Algebra

Ivan Prokić

Fakultet tehničkih nauka, Novi Sad

Predavanje 15

Na prethodnom času

- Svodljivost i nesvodljivost
- Osnovni stav algebre i faktorizacija nad $\mathbb{C}$, $\mathbb{R}$ i $\mathbb{Q}$
- Vijetove formule

Konstrukcije konačnih polja

Ostaci pri deljenju. Kongruencije

U domenu integriteta $(\mathbb{Z}, +, \cdot)$:

- Delimo brojem n i posmatramo ostatke
- Relacija $\equiv_n$ je relacija ekvivalencije
- Faktor skup $\mathbb{Z}/\equiv_n$, tj. $\mathbb{Z}_n$, ima n elemenata
- $\equiv_n$ je kongrunecija u odnosu na $+$ i $\cdot$
- Faktor prsten $(\mathbb{Z}/\equiv_n, +, \cdot)$ je polje akko je n prost broj

U domenu integriteta $(F[t], +, \cdot)$:

- Delimo polinomom P i posmatramo ostatke
- Relacija $\equiv_P$ je relacija ekvivalencije?
- Faktor skup $F[t]/\equiv_P$, tj. $F[t]/P$, ima koliko elemenata?
- $\equiv_P$ je kongrunecija u odnosu na $+$ i $\cdot$?
- Faktor prsten $(F[t]/\equiv_P, +, \cdot)$ je polje akko je P nesvodljiv polinom?

Nas zapravo interesuje slučaj kada je $F = \mathbb{Z}_p$

Za faktor skup $F[t]/\equiv_P$ pisaćemo i $F[t]/P$

Faktor skup $F[t]/P$ ima koliko elemenata?

Podsećanje: Ostatak pri deljenju sa n može biti samo broj iz skupa $\{0, 1, \ldots, n-1\}$. Zato $\mathbb{Z}/\equiv_n$, tj. $\mathbb{Z}_n$, ima n elemenata.

- Kao što smo rekli, nas zanima $\mathbb{Z}_p[t]/P$, gde je p prost prirodan broj i $P \in \mathbb{Z}_p[t]$
- Ako $\equiv_P$ jeste kongruencija na $\mathbb{Z}_p[t]$ (što ćemo pokazati kasnije), pitanje je: šta sve može biti ostatak pri deljenju sa P?
- Kada proizvoljan polinom $T \in \mathbb{Z}_p[t]$ podelimo da P, znamo da imamo jedinstvene $Q, R \in \mathbb{Z}_p[t]$ takve da je $T = QP + R$, pri čemu je $R = 0$ ili $dg(R) < dg(P)$
- Ako je $dg(P) = n$ tada imamo da je ostatak R oblika $R = a_{n-1}t^{n-1} + \ldots + a_1 t + a_0$, gde su koeficijenti $a_{n-1}, \ldots, a_1, a_0$ iz skupa $\mathbb{Z}_p$
- Dakle, skup svih ostataka deljenju sa P stepena n jeste

$$\mathbb{Z}_p[t]/P = \{a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \mid a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}_p\}$$

- Pošto $\mathbb{Z}_p$ ima p elemenata, imamo da koeficijent a_i u skupu gore uzima p različitih vrednosti, pa skup ostataka $\mathbb{Z}_p[t]/P$ ima p^n elemenata (setimo se broja elemenata polja).

Primeri

$$\mathbb{Z}_p[t]/P = \{a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \mid a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}_p\}$$

- Na skupu polinoma $\mathbb{Z}_2[t]$ ostaci pri deljenju sa $t^2 + t + 1$ su polinomi oblika $at + b$, pa imamo 2^2 elemenata

$$\mathbb{Z}_2[t]/_{(t^2+t+1)} = \{0, 1, t, t+1\}$$

- Na skupu polinoma $\mathbb{Z}_3[t]$ ostaci pri deljenju sa $t^2 + 1$ su polinomi oblika $at + b$, pa imamo 3^2 elemenata

$$\mathbb{Z}_3[t]/_{(t^2+1)} = \{0, 1, 2, t, 2t, t+1, t+2, 2t+1, 2t+2\}$$

Relacija $\equiv_P$ jeste kongruencija na $F[t]$

Podsećanje: Relacija $q \equiv_n s \Leftrightarrow n \mid q - s$ jeste kongruencija na $\mathbb{Z}$ u odnosu na $+$ i $\cdot$

Teorema

Neka je $P \neq 0$ i $\equiv_P$ binarna relacija skupa svih polinoma $F[t]$ definisana sa za sve $Q, S \in F[t]$ važi $Q \equiv_P S$ akko $P \mid Q - S$. Tada je $\equiv_P$ kongurencija u odnosu na sabiranje i množenje polinoma nad F.

Dokaz

- **Relacija ekvivalencije na $F[t]$:**
  - **Refleksivnost:** *Imamo $Q \equiv_P Q$ akko $P \mid Q - Q$, što je tačno.*
  - **Simetričnost:** *Ako je $Q \equiv_P S$ tada $P \mid Q - S$, odakle sledi $P \mid S - Q$, tj. $S \equiv_P Q$.*
  - **Tranzitivnost:** *Ako je $Q \equiv_P S$ i $S \equiv_P R$, tada $P \mid Q - S$ i $P \mid S - R$, odakle sledi $P \mid (Q - S + S - R)$, tj. $Q \equiv_P R$.*
- *Ako je $Q \equiv_p S$ i $R \equiv_P T$, tada iz $P \mid Q - S$ i $P \mid R - T$*
  - **Kongruencija u odnosu na $+$:** *sledi $P \mid (Q + R - (S + T))$, tj. $Q + R \equiv_P S + T$.*
  - **Kongruencija u odnosu na $\cdot$:** *sledi $P \mid (QR - SR)$ i $P \mid (SR - ST)$, tj. $P \mid (QR - SR + (SR - ST))$, tj. $QR \equiv_P ST$.*

Sabiranje i množenje polinoma po modulu P

Napomena: Kao što smo kod celih brojeva za klasu broja x u odnosu na relaciju $\equiv_n$ pisali C_x (ili $[x]$), tako ćemo i ovde za klasu polinoma Q u odnosu na relaciju $\equiv_P$ pisati C_Q (ili $[Q]$).

Definicija

Na skupu $F[t]/\equiv_P$ *definišemo operacije* $+$ *i* $\cdot$ *sa: za sve* $Q, R \in F[t]$

$$C_Q + C_R = C_{Q+R} \qquad i \qquad C_Q \cdot C_R = C_{QR}$$

Primer

Na skupu $\mathbb{Z}_2[t]/_{(t^2+t+1)} = \{0, 1, t, t+1\}$ *operacije* $+$ *i* $\cdot$ *su*

$+$	0	1	t	$t+1$
0	0	1	t	$t+1$
1	1	0	$t+1$	t
t	t	$t+1$	0	1
$t+1$	$t+1$	t	1	0

$\cdot$	0	1	t	$t+1$
0	0	0	0	0
1	0	1	t	$t+1$
t	0	t	$t+1$	1
$t+1$	0	$t+1$	1	t

Komutativan prsten sa jedinicom

Podsećanje: $(\mathbb{Z}_n, +, \cdot)$ je komutativan prsten sa jedinicom.

Teorema

Struktura $(F[t]/P, +, \cdot)$ *jeste komutativan prsten sa jedinicom.*

Dokaz

- $(F[t]/P, +)$ *je Abelova grupa:*
  - **Zatvorenost:** *Operacija je dobro definisana (pogledati teoremu o faktor grupoidu)*
  - **Asocijativnost:** *Sledi iz asocijativnosti sabiranja polinoma, tj.* $(C_Q + C_R) + C_S = C_{Q+R} + C_S = C_{(Q+R)+S} = C_{Q+(R+S)} = C_Q + C_{R+S} = C_Q + (C_R + C_S)$
  - **Komutativnost:** *Sledi iz komutativnosti sabiranja polinoma jer je* $C_{Q+R} = C_{R+Q}$
  - **Neutralni element:** C_0
  - **Inverzni elementi:** *Za* C_P *inverzni je* C_{-P}*, tj. koeficijenti od* $-P$ *su inverzni elementi od koeficijenata polinoma* P *u grupi* $(F, +)$
- $(F[t]/P, \cdot)$ *je komutativan monoid:*
  - **Zatvorenost, Asocijativnost, Komutativnost:** *Slično kao za operaciju* $+$
  - **Neutralni element:** *je* C_1
- **Distributivnost** $\cdot$ **prema** $+$**:** *Sledi iz distributivnosti* $\cdot$ *prema* $+$ *u* $(F[t], +, \cdot)$

Polje $F[t]/P$

Podsećanje: $(\mathbb{Z}_n, +, \cdot)$ je polje akko je n prost broj.

Teorema

Neka je F konačno polje. Struktura $(F[t]/P, +, \cdot)$ jeste polje ako je P nesvodljiv polinom nad poljem F.

Dokaz

Pošto $(F[t]/P, +, \cdot)$ jeste komutativan prsten sa jedinicom i F je konačan skup, preostaje samo da dokažemo da u $(F[t]/P, +, \cdot)$ nema delitelja nule (jer je svaki konačan domen integriteta polje). Neka je $C_Q C_R = C_0$. Odavde sledi da $P \mid QR$, a pošto je P nesvodljiv sledi da $P \mid Q$ ili $P \mid R$ (pogledaj dokaz da je $\mathbb{Z}_p$ polje). Sada imamo $C_Q = C_0$ ili $C_R = C_0$, tj. nemamo delioce nule.

Napomena

Prethodna teorema važi i za beskonačna polja F.

Kako konstrusati polje od p^n elemenata?

Rešenje: Nad poljem $\mathbb{Z}_p$ naći nesvodljiv polinom P stepena n. Tada je $(\mathbb{Z}_p[t]/P, +, \cdot)$ polje sa p^n elemenata, gde su $+$ i $\cdot$ sabiranje i množenje polinoma po modulu P.

Primer

Polje od 4 elementa je $(\mathbb{Z}_2[t]/_{(t^2+t+1)}, +, \cdot)$.

Primer

Zaokruži broj ispred polja $(\mathbb{Z}_p[t]/P, +, \cdot)$*:*

1. $(\mathbb{Z}_2[t]/_{(t+1)}, +, \cdot)$
2. $(\mathbb{Z}_3[t]/_{(t^2+1)}, +, \cdot)$
3. $(\mathbb{Z}_3[t]/_{(t^2+t+1)}, +, \cdot)$
4. $(\mathbb{Z}_5[t]/_{(t^2+1)}, +, \cdot)$

Kako konstrusati polje od p^n elemenata?

Rešenje: Nad poljem $\mathbb{Z}_p$ naći nesvodljiv polinom P stepena n. Tada je $(\mathbb{Z}_p[t]/P, +, \cdot)$ polje sa p^n elemenata, gde su $+$ i $\cdot$ sabiranje i množenje polinoma po modulu P.

Primer

Polje od 4 elementa je $(\mathbb{Z}_2[t]/_{(t^2+t+1)}, +, \cdot)$.

Primer

Zaokruži broj ispred polja $(\mathbb{Z}_p[t]/P, +, \cdot)$*:*

1. $(\mathbb{Z}_2[t]/_{(t+1)}, +, \cdot)$ *(polinom* $t+1$ *je nesvodljiv nad poljem* $\mathbb{Z}_2$*)*
2. $(\mathbb{Z}_3[t]/_{(t^2+1)}, +, \cdot)$
3. $(\mathbb{Z}_3[t]/_{(t^2+t+1)}, +, \cdot)$
4. $(\mathbb{Z}_5[t]/_{(t^2+1)}, +, \cdot)$

Kako konstrusati polje od p^n elemenata?

Rešenje: Nad poljem $\mathbb{Z}_p$ naći nesvodljiv polinom P stepena n. Tada je $(\mathbb{Z}_p[t]/P, +, \cdot)$ polje sa p^n elemenata, gde su $+$ i $\cdot$ sabiranje i množenje polinoma po modulu P.

Primer

Polje od 4 elementa je $(\mathbb{Z}_2[t]/_{(t^2+t+1)}, +, \cdot)$.

Primer

Zaokruži broj ispred polja $(\mathbb{Z}_p[t]/P, +, \cdot)$*:*

1. $(\mathbb{Z}_2[t]/_{(t+1)}, +, \cdot)$ *(polinom* $t+1$ *je nesvodljiv nad poljem* $\mathbb{Z}_2$*)*
2. $(\mathbb{Z}_3[t]/_{(t^2+1)}, +, \cdot)$ *(polinom* t^2+1 *je nesvodljiv nad poljem* $\mathbb{Z}_3$*)*
3. $(\mathbb{Z}_3[t]/_{(t^2+t+1)}, +, \cdot)$
4. $(\mathbb{Z}_5[t]/_{(t^2+1)}, +, \cdot)$

Kako konstrusati polje od p^n elemenata?

Rešenje: Nad poljem $\mathbb{Z}_p$ naći nesvodljiv polinom P stepena n. Tada je $(\mathbb{Z}_p[t]/P, +, \cdot)$ polje sa p^n elemenata, gde su $+$ i $\cdot$ sabiranje i množenje polinoma po modulu P.

Primer

Polje od 4 elementa je $(\mathbb{Z}_2[t]/_{(t^2+t+1)}, +, \cdot)$.

Primer

Zaokruži broj ispred polja $(\mathbb{Z}_p[t]/P, +, \cdot)$*:*

1. $(\mathbb{Z}_2[t]/_{(t+1)}, +, \cdot)$ *(polinom* $t+1$ *je nesvodljiv nad poljem* $\mathbb{Z}_2$*)*
2. $(\mathbb{Z}_3[t]/_{(t^2+1)}, +, \cdot)$ *(polinom* t^2+1 *je nesvodljiv nad poljem* $\mathbb{Z}_3$*)*
3. $(\mathbb{Z}_3[t]/_{(t^2+t+1)}, +, \cdot)$ *(*$P(1) = 0$ *u polju* $\mathbb{Z}_3$*)*
4. $(\mathbb{Z}_5[t]/_{(t^2+1)}, +, \cdot)$

Kako konstrusati polje od p^n elemenata?

Rešenje: Nad poljem $\mathbb{Z}_p$ naći nesvodljiv polinom P stepena n. Tada je $(\mathbb{Z}_p[t]/P, +, \cdot)$ polje sa p^n elemenata, gde su $+$ i $\cdot$ sabiranje i množenje polinoma po modulu P.

Primer

Polje od 4 elementa je $(\mathbb{Z}_2[t]/_{(t^2+t+1)}, +, \cdot)$.

Primer

Zaokruži broj ispred polja $(\mathbb{Z}_p[t]/P, +, \cdot)$*:*

1. $(\mathbb{Z}_2[t]/_{(t+1)}, +, \cdot)$ *(polinom* $t+1$ *je nesvodljiv nad poljem* $\mathbb{Z}_2$*)*
2. $(\mathbb{Z}_3[t]/_{(t^2+1)}, +, \cdot)$ *(polinom* t^2+1 *je nesvodljiv nad poljem* $\mathbb{Z}_3$*)*
3. $(\mathbb{Z}_3[t]/_{(t^2+t+1)}, +, \cdot)$ *(*$P(1)=0$ *u polju* $\mathbb{Z}_3$*)*
4. $(\mathbb{Z}_5[t]/_{(t^2+1)}, +, \cdot)$ *(*$P(2)=0$ *u polju* $\mathbb{Z}_5$*)*

Šta smo danas radili

- Relacija $\equiv_P$ na skupu $F[t]$
- Faktor skup $F[t]/P$
- Komutativan prsten sa jedinicom $(F[t]/P, +, \cdot)$
- Polje $(F[t]/P, +, \cdot)$, ako je polinom P nesvodljiv nad F
- Sva konačna polja su:
  - $(\mathbb{Z}_p, +, \cdot)$ ako je p prost ceo broj - ima p elemenata
  - $(\mathbb{Z}_p[t]/P, +, \cdot)$, ako je polinom P nesvodljiv nad poljem $\mathbb{Z}_p$ - ima p^n elemenata, za $dg(P) = n$