propozicija 5.1.15. *Gore definirana parametrizacija $x = \varphi(t)$, $y = \psi(t)$ ima sljedeća svojstva:*

(i) Za svaku točku $x_0, y_0 \in V$ osim njih konačno mnogo, postoji t_0 takav da vrijedi $(x_0,\ y_0) = (\varphi(t_0),\ \psi(t_0))$.

(ii) Osim za konačno mnogo točaka, taj t_0 je jedinstven.

Dokaz. Neka je $\chi(x, y)$ funkcija koja se preko izomorfizma $K(V) \to K(t)$ preslikanva u t. Tada vrijedi:

$$x = \varphi(\chi(x, y)), y = \psi(\chi(x, y)) \tag{5.1}$$

$$t = \chi(\varphi(t), \psi(t)) \tag{5.2}$$

Uzmimo $(x_0,\ y_0) \in V$. Kako je $\chi = \dfrac{p}{q} \in K(V)$, q i f su relativno prosti, a to povlači (zbog 4.2.6) da je jednakost

$$f(x_0,\ y_0) = q(x_0,\ y_0)$$

zadovoljena najviše za konačno mnogo $(x_0,\ y_0)$. Također, $\chi(x_0,\ y_0)$ može biti nultočka nazivnika od φ i ψ za najviše konačno točaka $(x_0,\ y_0)$. Prema tome, možemo staviti

$$t_0 = \chi(x_0,\ y_0)$$

i tada iz jednakosti 5.1 slijedi

$$(x_0,\ y_0) = (\varphi(t_0),\ \psi(t_0)).$$

Da je t_0 jedinstveno određen, osim za konačno $(x_0,\ y_0)$ za koje je $q(x_0,\ y_0) = 0$, na isti način slijedi iz jednakosti 5.2. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

5.2 Dovoljan uvjet za racionalnost krivulje

Svaka krivulja reda n u projektivnoj ravnini $\mathbb{P}^2$ ima zapis $\sum a_{ijk}x_0^i x_1^j x_2^k$, gdje se sumira po svim $i, j, k \in \mathbb{N}$ takvima da je $i + j + k = n$. Taj zapis je jedinstven do na zajednički faktor koeficijenata krivulje. Prema tome, krivulje možemo promatrati kao elemente projektivne ravnine $\mathbb{P}^N$, pri čemu koeficijenti a_{ijk} predstavljaju projektivne koordinate dane krivulje i $N = n(n + 3)/2$. Sljedeća lema pokazuje da je odabir projektivne ravnine jedinstven.

Lema 5.2.1. *Zamjenom koordinatnog sustava u $\mathbb{P}^2$ dobivamo ekvivalentne koordinatne sustave u $\mathbb{P}^N$.*

Dokaz. Neka je zamjena koordinata u $\mathbb{P}^2$ definirana s $x_i = \sum_{\alpha=0}^{2} A_{i\alpha}y_\alpha$ za $i = 0, 1, 2$. Tada krivulja $\Sigma a_{ijk}x_0^i x_1^j x_2^k$ u novim koordinatama postaje

$$\sum a_{ijk}\left(\sum_{\alpha=0}^{2} A_{0\alpha}y_\alpha\right)^i\left(\sum_{\alpha=0}^{2} A_{1\alpha}y_\alpha\right)^j\left(\sum_{\alpha=0}^{2} A_{2\alpha}y_\alpha\right)^k = \sum b_{pqr}y_0^p y_1^q y_2^r,$$

gdje je $b_{pqr} = \sum M_{ijk}^{pqr}a_{ij}k$, i svaki M_{ijk}^{pqr} polinom u $A_{00}, A_{01}, \ldots, A_{2,2}$. Determinanta ove transformacije je različita od nule jer se istim postupkom se možemo vratiti sa y u x. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Definicija 5.2.2. *Za krivulje koje razapinju potprostor $\mathbb{P}^R$ od $\mathbb{P}^N$ kažemo da tvore **linearni sustav** dimenzije R.*

Jasno, linearni sustav je jednoznačno određen s $R + 1$ linearno nezavisnih krivulja, te ako pripadajuće polinome tih krivulja označimo s $F_0(x), \ldots, F_R(x)$, svaka krivulja iz $\mathbb{P}^R$ je oblika

$$\sum_{i=0}^{n} \lambda_i F_i(x),$$

gdje su $\lambda_i \in K$.

S druge strane, zbog dualnosti, $\mathbb{P}^R$ se može zadati i kao presjek $N - R$ hiperravnina. Jednadžbu hiperravnine u $\mathbb{P}^N$ zovemo **linearni uvjet na krivulju reda n**. Kako N hi-

perravnina uvijek imaju barem jednu zajedničku točku, uvijek se može naći krivulja koja zadovoljava N ili manje linearnih uvjeta.

Posebno zanimljiv tip linearnih uvjeta se dobiva zahtjevom da dana točka leži na krivulji, te je multipliciteta barem r. Nužan i dovoljan uvjet na takvu krivulju jest da su sve parcijalne derivacije reda manjeg od r u danoj točki jednake nula, a takvih derivacija ima $r(r+1)/2$.

Definicija 5.2.3. *Za danu točku kao u gornjem odjeljku kažemo da je* ***bazna točka multipliciteta*** r. *Baznu točku multipliciteta* 1 *zovemo* ***jednostavna*** *bazna točka.*

Teorem 5.2.4. *Neka je dana krivulja V reda n koja nema višestrukih komponenata. Ukoliko su multipliciteti točaka P_i krivulje V jednaki r_i, tada vrijedi nejednakost*

$$n(n-1) \geq \sum r_i(r_i - 1).$$

Dokaz. Neka je F polinom pridružen krivulji V. Odaberemo koordinatni sustav tako da fundamentalne točke $(1:0:0)$, $(0:1:0)$, $(0:0:1)$ ne leže na V. Tada parcijalna derivacija $F_0 := \dfrac{\delta F}{\delta x_0}$ nije identički jednaka nula. U suprotnom, F ne bi ovisio o x_0 pa bi $(1:0:0)$ ležala na V.

Kako F nema višestrukih komponenti postoje ireducibilni međusobno neasocirani polinomi $G_1, G_2, \ldots, G_m$ takvi da je $F = G_1 G_2 \ldots G_m$ zbog ranijih argumenata, svaki od tih polinoma ovisi o x_0. Tada je

$$F_0 = \frac{\delta G_1}{\delta x_0} G_2 \ldots G_m + G_1 \frac{\delta G_2}{x_0} \ldots G_m + \ldots + G_1 G_2 \ldots \frac{\delta G_m}{\delta x_0}.$$

Svaki G_i dijeli F te sve pribrojnike od F_0 osim jednog. Stoga F i F_0 ne mogu imati zajedničku komponentu.

Točke P_i leže na krivulji $F_0(x) = 0$ reda $n-1$ i kratnosti su im $r_i - 1$, pa primjenom Teorema 4.6.7 na F i F_0 slijedi tvrdnja. Q.E.D.

Uz zahtjev da je krivulja ireducibilna, a kod racionalnih krivulja, kako ćemo vidjeti, taj zahtjev je uvijek zadovoljen, može se dobiti i jači rezultat.

Teorem 5.2.5. *Ukoliko ireducibilna krivulja V reda n ima višestruke točke P_i multipliciteta r_i, tada vrijedi*

$$(n-1)(n-2) \geq \sum r_i(r_i-1)$$

Dokaz. Prvo primjenimo prethodni teorem da dobijemo nejednakost:

$$\frac{\sum r_i(r_i-1)}{2} \leq \frac{n(n-1)}{2} \leq \frac{(n-1)(n-2)}{2}$$

Kako je $(n-1)(n-2)/2 = N$ dimenzija projektivne ravnine čiji elementi su krivulje dimenzije $n-1$, možemo definirati krivulju V' takvu da su P_i elementi od V' multipliciteta $r_i - 1$, te takvu da siječe V u još $N - \sum r_i(r_i-1)/2$ točaka.

Jasno je da V i V nemaju zajedničkih komponenata jer je V ireducibilna, a V' stupnja nižeg od n. Možemo primjeniti Teorem 4.6.7:

$$n(n-1) \geq r_i(r_i-1) + \frac{(n-1)(n+2)}{2} - \frac{\sum r_i(r_i-1)}{2}$$

Sređivanjem gornje nejednakosti dobiva se traženi rezultat. $\mathfrak{Q.E.D.}$

Teorem 5.2.6. *Ireducibilna krivulja reda n s točkama P_i multipliciteta r_i je racionalna ukoliko vrijedi*

$$(n-1)(n-2) = \sum r_i(r_i-1).$$

Dokaz. Neka je $F = 0$ dana krivulja. Neka je linearni sustav krivulja reda $n-1$ definiran baznim točkama P_i multipliciteta $r_i - 1$, te s još dodatnih $2n-3$ jednostavnih baznih točaka krivulje $F = 0$.

Za dimenziju R ovog linearnog sustava vrijedi:

$$R \geq (n-1)(n+2)/2 - \sum r_i(r_i-1)/2 - (2n-3) = 1$$

Pretpostavimo da je $R \geq 2$. Tada postoji krivulja $G = 0$ iz linearnog sustava koja sadrži još dvije točke krivulje F osim baznih točaka. Zbog $\sum r_i(r_i - 1) + 2n - 3 + 2 > n(n-1)$, teorem 4.6.7 povlači da F i G imaju zajedničku komponentu, no to je u kontradikciji s ireducibilnošću od F i stupnjem od G.

Dakle, $R = 1$ i sve krivulje linearnog sustava se mogu zapisati kao linearna kombinacija dviju nezavisnih krivulja G_1 i G_2. S izuzetkom krivulje G_2, svaka krivulja ima zapis

$$G_1 + \lambda G_2, \quad \lambda \in K$$

Odaberemo afine koordinate tako da je F stupnja n i u koordinati y i u koordinati x, te takve da su G_1 i G_2 stupnja $n-1$ u obje koordinate. Imamo situaciju

$$F = ay^n + \dots$$

$$G_1 = by^{n-1} + \dots$$

$$G_2 = cy^{n-1} + \dots$$

uz $abc \neq 0$ te takve da niti jedan presjek od F i G_1 ne leži na pravcu u beskonačnosti.

Neka je $Res_y(\tau, \lambda)$ rezultantu od F i $G_1 + \lambda G_2$ s obzirom na y.

$$Res_y(x, \lambda) = b_0(\lambda) + b_1(\lambda)x + \dots b_{n(n-1)}(\lambda)x^{n(n-1)}.$$

$Res_y(x, 0)$ je rezultanta polinoma F i G_1 i stupnja je $n(n-1)$ (ne može biti nula jer je F ireducibilan, a G_1 je manjeg stupnja od F). Prema tome, $b_{n(n-1)}(0) \neq 0$, pa se $b_{n(n-1)}$ poništava u najviše konačno mnogo vrijednosti od λ, i njih isključujemo u ostatku dokaza. Primjetimo da F i $G_1 + \lambda G_2$ nemaju sjecišta u beskonačnosti.

Ako je (a_i, b_i) n-terostruka točka krivulje F, teorem 4.6.6 povlači da je a_i barem $r_i(r_i-1)$-terostruka nultočka polinoma $Res_y(x, \lambda)$, a za preostalih $2n+3$ točaka $\left(c_j, d_j\right)$, je c_j jednostavna nultočka te rezultante. Kako je $\sum r_i(r_i-1) + 2n - 3 = n(n-1) - 1$, time smo pobrojali sve nultočke osim jedne.

Preostala nultočka je onda

$$\varphi(\lambda) = -\frac{b_{n(n-1)-1}(\lambda)}{b_{n(n-1)}(\lambda)} - \sum r_i(r_i - 1)a_i - \sum c_j$$

Slično, promatrajući rezultantu s obzirom na x, dolazimo do još jedne racionalne funkcije $\psi(\lambda)$. Ostaje još pokazati da te funkcije zadovoljavaju svojstva iz definicije racionalne krivulje.

Jasno je iz konstrukcije da za sve λ osim njih konačno mnogo, koje smo ranije isključili, vrijedi $F(\varphi(\lambda), \psi(\lambda)) = 0$. Nadalje, ako je (x_0, y_0) točka na F, koja nije na G_2, tada postoji jedinstveni $\lambda_0 = -G_1(x_0, y_0)/G_2(x_0, y_0)$ takav da je (x_0, y_0) na $G_1 + \lambda_0 G_2$. Zbog toga $Res_y(x, \lambda_0)$ ima korijen x_0 pa je $\varphi(\lambda_0) = x_0$, i analogno, $\psi(\lambda_0) = y_0$ Q.E.D.

Postavlja se pitanje vrijedi li i obrat. Odgovor je da vrijedi, no taj važan rezultat dajemo bez dokaza.

Teorem 5.2.7. *Ireducibilna krivulja reda n s jednostavnim singularnim točkama P_i multipliciteta r_i je racionalna ako i samo ako vrijedi*

$$(n-1)(n-2) = \sum r_i(r_i - 1).$$

Dokaz. Dokaz se može naći u [24], strana 188, Theorem 7.3. (i). Q.E.D.

5.3 Kvadratne transformacije

U prethodnom poglavlju smo dokazali nužan uvjet koji krivulja mora imati kako bi bila racionalna. Ipak, ukoliko dana krivulja ne zadovoljava nužan uvjet iz teorema 5.2.6, nećemo biti u stanju utvrditi radi li se o racionalnoj krivulji ili ne. Razlog tome je što teorem 5.2.7 ima dodatni zahtjev na krivulju: ona ne smije imati složeni singularitet. Postavlja se pitanje, je li moguće krivulju sa složenim singularitetima na neki način pretvoriti u krivulju čiji

su svi singulariteti jednostavni, a da pri tome ne promjenimo racionalnost. Takva metoda postoji i predstavljamo ju u ovoj sekciji.

Promotrimo dvije projektivne ravnine $\mathbb{P}^2$ i $\tilde{\mathbb{P}}^2$ te definirajmo relaciju među točkama tih dviju ravnina na sljedeći način:

$$y_i = x_j x_k$$

gdje su $i, j, k \in \{0, 1, 2\}$ međusobno različiti, $(x) = (x_0 : x_1 : x_2) \in \mathbb{P}^2$, a $(y) = (y_0 : y_1 : y_2)$ iz $\tilde{\mathbb{P}}^2$.

Definicija 5.3.1. *Gore opisano pridruživanje se naziva* ***kvadratna transformacija*** *i uz oznaku T možemo pisati $(y) = T(x)$.*

Definicija 5.3.2. *Za točke $(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)$ projektivne ravnine kažemo da su* ***fundamentalne točke****.*

Definicija 5.3.3. *Pravce $x_i = 0, i \in \{0, 1, 2\}$ zovemo* ***iregularni pravci*** *projektivne ravnine.*

Sljedeća lema daje očigledna svojstva kvadratne transformacije.

Lema 5.3.4. *(i) Izuzevši fundamentalne točke, svaka točka iz $\mathbb{P}^2$ se preslikava u jedinstvenu točku iz $\tilde{\mathbb{P}}^2$*

(ii) Svaka nefundamentalna točka iregularnog pravca $x_i = 0$ se preslikava u točku

$$y_i = 1, \quad y_j = y_k = 0$$

(iii) Označimo s T' transformaciju $x_i = y_j y_k$ iz $\tilde{\mathbb{P}}^2$ u $\mathbb{P}^2$. Ukoliko $(x) \in \mathbb{P}^2$ ne leži niti na jednom iregularnom pravcu, tada niti $(y) = T(x)$ ne leži na iregularnom pravcu te vrijedi $(x) = T'(y)$.

Napomena 5.3.5. *Zbog svojstva (ii) prethodne leme, u daljnjem promatramo samo one krivulje koje nemaju iregularne pravce kao komponente.*

Neka je sada $F(x_0, x_1, x_2) = F(x_i) = 0$ krivulja u $\mathbb{P}^2$. Kvadratne transformacije njenih točaka zadovoljavaju jednadžbu

$$G(y_i) := F(y_j y_k) = 0.$$

Ukoliko G ima iregularni pravac kao komponentu, pri obratnoj transformaciji će se taj pravac preslikati u fundamentalnu točku krivulje F. Stoga ima smisla, umjesto G promatrati krivulju F':

$$G(y) = y_0^{\alpha} y_1^{\beta} y_2^{\gamma} F'(y),$$

pri čemu niti jedan y_i ne dijeli F'.

Krivulju G nazivamo **algebarska transformacija**, a krivulju F' **transformacija** od F.

Teorem 5.3.6. *Ako je F' transformacija od F preko T, tada je F transformacija od F' preko T'. Izuzevši konačno mnogo iznimaka, točke ovih dviju krivulja su u 1-1 korespodenciji, te komponente krivulja također korespondiraju.*

Dokaz. Iz pretpostavki teorema vrijede sljedece jednakosti

$$F(y_1 y_2, y_2 y_0, y_0 y_1) = \pi_1(y) F'(y_0, y_1, y_2),$$

$$F'(x_1 x_2, x_2 x_0, x_0 x_1) = \pi_2(x) F''(x_0, x_1, x_2),$$

gdje su π_1 i π_2 su polinomi sastavljeni samo od iregularnih pravaca.

Slijedi

$$F(x_0^2 x_1 x_2, x_0 x_1^2 x_2, x_0 x_1 x_2^2) = \pi_3(x) F'(x_1 x_2, x_2 x_0, x_0 x_1) = \pi_4(y) F''(x_0, x_1, x_2)$$

Kako je F homogen polinom, lijeva strana gornje jednakosti je jednaka

$$(x_0 x_1 x_2)^n F(x_0, x_1, x_2).$$

Kako ni F ni F'' nisu djeljivi niti s jednim x_i, vrijedi $F = F''$. Nadalje,

1-1 korespodencija slijedi iz Leme 5.3.4 (iii) jer postoji samo konačan broj točaka od F i F' koje sijeku iregularne pravce. Korespodencija njihovih faktora slijedi iz jednakosti s početka dokaza. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Lema 5.3.7. *Racionalnost krivulje je invarijantno svojstvo s obzirom na kvadratnu transformaciju krivulje.*

Dokaz. Zbog prethodnog teorema, dovoljno je dokazati da je transformacija racionalne krivlje opet racionalna. Neka je racionalna krivulja C dana polinomom $f \in K[x, y]$ stupnja n. Iz definicije racionalnosti slijedi da je f ireducibilan, te da postoje racionalne funkcije $\varphi, \psi \in K(t)$, od kojih je barem jedna nekonstantna, takve da u $K(t)$ vrijedi $f(\varphi(t), \psi(t)) = 0$.

Pretpostavimo da je jedna od tih funkcija jednaka nuli. Bez smanjenja općenitosti možemo pretpostaviti da je $\psi = 0$ u $K(t)$. Ako je $f(x, 0) = 0$ u $K[x]$, tada y dijeli $f(x, y)$, no krivulja ne može imati iregularni pravac kao komponentu pa je to kontradikcija. Dakle, $f(x, 0)$ je nenul polinom u varijabli x, pa je $f(\varphi(t), 0) = 0$ ako i samo ako φ poprima konačno mnogo vrijednosti, a tada je φ zbog neprekidnosti konstantna, što je kontradikcija.

Projektivizacijom krivulje, uz $x = x_1/x_0$ i $y = x_2/x_0$ dobivamo krivulju u projektivnoj ravnini zadanu polinomom $F \in K[x_0, x_1, x_2]$. Transformacija te krivulje je krivulja zadana polinomom $F' \in K[y_0, y_1, y_2]$ tako da vrijedi

$$F'(y_0, y_1, y_2) = \pi(y_0, y_1, y_2) F(y_1y_2, y_0y_2, y_0y_1),$$

gdje je π produkt potencija varijabli y_0, y_1 i y_2. Polinom F' je također ireducibilan zbog tvrdnje prethodnog teorema da komponente transformacija međusobno korespondiraju.

Neka je još $f \in K[x, y]$ afina reprezentacija transformacije krivulje C. Uočimo da su racionalne funkcije $1/\varphi(t)$ i $1/\psi(t)$ različite od nula. Sada imamo da vrijedi

$$f'\left(\frac{1}{\varphi(t)}, \frac{1}{\psi(t)}\right) = F'\left(1, \frac{1}{\varphi(t)}, \frac{1}{\psi(t)}\right) = \pi\left(1, \frac{1}{\varphi(t)}, \frac{1}{\psi(t)}\right) F\left(\frac{1}{\varphi(t)\psi(t)}, \frac{1}{\psi(t)}, \frac{1}{\varphi(t)}\right) =$$

$$= \pi\left(1, \frac{1}{\varphi(t)}, \frac{1}{\varphi(t)}\right)\left(\frac{1}{\varphi(t)\psi(t)}\right)^n F(1, \varphi(t), \psi(t)) = \xi(t) f(\varphi(t), \psi(t)) \equiv 0.$$

Dakle, transformacija krivulje C je racionalna pa je time dokaz gotov.

$\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Teorem 5.3.8. *Neka je F krivulja reda n, čije fundamentalne točke $x_j = x_k = 0$ imaju multiplicitete $r_i \geq 0$, te takva da niti jedna tangenta u ovim točkama nije iregularan pravac. Tada vrijedi*

(i) Algebarska transformacija G od F ima pravac $y_i = 0$ kao r_i-terostruku komponentu, pa je zato stupanj od F' jednak $2n - \sum r_i$.

(ii) Postoji 1-1 korespodencija između tangenata u fundamentalnoj točki $x_j = x_k = 0$ krivulje F te nefundamentalnih sjecišta krivulje F' s $y_i = 0$.

(iii) Točke $y_j = y_k = 0$ su multipliciteta $n - r_j - r_k$ na F'. Nadalje, niti jedna od tangenata u tim točkama nije iregularni pravac i tangente odgovaraju nefundamentalnim sjecištima krivulje F s $x_i = 0$.

Dokaz. Promatramo fundamentalnu točku $(1, 0, 0)$. Kako je njen multiplicitet r_0, F mora biti oblika

$$F(x) = \sum_{i=r_0}^{n} x_0^{n-i} A_i(x_1, x_2),$$

gdje su A_i homogeni polinomi reda i, te $A_{r_0} A_n \neq 0$. Sada je

$$G(y) = \sum_{i=r_0}^{n} y_1^{n-i} y_2^{n-i} A_i(y_0 y_2, y_0 y_1) = \sum_{i=r_0}^{n} y_0^i y_1^{n-i} y_2^{n-i} A_i(y_2, y_1).$$

Jasno je da je r_0 najviša potencija od y_0 koja se može izlučiti u G, pa je time (i) dokazano.

Za pokazati (ii) dovoljno je uočiti da su tangente na krivulju F u točki $(1 : 0 : 0)$ komponente od $A_{r_0}(x_1, x_2)$, a sjecišta od F' i pravca $y_0 = 0$ korijeni od $y_1^{n-r_0-r_1} y_2^{n-r_0-r_2} A_{r_0}(y_2, y_1)$. Dakle, nefundamentalna sjecišta su nultočke od $A_{r_0}(y_2, y_1)$.

Konačno, zbog

$$F'(y) = \sum_{i=r_0}^{n} y_0^{n-i} y_1^{n-i-r_1} y_2^{n--i-r_2} A_i(y_2, y_1),$$

multiplicitet točke $(1 : 0 : 0)$ jednak je stupnju polinoma $B(y_1, y_2) = y_1^{-r_1} y_2^{-r_2} A_n(y_2, y_1)$, što je jednako $n - r_1 - r_2$. Tangente na F' u istoj točki su komponente polinoma $B(y_1, y_2)$. Pretpostavimo da je jedna od komponenata iregularni pravac, bez smanjenja općenitosti neka se radi o pravcu $y_1 = 0$. Tada je stupanj od $A_n(y_2, y_1)$ jednak $r > r_1$, što povlači da F ima r sjecišta s pravcem $x_0 = 0$ u točki $(0 : 1 : 0)$. No tada je jedna od tangenata u $(0 : 1 : 0)$ upravo iregularan pravac $x_0 = 0$ što se protivi pretpostavkama. Posljednja tvrdnja se dobije iz (ii), tako da promatramo transformaciju T'. Q.E.D.

Teorem 5.3.9. *Svaka r-terostruka točka na F koja ne leži niti na jednom iregularnom pravcu se transformira u r-terostruku točku na F' i pritom multipliciteti tangenata u ovim točkama korespondiraju.*

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti da se radi o točki $(1 : 1; 1)$. Kada bi bilo $P = (a_0 : a_1 : a_2)$, uveli bismo nove koordinate $x_i' = a_i^{-1} x_i$ i $y_i' = a_i y_i$, u kojima bi P, a onda i njena kvadratna transformacija imala koordinate $(1 : 1 : 1)$. Nadalje, kako se algebarska transformacija G i transformacija F' razlikuju u komponentama koje ne sadrže P, dovoljno je dokazati teorem za G.

Definiramo nove koordinate u $\mathbb{P}^2$:

$$z_0 = x_0, \quad z_1 = x_1 - x_0, \quad z_2 = x_2 - x_0$$

U novim koordinatama je $P = (1 : 0 : 0)$ i imamo

$$F(x) = F_1(z) = \sum_{i=r}^{n} z_0^{n-i} A_i(z_1, z_2) = \sum_{i=r}^{n} x_0^{n-i} A_i(x_1 - x_0, x_2 - x_0)$$

Slijedi

$$G(y) = \sum_{i=r}^{n} y_1^{n-i} y_2^{n-i} A_i(y_2 y_0 - y_1 y_2, y_0 y_1 - y_1 y_2)$$

Sada napravimo zamjenu koordinata u $\tilde{\mathbb{P}}^2$:

$$w_0 = y_0, \quad w_1 = y_0 - y_1, \quad w_2 = y_0 - y_2$$

U novom koordinatnom sustavu je $P' = (1 : 0 : 0)$ pa imamo

$$G(y) = G_1(w) = \sum_{i=r}^{n} (w_0 - w_1)^{n-i}(w_0 - w_2)^{n-i} A_i(w_0 w_1 - w_1 w_2, w_0 w_2 - w_1 w_2)$$

Najviša potencija koju w_0 poprima je $2n - r$, a koeficijent uz nju je $A_r(w_1, w_2)$. Prema tome, P' je r-terostruka točka, tangente u P' su komponente polinoma $A_r(w_1, w_2)$. Kako su tangente u P jednake komponentama od $A_r(z_1, z_2)$, tvrdnja teorema je dokazana. $\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

Teorem 5.3.10. *Od svake ireducibilne krivulje se nizom kvadratnih transformacija može dobiti krivulja čiji su svi singulariteti jednostavni.*

Dokaz. Definiramo indeks krivulje kao $\sum(r_i - 1)$, gdje su r_i multipliciteti svih složenih singularnih točaka. Teorem trivijalno vrijedi za krivulje indeksa 0 pa dokazujemo indukcijom.

Neka je I indeks krivulje F i pretpostavimo da teorem vrijedi za sve krivulje indeksa manjeg od I. Dovoljno je pokazati da se nizom kvadratnih transformacija krivulji može smanjiti indeks.

Neka je P složena singularna točka multipliciteta r. Odaberimo koordinatni sustav tako da vrijedi:

(i) $P = (1 : 0 : 0)$

(ii) Pravci $x_1 = 0$ i $x_2 = 0$ se sijeku F u $n - r$ točaka različitih od P

(iii) $x_0 = 0$ siječe $x_1 x_2 F$ u $n + 2$ različite točke

Preostale singularne točke nisu na F. Ako bi npr. točka $(0 : 1 : 0)$ bila na krivulji, tada bi pravac $x_0 = 0$ sjekao i F i pravac $x_2 = 0$ što je u kontradikciji s (iii). Sada na-

pravimo kvadratnu transformaciju i primjenimo teorem 5.3.8 (uz $r_0 = r$, $r_1 = r_2 = 0$). Dobivamo krivulju F' reda $2n - r$ sa svojstvima:

(iv) Svaki singularitet osim P se transformira u singularitet istog multipliciteta. Posebno, jednostavni singulariteti se transformiraju u jednostavne singularitete.

(v) F' ima tri nova jednostavna singulariteta: jedan reda n i dva reda $n - r$

(vi) Točki P odgovara konačan broj točaka krivulje F': P'_j, $j = 1, \ldots, k$ koje leže na pravcu $y_0 = 0$

Singulariteti iz (iv) i (v) ne mijenjaju indeks krivulje. Preostaje analizirati singularne točke iz (vi). Neka je r'_j multiplicitet točke P'_j. Indeks krivulje F' manji je od I za h koji možemo ograditi od dolje:

$$h \geq r - 1 - \sum_{j=1}^{k}(r'_j - 1) = r - \sum_{j=1}^{k} r'_j + k - 1$$

Teorem 5.3.8 (ii) povlači da je $r \geq \sum_{j=1}^{k} r'_j$ pa je $h \geq 0$. U slučaju $h > 0$, F' ima indeks manji od I pa iskoristimo induktivnu pretpostavku. U suprotnom, ako je $h = 0$, nužno mora biti $k = 1$ i $r'_1 = r$. Sada ponavljamo postupak na krivulji F' sve dok se indeks ne smanji.

Dokažimo još da se indeks mora smanjiti u konačnom broju ponavljanja. Neka je F_{p+1} krivulja dobivena od F preko $p + 1$ transformacija tako da je kod svake transformacije vrijedilo $h = 0$. Tada je F' reda $n_{p+1} = 2n_p - r$, a među singularitetima ove krivulje, nalaze se po dva singulariteta multipliciteta $n - r, n_1 - r, \ldots, n_p - r$ te po jedan singularitet multipliciteta $n, n_1, \ldots, n_p$ (Teorem 5.3.8 (iii)).

Teorem 5.2.5 povlači nejednakost:

$$M_{p+1} := (n_{p+1} - 1)(n_{p+2}) - 2\sum_{i=0}^{p}(n_i - r)(n_i - r - 1) - \sum_{i=0}^{p} n_i(n_i - 1) \geq 0$$

gdje je $n_0 = n$. Direktnim računom se dobije

$$M_{p+1} - M_p = -r(r-1) \leq -2,$$

jer je $r \geq 2$. Slijedi da nenegativan cijeli broj p pada kako p raste, pa prema tome, p ne može biti proizvoljno velik. Time je teorem dokazan.

$\mathfrak{Q}.\mathfrak{E}.\mathfrak{D}.$

5.4 Algoritam za određivanje racionalnosti ravninske krivulje

1. Ulazni podatak je ireducibilna afina krivulja C stupnja n zadana polinomom u $K[x, y]$ koja ima jedini složeni singularitet u ishodištu koje označimo s P.

2. Prvo projektiviziramo krivulju C i napravimo zamjenu koordinata koja fiksira točku $P = (1 : 0 : 0)$, te takvu da u novim koordinatama točka $(0 : 0 : 1)$ ne leži na krivulji.

3. Označimo s $F \in K[x_0, x_1, x_2]$ polinom kojim je krivulja zadana u novom projektivnom koordinatnom sustavu i neka je $f \in K[x, y]$, $f(x, y) = F(1, x, y)$ definirajući polinom afine reprezentacije krivulje.

4. Tražimo dva pravca L_1 i L_2 kroz P koja sijeku krivulju u još točno $n - r$ međusobno različitih točaka. Postojanje takvih pravaca garantira teorem 4.6.4, čiji dokaz daje postupak nalaženja takvih pravaca:

   a) Zapišemo f u obliku

   $$f(x, y) = f_r(x, y) + f_{r+1}(x, y) + \ldots + f_n(x, y),$$

   gdje su f_i homogeni polinomi stupnja i, za $r \leq i \leq n$.

b) Definiramo polinom $g \in K[x, \lambda]$ s $g(x, \lambda) = x^{-r} f(x, \lambda x)$

c) Odaberemo $\alpha, \beta \in K$ takve da $\alpha \neq \beta$ koji nisu nultočke polinoma

$$f_r(1, \lambda) f_n(1, \lambda) Res_x\left(g, \frac{\delta g}{\delta x}\right) \in K[\lambda]$$

d) Tada su traženi pravci L_1 i L_2 definirani jednadžbama

$$x_2 = \alpha x_1, \quad x_2 = \beta x_1.$$

5. Sada trebamo naći pravac P_3 koji siječe C u n međusobno različitih točaka od kojih ni jedna nije na pravcima L_1 i L_2.

a) Primjetimo prvo da su sve točke pravaca L_1 i L_2 osim točke P oblika $(\gamma, 1, \alpha)$, $(\gamma, 1, \beta)$, gdje je $\gamma \in K$. Ako za svaki $\gamma \in K$ definiramo pravce R_γ koji spajaju točke $(\gamma, 1, \alpha)$ i $(\gamma, 1, \beta)$, dobivamo pravce s jednadžbama

$$x_0 = \gamma x_1,$$

a to su upravo pravci kroz točku $(0 : 0 : 1)$ koja ne leži na krivulji pa sada dokaz teorema 4.6.3 daje uvjete na γ tako da dobijemo željeni pravac.

b) Odaberemo $\gamma \in K \setminus \{0\}$ takav da:

- $Res_y\left(f, \frac{\delta f}{\delta y}\right)\left(\frac{1}{\gamma}\right) \neq 0$,
- $F(\gamma, 1, \alpha) \neq 0$,
- $F(\gamma, 1, \beta) \neq 0$.

c) Pravac L_3 definiran s

$$x_0 = \gamma x_1$$

siječe pravce L_1 i L_2 van krivulje C, a krivulju siječe u n međusobno različitih točaka.

d) Označimo s P_1 sjecište pravaca L_1 i L_3, a s P_2 sjecište pravaca L_2 i L_3

6. Napravimo zamjenu koordinatnog sustava tako da su P, P_1 i P_2 fundamentalni vrhovi novog koordinatnog sustava kao u teoremu 4.1.5, tj. za matricu prijelaza uzmemo matricu čiji su stupci koordinate točaka P, P_1, P_2 tim redom. Polinome u novim koordinatama opet označimo s F, odnosno f.

7. Sada krivulja zadovoljava uvjete iz dokaza teorema 5.3.10. Napravimo kvadratnu transformaciju

$$G(y_0, y_1, y_2) = F(y_1y_2, y_0y_2, y_0y_1) = y_0^r F'(y_0, y_1, y_2).$$

Teorem 5.3.8 (i) sada povlači da F' nema iregularne pravce kao komponente.

8. Ako krivulja F' nema složenih singulariteta, gotovi smo. Ako ima, zamjenimo koordinatni sustav tako da bilo koja točka u kojoj krivulja ima složeni singularitet ima koordinate $(1 : 0 : 0)$ i vratimo se na korak 2.

Teorem 5.3.10 osigurava da ćemo u konačno mnogo koraka dobiti krivulju koja nema složene singularitete.

5.5 Primjeri

Pokazat ćemo primjenu algoritma na dvjema ireducibilnim krivuljama.

Primjer 5.5.1. Promotrimo krivulju $p(x, y) = x^2 + 2xy + y^2 + x^3 = 0$. Jednostavno se vidi da je jedina točka koja zadovoljava jednakosti

$$p(x, y) = p_x(x, y) = p_y(x, y)$$

ishodište, pa je ishodište jedini singularitet. Iz samog zapisa krivulje uočavamo da je ono reda 2 te da ima dvostruku tangentu $y = 0$, dakle $r = 2$.

Kako je točka $(0:0:1)$ element projektivizirane krivulje, promijenimo koordinate kao u drugom koraku algoritma. U ovom slučaju to je jednostavno, možemo samo zamijeniti varijable x i y. Dakle, sada radimo s krivuljom

$$f(x,y) = x^2 + 2xy + y^2 + y^3.$$

Njena projektivizacija je dana polinomom

$$F(x_0, x_1, x_2) = x_0x_1^2 + 2x_0x_1x_2 + x_0x_2^2 + x_2^3.$$

Definiramo polinom g kao u trećem koraku:

$$g(x,\lambda) = f(x,\lambda x)/x^2 = 1 + 2\lambda + \lambda^2 + \lambda^3 x,$$

Kako je g stupnja 1 u x, njegova diskriminanta s obzirom na x je jednaka 1. Nadalje,

$$f_2(1,\lambda) = 1 + 2\lambda + \lambda^2 = (1+\lambda)^2,$$

$$f_3(1,\lambda) = \lambda^3.$$

Prema tome, možemo uzeti $\alpha = 1$, $\beta = -2$, tj. pravci L_1 i L_2 su redom definirani jednadžbama

$$x_2 = x_1, \quad x_2 = -2x_1.$$

Prelazimo na četvrti korak algoritma. Diskriminanta polinoma f s obzirom na y jednaka je

$$x^3(4 - 27x).$$

Kako 1 nije nultočka diskriminante, te je

$$F(1,1,\alpha) = F(1,1,1) \neq 0,$$

$$F(1,1,\beta) = F(1,1,-2) \neq 0,$$

možemo staviti $\gamma = 1$ i tada je pravac L_3 zadan jednadžbom

$$x_1 = x_0.$$

Točka P_1 je sada sjecište pravaca $x_2 = x_1$ i $x_1 = x_0$ pa ima koordinate $(1 : 1 : 1)$, a točka P_2 je na sjecištu pravaca $x_2 = -2x_1$ i $x_1 = x_0$ pa ima koordinate $(1 : 1 : -2)$.

Sada definiramo matricu $A = \left[a_{ij}\right]_{0\leq i,j\leq 2}$ čiji su stupci koordinate točaka P, P_1 i P_2:

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & -2 \end{pmatrix}$$

i novi koordinatni sustav takav da vrijedi $x_i = \sum_{j=0}^{2} a_{ij}x'_i$, pa je jednadžba krivulje u novom projektivnom koordinatnom sustavu jednaka

$$G\left(x'_0, x'_1, x'_2\right) = F\left(x'_0 + x'_1 + x'_2, x'_1 + x'_2, x_1 - 2x_2\right) =$$

$$4x'_0x'^2_1 + 5x'^3_1 - 4x'_0x'_1x'_2 - 6x'^2_1x'_2 + x'_0x'^2_2 + 9x'_1x'^2_2 - 7x'^3_2.$$

Napravimo kvadratnu transformaciju projektivnog prostora pri čemu se krivulja G transformira u

$$H\left(y_0, y_1, y_2\right) = \frac{1}{y_0^2}G\left(y_1y_2, y_0y_2, y_0y_1\right) =$$
$$= -7y_0y_1^3 + 9y_0y_1^2y_2 + y_1^3y_2 - 6y_0y_1y_2^2 - 4y_1^2y_2^2 + 5y_0y_2^3 + 4y_1y_2^3$$

Sada, kako polazna krivulja nije imala singularitete osim u ishodištu, jedini mogući singulariteti krivulje H su fundamentalne točke $(1 : 0 : 0)$, $(0 : 1 : 0)$ i $(0 : 0 : 1)$ koje su redom multipliciteta $3, 1$ i 1 i jednostavne su, te točke koje se nalaze na pravcu $y_0 = 0$. Uvrštavanjem u jednadžbu krivulje, vidimo da se radi o točkama $(0 : 0 : 1)$, $(0 : 1 : 0)$ i $(0 : 2 : 1)$. Za prve dvije smo već zaključili da zapravo nisu singularne, a za posljednju promotrimo afinu reprezentaciju krivulje uz pravac u beskonačnosti $y_2 = 0$ i tada po definiciji singulariteta vidimo da ni točka $(0 : 2 : 1)$ nije singularna.

Dakle, krivulja H ima jedini singularitet, i to jednostavan, u točki $(1:0:0)$ multipliciteta 3. Slijedi da je desni dio jednakosti formule iz teorema 5.2.6 jednak $3 \cdot 2 = 6$, a kako je red krivulje 4, desni dio jednakosti je također $3 \cdot 2 = 6$. Slijedi da je krivulja racionalna.

Primjer 5.5.2. Neka je dana krivulja

$$f(x,y) = y^2 - 3x^2y - 2y^3 + 2x^4 + y^4.$$

Ona u ishodištu ima složeni singularitet reda 2, a u točki $(0, 1)$ jednostavan singularitet reda 2. Projektivizacija te krivulje je

$$F(x_0, x_1, x_2) = x_0^2x_2^2 - 3x_0x_1^2x_2 - 2x_0x_2^3 + 2x_1^4 + x_2^4.$$

Kako točka $(0:0:1)$ ne leži na krivulji F, možemo preskočiti drugi korak algoritma. Definiramo polinom

$$g(x,\lambda) = \frac{1}{x^2} f(x, \lambda x) = \lambda^2 - 3\lambda x - 2\lambda^3 x + 2x^2 + \lambda^4 x^2.$$

Kako se vrijednosti $1, -1$ ne poništavaju u

$$f_2(1,\lambda)\, f_4(1,\lambda)\, Res_x\left(g, \frac{\delta g}{\delta x}\right) = \lambda^2 \cdot \left(2 + \lambda^4\right) \cdot \lambda^2 \left(1 + 12\lambda^2\right)$$

možemo uzeti $\alpha = 1, \beta = -1$.

Nadalje, diskriminanta polinoma f s obzirom na y je jednaka

$$x^6\left(12 + 37x^2 - 4608x^4 + 2048x^6\right)$$

i ne poništava se u $x = 1$. Nadalje vrijedi $F(1,1,1) \neq 0$ i $F(1,1,-1) \neq 0$ pa možemo uzeti $\gamma = 1$. Sada su pravci L_1, L_2, L_3 redom dani jednakostima

$$x_2 = x_1, \quad x_2 = -x_1, \quad x_1 = x_0,$$

pa su $P_1 = (1,1,1)$ i $P_2(1,1,-1)$.

Matrica prijelaza je sada

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{pmatrix}$$

Krivulja je u novim koordinatama definirana s

$$G(x_0', x_1', x_2') = F(x_0' + x_1' + x_2', x_1' + x_2', x_1' - x_2') =$$

$$= x_0'^2 x_1'^2 - 3x_0' x_1'^3 - x_1'^4 - 2x_0'^2 x_1' x_2' + x_0' x_1'^2 x_2' + 2x_1'^3 x_2' +$$

$$+ x_0'^2 x_2'^2 - 5x_0' x_1' x_2'^2 + 16x_1'^2 x_2'^2 + 7x_0' x_2'^3 + 6x_1' x_2'^3 + 9x_2'^4$$

Kvadratnim transformacijama dobivamo krivulju

$$H(y_0, y_1, y_2) = \frac{1}{y_0^2} G(y_1 y_2, y_0 y_2, y_0 y_1) =$$

$$= 9y_0^2 y_1^4 + 6y_0^2 y_1^3 y_2 + 7y_0 y_1^4 y_2 + 16y_0^2 y_1^2 y_2^2 - 5y_0 y_1^3 y_2^2 + y_1^4 y_2^2 +$$

$$2y_0^2 y_1 y_2^3 + y_0 y_1^2 y_2^3 - 2y_1^3 y_2^3 - y_0^2 y_2^4 - 3y_0 y_1 y_2^4 + y_1^2 y_2^4$$

Nabrojimo sve singularitete ove krivulje:

- Jednostavni singularitet $(1 : 0 : 1)$ polazne krivulje nakon zamjene koordinata i kvadratne transformacije ima koordinate $(-1 : -2 : 2)$ te je i dalje jednostavan i multipliciteta 2.

- Fundamentalne točke $(1 : 0 : 0)$, $(0 : 1 : 0)$ i $(0 : 0 : 1)$ su jednostavne singularne točke krivulje multipliciteta redom $4, 2$ i 2.

- Ostali singulariteti se nalaze na pravcu $y_0 = 0$, uvrštavanjem vidimo da su to fundamentalne točke tog pravca i točka $(0 : 1 : 1)$. Direktno se po definiciji provjerava da je točka $(0 : 1 : 1)$ jednostavna multipliciteta 2

Zaključimo, krivulja H ima samo jednostavne singularitete i to četiri singulariteta multipliciteta 2 i jedan multipliciteta 4. Dakle, desni dio jednakosti iz teorema 5.2.6 je jednak $4 \cdot 2 \cdot 1 + 4 \cdot 3 = 20$, a to je jednako $5 \cdot 4$, tj. lijevoj strani jednakosti, jer je stupanj krivulje 6. Prema tome, krivulja je racionalna pa je racionalna i polazna krivulja.

Bibliografija

[1] P. Belmans, *An Algorithm to Determine the Intersection Multiplicity of Two Curves*, 2011, http://pbelmans.wordpress.com/2011/05/08/an-algorithm-to-determine-the-intersection-multiplicity-of-two-curves/, (21. 03. 2013.).

[2] E. BoĎa i D. Jašková, *On the Computation of Multiplicity by the Reduction of Dimension*, Acta Mathematica Universitatis Comenianæ **78** (2009), br. 2, 197–200, http://www.iam.fmph.uniba.sk/amuc/_vol-78/_no_2/_boda/boda.pdf, (21. 03. 2013.).

[3] D. Cox, J. Little i D. O'Shea, *Ideals, Varieties and Alghorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Texts in Mathematics, Springer–Verlag, 2006.

[4] T. H. Dang, *Computing Serre's Intersection Multiplicities*, 2011, http://arxiv.org/abs/1112.4417v1, (21. 03. 2013.).

[5] W. Decker, *Intersection Multiplicities: Some Pictures*, 2012, http://www.mathematik.uni-kl.de/~decker/Lehre/SS12/AlgebraicGeometry/material/picturesIM.pdf, (21. 03. 2013.).

[6] D. Eisenbud, *Commutative Algebra with a View Towards Algebraic Geometry*, Graduate Texts in Mathematics, sv. 150, Springer–Verlag, 1996.

[7] W. Fulton, *Intersection Theory*, Springer–Verlag, 1998.

[8] ———, *Algebraic curves: An Introduction to Algebraic Geometry*, 2008, http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf, (21. 03. 2013.).

[9] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, sv. 52, Springer–Verlag, 1977.

[10] B. Hassett, *Multiplicity computations*, 2010, http://math.rice.edu/~hassett/vigre/summer10/Multiplicitycomputations.pdf, (21. 03. 2013.).

[11] J. Hilmar, *Intersection of algebraic plane curves / Some results on the (monic) integer transfinite diameter*, 2013, http://www.maths.ed.ac.uk/pg/thesis/hilmar.pdf, (21. 03. 2013.).

[12] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics, sv. 73, Springer–Verlag, 1980.

[13] V. Kiritchenko, *Intersection Theory Course Notes*, 2013, http://www.mccme.ru/~valya/Notes.pdf, (21. 03. 2013.).

[14] J. Kollàr, *The Structure of Algebraic Threefolds: An Introduction to Mori's Program*, Bulletin (New Series) of the American Mathematical Society **17** (1987), br. 2, 211–273, http://projecteuclid.org/DPubS?service=UI&version=1.0&verb=Display&handle=euclid.bams/1183554173, (21. 03. 2013.).

[15] ———, *Which are the Simplest Algebraic Varieties?*, Bulletin (New Series) of the American Mathematical Society **38** (2001), br. 4, 409–433, http://www.ams.org/journals/bull/2001-38-04/S0273-0979-01-00917-X/, (21. 03. 2013.).

[16] S. Marcus, M. M. Maza i P. Vrbik, *On Fulton's Algorithm for Computing Intersection Multiplicities*, 2013, `http://www.csd.uwo.ca/~pvrbik/pdfs/ECCAD2012.pdf`, (21. 03. 2013.).

[17] R. Miranda, *Algebraic Curves and Riemann Surfaces*, Graduate Studies in Mathematics, sv. 5, American Mathematical Society, 1995.

[18] G. Muić, *Bilješke s predavanja iz kolegija "Algebarske krivulje"*, akademska godina 2011./2012.

[19] P. C. Roberts, *Intersection Multiplicities and Hilbert Polynomials*, Michigan Math Journal **48** (2000), br. 1, 517–530, `http://projecteuclid.org/DPubS?verb=Display&version=1.0&service=UI&handle=euclid.mmj/1030132731&page=record`, (21. 03. 2013.).

[20] R. J. Sendra i F. Winkler, *Symbolic Parametrization of Curves*, Journal of Symbolic Computation – JSC **12** (1991), br. 6, 607–632, `http://www.risc.jku.at/publications/download/risc_226/paper_41.pdf`, (21. 03. 2013.).

[21] I. R. Shafarevich, *Basic Algebraic Geometry 1: Varieties in Projective Space*, Springer–Verlag, 1994.

[22] ———, *Basic Algebraic Geometry 2: Schemes and Complex Manifolds*, Springer–Verlag, 1996.

[23] M. Tadić, *Bilješke s predavanja iz kolegija "Algebra 1" i "Algebra 2"*, akademska godina 2011./2012.

[24] R. J. Walker, *Algebraic Curves*, Springer–Verlag, 1978.

Sažetak

Ivan Krijan, Sara Muhvić:

Multipliciteti presjeka i racionalnost ravninskih krivulja

Rad u svome početku sadrži detaljan pregled svih algebarskih aparata koji su nam potrebni. Detaljno se obrađuju dvije definicije multipliciteta presjeka dviju afinih ravninskih krivulja, algebarska i geometrijska. Iz ključnog rezultata vezanog uz algebarsku definiciju dolazimo do algoritma koji je jedan od glavnih dijelova ovog rada. Algoritam se sastoji od provođenja elementarnih aritmetičkih operacija nad polinomima koji definiraju dane krivulje i jednoznačno određuje multiplicitet presjeka u bilo kojoj točki presjeka tih krivulja. Dana je implementacija algoritma u programskom jeziku C pa se račun može jednostavno obaviti uz pomoć računala. Jedan od centralnih (i originalnih) rezultata, uz spomenuti algoritam, je dokaz da su dvije navedene definicije međusobno jednake. Dano je mnoštvo primjera u kojima se vidi operativnost algoritma, ali i korisnost spomenutog dokaza jednakosti dviju definicija.

Nadalje se ulazi u osnove teorije o projektivnim mnogostrukostima. Dolazi se do Bézoutovog teorema koji je svojevrsno poopćenje osnovnog teorema algebre.

U drugom dijelu rada promatramo racionalne krivulje u ravnini te dajemo dokaz Lürothovog teorema koji povlači ekvivalenciju dviju standardnih definicija racionalnosti. Dajemo kriterij za racionalnost krivulje koji se temelji na poznavanju jednostavnih singulari-

teta krivulje i njihovih multipliciteta. Konačno, predstavljamo algoritam koji ireducibilnu krivulju nizom kvadratnih transformacija prevodi u krivulju čiji su svi singulariteti jednostavni, s ciljem određivanja racionalnosti polazne krivulje.

Ključne riječi: *afina ravnina, projektivna ravnina, ravninska krivulja, multiplicitet presjeka, racionalna krivulja, jednostavni singularitet*

Summary

Ivan Krijan, Sara Muhvić:

Intersection numbers and rationality of plane curves

The first part of this paper provides the reader with a thorough overview of all of the algebraic prerequsities and, later on, the two definitions of the intersection number of two affine plane curves, algebraic and geometric, are studied into a great detail. The key result about the algebraic definition brings us to the algorithm which is one of the central parts of the paper. The algorithm consists of elementary arithmetic operations on defining polynomials of the given two curves, and it uniquely determines the intersection number in any of the points of intersection of these curves. The implementation of the algorithm in C programming language is also given so that the computing can be easily done by the computer. Another central and original result of the paper, is the proof that the two definitions of the intersection number are in fact equal. A number of examples are made which show the functionality of the algorithm and the benefits of the theorem.

In addition we start off with basic theory of projective varieties and finish the first part of the paper with Bézout theorem.

In the second part of the paper the emphasis is put on the rational curves in the affine plane. We present the proof of the Lüroth theorem which gives, as a consequence, equivalence between two standard definitions of rational plane curves. The criteria for

determining the rationality of a curve, based on knowledge of all the ordinary singularities of a given curve is also given in the paper. Finally, we present the algorithm which, while not changing its rationality, transforms a given curve into a curve with only ordinary singularities.

Keywords: *affine plane, projective plane, plane curve, intersection number, rational curve, ordinary singularity*