Konačna polja

Kriste, Iva

Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odsjek

Iva Kriste

Konačna polja

Diplomski rad

Voditelj rada:
prof.dr.sc. Vedran Krčadinac

Zagreb, veljača 2017.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____ .

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

1 Uvod **1**

2 Algebarske osnove **2**

3 Prsteni polinoma **9**

4 Egzistencija i jedinstvenost konačnih polja **18**

5 Wedderburnov teorem **24**

Sažetak **29**

Summary **30**

Životopis **31**

1 Uvod

U ovom radu osnovni cilj bit će pokazati kako konstruirati i kakva je struktrura konačnih polja. Iz knjige "Konačna polja", R. Lidla i H. Niederreitera, kao i uz pomoć drugih knjiga navedenih u literaturi iskazani su i dokazani teoremi i leme potrebni za dokaz dva osnovana teorema cijelog rada. Prvi, teorem 4.21 kaže da za svaki prost broj p i za svaki prirodni broj n postoji konačno polje od p^n elemenata i ono je jedinstveno. Drugi je Wedderburnov teorem 5.10 koji kaže da je svako konačno tijelo polje.

U prvom poglavlju iznesene su osnovne definicije i svojstva vezana za prstene i polja kao jedne od osnovnih algebarskih struktura. U drugom poglavlju opisana je konstrukcija konačnih polja, dok su u trećem dokazana gore navedena dva teorema (teorem o postojanju i jedinstvenosti konačnih polja i Wedderburnov teorem). Budući da je za dokaz egzistencije i jedinstvenosti konačnih polja potrebno promatrati prstene polinoma nad konačnim poljima, jedan dio radnje je posvećen i tome, kao i definiciji ciklotomskih polinoma koji su potrebni za dokaz Wedderburnova teorema.

2 Algebarske osnove

Algebra je jedna od fundamentalnih grana matematike. U ovom poglavlju definirat ćemo neke od osnovnih *algebarskih struktura*. Pored grupa (koje ćemo uzeti kao poznate), prsteni su druge osnovne algebarske strukture koje se pojavljuju u analizi, u algebri, u teoriji brojeva, u algebarskoj geometriji i u mnogim drugim granama matematike.

Definicija 2.1. Prsten $(R, +, \cdot)$ je uređena trojka nepraznog skupa R sa dvije binarne operacije, označene simbolima "+" i "$\cdot$", koje zadovoljavaju sljedeće:

(i) R je Abelova grupa s obzirom na operaciju "+";

(ii) Operacija "$\cdot$" je asocijativna, tj. za sve $x, y, z \in R$ vrijedi:

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

(iii) Ispunjen je *zakon distributivnosti* tj. za sve $x, y, z \in R$ vrijedi:

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

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

Radi kratkoće zapisa, prsten $(R, +, \cdot)$ označavat ćemo samo slovom R. Element $0 = 0_R$, neutralni element u grupi $(R, +)$, zvat ćemo **nula** prstena R.

Ako postoji **jedinični element**, ili kraće **jedinica**, $1 = 1_R \in R$ takva da za sve $x \in R$ vrijedi:

$$1 \cdot x = x \cdot 1 = x,$$

onda kažemo da je R **prsten s jedinicom**.

Prsten R je **komutativan prsten** ako za sve $x, y \in R$ vrijedi:

$$x \cdot y = y \cdot x.$$

U suprotnom govorimo o **nekomutativnom prstenu**.

Iz definicije prstena dobijemo opća svojstva, tj. da za sve $x, y \in R$ vrijedi:

$$x \cdot 0 = 0 \cdot x = 0,$$

$$(-x) \cdot y = x \cdot (-y) = -xy.$$

Primjer 2.2. (1) Skup cijelih brojeva $\mathbb{Z}$ sa običnim zbrajanjem i množenjem je komutativan prsten s jedinicom.

(2) Funkcije $f, g : \mathbb{R} \to \mathbb{R}$ čine komutativan prsten s jedinicom, ako sumu $f + g$ i produkt $f \cdot g$ definiramo sa:

$$(f + g)(x) = f(x) + g(x), \forall x \in \mathbb{R},$$

$$(f \cdot g)(x) = f(x) \cdot g(x), \forall x \in \mathbb{R}.$$

(3) Skup svih 2×2 matrica s elementima iz $\mathbb{R}$ čini nekomutativan prsten s jedinicom obzirom na standardne operacije zbrajanja i množenja matrica.

Definicija 2.3. Prsten R je **integralna domena**, ako je on komutativan prsten s jedinicom $1 \neq 0$, u kojem nema djelitelja nule, tj. za sve $x, y \in R$ vrijedi:

$$x \cdot y = 0 \Rightarrow x = 0 \text{ ili } y = 0.$$

Definicija 2.4. Element $w \in R$, gdje je R prsten s jedinicom 1 je **invertibilan**, ako postoji $w' \in R$ takav da je

$$w \cdot w' = w' \cdot w = 1.$$

Oznaka koja se koristi:

$$R^\times := \text{grupa invertibilnih elementa u } R.$$

Definicija 2.5. Prsten R je **tijelo**, ili **prsten s dijeljenjem**, ako je svaki nenul element u R invertibilan; tj. ako vrijedi

$$R^\times = R \setminus \{0\}.$$

Komutativno tijelo zovemo **polje**.

Primjer 2.6. (1) Prvi i osnovni primjeri polja, koji su fundamentalni objekti u svim granama matematike, su **polje racionalnih brojeva** $\mathbb{Q}$, **polje realnih brojeva** $\mathbb{R}$ i **polje kompleksnih brojeva** $\mathbb{C}$, gdje su operacije zbrajanja i množenja standardno definirane. Znamo da vrijedi $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

(2) Skup cijelih brojeva $\mathbb{Z}$ je integralna domena, ali ne i polje.

Teorem 2.7. Svaka konačna integralna domena jest polje.

Dokaz. Neka je R neka konačna integralna domena i neka su $x_1, x_2, ..., x_n$ elementi iz R. Za neki fiksni element $x \in R$, $x \neq 0$ promotrimo produkte $xx_1, xx_2, ..., xx_n$. Oni su međusobno različiti, jer ako vrijedi $xx_i = xx_j$, za $i \neq j$, tada je $x(x_i - x_j) = 0$. Budući da je $x \neq 0$, slijedi da je $x_i - x_j = 0$, tj. $x_i = x_j$. Dakle, svaki element u R je oblika xx_i, pa je specijalno i $1 = xx_i$, za neki $1 \leq i \leq n$, gdje 1 predstavlja jedinicu u R. Budući da je po definiciji množenje u integralnoj domeni komutativno, vrijedi i da je $x_i x = 1$, što znači da je x_i multiplikativni inverz od x. Slijedi da elementi prstena R, koji su različiti od nule, čine Abelovu grupu obzirom na množenje. Dakle R je polje. □

Definicija 2.8. Skup $S \subseteq R$, gdje je R proizvoljni prsten, je **potprsten** od R ako je $S = (S, +, \cdot)$ i sam prsten. Drugim riječima, S je potprsten od R ako vrijede sljedeća dva uvjeta:

$$x - y \in S, \forall x, y \in S,$$

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

Oznaka koju koristimo, analogno kao i kod grupa $S \leq R$.

U teoriji prstena centralno mjesto pripada *idealima*. Malo slobodnije govoreći, ideali su za prstene ono što su normalne podgrupe za grupe.

Definicija 2.9. Skup $I \subseteq R$, gdje je R komutativan prsten, je (dvostrani ili obostrani) **ideal** tog prstena, ako je I potprsten prstena R, i ako za sve $x \in I$ i $r \in R$ vrijedi:

$$xr \in I \text{ i } rx \in I.$$

Činjenicu da je I ideal u prstenu R označavamo s $I \trianglelefteq R$.

Nadalje, reći ćemo da je ideal I od R **pravi ideal** ako je $I \neq R$ i $I \neq (0)$, gdje je sa (0) označen nulideal.

Napomena 2.10. Primjetimo da je nulideal doista ideal; to je trivijalna posljedica činjenice da je u svakom prstenu R njegova nula 0 zadovoljava $0x = x0 = 0$, za sve $x \in R$.

Primjer 2.11. (1) Neka R predstavlja polje racionalnih brojeva $\mathbb{Q}$. Tada je skup cijelih brojva $\mathbb{Z}$ potprsten od R, ali ne i ideal.
(Npr. $1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$, ali $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z}$).

(2) Neka je R komutativan prsten. Tada je najmanji ideal koji sadrži element $x \in R$ ideal $(x) = \{rx + nx \mid r \in R, n \in \mathbb{Z}\}$. Ako prsten R ima i jedinicu, tada je $(x) = \{rx \mid r \in R\}$.

Definicija 2.12. Neka je R komutativan prsten. Kažemo da je ideal I prstena R **glavni**, ako postoji element $x \in R$, takav da je $I = (x)$ (x je izvodnica ideala I).

Svaki ideal I prstena R definira neku particiju skupa R na disjunktne klase, koje zovemo **klase ostataka prstena R modulo ideala I**. Istoj klasi ostataka pripadaju elementi $x, y \in R$ koji su kongruentni modulo I ($x \equiv y \pmod{I}$), tj. takvi da je $x - y \in I$. Te klase označavamo s $[x] = x + I$.

Lako se provjeri da ako vrijedi $x \equiv y \pmod{I}$, tada vrijedi; $x + r \equiv y + r \pmod{I}$, $xr = yr \pmod{I}$, $rx = ry \pmod{I}$ i $nx = ny \pmod{I}$ za bilo koji $r \in R$, $n \in \mathbb{Z}$. Štoviše, ako je i $r \equiv s \pmod{I}$, tada je i $x + r \equiv y + s \pmod{I}$ i $xr \equiv ys \pmod{I}$.

Teorem 2.13. Neka je R prsten i $I \trianglelefteq R$ bilo koji ideal. Skup klasa ostataka prstena R modulo ideala I čini prsten obzirom na operacije definirane sa:

$$(x + I) + (y + I) = (x + y) + I, \forall x, y \in R, \tag{1}$$

$$(x + I)(y + I) = (xy) + I, \forall x, y \in R. \tag{2}$$

Taj prsten zovemo **kvocijentni prsten prstena R po idealu I** i označavamo s R/I.

Dokaz. Prvo ćemo dokazati da su gore navedene operacije dobro definirane, tj. da ne ovise o uzetim reprezentantima. Neka su x, x', y, y' elementi iz R takvi da je $x + I = x' + I$ i $y + I = y' + I$. Moramo pokazati da je

$$(x + I)(y + I) = (xy) + I = (x'y') + I = (x' + I)(y' + I). \tag{3}$$

Vidimo da vrijedi

$$(xy) + I = (x'y') + I \iff xy - x'y' = x(y - y') + (x - x')y' \in I. \tag{4}$$

Budući da je $x+I = x'+I$ ekvivalentno $x-x' \in I$, te $y+I = y'+I$ ekvivalentno $y - y' \in I$ i I je ideal, znamo da vrijedi $x(y - y') + (x - x')y' \in I$. Dakle vrijedi (4), odnosno (3).

Kako bismo vidjeli da se radi o prstenu, treba samo primjetiti da se i asocijativnost i distributivnost operacija "naslijeđuju" iz R. Također vidimo da je $0_{R/I} = 0 + I = I$ nula u R/I, a $1_R + I = 1_R + I = 1 + I$ jedinica. □

Primjer 2.14. (Kvocijentni prsten $\mathbb{Z}/(n)$.)

Klasu ostataka modulo $n \in \mathbb{N}$, koja sadrži broj $x \in \mathbb{Z}$, označimo sa $[x] = x + (n)$, gdje je (n) glavni ideal generiran brojem n. Elementi tog prstena su:

$$[0] = 0 + (n),\ [1] = 1 + (n),\ ...,\ [n - 1] = n - 1 + (n).$$

Teorem 2.15. $\mathbb{Z}/(p)$ je polje ako i samo ako je p prost broj.

Dokaz. Prema teoremu 2.7, dovoljno je pokazati da je $\mathbb{Z}/(p)$ komutativna integralna domena. Njegova jedinica je $[1]$, a jednadžba $[x][y] = [xy] = [0]$ je ispunjena ako i samo ako je $xy = kp$, za neki cijeli broj k. Budući da je p prost broj, on dijeli produkt xy onda i samo onda ako dijeli barem jedan od faktora. Slijedi da je ili $[x] = [0]$ ili $[y] = [0]$ tako da prsten $\mathbb{Z}/(p)$ nema djelitelja nule. Dakle, $\mathbb{Z}/(p)$ je integralna domena. Obratno, pretpostavimo da je p složen broj. Tada kvocijentni prsten $\mathbb{Z}/(p)$ ima djelitelje nule, pa nije polje. Dakle, istinitost tvrdnje slijedi iz obrata po kontrapoziciji. □

Kvocijentni prsten $\mathbb{Z}/(p)$ je primjer **konačnog polja**.

Definicija 2.16. Za prost broj p sa $\mathbb{F}_p$ označimo skup $\{0, ..., p-1\}$. Definiramo preslikavanje $\varphi : \mathbb{Z}/(p) \to \mathbb{F}_p$ sa $\varphi([x]) = x$, za $x = 0, 1, ..., p-1$. Skup $\mathbb{F}_p$ sa strukturom polja induciranim preslikavanjem φ zovemo **Galoisovo polje** reda p. Operacije zbrajanja i množenja:

$$\varphi([x] + [y]) = \varphi([x]) + \varphi([y]),$$

$$\varphi([x][y]) = \varphi([x])\varphi([y])$$

Struktura polja $\mathbb{F}_p$ podudara se sa strukturom polja $\mathbb{Z}/(p)$ i kod računanja primjenjujemo običnu aritmetiku brojeva s dijeljenjem modulo p.

Primjer 2.17. Promotrimo preslikavanje $\varphi : \mathbb{Z}/(5) \to \mathbb{F}_5 = \{0, 1, 2, 3, 4\}$. Tablice za dvije operacije "+" i "·" dane su sa:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Definicija 2.18. Neka je R proizvoljan prsten. Ako postoji prirodan broj n takav da je za svaki $r \in R$ ispunjeno $n \cdot r = 0$, tada najmanji od takvih brojeva n (označimo ga sa n_0) zovemo **karakteristika** prstena R, tj. kažemo da je R **prsten (pozitivne) karakteristike** n_0.
Ako takav prirodan broj ne postoji, kažemo da je R prsten karakteristike 0.

Teorem 2.19. Ako prsten $R \neq \{0\}$ s jedinicom 1 i bez djelitelja nule ima pozitivnu karakteristiku n, tada je n prost broj.

Dokaz. Budući da je $R \neq \{0\}$, tj. prsten R sadrži element različit od nule, karakteristika n tog prstena je veća ili jednaka 2. Pretpostavimo suprotno, neka je n složen broj. Onda je $n = k \cdot m$, gdje su $k, m \in \mathbb{Z}$, $1 < k, m < n$. Sada iz $0 = n1 = (k1)(m1)$ slijedi da je ili $k1 = 0$ ili $m1 = 0$, budući da u R nema djelitelja nule. Vidimo da ili je $kr = (k1)r = 0$ ili je $mr = (m1)r = 0$, za sve $r \in R$, a to je u kontradikciji s minimalnosti u definiciji karakteristike n. Dakle, n je prost broj. □

Korolar 2.20. Karakteristika konačnog polja je prost broj.

Dokaz. Prema teoremu 2.15, dovoljno je pokazati da bilo koje konačno polje $\mathbb{F}$ ima pozitivnu karakteristiku. Promotrimo u polju $\mathbb{F}$ elemente $1, 2\cdot 1, 3\cdot 1, ...$, višekratnike jedinice 1. Budući da $\mathbb{F}$ sadrži konačan broj različitih elemenata, postoje prirodni brojevi k i m, $1 \leq k \leq m$, takvi da je $k1 = m1$. Slijedi da je $(m-k)1 = 0$ iz čega slijedi da $\mathbb{F}$ ima pozitivnu karakteristiku. □

Sada želimo vidjeti kako treba izgledati ideal I prstena R da bi kvocijentni prsten R/I bio initegralna domena ili polje. Neka je R komutativni prsten s jedinicom. Element $x \in R$ je **djelitelj** elementa $y \in R$, ako postoji element $z \in R$ takav da je $xz = y$. Djelitelji jedinice su **invertibilni** elementi. Elementi $x, y \in R$ su **povezani** ako postoji invertibilni element ε takav da je $x = y\varepsilon$. Element z je **prosti element** prstena R, ako on nije invertibilan i nema drugih djelitelja, osim elemenata koji su povezani s njim ili invertibilnih elemenata.

Definicija 2.21. Ideal $P \neq R$ prstena R je **prosti ideal**, ako za $x, y \in R$ vrijedi $xy \in P$ samo u slučaju ako je $x \in P$ ili $y \in P$.

Definicija 2.22. Ideal $M \neq R$ je **maksimalan**, ako za bilo koji ideal I prstena R, za koji je $M \subseteq I$ slijedi da je $I = M$ ili $I = R$.

Definicija 2.23. Prsten R je **domena glavnih ideala** ako je integralna domena i svaki ideal I prstena R je glavni, tj. postoji element $x \in R$ takav da je

$$I = (x) = \{rx \mid r \in R\}.$$

Teorem 2.24. Neka je R komutativni prsten s jedinicom. Tada:

(i) Ideal M prstena R je maksimalan ako i samo ako je kvocijentni prsten R/M polje.

(ii) Ideal P prstena R je prost ako i samo ako je kvocijentni prsten R/P integralna domenena.

(iii) Svaki maksimalan ideal prstena R je prost.

(iv) Ako je R prsten glavnih ideala, tada je kvocijentni prsten $R/(p)$ polje, ako i samo ako je p prost element prstena R.

Dokaz. (i) ($\Rightarrow$) Pretpostavimo da je M maksimalni ideal prstena R. Tada je za $x \in R$, $x \notin M$ skup $I = \{xr + m \mid r \in R, m \in M\}$ ideal prstena R, koji sadrži M, ali je različit od M, pa je $I = R$. Dakle, postoje $r \in R$ i $m \in M$ takvi da vrijedi $xr + m = 1$, gdje je 1 jedinica prstena R. To znači, ako je klasa $x + M \in R/M$ i $x + M \neq M$, onda ona ima multiplikativni inverz, budući da vrijedi $(x + M)(r + M) = xr + M = (1 - m) + M = 1 + M$. Iz toga slijedi da je R/M polje.

($\Leftarrow$) Obratno, neka je R/M polje i neka je I takav ideal prstena R da je $I \supseteq M$ i $I \neq M$. Tada za $x \in I$ i $x \notin M$, klasa ostataka $x + M$ ima multiplikativni inverz, tj. $(x + M)(r + M) = 1 + M$, za neki $r \in R$. To znači

da je $xr + m = 1$ za neki $m \in M$. Budući da je I ideal i $1 \in I$ slijedi da je $I = R$. Dakle, M je maksimalni ideal prstena R.

(ii) $(\Rightarrow)$ Neka je P prost ideal prstena R. Tada je kvocijentni prsten R/P komutativni prsten s jedinicom $1 + P \neq P$. Neka je $(x + P)(y + P) = xy + P = P$. Budući da je $0 \in P$, mora biti $xy \in P$, a kako je P prost ideal mora vrijediti $x \in P$ ili $y \in P$, tj. $x + P = P$ ili $y + P = P$. Slijedi da R/P nema djelitelja nule što povlači da je R/P integralna domena.

$(\Leftarrow)$ Pretpostavimo sada da je R/P integralna domena, ali da P nije prost ideal. To znači da postoje neki $x, y \in R \setminus P$ takvi da je $xy \in P$. Vrijedi $xy \in P$ ako i samo ako je $(x+P)(y+P) = P$. No isto tako vrijedi $x \in R \setminus P$ ako i samo ako $x + P \neq P$ i $y \in R \setminus P$ ako i samo ako $y + P \neq P$. Iz toga slijedi da kvocijenti prsten R/P nije integralna domena, što je kontradikcija s pretpostavkom.

(iii) Ova tvrdnja slijedi iz (i) i (ii) budući da je svako polje integralna domena.

(iv) Neka je $p \in R$. Ako je p invertibilni element, tada je $(p) = R$ i kvocijentni prsten $R/(p)$ se sastoji od jedinstvenog elementa, pa ne može biti polje. Ako p nije invertibilni niti prosti element, tada p ima neki djelitelj $x \in R$, koji nije povezan s p, a nije ni invertibilan. Vidimo da je $x \neq 0$, jer iz $x = 0$, slijedi $p = 0$, tj. x bi bio povezan s p. Neka je $p = xy$, gdje je $y \in R$. Također, $x \neq (p)$, jer bi u protivnom bilo $x = pz = xyz$, gdje je $z \in R$, tj. $x(1 - yz) = 0$. Kako je $x \neq 0$, slijedi $yz = 1$, a to znači da je y invertibilan, što je u kontradikciji sa pretpostavkom da x nije povezan sa p. Iz toga svega slijedi $(p) \subseteq (x) \subseteq R$, tj. (p) nije maksimalni ideal i prema (i) $R/(p)$ ne može biti polje. Još trebamo promotriti, što ako je p prost element prstena R? U tom slučaju $(p) \neq R$, budući da p nije invertibilan element. Nadalje, ako je I ideal prstena R, $(p) \subseteq I$, tada je $I = (x)$, za neki $x \in R$, budući da je R prsten glavnih ideala. Slijedi da je $p \in (x)$, tj. x je djelitelj elementa p, pa je x ili invertibilan, ili povezan sa p, što povlači da je $I = R$ ili $I = (p)$. Dakle, (p) je maksimalni ideal prstena R i prema (i) $R/(p)$ je polje. □

3 Prsteni polinoma

U ovom poglavlju ćemo definirati polinome, prstene polinoma i sve što nam je potrebno kako bismo dokazali da za svaku prim potenciju $q = p^n$ postoji polje reda q.

Polinomi su osnovne funkcije u matematici. Posebno, polinomi nad $\mathbb{R}$

ili $\mathbb{C}$, tj. s realnim ili kompleksnim koeficijentima, su objekti bez kojih je nemoguće zamisliti mnoge grane u matematici.

Definicija 3.1. Neka je R komutativni prsten s jedinicom. **Polinom** nad R je izraz oblika:

$$f(x) := \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + ... + a_i x^i + ... + a_n x^n, n \in \mathbb{N}_0, a_i \in R, 0 \leq i \leq n.$$

Ovdje je x **varijabla**, a x^i je tzv. *i-ta potencija* od x. Elementi a_i zovu se **koeficijenti** polinoma $f(x)$; posebno, kažemo da je a_i *i-ti* koeficijent. Koeficijent a_0 zove se **slobodni koeficijent**, a a_n **vodeći koeficijent**. Kada govorimo o vodećem koeficijentu, mi zapravo pretpostavljamo da je $a_n \neq 0$.

Posebno definiramo **nulpolinom** kao

$$0 = 0 + 0x + 0x^2 + ...;$$

drugim riječima, nulpolinom je polinom kojem su svi koeficijenti jednaki 0.

Za polinom $f(x)$ kao gore, kojemu je vodeći koeficijent $a_n \neq 0$, definiramo **stupanj** polinoma $f(x)$ kao

$$\deg f(x) = \deg(f) := n,$$

tako govorimo da je $f(x)$ *polinom stupnja n*. Nadalje, dogovorno se uzima da je stupanj nulpolinoma jednak $-\infty$. Polinome stupnja manjeg ili jednakog 0 nazivamo **konstantni polinomi**.

Polinomi $f(x) := \sum_{i=0}^{m} a_i x^i$ i $g(x) := \sum_{i=0}^{n} b_i x^i$ nad R su jednaki ako i samo ako vrijedi:

$$n = m$$

i

$$a_i = b_i, 0 \leq i \leq n.$$

Uz pretpostavku da je $n > m$ i da su $a_i = 0$ za $m + 1 \leq i \leq n$ (što ne smanjuje općenitost) definiramo zbroj polinoma:

$$f(x) + g(x) := \sum_{i=0}^{n} (a_i + b_i) x^i$$

i produkt polinoma:

$$f(x)g(x) := \sum_{k=0}^{n+m} c_k x^k, \quad c_k = \sum_{i+j=k, 0 \leq i \leq m, 0 \leq j \leq n} a_i b_j.$$

Uz ovako definirane operacije zbrajanja i množenja polinoma skup svih polinoma nad prstenom R je **prsten polinoma sa koeficijentima iz** R, u oznaci $R[x]$. Nula prstena $R[x]$ je polinom kojem su svi koeficijenti jednaki nula (nulpolinom), u oznaci 0.

Ako prsten R ima jedinicu 1 i ako je vodeći koeficijent polinoma $f(x)$ jednak 1, onda kažemo da je polinom $f(x)$ **normiran**.

Ako su $f(x), g(x) \in R[x]$, tada vrijedi:

$$\deg(f+g) \leq max\{\deg(f), \deg(g)\}$$

i

$$\deg(fg) \leq \deg(f) + \deg(g).$$

Ako je R integralna domena, onda vrijedi:

$$\deg(fg) = \deg(f) + \deg(g).$$

Ako poistovjetimo konstantne polinome s elemetima prstena R, tada R možemo smatrati potprstenom prstena $R[x]$. Neka svojstva prstena R naslijeđena su u prstenu $R[x]$.

Teorem 3.2. Neka je R proizvoljan prsten. Tada vrijedi:
(i) $R[x]$ je komutativan prsten, ako i samo ako je R komutativan.
(ii) $R[x]$ je prsten s jedinicom, ako i samo ako je R prsten s jedinicom.
(iii) $R[x]$ je integralna domena, ako i samo ako je R integralna domena.

Prsten polinoma $R[x]$ može se formalno definirati na sljedeći način. Neka je S skup svih beskonačnih nizova oblika

$$(a_0, a_1, ..., a_n, ...),$$

gdje su komponente a_i elementi komutativnog prstena R s jedinicom, i konačno mnogo a_i-eva je različito od 0. Lako se pokaže da je S komutativan prsten s jedinicom sa operacijama zbrajanja i množenja definiranih na sljedeći način:

$$(a_0, a_1, ...) + (b_0, b_1, ...) = (a_0 + b_0, a_1 + b_1, ...),$$

$$(a_0, a_1, ...)(b_0, b_1, ...) = (a_0b_0, a_0b_1 + a_1b_0, ...),$$

gdje je $(n+1)$-va komponenta produkta $a_0b_n + a_1b_{n-1} + ... + a_{n-1}b_1 + a_nb_0$. Nula prstena S je $(0, 0, ...)$, a jedinica je $(1, 0, ...)$.

Uvodimo notaciju $x = (0, 1, 0, ...)$, odnosno za $n \geq 1$

$$x^n = (0, ...0, 1, 0, ...),$$

gdje je 1 na $(n+1)$-vom mjestu. Ako definiramo $x^0 = (1, 0, 0, ...)$, onda imamo

$$(a_0, a_1, a_2, ...) = (a_0, 0, 0...) + (0, a_1, 0, ...) + (0, 0, a_2, 0, ...) + ...$$

$$= (a_0, 0, 0...)(1, 0, 0, ...) + (a_1, 0, 0...)(0, 1, 0, ...) + (a_2, 0, 0...)(0, 0, 1, 0, ...) + ...$$

$$= (a_0, 0, 0...)1 + (a_1, 0, 0...)x + (a_2, 0, 0...)x^2 + ...$$

$$= a_0 + a_1x + a_2x^2 + ...a_nx^n$$

$$= f(x),$$

za bilo koji niz u S. Tako su elementi prstena S zapravo polinomi $f(x) \in R[x]$ definirani kao beskonačni niz sa konačno mnogo komponenti a_i različitih od 0.

U daljnjem radu, promatrat ćemo polinome nad poljima. Sa F označimo proizvoljno polje (ne mora biti konačno). Već smo uveli pojam djeljivosti u općem prstenu R, pa želimo pokazati kako se definira *djeljivost* u specijalnom slučaju kada je $R = F[x]$. Kažemo da polinom $g \in F[x]$ **dijeli** polinom $f \in F[x]$, ako postoji polinom $h \in F[x]$ takav da je $f = gh$. Također kažemo da je g **djelitelj** od f, a f **višekratnik** od g. Invertibilni elementi u prstenu $F[x]$ su djelitelji konstantnog polinoma 1, tj. svi konstantni polinomi različiti od nule.

Teorem 3.3. (Teorem o dijeljenju s ostatkom) Neka je F proizvoljno polje, te neka su $f(x)$ i $g(x) \neq 0$ polinomi iz $F[x]$. Tada postoje i jedinstveni su polinomi $q(x), r(x) \in F[x]$ takvi da je

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

i

$$\deg(r(x)) < \deg(g(x)).$$

Dokaz. (Egzistencija) Dokaz ćemo provesti po stupnju polinoma kojeg dijelimo, tj. polinoma $f(x)$. Neka su:

$$f(x) = a_0 + a_1x + ... + a_nx^n,$$

$$g(x) = b_0 + b_1x + ... + b_mx^m,$$

pri čemu je $a_n, b_m \neq 0$ i $a_n, b_m \in F$. Najprije pogledajmo bazu indukcije; tj. $n < m$. Imamo dvije mogućnosti:

(1) $\deg g(x) = 0$.

U tom slučaju $f(x) = a_0$ i $g(x) = b_0$, pa onda r i q definiramo $r(x) := 0$ i $q(x) := b_0^{-1}a_0$, pa je $gq + r = b_0(b_0^{-1}a_0) = a_0 = f$.

(2) $\deg(g(x)) > 0$.

U tom slučaju definiramo $r(x) := f(x)$ i $q(x) := 0$, pa je $gq + r = 0 + f = f$.

Nakon toga prelazimo na korak indukcije. Pretpostavimo da teorem vrijedi za sve polinome $f(x) \in F[x]$ stupnja manjeg od n, pa pokažimo da onda vrijedi i za sve polinome stupnja jednakog n. Bez smanjenja općenitosti pretpostavimo da vrijedi

$$\deg(g(x)) = m \leq n = \deg(f(x)).$$

Definirajmo "pomoćni" polinom $f_1(x)$ sa

$$f_1(x) := f(x) - a_n b_m^{-1} x^{n-m} g(x);$$

gdje koristimo činjenicu da je vodeći koeficijent b_m od $g(x)$ invertibilan u F. Iz ovako definiranog $f_1(x)$ vidimo da je

$$\deg(f_1(x)) < \deg(f(x)) = n.$$

Primjenom pretpostavke indukcije na polinom $f_1(x)$ dobijemo da postoje neki polinomi $q_1(x)$ i $r(x)$ takvi da vrijedi

$$f_1(x) = q_1(x)g(x) + r(x)$$

i

$$\deg(r(x)) < \deg(g(x)).$$

Iz tog slijedi da je

$$f(x) = q(x)g(x) + r(x),$$

gdje polinom $q(x)$ definiramo kao

$$q(x) := a_n b_m^{-1} x^{n-m} + q_1(x);$$

čime je egzistencija rastava dokazana.

(Jedinstvenost)

Pretpostavimo da postoje $q_i(x)$ i $r_i(x)$, za $i = 1, 2$, takvi da je

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

i deg $(r_i(x))$ <deg $(g(x))$, za $i = 1, 2$. Onda slijedi

$$(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x).$$

Želimo dokazati da je $q_1(x) - q_2(x) = 0$, odnosno $r_2(x) - r_1(x) = 0$. Naime, kada bi bilo $q_1(x) - q_2(x) \neq 0$, onda bismo imali

$$\deg((q_1(x) - q_2(x))g(x)) \geq m = \deg(g(x));$$

tj.

$$\deg(r_2(x) - r_1(x)) \geq m.$$

Ali budući da vrijedi $\deg(r_2(x) - r_1(x)) < m = \deg(g(x))$, dolazimo do kontradikcije, čime smo dokazali jedinstvenost, a time i teorem u potpunosti. □

Teorem 3.4. Ako je F polje, onda je prsten polinoma $F[x]$ prsten glavnih ideala.

Dokaz. Neka je $(0) \neq I \trianglelefteq F[x]$ neki ideal. Kako bismo pokazali da je on glavni, uzmimo polinom $g = g(x)$ takav da je $g \neq 0$ i $g \in I$, te stupanj $\deg(g)$ najmanji mogući; tj. $\deg(g) = min\{\deg \gamma \mid \gamma \in I\}$. (Takav g sigurno postoji; to je zapravo posljedica elementarne činjenice da svaki neprazan podskup od $\mathbb{N}$ ima najmanji element.) Tvrdimo da je

$$I = (g).$$

Dosita, očita je inkluzija $I \supseteq (g)$. Za obratno, uzmimo proizvoljan $f \in I$. Po teoremu 3.3, postoje neki q i r takvi da je $f = qg + r$ i $\deg(r) < \deg(g)$. Ali kako su $f, g \in I$, to slijedi da je također $r = f - qg \in I$. No, zbog minimalnosti stupnja od g, zaključujemo da nužno vrijedi $r = 0$. Dakle, $f = qg \in (g)$. □

Definicija 3.5. Polinom $f \in F[x]$ je **ireducibilan**, ako ima pozitivan stupanj i ako je jednakost $f = gh$, $g, h \in F[x]$ ispunjena samo u slučaju kada je ili g ili h konstantan polinom. Polinome pozitivnog stupnja, koji nisu ireducibilni nad F, zovemo **reducibilni** polinomi nad poljem F.

Reducibilnost i ireducibilnost promatranog polinoma ovisi o tome nad kojim ga poljem promatramo. Npr. polinom $f(x) = x^2 - 2$ je ireducibilan nad poljem $\mathbb{Q}$, ali je reducibilan nad poljem $\mathbb{R}$, budući da je $f(x) = (x + \sqrt{2})(x - \sqrt{2})$. Invertibilni elementi u prstenu $F[x]$ su konstantni polinomi različiti od nulpolinoma. Ireducibilni polinomi su zapravo prosti elementi u prstenu $F[x]$.

Ireducibilni polinomi imaju važnu ulogu u prstenu $F[x]$, budući da se svaki polinom iz $F[x]$ može na jedinstven način zapisati kao produkt ireducibilnih polinoma. Za dokaz će nam trebati sljedeća lema.

Lema 3.6. Ako ireducibilni polinom $f \in F[x]$ dijeli produkt $f_1 \cdots f_n$ polinoma $f_1, ..., f_n$ iz $F[x]$, tada je barem jedan od faktora f_i, $i = 1, ..., n$ djeljiv s f.

Dokaz. Budući da polinom f dijeli produkt $f_1 \cdots f_n$, u kvocijentnom prstenu $F[x]/(f)$ dobijemo jednakost:

$$(f_1 + (f)) \cdots (f_n + (f)) = (f_1 \cdots f_n) + (f) = (f).$$

Prema teoremu 2.24 (iv) taj kvocijentni prsten je polje, tako da postoji i, $1 \leq i \leq n$, takav da je $f_i + (f) = (f)$, a to znači da f dijeli f_i. □

Teorem 3.7. (O jednoznačnom rastavu na faktore) Neka je F proizvoljno polje. Svaki polinom pozitivnog stupnja $f \in F[x]$ možemo prikazati u obliku produkta

$$f = a f_1^{n_1} \cdots f_k^{n_k}, \tag{5}$$

gdje su $a \in F$, $f_1, ..., f_k \in F[x]$ različiti normirani ireducibilni polinomi, a $n_1, ..., n_k \in \mathbb{N}$. Štoviše, taj rastav je jedinstven do na poredak faktora.

Dokaz. (Egzistencija) Dokaz ćemo provoditi indukcijom po stupnju polinoma f. Baza, odnosno slučaj $\deg(f) = 1$ je trivijalan, budući da je bilo koji polinom prvog stupnja ireducibilan nad F. Pretpostavimo da tvrdnja vrijedi za sve nekonstantne polinome iz $F[x]$ stupnja manjeg od n. Pogledajmo sada korak indukcije. Ako je $\deg(f) = n$ i f ireducibilan nad F, tada je $f = a(a^{-1}f)$, gdje je a vodeći koeficijent polinoma f, a $a^{-1}f$ normirani ireducibilni polinom iz $F[x]$. Tada imamo traženi prikaz polinoma. Ako je f reducibilan, tada on dopušta rastav $f = gh$, gdje su $g, h \in F[x]$, $1 \leq \deg(g), \deg(h) \leq n$. Prema pretpostavci indukcije g i h možemo rastaviti kao u (5), pa slijedi da u tom obliku možemo prikazati i polinom f.

(Jedinstvenost) Pretpostavimo da f ima dva prikaza oblika (5).

$$f = af_1^{n_1} \cdots f_k^{n_k} = bg_1^{m_1} \cdots g_k^{m_r}. \tag{6}$$

Izjednačimo vodeće koeficijente; $a = b$.

Nadalje, ireducibilni polinom f_1 dijeli desnu stranu jednakosti (6), pa po lemi 3.6 on dijeli jedan od polinoma g_j, $1 \leq j \leq r$. Međutim, polionom g_j je također ireducibilan u prstenu $F[x]$, tako da je $g_j = cf_1$, gdje je c neka konstanta. Budući su f_1 i g_j normirani polinomi, slijedi da je $g_j = f_1$. Na taj način u jednadžbi (6), primjenjujući isti postupak dobijemo i jednakost ostalih polinoma. Nakon konačno mnogo koraka, dobit ćemo da se rastavi u (6) podudaraju do na poredak faktora. □

Rastav (5) zovemo **kanonski rastav** polinoma f u prstenu $F[x]$. Budući da su ireducibilni polinomi nad poljem F, zapravo, prosti elementi prstena $F[x]$, sljedeći rezultat slijedi iz teorema 2.24(iv).

Teorem 3.8. Neka je $f \in F[x]$. Kvocijentni prsten $F[x]/(f)$ je polje ako je polinom f ireducibilan nad poljem F.

Promotrimo strukturu kvocijentnog prstena $F[x]/(f)$, za proizvoljni polinom $f \in F[x]$, $f \neq 0$. Taj kvocijentni prsten sastoji se od klasa ostataka $[g] = g + (f)$, gdje je $g \in F[x]$. Dvije klase ostataka $g + (f)$ i $h + (f)$ su jednake ako i samo ako je $g \equiv h \pmod{f}$, tj. ako je polinom $g - h$ djeljiv sa f. To je ekvivalentno činjenici da g i h imaju isti ostatak kod dijeljenja sa f. Označimo taj ostatak sa $r \in F[x]$. Tada vrijedi da je $\deg(r) < \deg(f)$. Proces prelaska od g do r zovemo **dijeljenje modulo** f. Polinom r je jedinstven, jer iz pretpostavke da postoji polinom $r_1 \in g + (f)$, $\deg(r_1) < \deg(f)$, slijedi da razlika $r - r_1$ mora biti djeljiva s f. Budući da je $\deg(r - r_1) < \deg(f)$, $r - r_1 = 0$, tj. $r = r_1$. Sada možemo jasno opisati različite elemente kvocijentnog prstena $F[x]/(f)$. To su klase ostataka $r+(f)$, gdje su r, svi polinomi iz $F[x]$, stupnja manjeg od $\deg(f)$.

Primjer 3.9. (1) Neka je $f(x) = x \in \mathbb{F}_2[x]$. Kvocijentni prsten $\mathbb{F}_2[x]/(x)$ sazdrži $p^n = 2^1$ klasa ostataka i to su: $[0]$ i $[1]$, tj. kvocijentni prsten $\mathbb{F}_2[x]/(x)$ izomorfan je polju $\mathbb{F}_2$.

(2) (Primjer polja reda 4) Neka je $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. Kvocijentni prsten $\mathbb{F}_2[x]/(f)$ sastoji se iz $p^n = 2^2 = 4$ elemenata: $[0], [1], [x], [x+1]$. Operacije u tom prstenu dane su tablicama:

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[x+1]$	$[1]$
$[x+1]$	$[0]$	$[x+1]$	$[1]$	$[x]$

Iz tablice se vidi da je kvocijentni prsten $\mathbb{F}_2[x]/(f)$ polje (to slijedi iz teorema 3.8, jer je f ireducibilan polinom nad poljem $\mathbb{F}_2$).

(3) (Primjer polja reda 9) Neka je $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Kvocijentni prsten $\mathbb{F}_3[x]/(f)$ sastoji se iz $p^n = 3^2 = 9$ elemenata: $[0], [1], [2], [x], [x+1], [x+2], [2x], [2x+1], [2x+2]$. Budući da je $\mathbb{F}_3[x]/(f)$ komutativan prsten, dovoljno je zapisati samo elemente iznad glavne dijagonale, pa će operacije u tom prstenu biti dane tablicama:

$+$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[0]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[1]$		$[2]$	$[0]$	$[x+1]$	$[x+2]$	$[x]$	$[2x+1]$	$[2x+2]$	$[2x]$
$[2]$			$[1]$	$[x+2]$	$[x]$	$[x+1]$	$[2x+2]$	$[2x]$	$[2x+1]$
$[x]$				$[2x]$	$[2x+1]$	$[2x+2]$	$[0]$	$[1]$	$[2]$
$[x+1]$					$[2x+2]$	$[2x]$	$[1]$	$[2]$	$[0]$
$[x+2]$						$[2x+1]$	$[2]$	$[0]$	$[1]$
$[2x]$							$[x]$	$[x+1]$	$[x+2]$
$[2x+1]$								$[x+2]$	$[x]$
$[2x+2]$									$[x+1]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$		$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[2]$			$[1]$	$[2x]$	$[2x+2]$	$[2x+1]$	$[x]$	$[x+2]$	$[x+1]$
$[x]$				$[2]$	$[x+2]$	$[2x+2]$	$[1]$	$[x+1]$	$[2x+1]$
$[x+1]$					$[2x]$	$[1]$	$[2x+1]$	$[2]$	$[x]$
$[x+2]$						$[x]$	$[x+1]$	$[2x]$	$[2]$
$[2x]$							$[2]$	$[2x+2]$	$[x+2]$
$[2x+1]$								$[x]$	$[1]$
$[2x+2]$									$[2x]$

Na isti način bismo mogli konstruirati konačno polje bilo kojeg reda oblika p^n, kad bismo znali da postoji ireducibilni polinom stupnja n nad $\mathbb{F}_p$. (Egzistencija ireducibilnih polinoma dokazana je direktno u poglavlju 4.7 knjige [1]. U idućem poglavlju dokazat ćemo na drugi način egzistenciju i jedinstvenost konačnog polja reda p^n.)

4 Egzistencija i jedinstvenost konačnih polja

U ovom poglavlju ćemo promatrati proširenja polja i pojam polja razlaganja danog polinoma. Egzistencija i jedinstvenost polja reda $q = p^n$ bit će posljedica polja razlaganja polinoma $x^q - x$ nad poljem $\mathbb{F}_p$.

Definicija 4.1. Element $b \in F$ je **korijen** ili **nula** polinoma $f \in F[x]$, ako je $f(b) = 0$.

Teorem 4.2. Element $b \in F$ je korijen polinoma $f \in F[x]$ ako i samo ako polinom $x - b$ dijeli f.

Dokaz. Primjenjujući teorem 3.3, možemo pisati $f(x) = q(x)(x-b)+c$, gdje je $q \in F[x]$, $c \in F$. Ako umjesto varijable x stavimo b, dobijemo $f(b) = c$, što daje $f(x) = q(x)(x-b)+f(b)$. Iz ove jednakosti slijedi tvrdnja teorema. □

Definicija 4.3. Neka je $b \in F$ korijen polionoma $f \in F[x]$. **Kratnost** ili **strukost** korijena b je prirodan broj k za koji vrijedi $(x-b)^k$ dijeli f, ali $(x-b)^{k+1}$ ne dijeli f. Za $k = 1$ korijen b je **jednostruk**, a za $k > 1$ korijen b je **višestruk**.

Definicija 4.4. Neka je F polje. Podskup K polja F, koji je i sam polje obzirom na operacije definirane na polju F, je njegovo **potpolje**. U tom slučaju je polje F **proširenje** polja K. Ako je $K \neq F$, tada je K **pravo potpolje** polja F.

Ako je K potpolje konačnog polja $\mathbb{F}_p$, za neki prosti broj p, tada ono mora sadržavati elemente 0 i 1, ali i sve druge elemente polja $\mathbb{F}_p$, zbog zatvorenosti polja K obzirom na operaciju zbrajanja. Slijedi da polje $\mathbb{F}_p$ nema pravih potpolja.

Definicija 4.5. Polje koje nema pravih potpolja je **prosto polje**. Dakle, bilo koje polje reda p, gdje je p prost broj, je prosto polje. Polje $\mathbb{Q}$ je također primjer prostog polja. Presjek konačnog broja potpolja danog polja F ponovo je potpolje polja F. Presjek svih potpolja F je **prosto potpolje** polja F.

Teorem 4.6. Prosto potpolje polja F izomorfno je ili polju $\mathbb{F}_p$, za neki prost broj p ili polju $\mathbb{Q}$. Karakteristika polja F je p ili 0.

Dokaz. Neka je $\chi : \mathbb{Z} \to F$ homomorfizam prstenova (preslikavanje je aditivno i multiplikativno) definirano sa $\chi(n) = n1$, pri čemu 1 označava jedinicu polja F. Postoji $p \in \mathbb{Z}$ takav da je $Ker\chi = (p)$ jer je svaki ideal u $\mathbb{Z}$ glavni. Ako je $p = 0$, tada je χ injekcija, pa postoji izomorfizam od $\mathbb{Z}$ koji je potprsten od polja F. Postoji polje $Q \cong \mathbb{Q}$ čija je slika $Im\chi \subseteq Q \subseteq F$. Budući da je Q potpolje generirano s 1, ono je prosto potpolje polja F. Ako je $p \neq 0$, slijedi

$$\mathbb{Z}/(p) \cong Im_\chi \subseteq F.$$

Budući da je F polje, a Im_χ integralna domena, slijedi da je p prost broj i tada je $Im_\chi \cong \mathbb{F}_p$ prosto potpolje od F jer je to potpolje generirano s 1. □

Definicija 4.7. Neka je K potpolje polja F i M bilo koji podskup polja F. Tada definiramo polje $K(M)$ kao presjek svih potpolja polja F, koja istovremeno sadrže K i M. To je **proširenje polja K dobiveno dodavanjem elemenata skupa M**. U slučaju da je M konačan skup, $M = \{\theta_1, ..., \theta_n\}$, pisat ćemo $K(M) = K(\theta_1, ..., \theta_n)$, a ako se M sastoji od jednog elementa $\theta \in F$, tada je polje $K(\theta)$ **prosto proširenje** polja K sa **izvodnicom** θ.

Očigledno je $K(M)$ najmanje potpolje polja F, koje istovremeno sadrži i polje K i skup M.

Definicija 4.8. Neka je K neko potpolje polja F i $\theta \in F$. Ako θ zadovoljava netrivijalnu polinomijalnu jednadžbu s koeficijentima iz polja K; $a_n\theta^n + ... +$

$a_1\theta + a_0 = 0$, gdje su $a_i \in \mathbb{F}$ i barem jedan $a_i \neq 0$, $0 \leq i \leq n$, tada je θ **algebarski element** nad K.

Neka je element $\theta \in F$ algebarski nad K. Promotrimo skup $I = \{f \in K[x] \mid f(\theta) = 0\}$. Skup I je ideal prstena $K[x]$ i $I \neq 0$, budući da je θ algebarski element nad K. Prema teoremu 2.24 postoji i jednoznačno je određen normirani polinom $g \in K[x]$, takav da je $I = (g)$. Taj polinom je ireducibilan u $K[x]$. Prvo, g ima pozitivan stupanj jer ima korijen θ, a drugo, ako je $g = h_1 h_2 \in K[x]$, $1 \leq \deg(h_i) \leq \deg(g)$, $i = 1, 2$, tada iz $0 = g(\theta) = h_1(\theta)h_2(\theta)$, slijedi ili da h_1 ili h_2 leže u I, dakle, djeljiv je sa g, a to je nemoguće. Dakle, g je ireducibilan.

Definicija 4.9. Ako je θ algebarski element polja F nad potpoljem K tog polja, tada je jednoznačno određen normirani polinom $g \in K[x]$, koji generira ideal $I = \{f \in K[x] \mid f(\theta) = 0\}$ prstena $K[x]$ i kojeg zovemo **minimalni polinom** elementa θ nad poljem K. **Stupanj** elementa θ nad poljem K je stupanj njegovog minimalnog polinoma g.

Uočimo da i minimalni polinom algebarskog elementa θ i stupanj tog elementa ovise o polju K, nad kojim promatramo taj element. Ako je L proširenje polja K, tada L možemo promatrati kao **vektorski prostor** nad poljem K. Elementi polja L (tj. *vektori*) čine Abelovu grupu obzirom na zbrajanje. Također svaki vektor $a \in L$ možemo množiti skalaraom $\alpha \in K$ i pri tome produkt αa leži u L. Dakle, vrijede sljedeće jednakosti:

$$\alpha(a + b) = \alpha a + \alpha b,$$

$$(\alpha + \beta)a = \alpha a + \beta a,$$

$$(\alpha\beta)a = \alpha(\beta a),$$

$$1a = a, \alpha, \beta \in K, a, b \in L.$$

Preslikavanje $T : L \to L$ je linearni operator ako zadovoljava ova dva svojstva:

$$T(a + b) = T(a) + T(b),$$

$$T(\alpha a) = \alpha T(a), a, b \in L, \alpha \in K.$$

Definicija 4.10. Neka je L neko proširenje polja K. Ako je L, kao vektorski prostor nad K, konačne dimenzije, tada je L **konačno proširenje** polja K. Proširenje polja kojemu je svaki element algebarski nad tim poljem zovemo **algebarsko proširenje** polja. Dimenzija vektorskog prostora L nad K je **stupanj** polja L nad K. Oznaka: $[L : K]$.

Teorem 4.11. Ako je L konačno proširenje polja K i M konačno proširenje polja L, tada je M konačno proširenje polja K i vrijedi:

$$[M : K] = [M : L][L : K].$$

Dokaz. Neka je $[M : L] = m$, $[L : K] = n$ i neka je $\{\alpha_1, ..., \alpha_m\}$ baza vektorskog prostora M nad L i $\{\beta_1, ..., \beta_n\}$ baza vektorskog prostora L nad K. Tada se svaki element $\alpha \in M$ može zapisati kao linearna kombinacija $\alpha = \gamma_1\alpha_1 + ... + \gamma_m\alpha_m$, $\gamma_i \in L, 1 \leq i \leq m$, a svaki γ_i je linearna kombinacija $\gamma_i = r_{i_1}\beta_1 + ... + r_{i_n}\beta_n$, $r_{i_j} \in K$, $1 \leq j \leq n$. Spajanjem te dvije linearne kombinacije imamo:

$$\sum_{i=1}^{m} \gamma_i\alpha_i = \sum_{i=1}^{m}(\sum_{j=1}^{n} r_{i_j}\beta_j)\alpha_i = \sum_{i=1}^{m}\sum_{j=1}^{n} r_{i_j}\beta_j\alpha_i, r_{i_j} \in K.$$

Sada je, za dokaz teorema, dovoljno pokazati linearnu nezavisnost mn elemenata $\beta_j\alpha_i$, $1 \leq i \leq m$, $1 \leq j \leq n$, nad poljem K. Pretpostavimo da je $\sum_{i=1}^{m}\sum_{j=1}^{n} \delta_{i_j}\beta_j\alpha_i = 0$ s koeficijentima $\delta_{i_j} \in K$.

Tada je $\sum_{i=1}^{m}(\sum_{j=1}^{n} \delta_{i_j}\beta_j)\alpha_i = 0$ i zbog linearne nezavisnosti elemenata $\alpha_1, ..., \alpha_m$, slijedi da je $\sum_{j=1}^{n} \delta_{i_j}\beta_j = 0, 1 \leq i \leq m$. Kako su elementi $\beta_1, ..., \beta_n$ linearno nezavisni nad K, zaključujemo da su svi $\delta_{i_j} = 0, 1 \leq i \leq m, 1 \leq j \leq n$. □

Teorem 4.12. Svako konačno proširenje polja K je algebarsko nad K.

Dokaz. Neka je L konačno proširenje polja K, $[L : K] = m$ i $\theta \in L$. Tada je $m + 1$ elemenata $1, \theta, ..., \theta^m$ polja L linearno zavisno nad K, tako da vrijedi jednadžba $a_0 + a_1\theta + ... + a_m\theta^m = 0$, gdje su $a_i \in K$ i $a_i \neq 0$ za bar jedan $0 \leq i \leq m$. Dakle, θ je algebarski element nad K. □

Definicija 4.13. Neka polinom $f \in K[x]$ ima pozitivan stupanj i neka je F neko proširenje polja K. Tada kažemo da je polinom f **u potpunosti rastavljiv** u polju F, ako polinom f možemo zapisati u obliku produkta linearnih faktora iz $F[x]$, tj. postoje $\alpha_1, ..., \alpha_n \in F$ takvi da vrijedi $f(x) = a(x-\alpha_1)...(x-\alpha_n)$, gdje je a vodeći koeficijent polinoma f. Polje F je **polje razlaganja** polinoma f nad poljem K, ako je f u potpunosti rastavljiv u polju F.

Polje razlaganja F polinoma f nad poljem K je najmanje od polja koje istovremeno sadrže K i sve korijene polinoma f.

Teorem 4.14. (Postojanje i jedinstvenost polja razlaganja) Ako je K neko polje i f polinom pozitivnog stupnja iz $K[x]$, tada postoji polje razlaganja polinoma f nad K. Bilo koja dva polja razlaganja polinoma f nad poljem K su izomorfna, pri čemu izomorfizam fiksira polje K i preslikava korijene od f jedan u drugog.

Sada želimo pokazati jednu jednostavnu, neizbježnu tvrdnju o broju elemenata konačnog polja.

Lema 4.15. Neka je F konačno polje koje sadrži potpolje K sa q elemenata. Tada F ima q^m elemenata, gdje je $m = [F : K]$ stupanj polja F nad njegovim potpoljem K.

Dokaz. Polje F možemo shvatiti kao vektorski prostor nad poljem K. Kako je F konačno polje, slijedi da je F, kao vektori prostor, konačne dimenzije. Ako je $[F : K] = m$, tada F ima bazu nad poljem K sastavljenu od m elemenata; $b_1, ..., b_m$. Dakle, svaki element polja F možemo jednoznačno prikazati kao linearnu kombinaciju $a_1b_1 + ... + a_mb_m$, gdje su $a_1, ..., a_m \in K$. Budući da svaki koeficijent a_i može poprimiti točno q vrijednosti, $i = 1, ..., m$, polje F se sastoji od točno q^m elemenata. □

Teorem 4.16. Neka je F konačno polje. Tada se F sastoji od p^n elemenata, gdje je prost broj p karakteristika polja F, a prirodni broj n stupanj polja F nad njegovim prostim potpoljem.

Dokaz. Prema teoremu 4.6, prosto potpolje K polja F izomorfno je polju F_p, pa sadrži p elemenata. Budući da je $n = [F : K]$ iz leme 4.15 slijedi da se polje F sastoji od p^n elemenata. □

Lema 4.17. Ako je F konačno polje od q elemenata, tada za svaki element $a \in F$ vrijedi

$$a^q = a.$$

Dokaz. Za $a = 0$ jednakost $a^q = a$ trivijalno vrijedi. Elementi polja F, različiti od 0 čine grupu reda $q - 1$, tako da za svaki element $a \in F$, $a \neq 0$ vrijedi jednakost $a^{q-1} = 1$. Pomnožimo li obe strane te jednakosti s a dobit ćemo traženu jednakost. □

Lema 4.18. Ako je F konačno polje od q elemenata i K potpolje polja F, tada je polinom $x^q - x$ iz $K[x]$ u potpunosti rastavljiv u $F[x]$ na sljedeći način:

$$x^q - x = \prod_{a \in F} (x - a).$$

Dakle, F je polje razlaganja polinoma $x^q - x$ nad poljem K.

Dokaz. Polinom $x^q - x$ stupnja q ima najviše q različitih korijena u polju F. Prema lemi 4.17 svi elementi polja F su korijeni tog polinoma. Dakle, ima ih točno q. Iz toga slijedi da dani polinom ne može biti u potpunosti rastavljiv ni u jednom manjem polju. □

Sada ćemo dokazati osnovni teorem za konačna polja, čija je osnovna ideja sadržana u lemi 4.18. Iz teorema neposredno slijedi da za svaki prirodni broj n postoji ireducibilni polinom stupnja n iz $F_p[x]$. Prije teorema ćemo definirati i dokazati pomoćne tvrdnje.

Definicija 4.19. Derivacija polinoma $f(x) = a_0 + a_1x + ... + a_nx^n \in F[x]$ je polinom $f'(x) = a_1 + 2a_2x... + na_nx^{n-1} \in F[x]$.

Teorem 4.20. Korijen $b \in F$ polinoma $f \in F[x]$ je višestruki, ako i samo je istovremeno i korijen derivacije polinoma f.

Dokaz. Pretpostavimo da je k kratnost korijena $b \in F$ polinoma $f \in F[x]$. Tada polinom $(x - b)^k$ dijeli polinom f, tj. postoji polinom $g \in F[g]$ takav da je $f(x) = g(x)(x - b)^k$. Derivacija polinoma $f(x)$ je

$$f'(x) = g(x)k(x - b)^{k-1} + (x - b)^k g'(x).$$

Dakle, $f'(x)$ je djeljivo s $(x-b)^{k-1}$. Ako je korijen b višestruki, tada je $k > 1$, pa je b i korijen derivacije. Obrnuto, ako je b korijen derivacije onda $(x-b)^m$ dijeli polinom $f'(x)$, za $m \geq 1$, pa slijedi da k mora biti veće od 1, tj. b je višestruki korijen. □

Teorem 4.21. (Egzistencija i jedinstvenost konačnih polja) Za svaki prosti broj p i svaki prirodni broj n postoji konačno polje sa p^n elemenata. Bilo koje konačno polje sa $q = p^n$ elemenata izomorfno je polju razlaganja polinoma $x^q - x$ nad poljem $\mathbb{F}_p$.

Dokaz. (Egzistencija) Za $q = p^n$ promatramo polinom $x^q - x \in F_p[x]$. Neka je F polje razlaganja tog polinoma nad $\mathbb{F}_p$. Dani polinom ima q različitih korijena, jer je njegova derivacija $qx^{q-1} - 1 = -1$ iz $\mathbb{F}_p[x]$ i zbog toga ne može imati isti korijen kao $x^q - x$ (teorem 4.20). Neka je $S = \{a \in F \mid a^q - a = 0\}$. S je potpolje polja F jer vrijedi:

(i) S sadrži 0 i 1.

(ii) Ako su $a, b \in S$, tada vrijedi $(a-b)^q = a^q - b^q = a - b$, pa je $a - b \in S$.

(iii) Za $a, b \in S$, $b \neq 0$ vrijedi: $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$, pa je $ab^{-1} \in S$.

S druge strane $x^q - x$ je potpuno rastavljiv u S, jer S sadrži sve njegove korijene. To znači da je $S = F$, a budući se skup S sastoji od q elemenata, F je konačno polje od q elemenata.

(Jedinstvenost) Pretpostavimo da je F konačno polje od $q = p^n$ elemenata. Tada iz teorema 4.16 vidimo da F ima karakteristiku p, pa prema tome sadrži polje $\mathbb{F}_p$ kao svoje potpolje. Iz leme 4.18 slijedi da je F polje razlaganja polinoma $x^q - x$ nad poljem $\mathbb{F}_p$. Jedinstvenost sada slijedi iz jedinstvenosti polja razlaganja. □

Za prim potenciju $q = p^n$, polje reda q označavat ćemo $\mathbb{F}_q$. Oznaka ima smisla jer po prethodnom teoremu takvo polje postoji i jedinstveno je do na izomorfizam.

5 Wedderburnov teorem

Prije nego iskažemo i dokažemo Wedderburnov teorem, želimo opisati nekoliko pojmova i iskazati potrebne pomoćne tvrdnje (bez dokaza) koje ćemo koristiti. Svi dokazi mogu se naći u drugom poglavlju knjige [3] navedenoj u literaturi. Neka je D tijelo i F njegovo komutativno podtijelo (F ćemo nazivati potpoljem od D). Tada D možemo promatrati kao vektorski prostor nad poljem F. Ako je $F = \mathbb{F}_q$ i D je konačne dimenzije n nad $\mathbb{F}_q$, tada D ima q^n elemenata. Pisat ćemo D^* za multiplikativnu grupu elemenata različitih od nule.

Lema 5.1. Neka je $f \in \mathbb{F}_q[x]$ ireducibilan polinom nad konačnim poljem $\mathbb{F}_q$ i neka je α korijen tog polinoma u nekom proširenju polja $\mathbb{F}_q$. Tada za polinom $h \in \mathbb{F}_q[x]$ vrijedi jednakost $h(\alpha) = 0$ ako i samo ako polinom f dijeli polinom h.

Dokaz. Neka je a vodeći koeficijent polinoma f. Definiramo $g(x) = a^{-1}f(x)$. Tada je g normiran ireducibilan polinom iz $\mathbb{F}_q[x]$ takav da je $g(\alpha) = 0$. Dakle, g je minimalni polinom elementa α nad $\mathbb{F}_q$, pa g dijeli svaki polinom $h \in \mathbb{F}_q[x]$ za koji je $h(\alpha) = 0$. Time smo dokazali tvrdnju. □

Definicija 5.2. Za prirodan broj n, polje razlaganja polinoma $x^n - 1$ nad proizvoljnim poljem K je **n-to polje ciklotomije** nad K. Oznaka koju koristimo je $K^{(n)}$. Korijeni polinoma $x^n - 1$ iz polja $K^{(n)}$ su **n-ti korijeni jedinice nad K**. Skup tih korijena označavamo $E^{(n)}$.

Neka je K polje karakteristike p i $n \in \mathbb{N}$ broj koji nije djeljiv s p. Tada je $E^{(n)}$ ciklička grupa obzirom na množenje u $K^{(n)}$, a njezine izvodnice zovemo **primitivnim n-tim korijenima jedinice** nad poljem K.

Definicija 5.3. Neka je K polje karakteristike p, $n \in \mathbb{N}$ koji nije djeljiv s p i ξ primitivni n-ti korijen jedinice nad K. Tada je polinom

$$Q_n(x) = \prod_{s=\{1,\dots n\}, M(s,n)=1} (x - \xi^s)$$

n-ti ciklotomski polinom nad poljem K.

Polinom $Q_n(x)$ ne ovisi o izboru elemenata ξ. Njegov stupanj jednak je $\varphi(n)$, a njegovi koeficijenti pripadaju n-tom polju ciklotomije nad K. Pritom je $\varphi(n)$ Eulerova funkcija. To je polinom kojem su nultočke svi primitivni n-ti korijeni jedinice nad K.

Teorem 5.4. Neka je K polje karakteristike p i n prirodan broj koji nije djeljiv s p. Tada:

(i) $x^n - 1 = \prod_{d/n} Q_d(x)$ (produkt po svim djeliteljima d prirodnog broja n)

(ii) Koeficijenti n-tog ciklotomskog polinoma Q_n pripadaju prostom potpolju polja K (ako je p prost broj) ili prstenu $\mathbb{Z}$ (ako je $p = 0$).

Lema 5.5. Neka je d djelitelj prirodnog broja n, $1 \leq d < n$. Tada n-ti ciklotomski polinom $Q_n(x)$, definiran nad promatranim poljem, dijeli polinom $(x^n - 1)/(x^d - 1)$.

Definicija 5.6. Neka je G proizvoljna grupa, a $A \subseteq G$ neki skup, onda **normalizator** od A definiramo kao

$$N_G(A) = \{x \in G \mid x^{-1}Ax = A\}.$$

Teorem 5.7. Za bilo koji neprazni podskup S grupe G, normalizator $N(S)$ je podgrupa grupe G. Posebno, postoji bijekcija između lijevih klasa grupe G modulo $N(S)$ i različitih skupova aSa^{-1} konjugiranih sa S.

Gledajući sve elemente proizvoljne grupe s fiksnim elementom a, dobijemo skup koji zovemo **klasa konjugiranih elemenata s elementom a** ili **klasa konjugiranosti** promatrane grupe koja sadrži element a.

Definicija 5.8. Za proizvoljnu grupu G definiramo njen **centar** kao skup

$$C = \{c \in G \mid ac = ca, \forall a \in G\}.$$

Za elemente centra pripadajuće klase konjugiranosti sastoje se od jedinstvenog elementa. Grupa G je Abelova ako i samo ako je $C = G$. To nas dovodi do sljedećeg važnog rezultata.

Teorem 5.9. Neka je G konačna grupa s centrom C. Tada vrijedi jednakost

$$\mid G \mid = \mid C \mid + \sum_{i=1}^{k} n_i,$$

gdje je svaki $n_i \geq 2$, $1 \leq i \leq k$, djelitelj reda $\mid G \mid$, grupe G. Svi, $n_1, n_2, ..., n_k$ su kardinalni brojevi različitih klasa konjugiranosti grupe G, koje sadrže više od jednog elementa.

Teorem 5.10. (Wedderburnov teorem) Svako konačno tijelo je polje.

Dokaz. Neka je D konačno tijelo i $Z = \{z \in D \mid zd = dz, d \in D\}$ njegov **centar**. Lako je provjeriti da je Z polje. Vrijedi $Z = \mathbb{F}_q$ za neku prim potenciju q. Budući da je tijelo D vektorski prostor nad Z, konačne dimenzije n, D se sastoji od q^n elemenata. Dokazat ćemo da je $D = Z$, tj. da je $n = 1$.

Pretpostavimo suprotno, tj. da je $n > 1$. Neka je $a \in D$ i definiramo $N_a = \{b \in D \mid ab = ba\}$. Tada je N_a tijelo koje sadrži Z i prema tome ima q^r elemenata, gdje je $1 \leq r \leq n$. Želimo pokazati da broj r dijeli n. Kako je N_a^* podgrupa grupe D^*, broj $q^r - 1$ dijeli $q^n - 1$. Ako je $n = rm + t$, $0 \leq t < r$, tada je $q^n - 1 = q^{rm}q^t - 1 = q^t(q^{rm} - 1) + (q^t - 1)$. Budući da broj $q^r - 1$ dijeli i $q^n - 1$ i $q^{rm} - 1$, onda dijeli i $q^t - 1$. Međutim, $q^t - 1 < q^r - 1$, pa je $t = 0$. Iz toga zaključujemo da r dijeli n. Centar od D^* je Z^* reda $q - 1$. Ako je $a \in D^*$, tada je N_a^* normalizator elementa a u grupi D^*. Sada vidimo da se bilo koja klasa konjugiranosti grupe D^* koja sadrži više od jednog elementa, sastoji od $(q^n - 1)/(q^r - 1)$ elemenata, gdje je r neki djelitelj broja n, $1 \leq r < n$. Dakle jednadžba klasa konjugiranosti izgleda ovako

$$q^n - 1 = q - 1 + \sum_{i=1}^{k} \frac{q^n - 1}{q^{r_i} - 1}, \tag{7}$$

gdje su $r_1, ..., r_k$ (ne nužno različiti) pravi djelitelji broja n, $1 \leq r_i < n$ za $1 \leq i \leq k$.

Pogledajmo sada n-ti ciklotomski polinom Q_n nad poljem racionalnih brojeva. $Q_n(q)$ je cijeli broj (prema teoremu 5.4). Štoviše lema 5.5 kaže da $Q_n(q)$ dijeli $(q^n - 1)/(q^{r_i} - 1)$, za $1 \leq i \leq k$. Sada iz (7) dobijemo da broj $Q_n(q)$ dijeli $q - 1$, a to dovodi do kontradikcije. Po definiciji, imamo

$$Q_n(x) = \prod_{1 \leq s \leq n, gcd(s,n)=1} (x - \xi^s),$$

gdje je kompleksni broj ξ primitivni n-ti korijen iz jedinice nad poljem racionalnih brojeva. Gledajući modul kompleksnog broja

$$\mid Q_n(q) \mid = \prod_{1 \leq s \leq n, gcd(s,n)=1} \mid q - \xi^s \mid > \prod_{1 \leq s \leq n, gcd(s,n)=1} (q - 1) \geq q - 1,$$

gdje je $n > 1$ i $q \geq 2$. Ta nejednakost je nespojiva s tvrdnjom da $Q_n(q)$ dijeli $q - 1$. To povlači da je $n = 1$, tj. $D = Z$. □

Literatura

[1] J. Cameron, Combinatorics: Topics, Techniques, Algorithms, Cambridge University Press, 1994.

[2] T.W.Hungerford, Algebra, Springer, 2000.

[3] R. Lidl, H. Niederreiter, Finite fields, Cambridge University Press, 2003.

[4] Širola, Algebarske strukture, skripta, PMF-Matematički odsjek, 2009. Dostupno na:

https://web.math.pmf.unizg.hr/nastava/alg/predavanja/ASpred.pdf

Sažetak

U ovom diplomskom radu izneseni su osnovni pojmovi i teoremi vezani za konačna polja. Na samom početku definirani su prsteni, kao jedni od osnovnih algebarskih struktura, i sve vezano uz njih, uključujući polja. Objašnjeno je što su to prsteni polinoma i kvocijentni prsteni koji su bili potrebni za konstrukciju konačnih polja. Primjerima je pokazano na koji način možemo konstruirati konačno polje bilo kojeg reda oblika p^n, s pomoću ireducibilnog polinoma stupnja n nad $\mathbb{F}_p$. Koristeći pojam polja razlaganja dokazali smo egzistenciju i jedinstvenost konačnog polja reda p^n. Osim toga dokazali smo Wedderburnov teorem, za koji smo definirali ciklotomijske polinome.

Summary

In this thesis we present the main concepts and results which we need to define finite fields. At the beginning we define rings, as one of the fundamental algebraic structures and everything related to them, including fields. We define polynomials and residue class rings, which are required for the construction of finite fields. In examples we show how to construct a finite field of any order p^n from a irreducible polynomial of degree n over $\mathbb{F}_p$. Using the concept of splitting field, we prove the existence and uniqueness of the field of order p^n. In addition, we prove Wedderburn's theorem for which we define cyclotomic polynomials.

Životopis

Rođena sam 31.10.1992. godine u Dubrovniku. Nakon osnovne škole, koju sam pohađala od 2000. godine u Neumu, 2008. godine upisala sam Matematičku gimnaziju u Metkoviću. Godine 2011. započinjem studiranje na preddiplomskom sveučilišnom studiju Matematike na PMF-u. Nakon stjecanja diplome za sveučilišnu prvostupnicu, 2014. godine upisala sam diplomski sveučilišni studij Matematike, smjer Financijska i poslovna matematika. Za to vrijeme školovanja položila sam tri stupnja na Govorničkoj školi, kao i četiri semestra Hrvatskog znakovnog jezika.