Teorija eliminacije varijable i primjene u geometriji

Vrsaljko, Mirna

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Mirna Vrsaljko

TEORIJA ELIMINACIJE VARIJABLE I PRIMJENE U GEOMETRIJI

Diplomski rad

Voditelj rada:
prof. dr. sc. Goran Muić

Zagreb, rujan, 2021.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Hvala mome mentoru prof. dr. sc. Goranu Muiću na velikoj pomoći pri izradi rada te strpljenju i pristupačnosti.

Hvala najdražim kolegama s fakulteta, Martini na uvijek spremnim materijalima i informacijama, Kneži na zajedničkom učenju i pomoći oko gradiva i Matei za organiziranje proslava nakon uspješno (ili manje uspješno) položenih kolokvija.

Hvala svim mojim ostalim prijateljima koji su mi uljepšali i one teže dane studiranja.

Na kraju, posebno hvala mojoj obitelji koja je bila tu za mene od početka.

Sadržaj

Uvod

Teorija eliminacije naziv je za algoritamske pristupe uklanjanju nekih varijabli između polinoma s više varijabli, kako bi se riješili sustavi polinomijalnih jednadžbi. Na početku rada, uvest ćemo neke osnovne pojmove koji će nam biti potrebni za daljnje razumijevanje.

U prvom poglavlju definirat ćemo osnovne algebarske strukture, grupu, prsten, polje itd. Zatim ćemo definirati polinom u jednoj i u više varijabli te navesti glavne pojmove vezane za polinome poput koeficijenata i stupnja. Također ćemo definirati operacije zbrajanja i množenja nad polinomima. Iskazat ćemo i dokazati neke od teorema vezanih uz polinome poput teorema o dijeljenju s ostatkom te osnovnog teorema algebre. Zatim ćemo navesti najvažnije pojmove vezane uz vektorske prostore. Definirat ćemo vektorski prostor, njegovu bazu, dimenziju itd.

U drugom poglavlju definirat ćemo integralnu i faktorijalnu domenu, asocirane i ireducibilne elemente te iskazati i dokazati nekoliko propozicija. Na kraju ćemo napokon prijeći na samu teoriju eliminacije varijabli te iskazati i dokazati dva glavna teorema. Na kraju ćemo definirati hiperplohu te iskazati i dokazati korolar o jedinstvenosti jednadžbe ireducibilne hiperplohe.

Poglavlje 1

Preliminarni rezultati

1.1 Osnovne algebarske strukture

Na početku, navest ćemo neke osnovne algebarske strukture te dati primjere za svaku od njih.

Definicija 1.1.1. *Neka je S neprazan skup. Preslikavanje*

$$\cdot : S \times S \to S$$

*naziva se **binarna operacija** na skupu S. Binarna operacija $\cdot$ svakom uređenom paru $(x, y) \in S \times S$ pridružuje element $z = \cdot(x, y) \in S$ (pišemo još i $z = x \cdot y$).*

*Uređeni par $(S, \cdot)$ naziva se **grupoid**, odnosno kažemo da binarna operacija $\cdot$ određuje na skupu S algebarsku strukturu grupoida.*

Budući da je S kodomena preslikavanja $\cdot$ za sve $x, y \in S$ vrijedi

$$x \cdot y \in S.$$

Kažemo još da je binarna operacija **zatvorena** ili da je **dobro definirana**.

Primjer 1.1.2. *Oduzimanje prirodnih brojeva nije zatvorena operacija. Naime, oduzimanje možemo definirati kao operaciju $- : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$, ali struktura $(\mathbb{N}, -)$ nije grupoid. Na primjer, $1 - 3 = -2 \notin \mathbb{N}$, iako vrijedi $1, 3 \in \mathbb{N}$.*

Primjer 1.1.3. *Za razliku od oduzimanja, zbrajanje prirodnih brojeva **jest** zatvorena operacija te je stoga $(\mathbb{N}, +)$ grupoid.*

Primjer 1.1.4. *Grupoidi su također i* $(\mathbb{N}, \cdot), (\mathbb{Z}, +), (\mathbb{Z}, \cdot), (\mathbb{Q}, +)$ *itd.*

Definicija 1.1.5. ***Polugrupa*** *je grupoid* $(S, \cdot)$ *u kojem vrijedi asocijativnost, za sve* $x, y, z \in S$*:*

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

Primjer 1.1.6. *Grupoid* $(\mathbb{Z}, -)$ *nije polugrupa jer ne vrijedi asocijativnost oduzimanja. Na primjer,* $(5 - 3) - 2 = 0$*, ali* $5 - (3 - 2) = 4$*.*

Primjer 1.1.7. *Skupovi brojeva* $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *s obzirom na standardno zbrajanje i standardno množenje su polugrupe.*

Definicija 1.1.8. ***Monoid*** *je polugrupa* $(S, \cdot)$ *u kojoj postoji neutralni element (ili jedinica),* tj. *postoji* $e \in S$ *takav da za sve* $x \in S$ *vrijedi*

$$e \cdot x = x \cdot e = x\,.$$

Primjer 1.1.9. *Skupovi brojeva* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *s obzirom na standardno zbrajanje i standardno množenje su monoidi. Neutralni element zbrajanja je 0, a množenja* 1*.*

Primjer 1.1.10. *Polugrupa* $(\mathbb{N}, +)$ *nije monoid. Naime, kad bi postojao neutralni element* $e \in \mathbb{N}$ *s obzirom na operaciju zbrajanja, posebno bi moralo vrijediti* $1 + e = 1$*. No, uočimo da nijedan prirodan broj nema to svojstvo (Nula nije prirodan broj!).*
No, zato $(\mathbb{N}, \cdot)$ *jest monoid.*

Definicija 1.1.11. *Neka je* $(S, \cdot)$ *grupoid i neka je e njegov neutralni element. Ako za* $x \in S$ *postoji* $y \in S$ *takav da vrijedi*

$$xy = yx = e,$$

onda kažemo da je element x ***invertibilan****, a element y zovemo* ***inverzni element*** *ili kraće* ***inverz*** *elementa x.*

Definicija 1.1.12. *Monoid u kojem su svi elementi invertibilni naziva se* ***grupa****. Ako je binarna operacija komutativna onda govorimo o* ***komutativnoj*** *ili* ***Abelovoj grupi****.*

Grupu možemo definirati i drugačije, tako da nabrojimo sva svojstva koja grupoid mora zadovoljavati.

Definicija 1.1.13. *Neka je G neprazan skup i $\cdot$ binarna operacija. Uređeni par $(G, \cdot)$ nazivamo* ***grupom*** *ako vrijede sljedeća svojstva:*

(1) $xy \in G$ za sve $x, y \in G$ (zatvorenost),

(2) $(xy)z = x(yz)$ za sve $x, y, z \in G$ (asocijativnost),

(3) Postoji $e \in G$ takav da je $ex = xe = x$ za sve $x \in G$ (neutralni element),

(4) Za svaki $x \in G$ postoji $y \in G$ takav da je $xy = yx = e$ (inverzni element)

Ako vrijedi i svojstvo

(5) $xy = yx$ za sve $x, y \in G$ (komutativnost)

onda je $(G, \cdot)$ ***komutativna*** *ili* ***Abelova grupa****.*

Primjer 1.1.14. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ *su Abelove grupe.*

Primjer 1.1.15. *Uočimo da niti jedna od struktura $(\mathbb{N}, \cdot), (\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$ nije grupa, no nekima od njih nedostaje "malo" da to postanu. Svi elementi različiti od 0 u $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su invertibilni. Za element 0 ne postoji inverz, tj. ne postoji takav x iz navedenih skupova da bi vrijedilo $x \cdot 0 = 1$. Stoga promotrimo te iste skupove bez nule, to jest*

$$\mathbb{Q}^* = \mathbb{Q}\backslash\{0\},\ \mathbb{R}^* = \mathbb{R}\backslash\{0\},\ \mathbb{C}^* = \mathbb{C}\backslash\{0\}$$

Primijetimo da su svi ovi skupovi zatvoreni na operaciju množenja ($a \neq 0$, $b \neq 0$ povlači $ab \neq 0$) pa su $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$ Abelove grupe. Ostala svojstva grupe ovdje se lako provjere, pri čemu se asocijativnost i komutativnost izravno nasljeđuju na podskup pa ih i ne treba posebno provjeravati.

Definirajmo sada prsten.

Definicija 1.1.16. *Neka je R neprazan skup na kojem su definirane dvije binarne operacije $+$ i $\cdot$. Kažemo da je uređena trojka $(R, +, \cdot)$* ***prsten*** *ako vrijedi:*

(i) $(R, +)$ je Abelova grupa,

(ii) $(R, \cdot)$ je polugrupa (to jest operacija $\cdot$ je asocijativna),

(iii) distributivnost operacije $\cdot$ obzirom na operaciju $+$:

$$a(b + c) = ab + ac, \quad (a + b)c = ac + bc, \quad \text{za sve } a, b, c \in R.$$

Neutralni element grupe $(R, +)$ naziva se **nula** i označava s 0.
Ako postoji neutralni element strukture $(R, \cdot)$ onda se on naziva **jedinica** i označava s 1, a $(R, +, \cdot)$ se tada naziva **prsten s jedinicom**.
Ako je operacija. komutativna, onda govorimo o **komutativnom prstenu**. Naša konvencija u slučaju komutativnih prstena je da je $1 \neq 0$.

Primjer 1.1.17. $(\mathbb{Z}, +, \cdot)$ *je komutativni prsten s jedinicom.*

Definicija 1.1.18. *Komutativni prsten s jedinicom* $(R, +, \cdot)$ *u kojem je svaki element* $x \in R\backslash\{0\}$ *invertibilan naziva se* ***polje****.*

Polje možemo definirati i na drugi način.

Definicija 1.1.19. $(\mathbb{F}, +, \cdot)$ *je polje ako su* $(\mathbb{F}, +)$ *i* $(\mathbb{F}, \cdot)$ *grupoidi takvi da vrijedi:*

(i) $(\mathbb{F}, +)$ *je Abelova grupa,*

(ii) $(\mathbb{F}^*, \cdot)$ *je Abelova grupa* $(\mathbb{F}^* = \mathbb{F}\backslash\{0\})$*,*

(iii) distributivnost operacije $\cdot$ *s obzirom na operaciju* $+$*.*

Primjer 1.1.20. $(\mathbb{Q}, +, \cdot)$ *,*$(\mathbb{R}, +, \cdot)$ *i* $(\mathbb{C}, +, \cdot)$ *su polja.*

1.2 Polinomi

U ovom dijelu A je komutativni prsten (s $1 \neq 0$).

Definicija 1.2.1. *Izraz oblika*

$$p(X) := a_0 + a_1 X + \ldots + a_i X^i + \ldots + a_k X^k, \quad k \in \mathbb{N}_0, \quad a_i \in A$$

zove se ***polinom*** *u* X*.*

Drugi način zapisa polinoma je u obliku

$$p(X) = \sum_i a_i X^i$$

s tim da se onda podrazumijeva da je gornja suma zapravo konačna; tj., da sumacija "ide" od $i = 0$ *do nekog* $k \geq 0$*.*

Skup svih polinoma nad prstenom A, tj. polinoma sa koeficijentima iz prstena A, označava se sa $A[X]$.

Ovdje X nazivamo **varijablom**, a X^i je tzv. i -ta potencija od X.

Elementi a_i zovu se **koeficijenti** polinoma $p(X)$. Kažemo da je a_i i-ti koeficijent.

Koeficijent a_0 zove se **slobodni koeficijent**, a a_k se zove **vodeći koeficijent**. Kada govorimo o vodećem koeficijentu, mi zapravo pretpostavljamo da je $a_k \neq 0$.

Posebno definiramo nul-polinom kao

$$0 = 0 + 0X + 0X^2 + \cdots$$

Drugim riječima, nul-polinom je polinom koji je konstanta, i to baš konstanta $0 = 0_A$.

Navedimo sada neke od najvažnijih teorema vezane uz polinome.

Teorem 1.2.2. *(Teorem o nul-polinomu) Polinom $p(x) = a_0 + a_1X + \ldots + a_{n-1}X^{n-1} + a_nX^n$ je nul polinom ako i samo ako su svi koeficijenti $a_i = 0$, za sve $i = 0, 1, \ldots, n$.*

Teorem 1.2.3. *(Teorem o jednakosti dvaju polinoma) Polinomi f i g definirani s:*

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$$
$$g(X) = b_mX^m + b_{m-1}X^{m-1} + \ldots + b_1X + b_0,$$

su jednaki ako i samo ako je $m = n$ i $a_i = b_i$, za sve $i = 0, 1, \ldots, n$.

Za polinom $p(X) = a_0 + a_1X + \ldots + a_iX^i + \ldots + a_kX^k$, kojemu je vodeći koeficijent $a_k \neq 0$, definiramo **stupanj** polinoma $p(X)$ kao

$$\deg p(X) := k$$

pa govorimo da je $p(X)$ polinom stupnja k.

Dogovorno se uzima da je stupanj nul-polinoma jednak -1 ili se pak uopće ne definira.

Za polinome $p_1(X) = \sum_i a_i X^i$ i $p_2(X) = \sum_i b_i X^i$ standardno se definira **zbroj polinoma**:

$$p_1(X) + p_2(X) := \sum_i (a_i + b_i) X^i$$

tj., polinome zbrajamo tako da im "zbrojimo koeficijente uz iste potencije".

Isto tako, za polinome $p_1(X)$ i $p_2(X)$ kao gore, definira se **produkt polinoma**:

$$p_1(X) \cdot p_2(X) = p_1(X)p_2(X) := \sum_i c_i X^i$$

gdje su koeficijenti c_i dobiveni "konvolucijskim množenjem", tj., dani su kao $c_0 := a_0 b_0$, $c_1 := a_0 b_1 + a_1 b_0$, i općenito

$$c_i := a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0$$

Sada kada smo na skupu $A[X]$ definirali operacije zbrajanja i množenja polinoma, lako je provjeriti da $(A[X], +, \cdot)$ ima strukturu komutativnog prstena s jedinicom. Kraće pišemo $A[X]$ umjesto $(A[X], +, \cdot)$. Kažemo da je $A[X]$ prsten polinoma u X s koeficijentima iz A. Nula u tom prstenu je nul-polinom, a jedinica je konstanta $1 = 1_A$.

Sasvim analogno, definiraju se polinomi u više varijabli.

Definicija 1.2.4. *Izraz oblika*

$$p(X_1, \ldots, X_n) := \sum_{(i_1,\ldots,i_n)\in\mathbb{N}_0^n} a_{i_1\cdots i_n} X_1^{i_1} \cdots X_n^{i_n} \quad a_{i_1\cdots i_n} \in A$$

zove se ***polinom u varijablama*** $X_1, \ldots, X_n$.
Opet se podrazumijeva da je gornja suma konačna.

I ovdje se $a_{i_1\cdots i_n}$ -ovi zovu **koeficijenti**. Oznaka za skup svih polinoma nad A u varijablama X_i je

$$A[X_1, \ldots, X_n]$$

Stupanj polinoma više varijabli definiramo na sljedeći način. Za $p = p(X_1, \ldots, X_n)$, kao gore, stavimo

$$\deg p := \max\{i_1 + \cdots + i_n \mid a_{i_1\cdots i_n} \neq 0\}$$

tj., ako za monom

$$a_{i_1\cdots i_n} X_1^{i_1} \cdots X_n^{i_n}$$

definiramo njegov stupanj kao zbroj $i_1 + \cdots + i_n$ svih potencija od varijabli $X_1, \ldots, X_n$, onda je stupanj polinoma p jednak najvećem stupnju njegovih monoma.

Na skupu $A[X_1, \ldots, X_n]$ definiraju se operacije zbrajanja i množenja polinoma analogno kao i za polinome u jednoj varijabli. Naime, za polinom $p(X_1, \ldots, X_n)$ kao gore, i neki $q(X_1, \ldots, X_n)$ sa koeficijentima $b_{i_1\cdots i_n}$, imamo zbroj

$$p(X_1, \ldots, X_n) + q(X_1, \ldots, X_n) = \sum_{(i_1,\ldots,i_n)} \left(a_{i_1\cdots i_n} + b_{i_1\cdots i_n}\right) X_1^{i_1} \cdots X_n^{i_n}$$

Isto tako, produkt polinoma p i q dobivamo tako da svaki monom od p pomnožimo sa svakim monomom od q, i onda dobiveno sredimo tako da "pokupimo" sve koeficijente koji stoje uz neki konkretan produkt varijabli $X_1^{k_1} \cdots X_n^{k_n}$. Monome množimo po pravilu

$$\left(a_{i_1\cdots i_n} X_1^{i_1} \cdots X_n^{i_n}\right)\left(b_{j_1\cdots j_n} X_1^{j_1} \cdots X_n^{j_n}\right) := \left(a_{i_1\cdots i_n} b_{j_1\cdots j_n}\right) X_1^{i_1+j_1} \cdots X_n^{i_n+j_n}$$

Kao i za $A[X]$, imamo da i $A[X_1, \ldots, X_n]$, uz definirane operacije zbrajanja i množenja polinoma, ima strukturu komutativnog prstena s jedinicom. Kažemo da je $A[X_1, \ldots, X_n]$ prsten polinoma u $X_1, \ldots, X_n$ sa koeficijentima iz A.
Nula u tom prstenu je ponovo nul-polinom, tj. nula $0 = 0_A$ u A, a jedinica je konstanta $1 = 1_A$

Primijetimo da se prsten polinoma $A[X_1, \ldots, X_n]$, u n varijabli, zapravo može shvatiti kao

$$A[X_1, \ldots, X_n] \equiv A[X_1, \ldots, X_{n-1}][X_n]$$

tj., kao prsten u varijabli X_n s koeficijentima iz prstena polinoma u prvih $n-1$ varijabli. Tu zapravo mi "sredimo svaki polinom u varijablama X_i po potencijama od X_n".

Definicija 1.2.5. *Razmatrajući polinom $f \in A[X_1, \ldots, X_n]$ kao polinom u varijabli X_n s koeficijentima iz prstena $A[X_1, \ldots, X_n]$, tj. $f \in A[X_1, \ldots, X_{n-1}][X_n]$, možemo definirati* ***stupanj od*** *f* ***po varijabli*** *X_n koristeći raniju definiciju. Taj stupanj je općenito manji od stupnja od f.*

Zapravo, sasvim analogno imamo

$$A[X_1, \ldots, X_n] \equiv A[X_{u_1}, \ldots, X_{u_k}][X_{v_1}, \ldots, X_{v_m}]$$

gdje je $k + m = n, 1 \leq u_1 < \cdots < u_k \leq n, 1 \leq v_1 < \cdots < v_m \leq n$ i imamo disjunktnu uniju

$$\{u_1, \ldots, u_k\} \cup \{v_1, \ldots, v_m\} = \{1, 2, \ldots, n\}$$

tj., načinimo particiju skupa $\{1, 2, \ldots, n\}$ na u_i -ove i v_j -ove, a zatim svaki polinom iz $A[X_1, \ldots, X_n]$ sređujemo po potencijama od $X_{v_1}, \ldots, X_{v_m}$

Napomena 1.2.6. *Primijetimo da za proizvoljan A, u prstenu polinoma $A[X_1, \ldots, X_n]$ vrijedi sljedeće za stupnjeve: Ako su $p_1 = p_1(X_1, \ldots, X_n)$ i $p_2 = p_2(X_1, \ldots, X_n)$ ne-nul polinomi, onda je*

$$\deg(p_1 + p_2) \leq \max\{\deg p_1, \deg p_2\}$$
$$\deg(p_1 p_2) \leq \deg p_1 + \deg p_2$$

i posebno ćemo za stupanj produkta imati jednakost, ako je A integralna domena (prsten bez djelitelja nule).

Nadalje, za kompoziciju polinoma

$$(p_2 \circ p_1)(X) := p_2(p_1(X))$$

gdje su $p_1, p_2 \in A[X]$ polinomi u jednoj varijabli, imamo za stupanj kompozicije

$$\deg(p_2 \circ p_1) \leq (\deg p_1)(\deg p_2)$$

Ponovo, za slučaj da je A integralna domena, imamo jednakost.

Definicija 1.2.7. *Za polinom $f(X)$ kažemo da je **djeljiv** polinomom $g(X) \neq 0$ ako postoji polinom $h(X)$, stupnja većeg od nule, takav da je $f(X) = g(X) \cdot h(X)$.*

Teorem 1.2.8. *(Teorem o dijeljenju s ostatkom) Neka su $f(X)$ i $g(X)$ iz $A[X]$ polinomi, različiti od nul-polinoma, i pretpostavimo da je vodeći koeficijent u polinomu $g(X)$ iz $A^\times$, grupe invertibilnih elemenata u A. Tada postoje, i jedinstveni su, polinomi $q(X)$ i $r(X)$ iz $A[X]$ takvi da je*

$$f(X) = g(X)q(X) + r(X) \quad \& \quad \deg r(X) < \deg g(X)$$

Dokaz. (Egzistencija) Dokaz ćemo provesti indukcijom po stupnju polinoma kojeg dijelimo, tj. polinoma $f(X)$. Najprije zapišimo polinome:

$$f(X) = a_0 + a_1X + \cdots + a_nX^n, \quad g(X) = b_0 + b_1X + \cdots + b_mX^m$$

pri čemu je $a_n \neq 0$ i $b_m \in A^\times$.

Pogledajmo bazu indukcije, tj. $n = 0$. Imamo dvije mogućnosti:

(1) $\deg g(X) = 0$. Sada je $g(X) = b_0 \in A^\times$, pa onda uzmemo za r i q polinome konstante $r(X) := 0$ i $q(X) := b_0^{-1}a_0$

(2) $\deg g(X) > 0$.Sada uzmemo $r(X) := f(X)$ i $q(X) := 0$, nul-polinom.

Sada prelazimo na korak indukcije. Pretpostavimo da teorem vrijedi za sve polinome $f(X)$ stupnja $< n$, pa pokažimo da onda vrijedi i za sve polinome stupnja $= n$. Bez smanjenja općenitosti, pretpostavimo da je

$$\deg g(X) = m \leq n = \deg f(X)$$

Naime, ukoliko je $\deg g(X) > \deg f(X)$, onda uzmemo $q(X) := 0$ i $r(X) := f(X)$.

Zatim, definirajmo "pomoćni" polinom $f_1(X)$:

$$f_1(X) := f(X) - a_nb_m^{-1}X^{n-m}g(X)$$

Tu koristimo činjenicu da je vodeći koeficijent b_m od $g(X)$ invertibilan u A. Primijetimo da je zapravo $f_1(X) = (a_nX^n +$ niže potencije od $f) - \big(a_nb_m^{-1}X^{n-m}\,(b_mX^m +$ niže potencije od $g))$ pa se gore član a_nX^n "pokrati". Slijedi da je

$$\deg f_1(X) < \deg f(X) = n$$

Primjenom pretpostavke indukcije, sada na polinom $f_1(X)$, dobivamo da postoje neki polinomi $\widetilde{q}(X)$ i $r(X)$ takvi da je

$$f_1(X) = \widetilde{q}(X)g(X) + r(X) \quad \& \quad \deg r(X) < \deg g(X)$$

No, onda slijedi da je

$$f(X) = q(X)g(X) + r(X)$$

gdje polinom $q(X)$ definiramo kao

$$q(X) := a_n b_m^{-1} X^{n-m} + \tilde{q}(X)$$

Time je egzistencija rastava dokazana.

(Jedinstvenost) Pretpostavimo da imamo neke $q_i(X)$ i $r_i(X)$, za $i = 1, 2$, takve da je

$$q_1(X)g(X) + r_1(X) = f(X) = q_2(X)g(X) + r_2(X)$$

$$\deg r_i(X) < \deg g(X), \text{za} i = 1, 2.$$

Onda slijedi

$$(q_1(X) - q_2(X))\, g(X) = r_2(X) - r_1(X)$$

Tvrdimo da odavde slijedi da je $q_1(X) - q_2(X) = 0$, a onda imamo i $r_2(X) - r_1(X) = 0$. Naime, kad bi bilo $q_1(X) - q_2(X) \neq 0$, onda bismo imali

$$\deg\left((q_1(X) - q_2(X))\, g(X)\right) \geq m = \deg g(X)$$

Tu ponovo koristimo činjenicu da je vodeći koeficijent b_m od $g(X)$ invertibilan u A, pa posebno on nije djelitelj nule. Ali kako isto tako imamo da je

$$\deg\left(r_2(X) - r_1(X)\right) < m = \deg g(X)$$

dolazimo do kontradikcije. Tako je teorem u potpunosti dokazan. □

Definicija 1.2.9. *Polinom $h(X)$ naziva se **zajednička mjera** ili **zajednički djelitelj** $f(X)$ i $g(X)$ ako su i f i g djeljivi njime.*

Definicija 1.2.10. *Za zajedničku mjeru h polinoma f i g kažemo da je **najveća zajednička mjera** od f i g ako je h djeljiv sa svakom zajedničkom mjerom od f i g. Oznaka za najveću zajedničku mjeru je $M(f, g)$.*

Definicija 1.2.11. *Ako je za polinome $f(X)$ i $g(X)$ najveća zajednička mjera jednaka* 1*, onda kažemo da su oni* ***relativno prosti*** *polinomi.*

Neka je $A = \mathbb{C}$ u idućoj definiciji.

Definicija 1.2.12. *Nultočka polinoma $f \in \mathbb{C}[X]$ je svaki kompleksni broj α takav da je $f(\alpha) = 0$.*

Teorem 1.2.13. *(Bezaut) Kompleksan broj α je nultočka polinoma f ako i samo ako je f djeljiv linearnim polinomom $g(X) = X - \alpha$.*

Definicija 1.2.14. *Polje K je* ***algebarski zatvoreno*** *ako svaki polinom $f \in K[X]$ stupnja ≥ 1 ima nultočku u K, tj. postoji $\lambda \in K$ takva da je $f(\lambda) = 0$.*

Definicija 1.2.15. *Neka je K algebarski zatvoreno polje. Ako je polinom $f \in K[X]$ djeljiv polinomom $g(X) = (X - \alpha)^k$, $k \in \mathbb{N}$, $\alpha \in K$, a nije djeljiv polinomom $h(X) = (X - \alpha)^{k+1}$, onda kažemo da je $X = \alpha$* ***k-struka nultočka*** *polinoma f ili da je kratnost (višestrukost) nultočke $X = \alpha$ jednaka k.*

Iz kompleksne analize znamo:

Teorem 1.2.16. *(Osnovni teorem algebre) Svaki polinom $p \in \mathbb{C}[X]$, stupnja $n \geq 1$ ima barem jednu nultočku u skupu kompleksnih brojeva.*

Teorem 1.2.17. *Neka je K algebarski zatvoreno polje. Neka je $f(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$, $f(x) \in K[X]$, $a_i \in K$, $a_n \neq 0$, $n \geq 1$. Tada postoje $\lambda_1, \ldots, \lambda_n \in K$ t.d. $f(x) = a_n(X - \lambda_1)(X - \lambda_2)\ldots(X - \lambda_n)$.*

Dokaz. Teorem ćemo dokazati matematičkom indukcijom po stupnju n.
Kod baze indukcije imamo da je $n = 1$. Tada je

$$f(x) = a_1 X + a_0$$

To možemo zapisati i kao

$$f(x) = a_1 \left(X - \left(-\frac{a_0}{a_1} \right) \right)$$

Stavimo da je $\lambda = -\left(\frac{a_0}{a_1}\right)$ i tvrdnja vrijedi.
Po definiciji algebarski zatvorenog polja, postoji $\lambda \in K$ t.d. je $f(\lambda) = 0$. Iz toga slijedi

$$\lambda - X_1 \mid f(X)$$

u $K[X]$. Dakle, postoji $g \in K[X]$ nužno stupnja $n-1$ tako da

$$f(X) = (X - \lambda_1)g(X)$$

Uočimo da je vodeći koeficijent od g jednak vodećem koeficijentu od f, tj. jednak a_n. To se vidi množenjem polinoma u relaciji $f(X) = (X - \lambda_1)g(X)$. Sada primijenimo induktivnu pretpostavku. Postoje $\lambda_2, \ldots, \lambda_n \in K$ tako da

$$g(x) = a_n(X - \lambda_2)\ldots(X - \lambda_n)$$

odakle slijedi

$$f(X) = (X - \lambda_1)g(X) = a_n(X - \lambda_1)\ldots(X - \lambda_n)$$

□

Posebno, iz kompleksne analize znamo da je $K = \mathbb{C}$ algebarski zatvoreno, te navodimo, bez dokaza, sljedeći teorem.

Teorem 1.2.18. *Neka je $K = \mathbb{C}$ i f polinom iz $\mathbb{C}[X]$ stupnja ≥ 1 s vodećim koeficijentom $n = f_0$. Tada postoje $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ t.d. $f(X) = a_n(X - \lambda_1)(X - \lambda_2)\ldots(X - \lambda_n)$.*

1.3 Vektorski prostori

Sada ćemo definirati vektorske prostore i najvažnije pojmove vezane uz njih.

Definicija 1.3.1. *Neka je $(V, +)$ Abelova grupa, a K polje. Ako je zadano preslikavanje $\cdot : K \times V \to V$ koje zadovoljava sljedeća svojstva:*

(1) $\alpha \cdot (\beta \cdot a) = (\alpha\beta) \cdot a$, za sve $\alpha, \beta \in K, a \in V$ (kvaziasocijativnost),

(2) $(\alpha + \beta) \cdot a = \alpha \cdot a + \beta \cdot a$, za sve $\alpha, \beta \in K, a \in V$ (distributivnost operacije $\cdot$ u odnosu na zbrajanje u K),

(3) $\alpha \cdot (a + b) = \alpha \cdot a + \alpha \cdot b$, za sve $\alpha \in K, a, b \in V$ (distributivnost operacije $\cdot$ u odnosu na zbrajanje u V),

(4) $1 \cdot a = a$, za sve $a \in V$,

*tada se uređena trojka $(V, +, \cdot)$ naziva **vektorski prostor** nad poljem K.*

Elemente skupa V zovemo **vektorima**, a elemente polja K **skalarima**.

Neutralni element (nulu) Abelove grupe $(V, +)$ zovemo **nulvektor** i označavamo ga s 0_V.

Operaciju $\cdot$ nazivamo **množenje vektora skalarom** i umjesto $\alpha \cdot a$ često pišemo αa.

Skup koji se sastoji samo od nulvektora, $\{0_V\}$ također je vektorski prostor, a nazivamo ga **trivijalni prostor**.

Definicija 1.3.2. *Neka je V vektorski prostor nad poljem K, te $k \in \mathbb{N}$. Za $\alpha_1, \ldots, \alpha_k \in K$ i $a_1, \ldots, a_k \in V$ vektor oblika*

$$\alpha_1 a_1 + \cdots + \alpha_k a_k$$

*nazivamo **linearna kombinacija** vektora $a_1, \ldots, a_k$ s koeficijentima $\alpha_1, \ldots, \alpha_k$.*
Kraće zapisujemo kao $\sum_{i=1}^{k} \alpha_i a_i$.

Definicija 1.3.3. *Neka je $S \subseteq V$, $S \neq \emptyset$. Skup svih linearnih kombinacija vektora iz S naziva se **linearna ljuska** ili **linearni omotač** skupa S i označava s $[S]$.*

Dakle,

$$[S] = \{\alpha_1 a_1 + \cdots + \alpha_n a_n : n \in \mathbb{N}, a_1, \ldots, a_n \in S, \alpha_1, \ldots, \alpha_n \in \mathbb{F}\}$$

Ako je $S = \{a_1, \ldots, a_k\}$, onda je

$$[S] = [\{a_1, \ldots, a_k\}] = \{\alpha_1 a_1 + \cdots + \alpha_k a_k : \alpha_1, \ldots, \alpha_k \in \mathbb{F}\}$$

te skup $[\{a_1, \ldots, a_k\}]$ (u oznaci i $[a_1, \ldots, a_k]$) nazivamo linearnom ljuskom ili linearnim omotačem vektora $a_1, \ldots, a_k$.

Za prazan skup definira se njegova linearna ljuska kao $[\emptyset] = \{0_V\}$.

Definicija 1.3.4. *Neka je V vektorski prostor nad poljem $\mathbb{F}$ i $G \subseteq V$. Ako je $V = [G]$, odnosno ako se svaki vektor iz V može prikazati kao linearna kombinacija (konačno mnogo) vektora iz G, onda kažemo da je G **sustav izvodnica** ili **generatora** za prostor V, odnosno skup izvodnica ili generatora za V.*
*Još se može reći da skup G **razapinje** ili **generira** prostor V.*

Ako je $V = [G]$, onda za svaki $x \in V$ postoje vektori $a_1, \ldots, a_k \in G$ i skalari $\alpha_1, \ldots \alpha_k \in \mathbb{F}$ takvi da se x prikazuje kao

$$x = \alpha_1 a_1 + \cdots + \alpha_k a_k = \sum_{i=1}^{k} \alpha_i a_i$$

Prikaz vektora x u obliku linearne kombinacije nekih vektora iz skupa S općenito nije jednoznačan, to jest, pojedini vektor općenito se može na više načina prikazati kao linearna kombinacija vektora iz nekog sustava izvodnica.

Definicija 1.3.5. *Vektorski prostor je **konačno generiran** ako sadrži bar jedan konačan sustav izvodnica.*

Prisjetimo se, skup vektora na pravcu nazivamo V^1, u ravnini V^2 i u prostoru V^3.

Primjer 1.3.6. *Neka su $\vec{a}$ i $\vec{b}$ u V^2 nekolinearni vektori. Iz analitičke geometrije znamo da za svaki $\vec{c} \in V^2$ postoje (jedinstveni) skalari $\alpha, \beta \in \mathbb{R}$ takvi da je $\vec{c} = \alpha\vec{a} + \beta\vec{b}$. Dakle, možemo zaključiti da skup koji se sastoji od bilo koja dva nekolinearna vektora predstavlja sustav izvodnica za V^2.*

Primjer 1.3.7. *Analogno, skup od bilo koja tri nekomplanarna vektora predstavlja sustav izvodnica za V^3.*

Primjer 1.3.8. *Primjer vektorskog prostora koji **nije** konačnogeneriran je prostor polinoma.*

Neka je $\{p_0, p_1, \ldots, p_n\} \subset \mathcal{P}_n$ pri čemu je $p_i(X) = X^i$ za $i = 0, 1, \ldots, n$. Kako je za $p \in \mathcal{P}_n$

$$p(X) = \sum_{i=0}^{n} a_i X^i = \sum_{i=0}^{n} a_i p_i(X), \forall x \in \mathbb{R}$$

to jest $p = \sum_{i=0}^{n} a_i p_i$, slijedi da je $\{p_0 \ldots, p_n\}$ sustav izvodnica za $\mathcal{P}_n$. Skup $\{p_0, p_1, p_2, \ldots\} \subset \mathcal{P}$ razapinje vektorski prostor $\mathcal{P}$. Uočimo da je $\{p_0, p_1, p_2, \ldots\}$ beskonačan skup. Uz to, možemo zaključiti da ne postoji konačan skup polinoma koji razapinje prostor $\mathcal{P}$. Naime, u konačnom skupu polinoma postoji jedan ili više polinoma s najvećim stupnjem u tom skupu, recimo stupnjem m. Linearnim kombinacijama polinoma iz tog skupa ne može se dobiti polinom stupnja većeg od m pa taj skup očito ne može generirati čitav prostor $\mathcal{P}$.

Definicija 1.3.9. *Neka je V vektorski prostor nad poljem K i neka je* $S = \{a_1, \ldots, a_k\}$ *njegov podskup. Kažemo da je S* ***linearno nezavisan*** *skup vektora ako se nulvektor* 0_V *može na jedinstven način prikazati pomoću vektora iz S , to jest ako iz*

$$\alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_k a_k = 0_V$$

slijedi da je $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$

U suprotnom, to jest ako postoji izbor skalara $\alpha_1, \ldots, \alpha_k$ *takav da je bar jedan skalar* $\alpha_i \neq 0$ *i da vrijedi navedena jednakost, onda kažemo da je skup S* ***linearno zavisan****.*

Primjer 1.3.10. *Neka su* $\vec{a}, \vec{b}$ *u* V^2 *(ili u* V^3 *) nekolinearni. Onda je skup* $\{\vec{a}, \vec{b}\}$ *linearno nezavisan.*

Primjer 1.3.11. *Neka su* $\vec{a}, \vec{b}, \vec{c}$ *u* V^3 *nekomplanarni. Onda je skup* $\{\vec{a}, \vec{b}, \vec{c}\}$ *linearno nezavisan.*

Primjer 1.3.12. *Skup* $\{p_0, p_1, \ldots, p_n\}$ *je linearno nezavisan u prostoru polinoma. Zaista, iz*

$$\sum_{i=0}^{n} \alpha_i p_i = 0_{\mathcal{P}}$$

pri čemu smo s $0_{\mathcal{P}}$ *označili nul-polinom, slijedi da je*

$$\sum_{i=0}^{n} \alpha_i p_i(X) = 0$$

za sve $X \in \mathbb{R}$*, a to je jedino moguće za* $\alpha_0 = \cdots = \alpha_n = 0$ *(Teorem o nul-polinomu).*

Definicija 1.3.13. *Podskup B vektorskog prostora V je* ***baza*** *prostora V ako je B sustav izvodnica za V i linearno nezavisan skup u V.*

Primjer 1.3.14. *Neka su* $\vec{a}$ *i* $\vec{b}$ *nekolinearni vektori u* V^2*. Skup* $\{\vec{a}, \vec{b}\}$ *je baza za* V^2*.*

Primjer 1.3.15. *Neka su* $\vec{a}$ *,* $\vec{b}$ *i* $\vec{c}$ *nekomplanarni vektori u* V^3*. Skup* $\{\vec{a}, \vec{b}, \vec{c}\}$ *je baza za* V^3*.*

Primjer 1.3.16. *Skup* $\{p_0, p_1, \ldots, p_n\}$ *je baza za* $\mathcal{P}_n$*.*

Teorem 1.3.17. *Neka je $B = \{b_1, \ldots, b_n\}$ baza vektorskog prostora V. Tada za svaki $a \in V$ postoje jedinstveni skalari $\beta_1, \ldots, \beta_n$ takvi da je $a = \beta_1 b_1 + \cdots + \beta_n b_n$. Vrijedi i obrat. Ako se svaki vektor iz V jedinstveno prikazuje kao linearna kombinacija vektora iz B, onda je B baza za V.*

Definicija 1.3.18. *Vektorski prostor koji ima konačnu bazu naziva se **konačno dimenzionalnim**. Trivijalan prostor $V = \{0_V\}$ smatra se konačnodimenzionalnim. Netrivijalni vektorski prostor koji nema konačnu bazu je **beskonačno dimenzionalan**.*

Teorem 1.3.19. *(Steinitz). Svake dvije baze netrivijalnog konačno generiranog vektorskog prostora su jednakobrojne (ekvipotentne).*

Na temelju prethodnog teorema možemo definirati dimenziju vektorskog prostora.

Definicija 1.3.20. *Neka je V konačnodimenzionalan vektorski prostor i $V \neq \{0_V\}$. Broj vektora u bilo kojoj bazi prostora V naziva se **dimenzija** vektorskog prostora V i označava s* $\dim V$. *Ako je* $\dim V = n$, *onda kažemo da je V n-dimenzionalan vektorski prostor.*

Za $V = \{0_V\}$ stavljamo da je $\dim V = 0$

Primjer 1.3.21. $\dim V^1 = 1$, $\dim V^2 = 2$, $\dim V^3 = 3$

Primjer 1.3.22. $\dim \mathbb{R}^n = n$, *gdje je* $\mathbb{R}^n = \{(x_1, \ldots, x_n) \mid x \in \mathbb{R}\}$

Primjer 1.3.23. $\dim \mathcal{P}_n = n + 1$

Poglavlje 2

Teorija eliminacije varijable

2.1 Faktorijalne domene

Neka je $(D, +, \cdot)$ komutativan prsten s jedinicom $1 \neq 0$, primjerice polje.

Definicija 2.1.1. *Za $a, b \in D$ kažemo da a **dijeli** b i pišemo $a \mid b$ ako postoji $c \in D$ t.d. $b = ac$.*

Definicija 2.1.2. *Element $a \in D$ naziva se **lijevi djelitelj nule** ako postoji $b \in D, b \neq 0$, takav da je $ab = 0$. Analogno se definira i **desni djelitelj nule**. Ako je a lijevi i desni djelitelj nule, onda se a naziva **djelitelj nule**.*

Definicija 2.1.3. *D je **integralna domena** ako $ab = 0$, $a, b \in D$ povlači $a = 0$ ili $b = 0$.*

Primijetimo da je D integralna domena ako i samo ako je $0 \in D$ jedini djelitelj nule u D.

Primjer 2.1.4. *$(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$ i $(\mathbb{C}, +, \cdot)$ su integralne domene.*

Definicija 2.1.5. ***Jedinica** (ili **invertibilni element**) prstena D je element $\varepsilon \in D$ za koji postoji $\eta \in D$ tako da vrijedi $\varepsilon\eta = 1$.*

Skup svih jedinica, odnosno invertibilnih elemenata u D označavat ćemo s $D^\times$.
$D^\times = \{\varepsilon \in D : \varepsilon$ jedinica u $D\}$ je multiplikativna grupa.

Primjer 2.1.6. *U $(\mathbb{Z}, +, \cdot)$ invertibilni elementi su -1 i 1.*

Primjer 2.1.7. *U* $(\mathbb{Q}, +, \cdot)$ *invertibilni elementi su svi osim nule.*

Propozicija 2.1.8. *Neka je K polje. Stavimo* $D = K[X_1, \ldots, X_n]$. *Tada je* $D^\times = K\backslash\{0\}$.

Dokaz. Neka je $\varepsilon \in D^\times$. Želimo dokazati da je $\varepsilon \in K\backslash\{0\}$, tj. da $\varepsilon \neq 0$. Budući da je $\varepsilon \in D^\times$, onda iz definicije slijedi da postoji postoji polinom $\eta \in D$ tako da vrijedi $1 = \varepsilon \cdot \eta$. Uspoređujući stupnjeve imamo:

$$0 = \deg(1) = \deg(\varepsilon \cdot \eta) = \deg(\varepsilon) + \deg(\eta)$$

odakle slijedi

$$\deg(\varepsilon) = -\deg(\eta)$$

Budući da stupanj općenito jedino može biti nula ili prirodan broj, uočimo da stoga mora vrijediti:

$$\deg(\varepsilon) = \deg(\eta) = 0$$

Iz toga zaključujemo da je ε konstantni polinom, različit od nule. □

Definicija 2.1.9. *Kažemo da su* $a, b \in D$, $a, b \neq 0$ ***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 $a \mid b$ i $b \mid a$.

Primjer 2.1.10. *U* $(\mathbb{Z}, +, \cdot)$ *jedinice su* ± 1 *pa je elementu* $a \in \mathbb{Z}$ *asocirani element* $\pm a$.

Propozicija 2.1.11. *Neka je K polje i* $D = K[X_1, \ldots, X_n]$. *Polinomi* $a, b \in D\backslash\{0\}$ *su asocirani ako i samo ako postoji konstanta* ε *iz K različita od nule tako da vrijedi* $b = \varepsilon \cdot a$, *tj. razlikuju se do na umnožak konstantom iz K različitom od nule.*

Dokaz. U prethodnoj propoziciji dokazano je da su prstenu polinoma invertibilni elementi ne-nul konstante pa tvrdnja odmah slijedi. □

Definicija 2.1.12. *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 $c \in D^\times$.*

Odnosno, element je ireducibilan ako je ne-nul neinvertibilan element koji se ne može zapisati kao produkt dva neinvertibilna elementa. Ako $a \in D$ nije ireducibilan, kažemo da je **reducibilan**.

Propozicija 2.1.13. *Neka je K polje i $D = K[X_1, \ldots, X_n]$. Tada vrijedi:*

(i) Svaki polinom stupnja 1 iz D je ireducibilan.

(ii) Neka je $n \geq 2$ i $h \in K[x_1, \ldots, X_{n-1}]$ bilo koji polinom. Tada je $X_n - h$ ireducibilan u D.

(iii) Ako je K algebarski zatvoreno i $n = l$, onda su ireducibilni elementi u $K[X]$, $X = X_1$ upravo svi polinomi stupnja 1, tj. $a(x - b)$, $a \in K\backslash\{0\}$, $b \in K$.

Dokaz. (i) Neka je $a \in D$ polinom stupnja 1. Moramo dokazati da je ireducibilan. Koristimo definiciju ireducibilnosti. Najprije, a nije nul polinom i nije konstanta, tj. nije iz $D^\times = K\backslash\{0\}$. Ako vrijedi $a = b \cdot c$, za neke polinome $b, c \in D$, onda uspoređujući stupnjeve slijedi:

$$1 = \deg(a) = \deg(b \cdot c) = \deg(b) + \deg(c)$$

odakle mora biti

$$\deg(b) = 0 \quad \text{ili} \quad \deg(b) = 0$$

To znači da je $b \in K\backslash\{0\} = D^\times$ ili $c \in K\backslash\{0\} = D^\times$. Ovime je (i) dokazano.

(ii) Neka je $a = X_n - h$. Želimo dokazati da je ireducibilan. Očito $a \notin K$ nije konstanta jer h ne ovisi o X_n. Dakle, $a \notin D^\times$ i $a \neq 0$. Sada trebamo dokazati da ako vrijedi $a = b \cdot b$ za neke polinome b i $c \in D$, da je $b \in D^\times$ ili $c \in D^\times$, tj. da je ili b ili c konstantni ne-nul polinom.

Uspoređujući stupnjeve u varijabli X_n nalazimo da je ili b stupnja nula u X_n ili c stupnja nula u X_n (jer je a stupnja 1 u X_n). Argument je sličan onom iz i).

Neka je b stupnja nula u X_n. To znači da je $b \in K[X_1, \ldots, X_{n-1}]$. Tada je c stupnja 1 u X_n te izgleda ovako:

$$c = h_1 \cdot X_n + h_2, \quad h_1, h_2 \in K[X_1, \ldots, X_{n-1}]$$

Na kraju, imamo:

$$X_n - h = a = b \cdot c = b(h_1 \cdot X_n + h_2) = (b \cdot h_1)X_n + (b \cdot h_2)$$

Važno je napomenuti $b \cdot h_1, b \cdot h_2 \in K[X_1, \ldots, X_n]$, a gornja relacija iz teorema o jednakosti polinoma daje:

$$b \cdot h_1 = 1$$

Uspoređujući koeficijente uz X_n slično kao u propoziciji 2.1.8. imamo:

$$0 = \deg(1) = \deg(b) + \deg(h_1)$$

iz čega slijedi $b \in K\backslash\{0\} = D^\times$. Ovim je ii) dokazano.

iii) Slijedi odmah iz i) koristeći Bezoutov teorem i teorem 1.1.36. □

Definicija 2.1.14. *Integralna domena D naziva se **faktorijalna domena** ako:*

(i) $\forall a \in D, a \neq 0, a \notin D^\times$*, postoje ireducibilni elementi* $a_1, \ldots, a_k \in D$ *t.d.je* $a = a_1 \ldots a_n$.

(ii) (jedinstvenost zapisa) Ako je također $a = b_1 \ldots b_l$*, za ireducibilne elemente* $b_1, \ldots, b_l$*, onda je* $k = l$ *te postoji permutacija* $\pi \in S_k$ *i* $\varepsilon_1, \ldots, \varepsilon_k \in D^\times$ *t.d. je* $b_i = \varepsilon_i a_{\pi(i)}, \forall i \in \{1, \ldots, k\}$.

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 $= \{\pm 2, \pm 3, \pm 5, \ldots\}$. Obično uzimamo IRR $(D) = \{2, 3, 5, \ldots\}$). Sada $\forall a \in D, 0 \neq a \notin D^\times$, postoje jedinstveni $a_1, \ldots, a_k \in \text{IRR}(D)$ $m_1, \ldots, m_k \in \mathbb{N} i \varepsilon \in D^\times$ t.d. je $a = \varepsilon a_1^{m_1} \ldots a_k^{m_k}$

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 2.1.15. *Ako je D faktorijalna domena, onda je i* $D[X]$ *faktorijalna domena.*

Teorem nećemo dokazivati, ali navodimo leme koje su bitne za njegovo dokazivanje.

Lema 2.1.16. *Neka su $a \in D$ i $f \in D[X]$ takvi da $a \mid f$ u $D[X]$. Tada a dijeli svaki koeficijent od f u D.*

Lema 2.1.17. *Neka su $a, b, c \in D$, a ireducibilan takvi da $a \mid bc$. Tada $a \mid b$ ili $a \mid c$ u D,*

Lema 2.1.18. *Neka je $d \in D$ ireducibilan i $f, g \in D[X]$. Ako $d \mid fg$, onda $d \mid f$ ili $d \mid g$.*

Lema 2.1.19. *Neka je K polje razlomaka od D i $f \in D[X]$ ireducibilan nekonstantan polinom. Tada je $f \in K[X]$ ireducibilan.*

Lema 2.1.20. *(egzistencija NZM polinoma u $K[X]$) Ako su f i g ne-nul polinomi iz $K[X]$, onda postoji polinom $h \in K[X]$ sa svojstvima:*

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

(ii) Za svaki $k \in K[X]$ 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 $A, B \in K[X]$ takvi da je $Af + Bg = h$.

Lema 2.1.21. *Neka je K polje, f, g, $h \in K[X]$ i f ireducibilan. Ako $f \mid gh$, onda $f \mid g$ ili $f \mid h$.*

Lema 2.1.22. *Neka je D faktorijalna domena, $f, g, h \in D[X]$, f ireducibilan i $f \mid gh$ u $D[X]$. Tada $f \mid g$ ili $f \mid h$ u $D[X]$.*

Korolar 2.1.23. *Ako je D faktorijalna domena, onda je i $D[X_1, \ldots, X_n]$ faktorijalna domena.*

Korolar 2.1.24. *Ako je K polje, onda je $K[X_1, \ldots, X_n]$ faktorijalna domena.*

2.2 Teorija eliminacije varijable

Sada ćemo iskazati i dokazati osnovni teorem o eliminaciji varijable.

Teorem 2.2.1. *Neka je* $f = a_0 + a_1 \cdot X + \ldots + a_n \cdot X^n, a_i \in D, a_n \neq 0, n \geq 1$ *i* $g = b_0 + b_1 \cdot X + \ldots + b_m \cdot X^m, b_i \in D, b_m \neq 0, m \geq 1$. *Tada vrijedi:*

(i) f *i* g *imaju zajednički nekonstantni faktor ako i samo ako postoje* $F, G \in D[X], F, G \neq 0$ *tako da vrijedi* $\deg(F) \leq m-1$, $\deg(G) \leq n-1$ *i* $F \cdot f + G \cdot g = 0$ *(relacija u* $D[X]$*).*

(ii) f *i* g *imaju zajednički nekonstantni faktor ako i samo ako rezultanta* $\mathrm{Res}(f,g) \in D$ *iščezava, tj.* $\mathrm{Res}(f,g) = 0$.

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

Primjer 2.2.2. $n = 3, m = 2$

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

Dokaz. (i)$\Longrightarrow$ Neka je h zajednički nekonstantni faktor od f i g. tj. neka je h takav da $\deg(h) > 0$, $h \mid f$ i $h \mid g$ u $D[X]$. Iz toga slijedi da postoje $k, l \in D[X]$ tako da $f = h \cdot k$ i $g = h \cdot l$. Množenjem f sa l i g sa $-k$ te zbrajanjem jednakosti dobijemo:

$$l \cdot f - k \cdot g = 0$$

Zatim, iz $f = h \cdot k$ uspoređivanjem stupnjeva slijedi:

$$n = \deg(f) = \deg(h) + \deg(k) \geq 1 + \deg(k) \Longrightarrow \deg(k) \leq n - 1$$

Slično, iz $g = h \cdot l$ imamo $\deg(l) \leq m - 1$. Sada uzmemo $F = l$ i $G = -k$ i tvrdnja vrijedi.

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

$$F \cdot f = -G \cdot g$$

slijedi da svaki ireducibilni faktor l od g koji ovisi o X mora dijeliti $F \cdot f$ pa Lema 2.1.22. i pretpostavka povlače da l dijeli F. Rastavimo f na ireducibilne faktore:

$$g = \lambda g_1^{n_1} \cdot \ldots \cdot g_r^{n_r}$$

gdje su g_i ireducibilni faktori od g koji ovise o X, a λ produkt svih ireducilbilnih faktora koji ne ovise o X.
Dakle, rastavom na ireducibilne faktore svakog od F, f, G i g u jednakosti $F \cdot f = -G \cdot g$ slijedi:

$$g_1^{n_1} \cdot \ldots \cdot g_r^{n_r} \mid F$$

u $D[X]$. Uspoređujući stupnjeve nalazimo:

$$\deg(g) = \deg(\lambda) + \deg(g_1^{n_1} \cdot \ldots \cdot g_r^{n_r}) = \deg(g_1^{n_1} \cdot \ldots \cdot g_r^{n_r}) \leq \deg(F)$$

Međutim, iz pretpostavke teorema imamo:

$$\deg(F) \leq m - 1 = \deg(g) - 1$$

što je kontradikcija.

(ii) Neka f i g imaju zajednički nekonstantni faktor. Tada, prema (i) vrijedi relacija:

$$F \cdot f + G \cdot g = 0$$

gdje su

$$F = \alpha_0 + \alpha_1 X + \ldots + \alpha_{m-1} X^{m-1}$$

i

$$G = \beta_0 + \beta_1 X + \ldots + \beta_{n-1} X^{n-1}, \quad \alpha_i, \beta_j \in D \text{ nepoznati}$$

Tada uvrštavanjem slijedi:

$$\begin{aligned} &\left(\alpha_0 + \alpha_1 X + \ldots + \alpha_{m-1} X^{m-1}\right) \cdot (a_0 + a_1 X + \ldots + a_n X^n) + \\ &\left(\beta_0 + \beta_1 X + \ldots + \beta_{n-1} X^{n-1}\right)(b_0 + b_1 X + \ldots + b_m X^m) = 0 \end{aligned}$$

uz uvjet da barem jedan $\alpha_i \neq 0$ ili $\beta_j \neq 0$.

Iz polinomijalne jednakosti slijedi:

$$\alpha_i = 0 \text{ za svaki } i \Leftrightarrow \beta_j = 0 \text{ za svaki } j \tag{2.1}$$

Sada izjednačavamo koeficijente uz:

$$\begin{aligned} &X^0 : a_0\alpha_0 + b_0\beta_0 = 0 \\ &X^1 : a_1\alpha_0 + a_0\alpha_1 + b_0\beta_1 + b_1\beta_0 = 0 \\ &\vdots \\ &X^{m+n-1} : a_n\alpha_{m-1} + b_m\beta_{n-1} = 0 \end{aligned}$$

Prema teoriji homogenih sustava jednadžbi, ovo je homogeni $(m+n) \times (m+n)$ sustav u varijablama $(\alpha_0, \ldots, \alpha_{m-1}, \beta_0, \ldots, \beta_{n-1})$. Zbog (2.1) postoji rješenje različito od $(0, \ldots, 0)$. Dakle, determinanta sustava koja je $\mathrm{Res}(f, g)^\top$ je jednaka 0 što dokazuje tvrdnju. □

Primjer 2.2.3. $m = 2, n = 3$

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

Izjednačavanjem koeficijenata dobijemo:

$$\begin{aligned}
X^0 &: a_0\alpha_0 + b_0\beta_0 = 0 \\
X^1 &: a_1\alpha_0 + a_0\alpha_1 + b_0\beta_1 + b_1\beta_0 = 0 \\
X^2 &: a_2\alpha_0 + a_1\alpha_1 + b_2\beta_0 + b_1\beta_1 + b_0\beta_2 = 0 \\
X^3 &: a_3\alpha_0 + a_2\alpha_1 + b_1\beta_2 + b_2\beta_1 = 0 \\
X^4 &: a_3\alpha_1 + b_2\beta_2 = 0
\end{aligned}$$

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

Neka je K polje. Gledamo prsten polinoma u r varijabli, $r \geq 1$. $K[X_1, \ldots, X_r] = K[X_1, \ldots, X_{r-1}][X_r]$, gdje je $K[X_1, \ldots, X_{r-1}]$ faktorijalna domena, nazovimo ju D. $f, g \in K[X_1, \ldots, T_r]$ ovise o X_r (tj. pozitivnog su stupnja u X_r), $f, g \in D[X_r]$ ovise o X_r

1. teorem iz ovog poglavlja tada nam daje sljedeću propoziciju:

Propozicija 2.2.4. *f, g imaju zajednički ireducibilni faktor u $K[X_1, \ldots, X_r]$ koji ovisi o X_r ako i samo ako* $\mathrm{Res}_{X_r}(f, g) = 0$ *(nul-polinom u $K[X_1, \ldots, X_{r-1}]$) gdje je $f = a_0 + a_1 X + \ldots + a_n X^n$, $a_i \in D = K[X_1, \ldots, X_{r-1}]$, $a_n \neq 0$, $n \geq 1$ i $g = b_0 + b_1 X + \ldots + b_m X^m$, $b_i \in D = K[X_1, \ldots, X_{r-1}]$, $b_m \neq 0$, $m \geq 1$.*

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

je očito polinom iz $K[X_1, \ldots, T_{r-1}]$.

Sada ćemo se baviti geometrijskom primjenom. Ukoliko uzmemo

$$(\alpha_1, \ldots, \alpha_{r-1}) \in K^r$$

i napravimo parcijalnu evaluaciju:

$$f(\alpha_1, \ldots, \alpha_{r-1}, X_r) = \sum_{i=0}^{n} a_i(\alpha_1, \ldots, \alpha_{r-1}) X_r^i$$

$$g(\alpha_1, \ldots, \alpha_{r-1}, X_r) = \sum_{i=0}^{m} b_i(\alpha_1, \ldots, \alpha_{r-1}) X_r^i$$

dobili smo polinome iz $K[X_r]$. Uočimo da je stupanj polinoma $f(\alpha_1, \ldots, \alpha_{r-1}, X_r)$ jednak n ako i samo ako $a_n(\alpha_1, \ldots, \alpha_{r-1}) \neq 0$, a stupanj polinoma $g(\alpha_1, \ldots, \alpha_{r-1}, X_r)$ jednak m ako i samo ako $b_m(\alpha_1, \ldots, \alpha_{r-1}) \neq 0$. Dakle, ako izaberemo $(\alpha_1, \ldots, \alpha_{r-1}) \in K^{r-1}$ tako da se polinom $a_n \cdot b_m \in K[X_1, \ldots, X_{r-1}]$ ne poništava u toj točki, onda smo osigurali da su stupnjevi baš takvi. To nije uvijek moguće ako polje K ima konačno elemenata, ali ako K ima beskonačno elemenata to slijedi iz iduće leme koju navodimo bez dokaza.

Lema 2.2.5. *Neka je K polje sa beskonačno elemenata. Onda za svaki $F \in K[X_1, \ldots, X_r], F \neq 0$ postoji $(\alpha_1, \ldots, \alpha_r) \in K^r$ tako da je $F(\alpha_1, \ldots, \alpha_r) \neq 0$*

Posebno, algebarski zatvoreno polje zadovoljava prethodnu lemu zbog idućeg rezultata.

Lema 2.2.6. *K je algebarski zatvoreno polje* $\Longrightarrow$ *K ima beskonačno elemenata. (K je algebarski zatvoreno ako za* $\forall f \in K[X]$ *stupnja* $\geq 1 \exists \lambda \in K$ *tako da* $f(\lambda) = 0$. *)*

Kada vrijedi

$$a_n(\alpha_1, \ldots, \alpha_{r-1}) \cdot b_m(\alpha_1, \ldots, \alpha_{r-1}) \neq 0$$

onda $f(\alpha_1, \ldots, \alpha_{r-1}, X_r)$ i $g(\alpha_1, \ldots, \alpha_{r-1}, X_r)$ ovise o X_r te možemo izračunati rezultantu

$$\mathrm{Res}_{X_r}(f(\alpha_1, \ldots, \alpha_{r-1}, X_r), g(\alpha_1, \ldots, \alpha_{r-1}, X_r)) \in K$$

Nadalje, ta rezultanta jednaka je evaulaciji polinoma

$$\mathrm{Res}_{X_r}(f, g)(\alpha_1, \ldots, \alpha_{r-1}, X_r) \in K[X_1, \ldots, X_{r-1}]$$

u točki $(\alpha_1, \ldots, \alpha_{r-1})$

Teorem 2.2.7. *Neka je K algebarski zatvoreno polje i neka su* $f, g \in K[X_1, \ldots, X_r]$, *g ireducibilan. Ako vrijedi*

$$(\forall (\alpha_1, \ldots, \alpha_r) \in K^r)\, g(\alpha_1, \ldots, \alpha_r) = 0 \Longrightarrow f(\alpha_1, \ldots, \alpha_r) = 0 \qquad (\star)$$

onda $g \mid f$ *u* $K[X_1, \ldots, X_r]$.

Dokaz. Budući da je g ireducibilan, onda nije konstantan, tj. ovisi o nekoj od varijabla $X_1, \ldots, X_r$. Bez smanjenja općenitosti uzmimo da ovisi o X_r.
Sada imamo dva slučaja:

(i) f ne ovisi o X_r

(ii) f ovisi o X_r

Razmotrimo najprije slučaj (i). Budući da g ovisi o X_r, možemo ga napisati kao prije:

$$g = \sum_{i=0}^{m} b_i X_r^i, \quad b_i \in K[X_1, \ldots, X_{r-1}],\ b_m \neq 0,\ m \geq 1$$

Kako $f \in K[X_1, \ldots, X_{r-1}]$, tada imamo

$$f \cdot b_i \in K[X_1, \ldots, X_{r-1}]$$

te imamo prikaz od $f \cdot g$ po varijabli X_r:

$$f \cdot g = \sum_{i=0}^{m} (f \cdot b_i) X_r^i$$

Ako je f nul-polinom, onda tvrdnja teorema vrijedi, tj. $g \mid f$. Ako f nije nul-polinom, onda niti $f \cdot b_m$ nije nul-polinom u $K[X_1, \ldots, X_{r-1}]$. Kako je K algebarski zatvoreno, onda postoji $\alpha_1, \ldots, \alpha_{r-1} \in K^{r-1}$ tako da

$$f(\alpha_1, \ldots, \alpha_{r-1}) \cdot b_m(\alpha_1, \ldots, \alpha_{r-1}) \neq 0$$

Posebno, nalazimo

$$f(\alpha_1, \ldots, \alpha_{r-1}) \neq 0 \tag{$\triangle$}$$

$$g(\alpha_1, \ldots, \alpha_{r-1}, X_r) \in K[X_r] \quad \text{polinom stupnja} \quad m \geq 1 \tag{$\triangle\triangle$}$$

Kako je $g(\alpha_1, \ldots, \alpha_{r-1}$ stupnja $m \geq 1$ i K algebarski zatvoreno, tada slijedi da postoji $\alpha_r \in K$ tako da $g(\alpha_1, \ldots, \alpha_{r-1}, \alpha_r) = 0$, tj. $g(\alpha_1, \ldots, \alpha_{r-1}, X_r)$ ima nultočku u K.

Sada primijenimo ($\star$). Imamo:

$$g(\alpha_1, \ldots, \alpha_{r-1}, \alpha_r) = 0$$

Zatim, budući da f ne ovisi o X_r i primjenjujući ($\triangle$) slijedi:

$$f(\alpha_1, \ldots, \alpha_{r-1}, \alpha_r) = f(\alpha_1, \ldots, \alpha_{r-1}) \neq 0$$

To je kontradikcija s ($\star$) jer $g(\alpha_1, \ldots, \alpha_r) = 0 \Longrightarrow f(\alpha_1, \ldots, \alpha_r = 0)$, što ne vrijedi.

Razmotrimo slučaj ii). Tada f ovisi o X_r te možemo izračunati $\mathrm{Res}_{X_r}(f, g) \in K[X_1, \ldots, X_{r-1}]$. Nadalje, prema Teoremu 3.14 iz skripte ([3]). postoje polinomi $A, B \in K[X_1, \ldots, X_r]$ tako da

$$A \cdot f + B \cdot g = \mathrm{Res}_{X_r}(f, g)$$

Sada koristeći ($\star$), nalazimo da vrijedi

$$g(\alpha_1, \ldots, \alpha_r) = 0 \Longrightarrow \mathrm{Res}_{X_r}(f, g)(\alpha_1, \ldots, \alpha_r) = \mathrm{Res}_{X_r}(f, g)(\alpha_1, \ldots, \alpha_{r-1}) = 0$$

Dakle, ($\star$) vrijedi kada se f zamijeni s $\mathrm{Res}_{X_r}(f, g)$ koji ne ovisi o X_r. Tada argument iz dijela i) povlači da je $\mathrm{Res}_{X_r}(f, g)$ nul-polinom u $K[X_1, \ldots, X_{r-1}]$. Sada prema glavnom teoremu f i g imaju zajednički ireducibilan faktor u $K[X_1, \ldots, X_r]$. Međutim, f je ireducibilan pa je upravo zajednički ireducibilan faktor, tj $g \mid f$. □

Ovaj teorem generalizira idući teorem iz Uvoda u matematiku. Ako je $r = 1$, onda kako je K algebarski zatvoreno, g do na umnožak konstantom jednak je $g = X - \alpha$, za neki $\alpha \in K$. Sada ($\star$) glasi $f(\alpha) = 0$ jer je α jedina nultočka od g. Zaključak teorema je $X - \alpha \mid f$. Drugim riječima,

$$f(\alpha) = 0 \Longrightarrow X - \alpha \mid f$$

Definirajmo sada hiperplohu.

Definicija 2.2.8. *U prostoru K^r definiramo **hiperplohu** kao skup*

$$Z(g) = \{(\alpha_1, \ldots, \alpha_r) \in K^r \mid g(\alpha_1, \ldots, \alpha_r) = 0\}$$

*gdje je $g \in K[X_1, \ldots, X_r]$ polinom koji nije konstantan. Ako je $r = 2$ hiperplohu nazivamo **ravninska krivulja**.*

Hiperploha je ireducibilna ukoliko je $g \in K[X_1, \ldots, X_r]$ ireducibilan polinom.

Korolar 2.2.9. *Ireducibilna hiperploha određuje svoju jednadžbu jedinstveno do na umnožak konstantom iz K različitom od nule.*

Dokaz. Ako ireducibilna hiperploha ima dvije ireducibilne jednadžbe g_1 i g_2, tj. $Z(g_1) = Z(g_2)$, onda imamo

$$g_1(\alpha_1, \ldots, \alpha_r) = 0 \Longrightarrow (\alpha_1, \ldots, \alpha_r) \in Z(g_1) = Z(g_2)$$

iz čega slijedi

$$g_2(\alpha_1, \ldots, \alpha_r) = 0$$

Dakle, prema teoremu 2.2.7 vrijedi $g_1 \mid g_2$. Kako su g_1, g_2 ireducibilni, vrijedi $g_2 = \lambda g_1$, za neki $\lambda \in K\backslash\{0\}$. □

Bibliografija

[1] D. Cox, J. Little, D. O'Shea, *Ideals, varieties and algorithms: an introduction to computational algebraic geometry and commutative algebra.* Springer-Verlag, New York, 1992.

[2] Z. Franušić, J. Šiftar, *Linearna algebra 1*, skripta, dostupno na `https://web.math.pmf.unizg.hr/fran/predavanja-LA1.pdf` (rujan, 2021.)

[3] G. Muić, *Algebarske krivulje*, skripta, dostupno na `https://www.pmf.unizg.hr/_download/repository/Algebarske_krivulje_ispravljeno.pdf` (rujan, 2021.)

[4] B. Širola, *Algebarske strukture*, skripta, dostupno na `https://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf` (rujan, 2021.)

Sažetak

U ovome radu, najprije smo definirali osnovne algebarske strukture, grupe, prstene i polja. Zatim smo definirali polinome, operacije nad njima te naveli nekoliko glavnih teorema. Definirali smo i vektorski prostor te najvažnije pojmove vezane uz njega. U drugom poglavlju bavili smo se faktorijalnom domenom te na kraju iskazali i dokazali dva glavna teorema vezana uz eliminaciju varijable.

Summary

In this thesis, we have first defined the fundamental algebraic structures, groups, rings and fields. Then, we have defined polynomials, operations on them and mentioned some of the main theorems. We have also defined the vector space and the most important terms related to it. In the second chapter, we have studied the factorial domain and in the end we have stated and proved two main theorems related to the elimination of variable.

Životopis

Rođena sam 13. travnja 1996. godine u Zagrebu. Svoje obrazovanje započela sam 2003. godine u Osnovnoj školi Petra Preradovića u Zagrebu te ga nastavila u Klasičnoj gimnaziji. Maturirala sam 2015. godine te upisala Preddiplomski sveučilišni studij Matematike na Prirodoslovno-matematičkom fakultetu u Zagrebu. Sljedeće godine prebacila sam se na nastavnički smjer matematike, na istom fakultetu. 2019. godine završila sam Preddiplomski sveučilišni studij te upisala Diplomski sveučilišni studij Matematika; smjer: nastavnički. Stručnu praksu obavljala sam u Osnovnoj školi Marina Držića te XV. gimnaziji u Zagrebu.

Uz studiranje, radila sam u Photomath-u kao kreator matematičkog sadržaja te držala instrukcije iz matematike učenicima osnovnih i srednjih škola.

Osim matematike, volim i glazbu te sam pohađala Glazbenu školu Pavla Markovca u Zagrebu, smjer: kontrabas, a također sviram i klavir i gitaru.