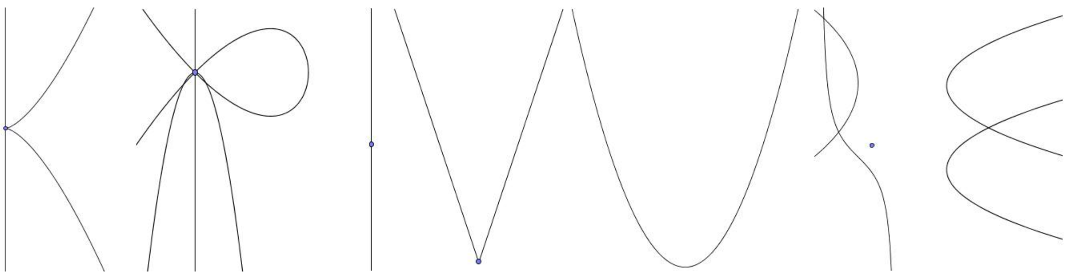
ALGEBARSKE



Bilješke s predavanja profesora Gorana Muića, ak. god. 2015/16.

Natipkali u LaTeX-u:

Alen Andrašek, Barbara Bošnjak, Zlatko Brozinčević, Josip Novak, Veronika Pedić,

Antonela Trbović

7. studenoga 2016.

Poglavlje 1

Osnovni rezultati iz algebre

U ovom poglavlju s $(D,+,\cdot)$ ćemo označavati komutativan prsten s jedinicom $1 \neq 0$, primjerice polje.

Preslikavanje $\phi : D \to D'$ je homomorfizam ako vrijedi $\phi(a+b) = \phi(a)+\phi(b)$, $\phi(ab) = \phi(a)\phi(b)$ i $\phi(1_D) = 1_{D'}$.

D je integralna domena ako $ab = 0 \Rightarrow a = 0$ ili $b = 0, \forall x \in D$.

Za integralnu domenu D konstruiramo polje razlomaka K (direktno poopćenje situacije $D = \mathbb{Z}, K = \mathbb{Q}$): na $D \times D \setminus \{0\}$ definiramo relaciju $\sim$ t.d. $(a,b) \sim (a',b') \Leftrightarrow ab' = a'b$. Tada je $\sim$ relacija ekvivalencije čije klase označavamo s $\frac{a}{b}$. Skup $K = \{\frac{a}{b} : a,b \in D, b \neq 0\}$ s operacijama

zbrajanja: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

i množenja: $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$
čini polje. D ulažemo u K tako da identificiramo $a \equiv \frac{a}{1}$.

Vrijedi tzv. univerzalno svojstvo: Neka je D integralna domena, K' neko polje i $\phi : D \to K'$ ulaganje. Tada postoji jedinstven homomorfizam $\phi' : K \to K'$ koji proširuje ϕ.

Neka je D prsten. Definiramo prsten polinoma $D[T]$ s nezavisnom varijablom T kao skup nizova $f = (a_0, a_1, a_2, ...)$, $a_i \in D$, t.d. postoji $m = m(f) \geq 0$ t.d. $a_i = 0, \forall i \geq m$.

Uz definirano zbrajanje $f + g = (a_0 + b_0, a_1 + b_1, ...)$ i množenje $fg = (a_0b_0, a_0b_1 + a_1b_0, ..., \sum_{i=0}^{k} a_ib_{k-i}, ...)$, uređena trojka $(D[T], +, \cdot)$ je prsten s jedinicom $(1,0,0,...)$.

Imamo ulaganje $D \hookrightarrow D[T]$, $a \mapsto (a,0,0...)$.

Po definiciji je $T = (0,1,0,0,...), T^0 = (1,0,0,...) = 1$. Matematičkom indukcijom dobivamo da je $T^n = (0,...,0,1,0,...)$ (1 na n-tom mjestu). Uz ovu identifikaciju imamo: $\forall f \in D[T], f = (a_0, a_1, ..., a_n, 0, ...) = a_0 + a_1T + a_2T^2 + ...a_nT^n$.

Princip jednakosti polinoma:
$f = a_0 + a_1T + ... + a_nT^n$ i $g = b_0 + b_1T + ... + b_mT^m$ su jednaki akko je $m = n$ i $a_i = b_i, \forall i$.

Za $f = a_0 + a_1T + ... + a_nT^n$ t.d. je $a_n \neq 0$ i $a_k = 0, \forall k \geq n$, definiramo $\deg f = n$.

Zadatak 1.1. *Ako je D integralna domena i $f, g \in D[T]$ ne-nul polinomi, onda je $f \cdot g \neq 0$ i $\deg(f \cdot g) = \deg f + \deg g$.*

Notacija: $f = a_0 + a_1T + ...a_nT^n = \sum_{i=0}^{\infty} a_iT^i$, uz $a_i = 0$ za $i > n$.

Univerzalno svojstvo prstena $D[T]$:
Neka je $\phi : D \to D'$ homomorfizam i $\alpha \in D$. Onda postoji jedinstveni homomorfizam $\hat{\phi} : D[T] \to D'$ t.d. je $\hat{\phi}|_D = \phi$ i $\hat{\phi}(T) = \alpha$.

Posebno važan slučaj:
Neka je $\phi : D \to D'$ ulaganje. Tada možemo identificirati $\phi(a) \equiv a$, $\forall a \in D$, i uz tu identifikaciju je $D \subset D'$. Onda za svaki $\alpha \in D$ postoji jedinstven homomorfizam $D[T] \to D'$, $f = \sum_{i=0}^{m} a_iT^i \mapsto f(\alpha) = \sum_{i=0}^{m} a_i\alpha^i$.

Kažemo da je α nultočka od f ako je $f(\alpha) = 0$.

Napomena 1.2. *Za svaki $f \in D[T]$ definirana je funkcija $f : D \to D$, $\alpha \mapsto f(\alpha)$. Međutim, ova funkcija ne određuje jedinstveno polinom. Primjerice, za p prost broj i $D = \mathbb{Z}/p\mathbb{Z}$, polinom $f = T^p - T \neq 0$, ali $f(a) = 0$, $\forall a \in D$ (mali Fermatov teorem).*

Zadatak 1.3. *Dokažite univerzalno svojstvo za polinome.*

Zadatak 1.4. *Ako je D integralna domena, onda je i $D[T]$ integralna domena.*

Sada rekurzivno definiramo polinome u više varijabli.

$D[T1]$ znamo.

$D[T_1,T_2] := D[T_1][T_2]$ (polinom u varijabli T_2 s koeficijentima iz prstena $D[T_1]$).

$D[T_1,...,T_n] := D[T_1,...,T_{n-1}][T_n]$.

Slijedi da za $f \in D[T1,...,T_n]$ postoje jedinstveni polinomi $a_0,...,a_l \in D[T_1,...,T_{n-1}]$ takvi da je $f = \sum_{i=0}^{l} a_i T_n^i$.

Zadatak 1.5. *Za svaki* $\{i_1,...,i_k\} \subset \{1,...,n\}$ *vrijedi* $D[T1,...,T_n] \cong D[T_1,..,\widehat{T_{i_1}},..,\widehat{T_{i_k}},..,T_n][T_{i_1},...,T_{i_k}]$.

Zadatak 1.6. *Ako je D integralna domena, onda je i $D[T_1,...,T_n]$ integralna domena.*

Zadatak 1.7. *Ako je K polje, onda je $K[T_1,...,T_n]$ integralna domena.*

Definicija 1.8. *Polje razlomaka integralne domene $K[T_1,...,T_n]$ naziva se poljem racionalnih funkcija u n varijabli i označavamo ga s $K(T_1,...,T_n)$.*

Teorem 1.9. *Neka je D integralna domena, neka su $f,\ g \in D[T]$, $g \neq 0$. Tada postoji $a \in D \setminus \{0\}$ i $q,r \in D[T]$ takvi da:*

(i) $af = qg + r$

(ii) $r = 0$ *ili* $\deg r < \deg g$.

Dokaz. Ako je K polje razlomaka od D, onda za $f,g \in K[T]$ Euklidov algoritam dijeljenja daje jedinstvene $q',r' \in K[T]$ takve da vrijedi $f = q'g + r'$ i $r' = 0$ ili $\deg r' < \deg g$. Koeficijenti polinoma q' i r' su iz K, pa definiramo $a = \prod_{c/d} d$, pri čemu c/d prolazi po svim ne-nul koeficijentima od q' i r'. Onda je $q := aq' \in D[T]$, $r := ar' \in D[T]$, $af = qg + r$ i $\deg r = \deg r'$ (jer je D integralna domena). $\square$

Do kraja ove točke pretpostvljamo da je D integralna domena.

Definirajmo još neke važne pojmove:

- Za $a, b \in D$ kažemo da a dijeli b i pišemo $a|b$ ako postoji $c \in D$ t.d. $b = ac$.

- Jedinica (ili invertibilni element) prstena D je element $\varepsilon \in D$ za koji postoji $\eta \in D$ t.d. je $\varepsilon\eta = 1$. $D^x = \{\varepsilon \in D : \varepsilon$ jedinica u $D\}$ je multiplikativna grupa.

Primjer 1.10. *Za K polje,* $K^\times = K \setminus \{0\}$. $\mathbb{Z}^\times = \{\pm 1\}$.

Zadatak 1.11. $D[T_1, ..., T_n]^\times = D^\times$.

Zadatak 1.12. *Ako je K polje, onda je* $K[T_1, ..., T_n]^\times = K \setminus \{0\}$.

- Kažemo da su $a, b \in D$ asocirani ako postoji jedinica ε t.d. je $a = \varepsilon b \Leftrightarrow b = \varepsilon^{-1} a$. Biti asociran je relacija ekvivalencije. Ekvivalentno, možemo definiciju izreći ovako: $a, b \in D$ su asocirani ako i samo ako $a|b$ i $b|a$.

- Kažemo da je $a \in D$ ireducibilan ako $a \neq 0$, $a \notin D^\times$ i ako vrijedi: $a = bc \Rightarrow b \in D^\times$ ili $c \in D^\times$.

Definicija 1.13. *Integralna domena D naziva se faktorijalna domena ako:*
(i) $\forall a \in D$, $a \neq 0$, $a \notin D$, *postoje ireducibilni elementi* $a_1, ..., a_k \in D$ *t.d. je* $a = a_1 ... a_n$.
(ii) (jedinstvenost zapisa) Ako je također $a = b_1 ... b_l$, *za ireducibilne elemente* $b_1, ..., b_l$, *onda je* $k = l$ *te postoji permutacija* $\pi \in S_k$ *i* $\varepsilon_1, ..., \varepsilon_k \in D^\times$ *t.d. je* $b_i = \varepsilon_i a_{\pi(i)}$, $\forall i \in \{1, ..., k\}$.

Napomena 1.14. *Označimo s IrrD skup svih ireducibilnih elemenata od D. Definiramo relaciju* $\sim$ *na IrrD sa:* $a \sim b \Leftrightarrow a, b$ *su asocirani. Onda je* $\sim$ *relacija ekvivalencije na IrrD. Gledamo* $IrrD/\sim$ *i u svakoj klasi izaberemo jednog predstavnika. Označimo s* $IRR(D)$ *skup reprezentanata. (Npr.* $D = \mathbb{Z}, IrrD = \{\pm 2, \pm 3, \pm 5, ...\}$. *Obično uzimamo* $IRR(D) = \{2, 3, 5, ...\}$*). Sada* $\forall a \in D$, $0 \neq a \notin D^\times$, *postoje jedinstveni* $a_1, ..., a_k \in IRR(D)$, $m_1, ..., m_k \in \mathbb{N}$ *i* $\varepsilon \in D^\times$ *t.d. je* $a = \varepsilon a_1^{m_1} ... a_k^{m_k}$.

Napomena 1.15. *Važan primjer faktorijalne domene je polje. Naime, polje je faktorijalna domena u kojoj nema ireducibilnih elemenata jer je svaki element ili* 0 *ili invertibilan, pa je uvjet iz definicije trivijalno zadovoljen.*

Teorem 1.16. *Ako je D faktorijalna domena, onda je i* $D[T]$ *faktorijalna domena.*

Najprije ćemo dokazati sedam pomoćnih lema koje nam trebaju za dokaz Teorema 1.16..

Lema 1.17. *Neka su $a \in D$ i $f \in D[T]$ takvi da $a|f$ u $D[T]$. Tada a dijeli svaki koeficijent od f u D.*

Dokaz. Zapišemo $f = b_0 + b_1T + ... + b_nT^n$. $a|f$ u $D[T]$, pa postoji $g \in D[T]$, $g = c_0 + ... + c_mT^m$ t.d. je $f = ag$. Slijedi $\sum_{i=0}^{\infty} b_iT^i = \sum_{i=0}^{\infty} ac_iT^i \Leftrightarrow b_i = ac_i$, $\forall i \Leftrightarrow a|b_i$, $\forall i$. $\square$

Lema 1.18. *Neka su $a,b,c \in D, a$ ireducibilan, takvi da $a|bc$. Tada $a|b$ ili $a|c$ u D.*

Dokaz. Slučajevi $b = 0$, $c = 0$, $b \in D^{\times}$ ili $c \in D^{\times}$ su očiti. Pretpostavimo $b,c \neq 0$, $b,c \notin D^{\times}$. Onda ih možemo rastaviti na ireducibilne faktore: $b = b_1...b_l$, $c = c_1...c_k$. Jer $a|bc$, postoji $d \in D$ takav da je $b_1...b_lc_1...c_k = ad$. Rastavimo i desnu stranu na ireducibilne faktore, pa zbog jedinstvenosti rastava a mora biti asociran nekom faktoru s lijeve strane. Dakle, postoji $i \in \{1,...,l\}$ ili $j \in \{1,...,k\}$ t.d. $a \sim b_i$ ili $a \sim c_j$. U prvom slučaju $a|b$, a u drugom $a|c$. $\square$

Lema 1.19. *Neka je $d \in D$ ireducibilan i $f,g \in D[T]$. Ako $d|fg$, onda $d|f$ ili $d|g$.*

Dokaz. Tvrdnja je očita ako je $f = 0$ ili $g = 0$. Zato pretpostavimo $f,g \neq 0$. Zapišemo $f = b_0 + b_1T + ...$ i $g = c_0 + c_1T + ...$ Onda je $fg = b_0c_0 + (b_0c_1 + b_1c_0)T + ... + \left(\sum_{i=0}^{k} b_ic_{k-i}\right)T^k + ...$ Pretpostavimo da $d|fg$. Onda prema Lemi 1.17. $d|\sum_{i=0}^{k} b_ic_{k-i}$, $\forall k \geq 0$. Želimo dokazati da vrijedi $d|c_k$, $\forall k \geq 0$ ili $d|b_k$, $\forall k \geq 0$. Pretpostavimo da to ne vrijedi. Onda postoje p i q takvi da $d|b_0$,..., $d|b_{p-1}$, ali $d \nmid b_p$ i $d|c_0$,..., $d|c_{q-1}$, ali $d \nmid c_q$. Pogledajmo sada koeficijent uz T^{p+q}: $A_{p+q} = b_0c_{p+q} + b_1c_{p+q-1} + ... + b_pc_q + ... + b_{p+q}c_0$. Budući da d dijeli svaki koeficijent od fg, dijeli i A_{p+q}. Također, d dijeli sve koeficijente od f prije p-tog i sve koeficijente od g prije q-tog. Iz toga slijedi da $d|b_pc_q$, pa po Lemi 1.18. $d|b_p$ ili $d|c_q$. No to je kontradikcija s našom pretpostavkom. Dakle, mora vrijediti $d|f$ ili $d|g$. $\square$

Lema 1.20. *Neka je K polje razlomaka od D i $f \in D[T]$ ireducibilan nekonstantan polinom. Tada je $f \in K[T]$ ireducibilan.*

Dokaz. Pretpostavimo da $f \in K[T]$ nije ireducibilan. Tada postoje $g,h \in K[T]$ koji oba ovise o T, tj. nisu konstante, takvi da je $f = gh$. Onda postoje $a,b \in D \setminus \{0\}$ takvi da je $g_1 := ag \in D[T]$ i $h_1 := bh \in D[T]$. Sada imamo $abf = (ag)(bh) = g_1h_1$ jednakost polinoma u $D[T]$. Promatramo dva slučaja:

1) Ako je $ab \in D^\times$, onda je $f = (ab)^{-1}g_1h_1$, što je u kontradikciji s pretpostavkom da je f ireducibilan u $D[T]$.

2) Ako $ab \notin D^\times$, onda ga možemo rastaviti na ireducibilne faktore. Tada imamo $c_1...c_t f = g_1h_1$, pa $c_1|g_1h_1$. Prema Lemi 1.19. $c_1|g_1$ ili $c_1|h_1$, pa bez smanjenja općenitosti možemo pretpostaviti da $c_1|g_1$. Definiramo $g_2 := \frac{1}{c_1}g_1$ i zbog Leme 1.17. je $g_2 \in D[T]$. Sada imamo $c_2...c_t f|g_2h_1$, pa analogno postupamo da se riješimo faktora $c_2,...,c_t$. Na kraju dobivamo $f = \tilde{g}\tilde{h}$, pri čemu su $\tilde{g},\tilde{h} \in D[T]$ i ovise o T. No to je u kontradikciji s pretpostavkom da je f ireducibilan. □

Lema 1.21. *(egzistencija NZM polinoma u $K[T]$) Ako su f i g ne-nul polinomi iz $K[T]$, onda postoji polinom $h \in K[T]$ sa svojstvima:*

(i) $h|f$ i $h|g$ u $K[T]$

(ii) Za svaki $k \in K[T]$ t.d. $k|f$ i $k|g$, vrijedi $k|h$

(iii) $h = NZM(f,g)$ je jedinstven do na množenje konstantom $c \in K^\times$

(iv) Postoje $A,B \in K[T]$ takvi da je $Af + Bg = h$.

Lema 1.22. *Neka je K polje, $f,g,h \in K[T]$ i f ireducibilan. Ako $f|gh$, onda $f|g$ ili $f|h$.*

Dokaz. Ako $f|g$, gotovi smo. Ako $f \nmid g$, onda je $h = NZM(f,g) = const. \neq 0$. (Naime, prema Lemi 1.21. $NZM(f,g)$ postoji, a budući da je f ireducibilan, $h|f$ i $f \nmid g$, h mora biti konstanta). Sada iz Leme 1.21. (iv) slijedi da postoje $A,B \in K[T]$ takvi da je $Af + Bg = 1$, pa je $f(Ah) + B(gh) = h$. Sada iz pretpostavke $f|gh$ slijedi da $f|h$. □

Lema 1.23. *Neka je D faktorijalna domena, $f,g,h \in D[T]$, f ireducibilan i $f|gh$ u $D[T]$. Tada $f|g$ ili $f|h$ u $D[T]$.*

Dokaz. Ako je $f \in D$ konstanta, onda tvrdnja slijedi iz Leme 1.19.

Inače, f ovisi o T, pa je prema Lemi 1.20. f ireducibilan u $K[T]$. Očito, $f|gh$ u $K[T]$. Sada prema Lemi 1.22. $f|g$ ili $f|h$ u $K[T]$. BSO pretpostavimo da $f|g$. Tada postoji

$k \in K[T]$ takav da je $g = fk$ i postoji $a \in D \setminus \{0\}$ takav da je $k_1 := ak \in D[T]$. Onda je $ag = fk_1$ u $D[T]$, pa razlikujemo dva slučaja. Ako je $a \in D^\times$, onda je $g = a^{-1}fk_1$, pa $g|f$. Inače f rastavimo na ireducibilne faktore $a_1...a_t$. Iz Leme 1.19. slijedi da $a_1|f$ ili $a_1|k_1$. No prvi slučaj nije moguć, pa $a_1|k_1$. Iz Leme 1.17. slijedi da je $k_2 := \frac{1}{a_1}k_1$ iz $D[T]$, pa je $a_2...a_tg = gk_2$ u $D[T]$. Analogno se riješimo ostalih faktora s lijeve strane i dobivamo $g = f\tilde{k}$ u $D[T]$, pa $f|g$ u $D[T]$. $\square$

Sada smo spremni za dokaz Teorema 1.16.:

Dokaz. Primijetimo prvo: ako je $d \in D$ ireducibilan, onda je d ireducibilan i u $D[T]$. Također vrijedi: ako su $h, l \in D[T]$ ireducibilni onda je $h \sim l \Leftrightarrow h|l \Leftrightarrow l|h$. (Naime, ako je $h = l\varepsilon$ za neki $\varepsilon \in D^\times$, onda je $l = h\varepsilon^{-1}$, pa $h|l$. Obratno, ako $h|l$, onda je $l = hk$, za neki $k \in D[T]$. Zbog ireducibilnosti je $k \in D[T]^\times$ ili $h \in D[T]^\times$. Ali drugo je nemoguće jer je h ireducibilan, pa je $k \in D[T]^\times$, to jest $h \sim l$.)

Iz ovoga odmah dobivamo jedinstvenost rastava. Naime, ako je $f_1...f_t = f = g_1...g_s$, onda $g_1|f_1...f_t$. Indukcijom iz Leme 1.23. lako dobijemo da iz ovoga slijedi $g_1|f_i$, za neki $i \in \{1,...,t\}$, pa je $g_1 = f_i\varepsilon$ (BSO možemo uzeti i=1). Slijedi $f_1\varepsilon g_2...g_s = f_1...t_t$, pa je $g_2...g_s = f_2...f_t$. Nastavimo ovaj postupak za $g_2,...,g_s$ i dobivamo da je $s = t$ i $f_i \sim g_j$.

Dokažimo sada egzistenciju rastava. Uzmemo $f \in D[T]$, $f \neq 0$, $f \notin D^\times$. Razlikujemo dva slučaja:

1) Ako je $f \in D$, onda on ima rastav na ireducibilne faktore u D jer je D faktorijalna domena, a na početku dokaza smo konstatirali da su ireducibilni elementi u D ireducibilni i u $D[T]$.

2) Ako f ovisi o T, zapišemo ga kao $f = a_0 + a_1T + ... + a_kT^k$, $a_i \in D$, $a_k \neq 0$, $k > 0$. Izaberemo skup reprezentanata $IIR(D)$ i svaki $a_i \neq 0$ rastavimo da ireducibilne faktore. Izlučimo zajedničke faktore iz svih koeficijenata i dobivamo $f = af_1$, pri čemu koeficijenti polinoma f_1 nemaju zajedničkih ireducibilnih faktora i f_1 ovisi o T. Ako je f_1 ireducibilan, gotovi smo. Inače, $f_1 = g_1h_1$ za neke $g_1, h_1 \in D[T]$, $g_1, h_1 \notin D[T]^\times$. (Primijetimo, g_1 i h_1 ovise o T jer koeficijenti od f_1 nemaju zajedničkih ireducibilnih faktora). Sada nastavljamo raditi s g_1 i h_1 ono što smo radili za f_1, rastavljamo ih na faktore dok u konačno mnogo koraka ne dođemo do ireducibilnih faktora koji u produktu daju f_1. $\square$

Alternativni kraj dokaza: Definiramo $J = \{f \mid f \in D[T]$ ovisi o T i f nema rastav na ireducibilne fakotre$\}$. Ako je $J = \emptyset$, gotovi smo. Inače, uzmemo $f \in J$ najmanjeg stupnja. Za njega kao i prije konstruiramo $f_1, g_1, h_1 \in D[T]$ koji ovise o T i $a \in D \setminus \{0\}$ takve da je $f = af_1 = g_1 h_1$. Budući da f nema rastav na ireducibilne faktore, nemaju ga ni g_1, h_1. Ali $\deg g_1 < \deg f$ pa imamo kontradikciju s minimalnošću od f. $\square$

Zadatak 1.24. *Dokaz indukcijom po stupnju polinoma.*

Navedimo na kraju dvije posljedice ovog teorema:

Korolar 1.25. *Ako je D faktorijalna domena, onda je i $D[T_1, \dots, T_n]$ faktorijalna domena.*

Korolar 1.26. *Ako je K polje, onda je $K[T_1, \dots, T_n]$ faktorijalna domena.*

Poglavlje 2

Derivacija polinoma

Definicija 2.1. *Neka je D integralna domena i $f = a_0 + a_1T + \ldots + a_nT^n \in D[T]$. Polinom $f' = a_1 + 2a_3T + \ldots + na_nT^{n-1} \in D[T]$ zovemo (formalnom) derivacijom polinoma f. Pridruživanje $f \mapsto f'$ zove se deriviranje.*

Zadatak 2.2. *Neka je D integralna domena. Za sve $a \in D$ i $f, g \in D[T]$ vrijedi:*

a) $(af + g)' = af' + g'$, *tj. deriviranje je D - linearno*

b) $a' = 0$

c) $(fg)' = f'g + fg'$ *(Leibnizovo pravilo)*

d) $(f^n)' = nf^{n-1} \cdot f'$, $(n \in \mathbb{N})$

e) *Za polinom $h = g(f) \in D[T]$ dobiven evaluacijom polinoma g u $f \in D[T]$ vrijedi $h' = g'(f) \cdot f'$.*

Rješenje. Neka su $f = \sum_{k\geq 0} a_kT^k$ i $g = \sum_{k\geq 0} b_kT^k$.

a)

$$(af+g)' = \left(\sum_{k\geq 0}(aa_k + b_k)T^k\right)' = \sum_{k\geq 1} k(aa_k+b_k)T^{k-1} = a\sum_{k\geq 1} ka_kT^{k-1} + \sum_{k\geq 1} kb_kT^{k-1} = = af' + g'.$$

b) Slijedi direktno iz definicije.

c) Iz $fg = \sum_{k\geq 0}\left(\sum_{j=0}^{k} a_j b_{k-j}\right) T^k$ slijedi $(fg)' = \sum_{k\geq 1} k(\sum_{j=0}^{k} a_j b_{k-j})T^{k-1}$, pa imamo

$$fg' + f'g = \left(\sum_{k\geq 0} a_k T^k\right)\left(\sum_{k\geq 0}(k+1)b_{k+1}T^k\right) + \left(\sum_{k\geq 0}(k+1)a_{k+1}T^k\right)\left(\sum_{k\geq 0} b_k T^k\right) =$$

$$= \sum_{k\geq 0}\left(\sum_{j=0}^{k}(k+1-j)a_j b_{k+1-j}\right) T^k + \sum_{k\geq 0}\left(\sum_{j=0}^{k}(j+1)a_{j+1}b_{k-j}\right) T^k =$$

$$= \sum_{k\geq 0}\left(\sum_{j=0}^{k}(k+1-j)a_j b_{k+1-j} \; + \; \sum_{j=1}^{k+1} j a_j b_{k+1-j}\right) T^k =$$

$$= \sum_{k\geq 0}\left(\sum_{j=0}^{k+1}(k+1)a_j b_{k+1-j}\right) T^k = \sum_{k\geq 1} k\left(\sum_{j=0}^{k} a_j b_{k-j}\right) T^{k-1} = (fg)'.$$

d) Za $n = 1$ imamo $(f^1)' = f' = 1 \cdot 1_D \cdot f' = 1 \cdot f^{1-1} \cdot f'$.

Pretpostavimo da tvrdnja vrijedi za $n \in \mathbb{N}$. Tada koristeći (c) dio zadatka dobivamo $(f^{n+1})' = (f^n \cdot f)' = (f^n)' \cdot f + f^n \cdot f' = nf^{n-1} \cdot f' \cdot f + f^n \cdot f' = (n+1)f^n \cdot f'$.

e) Iz (a), (b) i (d) slijedi

$$h' = \left(\sum_{k\geq 0} b_k f^k\right)' = \sum_{k\geq 0} b_k (f^k)' = \sum_{k\geq 1} b_k (k f^{k-1} \cdot f') = \left(\sum_{k\geq 1} k b_k f^{k-1}\right) \cdot f' = g'(f) \cdot f'.$$

□

Napomena 2.3. *Za polinom $f \in D[T]$ derivacije višeg reda definiraju se induktivno: $f'' := (f')'$ i općenito za $n \in \mathbb{N}, n > 1, f^{(n)} := (f^{(n-1)})'$. Također stavljamo $f^{(0)} := f$. Pridruživanje $f \mapsto f^{(n)}$ D - linearno je za sve $n \in \mathbb{Z}_{\geq 0}$.*

Neka je $n \in \mathbb{N}, n \geq 2$. Po definiciji vrijedi $D[T_1,\ldots,T_n] = D[T_1,\ldots,T_{n-1}][T_n]$, pa svaki polinom $f \in D[T_1,\ldots,T_n]$ ima jedinstven zapis oblika

$$f = \sum_{j\geq 0} f_j T_n^j \; , \; \; f_j \in D[T_1,\ldots,T_{n-1}], j \in \mathbb{Z}_{\geq 0} \; , \quad (*)$$

($f_j \neq 0$ samo za konačno mnogo $j \in \mathbb{Z}_{\geq 0}$). Pretpostavimo da svaki polinom $g \in D[T_1,\dots,T_{n-1}]$ ima jedinstven zapis oblika

$$g = \sum_{\alpha \in \mathbb{Z}_{\geq 0}^{n-1}} a_\alpha T_1^{\alpha_1} \dots T_{n-1}^{\alpha_{n-1}}, \alpha = (\alpha_1,\dots,\alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}, a_\alpha \in D$$

($a_\alpha \neq 0$ samo za konačno mnogo $\alpha \in \mathbb{Z}_{\geq 0}^{n-1}$).

Tada iz $(*)$ dobivamo

$$f = \sum_{j \geq 0} \underbrace{\left(\sum_{\alpha \in \mathbb{Z}_{\geq 0}^{n-1}} a_{\alpha,j} T_1^{\alpha_1} \dots T_{n-1}^{\alpha_{n-1}} \right)}_{=f_j} T_n^j = \sum_{\alpha \in \mathbb{Z}_{\geq 0}^{n}} a_\alpha T_1^{\alpha_1} \dots T_n^{\alpha_n},$$

gdje su $a_\alpha \in D$ jedinstveno određeni polinomom f i $a_\alpha \neq 0$ samo za konačno mnogo $\alpha \in \mathbb{Z}_{\geq 0}^n$. Za $\alpha = (\alpha_1,\dots,\alpha_n) \in \mathbb{Z}_{\geq 0}^n$ uvodimo oznake $T^\alpha := T_1^{\alpha_1} \dots T_n^{\alpha_n}$ i $|\alpha| := \alpha_1 + \ldots + \alpha_n$. Tada svaki polinom $f \in D[T_1,\dots,T_n]$ ima jedinstven zapis:

$$f = \sum_{\alpha \in \mathbb{Z}_{\geq 0}^n} a_\alpha T^\alpha.$$

Stupanj polinoma $f \neq 0$ definiramo s $deg(f) := \max_{a_\alpha \neq 0} |\alpha|$.

Neka je sada $1 \leq k \leq n$. Prema zadatku 1.5. vrijedi $D[T_1,\dots,T_n] \cong D[T_1,...,T_{k-1},T_{k+1},...,T_n][T_k]$, pa se svaki polinom $f \in D[T_1,\dots,T_n]$ može na jedinstven način zapisati

$$f = \sum_{j \geq 0} g_j T_k^j,$$

gdje su $g_j \in D[T_1,...,T_{k-1},T_{k+1},...,T_n]$ i $g_j \neq 0$ za samo konačno mnogo j. U tom slučaju definiramo $k-$tu parcijalnu derivaciju polinoma f, u oznaci $\frac{\partial f}{\partial T_k}$, kao derivaciju polinoma f u prstenu $D[T_1,...,T_{k-1},T_{k+1},...,T_n][T_k]$:

$$\frac{\partial f}{\partial T_k} := \sum_{j \geq 1} j g_j T_k^{j-1}.$$

Uočimo da je $k-$ to parcijalno deriviranje $f \mapsto \frac{\partial f}{\partial T_k}$ zapravo "obično" deriviranje u prstenu $D[T_1,...,T_{k-1},T_{k+1},...,T_n][T_k]$, pa iz zadatka 2.2. slijedi da je ono

$D[T_1,...,T_{k-1},T_{k+1},...,T_n]$ - linearno (pa onda i D - linearno), te $\frac{\partial f}{\partial T_k} = 0$ za sve $f \in D[T_1,...,T_{k-1},T_{k+1},...,T_n]$. Također vrijedi Leibnizova formula za produkt, tj. za sve $f,g \in D[T_1,\dots,T_n]$

$$\frac{\partial(fg)}{\partial T_k} = \frac{\partial f}{\partial T_k}\cdot g + f\cdot\frac{\partial g}{\partial T_k}.$$

Zadatak 2.4. *Neka je D integralna domena, $g_1,...,g_n \in D[T]$ i $f \in D[T_1,\dots,T_n]$. Tada za polinom $h = f(g_1,\dots,g_n) \in D[T]$ dobiven evaluacijom polinoma f u $g_1,...,g_n \in D[T]$ vrijedi tzv. lančano pravilo:*

$$h' = \sum_{k=1}^{n}\frac{\partial f}{\partial T_k}(g_1,\dots,g_n)\cdot g_k'.$$

Rješenje. Dokaz provodimo indukcijom po $n \in \mathbb{N}$. Za $n = 1$ to je tvrdnja (e) zadatka 2.2. Pretpostavimo da za $n > 1$ tvrdnja vrijedi za $n-1$, te neka je $f \in D[T_1,\dots,T_n]$. Ako je $f \in D[T_1,\dots,T_{n-1}]$, onda smo gotovi. Inače f "ovisi" o T_n, tj.

$$f = \sum_{j=0}^{m} f_j T_n^j$$

za neke $f_0,...,f_m \in D[T_1,\dots,T_{n-1}], m \geq 1, f_m \neq 0$, pa je

$$h = \sum_{j=0}^{m} h_j g_n^j\ ,$$

gdje je $h_j = f_j(g_1,...,g_{n-1}) \in D[T]$. Sada koristeći tvrdnje zadatka 2.2. imamo

$$h' = \left(\sum_{j=0}^{m} h_j g_n^j\right)' = \sum_{j=0}^{m}(h_j g_n^j)' = \sum_{j=0}^{m} h_j' g_n^j + \sum_{j=1}^{m} j h_j g_n^{j-1} g_n' =$$

$$= \sum_{j=0}^{m}\underbrace{\left(\sum_{k=1}^{n-1}\frac{\partial f_j}{\partial T_k}(g_1,\dots,g_{n-1})g_k'\right)}_{\text{pretp. indukcije}} g_n^j + \underbrace{\left(\sum_{j=1}^{m} j f_j(g_1,...,g_{n-1})g_n^{j-1}\right)}_{=\frac{\partial f}{\partial T_n}(g_1,\dots,g_n)} g_n' =$$

$$= \sum_{k=1}^{n-1}\underbrace{\left(\sum_{j=0}^{m}\frac{\partial f_j}{\partial T_k}(g_1,\dots,g_{n-1})g_n^j\right)}_{=\frac{\partial f}{\partial T_k}(g_1,\dots,g_n)} g_k' + \frac{\partial f}{\partial T_n}(g_1,\dots,g_n)\cdot g_n' = \sum_{k=1}^{n}\frac{\partial f}{\partial T_k}(g_1,\dots,g_n)\cdot g_k'.$$

$\square$

Zadatak 2.5. *(Schwarzova jednakost) Neka su $i, j, n \in \mathbb{N}, 1 \leq i, j \leq n$.*

Tada za svaki polinom $f \in D[T_1, \ldots, T_n]$ vrijedi

$$\frac{\partial}{\partial T_i}\left(\frac{\partial f}{\partial T_j}\right) = \frac{\partial}{\partial T_j}\left(\frac{\partial f}{\partial T_i}\right).$$

(Uputa: Tvrdnju je dovoljno pokazati za monome $T_1^{\alpha_1} \ldots T_n^{\alpha_n} \in D[T_1, \ldots, T_n]$, $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. Opći slučaj tada slijedi iz D- linearnosti operatora $\frac{\partial}{\partial T_k}$.) □

Zadatak 2.6. *Neka je $\alpha = (\alpha_1, \ldots, \alpha) \in \mathbb{Z}^n_{\geq 0}$, $|\alpha| = m$. Na $D[T_1, \ldots, T_n]$ definirajte operator $\frac{\partial^m f}{\partial T_1^{\alpha_1} \ldots \partial T_n^{\alpha_n}}$. Pomoću prethodnog zadatka pokažite da je definicija dobra, tj. ne ovisi o redoslijedu deriviranja. Pokažite da je tako definiran operator D- linearan.*

□

Definicija 2.7. *Neka je D integralna domena i $\mathbb{K}$ polje razlomaka od D. Karakteristiku domene D definiramo kao karakteristiku polja $\mathbb{K}$, tj. $char(D) := char(\mathbb{K})$.*

Zadatak 2.8. *Neka je $f = a_0 + a_1 T + \ldots + a_n T^n \in D[T], a_n \neq 0$ i $a \in D$. Tada postoje jedinstveni $A_0, ..., A_n \in D$ takvi da je*

$$f = \sum_{k=0}^{n} A_k (T-a)^k, \; A_n \neq 0$$

Ako je $char(D) = 0$, onda za koeficijente $A_0, \ldots, A_n$ vrijedi

$$A_k = \frac{f^{(k)}(a)}{k!}, \; k = 0, \ldots, n.$$

Rješenje. Neka je $\phi : D[T] \to D[T]$ evaluacija u $T - a \in D[T]$. Lako se vidi da je evaluacija u $T + a \in D[T]$, $\psi : D[T] \to D[T]$, obostrani inverz od ϕ. Stoga je $\phi : D[T] \to D[T]$ bijekcija, pa postoji jedinstven $g \in D[T]$ t.d. $f = \phi(g) = g(T-a)$. Također,

$$deg(f) = deg(T-a) \cdot deg(g) = deg(g),$$

pa postoje $A_0, \ldots, A_n \in D, A_n \neq 0$ t.d.

$$g = \sum_{k=0}^{n} A_k T^k,$$

što povlači

$$f = \sum_{k=0}^{n} A_k (T-a)^k.$$

Jedinstvenost slijedi iz $g = \psi(f)$. Nadalje, uzastopnim deriviranjem lako se dobije

$$f^{(k)} = \sum_{j=k}^{n} \frac{j!}{(j-k)!} A_j (T-a)^{j-k},\ k = 0,1,\dots,n$$

a odavde evaluacijom polinoma $f^{(k)}$ u $a \in D$

$$f^{(k)}(a) = k! A_k\ ,\ k = 0,1,\dots,n.$$

Neka je $\mathbb{K}$ polje razlomaka domene D. Ako je $char(\mathbb{K}) = 0$, onda je $k! \cdot 1_K \neq 0$, pa računom u $\mathbb{K}$ dobivamo

$$A_k = (k! \cdot 1_K)^{-1}(k! A_k) = \frac{f^{(k)}(a)}{k!},\ k = 0,1,\dots,n.$$

□

Zadatak 2.9. *Neka je D integralna domena, $a_1,\dots,a_n \in D$ i $f \in D[T_1,\dots,T_n]$. Tada postoji jedinstven polinom $g \in D[T_1,\dots,T_n]$ takav da je $f = g(T_1 - a_1,\dots,T_n - a_n)$.*

(Uputa: Slično kao prvi dio prethodnog zadatka, s tim da se sada promatra $\phi : D[T_1,\dots,T_n] \to D[T_1,\dots,T_n]$ evaluacija u $(T_1 - a_1,\dots,T_n - a_n) \in D[T_1,\dots,T_n]^n$.) □

Zadatak 2.10. *Neka je D integralna domena karakteristike nula, $a_1,\dots,a_n \in D$ i $f \in D[T_1,\dots,T_n]$. Tada vrijedi Taylorov razvoj:*

$$f = \sum_{m\geq 0} \left(\sum_{\substack{\alpha\in\mathbb{Z}^n_{\geq 0} \\ |\alpha|=m}} \frac{1}{\alpha_1!\cdots\alpha_n!} \cdot \frac{\partial^m f}{\partial T_1^{\alpha_1}\dots\partial T_n^{\alpha_n}}(a_1,\dots,a_n) \cdot (T_1 - a_1)^{\alpha_1}\cdots(T_n - a_n)^{\alpha_n} \right).$$

(Uputa: Iskoristi se tvrdnja prethodnog zadatka. Dalje se postupa slično kao u drugom dijelu zadatka 2.8.) □

Teorem 2.11. *Neka je D faktorijalna domena karakteristike nula, $g \in D[T]$ ireducibilan polinom pozitivnog stupnja i $f \in D[T]$. Tada $g^2 \mid f$ ako i samo ako $g \mid f$ i $g \mid f'$.*

Dokaz. Ako $g^2 \mid f$, onda je $f = hg^2$ za neko $h \in D[T]$, pa iz tvrdnja (c) i (d) zadatka 2.2. slijedi $f' = h'g^2 + 2hgg' = (h'g + 2hg')g$. Dakle, $g \mid f'$. Očito $g \mid f$.
Obrnuto, neka $g \mid f$ i $g \mid f'$. Tada postoje $h, k \in D[T]$ t.d. $f = hg$ i $f' = kg$. Primjenom tvrdnje (c) zadatka 2.2. na prvu jednakost dobivamo $f' = h'g + hg'$, što zajedno s drugom daje $h'g + hg' = kg$, pa $g \mid hg'$. Kako je D faktorijalna domena i $g \in D[T]$ ireducibilan, iz leme 1.23. slijedi $g \mid h$ ili $g \mid g'$. Pretpostavimo da $g \mid g'$. Tada je $g' = Fg$ za neko $F \in D[T]$. Nadalje, polinom g pozitivnog je stupnja i domena D karakteristike nula, pa mora biti $g' \neq 0$. Odavde slijedi $F \neq 0$, pa kako je $D[T]$ integralna domena imamo $0 < deg(g) \leq deg(F) + deg(g) = deg(g')$, što je kontradikcija. Dakle, $g \nmid g'$, pa mora biti $g \mid h$, što povlači $g^2 \mid hg = f$.

□

Zadatak 2.12. *Neka je D integralna domena karakteristike $char(D) = p > 0$ i $f \in D[T]$, $f \neq 0$. Tada je $f' = 0$ ako i samo ako postoji polinom $g \in D[T]$ t.d. vrijedi $f = g(T^p)$.*

Rješenje. Neka je $f = \sum_{k \geq 0} a_k T^k \in D[T] \setminus \{0\}$. Iz pretpostavke $f' = 0$ slijedi

$$\sum_{k \geq 1} k a_k T^{k-1} = 0 \ ,$$

pa je $k \cdot a_k = 0$ za sve $k \geq 1$. Neka je $\mathbb{K}$ polje razlomaka od D. Po pretpostavci zadatka vrijedi $char(\mathbb{K}) = p > 0$, pa za $k \geq 1$ t.d. $a_k \neq 0$ imamo (račun u $\mathbb{K}$)

$$k \cdot 1_K = (k \cdot a_k) a_k^{-1} = 0.$$

Dakle, $p \mid k$. pa je $k = p j_k$ za neko $j_k \in \mathbb{N}$. Za $k = 0$ stavimo $j_0 = 0$ i definiramo

$$g := \sum_{k; a_k \neq 0} a_k T^{j_k}.$$

Tada imamo

$$f = \sum_{k; a_k \neq 0} a_k T^k = \sum_{k; a_k \neq 0} a_k (T^p)^{j_k} = g(T^p).$$

Obrnuto, ako je $f = g(T^p)$ za neko $g \in D[T]$, onda iz tvrdnji (e) i (d) zadatka 2.2. slijedi

$$f' = g'(T^p) \cdot (T^p)' = p g'(T^p) T^{p-1} = 0.$$

□

Poglavlje 3

Teorija eliminacije varijabli

D= faktorijalna domena u ovom poglavlju

Primjer 3.1. *D=K polje ili D=K$[T_1,...T_n]$ prsten polinoma*

Neka su $f,g \in D[T]$, f,g $\neq$ const.($\Longrightarrow$ f i g su pozitivnog stupnja u T). Znamo da je i $D[T]$ faktorijalna domena. Zanima nas kriterij kada f i g imaju zajednički ireducibilan faktor koji ovisi o T.

Napomena 3.2. *f i g mogu imati zajednički ireducibilan faktor koji je iz D. Takvi nas ne zanimaju.*

Zadatak 3.3. *$f,g \in D[T]$, f,g $\neq$ const. imaju zajednički faktor u $D[T]$ koji ovisi o T ako i samo ako f i g gledano kao polinomi iz $K[T]$ imaju zajednički ireducibilan faktor iz $K[T]$ koji ovisi o T (K je polje razlomaka od D).*

Efektivno: primijenimo Euklidov algoritam za traženje NZM u $K[T]$. To rješava problem egzistencije traženog faktora koji ovisi o T (vidi poglavlje 1).

Primjer 3.4. *D= $\mathbb{Z}$ i K= $\mathbb{Q}$*

Rješenje: $\Longrightarrow$ očito

$\Longleftarrow$ Neka je h NZM od f i g u $K[T]$. Po pretpostavci h ovisi o T $\Longrightarrow$ f=h·k i g=h·l,

$k,l \in K[T]$. Izaberemo a,b,c $\in D \setminus \{0\}$ tako da a·h,b·k,c·l $\in D[T]$ (riješimo se nazivnika). (ab)f=(ah)(bk) i (ac)g=(ah)(cl) jednakosti u $D[T]$ te a·h posjeduje ireducibilan faktor F koji ovisi o T $\Longrightarrow$ F | ab·f i F | ac·g (Lema 1.23.) $\Longrightarrow$ F | f i F | g (jer F $\nmid$ ab i F $\nmid$ ac jer su to konstante i F je ireducibilan faktor $\Longleftrightarrow$ prost). $\square$

Teorem 3.5. *f=* $a_0+a_1 \cdot T+...+a_n \cdot T^n$, $a_i \in D$, $a_n \neq 0$, $n \geq 1$,
g= $b_0+b_1 \cdot T+...+b_m \cdot T^m$, $b_i \in D$, $b_m \neq 0$, $m \geq 1$. *Tada vrijedi:*
(i) f i g imaju zajednički nekonstantni faktor ako i samo ako postoje F, G $\in D[T]$, *F, G*$\neq 0$ *tako da vrijedi deg(F)*$\leq$ *m-1, deg(G)*$\leq$ *n-1 i F·f+G·g=0 (relacija u* $D[T]$*).*
(ii) f i g imaju zajednički nekonstantni faktor ako i samo ako rezultanta $Res(f,g) \in D$ *iščezava, tj.* $Res(f,g)$*=0.*

$$Res(f,g) = \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & a_n & & & \\ & a_0 & a_1 & a_2 & \cdots & a_n & & \\ & & \ddots & & & & \ddots & \\ & & & a_0 & a_1 & a_2 & \cdots & a_n \\ b_0 & b_1 & b_2 & \cdots & b_m & & & \\ & b_0 & b_1 & b_2 & \cdots & b_m & & \\ & & \ddots & & & & \ddots & \\ & & & b_0 & b_1 & b_2 & \cdots & b_m \end{vmatrix}$$

Primjer 3.6. *n=3, m=2*

$$Res(f,g) = \begin{vmatrix} a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 \end{vmatrix}$$

Dokaz: (i) $\Longrightarrow$ Neka je h takav da deg(h)$>$ 0, h | f i h | g u $D[T]$ $\Longrightarrow$ $\exists$ k,l $\in D[T]$ tako da f=h·k i g=h·l. Množenjem f sa l i g sa -k te zbrajanjem jednakosti dobijemo l·f-k·g=0.

n= deg(f)= deg(h) + deg(k) $\geq$ 1+ deg(k) $\implies$ deg(k) $\leq$ n-1. Slično deg(l) $\leq$ m-1. Sada uzmemo F=l i G=k.

$\Longleftarrow$ Pretpostavimo da f i g nemaju zajednički ireducibilan faktor koji ovisi o T.

F·f=-G·g pa slijedi da svaki ireducibilni faktor l od g koji ovisi o T mora dijeliti F·f pa Lema 1.23. i pretpostavka povlače da l dijeli F. Rastavimo:

$$g = \lambda g_1^{n_1} \cdot ... \cdot g_r^{n_r}, \tag{3.1}$$

gdje su g_i ireducibilni faktori od g koji ovise o T $\implies$ $g_1^{n_1} \cdot ... \cdot g_r^{n_r}$ | F $\implies$

deg(g) $\leq$ deg(F) $\leq$ deg(g) -1 $\Rightarrow\Leftarrow$

(ii) Raspišemo uvjet iz *(i)*:

$F = \alpha_0 + \alpha_1 T + ... + \alpha_{m-1} T^{m-1}$,

$G = \beta_0 + \beta_1 T + ... + \beta_{n-1} T^{n-1}$, $\alpha_i, \beta_j \in D$ nepoznati.

$(\alpha_0 + \alpha_1 T + ... + \alpha_{m-1} T^{m-1}) \cdot (a_0 + a_1 T + ... + a_n T^n) + (\beta_0 + \beta_1 T + ... + \beta_{n-1} T^{n-1}) \cdot (b_0 + b_1 T + ... + b_m T^m) = 0$ uz uvjet da barem jedan $\alpha_i \neq 0$ ili $\beta_j \neq 0$.

VAŽNO: $\alpha_i = 0$ za svaki $i \Leftrightarrow \beta_j = 0$ za svaki j, što slijedi iz polinomijalne jednakosti.

Izjednačavamo koeficijente uz:

$T^0 : a_0\alpha_0 + b_0\beta_0 = 0$

$T^1 : a_1\alpha_0 + a_0\alpha_1 + b_0\beta_1 + b_1\beta_0 = 0$

$\vdots$

$T^{m+n-1} : a_n\alpha_{m-1} + b_m\beta_{n-1} = 0.$

Ovo je homogeni $(m+n)$x$(m+n)$ sustav u varijablama $(\alpha_0, ..., \alpha_{m-1}, \beta_0, ..., \beta_{n-1})$.

Zbog VAŽNO postoji rješenje različito od $(0, ..., 0)$. Dakle, determinanta sustava koja je $Res(f, g)^{\intercal}$ je jednaka 0.

$m = 2, n = 3$

$(\alpha_0 + \alpha_1 T) \cdot (a_0 + a_1 T + a_2 T^2 + a_3 T^3) + (\beta_0 + \beta_1 T + \beta_2 T^2) \cdot (b_0 + b_1 T + b_2 T^2) = 0$

Izjednačavanjem koeficijenata dobijemo:

$T^0 : a_0\alpha_0 + b_0\beta_0 = 0$

$T^1 : a_1\alpha_0 + a_0\alpha_1 + b_0\beta_1 + b_1\beta_0 = 0$

$T^2 : a_2\alpha_0 + a_1\alpha_1 + b_2\beta_0 + b_1\beta_1 + b_0\beta_2 = 0$

$T^3 : a_3\alpha_0 + a_2\alpha_1 + b_1\beta_2 + b_2\beta_1 = 0$

$T^4 : a_3\alpha_1 + b_2\beta_2 = 0$

$$\begin{bmatrix} a_0 & 0 & b_0 & 0 & 0 \\ a_1 & a_0 & b_1 & b_0 & 0 \\ a_2 & a_1 & b_2 & b_1 & b_0 \\ a_3 & a_2 & 0 & b_2 & b_1 \\ 0 & a_3 & 0 & 0 & b_2 \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \beta_0 \\ \beta_1 \\ \beta_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Determinanta gornje matrice jednaka je $Res(f,g)$. □

Pretpostavimo da je char D=0.

$\implies f \in D[T], deg(f) \geq 1 \implies f' \neq 0, deg(f') = deg(f) - 1$

$f = a_0 + a_1 T + ... + a_n T^n, a_i \in D, a_n \neq 0, n \geq 1,$

$f' = a_1 + 2a_2 T + ... + na_n T^{n-1}$, gdje je $na_n \neq 0$ jer je char D $\neq 0$.

Definicija 3.7. *Diskriminanta od f je Res(f,f'), uz gornje pretpostavke.*

Korolar 3.8. *Ako je D faktorijalna domena, char D $\neq$ 0, tada polinom $f \in D[T]$ stupnja ≥ 2 ima ireducibilan faktor koji ovisi o T multipliciteta ≥ 2 ako i samo ako je Res(f,f')=0.*

Dokaz: Slijedi iz Teorema 2.11. i Teorema 3.5. □

Korolar 3.9. *D=K polje karakteristike 0. Tada $f \in K[T]$ stupnja ≥ 2 ima ireducibilan faktor multipliciteta barem 2 ako i samo ako Res(f,f')=0.*

Napomena 3.10. *Iz prvog poglavlja $\implies$ ireducibilni polinomi u K[T] ne mogu biti iz K (zato u gornjem iskazu ispuštamo da ireducibilan faktor ovisi o T).*

Primjer 3.11. *λ iz algebarskog zatvarača od K.*

λ je dvostruka nultočka od f $\Leftrightarrow f(\lambda) = f'(\lambda) = 0 \Leftrightarrow (T-\lambda)^2 | f \Leftrightarrow (T-\lambda)|f, (T-\lambda)|f'$

$\Leftrightarrow$ Res(f,f')=0

Zadatak 3.12. *Neka su p,q iz K. Diskriminanta od $T^3 + pT + q$ jednaka je $4p^3 + 27q^2$.*

Zadatak 3.13. *Neka su a,b iz K. Diskriminanta od $aT^2 + bT + c$ jednaka je $-a(b^2 - 4ac)$.*

Teorem 3.14. *Neka je D faktorijalna domena, neka su $f,g \in D[T]$ koji ovise o T, deg(f)=n ≥ 1, deg(g)=m ≥ 1. Tada postoje ne-nul polinomi $F,G \in D[T]$ takvi da deg(F) $\leq m-1$, deg(G) $\leq n-1$, $Ff+Gg = Res(f,g) \in D$.*

Dokaz: Koristimo oznake iz iskaza i dokaza prvog teorema iz ovog poglavlja.

Ako je Res(f,g)=0, onda po istom teoremu imamo tvrdnju.

Ako Res(f,g) $\neq 0$, onda:

$F = \alpha_0 + \alpha_1 T + ... + \alpha_{m-1}T^{m-1}$,

$G = \beta_0 + \beta_1 T + ... + \beta_{n-1}T^{n-1}$, $\alpha_i, \beta_j \in D$ nepoznati koje tražimo iz

$(\alpha_0 + \alpha_1 T + ... + \alpha_{m-1}T^{m-1}) \cdot (a_0 + a_1 T + ... + a_n T^n) + (\beta_0 + \beta_1 T + ... + \beta_{n-1}T^{n-1}) \cdot (b_0 + b_1 T + ... + b_m T^m) = Res(f,g)$.

Iz toga se mogu izračunati koeficijenti jer dobijemo:

$$\begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_n & & & \\ & a_0 & a_1 & a_2 & \cdots & a_n & & \\ & & \ddots & & & & \ddots & \\ & & & a_0 & a_1 & a_2 & \cdots & a_n \\ b_0 & b_1 & b_2 & \cdots & b_m & & & \\ & b_0 & b_1 & b_2 & \cdots & b_m & & \\ & & \ddots & & & & \ddots & \\ & & & b_0 & b_1 & b_2 & \cdots & b_m \end{bmatrix}^T \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{m-1} \\ \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{n-1} \end{bmatrix} = \begin{bmatrix} Res(f,g) \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

det=Res(f,g)$\neq 0 \implies$ Cramerov sustav ima jedinstveno rješenje $\square$

Napomena 3.15. *Cramerov sustav riješavamo u polju razlomaka K od D. Ima rješenja oblika $\alpha_i = (\frac{"gornjadet"}{Res(f,g)})$, $\beta_j = (\frac{"gornjadet"}{Res(f,g)})$. Da su α_i i β_j iz D lako se vidi iz izračuna "gornja det" Laplaceovim razvojem po stupcu u koji smo stavili vektor sa desne strane jednakosti.*

Dokaz: (drugi način)

$f = a_0 + a_1 T + ... + a_n T^n$

$Tf = a_0T + a_1T^2 + ... + a_nT^{n+1}$

$\vdots$

$T^{m-1}f = a_0T^{m-1} + a_1T^m + ... + a_nT^{m+n-1}.$

$g = b_0 + b_1T + ... + b_mT^m$

$Tg = b_0T + b_1T^2 + ... + b_mT^{m+1}$

$\vdots$

$T^{n-1}g = b_0T^{n-1} + b_1T^n + ... + a_nT^{m+n-1}.$

Matrični zapis:

$$\begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_n & & & & \\ & a_0 & a_1 & a_2 & \cdots & a_n & & & \\ & & \ddots & & & & \ddots & & \\ & & & a_0 & a_1 & a_2 & \cdots & a_n \\ b_0 & b_1 & b_2 & \cdots & b_m & & & & \\ & b_0 & b_1 & b_2 & \cdots & b_m & & & \\ & & \ddots & & & & \ddots & & \\ & & & b_0 & b_1 & b_2 & \cdots & b_m \end{bmatrix} \begin{bmatrix} 1 \\ T \\ T^2 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ T^{m+n-1} \end{bmatrix} = \begin{bmatrix} f \\ Tf \\ \vdots \\ T^{m-1}f \\ g \\ Tg \\ \vdots \\ T^{n-1}g \end{bmatrix}$$

Matrica sustava ima koeficijente iz D i determinanta joj je Res(f,g) za koju pretpostavljamo da je $\neq 0$.

Sjetimo se: $\tilde{A}$ adjungirana matrica

$(\tilde{A})_ij = (-1)^{i+j}\cdot$ minora od A dobivena izbacivanjem j-tog retka i i-tog stupca $(\in D)$

VAŽNO SVOJSTVO: $\tilde{A} \cdot A = A \cdot \tilde{A} = (detA) \cdot I_{m+n}$.

$\Longrightarrow$

$$\tilde{A} \begin{bmatrix} f \\ Tf \\ \vdots \\ T^{n-1}g \end{bmatrix} = detA \begin{bmatrix} 1 \\ T \\ \vdots \\ T^{m+n-1} \end{bmatrix}$$

$((\tilde{A})_{11}f + (\tilde{A})_{12}Tf + \cdots + (\tilde{A})_{1m}T^{m-1}f) + ((\tilde{A})_{1,m+1}g + (\tilde{A})_{1,m+2}Tg + \cdots + (\tilde{A})_{1,m+n}T^{n-1}g) = Res(f,g) \cdot 1$

pa iz prve zagrade izlučimo f, a iz druge g. $\square$

K polje. Gledamo prsten polinoma u r varijabli, r ≥ 1.

$K[T_1,...,T_r] = K[T_1,...,T_{r-1}][T_r]$, gdje je $= K[T_1,...,T_{r-1}]$ faktorijalna domena, nazovimo ju D.

$f,g \in K[T_1,...,T_r]$ koji ovise o T_r (tj. pozitivnog su stupnja u T_r)

$f,g \in D[T_r]$ ovise o T_r

1. teorem iz ovog poglavlja tada daje: f,g imaju zajednički ireducibilni faktor u $K[T_1,...,T_r]$ koji ovisi o $T_r \Leftrightarrow Res_{T_r}(f,g) = 0$ (nul-polinom u $K[T_1,...,T_{r-1}]$)

$f = a_0 + a_1T + ... + a_nT^n, a_i \in D = K[T_1,...,T_{r-1}], a_n \neq 0, n \geq 1,$

$g = b_0 + b_1T + ... + b_mT^m, b_i \in D = K[T_1,...,T_{r-1}], b_m \neq 0, m \geq 1.$

$$Res_{T_r}(f,g) = \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & a_n & & & \\ & a_0 & a_1 & a_2 & \cdots & a_n & & \\ & & \ddots & & & & \ddots & \\ & & & a_0 & a_1 & a_2 & \cdots & a_n \\ b_0 & b_1 & b_2 & \cdots & b_m & & & \\ & b_0 & b_1 & b_2 & \cdots & b_m & & \\ & & \ddots & & & & \ddots & \\ & & & b_0 & b_1 & b_2 & \cdots & b_m \end{vmatrix}$$

očito polinom iz $K[T_1,...,T_{r-1}]$.

Uzmemo $(\alpha_1,...,\alpha_{r-1}) \in K^r$ i napravimo sljedeće:

Parcijalna evaluacija: $f(\alpha_1,...,\alpha_{r-1},T_r) = \sum_{i=0}^{n} a_i(\alpha_1,...,\alpha_{r-1})T_r^i$,

$g(\alpha_1,...,\alpha_{r-1},T_r) = \sum_{i=0}^{m} b_i(\alpha_1,...,\alpha_{r-1})T_r^i$, polinomi iz $K[T_r]$.

Ako smo izabrali $(\alpha_1,...,\alpha_{r-1}) \in K^{r-1}$ tako da $a_n(\alpha_1,...,\alpha_{r-1}) \cdot b_m(\alpha_1,...,\alpha_{r-1}) \neq 0 \quad (\star)$

$\implies f(\alpha_1,...,\alpha_{r-1},T_r)$ stupnja n u T_r, $g(\alpha_1,...,\alpha_{r-1},T_r)$ stupnja m u T_r.

Oni su istog stupnja kakvog su bili $f,g \in K[T_1,...,T_r]$ u varijabli T_r. To omogućuje da se izračuna:

$$Res_{T_r}(f(\alpha_1,...,\alpha_{r-1},T_r), g(\alpha_1,...,\alpha_{r-1},T_r)) \in K \Leftrightarrow Res_{T_r}(f,g)(\alpha_1,...,\alpha_{r-1},T_r) \in K \tag{3.2}$$

PITANJE: Ima li uopće takvih $(r-1)$ -torki da vrijedi $(\star)$?

Krenuli smo od $a_n, b_m \neq 0$ u $K[T_1,...,T_{r-1}] \implies$ (jer je $K[T_1,...,T_{r-1}]$ integralna domena)

$a_n \cdot b_m \neq 0$, nije nul-polinom.

? Ako $F \in K[T_1,...,T_r]$ nije nul-polinom, onda $\exists(\alpha_1,...,\alpha_r) \in K^r$ tako da $F(\alpha_1,...,\alpha_r) \neq 0$.

To ne vrijedi nužno:

- $K = \mathbb{Q}$, beskonačno polje $\longrightarrow$ postoji barem za $r = 1$; $F \neq 0 \implies \exists \alpha_1 \in \mathbb{Q}$ tako da $F(\alpha_1) \neq 0$
- $K = \mathbb{Z}/p\mathbb{Z}$ (p prost), konačno polje $\longrightarrow$ ne vrijedi! Uzmemo $f = T^p - T$, $f(\lambda) = 0, \forall \lambda \in K$

Lema 3.16. *Neka je K polje sa beskonačno elemenata. Onda za* $\forall F \in K[T_1,...,T_r]$, $F \neq 0, \exists(\alpha_1,...,\alpha_r) \in K^r$ *tako da je* $F(\alpha_1,...,\alpha_r) \neq 0$.

Dokaz: Dokazujemo indukcijom po broju varijabli r:

Baza: $r = 1$ očito (polinom stupnja n ima najviše n nultočaka u K)

Pretpostavka: Neka tvrdnja vrijedi za $r-1$.

Korak: $F \in K[T_1,...,T_r]$

1. slučaj: F ne ovisi o $T_r \longrightarrow$ koristimo pretpostavku indukcije

2. slučaj: F ovisi o T_r: $F = \sum_{i=1}^{r} F_i(T_1,...,T_{r-1})T_r^i$

F je stupnja $n \geq 1$ u $T_r \implies F_n \neq 0$ u $K[T_1,...,T_{r-1}] \implies$ (po induktivnoj pretpostavci) $F_n(\alpha_1,...,\alpha_{r-1}) \neq 0 \implies F(\alpha_1,...,\alpha_{r-1},T_r) \in K[T_r]$ stupnja $n \geq 1$ koji se poništava za svaki $\alpha_r \in K \Rightarrow\Leftarrow$ $\square$

Lema 3.17. *K je algebarski zatvoreno polje* $\implies$ *K ima beskonačno elemenata.*

(K je algebarski zatvoreno ako za $\forall f \in K[T]$ *stupnja* ≥ 1 $\exists \lambda \in K$ *tako da* $f(\lambda) = 0$ *.)*

Dokaz: Ako je $K = \{\lambda_1,...,\lambda_n\}$, definiramo $f(T) = (T-\lambda_1)\cdots(T-\lambda_n)+1$ koji očito nema korijena u K. $\Rightarrow\Leftarrow$ $\square$

Srednja škola:

$\lambda \in K, f \in K[T]$. $T - \lambda | f \Leftrightarrow f(\lambda) = 0$

Netrivijalni dio tvrdnje: Ako se f poništava gdje i ireducibilan polinom $g = T - \lambda$, onda $g|f$. (Bezoutov teorem)

Teorem 3.18. *Neka je K algebarski zatvoreno polje i neka su* $f, g \in K[T_1, ..., T_r]$*, g ireducibilan. Ako vrijedi:* $(\star)$ $(\forall(\alpha_1, ..., \alpha_r) \in K^r)$ $g(\alpha_1, ..., \alpha_r) = 0 \implies f(\alpha_1, ..., \alpha_r) = 0$*, onda* $g|f$ *u* $K[T_1, ..., T_r]$.

Dokaz: g je ireducibilan $\implies g \neq const. \implies g$ ovisi o nekom T_i, BSO $i = r$.

Korak 1: Ako je $f \neq 0$ bilo koji polinom koji zadovoljava $(\star)$, onda f također ovisi o T_r.

Dokaz koraka 1: Pretpostavimo da f ne ovisi o $T_r \implies f \in K[T_1, ..., T_{r-1}]$. $g = \sum_{i=1}^{l} g_i(T_1, ..., T_{r-1})T_r^i$, $l \geq 1$, $g_l \neq 0$, jer g ovisi o T_r.

$f, g_l \in K[T_1, ..., T_r - 1 \neq 0] \implies f \cdot g_l \neq 0$ pa prethodne leme povlače da $\exists(\alpha_1, ..., \alpha_{r-1}) \in K^r$ tako da $f(\alpha_1, ..., \alpha_{r-1}) \cdot g(\alpha_1, ..., \alpha_{r-1}) \neq 0$. Fiksiramo takav $(\alpha_1, ..., \alpha_{r-1})$.

Što imamo?

(1) $f(\alpha_1, ..., \alpha_{r-1}) \neq 0$

(2) $g(\alpha_1, ..., \alpha_{r-1}, T_r) = \sum_{i=1}^{l} g_i(\alpha_1, ..., \alpha_{r-1})T_r^i$ je polinom stupnja $l \geq 1$ (jer $g(\alpha_1, ..., \alpha_{r-1}) \neq 0$) s koeficijentima iz K

(3) K je algebarski zatvoreno $\implies \exists \alpha_r \in K$ tako da $g(\alpha_1, ..., \alpha_{r-1}, \alpha_r) = 0$ (jer polinom iz *(2)* ima nultočku α_r). $(\star) \implies f(\alpha_1, ..., \alpha_{r-1}, \alpha_r) = 0$ no α_r možemo ispustiti iz notacije jer f ne ovisi o $T_r \implies f(\alpha_1, ..., \alpha_{r-1}) = 0 \Rightarrow\Leftarrow$ s *(1)* $\square$

Korak 2: (Dokaz teorema)

$f = 0 \implies$ jasno je da $g|0 = f$

$f \neq 0 \implies$ (po Koraku 1) f ovisi o T_r. Dakle, i f i g ovise o $T_r \implies Res_{T_r}(f, g)$ dobro definirana pa po prethodnom teoremu $\exists F, G \in D[T_r] = K[T_1, ..., T_r]$ tako da $F \cdot f + G \cdot g = Res_{T_r}(f, g)$.

Sada korisitimo $(\star)$: $(\forall(\alpha_1, ..., \alpha_r) \in K^r)$ $g(\alpha_1, ..., \alpha_r) = 0 \implies f(\alpha_1, ..., \alpha_r) = 0$.

$F(\alpha_1, ..., \alpha_r) \cdot f(\alpha_1, ..., \alpha_r) + G(\alpha_1, ..., \alpha_r) \cdot g(\alpha_1, ..., \alpha_r) = Res_{T_r}(f, g)(\alpha_1, ..., \alpha_{r-1})$

$\implies Res_{T_r}(f, g)(\alpha_1, ..., \alpha_{r-1}) = 0, \forall(\alpha_1, ..., \alpha_r \in K^r)$ takve da $g(\alpha_1, ..., \alpha_r) = 0$. Sada ovo i Korak 1 za $f = Res_{T_r}(f, g)$ povlači da je ili $Res_{T_r}(f, g) = 0$ ili ovisi o $T_r \implies Res_{T_r}(f, g) = 0$. Sada prvi teorem u ovom poglavlju daje f i g imaju zajednički ireducibilan faktor u $D[T_r] = K[T_1, ..., T_r]$ koji ovisi o T_r. Kako je g ireducibilan, taj faktor je g $\implies g|f$ $\square$

Poglavlje 4

Homogeni polinomi

Neka je K bilo koje polje i $f \in K[T_1, ...T_n]$. Iz poglavlja 2 znamo da je tada f oblika

$$f = \sum_{\alpha} a_\alpha T^\alpha,\ \alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{Z}^n_{\geq 0},\ |\alpha| = \alpha_1 + ... + \alpha_n,\ a_\alpha \in K.$$

(Za sve osim konačno mnogo $\alpha \in \mathbb{Z}^n_{\geq 0}$ je $a_\alpha = 0$.)

Preslaganjem dobijemo:

$$f = \sum_{m=0}^{+\infty} \underbrace{\left(\sum_{\substack{\alpha \\ |\alpha|=m}} a_\alpha T^\alpha \right)}_{=f_m} = f_0 + f_1 + f_2 + ...,$$

gdje je f_m m-ta homogena komponenta polinoma f.

Definicija 4.1. *f je homogen polinom stupnja homogenosti $m \geq 0$ ako je $f = f_m$. Nulpolinom je homogen svakog stupnja.*

Označimo sa $K[T_1, ..., T_n]_m$ skup svih homogenih polinoma stupnja m. To je vektorski prostor nad K čija je baza $(T^\alpha, |\alpha| = m)$.

Npr., ako je $m = 0$, tada je $K[T_1, ..., T_n] = K$ (samo konstante).

Ako je $m = 1$, tada je $K[T_1, ..., T_n] = KT_1 \dotplus ... \dotplus KT_n$, itd.

Dimenzija $\dim K[T_1, ...T_n]_m$ je jednaka broju svih $\alpha \in \mathbb{Z}^n_{\geq 0}$ takvih da je $|\alpha| = m$. Dakle,

$$\dim K[T_1, ...T_n]_m = \binom{m+n-1}{n-1}.$$

Zadatak 4.2. *Ako je $f \in K[T_1,...T_n]_m$ i $g \in K[T_1,...T_n]_l$, tada je $f \cdot g \in K[T_1,...T_n]_{m+l}$.*

Rješenje. $f = T^\alpha$, $|\alpha| = m$, $g = T^\beta$, $|\beta| = l \implies f \cdot g = T^{\alpha+\beta}$, $|\alpha+\beta| = l+m$. $\square$

Zadatak 4.3. *Neka su $f \neq 0$ i $g \neq 0$ polinomi iz $K[T_1,...,T_n]$ takvi da je $f \cdot g \in K[T_1,...,T_n]_m$, za neki $m \geq 0$. Tada su f i g homogeni.*

Rješenje. Rastavimo f i g na homogene komponente:

$$f = f_0 + f_1 + ... + f_k, \;\; f_k \neq 0,$$

$$g = g_0 + g_1 + ... + g_l, \;\; g_l \neq 0.$$

Rastavimo i $f \cdot g$ na homogene komponente:

$$f \cdot g = f_k \cdot g_l + (f_k \cdot g_{l-1} + f_{k-1} \cdot g_l) + ... + f_0 \cdot g_0.$$

Iz pretpostavke slijedi: $f_k \cdot g_{l-1} + f_{k-1} \cdot g_l = 0, ..., f_0 \cdot g_0 = 0$.
Cilj nam je dokazati da je $f = f_k$ i $g = g_l$.

Zapišimo f kao

$$f = f_t + ... + f_k,$$

gdje je $t < k$ i f_t prva homogena komponenta od f različita od nulpolinoma. Slično, neka je

$$g = g_u + ... + g_l,$$

ali sada $u \leq l$. Računamo:

$$f \cdot g = (f_t + ... + f_k) \cdot (g_u + ... + g_l) = f_t \cdot g_u + ... + f_k \cdot g_l.$$

Iz $u \leq l$ i $t < k$ zaključujemo da je $u + t < k + l = m$. Dakle, $f_t \cdot g_u = 0$, ali to je kontradikcija s $f_t \neq 0$, $g_u \neq 0$. $\square$

Sjetimo se:
$K[T_1,...T_n]$ je faktorijalna domena, invertibilni elementi u $K[T_1,...T_n]$ su $K^\times$.
f i g su asocirani ako postoji $\lambda \in K^\times$ takav da $f = \lambda g$.
Iz poglavlja 1:

$IRR(K[T_1,...T_n])$ =skup predstavnika klasa ireducibilnih elemenata iz $K[T_1,...T_n]$ u odnosu na asociranost.
Za svaki $f \in K[T_1,...T_n]$ postoje jedinstveni $\lambda \in K$, $f_1,...,f_u \in IRR(K[T_1,...T_n])$ te $m_1,...,m_u \geq 1$ takvi da je

$$f = \lambda f_1^{m_1} \cdot ... \cdot f_u^{m_u}. \tag{4.1}$$

Napomena 4.4. *Ako je K algebarski zatvoreno, možemo pisati $\lambda = (npr.) = \mu^{m_1}$, pa je tada $f = (\mu f_1)^{m_1} \cdot ... \cdot f_u^{m_u}$.*
Vidimo da se svaki $f \in K[T_1,...T_n]$ može zapisati kao $f = f_1^{m_1} \cdot ... \cdot f_u^{m_u}$, a prikaz je jedinstven do na permutaciju i asociranje.

Zadatak 4.5. *Uz oznake iz (4.1), ako je f homogen, tada su $f_1,...,f_u$ također homogeni.*

Rješenje. $f = \lambda f_1^{m_1} \cdot ... \cdot f_u^{m_u}$ je homogen. Iz zadatka 4.3 lako indukcijom dobijemo da su $f_1,...,f_u$ homogeni polinomi. □

Poglavlje 5

Algebarski skupovi u afinom prostoru

Neka je K nadalje algebarski zatvoreno polje. S algebre je poznata tvrdnja:

Teorem 5.1. *Za svako polje K postoji jedinstveno (do na izomorfizam) algebarski zatvoreno polje $\overline{K}$ koje sadrži početno polje K.*

Dakle postoje $\overline{\mathbb{Z}/p\mathbb{Z}}$, $\overline{\mathbb{Q}}$=polje algebarskih brojeva, $\overline{\mathbb{R}} = \mathbb{C}$. Prema tome, algebarska zatvorenost polja nije ograničavajući zahtjev.

Definicija 5.2. *n-dimenzionalni afini prostor $\mathbb{A}^n = K^n = \{(x_1,...,x_n)|x_i \in K\}$.*

Iz jednog koordinatnog sustava $X = (x_1,...,x_n)$ možemo u preći u novi $Y = (y_1,...,y_n)$ afinim preslikavanjem $Y = AX + b$, gdje je A regularni operator, a $b \in K^n$.

Za $f \in K[T_1,\dots,T_n]$ definiramo *evaluaciju* polinoma u točki $P = (t_1,...,t_n)$ na način:

$$f(P) = f(t_1,...,t_n) \in K$$

Definicija 5.3. *Algebarski skup $X \subset \mathbb{A}^n$ je svaki skup oblika*

$$X = \mathscr{Z}(f_1,...,f_n) := \{(t_1,...,t_n) \in \mathbb{A}^n | f_i(t_1,...,t_n) = 0, i = 1\dots n\}$$

to jest, skup nultočaka konačno mnogo polinoma.

Pretpostavimo da je $L \subset K$ neko potpolje npr. kao što su $\mathbb{Q}, \mathbb{R} \subset \mathbb{C}$. Neka su $f_1,...,f_n \in L[T_1,...,T_n]$. Možemo promatrati nultočke polinoma na nekom potpolju (npr. samo realne nultočke umjesto kompleksnih). Zato definiramo:

$$X(L) := \{(t_1,...,t_n) \in L^n | f_i(t_1,...,t_n) = 0, i = 1\ldots n\}$$

Primjeri: $L = \mathbb{R}, K = \mathbb{C}$

$X = \{(t_1,t_2) \in \mathbb{C}^2 | t_1^2 + t_2^2 + 1 = 0\}$ je beskonačan skup, ali $X \cap \mathbb{R}^2 = X(\mathbb{R}) = \emptyset$.

Slično tome, skupovi $X = \{(t_1,t_2) \in \mathbb{C}^2 | t_1^2 + t_2^2 - 1 = 0\}$ i $X = \{(t_1,t_2) \in \mathbb{C}^2 | t_1^2 + t_2^2 = 0\}$ se razlikuju od skupova rješenja istih jednadžbi u $\mathbb{R}$ (kružnica i točka).

Za $f_1,...,f_n \in \mathbb{R}[T_1,...,T_n]$ vrijedi:

$$\mathscr{X}(f_1,...,f_n)(\mathbb{R}) \neq \emptyset \Longleftrightarrow \text{ideal generiran s } f_1,...,f_n \text{ je pravi.}$$

Ovdje se nultočke traže u $\mathbb{C}$. S druge strane, problem ustvrđivanja $\mathscr{X}(f_1,...,f_n)(\mathbb{R}) \neq \emptyset$ je težak!

Ako je $X \subset \mathbb{A}^n = K^n$ algebarski zatvoreno polje, definiramo ideal

$$I(X) = \{f \in K[T_1,...,T_n] | \forall x \in X, f(x) = 0\}$$

tj. svi polinomi koji se poništavaju na nekom skupu X.

Na primjer:

Ako je $X = \mathbb{A}^n$, onda je $I(\mathbb{A}^n) = 0$.

Ako je $X = \emptyset$, onda je $I(\emptyset) = K[T_1,...,T_n]$.

I obratno:

Ako je $I(X) = K[T_1,...,T_n] \Longrightarrow 1$ se poništava u X, dakle $X = \emptyset$.

Isto $X \neq \emptyset \Longrightarrow I(X) \neq K[T_1,...,T_n]$

Kažemo da je I *radikal* ako $\forall a \in R$ t.d. $\exists k \geq 1$ t.d. $a^k \in I \Longrightarrow a \in I$.

Zadatak 5.4. *Dokažite: Za svaki $X \subset \mathbb{A}^n$ $I(X)$ je radikal u $K[T_1,...,T_n]$.*

Promotrimo strukturu ideala u $K[T_1,...,T_n]$. Za $n = 1$, $K[T_1]$ je domena glavnih ideala (naime imamo euklidov algoritam za polinome) - dakle svaki ideal je glavni. S druge strane, za $n \geq 2$ $K[T_1,...,T_n]$ nije(!) domena glavnih ideala.

Za dokaz toga, razmotrite ideal generiran s linearnim polinomima $\{x_1, x_2\}$.

Definicija 5.5. *Skup nultočaka jednog polinoma $f \in K[T_1,...,T_n], f \neq const.$:*

$$\mathscr{Z}(f) = \{(t_1,...,t_n) \in K^n | f(t_1,...,t_n) = 0\}.$$

nazivamo afina hiperploha.

Izdvojili smo konstantni polinom jer ako je $f = 0$ tada bi dobili cijeli $\mathbb{A}^n$, a u suprotnom bi imali $f = const \neq 0$ pa bi skup bio prazan.

Primjer 5.6. *Za $n = 1$, $f \in K[T_1], f \neq const.$ svaki f je oblika:*

$$f = \lambda(T-\mu_1)\dots(T-\mu_k), \lambda \in K \setminus \{0\}, \mu_i \in K$$

iz čega se jasno vidi da je $\mathscr{Z} = \{\mu_1,...,\mu_k\}$.

Zadatak 5.7.

1) Neka je $n \geq 1$ i $f \in K[T_1,...,T_n], f \neq 0$. Tada skup $\{(x_1,...,x_n) \in K^n | f(x_1,...,x_n) \neq 0\}$ ima beskonačno elemenata.

2) Neka je $n \geq 2, f \in K[T_1,...,T_n], f \neq const$. Tada hiperploha $\mathscr{Z}(f)$ ima beskonačno točaka. Uputa: Lema 3.16, 3.17. iz §3.

Teorem 5.8. *Neka su $f, g \in K[T_1,...,T_n] \neq const$. Tada je:*

1) $I(\mathscr{Z}(f))$ =glavni ideal u $K[T_1,...,T_n]$ generiran produktom $f_1,...,f_k$ gdje je $f = f_1^{m_1}...f_k^{m_k}$, f_i su ireducibilni i međusobno neasocirani. Pišemo $I(\mathscr{Z}(f)) = (f_1,...,f_n)$.

2) $\mathscr{Z}(f) = \mathscr{Z}(f_1) \cup \mathscr{Z}(f_2) \cup ... \cup \mathscr{Z}(f_k)$ i $\mathscr{Z}(f_i) \not\subset \mathscr{Z}(f_j)$ za $i \neq j$.

$\mathscr{Z}(f_i)$ nazivamo ireducibilne komponente od $\mathscr{Z}(f)$. Dakle, imamo rastav u ireducibilne komponente.

3) $\mathscr{Z}(f) = \mathscr{Z}(g) \Longleftrightarrow$ uz rastav od f kao gore i analogno za $g = g_1^{n_1}...g_l^{n_l}$, vrijedi:

$k = l$ i $(f_1...f_k) = (g_1...g_l)$ tj. postoji permutacija π t.d. $g_i = \lambda_i f_{\pi(i)}$ za $i = 1 \dots l$

Napomena: Hiperploha određuje ireducibilne faktore od f do na multiplicitet.

To je generalizacija činjenice da produkt $(T-\alpha_1)^{m_1}...(T-\alpha_k)^{m_k}$ ima nultočke $\alpha_1,...,\alpha_k$ neovisno o eksponentima $m_1,...,m_k$.

Dokaz teorema. 1) $\boxed{\subseteq}$ Neka je $h \in (f_1,...,f_k)$. Kako je to glavni ideal, slijedi da je h oblika $h = f_1...f_k \cdot F$ za neki $F \in K[T_1,...,T_n]$. Očito je svaka nultočka od f_i ujedno i nultočka od h, odnosno:

$\forall x \in \mathscr{Z}(f_1...f_k)$ vrijedi $h(x) = (f_1...f_k)(x)F(x) = 0$.

Dakle, $h(x) \in I(\mathscr{Z}(f)) \Longrightarrow (f_1...f_k) \subset (\mathscr{Z}(f))$.

$\boxed{\supseteq}$ Neka je $h \in I(\mathscr{Z}(f)) \Longrightarrow h(x) = 0, \forall x \in \mathscr{Z}(f_i), \forall i$

Fiksirajmo i: ako $f_i(x)$, onda $h(x) = 0$.

Prema teoremu 3.18. $f_i|h$ jer je f ireducibilan. $\Longrightarrow f_i|h, \forall i \Longrightarrow h \in (f_1...f_k)$.

2) $\mathscr{Z}(f)$ su nultočke of f pa za faktore od f očito vrijedi:

$$\mathscr{Z}(f) = \mathscr{Z}(f_1) \cup \mathscr{Z}(f_2) \cup ... \cup \mathscr{Z}(f_k) = \mathscr{Z}(f_1...f_k).$$

Za drugu tvrdnju pretpostavimo suprotno: $\mathscr{Z}(f_i) \subset \mathscr{Z}(f_j)$, za neke i, j.

$\Longrightarrow \forall x \in K, f_i(x) = 0 \Longrightarrow f_j(x) = 0$

$\xRightarrow{\text{Tm 3.18}} f_i|f_j \Longrightarrow f_i, f_j$ su asocirani jer su ireducibilni. $\Rightarrow\Leftarrow$

3) $\mathscr{Z}(f) = \mathscr{Z}(g) \implies I(\mathscr{Z}(f)) = I(\mathscr{Z}(g)) \xRightarrow{1)} (f_1...f_k) = (g_1...g_l)$

To znači da je $f_1...f_k = g_1...g_l \cdot F$ i $g_1...g_l = f_1...f_k \cdot G$. Množeći obje jednadžbe i krateći (jer je $K[T_1, ..., T_n$ integralna domena) dobijemo $FG = 1$ tj. F, G su konstantni pa su $f_1...f_k$ i$g_1...g_l$ asocirani. Iz ireducibilnosti f_i i g_i lako vidimo da za svaki faktor s lijeve ima odgovarajući faktor s desne strane pa je $k = l$. □

Korolar 5.9. *Neka je $X \subset \mathbb{A}^n$ hiperploha. $I(X)$ je generiran polinomom čiji su faktori multipliciteta 1 koji su jedinstveni do na konstantu. Ako je F taj polinom, onda $I(X) = (F)$, $\mathscr{Z}(F) = X$. F se naziva reducirana jednadžba hiperplohe.*

Npr. Za $n = 1$, imamo faktorizaciju $f = (T - \alpha_1)^{m_1}...(T - \alpha_k)^{m_k}$

Tada je $X = \mathscr{Z}(f)$ hiperploha u $\mathbb{A}^1 \Longrightarrow I(X) = ((T - \alpha_1)...(T - \alpha_k))$.

Ovdje je $(T - \alpha_1)...(T - \alpha_k)$ reducirana jednaždba hiperplohe.

Definicija 5.10. *Stupanj hiperplohe X je stupanj reducirane jednadžbe* $\deg X = \deg F$.

Primijetimo da je po korolaru defincija dobra. Obzirom na stupnjeve imamo nazivlje:

$n = 2$: pravac, konika, kubika, kvadrika

$n = 3$: ravnina, kvadrika

Općenito: hiperploha X stupnja 1 naziva se *hiperravnina*.

Zadatak 5.11. *Ako su f, g ireducibilni, $\mathscr{Z}(f) \subseteq \mathscr{Z}(g) \implies \mathscr{Z}(f) = \mathscr{Z}(g)$. ($f$ i g su asocirani).*

Zadatak 5.12. *Svaki algebarski skup* $X \subset \mathbb{A}^n, X \neq \emptyset, X \neq \mathbb{A}^n$ *je presjek konačnog broja hiperploha.*

Rješenje. Neka je X algebarski skup $\neq \emptyset, \mathbb{A}^n$. Tada je $X = \mathscr{Z}(f_1...f_l), f_i \in K[T_1,...,T_n]$.
Kako $X \neq \emptyset \implies f_i$ nisu konstantni.
Dakle $x \in X \iff f_1(x) = f_2(x) = ... = f_k(x) = 0 \iff \underbrace{x \in \mathscr{Z}(f_1) \cap ... \cap \mathscr{Z}(f_k)}_{\text{konačni presjek hiperploha}}$.

Zadatak 5.13. *Točka* $x = (x_1,...,x_n) \in \mathbb{A}^n$ *je presjek od n hiperploha* $\mathscr{Z}(T - x_i)$ *tj.*

$$\{x\} = \mathscr{Z}(T - x_1,...,T - x_n)$$

To znači da je točka alg. skup, ali nije hiperploha ukoliko je $n \geq 2$. *Naime, hiperploha ima beskonačno elemenata za* $n \geq 2$.

Zadatak 5.14. $P = (x_1,...,x_n), Q = (y_1,...,y_n)$ *onda pravac kroz točke* $P \neq Q$ *je:*
$PQ := \{(t_1,...,t_n) \in \mathbb{A}^n | t_i = x_i + u(y_i - x_i), 1 \leq i \leq n,$ *za neki* $u \in K\}$.
PQ je algebarski skup.

Zadatak 5.15. *Pojam hiperravnine i pojam pravca podudaraju se u* $\mathbb{A}^2$.

Definicija 5.16. *Hiperploha* $X \subset \mathbb{A}^n$ *je ireducibilna ako je generiran od* $I(X)$ *ireducibilan. (tj. reducirana jednadžba je ireducibilna).*

Napomena 5.17. *Ideal* $I \subset K[T_1,...,T_n]$ *je prost ako*
1)$I \neq K[T_1,...,T_n]$ *(I mora biti pravi ideal)*
2)$(\forall f, g \in K[T_1,...,T_n]) fg \in I \implies f \in I$ *ili* $g \in I$
Ekvivalentni zahtjev je: $\frac{K[T_1,...,T_n]}{I}$ *je integralna domena.*

Teorem 5.18. *Neka je* $X \subset \mathbb{A}^n$ *hiperploha. X je ireducibilan* $\iff I(X)$ *je prost.*

Dokaz. $\boxed{\Rightarrow}$Ako je X ireducibilan, $I(X) = (F)$, za ireducibilan polinom F.
Kako je F ireducibilan, nije konstanta pa je ideal (F) pravi.
Nadalje, ako je $fg \in (F) \iff F|fg \overset{1.23.}{\Longrightarrow} F|f$ ili $F|g \implies f \in (F)$ ili $g \in (F)$.
$\boxed{\Leftarrow}$ Neka je X hiperploha t.d. $I(X)$ je prost. Kako je X hiperploha $X = \mathscr{Z}(f)$ za neki f.
Faktoriziramo $F = F_1^{m_1}...F_k^{m_k}$, F_i su ireducibilni i neasocirani, $m_i \geq 1$.
Slijedi $I(X) = (F_1...F_k) \implies k = 1$.

Naime, za $k \geq 2 \implies F_1 \dots F_{k-1} \notin (F_1 \dots F_k)$ i $F_k \notin (F_1 \dots F_k)$, ali $(F_1 \dots F_{k-1})(F_k) \in (F_1 \dots F_k)$. Dakle, za $k \geq 2$ $I(X)$ ne bi bio prosti ideal. $\square$

Definicija 5.19. *Neka je $X \subset \mathbb{A}^n$ algebarski skup, $X \neq \emptyset$ ($iff I(X)$ je pravi ideal) je ireducibilan ako $I(X)$ je prost.*
Za $X \neq \emptyset$ kažemo da je reducibilan ako nije ireducibilan.

Zadatak 5.20. *Neka je X algebarski skup $\neq \emptyset, \mathbb{A}^n$. X je ireducibilan $\iff$*

$$(\forall f, g \in K[T_1, \dots, T_n])\ f(x)g(x) = 0, \forall x \in X \implies f(x) = 0, \forall x \in X \text{ ili } g(x) = 0, \forall x \in X$$

Uputa: $fg \in I(X) \implies f \in I(X)$ ili $g \in I(X)$.

Zadatak 5.21. *Pravac je ireducibilan algebarski skup.*

Rješenje. $PQ = \{(t_1, \dots, t_n) | t_i = x_i + u(y_i - x_i), u \in K, 1 \leq i \leq n\}$, $n \in K$ je parametar. Izračunati $I(PQ)$ nije lako te iz tog vidjeti da je prost. No, koristeći prethodni zadatak imamo
$f(t)g(t) = 0, \forall t \in PQ \implies f(x + u(y - x))g(x + u(y - x)) = 0, \forall u \in K$
Stavimo U varijablu $\implies f(x_1 + U(y_1 - x_1), \dots, x_n + U(y_n - x_n))g(x_1 + U(y_1 - x_1), \dots, x_n + U(y_n - x_n)) = 0$ u $K[U]$.
Jer je $K[U]$ integralna domena $\implies f(x + U(y - x)) = 0$ ili $g(x + U(y - x)) = 0$.
Evaluiramo $U \leftrightarrow u \in K \implies f = 0$ na PQ ili $g = 0$ na PQ.
Iz zadatka 5.21. slijedi tvrdnja.

Poglavlje 6

Algebarski skupovi u projektivnom prostoru

U ovom poglavlju, K će biti algebarski zatvoreno polje.

Definicija 6.1. *Neka je $n \in \mathbb{N}$. Definirajmo $\mathbb{A}^{n+1} := \{(x_0, x_1, \ldots, x_n) |\ x_i \in K\}$ i $O := (0, 0, \ldots, 0) \in \mathbb{A}^{n+1}$. Na skupu $\mathbb{A}^{n+1} \setminus \{O\}$ definiramo relaciju:*

$$P \sim Q \iff O, P \text{ i } Q \text{ leže na istom pravcu}$$

(u smislu zadatka 6. u poglavlju 5.)

Napomena 6.2. *Neka je $P = (x_0, \ldots, x_n)$, a $Q = (y_0, \ldots, y_n)$. O, P i Q će ležati na istom pravcu ako i samo ako postoji $\lambda \in K \setminus \{O\}$, takav da vrijedi $y_i = \lambda x_i$, za svaki $0 \leq i \leq n$.*

Zadatak 6.3. *Relacija $\sim$ je relacija ekvivalencije na $\mathbb{A}^{n+1} \setminus \{O\}$.*

Zbog prethodnog zadatka sada možemo definirati:

Definicija 6.4. *Neka je $P = (x_0, \ldots, x_n) \in \mathbb{A}^{n+1} \setminus \{O\}$. Definiramo klasu ekvivalencije: $(x_0 : \ldots : x_n) := \{(\lambda x_0, \ldots, \lambda x_n) |\ \lambda \in K \setminus \{0\}\} = OP \setminus \{O\}$.*

Definicija 6.5. *Neka je $n \in \mathbb{N}$. Definiramo n-dimenzionalni projektivni prostor:*
$\mathbb{P}^n := \mathbb{A}^{n+1} \setminus \{0\}/_\sim = \{(x_0 : \ldots : x_n) |\ (x_0, \ldots, x_n)\ \in \mathbb{A}^{n+1} \setminus \{O\}\}$.

Napomena 6.6. *Projektivni prostor $\mathbb{P}^n$ je moguće identificirati sa skupom pravaca u $\mathbb{A}^{n+1} \setminus \{O\}\}$.*

Sada je jasno definirano *kanonsko preslikavanje*, $(x_0,\ldots,x_n) \vdash (x_0:\ldots:x_n)$, definirano sa $\mathbb{A}^{n+1}\setminus\{O\}\}$ u $\mathbb{P}^n$.

Napomena 6.7. *Koordinate* $(x_0:\ldots:x_n)=(tx_0:\ldots:tx_n), \forall t\in K\setminus\{0\}$ *nazivamo homogenim koordinatama. Uvijek uzimamo da je barem jedan* $x_i \neq 0$.

Nakon ovakve definicije nailazimo na problem: nema smisla evaluirati polinom $f \in K[T_1,\ldots,T_n]$ u točkama projektivnog prostora. Ipak, za danu točku projektivnog prostora $(x_0:\ldots:x_n)$, htjeli bismo imati vezu sa evaluacijom polinoma u pripadnoj točki $(x_0,\ldots,x_n)$ afinog prostora. Pretpostavimo da je f homogen stupnja homogenosti m. Tada je $f(tx_0:\ldots:tx_n)=t^m f(x_0,\ldots,x_n)$, za svaki t. I dalje ne možemo reći kolika je vrijednost od f u točki projektivnog prostora, ali možemo reći poništava li se f u njoj ili ne.

Definicija 6.8. *Kažemo da se polinom* $f\in K[T_1,\ldots,T_n]$ *poništava u točki* $(x_0:\ldots:x_n)$ *projektivnog prostora ako vrijedi* $f(x_0,\ldots,x_n)\neq 0$.

Napomena 6.9. *Ako je* f *homogen stupnja homogenosti* ≥ 1, *odnosno, ako je* f *nekonstantan polinom, onda je* $f(0,\ldots,0)=0$.

Dakle, sada možemo ovako definirati:

Definicija 6.10. *Homogen polinom* $f\in K[T_1,\ldots,T_n]$ *poništava se u točki* $(x_0:\ldots:x_n)$ *ako i samo ako se poništava na cijelom afinom pravcu koji prolazi kroz O i* $((x_0,\ldots,x_n)$.

Napomena 6.11. *Polinom* f *se ne poništava u* $(x_0:\ldots:x_n)$ *ako i samo ako je* $f(P)\neq 0$, *za svaku točku tog pravca, osim za* $P=O$.

Definicija 6.12. *Algebarski skup u* $\mathbb{P}^n$ *je skup* $X\subseteq\mathbb{P}^n$ *oblika* $X=\mathscr{Z}(f_1,\ldots,f_t)$, *gdje su* $f_!,\ldots,f_t$ *homogeni polinomi (ne nužno istog stupnja).*
Slično kao i prije, $\mathscr{Z}(f_1,\ldots,f_t)=\{(x_0:\ldots.:x_n)|\ f_i(x_0,\ldots,x_n)=0,\forall i\}$.

Definicija 6.13. *Za homogen, nekonstantan polinom* f, $\mathscr{Z}(f)$ *nazivamo (projektivnom) hiperplohom.*
Skup $D(f)=\mathbb{P}^n\setminus\mathscr{Z}(f)$ *nazivamo glavnim otvorenim skupom u* $\mathbb{P}^n$.

Važna će nam biti sljedeća konstrukcija:

Neka je $X \subseteq \mathbb{P}^n$ bilo koji skup.

KORAK 1: Neka je $\mathscr{F}$ skup svih homogenih polinoma iz $K[T_0,\dots,T_n]$ koji se poništavaju u svakoj točki skupa X.

KORAK 2: Definiramo $I(X) \subseteq K[T_0,\dots,T_n]$ ideal generiran skupom $\mathscr{F}$ iz koraka 1.

Eksplicitno, imamo:

$I(X) = \{\sum_{i=1}^{l} h_i g_i |\ h_i \in K[T_0,\dots,T_n], g_i \in \mathscr{F}, l \geq 1\}$

Definicija 6.14. *Ideal $I \subseteq K[T_0,\dots,T_n]$ je homogen, ako za svaki polinom $f \in I$ vrijedi da je $f_m \in I, \forall m \geq 0$ (vidi poglavlje 4).*

Zadatak 6.15. *Ideal generiran homogenim polinomima (konačno ili beskonačno mnogo njih) je homogen.*

Zadatak 6.16.

1) $I(X)$ je homogen radikal.

2) $I(X)$ je pravi ideal $\iff X \neq 0$.

3) $f \in I(X)$ je homogen $\iff$ f se poništava u svakoj točki od X.

Rješenje. Pokažimo prvo da je $I(X)$ homogen.

Neka je $\mathscr{F}$ skup svih polinoma koji se poništavaju na X.

Tada za svaki $f \in I(X)$ postoje $m \geq 1$ te $g_1,\dots,g_m \in \mathscr{F}$ i $h_1,\dots,h_m \in K[T_0,\dots,T_n]$ takvi da vrijedi:

$f = \sum_{i=1}^{m} h_i g_i = \sum_{i=1}^{m} \sum_{n\geq 0} (h_i)_n g_i = \{\text{složimo po stupnju od h}\} = \sum_{t\geq 0}(\sum_{n\geq 0, 1\leq i\leq m, n+deg(g_i)=t} (h_i)_n g_i)$.

Budući da je posljednji izraz u zagradama očito element od $I(X)$, slijedi da je $f_t \in I(X), \forall t \geq 0$, odnosno, $I(X)$ je homogen.

3) Ako je f homogen, tada postoji $t \geq 0$ takav da je $f = f_t$. Budući da se g_i poništava na X, slijedi da je $f = f_t = 0$ na X.

2) $I(X) \neq K[T_0,\dots,T_n] \iff \mathbb{1} \notin I(X) \iff \mathbb{1}$ se ne poništava na X (koristimo 3) i činjenicu da je $\mathbb{1}$ homogen) $\iff X \neq 0$.

1) Još nam je preostalo pokazati da je $I(X)$ radikal.

Želimo pokazati: $f^t \in I(X) \implies f \in I(X)$, gdje je $f \in K[T_0,\dots,T_n]$, $t \geq 1$ proizvoljan.

Ako je $f = 0$, tvrdnja očito vrijedi.

Pretpostavimo zato da $f \neq 0$. Tada je $f = f_0 + \cdots + f_n$, gdje je $f_n \neq 0$. Po zadatku 1 iz poglavlja 4 (to treba popraviti) znamo da je:

$$f^t = f_m^t + \text{(homogene komponente stupnja} < t \cdot m) \qquad .$$

Budući da je $I(X)$ homogen, slijedi da je $f_m^t \in I(X)$, a iz toga po 3) slijedi da je $f_m^t = 0$ na X. Dakle, $f_m = 0$ na X, pa je $f_m \in I(X)$.

Slijedi:

$(f - f_m)^t =$ binomni teorem $= f^t + \sum_{i=0} t - 1 \binom{t}{i} f^i (-1)^{t-i} f_m^{t-i}$.

Kako je prvi sumand po pretpostavci iz $I(X)$, a drugi sumand je iz $I(X)$ jer je $f_m \in I(X)$ i $t - i \geq 1$, slijedi da je $(f - f_m)^t \in I(X)$. Dalje se nastavi indukcijom.

Definicija 6.17. *Algebarski skup $X \subseteq \mathbb{P}^n$ je ireducibilan ako je X neprazan i $I(X)$ prost ideal. (Usporedite s poglavljem 5).*

Algebarski skup $X \subseteq \mathbb{P}^n$ je reducibilan ako je X neprazan i $I(X)$ nije prost ideal.

Ireducibilan algebarski skup u $\mathbb{P}^n$ se naziva projektivna mnogostrukost.

Zadatak 6.18. *(Karakterizacija ireducibilnosti)*

Neka je $X \subseteq \mathbb{P}^n$ neprazan. Tada je X ireducibilan ako i samo ako za sve nekonstantne $f, g \in K[T_0, \ldots, T_n]$ vrijedi:

$$f \cdot g = 0 \text{ na } X \implies f = 0 \text{ na } X \text{ ili } g = 0 \text{ na } X \qquad (\star)$$

Rješenje. Lako je pokazati da možemo dozvoliti da f i g budu konstantni jer tada zaključak u $(\star)$ vrijedi.

Uz tu napomenu slijedi reformulacija od $(\star)$:

$$(\forall f, g \text{ homogen})\ f \cdot g \in I(X) \implies f \in I(X) \text{ ili } g \in I(X) \quad (\star - 1).$$

Po definiciji vrijedi: X ireducibilan $\iff$ X prost $\iff$

$$(\forall f, g)\ f \cdot g \in I(X) \implies f \in I(X) \text{ ili } g \in I(X) \quad (\star\star) \qquad .$$

Dakle, preostaje nam pokazati da je: $(\star - 1) \iff (\star\star)$.

$(\impliedby)$ očito vrijedi. Pokažimo još obrat.

$(\implies)$ Pretpostavimo suprotno, tj. da je $f \cdot g \in I(X)$, ali $f \notin I(X)$ i $g \notin I(X)$. Budući da $f \cdot g \in I(X)$, slijedi da postoji homogena komponenta od f koja nije u $I(X)$. Analogno, postoji homogena komponenta od g koja nije u $I(X)$.

Neka je $f = F_1 + F_2$, pri čemu je F_1 suma homogenih komponenti od f sadržanih u $I(X)$, a F_2 suma homogenih komponenti od f koje nisu sadržane u $I(X)$. Analogno, neka je

$g = G_1 + G_2$. Po našoj pretpostavci, $F_2, G_2 \neq 0$, odnosno $F_2 = (F_2)_0 + \cdots + (F_2)_v$, pri čemu je $(F_2)_v \neq 0$ i $G_2 = (G_2)_0 + \cdots + (G_2)_w$, pri čemu je $(G_2)_w \neq 0$.

Budući da je $f \cdot g \in I(X)$, slijedi da je $(F_1 + F_2) \cdot (G_1 + G_2) \in (X)$, pa je i $F_2 \cdot G_2 \in I(X)$, odnosno $((F_2)_v \cdot (G_2)_w +$ niži stupnjevi homogenosti$) \in I(X)$.

Dakle, s obzirom da je $I(X)$ homogen, slijedi da je $(F_2)_v \cdot (G_2)_w \in I(X)$, pa po $(\star - 1)$ slijedi da je $(F_2)_v$ ili $(G_2)_w \in I(X)$. No, to je kontradikcija s konstrukcijom F_2 i G_2.

Neka je $f \in K[T_1, \ldots, T_n]$ homogen i nekonstantan. Tada je $\mathscr{Z}(f)$ hiperploha.

Po zadatku 3 iz poglavlja 4 (popraviti) znamo da je $f = f_1^{k_1} \cdots f_t^{k_t}$, gdje su f_i ireducibilni međusobno neasocirani homogeni polinomi, a $k_i \geq 1$. Zato je $\mathscr{Z}(f_i)$ dobro definirana hiperploha, za svaki i.

Kao u 5. poglavlju, imamo $\mathscr{Z}(f) = \mathscr{Z}(f_1) \cup \cdots \cup \mathscr{Z}(f_t) = \mathscr{Z}(f_1 \cdots f_t)$. Također, za homogen i nekonstantan $g \in K[T_1, \ldots, T_n]$ je $g = g_1^{l_1} \cdots g_n^{l_n}$ te je $\mathscr{Z}(g) = \mathscr{Z}(g_1) \cup \cdots \cup \mathscr{Z}(g_n) = \mathscr{Z}(g_1 \cdots g_n)$. Slijedi analogon Teorema 1 iz poglavlja 5:

Teorem 6.19.

1) $I(\mathscr{Z}(f)) =< f_1 \cdots f_t >$

2) $\mathscr{Z}(f_i) \nsubseteq \mathscr{Z}(f_j)$, *za* $i \neq j$

3) $\mathscr{Z}(f) = \mathscr{Z}(g) \iff t = n$ *te se* f_i *i* g_j *ne razlikuju do na permutaciju i asociranost.*

Skica dokaza. Redukcija na afini slučaj (Teorem 1, poglavlje 5).

Imamo kanonsko preslikavanje ϕ koje $(x_0, \ldots, x_n) \in \mathbb{A}^{n+1} \setminus \{0\}$ pridružuje $(x_0 : \cdots : x_n)$ te promatramo afine analogone funkcija f, f_i, g, g_i. Važno je uočiti da nijedna od tih funkcija nije konstantna i sve su homogene. Zato se sve poništavaju u $O \in \mathbb{A}^{n+1}$.

Na primjer:

$\mathscr{Z}_{\mathbb{A}^{n+1}}(f) = \{(x_0 : \cdots : x_n) \in \mathbb{A}^{n+1} | \, f(x_0, \cdots, x_n) = 0\}$ i

$\mathscr{Z}(f) = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n | \, f(x_0, \cdots, x_n) = 0\}$.

$\phi^{-1}(\mathscr{Z}(f)) = \mathscr{Z}_{\mathbb{A}^{n+1}} \setminus \{0\}$.

$\phi(\mathscr{Z}_{\mathbb{A}^{n+1}}(f) \setminus \{0\}) = \mathscr{Z}(f)$.

$\mathscr{Z}_{\mathbb{A}^{n+1}}(f)$ je afini konus nad projektivnim algebarskim skupom $\mathscr{Z}(f)$. Znamo: $I_{\mathbb{A}^{n+1}}(\mathscr{Z}_{\mathbb{A}^{n+1}}(f)) =< f_1 \cdots f_t >$.

Za domaću zadaću pokažite da iz zadatka 1 iz ovog poglavlja slijedi $I(\mathscr{Z}(f)) =< f_1, \ldots, f_t >$

te da 2) i 3) slijede iz Teorema 1 iz poglavlja 5.

Zadatak 6.20. *Opišite hiperplohe u* $\mathscr{P}^1$.

Rješenje. $\mathbb{P}^1 = \{(s,t)|\ s,\ t \in K,\ s \neq 0 \text{ ili } t \neq 0\}$.

Neka je $f \in K[S,\ T]$ homogen stupnja m i nekonstantan te $\mathscr{Z}(f) = \{(s,t)|\ f(s,t) = 0\}$ hiperploha u $\mathbb{P}^1$. Tada je $f = a_m \cdot S^m + a_{m-1} \cdot S^{m-1} \cdot T + \cdots + a_1 \cdot S \cdot T^{m-1} + a_0 \cdot T^m$, gdje su $a_i \in K$, a barem jedan je različit od 0. Neka je $k \leq m$ najveći takav da je $a_k \neq 0$. Dakle, $a_m = a_{m-1} = \cdots = a_{k+1} = 0$, $a_k \neq 0$.

Tada je:

$f = a_k \cdot S^k \cdot T^{m-k} + \cdots + a_0 \cdot T^m$ u polju racionalnih funkcija

$= T^m(a_k \cdot (\frac{S}{T})^k + a_{k-1} \cdot (\frac{S}{T})^{k-1} + \cdots + a_1 \cdot (\frac{S}{T}) + a_0)$

(izraz u zagradi je polinom s koeficijentima iz K stupnja k u $\frac{S}{T}$)

$= T^m a_k \cdot (\frac{S}{T} - \alpha_1) \cdots (\frac{S}{T} - \alpha_k)$, za neke $\alpha_1, \ldots \alpha_k \in K$ (algebarski zatvoreno polje)

$= T^{m-k} a_k \cdot (S - \alpha_1 T) \cdots (S - \alpha_k T)$.

Ovime smo dobili faktorizaciju polinoma f u ireducibilne faktore.

Tražimo $(s : t)$ takve da je $f(s,t) = 0$. Prva mogućnost je da je $t = 0$, ako je $m - k \geq 1$). U tom slučaju, $s \neq 0$ i rješenje je $(s : t) = (s : 0) = (1 : 0)$ (zbog homogenosti). Druga mogućnost je da je $s = \alpha_i$, a tada je $t \neq 0$ jer inače bi i t i s bili 0. Dakle, u tom slučaju rješenje je $(s : t) = (\alpha_i t : t) = (\alpha_i : 1)$.

Dakle, dobili smo da je $\mathscr{Z}(f) = \{(1:0), (\alpha_1 : 1), \ldots (\alpha_k : 1)\}$, pri čemu prva točka postoji ako je $k \leq m$, a drugih k točaka postoji ako je $k > 0$.

Zadatak 6.21. *(Obrat)*

Svaki konačan neprazan $X \subseteq \mathbb{P}^1$ *je hiperploha.*

(Uputa: Obratan smjer zaključivanja; prvo krenemo od skupa, sastavimo polinom.)

Napomena 6.22. *U* $\mathbb{P}^1$ *postoje hiperplohe koje se ne sijeku.*

$$\{(1:0)\} \cap \{(0:1)\} \neq \emptyset$$

Međutim, u 8. poglavlju ćemo dokazati da se u $\mathbb{P}n, n \geq 2$ *sve hiperplohe sijeku.*

Zadatak 6.23. *Svaki neprazan algebarski skup u* $\mathbb{P}^n$*, koji nije jednak cijelom* $\mathbb{P}^n$*, je presjek konačnog broja hiperploha. (Uputa: zadatak 4 iz poglavlja 5)*

Zadatak 6.24. *Definirajte pojam stupnja hiperplohe (kao u 5. poglavlju) i pojam stupnja reducirane jednadžbe hiperplohe.*

Znamo: hiperploha X je ireducibilna $\iff$ ideal $I(X)$ je ireducibilan. (Teorem 1, poglavlje 5). Hiperravninu, pravac u $\mathbb{P}^2$ i krivulju u $\mathbb{P}^2$ definiramo jednako kao i u afinom slučaju (vidi poglavlje 5).

Poglavlje 7

Neki rezultati o homogenim polinomima

U §7. *iznimno* dopuštamo da polje K nije algebarski zatvoreno. Dakle K je nadalje proizvoljno polje: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}, \mathbb{C}(T_1, ..., T_n)$ Neka su $f, g \in K[T_0, ..., T_n]$ nekonstantni homogeni polinomi stupnjeva $l, m > 0$ respektivno .

$\implies f =$ zapis po varijabli $T_n = \sum\limits_{i=0}^{l} f_i T_n^i$ gdje su $f_i \in K[T_0, ..., T_{n-1}]$ homogeni polinomi stupnja $l - i \implies f_l = const.$

Isto, $g = \sum\limits_{j=0}^{m} f_j T_n^i$ gdje su g_i homogeni stupnja $m - i$, $g_m = const$

Za $0 \leq i \leq l - 1 \implies f_i$ stupnja $l - i \geq 1 \implies f_i \underbrace{(0, ..., 0)}_{\text{n-1}} = 0$

Za Za $0 \leq i \leq m - 1 \implies g_j$ stupnja $m - j \geq 1 \implies g_i(0, ..., 0) = 0$

Iz toga se vidi da $f(0, ..., 0, 1) \neq 0$ tj. $f_l \neq 0$. Analogno $g_m \neq 0$.

Dakle: ako je $f(0, ..., 0, 1) \neq 0 \implies f$ polinom stupnja l u varijabli T_n.

pa se može zapisati $f = \underset{\neq 0}{f_l} T_n^l +$ niže potencije od T_n. Slično za g.

Propozicija 7.1. *Ako su $f, g \in K[T_0, ..., T_n]$ homogeni, stupnjeva $l, m > 0$ te ako $f(0, ..., 0, 1) \neq 0, g(0, ..., 0, 1) \neq 0$, tada:*

1) $\mathrm{Res}_{T_n}(f, g) \in K[T_0, ..., T_{n-1}$ *je homogen stupnja homogenosti lm*

2) $\mathrm{Res}_{T_n}(f, g) \neq 0 \iff$ *f i g nemaju zajedničkih faktora u $K[T_0, ..., T_n]$*

3) $\exists A, B \in K[T_0, ..., T_n]$ *t.d.* $Af + Bg = \mathrm{Res}_{T_n}(f, g)$

Dokaz: $f(0,...,0,1), g(0,...,0,1) \neq 0 \implies f$ i g stupnja l,$m > 0$, u varijabli T_n.

$$\mathrm{Res}_{T_n}(f,g) = §3 = \begin{vmatrix} f_0 & f_1 & f_2 & \cdots & f_l & & & \\ & f_0 & f_1 & f_2 & \cdots & f_l & & \\ & & \ddots & & & & \ddots & \\ & & & f_0 & f_1 & f_2 & \cdots & f_l \\ g_0 & g_1 & g_2 & \cdots & g_m & & & \\ & g_0 & g_1 & g_2 & \cdots & g_m & & \\ & & \ddots & & & & \ddots & \\ & & & g_0 & g_1 & g_2 & \cdots & g_m \end{vmatrix} \in K[T_0,...,T_{n-1}]$$

Prema teoremu 3.14. slijedi 3).

Prema teoremu 3.5. $\mathrm{Res}_{T_n}(f,g) = 0 \iff f,g$ nemaju zajedničkih ireducibilnih faktora koji ovise o T_n.

Iduća napomena dokazuje tvrdnju 2):

f,g nemaju zajednički faktor $h \neq const, h \in K[T_0,...,T_{n-1}][T_n]$

Zašto? Kad bi postojao h tako da $h|f, h|g \implies f = hF, g = hG\ F,G \in K[T_1,...,T_n]$

Imali bi: $f_l T_n^n + f_{l-1}T_n^{l-1} + ... + f_1 T^n + f_0 = f = h \cdot F = h(F_{l_1}T_n^{l_1} + ... + F_1 T^n + F_0)$.

Kako h ne ovisi o T_n moralo bi biti $l = l_1$. No tada je $hF_{l_1} = f_l = const \neq 0$ pa je h konstantan $\implies$. Ovo dokazuje tvrdnju 2).

Preostaje tvrdnja 1) $\mathrm{Res}_{T_n}(f,g)$ homogen, stupnja $l \cdot m$.

Na mjestu (i,j) u $\mathrm{Res}_{T_n}(f,g)$ nazovimo odgovarajući polinom $F_{i,j}$.

Po definiciji determinante $Res_{T_n}(f,g) = \sum\limits_{\substack{\pi perm. \\ \{1,2,...,l+m\}}} (-1)^{\text{parnost od }\pi} \cdot F_{1,\pi(1)} \cdot ... \cdot F_{l+m,\pi(l+m)}$

$\forall \pi$, $\prod\limits_{i=1}^{l+m} F_{i,\pi(i)}$ homogen stupnja $l \cdot m$ - najčešće je ovo 0. Tada je stvar jasna.

Tražimo kada je moguće $\neq 0$? Neka je $1 \leq i \leq m \implies$

$$F_{1,1} = f_0, F_{1,2} = f_1, ..., F_{1,l+1} = f_l$$
$$F_{2,2} = f_0, F_{2,3} = f_1, ..., F_{2,l+2} = f_l$$
$$\vdots$$
$$F_{i,i} = f_0, F_{i,i+1} = f_1, ..., F_{i,l+i} = f_l$$

Za $m+1 \leq i \leq l+m$ vrijedi:

$F_{i,i} = g_m, F_{i,i+1} = g_{m-i}, ..., F_{i,i-m} = g_0$ (od dijagonale prema lijevo)

Ako je $\prod_{i=1}^{l+m} F_{i,\pi(i)} \neq 0 \implies 1 \leq i \leq m, i \leq \pi(i) \leq i+l$ pa imamo produkt:

$$\prod_{i=1}^{l+m} F_{i,\pi(i)} = \prod_{i=1}^{m} F_{i,\pi(i)} \prod_{i=m+1}^{m+l} F_{i,\pi(i)} = \prod_{i=1}^{m} f_{\pi(i)-i} \prod_{i=m+1}^{m+l} g_{m-i+\pi(i)}$$

Računamo stupanj: $f_{\pi(i)-i}$ je stupnja homogenosti $l - (\pi(i) - i)$

Isto tako $g_{m+\pi(i)-i}$ je stupnja homogenosti $m - (m + \pi(i) - i) = i - \pi(i)$

Ukupni stupanj je:

$$\sum_{i=1}^{m}(l - \pi(i) + i) + \sum_{i=m+1}^{l+m}(i - \pi(i)) = lm + \sum_{i=1}^{l+m}(i - \pi(i)) = lm + \sum_{i=1}^{l+m} i - \sum_{i=1}^{l+m} \pi(i) = lm$$

□

Primjene u algebri:

Neka je $l, m > 0$ i promotrimo polinome iz $K[T, R_1, ..., R_l, U_1, ..., U_m]$. Stavimo

$f = \prod_{i=1}^{l}(T - R_i) = T^l - (R_1 + ... + R_k)T^{l-1} + ... + (-1)^l R_1 ... R_l$

$g = \prod_{i=1}^{m}(T - U_i) = T^l - (U_1 + ... + U_m)T^{l-1} + ... + (-1)^l U_1 ... U_m$

$T - R_i, T - U_j, R_i - U_j, 1 \leq i \leq$ su homogeni, stupnja 1 pa ireducibilni te međusobno neasocirani.

Vrijedi $f(1, \underbrace{0, ..., 0}_{\text{R-dio}}, \underbrace{0, ..., 0}_{\text{U-dio}}) = (1)^l = 1 \neq 0$

isto tako $g(1, \underbrace{0, ..., 0}_{\text{R-dio}}, \underbrace{0, ..., 0}_{\text{U-dio}}) = (1)^m = 1 \neq 0$

Može se primijeniti propozicija 7.1.

Korolar 7.2.

$$\mathrm{Res}_T(f, g) = (-1)^{lm} \prod_{i=1}^{l} \prod_{j=1}^{m} (R_i - U_j)$$

Dokaz: 1. KORAK

Prema propoziciji 7.1. $\text{Res}_T(f,g)$ homogen je polinom iz $K[R_1,...,R_l,U_1,...,U_m]$

2. KORAK

Desna strana $\prod_{i=1}^{l}\prod_{j=1}^{m}(R_i-U_j)$ je također stupnja lm, produkt neasociranih linearnih faktora R_i-U_j.

Dokažimo OPĆU LEMU:

Neka je $F=F(S,S_1,...,S_t)\in K[S,S_1,...,S_t]$. Tada

$(S-S_i)|F$ u $K[S_1,...,S_t]$, $\forall i=1...t \iff F(S_i,S_1,...,S_t)=0$ (nul-polinom) u $K[S_1,...,S_t]$.

Dokaz: $K[S,S_1,...,S_t]=D[S]$, uzimajući pritom $D=K[S_1,...,S_t]$.

F, $S-S_i\in D[S]$ su zadani $i\in\{1,...,t\}$

$S-S_i$ ima vodeći koeficijent 1. Koristeći Euklidov algoritam

$$F=(S-S_i)G-R,G\in D[S],R\in D$$

Uvrstimo $S_i \implies F(S_i,...,S_t)=(S_i-S_i)(...)+R(S_1,...,S_t) \implies R(S_1,...,R_t)=0$

3. KORAK $(R_i-U_j)|\text{Res}_T(f,g),\forall i,j$

Dokažimo to! $\text{Res}_T(f,g)(R_1,...,R_{i-1},R_i,R_{i+1},...,R_l,U_1,...,U_{j-1},U_j,U_{j+1},...,U_m)$

Ako uvrstimo U_j dobili bi rezultantu po T od f_1 i g, gdje je $f_1=f$ do na neki $T-U_j$. Tada bi polinomi imali zajednički faktor $T-U_j \implies \text{Res}(f,g)=0 \implies$ Opća lema $\implies (R_i-U_j)|\text{Res}_T(f,g)$

4. KORAK $\prod_{i=1}^{l}\prod_{j=1}^{m}(R_i-U_j)|\text{Res}_t(f,g)$

Dokaz: Slijedi iz koraka 3 i što su R_i-U_j međusobno neasocirani i ireducibilni.

5. KORAK $\text{Res}_T(f,g)=\underset{\in K}{a}\cdot\prod_{i=1}^{l}\prod_{j=1}^{m}(R_i-U_j)$

Dokaz: Koraci 1,2,4.

6. KORAK $a=(-1)^{lm}$

Dokaz: Raspišemo rezultantu:

$$\operatorname{Res}_T(f,g) = \begin{vmatrix} (-1)^l R_1 ... R_l & \cdots & -(R_1 + ... + R_l) & 1 & & \\ & \ddots & & \ddots & & \\ & & \ddots & & \ddots & \\ & & (-1)^l R_1 ... R_l & \cdots & -(R_1 + ... + R_l) & 1 \\ (-1)^m U_1 ... U_m & \cdots & 1 & & & \\ \ddots & & \ddots & & & \\ & \ddots & & \ddots & & \\ & & (-1)^m U_1 ... U_m & \cdots & 1 & \end{vmatrix} \in K[T_0, ..., T_{n-1}]$$

Računamo rezultantu po Laplaceovom razvoju - zanima nas samo koeficijent uz $(R_1 ... R_l)^m$!
$\Longrightarrow \operatorname{Res}_T(f,g) = ((-1)^l (R_1 ... R_l))^m + ... = (-1)^{lm} (R_1 ... R_m)^m + ...$
S druge strane $\prod\limits_{i=1}^{l} \prod\limits_{j=1}^{m} (R_i - U_j) = (R_1 ... R_l)^m + ...$ pa uspoređivanjem koeficijenata napokon dobijemo $a = (-1)^{lm}$. □

Korolar 7.3. *Ako je K polje i L algebarski zatvoreno polje ($K \subset L$).*
$f, g \in K[T]$ stupnja $l, m > 0$ respektivno $\Longrightarrow \operatorname{Res}(f,g) = (-1)^{lm} a^m \prod\limits_{i=1}^{l} g(\alpha_i)$
(α_i su korijeni od f).

Dokaz:

$$\operatorname{Res}_T((T - R_1)...(T - R_l), (T - U_1)...(T - U_m)) \overset{\text{Kor7.2}}{=} (-1)^{lm} \prod_{i=1}^{l} \prod_{j=1}^{m} (\alpha_i - \beta_j)$$

Iz definicije rezultante (i svojstava determinanti):

$$\operatorname{Res}\left(\frac{f}{a}, \frac{g}{b}\right) = \frac{1}{a^m} \frac{1}{b^l} \operatorname{Res}(f,g)$$

$$\Longrightarrow Res(f,g) = (-1)^{lm} a^m \prod_{i=1}^{l} \left(b \prod_{j=1}^{m} (\alpha_i - \beta_j) \right) = (-1)^{lm} a^m \prod_{j=1}^{l} g(\alpha_i)$$

□

Korolar 7.4. *Neka su $f_1, f_2, g \in K[T]$ pozitivnog stupnja u T. Vrijedi*

$$\operatorname{Res}(f_1 f_2, g) = \operatorname{Res}(f_1, g) \operatorname{Res}(f_2, g)$$

Za char$K = 0$, bilo koje polje ($\subset L$, neko alg. zatvoreno polje). Uzimajući $f = aT^l + ...$, derivacija je $f' = laT^{l-1} + ...$ Kako je *diskriminanta* polinoma f jednaka $\mathrm{Res}(f, f')$, iz prethodnog korolara dobivamo:

$$\mathrm{disc}(f) = (-1)^{l(l-1)} a^{l-1} \prod_{i=1}^{l} f'(\alpha_i)$$

Kako je za $f = a(T - \alpha_1)...(T - \alpha_l) \implies f' = a \sum_{i=1}^{l} \prod_{j \neq i} (T - \alpha_j)$

$$\implies \mathrm{Res}(f, f') = (-1)^{l(l-1)} a^{l-1} \prod_{i=1}^{l} f'(\alpha_i) = (-1)^{l(l-1)} a^{2l-1} \prod_{\substack{i,j \\ i \neq j}}$$

$$= (-1)^{l(l-1)} a^{2l-1} \prod_{1 \leq i < j \leq l} \left(-(\alpha_i - \alpha_j)^2\right) = (-1)^{l(l-1)} a^{2l-1} (-1)^{\frac{l(l-1)}{2}} \prod_{1 \leq i < j \leq l} (\alpha_i - \alpha_j)^2$$

Korolar 7.5.

$$\mathrm{disc}(f) = \mathrm{Res}(f, f') = (-1)^{\frac{l(l-1)}{2}} a^{2l-1} \prod_{1 \leq i < j \leq l} (\alpha_i - \alpha_j)^2$$

Zadatak 7.6. *Neka je K bilo koje polje, $f \in K[T_1, ..., T_n]$ homogen stupnja m. Vrijedi:*
1.) $\frac{\partial f}{\partial T_i} \in K[T_1, ..., T_n]$ je homogen stupnja $m - 1$
2.) Eulerova formula:

$$\sum_{i=0}^{n} T_i \frac{\partial f_i}{\partial T_i} = mf$$

Uputa: provjerite za monome, iskoristite linearnost derivacije.

Poglavlje 8

Primjeri projektivnih mnogostrukosti, centralna projekcija i primjene

U ovom poglavlju K će biti algebarski zatvoreno polje.

Sjetimo se:
$X \subseteq \mathbb{P}^n$ algebarski skup $\stackrel{def.}{=}$ skup svih nultočki konačnog broja homogenih polinoma iz $K[T_0, ..., T_n]$.
$I(X)$ je ideal u $K[T_0, ..., T_n]$ generiran svim homogenim polinomima koji se poništavaju na X.
$X \neq \emptyset \iff I(X)$ je pravi ideal, tj. $I(X) \neq K[T_0, ..., T_n]$.
Algebarski skup $X \neq \emptyset$ je ireducibilan ako je $I(X)$ prost ideal. Ireducibilan algebarski skup naziva se projektivna mnogostrukost.

Koje primjere projektivnih mnogostrukosti znamo?

Ireducibilne hiperplohe: $X = \mathcal{Z}(f)$, gdje je $f \neq const.$ homogen ireducibilan polinom, $I(X) = (f)$ je prost ideal.
Stupanj hiperplohe X je jednak stupnju reducirane jednadžbe F, tj. $degX = degF$.

8.1 Primjeri iz projektivne geometrije

Definicija 8.1. *Linearna mnogostrukost dimenzije k u $\mathbb{P}^n$ je slika pri kanonskoj projekciji vektorskog potprostora u K^{n+1} dimenzije $k+1$ iz kojeg je izbačena točka* 0.

Neka je $\overline{V} \subseteq K^{n+1}$ potprostor dimenzije $dim\overline{V} = k+1$. Definiramo

$$V = \{(x_0 : x_1 : ... : x_n) \in \mathbb{P}^n : (x_0, x_1, ..., x_n) \in \overline{V}\}.$$

V je linearna mnogostrukost dimenzije k.

Navedimo sada neke primjere.

- Neka je $\overline{V} = \{0\}$ nul-potprostor. Tada je $V = \emptyset$.

  $dim\overline{V} = 0 \implies dimV = 0 - 1 = -1.$

  Prazan skup je linearna mnogostrukost dimenzije -1.

- $dim\overline{V} = 1 \implies \overline{V} = \{(t \cdot a_0, t \cdot a_1, ..., t \cdot a_n) : t \in K\}$. Tada je $V = \{(a_0 : a_1 : ... : a_n)\}$.

  $dimV = 1 - 1 = 0.$

  Točka u $\mathbb{P}^n$ je linearna mnogostrukost dimenzije 0.

- $dim\overline{V} = 2 \implies \overline{V} = \{(s \cdot a_0 + t \cdot b_0, s \cdot a_1 + t \cdot b_1, ..., s \cdot a_n + t \cdot b_n) : t, s \in K\}$, gdje su $(a_0, ..., a_n)$ i $(b_0, ..., b_n)$ linearno nezavisni vektori u K^{n+1}. Tada je $V = \{(s \cdot a_0 + t \cdot b_0 : s \cdot a_1 + t \cdot b_1 : ... : s \cdot a_n + t \cdot b_n) : t, s \in K, s \neq 0 \text{ ili } t \neq 0\}$.

  Ovaj skup se naziva projektivni pravac (kroz točke $(a_0, ..., a_n)$ i $(b_0, ..., b_n)$.)

- $dim\overline{V} = n \implies dimV = n - 1.$

  Skup V nazivamo projektivnom hiperravninom.

- $dim\overline{V} = n + 1 \implies dimV = n,\ V = \mathbb{P}^n.$

Zadatak 8.2. *1. Za svake 2 točke $A, B \in \mathbb{P}^n$, postoji jedinstveni pravac $p \subseteq \mathbb{P}^n$ takav da je $A, B \in p$. Oznaka: $P = AB$.*

Uputa: $A=(a_0:...:a_n),\ B=(b_0:...:b_n)$.

$$A=B \iff \begin{vmatrix} a_i & a_j \\ b_i & b_j \end{vmatrix} \neq 0,\ \text{za sve } i,j=0,1,...,n.$$

Ako je $A\neq B$, tada postoje i,j takvi da je $\begin{vmatrix} a_i & a_j \\ b_i & b_j \end{vmatrix} \neq 0$. Tada su $(a_0,...,a_n)$ i $(b_0,...b_n)$ linearno nezavisni u $K^{n+1} \implies AB=\{(s\cdot a_0+t\cdot b_0 : s\cdot a_1+t\cdot b_1 : ... : s\cdot a_n+t\cdot b_n) : t,s\in K, s\neq 0 \text{ ili } t\neq 0\}$.

2. Stara i nova definicija hiperravnine se podudaraju.

3. Linearna mnogostrukost je algebarski skup.

   Uputa: $dimV=-1 \implies V=\emptyset$.

   $dimV=k\geq 0 : V$ je slika od $\overline{V}\backslash\{0\}$, $\overline{V}$ je vektorski potprostor od K^{n+1} dimenzije $dim\overline{V}=k+1$.

$$a^{(j)}=(a_0^{(j)},...,a_n^{(j)}), 1\leq j\leq k+1 \text{ je baza za } \overline{V}.$$

   Dakle, $\overline{V}=\left\{\sum_{i=0}^{k+1} t_i a^{(i)} : t_i\in K\right\} \stackrel{(*)}{\Longrightarrow} V=\left\{\left(\sum_{i=0}^{k+1} t_i a_0^{(i)} : ... : \sum_{i=0}^{k+1} t_i a_n^{(i)}\right) : t_i\in K, \text{ ne svi } =0\right\}$.

   Je li V algebarski skup?

   Neka je $\alpha=(\alpha_0,...,\alpha_n)\in K^{n+1}$. Definiramo linearni funkcional

$$f_\alpha(x)=\sum_{i=0}^{n}\alpha_i x_i,\ x=(x_0,...,x_n).$$

   Svaki funkcional dobijemo za jedinstveni α.

   Vidimo: $\overline{V}=((\overline{V})^o)^o$.

$$\overline{V}^o=\left\{f\in K^{n+1} : f(X)=0, \forall x\in\overline{V}\right\}$$

$$\implies \overline{V}=\left\{x\in K^{n+1} : f(X)=0, \forall f\in\overline{V}^o\right\}.$$

   Ako je $f_\alpha^{(1)},...,f_\alpha^{(l)}$ baza za $\overline{V}^o$, tada je V zadan jednadžbama $f_\alpha^{(1)}=...=f_\alpha^{(l)}=0$.

$$\overline{V}=Z_{\mathbb{A}^{n+1}}\left(\sum_{i=0}^{n}\alpha_i^{(j)}T_i : 1\leq j\leq n\right) \implies V=Z\left(\sum_{i=0}^{n}\alpha_i^{(j)}T_i : 1\leq j\leq n\right).$$

Npr. $a^{(j+1)} = (0,...,0,1,0,...,0)$, jedinica na $j-$tom mjestu, $0 \leq j \leq k$.

$\overline{V} = \{(\lambda_0,...\lambda_k,0,...,0) : \lambda_i \in K\}$

$\overline{V} = \mathcal{Z}(T_{k+1},...,T_n) \implies V = \mathcal{Z}(T_{k+1},...,T_n)$.

4. Neka su $V,W \in \mathbb{P}^n$ linearne mnogostrukosti dimenzija $k,l \geq 0$, respektivno, i neka je $k+l \geq n$. Tada je $V \cap W \neq \emptyset$.

   Uputa: $dim\overline{V} = k+1, dim\overline{W} = l+1$

   $dim\overline{V} + dim\overline{W} = k+l+2 \geq (n+1)+1 \implies V \cap W \neq \emptyset$

5. Pravac i hiperravnina u $\mathbb{P}^n$ se sijeku.

   Uputa: $n = 1$: pravac= $\mathbb{P}^n$, hiperravnina= $\{$točka$\}$.

   $n \geq 2 : H$ =hiperravnina, p =pravac

   4. $\implies p \cap H \neq \emptyset$.

Napomena 8.3. *U $\mathbb{P}^2$ pravac=hiperravnina $\implies$ svaka 2 pravca se sijeku.*

Propozicija 8.4. *Neka je $V \subseteq \mathbb{P}^n$ linearna mnogostrukost, $dimV \geq 0$ (tj. $V \neq \emptyset$). Tada je V projektivna mnogostrukost.*

Skica dokaza. Iz zadatka (??) vidimo da je V algebarski skup. Ostaje dokazati da je V ireducibilan.

Teško: $I(V)$ je prost ideal.

Lakše: koristimo kriterij za ireducibilnost (poglavlje 6., zadatak (??)) i parametrizaciju $(*)$ i postupamo kao u (poglavlje 5., zadatak (??)) $\square$

Korolar 8.5. *Idući skupovi su projektivne mnogostrukosti:*

- $\{$*točka*$\}$
- *pravac* $\subseteq \mathbb{P}^n$
- *hiperravnina*

- $\mathbb{P}^n$.

Definicija 8.6. *Ako je $P \in \mathbb{P}^n$ točka i $H \subseteq \mathbb{P}^n$ hiperravnina koja ne prolazi točkom P, centralna projekcija je preslikavanje $\pi : \mathbb{P}^n \backslash \{P\} \to H, \pi(Q) = Q', \{Q'\} = PQ \cap H$.*

Zamjena koordinata: (u stvari zamjena koordinata u vektorskom prostoru K^{n+1})

$$\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{bmatrix} = A \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_n \end{bmatrix}, \; A \in M_{(n+1)\times(n+1)}, \; detA \neq 0 \implies y_i = \sum_{j=0}^{n} a_{ij} x_j, \; 0 \geq i \geq n.$$

Zadatak 8.7. *Zamjena koordinata: $P = (0 : ... : 0 : 1)$, $H = Z(T_n) = (x_n = 0)$.*

Uputa: $\overline{H} \subseteq K^{n+1}$ je potprostor dimenzije n,

$\overline{\{P\}}$ je potprostor dimenzije 1.

$P \notin H \iff \overline{H} \cap \overline{\{P\}} = \{0\} \implies K^{n+1} = \overline{H} \oplus \overline{\{P\}}$

Zadatak 8.8. *Ako je $P = (0 : ... : 0 : 1)$ i $H = (x_n = 0) = Z(T_n)$, onda je $\pi(x_0 : ... : x_n) = (x_0 : ... : x_{n-1} : 0), \forall (x_0 : ... : x_n) \in \mathbb{P}^n, (x_0 : ... : x_n) \neq (0 : ... : 0 : 1)$.*

Napomena 8.9. $H = \{(x_0 : ... : x_{n-1} : 0) : x_i \in K,$ *ne svi* $= 0\} \equiv \mathbb{P}^{n-1} \implies \pi : \mathbb{P}^n \backslash \{P\} \to \mathbb{P}^{n-1}$.

Rješenje. Neka je $Q = (x_0 : ... : x_n) \neq P$.

$$PQ = \{ \underbrace{(t \cdot x_0 : ... : t \cdot x_{n-1} : t \cdot x_n + s \cdot 1)}_{\in PQ \cap H \iff tx_n + s = 0 \implies s = -tx_n} : s, t \in K, \text{ nisu oba } = 0\}.$$

Također, $t \neq 0$, jer kad bi bilo $t = 0$, onda bi bilo i $s = 0$, ali to je nemoguće. Vidimo da točka presjeka izgleda ovako: $(t \cdot x_0 : ... : t \cdot x_{n-1} : 0) = (x_0 : ... : x_{n-1} : 0)$. $\square$

Prethodni zadatak je bio još jedan dokaz da pravac siječe hiperravninu.

Pretpostavimo sada da je $charK \neq 2$.

Definicija 8.10. *Kvadratni skup u $\mathbb{P}^n$ (ili hiperkvadrika) je skup sljedećeg oblika:*

$$(x_0,...,x_n)Q\begin{bmatrix}x_0\\ \vdots\\ x_n\end{bmatrix}=0,\ tj.\ Z\left((T_0,...,T_n)Q\begin{bmatrix}T_0\\ \vdots\\ T_n\end{bmatrix}\right),$$

gdje je $Q=$*simetrična* $(n+1)\times(n+1)$ *matrica s koeficijentima iz* K, $Q\neq 0$.

Radi se o algebarskom skupu, ali je li on ireducibilan?

Npr. $Q=\begin{bmatrix}a & c\\ c & b\end{bmatrix}\neq 0, n=1.$

$(x_0,x_1)Q\begin{bmatrix}x_0\\ x_1\end{bmatrix}=ax_0^2+2cx_0x_1+bx_1^2=0.$

1.slučaj. $a\neq 0$

$a\left(x_0^2+\dfrac{2c}{a}x_0x_1+\left(\frac{c}{a}x_1\right)^2\right)+bx_1-\left(\frac{c}{a}x_1\right)^2=a\Big(\underbrace{x_0+\dfrac{c}{a}x_1}_{=y_0}\Big)^2+\Big(\underbrace{\sqrt{b-\left(\dfrac{c}{a}\right)^2}x_1}_{=y_1}\Big)^2=ay_0^2+$
$y_1^2=(\underbrace{\sqrt{a}y_0}_{=z_0})^2+\underbrace{y_1^2}_{=z_1}=z_0^2+z_1^2,\ b-\left(\frac{c}{a}\right)^2\neq 0.$

Zamjenom varijabli u $\mathbb{P}^2$ skup postaje $(z_0^2+z_1^2=0)$.

2.slučaj. $b\neq 0$

Slično.

3.slučaj. $a=b=0$

Sada je nužno $c\neq 0$, jer $Q\neq 0$. Imamo $2cx_0x_1=0$. Primijetimo da je $2c\neq 0$ jer smo pretpostavili da je $charK\neq 2$, pa je zato $x_0x_1=0$. Stavimo

$$x_0=y_0+\sqrt{-1}y_1,$$

$$x_0=y_0-\sqrt{-1}y_1.$$

Dakle, $0=x_0x_1=(y_0+\sqrt{-1}y_1)(y_0-\sqrt{-1}y_1)=y_0^2+y_1^2.$

Zadatak 8.11. *Neka je* $n\geq 2$ *i* $charK\neq 2$. *Tada je* $X=(x_0^2+...+x_k^2=0)$ *ireducibilna hiperkvadrika ako i samo ako je* $k\neq 1$.

Napomena 8.12. *Ako je* $k=1$, *imamo skup*

$$(x_0^2+x_1^2=0)=\mathcal{Z}(T_0^2+T_1^2)=\mathcal{Z}((T_0+\sqrt{-1}T_1)(T_0-\sqrt{-1}T_1))=$$

$$=\mathcal{Z}(T_0+\sqrt{-1}T_1)\cup\mathcal{Z}(T_0-\sqrt{-1}T_1)=\textit{unija dvije različite hiperravnine.}$$

Rješenje. (Primjena teorema (??, poglavlje 6.))

$k=0: X=\mathcal{Z}(T_0^2)=\mathcal{Z}(T_0),\ I(X)=(T_0).$

$k\geq 2$: Moramo dokazati da je polinom $T_0^2+...+T_k^2$ ireducibilan. Ako nije, onda ima linearan faktor koji ovisi o T_0 (jer je slobodni član uz T_0^2 jednak 1) $T_0+a_1T_1+...+a_nT_n$ (moramo dozvoliti sve varijable, ne sam o k). Kako $T_0^2+...+T_k^2$ ne ovisi o $T_{k+1},...,T_n$, zaključujemo da je $a_{k+1},...,a_n=0$.

$T_0+a_1T_1+...+a_nT_n$ je ireducibilan faktor.

$$\implies 0=Res_{T_0}(T_0^2+...+T_k^2,T_0+a_1T_1+...+a_nT_n)=$$

$$=\begin{vmatrix} T_1^2+...+T_k^2 & 0 & 1\\ a_1T_1+...+a_nT_n & 1 & 0\\ 0 & a_1T_1+...+a_nT_n & 1\end{vmatrix}=T_1^2+...+T_k^2-(a_1T_1+...+a_nT_n)^2.$$

Dakle,

$$T_1^2+...+T_k^2=(a_1T_1+...+a_nT_n)^2 \text{ u } K[T_1,...,T_k].$$

$$T_1^2+...+T_k^2=a_1^2T_1^2+...+a_k^2T_k^2+\sum_{1\leq i<j\leq k}2a_ia_jT_iT_j \implies a_1^2=a_2^2=1,\ 2a_1a_2=0,$$

što je kontradikcija s $charK\neq 2$.

$T_0^2+...+T_k^2$ ireducibilan za $k\geq 2 \implies I(X)=(T_0^2+...+T_k^2)$ ireducibilan $\implies I(X)$ je prost $\implies X$ je ireducibilan. $\square$

Iz poglavlja 6 znamo da ako je X hiperploha, onda je $I(X)=(f)$ glavni ideal, gdje je f određen do na umnožak konstantom $\neq 0$. Dakle, stupanj hiperplohe $degX=deg(f)$ je dobro definiran.

X je ireducibilna $\iff$ f je ireducibilan.

Zadatak 8.13. *(generalizacija "teorema" o presjeku pravca i hiperravnine)*

Ako je $p \subseteq \mathbb{P}^n$ i $X \subseteq \mathbb{P}^n$ hiperravnina, onda je:

1. $p \cap X \neq \emptyset$;
2. $\#(p \cap X) \geq degX + 1 \implies p \subseteq X$.

Npr. Ako uzmemo koniku C, imamo $degC = 2$, pravci ju sijeku u 2 različite točke.

Bizaran slučaj:

$n = 1$: hiperploha X je skup koji se sastoji od konačno točaka, a pravac $p = \mathbb{P}^1$ je sve. Dakle, $X \subseteq p$, tj. $\#(p \cap X) = \#X = degX$.

$n \geq 2$: situacija je normalna.

Rješenje. Pretpostavimo da vrijedi $p \nsubseteq X$. Želimo dokazati da je $1 \leq \#(p \cap X) \leq degX$.

Neka je $I(X) = (f), degX = degf = m$. Budući da $p \nsubseteq X$, postoji neka točka $A = (a_0 : ... : a_n)$ koja leži na pravci p, a nije $\notin X$.

$$A \notin X \iff f(a_0, ..., a_n) \neq 0.$$

Neka je $B = (b_0 : ... : b_n)$ neka druga točka na p.

$$\implies p = AB = \{(s \cdot a_0 + t \cdot b_0 : s \cdot a_1 + t \cdot b_1 : ... : s \cdot a_n + t \cdot b_n) : t, s \in K, s \neq 0 \text{ ili } t \neq 0\}$$

Računamo presjek $p \cap X$:

$$f(s \cdot a_0 + t \cdot b_0, s \cdot a_1 + t \cdot b_1, ..., s \cdot a_n + t \cdot b_n) = 0$$

f je homogen polinom stupnja m, pa ga možemo zapisati u obliku

$$f = \sum_{|\alpha| = m} c_\alpha T^\alpha, \alpha = (\alpha_0, ..., \alpha_n) \in \mathbb{Z}^n_{\geq 0}, c_\alpha \in K, T^\alpha = T_0^{\alpha_0} \cdot ... \cdot T_n^{\alpha_n}$$

Izmnožimo:

$$\underbrace{f(a_o, ..., a_n)}_{\neq 0 \;\; jer \;\; A \notin X} s^m + \text{monomi } s^i t^{m-i} + f(b_0, ..., b_n) t^m = 0.$$

Primijetimo da je sigurno $T \neq 0$, jer inače imamo $f(a_0,...,a_n)s^m = 0$. Iz toga slijedi da je $s = 0$, što je kontradikcija s time da nisu oba s i t jednaki nuli.

Dakle, $t \neq 0$, pa zbog homogenosti možemo uzeti $t = 1$. s računamo iz gornje polinomijalne jednadžbe. Ta jednadžba ima najviše m različitih rješenja po s.

Ako su $s_1,...,s_m$ rješenja (s kratnostima), slijedi

$$p \cap X = \{(s_i \cdot a_0 + b_0 : s_i \cdot a_1 + b_1 : ... : s_i \cdot a_n + b_n) : 1 \leq i \leq m\}$$

$$\implies 1 \leq \#p \cap X \leq m = degX. \quad \square$$

8.2 Geometrijska interpretacija stupnja hiperplohe

Ako je X hiperploha, tada je $I(X) = (f), degX = deg(f)$.

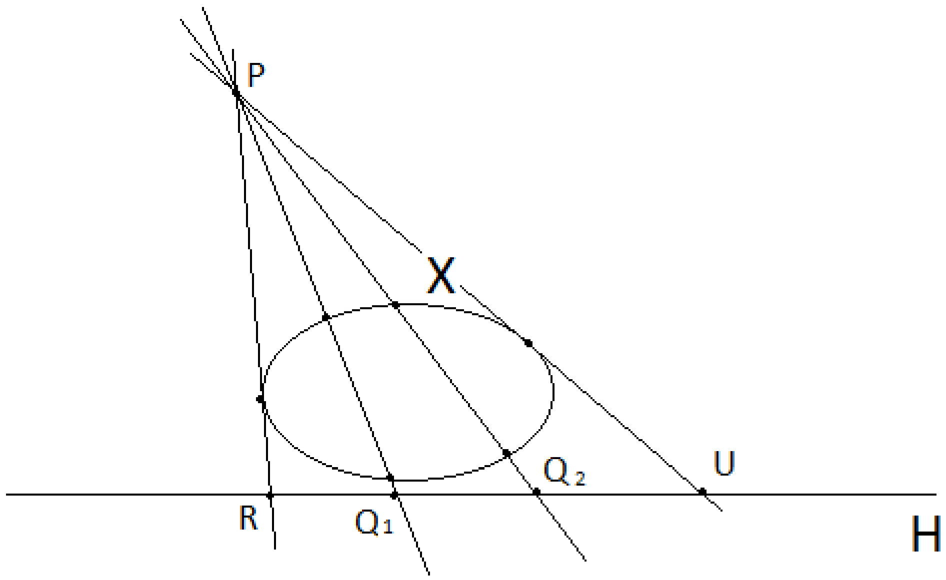
Stupanj hiperplohe (u $\mathbb{P}^n$, $n \geq 2$) je broj točaka presjeka hiperplohe s pravcem u "općem položaju" (generički pravac).

Neka je H hiperravnina u $\mathbb{P}^n$ koja ne prolazi točkom P, $H \equiv \mathbb{P}^{n-1}$.

Pravce kroz točku P možemo parametrizirati na sljedeći način:
uzmemo točku $Q \in H$ i gledamo pravac PQ. Sve pravce možemo dobiti na taj način.

PQ je u općem položaju ako postoji algebarski skup $Z \subseteq \mathbb{P}^{n-1} \equiv H$ takav da $Q \notin Z$.

Na slici je to $Z = \{R,U\}$.



Teorem 8.14. *Neka je* $charK = 0$ *i* $n \geq 0$*. Neka je* $X \subseteq \mathbb{P}^n$ *hiperploha, neka je* $P \in \mathbb{P}^n \backslash \{X\}$ *i* $H \subseteq \mathbb{P}^n$ *bilo koja hiperravnina koja ne prolazi točkom P. Tada postoji algebarski skup* $Y \subseteq H, Y \neq H$ *(ali moguće* $Y = \emptyset$*) takav da* $\forall Q \in H \backslash Y$ *vrijedi da* $PQ \cap X$ *ima točno* $degX$ *točaka.*

Dokaz. Zamjenom koordinata možemo dobiti $P = (0 : ... : 0 : 1), H = (x_n = 0) = \mathcal{Z}(T_n) = \{(b_0 : b_1 : ... : b_{n-1} : 0) \mid b_i \in K, \text{ ne svi} = 0\}) \equiv \mathbb{P}^n$.

Uzmimo $Q = (b_0 : b_1 : ... : b_{n-1} : 0) \in H$. Sada je

$$PQ = \{(s \cdot 0 + t \cdot b_0 : s \cdot 0 + t \cdot b_1 : ... : s \cdot 0 + t \cdot b_{n-1} : s \cdot 1) \mid s, t \in K, \text{ ne oba} = 0\}.$$

$\Longrightarrow$ ako imamo točku $\in PQ \cap X$, ona je oblika $(t \cdot b_0 : ... : t \cdot b_{n-1} : s \cdot 1)$.

Sigurno je $t \neq 0$ jer $P \notin X$. Zbog homogenosti možemo uzeti $t = 1$. Točke presjeka određene su s $f(b_0, ..., b_{n-1}, s) = 0$, gdje je $I(X) = (f), X = \mathcal{Z}(f)$, f nema višestrukih ireducibilnih faktora.

Iz početka poglavlja 7 znamo:

$$f(0, ..., 0, 1) \neq 0 \implies f = f_l T_n^l + \sum_{i=0}^{l-1} f_i(T_1, ..., T_{n-1}) T_n^i, f_l \neq 0, l \geq 1.$$

Kao u dokazu propozicije (?? 7.1) zaključujemo da f nema ireducibilnih faktora koji ne ovise o T_n.

$$\frac{\partial f}{\partial T_n} = f_l \cdot l \cdot T_n^{l-1} + ... \ , f_l \cdot l \neq 0, \text{jer je } charK = 0$$

Ako je $l = 1$, tada je X hiperploha i $\#PQ \cap X = 1, \forall Q \in H$, tj. $Y = \emptyset$. Zato pretpostavimo da je $l \geq 2$.

f nema višestrukih ireducibilnih faktora, pa je $Res_{T_n}(f, \frac{\partial f}{\partial T_n}) \neq 0$ u $K[T_0, ..., T_{n-1}]$ i ta rezultanta je homogen polinom stupnja $l(l-1) \geq 2$. Dakle, to nije konstanta. Zato je sa $\mathcal{Z}(Res_{T_n}(f, \frac{\partial f}{\partial T_n}))$ definirana jedna hiperphola u $\mathbb{P}^{n-1} \equiv H$, označimo ju s Y.

Konačno, jer $Q = (b_0 : ... : b_{n-1}) \notin Y$, $f(b_o, ...b_{n-1}, T_n)$ nema višestrukih korijena (po T_n) jer je $Res(f(b_o, ...b_{n-1}, T_n), \frac{\partial f}{\partial T_n}(b_o, ...b_{n-1}, T_n)) = Res_{T_n}(f, \frac{\partial f}{\partial T_n})(b_o, ...b_{n-1}) \neq 0$.

Budući da je $l = deg(f)$ ima l razičitih nultočaka (jer f nema višestrukih ireducibilnih faktora). $\square$

Teorem 8.15. *Neka je $n \geq 2$ i neka su $f, g \in K[T_0, ...T_n]$ nekonstantni homogeni polinomi takvi da je $f(0, ...0, 1), g(0, ...0, 1) \neq 0$. Neka je $P = (0 :, , , : 0 : 1), X = \mathcal{Z}(f), Y = \mathcal{Z}(g), H = (x_n = 0)$ i*

$$\pi : \mathbb{P}^n \backslash \{P\} \to H,$$

$$\pi(x_0 : ... : x_n) = (x_0 : ... : x_{n-1})$$

centralna projekcija. Tada je $\pi(X \cap Y) = \mathcal{Z}(Res_{T_n}(f, g))$. Posebno, $X \cap Y \neq \emptyset$.

Dokaz.

$$f(0, ..., 0, 1) \neq 0 \implies f = f_l T_n^l + \sum_{i=0}^{l-1} f_i(T_1, ..., T_{n-1}) T_n^i, \ f_l \neq 0, \ l \geq 1,$$

$$g(0, ..., 0, 1) \neq 0 \implies g = g_m T_n^m + \sum_{j=0}^{m-1} g_j(T_1, ..., T_{n-1}) T_n^j, \ g_m \neq 0, \ m \geq 1.$$

$\implies Res_{T_n}(f, g) \in K[T_0, ..., T_{n-1}]$ homogen stupnja $lm \geq 1$. Posebno, $Res_{T_n}(f, g) \neq 0$. Dakle, $\mathcal{Z}(Res_{T_n}(f, g))$ je hiperploha u $\mathbb{P}^{n-1}$.

Nap. $Res_{T_n}(f, g) = 0$ ako i samo ako f i g imaju zajednički ireducibilni faktor $\implies \mathcal{Z}(Res_{T_n}(f, g)) = \mathbb{P}^n$.

Neka je sada $(x_o : ... : x_n) \in X \cap Y$. Tada je $f(x_0,...,x_n) = g(x_0,...,x_n) = 0$. Iz propozicije (?? 7.1) slijedi da postoje $A, B \in K[T_0,...,T_n]$ takvi da je

$$Res_{T_n}(f,g)(x_0,...,x_{n-1}) = A(x_0,...,x_n)f(x_0,...,x_n) + B(x_0,...,x_n)g(x_0,...,x_n).$$

Sada je

$$Res_{T_n}(f,g)(x_0,...,x_{n-1}) = A(x_0,...,x_n)\cdot 0 + B(x_0,...,x_n)\cdot 0 = 0.$$

Slijedi $(x_0 : ... : x_{n-1}) \in \mathcal{Z}(Res_{T_n}(f,g))$. Dakle,

$$\pi(x_0 : ... : x_n) = (x_0 : ... : x_{n-1}) \in \mathcal{Z}(Res_{T_n}(f,g)) \implies \pi(X \cap Y) = \mathcal{Z}(Res_{T_n}(f,g)).$$

Obratno, neka je $(x_0 : ... : x_{n-1}) \in \mathcal{Z}(Res_{T_n}(f,g))$.

$$Res_{T_n}(f,g)(x_o,...x_{n-1}) = Res(f(x_o,...x_{n-1},T_n), g(x_o,...x_{n-1},T_n)) = 0.$$

$\implies f(x_o,...x_{n-1},T_n), g(x_o,...x_{n-1},T_n) \in K[T_n]$ imaju zajednični korijen $x_n \in K$. Dakle,

$$(x_0 : ... : x_n) \in X \cap Y \implies \mathcal{Z}(Res_{T_n}(f,g)) \subseteq \pi(X \cap Y).$$

□

Korolar 8.16. *Uz oznake kao i prethodnom teoremu, ako X i Y nemaju zajedničku ireducibilnu komponentu (tj. po definiciji f i g nemaju zajednički ireducubilni faktor), onda je $\mathcal{Z}(Res_{T_n}(f,g))$ hiperploha i $\pi(X \cap Y) = \mathcal{Z}(Res_{T_n}(f,g))$.*

Zadatak 8.17. *($n \geq 2$) Svake dvije hiperplohe se sijeku.*

Uputa: zamjena koordinata prevodi u situaciju iz prethodnog teorema. □

Sjetimo se (iz poglavlja 6) da jeprojektivna ravninska krivulja po definiciji hiperphola u $\mathbb{P}^2$.

Teorem 8.18. ***(Bezoutov teorem)*** *Neka su $X, Y \in \mathbb{P}^2$ ravninske krivulje. Tada je $X \cap Y \neq \emptyset$ i ako je*

$$\#X \cap Y \geq (degX)(degY) + 1,$$

tada X i Y imaju zajedničku ireducibilnu komponentu, tj. ako X i Y nemaju zajedničku ireducibilnu komponentu, tada je

$$\#(X \cap Y) \leq (degX)(degY).$$

Dokaz. $X \cap Y \neq \emptyset$ slijedi iz teorema 8.15 i zadatka 8.17.

Neka je sada $I(X) = (f)$ i $I(Y) = (g)$. Po pretpostavci f i g nemaju zajednički ireducibilni faktor pa je $Res_{T_n}(f,g) \neq 0$ homogen polinom stupnja $lm \geq 1$.

BSO možemo uzeti $P = (0:0:1) \notin X,Y$, inače zamjena koordinata.
Imamo projekciju

$$\pi : \mathbb{P}^2 \backslash \{P\} \to \mathbb{P}^1,$$

$$\pi(x_0 : x_1 : x_2) = (x_0 : x_1) \in \mathbb{P}^1.$$

Iz teorema 8.15 slijedi da je $\pi(X \cap Y) = \mathcal{Z}(Res_{T_n}(f,g))$. Dakle,$\pi(X \cap Y)$ ima najviše $l \cdot m$ točaka.

$\implies \#\pi(X \cap Y) \leq (degX)(degY).$

Kada bi imali da je restrikcija od π na $X \cap Y$ injekcija, bili bismo gotovi.

Izaberimo prvo točku P.

Cilj nam je dokazati da je $\#X \cap Y \leq (degX)(degY)$. Ako ne, možemo izabrati međusobno različite točke $P_1, P_2, ..., P_{s+1} \in X \cap Y$, $s = (degX)(degY) = l \cdot m$.

Neka je $P_iP_j,\ i,j = 1,...,s+1, P_iP_j = \mathcal{Z}(l_{ij}), l_{ij} \in K[T_0,...,T_n]$ stupnja 1. Vrijedi:

$$X \cup Y \cup \left(\bigcup_{i,j=1}^{s+1} P_iP_j \right) = \mathcal{Z}\left(f \cdot g \prod_{i,j=1}^{s+1} l_{ij} \right) \neq \mathbb{P}^2,$$

pa možemo izabrati

$$P \in X \cup Y \cup \left(\bigcup_{i,j=1}^{s+1} P_iP_j \right).$$

Sada tvrdimo da je $\pi : \{P_1,...,P_{s+1}\} \to \mathbb{P}^1$ injekcija.

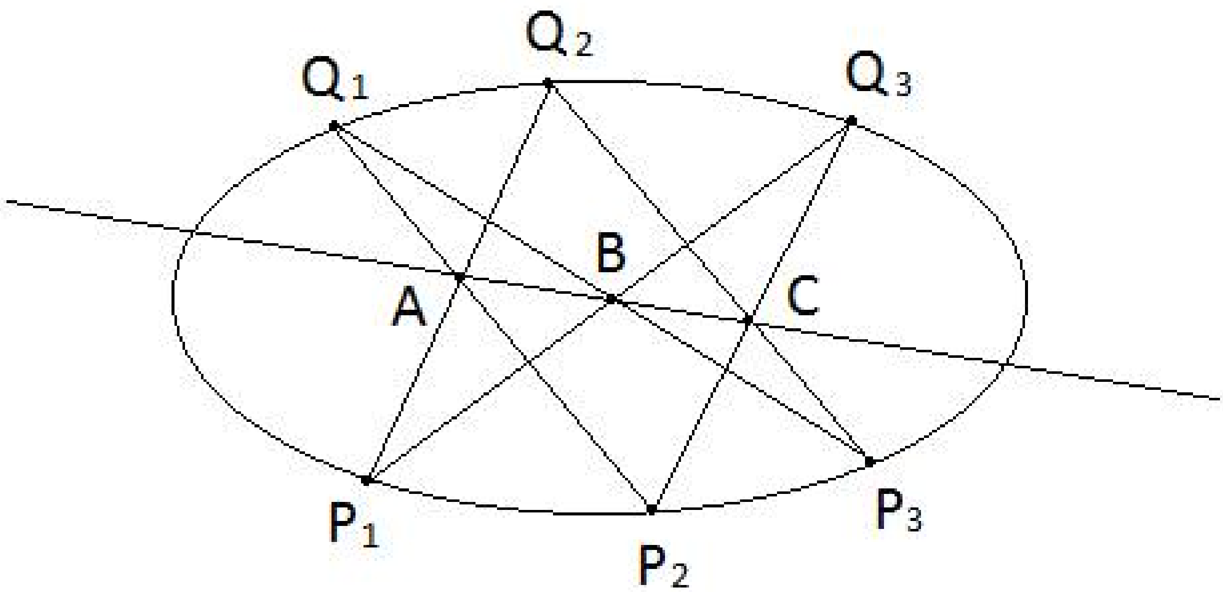
Ako je $\pi(P_i) = \pi(P_j)$, tada je $P_i, P_j \in P\pi(P_i)$, za $i \neq j$, ali to je kontradikcija s izborom točke P.

Iz činjenice da je π injekcija, slijedi da je $s+1 \leq \#X \cap Y \leq l \cdot m = s$. $\square$

Zadatak 8.19. *Kako koristeći Bezoutov teorem možemo računati presjeke krivulja?*

Uputa: injektivnost projekcije iz prethodnog teorema + metode dokaza teorema 8.15. $\square$

Zadatak 8.20. ***(Pascalov teorem)*** *Neka je $\mathcal{C}$ ireducibilna krivulja stupnja 2 (=konika). Neka su $P_1, P_2, P_3, Q_1, Q_2, Q_3 \in \mathcal{C}$ međusobno različite točke. Tada su A, B i C kolinearne.*



Rješenje:

$P_1Q_2 = \mathcal{Z}(l_{12}), l_{12} \in K[T_0, T_1, T_2]$ homogen stupnja 1

$P_2Q_1 = \mathcal{Z}(l_{21}), l_{21} \in K[T_0, T_1, T_2]$ homogen stupnja 1

$\implies \{A\} = P_1Q_2 \cap P_2Q_1$

$P_1Q_3 = \mathcal{Z}(l_{13}), l_{13} \in K[T_0, T_1, T_2]$ homogen stupnja 1

$P_3Q_1 = \mathcal{Z}(l_{31}), l_{31} \in K[T_0,T_1,T_2]$ homogen stupnja 1
$\implies \{B\} = P_1Q_3 \cap P_3Q_1$

$P_2Q_3 = \mathcal{Z}(l_{23}), l_{23} \in K[T_0,T_1,T_2]$ homogen stupnja 1
$P_3Q_2 = \mathcal{Z}(l_{32}), l_{32} \in K[T_0,T_1,T_2]$ homogen stupnja 1
$\implies \{C\} = P_2Q_3 \cap P_3Q_2$

Neka je $\lambda \in K$ za sada neodređen parametar. Definirajmo

$$F = l_{12}l_{23}l_{31} - \lambda l_{13}l_{32}l_{21}.$$

l_{ij} su međusobno neasocirani jer su pravci međusobno različiti. Dakle $F \neq 0$ je homogen polinom stupnja 3.

Budući da $\mathcal{C}$ ima beskonano točaka, izaberemo točku $R \in \mathcal{C}, R \neq P_1,P_2,P_3,Q_1,Q_2,Q_3$ i tražimo $F(R) = 0$, što određuje jedinstveni λ.

$\implies R,P_1,P_2,P_3,Q_1,Q_2,Q_3 \in (C) \cap \mathcal{Z}(F)$, pa po Bezoutovom teoremu $\mathcal{C}$ i $\mathcal{Z}(F)$ imaju zajedničku ireducibilnu komponentu. Tada je $\mathcal{C}$ (zbog ireducibilnosti) ta ireducibilna komponenta.

$\mathcal{Z}(F)$ je najviše stupnja 3 i $F(A) = F(B) = F(C) = 0$ (tj. $A,B;C \in \mathcal{Z}(F)$) $\implies$ točke A,B i C nisu na konici $\mathcal{C}$.

No, tada je $\mathcal{Z}(F) = pravac \cup \mathcal{C}$ pa točke A,B i C leže na pravcu. $\square$

Definicija 8.21. *Hiperploha $X \subseteq \mathbb{P}^n$ je glatka ili nesingularna u svojoj točki $A = (a_0 : ... : a_n) \in X$ ako postoji $i \in \{0,1,...,n\}$ takav da je $\frac{\partial f}{\partial T_i}(a_0,...,a_n) \neq 0$, gdje je f polinom određen do na umnočak s konstantom $\neq 0$ uvjetom $I(X) = (f)$.*
X je nesingularna ako je glatka u svakoj svojoj točki.

Ako imamo $X = \mathcal{Z}(F), A = (a_0 : ... : a_n)$ je nesingularna ako postoji $i \in \{0,1,...,n\}$ takav da je $\frac{\partial F}{\partial T_i}(a_0,...,a_n) \neq 0$.

Zašto to ne valja?

Npr. ako je $F = T_0^2$, imamo $X = \mathcal{Z}(T_0^2) = (x_0^2 = 0)$. Za svaku točku $(a_0 : ... : a_n)$ na tom pravcu i za svaki $i \in \{0,1,...,n\}$ je $\frac{\partial F}{\partial T_i}(a_0,...,a_n) = \begin{cases} 2a_0, & \text{ako je } i = 0. \\ 0, & \text{ako je } i \neq 0. \end{cases}$

No, ako gledamo $I(X) = (T_0)$, $f = T_0$, imamo $\frac{\partial f}{\partial T_i}(a_0,...,a_n) = 1$.

Zato kod definicije glatkoće ne polazimo od bilo koje jednadžbe za X već od one ireducibilne.

Neka je $A = (a_0 : ... : a_n) \in X$ nesingularna točka. Definiramo tangencijalnu hiperravninu na X u točki A sa $\mathcal{Z}\left(\sum_{i=0}^n \frac{\partial f}{\partial T_i}(a_0,...,a_n)T_i\right)$.

Primjer 8.22. 1. Pogledajmo hiperravninu $X = \mathcal{Z}(\sum_{i=0}^n b_iT_i) = (\sum_{i=0}^n b_ix_i = 0)$. Vrijedi: $I(X) = (\sum_{i=0}^n b_iT_i)$

DZ: Svaka točka iz X je nesingularna i tangencijalna ravnina u njoj je jednaka X.

2. Neka je char$X \neq 2$. Pogledajmo hiperkvadriku $X = \mathcal{Z}(T_0^2 + ... + T_k^2)$, $2 \leq k \leq n$. Vrijedi: $I(X) = (T_0^2 + ... + T_k^2)$.

DZ: Singularne točke postoje ako i samo ako $k < n$ i dane su s $(0 : ... : 0 : a_{k+1} : ... : a_n)$.

Posebno, za $n = 2$ imamo $\mathcal{C} = \mathcal{Z}(T_0^2 + T_1^2 + T_2^2)$.

DZ: Izračunajte u općem slučaju tangencijalnu hiperravninuu u nesingularnim točkama.

Zadatak 8.23. *($n \geq 2$) Ako je hiperploha nesingularna, tada je ireducibilna.*

Rješenje. $X \subseteq \mathbb{P}^n$ hiperploha $\implies I(X) = (f)$, f nema višestrukih ireducibilnih faktora, tj. $f = f_1 \cdot ... \cdot f_t$, gdje su f_i neasocirani. Cilj nam je dokazati da je$t = 1$. U protivnom, $t \geq 2$ i definiramo $F = f_1 \cdot ... \cdot f_{t-1}$.

$n \geq 2 \implies \mathcal{Z}(F) \cap \mathcal{Z}(f_t) \neq 0$ i $X = \mathcal{Z}(F) \cup \mathcal{Z}(f_t)$.

Neka je $(a_0 : ... : a_n) \in \mathcal{Z}(F) \cap \mathcal{Z}(f_t)$. Leibnizovo pravilo: $f = F \cdot F_t$.

$$\frac{\partial f}{\partial T_i}(a_0,...,a_n) = F(a_0,...,a_n)\frac{\partial f_t}{\partial T_i}(a_0,...,a_n) + \frac{\partial F}{\partial T_i}(a_0,...,a_n)f_t(a_0,...,a_n) = 0.$$

Iz toga slijedi da je točka $(a_0 : ... : a_n)$ singularna, a to je kontradikcija s pretpostavkom da je hiperploha nesingularna. Dakle, $t = 1$. $\square$

Zadatak 8.24. *Neka je* $charK = 0$*. Tada na svakoj ireducibilnoj krivulji* $X \subseteq \mathbb{P}^2$ *ima samo konačno nesingularnih točaka.*

Rješenje. Neka je X ireducibilna. Tada je $I(X) = (f)$, gdje je f ireducibilan stupnja $l \geq 1$.

f ovisi o nekoj varijabli, možemo uzeti T_n. Dakle,

$$f = \sum_{i=0}^{k} f_i(T_0, ..., T_{n-1})T_n^i, \ k \geq 1, \ f_k(T_0, ..., T_{n-1}) \neq 0.$$

Sada je

$$\frac{\partial f}{\partial T_n} = f_k(T_0, ..., T_{n-1}) \cdot k \cdot T_n^{k-1} + ...(\text{niže potencije}).$$

Ako je A singularna točka na X, tada je $A \in Z(f) \cap Z(\frac{\partial f}{\partial T_n})$. Ta dva skupa iz presjeka nemaju zajedničke ireducibilne komponente jer je f ireducibilan, a $\frac{\partial f}{\partial T_n}$ je manjeg stupnja (u T_n) od f, pa f nije zajednička komponenta. Dakle, prema Bezoutovom teoremu presjek ima konačno točaka. $\square$

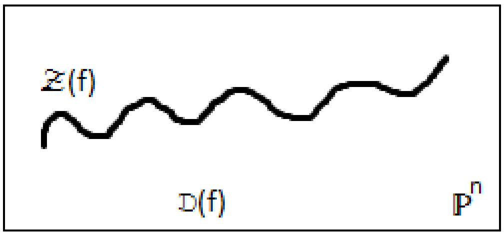
Zadatak 8.25. *Neka je X hiperploha,* $I(X) = (f)$*. Tada je skup singularnih točaka u X jednak* $Z\left(\frac{\partial f}{\partial T_0}, ..., \frac{\partial f}{\partial T_n}\right) \subseteq Z(f) = X$.

Uputa. Eulerov identitet dokazuje gornju inkluziju. Dakle, skup singularnih točaka na hiperplohi X je algebarski skup.

Poglavlje 9

Hiperravnina u beskonačnosti

$f \in K[T_0, ..., T_n]$, homogen i nekonstantan, $X = \mathscr{Z}(f) = (f(x_0, ..., x_n) = 0)$ je hiperploha.
$\mathbb{P}^n \setminus X =: \mathscr{D}(f) = (f(x_0, ..., x_n) \neq 0)$ zovemo GLAVNI OTVORENI SKUP.



Poseban slučaj: $f = T_i, 0 \leq i \leq n$, $\mathbb{P}^n = \mathscr{D}(T_i) \quad \cup \underbrace{\mathscr{Z}(T_i)}_{\text{hiperravnina}}$, $\mathscr{D}(T_i) \to \mathbb{A}^n$ bijektivno,

$\mathbb{P}^n = \mathbb{A}^n \quad \cup \quad \underbrace{\mathscr{Z}(T_i)}_{\text{hiperravnina u } \infty}$.

$\mathscr{D}(T_i) = (x_i \neq 0)$, $(x_0, ..., x_n) \in \mathscr{D}(T_i) \implies (\frac{x_0}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_n}{x_i}) \in \mathbb{A}^n$.

Oznake: $i = 0$, $\mathscr{D}(T_0) = (x_0 \neq 0)$, $(x_0 : ... : x_n) \mapsto (\frac{x_1}{x_0}, ..., \frac{x_n}{x_0}) =: (y_1, ..., y_n)$, $\mathscr{D}(T_0) \equiv (A)^n$, $(x_0 : ... : x_n) \equiv (y_1, ..., y_n)$, gdje su prve projektivne, a druge afine koordinate.

Točke s hiperravnine u ∞ $\mathscr{Z}(T_0)$. Točke oblika $(0 : x_1 : ... : x_n)$ nemaju afine koordinate.

$\mathbb{P}^n = \bigcup_{i=0}^{n} \mathscr{D}(T_i) \implies$ svaka točka iz $(P)^n$ pripada nekom $\mathscr{D}(T_j)$ jer ima neku koordinatu $\neq 0$.

Primjer 9.1. $(0 : 1 : 2 : 0 : ... : 0) \in \mathscr{D}(T_1)$, *ali gledano iz* $\mathscr{D}(T_0)$ *je u beskonačnosti.* $(\frac{0}{1}, \frac{2}{1}, \frac{0}{1}, ..., \frac{0}{1}) = (0, 2, 0, ..., 0)$ *kao točka iz* $\mathscr{D}(T_1)$.

$$\underbrace{\mathbb{P}^n}_{\text{globalan objekt kao i algebarski skupovi u } \mathbb{P}^n} \longrightarrow \underbrace{\mathbb{A}^n \equiv \mathscr{D}(T_i)}_{\text{sadrži lokalne objekte}}$$

Lema 9.2. *1) $f \in K[R_1,...,R_n], f \neq 0$, homogenizacija $\tilde{f} \in K[T_0,...,T_n]$ definirana sa $\tilde{f} = T_0^{degf} f(\frac{T_1}{T_0},...,\frac{T_n}{T_0})$, evaluacija u polju $K(T_0,...,T_n)$. $\tilde{f} \neq 0$ homogen stupnja $degf$, $T_0 \nmid \tilde{f}$, $f = \tilde{f}(1,R_1,...,R_n)$.*

2) $F \in K[T_0,...,T_n]$, homogen, $F \neq 0$. Dehomogenizacija $\hat{F} = F(1,R_1,...,R_n) \in K[R_1,...,R_n]$, $deg\hat{F} = degF - e$, gdje je e najveći eksponent od T_0 tako da $T_0^e | F$ u $K[T_0,...,T_n]$. $F = T_0^e \tilde{\hat{F}}$.

3) f iz 1) ireducibilan $\implies$ $\tilde{f}$ ireducibilan i nije asociran s T_0

4) F ireducibilan i neasociran s T_0 $\implies$ $\hat{F}$ ireducibilan.

Dokaz:

1)

$$f = \sum_{\alpha} a_\alpha R^\alpha,$$

$\alpha \in \mathbb{Z}^n_{\geq 0}$, $a_\alpha \in K$, $R^\alpha = R_1^{\alpha_1} \cdots R_n^{\alpha_n}$.

$degf =: m \implies \exists \beta \in \mathbb{Z}^n_{\geq 0}$ takav da $|\beta| = \beta_1 + \cdots + \beta_n = m, a_\beta \neq 0$

$\forall \alpha \in \mathbb{Z}^n_{\geq 0} \implies$ ako $a_\alpha \neq 0$, onda $|\alpha| \leq m$

$$\begin{aligned}\tilde{f} = T_0^m \cdot f(\frac{T_1}{T_0},...,\frac{T_n}{T_0}) &= \sum_{\alpha\neq\beta} a_\alpha T_0^m (\frac{T_1}{T_0})^{\alpha_1} \cdots (\frac{T_n}{T_0})^{\alpha_n} + a_\beta T_0^m (\frac{T_1}{T_0})^{\beta_1} \cdots (\frac{T_n}{T_0})^{\beta_n} \\ &= \sum_{\alpha\neq\beta} a_\alpha T_0^{m-|\alpha|} T_1^{\alpha_1} \cdots T_n^{\alpha_n} + a_\beta T_1^{\beta_1} \cdots T_n^{\beta_n}\end{aligned}$$

Dakle, $\tilde{f}$ je homogen polinom stupnja m te kako sadrži monom $a_\beta T_1^{\beta_1} \cdots T_n^{\beta_n}$ nije djeljiv sa T_0.

2)

$F = T_0^e \cdot G$, G homogen, $degG = degF - e$, $T_0 \nmid G$

$$\hat{F} = F(1,R_1,\ldots,R_n) = G(1,R_1,\ldots,R_n)$$

$T_0 \nmid G \implies G$ sadrži u svom prikazu monom $c\dot{T}_1^{\gamma_1} \cdots T_n^{\gamma_n}$, $c \in K$, $c \neq 0$,

$\gamma_1 + \cdots + \gamma_n = m = degG$

$$\implies \hat{F} = G(1,R_1,\ldots,R_n) = \sum_{\alpha\neq\gamma} a_\alpha R_1^{\alpha_1} \cdots R_n^{\alpha_n} + c\dot{R}_1^{\gamma_1} \cdots R_n^{\gamma_n}$$

$\implies deg\hat{F} = m =: degG = degF - e$

$\tilde{\hat{F}} = G(1, \tilde{R_1, \ldots, R_n}) = T_0^m \cdot G(1, \frac{T_1}{T_0}, ..., \frac{T_n}{T_0}) \overset{\text{G homogen}}{=} G(T_0, \ldots, T_n) \implies T_0^e \tilde{\hat{F}} = T_0^e G = F$

3)

f ireducibilan $\implies f \neq const. \Leftrightarrow degf \geq 1 \overset{1)}{\implies} deg\tilde{f} \geq 1 \implies \tilde{f}$ nije konstanta.

Pretpostavimo $\tilde{f} = G \cdot H$, G, H homogeni, nekonstantni $\implies f \overset{1)}{=} \hat{\tilde{f}} = \hat{G} \cdot \hat{H}$

No, $deg\hat{G} = degG$ i $deg\hat{H} = degH \implies \hat{G}, \hat{H} \neq const. \Rightarrow\Leftarrow$

4)

$T_0 \nmid F \implies deg\hat{F} = degF \geq 1$ jer F ireducibilan $\implies \hat{F} \neq const.$

$\hat{F} = g \cdot h$, g, h nekonstantni $\overset{2)}{\implies} F = \tilde{\hat{F}} = \tilde{g} \cdot \tilde{h}$, $\tilde{g}, \tilde{h} \neq const. \Rightarrow\Leftarrow$ □

Definicija 9.3. *Neka je $X \subset \mathbb{A}^n$ afina hiperploha (vidi 5. poglavlje). Projektivizacija ili projektivni zatvarač $\bar{X}$ od X je (projektivna) hiperploha $\bar{X} = \mathscr{Z}(\tilde{f})$ ako je $I_{\mathbb{A}^n}(X) = (f)$.*

DZ: $I(\bar{X}) = (\tilde{f})$

Uputa: Teorem 5.8. $\implies f$ nema višestrukih ireducibilnih faktora $\overset{\text{Lema 9.2.}}{\implies} \tilde{f}$ nema višestrukih ireducibilnih faktora $\overset{\text{Teorem 6.19.}}{\implies} I(\bar{X}) = (\tilde{f})$

Teorem 9.4. *1) $\bar{X} \cap \mathbb{A}^n = X$, hiperravnina $(x_0 = 0) = \mathscr{Z}(T_0)$ nije ireducibilna komponenta od $\bar{X}$.*

2) $Y \subset \mathbb{P}^n$ hiperploha takva da $\mathscr{Z}(T_0)$ nije ireducibilna komponenta od Y. Onda $Y_{af} \overset{def}{=} Y \cap \mathbb{A}^n$ je afina hiperploha takva da $I_{\mathbb{A}^n}(Y_{af}) = (\hat{F})$ ako je $I(Y) = (F)$.

3) X ireducibilna (vidi 1)) $\implies \bar{X}$ ireducibilna u $\mathbb{P}^n$

4) Y ireducibilna (kao u 2)) $\implies Y_{af} \subset \mathbb{A}^n$ ireducibilna.

Skica dokaza:

1)

$I_{\mathbb{A}^n}(X) = (f)$

$(x_0 : ... : x_n) = (y_1, ..., y_n) \in X \bar{\cap} \mathbb{A}^n \implies \tilde{f}(x_0, ., x_n) = 0$ i $x_0 \neq 0 \Leftrightarrow f = \hat{\tilde{f}}(1, y_1, ..., y_n) = 0 \Leftrightarrow (y_1, ..., y_n) \in X$

1) iz prethode leme tada daje: $T_0 \nmid \tilde{f} \overset{\text{Teorem 6.19.}}{\implies} \mathscr{Z}(T_0)$ nije ireducibilna komponenta od $\mathscr{Z}(\tilde{f}) = \bar{X}$.

2)

$I(Y) = (F)$

$\mathscr{Z}(T_0)$ nije ireducibilna komponenta od $Y \overset{\text{Teorem 6.19.}}{\Longrightarrow} T_0 \nmid F$

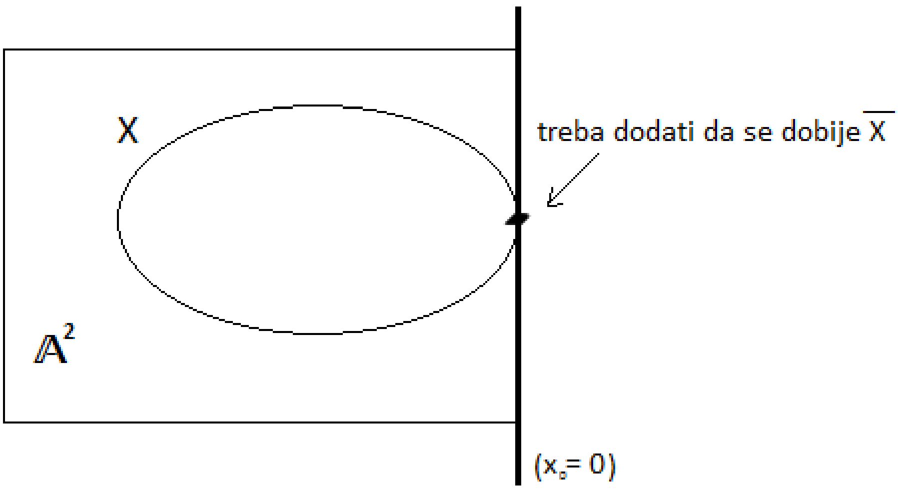
$(x_0 : \dots : x_n) = (y_1, ..., y_n) \in Y \cap \mathbb{A}^n \Leftrightarrow F(x_0, \dots, x_n) = 0$ i $x_0 \neq 0 \Leftrightarrow F(1, y_1, \dots, y_n) = 0$, $y_i = \frac{x_i}{x_0} \Leftrightarrow \hat{F}(y_1, \dots, y_n) = 0$

$Y \cap \mathbb{A}^n = \mathscr{Z}(\hat{F})$, pri čemu $\hat{F}$ nije konstanta zbog prethodne leme: $deg\hat{F} = degF \geq 1$. F zbog $I(Y) = (F)$ nema višestrukih ireducibilnih faktora $\implies \hat{F}$ nema višestrukih ireducibilnih faktora $\overset{\text{Teorem 5.8.}}{\Longrightarrow} I_{\mathbb{A}^n}(Y_{af}) = (\hat{F})$

3), 4) kao u prethodnoj lemi

Zadatak 9.5. *Za $n \geq 2$ dokazati: $X \subseteq \mathbb{A}^n$ hiperploha $\implies \bar{X} \cup \mathscr{Z}(T_0) \neq \emptyset$ te za $n = 2$ imamo konačan presjek.*

Primijetimo da je $\mathscr{Z}(T_0)$ pravac u beskonačnosti.



Uputa:

1. dio: Teorem 8.15. , svake dvije hiperplohe u $\mathbb{P}^n$ se sijeku, $n \geq 2$

2. dio: Teorem 8.18.

D.Z. (veza Definicije 9.3.) Umjesto reducirane jednadžbe f u Definiciji 9.3. možemo uzeti bilo koji g tako da $X = \mathscr{Z}^n_{\mathbb{A}}(g) \implies \bar{X} = \mathscr{Z}(\tilde{g})$. Uputa: Teorem 6.19.

Zadatak 9.6. *Izračunajte projektivizacije i presjek s pravcem u ∞:*

1) $X = (a_1y_1 + a_2y_2 + b = 0) = \mathscr{Z}(a_1R_1 + a_2R_2 + b)$, $a_1, a_2, b \in K$, $a_1a_2 \neq 0$, afini pravac

2) $X = (y_1 - y_2^2 = 0) = \mathscr{Z}(R_1 - R_2^2)$, parabola

3) $X = (y_1^2 + y_2^2 - 1 = 0) = \mathscr{Z}(R_1^2 + R_2^2 - 1)$, *elipsa*

Napomena: $(y_1^2 - y_2^2 = 1)$ *je elipsa:* $y_1^2 + (\sqrt{-1}y_2)^2 = 1$

Rješenje:

$0 = y_1 - y_2^2 = \frac{x_1}{x_0} - (\frac{x_2}{x_0})^2 / \cdot x_0^2$

$0 = x_1 x_0 - x_2^2 \ldots \bar{X}$

Presjek s $(x_0 = 0)$ daje: $x_0 = x_2 = 0 \implies x_1 \neq 0 \implies$ presjek s pravcem u ∞ je točka $(0:1:0)$.

Zadatak 9.7. *Dokažite da $f \in K[R_2]$ povlači $R_1 - f(R_2)$ je ireducibilan polinom u $K[R_1, R_2]$. Izračunajte homogenizaciju $R_1 - \tilde{f}(R_2) \in K[T_0, T_1, T_2]$ i $\bar{X}$ za $X = \mathscr{Z}(R_1 - f(R_2))$. Na kraju, ispitajte glatkoću $\bar{X}$ uz pretpostavku da je char $K = 0$.*

Zadatak 9.8. *(Hipereliptičke krivulje) Neka je $l \geq 1$, $z_1, \ldots, z_l \in K$ međusobno različite. Dokažite: $R_2^2 - (R_1 - z_1)\ldots(R_1 - z_l)$ je ireducibilan računajući rezltantu s $P(R_1)R_2 + Q(R_1)$, gdje su $P, Q \in K[R_1], P \neq 0$. (Zadatak 8.8.) Nadalje, odredite projektivizaciju i ispitajte njezinu glatkoću ako je char $K = 0$.*

$X \subseteq \mathbb{P}^2$ krivulja

$A = (a_0 : a_1 : a_2) \in X \implies a_0 \neq 0$ ili $a_1 \neq 0$ ili $a_2 \neq 0$

$\implies A \in X \cup D(T_0)$ ili $A \in X \cup D(T_1)$ ili $A \in X \cup D(T_2)$, gdje je svaki $X \cup D(T_i) \equiv \mathbb{A}^2$.

Nemojte zaboraviti: $X \backslash X \cup D(T_i)$ je konačan i neprazan skup za svaki $i = 0, 1, 2$

(Zadatak 9.5.) $\implies X \cup \mathscr{Z}(T_i)$ konačan ukoliko $\mathscr{Z}(T_i)$ nije ireducibilna komponenta od X (Teorem 8.18.)

Neka je na primjer $A \in D(T_0) \implies A = (a_0 : a_1 : a_2) = (\frac{a_1}{a_0}, \frac{a_2}{a_0}) = (a, b)$.

Prisjetimo se: (Teorem 9.4.) $X \subset \mathbb{P}^n$ hiperploha takva da $\mathscr{Z}(T_0)$ nije ireducibilna komponenta od X. Onda $X_{af} \overset{\text{def}}{=} X \cap \mathbb{A}^n$ je afina hiperploha takva da $I_{\mathbb{A}^n}(X_{af}) = (\hat{F})$ ako je $I(X) = (F)$.

Zadatak 9.9. *Točka $A \in X$ je glatka $\Leftrightarrow \frac{\partial f}{\partial R_1}(a, b) \neq 0$ ili $\frac{\partial f}{\partial R_2}(a, b) \neq 0$. Uputa: (Definicija 8.21.) + Eulerov identitet.*

Klasična definicija glatkoće: $I_{\mathbb{A}^2}(X_{af}) = (f)$

Točka (a,b) na X je glatka $\Leftrightarrow \frac{\partial f}{\partial R_i}(a,b) \neq 0$ za neki $i \in \{1,2\}$

Zadatak 9.10. *Tangencijalni pravac na X_{af} u nesingularnoj točki $(a,b) \in X_{af}$ je po definiciji $\frac{\partial f}{\partial R_1}(a,b)(y_1 - a) + \frac{\partial f}{\partial R_2}(a,b)(y_2 - b) = 0$. (lokalno)*
Dokažite: jednak je presjeku $D(T_0)$ i projektivnog tangencijalnog pravca ($\sum_{i=0}^{2} \frac{\partial F}{\partial T_i}(a_0,a_1,a_2)X_i = 0$) na X u točki A. (globalno)

f je reducirani polinom za X_{af}, $f \in K[R_1,R_2]$, rastavimo ga na homogene komponente
Taylorov razvoj oko točke (a,b) (vidi 2. poglavlje):

$$f_m(R_1,R_2) \stackrel{\text{def}}{=} \frac{1}{m!}\sum_{i=0}^{m}\binom{m}{i}\frac{\partial^m f}{\partial R_1^i \partial R_2^{m-i}}(a,b)R_1^i R_2^{m-i}$$

$$\implies f = \sum_{m=0}^{degf} f_m(R_1 - a, R_2 - b)$$

(Zadatak 9.9.) $\implies$ A glatka $\Leftrightarrow f_1 \neq 0$ (nul-polinom)

Definicija 9.11. *$A \in X_{af}$ je kratnosti $r \geq 1$ (ili r-struka točka) ako $f_0 = f_1 = \cdots = f_{r-1} = 0$ (nul-polinomi).*

Na primjer, (Zadatak 9.9.) $r = 1 \Leftrightarrow A$ glatka, tj. $r \geq 2$ znači da je točka A singularna.
Koliko ima točaka $A \in X_{af}$ tako da $r \geq 2$?
Ima ih konačno (moguće 0) jer na X postoji samo konačno singularnih točaka (vidi 8. poglavlje).
A r-struka točka $\implies f = f_r(R_1-a,R_2-b)+\cdots+f_{degf}(R_1-a,R_2-b)$, $f_r \neq 0$, homogen polinom stupnja r u varijablama R_1,R_2
(Kao u Zadatku 6.20., gdje smo studirali hiperplohe u $\mathbb{P}^1$)

$$f_r = \prod_{i=1}^{r}(A_iR_1 + B_iR_2), A_i, B_i \in K$$

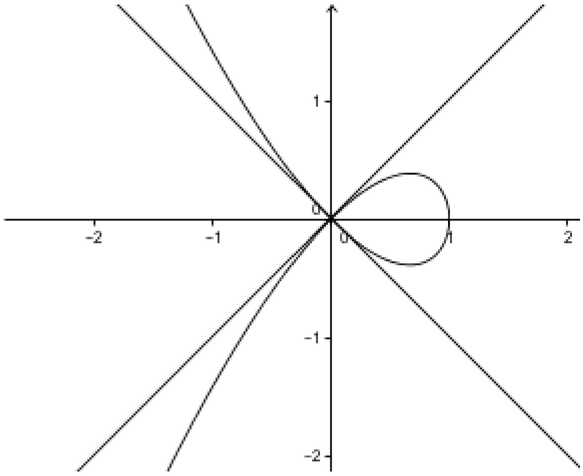
$\mathscr{Z}_{\mathbb{A}^2}(A_i(R_1-a)+B_i(R_2-b)), 1 \leq i \leq r$, tangente na X_{af} u točki A.
A je *jednostavna* ako ima r različitih tangenti, tj. f_r nema višestruke ireducibilne faktore, npr. A je glatka. $r = 2$ takva jednostvna točka naziva se *čvor*.
$K = \mathbb{C}$

$f = (-R_1^2 + R_2^2) + R_1^3$, Taylorov razvoj oko $(0,0)$

$A = (0,0)$, $f_0 = f(0,0) = 0$

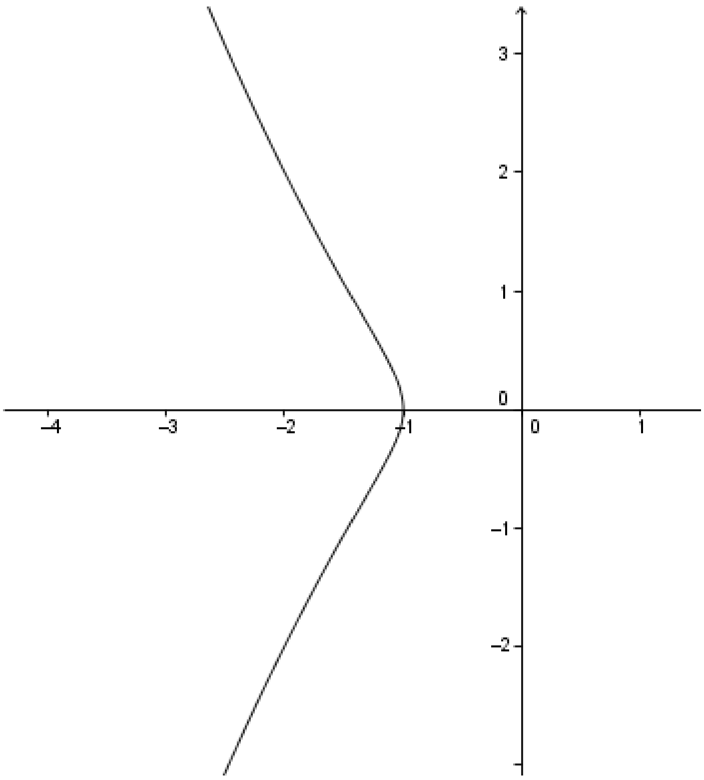
$f_1 = 0$, $f_2 = -R_1^2 + R_2^2 = (-R_1 + R_2)(R_1 + R_2)$, $f_3 = R_1^3$

Vidimo da zbog f_2 imamo dvije različite tangente pa je A čvor.



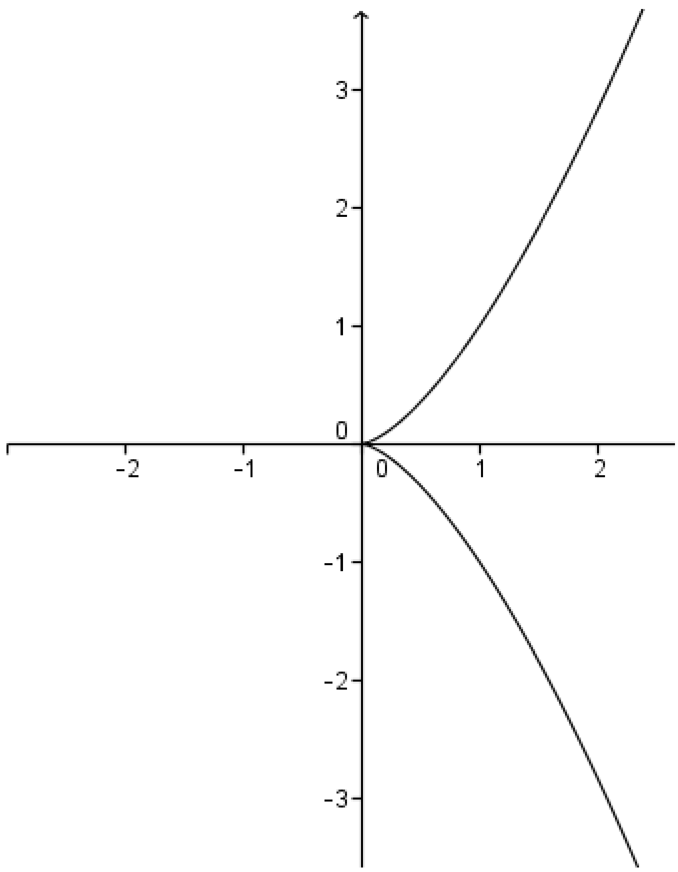
$f = (R_1^2 + R_2^2) + R_1^3$, Taylorov razvoj oko $(0,0)$

$f_0 = f_1 = 0$, $f_2 = R_1^2 + R_2^2 = (R_1 + iR_2)(R_1 - iR_2)$, $f_3 = R_1^3$, gdje opet vidimo da imamo dvije različite tangente za f_2



$f = -R_2^2 + R_1^3$, Taylorov razvoj oko $(0,0)$

$f_0 = f_1 = 0$, $f_2 = -R_2^2 = (-R_2)R_2$, $f_3 = R_1^3$. U ovom slučaju f_2 ima dvostruku tangentu: *šiljak* $\Longrightarrow$ $(0,0)$ nije čvor.



Poglavlje 10

Racionalne funkcije

Iz 6. poglavlja znamo da je projektivna mnogostrukost algebarski skup $X \subseteq \mathbb{P}^n$ takav da je $I(X)$ prost, tj X ireducibilan.
U 8. poglavlju vidjeli smo mnogo primjera projektivnih mnogostrukosti: linearne mnogostrukosti, kvadrike itd.

Ako je $f \in K[T_0, ..., T_n]$ homogen, definiramo glavni otvoreni skup u $\mathbb{P}^n$
$D(f) = \{(x_0 : ... : x_n) \in \mathbb{P}^n : f(x_0, ..., x_n) \neq 0\}$. Tada je $\mathbb{P}^n = \mathcal{Z}(f) \cup D(f)$.

Definicija 10.1. *$U \subseteq \mathbb{P}^n$ je otvoren ako je unija (konačna ili beskonačna) glavnih otvorenih skupova.*

Zadatak 10.2. *Ako su f i g homogeni polinomi, onda vrijedi:*

1. $D(f) \cap D(g) = D(fg)$
   $\mathcal{Z}(f) \cap \mathcal{Z}(g) = \mathcal{Z}(f, g)$
   $\mathcal{Z}(f) \cup \mathcal{Z}(g) = \mathcal{Z}(fg)$
2. *Ako je X ireducibilan u $\mathbb{P}^n$ i $D(f) \cap X \neq \emptyset$, $D(g) \cap X \neq \emptyset$, onda je $D(f) \cap D(g) \cap X \neq \emptyset$.*

Rješenje. Dokazujemo drugu tvrdnju. Ako je $D(f) \cap D(g) \cap X = \emptyset$, onda je $D(fg) \cap X = \emptyset$, pa je $X \subseteq \mathcal{Z}(fg)$. Slijedi da je $fg \in I(X)$, pa je $f \in I(X)$ ili $g \in I(X)$ (jer je $I(X)$ prost), pa je $X \subseteq \mathcal{Z}(f)$ ili $X \subseteq \mathcal{Z}(g)$, što je kontradikcija.

Definicija 10.3. *Neka je $X \subseteq \mathbb{P}^n$ projektivna mnogostrukost. Skup $S \subseteq X$ je gust ako za svaki homogen $f \in K[T_0, ..., T_n]$ $f = 0$ na S povlači $f = 0$ na X.*

Napomena 10.4. *$\mathbb{A}^1$ nije projektivna mnogostrukost, ali za $K = \mathbb{C}$, $\mathbb{A}^1 = \mathbb{C}$ i $\mathbb{Z} \subseteq \mathbb{C}$ je gust u njemu: $\forall f \in K[T]$, $f = 0$ na $\mathbb{Z} \Rightarrow f = 0$ na $\mathbb{C}$.*

Zadatak 10.5. *Neka je $X \subseteq \mathbb{P}^n$ projektivna mnogostrukost i $f \neq const$ homogen polinom takav da je $D(f) \cap X \neq \emptyset$. Tada je $S = D(f) \cap X$ gust u X.*

Neka je f homogen polinom stupnja l. Onda je $f(tx_0, ..., tx_n) = t^l f(x_0, ..., x_n)$. f ne definira vrijednost u točki $A = (x_0 : ... : x_n)$. Ali ako je g također homogen stupnja l i $A \notin \mathcal{Z}(g)$, onda je $g(tx_0, ..., tx_n) = t^l g(x_0, ..., x_n) \neq 0$ za $t \neq 0$, pa je

$$\frac{f(tx_0, ..., tx_n)}{g(tx_0, ..., tx_n)} = \frac{t^l f(x_0, ..., x_n)}{t^l g(x_0, ..., x_n)} = \frac{f(x_0, ..., x_n)}{g(x_0, ..., x_n)}.$$

Dakle, vrijednost od $\frac{f}{g}$ ne ovisi o izboru reprezentanta, pa je funkcija

$$D(g) \to K, \quad A \mapsto \left(\frac{f}{g}\right)(A) := \frac{f(x_0, ..., x_n)}{g(x_0, ..., x_n)}$$

dobro definirana.

Definicija 10.6. *Neka je $X \subseteq \mathbb{P}^n$ projektivna mnogostrukost. Definiramo skup*

$$\mathscr{O}_X = \left\{ \frac{f}{g} \ : \ f, g \in K[T_0, ..., T_n] \ homogeni \ istog \ stupnja, \ \ g \notin I(X) \right\}.$$

$(\mathscr{O}_X, +, \cdot)$ je komutativan prsten s jedinicom uz operacije:

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1 g_2 + f_2 g_1}{g_1 g_2}, \qquad \frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2}.$$

Definicije su dobre jer ako $g_1, g_2 \notin I(X)$, onda $g_1 g_2 \notin I(X)$.

Također $\mathscr{O}_X \supseteq K$, $\frac{\lambda}{1} \in \mathscr{O}_X$, $\forall \lambda \in K$, pa je $\mathscr{O}_X$ vektorski prostor na K. Dakle $\mathscr{O}_X$ je komutativna K-algebra.

Označimo $\mathfrak{M}_X = \left\{ \frac{f}{g} : f, g \ homogeni \ istog \ stupnja, \ f \in I(X), \ g \notin I(X) \right\}$. To je jedinstveni maksimalni ideal od $\mathscr{O}_X$. Naime, $\alpha \in \mathscr{O}_X \setminus \mathfrak{M}_X \Rightarrow \alpha = \frac{f}{g}$, $f, g \notin I(X) \Rightarrow \alpha^{-1} =$

$\frac{g}{f} \in \mathscr{O}_X$, tj. α je invertibilan.

Komutativan prsten s jedinstvenim maksimalnim idealom naziva se lokalan prsten.

Polje racionalnih funkcija je $K(X) := \mathscr{O}_X/\mathfrak{M}_X$.

$K(X) \supseteq K,\ \lambda = \frac{\lambda}{1} + \mathfrak{M}_X$.

Definicija 10.7. *$\phi \in K(X)$ je regularna u $A \in X$ ako postoje f, g homogeni polinomi istog stupnja takvi da je*

1. $\phi = \frac{f}{g} + \mathfrak{M}_X$
2. $A \in D(g) \cap X$.

Tada definiramo $\phi(A) = \frac{f(x_0,\ldots,x_n)}{g(x_0,\ldots,x_n)}$.

Vrijedi (ali je teško pokazati): Ako je ϕ regularna u svakom $A \in X$, onda je $\phi = const \in K$.

Domena od ϕ je $\mathcal{D}_\phi = \{A \in X\ :\ \phi \text{ regularno u } A\}$. Iz definicije se vidi da je $\mathcal{D}_\phi$ otvoren skup.

Definicija $\phi(A)$ ne ovisi o izboru funkcija f i g koje zadovoljavaju uvjete 1. i 2. (DZ)

Napomena 10.8. $\frac{f_1}{g_1} + \mathfrak{M}_X = \frac{f_2}{g_2} + \mathfrak{M}_X$

$\Leftrightarrow \frac{f_1g_2 - f_2g_1}{g_1g_2} \in \mathfrak{M}_X$

$\Leftrightarrow \frac{f_1g_2 - f_2g_1}{g_1g_2} = \frac{F}{G},\ F \in I(X),\ G \notin I(X)$ *homogeni istog stupnja*

$\Leftrightarrow G(f_1g_2 - f_2g_1) = Fg_1g_2 \in I(X)$

$\Leftrightarrow f_1g_2 - f_2g_1 \in I(X)$.

Zadatak 10.9. *Neka je $\phi \in K(X)$ regularna u svim točkama nekog nepraznog otvorenog skupa u X i neka je $\phi = 0$ tamo. Tada je $\phi = 0$ u $K(X)$.*

Rješenje. Neka je $\phi = \frac{f}{g} + \mathfrak{M}_X$, f, g homogeni istog stupnja. Neka je $V \subseteq \mathbb{P}^n$ otvoren skup takav da je $\phi(A) = 0$ za svaki $A \in X \cap V$. Tada $X \cap V = \bigcup X \cap \mathcal{D}(G)$, G homogen. Izaberimo neki takav G i točku $A \in X \cap \mathcal{D}(G)$. Tada je ϕ definiran u A i $\phi(A) = 0$. Onda postoji prikaz of ϕ takav da je $A \in \mathcal{Z}(f)$ i $A \in \mathcal{D}(g)$. Ali tada je ϕ dana prikazom $\frac{f}{g} + \mathfrak{M}_X$ na $(\mathcal{D}(g) \cap X) \cap (\mathcal{D}(G) \cap X) \neq \emptyset$. Dakle, na $\mathcal{D}(gG) \cap X$, $\phi = \frac{f}{g} + \mathfrak{M}_X = \frac{fG}{gG} +$

$\mathfrak{M}_X = \frac{f_1}{g_1} + \mathfrak{M}_X$, pa je $X \subseteq \mathcal{D}(g_1) \cup \mathcal{Z}(g_1)$. Po pretpostavci je $f_1 = 0$ na $\mathcal{D}(g_1)$, pa je $X \subseteq \mathcal{Z}(f_1) \cup \mathcal{Z}(g_1) = \mathcal{Z}(f_1 g_1)$. Slijedi $f_1 g_1 \in I(X)$, pa je $f_1 \in I(X)$ (jer $\mathcal{D}(g_1) \cap X \neq \emptyset$), pa je $\phi = \frac{f_1}{g_1} + \mathfrak{M}_X = \mathfrak{M}_X$, to jest $\phi = 0$ u $K(X)$.

Neka je $E \subseteq F$ proširenje polja. F je konačnogenerirano od E ako postoje $\alpha_1, ..., \alpha_l \in F$ takvi da je $F = E(\alpha_1, ..., \alpha_l) = \left\{ \frac{P(\alpha_1,...,\alpha_l)}{Q(\alpha_1,...,\alpha_l)} \ : \ P, Q \in E[T_1, ..., T_l],\ Q(\alpha_1, ..., \alpha_l) \neq 0 \right\}$.

Napomena 10.10. *Neka je $X \subseteq \mathbb{P}^n$ projektivna mnogostrukost. Tada postoji $i \in \{0, 1, ..., n\}$ takav da $X \nsubseteq \mathcal{Z}(T_i)$ jer je $\cap_{i=0}^{n} (x_i = 0) = \emptyset$. Najčešći izbor je $i = 0$.*

Lema 10.11. *Ako $X \nsubseteq (x_0 = 0)$, onda je $X_{af} = X \cap \mathbb{A}^n$ afina mnogostrukost. (Ovdje je $\mathbb{A}^n \equiv \mathcal{D}(T_0)$.)*

(Napomena: Teorem 9.4. je bio dokaz za ireducibilne hiperplohe.)

Dokaz. $X = \mathcal{Z}(f_1, ..., f_l)$, $f_i \in K[T_0, ..., T_n]$ homogeni. Onda je $X_{af} = \mathcal{Z}_{\mathbb{A}^n}(\hat{f}_1, ..., \hat{f}_l)$, ($\hat{f}_i = f_i(1, R_1, ..., R_n)$), pa je X_af algebarski skup, neprazan zbog $X \nsubseteq (x_0 = 0)$. Ostaje dokazati da je $I_{\mathbb{A}^n}(X_{af})$ prost.

Neka su $f, g \in K[R_1, ..., R_n]$ takvi da je $fg \in I_{\mathbb{A}^n}(X_{af})$. Tada je $\tilde{f}\tilde{g} = 0$ na X_{af}. Jer je $X \subseteq (x_0 = 0) \cup X_{af}$, slijedi $X \subseteq \mathcal{Z}(T_0 \tilde{f}\tilde{g})$. Dakle, $T_0 \tilde{f}\tilde{g} \in I(X)$, pa je $\tilde{f}\tilde{g} \in I(X)$ ($T_0 \notin I(X)$ jer $X \nsubseteq (x_0 = 0)$). Slijedi $\tilde{f} = 0$ na X ili $\tilde{g} = 0$ na X, pa i na X_{af}. Onda je prema Lemi 9.2. $f = 0$ na X_{af} ili $g = 0$ na X_{af}, pa je $f \in I_{\mathbb{A}^n}(X_{af})$ ili $g \in I_{\mathbb{A}^n}(X_{af})$. $\square$

$I_{\mathbb{A}^n}(X_{af})$ je prost ako i samo ako je $K[R_1, ..., R_n]/I$ integralna domena.

Imamo polje razlomaka, u oznaci $K(X_{af})$ koje je po definiciji polje racionalnih funkcija na X_{af}.

Slično kao ranije definiramo vrijednost $\phi \in K(X_{af})$ u točki $A = (a_1, ..., a_n)$:

ϕ je regularna u A ako postoje P, Q polinomi iz $K[R_1, ..., R_n]$ takvi da je $\phi = \frac{P + I_{\mathbb{A}^n}(X_{af})}{Q + I_{\mathbb{A}^n}(X_{af})}$ i $Q(a_1, ..., a_n) \neq 0$. U tom slučaju definiramo $\phi(A) = \frac{P(a_1,...,a_n)}{Q(a_1,...,a_n)}$.

Uočimo, u $K(X_{af})$ postoje funkcije koje su svuda regularne:

$\phi = P + I_{\mathbb{A}^n}(X_{af}) = \frac{P + I_{\mathbb{A}^n}(X_{af})}{1 + I_{\mathbb{A}^n}(X_{af})}$ i općenito nisu konstante.

Tvrdimo: *Polje $K(X_{af})$ generirano je nad K s $R_i + I_{\mathbb{A}^n}(X_{af})$, $i = 1, ..., n$.*

Dokaz. Gledamo kanonski epimorfizam $K[R_1, ..., R_n] \to K[R_1, ..., R_n]/I_{\mathbb{A}^n}(X_{af})$. Općeniti

$P = \sum_\alpha a_\alpha R_1^{\alpha_1}...R_n^{\alpha_n}$ se preslikava u

$P + I_{\mathbb{A}^n}(X_{af}) = \sum_\alpha a_\alpha (R_1 + I_{\mathbb{A}^n}(X_{af}))^{\alpha_1}...(R_n + I_{\mathbb{A}^n}(X_{af}))^{\alpha_n} = P(R_1 + I_{\mathbb{A}^n}(X_{af}),...,R_n + I_{\mathbb{A}^n}(X_{af}))$.

Konačno, za $\phi \in K(X_{af})$, $\phi = \frac{P+I_{\mathbb{A}^n}(X_{af})}{Q+I_{\mathbb{A}^n}(X_{af})} = \frac{P(R_1+I_{\mathbb{A}^n}(X_{af}),...,R_n+I_{\mathbb{A}^n}(X_{af}))}{Q(R_1+I_{\mathbb{A}^n}(X_{af}),...,R_n+I_{\mathbb{A}^n}(X_{af}))}$, pa je $K(X_{af})$ generiran iznad K s $R_i + I_{\mathbb{A}^n}(X_{af})$. $\square$

Propozicija 10.12. *Neka je $X \subseteq \mathbb{P}^n$ projektivna mnogostrukost, $X \nsubseteq (x_0 = 0)$. Tada je $K(X) \cong K(X_{af})$ (K-linearan izmorfizam polja). Nadalje, ako $\phi \in K(X)$ korespondira $\psi \in K(X_{af})$, tada je za svaki $A \in X_{af}$ ϕ definiran u A ako i samo ako je ψ definiran u A i u tom slučaju je $\phi(A) = \psi(A)$. Konačno, $K(X)$ je generiran iznad K s $\frac{T_i}{T_0} + \mathfrak{M}_X$, $i = 1,...,n$.*

Skica dokaza.

(i) Konstrukcija: $K[R_1,...,R_n] \longrightarrow K(X)$, $P \mapsto P\left(\frac{T_1}{T_0} + \mathfrak{M}_X,...,\frac{T_n}{T_0} + \mathfrak{M}_X\right) = \frac{\tilde{P}}{T_0^{\deg P}} + \mathfrak{M}_X$.

(ii) Jezgra ovog preslikavanja je $I_{\mathbb{A}^n}(X_{af})$. (uputa: $\frac{\tilde{P}}{T_0^{\deg P}} + \mathfrak{M}_X = \mathfrak{M}_X$ akko $\frac{\tilde{P}}{T_0^{\deg P}} \in \mathfrak{M}_X$ akko $\tilde{P} \in I(X)$ akko $P = \hat{\tilde{P}} \in I_{\mathbb{A}^n}(X_{af})$.)

(iii) Univerzalno svojstvo lokalizacije: $K(X_{af}) \xrightarrow{K-lin.\ inj.} K(X)$

$\frac{P+I_{\mathbb{A}^n}(X_{af})}{Q+I_{\mathbb{A}^n}(X_{af})} \mapsto \frac{P\left(\frac{T_1}{T_0}+\mathfrak{M}_X,...,\frac{T_n}{T_0}+\mathfrak{M}_X\right)}{Q\left(\frac{T_1}{T_0}+\mathfrak{M}_X,...,\frac{T_n}{T_0}+\mathfrak{M}_X\right)}$.

(iv) Surjektivnost u (iii):

$\phi = \frac{f}{g} + \mathfrak{M}_X \in K(X)$ akko $\frac{f}{T_0^l} + \mathfrak{M}_X = \phi\left(\frac{g}{T_0^l} + \mathfrak{M}_X\right)$, gdje je $l = \deg f = \deg g$.

Korolar 10.13. $K(\mathbb{P}^n) \overset{Prop\ 10.12.}{\cong} K(\mathbb{A}^n) \cong K(R_1,...,R_n)$.

Neka je $X \subseteq \mathbb{P}^n$ hiperploha i neka $X \nsubseteq (x_0 = 0)$. Prema Tm 9.4. je $X_{af} = X \cap \mathbb{A}^n$ ireducibilna hiperploha. Dalje je prema Propoziciji 10.12. $K(X) \cong K(X_{af})$.

Računamo $K(X_{af})$: Znamo da je $I_{\mathbb{A}^n}(X_{af}) = (f)$, za $f \in K[R_1,...,R_n]$ ireducibilni polinom. Prema Propoziciji 10.12. je $K(X_{af})$ = polje razlomaka $K(X_{af})/I_{\mathbb{A}^n}(X_{af})$. f je ireducibilan, pa ovisi npr. o R_n. Možemo pisati $f = \sum_{i=0}^l f_i(R_1,...,R_{n-1})R_n^i$, za $f_i \in K[R_1,...,R_{n-1}]$, $l \geq 1$, $f_l \neq 0$. Imamo kanonsko preslikavanje $K[R_1,...,R_n] \to K[R_1,...,R_n]/I_{\mathbb{A}^n}(X_{af}) \subseteq K(X_{af})$, $f \mapsto f + I_{\mathbb{A}^n}(X_{af}) = I_{\mathbb{A}^n}(X_{af})$, jer je $f \in I_{\mathbb{A}^n}(X_{af})$.

S druge strane, $f + I_{\mathbb{A}^n}(X_{af}) = \sum_{i=0}^l f_i(R_1 + I_{\mathbb{A}^n}(X_{af}),...,R_{n-1} + I_{\mathbb{A}^n}(X_{af}))(R_n + I_{\mathbb{A}^n}(X_{af}))^i$,

pa $z_i = R_i + I_{\mathbb{A}^n}(X_{af})$, $i = 1,...,n$, generiraju $K(X_{af})$ iznad K.

Vrijedi: $0 = f(z_1,...,z_n)$, pa z_n poništava polinom $f = \sum_{i=0}^l f_i(z_1,...,z_{n-1})T^i \in K(z_1,...,z_{n-1})[T]$.

Tvrdimo da je $f_l(z_1,...,z_{n-1}) \neq 0$ u $K(z_1,...,z_{n-1})$.

$f_l(z_1,...,z_{n-1}) = 0 \;\Leftrightarrow\; f_l + I_{\mathbb{A}^n}(X_{af}) = I_{\mathbb{A}^n}(X_{af}) \;\Leftrightarrow\; f_l \in I_{\mathbb{A}^n}(X_{af}) = (f) \;\Leftrightarrow\; f|f_l$, no to je nemoguće jer $f_l \neq 0$.

Dakle, z_n je algebarski element nad $K(z_1,...,z_{n-1})$.

Opće situacija:

Neka je $E \subset F,\ \alpha \in F$ algebarski nad E. Tada postoji $P \in E[T]$ takav da je $P(\alpha) = 0$. Skup svih takvih polinoma je ideal u $E[T]$, dakle, oblika (f) za neki $f \in E[T]$. Uočimo, f je ireducibilan u $E[T]$ jer

$f = f_1 f_2 \Rightarrow f(\alpha) = f_1(\alpha) f_2(\alpha) \Rightarrow f_1(\alpha) = 0$ ili $f_2(\alpha) = 0 \Rightarrow f_1 \in (f)$ ili $f_2 \in (f) \Rightarrow$ $f_1 = const$ ili $f_2 = const$.

Ako je $f = \sum_{i=1}^{l} f_i T^i,\ f_i \in E,\ f_l \neq 0,\ l \geq 1$, onda su $1,\ \alpha,...,\alpha^{l-1}$ algebarski nezavisni nad E i razapinju polje generirano s E i α u oznaci $E(\alpha) = E[T]/(f)$. Vrijedi $\dim_E E(\alpha) = l$ (stupanj proširenja).

Uočimo, kao kod dokaza $f_l(z_1,...,z_{n-1}) \neq 0$, imamo da je svaki $P \in K[z_1,...,z_{n-1}]$ takav da je $P(z_1,...,z_{n-1}) = 0$ nulpolinom.

Ako je $f \in K[R_1,...,R_n]$ ireducibilan, onda iz prvog poglavlja znamo da je $f \in K(R_1,...,R_{n-1})(R_n)$ ireducibilan, pa je $f(z_1,...,z_{n-1},T)$ ireducibilan u $K(z_1,...,z_{n-1})[T]$.

To dokazuje da je $K(z_1,...,z_n)$ algebarsko proširenje od $K(z_1,...,z_{n-1})$.

Propozicija 10.14. *$[K(X_{af} : K(z_1,...,z_{n-1})] = l$ i z_n ima ireducibilan polinom $f(z_1,...,z_{n-1},T) = \sum_{i=0}^{l} f_i(z_1,...,z_{n-1})T^i$, gdje je f određen s $I_{\mathbb{A}^n}(X_{af}) = (f)$ i ovisi o T_n.*

Poglavlje 11

Lokalni prsteni

Definicija 11.1. *Neka je $X \subseteq \mathbb{P}^n$ projektivna mnogostrukost i $P \in X$. Lokalni prsten od X u točki P je $\mathscr{O}_{X,P} = \{\varphi \in K(X) \mid \varphi$ regularan u $P\}$.*

Zadatak 11.2. *Dokažite da je $\mathscr{O}_{X,P}$ lokalan prsten s jedinstvenim maksimalnim idealom $\mathfrak{M}_{X,P} = \{\varphi \in \mathscr{O}_{X,P} \mid \varphi(P) = 0\}$.*

Također, dokažite da je $\frac{\mathscr{O}_{X,P}}{\mathfrak{M}_{X,P}} \simeq K$, gdje je pripadni izomorfizam: $\varphi \mapsto \varphi(P)$.

Na primjer, $\mathbb{Z}$ ima beskonačno mnogo ideala: (2), (3), $(5), \dots$ Ako fiksiramo prost broj p, onda imamo: $\mathbb{Z}(p) = \{\frac{m}{n} \in \mathbb{Q} \mid m \in \mathbb{Z}$, n nije djeljiv s $p\}$ i $\mathfrak{M}(p) = \{\frac{m}{n} \in \mathbb{Q} \mid m,n \in \mathbb{Z}$, m,n nije djeljiv s $p\}$.

11.1 Eksplicitni prikaz

Zadatak 11.3. *Neka $X \nsubseteq (x_0 = 0)$ i $P = (a_1, \dots, a_n) \in X_{af} = X \cap \mathbb{A}^n$. Tada je:*

$\mathscr{O}_{X,P} = \{\frac{f + I(X_{af})}{g + I(X_{af})} \,\Big|\, f,g \in K[R_1, \dots, R_n],\ g(P) \neq 0\}$, te je

$\mathfrak{M}_{X,P} = \{\frac{f + I(X_{af})}{g + I(X_{af})} \,\Big|\, f,g \in K[R_1, \dots, R_n],\ g(P) \neq 0,\ f(P) = 0\}$.

Zadatak 11.4. *(Neka je char $K = 0$.) Uz oznake iz prethodnog zadatka, pokažite da je*

$\mathfrak{M}_{X,P}$ generiran s $R_i - a_i + I(X_{af})$, za $1 \leq i \leq n$, tj. ima n generatora.

Rješenje.

$$\underbrace{\frac{f+I(X_{af})}{g+I(X_{af})}}_{\in \mathfrak{M}_{X,P}} = \underbrace{(g+I(X_{af}))^{-1}\cdot}_{\in \mathscr{O}_{X,P}} \quad \underbrace{(f+I(X_{af}))}_{\text{Taylorov razvoj oko P}} \quad . \ (\star)$$

Imamo: $f =$ "nejedinstveno" $= \sum_{i=1}^{n}(R_i - ai)g_i$, $g_i \in K[R_1, \ldots, R_n]$, pa je:

$f + I(X_{af}) = \sum_{i=1}^{n}[(R_i - a_i) + I(X_{af})] \cdot (g + I(X_{af}))$.

Zato je $(\star) = \sum_{i=1}^{n}[(R_i - a_i) + I(X_{af})] \cdot \frac{g_i + I(X_{af})}{g + I(X_{af})}$.

$\mathfrak{M}_{X,P} = \mathscr{O}_{X,P} z_1 + \ldots + \mathscr{O}_{X,P} z_n = (z_1, \ldots, z_n)$.

Važno je naglasiti da $z_1, \ldots, z_n$ nisu međusobno nezavisni!

$$f \in I(X_{af}) \Longrightarrow f = \underbrace{F(R_1 - a_1, \ldots, R_n - a_n)}_{T.razvoj}$$

$$0 = I(X_{af}) = f + I(X_{af}) = F(\underbrace{R_1 - a_1 + I(X_{af})}_{z_1}, \ldots, \underbrace{R_n - a_n + I(X_{af})}_{z_n})$$

$F(z_1, \ldots, z_n) = 0, \forall f \in I(X_{af})$

Parametri $z_1, \ldots, z_n$ se nazivaju *lokalni parametri od X u P.*

Definicija 11.5. *D je domena diskretne valuacije (DDV) ako je:*

(1) domena glavnih ideala

(2) lokalni prsten (pa ima jedinstven maksimalni ideal)

Primjer 11.6. *Ako je D polje, onda je i DDV, a maksimalni ideal je 0.*

Netrivijalna DDV je ona u kojoj je maksimalni ideal različit od 0.

Ako je D netrivijalna DDV, onda je maksimalni ideal $\mathfrak{M} = \langle t \rangle \neq 0$ jedinstven do na umnožak D^x. (t je lokalni parametar.)

D je DGI $\Longrightarrow$ D je faktorijalna domena $\Longrightarrow$ ireducibilni elementi su generatori maksimalnih ideala u D $\Longrightarrow$ do na asociranost, t je jedini ireducilbilni u D.

Za svaki $d \in D$, $d \neq 0$ $\exists! u \in D^x$ $\exists k \geq 0$ takav da $d = u \cdot t^k$. Oznaka: $\nu(d) = k$.

Zadatak 11.7. *Funkcija $\nu : D \setminus \{0\} \Longrightarrow \mathbb{Z}$ zadovoljava:*

(i) $\nu(d_1 d_2) = \nu(d_1) + \nu(d_2), \forall d_1, d_2 \in D \setminus \{0\}$.

(ii) $\nu(d_1 + d_2) \geq min\{\nu(d_1), \nu(d_2)\}, d_1, d_2, d_1 + d_2 \in D \setminus \{0\}$.

Napomena 11.8. *(1) Preslikavanje ν koje zadovoljava (i) i (ii) naziva se* valuacija na D.

(2) ν ne ovisi o izboru od t.

Zadatak 11.9. *(TEST ZA DDV) Neka je A integralna domena takva da $\exists t \in A$, $t \notin A^x$, $t \neq 0$ takva da $\forall a \in A \setminus \{0\}$ postoji, ne nužno jedinstven, $k \geq 0$ i $b \in A^x$ takav da je $a = b \cdot t^k$.*

Tada je A netrivijalna domena diskretne valuacije, t je lokalni parametar i $\mathfrak{M} = \langle t \rangle$.

Rješenje. (skica)

(1) jedinstvenost zapisa: PPS, tj. $a = b \cdot t^k = b_1 \cdot t^{k_1}$ (i $b \neq b_1, k \neq k_1$).

(a) $k = k_1 \Longrightarrow t^k(b - b_1) = 0 \Longrightarrow b = b_1$. (jer je A integralna domena)

(b) $k > k_1 \Longrightarrow t^{k_1}(t^{k-k_1}b - b_1) = 0 \Longrightarrow t^{k-k_1} \cdot b = b_1 \Longrightarrow t$ je invertibilan $\Longrightarrow$

$b = b_1$ i $k = k_1$. (posljednja implikacija slijedi iz toga što je A integralna domena)

(2) A je DGI:

$I \subseteq A$ ideal $\Longrightarrow I = \{0\} = \langle 0 \rangle$ ili $I \neq \{0\}$, prema (1), $\forall a \in I\{0\} \Longrightarrow \exists b \in A^x, \exists b \geq 0$, $a = b \cdot t^k$. Posebno, k je jedinstveno određen sa a.

Neka je $a_0 \in I \setminus \{0\}$ takav da je k_0 minimalan moguć $\Longrightarrow I = \langle a_0 \rangle$.

(3) $m = \langle t \rangle$ je jedinstven maksimalni ideal jer $A \setminus m = A^x$ prema (1).

Koristimo oznake iz drugog zadatka ovog poglavlja, $n = 2$. $I(X_{af}) = \langle f \rangle$.

Iz trećeg zadatka ove lekcije slijedi da je $\mathfrak{M}_{X,P} = \mathscr{O}_{X,P}z_1 + \mathscr{O}_{X,P}z_2$

$z_i = R_i - a_i + I(X_{af})$, $i = 1, 2$.

$f(z_1, z_2) = 0$ u $\mathscr{O}_{X,P}$.

Teorem 11.10. *(char $K = 0$)*

Neka je $X \subseteq \mathbb{P}^2$ ireducibilna projektivna krivulja. Ako je $P \in X$ nesingularna točka, onda je $\mathscr{O}_{X,P}$ netrivijalna DDV.

Dokaz. BSO $P \in X_{af}$ kao i do sada. (2., 3. zadatak)

CILJ:

(1) $\mathfrak{M}_{X,P} \neq \{0\}$ (netrivijalnost)

(2) (Znamo da je $\mathscr{O}_{X,P}$ kao potprostor u polju $K(X)$ integralna domena.) Želimo konstruirati t takav da je:

$$\forall u \in \mathscr{O}_{X,P} \exists v \in \mathscr{O}_{X,P}^{x} \exists h \geq 0 \text{ takav da je } u = v \cdot t^k. \text{ (zadatak 5.)}$$

Moramo paziti da je $t \neq 0$, $t \notin \mathscr{O}_{X,P}^{x}$.

Znamo: P je nesingularna točka za X, pa je P nesingularna točka za X_{af} (po 5.zadatku iz 9.poglavlja).

$\frac{\partial}{\partial R_i} f(a_1, a_2) \neq 0$, za neki $i \in \{1, 2\}$.

$\frac{\partial}{\partial R_i} f(a_1, a_2) \neq 0 \Longrightarrow t := z_1$. (i obratno.) Analogno teoremu o implicitno zadanoj funkciji.

Pretpostavimo da je $\frac{\partial}{\partial R_i} f(a_1, a_2) \neq 0$ i neka je $t := z_1$ i $z = z_2$.

$t(P) = z_1(P) = [R_1 - a_1 + I(X_{af})](P) = a_1 - a_1 = 0 \Longrightarrow t \in$ maksimalnog ideala.

$t \neq 0$ u $\mathscr{O}_{X,P}$, jer ako $t = 0$, onda je $R_1 - a_1 \in I(X_{af}) = \langle f \rangle \Longrightarrow f \mid (R_1 - a_1) \Longrightarrow f =$

$(const.) \cdot (R_1 - a_1)$, tj. f ne ovisi o R_2.

No, to je kontradikcija jer je $\frac{\partial}{\partial R_i} f(a_1, a_2) \neq 0$.

Dakle, $t \neq 0$ i $t \in \mathfrak{M}_{X,P} \Longrightarrow \mathfrak{M}_{X,P} \neq \{0\} \Longrightarrow (1)$ netrivijalnost.

Odavde slijedi i $t \neq 0$ i $t \notin \mathscr{O}_{X,P}$.

Taylorov razvoj oko $P = (a_1, a_2)$:

$f =$ članovi koji ne ovise o $(R_2 - a_2) +$ članovi koji ovise o $R_2 - a_2$

$= (R_1 - a_1) \cdot F(R_1 - a_1) + (R_2 - a_2)[\frac{\partial f}{\partial R_2}(a_1, a_2) + G(R_1 - a_1, R_2 - a_2)]$,

gdje je F neki polinom s koeficijentima iz K, a G polinom takav da je $G(0,0) = 0$.

$0 = I(X_{af}) = f + I(X_{af}) = [(R_1 - a_1) + I(X_{af}]F((R_1 - a_1 + I(X_{af})) + (R_2 - a_2 + I(X_{af}) \cdot [\frac{\partial f}{\partial R_2}(a_1, a_2) + I(X_{af})] + G(\dots)$.

U $\mathscr{O}_{X,P}$:

$t \cdot F(t) + [\frac{\partial f}{\partial R_2}(a_1, a_2) + G(t, z)] \cdot z = 0 \Longrightarrow \frac{\partial f}{\partial R_2}(a_1, a_2) + G(t, z) \in \mathscr{O}_{X,P}^x$.

Dakle, $z = (\dots)^{-1} \cdot F(t) \cdot t$, tj. $z = v \cdot t$, $v \in \mathscr{O}_{X,P}$.

Napomena 11.11. $\mathfrak{M}_{X,P} = \mathscr{O}_{X,P} \cdot t + \mathscr{O}_{X,P} \cdot z = (\mathscr{O}_{X,P} + \mathscr{O}_{X,P} \cdot v) \cdot t = \mathscr{O}_{X,P} \cdot t = \langle t \rangle$.

Uzmimo $u \in \mathscr{O}_{X,P} \setminus \{0\} \Longrightarrow u = \frac{F + I(X_{af})}{G + I(X_{af})}, G(p) \neq 0$.

$u \neq 0 \Longrightarrow F \notin I(X_{af}) = \langle f \rangle \iff f \nmid F$.

Cilj nam je pokazati da postoji neki $u' \in \mathscr{O}_{X,P}^x$ i neki $k \geq 0$ takvi da je $u = u' \cdot t^k$.

Koliko za zadani u može k biti velik?

(1) F ovisi o $R_2 - a_2$ (nakon što ga razvijemo u Taylorov razvoj)

$$\Longrightarrow F = c_k \cdot (R_1 - a_1)^k + c_{k+1} \cdot (R_1 - a_1)^{k+1} + \dots$$

$$= (R_1 - a_1)^k \cdot [c_k + c_{k+1}(R_1 - a_1) + \dots], c_i \in K.$$

$\implies F + I(X_{af}) = t^k \cdot$ neki invertibilni element (nazovimo ga y).

$\implies u = t^k \cdot \frac{y}{G+I(X_{af})} =: u'$.

(2) F ovisi o $R_2 - a_2$

f ovisi o $R_2 - a_2$ jer $\frac{\partial f}{\partial R_2}(a_1, a_2) \neq 0$

$\implies \exists A, B$ polinomi takvi da je $A \cdot f + B \cdot F = Res_{R_2 - a_2}(F, f)$.

$\implies (A + I(X_{af}))(f + I(X_{af}) + (B + I(X_{af}))(F + I(X_{af})) = Res_{R_2 - a_2}(F, f) + I(X_{af})$

$\implies (B + I(X_{af}) \cdot (F + I(X_{af})) = Res_{R_2 - a_2}(F, f) + I(X_{af})$

$= c_k(R_1 - a_1)^k + c_{k+1}(R_1 - a_1)^{k+1} + \dots$

$= c_k t^k + c_{k+1} t^{k+1} + \dots$

$= t^k \underbrace{(c_k + c_{k+1} t + \dots)}_{invertibilan}.$

Važno: $Res_{R_2 - a_2}(F, f) \neq 0$ jer $f \nmid F$ po pretpostavci, f ireducibilan te $\exists c_k \neq 0$ kakav tvrdimo.

Sada: $u = \frac{F+I(X_{af})}{G+I(X_{af})} = t^l u'$, $l \geq 0$, $u' \in \mathscr{O}_{X,P}^x \iff u'(P) \neq 0$.

Koliki l može biti?

$(B + I(X_{af})) \cdot u = (G + I(X_{af}))^{-1} t^k$ (invertibilan)

Definirajmo: $w := (B + I(X_{af}))u'$.

$w \cdot t^l = t^k \cdot w_1$

$w_1 =$ invertibilan $= (G + I(X_{af})^{-1}$.

Tvrdimo: $l \leq k$.

Naime, ako $l \geq k$, onda $t^k(wt^{l-k} - w_1) = 0$, pa je $\underbrace{w(P)t^{l-k}(P)}_{=0} = \underbrace{w_1(P)}_{\neq 0}$, što je kontradikcija.

Zapravo smo dokazali i više:

Za svaki $u \in \mathcal{O}_{X,P} \setminus \{0\}$ postoji $k \geq 0$ koji se efektivno može izračunati tako da ako je $u = t^k u^{'}$, za neki $u^{'} \in \mathcal{O}_{X,P}$, ne nužno invertibilan, onda je $l \leq k$.

$\forall u \in \mathcal{O}_{X,P} \setminus \{0\} \exists k \geq 0 \exists u^{'} \in \mathcal{O}_{X,P}^{x}$ takav da $u = u^{'} t^k$.

($\Longrightarrow$ (2) s početka dokaza).

$u = \frac{F+I(X_{af})}{G+I(X_{af})}$, $G(P) \neq 0$.

Ako je $F(P) \neq 0$, onda je u invertibilan i možemo uzeti $u^{'} = u$, $k = 0$.

Ako je $F(P) = 0$, onda je $F =$ Taylorov razvoj oko P = suma monoma u $R_1 - a_1, R_2 - a_2$ stupnja ≥ 1.

$\Longrightarrow F + I(X_{af}) =$ suma monoma u t, z stupnja ≥ 1.

Izraz s početka dokaza: $z = v \cdot t$, za neki $v \in \mathcal{O}_{X,P}$ = $t\cdot$ neki element iz $\mathcal{O}_{X,P}$ (nazovimo ga d) = suma monoma u $t, v \cdot t$ stupnja ≥ 1

$\Longrightarrow u = \frac{F+I(X_{af})}{G+I(X_{af})} = t \cdot \frac{d}{G+I(X_{af})}$.

Zaključak: $u \notin \mathcal{O}_{X,P}^{x} \Longrightarrow u = t \cdot u_1$, za neki $u_1 \mathcal{O}_{X,P}$.

Ako je u_1 invertibilan, onda smo gotovi, ako ne, onda $u_1 = t u_2 \Longrightarrow u = t^2 u_2$ itd.

Zbog $(\star)$ proces mora stati i završni u_k je invertibilan, tj. $u = t^k u_k$, $u_k \in \mathcal{O}_{X,P}^{x}$.

$\square$

Definicija 11.12. *Neka je $C \subseteq \mathbb{P}^2$ glatka projektivna krivulja (, pa i ireduc.).* Grupa divizora *na C je slobodna Abelova grupa: $Div(C) = \bigoplus_{c \in C} \mathbb{Z}_c$.*

$D = \sum_{c \in C} k_c \cdot c$, $k_c \in \mathbb{Z}_c$, $k_c = 0$ osim za konačno mnogo točaka $c \in C$.

$D = 0$, tj. $k_c = 0, \forall c \in C$ NUL - DIVIZOR.

D je *efektivan* ako je $k_c \geq 0, \forall c \in C$ i ako je $D \neq 0$. Tada pišemo: $D > 0$.

D je *prost* ako je $D = c$, za neki $c \in C$.

11.2 Stupanj divizora

Neka je $D = \sum_{c \in C} k_c \cdot c$. Stupanj divizora D je:

$deg(D) =$ suma multipliciteta $k_c = \sum_{c \in C} k_c$, gdje je k_c *multiplicitet od D u točki* $c \in C$.

Funkcija deg: Div(C) $\to \mathbb{Z}$ je homomorfizam.

Skup supp(D) = $\{c \in C \mid k_c \neq 0\}$ je konačan i nazivamo ga *nosačem divizora*.

(Konstrukcija) Divizor pridružen homogenom polinomu $g \notin I(C)$.

$g \notin I(C) \Longrightarrow \#Z(g) \cap C < \infty$

(jer ako ne, Z(g) i C imaju ireducibilnu komponentu zajedničku $\Longrightarrow$ C je ireducibilna komponenta u Z(g) $\Longrightarrow g \in I(g)$).

$div(g) \in Div(C)$

$div(g) = \sum_{P \in C} k_P P \to$ efektivan divizor, DZ.

C je glatka u $P \Longrightarrow \mathscr{O}_{C,P}$ netrivijalna DDV, $t_{C,P}$ lokalni parametar.

$P = (a_0 : a_1 : a_2) \Longrightarrow \exists i$ takav da $a_i \neq 0$ te ako je g stupnja l, onda je $\frac{g}{T_i^l} + \mathfrak{M}_C \in \mathscr{O}_{C,P}$.

k_P definiramo: $\frac{g}{T_i^l} + \mathfrak{C} = t_{C,P}^{k_P}$.

Mogli smo uzeti bilo koji h homogen stupnja istog kao g (mi smo uzeli T_i^l) takav da je $h(P) \neq 0$) i definirati: $\frac{g}{h} + \mathfrak{M}_C \in \mathscr{O}_{C,P}$.

Onda bi definirali k_P sa $\frac{g}{h} + \mathfrak{M}_C = t_{C,P}^{k_P}$.

Naime, $\frac{g}{h} + \mathfrak{M}_C = (\frac{g}{T_i^l + \mathfrak{M}_C})(\frac{T_i^l}{h} + \mathfrak{M}_C) \Longrightarrow$ isto do na invertibilan element.

DZ: Ako je stvarno $P \in Z(g) \cap C \iff g(P) = 0 \iff k_{C,P} \geq 1$.

Sada vrijedi sljedeći rezultat, poopćenje Bezoutova teorema:

Teorem 11.13. *(potpuni Bezoutov teorem) Neka je C nesingularna projektivna krivulja u* $\mathbb{P}^2$ *i* $g \notin I(C)$ *homogen polinom. Tada je* $\sum_{P \in C} \nu_{C,P}(g) = deg(g) \cdot deg(C)$.

Napomena 11.14. *Iz teorema 3 u 8.poglavlju slijedi:* $\#C \cap Z(g) \leq deg(g)deg(C) \Longrightarrow$ *divizor određuje multiplicitet presjeka.*

Napomena 11.15. *Poopćenje Osnovnog teorema algebre:*

$f = (R - a_1)^{n_1} \cdot \dots \cdot (R - a_l)^{n_l} \in K[R]$, *gdje je* $n_1 + n_2 + \ldots + n_l = deg(f)$.

C ireducibilna projektivna krivulja u $\mathbb{P}^2$

$\rightarrow C$ je nesingularna svugdje osim možda u konačno mnogo točaka (znamo iz poglavlja 8).

$\rightarrow P \in C$ nesingularna točka $\Longrightarrow \mathscr{O}_{C,P} = \{\phi \in K(C) \mid \phi$ regularna u P$\}$ je netrivijalna DDV (Po teoremu 1).

$\mathfrak{M}_{C,P}$ jedinstven maksimalan ideal $\mathfrak{M}_{C,P} = \langle t_{C,P} \rangle$.

$\forall u \in \mathscr{O}_{X,P} \Longrightarrow \exists u^{'} \in \mathscr{O}^{x}_{X,P}$, $k \geq 0$.

$u = u^{'} t^{k}_{X,P}$, $0 \neq u^{'}(P) \in K$.

$\rightarrow C$ nesingularna (npr. pravac ili konika).

Za svaki homogen $g \in K[T_0, T_1, T_2]$, $g \notin I(C)$ možemo definirati $div(g) = \sum_{c \in C} \underbrace{\nu_{C,c}(g)}_{presjecni.divizor} \cdot c$,

$c = (a_0 : a_1 : a_2) \in C$ izaberemo bilo koji homogen polinom h istog stupnja kao g takav da je $h(c) \neq 0$.

Npr., $\exists i \in \{1,2,3\}$ takav da $a_i \neq 0$ te možemo uzeti $h = T_i^{deg(g)} \Longrightarrow \frac{g}{h} \in \mathscr{O}_C$ (vidi poglavlje 10).

$\Longrightarrow \varphi := \frac{g}{h} + \mathfrak{M}_C \in K(C)$ očito regularan u $c \Longrightarrow \varphi \in \mathscr{O}_{C,c}$, $\varphi(c) = \frac{g(c)}{h(c)}$.

$\varphi = \varphi^{'} t_{C,c}$, $\varphi^{'}(C) \neq 0$.

(1) Definicija ne ovisi o izboru od h.

(2) $\nu_{C,c}(g) \geq 1 \iff \varphi(c) = 0 \iff \varphi \in \mathfrak{C}, \mathfrak{c}$.

($\varphi(c) = 0 \iff g(c) = 0 \iff c \in Z(g) \cap C$, Z(g) konačan skup)

(3) div(g) = $\sum_{c \in Z(g) \cap C} \nu_{C,c}(g) \cdot c$ (ostali $\nu = 0$)

$\sum \nu_{C,c}(g) = deg(g) deg(c)$ (Bezout).

deg(div(g)) = stupanj presječnog divizora.

Zadatak 11.16. *(DZ)*

$(1) g_1, g_2$ *homogeni,* $g_2 \notin I(C), g_1 - g_2 \in I(C)$.

(a) $g_1 \notin I(C)$.

(b) g_1 *je istog stupnja homogenosti kao i* g_2

(jer $I(C)$ *homogen stupnja k, inače iz* $g_1 - g_2 \in I(C)$ *slijedi* $g_1, g_2 \in I(C)$*)*

(c) $div(g_1) = div(g_2)$

$(2) f, g homogeni \notin I(C)$

$\implies f, g \notin I(C)$ *(jer je* $I(C)$ *prost!).*

Vrijedi: $div(f \cdot g) = div(f) + div(g)$.

Korolar 11.17. *(Bezoutova teorema)*

$deg(div(\varphi)) = 0$, *tj.* $\sum_{i=1}^{l} n_i = \sum j = 1^k m_j$.

(Broj nula računato s kratnostima = broj polova računato s kratnostima.)

Važno: $\varphi =$ const. $\implies l = k = 0$.

$\varphi \neq$ const $\implies l, k \geq 1$.

Dokaz. (korolara)

Teorem 2 $\Longrightarrow deg(div\varphi) = deg(divf) - deg(divg) = deg(f)\cdot deg(C) - deg(g)\cdot deg(C) =$ 0. $\square$

Neka je C pravac ($x_2 = 0$).

$C = \{(x_0 : x_1 : 0) \mid x_0, x_1 \in K$, ne oba nula$\}$

$\equiv \mathbb{P}^1 = \{(x_0 : x_1) \mid x_0, x_1 \in K$, ne oba nula$\}$

Notacija iz 9. poglavlja: $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$.

$\mathbb{A}^1 = \{(x_0 : x_1) \mid x_0 \neq 0\}$.

Propozicija 1 iz 9.poglavlja $\Longrightarrow K(C) \simeq K(R)$, R varijabla.

$(x_0 : x_1 = \in \mathbb{A}^1 = Y = \frac{x_1}{x_0}$ (afina koordinata).

$C = (a_0 : a_1) = \frac{a_1}{a_0} = \lambda \in K$.

$\varphi \in K(R) \Longrightarrow \varphi = \varphi'(R-\lambda)^k$, pri čemu φ' definiramo $\neq 0$ u točki λ.

Npr. $\varphi = \frac{P}{Q}$, $P, Q \in K[R]$.

$P = (R-\lambda)^l \cdot P_1;\ P_1(\lambda) \neq 0.$

$Q = (R-\lambda)^m \cdot Q_1;\ Q_1(\lambda) \neq 0$

$\varphi = \frac{P}{Q} = (R-\lambda)^{l-m} \cdot \frac{P_1}{Q_1}$

$(R-\lambda)$ je lokalni parametar u točki c.

Što je lokalni parametar u ∞?

$\mathbb{P}^1 = \mathbb{A}^1 \cup \{(0:1)\}$

Slična konstrukcija kao u prvom dijelu za slučaj $\lambda = 0$.

$K(C) \simeq K(R^{'})$, $R^{'}$ nova varijabla.

Gledamo iz afine situacije: npr. $\varphi = a_n R^n + \ldots + a_1 R + a_0 \in K(R) \equiv K(\mathbb{C})$

$v_{C,\infty}(\varphi) = -m$ stupanj od polinoma φ.

$\varphi = \prod_{i=1}^{l}(R-\lambda_i)^{m_i}$

Svaka dva otvorena skupa u X se sijeku (po zadatku 1, iz poglavlja 10).

Definicija 11.18. Racionalno preslikavanje$\varphi : X \to \mathbb{P}^m$ *je u stvari preslikavanje* $\varphi : U \to \mathbb{P}^m$*,* $U \subseteq X_{af}$ *regularan, takvo da je* $\forall P \in U$ $\exists$ *okolina* V*,* $P \in V \subseteq U$ *i* $\exists$ *homogeni polinomi* $F_0, \ldots, F_m$ *istog stupnja homogenosti takvi da:* $\varphi(x_0 : \ldots : x_n) = (F_0(x_0, \ldots, x_n) : \ldots : F_m(x_0, \ldots, x_n)) \in \mathbb{P}^n$*,* $\forall (x_0 : \ldots : x_n) \in V$*.*

Definicija 11.19. *Preslikavanje* φ *je regularno ako je racionalno i definirano na cijelom* X*.*

Projekcija iz točke $(0:0:\ldots:0:1)$ na $\mathbb{P}^{n-1}$ je racionalno preslikavanje : $\mathbb{P}^n \to \mathbb{P}^{n-1}$, $(x_0 : \ldots : x_{n-1} : x_n) \mapsto (x_0 : \ldots : x_{n-1})$.

Npr. za $X \subseteq \mathbb{P}^n$ projektivnu mnogostrukost, $(0 : \ldots : 0 : 1) \notin X$, projekcija : $X \to \mathbb{P}^{n-1}$ je regularna na X.

Definicija 11.20. *Projektivne mnogostrukosti* X *i* Y *su* biracionalno ekvivalentne *ako postoji racionalno preslikavanje* $\alpha : X \to Y$*,* $\beta : Y \to X$ *takvo da je* $\alpha \circ \beta = \mathbb{1}_X$*, pri čemu jednakost vrijedi na nekom otvorenom skupu u* X *i* Y *(, a ne svugdje!).*

11.3 Karakterizacija biracionalne ekvivalencije

X, Y biracionalno ekvivalentni $\iff$ $K(X) \simeq K(Y)$.

Definicija 11.21. Algebarska krivulja *u* $\mathbb{P}^n$ *je projektivna mnogostrukost* X *za koju postoji ireducibilna ravninska projektivna krivulja* $Y \subseteq \mathbb{P}^2$ *koja je biracionalno ekvivalentna sa* X*.*

Koja je najjednostavnija krivulja? $\mathbb{P}^1$ pravac, npr realiziran kao $(x_2 = 0)$.

$L(\mathbb{P}^1) \simeq K(T)$

Definicija 11.22. *Krivulja $C \subset \mathbb{P}^n$ je* racionalna *ako je biracionalno ekvivalentna $\mathbb{P}^1$ $\iff$ $K(X) =$ polje racionalnih funkcija u jednoj varijabli na K.*

Neka je C ireducibilna konika u $\mathbb{P}^2$.

char $K = 0$, X projektivizacija (poglavlje 9).

$y_2^2 = y_1^3 + py_1 + q$, $p, q \in K$, $4p^3 + 27q^2 \neq 0 \Longrightarrow X$ nije racionalna.

$\to$ eliptička krivulja.