Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Tena Tomičević

Polja i prsteni

Završni rad

Osijek, 2016.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Tena Tomičević

Polja i prsteni

Završni rad

mentor: izv. prof. dr. sc. Ivan Matić

Osijek, 2016.

Sažetak. Glavna ideja ovog završnog rada je upoznavanje s algebarskim strukturama prstenima i poljima. Upoznat ćemo najvažnija svojstva binarnih operacija tih struktura i najbitnije definicije. Kako bi svojstva i definicije bile što razumljivije, navedeni su i neki primjeri prstena i polja. Opisano je i računanje pomoću Karatsubinog algoritma što uvelike skraćuje posao u računanju s velikim brojevima.

Ključne riječi: Prsteni, polja, Karatsubin algoritam

Abstract. The main idea of this Final Paper is introducing algebraic structures: rings and fields. We are going to introduce the most important properties of binary operations and main definitions. For better understanding of these properties and definitions, there are some examples of rings and fields set out. It is also described calculation by Karatsuba algorithm which makes work quicker when we calculate with large numbers.

Keywords: Rings, fields, Karatsuba multiplication

Sadržaj

1. Uvod

Algebra je jedna od fundamentalnih grana matematike. Jedna od mogućih definicija bila bi da je to nauka o algebarskim operacijama, odnosno proučavanje algebarskih struktura. Pritom priroda samih elemenata skupa na kojemu se izvode spomenute algebarske operacije nije od primarne važnosti već je primarni cilj proučavanje tih algebarskih operacija. Algebarske strukture možemo podijeliti na tri cjeline: grupe, prstene i polja.
U ovom radu naglasak će biti na prstene i polja. Cilj rada je prikazati pojmovno određenje prstena i polja, njihove najvažnije karakteristike, te primjere takvih struktura.
Osim navedenog dotaknut ćemo se i nekih posljedica aksioma vezanih uz operacije u komutativnom prstenu.

2. Prsteni

Za početak promotrimo jedan primjer.

Primjer 2.1 *Pretpostavimo da želimo naći neki cijeli broj x kako bi riješili sljedeću jednadžbu:*

$$(3 + x) + 4 = 9.$$

U rješenju jednadžbe se koriste različita svojstva jednakosti, primjerice: ako je $a = b$, tada je i $b = a$ (simetričnost), ako je $a = b$ i $b = c$ onda je $a = c$ (tranzitivnost) i ako je $a = b$, onda je $a + c = b + c$.
Za rješavanje jednadžbe prvo se koristi svojstvo komutativnosti, odnosno pišemo:

$$3 + x = x + 3,$$

te se broj 4 dodaje na obje strane i dobivamo:

$$(3 + x) + 4 = (x + 3) + 4.$$

Korištenjem svojstva asocijativnosti slijedi:

$$(x + 3) + 4 = x + (3 + 4) = x + 7.$$

Korištenjem svojstva tranzitivnosti dobivamo izraz:

$$(3 + x) + 4 = x + 7.$$

Simetričnost i tranzitivnost jednakosti nam daju:

$$x + 7 = 9.$$

Zatim dodamo -7 na obje strane:

$$(x + 7) + (-7) = 9 + (-7) = 2.$$

Korištenjem svojstva asocijativnosti imamo:

$$(x + 7) + (-7) = x + (7 + (-7)).$$

S obzirom da je $7 + (-7) = 0$ prijenosom jednakosti dobivamo:

$$(x + 7) + -7 = x + 0.$$

I na kraju ponovnim sumiranjem jednakosti i korištenjem svojstva simetričnosti, konačan rezultat je:

$$x = 2.$$

Za ovako pomalo mukotrpno rješavanje ove jednadžbe korišteni su cijeli brojevi i njihova svojstva: svojstvo da je zbroj dvaju cijelih brojeva cijeli broj, svojstva komutativnosti, asocijativnosti i tranzitivnosti. Primjetimo da svi cijeli brojevi imaju svoje inverze obzirom na operaciju zbrajanja a neutralni element je 0. Skup cijelih brojeva $\mathbb{Z}$ s navedenom operacijom zbrajanja i spomenutim svojstvima naziva se Abelova ili komutativna grupa.

Za razliku od grupa gdje postoji samo jedna binarna operacija, kod prstena imamo dvije. Imajući na umu prsten $(\mathbb{Z},+,*)$ kao prvi pravi i osnovni primjer, binarne operacije su zbrajanje i množenje. Preciznije, zapišimo sljedeću definiciju:

Definicija 2.1 *Za neprazan skup R na kome su zadane binarne operacije zbrajanja $+\colon R \times R \to R$ i množenja $*\colon R \times R \to R$ sa svojstvima:*

- *$(R,+)$ je komutativna (Abelova) grupa, sa neutralnim elementom* 0
- *$(R,*)$ je polugrupa, tj. množenje je asocijativno*
- *vrijedi distributivnost množenja prema zbrajanju, odnosno*

$$x * (y + z) = x * y + x * z$$
$$(x + y) * z = x * z + y * z, \ \forall x,\ y,\ z \in R,$$

kažemo da je prsten i označavamo ga s: $R = (R,+,*)$.

2.1. Karakteristike prstena

Ako je množenje u prstenu R komutativno, R nazivamo *komutativni prsten.*
U suprotnom govorimo o nekomutativnom prstenu.
Kažemo da je R *prsten s jedinicom* ili *unitalni prsten* ako postoji element $1 \in R$ takav da je $1 * a = a * 1 = a$, $\forall a \in R$.
Element 1 s tim svojstvom je jedinstven i naziva se *jedinica prstena* R.
Ako imamo situaciju da je jedinica prstena jednaka nuli tog prstena, tada se taj prsten naziva *trivijalan prsten.*
Vrlo važan pojam vezan uz komutativan prsten je integralna domena. No prvo definirajmo djelitelj nule u prstenu.

Definicija 2.2 *Kažemo da je element $a \in R$ $(a \neq 0)$ djelitelj nule ako postoji $b \in R$, $(b \neq 0)$ takav da je $a * b = 0$.*

Definicija 2.3 *Kažemo da je komutativan unitalan prsten R $(R \neq \{0\})$ integralna domena ako R nema djelitelja nule.*

Definicija 2.4 *Za skup S koji je podskup prstena R $(S \neq \{\emptyset\})$ kažemo da je potprsten prstena R ako je S i sam prsten uz iste operacije, pri čemu za proizvoljne $a, b \in S$ vrijedi:*

- $(a - b) \in S$
- $(a * b) \in S$.

Inače, pri istraživanju algebarskih struktura često se može naići na pojmove *homomorfizma* i *izomorfizma* pa ih je prirodno ovdje definirati iako se ovom prilikom nećemo baviti njihovim proučavanjem.

Definicija 2.5 *Za preslikavanje $\varphi\colon R \to S$ kažemo da je homomorfizam prstenova R i S ako vrijedi:*

- $\varphi(a + b) = \varphi(a) + \varphi(b)$
- $\varphi(a * b) = \varphi(a) * \varphi(b)$, $\forall a, b \in R$.

Ako je preslikavanje φ homomorfizam i bijekcija, onda se takvo preslikavanje naziva *izomorfizam* prstena R i S i pišemo $R \cong S$.

Elementarna svojstva prstena dana su sljedećim teoremom.

Teorem 2.1 *Neka je R prsten. Tada $\forall a, b, c \in R$ vrijedi:*

$$a * 0 = 0 * a = 0 \tag{1}$$

$$a * (-b) = -(a * b) = (-a) * b \tag{2}$$

$$a * (b - c) = a * b - a * c, (a - b) * c = a * c - b * c. \tag{3}$$

Dokaz: (1) Iz distributivnosti množenja prema zbrajanju slijedi:

$$a * 0 = a * (0 + 0) = a * 0 + a * 0$$

što prema definiciji neutralnog elementa implicira $a * 0 = 0$. Slično se pokazuje da je

$$0 * a = 0.$$

(2) Distributivnost množenja daje:

$$0 = a * 0 = a * (b + (-b)) = a * b + a * (-b)$$

pa iz definicije inverznog elementa slijedi $a * (-b) = -(a * b)$. Slično se pokazuje da je

$$-(a * b) = (-a) * b.$$

(3) Koristeći svojstvo (iz dokaza (2)) dobivamo:

$$0 = a * (b - c) = a * (b + (-c)) = a * b + a * (-c) = a * b - a * c$$

i slično: $(a - b) * c = (a + (-b)) * c = a * c + (-b) * c = a * c - b * c.$ □

Navedimo neke primjere prstena:

- *Neka je (R,+) Abelova grupa. Ako na R definiramo množenje s* $a * b = 0$ $\forall a,\ b \in R$*, tada dobivamo trivijalni prsten.*
- *Standardni primjeri prstena s jedinicom su skupovi brojeva* $\mathbb{Q}$, $\mathbb{R}$ *i* $\mathbb{C}$ *sa standardnim operacijama zbrajanja i množenja.*
- *Neka je* $M_n(F)$ *skup kvadratnih matrica reda n nad* $F = \mathbb{R}$ *ili* $\mathbb{C}$*.* $M_n(F)$ *je prsten s operacijama matričnog zbrajanja i množenja. Nula u prstenu je nul matrica, a jedinica je jedinična matrica.*

I navedimo neke primjere koji nisu prsteni:

- *Skup prirodnih brojeva* $\mathbb{N}$ *s uobičajenim operacijama zbrajanja i množenja.*
- *Skup svih nenegativnih realnih brojeva* $\mathbb{R}_+$ *s uobičajenim operacijama zbrajanja i množenja.*
- *Skup* $\mathbb{Z}\backslash\{3\}$ *s uobičajenim operacijama zbrajanja i množenja.*

2.2. Komutativni prsteni i Karatsubin algoritam

Prema Knjizi 2 Euklidovih Elemenata primjenom zakona distributivnosti za elemente A i B proizvoljnog komutativnog prstena prstena dobivamo jednakost:

$$A^2 - B^2 = (A + B)(A - B).$$

Sada ćemo provesti pomalo mukotrpan postupak, ali iz razloga što ćemo gornji izraz dokazati pomoću svojstava komutativnog prstena.

$$\begin{aligned}
(A+B)(A-B) &= (A+B)(A+(-B)) \\
&= A(A+(-B)) + B(A+(-B)) \text{ (zakon distributivnosti)} \\
&= (A^2 + A(-B)) + (BA + B(-B)) \text{ (zakon distributivnosti)} \\
&= (A^2 + (-(AB))) + (BA + (-(B^2))) \text{ (Teorem 2.1.)} \\
&= (A^2 + (-AB))) + (AB + (-(B^2))) \text{ (komutativnost množenja)} \\
&= (A^2 + (-AB + AB)) + (-(B^2)) \text{ (asocijativnost)} \\
&= (A^2 - 0) - B^2 \text{ (definicija neutralnog elementa)} \\
&= A^2 - B^2 \text{ (definicija nule).}
\end{aligned}$$

Tablicom 1. je prikazano uobičajeno množenje:

	a_1 b_1	a_0 b_0
 a_1b_1	a_1b_0 a_0b_1	a_0b_0
a_1b_1	$a_0b_1 + a_1b_0$	a_0b_0

Tablica 1.

Primjenjujući zakon distributivnosti tri puta (u prva dva reda dokaza), dobivamo isto kao da primjenjujemo način množenja koji se još naziva $FOIL$ (First, Outside, Inside, Last). Kako bi pomnožili izraz $(1+2)\cdot(3+4)$ prema $FOIL$-u prvo množimo 1 i 3, zatim vanjske brojeve 1 i 4, nakon toga unutarnje 2 i 3 te na kraju ostaju još brojevi 2 i 4, a onda sve sumiramo i krajnji rezultat nam izgleda ovako: $3+4+6+8=21$. Jednostavna posljedica takvog načina množenja je sljedeća propozicija:

Propozicija 2.1 *Za sve elemente komutativnog prstena a_0, a_1, b_0, b_1 vrijedi jednakost:*

$$a_1 \cdot b_0 + a_0 \cdot b_1 = (a_1 \cdot b_1 + a_0 \cdot b_0) - (a_1 - a_0) \cdot (b_1 - b_0).$$

Posljedicu ove propozicije otkrio je Anatolij Aleksejević Karatsuba još 1960. ali objavio ju je dvije godine nakon otkrića. Obratimo pozornost na standardni algoritam za množenje prikazan u Tablici 1.

Uobičajeno je korišten zakon distributivnosti, asocijativnost zbrajanja, te komutativnost zbrajanja i množenja što uključuje množenje znamenaka četiri puta:
$a_1 \cdot b_1$, $a_0 \cdot b_1$, $a_1 \cdot b_0$ i $a_0 \cdot b_0$.

Algoritam:

$$\begin{aligned}(a_1r + a_0)(b_1r + b_0) &= (a_1b_1r_2 + a_1b_0r) + (a_0b_1r + a_0b_0)\\ &= a_1b_1r_2 + a_1b_0r + a_0b_1r + a_0b_0\\ &= a_1b_1r_2 + (a_1b_0 + a_0b_1)r + a_0b_0.\end{aligned}$$

Propozicija 2.1. nam upravo govori da središnji izraz iz Tablice 1. $a_0b_1 + a_1b_0$ možemo zamijeniti izrazom $(a_1b_1 + a_0b - 0) - (a_1 - a_0)(b_1 - b_0)$. Sada naš algoritam izgleda nešto drugačije pa pogledajmo Tablicu 2.

Algoritam:

$$\begin{aligned}(a_1r + a_0)(b_1r + b_0) &= a_1b_1r_2 + (a_1b_0 + a_0b_1)r + a_0b_0)\\ &= a_1b_1r_2 + (a_1b_1r + a_0b_0r - (a_1 - a_0)(b_1 - b_0)r) + a_0b_0\\ &= (a_0b_0r + a_0b_0) + (a_1b_1r_2 + a_1b_1r) - (a_1 - a_0)(b_1 - b_0)r.\end{aligned}$$

	a_1 b_1	a_0 b_0
a_1b_1	a_0b_0 a_1b_1 $-(a_1 - a_0)(b_1 - b_0)$	a_0b_0
a_1b_1	$a_0b_1 + a_1b_0$	a_0b_0

Tablica 2.

Ovaj način množenja opisuje se algoritmom i naziva Karatsuba-Ofman algoritam. Upravo on se koristi za brzo množenje brojeva. Karatsuba je došao do zaključka da je za računanje produkta dva dvoznamenkasta broja dovoljno samo tri množenja znamenaka, za razliku od standardnih četiri.

$$a_0 \cdot b_0$$
$$a_1 \cdot b_1$$
$$(a_1 - a_0) \cdot (b_1 - b_0)$$

što je brže i kraće nego:

$$a_0 \cdot b_0$$
$$a_1 \cdot b_1$$
$$a_1 \cdot b_0$$
$$a_0 \cdot b_1.$$

Moć ovog algoritma se očituje u tome da je on vrlo efikasan za velike brojeve. Kako bi zbrojili dva četveroznamenkasta broja (zapisana u dekadskoj bazi) napišemo ih u obliku: $a_1 \cdot 10^2 + a_0$ i $b_1 \cdot 10^2 + b_0$.
Zatim koristeći Karatsubino množenje imamo:

$$(a_1 \cdot 10^2 + a_0) \cdot (b_1 \cdot 10^2 + b_0) = (a_1 \cdot b_1 \cdot 10^4 + (a_1 \cdot b_1 + a_0 \cdot b_0 - (a_1 - a_0) \cdot (b_1 - b_0)) \cdot 10^2 + a_0 \cdot b_0$$

što uključuje množenje dvoznamenkastih brojeva 3 puta, a množenje pojedine znamenke se ponavlja još tri puta pa sveukupno imamo 9 množenja svake znamenke. Standardno množenje bi zahtijevalo 16 množenja iz čega je vidljiva ranije spomenuta efikasnost. U praksi se za brojeve s manje znamenki koristi uobičajeni algoritam, a za brojeve s više znamenki Karatsubin.

3. Polja

Analogno kao u prošlom poglavlju započet ćemo primjerom.

Primjer 3.1 *Sada nas u sustavu racionalnih brojeva $\mathbb{Q}$ zanima rješenje jednadžbe:*

$$(3x+1)\cdot\frac{2}{5}=7.$$

U rješavanju ćemo koristiti svojstva kao i u jednadžbi iz poglavlja Prsteni:

$$\begin{aligned}(3x+1)\cdot\frac{2}{5} &= (3x)\cdot\frac{2}{5}+1\cdot\frac{2}{5} \text{ (distributivnost)}\\ &= (3x)\cdot\frac{2}{5}+\frac{2}{5} \text{ (1 je neutralan element za množenje)}\\ &= 3\cdot\left(x\cdot\frac{2}{5}\right)+\frac{2}{5} \text{ (asocijativnost)}\\ &= 3\cdot\left(\frac{2}{5}\cdot x\right)+\frac{2}{5} \text{ (komutativnost)}\\ &= \left(3\cdot\frac{2}{5}\right)\cdot x+\frac{2}{5} \text{ (asocijativnost)}\\ &= \frac{6}{5}\cdot x+\frac{2}{5}\,.\end{aligned}$$

Simetrijom i prijenosom jednakosti izvorna jednadžba je

$$\frac{6}{5}\cdot x+\frac{2}{5}=7.$$

Potom na obje strane se dodaje $-\frac{2}{5}$ i s desne strane dobivamo:

$$7+\left(-\frac{2}{5}\right)=\frac{33}{5}.$$

Odnosno

$$\begin{aligned}\left(\frac{6}{5}\cdot x+\frac{2}{5}\right)-\frac{2}{5} &= \frac{6}{5}\cdot x+\left(\frac{2}{5}+\left(-\frac{2}{5}\right)\right) \text{ (asocijativnost)}\\ &= \frac{6}{5}\cdot x+0\\ &= \frac{6}{5}\cdot x.\end{aligned}$$

Zatim se dobiva jednadžba:

$$\frac{6}{5}\cdot x=\frac{33}{5}.$$

Metodom asocijativnosti slijedi:

$$\left(\frac{5}{6}\cdot\frac{6}{5}\right)\cdot x=1\cdot x=x\Rightarrow x=\frac{5}{6}\cdot\frac{33}{5}=\frac{33}{6}.$$

U navedenoj jednadžbi korištena su svojstva:

- *distributivnost množenja*
- *komutativnost množenja*
- *1 je neutralan element za množenje*
- *svaki racionalan broj osim nula ima svoj inverz.*

Uz navedena svojstva i dvije binarne operacije (zbrajanje i množenje) skup racionalnih brojeva $\mathbb{Q}$ je polje. Kako bismo bolje razumjeli definiciju polja prisjetimo se što su to invertibilni elementi.

Definicija 3.1 *U komutativnom prstenu R za element $a \in R$ kažemo da je invertibilan ako postoji element $b \in R$ takav da vrijedi: $a \cdot b = b \cdot a = 1$.*

Skup svih invertibilnih elemenata nekog prstena R označavamo sa R^*. Primjerice $\mathbb{Z}^* = \{1, -1\}$ i $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.

Definicija 3.2 *Kažemo da je prsten R tijelo, ili prsten s dijeljenjem, ako je svaki element različit od nule u R invertibilan.*

Komutativno tijelo naziva se *polje*.

Definicija 3.3 *Kažemo da je F polje, ako je F komutativni prsten koji zadovoljava dodatna dva svojstva:*

1. *Svaki nenul element iz F je invertibilan*
2. *F ima barem dva elementa (netrivijalno polje).*

3.1. Karakteristike polja i primjeri

Eksplicitno, polje je definirano svojstvom zatvorenosti na zbrajanje i množenje, pri čemu su zbrajanje i množenje asocijativne i komutativne binarne operacije te vrijedi distributivnost množenja prema zbrajanju.
Također, postoji i neutralan element za zbrajanje, to je nula, te neutralan element za množenje, to je jedan. Osim neutralnog elementa, postoji i inverzni element za zbrajanje i množenje. Uvjet da je nula različito od jedan osigurava da skup koji sadrži samo jedan element nije polje.
Navedimo neke osnovne primjere:

- *Polje racionalnih brojeva* $\mathbb{Q}$.
- *Polje realnih brojeva* $\mathbb{R}$.
- *Polje kompleksnih brojeva* $\mathbb{C}$.

Promotrimo skup $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$. $\mathbb{Z}_p$ je prsten uz operacije zbrajanja i množenja modulo p.
Pokažimo na primjeru kako su definirane operacije u prstenu $\mathbb{Z}_p$.

Primjer 3.2 *Neka je naš* $p = 5$. $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

$$2 +_5 4 = 6 \pmod 5 = 1.$$

$$2 \cdot_5 4 = 8 \pmod 5 = 3.$$

U polju nam je $\mathbb{Z}_p \setminus \{0\} = (\mathbb{Z}_p)^*$. Prsten $\mathbb{Z}_p$ je polje ako i samo ako je p prirodan prost broj. Primijetimo da je $\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$.
Za prstene ostataka modulo n vrijedi: $\mathbb{Z}/n\mathbb{Z}$ je polje ako je $\mathbb{Z}/n\mathbb{Z}$ integralna domena ako i samo ako je n prost prirodan broj. Ta činjenica je zapravo samo specijalan slučaj općenitog fenomena koji govori da je svaka konačna integralna domena polje. Taj se rezultat dokazuje u dva koraka. Prvi je vrlo jednostavan i govori da je svaka konačna integralna domena tijelo. Drugi korak, koji je dosta kompliciraniji, predmet je tzv. Wedderburnovog teorema koji kaže da je svako konačno tijelo štoviše i polje, odnosno čim imamo konačnost imamo i komutativnost.

4. ZAKLJUČAK

Polje je algebarska struktura u kojoj se izvode operacije zbrajanja, oduzimanja, množenja i dijeljenja (osim dijeljenja s nulom) i gdje vrijede pravila iz aritmetike.
Sva polja predstavljaju i prstene, ali nisu svi prsteni polja. Glavna razlika je što je operacija dijeljenja u polju moguća te operacija množenja uvijek komutativna.
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 $\mathbb{C}$.
Osnovna podjela prstena je na komutativne i nekomutativne. Naime, isto kao i kod grupa, u pravilu je proučavanje strukture nekomutativnih prstena puno kompliciranije nego kod onih koji su komutativni.
Karatsuba algoritam je primjer algoritma koji uvelike skraćuje broj i vrijeme izvođenja operacija množenja te je izuzetno efikasan za velike brojeve.

5. LITERATURA

[1] N.L. Childs: A Concrete Introduction to Higher Algebra, Third Edition, Springer, 2000.

[2] C.K. Koc: High-Speed RSA Implementation , TR 201, RSA Laboratories, 1994.

[3] H. Kraljević: Algebra, Odjel za matematiku, Sveučilište Josipa Jurja Strossmayera u Osijeku, 2007.

[4] S. Krešić-Jurić: Algebarske strukture, Skripta, PMF - Odjel za matematiku, Sveučilište u Splitu, 2013.

[5] B. Širola: Algebarske sturkture, predavanja, PMF - Matematički odsjek, Sveučilište u Zagrebu, 2008.