

UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET

Zoran Stojaković

Đura Paunić

ZADACI IZ ALGEBRE

GRUPE, PRSTENI, POLJA

Novi Sad

1998

Naziv udžbenika: "ZADACI IZ ALGEBRE - grupe, prsteni, polja"

Autori: Dr Zoran Stojaković, redovni profesor Prirodno-matematičkog
fakulteta u Novom Sadu
Dr Đura Paunić, redovni profesor Prirodno-matematičkog
fakulteta u Novom Sadu

Recenzenti: Dr Ratko Tošić, redovni profesor Prirodno-matematičkog
fakulteta u Novom Sadu
Dr Biljana Janeva, vanredni profesor Prirodno-matematičkog
fakulteta u Skoplju

Izdavač: Univerzitet u Novom Sadu
Prirodno-matematički fakultet u Novom Sadu

Glavni i odgovorni urednik pojedinačnog izdanja: Dr Ištvan Bikit, dekan
Prirodno-matematičkog fakulteta u Novom Sadu

Štampa: "S PRINT", Novi Sad, Bulevar Vojvode Stepe 133, Tel: 021/401-974

Štampano u 500 primeraka

Ova publikacija je sufinansirana sredstvima Ministarstva prosvete Republike Srbije

CIP - Каталогизација у публикацији
Библиотека Матице српске. Нови Сад

512 (076.58)

СТОЈАКОВИЋ, Зоран

Zadaci iz algebre - grupe, prsteni, polja / Zoran Stojaković.
Đura Paunić.- Novi Sad: Univerzitet: Prirodno-matematički
fakultet, 1998 (Novi Sad: S print).- 279 str.; 24 cm.- (Edicija
"Univerzitetski udžbenik"; 60)

Tiraž 500.- Bibliografija: str. 277-279.

ISBN 86-499-0011-9

1. Паунић, Ђура
а) Алгебра - Задачи

0

Tel./faks za porudžbine: (021) 350-371

Sadržaj

Predgovor	3
I GRUPE	5
1.1 Pregled definicija i teorema	5
1.2 Primeri i aksiomatika	19
1.3 Osnovne osobine	47
1.4 Homomorfizam, izomorfizam	55
1.5 Cikličke i Ablove grupe	65
1.6 Grupe permutacija	73
1.7 Podgrupe, normalne podgrupe i faktor grupe	81
1.8 Direktan proizvod grupa	99
1.9 Komutatori, rešive grupe	103
1.10 Teoreme Silova	115
1.11 Automorfizmi grupa	123
II PRSTENI	129
2.1 Pregled definicija i teorema	129
2.2 Primeri i aksiomatika	142
2.3 Osnovne osobine	152
2.4 Ideali i homomorfizmi	174
2.5 Maksimalni i prosti ideali	189
2.6 Prsten polinoma	198
2.7 Simetrični polinomi	216

III POLJA	223
3.1 Pregled definicija i teorema	223
3.2 Primeri i osnovne osobine	231
3.3 Proširenja polja	238
3.4 Teorija Galoa	258
 Pregled oznaka	 275
 Literatura	 276

Predgovor

Ova zbirka primera, zadataka i problema je namenjena studentima matematike, ali može biti od koristi i studentima drugih fakulteta, pre svega tehničkih, inženjerima, fizičarima, hemičarima i svim onima koji žele da se upoznaju sa teorijom grupa, prstena i polja.

Knjiga je podeljena u tri dela. U prvom delu je obrađena teorija grupa, u drugom teorija prstena i u trećem teorija polja. Na početku svakog dela je naveden pregled teorije, definicije i teoreme čije poznavanje potrebno za rešavanje zadataka koji slede. Većina zadataka je rešena, za neke su data uputstva, a jedan deo zadataka je ostavljen čitaocu za samostalno rešavanje. Autori su nastojali da se izborom i redosledom zadataka ostvari postupnost u izlaganju materije. U zbirku je u uključen i izvestan broj zadataka iz matematičkih časopisa i uz takve zadatke navedena je literatura koja čitaocu omogućuje da se detaljnije upozna sa pojedinim problemima.

Autori se zahvaljuju recenzentima dr Ratku Tošiću i dr Biljani Janevoj, kao i dr J. Ušanui koji su pregledali rukopis i dali niz korisnih sugestija i primedbi.

Novi Sad,
10. februar 1998.

Autori

I

GRUPE

1.1 Pregled definicija i teorema

1.1. Funkcija $f : S \times S \rightarrow S$, gde je S neprazan skup, naziva se binarna operacija na skupu S .

Dakle, binarna operacija f definisana na skupu S pridružuje svakom uređenom paru elemenata iz S jedan element iz S . Da uređenom paru (a, b) odgovara element c zapisujemo sa $f(a, b) = c$ ili $a f b = c$.

Često se ovako definisana binarna operacija naziva unutrašnja binarna operacija (za razliku od spoljašnje binarne operacije koja se definiše kao preslikavanje $g : S \times T \rightarrow R$, gde su S, T i R neprazni skupovi).

1.2. Ako je n prirodan broj, S neprazan skup i $S^n = \underbrace{S \times \dots \times S}_{n \text{ puta}}$, onda se funkcija $f : S^n \rightarrow S$ naziva n -arna operacija na skupu S . Broj n naziva se dužina ili arnost operacije f . n -arna operacija se za $n = 1$ naziva unarna, a za $n = 3$ ternarna (za $n = 2$ dobija se ranije definisana binarna operacija).

1.3. Ako je S skup na kome je definisana binarna operacija $*$, a T podskup od S takav da za svako $a, b \in T$

$$a * b \in T,$$

onda kažemo da je skup T zatvoren u odnosu na operaciju $*$.

1.4. Ako je na skupu G definisana binarna operacija $*$, onda se uređen

par $(G, *)$ naziva grupoid. Kaže se, takođe, da je G grupoid u odnosu na operaciju $*$.

Često ćemo, kada se podrazumeva o kojoj je operaciji reč, govoriti samo „grupoid G ” (umesto „grupoid $(G, *)$ ”).

1.5. Binarna operacija $*$ definisana na skupu G je asocijativna ako i samo ako je za svako $a, b, c \in G$

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

Operacija $*$ naziva se komutativna ako i samo ako je za svako $a, b \in G$

$$a * b = b * a.$$

1.6. Grupoid $(G, *)$ naziva se polugrupa ako i samo ako je $*$ asocijativna operacija.

1.7. Ako je $(G, *)$ grupoid i postoji element $e \in G$ takav da za svako $a \in G$ važi

$$a * e = e * a = a,$$

onda se e naziva neutralni (ili jedinični) element grupoida $(G, *)$.

Ako je element $e' \in G$ takav da za svako $a \in G$ važi

$$a * e' = a,$$

onda se e' naziva desni neutralni element, a ako je element $e'' \in G$ takav da za svako $a \in G$ važi

$$e'' * a = a,$$

onda se e'' naziva levi neutralni element grupoida $(G, *)$.

1.8. Grupoid $(G, *)$ u kome za svako $a, b \in G$ jednačine

$$a * x = b, \quad y * a = b,$$

imaju jedinstveno rešenje po x i y u G , naziva se kvazigrupa.

Kvazigrupa sa neutralnim elementom naziva se lupa.

1.9. Grupoid $(G, *)$ se naziva grupa ako i samo ako važe sledeći aksiomi:

G1. Za svako $a, b, c \in G$

$$a * (b * c) = (a * b) * c,$$

(operacija je asocijativna).

G2. Postoji element $e \in G$ tako da je za svako $a \in G$

$$e * a = a,$$

(postoji levi neutralni element).

G3. Za svako $a \in G$ postoji element $a^{-1} \in G$ tako da je

$$a^{-1} * a = e,$$

(svaki element a ima levi inverzni element a^{-1}).

1.10. Sa definicijom 1.9 je ekvivalentna definicija grupe koja se dobija iz 1.9 na sledeći način: u G2 se zahteva egzistencija desnog neutralnog elementa (umesto levog), u G3 se zahteva egzistencija desnog inverznog elementa (umesto levog), a sve ostalo u 1.9 ostaje neizmenjeno.

1.11. Grupa $(G, *)$ u kojoj je operacija $*$ komutativna naziva se komutativna grupa ili Abelova grupa.

1.12. Ako je $(G, \cdot)$ grupa (definicija 1.9), onda važi (pri tom, kada operaciju označavamo znakom $\cdot$ pišaćemo često umesto $a \cdot b$ skraćeno ab) :

a) Ako je e levi neutralni element, onda je e i desni neutralni element, tj. e je neutralni element.

b) Neutralni element je jedinstven.

c) Ako je a^{-1} levi inverzni element elementa a , onda je a^{-1} i desni inverzni element elementa a (dakle, a^{-1} je inverzni element za a).

d) Svaki element grupe ima jedinstven inverzni element.

e) Za svako $a \in G$

$$(a^{-1})^{-1} = a.$$

f) Za svako $a, b \in G$,

$$(ab)^{-1} = b^{-1}a^{-1}.$$

g) Za svako $a, b, c \in G$

$$ac = bc \Rightarrow a = b \quad \text{i} \quad ca = cb \Rightarrow a = b,$$

(važe zakoni desne i leve kancelacije (skraćivanja)).

h) Za svako $a, b \in G$ jednačine

$$ax = b \quad \text{i} \quad ya = b$$

imaju jedinstveno rešenje po x i y u G .

1.13. Red grupe G je kardinalni broj skupa G i označavamo ga sa $|G|$. Ako je $|G|$ konačan broj grupa se naziva konačna.

Sa $|S|$ označavaćemo i kardinalni broj proizvoljnog podskupa S grupe G .

1.14. Red elementa a grupe G je najmanji prirodan broj n za koji je $a^n = e$, ako takvo n postoji. Ako takav prirodan broj ne postoji, a je beskonačnog reda. Red elementa a označavaćemo sa $|a|$.

1.15. Ako je $(G, \cdot)$ grupa, podskup H grupe G naziva se podgrupa grupe G ako i samo ako je H grupa u odnosu na restrikciju operacije $\cdot$ na H .

U grupi G skup koji sadrži samo jedinični element $\{e\}$ i sama grupa G su podgrupe i te podgrupe nazivaju se trivijalne. Ostale podgrupe nazivaju se netrivijalne.

Podgrupe grupe G različite od G nazivaju se prave.

1.16. Neprazan podskup H grupe G je podgrupa ako i samo ako za svako $x, y \in H$, $xy^{-1} \in H$.

1.17. Konačan neprazan podskup H grupe G je podgrupa ako i samo ako za svako $x, y \in H$, $xy \in H$.

1.18. Homomorfizam grupe $(G_1, *)$ u grupu $(G_2, \cdot)$ je preslikavanje f skupa G_1 u skup G_2 za koje za svako $x, y \in G_1$ važi

$$f(x * y) = f(x) \cdot f(y).$$

Jezgro homomorfizma f je skup svih elemenata iz G_1 koji se preslikavaju u neutralni element e_2 grupe G_2 . Jezgro homomorfizma f označavaćemo sa $\text{Ker } f$, dakle,

$$\text{Ker } f = \{x \mid x \in G_1 \text{ i } f(x) = e_2\}.$$

Sa $\text{Im } f$ (ili sa $f(G_1)$) označavaćemo skup

$$\text{Im } f = f(G_1) = \{y \mid y \in G_2 \text{ i } (\exists x \in G_1) f(x) = y\}$$

i taj skup nazivamo slika homomorfizma f .

Ako je f surjektivno preslikavanje (tj. $f(G_1) = G_2$), G_2 se naziva homomorfna slika grupe G_1 . U tom slučaju homomorfizam se naziva epimorfizam.

Homomorfizam koji je injektivno preslikavanje naziva se monomorfizam.

Ako postoji monomorfizam grupe G_1 u grupu G_2 , kažemo da se G_1 može potopiti u G_2 .

1.19. Homomorfizam koji je epimorfizam i monomorfizam (tj. bijekcija) naziva se izomorfizam. Grupa G_1 je izomorfna grupi G_2 ako i samo ako postoji izomorfizam $f : G_1 \rightarrow G_2$. Da je grupa G_1 izomorfna grupi G_2 označavaćemo sa $G_1 \cong G_2$.

1.20. Homomorfizam kojim se grupa G preslikava u sebe naziva se endomorfizam, a izomorfizam grupe G u sebe naziva se automorfizam.

1.21. Neka je a element grupe G . Tada je skup $A = \{a^n \mid n \in \mathbb{Z}\}$ podgrupa grupe G . A je najmanja podgrupa koja sadrži a .

Pri tome, a^n je definisano na sledeći način. Ako je n prirodan broj, $a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ puta}}$, $a^{-n} = (a^{-1})^n$, a^0 je neutralni element grupe G .

1.22. Ako u grupi G postoji element $a \in G$ takav da je $G = \{a^n \mid n \in \mathbb{Z}\}$, onda se G naziva ciklička grupa (generisana elementom a), a a se naziva generator grupe G . Da je grupa G generisana sa a označavaćemo sa $G = \langle a \rangle$.

1.23. Neka je G ciklička grupa generisana elementom a .

Ako je G grupa konačnog reda n , onda je a^k generator grupe G ako i samo ako su k i n uzajamno prosti brojevi.

Ako je G beskonačna grupa, onda su a i a^{-1} jedini generatori grupe G .

1.24. Konačne cikličke grupe istog reda su izomorfne. Svake dve beskonačne cikličke grupe su izomorfne. Cikličku grupu reda n označavaćemo sa C_n .

1.25. Svaka podgrupa cikličke grupe je ciklička.

1.26. Ako je S neprazan podskup grupe G , minimalna podgrupa grupe G koja sadrži S se označava sa $\langle S \rangle$ i naziva podgrupa generisana skupom S . Kada je $S = \{a_1, a_2, \dots, a_n\}$ tada $\langle S \rangle$ označavamo sa $\langle a_1, a_2, \dots, a_n \rangle$. Elementi skupa S se nazivaju generatori grupe $\langle S \rangle$.

$\langle S \rangle$ je presek svih podgrupa koje sadrže S .

1.27. Grupa G je generisana nepraznim skupom S ako i samo ako se svaki element grupe G može prikazati u obliku proizvoda

$$a_1^{k_1} a_2^{k_2} \dots a_m^{k_m}, \quad m \in \mathbb{N}, \quad a_1, a_2, \dots, a_m \in S, \quad k_1, k_2, \dots, k_m \in \mathbb{Z}$$

konačnog broja stepena elementa iz S .

1.28. Ako u grupi G postoji konačan skup S tako da je $G = \langle S \rangle$, grupa G se naziva konačno generisana grupa.

1.29. Skup generatora grupe se naziva nezavisan ako i samo ako se ni jedan element tog skupa ne može prikazati kao proizvod konačnog broja stepena sa celim eksponentima ostalih elemenata.

Skup generatora S je nezavisan ako i samo ako za svako $x \in S$, x ne pripada grupi generisanoj skupom $S \setminus \{x\}$.

1.30. Svako bijektivno preslikavanje nepraznog skupa S na S naziva se permutacija skupa S .

1.31. Skup svih permutacija nepraznog skupa S je grupa u odnosu na množenje (kompoziciju) preslikavanja.

1.32. Grupa G se naziva grupa permutacija ako i samo ako je G podgrupa grupe svih permutacija nekog skupa S .

1.33. Grupa svih permutacija skupa $\{1, 2, \dots, n\}$ se naziva simetrična grupa stepena n i označava sa S_n . Ta grupa ima $n!$ elemenata.

Permutaciju $p \in S_n$ definisanu sa $p(k) = i_k$, $k \in \{1, 2, \dots, n\}$ označavamo sa $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ ili sa $[i_1 \ i_2 \ \dots \ i_n]$.

1.34. (Kejli (Cayley)) Svaka grupa G je izomorfna sa nekom grupom permutacija skupa G .

Svaka konačna grupa reda n je izomorfna sa nekom podgrupom grupe S_n .

1.35. Permutacija $p \in S_n$ se naziva ciklus dužine k ($k \leq n$) ako i samo ako je

$$p(a_1) = a_2, \quad p(a_2) = a_3, \quad \dots, \quad p(a_{k-1}) = a_k, \quad p(a_k) = a_1,$$

gde su $a_1, a_2, \dots, a_k$ različiti elementi skupa $\{1, 2, \dots, n\}$, a ostale elemente permutacija p ostavlja neizmenjene ($p(x) = x$, $x \neq a_i$, $i = 1, 2, \dots, k$).

Ciklus p ćemo označavati simbolom

$$p = (a_1 a_2 \dots a_k)$$

1.36. Ciklus dužine 2 nazivamo transpozicija, a ciklus dužine 3 tercet.

1.37. Ciklusi $(a_1 a_2 \dots a_k), (b_1 b_2 \dots b_l) \in S_n$ se nazivaju disjunktni ako i samo ako je

$$\{a_1, a_2, \dots, a_k\} \cap \{b_1, b_2, \dots, b_l\} = \emptyset.$$

1.38. Svaka permutacija grupe S_n može se prikazati kao proizvod disjunktnih ciklusa.

1.39. Skup svih transpozicija generiše grupu S_n .

1.40. Permutacija grupe S_n se naziva parna ako i samo ako se može prikazati kao proizvod parnog broja transpozicija, a u suprotnom permutacija se naziva neparna.

Skup A_n svih parnih permutacija grupe S_n je podgrupa (normalna, v. 1.56) grupe S_n . Grupa A_n ima $\frac{n!}{2}$ elemenata i naziva se alternativna grupa stepena n .

1.41. Matrica formata $n \times n$ se naziva permutaciona matrica ako i samo ako je dobijena od jedinične matrice permutovanjem njenih vrsta.

1.42. Ako je P_n skup svih permutacionih matrica formata $n \times n$, onda je P_n grupa u odnosu na množenje matrica.

1.43. Preslikavanje $\phi : S_n \rightarrow P_n$ definisano sa $\phi : q \mapsto A_q$ gde je A_q matrica dobijena od jedinične matrice permutovanjem njenih vrsta onako kako to propisuje permutacija q , je izomorfizam grupe S_n na grupu P_n .

1.44. Na osnovu Kejljeve teoreme (1.34) i 1.43, sledi da je svaka konačna grupa reda n izomorfna sa nekom podgrupom grupe P_n svih permutacionih matrica formata $n \times n$.

1.45. Neka su A i B neprazni podskupovi grupe G . Proizvod AB definisan je sa

$$AB = \{ab \mid a \in A, b \in B\}.$$

1.46. Neka je H podgrupa grupe G i $a \in G$. Skup $aH = \{ah \mid h \in H\}$ naziva se levi suskup (ili koset) podgrupe H , a skup $Ha = \{ha \mid h \in H\}$ je desni suskup (ili koset) podgrupe H .

Element a nazivamo predstavnikom suskupova aH , odnosno Ha .

1.47. Neka je H podgrupa grupe G , a aH levi suskup podgrupe H . Ako je $g \in aH$, onda je $aH = gH$, tj. svaki element suskupa aH može da bude predstavnik tog suskupa. Analogno tvrđenje važi i za desne suskupove.

1.48. Neka je H podgrupa grupe G i neka su aH i bH dva leva suskupa podgrupe H . Tada se aH i bH ili poklapaju ili su disjunktni, tj. skup levih suskupova je particija skupa G . Analogno tvrđenje važi za desne suskupove.

1.49. Ako je H podgrupa grupe G , onda je za svako $a \in G$

$$|H| = |aH| = |Ha|.$$

1.50. (Lagranž (Lagrange)). Ako je H podgrupa konačne grupe G , onda je red podgrupe H delitelj reda grupe G .

1.51. Red elementa konačne grupe je delitelj reda grupe.

1.52. Grupa reda p , gde je p prost broj, je ciklička grupa i ta grupa nema pravih podgrupa.

1.53. Ako je H podgrupa grupe G , onda je preslikavanje $f : aH \mapsto Ha$ bijekcija između skupa svih levih i skupa svih desnih suskupova podgrupe H . Dakle, broj levih suskupova jednak je broju desnih suskupova podgrupe H . Ako je taj broj konačan on se naziva indeks podgrupe H u grupi G (ili indeks grupe G po podgrupi H) i označava se sa $[G : H]$.

Ako je G beskonačna grupa, a H njena podgrupa takva da je skup svih levih suskupova podgrupe H beskonačan (tada je beskonačan i skup svih desnih suskupova), onda kažemo da je H beskonačnog indeksa u G .

1.54. Ako je G konačna grupa, a H njena podgrupa, onda je $|G| = |H| \cdot [G : H]$.

1.55. Neka su H i K konačne podgrupe grupe G . Tada važi

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

1.56. Podgrupa H grupe G je normalna podgrupa grupe G ako i samo ako za svako $x \in G$

$$xHx^{-1} = H.$$

Da je H normalna podgrupa grupe G označavaćemo sa $H \triangleleft G$.

1.57. Ako je H podgrupa grupe G , onda su sledeća tvrđenja ekvivalentna:

- (i) H je normalna podgrupa grupe G .
- (ii) $xH = Hx$, za svako $x \in G$.
- (iii) Svaki levi suskup podgrupe H je i desni suskup podgrupe H .
- (iv) $xHx^{-1} \subseteq H$, za svako $x \in G$.

1.58. Presek proizvoljne familije normalnih podgrupa grupe G je normalna podgrupa grupe G .

1.59. U grupi G element $a \in G$ je konjugovan sa elementom $b \in G$ ako i samo ako postoji $c \in G$ tako da je

$$a = c b c^{-1}.$$

Konjugovanost elemenata grupe je relacija ekvivalencije.

1.60. Ako je H podgrupa grupe G , a $x \in G$, onda je xHx^{-1} takođe podgrupa grupe G . Podgrupa xHx^{-1} se naziva podgrupa konjugovana sa H .

1.61. Neka je H podgrupa grupe G , $x \in G$. Podgrupa xHx^{-1} je izomorfna sa H , a preslikavanje $f : a \mapsto xax^{-1}$ je izomorfizam grupa H i xHx^{-1} .

1.62. Podgrupa H grupe G je normalna podgrupa u G ako i samo ako se H poklapa sa svim svojim konjugovanim podgrupama.

1.63. Neka je H normalna podgrupa grupe G . Ako se na skupu svih suskupova podgrupe H definiše binarna operacija sa

$$(aH) \cdot (bH) = (ab)H,$$

onda taj skup suskupova u odnosu na ovako definisanu operaciju čini grupu. Ta grupa se naziva faktor grupa grupe G po podgrupi H , označava se sa G/H i njen red je $[G : H]$.

1.64. (Prva teorema o izomorfizmu). Neka je $f : G \rightarrow H$ homomorfizam grupe G u grupu H . Tada je jezgro $\text{Ker} f$ normalna podgrupa grupe G , $f(G)$ je podgrupa grupe H i

$$G/\text{Ker} f \cong f(G).$$

(Svaka homomorfna slika grupe G je izomorfna sa faktor grupom grupe G .)

1.65. Neka je H normalna podgrupa grupe G . Tada je preslikavanje $\pi : G \rightarrow G/H$ definisano sa $\pi : g \mapsto gH$ homomorfizam grupe G na faktor grupu G/H čije je jezgro H . π se naziva prirodni (ili kanonički) homomorfizam grupe G na faktor grupu G/H .

1.66. Neka je $f : G_1 \rightarrow G_2$ epimorfizam grupe G_1 na grupu G_2 i neka je H_2 podgrupa grupe G_2 . Tada je skup H_1 svih elemenata iz G_1 čije su slike elementi iz H_2 podgrupa grupe G_1 koja sadrži $\text{Ker } f$. Ako je $H_2 \triangleleft G_2$, onda je i $H_1 \triangleleft G_1$.

1.67. (Teorema o korespondenciji). Neka je H normalna podgrupa grupe G i neka je preslikavanje $\pi : G \rightarrow G/H$ definisano sa $\pi : g \mapsto gH$. π je prirodni homomorfizam grupe G na grupu G/H . Neka je f funkcija definisana na skupu svih podgrupa grupe G koje sadrže H , određena na sledeći način:

$$f : K \mapsto \pi(K).$$

Funkcija f je bijekcija skupa svih podgrupa grupe G koje sadrže H i skupa svih podgrupa faktor grupe G/H .

Ako je N skup svih normalnih podgrupa grupe G koje sadrže H , onda je restrikcija f na N bijekcija skupa N i skupa svih normalnih podgrupa faktor grupe G/H .

1.68. (Druga teorema o izomorfizmu) Neka je H podgrupa, a K normalna podgrupa grupe G . Tada je $H \cap K \triangleleft H$, HK je podgrupa grupe G i

$$(HK)/K \cong H/(H \cap K).$$

1.69. (Treća teorema o izomorfizmu) Neka je G grupa, $H \triangleleft G$, $K \triangleleft G$ i K podgrupa grupe H . Tada je $H/K \triangleleft G/K$ i

$$(G/K)/(H/K) \cong G/H.$$

1.70. Neka su $(G_1, \cdot)$ i $(G_2, *)$ grupe. Skup

$$G_1 \times G_2 = \{(a_1, a_2) \mid a_1 \in G_1, a_2 \in G_2\}$$

u odnosu na binarnu operaciju $\circ$ definisanu sa

$$(a_1, a_2) \circ (b_1, b_2) = (a_1 \cdot b_1, a_2 * b_2),$$

je grupa koja se naziva direktan proizvod grupa G_1 i G_2 . U daljem ćemo, kad god su G_1 i G_2 grupe, sa $G_1 \times G_2$ označavati ovu grupu.

Analogno se definiše direktan proizvod proizvoljnog konačnog broja grupa.

1.71. Ako su A i B grupe, grupa $G = A \times B$ sadrži podgrupu $A_1 = \{(a, e_B) \mid a \in A\}$ koja je izomorfna sa A i sadrži podgrupu $B_1 = \{(e_A, b) \mid b \in B\}$ koja je izomorfna sa B , gde su e_A i e_B neutralni elementi grupa A i B respektivno. Svaki element grupe G se može na jedinstven način prikazati kao proizvod jednog elementa iz A_1 i jednog iz B_1 i taj proizvod komutira. Takođe je

$$G/A_1 \cong B \quad \text{i} \quad G/B_1 \cong A.$$

(Za elemente $a, b \in G$ kažemo da komutiraju ako i samo ako je $ab = ba$.)

1.72. Neka su G, H i K grupe. Tada je

$$(G \times H) \times K \cong G \times (H \times K) \cong G \times H \times K.$$

1.73. Ako su A i B normalne podgrupe grupe G takve da je $AB = G$ i $A \cap B = \{e\}$, onda je

$$G \cong A \times B.$$

Ako su $H_1, H_2, \dots, H_k$ normalne podgrupe grupe G takve da je

(i) $G = H_1 H_2 \dots H_k$,

(ii) za svako $i \in \{1, 2, \dots, k\}$, $H_i \cap H_1 \dots H_{i-1} H_{i+1} \dots H_k = \{e\}$,

onda je $G \cong H_1 \times H_2 \times \dots \times H_k$.

1.74. Centar $\mathcal{Z}(G)$ grupe G je skup svih elemenata koji komutiraju sa svakim elementom grupe G , tj.

$$\mathcal{Z}(G) = \{x \mid x \in G \wedge (\forall a \in G) xa = ax\}.$$

Centar $\mathcal{Z}(G)$ je normalna podgrupa grupe G .

1.75. Ako je A neprazan podskup grupe G , onda je centralizator $\mathcal{C}(A)$ skupa A skup svih elemenata iz G koji komutiraju sa svakim elementom iz A , tj.

$$\mathcal{C}(A) = \{x \mid x \in G \wedge (\forall a \in A) xa = ax\}.$$

Centralizator $\mathcal{C}(A)$ je podgrupa grupe G .

1.76. Normalizator nepraznog podskupa A grupe G je skup

$$\mathcal{N}(A) = \{x \mid x \in G, \quad xA = Ax\}.$$

Normalizator $\mathcal{N}(A)$ je podgrupa grupe G .

1.77. Ako je H podgrupa grupe G , onda je normalizator $\mathcal{N}(H)$ maksimalna podgrupa grupe G u kojoj je H normalna podgrupa.

1.78. Podgrupa H grupe G je normalna ako i samo ako je $\mathcal{N}(H) = G$.

1.79. Broj elemenata konjugovanih sa elementom a u grupi G jednak je $[G : \mathcal{N}(a)]$.

1.80. Broj različitih podgrupa konjugovanih s podgrupom H grupe G je $[G : \mathcal{N}(H)]$.

1.81. Ako je G grupa, $x, y \in G$, onda se $xyx^{-1}y^{-1}$ naziva komutator uređenog para elemenata x, y . Komutator elemenata x i y označavaćemo sa $[x, y]$.

1.82. Podgrupa grupe G generisana skupom svih komutatora naziva se izvod (ili komutatorska podgrupa ili izvodna podgrupa) grupe G . Izvod grupe G označavaćemo sa G' . (Dakle, izvod je podgrupa generisana skupom komutatora, a ne skup svih komutatora. Moguće je da neki element grupe bude jednak proizvodu komutatora, a da sam ne bude komutator.)

1.83. U grupi G izvod G' je normalna podgrupa.

1.84. Drugi izvod G'' grupe G je izvod izvoda G' . n -ti izvod $G^{(n)}$ grupe G je izvod $(n-1)$ -og izvoda $G^{(n-1)}$, $n = 2, 3, \dots$.

1.85. Normalna podgrupa H grupe G je maksimalna normalna podgrupa ako i samo ako ne postoji prava normalna podgrupa grupe G različita od H , koja sadrži H .

1.86. Grupa G se naziva prosta ako i samo ako G nema netrivialne normalne podgrupe.

1.87. Normalna podgrupa H grupe G je maksimalna normalna podgrupa ako i samo ako je faktor grupa G/H prosta.

1.88. Kompozicioni niz grupe G je konačan niz

$$G, H_1, H_2, \dots, H_k = \{e\}$$

različitih podgrupa grupe G u kome je svaki član niza maksimalna normalna podgrupa prethodnog člana.

1.89. Ako je $G, H_1, H_2, \dots, H_k = \{e\}$ kompozicioni niz grupe G , onda se niz

$$G/H_1, H_1/H_2, \dots, H_{k-1}/H_k$$

naziva kompozicioni niz faktor grupa grupe G .

Kompozicioni niz indeksa grupe G je niz

$$m_1, m_2, \dots, m_k$$

gde je m_i red i -te po redu faktor grupe iz kompozicionog niza faktor grupa grupe G .

1.90. Dva kompoziciona niza grupe G nazivaju se izomornim ako i samo ako se faktor grupe jednog niza mogu bijektivno preslikati na faktor grupe drugog niza, tako da odgovarajuće faktor grupe budu izomorfne.

1.91. (Žordan-Helder (Jordan-Hölder)) Svaka dva kompoziciona niza grupe G su izomorfna.

1.92. Grupa G se naziva rešiva ako i samo ako se njen n -ti izvod $G^{(n)}$, za neki konačan broj n , sastoji samo od neutralnog elementa.

1.93. Konačna grupa G je rešiva ako i samo ako je njen kompozicioni niz faktor grupa niz cikličkih grupa prostog reda (tj. njen kompozicioni niz indeksa je niz prostih brojeva).

1.94. Svaka komutativna grupa je rešiva.

1.95. Svaka konačna grupa neparnog reda je rešiva¹.

1.96. Ako je p prost broj, grupa G se naziva p -grupa ako i samo ako je red svakog elementa grupe G neki stepen broja p .

1.97. (Koši(Cauchy)) Ako je G konačna grupa čiji je red deljiv prostim brojem p , onda G sadrži element reda p .

1.98. Konačna grupa G je p -grupa ako i samo ako je red grupe G stepen broja p .

1.99. Svaka konačno generisana Abelova grupa je izomorfna direktnom proizvodu cikličkih grupa, a svaka od tih cikličkih grupa je ili beskonačna ili

¹Ovo tvrđenje, kojim se daje potvrđan odgovor na dugi niz godina nedokazanu hipotezu Bernsajda (Burnside), dokazali su Feit (Feith) i Thompson (Thompson) 1963.g. Njihov dokaz, veoma dubok i neelementaran, objavljen je na 255 strana u radu:

Feith, W., Thompson J.G. *Solvability of Groups of Odd Order*, Pacific Journal of Mathematics, Vol. 13 (1963), 775-1029.

je njen red stepen prostog broja.

Specijalno, svaka konačna Abelova grupa je izomorfna direktnom proizvodu konačnih cikličkih grupa.

1.100. Neka su G i H Abelove grupe reda p^n , p prost broj, i neka je $G = A_1 \times \dots \times A_k$, pri čemu je svaki činilac A_i ciklička grupa reda p^{g_i} , $g_1 \geq \dots \geq g_k > 0$, a $H = B_1 \times \dots \times B_s$, pri čemu je svaki činilac B_i ciklička grupa reda p^{h_i} , $h_1 \geq \dots \geq h_s > 0$. Tada su G i H izomorfne grupe ako i samo ako je $k = s$ i za svako i $g_i = h_i$.

1.101. Ako je G konačna Abelova grupa reda n , onda u G postoji podgrupa reda m za svaki pozitivan broj m koji je delitelj n .

1.102. Neka je p prost broj. Podgrupa P grupe G se naziva p -podgrupa Silova grupe G ako i samo ako je P maksimalna p -podgrupa grupe G .

1.103. (Prva teorema Silova (Sylow)) Neka je G grupa reda $p^n q$, gde je p prost broj uzajamno prost sa q , $n \in \mathbb{N}$. Tada G sadrži podgrupu reda p^i za svako $i \in \{1, 2, \dots, n\}$ i svaka podgrupa grupe G reda p^i ($i < n$) je normalna u nekoj podgrupi reda p^{i+1} .

1.104. Ako u grupi G postoji tačno jedna p -podgrupa Silova, onda je ta podgrupa normalna podgrupa grupe G .

1.105. Ako je G grupa reda n , onda su p -podgrupe Silova reda p^r , gde je p^r najveći stepen p koji je delitelj n .

1.106. (Druga teorema Silova) Svake dve p -podgrupe Silova grupe G su konjugovane. Ukupan broj p -podgrupa Silova je $[G : \mathcal{N}(P)]$, gde je P bilo koja p -podgrupa Silova.

1.107. (Treća teorema Silova) Broj različitih p -podgrupa Silova konačne grupe G je $1 + kp$, gde je k nenegativan ceo broj, a $1 + kp$ je delitelj reda grupe G .

1.108. Neka je G grupa i $a \in G$. Preslikavanje $f : G \rightarrow G$ definisano sa

$$f(x) = axa^{-1}, \quad \text{za svako } x \in G,$$

je automorfizam grupe G . f se naziva unutrašnji automorfizam određen elementom a .

1.109. Automorfizam grupe koji nije unutrašnji naziva se spoljašnji automorfizam.

1.110. Skup $\mathcal{A}(G)$ svih automorfizama grupe G je grupa u odnosu

na kompoziciju preslikavanja. Skup $\mathcal{U}(G)$ svih unutrašnjih automorfizama grupe G je normalna podgrupa grupe $\mathcal{A}(G)$.

$\mathcal{A}(G)$ se naziva grupa automorfizama grupe G , a $\mathcal{U}(G)$ se naziva grupa unutrašnjih automorfizama grupe G .

1.111. Grupa $\mathcal{U}(G)$ unutrašnjih automorfizama grupe G je izomorfna faktor grupi grupe G po centru $\mathcal{Z}(G)$,

$$\mathcal{U}(G) \cong G/\mathcal{Z}(G).$$

1.2 Primeri i aksiomatika

1. Ispitati da li sledeći skupovi čine grupe u odnosu na odgovarajuće operacije (operacije $+$, $-$, $\cdot$, $:$ su uobičajene operacije sabiranja, oduzimanja, množenja i deljenja).

- a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$,
- b) $(S, +)$, gde je $S = \{-5, -4, \dots, 4, 5\}$,
- c) $(\mathbb{Z}, -)$,
- d) $(\mathbb{Q}, \cdot)$,
- e) $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$,
- f) $(\mathbb{Q}^+, *)$, gde je $a * b = b : a$,
- g) $(\mathbb{Q}^+, \cdot)$, $(\mathbb{R}^+, \cdot)$.

Rešenje. a) $(\mathbb{Z}, +)$ je grupa jer zadovoljava aksiome navedene u definiciji 1.9. Zaista,

– zbir dva cela broja je ceo broj (dakle, $+$ je binarna operacija definisana na $\mathbb{Z}$),

- asocijativnost važi za sabiranje celih brojeva (G1),
- $0 \in \mathbb{Z}$ je levi neutralni element: $0 + a = a$, za svako $a \in \mathbb{Z}$ (G2),
- za svako $a \in \mathbb{Z}$ postoji $-a \in \mathbb{Z}$ tako da je $(-a) + a = 0$ (G3).

Sabiranje celih brojeva je komutativno, pa je $(\mathbb{Z}, +)$ Abelova grupa.

Slično se pokazuje da su i $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ i $(\mathbb{C}, +)$ Abelove grupe.

b) U ovom slučaju $+$ nije binarna operacija na S , pa $(S, +)$ nije grupa

(sabiranje jeste binarna operacija na skupu $\mathbb{Z}$ svih celih brojeva, ali skup S nije zatvoren u odnosu na sabiranje).

c) Oduzimanje je binarna operacija na $\mathbb{Z}$, ali ta operacija nije asocijativna, pa $(\mathbb{Z}, -)$ nije grupa.

d) Množenje je binarna operacija na $\mathbb{Q}$, važe aksiomi G1 i G2, ali $0 \in \mathbb{Q}$ nema inverzni element ($0 \cdot a = 0 \neq 1$, za svako $a \in \mathbb{Q}$), pa $(\mathbb{Q}, \cdot)$ nije grupa.

e) Skup $\mathbb{Q}$ iz koga je isključena nula je Abelova grupa u odnosu na množenje. Takođe i $(\mathbb{R} \setminus \{0\}, \cdot)$ i $(\mathbb{C} \setminus \{0\}, \cdot)$ su Ablove grupe.

f) Nije grupa.

g) Jesu grupe.

PRIMEDBA. U primeru d) grupoid $(\mathbb{Q}, \cdot)$ zadovoljava sve aksiome grupe sem G3, a u primeru f) grupoid $(\mathbb{Q}^+, \cdot)$ zadovoljava sve aksiome sem G1. Prema tome, svaki od aksioma G3 i G1 iz definicije grupe 1.9 je nezavisan od ostalih aksioma iz te definicije.

2. Da li skupovi

a) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}, a^2 + b^2 \neq 0\}$

b) $\{a + b\sqrt{2} + c\sqrt{3} \mid a, b, c \in \mathbb{Q}, a^2 + b^2 + c^2 \neq 0\}$

čine multiplikativne grupe?

3. Na skupu $G = \{(a, b) \mid a, b \in \mathbb{R}, a \neq 0\}$ je definisana binarna operacija $*$:

$$(a, b) * (c, d) = (ac, ad + b).$$

Dokazati da je $(G, *)$ grupa.

4. Dokazati da sledeći skupovi čine grupe u odnosu na množenje

a) $\{-1, 1\}$,

b) $\left\{1, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2}\right\}$,

c) $\{1, -1, i, -i\}$,

gde je $i^2 = -1$.

(Ovo su specijalni slučajevi grupe iz zadatka 5).

5. Dokazati da je skup S svih n -tih korena iz jedinice (n je fiksiran prirodan broj) grupa u odnosu na množenje.

Rešenje. Kompleksan broj a je n -ti koren iz jedinice ako i samo ako je $a^n = 1$, pa su n -ti koreni iz jedinice svi kompleksni brojevi oblika

$$e^{\frac{2k\pi i}{n}}, \quad k = 0, 1, 2, \dots, n-1.$$

Ako su $a, b \in S$, tada je

$$(ab)^n = a^n b^n = 1,$$

pa je i $ab \in S$ (dakle, skup S je zatvoren u odnosu na množenje).

Asocijativnost važi za množenje svih kompleksnih brojeva, pa važi i u S (jer je $S \subseteq \mathbb{C}$).

$1 \in S$ i $1 \cdot a = a$, za svako $a \in S$, pa postoji levi neutralni element.

Za svaki element $a \in S$,

$$\left(\frac{1}{a}\right)^n = \frac{1}{a^n} = 1,$$

pa i $\frac{1}{a} \in S$, a kako je $\frac{1}{a} \cdot a = 1$, svaki element skupa S ima levi inverzni element.

Prema tome, skup S je grupa u odnosu na množenje.

Kako je množenje kompleksnih brojeva komutativno, a S je podskup skupa kompleksnih brojeva i množenje u S je komutativno, pa je $(S, \cdot)$ Abelova grupa.

(Za $n = 2, 3$ i 4 dobijaju se grupe iz prethodnog zadatka).

PRIMEDBA. Ovim je pokazano da postoje konačne grupe bilo kog reda.

6. Dokazati da je skup svih korena iz jedinice, tj. skup

$$S = \{z \mid z \in \mathbb{C} \wedge (\exists n \in \mathbb{N}) z^n = 1\},$$

multiplikativna Abelova grupa.

7. Dokazati da je skup svih kompleksnih brojeva čiji je modul jednak jedinici multiplikativna Abelova grupa.

8. Neka je p fiksiran prost broj a

$$\mathbb{Z}_p^\infty = \{z \mid z \in \mathbb{C} \wedge (\exists n \in \mathbb{N}) z^{p^n} = 1\}.$$

Dokazati da je $(\mathbb{Z}_p^\infty, \cdot)$ Abelova grupa, ako je $\cdot$ množenje kompleksnih brojeva.

PRIMEDBA. Ova grupa se naziva p -Priferova (Prüfer) (ili samo Priferova grupa) ili kvaziciklička grupa.

9. Da li je skup $S = \{a, b, c\}$ grupa u odnosu na operaciju koja je zadana sledećom Kejljevom tablicom:

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Rešenje. Iz tablice se lako uočava da je binarna operacija dobro definisana i da je a neutralni element.

S obzirom da se neutralni element a nalazi u svakoj koloni tablice, zaključujemo da svaki element skupa S ima levi inverzni element.

Da ispitamo da li je operacija asocijativna potrebno je da proverimo da li je

$$\begin{aligned} a(aa) &= (aa)a \\ a(ab) &= (aa)b \\ a(ac) &= (aa)c \\ a(ba) &= (ab)a \\ &\dots\dots\dots \end{aligned}$$

itd. za sve uređene trojke elemenata iz S (takvih trojki ima n^3 za skup od n elemenata, u našem primeru $3^3 = 27$). Ako izračunamo sve ove proizvode videćemo da važi asocijativnost, pa je S grupa.

Pošto je gornja tablica simetrična u odnosu na glavnu (padajuću) dijagonalu, operacija je komutativna, pa je skup S u odnosu na tu operaciju Abelova grupa.

Da je $(S, \cdot)$ grupa može se proveriti i na sledeći način. Važi, naime, sledeća teorema:

Grupoid $(G, \cdot)$ je grupa ako i samo ako važi:

(i) za svako $a, b \in G$, jednačine

$$ax = b, \quad ya = b$$

imaju u G bar jedno rešenje po x, y ,

$$(ii) a(bc) = (ab)c$$

za svako $a, b, c \in G$, takvo da je $a \neq b \neq c \neq a$, (dakle, asocijativnost važi za svaku uređenu trojku različitih elemenata). (A. Wagner, *On the associative law of groups*, Rend. Mat. e Applic. Roma, 21 (1962), 60–76.)

Prema tome dovoljno je proveriti:

(i) da li se u svakoj vrsti i koloni tablice nalaze svi elementi skupa S (što je ispunjeno),

(ii) da li važi asocijativnost za sve uređene trojke različitih elemenata (za skup od n elemenata takvih trojki ima $n(n-1)(n-2)$, u našem primeru za $n = 3$ ima 6 trojki), tj. da li je

$$\begin{aligned} a(bc) &= (ab)c, & b(ca) &= (bc)a, \\ a(cb) &= (ac)b, & c(ab) &= (ca)b, \\ b(ac) &= (ba)c, & c(ba) &= (cb)a, \end{aligned}$$

što je takođe ispunjeno, pa je i na ovaj način dokazano da je S grupa.

Korišćenjem ove teoreme olakšava se proveravanje asocijativnosti – za grupoid od n elemenata treba izračunati $4n(n-1)(n-2)$ proizvoda (umesto $4n^3$ koliko je potrebno kad se asocijativnost proverava za sve uređene trojke).

(Napominjemo da se u definiciji grupe 1.9 aksiom G1 ne može zameniti ovako oslabljenom asocijativnošću.)

10. Ispitati da li su skupovi

$$A = \{a, b\}, \quad B = \{x, y, z\}, \quad C = \{1, 2, 3, 4\}$$

grupe u odnosu na operacije zadane sledećim Kelijevim tablicama:

$$\begin{array}{c|cc} & a & b \\ \hline a & a & b \\ b & b & a \end{array}, \quad \begin{array}{c|ccc} & x & y & z \\ \hline x & x & y & z \\ y & z & x & y \\ z & y & z & x \end{array}, \quad \begin{array}{c|cccc} & 1 & 1 & 3 & 4 \\ \hline 1 & 3 & 1 & 4 & 2 \\ 2 & 1 & 2 & 3 & 4 \\ 3 & 4 & 3 & 2 & 1 \\ 4 & 2 & 4 & 1 & 3 \end{array}.$$

11. Sledeća tablica je deo Kejljeve tablice jedne grupe:

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d		
b	b					
c	c	f				a
d	d					
f	f					

Kompletirati tablicu.

Rešenje. S obzirom da se u Kejljevoj tablici grupe svaki element pojavljuje tačno jedanput u svakoj vrsti i koloni tablice, odmah sledi da je $af = c$ i $ad = f$. Neutralni element je, očigledno, e , pa iz $ab = e$ sledi $ba = e$. Sada se iz druge kolone dobija da je $da = c$ (jer je c jedini element koji se ne nalazi u petoj vrsti i drugoj koloni), a slično je i $fa = d$. Na isti način zaključujemo da je $cb = d$. Kako je $a^2 = b$, onda je $b^2 = ba^2 = (ba)a = a$. Sada se u preseku treće vrste i četvrte kolone mora nalaziti f , tj. $bc = f$. Slično dobijamo da je $bd = c$, $bf = d$, $db = f$, $fb = c$.

Za element c^2 postoje dve mogućnosti: $c^2 \in \{e, b\}$. Ako je $c^2 = b$, onda je $cb = c^3 = bc$, a to je protivrečnost. Dakle, $c^2 = e$. Dalje je $cd = c(cb) = (cc)b = b$ i $dc = (ac)c = ac^2 = a$. Ostatak tablice se lako određuje, pa je kompletna tablica ove grupe

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

12. U skupu ostataka po modulu m ,

$$Z_m = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\},$$

definisano je sabiranje i množenje:

$$\overline{a} + \overline{b} = \overline{a+b}, \quad \overline{a} \cdot \overline{b} = \overline{ab}.$$

Da li su $(\mathbb{Z}_m, +)$, $(\mathbb{Z}_m, \cdot)$ i $(\mathbb{Z}_m \setminus \{\bar{0}\}, \cdot)$ grupe?

PRIMEDBA. Ako je m fiksiran prirodan broj, skup celih brojeva se može razložiti na klase ekvivalencije tako da su dva cela broja u istoj klasi ako i samo ako su kongruentni po modulu m (tj. ako daju isti ostatak pri deobi sa m). Ove klase se nazivaju klase ostataka po modulu m , a skup svih klasa skup (ili sistem) ostataka po modulu m (označavaćemo ga sa $\mathbb{Z}_m$). Sa $\bar{a}$ označavamo klasu u kojoj se nalazi ceo broj a . Da su celi brojevi a i b kongruentni po modulu m zapisivaćemo sa $a \equiv b \pmod{m}$.

Rešenje. Najpre ćemo dokazati da su gornje operacije dobro definisane, tj. da je rezultat sabiranja (odnosno množenja) $\overline{a+b}$ (odnosno $\overline{ab}$) uvek isti bez obzira na to koje predstavnike klasa $\bar{a}$ i $\bar{b}$ uzimamo.

Uzmimo bilo koji element klase $\bar{a}$, on mora biti oblika $a+k_1m$, ($k_1 \in \mathbb{Z}$), slično neka je $b+k_2m$ ($k_2 \in \mathbb{Z}$) proizvoljan element klase $\bar{b}$. Tada je

$$(\overline{a+k_1m}) + (\overline{b+k_2m}) = \overline{a+k_1m+b+k_2m} = \overline{a+b+(k_1+k_2)m}.$$

Kako je $a+b \equiv a+b+(k_1+k_2)m \pmod{m}$, sledi da je

$$(\overline{a+k_1m}) + (\overline{b+k_2m}) = \overline{a+b+(k_1+k_2)m} = \overline{a+b}.$$

Da je množenje dobro definisano dokazuje se slično:

$$(\overline{a+k_1m}) \cdot (\overline{b+k_2m}) = \overline{ab+(k_1b+k_2a+k_1k_2m)m} = \overline{ab}$$

Sada ćemo dokazati da je $(\mathbb{Z}_m, +)$ grupa:

- očigledno je da je operacija unutrašnja,
- $(\bar{a} + \bar{b}) + \bar{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \bar{a} + \overline{(b+c)} = \bar{a} + (\bar{b} + \bar{c})$, za svako $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$,

pa je sabiranje asocijativno,

- $\bar{0}$ je neutralni element,
- $\overline{m-a}$ je inverzni element za $\bar{a}$,

i kako je još

$$\bar{a} + \bar{b} = \bar{b} + \bar{a}, \quad \text{za svako } \bar{a}, \bar{b} \in \mathbb{Z}_m,$$

$(\mathbb{Z}_m, +)$ je Abelova grupa.

$(\mathbb{Z}_m, \cdot)$ nije grupa jer $\bar{0}$ nema inverzni element ($\bar{a} \cdot \bar{0} = \bar{0} \neq \bar{1}$, za svako $\bar{a} \in \mathbb{Z}_m$).

Ispitajmo sada da li je $(\mathbb{Z}_m \setminus \{\bar{0}\}, \cdot)$ grupa.

Ako je m složen broj, $m = pq$, tada je $\overline{pq} = \overline{m} = \bar{0}$, pa u tom slučaju množenje nije unutrašnja operacija, odnosno $(\mathbb{Z}_m \setminus \{\bar{0}\}, \cdot)$ nije grupa.

Ako je m prost broj, onda je množenje unutrašnja operacija, asocijativnost važi, $\bar{1}$ je neutralni element. Za svako $\bar{a} \neq \bar{0}$, a i m su uzajamno prosti brojevi, pa postoje celi brojevi r i s tako da je

$$ra + sm = 1.$$

Inverzni element za $\bar{a}$ je $\bar{r}$, jer je

$$\bar{r}\bar{a} = \overline{ra} = \overline{1 - sm} = \bar{1}.$$

Prema tome, $(\mathbb{Z}_m \setminus \{\bar{0}\}, \cdot)$ je grupa ako i samo ako je m prost broj.

13. a) Dokazati da je skup $\{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$ ostataka po modulu 10 grupa u odnosu na množenje.

b) Dokazati da je skup ostataka po modulu n onih celih brojeva koji su uzajamno prosti sa n , u odnosu na množenje Abelova grupa.

14. Dokazati da je skup svih polinoma s koeficijentima iz $\mathbb{Z}_n$ u odnosu na sabiranje polinoma Abelova grupa.

15. Skup svih permutacija skupa M (bijektivnih preslikavanja skupa M na sebe) čini grupu u odnosu na operaciju množenja (kompozicije) preslikavanja (ako su p, q permutacije onda je njihov proizvod pq preslikavanje definisano sa $(pq)(x) = p(q(x))$, za svako $x \in M$).

Dokazati.

PRIMEDBA. Ako je $M = \{1, 2, \dots, n\}$, grupa permutacija sa ovako definisanim množenjem se naziva simetrična grupa stepena n i označava sa S_n . Ta grupa ima $n!$ elemenata.

16. Naći grupu simetrija

- a) jednakostraničnog trougla,
- b) kvadrata,
- c) pravougaonika,
- d) pravilnog n -tougla,
- e) pravilnog tetraedra,

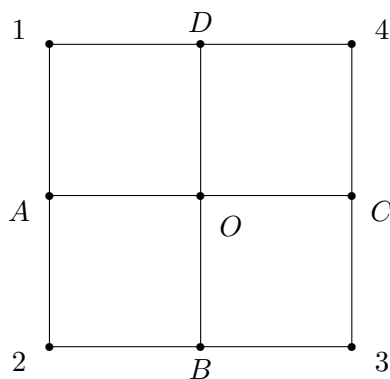
f) kocke.

PRIMEDBA. Simetrija neke geometrijske figure je svako bijektivno preslikavanje tačaka te figure na tačke te figure koje ne menja rastojanje tačaka (tj. rastojanje bilo koje dve tačke jednako je rastojanju slika tih tačaka)². Skup svih simetrija neke figure čini grupu u odnosu na množenje preslikavanja definisano kao uzastopno primenjivanje preslikavanja.

Ova definicija simetrije je šira od uobičajene geometrijske definicije simetrije i može da obuhvati pored centralne, osne i ravanske simetrije i sva druga preslikavanja sa navedenom osobinom (rotacije, translacije i sl.)³

Rešenje. b) Svaka od simetrija kvadrata potpuno je određena slikama njegovih temena, pa ćemo te simetrije prikazati kao permutacije temena.

Označimo temena kvadrata sa 1, 2, 3, 4, središte sa O , a sa A, B, C, D središta stranica 12, 23, 34 i 41 (v. sliku).



Grupu simetrija kvadrata čine sledeće permutacije:

– rotacije kvadrata u ravni oko tačke O za uglove $0, \pi/2, \pi$ i $3\pi/2$:

²Kada je geometrijska figura koja se preslikava ravan odnosno ceo prostor, onda se ovako definisana simetrija naziva izometrija (ili transformacija podudarnosti) ravni odnosno prostora.

³Može se dokazati da za ovako definisanu simetriju važi: svaka simetrija ravne figure može se prikazati kao proizvod najviše tri osne simetrije, a svaka simetrija prostorne figure može se prikazati kao proizvod najviše četiri ravanske simetrije (v. na primer, M.Prvanović: *Osnovi geometrije*, Beograd, 1980).

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix},$$

– simetrije u odnosu na prave AC , BD , 13 i 24 :

$$d = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

Lako se proverava da drugih simetrija kvadrata nema i da ovih osam permutacija zaista čine grupu.

d) Elementi grupe simetrija su rotacije oko središta O opisane kružnice za ugao od $\frac{2k\pi}{n}$, $k = 0, 1, \dots, n-1$. Ako se sa r označi rotacija za ugao od $\frac{2\pi}{n}$ tada svaka rotacija može da se predstavi kao r^k , $k = 0, 1, \dots, n-1$, pa je $r^n = e$, gde je e identičko preslikavanje (neutralni element grupe simetrija). Pored rotacija, simetrije su i n osnih simetrija u odnosu na n pravih koje spajaju tačku O sa temenima i središtima stranica n -tougla.

Dakle, ima najmanje $2n$ elemenata grupe simetrija pravilnog n -tougla, a lako se može pokazati da su to i jednine simetrije.

Ako se sa A označi jedno teme n -tougla, sa s osna simetrija u odnosu na pravu OA , onda je $s^2 = e$, a svi elementi grupe simetrija su

$$e, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}.$$

Veza između s i r je $r^k s = sr^{n-k}$, $k = 1, 2, \dots, n-1$.

PRIMEDBA. Grupa simetrija pravilnog n -tougla se naziva diedarska grupa, označava se da D_n i to je nekomutativna grupa koja ima $2n$ elemenata. Ranije konstruisana grupa simetrija kvadrata je diedarska grupa od 8 elemenata ($n = 4$).

17. Naći grupe permutacija skupa $S = \{1, 2, 3, 4\}$ za koje sledeće realne funkcije ostaju nepromenjene:

$$\text{a) } f(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4,$$

$$\text{b) } f(x_1, x_2, x_3, x_4) = x_1 + x_2,$$

$$\text{c) } f(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4.$$

(Ako je σ permutacija skupa S , onda se f ne menja permutacijom σ ako i samo ako je $f(x_1, x_2, x_3, x_4) = f(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$ za svako $x_1, x_2, x_3, x_4 \in \mathbb{R}$.)

18. Ispitati da li sledeći skupovi funkcija koje preslikavaju $\mathbb{R} \setminus \{0, 1\}$ u $\mathbb{R}$

$$\text{a) } \left\{ f_1(x) = x, f_2(x) = -x, f_3(x) = \frac{1}{x}, f_4(x) = -\frac{1}{x} \right\},$$

$$\text{b) } \left\{ f_1(x) = x, f_2(x) = \frac{1}{x}, f_3(x) = 1 - x, f_4(x) = -\frac{1}{1 - x}, \right.$$

$$\left. f_5(x) = \frac{x - 1}{x}, f_6(x) = \frac{x}{x - 1} \right\},$$

čine grupe u odnosu na operaciju $*$ definisanu sa

$$(f_i * f_j)(x) = f_i(f_j(x)), \text{ za svako } x \in \mathbb{R} \setminus \{0, 1\}.$$

Uputstvo. Formirati Kejljevu tablicu i zatim kao u zadatku 9 iz tablice utvrditi da je operacija dobro definisana, postojanje neutralnog elementa i inverznih elemenata. Ovako definisano množenje funkcija je asocijativno za sve funkcije uopšte (što se lako može pokazati), pa je asocijativno i za date skupove funkcija.

19. Da li sledeći skupovi čine grupe u odnosu na odgovarajuće operacije:

a) Skup L svih realnih funkcija oblika

$$f(x) = ax + b, \quad a, b \in \mathbb{R}, \quad a \neq 0,$$

u odnosu na kompoziciju funkcija

$$(fg)(x) = f(g(x)),$$

b) isti skup L u odnosu na sabiranje funkcija

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

c) skup P svih realnih periodičnih funkcija sa periodom $\omega \in \mathbb{R}$ u odnosu na sabiranje funkcija,

d) isti skup P u odnosu na kompoziciju funkcija.

Koje od navedenih operacija su komutativne?

20. Neka je S bilo koji neprazan skup, a $(G, *)$ bilo koja grupa. Kako se može definisati množenje preslikavanja pa da skup svih preslikavanja skupa S u G bude grupa?

21. Dokazati da sledeći skupovi matrica sa realnim (kompleksnim) elementima čine multiplikativne grupe:

- a) sve regularne matrice formata $n \times n$,
- b) sve ortogonalne matrice formata $n \times n$,
- c) sve matrice formata $n \times n$ čije su determinante jednake 1.

22. Naći red multiplikativne grupe G regularnih matrica formata 2×2 sa elementima iz $\mathbb{Z}_p$, gde je p prost broj.

Uputstvo. Prva kolona matrice može da bude bilo koji nenula vektor, a druga kolona može da bude bilo koji nenula vektor koji nije skalarni umnožak prvog.

Rezultat. $(p^2 - 1)(p^2 - p)$.

23. Neka je p neparan prost broj. Dokazati da je skup matrica

$$G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \mid a \in \mathbb{Z}_p \setminus \{0\} \right\}$$

Abelova grupa u odnosu na množenje matrica.

Da li analogno tvrđenje važi

- a) za matrice formata $n \times n$,
- b) ako je p proizvoljan prirodan broj ?

Uputstvo. Neutralni element je matrica $\begin{bmatrix} e & e \\ e & e \end{bmatrix}$, gde je $e \equiv 2^{-1} \pmod{p}$, a inverzna matrica za matricu $\begin{bmatrix} a & a \\ a & a \end{bmatrix}$ je matrica $\begin{bmatrix} b & b \\ b & b \end{bmatrix}$, gde je $b \equiv (4a)^{-1} \pmod{p}$.

24. Da li skup matrica

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \right\},$$

$$\left\{ \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} \right\}$$

($i^2 = -1$), čini grupu u odnosu na množenje matrica?

Da li neki podskupovi ovog skupa čine grupe?

25. Da li je skup matrica sa elementima iz $\mathbb{Z}_2$

$$\left\{ \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{bmatrix}, \begin{bmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{bmatrix} \right\}$$

grupa u odnosu na množenje matrica ?

26. Dokazati da je skup matrica

$$\left\{ \begin{bmatrix} \pm 1 & a \\ 0 & 1 \end{bmatrix} \mid a \in \mathbb{Z}_n \right\}$$

u odnosu na množenje matrica konačna nekomutativna grupa reda $2n$.

27. Ako je neki skup matrica grupa u odnosu na množenje matrica, dokazati da su tada ili sve matrice tog skupa singularne ili su sve regularne.

PRIMEDBA. Neutralni element te grupe ne mora biti jedinična matrica

$$E = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}.$$

Na primer, skup matrica

$$\left\{ \begin{bmatrix} x & x \\ 0 & 0 \end{bmatrix} \mid x \in \mathbb{R} \setminus \{0\} \right\}$$

je grupa u odnosu na matricno množenje, a neutralni element nije

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

28. Neka je G skup matrica oblika

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix},$$

gde su a, b, c elementi polja F . Dokazati da je G grupa u odnosu na množenje matrica.

29. U skupu svih uređenih parova realnih brojeva preslikavanja $A_\theta : (x, y) \mapsto (x', y')$ definisana su sa

$$\begin{aligned}x' &= x \cos \theta + y \sin \theta, \\y' &= -x \sin \theta + y \cos \theta.\end{aligned}$$

Dokazati da skup $L = \{A_\theta \mid \theta \in \mathbb{R}\}$ svih preslikavanja tog oblika čini grupu u odnosu na operaciju kompozicije preslikavanja. Dati geometrijsku interpretaciju.

30. Na skupu $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ definisana je operacija $\circ$ sa

$$a \circ b = \begin{cases} ab, & a > 0, \\ \frac{a}{b}, & a < 0. \end{cases}$$

Da li je $(\mathbb{R}^*, \circ)$ grupa?

Rešenje. Binarna operacija $\circ$ je asocijativna. Da se to proveriti potrebno je analizirati različite slučajeve: $a > 0, b > 0$; $a > 0, b < 0$; $a < 0, b < 0$; $a < 0, b > 0$; i c proizvoljan element iz $\mathbb{R}^*$.

Ako je $a > 0, b > 0$, onda je

$$a \circ (b \circ c) = a \circ (bc) = abc, \quad (a \circ b) \circ c = (ab) \circ c = abc.$$

Ako je $a > 0, b < 0$, onda je

$$a \circ (b \circ c) = a \circ \frac{b}{c} = \frac{ab}{c}, \quad (a \circ b) \circ c = (ab) \circ c = \frac{ab}{c}.$$

Slično se proveravaju i ostali slučajevi, pa je operacija $\circ$ asocijativna.

Levi neutralni element je 1 jer je za svako $a \in \mathbb{R}^*$ $1 \circ a = a$.

Za $a > 0$ levi inverzni element je $\frac{1}{a}$, a za $a < 0$ levi inverzni element je sam element a .

Prema tome, $(\mathbb{R}^*, \circ)$ je grupa.

31. U skupu $\mathbb{Z}^3$ svih uređenih trojki celih brojeva definisano je množenje

$$(a, b, c)(x, y, z) = (a + (-1)^b x, \quad b + (-1)^c y, \quad (-1)^x c + z).$$

Dokazati da je $\mathbb{Z}^3$ u odnosu na ovo množenje grupa.

32. Neka je $\mathbb{Z}^\infty$ skup svih beskonačnih nizova celih brojeva i neka je na $\mathbb{Z}^\infty$ definisana operacija $*$ sa

$$(f_0, f_1, \dots, f_n, \dots) * (g_0, g_1, \dots, g_n, \dots) = \\ = (f_0 + g_0, (-1)^{g_0} f_1 + g_1, (-1)^{g_0+g_1} f_2 + g_2, \dots, (-1)^{g_0+\dots+g_{n-1}} f_n + g_n, \dots).$$

Dokazati da je $(\mathbb{Z}^\infty, *)$ grupa.

33. Neka je $G = \{(a, b, c) \mid a, b, c \in \{0, 1, \dots, p-1\}\}$, gde je p prost broj i

$$(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2 + a_1 b_2),$$

gde su operacije $+$ i $\cdot$ redom sabiranje i množenje po modulu p .

Dokazati da je $(G, *)$ nekomutativna grupa reda p^3 .

34. Neka je $G = \{(a, b) \mid a \in \{0, 1, \dots, p-1\}, b \in \{0, 1, \dots, p^2-1\}\}$, gde je p prost broj, a operacija $*$ definisana sa

$$(a_1, b_1) * (a_2, b_2) = (a_1 + a_2, b_1 + b_2 + b_1 a_2 p),$$

pri čemu su operacije $+$ i $\cdot$ u prvoj koordinati po modulu p , a u drugoj po modulu p^2 .

Dokazati da je $(G, *)$ nekomutativna grupa reda p^3 .

35. Neka je p prost broj, $G = \{(a, b, c, d) \mid a, b, c, d \in \{0, 1, \dots, p^2-1\}\}$ i

$$(a_1, b_1, c_1, d_1) * (a_2, b_2, c_2, d_2) = \\ = (a_1 + a_2 + p c_1 a_2, b_1 + b_2 + p d_1 b_2, c_1 + c_2 + p c_1 b_2, d_1 + d_2 + p b_1 a_2),$$

gde su $+$ i $\cdot$ po modulu p^2 .

Dokazati da je $(G, *)$ grupa.

36. Neka je p prost broj a

$$\mathbb{Q}_p = \left\{ \frac{a}{b} \mid \frac{a}{b} \in \mathbb{Q} \text{ i } b \text{ je uzajamno prost sa } p \right\}.$$

Dokazati da je $(\mathbb{Q}_p, +)$ Abelova grupa ($+$ je sabiranje racionalnih brojeva).

37. Neka je p prost broj,

$$\mathbb{Q}^p = \left\{ \frac{a}{b} \mid \frac{a}{b} \in \mathbb{Q} \text{ i } (\exists n \in \mathbb{N} \cup \{0\}) b = p^n \right\}.$$

Dokazati da je $(\mathbb{Q}^p, +)$ Abelova grupa (+ je sabiranje racionalnih brojeva).

38. Neka je S proizvoljan neprazan skup. Definišimo operaciju Δ na partitivnom skupu $\mathcal{P}(S)$ skupa S na sledeći način:

$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

Dokazati da je $(\mathcal{P}(S), \Delta)$ grupa.

($A \Delta B$ se naziva simetrična razlika skupova A i B .)

Rešenje. Operacija Δ je očigledno dobro definisana. Dokažimo asocijativnost te operacije. Neka je $\chi_A : S \rightarrow \{0, 1\}$ karakteristična funkcija skupa A ,

$$\chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}.$$

Ako definišemo sabiranje karakterističnih funkcija sa

$$(\chi_A + \chi_B)(x) = \chi_A(x) + \chi_B(x), \quad \text{za svako } x \in S,$$

gde je sabiranje na desnoj strani jednakosti po modulu 2, onda se neposredno proverava da je za svako $A, B \subseteq S$

$$\chi_A + \chi_B = \chi_{A \Delta B}.$$

S obzirom da je ovako definisano sabiranje karakterističnih funkcija asocijativno, neposredno sledi da je

$$\chi_{A \Delta (B \Delta C)} = \chi_{(A \Delta B) \Delta C}.$$

Dva skupa čije su karakteristične funkcije jednake moraju biti jednaki, dakle,

$$A \Delta (B \Delta C) = (A \Delta B) \Delta C.$$

Neposredno se proverava da je prazan skup $\emptyset$ neutralni element za operaciju Δ i da je $A^{-1} = A$, tj. $A \Delta A = \emptyset$.

39. Dokazati da su definicije 1.9 i 1.10 ekvivalentne.

40. Dokazati da je grupoid $(G, \cdot)$ grupa ako i samo ako je

- (i) operacija asocijativna,
- (ii) za svako $a, b \in G$ jednačine

$$a \cdot x = b, \quad y \cdot a = b$$

imaju u G rešenja po x i y .

41. Na skupu G je definisana binarna operacija $(a, b) \mapsto ab$ i unarna operacija $a \mapsto a^{-1}$, tako da važe sledeći aksiomi:

G1'. za svako $a, b, c \in G$

$$(ab)c = a(bc),$$

G2'. za svako $a, b \in G$

$$a^{-1}(ab) = b = (ba)a^{-1}.$$

Dokazati da je ovaj sistem aksioma ekvivalentan sa sistemom aksioma G1-3 kojima je definisana grupa u 1.9.

Rešenje. Iz aksioma G1-3 navedenih u 1.9 očividno slede gornji aksiomi. Pokazaćemo da i obrnuto, iz gornjih aksioma slede aksiomi G1-3.

Ako u jednakosti

$$b = (ba)a^{-1}, \quad (\text{G2'})$$

zamenimo b sa $c^{-1}c$, dobijamo

$$c^{-1}c = ((c^{-1}c)a)a^{-1} = (c^{-1}c)(aa^{-1}) = c^{-1}(c(aa^{-1})) = aa^{-1}.$$

Za $c = a$ odavde sledi da je $a^{-1}a = aa^{-1}$ i da element $a^{-1}a$ ne zavisi od a . Uvedimo oznaku

$$(1) \quad a^{-1}a = e.$$

Kako je

$$eb = (a^{-1}a)b = a^{-1}(ab) = b,$$

važi aksiom G2, a iz (1) sledi da važi i G3, pa je time dokazana ekvivalentnost ova dva sistema aksioma.

42. Dokazati da je grupoid $(G, \cdot)$ Abelova grupa ako i samo ako važe sledeći aksiomi:

G"1. za svako $a, b, c \in G$

$$a(bc) = (ba)c,$$

i aksiomi G2 i G3 iz definicije 1.9.

43. Ako je na skupu G definisana jedna binarna operacija $(a, b) \mapsto ab$ i jedna unarna operacija $a \mapsto a'$ i ako za svako $a, b, c, d, f, \in G$

$$(ab)c = (ad)f \Rightarrow b = d(fc'),$$

onda je G grupa. Dokazati.

Literatura:

Slater M., *A single postulate for groups*, Amer. Math. Monthly, 68 (1961), 346–347.

Rešenje. Kako je $(ab)c = (ab)c$, sledi

$$(2) \quad b = b(cc'), \quad \text{za svako } b, c \in G.$$

Označimo proizvod aa' sa a^* . Tada je prema (2)

$$a = ab^* = ad^* \quad \text{i} \quad (ab^*)c = (ad^*)c,$$

a odatle sledi

$$b^* = d^*c^* = d^*.$$

Dakle, za svako $a \in G$, $aa' = e$, pa je na osnovu svega pokazanog e desni neutralni element i a' je desni inverzni element za a .

Preostaje, prema tome, još da dokažemo da je binarna operacija asocijativna. Radi toga ćemo prethodno izvesti neke posledice datog aksioma.

Ako je $ab = ad$, onda je

$$(ab)c = (ad)c,$$

a odatle

$$b = d(cc') = d,$$

što znači da važi leva kancelacija.

Iz $(ae)b = (ab)e$ sledi $e = b(eb')$.

Kako je $e = bb'$ dobijamo da je (primenjujući levu kancelaciju) $b' = eb'$. Specijalno $e' = ee' = e$.

Dalje je

$$(ab)e = (ae)b,$$

odakle imamo

$$b = e(be') = eb,$$

tj. e je i levi neutralni element.

Iz

$$(ec)c' = (ed)d'$$

dobija se

$$c = d(d'c'').$$

Stavljajući $d = e$ imaćemo da je $c = c''$, pa je

$$c = d(d'c).$$

To znači da jednačina $a = bx$, za svako $a, b \in G$ ima rešenje $x = b'a$.

Sada se može dokazati da važi asocijativnost.

Ako su a, b, c bilo koji elementi skupa G , možemo izabrati d tako da bude

$$(a(bc))d = (ab)c,$$

odakle

$$bc = b(cd'),$$

pa je dalje

$$ce = c = cd', \quad e = d' \quad \text{ i } \quad d = e.$$

Dobili smo da je

$$a(bc) = (ab)c, \quad \text{ za svako } a, b, c \in G,$$

a time je i dokaz dovršen.

44. Neka je G skup na kome je definisana binarna operacija $\cdot$ tako da važi

(i) $a(bc) = (ab)c$, za svako $a, b, c \in G$,

- (ii) postoji $e \in G$ tako da je $ae = ea = a$, za svako $a \in G$,
 (iii) za svako $a \in G$ postoji $a' \in G$ tako da je $aa' = e$ ili $a'a = e$.

Da li je $(G, \cdot)$ grupa?

Rešenje. Neka a ima desni inverzni element a'

$$aa' = e.$$

Dokažimo da a' mora tada biti i levi inverzni element. Označimo sa $b = a'a$. Tada je

$$b^2 = (a'a)(a'a) = a'(aa')a = a'(ea) = a'a = b.$$

Element b ima desni ili levi inverzni element b' , pa ako jednakost $b^2 = b$ pomnožimo sleva (ako je b' levi inverzni) ili zdesna (ako je b' desni inverzni) sa b' , dobijamo u oba slučaja

$$a'a = b = e.$$

Prema tome, a' je i levi inverzni element, a to znači da je $(G, \cdot)$ grupa.

45. Primerom pokazati da se aksiom (ii) u prethodnom zadatku ne može zameniti slabijim aksiomom:

- (ii)' postoji $e \in G$ tako da je $ea = a$, za svako $a \in G$.

Literatura:

Colonel Johnson, *A mixed non-group*, Amer. Math. Monthly, 71 (1964), 785.

Rešenje. Neka je

$$M = \left\{ \begin{bmatrix} x & y \\ x & y \end{bmatrix} \mid x, y \in \mathbb{R}, \ x + y \neq 0 \right\},$$

a operacija množenje matrica.

Lako se proverava da je skup M zatvoren u odnosu na množenje.

- (i) Množenje matrica je asocijativno.

- (ii) Matrica $I = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ pripada M i kako je

$$IA = A, \quad \text{za svako } A \in M,$$

I je levi neutralni element.

(iii) Za svaku matricu $A = \begin{bmatrix} x & y \\ x & y \end{bmatrix}$ iz M matrica

$$B = \begin{bmatrix} 0 & \frac{1}{x+y} \\ 0 & \frac{1}{x+y} \end{bmatrix}$$

pripada skupu M i $AB = I$, tj. B je desni inverzni element za matricu A .

Međutim, I nije desni neutralni element, pa M nije multiplikativna grupa.

Još jedan primer za isto tvrđenje je grupoid $(\{a, b\}, \cdot)$ čija je operacija definisana sledećom Kejljevom tablicom:

	a	b
a	a	b
b	a	b

46. Neka je S polugrupa sa jedinstvenom desnom jedinicom e . Ako za svaki element $x \in S$ postoji $\bar{x} \in S$ tako da je $\bar{x}x = e$, dokazati da je S grupa.

Rešenje. Dovoljno je dokazati da je $x\bar{x} = e$. Neka je $b = x\bar{x}$. Tada je $b^2 = x(\bar{x}x)\bar{x} = b$, pa je $eb = \bar{b}bb = \bar{b}b = e$. Ako je $s \in S$, onda se dobija da je $sb = (se)b = s(eb) = se = s$, pa je b desna jedinica. Zbog jedinstvenosti desne jedinice je $b = e = x\bar{x}$ i S je grupa.

47. Neka je G grupoid sa jedinicom u kome važi $(xy)z = (xz)y$ za svako $x, y, z \in G$. Dokazati da je G komutativna polugrupa.

Rešenje. Ako se stavi $x = e$ dobija se da je $yz = zy$. Koristeći komutativnost se dobija

$$(xy)z = (xz)y = (zx)y = (zy)x = (yz)x = x(yz).$$

48. Dokazati da je konačna polugrupa G u kojoj važe zakoni kancelacije grupa.

Rešenje. Neka je

$$G = \{a_1, a_2, \dots, a_n\}$$

konačna polugrupa u kojoj važe zakoni kancelacije. Tada su za bilo koje $a_i \in G$

$$a_1a_i, a_2a_i, \dots, a_na_i$$

različiti elementi skupa G (jer pretpostavka da je $a_k a_i = a_l a_i$ zbog kancelacije dovodi do protivrečnosti $a_k = a_l$), a kako ih ima n sledi da su to svi elementi skupa G .

Prema tome, za svako $a_i, a_j \in G$ postoji element $x \in G$ tako da je

$$x a_i = a_j,$$

tj. jednačina

$$x a = b,$$

za svako $a, b \in G$ ima rešenje u G .

Analogno se pokazuje da i jednačina

$$a y = b,$$

za svako $a, b \in G$ ima rešenje u G , pa je, prema definiciji grupe iz zadatka 40, G grupa.

PRIMEDBA. Pretpostavka da je polugrupa konačna je bitna jer, na primer, skup prirodnih brojeva u odnosu na sabiranje je polugrupa sa kancelacijom ali nije grupa.

Primerom pokazati da stav ne važi ako se pretpostavi da važi samo leva (ili samo desna) kancelativnost.

49. Neka je $(S, \cdot)$ konačna polugrupa u kojoj za svako $a, b, x \in S$ iz $ax = xb$ sledi da je $a = b$. Dokazati da je $(S, \cdot)$ Abelova grupa.

Rešenje. Iz $aba = aba$ sledi da je $ab = ba$, pa je polugrupa komutativna. Iz $ab = ac$ se dobija da je $ab = ba = ac$, pa je $b = c$ i u S važi zakon kancelacije. Na osnovu prethodnog zadatka onda sledi da je $(S, \cdot)$ Abelova grupa.

50. Polugrupa S ima osobinu da za svako $x \in S$ postoji element $x' \in S$ takav da je za svako $y \in S$

$$y x x' = y.$$

Da li je S grupa?

51. Neka je S polugrupa u kojoj važe zakoni kancelacije. Ako za svako $a \in S$ postoji prirodan broj $n_a > 1$ takav da je

$$a^{n_a} = a,$$

da li je S grupa?

Rešenje. Kako je za $a, b \in S$

$$a^{n_a}b = aa^{n_a-1}b = ab,$$

sledi

$$a^{n_a-1}b = b, \quad \text{za svako } b \in S.$$

Analogno je

$$ba^{n_a-1} = b, \quad \text{za svako } b \in S,$$

što znači da je a^{n_a-1} neutralni element.

Dva različita neutralna elementa e_1, e_2 u S ne mogu postojati jer je $e_1 = e_1e_2 = e_2$, pa je za svako $a \in S$

$$a^{n_a-1} = e.$$

Za $n_a > 2$ je

$$a^{-1} = a^{n_a-2},$$

a za $n = 2$ je

$$a^2 = a = e,$$

tj. $a^{-1} = a$. Prema tome, S ima neutralni element i za svaki element postoji inverzni, a to znači da je S grupa.

52. Na skupu svih realnih brojeva definisana je operacija $*$:

$$x * y = ax + by + c, \quad a, b, c \in \mathbb{R}, \quad ab \neq 0.$$

Dokazati da je $(\mathbb{R}, *)$ kvazigrupa. Koje uslove treba da zadovoljavaju a, b, c pa da $(\mathbb{R}, *)$ bude grupa?

53. Neka je operacija $*$ definisana na skupu prirodnih brojeva sa $a * b = \text{nzd}(a, b)$. Dokazati:

- $(\mathbb{N}, *)$ je komutativna polugrupa sa nulom bez jedinice.
- Svaki element $a \in \mathbb{N}$ je delitelj nule.
- Za svako $x \in \mathbb{N}$ postoji beskonačno mnogo elemenata $y \in \mathbb{N}$ tako da je $x * y * x = x$.
- Za svako $x \in \mathbb{N}$ postoji konačno mnogo elemenata $y \in \mathbb{N}$ tako da je $x * y * x = y$.

PRIMEDBA. U polugrupi $(S, \cdot)$ element a je nula ako i samo ako je za svako $x \in S$ $ax = xa = a$.

54. Neka je $(S, \cdot)$ polugrupa u kojoj važi

$$(\forall a \in S)(\exists x, y \in S)(xaa = a \wedge aay = a).$$

Dokazati:

a) $(\forall a \in S)(\exists e_a \in S)(e_a a = ae_a = a).$

b) $(\forall a \in S)(\exists b_a \in S)(b_a a = ab_a = e_a).$

Rešenje. Neka je $xaa = a = aay$. Označimo se $e_a = xa$. Tada je $e_a = xa = x(aay) = (xaa)y = ay$, pa je $e_a a = xaa = aay = ae_a = a$.

Neka je $b_a = xa = xay = ayy$. Tada je

$$b_a a = xaa = xa = e_a = ay = aayy = ab_a.$$

55. Dokazati da su lupe reda 1,2,3,4 grupe i naći lupu reda 5 koja nije grupa.

56. Neka je G lupa u kojoj za svako $x, y, z \in G$ važi $(xy)z = (xz)y$. Dokazati da je G Abelova grupa.

Uputstvo. Koristiti zadatak 47.

57. Neka je G skup na kome je definisana ternarna operacija $f : G \times G \times G \rightarrow G$ za koju važi:

1. $f(x, y, f(z, u, v)) = f(x, f(u, z, y), v) = f(f(x, y, z), u, v),$
2. $f(x, y, y) = f(y, y, x) = x,$

za svako $x, y, z, u, v \in G$.

Koristeći se ternarnom operacijom f , definisati jednu binarnu operaciju $\cdot$ na skupu G tako da $(G, \cdot)$ bude grupa.

Rešenje. Uočimo proizvoljan element e skupa G i definišimo binarnu operaciju $\cdot$ na G na sledeći način:

$$a \cdot b = f(a, e, b).$$

Tada je

$$a \cdot (b \cdot c) = f(a, e, f(b, e, c)) = f(f(a, e, b), e, c) = (a \cdot b) \cdot c,$$

i

$$a \cdot e = f(a, e, e) = a.$$

Ako uvedemo oznaku $a^{-1} = f(e, a, e)$, onda je

$$a \cdot a^{-1} = f(a, e, f(e, a, e)) = f(f(a, e, e), a, e) = f(a, a, e) = e,$$

pa je $(G, \cdot)$ grupa.

PRIMEDBA. Ako je data proizvoljna grupa $(G, \cdot)$, onda se na G može definisati ternarna operacija f sa gornjim osobinama na sledeći način:

$$f(x, y, z) = x \cdot y^{-1} \cdot z.$$

O strukturi definisanoj u zadatku i nekim njenim generalizacijama videti:

A. G. Kuroš, *Obščaja algebra, lekci 1969 - 1970 učebnogo goda*, Nauka, Moskva, 1974, str. 34-38.

58. Neka u grupoidu $(G, *)$ važe sledeći identiteti:

1. $(x * z) * (y * z) = x * y$,
2. $x * (y * y) = x$,
3. $(x * x) * (y * z) = z * y$.

Koristeći se operacijom $*$ definisati na G operaciju $\cdot$ tako da $(G, \cdot)$ bude grupa.

Rešenje. Definisaćemo unarnu operaciju $x \mapsto x^{-1}$ i binarnu operaciju $\cdot$ na sledeći način:

$$x^{-1} = (x * x) * x, \quad x \cdot y = x * ((y * y) * y) = x * y^{-1}.$$

Na osnovu 1. i 2. sledi

$$(x * y) * y^{-1} = (x * y) * ((y * y) * y) = x * (y * y) = x,$$

a iz gornje jednakosti i 1. i 2. dobija se

$$(x * y^{-1}) * y = (x * y^{-1}) * ((y * y) * y^{-1}) = x * (y * y) = x.$$

Iz 3. sledi

$$(x * y)^{-1} = ((x * y) * (x * y)) * (x * y) = y * x.$$

Dokazaćemo da je operacija $\cdot$ asocijativna:

$$\begin{aligned} x \cdot (y \cdot z) &= x * (y * z^{-1})^{-1} = x * (z^{-1} * y) = ((x * y^{-1}) * y) * (z^{-1} * y) = \\ &= (x * y^{-1}) * z^{-1} = (x \cdot y) \cdot z. \end{aligned}$$

Neka je x proizvoljan element iz G . Ako uvedemo oznaku $e = x * x$, onda element e ne zavisi od x . Zaista, iz 3. sledi

$$(x * x) * (y * y) = y * y,$$

a iz 2. je

$$(x * x) * (y * y) = x * x,$$

pa je za svako $x, y \in G$, $x * x = y * y$.

Iz 2. sledi da je e desni neutralni element za operaciju $\cdot$.

S obzirom da iz 2. i 3. sledi

$$(x^{-1})^{-1} = (((x * x) * x) * ((x * x) * x)) * ((x * x) * x) = x * (x * x) = x,$$

onda je

$$x \cdot x^{-1} = x * (x^{-1})^{-1} = x * x = e,$$

tj. x^{-1} je desni inverzni element za x , pa je $(G, \cdot)$ grupa.

PRIMEDBA. Ako se u proizvoljnoj grupi $(G, \cdot)$ definiše operacija $*$ sa $x * y = x \cdot y^{-1}$ onda grupoid $(G, *)$ zadovoljava aksiome 1, 2 i 3.

59. Dokazati da se u prethodnom zadatku aksiomi 2. i 3. mogu zameniti aksiomom

$$2'. \quad (x * x) * ((y * y) * y) = y.$$

PRIMEDBA. U radu Higman G., Neumann B.H., *Groups as groupoids with one law*, Publ. Math. Debrecen, 2 (1952), 215–221, je dokazano da se aksiomi 1. i 2'. mogu zameniti jednim aksiomom

$$x * (((x * x) * y) * z) * (((x * x) * x) * z) = y.$$

U sledećih 5 zadataka je izložen dokaz ovog tvrđenja. Dokaz je obradio dr V. Tasić, koji je u to vreme bio student. Još neki rezultati u vezi sa definisanjem grupe jednim identitetom dati su u:

V. Tasić, *On single-law definitions of groups*, Bull. Austral. Math. Soc. 37(1988), no. 1, 101–106.

60. Neka je dat grupoid $(G, *)$ i neka je $x \in G$. Definišimo preslikavanja L_x i D_x sa

$$L_x : y \mapsto x * y, \quad D_x : y \mapsto y * x.$$

Dokazati da grupoid G zadovoljava identitet

$$(1) \quad x * (((x * x) * y) * z) * (((x * x) * x) * z) = y$$

ako i samo ako važi

$$(2) \quad L_x \circ D_{((x*x)*x)*z} \circ D_z \circ L_{x*x} = \text{id}_G,$$

gde je $\circ$ množenje (kompozicija) preslikavanja, a id_G identičko preslikavanje skupa G .

61. Ako grupoid $(G, *)$ zadovoljava identitet (1), onda su preslikavanja L_x i D_x bijekcije. Dokazati.

Rešenje. Ako je $f \circ g = h$ i h je bijekcija, onda je g injektivno, a f surjektivno preslikavanje. Po pretpostavci i na osnovu prethodnog zadatka važi (2). Iz (2) se odmah vidi da je L_x surjektivno i L_{x*x} injektivno preslikavanje za svako $x \in G$. Prema tome, L_{x*x} je bijekcija. Dakle,

$$L_x \circ D_{((x*x)*x)*z} \circ D_z = L_{x*x}^{-1},$$

odakle sledi da je D_z injektivno preslikavanje za svako $z \in G$. Ako stavimo da je $x = w * w$, gde je w bilo koji element iz G , onda je za takvo x L_x bijekcija, pa je

$$D_{((x*x)*x)*z} \circ D_z = L_x^{-1} \circ L_{x*x}^{-1},$$

odakle sledi, s obzirom da je D_z injektivno za svako $z \in G$, da je preslikavanje $D_{((x*x)*x)*z}$ bijekcija. Prema tome,

$$D_z = D_{((x*x)*x)*z}^{-1} \circ L_x^{-1} \circ L_{x*x}^{-1},$$

što znači da je za ovako izabrano x i D_z bijekcija. Međutim, z ne zavisi od izbora x , pa se dobija da je preslikavanje D_z bijekcija za svako $z \in G$. Dokazali smo da su u (2) sva preslikavanja osim L_x bijekcije, a to znači da i L_x mora biti bijekcija za svako $x \in G$.

62. Ako u grupoidu $(G, *)$ važi identitet (1) tada izraz $u * u$ ne zavisi od u .

Rešenje. Koristeći prethodni zadatak iz (2) se dobija

$$D_{((x*x)*x)*z} \circ D_z = L_x^{-1} \circ L_{x*x}^{-1}.$$

Desna strana ne zavisi od z pa sledi

$$D_{((x*x)*x)*z} \circ D_z = D_{((x*x)*x)*w} \circ D_w,$$

tj. u $(G, *)$ važi identitet

$$(3) \quad (y * z) * (((x * x) * x) * z) = (y * w) * (((x * x) * x) * w).$$

Ako se u (3) stavi $y = (x * x) * x$, dobija se

$$(((x * x) * x) * z) * (((x * x) * x) * z) = (((x * x) * x) * w) * (((x * x) * x) * w).$$

S obzirom da je $L_{(x*x)*x}$ bijekcija, za proizvoljno $u, v \in G$ postoje $z, w \in G$ takvi da je $L_{(x*x)*x}(z) = u$ i $L_{(x*x)*x}(w) = v$, pa iz prethodne jednakosti sledi

$$(4) \quad u * u = v * v.$$

63. Ako se sa e označi konstanta $u * u$ iz prethodnog zadatka dokazati da je $e * e = e$.

64. Neka je $(G, *)$ grupoid u kome važi identitet (1). Dokazati da je tada $(G, \cdot)$ grupa, gde je operacija $\cdot$ definisana sa $x \cdot y = x * ((y * y) * y)$.

Rešenje. Na osnovu prethodnog zadatka se (1) može napisati u obliku

$$(5) \quad x * (((e * y) * z) * ((e * x) * z)) = y,$$

pa se za $y = x$ dobija

$$y * (((e * y) * z) * ((e * y) * z)) = y$$

tj. $y * e = y$ za svako $y \in G$.

Kada se u (5) stavi da je $x = z = e$ dobija se $e * (e * y) = y$, pa zbog $e = x * x = y * y$ u G važi

$$(6) \quad (x * x) * ((y * y) * y) = y.$$

Iz (5) sledi $((e * y) * z) * ((e * x) * z) = L_x^{-1}(y)$, pa izraz na levoj strani ne zavisi od z . To znači da je

$$((e * y) * z) * ((e * x) * z) = ((e * y) * e) * ((e * x) * e) = (e * y) * (e * x),$$

Kako je L_x bijekcija, stavljajući u prethodnu jednakost $u = e * y$ i $v = e * x$, dobija se da u G važi identitet

$$(7) \quad (u * z) * (v * z) = u * v.$$

Identiteti (6) i (7) koje smo dobili su identiteti 1. i 2'. iz zadataka 45 i 46, pa na osnovu tih zadataka sledi da je $(G, \cdot)$ grupa.

1.3 Osnovne osobine

65. Dokazati da iz definicije grupe 1.9 slede stavovi navedeni u 1.12.

66. Dokazati da u grupi G jednačina $axa = b$, $a, b \in G$, ima rešenje po x ako i samo ako je ab kvadrat nekog elementa iz G .

67. Dokazati da je jednačina $x^2ax = a^{-1}$ rešiva po x u grupi G ako i samo ako postoji $b \in G$ takvo da je $b^3 = a$.

Uputstvo. Dokazati da iz $x^2axa = e$ sledi $xaxax = e$.

68. Neka je G konačna grupa i neka je n ceo broj uzajamno prost sa redom grupe G . Dokazati da za svaki element g grupe G jednačina $x^n = g$ ima jedinstveno rešenje.

Rešenje. Neka je k red grupe G . Kako je $\text{nzd}(k, n) = 1$, to postoje celi brojevi u i v takvi da je $ku + nv = 1$. Neka je $x = g^v$. Tada je

$$x^n = (g^v)^n = g^{nv} = g^{ku+nv} = g.$$

Ako je $x^n = y^n$, tada je

$$x = x^{ku+nv} = (x^n)^v = (y^n)^v = y^{ku+nv} = y.$$

69. Dokazati da u Priferovoj grupi G (zadatak 8) jednačina $x^n = g$ ima rešenje za svako $g \in G$ i svaki prirodan broj n .

Rešenje. Neka je p^r red elementa g . Tada je g oblika

$$g = \cos \frac{2m\pi}{p^r} + i \sin \frac{2m\pi}{p^r}, \quad 1 \leq m < p^r, \quad \text{nzd}(m, p) = 1.$$

Neka je $n = p^s k$, gde $s \in \mathbb{N} \cup \{0\}$ i $\text{nzd}(k, p) = 1$. Ako je $h_0 = \cos \frac{2m\pi}{p^{r+s}} + i \sin \frac{2m\pi}{p^{r+s}}$, tada je $h_0^{p^s} = g$. Međutim, k i p su uzajamno prosti, pa postoje celi brojevi a i b takvi da je $ak + bp^{r+s} = 1$ zbog čega je

$$h_0 = h_0^{ak+bp^{r+s}} = h_0^{ak} h_0^{bp^{r+s}} = h_0^{ak}.$$

Neka je $h = h_0^a$. Dobija se da je

$$h^n = (h_0^a)^{kp^s} = (h_0^{ak})^{p^s} = h_0^{p^s} = g.$$

70. Neka je G konačna grupa reda n . Ako je n parno, onda je broj rešenja u G jednačine $x^2 = e$ paran (tj. u G ima neparan broj elemenata reda 2). Dokazati.

Rešenje. $x^2 = e$ ako i samo ako je $x = x^{-1}$. To znači da treba odrediti broj skupova $\{x, x^{-1}\}$ koji su jednočlani. S obzirom da je $e = e^{-1}$ i

$$G = \{e\} \cup \{x, x^{-1}\} \cup \{y, y^{-1}\} \cup \dots,$$

a G ima paran broj elemenata, sledi da jednačina $x^2 = e$ ima u G paran broj rešenja. (Svako rešenje jednačine $x^2 = e$, sem e , je element reda 2, pa prema tome u G ima neparan broj elemenata reda 2.)

71. Neka je G konačna grupa reda n . Dokazati da je n neparan broj ako i samo ako je svaki element iz G kvadrat (tj. ako za svako $a \in G$ postoji $b \in G$ tako da je $a = b^2$).

Rešenje. Ako je $n = 2k + 1$, onda je za svako $a \in G$ $a^{2k+1} = e$, tj. $(a^{k+1})^2 = a$.

Obrnuto, pretpostavimo da za svako $a \in G$ postoji $b \in G$ tako da je $a = b^2$. Ako pretpostavimo da je n paran broj, onda na osnovu zadatka 70 sledi da postoji $a_1 \in G$ takvo da je $a_1^2 = e$ i $a_1 \neq e$. To znači da se u nizu kvadrata svih elemenata grupe G

$$e^2, a_1^2, a_2^2, \dots, a_{n-1}^2$$

element e pojavljuje dva puta, dakle, postoji element $a_i \in G$ koji se u gornjem nizu uopšte ne pojavljuje tj. a_i nije kvadrat. Iz ove protivrečnosti sledi da je n neparan broj.

72. Neka je G grupa i neka su $a, b \in G$.

a) Ako važi $a^2 = e$ i $b^2 a = ab^3$, dokazati da je $b^5 = e$.

b) Ako važi $a^k = e$ i $b^r a = ab^s$, gde su k, r i s prirodni brojevi i $r \neq s$, dokazati da tada postoji prirodan broj n takav da je $b^n = e$ i naći bar jedan takav prirodan broj.

Rešenje.

$$\text{a) } b^5 = b^5 a^2 = b^3 ab^3 a = bab^6 a = bab^4 ab^3 = bab^2 ab^6 = ba^2 b^9 = b^{10},$$

odakle sledi $b^5 = e$.

b) Ovo je generalizacija tvrđenja pod a) i u njenom dokazivanju primenićemo postupak sličan prethodnom.

Neka je $s > r$.

$$\begin{aligned} b^{r^k} &= b^{r^k} a^k = ab^{r^{k-1}s} a^{k-1} = a^2 b^{r^{k-2}s^2} a^{k-2} = \dots = \\ &= a^{k-1} b^{rs^{k-1}} a = b^{s^k}, \end{aligned}$$

odakle sledi

$$b^{s^k - r^k} = e.$$

73. Neka za elemente a, b grupe G važi $ab^3 = b^2a$ i $ba^3 = a^2b$. Dokazati da je $a = b = e$.

Rešenje. Primenjujući date relacije dobijamo da važe sledeće jednakosti

$$(1) \quad a^2 b^3 = ba^3 b^2 = bababa^3,$$

$$a^2 b^3 = ab^2 a,$$

pa je

$$bababa^3 = ab^2 a,$$

tj.

$$bababa^2 = ab^2,$$

$$(2) \quad abababa^2 = a^2 b^2.$$

Dalje je

$$(3) \quad a^2 b^2 = ba^3 b = baba^3,$$

pa iz (2) i (3) sledi

$$ababab = baba,$$

a odavde je

$$bababab = b^2aba = ab^4a = ab^2ab^3 = a^2b^6.$$

Iz poslednjeg niza jednakosti se dobija

$$(4) \quad bababa = a^2b^5.$$

Iz (1) sledi

$$a^2b^5 = bababa^3b^2 = babababa^3b = (ba)^4ba^3,$$

pa odavde i iz (4) imamo

$$e = baba^3,$$

i na osnovu (3)

$$e = a^2b^2,$$

tj. $a^2 = b^{-2}$. Stavljajući u drugu od datih jednakosti b^{-1} umesto a^2 biće

$$b^{-1}a = b^{-1},$$

tj. $a = b = e$.

74. U grupi G elementi

a) a i a^{-1} ,

b) a i $b^{-1}ab$,

c) ab i ba ,

imaju isti red. Dokazati.

Rešenje.

$$a) \quad (a^{-1})^{|a|} = (a^{|a|})^{-1} = e^{-1} = e,$$

odakle sledi da je

$$|a^{-1}| \leq |a|,$$

(sa $|a|$ označavamo red elementa a). Slično

$$a^{|a^{-1}|} = ((a^{-1})^{-1})^{|a^{-1}|} = ((a^{-1})^{|a^{-1}|})^{-1} = e^{-1} = e,$$

odakle je

$$|a| \leq |a^{-1}|.$$

Iz ovih dveju nejednakosti sledi $|a| = |a^{-1}|$.

b) Lako se može dokazati da je za svako $n \in \mathbb{Z}$

$$(b^{-1}ab)^n = b^{-1}a^n b,$$

pa je

$$(b^{-1}ab)^{|a|} = b^{-1}a^{|a|}b = e,$$

tj.

$$|b^{-1}ab| \leq |a|.$$

Takođe je

$$a^{|b^{-1}ab|} = bb^{-1}a^{|b^{-1}ab|}bb^{-1} = b(b^{-1}ab)^{|b^{-1}ab|}b^{-1} = e,$$

tj.

$$|a| \leq |b^{-1}ab|,$$

pa je $|b^{-1}ab| = |a|$.

c) Elementi ab i ba su konjugovani ($ab = b^{-1}(ba)b$), pa iz tvrđenja dokazanog pod b) sledi traženi zaključak.

75. Neka su a i b elementi grupe G , $b \neq e$, takvi da je $a^5 = e$ i $aba^{-1} = b^2$. Odrediti red elementa b .

Rešenje. Iz $aba^{-1} = b^2$ se množenjem sleva sa a i zdesna sa a^{-1} dobija da je

$$a^2ba^{-2} = ab^2a^{-1} = (aba^{-1})(aba^{-1}) = b^2b^2 = b^4.$$

Ponavljajući ovaj postupak dobija se da je $b = a^5ba^{-5} = b^{32}$, pa je $b^{31} = e$. Red elementa b je delitelj prostog broja 31, $b \neq e$, pa je red $b = 31$.

76. Dokazati da u grupi G definisanoj u zadatku 3

a) postoji beskonačno mnogo elemenata reda 2,

b) ne postoji nijedan element reda 3.

Rešenje. U grupi G neutralni element je $(1, 0)$. Za svako $a \in \mathbb{R}$

$$(-1, a) * (-1, a) = (1, -a + a) = (1, 0),$$

pa je $(-1, a)$ element reda 2. Prema tome, u G ima beskonačno mnogo elemenata reda 2.

b) Ako pretpostavimo da je (a, b) element reda 3, onda je

$$(1, 0) = (a, b)^3 = (a^3, b(a^2 + a + 1))$$

odakle sledi da je $a = 1$, $b = 0$, tj. $(a, b) = (1, 0)$, pa je (a, b) neutralni element. To znači da u G nema elemenata reda 3.

77. Neka je u grupi G element a reda p , a element b reda q . Ako je $ab = ba$ i p i q su uzajamno prosti brojevi, dokazati da je tada element ab reda pq .

78. Neka je G Abelova grupa neparnog reda. Dokazati da je proizvod svih elemenata grupe G neutralni element te grupe.

Rešenje. Pošto je red elementa delitelj reda grupe, a red grupe G je neparan broj, u grupi nema elemenata reda 2. Za svako $g \in G$ jednačina $gx = e$ ima jednoznačno rešenje $x \neq g$, pa se elementi grupe G mogu prikazati na sledeći način

$$g_1, g_2, \dots, g_n, g_1^{-1}, g_2^{-1}, \dots, g_n^{-1}, e,$$

a njihov proizvod je e .

79. Neka je G konačna Abelova grupa. Dokazati da je proizvod svih elemenata grupe G :

- a) e , ako u G nema elemenata reda 2 ili ima bar dva elementa reda 2.
- b) g , ako u G postoji jedinstven element g reda 2.

80. Ako grupa G sadrži tačno jedan element a reda 2, onda je za svako $x \in G$ $xa = ax$. Dokazati.

Rešenje. Elementi a i $x^{-1}ax$ za svako $x \in G$ imaju isti red (zadatak 74). To znači da je $x^{-1}ax$ reda 2, a kako je a po pretpostavci jedini element reda 2 u grupi G , sledi da je

$$a = x^{-1}ax, \quad \text{tj.} \quad xa = ax, \quad \text{za svako} \quad x \in G.$$

81. Neka su x i y elementi grupe G takvi da je za svaki element $g \in G$ $(xy)g = g(xy)$. Dokazati da je $xy = yx$.

Rešenje.

$$yx = x^{-1}(xy)x = (xy)x^{-1}x = xy.$$

82. Neka su a, b elementi grupe G , $a \neq e$, $b \neq e$, za koje važi $a^3 = b^4 = e$ i $ba = ab^3$. Izračunati red elemenata ab i ba .

Rešenje. Iz $a(ba)ba = a(ab^3)ba = a^2b^4a = e$ sledi da je

$$(*) \quad bab = a^3baba^3 = a^2(ababa)a^2 = a^4 = a.$$

S druge strane je

$$b^2 = (ababa)b(ababa)b = a(bab)a(bab)a(bab) = a^6 = e.$$

Iz ove jednakosti i (*) sledi da je $ab = ba$. Uzastopnim stepenovanjem ab se dobija da je $(ab)^i \neq e$, $i = 1, 2, \dots, 5$, $(ab)^6 = e$, pa je red ab 6.

83. Neka je G konačna grupa reda n a k ceo broj uzajamno prost sa n . Dokazati da je preslikavanje $f : G \rightarrow G$ definisano sa $f(x) = x^k$ permutacija skupa G . (Drugim rečima, ako se svaki element grupe G stepenuje brojem k , dobija se opet ceo skup G .)

Rešenje. Pretpostavimo da postoje $a, b \in G$ tako da je

$$a^k = b^k, \quad a \neq b.$$

Ako je p red elementa a , a q red elementa b , onda je

$$(a^k)^p = (b^k)^p = e,$$

odakle sledi da je q delitelj broja kp . Kako je red elemenata delitelj reda grupe, q i k su uzajamno prosti brojevi, pa je q delitelj broja p .

Analognim postupkom se može pokazati da je i p delitelj q , što znači da je $p = q$.

k i p su uzajamno prosti brojevi, dakle, postoje celi brojevi s i t tako da je $sk + tp = 1$, pa je

$$a^{ks-1} = a^{tp} = e,$$

odakle je $a = a^{ks}$. Slično je i $b = b^{ks}$, pa je konačno

$$(a^k)^s = (b^k)^s, \quad \text{tj.} \quad a = b.$$

Pokazali smo da u skupu k -tih stepena svih elemenata iz G nema jednakih, to je konačan skup sa n elemenata, pa sledi traženi zaključak.

84. Ako je G grupa sa bar dva elementa i svi elementi iz G različiti od neutralnog imaju isti konačan red n , onda je n prost broj. Dokazati.

Uputstvo. Pretpostaviti da je $n = pq$, $1 < p < n$ i naći red elementa $a^p \neq e$.

85. (Mala Fermaova teorema) Ako je a ceo broj a p prost broj, onda je

$$a^p \equiv a \pmod{p}.$$

Dokazati.

Rešenje. Grupa $(\mathbb{Z}_p \setminus \{\bar{0}\}, \cdot)$ ima $p - 1$ element, pa je, s obzirom da red svakog elementa deli red grupe, za svaki ceo broj a za koji je $\bar{a} \neq \bar{0}$

$$(\bar{a})^{p-1} = \bar{1},$$

ili

$$a^{p-1} \equiv 1 \pmod{p}, \quad (a \not\equiv 0 \pmod{p}).$$

Množeći sa a gornju kongruenciju dobijamo

$$a^p \equiv a \pmod{p}, \quad \text{za svako } a \not\equiv 0 \pmod{p}.$$

Međutim, ova kongruencija očividno važi i za $a \equiv 0 \pmod{p}$, pa je time teorema u potpunosti dokazana.

86. Dokazati da u grupi mogu da postoje elementi konačnog reda čiji je proizvod beskonačnog reda.

Rešenje. U multiplikativnoj grupi regularnih matrica formata 2×2 takvi elementi su matrice

$$\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}.$$

87. Dati primer grupe beskonačnog reda čiji svi elementi imaju konačan red.

Rešenje. Priferova grupa definisana u zadatku 8 ima to svojstvo.

88. Grupa G u kojoj svaki element sem neutralnog ima red 2 mora biti Abelova. Dokazati.

Rešenje. Iz

$$(ab)^2 = e,$$

množenjem zdesna sa b a sleva sa a (i koristeći da je $a^2 = b^2 = e$) dobijamo za svako $a, b \in G$

$$ab = ba.$$

89. Neprazan podskup H grupe G je podgrupa ako i samo ako iz $x, y \in H$ sledi $xy^{-1} \in H$. Dokazati.

90. Neprazan podskup H grupe G je podgrupa ako i samo ako je $hH = H$, za svako $h \in H$. Dokazati.

91. Konačan neprazan podskup H grupe G je podgrupa ako i samo ako iz $x, y \in H$ sledi $xy \in H$. Dokazati.

92. Neka je $X = \{x_1, x_2, \dots, x_n\}$ podskup grupe G za koji važi

$$x_i x_j \in X \quad \text{za} \quad 1 \leq i \leq j \leq n.$$

Dokazati da je X podgrupa grupe G .

Uputstvo. Dokazati najpre da $x_i^m \in X$ za svako $i \in \{1, \dots, n\}$ i svako $m \in \mathbb{N}$, i da iz toga sledi $x_i^{-1} \in X$. Dokazati zatim da ako je $x_i X = X$ tada je i $x_i^{-1} X = X$. Na kraju dokazati da je $x_j X = X$ za svako $j \in \{1, \dots, n\}$ i primeniti zadatak 90.

93. Dokazati da elementi konačnog reda Abelove grupe čine podgrupu.

Rešenje. U Abelovoj grupi G skup svih elemenata konačnog reda označimo sa H . Ako su $a, b \in H$, onda je $a^n = e$, $b^m = e$, pa je

$$(ab^{-1})^{nm} = a^{nm}(b^{-1})^{nm} = a^{nm}(b^{nm})^{-1} = e,$$

što znači da je

$$|ab^{-1}| < \infty.$$

Prema tome, $ab^{-1} \in H$, pa je H podgrupa.

94. Ako svi elementi beskonačnog reda Abelove grupe G zajedno sa neutralnim elementom čine podgrupu H , dokazati da tada G nema elemente konačnog reda (osim e).

Rešenje. Neka je element $a \in G$ konačnog reda, a $b \in G$ beskonačnog reda. Lako se proverava da je $c = ab$ beskonačnog reda. Tada je $a = cb^{-1} \in H$, tj. $a = e$.

1.4 Homomorfizam, izomorfizam

95. Dokazati da je preslikavanje $f : x \mapsto i^x$ homomorfizam grupe $(\mathbb{Z}, +)$ u grupu $(\{1, -1, i, -i\}, \cdot)$ i naći jezgro tog homomorfizma ($i^2 = -1$).

Rešenje. $f(a+b) = i^{a+b} = i^a \cdot i^b = f(a) \cdot f(b)$, za svako $a, b \in \mathbb{Z}$, a to znači da je f homomorfizam grupe $(\mathbb{Z}, +)$ u grupu $(\{1, -1, i, -i\}, \cdot)$. Preslikavanje je očevидno surjektivno, pa je f epimorfizam.

Jezgro $\text{Ker } f$ ovog homomorfizma je skup svih $a \in \mathbb{Z}$ za koje je $f(a) = 1$, tj. $i^a = 1$. Dakle,

$$\text{Ker } f = \{4k \mid k \in \mathbb{Z}\}.$$

96. Grupa $(\mathbb{Z}, +)$ se preslikava na grupu $(\mathbb{Z}_6, +)$ funkcijom $f : a \mapsto \bar{a}$. Dokazati da je f homomorfizam.

97. Sledeće funkcije preslikavaju multiplikativnu grupu nenula racionalnih brojeva u sebe:

a) $x \mapsto \frac{1}{x},$

b) $x \mapsto |x|,$

c) $x \mapsto x^n, \quad n \text{ fiksiran ceo broj,} \quad \text{d) } x \mapsto -x.$

Koje od tih funkcija su homomorfizmi? Za one funkcije koje su homomorfizmi odrediti homomorfne slike i jezgra. Koje funkcije su epimorfizmi, a koje monomorfizmi?

98. Neka je G multiplikativna grupa kompleksnih brojeva čiji je modul jednak jedinici. Dokazati da je preslikavanje

$$e^{i\theta} \mapsto e^{ki\theta}, \quad k \text{ fiksiran ceo broj,}$$

endomorfizam i odrediti jezgro.

99. Grupa G_2 je homomorfna slika grupe G_1 . Tada:

a) Ako je G_1 Abelova i G_2 je Abelova grupa.

b) Slika neutralnog elementa grupe G_1 je neutralni element grupe G_2 .

c) Ako je a^{-1} inverzni element elementa $a \in G_1$, onda je $f(a^{-1})$ inverzni element elementa $f(a) \in G_2$. (f je homomorfizam grupe G_1 na grupu G_2 .)

Dokazati.

Rešenje.

a) Za svako $a_2, b_2 \in G_2$ postoje $a_1, b_1 \in G_1$ tako da je

$$f(a_1) = a_2, \quad f(b_1) = b_2,$$

pa je

$$a_2 b_2 = f(a_1) f(b_1) = f(a_1 b_1) = f(b_1 a_1) = f(b_1) f(a_1) = b_2 a_2.$$

b) Za svako $a_2 \in G_2$ postoji $a_1 \in G_1$ tako da je $f(a_1) = a_2$, pa ako je e_1 neutralni element grupe G_1 iz

$$a_1 e_1 = e_1 a_1 = a_1,$$

sledi

$$f(a_1)f(e_1) = f(e_1)f(a_1) = f(a_1)$$

ili

$$a_2 f(e_1) = f(e_1) a_2 = a_2,$$

što znači da je slika neutralnog elementa e_1 grupe G_1 neutralni element e_2 grupe G_2 .

c) Iz $aa^{-1} = e_1$, sledi $f(a)f(a^{-1}) = f(e_1) = e_2$, tj. $(f(a))^{-1} = f(a^{-1})$.

100. Neka je $f : G_1 \rightarrow G_2$ izomorfizam grupe G_1 na grupu G_2 . Ako je $g_2 = f(g_1)$, dokazati da je red elementa $g_1 \in G_1$ jednak redu elemenata $g_2 \in G_2$.

101. Dokazati da je u skupu grupa istog reda izomorfizam relacija ekvivalencije.

Rešenje.

(i) Identičko preslikavanje grupe G na sebe je izomorfizam, pa je uvek $G \cong G$.

(ii) Neka je f izomorfizam grupe G_1 na grupu G_2 . Tada je inverzno preslikavanje f^{-1} takođe bijekcija. Ako su $b_1, b_2 \in G_2$, onda, s obzirom da je f surjektivno preslikavanje, postoje $a_1, a_2 \in G_1$ tako da je $f(a_1) = b_1$, $f(a_2) = b_2$, tj. $f^{-1}(b_1) = a_1$, $f^{-1}(b_2) = a_2$. Kako je

$$f(a_1 a_2) = f(a_1) f(a_2) = b_1 b_2,$$

biće

$$f^{-1}(b_1 b_2) = f^{-1}(f(a_1 a_2)) = a_1 a_2 = f^{-1}(b_1) f^{-1}(b_2),$$

što znači da je f^{-1} izomorfizam grupe G_2 na grupu G_1 , dakle, $G_2 \cong G_1$.

(iii) Neka je f izomorfizam grupe G_1 na grupu G_2 , a h izomorfizam grupe G_2 na grupu G_3 . Tada funkcija $g = hf$ bijektivno preslikava grupu G_1 na grupu G_3 . Ako su $a_1, a_2 \in G_1$, onda je

$$g(a_1 a_2) = (hf)(a_1 a_2) = h(f(a_1) f(a_2)) = (hf)(a_1) (hf)(a_2) = g(a_1) g(a_2),$$

a to znači da je $G_1 \cong G_3$.

Time je pokazano da je izomorfizam grupa refleksivna, simetrična i tranzitivna relacija.

102. Dokazati da je grupa $(\mathbb{Z}_4, +)$ izomorfna grupi $(G, *)$, gde je $G = \{a, b, c, d\}$ a operacija $*$ je zadata sledećom Kejljevom tablicom:

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Rešenje. Formiraćemo Kejljevu tablicu za grupu $(\mathbb{Z}_4, +)$:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Ako je $f : \mathbb{Z}_4 \rightarrow G$ izomorfizam, onda na osnovu zadatka 99 mora biti $f(\bar{0}) = a$ (a je neutralni element grupe G). Element $\bar{2}$ je sam sebi inverzan, pa na osnovu zadatka 99 njegova slika mora biti element koji je sam sebi inverzan, jedini takav element u G je c , dakle, $f(\bar{2}) = c$. Prema tome, f preslikava

$$\bar{1} \mapsto b, \bar{3} \mapsto d \quad \text{ili} \quad \bar{1} \mapsto d, \bar{3} \mapsto b.$$

Ispitajmo da li je funkcija koja preslikava

$$\bar{0} \mapsto a, \bar{1} \mapsto b, \bar{2} \mapsto c, \bar{3} \mapsto d$$

izomorfizam dveju datih grupa. Da to utvrdimo proverićemo da li je $f(x + y) = f(x) * f(y)$ za svaki par elemenata iz $\mathbb{Z}_4$. Na primer, $\bar{1} + \bar{2} = \bar{3}$, a $f(\bar{1}) * f(\bar{2}) = b * c = d$, pa treba utvrditi da li je $f(\bar{3}) = d$?

U našem primeru ova jednakost je tačna i nastavljajući taj postupak za sve parove elemenata iz $\mathbb{Z}_4$ vidimo da je ovako definisana funkcija f zaista izomorfizam.

Na sličan način se može pokazati da je i funkcija

$$g : \bar{0} \mapsto a, \quad \bar{1} \mapsto d, \quad \bar{2} \mapsto c, \quad \bar{3} \mapsto b$$

takođe jedan izomorfizam grupa $(\mathbb{Z}_4, +)$ i $(G, *)$.

103. Dokazati da su grupe $(\mathbb{Z}_4, +)$ i $(\mathbb{Z}_5 \setminus \{\bar{0}\}, \cdot)$ izomorfne.

104. Dokazati da je grupa definisana u zadatku 28 kada je polje $F = \mathbb{Z}_p$ izomorfna grupi definisanoj u zadatku 33.

Uputstvo. Koristiti preslikavanje f definisano sa

$$f : (a, b, c) \mapsto \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}.$$

105. Kako se grupa $(\mathbb{Z}_3, +)$ može homomorfno preslikati u grupu $(\mathbb{Z}_2, +)$?

106. Neka je $(F, +, \cdot)$ polje. Definišimo novu binarnu operaciju $*$ na F sa

$$a * b = a + b - ab.$$

Dokazati:

a) $(F \setminus \{1\}, *)$ je grupa.

b) $(F \setminus \{1\}, *) \cong (F \setminus \{0\}, \cdot)$.

Uputstvo. Koristiti da je $a * b = 1 - (1 - a)(1 - b)$.

107. Dati su skupovi

$$G = \{1, -1, i, -i\} \quad \text{i} \quad A = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \subseteq \mathbb{Z}_8.$$

Dokazati da grupa $(G, \cdot)$ nije izomorfna sa grupom $(A, \cdot)$, pri čemu je u G operacija $\cdot$ množenje kompleksnih brojeva, a $\cdot$ u A je množenje klasa ostataka po modulu 8.

108. Dokazati da se simetrična grupa S_n može homomorfno preslikati na grupu sa dva elementa.

109. Homomorfizam grupe G_1 u grupu G_2 je monomorfizam ako i samo ako je jezgro tog homomorfizma neutralni element e_1 grupe G_1 . Dokazati.

Rešenje. Pretpostavimo da je f monomorfizam i da jezgro sadrži neki element $a \neq e_1$. Tada je

$$f(a) = f(e_1) = e_2,$$

gde je e_2 je neutralni element grupe G_2 , a to je u protivrečnosti sa pretpostavkom da je f monomorfizam (dva različita elementa imaju istu sliku). Prema tome, $\text{Ker } f = \{e_1\}$.

Obrnuto, pretpostavimo da je $\text{Ker } f = \{e_1\}$ i f nije monomorfizam, tj. da je $f(a) = f(b)$, $a \neq b$. Onda je

$$f(ab^{-1}) = f(a) \cdot (f(b))^{-1} = e_2,$$

pa element ab^{-1} pripada jezgru, što znači da mora biti $ab^{-1} = e_1$, tj. $a = b$. Ovo je protivrečnost, pa je, dakle, f monomorfizam.

110. Neka je f homomorfizam grupe G_1 u grupu G_2 , a g homomorfizam grupe G_2 u grupu G_3 . Ako je fg izomorfizam, dokazati da onda f mora biti epimorfizam a g mora biti monomorfizam.

111. Dokazati da je grupa G Abelova ako i samo ako je preslikavanje $f : a \mapsto a^{-1}$ automorfizam te grupe.

Rešenje. Neka je G Abelova grupa. f je injektivno preslikavanje, jer iz $f(a) = f(b)$, tj. $a^{-1} = b^{-1}$, sledi $a = b$. f je surjektivno preslikavanje jer je svaki element a slika elementa a^{-1} . Za svako $a, b \in G$ je

$$f(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a)f(b),$$

pa je f automorfizam.

Obrnuto, ako je preslikavanje $f : a \mapsto a^{-1}$ automorfizam, onda je $(ab)^{-1} = a^{-1}b^{-1}$, za svako $a, b \in G$, a s obzirom da je u svakoj grupi $(ab)^{-1} = b^{-1}a^{-1}$, sledi $a^{-1}b^{-1} = b^{-1}a^{-1}$, a odatle je za svako $a, b \in G$ $ab = ba$.

112. Na skupu

$$A = \left\{ x \mid x \in \mathbb{R}, -\frac{\pi}{2} < x < \frac{\pi}{2} \right\},$$

definisati operaciju $*$ tako da bude $(\mathbb{R}, +) \cong (A, *)$.

Rešenje. Ako je f izomorfizam $\mathbb{R} \rightarrow A$, onda je inverzno preslikavanje f^{-1} izomorfizam $A \rightarrow \mathbb{R}$, tj. za svako $a, b \in A$

$$f^{-1}(a * b) = f^{-1}(a) + f^{-1}(b),$$

što je ekvivalentno sa

$$a * b = f(f^{-1}(a) + f^{-1}(b)).$$

Dovoljno je, prema tome, naći bilo koju funkciju koja bijektivno preslikava $\mathbb{R}$ na A i pomoću nje kao što je pokazano definisati operaciju $*$.

Na primer, $f(x) = \arctg x$ preslikava bijektivno $\mathbb{R}$ na A , pa je

$$a * b = \arctg(\operatorname{tg} a + \operatorname{tg} b).$$

Lako se proverava da je funkcija $\arctg x$ izomorfizam grupa $(\mathbb{R}, +)$ i $(A, *)$.

113. Dokazati da je multiplikativna grupa n -tih korena iz jedinice (zadatak 5) izomorfna sa grupom $(\mathbb{Z}_n, +)$ (zadatak 12).

114. Skup matrica

$$A = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R}, a^2 + b^2 \neq 0 \right\}$$

je multiplikativna grupa. Dokazati ovo uspostavljajući izomorfizam grupoida $(A, \cdot)$ sa multiplikativnom grupom nenula kompleksnih brojeva.

115. Neka je u multiplikativnoj grupi regularnih matrica reda 2 skup G generisan matricama

$$R = \begin{bmatrix} \cos \frac{2\pi}{n} & \sin \frac{2\pi}{n} \\ -\sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

pri čemu je $n > 1$ fiksiran prirodan broj. Dokazati:

- a) G je konačna nekomutativna grupa u odnosu na množenje matrica.
- b) Grupa G je izomorfna diedarskoj grupi D_n (zadatak 16 d)).

Uputstvo. Dokazati da je preslikavanje $f : G \rightarrow D_n$ takvo da je $f(R) = r$ i $f(S) = s$ izomorfizam.

116. Dokazati da su grupe definisane u zadacima 26 i 217 izomorfne diedarskoj grupi D_n (zadatak 16 d)).

117. Neka je $G = \{x \mid x \in \mathbb{R}, x^2 < 1\}$. Dokazati da je $(G, *)$, gde je $*$ definisano sa

$$x * y = \frac{x + y}{1 + xy},$$

grupa izomorfna grupi $(\mathbb{R}, +)$.

Uputstvo. Posmatrati funkciju $f : G \rightarrow \mathbb{R}$ definisanu sa

$$f(x) = \log \frac{1+x}{1-x}.$$

118. Skup svih regularnih matrica formata 2×2 sa elementima iz $\mathbb{Z}_2$ (v. zadatak 25) je multiplikativna grupa izomorfna simetričnoj grupi S_3 . Dokazati.

119. Dokazati da je skup svih regularnih linearnih transformacija n -dimenzionalnog vektorskog prostora nad poljem F u odnosu na kompoziciju preslikavanja grupa izomorfna multiplikativnoj grupi regularnih kvadratnih matrica formata $n \times n$ nad poljem F .

PRIMEDBA. Taj izomorfizam, kao što je poznato, zavisi od izbora baze u vektorskom prostoru, pa, u opštem slučaju, postoji više različitih izomorfizama između ove dve grupe.

120. Sledeće grupe su grupe reda 8:

- a) $(\mathbb{Z}_8, +)$,
- b) grupa simetrija kvadrata (zad. 16),
- c) $(G, \cdot)$, gde je $G = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\} \subseteq \mathbb{Z}_{15}$,
- d) $(\mathcal{P}(S), \Delta)$, gde je $\mathcal{P}(S)$ partitivni skup skupa $S = \{a, b, c\}$, a Δ simetrična razlika skupova (zad. 38).

Dokazati da među ovim grupama nema izomorfni.

Rešenje. Za svaku od datih grupa navešćemo jedno svojstvo koje ta grupa ima a ostale nemaju, odakle sledi da nijedne dve od tih grupa ne mogu biti izomorfne.

- a) Grupa je ciklička.
- b) Grupa nije komutativna.
- c) Grupa je komutativna, nije ciklička i ima element reda 4 (to je $\bar{2}$).
- d) Svaki element grupe, sem neutralnog, je reda 2.

121. Dokazati da grupe $(\mathbb{Q}_p, +)$ i $(\mathbb{Q}^p, +)$ nisu izomorfne (zadaci 36 i 37).

Uputstvo. Pretpostaviti suprotno, tj. da je $f : \mathbb{Q}_p \rightarrow \mathbb{Q}^p$ izomorfizam

grupe $\mathbb{Q}_p$ na $\mathbb{Q}^p$. Koristiti da za svako $x \in \mathbb{Q}_p$ i za svaki prost broj q različit od p , postoji $y \in \mathbb{Q}_p$ takvo da je $\underbrace{y + \dots + y}_q = x$. Tada bi bilo

$$f(\underbrace{y + \dots + y}_q) = f(y) + \dots + f(y) = f(x),$$

tj. svako $z \in \mathbb{Z}^p$ bi se moglo napisati kao zbir q sabiraka, što je nemoguće.

122. Dokazati da grupe iz zadataka 33 i 34 nisu izomorfne.

Uputstvo. Grupa iz zadatka 34 ima element reda p^2 . Koristiti zadatak 100.

123. Skup $\text{Hom}(G, A)$ definišemo kao skup svih homomorfizama grupe G u Abelovu grupu A . Kako se množenje homomorfizama može pogodno definisati pa da $\text{Hom}(G, A)$ bude Abelova grupa?

124. Naći grupu permutacija izomorfnu sa grupom $(\mathbb{Z}_4, +)$.

Rešenje. Na osnovu Kejljeve teoreme (1.34) grupa $\mathbb{Z}_4$ je izomorfna sa podgrupom grupe S_4 . Označimo sa $f_{\bar{0}}, f_{\bar{1}}, f_{\bar{2}}, f_{\bar{3}}$ permutacije grupe S_4 koje odgovaraju respektivno elementima $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ grupe $\mathbb{Z}_4$. Tada je $f_{\bar{1}}$ permutacija koja elemente $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ preslikava respektivno u $\bar{1} + \bar{0}, \bar{1} + \bar{1}, \bar{1} + \bar{2}, \bar{1} + \bar{3}$, tj. u $\bar{1}, \bar{2}, \bar{3}, \bar{0}$, ($f_{\bar{1}}(x) = \bar{1} + x$, za svako $x \in \mathbb{Z}_4$).

Slično dobijamo i ostale permutacije:

$$\begin{aligned} f_{\bar{1}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{1} & \bar{2} & \bar{3} & \bar{0} \end{pmatrix}, & f_{\bar{2}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{2} & \bar{3} & \bar{0} & \bar{1} \end{pmatrix}, \\ f_{\bar{3}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{3} & \bar{0} & \bar{1} & \bar{2} \end{pmatrix}, & f_{\bar{0}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{0} & \bar{1} & \bar{2} & \bar{3} \end{pmatrix}. \end{aligned}$$

Ako ove permutacije skupa $\mathbb{Z}_4$ interpretiramo kao permutacije skupa $\{1, 2, 3, 4\}$ biće

$$f_1 = [2341], \quad f_2 = [3412],$$

$$f_3 = [4123], \quad f_0 = [1234].$$

Na osnovu Kejljeve teoreme skup permutacija $\{f_{\bar{0}}, f_{\bar{1}}, f_{\bar{2}}, f_{\bar{3}}\}$ čini grupu u odnosu na množenje permutacija izomorfnu grupi $(\mathbb{Z}_4, +)$. Takođe je i podgrupa $\{f_0, f_1, f_2, f_3\}$ simetrične grupe S_4 izomorfna sa $(\mathbb{Z}_4, +)$.

125. Za grupu $(\{1, -1, i, -i\}, \cdot)$ naći izomorfnu grupu permutacija.

126. Naći podgrupu simetrične grupe S_6 izomorfnu simetričnoj grupi S_3 .

127. Naći grupu regularnih matrica formata 3×3 izomorfnu simetričnoj grupi S_3 .

Rešenje. Svaka grupa permutacija skupa od n elemenata izomorfna je nekoj multiplikativnoj grupi permutacionih⁴ matrica formata $n \times n$. (Oдавde na osnovu Kejljeve teoreme odmah sledi da je svaka konačna grupa reda n izomorfna sa nekom grupom permutacionih matrica formata $n \times n$.)

Formirajmo sada grupu matrica izomorfnu grupi

$$S_3 = \{[123], [231], [132], [321], [213], [312]\}.$$

Permutaciji $[123]$ odgovara jedinična matrica

$$E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

permutaciji $[213]$ odgovara matrica koja se dobija od jedinične kada se njene vrste permutuju onako kako to propisuje permutacija (1 se preslikava u 2 – to znači da se prva vrsta jedinične matrice premešta na mesto druge itd.):

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Na ovaj način dobijamo i preostale matrice:

$$\begin{aligned} [132] &\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, & [321] &\mapsto \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \\ [231] &\mapsto \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, & [312] &\mapsto \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}. \end{aligned}$$

⁴Matrica u kojoj se u svakoj vrsti i koloni nalazi tačno jedna jedinica, a svi ostali elementi su nule naziva se permutaciona matrica (to je, dakle, matrica dobijena od jedinične matrice permutovanjem njenih vrsta).

Ovih šest matrica čine multiplikativnu grupu izomorfnu grupi S_3 .

128. Naći grupu matrica izomorfnu grupi $(\mathbb{Z}_4, +)$.

Uputstvo. Koristiti zadatke 124 i 127.

1.5 Cikličke i Abelove grupe

129. Neka je G grupa u kojoj za svako $a, b, c, x, y \in G$

$$xay = bac \Rightarrow xy = bc.$$

Dokazati da je G Abelova grupa.

Rešenje. Iz $(xy)xe = ex(yx)$ sledi $xy = yx$.

130. Dokazati da je grupa G Abelova ako i samo ako je za svako $a, b \in G$

$$(ab)^2 = a^2b^2.$$

Rešenje. U Abelovoj grupi G je

$$(ab)^2 = (ab)(ab) = a(ba)b = (aa)(bb) = a^2b^2.$$

Obrnuto, neka je za svako $a, b \in G$

$$(ab)^2 = a^2b^2.$$

Odavde sledi

$$(ab)(ab) = (aa)(bb)$$

ili

$$a(ba)b = a(ab)b.$$

Pomnožimo li ovu jednakost sleva sa a^{-1} , a zdesna sa b^{-1} , dobijamo

$$ba = ab,$$

za svako $a, b \in G$.

131. Neka je G konačna grupa čiji red nije deljiv sa 3 i u kojoj važi $(xy)^3 = x^3y^3$ za svako $x, y \in G$. Dokazati da je G Abelova grupa.

Rešenje. Na osnovu prethodnog zadatka $y^2 \in \mathcal{Z}(G)$, pa je

$$(xy)^3 = x^2xy^2y = x^2y^2xy$$

odakle sledi $(xy)^2 = x^2y^2$. Na osnovu zadatka 130 grupa G je Abelova.

132. Neka je G grupa koja nema elemenata reda 2. Ako je $(xy)^2 = (yx)^2$ za svako $x, y \in G$, dokazati da je tada G Abelova grupa.

Rešenje. Primetimo najpre da je

$$x^2 = ((xy^{-1})y)^2 = (y(xy^{-1}))^2 = yx^2y^{-1},$$

što je ekvivalentno sa $x^2y = yx^2$. Dalje u G važi

$$x^{-1}y^{-1}x = x(x^{-1})^2y^{-1}x = xy^{-1}(x^{-1})^2x = xy^{-1}x^{-1}.$$

Analogno važi i $y^{-1}x^{-1}y = yx^{-1}y^{-1}$.

Neka je $z = xyx^{-1}y^{-1}$. Tada je

$$\begin{aligned} z^2 &= xy(x^{-1}y^{-1}x)yx^{-1}y^{-1} = xy(xy^{-1}x^{-1})yx^{-1}y^{-1} = \\ &= xyx(y^{-1}x^{-1}y)x^{-1}y^{-1} = xyx(yx^{-1}y^{-1})x^{-1}y^{-1} = \\ &= (xy)^2((yx)^2)^{-1} = (yx)^2((yx)^2)^{-1} = e. \end{aligned}$$

Pošto u G nema elemenata reda 2 iz $z^2 = e$ sledi $z = e$, tj. $xy = yx$.

133. Ako u grupi G za svako $a, b \in G$ važi jednakost

$$(ab)^i = a^ib^i,$$

za tri uzastopna cela broja i , onda je G Abelova grupa. Dokazati.

Rešenje. Neka su ta tri uzastopna cela broja $n-1$, n i $n+1$. Ako jednakost

$$(ab)^{n+1} = a^{n+1}b^{n+1}$$

pomnožimo sleva sa a^{-1} i zdesna sa b^{-1} , biće

$$(ba)^n = a^n b^n.$$

Kako je

$$(ab)^n = a^n b^n,$$

sledi

$$(1) \quad (ba)^n = (ab)^n.$$

Slično, iz

$$(ab)^n = a^n b^n$$

sledi da je

$$(ba)^{n-1} = (ab)^{n-1},$$

pa, s obzirom da za svaki element grupe postoji jedinstven inverzni element, mora biti

$$(2) \quad ((ba)^{n-1})^{-1} = ((ab)^{n-1})^{-1}.$$

Množeći leve i desne strane jednakosti (1) i (2) dobija se

$$ba = ab.$$

PRIMEDBA. Primerom pokazati da se gornji zaključak ne može izvesti iz pretpostavke da identitet

$$(ab)^i = a^i b^i,$$

važi samo za dva uzastopna cela broja među kojima se ne nalazi 2 ili -1 .

134. Neka je G grupa u kojoj za svako $x, y \in G$ važi $(xy)^3 = x^3 y^3$ i $(xy)^8 = x^8 y^8$. Dokazati da je G Abelova grupa.

Rešenje. Iz $(xy)^3 = x^3 y^3$ sledi da je $(yx)^2 = x^2 y^2$ iz čega se dobija $(yx)^6 = (x^2 y^2)^3 = x^6 y^6$. Kada se ova jednakost pomnoži sleva sa x i zdesna sa y dobija se da je $(xy)^7 = x^7 y^7$. Takođe važi $(xy)^9 = (x^3 y^3)^3 = x^9 y^9$. Dobili smo da je za svako $x, y \in G$ $(xy)^i = x^i y^i$, za $i = 7, 8, 9$, pa na osnovu prethodnog zadatka sledi da je G Abelova grupa.

135. Koje od sledećih grupa su cikličke:

$$(\mathbb{Z}, +), (\{1, -1, i, -i\}, \cdot), (\mathbb{Q}, +),$$

$$(\mathbb{Z}_n, +), (\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}, \cdot), \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \subseteq \mathbb{Z}_8 ?$$

136. Cikličke grupe istog reda su izomorfne. Sve beskonačne cikličke grupe su međusobno izomorfne. Dokazati.

Rešenje. Ako je a generatorni element cikličke grupe G_1 reda n , a b generatorni element cikličke grupe G_2 istog reda, onda je preslikavanje $a^k \mapsto b^k$, $k = 1, 2, \dots, n$, izomorfizam grupa G_1 i G_2 .

Funkcija f koja beskonačnu cikličku grupu sa generatornim elementom a preslikava na aditivnu grupu celih brojeva $f : a^k \mapsto k$, je izomorfizam. Prema tome, sve beskonačne cikličke grupe su izomorfne grupi $(\mathbb{Z}, +)$.

137. Dokazati da beskonačna ciklička grupa ima prebrojivo mnogo elemenata.

138. Red elementa a konačne grupe G je delitelj reda grupe. Dokazati.

Rešenje. Ciklička podgrupa generisana elementom a je reda jednakog redu elemenata a , pa na osnovu Lagranžove teoreme (1.50) sledi da je red elementa a delitelj reda grupe G .

139. Svaka grupa čiji je red prost broj je ciklička. Dokazati.

140. U cikličkoj grupi C_n reda n generisanoj elementom a , element a^m je generator ako i samo ako su m i n uzajamno prosti brojevi. Dokazati.

Rešenje. Ako je $\text{nzd}(n, m) = 1$, onda su sledećih n elemenata međusobno različiti

$$a^m, a^{2m}, \dots, a^{nm} = e.$$

Zaista, iz

$$a^{im} = a^{jm}, \quad 1 \leq j < i \leq n,$$

sledi

$$a^{(i-j)m} = e,$$

tj. n mora biti delitelj broja $(i - j)m$, a to je, s obzirom na pretpostavku, kontradikcija. Prema tome, a^m je generator grupe C_n .

Neka je sada a^m generator grupe C_n i pretpostavimo da je $\text{nzd}(n, m) = d > 1$. Tada je

$$(a^m)^{n/d} = (a^n)^{m/d} = e,$$

a kako je $n/d < n$, element a^m ne može biti generator grupe C_n . Pretpostavka od koje smo pošli stoga ne važi, pa je $\text{nzd}(n, m) = 1$.

141. Ako su u cikličkoj grupi C_n elementi a, b takvi da je $a^s = b^s$, pri čemu je s uzajamno prosto sa n , dokazati da je tada $a = b$.

Rešenje. Ciklička grupa je Abelova, pa iz $a^s = b^s$ sledi da je $(ab^{-1})^s = e$. Neka je g generator C_n . Tada je $ab^{-1} = g^r$, pa se dobija da je $g^{rs} = e$ iz čega sledi da je n delitelj rs . Međutim, n i s su uzajamno prosti, što znači da n deli r . Neka je $r = nq$. Tada je $ab^{-1} = g^r = g^{nq} = e$, tj. $a = b$.

142. Svaka podgrupa cikličke grupe je takođe ciklička. Dokazati.

Rešenje. Neka je $H \neq \{e\}$ podgrupa cikličke grupe C generisane elementom a . Neka je najmanji pozitivan stepen elementa a koji se nalazi u

H , $a^k \in H$ (s obzirom da je H podgrupa takvo k uvek postoji). Ako je a^l proizvoljan element podgrupe H , mora biti

$$l = kq + r, \quad q, r \in \mathbb{Z}, \quad 0 \leq r < k,$$

pa je, prema tome,

$$a^r = a^{l-kq} = a^l (a^k)^{-q},$$

odakle sledi da $a^r \in H$.

Kako je k bio minimalan pozitivan stepen, mora biti $r = 0$, a to znači da je l deljivo sa k , tj. $a^l = (a^k)^q$, pa je a^k generator podgrupe H , koja je, prema tome, ciklička.

143. Dokazati da je svaka konačno generisana podgrupa G aditivne grupe racionalnih brojeva $(\mathbb{Q}, +)$ ciklička.

Rešenje. Neka je u grupi $(\mathbb{Q}, +)$ podgrupa G generisana sa $g_1, g_2, \dots, g_n$. Tada je

$$G = \{g \mid g = k_1 g_1 + k_2 g_2 + \dots + k_n g_n, \quad k_i \in \mathbb{Z}\}.$$

Označimo sa d najmanji zajednički sadržalac za imeniocce brojeva $g_1, g_2, \dots, g_n$. Neka je $dG = \{dg \mid g \in G\}$. Neposredno sledi da je dG aditivna podgrupa u grupi $(\mathbb{Z}, +)$, a na osnovu prethodnog zadatka svaka podgrupa aditivne grupe celih brojeva je ciklička, dakle, dG je ciklička grupa i neka je c generator grupe dG . Ako se sada svaki element u dG podeli sa d , dobija se ponovo G i to je ciklička grupa čiji je generator $\frac{c}{d}$.

144. Mora li grupa G da bude ciklička ako su sve njene prave podgrupe cikličke?

Rezultat. Priferova grupa (zadatak 8) nije ciklička, a sve njene prave podgrupe su cikličke.

145. U cikličkoj grupi C preslikavanje f je endomorfizam ako i samo ako je za svako $x \in C$

$$f(x) = x^c,$$

c fiksiran ceo broj. Dokazati.

146. Naći sve endomorfizme grupe $(\mathbb{Z}, +)$.

147. U cikličkoj grupi C_n reda n preslikavanje $f(x) = x^m$ je automorfizam ako i samo ako su m i n uzajamno prosti brojevi.

Uputstvo. Koristiti zadatak 140.

148. Navesti sve endomorfizme cikličke grupe reda 12. Koji od njih su automorfizmi?

149. Naći red svakog elementa cikličke grupe reda 30.

150. Neka je C_n ciklička grupa reda n . Ako je m delitelj broja n , dokazati da onda C_n ima jednu i samo jednu podgrupu reda m .

Rešenje. Ako je a generator grupe C_n , onda element $a^{n/m}$ generiše podgrupu H reda m . Pretpostavimo da postoji još jedna podgrupa K reda m . Ona mora biti ciklička (zadatak 142) i neka je njen generator a^l .

Tada je

$$a^{lm} = e,$$

što znači da je lm deljivo sa n , $\frac{lm}{n} = k$, pa je odatle

$$a^l = a^{kn/m} = (a^{n/m})^k.$$

Prema tome, $a^l \in H$, $|H| = |K|$, odakle sledi da je $H = K$.

151. Naći sve podgrupe cikličke grupe reda 30.

Uputstvo. Koristiti zadatke 142 i 150.

152. Dokazati da klase ostataka $\overline{(2i+1)}$ po modulu 16, $i = 0, 1, \dots, 7$ čine multiplikativnu grupu i naći sve njene podgrupe.

153. Dokazati da je Abelova grupa G reda $p_1 p_2 \cdots p_n$, gde su p_i međusobno različiti prosti brojevi, ciklička.

Rešenje. Na osnovu Košijeve teoreme (1.97), u G postoje elementi g_i reda p_i , $i = 1, 2, \dots, n$. Tada je $m = p_1 p_2 \cdots p_n$ red elementa $g = g_1 g_2 \cdots g_n$ (zadatak 77), pa je G ciklička grupa čiji je generator g .

154. Neka je G konačna Abelova grupa čiji je red p^k , p prost broj, a k prirodan broj. Ako u G jednačina $x^n = e$ za svaki prirodan broj n ima najviše n rešenja, dokazati da je G ciklička grupa.

Rešenje. Svaki element grupe G ima red koji je delitelj broja p^k (1.97). Neka je a element grupe G čiji je red maksimalan i neka je $|a| = p^m$. Tada su

$$e, a, a^2, \dots, a^{p^m-1},$$

međusobno različiti elementi koji su različita rešenja jednačine $x^{p^m} = e$, pa kako ta jednačina po pretpostavci nema više od p^m rešenja to su sva rešenja.

Neka je b proizvoljan element grupe G . Njegov red je p^i , $i \leq m$, pa je

$$b^{p^m} = (b^{p^i})^{p^{m-i}} = e,$$

tj. b je takođe rešenje jednačine $x^{p^m} = e$. To znači da je $b = a^s$ za neko s , dakle, G je ciklička grupa čiji je generator a .

155. Neka je G konačna Abelova grupa u kojoj za svaki prirodan broj n jednačina $x^n = e$ ima najviše n rešenja. Dokazati da je G ciklička grupa.

Uputstvo. Ako je G reda k , onda je $k = p_1^{i_1} p_2^{i_2} \dots p_j^{i_j}$, gde su $p_1, p_2, \dots, p_j$ različiti prosti brojevi, pa G ima podgrupe $H_1, H_2, \dots, H_j$ reda $p_1^{i_1}, p_2^{i_2}, \dots, p_j^{i_j}$ respektivno (1.103). Uslov da za svako $n \in \mathbb{N}$ $x^n = e$ ima najviše n rešenja važi i za podgrupe grupe G , pa na osnovu prethodnog zadatka sledi da su sve podgrupe $H_1, H_2, \dots, H_j$ cikličke. Generator c_1 grupe H_1 je reda $p_1^{i_1}$, generator c_2 grupe H_2 je reda $p_2^{i_2}$, pa na osnovu zadatka 77 sledi da je $c_1 c_2$ reda $p_1^{i_1} p_2^{i_2}$. Ako je c_3 generator H_3 , posmatrajući $c_1 c_2$ i c_3 dobijamo da je $c_1 c_2 c_3$ reda $p_1^{i_1} p_2^{i_2} p_3^{i_3}$. Produžujući ovaj postupak dobijamo da u G postoji element čiji je red jednak redu grupe, tj. G je ciklička grupa.

156. Neka je G konačna Abelova grupa. Označimo sa $\overline{G}$ skup svih homomorfizama grupe G u multiplikativnu grupu kompleksnih brojeva $(\mathbb{C} \setminus \{0\}, \cdot)$. Ako su $\phi_1, \phi_2 \in \overline{G}$ definišimo množenje homomorfizama sa

$$(\phi_1 \cdot \phi_2)(g) = \phi_1(g)\phi_2(g), \quad \text{za svako } g \in G.$$

Dokazati:

a) Za svako $g \in G$ $\phi(g)$ je koren iz jedinice.

b) $(\overline{G}, \cdot)$ je konačna Abelova grupa.

Rešenje. a) Iz $\phi(e) = \phi(e \cdot e) = \phi(e)\phi(e)$ sledi da je $\phi(e) = 1$.

Neka je n red grupe G . Tada je $g^n = e$, za svaki element grupe G , i kada se primeni homomorfizam ϕ dobija se da je $\phi(g^n) = (\phi(g))^n = 1$.

b) Dokažimo zatvorenost skupa $\overline{G}$ u odnosu na množenje homomorfizama. Ako su $\phi_1, \phi_2 \in \overline{G}$, onda je

$$\begin{aligned} (\phi_1 \cdot \phi_2)(gh) &= \phi_1(gh)\phi_2(gh) = \phi_1(g)\phi_1(h)\phi_2(g)\phi_2(h) = \\ &= \phi_1(g)\phi_2(g)\phi_1(h)\phi_2(h) = (\phi_1 \cdot \phi_2)(g)(\phi_1 \cdot \phi_2)(h), \end{aligned}$$

pa je proizvod dva homomorfizma opet homomorfizam.

Jasno je da je zbog asocijativnosti i komutativnosti množenja kompleksnih brojeva i proizvod homomorfizama asocijativna i komutativna operacija.

Lako se proverava da je preslikavanje ϕ_0 definisano sa $\phi_0(g) = 1$ za svako $g \in G$, homomorfizam koji je neutralni element za množenje homomorfizama.

Iz $gg^{-1} = e$ se dobija da je $\phi(gg^{-1}) = \phi(g)\phi(g^{-1}) = 1$, pa je $\phi(g^{-1}) = \frac{1}{\phi(g)}$ multiplikativni inverzni element za $\phi(g)$. Na osnovu a) je $|\phi(g)| = 1$, pa je $\phi(g^{-1}) = \overline{\phi(g)}$ (kompleksan broj konjugovan broju $\phi(g)$). Ako definišemo homomorfizam $\bar{\phi}$ sa $\bar{\phi}(g) = \overline{\phi(g)}$ za svako $g \in G$, odmah se dobija da je $\phi\bar{\phi} = \phi_0$.

157. Ako je C_n ciklička grupa reda n , dokazati da je grupa $(\overline{C_n}, \cdot)$ homomorfizama definisana u prethodnom zadatku izomorfna sa C_n .

Uputstvo. Ako je g generator grupe C_n , dokazati da je preslikavanje definisano sa

$$\phi : g^k \mapsto \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n},$$

traženi izomorfizam.

158. Ako je G konačna Abelova grupa, dokazati da je tada grupa $(\overline{G}, \cdot)$ homomorfizama definisana u zadatku 156 izomorfna sa G .

Uputstvo. Koristiti da je konačna Abelova grupa direktni proizvod cikličkih grupa i prethodni zadatak.

159. Neka je G konačna Abelova grupa i $\overline{G}$ grupa homomorfizama definisana u zadatku 156. Ako je $\phi \in \overline{G} \setminus \{\phi_0\}$, gde je ϕ_0 neutralni element grupe $\overline{G}$ (tj. ϕ_0 je homomorfizam definisan sa $\phi_0(g) = 1$ za svako $g \in G$), dokazati da je

$$\sum_{g \in G} \phi(g) = 0.$$

Rešenje. Neka je a fiksni element grupe G . Ako je g proizvoljan element grupe G , tada je $g = ah$ za neki element $h \in G$ i pri tome ako g prolazi kroz sve elemente grupe G i h prolazi kroz sve elemente grupe G , pa je

$$\sum_{g \in G} \phi(g) = \sum_{ah \in G} \phi(ah) = \sum_{ah \in G} \phi(a)\phi(h) = \phi(a) \sum_{h \in G} \phi(h),$$

odakle je

$$(1 - \phi(a)) \sum_{g \in G} \phi(g) = 0.$$

Ako se a izabere tako da je $\phi(a) \neq 1$, a to je moguće jer je $\phi \neq \phi_0$, dobija se da je $\sum_{g \in G} \phi(g) = 0$.

1.6 Grupe permutacija

160. Sledeće permutacije napisati kao proizvod disjunktних ciklusa:

$$\begin{array}{ll} a) & p = [4512367], \quad b) \quad q = [1325647], \\ c) & r = [238451967], \quad d) \quad s = [654321]. \end{array}$$

Rešenje. a) Kako je $p(1) = 4, p(4) = 2, p(2) = 5, p(5) = 3, p(3) = 1$ i $p(6) = 6, p(7) = 7$, imamo

$$p = [4512367] = (14253).$$

S obzirom na definiciju ciklisa očividno je da se p može pisati i na sledeći način:

$$\begin{aligned} p &= (14235) = (42531) = (25314) = \\ &= (53142) = (31425) = (14253)(6) = \\ &= (7)(14253) = (14253)(6)(7). \end{aligned}$$

(Ovde ciklus koji se sastoji od samo jednog simbola označava da je taj simbol nepromenjen.)

$$b) \quad q = [1235647] = (23)(456) = (23)(456)(1)(7),$$

161. Sledeće permutacije prikazati kao proizvod disjunktних ciklusa

$$\begin{array}{ll} a) & (234)(125)(3617), \quad b) \quad (1234)(123)(12), \\ c) & (123)(435)(1346), \quad d) \quad (12)(23)(34)(45). \end{array}$$

$$\text{Rešenje. a) } (234)(125)(3617) = (17425)(36).$$

(S obzirom da argument pišemo zdesna računanje počinjemo od krajnjeg desnog ciklusa.)

$$b) (1234)(123)(12) = (14)(23).$$

162. Bilo koje dve permutacije koje pomeraju disjunktne skupove simbola komutiraju. Dokazati.

163. Ciklus dužine n je reda n . Dokazati.

(Red permutacije je njen red kao elementa simetrične grupe S_n .)

Rešenje. Neka je q ciklus dužine n :

$$q(a_1) = a_2, q(a_2) = a_3, \dots, q(a_n) = a_1, q(x) = x, x \neq a_1, a_2, \dots, a_n.$$

Tada je $q^2(a_i) = a_{i+2}$ i, uopšte, $q^k(a_i) = a_{i+k}$, za svako $k \in \mathbb{N}$ (gde su svi indeksi redukovani na najmanji pozitivan ostatak po modulu n). q^k će biti identičko preslikavanje ako i samo ako je $a_i = a_{i+k}$, tj. ako i samo ako je $k \equiv 0 \pmod{n}$. Najmanji takav pozitivan broj k je n , pa je, prema tome, ciklus q reda n .

164. Neka je $q = (12 \dots m)$ ciklus dužine m . Dokazati:

a) q^n je ciklus dužine m ako i samo ako su m i n uzajamno prosti brojevi.

b) Ako je d najveći zajednički delitelj za m i n , tada je q^n proizvod d ciklusa.

165. Dokazati da je red permutacije najmanji zajednički sadržalac dužina njenih disjunktних ciklusa.

Rešenje. Neka je permutacija p prikazana kao proizvod disjunktних ciklusa, $p = q_1 q_2 \dots q_k$. Disjunktни ciklusi komutiraju, pa je

$$p^n = q_1^n q_2^n \dots q_k^n.$$

Oдавde sledi da je p^n identičko preslikavanje ako i samo ako je svaki od ciklusa q_i^n takođe identičko preslikavanje, pa je prema zadatku 163 red permutacije p zaista najmanji zajednički sadržalac dužina ciklusa $q_1, q_2, \dots, q_k$.

166. Naći red permutacija

a) $(245)(18)(6739)$,

b) $(134)(236)$.

Rešenje. a) Ova permutacija je proizvod disjunktних ciklusa dužine 3, 2 i 4, pa je njen red 12.

b) Najpre ćemo datu permutaciju prikazati kao proizvod disjunktних ciklusa:

$$(134)(236) = (13624),$$

pa je red ove permutacije 5.

167. U simetričnoj grupi S_n opisati sve elemente čiji je red prost broj p .

168. Naći element najvećeg reda u grupi S_n za $n = 2, 3, \dots, 10$.

169. Dokazati da je $(12 \dots n)^{-1} = (n \ n-1 \dots 2 \ 1)$.

170. Ako je

$$p = (a_{11}a_{12} \dots a_{1k_1})(a_{21}a_{22} \dots a_{2k_2}) \dots (a_{l1}a_{l2} \dots a_{lk_l}),$$

dokazati da je tada

$$p^{-1} = (a_{lk_l} \dots a_{l2}a_{l1}) \dots (a_{2k_2} \dots a_{22}a_{21})(a_{1k_1} \dots a_{12}a_{11}).$$

171. Neka su $(a_1 \dots a_k)$ i $(b_1 \dots b_l)$ ciklusi koji imaju zajednički jedan i samo jedan simbol. Dokazati da je $(a_1 \dots a_k)(b_1 \dots b_l)$ takođe ciklus i naći njegovu dužinu.

172. U grupi S_n naći permutacije koje komutiraju sa ciklusom $p = (a_1a_2 \dots a_n)$.

Rešenje. Neka je $q \in S_n$ tako da je $pq = qp$. Ako je $q(a_1) = a_l$, biće

$$(qp)(a_1) = q(a_2)$$

i

$$(pq)(a_1) = p(a_l) = a_{l+1},$$

pa kako je $pq = qp$, mora biti $q(a_2) = a_{l+1}$. Indukcijom se lako dokazuje da je

$$q(a_k) = a_{l+(k-1)}, \quad k = 1, 2, \dots, n,$$

(svi indeksi u ovom razmatranju su redukovani na najmanji pozitivan ostatak po modulu n). To znači da je $q = p^k$, a kako je $p^k p = p p^k$ sledi da sa ciklusom p komutiraju stepeni tog ciklusa i samo oni.

173. Neka je

$$a = (x_1x_2 \dots x_m)(x_{m+1})(x_{m+2}) \dots (x_n)$$

jedan element grupe S_n . Ako element b ($b \in S_n$) zadovoljava uslov $ba = ab$, onda b ima oblik $a^k p$, gde je k prirodan broj i p ($p \in S_n$) sa fiksnim elementima $x_1, x_2, \dots, x_m$. Dokazati.

Rešenje. Pretpostavimo da je $b(x_i) = x_j$,

$$x_i \in \{x_1, x_2, \dots, x_m\} = A, \quad x_j \in \{x_{m+1}, x_{m+2}, \dots, x_n\} = B.$$

Tada je

$$ab(x_i) = x_j, \quad ba(x_{(i-1)'}) = x_j,$$

gde je

$$(i-1)' = \begin{cases} i-1, & \text{za } i > 1 \\ m, & \text{za } i = 1 \end{cases},$$

što zbog $ab = ba$ ne može biti, pa sledi da je

$$(\forall x_i \in A) b(x_i) \in A \quad \text{i} \quad (\forall x_j \in B) b(x_j) \in B.$$

Prema tome, $b = qp$, gde permutacija q ima za fiksne elemente $x_{m+1}, x_{m+2}, \dots, x_n$ a fiksni elementi permutacije p su $x_1, x_2, \dots, x_m$.

Svaka permutacija sa fiksnim elementima $x_1, x_2, \dots, x_m$ je komutativna sa a i q , pa još treba odrediti oblik permutacije q .

S obzirom da je a ciklus dužine m sa fiksnim elementima $x_{m+1}, x_{m+2}, \dots, x_n$, a q permutacija čiji su fiksni elementi takođe $x_{m+1}, x_{m+2}, \dots, x_n$ i kako mora biti $aq = qa$, na osnovu prethodnog zadatka sledi da je $q = a^k$, gde je k prirodan broj.

Prema tome, mora biti $b = a^k p$, gde je k prirodan broj a p permutacija sa fiksnim elementima $x_1, x_2, \dots, x_m$.

174. Dokazati da je

$$(a_1 a_2 \dots a_n) = (a_1 a_n)(a_1 a_{n-1}) \dots (a_1 a_2).$$

Rešenje. Proverom se neposredno utvrđuje da je gornja jednakost tačna.

175. Dokazati da je ciklus dužine n parna permutacija ako je n neparan broj, a neparna permutacija ako je n paran broj.

Rešenje. Posledica prethodnog zadatka.

176. Permutaciju $p = [2157346]$ napisati kao proizvod

a) transpozicija,

b) terceta.

Rešenje. a) Permutaciju ćemo prikazati kao proizvod ciklusa, a zatim primeniti zadatak 174.

$$p = [2157346] = (12)(35)(476) = (12)(35)(46)(47).$$

b) Pokazano je da je $p = (12)(35)(46)(47)$ parna permutacija, pa se ona, prema tome, može prikazati kao proizvod terceta. Kako je

$$\begin{aligned} (12)(35) &= (12)((23)^{-1}(23))(35) = (12)((23)(23))(35) = \\ &= ((12)(23))((23)(35)) = (123)(352), \\ (46)(47) &= (476), \end{aligned}$$

biće

$$p = (123)(352)(476).$$

177. Ako je permutacija $p \in S_n$ proizvod k disjunktних ciklusa (uzimajući u obzir i sve cikluse dužine 1), onda je permutacija p parna ili neparna prema tome da li je $n - k$ paran ili neparan broj. Dokazati.

178. Permutacija koja je prikazana kao proizvod ciklusa je parna ili neparna prema tome da li sadrži paran ili neparan broj ciklusa parne dužine. Dokazati.

179. Dokazati da je svaka permutacija $p \in S_{10}$ reda 20 neparna.

Rešenje. Permutaciju p rastavimo u proizvod disjunktних ciklusa. Kako je red permutacije najmanji zajednički sadržalac dužina njenih disjunktних ciklusa (zadatak 165), ciklusi koji čine permutaciju p mogu biti samo dužina 1, 2, 4, 5, 10. Zbir dužina ciklusa je 10 (jer je p permutacija skupa od 10 simbola), pa treba utvrditi kako se 10 može prikazati kao zbir nekih od brojeva 1, 2, 4, 5, 10, ali tako da najmanji zajednički sadržalac tih sabiraka bude 20. Postoji samo jedan način da se to učini: $5 + 4 + 1 = 10$, pa je, prema tome, p proizvod ciklusa dužine 5, 4 i 1. Na osnovu zadatka 178 (ili 177) permutacija p je neparna.

180. Permutacije $p, q \in S_n$ su konjugovani elementi u grupi S_n ako i samo ako se mogu rastaviti na jednak broj disjunktних ciklusa i među tim ciklusima se može uspostaviti bijektivno preslikavanje tako da su odgovarajući ciklusi iste dužine. Dokazati.

185. Dokazati da ciklusi $p = (1\ 2\ \dots\ n-1)$ i $q = (1\ 2\ \dots\ n-1\ n)$ generišu grupu S_n .

Rešenje. Neposredno se proverava da je $r = pqp^{n-3} = (2\ n)$. Ako se r konjuguje stepenima elementa p , tj. izračuna $p^i r p^{-i}$, $i = 1, 2, \dots, n-1$, dobijaju se transpozicije

$$(1\ n), (2\ n), \dots, (n-1\ n).$$

Da ove transpozicije generišu S_n se dokazuje analogno kao u zadatku 183.

186. Dokazati da se transpozicijama

$$(1\ 2), (2\ 3), \dots, (n-1\ n)$$

može generisati S_n .

Uputstvo. $(1\ 2)(2\ 3) = (1\ 2\ 3)$, $(1\ 2)(2\ 3)(3\ 4) = (1\ 2\ 3\ 4)$, itd. Koristiti prethodni zadatak.

187. Permutaciju $[4231]$ prikazati kao proizvod transpozicije $[2134]$ i terceta $[1342]$.

Uputstvo. Koristiti zadatak 184.

188. Odrediti broj elemenata u svakoj klasi konjugovanih elemenata grupe S_n .

Rezultat. U klasi čiji su elementi permutacije koje se rastavljene u proizvod disjunktih ciklusa sastoje od j_1 ciklusa dužine 1, j_2 ciklusa dužine 2, $\dots$, j_k ciklusa dužine k , ima

$$\frac{n!}{1^{j_1} \cdot 2^{j_2} \cdot \dots \cdot n^{j_n} \cdot j_1! j_2! \dots j_n!}$$

elemenata.

189. Odrediti podgrupe reda 6

a) simetrične grupe S_4 ,

b) alternativne grupe A_4 .

190. Dokazati da $n-2$ terceta:

$$(123), (124), \dots, (12n)$$

generišu alternativnu grupu A_n ($n \geq 3$).

Uputstvo. Koristiti

$$(xyz) = (1zx)(1xy), \quad (1xy) = (1y2)(12x)(12y), \quad (1y2) = (12y)^{-1}.$$

191. Dokazati da se podgrupa parnih permutacija A_n simetrične grupe S_n , $n \geq 3$, može generisati permutacijama (123) i $(12 \dots n)$ ako je n neparan broj, a permutacijama (123) i $(23 \dots n)$ ako je n paran broj.

192. Neka je G podgrupa grupe S_n generisana ciklusima:

$$(a_1 a_2 \dots a_m a_{m+1}), (a_1 a_2 \dots a_m a_{m+2}), \dots, (a_1 a_2 \dots a_m a_n),$$

gde je $m < n - 1$. Dokazati da je $G = S_n$ ako je m neparan broj, a $G = A_n$ ako je m paran broj.

Uputstvo. Označimo ciklus $(a_1 a_2 \dots a_m a_i)$ sa p_i , $i = m + 1, \dots, n$. Ako je $m = 2r + 1$, dokazati da je za $i \neq j$

$$(p_i p_j)^r p_i^2 p_j = (a_1 a_2),$$

$$(p_i p_j)^{r+1} p_j = (a_1 a_i),$$

$$(p_i p_j)^{r+1} p_j^{2r+3-t} p_i^{t-1} p_j = (a_1 a_t) \quad \text{za } t = 3, 4, \dots, m.$$

Ako je $m = 2s$, dokazati da je

$$(p_i p_j)^{s-1} p_i^3 p_j = (a_1 a_2 a_3),$$

$$(p_i p_j)^s p_j^2 = (a_1 a_2 a_i),$$

$$(p_i p_j)^s p_j^{2s+3-t} p_i^t p_j = (a_1 a_2 a_t) \quad \text{za } t \neq 3.$$

Literatura:

L. Miller, *Generators of the symmetric and alternating group*, Amer. Math. Monthly, 48 (1941), 43–44.

193. Ako prava normalna podgrupa N grupe S_n sadrži jedan tercet, dokazati da N sadrži sve tercete. Na osnovu toga dokazati da je $N = A_n$.

1.7 Podgrupe, normalne podgrupe i faktor grupe

194. Neka su H i K podgrupe grupe G , a x, y elementi grupe G . Dokazati da iz $Hx = Ky$ sledi $H = K$.

Rešenje. Iz $Hx = Ky$ sledi da postoji element $k \in K$ takav da je $ex = ky$, tj. $yx^{-1} = k^{-1} \in K$, pa iz $Hx = Ky$ sledi $H = Kyx^{-1} = K$.

195. Neka su H i K podgrupe grupe G . Dokazati da je $H \cup K$ podgrupa grupe G ako i samo ako je $H \subseteq K$ ili $K \subseteq H$.

Rešenje. Ako je $H \subseteq K$ ili $K \subseteq H$, onda je, očigledno, $H \cup K$ podgrupa grupe G .

Ako pretpostavimo da nijedna od datih podgrupa ne sadrži drugu, onda postoje elementi $a \in H \setminus K$ i $b \in K \setminus H$. Iz $ab \in H$ sledi $a^{-1}(ab) = b \in H$, a to je protivrečnost. Iz $ab \in K$ analogno dolazimo do protivrečnosti, pa, prema tome, $H \cup K$ nije podgrupa.

196. Ako je A podgrupa grupe G takva da je $(G \setminus A) \cup \{e\}$ takođe podgrupa, dokazati da je ili $A = \{e\}$ ili $A = G$.

Uputstvo. Primeniti prethodni zadatak.

197. Neka je G grupa definisana u zadatku 3. Ispitati koji od sledećih podskupova su podgrupe grupe G :

- a) $H = \{(a, 0) \mid a > 0\}$,
- b) $K = \{(1, b) \mid b \in \mathbb{R}\}$,
- c) $I = \{(a, k(a-1)) \mid a \in \mathbb{R} \setminus \{0\}\}$, gde je k fiksiran realan broj,
- d) $J = \{(a, na^n) \mid a \in \mathbb{R} \setminus \{0\}\}$, gde je n fiksiran prirodan broj.

Rešenje. a) U grupi G neutralni element je $(1, 0)$, a inverzni element za $(x, y) \in G$ je $(x, y)^{-1} = \left(\frac{1}{x}, -\frac{y}{x}\right)$. Ako su $(x, 0), (y, 0) \in H$, onda je

$$(x, 0) * (y, 0)^{-1} = (x, 0) * \left(\frac{1}{y}, 0\right) = \left(\frac{x}{y}, 0\right) \in H,$$

što znači da je H podgrupa (1.16).

- b) K je podgrupa, jer iz $(1, x), (1, y) \in K$ sledi

$$(1, x) * (1, y)^{-1} = (1, x) * (1, -y) = (1, x - y) \in K,$$

c) I je podgrupa, jer iz $(x, k(x-1)), (y, k(y-1)) \in I$ sledi

$$\begin{aligned} & (x, k(x-1)) * (y, k(y-1))^{-1} = \\ & = (x, k(x-1)) * \left(\frac{1}{y}, -\frac{k(y-1)}{y} \right) = \left(\frac{x}{y}, \frac{k(x-y)}{y} \right) \in I. \end{aligned}$$

d) Ako je $n = 0$, J je podgrupa (tada je $J = H$), a ako je $n \neq 0$, J nije podgrupa jer ne sadrži neutralni element $(1, 0)$.

198. Neka je G konačna grupa, a H i K njene podgrupe takve da su $|H|$ i $|K|$ uzajamno prosti brojevi. Dokazati da je $H \cap K = \{e\}$.

Rešenje. Neka je $a \in H \cap K$. Tada je red elementa a delitelj $|H|$ i $|K|$, a kako je $\text{nzd}(|H|, |K|) = 1$ sledi da je $|a| = 1$, tj. $a = e$, pa je $H \cap K = \{e\}$.

199. Dokazati da je grupa konačna ako i samo ako sadrži konačno mnogo podgrupa.

200. Naći levu (desnu) dekompoziciju grupe simetrija kvadrata

$$G = \{[1234], [2341], [3412], [4123], [2143], [4321], [3214], [1432]\}$$

(v. zadatak 16 b)) po podgrupi $H = \{[1234], [1432]\}$.

Rešenje. Permutacije koje čine grupu G označimo (onim redom kojim su u tekstu zadatka navedene, tj. isto kao u zadatku 16 b)) sa e, a, b, c, d, f, g, h .

Tada je $H = \{e, h\}$. Element $a \notin H$, pa je aH levi suskup različit od H . Kako je $ae = a$,

$$ah = [2341][1432] = [2143] = d,$$

sledi

$$aH = \{a, d\}.$$

(Kada se permutacije ovako označavaju, onda se proizvod dve permutacije najjednostavnije izračunava tako što se elementi prve permutacije napišu u rezultatu onim redom kako to propisuje druga permutacija – u našem primeru najpre prvi element prve permutacije, pa zatim četvrti, treći i na kraju drugi element prve permutacije.) Produžujući ovaj postupak dobijamo suskupove:

$$bH = \{b, g\}$$

i

$$cH = \{c, f\},$$

pa je

$$G = H \cup aH \cup bH \cup cH.$$

Naravno, s obzirom da predstavnik jednog suskupa može biti bilo koji element tog suskupa (na primer $aH = dH$) ova ista dekompozicija se može prikazati i u ovom obliku:

$$G = H \cup dH \cup gH \cup fH.$$

Kako je $aH = \{a, d\}$ a $Ha = \{a, f\}$ vidimo da je $aH \neq Ha$, pa H nije normalna podgrupa, dakle, desna dekompozicija se razlikuje od leve dekompozicije (desna dekompozicija grupe G po podgrupi H jednaka je levoj ako i samo ako je H normalna podgrupa grupe G). Desna dekompozicija je:

$$G = H \cup Hc \cup Hb \cup Ha.$$

201. Naći levu i desnu dekompoziciju simetrične grupe S_3 po podgrupi $H = \{[123], [213]\}$. Da li se te dve dekompozicije razlikuju?

202. Ako je

$$G = a_1H \cup a_2H \cup \dots \cup a_nH$$

leva dekompozicija grupe G po podgrupi H , dokazati da je onda

$$G = Ha_1^{-1} \cup Ha_2^{-1} \cup \dots \cup Ha_n^{-1}$$

desna dekompozicija grupe G po podgrupi H .

203. Dokazati da za neprazan podskup K grupe G iz $a, b, c \in K$ sledi $ab^{-1}c \in K$ ako i samo ako je K levi suskup za neku podgrupu H grupe G .

Rešenje. Pretpostavimo da za svako $a, b, c \in K$, $ab^{-1}c \in K$. Neka je $H = \{x \mid x = a^{-1}b, a, b \in K\}$. Ako $x, y \in H$, onda postoje $a, b, c, d \in K$ tako da je $x = a^{-1}b$ i $y = c^{-1}d$, pa je

$$xy^{-1} = a^{-1}b(c^{-1}d)^{-1} = a^{-1}(bd^{-1}c) \in H$$

jer je $bd^{-1}c \in K$. Dakle, H je podgrupa.

Za fiksno $a \in K$, $aH \subseteq K$, a i $aa^{-1}b = b \in aH$ za svako $b \in K$, pa $K \subseteq aH$ i, prema tome, $K = aH$.

Obrnuto, neka je $K = xH$ za neku podgrupu H . Ako su $a, b, c \in K$ tada je

$$ab^{-1}c = xh_1(xh_2)^{-1}xh_3 = xh_1h_2^{-1}x^{-1}xh_3 = xh_1h_2^{-1}h_3 \in xH,$$

gde $h_1, h_2, h_3 \in H$.

PRIMEDBA. Potpuno analogno tvrđenje važi ako se u zadatku reč „levi“ zameni sa „desni“. U tom slučaju, uzimajući skup $H_1 = \{x \mid x = ab^{-1}, a, b \in K\}$ dobijaju se desni suskupovi po podgrupi H_1 .

204. Ako su H i K podgrupe grupe G , onda je HK podgrupa ako i samo ako je $HK = KH$. Dokazati.

Rešenje. Pretpostavimo da je $HK = KH$ i neka su $x, y \in HK$. Tada je

$$x = h_1k_1, \quad y = h_2k_2, \quad h_1, h_2 \in H, \quad k_1, k_2 \in K,$$

pa iz

$$xy = h_1k_1h_2k_2,$$

s obzirom da je $k_1h_1 = h_3k_3$, $h_3 \in H$, $k_3 \in K$ (zbog $HK = KH$), sledi

$$xy = (h_1h_3)(k_3k_2) \in HK.$$

Pošto je i

$$x^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH = HK,$$

dokazali smo da je skup HK podgrupa grupe G .

Obrnuto, ako je HK podgrupa, onda za svako $h \in H$ i svako $k \in K$, $h, k \in HK$ (jer i H i K sadrže neutralni element), pa $kh \in HK$ a to znači da je

$$KH \subseteq HK.$$

Za svako $x \in HK$, $x^{-1} \in HK$, tj. $x^{-1} = hk$, odakle je $x = k^{-1}h^{-1} \in KH$, pa smo dobili da je

$$HK \subseteq KH.$$

Prema tome,

$$HK = KH.$$

205. Neka su A, B i C podgrupe grupe G takve da je $AB = BA$ i $A \subseteq C$. Dokazati da je

$$C \cap (AB) = A(C \cap B).$$

Rešenje. Na osnovu prethodnog zadatka AB je podgrupa grupe G . Neka je $M = C \cap (AB)$. M je, kao presek dve podgrupe, takođe podgrupa. Očividno je $(AB) \cap B = B$, pa je i $M \cap B = C \cap (AB) \cap B = C \cap B$. Treba dokazati da je $A(M \cap B) = M$.

$M \supseteq A$, jer $C \supseteq A$ i $AB \supseteq A$, a i $M \supseteq M \cap B$ pa, pošto je M podgrupa, sledi $M \supseteq A(M \cap B)$.

S druge strane $AB \supseteq M$, pa je svako $m \in M$ oblika $m = ab$, $a \in A$, $b \in B$, tj. $b = a^{-1}m$ što znači da $b \in M$, jer $M \supseteq A$, pa $b \in M \cap B$. Prema tome, $m = ab \in A(M \cap B)$, tj. $M \subseteq A(M \cap B)$.

206. a) Presek svake dve netrivialne podgrupe grupe $(\mathbb{Z}, +)$ je netrivialna podgrupa.

b) Presek svake dve netrivialne podgrupe grupe $(\mathbb{Q}, +)$ je netrivialna podgrupa.

Dokazati.

Uputstvo. a) Ako su H i K podgrupe grupe $\mathbb{Z}$, onda postoje celi brojevi h i k tako da je $H = \{x \mid x = zh, z \in \mathbb{Z}\}$, $K = \{x \mid x = zk, z \in \mathbb{Z}\}$. Tada je $H \cap K = \{x \mid x = zhk, z \in \mathbb{Z}\}$.

b) Koristiti a) i činjenicu da ako je H podgrupa grupe $\mathbb{Q}$, onda iz $\frac{a}{b} \in H$ sledi $a \in H$ ($a, b \in \mathbb{Z}$).

207. Neka su $(\mathbb{Q}^p, +)$ i $(\mathbb{Q}_p, +)$ podgrupe (definisane u zadacima 36 i 37) aditivne grupe racionalnih brojeva $(\mathbb{Q}, +)$. Dokazati da je

a) $\mathbb{Q}^p \cap \mathbb{Q}_p = \mathbb{Z}$,

b) $\mathbb{Q}^p + \mathbb{Q}_p = \mathbb{Q}$,

c) $\mathbb{Q}^p \cap \mathbb{Q}^q = \mathbb{Z}$, za proste brojeve p, q , $p \neq q$.

208. Neka je $H_1 \subseteq H_2 \subseteq \dots \subseteq H_n \subseteq \dots$ niz podgrupa grupe G . Dokazati da je $H = \bigcup_{n=1}^{\infty} H_n$ podgrupa grupe G .

209. Naći bar tri skupa nezavisnih generatornih elemenata grupe $(\mathbb{Z}, +)$.

Rešenje. Grupa $(\mathbb{Z}, +)$ je ciklička, pa ima skup generatora koji se sastoji od jednog elementa: $\mathbb{Z} = \langle 1 \rangle$. Element -1 takođe generiše grupu $\mathbb{Z}$, pa je $\mathbb{Z} = \langle -1 \rangle$. Lako se može proveriti da je $\mathbb{Z} = \langle 2, 3 \rangle$. Kako se ni jedan od elemenata 2 i 3 ne može prikazati kao umnožak onog drugog, skup generatora $\{2, 3\}$ je nezavisan.

Analogno se dokazuje da je $\mathbb{Z} = \langle k, l \rangle$, gde su k i l proizvoljni uzajamno prosti celi brojevi.

210. Svaka konačna grupa ima skup nezavisnih generatora. Dokazati.

211. Odrediti koliko ima različitih skupova nezavisnih generatora od po 2 elementa u cikličkoj grupi reda 20.

Rezultat. 16.

212. Naći skup nezavisnih generatora multiplikativne grupe:

- a) pozitivnih racionalnih brojeva.
- b) nenula racionalnih brojeva.

Rezultat. a) Skup svih prostih brojeva.

b) Skup svih prostih brojeva i -1 .

213. Dokazati da je skup

$$M = \left\{ 1, \frac{1}{2}, \frac{1}{6}, \dots, \frac{1}{n!}, \dots \right\}$$

skup generatora za aditivnu grupu racionalnih brojeva. Da li je svaki beskonačni podskup skupa M takođe skup generatora te grupe?

214. U multiplikativnoj grupi nenula racionalnih brojeva odrediti podgrupu generisanu skupom $\{2, 3\}$.

215. Neka su a i b elementi grupe G . Dokazati da je

$$H = \{a^{n_1}b^{n_2}a^{n_3}b^{n_4} \dots a^{n_{k-1}}b^{n_k} \mid k \in \mathbb{N}, n_i \in \mathbb{Z}\}$$

podgrupa koja sadrži a i b i da svaka podgrupa K koja sadrži a i b sadrži i H .

216. Neka je G multiplikativna grupa generisana realnim matricama

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{i} \quad B = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}.$$

a) Dokazati da je $BAB^{-1} = A^2$.

b) Dokazati da se svaki element grupe G može napisati u obliku $B^i A^j B^k$ gde su i, j, k neki celi brojevi.

217. Dokazati da u multiplikativnoj grupi regularnih kompleksnih matrica reda 2 matrice

$$A = \begin{bmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{bmatrix} \quad \text{i} \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

generišu konačnu podgrupu reda $2n$.

218. Ako je G konačno generisana grupa i $H_1 \subseteq H_2 \subseteq \dots \subseteq H_n \subseteq \dots$ niz podgrupa grupe G takav da je $G = \bigcup_{n=1}^{\infty} H_n$, dokazati da postoji prirodan broj k takav da je $G = \bigcup_{n=1}^k H_n$.

219. Dokazati:

a) $(\mathbb{Q}, +)$ nije konačno generisana grupa.

b) $(\mathbb{Z}_p^\infty, \cdot)$ nije konačno generisana grupa.

Uputstvo. Koristiti prethodni zadatak, pošto se dokaže

a) da je $(\mathbb{Q}, +) = \bigcup_{n=1}^{\infty} H_n$, gde je $H_n = \{x \mid x = \frac{a}{n!}, a \in \mathbb{Z}\}$,

a) da je $(\mathbb{Z}_p^\infty, \cdot) = \bigcup_{n=1}^{\infty} H_n$, gde je $H_n = \{x \in \mathbb{C} \mid x^{p^n} = 1\}$.

220. Homomorfna slika grupe s konačnim brojem generatora je takođe grupa s konačnim brojem generatora. Dokazati.

Uputstvo. Ako je $G_1 = \langle a_1, a_2, \dots, a_n \rangle$ a f homomorfizam grupe G_1 na grupu G_2 , onda je $G_2 = \langle f(a_1), f(a_2), \dots, f(a_n) \rangle$.

221. Svaka beskonačna grupa sa konačnim brojem generatora je prebrojiva. Dokazati.

222. Ako su u konačnoj grupi G svi elementi sem neutralnog reda 2, onda je red grupe G stepen broja 2.

Rešenje. Već smo dokazali u zadatku 88 da grupa G mora biti Abelova. Kako je grupa konačna ona ima konačan skup nezavisnih generatornih elemenata, $G = \langle a_1, a_2, \dots, a_n \rangle$. Bilo koji element g grupe G može se, prema tome, napisati u obliku

$$(1) \quad g = a_1^{k_1} a_2^{k_2} \dots a_n^{k_n}, \quad k_i \in \{0, 1\}, \quad i = 1, 2, \dots, n,$$

i to na jedinstven način, jer iz pretpostavke da se neki element iz G može

prikazati na dva različita načina dobili bismo da elementi $a_1, a_2, \dots, a_n$ nisu nezavisni.

S obzirom da eksponenata u (1) ima n i oni uzimaju samo vrednosti 0 i 1, sledi da u G ima 2^n elemenata.

223. Neka je G grupa čije su sve konačno generisane podgrupe cikličke.

a) Dokazati da je G Abelova grupa.

b) Dokazati da za proizvoljne podgrupe A, B, C grupe G važi

$$A(B \cap C) = (AB) \cap (AC).$$

Rešenje. a) G je Abelova grupa, jer za svako $x, y \in G$, $\langle x, y \rangle = \langle z \rangle$, pa je $x = z^r$, $y = z^s$ ($r, s \in \mathbb{Z}$) i $xy = z^r z^s = z^s z^r = yx$.

b) Nadalje ćemo koristiti aditivnu notaciju za operaciju u grupi G , jer je G komutativna grupa.

$$B \cap C \subseteq B, \text{ pa je } A + (B \cap C) \subseteq A + B,$$

analogno je

$$B \cap C \subseteq C, \text{ pa je } A + (B \cap C) \subseteq A + C,$$

i sledi da je

$$A + (B \cap C) \subseteq (A + B) \cap (A + C).$$

Neka je $x \in (A + B) \cap (A + C)$. Tada je $x = a_1 + b = a_2 + c$, gde $a_1, a_2 \in A$, $b \in B$ i $c \in C$. $\langle b, c \rangle = \langle d \rangle$ po pretpostavci, pa je $b = md$ i $c = nd$, $n, m \in \mathbb{Z}$.

Neka je najveći zajednički delitelj za m i n broj l . Tada je $m = m_1 l$ i $n = n_1 l$, gde su m_1 i n_1 uzajamno prosti brojevi, pa postoje celi brojevi r i s takvi da je $rm_1 + sn_1 = 1$.

Tada je

$$\begin{aligned} x &= rm_1 x + sn_1 x = rm_1(a_2 + c) + sn_1(a_1 + b) = \\ &= rm_1 a_2 + sn_1 a_1 + rm_1 c + sn_1 b = a_3 + rm_1 nd + sn_1 md = \\ &= a_3 + rm_1 n_1 ld + sn_1 m_1 ld = a_3 + (r + s)m_1 n_2 ld. \end{aligned}$$

Kako je

$$m_1 n_1 ld = m_1 nd = m_1 c \in C,$$

a i

$$m_1 n_1 l d = n_1 m c = n_1 b \in B,$$

onda je

$$m_1 n_1 l d \in B \cap C, \text{ tj. } x \in A + (B \cap C).$$

224. Naći sve neizomorfne grupe reda 1, 2, 3, 4, 5, 6 i 7.

Rešenje. Svaka grupa čiji je red prost broj je ciklička, pa su cikličke grupe jedine grupe reda 1, 2, 3, 5 i 7.

(i) Neka je G grupa reda 4, $G = \{e, a, b, c\}$. Red elemenata je delitelj reda grupe pa su a, b i c reda 2 ili 4.

Ako u G postoji element reda 4, G je ciklička grupa reda 4.

Ako u G nema elemenata reda 4, onda je

$$a^2 = b^2 = c^2 = e.$$

Na osnovu zadatka 88 grupa G mora biti Abelova. Posmatrajmo element ab . Svaka od pretpostavki

$$ab = e, \quad ab = a, \quad ab = b,$$

dovodi do kontradikcije, pa sledi da mora biti $ab = c$. Sada se mogu lako izračunati preostali proizvodi, pa se dobija Kejljeva tablica:

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Iz tablice se utvrđuje da je G zaista grupa.

Ova grupa se naziva Klajnova (Klein) četvorna grupa.

(ii) Posmatrajmo sada grupu G sa 6 elemenata. Svi njeni elementi sem neutralnog su reda 2, 3 ili 6.

Ako grupa ima element reda 6 ona je ciklička.

Ako u grupi G nema elemenata reda 6, onda su svi elementi sem neutralnog reda 2 ili 3. Na osnovu zadatka 222 zaključujemo da svi elementi

grupe ne mogu biti reda 2 (jer je $|G| = 6 \neq 2^n$), pa, prema tome, u G postoji element a reda 3. Dakle, e, a i a^2 su različiti elementi grupe G . Neka je b element iz G različit od e, a i a^2 . Pokažimo da su tada

$$e, a, a^2, b, ab, a^2b$$

međusobno različiti elementi. Pretpostavke da je

$$ab = e, \quad ab = a, \quad ab = a^2, \quad ab = b$$

očevidno dovode do kontradikcije, pa je ab različito od e, a, a^2 i b .

Svaka od pretpostavki

$$a^2b = e, \quad a^2b = a, \quad a^2b = a^2, \quad a^2b = b, \quad a^2b = ab,$$

takođe dovodi do protivrečnosti, pa su

$$e, a, a^2, b, ab, a^2b$$

zaista različiti elementi, a kako ih ima 6 sem njih grupa G nema drugih elemenata.

Da bi formirali multiplikativnu tablicu grupe G odredićemo proizvode elemenata te grupe. b^2 je jedan od elemenata grupe, ako pretpostavimo da je

$$b^2 = b, \quad b^2 = ab, \quad b^2 = a^2b,$$

skraćivanjem ovih jednakosti odmah dolazimo do kontradikcije. Iz $b^2 = a$ sledi da je b reda 3, pa množenjem sa b dobijamo $b^3 = e = ab$, što je kontradikcija. Analogno pokazujemo da je $b^2 \neq a^2$, pa preostaje da mora biti $b^2 = e$.

Slično kao ranije, svaka od jednakosti

$$ba = e, \quad ba = a, \quad ba = a^2, \quad ba = b$$

odmah dovodi do kontradikcije. Ako je $ba = ab$, onda je

$$(ab)^2 = a^2b^2 = a^2 \neq e, \quad (ab)^3 = a^3b^3 = b \neq e,$$

pa je ab reda 6, što ne može biti. Prema tome $ba = a^2b$, (tj. $(ab)^2 = e$).

Preostali proizvodi se sada mogu lako izračunati, pa se dobija Kejljeva tablica:

	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

Iz tablice se utvrđuje da je G zaista grupa.

Ova grupa je nekomutativna, generisana je elementima a i b koji zadovoljavaju relacije

$$a^3 = b^2 = (ab)^2 = e.$$

(Videli smo da ove relacije potpuno određuju grupu.)

225. Naći Kejljevu tablicu za grupu generisanu elementima a i b koji zadovoljavaju sledeće relacije

$$a^4 = b^2 = (ab)^2 = e.$$

Dokazati da je ta grupa izomorfna sa grupom simetrija kvadrata (zadatak 16 b).

226. Dokazati da je simetrična grupa S_3 izomorfna sa nekomutativnom grupom reda 6 opisanom u zadatku 224.

227. Podgrupa H grupe G je normalna ako i samo ako za svako $a, b \in G$ iz $ab \in H$ sledi $ba \in H$. Dokazati.

Rešenje. Ako je $h \in H$, tada $g^{-1}(gh) \in H$, pa sledi $ghg^{-1} \in H$.

Obrnuto, neka je H normalna podgrupa, $a, b \in H$ i neka $ab \in H$. Tada je $a^{-1}(ab)a = ba \in H$.

Literatura:

F. E. Masat, *A useful characterization of a normal subgroup*, Math. Magazine, 52 (1979), 171-173.

228. Ako u grupi G normalne podgrupe H i K imaju zajednički samo neutralni element, onda svaki element iz H komutira sa svakim elementom iz K . Dokazati.

Uputstvo. Neka je $a \in H$, $b \in K$. Posmatrati $(aba^{-1})b^{-1} = a(ba^{-1}b^{-1})$ i iskoristiti da $aba^{-1} \in K$, $ba^{-1}b^{-1} \in H$ zbog normalnosti podgrupa H i K .

229. Dokazati da je skup xHx^{-1} podgrupa grupe G za svako $x \in G$, ako i samo ako je H podgrupa grupe G .

PRIMEDBA. xHx^{-1} se naziva podgrupa konjugovana sa podgrupom H .

230. Podgrupa grupe G je normalna ako i samo ako se poklapa sa svim svojim konjugovanim podgrupama. Dokazati.

231. a) Dokazati da konjugovane podgrupe imaju isti red.

b) Neka je H podgrupa grupe G . Ako je K podgrupa grupe G konjugovana sa H onda, ako je H komutativna mora i K biti komutativna. Dokazati.

c) U grupi G podgrupa H je ciklička i njen generator je a . Ako je K podgrupa grupe G konjugovana sa H , $K = xHx^{-1}$, onda je i K ciklička podgrupa i njen generator je xax^{-1} . Dokazati.

Uputstvo. Preslikavanje $f : H \rightarrow K$ podgrupe H na podgrupu $K = xHx^{-1}$ grupe G dato sa $f : a \mapsto xax^{-1}$ je izomorfizam.

232. Ako je u grupi G svaka podgrupa normalna, dokazati da svaka dva elementa čiji su redovi uzajamno prosti komutiraju.

Uputstvo. Posmatrati cikličke podgrupe generisane tim elementima.

233. Dokazati da je u grupi G podgrupa generisana kvadratima elemenata iz G normalna (element $x \in G$ je kvadrat ako i samo ako postoji $g \in G$ tako da je $x = g^2$).

234. Odrediti normalne podgrupe grupe simetrija kvadrata (v. zadatke 16 b, 200).

235. Ako se izvrši particija grupe G na disjunktne podskupove, kada će familija tih podskupova biti grupa u odnosu na operaciju množenja skupova definisanu u 1.45?

236. U aditivnoj grupi celih brojeva $(\mathbb{Z}, +)$ sa H je označena podgrupa svih brojeva deljivih sa 4. Izvršiti razlaganje grupe $\mathbb{Z}$ po podgrupi H i naći faktor grupu $\mathbb{Z}/H$.

Rešenje. H je normalna podgrupa jer je $(\mathbb{Z}, +)$ komutativna grupa, pa se leva i desna dekompozicija grupe $\mathbb{Z}$ po H poklapaju.

U H se nalaze svi brojevi oblika $4k$, $k \in \mathbb{Z}$, pa ćemo izabrati bilo koji element koji ne pripada H , recimo 1, i sabrati ga sa svakim elementom iz H ,

tako dobijamo suskup

$$1 + H = \{1 + 4k \mid k \in \mathbb{Z}\}.$$

Ako sada uzmemo bilo koji element koji nije ni u H ni u $1 + H$, recimo 2, i saberemo ga sa H dobijamo suskup

$$2 + H = \{2 + 4k \mid k \in \mathbb{Z}\}.$$

Produžavajući ovaj postupak dobijamo i suskup

$$3 + H = \{3 + 4k \mid k \in \mathbb{Z}\}.$$

Unija navedenih suskupova je cela grupa G , pa je time dovršeno razlaganje grupe $\mathbb{Z}$ po podgrupi H :

$$Z = H \cup (1 + H) \cup (2 + H) \cup (3 + H).$$

Ovi suskupovi su elementi faktor grupe $\mathbb{Z}/H$. (Faktor grupa $(\mathbb{Z}/H, +)$ je ustvari grupa $(\mathbb{Z}_4, +)$ ostataka po modulu 4 (zadatak 12).)

237. Neka je $C_{12} = \{a, a^2, \dots, a^{12} = e\}$ ciklička grupa reda 12, a $H = \{e, a^4, a^8\}$ njena podgrupa. Naći faktor grupu C_{12}/H i formirati Kejljevu tablicu te grupe.

Rešenje.

$$\begin{aligned} H &= \{e, a^4, a^8\}, \\ aH &= \{a, a^5, a^9\}, \\ a^2H &= \{a^2, a^6, a^{10}\}, \\ a^3H &= \{a^3, a^7, a^{11}\}, \end{aligned}$$

su suskupovi koji predstavljaju elemente faktor grupe

$$C_{12}/H = \{H, aH, a^2H, a^3H\}.$$

S obzirom da je $aH \cdot bH = abH$, jednostavno se formira Kejljeva tablica (na primer, $aH \cdot a^3H = a^4H = H$ itd.).

238. Dokazati da je svaka faktor grupa cikličke grupe ciklička.

Uputstvo. Ako je a generatorni element cikličke grupe C , a H njena podgrupa, dokazati da onda suskup aH generiše faktor grupu C/H .

239. Ako je aditivnoj grupi kompleksnih brojeva $(\mathbb{C}, +)$, $\mathbb{R}$ podgrupa svih realnih brojeva naći faktor grupu $\mathbb{C}/\mathbb{R}$.

Kako se elementi ove faktor grupe mogu grafički predstaviti u kompleksnoj ravni?

Rezultat. $\mathbb{C}/\mathbb{R} = \{\mathbb{R} + bi \mid b \in \mathbb{R}\}$.

240. Naći sve neizomorfne homomorfne slike cikličke grupe C_6 reda 6.

Rešenje. Prema prvoj teoremi o izomorfizmu grupa (1.64) svaka homomorfna slika grupe G je izomorfna nekoj faktor grupi grupe G . Prema tome, da bi našli sve homomorfne slike grupe $C_6 = \{a, a^2, \dots, a^6 = e\}$ odredićemo sve faktor grupe te grupe. Podgrupe grupe C_6 su

$$H_1 = \{e\}, \quad H_2 = \{e, a^3\}, \quad H_3 = \{e, a^2, a^4\}, \quad C_6,$$

drugih podgrupa nema (zadatak 150), ove podgrupe su normalne jer je grupa komutativna, pa su faktor grupe

$$C_6/H_1, \quad C_6/H_2, \quad C_6/H_3, \quad C_6/C_6,$$

tražene neizomorfne homomorfne slike.

Na primer, preslikavanje $f : x \mapsto xH_2$ je homomorfizam grupe C_6 na grupu $C_6/H_2 = \{H_2, aH_2, a^2H_2\}$.

241. Neka je p prost broj. Dokazati da je $\mathbb{Z}_p^\infty = \mathbb{Q}^p/\mathbb{Z}$.

242. Dokazati da je u grupi svaka podgrupa indeksa 2 normalna podgrupa.

243. Neka je H podgrupa simetrične grupe S_n ($n > 1$). Ako H sadrži bar jednu neparnu permutaciju, dokazati da H sadrži podgrupu K takvu da je $[H : K] = 2$.

Rešenje. Ako H sadrži bar jednu neparnu permutaciju, onda je $HA_n = S_n$. Iskoristimo drugu teoremu o izomorfizmu (1.68):

$$H/H \cap A_n \cong HA_n/A_n \cong S_n/A_n \cong C_2,$$

pa je $H \cap A_n = K$ podgrupa grupe H indeksa 2.

244. Dokazati da grupa S_3 nema pravih normalnih podgrupa različitih od A_3 .

245. Navesti primer grupe G u kojoj postoje podgrupe A i B takve da je $A \subseteq B$, A je normalna podgrupa grupe B , B je normalna podgrupa grupe G , ali A nije normalna podgrupa grupe G .

246. Neka je grupa G_2 homomorfna slika grupe G_1 .

a) Ako je $H_1 \triangleleft G_1$, onda je i slika podgrupe H_1 normalna podgrupa grupe G_2 .

b) Ako je $H_2 \triangleleft G_2$, onda je skup svih elemenata iz G_1 koji se preslikavaju na elemente iz H_2 normalna podgrupa grupe G_1 . Dokazati.

247. Ako je A podgrupa a N normalna podgrupa grupe G , dokazati da je tada

- a) AN podgrupa,
- b) $A \cap N \triangleleft A$,
- c) $A/A \cap N \cong AN/N$.

Uputstvo. Posmatrati restrikciju f_A homomorfizma $f : G \rightarrow G/N$ na A . Dokazati da je $A \cap N$ jezgro, a AN/N slika homomorfizma f_A i primeniti prvu teoremu o izomorfizmu (1.64).

248. Neka su K i H normalne podgrupe grupe G takve da je $K \subseteq H$. Tada je

- a) H/K normalna podgrupa grupe G/K ,
- b) $G/H \cong (G/K)/(H/K)$.

Dokazati.

Uputstvo. Definirati preslikavanje $f : G/K \rightarrow G/H$ sa $f : Ka \mapsto Ha$. Dokazati da je f funkcija, homomorfizam, da je H/K jezgro f , da je G/H slika homomorfizma f i primeniti prvu teoremu o izomorfizmu (1.64).

249. Neka je K normalna podgrupa grupe G i $f : G \rightarrow G/K$ preslikavanje definisano sa $f : g \mapsto gK$. Dokazati:

- a) f preslikava bijektivno podgrupe grupe G koje sadrže K na podgrupe grupe G/K .
- b) f preslikava bijektivno normalne podgrupe grupe G koje sadrže K na normalne podgrupe grupe G/K .

250. Neka je H normalna podgrupa konačne grupe G takva da su joj

red $|H|$ i indeks $[G : H]$ uzajamno prosti brojevi. Dokazati da je H jedina podgrupa grupe G koja ima red $|H|$.

Uputstvo. Pretpostaviti da postoji podgrupa K takva da je $|K| = |H|$. U šta se preslikava K pri preslikavanju $f : G \rightarrow G/H$, $f : x \mapsto xH$?

251. Dokazati da konačna grupa reda $2n$ koja sadrži element reda n ima najmanje $\tau(n) + 1$ normalnih podgrupa. Sa $\tau(n)$ je označen broj svih delitelja broja n .

252. Ako je grupa G unija familije pravih normalnih podgrupa, takvih da je neutralni element jedini zajednički element za bilo koje dve od tih podgrupa, onda je G Abelova grupa. Dokazati.

Rešenje. Neka je $G = \bigcup_{i \in I} N_i$, gde je $N_i \triangleleft G$, $N_i \neq G$, $i \in I$, $N_i \cap N_j = \{e\}$, $i \neq j$, i neka su $a \in N_i$, $b \in N_j$, $i \neq j$. Ako je

$$c = aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1},$$

onda, s obzirom da su N_i i N_j normalne podgrupe,

$$ba^{-1}b^{-1} \in N_i, \quad aba^{-1} \in N_j,$$

pa $c \in N_i$, $c \in N_j$. Prema tome, $c = e$, odnosno $ab = ba$.

Pretpostavimo sada da $a, b \in N_i$. Kako je N_i prava podgrupa postoji $g \in G$, $g \notin N_i$ i element $ga \in N_i$. Na osnovu onoga što smo ranije dokazali, g i ga komutiraju sa svakim elementom iz N_i , pa i sa ba , dakle,

$$e = (ga)(ba)(ga)^{-1}(ba)^{-1} = aba^{-1}b^{-1},$$

tj. $ab = ba$.

253. Neka je K normalna podgrupa grupe G takva da je faktor grupa G/K reda n . Dokazati:

a) $x^n \in K$ za svako $x \in G$.

b) Ako $x \in G$ i $x^k \in K$ za neki ceo broj k koji je uzajamno prost sa n , tada $x \in K$.

Rešenje. a) Faktor grupa G/K je reda n , pa je $(xK)^n = x^nK = K$, tj. $x^n \in K$.

b) Ako su n i k uzajamno prosti brojevi, tada postoje celi brojevi r i s tako da je $rk + sn = 1$, pa je

$$x^{rk+sn} = (x^k)^r \cdot (x^n)^s = x.$$

$x^k \in K$ i $x^n \in K$, pa i $x \in K$.

254. Neka je $(G, +)$ Abelova grupa koja ima sledeću osobinu: za svaki prirodan broj n i svako $x \in G$ postoji $y \in G$ tako da je $ny = x$. Dokazati:

a) G je beskonačna grupa.

b) Ako je H podgrupa grupe G , tada i faktor grupa G/H ima navedenu osobinu.

c) Podgrupa grupe G ne mora da ima tu osobinu.

Rešenje. a) Ako pretpostavimo da je G konačna grupa, $|G| = n$, onda je $ny = 0$ za svako $y \in G$, pa za $x \neq 0$ ne postoji $y \in G$ tako da bude $ny = x$. Iz ove protivrečnosti sledi da je grupa G beskonačna.

b) Neka je $x \in G/H$, tj. $X = x + H$ za neko $x \in G$. U G postoji takvo y da je $ny = x$, pa tada za klasu $y + H = Y$ važi

$$nY = n(y + H) = ny + nH = x + H = X,$$

tj. G/H ima navedenu osobinu.

c) $(\mathbb{Q}, +)$ zadovoljava dati uslov, a njena podgrupa $(\mathbb{Q}^p, +)$ (zadatak 37) ne zadovoljava (za $x = \frac{1}{p}$ i $n \neq p^k$, $k \in \mathbb{N}$).

255. Neka su A, B i C normalne podgrupe grupe G takve da je $A \subseteq B$, $AC = BC$ i $A \cap C = B \cap C$. Dokazati da je tada $A = B$.

Rešenje. Lako se proverava da je $B = B \cap (BC)$ i $A = A \cap (AC)$ i da važe sledeće jednakosti:

$$A = A \cap (AC) = A(A \cap C) = A(A \cap B) = B \cap (AC) = B \cap (BC) = B.$$

256. Neka je G konačna grupa u kojoj za fiksni prirodan broj $n > 1$ važi $(xy)^n = x^n y^n$ za svako $x, y \in G$. Neka je $G_n = \{x \mid x \in G, x^n = e\}$ i $G^n = \{x \mid x \in G, (\exists z \in G) x = z^n\}$. Dokazati:

a) G_n i G^n su normalne podgrupe grupe G .

b) Red podgrupe G^n je jednak indeksu podgrupe G_n u G .

Uputstvo. Primeniti prvu teoremu o izomorfizmu (1.64) na homomorfizam $f : G \rightarrow G$ dat sa $f : x \mapsto x^n$.

257. Neka je H podgrupa indeksa k grupe G . Dokazati da postoji homomorfizam $h : G \rightarrow S_k$ takav da je jezgro homomorfizma h maksimalna normalna podgrupa grupe G sadržana u H .

Rešenje. Posmatrajmo skup $X = \{H, g_2H, \dots, g_kH\}$ svih levih suskupova grupe H u G . Lako se proverava da je za svako $a \in G$ preslikavanje $f_a : X \rightarrow X$ definisano sa

$$f_a = \begin{pmatrix} H & g_2H & \dots & g_kH \\ aH & ag_2H & \dots & ag_kH \end{pmatrix}$$

permutacija skupa X . Ako označimo sa S_X grupu svih permutacija skupa X , onda je preslikavanje $h : G \rightarrow S_X \cong S_k$ definisano sa $h : a \mapsto f_a$ homomorfizam. Zaista,

$$h(ab) = f_{ab} = f_a f_b = h(a)h(b).$$

Neka $a \in \text{Ker } h$, tada je f_a identičko preslikavanje, tj. $abH = bH$ za svako $b \in G$. Za $b = e$ je

$$aH = aeH = eH = H,$$

pa $a \in H$. Prema tome, $\text{Ker } h \subseteq H$.

Neka je N proizvoljna normalna podgrupa grupe G sadržana u H . Tada je $x^{-1}yx \in N \subseteq H$ za svako $y \in N$ i svako $x \in G$, pa je $x^{-1}yxH = H$, a odatle je $yaH = aH$, tj. $y \in \text{Ker } h$. Dokazali smo da je $N \subseteq \text{Ker } h$, $\text{Ker } h$ je normalna podgrupa grupe G (jer je jezgro svakog homomorfizma normalna podgrupa), pa je, prema tome, $\text{Ker } h$ maksimalna normalna podgrupa grupe G sadržana u H .

258. Ako beskonačna grupa G sadrži pravu podgrupu H konačnog indeksa, tada G sadrži i pravu normalnu podgrupu konačnog indeksa. Dokazati.

Rešenje. Neka je $[G : H] = k$. Na osnovu prethodnog zadatka sledi da postoji homomorfizam $h : G \rightarrow S_k$ čije je jezgro sadržano u H . Pošto je $\text{Ker } h$ jezgro homomorfizma, ono je podgrupa grupe G , a faktor grupa $G/\text{Ker } h$ je izomorfna sa nekom podgrupom konačne grupe S_n . Prema tome, normalna podgrupa $\text{Ker } h$ je konačnog indeksa u G .

259. Ako je G konačna grupa reda n , H prava podgrupa indeksa k grupe G i n nije delitelj $k!$, dokazati da H sadrži netrivialnu normalnu podgrupu grupe G .

Rešenje. S obzirom da n nije delitelj $k!$ na osnovu Lagranžove teoreme (1.50) sledi da S_k nema podgrupu reda n , tj. homomorfizam h definisan u

rešenju zadatka 257 ne može biti izomorfizam. Dakle, jezgro tog homomorfizma koje je normalna podgrupa grupe G , nije trivijalna podgrupa $\{e\}$.

260. a) Ako je u grupi G reda 99 H podgrupa reda 11, dokazati da je H normalna podgrupa.

b) Dokazati da grupe reda 20, 28 i 44 nisu proste.

Rešenje. a) S obzirom da je $[G : H] = 9$ i 99 nije delitelj $9!$, na osnovu prethodnog zadatka H sadrži netrivialnu normalnu podgrupu N grupe G . Kako je red podgrupe H prost broj, H nema netrivialnih podgrupa, prema tome, $N = H$, tj. H je normalna podgrupa grupe G .

1.8 Direktan proizvod grupa

261. Neka su A i B grupe. Direktan proizvod $A \times B$ sadrži podgrupe A' i B' izomorfne redom grupama A i B . Svaki element grupe $A \times B$ se može na jedinstven način prikazati kao proizvod jednog elementa iz A' i jednog iz B' i elementi u tom proizvodu komutiraju. Dokazati.

Rešenje. S obzirom da su A i B grupe, lako se dokazuje da je $A \times B$ grupa.

Skup $A' = A \times \{e_B\} = \{(a, e_B) \mid a \in A\}$ je podgrupa grupe $A \times B$ izomorfna sa A , a $B' = \{e_A\} \times B = \{(e_A, b) \mid b \in B\}$ je podgrupa izomorfna sa B (sa e_A i e_B označili smo neutralne elemente redom grupa A i B).

Ako je (a, b) bilo koji element grupe $A \times B$, onda je

$$(a, b) = (a, e_B)(e_A, b) = (e_A, b)(a, e_B)$$

i ovo je očevidno jedini način da se (a, b) napiše kao proizvod jednog elementa iz A' i jednog elementa iz B' .

262. Ako su $C_2 = \{a, a^2 = e_1\}$ i $C_3 = \{b, b^2, b^3 = e_2\}$ cikličke grupe reda dva i tri, naći $C_2 \times C_3$.

Rešenje. Elementi grupe $C_2 \times C_3$ su sledećih šest uređenih parova

$$\begin{aligned} &(e_1, e_2), \quad (e_1, b), \quad (e_1, b^2), \\ &(a, e_2), \quad (a, b), \quad (a, b^2). \end{aligned}$$

Kako je

$$(a, b)^2 = (e_1, b^2), \quad (a, b)^3 = (a, e_2), \quad (a, b)^4 = (e_1 b), \\ (a, b)^5 = (a, b^2), \quad (a, b)^6 = (e_1, e_2),$$

grupa $C_2 \times C_3$ je ciklička, a njen generator je (a, b) .

263. Direktan proizvod $C_n \times C_m$ cikličkih grupa je ciklička grupa ako i samo ako su m i n uzajamno prosti brojevi. Dokazati.

264. Ako je grupa G direktan proizvod grupa A i B , dokazati da su podgrupe A' i B' definisane u rešenju zadatka 261 normalne, i da je

$$G/A' \cong B, \quad G/B' \cong A.$$

265. Neka je G grupa i neka je $\tilde{G} = \{x \mid x = (g, g), g \in G\}$ podskup direktnog proizvoda $G \times G$. Dokazati:

a) $\tilde{G}$ je podgrupa grupe $G \times G$ i $\tilde{G} \cong G$.

b) $\tilde{G}$ je normalna podgrupa grupe $G \times G$ ako i samo ako je G Abelova grupa.

Rešenje. b) Neka je $\tilde{G}$ normalna podgrupa grupe $G \times G$. Tada je za svako $a, g \in G$

$$(e, a)(g, g)(e, a)^{-1} = (g, aga^{-1}) \in \tilde{G},$$

pa je $g = aga^{-1}$, tj. $ag = ga$. Obrnuto važi očigledno.

266. Navesti primer grupe G koja ima normalne podgrupe H i K tako da važi:

a) $H \cong K$, a $G/H \not\cong G/K$.

b) $H \not\cong K$, a $G/H \cong G/K$.

Rešenje.

a) $G = C_2 \times C_4$, $H = C_2 \times 1$, $K = 1 \times C_2$.

b) $G = C_2 \times C_4$, $H = C_2 \times C_2$, $K = 1 \times C_4$.

(Sa 1 je označena grupa koja se sastoji samo od neutralnog elementa.)

267. Navesti primer dve neizomorfne grupe G_1 i G_2 , pri čemu grupa G_1 ima normalnu podgrupu K_1 a grupa G_2 ima normalnu podgrupu K_2 , tako da je

$$K_1 \cong K_2 \quad \text{i} \quad G_1/K_1 \cong G_2/K_2.$$

Rešenje.

$$G_1 = C_2 \times C_2, \quad G_2 = C_4, \quad K_1 = C_2 \times 1, \quad K_2 = C_2.$$

268. Ako su A i B podgrupe grupe G takve da je $AB = G$, jedini zajednički element podgrupa A i B je neutralni element e i ako svaki element iz A komutira sa svakim elementom iz B , onda je $G \cong A \times B$. Dokazati.

Rešenje. S obzirom da je $G = AB$, svaki element g grupe G može se prikazati u obliku $g = ab$, $a \in A$, $b \in B$ i to na jedinstven način, jer iz pretpostavke

$$ab = a_1b_1, \quad a, a_1 \in A, \quad b, b_1 \in B,$$

sledi

$$a_1^{-1}a = b_1b^{-1},$$

pa kako je $A \cap B = \{e\}$, mora biti $a_1^{-1}a = b_1b^{-1} = e$, tj. $a = a_1$, $b = b_1$.

Preslikavanje $f : ab \mapsto (a, b)$ je izomorfizam grupe G na grupu $A \times B$ jer je to preslikavanje očividno bijekcija i ako su $x, y \in G$, onda je

$$x = a_1b_1, \quad y = a_2b_2, \quad a_1, a_2 \in A, \quad b_1, b_2 \in B,$$

pa je

$$\begin{aligned} f(xy) &= f(a_1b_1a_2b_2) = f(a_1a_2b_1b_2) = (a_1a_2, b_1b_2) = \\ &= (a_1, b_1)(a_2, b_2) = f(x)f(y). \end{aligned}$$

Dakle, $G \cong A \times B$.

269. Ako su A i B normalne podgrupe grupe G takve da im je neutralni element jedini zajednički element i ako je $G = AB$, onda je $G \cong A \times B$. Dokazati.

Uputstvo. Koristiti zadatke 228 i 268.

270. Dokazati da je za svako $k \in \mathbb{N}$

$$D_{2(2k+1)} \cong D_{2k+1} \times C_2,$$

gde je D_n diedarska grupa (zadatak 16 d)).

Uputstvo. Ako su $r, s \in D_{2(2k+1)}$ takvi da je $r^{2(2k+1)} = e$, $s^2 = e$ i $rs = sr^{4k+1}$ dokazati da su $H = \langle r^{2k+1} \rangle \cong C_2$ i $K = \langle r^2, s \rangle \cong D_{2k+1}$ normalne podgrupe, da im je presek $\{e\}$ i koristiti prethodni zadatak.

271. Dokazati da grupe $\underbrace{C_n \times \dots \times C_n}_k$ i C_{n^k} , $n, k > 1$, nisu izomorfne.

Rešenje. Grupa C_{n^k} ima element reda n^k , a svaki element grupe $\underbrace{C_n \times \dots \times C_n}_k$ je reda koji je delitelj n .

272. Dokazati da je skup klasa ostataka uzajamno prostih sa 21 po modulu 21 multiplikativna grupa izomorfna sa direktnim proizvodom cikličkih grupa reda 6 i 2.

Rešenje. Ranije (zadatak 13 b) je pokazano da je

$$G = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{8}, \bar{10}, \bar{11}, \bar{13}, \bar{16}, \bar{17}, \bar{19}, \bar{20}\} \subseteq \mathbb{Z}_{21}$$

multiplikativna grupa. $A = \{\bar{2}, \bar{4}, \bar{8}, \bar{16}, \bar{11}, \bar{1}\}$ je ciklička podgrupa reda 6 (jedan njen generator je $\bar{2}$), a $B = \{\bar{1}, \bar{13}\}$ ciklička podgrupa reda 2, pa kako je G komutativna grupa i $A \cap B = \{\bar{1}\}$, $AB = G$, na osnovu zadatka 268 sledi da je $G \cong A \times B$.

273. Koje od sledećih multiplikativnih grupa su izomorfne netrivialnom direktnom proizvodu:

- a) $\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \subseteq \mathbb{Z}_8$,
- b) $\{\bar{1}, \bar{3}, \bar{9}, \bar{11}\} \subseteq \mathbb{Z}_{16}$,
- c) $\{\bar{1}, \bar{7}, \bar{9}, \bar{15}\} \subseteq \mathbb{Z}_{16}$.

274. Da li je ciklička grupa reda 25 izomorfna netrivialnom direktnom proizvodu?

Rešenje. Ne, jer ima samo jednu netrivialnu podgrupu C_5 (v. 1.71), a $C_5 \times C_5$ nije ciklička grupa.

275. Naći sve neizomorfne Abelove grupe reda 36.

Rešenje. Svaka konačna Abelova grupa je izomorfna direktnom proizvodu cikličkih grupa (1.99), a redovi tih grupa su delitelji reda grupe (1.50). To znači da treba naći sve neizomorfne direktne proizvode reda 36 cikličkih grupa. Kako je $36 = 2^2 \cdot 3^2$, postoje četiri neizomorfne Abelove grupe reda 36:

$$C_{2^2} \times C_{3^2}, \quad C_2 \times C_2 \times C_{3^2}, \quad C_{2^2} \times C_3 \times C_3, \quad C_2 \times C_2 \times C_3 \times C_3.$$

Pri tome smo koristili činjenicu da grupe C_{p^2} i $C_p \times C_p$ nisu izomorfne (zadatak 271).

276. Naći sve neizomorfne Abelove grupe reda 77, 98, 100, p^2q^4 , $p^2q^4r^2$, gde su p, q i r različiti prosti brojevi.

Rešenje. Koristićemo postupak opisan u prethodnom zadatku. Kako je $77 = 7 \cdot 11$, sve Abelove grupe reda 77 su izomorfne grupi $C_7 \times C_{11}$ ($\cong C_{77}$). $98 = 2 \cdot 7^2$, pa ima dve neizomorfne Abelove grupe reda 98, to su $C_2 \times C_7 \times C_7$ i $C_2 \times C_{49}$. $100 = 2^2 \cdot 5^2$, pa ima 4 neizomorfne Abelove grupe reda 100. Neizomorfnih Abelovih grupa reda p^2q^4 ima 10, a reda $p^2q^4r^2$ ima 20.

277. Za koje n su izomorfne sve Abelove grupe reda n ?

Rešenje. Za $n = p_1p_2 \dots p_k$, gde su $p_1p_2 \dots p_k$ različiti prosti brojevi (1.99, 1.100).

1.9 Komutatori, rešive grupe

278. Dokazati da je u grupi G centar $Z(G)$ (definicija 1.74) normalna podgrupa.

279. Neka su x i y elementi grupe G takvi da xy pripada centru grupe G . Dokazati da je $xy = yx$.

Rešenje.

$$xy = e(xy) = (yy^{-1})(xy) = y(xy)y^{-1} = yx.$$

280. U grupi simetrija kvadrata (zadatak 16 b) naći centar.

281. Odrediti centar multiplikativne grupe G realnih regularnih matrica formata 2×2 .

Rešenje. Neka je

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

matrica koja pripada centru. Ona komutira sa svim matricama iz G , pa je

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

odakle dobijamo da je $b = c = 0$. Takođe mora biti

$$\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix},$$

odakle je $a = d$.

Prema tome, $A = aE$, $a \neq 0$ (E je jedinična matrica), a kako je očividno za svako $B \in G$

$$(aE)B = B(aE),$$

centar grupe G se sastoji od svih matrica oblika aE (takve matrice se nazivaju skalarne).

PRIMEDBA. Može li se gornji zaključak uopštiti za multiplikativnu grupu regularnih matrica formata $n \times n$?

282. Neka je G grupa matrica definisana u zadatku 28. Dokazati da je $\mathcal{Z}(G) \cong F^+$, gde je sa F^+ označena aditivna grupa polja F .

Rešenje. Neka

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \in \mathcal{Z}(G).$$

Tada je

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix},$$

odakle se dobija

$$\begin{bmatrix} 1 & x+a & y+az+b \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+x & b+cx+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{bmatrix}.$$

Iz ove matrične jednakosti sledi da je $az = cx$ za svako $x, z \in F$. Ako se stavi da je $x = 1$ i $z = 0$ dobija se da je $c = 0$, a za $x = 0$ i $z = 1$ je $a = 0$, pa su sve matrice koje pripadaju centru $\mathcal{Z}(G)$ oblika

$$\begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Za matrice ovog oblika se lako proverava da čine multiplikativnu grupu izomorfnu F^+ .

283. Dokazati da je faktor grupa $G/\mathcal{Z}(G)$ grupe matrica definisanih u zadatku 28 izomorfna grupi $F^+ \times F^+$, gde je F^+ aditivna grupa polja F .

Uputstvo. Koristeći zadatak 282 dokazati da se u svakom suskupu iz $G/\mathcal{Z}(G)$ može izabrati matrica oblika

$$\begin{bmatrix} 1 & a & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

i odrediti predstavnika proizvoda dva suskupa.

284. Neka je $\mathcal{Z}(G)$ centar grupe G . Ako je faktor grupa $G/\mathcal{Z}(G)$ ciklička, onda je grupa G Abelova grupa. Dokazati.

Rešenje. Neka je $a\mathcal{Z}(G)$ generatorni element cikličke grupe $G/\mathcal{Z}(G)$. Tada se svaki element grupe $G/\mathcal{Z}(G)$ može prikazati u obliku $a^n\mathcal{Z}(G)$, za neki ceo broj n . Prema tome, svaki element grupe G može se prikazati u obliku $a^n x$, $x \in \mathcal{Z}(G)$. Ako su p, q dva proizvoljna elementa grupe G , onda je

$$p = a^n x, \quad q = a^m y, \quad x, y \in \mathcal{Z}(G),$$

i

$$pq = a^n x a^m y = a^n a^m xy = a^m a^n yx = a^m y a^n x = qp,$$

pa je G Abelova grupa.

285. Ako je A neprazan podskup grupe G , onda je centralizator $\mathcal{C}(A)$ skupa A u G skup svih elemenata iz G koji komutiraju sa svakim elementom iz A , tj.

$$\mathcal{C}(A) = \{x \mid x \in G, \quad (\forall y \in A) xy = yx\}.$$

Ako $A, B \subseteq G$, dokazati:

- a) $\mathcal{C}(A)$ je podgrupa grupe G ,
- b) Iz $A \subseteq B$ sledi $\mathcal{C}(A) \supseteq \mathcal{C}(B)$,
- c) $A \subseteq \mathcal{C}(\mathcal{C}(A))$,
- d) $\mathcal{C}(A) = \mathcal{C}(\mathcal{C}(\mathcal{C}(A)))$.

286. Koji elementi simetrične grupe S_3 su komutatori? Naći izvod grupe S_3 .

Rešenje. S obzirom da je komutator proizvod 4 permutacije od kojih su dve i dve iste parnosti, sledi da svaki komutator mora biti parna permutacija. Prema tome, komutatori mogu biti jedino permutacije

$$[123], [231], [312].$$

Ove permutacije zaista su komutatori, jer je

$$[213] [213] [213]^{-1} [213]^{-1} = [123],$$

$$[132] [213] [132]^{-1} [213]^{-1} = [231],$$

$$[321] [213] [321]^{-1} [213]^{-1} = [312],$$

pa kako one čine grupu (to je A_3 , podgrupa svih parnih permutacija) dobijamo da je izvod grupe S_3 alternativna podgrupa A_3 .

287. Neka je G grupa. Dokazati da je

$$G' = \{x \mid x = g_1 \cdots g_k g_1^{-1} \cdots g_k^{-1}, k \in \mathbb{N}, g_i \in G\}.$$

Rešenje. Neka je

$$H = \{x \mid x = g_1 \cdots g_k g_1^{-1} \cdots g_k^{-1}, k \in \mathbb{N}, g_i \in G\}.$$

Ako su $a, b \in G$ i $g_1 = a$, $g_2 = ba^{-1}$ i $g_3 = b^{-1}$, tada je

$$g_1 g_2 g_3 = aba^{-1}b^{-1} = [a, b]$$

i

$$g_1^{-1} g_2^{-1} g_3^{-1} = a^{-1} (ba^{-1})^{-1} (b^{-1})^{-1} = a^{-1} ab^{-1}b = e,$$

pa je $g_1 g_2 g_3 g_1^{-1} g_2^{-1} g_3^{-1} = [a, b]$.

Ovo važi za svaki komutator, pa stoga za proizvod komutatora važi

$$\begin{aligned} [a, b][c, d] &= g_1 g_2 g_3 g_1^{-1} g_2^{-1} g_3^{-1} h_1 h_2 h_3 h_1^{-1} h_2^{-1} h_3^{-1} = \\ &= g_1 g_2 g_3 h_1 h_2 h_3 g_1^{-1} g_2^{-1} g_3^{-1} h_1^{-1} h_2^{-1} h_3^{-1}, \end{aligned}$$

gde je korišćeno da je $g_1^{-1} g_2^{-1} g_3^{-1} = e$. To znači da je $G' \subseteq H$.

Dokažimo da je $H \subseteq G'$ matematičkom indukcijom. Za $k=1$ ($g_1 g_1^{-1} = e \in G'$) i $k=2$ ($g_1 g_2 g_1^{-1} g_2^{-1} \in G'$) tvrđenje važi. Pretpostavimo da je za svaki niz od k elemenata iz G $g_1 \cdots g_k g_1^{-1} \cdots g_k^{-1} \in G'$. Tada je

$$\begin{aligned} &g_1 g_2 g_3 \cdots g_{k+1} g_1^{-1} g_2^{-1} g_3^{-1} \cdots g_{k+1}^{-1} = \\ &= \underbrace{(g_1 g_2 g_1^{-1} g_2^{-1})}_{[g_1, g_2]} \underbrace{(g_2 g_1) g_3 \cdots g_{k+1} (g_2 g_1)^{-1} g_3^{-1} \cdots g_{k+1}^{-1}}_{\text{po inducijskoj pretpostavci u } G'}, \end{aligned}$$

pa je $H \subseteq G'$.

288. Neka je G grupa. Dokazati da $a \in G'$ ako i samo ako postoje elementi $g_1, \dots, g_k \in G$, za neko $k \in \mathbb{N}$, takvi da je

$$a = g_1 \dots g_k \quad \text{i} \quad e = g_k \dots g_1.$$

Rešenje. Za svaki komutator $u = aba^{-1}b^{-1} = a(ba^{-1})b^{-1}$ važi $b^{-1}(ba^{-1})a = e$, pa i za proizvod komutatora postoji niz elemenata $g_1, \dots, g_k$ sa traženom osobinom.

Obrnuto, neka je $u = g_1 \dots g_k$ i $e = g_k \dots g_1$, tada je

$$u = ue^{-1} = g_1 \dots g_k g_1^{-1} \dots g_k^{-1},$$

pa na osnovu prethodnog zadatka $u \in G'$.

289. Dokazati da je u grupi G izvod G' normalna podgrupa.

290. Neka je H normalna podgrupa grupe G . Dokazati da je faktor grupa G/H Abelova ako i samo ako H sadrži izvod G' .

Rešenje. Neka je G/H Abelova grupa i $x, y \in G$. Tada je

$$\begin{aligned} xyx^{-1}y^{-1}H &= (xH)(yH)(x^{-1}H)(y^{-1}H) = \\ &= (xH)(yH)(xH)^{-1}(yH)^{-1} = (xH)(xH)^{-1}(yH)(yH)^{-1} = H, \end{aligned}$$

pa je $[x, y] = xyx^{-1}y^{-1} \in H$. Prema tome, $G' \subseteq H$.

Obrnuto, neka je $G' \subseteq H$. To znači da je za svako $x, y \in G$, $xyx^{-1}y^{-1} \in H$, tj. $xyx^{-1}y^{-1}H = H$. Poslednja jednakost je ekvivalentna sa $(xH)(yH)(xH)^{-1}(yH)^{-1} = H$, tj.

$$(xH)(yH) = (yH)(xH),$$

pa je G/H Abelova grupa.

PRIMEDBA. Direktna posledica ovog tvrđenja je da je G/G' Abelova grupa.

291. Neka je G konačna grupa neparnog reda. Dokazati da je proizvod svih elemenata grupe G element komutatorske podgrupe G' .

Rešenje. Neka je $G = \{g_1, g_2, \dots, g_n\}$. G' je normalna podgrupa grupe G , pa je

$$(g_1 g_2 \dots g_n)G' = (g_1 G')(g_2 G') \dots (g_n G') = X^m,$$

gde je m red grupe G' , a X je proizvod svih elemenata grupe G/G' . Grupa G je neparnog reda, pa je i red Abelove grupe G/G' takođe neparan broj. Na osnovu zadatka 78 je $X = G'$, pa sledi da je $(g_1 g_2 \dots g_n)G' = G'$, tj. $g_1 g_2 \dots g_n \in G'$.

292. Naći izvod G' grupe G regularnih matrica formata 2×2 nad poljem realnih brojeva $\mathbb{R}$.

Rešenje. Neka je ϕ preslikavanje grupe G u multiplikativnu grupu nenula realnih brojeva $\mathbb{R}^*$, definisano sa $\phi(A) = \det(A)$. ϕ je homomorfizam jer je $\det(AB) = \det(A)\det(B)$ za proizvoljne matrice A, B iz G . Jezgro homomorfizma ϕ su matrice iz G za koje važi $\det(A) = 1$.

Pošto je $\mathbb{R}^*$ Abelova grupa, na osnovu zadatka 290 sledi $G' \subseteq \text{Ker } \phi$.

Neka je $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{Ker } \phi$. Tada je ili

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & \frac{a-1}{c} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} \begin{bmatrix} 1 & \frac{d-1}{c} \\ 0 & 1 \end{bmatrix} \quad \text{kad je } c \neq 0,$$

ili je

$$A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 1/a \end{bmatrix} \begin{bmatrix} 1 & b/a \\ 0 & 1 \end{bmatrix} \quad \text{kad je } c = 0. \text{ Matrice}$$

$$\begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -r \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1/2 \end{bmatrix} \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = X^{-1}Y^{-1}XY,$$

$$\begin{bmatrix} 1 & 0 \\ s & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ s & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1/2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -s & 1 \end{bmatrix} = U^{-1}V^{-1}UV,$$

$$\begin{bmatrix} t & 0 \\ 0 & 1/t \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} t & 2t \\ 2t^2 & t^2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -\frac{1}{3}t & \frac{2}{3}t^2 \\ \frac{2}{3}t & -\frac{1}{3}t^2 \end{bmatrix} = W^{-1}Z^{-1}WZ,$$

su komutatori pa je $A \in G'$. Dakle, $G' = \text{Ker } \phi$, odnosno $G' = \{A \mid A \in G \text{ i } \det(A) = 1\}$.

293. Dokazati da su u grupi $(G, *)$ iz zadatka 35 elementi $x = (p, 0, 0, 0)$ i $y = (0, p, 0, 0)$ komutatori, a xy nije komutator.

294. Neka je G multiplikativna grupa matrica formata 2×2 nad poljem realnih brojeva sledećeg oblika

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \mid a, b \in \mathbb{R}, a > 0 \right\}.$$

Identifikovati matricu $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ sa tačkom (a, b) u ravni $\mathbb{R} \times \mathbb{R}$.

a) Šta odgovara komutatorskoj podgrupi G' ?

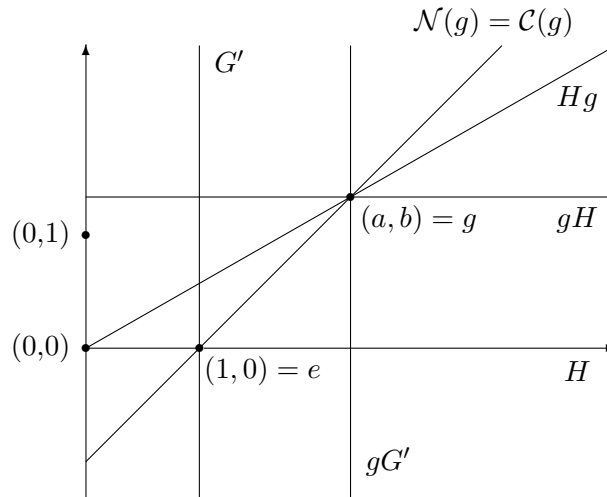
b) Šta odgovara faktor grupi G/G' ?

c) Šta odgovara podgrupi $H = \{x \mid x = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \text{ i } a > 0\}$?

d) Šta odgovara levim, a šta desnim suskupovima po podgrupi H ?

e) Šta odgovara normalizatoru $\mathcal{N}(g)$ i centralizatoru $\mathcal{C}(g)$ elementa $g = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$?

Rezultat. Na sledećoj slici su prikazani traženi skupovi.



Literatura:

G. Dobbins, G. Strate, *Matrix examples in modern algebra*, Amer. Math. Monthly, 85 (1978), 377–380.

295. Dokazati da je u grupi G svaka podgrupa H koja sadrži izvod grupe G ($H \supseteq G'$) normalna podgrupa grupe G .

Uputstvo. Koristiti da je faktor grupa G/G' Abelova, da je svaka podgrupa Abelove grupe normalna i zadatak 249 b.

296. Neka je $(G, *)$ grupa iz zadatka 35. Dokazati da je $G' \subseteq Z(G)$.

297. Neka je grupa G takva da je $G' \subseteq Z(G)$. Dokazati da za svako $x, y \in G$ i svaki prirodan broj n važi:

a) $[x^n, y^n] = [x, y]^{n^2},$

b) $(yx)^n = y^n x^n [x, y]^{\frac{n(n-1)}{2}}.$

Rešenje.

$$\begin{aligned} \text{a) } [x^n, y^n] &= x^n y^n x^{-n} y^{-n} = \underbrace{xx \dots x}_n \underbrace{(xy)y \dots y}_n x^{-n} y^{-n} = \\ &= \underbrace{x \dots x}_{n-1} ([x, y]yx) \underbrace{y \dots y}_{n-1} x^{-n} y^{-n} = \\ &= \underbrace{x \dots x}_{n-1} y(xy) \underbrace{y \dots y}_{n-2} x^{-n} y^{-n} [x, y] = \dots = \\ &= x^{n-1} y^n x^{-n+1} y^{-n} [x, y]^n = \dots = [x, y]^{n^2}. \end{aligned}$$

b) Primenimo indukciju po n . Za $n = 1$ tvrđenje očigledno važi. Ako pretpostavimo da važi za n , onda je

$$(yx)^{n+1} = (yx)^n yx = y^n x^n [x, y]^{\frac{n(n-1)}{2}} yx = y^n x^n yx [x, y]^{\frac{n(n-1)}{2}}.$$

Ako sad na $y^n x^n yx$ primenimo isti postupak koji je pod a) primenjen na $x^n y^n x^{-n} y^{-n}$, dobićemo da je

$$y^n x^n yx = y^{n+1} x^{n+1} [x, y]^n,$$

pa je

$$(yx)^{n+1} = y^{n+1} x^{n+1} [x, y]^{n + \frac{n(n-1)}{2}} = y^{n+1} x^{n+1} [x, y]^{\frac{n(n+1)}{2}}.$$

298. Neka je u grupi G G' izvod a $Z(G)$ centar. Ako za normalnu podgrupu $N \neq Z(G)$ važi $N \cap G' = \{e\}$, tada je $N \subseteq Z(G)$. Dokazati.

Rešenje. Pošto je N normalna podgrupa za svako $g \in G$ i svako $x \in N$, $gxg^{-1} \in N$, pa je i $[g, x] = (gxg^{-1})x^{-1} \in N$. S obzirom da $[g, x] \in G'$, mora biti $gxg^{-1}x^{-1} = e$, tj. $gx = xg$, što znači da $x \in Z(G)$. Prema tome, $N \subseteq Z(G)$.

299. Neka je u grupi G centar $Z(G)$ podgrupa indeksa n . Dokazati da G ima najviše n^2 različitih komutatora.

Rešenje. Neka su $x, y, u, v \in G$. Ako x i u pripadaju suskupu $a\mathcal{Z}(G)$, a y i v pripadaju suskupu $b\mathcal{Z}(G)$, dokazaćemo da je onda $[x, y] = [u, v]$. Tada je $x = ac_1$, $u = ac_2$, $c_1, c_2 \in \mathcal{Z}(G)$, pa je

$$xu^{-1} = ac_1(ac_2)^{-1} = ac_1c_2^{-1}a^{-1} = aa^{-1}c_1c_2^{-1} = c_1c_2^{-1} \in \mathcal{Z}(G).$$

Analogno, iz $y, v \in b\mathcal{Z}(G)$ sledi da $yv^{-1} \in \mathcal{Z}(G)$. Prema tome,

$$xyx^{-1}y^{-1} = (xu^{-1})u(yv^{-1})vu^{-1}(xu^{-1})^{-1}v^{-1}(yv^{-1})^{-1} = uvu^{-1}v^{-1}.$$

Dva elementa se iz n skupova mogu izabrati na n^2 različitih načina, dakle, u G ima najviše n^2 različitih komutatora.

300. Neka je G grupa, a $f : G \rightarrow G$ homomorfizam koji komutira sa svakim unutrašnjim automorfizmom grupe G . Neka je $K = \{x \mid x \in G \text{ i } f(f(x)) = f(x)\}$. Dokazati da je K normalna podgrupa grupe G koja sadrži G' .

Rešenje. Pošto g komutira sa svim unutrašnjim automorfizmima grupe G , onda je $f(a^{-1}xa) = a^{-1}f(x)a$ za svako $a \in G$.

Skup K očigledno nije prazan jer je $e \in K$. Neka $a, b \in K$, tada je

$$\begin{aligned} f(f(ab^{-1})) &= f(f(a)f(b^{-1})) = f(f(a))f(f(b^{-1})) = f(a)f((f(b))^{-1}) = \\ &= f(a)(f(f(b)))^{-1} = f(a)(f(b))^{-1} = f(a)f(b^{-1}) = f(ab^{-1}), \end{aligned}$$

pa je K podgrupa. Neka je $x \in G$, tada je

$$\begin{aligned} f(f(xax^{-1})) &= f(xf(a)x^{-1}) = xf(f(a))x^{-1} = \\ &= xf(a)x^{-1} = f(xax^{-1}), \end{aligned}$$

pa je K normalna podgrupa.

Neka $x, y \in G$, tada je

$$\begin{aligned} f(f(xy x^{-1} y^{-1})) &= f(f(xy x^{-1}) f(y)^{-1}) = f(xf(y)x^{-1} f(y)^{-1}) = \\ &= f(x)f(f(y)x^{-1} f(y)^{-1}) = f(x)f(y)f(x)^{-1} f(y)^{-1} = f(xy x^{-1} y^{-1}) \end{aligned}$$

pa K sadrži sve komutatore, dakle, sadrži i G' .

301. (i) Grupa G se naziva rešiva ako se njen n -ti izvod $G^{(n)}$, za neki konačan broj n , sastoji samo od neutralnog elementa.

(ii) Konačna grupa je rešiva ako je njen kompozicioni niz faktor grupa niz cikličkih grupa prostog reda (tj. ako je njen kompozicioni niz indeksa niz prostih brojeva).

Dokazati da su za konačne grupe ove dve definicije ekvivalentne.

302. Svaka komutativna grupa je rešiva. Dokazati.

Rešenje. Ako je G komutativna grupa svih komutatori su jednaki neutralnom elementu, pa je $G' = \{e\}$. Time je teorema dokazana.

Dokazaćemo ovu teoremu za konačne grupe još jednom koristeći samo definiciju (ii) iz prethodnog zadatka.

Neka je G konačna komutativna grupa, a H njena maksimalna normalna podgrupa. Prema poznatoj teoremi (H je maksimalna normalna podgrupa ako i samo ako je G/H prosta grupa) sledi da je G/H prosta grupa (grupa se naziva prostom ako nema netrivialne normalne podgrupe). Grupa G/H je Abelova pa, prema tome, G/H uopšte nema netrivialne podgrupe, odakle odmah sledi da je G/H ciklička grupa prostog reda.

Produžujući ovaj postupak, analognim rasuđivanjem dobijamo da je kompozicioni niz faktor grupa niz cikličkih grupa prostog reda, a to znači da je grupa G rešiva.

303. Dokazati da je grupa reda p^2 , gde je p prost broj, rešiva grupa.

Uputstvo. Koristiti zadatak 324.

PRIMEDBA. Generalizacija ovog zadatka je zadatak 308.

304. Svaka podgrupa rešive grupe je rešiva. Dokazati.

305. Svaka faktor grupa rešive grupe je rešiva. Dokazati.

306. Dokazati da je konačna grupa G rešiva ako i samo ako je njen kompozicioni niz faktor grupa niz Abelovih grupa.

307. Neka je N normalna podgrupa konačne grupe G . Ako su N i G/N rešive grupe, dokazati da je tada i G rešiva grupa.

Rešenje. Pošto su N i G/N rešive grupe, postoje prirodni brojevi m_1 i m_2 takvi da je $N^{(m_1)} = \{e\}$ i $(G/H)^{(m_2)} = N$. Neka je $m = \max(m_1, m_2)$. Neka je $f : G \rightarrow G/N$ prirodni homomorfizam. Lako se proverava da je za svako $n \in \mathbb{N}$ $f(G^{(n)}) \subseteq (G/H)^{(n)}$, pa je $f(G^{(m)}) \subseteq N$, tj. $G^{(m)} \subseteq N$. Tada je $G^{(2m)} = (G^{(m)})^{(m)} \subseteq N^{(m)} = \{e\}$, pa je G rešiva grupa.

PRIMEDBA. Ovo tvrđenje može se dokazati na drugi način koristeći direktno teoreme o korespondenciji podgrupa 1.67 i 1.69.

308. Dokazati da je svaka grupa G reda p^n , gde je p prost broj, $n \in \mathbb{N}$,

rešiva.

Uputstvo. Primeniti indukciju po n , koristeći zadatak 303, $G/Z(G)$ i činjenicu da je $Z(G)$ rešiva grupa.

309. Neka je G konačna grupa i neka je f netrivialan automorfizam grupe G takav da je za svako $x \in G$, $f(x) = x$ ili $f(x) = x^{-1}$. Dokazati da je G rešiva grupa.

Rešenje. Neka je $H = \{x \mid x \in G \text{ i } f(x) = x\}$. H je podgrupa grupe G , jer ako $x, y \in H$ onda $f(x) = x$ i $f(y) = y$, pa je i $f(x)f(y) = xy$, tj. $f(xy) = xy$, i na osnovu 1.17 konačan skup H je podgrupa.

Neka $h \in H$ i $a \notin H$, tada je $f(ah) = f(a)h = a^{-1}h$, a sa druge strane, $f(ah)$ je ili ah ili $(ah)^{-1}$, pa je ili $ah = a^{-1}h$ ili $(ah)^{-1} = a^{-1}h$. Iz $ah = a^{-1}h$ sledi $a = a^{-1}$, pa bi bilo $f(a) = a^{-1} = a$, tj. $a \in H$ što je kontradikcija. Dakle, $(ah)^{-1} = a^{-1}h$, tj. $a^{-1}ha = h^{-1}$. Iz ovoga sledi da je H normalna podgrupa grupe G .

Neka je $h, k \in H$ i $a \notin H$. Tada je

$$h^{-1} = (ak)^{-1}h(ak) = k^{-1}a^{-1}hak = k^{-1}h^{-1}k,$$

$hk = kh$, pa je H Abelova grupa.

Neka je $a, b \notin H$. Proizvod ab ili pripada ili ne pripada H . Ako $ab \notin H$, tada je

$$f(a^{-1}b^{-1}) = (a^{-1}b^{-1})^{-1} = f(a^{-1})f(b^{-1}) = (a^{-1})^{-1}(b^{-1})^{-1},$$

pa je $ba = ab$ i tada je $aHbH = abH = bHaH$. Ako $ab \in H$, tada i ba pripada H (jer ako $ba \notin H$, tada je $ba = ab \notin H$, što je kontradikcija) pa je $aHbH = abH = H = bHaH$. Dakle, G/H je Abelova grupa. H i G/H su rešive grupe, pa je na osnovu zadatka 307 i G rešiva grupa.

310. Dokazati da je direktan proizvod rešivih grupa rešiva grupa.

311. Za cikličku grupu C_{60} naći bar dva kompoziciona niza faktor grupa i proveriti izomorfnost tih nizova.

Rešenje. Neka je $C_{60} = \{a, a^2, \dots, a^{60} = e\}$. Ova grupa je komutativna pa su sve njene podgrupe normalne.

$$H_{30} = \{a^2, a^4, \dots, a^{60} = e\}$$

je jedna maksimalna normalna podgrupa grupe C_{60} .

$$H_{10} = \{a^6, a^{12}, \dots, a^{60} = e\}$$

je maksimalna normalna podgrupa grupe H_{30} , a

$$H_5 = \{a^{12}, a^{24}, \dots, a^{60} = e\}$$

je maksimalna normalna podgrupa grupe H_{10} . Na kraju,

$$H_1 = \{e\}$$

je maksimalna normalna podgrupa grupe H_5 , pa je kompozicioni niz faktor grupa:

$$C_{60}/H_{30}, H_{30}/H_{10}, H_{10}/H_5, H_5/H_1,$$

a kompozicioni niz indeksa:

$$2, 3, 2, 5.$$

Ako posmatramo sada niz podgrupa grupe C_{60} :

$$C_{60}, H_{20} = \{a^3, a^6, \dots, a^{60} = e\}, H_{10}, H_2 = \{a^{30}, a^{60} = e\}, H_1,$$

vidimo da je svaka podgrupa tog niza maksimalna normalna podgrupa prethodne, pa je to kompozicioni niz grupe C_{60} a kompozicioni niz faktor grupa je

$$C_{60}/H_{20}, H_{20}/H_1, H_{10}/H_2, H_2/H_1,$$

dok je kompozicioni niz indeksa

$$3, 2, 5, 2.$$

Na osnovu Žordan-Helderove (Jordan-Hölder) teoreme (1.91), faktor grupe jednog kompozicionog niza faktor grupa se mogu obostrano jednoznačno preslikati na faktor grupe drugog niza, tako da odgovarajuće faktor grupe budu izomorfne. Zaista,

$$\begin{aligned} C_{60}/H_{30} &\cong H_{20}/H_{10}, & H_{30}/H_{10} &\cong C_{60}/H_{20}, \\ H_{10}/H_5 &\cong H_2/H_1, & H_5/H_1 &\cong H_{10}/H_2. \end{aligned}$$

312. Da li dve grupe koje imaju izomorfne kompozicione nizove faktor grupa moraju biti izomorfne?

Rešenje. Ciklička grupa reda 6 i nekomutativna grupa reda 6 imaju izomorfne kompozicione nizove faktor grupa, ali nisu izomorfne.

313. Svaki prirodan broj n može se na jedinstven način prikazati kao proizvod prostih brojeva (ne uzimajući u obzir poredak). Dokazati ovo koristeći Žordan - Helderovu teoremu (1.91).

Uputstvo. Posmatrati grupu $(\mathbb{Z}_n, +)$.

1.10 Teoreme Silova

314. Normalizator nepraznog podskupa S grupe G je skup $\mathcal{N}(S) = \{x \mid x \in G, xS = Sx\}$.

Dokazati da je $\mathcal{N}(S)$ podgrupa grupe G .

Rešenje. Ako je $a, b \in \mathcal{N}(S)$, tj. $aS = Sa$ i $bS = Sb$, onda je

$$abS = aSb = Sab,$$

a to znači da je $ab \in \mathcal{N}(S)$. Iz jednakosti $aS = Sa$ množenjem sleva i zdesna sa a^{-1} dobijamo

$$Sa^{-1} = a^{-1}S, \quad \text{pa } a^{-1} \in \mathcal{N}(S).$$

Time je dokazano da je $\mathcal{N}(S)$ podgrupa.

315. Neka je G grupa i $\tilde{G} = \{x \mid x = (g, g), g \in G\}$ podgrupa direktnog proizvoda $G \times G$ (zadatak 265). Dokazati da je $\mathcal{N}(\tilde{G}) = \tilde{G}$ ako i samo ako je $\mathcal{Z}(G) = \{e\}$.

316. Dokazati da postoji bijektivno preslikavanje između skupa svih elemenata konjugovanih sa elementom a grupe G i skupa svih levih suskupova normalizatora $\mathcal{N}(a)$.

Rešenje. Definišimo preslikavanje f skupa svih levih suskupova normalizatora $\mathcal{N}(a)$ na skup svih elemenata konjugovanih sa a na sledeći način

$$f(x\mathcal{N}(a)) = xax^{-1}.$$

Dokažimo najpre da je f dobro definisana funkcija. Ako je $y\mathcal{N}(a) = x\mathcal{N}(a)$, onda je $y = xn$, $n \in \mathcal{N}(a)$, pa je

$$yay^{-1} = (xn)a(xn)^{-1} = x(nan^{-1})x^{-1} = xax^{-1},$$

(koristili smo da je $nan^{-1} = a$).

Funkcija f je očigledno surjektivna, pa preostaje da se dokaže da je i injektivna. Pretpostavimo da je $f(x\mathcal{N}(a)) = f(y\mathcal{N}(a))$, tj.

$$xax^{-1} = yzy^{-1}.$$

Onda je

$$(y^{-1}x)a = a(y^{-1}x),$$

pa $y^{-1}x \in \mathcal{N}(a)$, što znači da x i y pripadaju istom suskupu normalizatora $\mathcal{N}(a)$, tj. $xN(a) = yN(a)$.

317. Broj elemenata konjugovanih sa elementom a u grupi G jednak je indeksu normalizatora $\mathcal{N}(a)$ u toj grupi. Dokazati.

Rešenje. Posledica prethodnog zadatka.

PRIMEDBA. Primenom Lagranžove teoreme (1.50) odavde dobijamo da je broj elemenata u klasi međusobno konjugovanih elemenata konačne grupe uvek delitelj reda grupe.

318. Broj različitih podgrupa konjugovanih s podgrupom H grupe G jednak je indeksu normalizatora $\mathcal{N}(H)$ u grupi G . Dokazati.

Uputstvo. Dokaz je analogan dokazu u zadacima 316 i 317.

319. Jedina konačna grupa koja ima tačno dve klase konjugovanih elemenata je grupa reda 2. Dokazati.

Uputstvo. Uzeti u obzir da neutralni element sam čini jednu klasu konjugovanih elemenata, a zatim koristiti primedbu uz zadatak 317.

320. Odrediti sve neizomorfne konačne grupe koje imaju tačno tri klase konjugovanih elemenata.

Rešenje. Neka konačna grupa G ima 3 klase konjugovanih elemenata G_0, G_1, G_2 . Neka je G_0 klasa koja sadrži samo neutralni element, $|G_0| = 1$.

Ako se u centru $\mathcal{Z}(G)$ grupe G nalazi element $a (\neq e)$, tada $\{a\}$ čini posebnu klasu, tj. $|G_1| = 1$, pa se dobija $1 + 1 + n_2 = n$ gde je $|G_2| = n_2$. Pošto je $|G_2| = n_2$ indeks normalizatora nekog elementa iz G_2 , to je n_2 delitelj reda $n = |G|$ grupe G (1.54), pa je zbog $2 = n - n_2$, n_2 delitelj broja 2, tj. n_2 je 1 ili 2. $n_2 = 2$ ne može biti jer bi tada bilo $|G| = 4$, a sve grupe reda 4 su komutativne pa imaju 4 klase konjugovanih elemenata, dakle, $n_2 = 1$ i G je ciklička grupa reda 3.

Ako je $\mathcal{Z}(G) = \{e\}$, tada je i $n_1 > 1$ i $n_2 > 1$. Pošto su n_1 i n_2 delitelji broja n , a $1 + n_1 + n_2 = n$, imamo da je n_2 delitelj $1 + n_1$, a i n_1 delitelj $1 + n_2$. Rešavajući sistem jednačina

$$1 + n_1 = kn_2, \quad 1 + n_2 = ln_1, \quad k, l \in \mathbb{N},$$

uz uslov $n_1 > 1$ i $n_2 > 1$, dobija se rešenje $n_1 = 2$ i $n_2 = 3$, pa je G nekomutativna grupa reda 6, tj. $G \cong S_3$.

321. Red svakog elementa a konačne grupe G je stepen fiksnog prostog

broja p ako i samo ako je red grupe G stepen prostog broja p . Dokazati.

Uputstvo. Koristiti Košijevu teoremu (1.97).

322. Neka je H normalna podgrupa grupe G . Ako su H i G/H p -grupe dokazati da je i G p -grupa.

323. Ako je G konačna grupa reda p^n (p prost broj, n prirodan broj), onda centar te grupe ima bar dva elementa. Dokazati.

Rešenje. Neka su $K_1, K_2, \dots, K_m$ klase međusobno konjugovanih elemenata. S obzirom da je broj elemenata svake od tih klasa deljitelj reda grupe (zadatak 317), onda te klase imaju respektivno

$$p^{n_1}, p^{n_2}, \dots, p^{n_m}, \quad n \geq n_i \geq 0$$

elemenata, pa je

$$p^n = p^{n_1} + p^{n_2} + \dots + p^{n_m}.$$

Kako, međutim, jedna od klasa, recimo K_i , ima samo jedan element (neutralni), biće

$$p^n - (p^{n_1} + p^{n_2} + \dots + p^{n_{i-1}} + p^{n_{i+1}} + \dots + p^{n_m}) = 1.$$

Leva strana je deljiva sa p a desna nije, pa to znači da bar jedno n_j , $j = 1, 2, \dots, i-1, i+1, \dots, m$ mora biti 0, odnosno u grupi G postoji još jedna klasa konjugovanih elemenata koja se sastoji samo od jednog elementa (različitog od neutralnog). Taj element očividno pripada centru, pa je time tvrđenje dokazano.

324. Grupa reda p^2 , p prost broj, mora biti Abelova. Dokazati.

Rešenje. Centar $Z(G)$ ove grupe je podgrupa, pa je, prema tome, (na osnovu Lagranžove teoreme) red centra 1, p ili p^2 . Na osnovu prethodnog zadatka red centra nije 1. Ako pretpostavimo da $Z(G)$ ima p elemenata, onda faktor grupa $G/Z(G)$ ima p elemenata, pa kako je p prost broj grupa $G/Z(G)$ je ciklička. Međutim, na osnovu zadatka 284, sledi da je G Abelova grupa, pa centar te grupe ima p^2 elemenata, što je kontradikcija.

Prema tome, centar je reda p^2 , a to znači da je G Abelova grupa.

325. Neka je grupa G reda p^2q , gde su p i q različiti prosti brojevi takvi da je $p^2 \not\equiv 1 \pmod{q}$ i $q \not\equiv 1 \pmod{p}$. Dokazati da je G Abelova grupa.

Uputstvo. Dokazati da su podgrupe Silova normalne. Iskoristiti zadatak 324 i 1.73.

326. Naći sve neizomorfne grupe reda 8.

327. Naći sve neizomorfne grupe reda 9.

Uputstvo. Koristiti zadatak 324.

328. Neka je grupa G reda p^n (p prost broj). Dokazati da za svako $k \in \{0, 1, \dots, n\}$ postoji normalna podgrupa H grupe G takva da je $|H| = p^k$.

Rešenje. Dokaz ćemo dati indukcijom po n . Za $n = 1$ tvđenje je očevidno tačno. Pretpostavimo da je tačno za svako $m < n$ tj. u svakoj grupi reda p^m postoji normalna podgrupa reda p^k za svako $k \in \{0, 1, \dots, m\}$.

Na osnovu zadatka 323 $\mathcal{Z}(G) \neq \{e\}$. S obzirom da je $|\mathcal{Z}(G)|$ delitelj reda grupe G , biće $|\mathcal{Z}(G)| = p^r$, pa na osnovu Košijeve teoreme (1.97) $\mathcal{Z}(G)$ sadrži element a reda p . Ako je K ciklička podgrupa reda p generisana elementom a , onda je K normalna podgrupa grupe G (jer je svaka podgrupa centra $\mathcal{Z}(G)$ normalna podgrupa grupe G). Prema tome, $|G/K| = p^{n-1}$.

Na osnovu indukcijske pretpostavke G/K ima normalnu podgrupu $\overline{H}$ reda p^k za svako $k \in \{0, 1, \dots, n-1\}$. Prema 1.69 postoji normalna podgrupa H grupe G koja sadrži K takva da je $H/K = \overline{H}$. Red podgrupe H je p^{k+1} . Dakle, dokazali smo da G sadrži normalnu podgrupu reda p^k za svako $k \in \{1, 2, \dots, n\}$. Za $k = 0$ takva podgrupa je $\{e\}$, pa je time dokaz završen.

329. Neka je G konačna p -grupa i neka je H netrivialna normalna podgrupa grupe G . Dokazati da je $|H \cap \mathcal{Z}(G)| > 1$.

330. Dokazati da je u nekomutativnoj grupi reda p^3 , p prost broj, centar reda p .

Uputstvo. Koristiti zadatak 284.

331. Neka je G nekomutativna grupa reda p^3 , gde je p prost broj. Dokazati da je $G' = \mathcal{Z}(G)$.

Rešenje. Na osnovu prethodnog zadatka $|\mathcal{Z}(G)| = p$, a tada je $|G/\mathcal{Z}(G)| = p^2$, pa je na osnovu zadatka 324 $G/\mathcal{Z}(G)$ Abelova grupa, tj. $G' \subseteq \mathcal{Z}(G)$ (zadatak 290). Pošto je G nekomutativna grupa $G' \neq \{e\}$, pa je $G' = \mathcal{Z}(G)$ (jer je $\mathcal{Z}(G)$ grupa prostog reda pa nema netrivialne podgrupe).

332. Naći sve podgrupe Silova simetrične grupe S_4 .

Rezultat. $|S_4| = 3 \cdot 2^2$, ima četiri podgrupe Silova reda 3

$$H_1 = \{(1), (123), (132)\}, \quad H_2 = \{(1), (124), (142)\},$$

$$H_3 = \{(1), (134), (143)\}, \quad H_4 = \{(1), (234), (243)\},$$

i tri podgrupe Silova reda 8

$$K_1 = \{(1), (1234), (13)(24), (1432), (14)(23), (12)(34), (13), (24)\},$$

$$K_2 = \{(1), (1243), (14)(23), (1342), (13)(24), (12)(34), (23), (14)\},$$

$$K_3 = \{(1), (1324), (12)(34), (1423), (13)(24), (14)(32), (12), (34)\},$$

333. Ako je P p -podgrupa Silova konačne grupe G , dokazati da je $\mathcal{N}(\mathcal{N}(P)) = \mathcal{N}(P)$.

Rešenje. Neka je $x \in \mathcal{N}(\mathcal{N}(P))$, tada je

$$x\mathcal{N}(P)x^{-1} = \mathcal{N}(P),$$

odakle, pošto je $P \subseteq \mathcal{N}(P)$, sledi

$$xPx^{-1} \subseteq \mathcal{N}(P).$$

P je normalna podgrupa grupe $\mathcal{N}(P)$ (1.77), pa je na osnovu 1.106 P jedina podgrupa Silova u $\mathcal{N}(P)$. Konjugovanje sa $x \in \mathcal{N}(\mathcal{N}(P))$ prevodi P u podgrupu Silova grupe $\mathcal{N}(P)$, a pošto je P jedina takva podgrupa mora biti $xPx^{-1} = P$, tj. $x \in \mathcal{N}(P)$.

Dokazali smo da je $\mathcal{N}(\mathcal{N}(P)) \subseteq \mathcal{N}(P)$, da važi $\mathcal{N}(\mathcal{N}(P)) \supseteq \mathcal{N}(P)$ očigledno je, pa je $\mathcal{N}(\mathcal{N}(P)) = \mathcal{N}(P)$.

334. Ako je u konačnoj grupi G svaka p -podgrupa Silova normalna podgrupa za svaki prost broj p , dokazati da je grupa G izomorfna direktnom proizvodu svojih podgrupa Silova.

335. Neka je H p -podgrupa Silova konačne grupe G . Dokazati da su svi elementi normalizatora $\mathcal{N}(H)$ koji su reda p^k , $k \in \mathbb{N}$, sadržani u H .

Uputstvo. Koristiti da je svaka podgrupa reda p^k sadržana u nekoj p -podgrupi Silova i da je H normalna podgrupa u $\mathcal{N}(H)$.

336. Neka je G grupa reda $11^2 \cdot 13^2$. Dokazati da je G Abelova grupa.

Rešenje. Po teoremama Silova (1.105, 1.106, 1.107) G ima $1 + 11k$ podgrupa reda 11^2 i $1 + 13l$ podgrupa reda 13^2 . Pošto su $1 + 11k$ i $1 + 13l$ indeksi odgovarajućih normalizatora, to $1 + 11k$, odnosno $1 + 13l$, moraju biti delitelji $11^2 \cdot 13^2$, a to je moguće jedino kad je $k = l = 0$. Znači, postoji tačno jedna podgrupa H reda 11^2 i tačno jedna podgrupa K reda 13^2 .

Pošto su sve podgrupe koje su konjugovane sa podgrupom Silova takođe podgrupe Silova istog reda, a H i K su jedine podgrupe Silova reda 11^2 i 13^2 sledi da su H i K normalne podgrupe grupe G .

Na osnovu zadatka 324, podgrupe H i K su komutativne.

Pošto su 11 i 13 uzajamno prosti brojevi, mora biti $H \cap K = \{e\}$. Ako $a, b \in H$, $c, d \in K$, iz $ac = bd$ sledi $b^{-1}a = dc^{-1} \in H \cap K = \{e\}$, tj. $a = b$ i $c = d$, prema tome, $HK = G$.

Ako $h \in H$, $k \in K$, onda $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$ jer je H normalna podgrupa, a takođe je $hkh^{-1}k^{-1} = (hkh^{-1})k \in K$, jer je i K normalna podgrupa, dakle, $hkh^{-1}k^{-1} \in H \cap K = \{e\}$, tj. $hk = kh$.

Pošto je $G = HK$, a za svako $h \in H$, $k \in K$, $hk = kh$, grupa G je Abelova.

337. Dokazati da je svaka grupa reda 15 ciklička.

338. Odrediti sve neizomorfne grupe reda 99.

Rezultat. Ako je G grupa reda 99, onda je

$$G \cong C_3 \times C_3 \times C_{11} \quad \text{ili} \quad G \cong C_9 \times C_{11}.$$

339. Dokazati da grupa G reda 72 sadrži bar jednu netrivialnu normalnu podgrupu.

Rešenje. $72 = 2^3 \cdot 3^2$, pa na osnovu 1.107 sledi da ima $1 + 3k$ podgrupa reda 3^2 . $1 + 3k$ je činilac broja 72 za $k = 0$ i $k = 1$.

Dakle, G ima jednu ili četiri podgrupe Silova reda 3^2 . Ako G ima jednu podgrupu Silova H reda 3^2 , onda, s obzirom da su sve podgrupe Silova istog reda konjugovane, podgrupa H je normalna.

Ako G ima četiri podgrupe Silova reda 3^2 , onda su te podgrupe konjugovane a drugih sa njima konjugovanih nema, pa na osnovu zadatka 318 sledi da je indeks u G normalizatora svake od tih podgrupa 4. S obzirom da 72 nije delitelj $4!$, na osnovu zadatka 259 normalizator sadrži netrivialnu normalnu podgrupu grupe G .

340. Ako je grupa G reda $p^n q$, gde su p i q prosti brojevi i $p > q$, dokazati da tada G sadrži jedinstvenu normalnu podgrupu indeksa q .

341. Neka je G grupa reda 48. Dokazati da G ima bar jednu netrivialnu normalnu podgrupu.

Rešenje. Pošto je $48 = 2^4 \cdot 3$ G sadrži $1 + 2k$ 2-podgrupa Silova reda 16. $1 + 2k$ je delitelj broja 48 za $k = 0$ i $k = 1$. Za $k = 0$ G sadrži tačno jednu podgrupu Silova reda 16 koja mora biti normalna.

Za $k = 1$ ima 3 podgrupe Silova reda 16. Neka su H i K dve različite podgrupe Silova reda 16. Posmatrajmo podgrupu $H \cap K$. To je podgrupa čiji je red delitelj broja 16, dakle, 1, 2, 4 ili 8. Mogućnosti 1, 2 i 4 ne dolaze u obzir jer je tada (na osnovu 1.55)

$$|HK| = \frac{|H| |K|}{|H \cap K|} \geq 64,$$

a u G ima samo 48 elemenata.

Neka je $|H \cap K| = 8$. Tada je $H \cap K$ podgrupa indeksa 2 i u H i K , pa je $H \cap K$ normalna podgrupa u H i u K . Normalizator $\mathcal{N}(H \cap K)$ sadrži HK , pa je

$$|\mathcal{N}(H \cap K)| \geq |HK| = \frac{|H| |K|}{|H \cap K|} = 32.$$

Normalizator je podgrupa u G , pa je red $\mathcal{N}(H \cap K)$ delitelj 48 (1.50). Jedini činilac 48 veći od 32 je 48, pa je $\mathcal{N}(H \cap K) = G$.

Pošto je svaka podgrupa normalna podgrupa svog normalizatora (1.77), $H \cap K$ je netrivialna normalna podgrupa u G .

342. Dokazati da grupa G reda 56 ima pravu normalnu podgrupu.

Rešenje. Pošto je $56 = 2^3 \cdot 7$, u G postoji podgrupa Silova H reda 8. Posmatrajmo grupe Silova reda 7, njih ima $1 + 7k$ i $1 + 7k$ je delitelj 56. Dakle, ima jedna ($k = 0$) ili osam ($k = 1$) podgrupa Silova reda 7. Ako ima jedna, ona je normalna podgrupa. Ako ima osam podgrupa $K_1, K_2, \dots, K_8$, onda je $K_i \cap K_j = \{e\}$, $i \neq j$, pa je $\left| \bigcup_{i=1}^8 K_i \right| = 49$, tj. u G ima 48 elemenata reda 7. Podgrupa H ima 8 elemenata (od kojih nijedan nije reda 7), pa kako je $48 + 8 = 56$, postoji samo jedna podgrupa reda 8 i ona je u tom slučaju normalna podgrupa.

343. Grupe reda 12 i 200 sadrže normalnu podgrupu Silova. Dokazati.

344. Neka je K konačna normalna podrgrupa grupe G , a P podgrupa Silova u K . Dokazati da je $G = \mathcal{N}_G(P)K$, gde je $\mathcal{N}_G(P)$ normalizator P u G .

Rešenje. Neka je $g \in G$. P je podgrupa grupe K , pa je tada gPg^{-1} podgrupa u $gKg^{-1} = K$, jer je K normalna podgrupa u G . Svake dve podgrupe

Silova su konjugovane (1.106), pa postoji $h \in K$ takvo da je $gPg^{-1} = hPh^{-1}$, odakle je $h^{-1}gPg^{-1}h = P$ i $h^{-1}g$ je u normalizatoru $\mathcal{N}_G(P)$. Normalizator je podgrupa (zadatak 314), pa i $(hg^{-1})^{-1} = gh^{-1}$ pripada normalizatoru, a tada $g \in \mathcal{N}_G(P)K$. g je bio proizvoljan element u G i sledi $G \subseteq \mathcal{N}_G(P)K$, a pošto je $\mathcal{N}_G(P)K \subseteq G$, dobili smo da je $G = \mathcal{N}_G(P)K$.

345. Dokazati da postoje samo dve neizomorfne grupe reda $2p$, gde je p neparan prost broj.

Rešenje. Neka je G grupa reda $2p$, gde je p neparan prost broj. Na osnovu prve teoreme Silova u G postoji podgrupa reda 2, ona je ciklička i neka je njen generator a i postoji podgrupa reda p , ona je takođe ciklička i neka je njen generator b (zadatak 139). Grupa $\langle b \rangle$ je indeksa 2, pa je normalna. Dakle, $aba^{-1} = b^k$ pa je

$$b = a^2ba^{-2} = ab^ka^{-1} = (aba^{-1})^k = b^{k^2}.$$

Otuda je $k^2 \equiv 1 \pmod{p}$. Ova jednačina ima 2 rešenja $k = 1$ i $k = p - 1$. Za $k = 1$ je $aba^{-1} = b$, tj. $ab = ba$. Lako se proverava da među elementima $(ab)^i$, $i = 1, 2, \dots, 2p$, ne može biti jednakih, dakle G je ciklička grupa reda $2p$. Za $k = p - 1$ u grupi G važi $aba^{-1} = b^{p-1}$ pa je grupa izomorfna grupi simetrija pravilnog p -ougla (zadatak 16 d)).

346. Neka je G konačna grupa reda pq , gde su p i q prosti brojevi. Dokazati da G nije prosta grupa.

Rešenje. Ako je $p = q$, tvrđenje odmah sledi na osnovu zadatka 324.

Neka je $p > q$ i neka je C_p podgrupa generisana elementom reda p (1.97). Red grupe C_p nije delitelj $q!$, pa na osnovu zadatka 259 C_p sadrži normalnu podgrupu grupe G različitu od $\{e\}$. p je prost broj, pa je C_p jedina podgrupa u C_p različita od $\{e\}$, dakle, C_p je normalna podgrupa u G .

347. Neka je red grupe G proizvod tri različita prosta broja. Dokazati da grupa G nije prosta.

Rešenje. Neka je $|G| = pqr$, gde su p , q i r prosti brojevi takvi da je $p > q > r$. Neka u G ima s_p , s_q i s_r podgrupa Silova reda p , q i r respektivno. Ako je grupa G prosta, tada su $s_p > 1$, $s_q > 1$ i $s_r > 1$ na osnovu 1.104. S obzirom da su p -podgrupe Silova reda p , presek dve različite p -podgrupe Silova sadrži samo e . To znači da s_p različitih p -podgrupa Silova grupe G sadrže $s_p(p - 1)$ različitih elemenata reda p . Analogno tvrđenje važi i za q -

i r -podgrupe Silova pa se dobija da je

$$|G| = pqr \geq 1 + s_p(p-1) + s_q(q-1) + s_r(r-1).$$

Na osnovu druge i treće teoreme Silova (1.105 i 1.106) s_p deli qr i $s_p = 1 + kp$, za prirodan broj $k \geq 1$, tj. $s_p > p$. Međutim, $p > q$ i $p > r$ pa mora biti $s_p = qr$. Iz istih razloga, s_q deli pr i $s_q > q$ pa je $s_q = p$ ili $s_q = pr$, a u svakom slučaju je $s_q \geq p$, a analogno se dobija i $s_r \geq q$. Ako se ove granice za s_p , s_q i s_r uvrste u gornju nejednakost dobija se

$$pqr \geq 1 + qr(p-1) + p(q-1) + q(r-1),$$

a odavde sledi

$$0 \geq (p-1)(q-1),$$

što je protivrečnost. Dakle, neki od s_p , s_q ili s_r mora biti 1, a tada G sadrži normalnu podgrupu zbog 1.104.

1.11 Automorfizmi grupa

348. Skup $\mathcal{A}(G)$ svih automorfizama grupe G u odnosu na kompoziciju preslikavanja čini grupu. Dokazati.

349. Dokazati da je grupa automorfizama grupe $(\mathbb{Z}_n, +)$ izomorfna grupi ostataka po modulu n uzajamno prostih sa n u odnosu na množenje.

Uputstvo. Koristiti zadatak 147.

350. Dokazati da je grupa automorfizama grupe $(\mathbb{Q}, +)$ izomorfna grupi $(\mathbb{Q} \setminus \{0\}, \cdot)$.

351. Naći grupu automorfizama $\mathcal{A}(G)$ nekomutativne grupe G reda 6.

Rešenje. Grupa G je generisana elementima a, b i pritom je $a^3 = b^2 = (ab)^2 = e$ (zadatak 224). Svaki automorfizam će biti potpuno određen ako znamo slike elemenata a i b . Kako slika elementa $a^3 (= e)$ mora biti e , sledi da slika elementa a ima red 3 i, analogno, slika od b je reda 2 (nijedna od tih slika ne može biti e jer je automorfizam injektivno preslikavanje). Prema tome, slike od a mogu biti samo a i a^2 , a slike od b elementi b, ab, a^2b , tj. automorfizama može biti 6 (elementi u koloni ispod oznake funkcije

predstavljaju slike elemenata grupe dobijene tom funkcijom):

	f_1	f_2	f_3	f_4	f_5	f_6
e	e	e	e	e	e	e
a	a	a	a	a^2	a^2	a^2
a^2	a^2	a^2	a^2	a	a	a
b	b	ab	a^2b	b	ab	a^2b
ab	ab	a^2b	b	a^2b	b	ab
a^2b	a^2b	b	ab	ab	a^2b	b

Svako od preslikavanja f_i , $i = 1, 2, \dots, 6$, prikazanih u tabeli je zaista automorfizam. Kako je

$$f_3^3 = f_4^2 = (f_3 f_4)^2 = f_1,$$

grupa automorfizama $\mathcal{A}(G)$ je nekomutativna grupa sa 6 elemenata, tj. izomorfna je grupi G .

352. Naći grupu automorfizama Klajnove četvorne grupe (zadatak 224).

Rezultat. Grupa automorfizama je izomorfna grupi S_3 .

353. Dokazati da je u grupi G preslikavanje $f_a : x \mapsto axa^{-1}$, automorfizam.

(Takav automorfizam naziva se unutrašnji (1.108, 1.110).)

Rešenje. Dokažimo najpre da je f_a bijekcija. Ako je $f_a(x) = f_a(y)$, tj. $axa^{-1} = aya^{-1}$, onda mora biti $x = y$, pa je f injektivno preslikavanje.

Svaki element $x \in G$ je slika elementa $a^{-1}xa$, jer je $f_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x$, tj. f je surjektivno. Kako je

$$f_a(x)f_a(y) = (axa^{-1})(aya^{-1}) = a(xy)a^{-1} = f_a(xy),$$

za svako $x, y \in G$, preslikavanje f_a je zaista automorfizam.

354. Dokazati da je skup unutrašnjih automorfizama normalna podgrupa grupe svih automorfizama.

355. Naći sve unutrašnje automorfizme grupe simetrija kvadrata (zadatak 16 b).

356. Dokazati da je grupa $\mathcal{U}(G)$ svih unutrašnjih automorfizama grupe G homomorfna slika grupe G .

Rešenje. Ako sa f_a označimo unutrašnji automorfizam koji je određen elementom a , $f_a : x \mapsto axa^{-1}$, onda funkcija $\phi : a \mapsto f_a$ preslikava G na skup $\mathcal{U}(G)$ svih unutrašnjih automorfizama. Kako je

$$(f_a \cdot f_b)(x) = f_a(f_b(x)) = a(f_b(x))a^{-1} = a(bxb^{-1})a^{-1} = abx(ab)^{-1} = f_{ab}(x),$$

biće

$$\phi(ab) = f_{ab} = f_a \cdot f_b = \phi(a)\phi(b),$$

pa je time pokazano da je ϕ homomorfizam. Homomorfna slika grupe je grupa, pa je, prema tome, $\mathcal{U}(G)$ grupa.

357. Odrediti jezgro homomorfizma ϕ definisanog u rešenju zadatka 356.

Rešenje. Neutralni element grupe unutrašnjih automorfizama je identičko preslikavanje, pa jezgro homomorfizma ϕ čine svi elementi a za koje je preslikavanje $f_a(x) = axa^{-1}$ identičko, $x = axa^{-1}$, za svako $x \in G$, tj. $ax = xa$, za svako $x \in G$.

Prema tome, jezgro ovog homomorfizma je centar $\mathcal{Z}(G)$ grupe G , pa je prema prvoj teoremi o izomorfizmu grupa (1.64)

$$G/\mathcal{Z}(G) \cong \mathcal{U}(G).$$

358. Ako je grupa $\mathcal{U}(G)$ unutrašnjih automorfizama grupe G ciklička grupa, onda je $\mathcal{U}(G)$ trivijalna grupa. Dokazati.

Rešenje. Na osnovu zadatka 357 $\mathcal{U}(G) \cong G/\mathcal{Z}(G)$, pa je na osnovu zadatka 284 G Abelova grupa.

359. Neka je f automorfizam konačne grupe G takav da je $f(x) = x$ samo za $x = e$. Dokazati:

a) Preslikavanje $g : G \rightarrow G$ definisano sa $g(x) = f(x)x^{-1}$, je bijekcija.

b) Ako je f^2 identičko preslikavanje, tada je G Abelova grupa neparnog reda.

Rešenje. a) Iz pretpostavke $g(x) = g(y)$, tj. $f(x)x^{-1} = f(y)y^{-1}$, sledi $(f(y))^{-1}f(x) = y^{-1}x$, tj. $f(y^{-1}x) = y^{-1}x$. Dakle, $y^{-1}x = e$, tj. $x = y$, pa je g injektivno. S obzirom da je G konačan skup g mora biti bijekcija.

b) Za svako $x \in G$ je

$$f(g(x)) = f(f(x)x^{-1}) = xf(x^{-1}) = (f(x)x^{-1})^{-1} = (g(x))^{-1}.$$

S obzirom da je g bijekcija, onda za svako $x \in G$ $f(x) = x^{-1}$, pa je

$$y^{-1}x^{-1} = (xy)^{-1} = f(xy) = f(x)f(y) = x^{-1}y^{-1},$$

odakle sledi $xy = yx$, za svako $x, y \in G$.

Ako bi red grupe bio paran broj, onda bi na osnovu zadatka 70 postojao u G element z reda 2, dakle, bilo bi $z^{-1} = z$, $z \neq e$, tj. $f(z) = z$, što je protivrečnost. Prema tome, grupa G je neparnog reda.

360. Ako je G konačna grupa a k prirodan broj koji je uzajamno prost sa $|G|$ i ako je za svako $a, b \in G$

$$(ab)^k = a^k b^k$$

dokazati da je

- a) $f : x \mapsto x^k$ automorfizam grupe G ,
- b) za svako $a \in G$, $a^{k-1} \in \mathcal{Z}(G)$.

Rešenje. a) Preslikavanje f je homomorfizam jer je

$$f(ab) = (ab)^k = a^k b^k = f(a)f(b).$$

Neka je $a \in \text{Ker } f$, tada je $f(a) = e$, tj. $a^k = e$, a pošto je k uzajamno prosto sa $|G|$ to je $a = e$ (jer bi inače postojala podgrupa čiji red ne deli red grupe) i f je monomorfizam (zadatak 108). Monomorfizam konačne grupe je i epimorfizam, pa je f automorfizam.

- b) Iz $a^k b^k = (ab)^k$ sledi $a^{k-1} b^{k-1} = (ba)^{k-1}$, pa je

$$a^{k-1} b^k a = (ba)^k = b^k a^k,$$

tj.

$$a^{k-1} b^k = b^k a^{k-1}.$$

S obzirom na a) za svako $x \in G$ postoji $b \in G$ tako da je $x = b^k$, dakle, za svako $x \in G$ $a^{k-1} x = x a^{k-1}$, tj. $a^{k-1} \in \mathcal{Z}(G)$.

361. Grupa automorfizama nekomutativne grupe ne može biti ciklička. Dokazati.

Uputstvo. Koristiti zadatke 284, 357 i 142.

362. Dokazati da ne postoji grupa G čija je grupa automorfizama $\mathcal{A}(G)$ ciklička grupa neparnog reda većeg od 1.

Rešenje. Pretpostavimo da je G grupa čija je grupa automorfizama ciklička grupa neparnog reda većeg od 1. Na osnovu zadatka 361, grupa G mora biti Abelova grupa. Abelova grupa uvek ima automorfizam $\phi : x \mapsto x^{-1}$. Ako je za neko $x \in G$, $x \neq x^{-1}$, tada je $\phi \neq \text{id}_G$ i $\phi^2 = \text{id}_G$, pa bi red grupe $\mathcal{A}(G)$ bio paran. Ako su svi elementi u grupi G reda 2, tada je ili $|G| = 2$ i G ima samo jedan element reda 2 ili je $|G| > 2$. Ako u G ima samo jedan element reda dva, tada je grupa automorfizama trivijalna $\mathcal{A}(G) = \{\text{id}_G\}$, a ako u G ima bar dva elementa a, b reda 2, tada G sadrži podgrupu $H = \langle a, b \rangle$ reda 4 izomorfnu Klajnovoj četvornoj grupi ($C_2 \times C_2$). Svaki automorfizam f podgrupe H može se proširiti do automorfizma cele grupe G (ako se definiše $f(x) = x$ za svako $x \in G \setminus H$), pa kako je $\mathcal{A}(H) \cong S_3$ (zadatak 352), sledi da $\mathcal{A}(G)$ ima nekomutativnu podgrupu.

363. Ako je grupa G bez centra (tj. centar se sastoji samo od neutralnog elementa), onda je i njena grupa automorfizama bez centra. Dokazati.

Rešenje. Neka je f automorfizam grupe G različit od identičkog preslikavanja i neka je element $a \in G$ takav da je $f(a) = b$, $b \neq a$. Ako pretpostavimo da f pripada centru grupe automorfizama, onda f komutira sa unutrašnjim automorfizmom proizvedenim elementom a , tj. za svako $g \in G$

$$af(g)a^{-1} = f(aga^{-1}) = bf(g)b^{-1}.$$

Odavde je

$$(a^{-1}b)f(g) = f(g)(a^{-1}b),$$

pa pošto $f(g)$ prolazi kroz celu grupu G kad g prolazi kroz G , sledi da element $a^{-1}b$ ($\neq e$) pripada centru grupe G . To je protivrečno sa pretpostavkom da G nema centra, pa sledi da ni grupa $\mathcal{A}(G)$ ne može imati centar.

364. Bijektivno preslikavanje f grupe G na grupu G naziva se antiautomorfizam ako je za svako $x, y \in G$

$$f(xy) = f(y)f(x).$$

Dokazati da je f antiautomorfizam grupe G ako i samo ako je $f = gh$, gde je $g(x) = x^{-1}$, za svako $x \in G$, a h je automorfizam grupe g .

Rešenje. Označimo sa g funkciju koja preslikava $x \mapsto x^{-1}$, (u zadatku 110 je pokazano da je g bijekcija grupe G na sebe). S obzirom da su elementi x i x^{-1} jedan drugom inverzni, zaključujemo da se inverzno preslikavanje g^{-1} poklapa sa g , tj. $g = g^{-1}$.

Neka je f antiautomorfizam grupe G . Onda za svako $x, y \in G$ iz

$$f(xy) = f(y)f(x),$$

sledi

$$(f(xy))^{-1} = (f(x))^{-1}(f(y))^{-1},$$

ili drugačije napisano

$$(gf)(xy) = (gf)(x)(gf)(y),$$

a kako je gf bijekcija (jer su g i f bijekcije) sledi da je gf automorfizam grupe G . Označimo li taj automorfizam sa h , imamo $gf = h$, ili $f = g^{-1}h$, pa kako smo ranije videli da je $g^{-1} = g$, dobijamo da je $f = gh$, što je trebalo dokazati.

Obrnuto, neka je $f = gh$, gde je h automorfizam grupe G , $g : x \mapsto x^{-1}$. f je bijekcija jer je proizvod dve bijekcije. Pored toga je

$$\begin{aligned} f(xy) &= (gh)(xy) = (h(x)h(y))^{-1} = (h(y))^{-1}(h(x))^{-1} = \\ &= (gh)(y)(gh)(x) = f(y)f(x), \end{aligned}$$

za svako $x, y \in G$, što znači da je f antiautomorfizam.

II

PRSTENI

2.1 Pregled definicija i teorema

2.1. Neka je R neprazan skup na kome su definisane dve binarne operacije $+$ i $\cdot$ (koje ćemo nazivati „sabiranje” i „množenje” respektivno). Tada se uređena trojka $(R, +, \cdot)$ naziva prsten ako i samo ako važi:

R1. $(R, +)$ je Abelova grupa.

R2. Za svako $a, b, c \in R$ $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (množenje je asocijativno).

R3. Za svako $a, b, c \in R$ $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,
(leva distributivnost množenja u odnosu na sabiranje).

Za svako $a, b, c \in R$ $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$,
(desna distributivnost množenja u odnosu na sabiranje).

Često ćemo, kada se podrazumeva o kojim je operacijama reč, umesto prsten $(R, +, \cdot)$ pisati samo prsten R . Kao i kod grupa, obično ćemo izostavljati znak $\cdot$ i pisati ab umesto $a \cdot b$. Takođe ćemo umesto $(ab) + (ac)$ pisati $ab + ac$, podrazumevajući da se najpre primenjuje operacija $\cdot$ pa tek onda operacija $+$.

Neutralni element za sabiranje u prstenu R ćemo označavati sa 0 (ili sa 0_R). Inverzni element elementa $a \in R$ u odnosu na operaciju $+$ označavaćemo sa $-a$ i nazvaćemo ga suprotni element elementa a . Umesto $a + (-b)$ pišaćemo $a - b$.

2.2. Prsten $(R, +, \cdot)$ se naziva komutativan prsten ako i samo ako je operacija $\cdot$ komutativna, tj. za svako $a, b \in R$ $ab = ba$.

2.3. Prsten $(R, +, \cdot)$ se naziva prsten sa jedinicom ako i samo ako postoji element $1 \in R$ takav da je za svako $a \in R$

$$1 \cdot a = a \cdot 1 = a.$$

Element 1 nazivamo jedinica prstena (jedinicu prstena R označavaćemo u nekim slučajevima sa 1_R ili sa e).

Ako je R prsten sa jedinicom sa bar dva elementa, onda je uvek $1 \neq 0$. Uбудуće ćemo kad god kažemo „prsten sa jedinicom” podrazumevati da je reč o prstenu sa bar dva elementa.

2.4. U prstenu $(R, +, \cdot)$ za svako $a, b, c \in R$ i svako $n \in \mathbb{Z}$ važi:

- (i) $a0 = 0a = 0$,
- (ii) $a(b - c) = ab - ac$, $(a - b)c = ac - bc$,
- (iii) $a(-b) = (-a)b = -(ab)$,
- (iv) $(-a)(-b) = ab$,
- (v) $(na)b = a(nb) = n(ab)$,

pri tom, ako je x element prstena R , a n ceo broj, onda je nx definisano sa

$$nx = \begin{cases} \underbrace{x + \dots + x}_{n \text{ sabiraka}}, & \text{za } n > 0, \\ 0_R, & \text{za } n = 0, \\ (-n)(-x), & \text{za } n < 0. \end{cases}$$

2.5. U prstenu R element a se naziva levi (desni) delitelj elementa $b \neq 0$ ako i samo ako postoji element $c \in R$ tako da je $b = ac$ ($b = ca$). Element a prstena R koji je levi ili desni delitelj elementa $b \in R$ se naziva delitelj elementa b .

Da je u komutativnom prstenu R element a delitelj elementa b zapisivaćemo sa $a|b$, a da a nije delitelj b zapisivaćemo sa $a \nmid b$.

Element $a \neq 0$ se naziva levi (desni) delitelj nule ako i samo ako postoji element $b \neq 0$ takav da je $ab = 0$ ($ba = 0$). Element prstena koji je levi ili desni delitelj nule naziva se delitelj nule.

2.6. U prstenu R važe zakoni levog i desnog skraćivanja (kancelacije) za množenje (1.12 g) ako i samo ako prsten R nema delitelja nule.

2.7. Komutativan prsten sa jedinicom bez delitelja nule se naziva domen integriteta (ili integralni domen ili samo domen).

2.8. Element $x \neq 0$ prstena R se naziva levo (desno) regularan ako i samo ako za element x važi zakon leve (desne) kancelacije, tj. iz $xa = xb$ sledi $a = b$ (iz $ax = bx$ sledi $a = b$). Element koji je levo i desno regularan naziva se regularan.

2.9. Prsten R u kome su regularni svi elementi različiti od nule, nema delitelja nule.

2.10. Ako je u prstenu sa jedinicom R element $a \in R$ takav da postoji element $b \in R$ tako da je $ba = 1$ ($ab = 1$) onda se b naziva levi (desni) multiplikativan inverzni element za a .

Ako je b takvo da je

$$ab = ba = 1,$$

onda se b naziva multiplikativan inverzni (ili samo inverzni) element za a . Tada je b jedini multiplikativan inverzni element elementa a i označava se sa a^{-1} .

Ako za element a postoji multiplikativan inverzni element a^{-1} , onda se a naziva invertibilan element.

2.11. Ako u prstenu R element a ima levi (desni) inverzni element, tada je a levo (desno) regularan.

2.12. Najmanji prirodan broj n (ako takav broj postoji) takav da je za svaki element x prstena R

$$nx = 0$$

naziva se karakteristika prstena R . Ukoliko takav broj ne postoji, kažemo da je prsten R karakteristike nula. Karakteristiku prstena R označavaćemo sa $\text{Char } R$.

Prsten s jedinicom je karakteristike n ako i samo ako je $n1 = 0$ i $k1 \neq 0$ za svako $k \in \{1, \dots, n-1\}$.

2.13. Prsten s jedinicom u kome je svaki element različit od nule invertibilan se naziva telo (ili prsten sa deljenjem).

2.14. Prsten $(R, +, \cdot)$ je telo ako i samo ako je $(R \setminus \{0\}, \cdot)$ grupa.

2.15. Komutativan prsten s jedinicom u kome je svaki element različit od nule invertibilan se naziva polje.

2.16. Prsten $(R, +, \cdot)$ je polje ako i samo ako je $(R \setminus \{0\}, \cdot)$ Abelova grupa.

2.17. Element x prstena R se naziva idempotentan (ili idempotent) ako i samo ako je $x^2 = x$.

2.18. Prsten sa jedinicom u kome su svi elementi idempotentni se naziva Bulov (Boole) prsten. Svaki Bulov prsten je komutativan i ima karakteristiku 2.

2.19. Prsten sa jedinicom R u kome za svako $x \in R$ postoji $y \in R$ takvo da je

$$xyx = x$$

se naziva fon Nojmanov (von Neumann) regularan prsten (ili samo regularan prsten).

2.20. Svako telo, svako polje i svaki Bulov prsten su fon Nojmanovi regularni prsteni.

2.21. Element x prstena R se naziva nilpotentan ako i samo ako postoji prirodan broj n takav da je $x^n = 0$.

2.22. Prsten u kome je jedini nilpotentan element 0 nazivaćemo prsten bez nilpotentnih elemenata.

2.23. U komutativnom prstenu sa jedinicom R element $c \neq 0$ naziva se nesvodljiv ako i samo ako važe sledeći uslovi:

- (i) c nije invertibilan element u R ,
- (ii) ako je $c = ab$, tada je a ili b invertibilan element prstena R , tj. c se ne može prikazati u obliku proizvoda dva neinvertibilna elementa.

2.24. Domen integriteta R se naziva domen sa jednoznačnom faktORIZACIJOM ako i samo ako važe sledeći uslovi:

- (i) svaki element $r \in R$, $r \neq 0$, koji nije invertibilan u R može se prikazati u obliku

$$r = c_1 c_2 \dots c_n,$$

gde su c_i , $i = 1, 2, \dots, n$, nesvodljivi elementi iz R .

- (ii) iz

$$r = c_1 c_2 \dots c_n = d_1 d_2 \dots d_m,$$

gde su c_i , $i = 1, 2, \dots, n$, d_j , $j = 1, 2, \dots, m$ nesvodljivi elementi iz R , sledi da je $n = m$, da postoji permutacija σ skupa $\{1, 2, \dots, n\}$ i invertibilni elementi u_i , $i = 1, 2, \dots, n$, tako da je

$$c_i = u_i d_{\sigma(i)}, \quad i = 1, 2, \dots, n.$$

2.25. Domen integriteta R se naziva Euklidov prsten (ili Euklidov domen) ako i samo ako je svakom elementu $a \in R$, $a \neq 0$, pridružen neneгатivan ceo broj $\phi(a)$, tj. definisana je funkcija

$$\phi : R \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\},$$

tako da važe sledeći uslovi:

E1. Za svako $a, b \in R \setminus \{0\}$

$$\phi(ab) \geq \phi(a).$$

E2. Za svako $a, b \in R$, $b \neq 0$, postoje $q, r \in R$ (q – „količnik”, r – „ostatak”) tako da je

$$a = bq + r,$$

gde je $\phi(r) < \phi(b)$ ili je $r = 0$.

2.26. Neka je $(R, +, \cdot)$ prsten, a S neprazan podskup od R . S se naziva potprsten prstena R ako i samo ako je S prsten u odnosu na restrikcije operacija $+$ i $\cdot$ na S .

2.27. Neka je $(R, +, \cdot)$ prsten, a S neprazan podskup od R . S je potprsten prstena R ako i samo ako za svako $a, b \in S$, $a - b \in S$ i $ab \in S$.

2.28. U prstenu R skup

$$\mathcal{C}(R) = \{x \in R \mid xa = ax, \text{ za svako } a \in R\}$$

se naziva centar prstena R .

$\mathcal{C}(R)$ je potprsten prstena R .

2.29. Neka su A i B podskupovi prstena R . Sa $A + B$ označićemo skup

$$A + B = \{x \mid x = a + b, a \in A, b \in B\},$$

a sa AB skup

$$AB = \{x \mid x = a_1 b_1 + \dots + a_k b_k, k \in \mathbb{N}, a_i \in A, b_i \in B, i = 1, \dots, k\},$$

tj. AB je skup svih konačnih suma proizvoda $a_i b_i$, $a_i \in A$, $b_i \in B$.

Umesto $\{x\} + A$ pišaćemo $x + A$, a umesto $\{x\}A$ pišaćemo xA .

2.30. Neprazan podskup I prstena R se naziva levi (desni) ideal u R ako i samo ako važi:

(i) $(I, +)$ je podgrupa grupe $(R, +)$,

(ii) za svako $x \in I$ i svako $r \in R$

$$rx \in I \quad (xr \in I).$$

2.31. Ako je I i levi i desni ideal u prstenu R , I se naziva ideal u R .

2.32. Presek proizvoljne familije ideala prstena R je ideal u R .

2.33. U prstenu R skup $\{0\}$ i sam skup R su ideali i ti ideali se nazivaju trivijalni. Ostali ideali se nazivaju netrivijalni.

Ideali u prstenu R različiti od R nazivaju se pravi.

2.34. Ideal M , $M \neq R$, prstena R je maksimalan ideal ako i samo ako ne postoji pravi ideal u R različit od M a koji sadrži M , tj. za svaki ideal I za koji je $M \subseteq I \subseteq R$ sledi $I = M$ ili $I = R$.

Analogno se definiše maksimalan levi (desni) ideal, a takođe i minimalni ideal, odnosno minimalan levi (desni) ideal.

2.35. Neka je R prsten sa jedinicom. Tada je svaki ideal sadržan u nekom maksimalnom idealu prstena R .

Analogno tvrđenje važi za leve (desne) ideale.

2.36. U prstenu R ideal $P \neq R$ se naziva prost ideal ako i samo ako za svaka dva ideala I, J u R važi

$$IJ \subseteq P \Rightarrow I \subseteq P \text{ ili } J \subseteq P.$$

2.37. U komutativnom prstenu R ideal $P \neq R$ je prost ideal ako i samo ako za svako $a, b \in R$

$$ab \in P \Rightarrow a \in P \text{ ili } b \in P.$$

2.38. Neka je S podskup prstena R . Presek svih ideala koji sadrže S (tj. minimalan ideal koji sadrži S) naziva se ideal generisan skupom S i

označava se sa (S) . Elementi skupa S se nazivaju generatori ideala (S) . Ako je $S = \{x_1, x_2, \dots, x_n\}$ umesto $(\{x_1, x_2, \dots, x_n\})$ pisaćemo $(x_1, x_2, \dots, x_n)$.

Analogno se definiše levi (desni) ideal generisan skupom S .

2.39. Ideal generisan jednim elementom nazivamo glavni ideal. Glavni ideal generisan elementom a označavaćemo sa (a) , a u slučaju komutativnog prstena sa jedinicom R i sa Ra (ako je R komutativan prsten sa jedinicom glavni ideal (a) se sastoji od svih proizvoda oblika ra , $r \in R$).

2.40. Prsten u kome je svaki ideal glavni se naziva prsten glavnih ideala.

2.41. U komutativnom prstenu sa jedinicom R skup svih nilpotentnih elemenata je ideal koji je jednak preseku svih prostih ideala prstena R .

2.42. Homomorfizam prstena $(R, +, \cdot)$ u prsten $(S, *, \circ)$ je preslikavanje $f : R \rightarrow S$ za koje za svako $x, y \in R$ važi

$$(i) \ f(x + y) = f(x) * f(y),$$

$$(ii) \ f(x \cdot y) = f(x) \circ f(y).$$

2.43. Jezgro homomorfizma f prstena R u prsten S je skup svih elemenata iz R koji se preslikavaju u nulu prstena S . Jezgro homomorfizma f označavaćemo sa $\text{Ker } f$, dakle,

$$\text{Ker } f = \{x \in R \mid f(x) = 0\}.$$

Sa $\text{Im } f$ (ili sa $f(R)$) označavaćemo skup

$$\text{Im } f = f(R) = \{y \in S \mid (\exists r \in R) \ f(r) = y\},$$

i taj skup nazivamo slika homomorfizma f .

2.44. Homomorfizam prstena koji je injektivno preslikavanje se naziva monomorfizam, homomorfizam koji je surjektivno preslikavanje se naziva epimorfizam, dok se homomorfizam koji je bijekcija naziva izomorfizam.

Prsten R je izomorfan prstenu S ako i samo ako postoji izomorfizam $f : R \rightarrow S$. Da je prsten R izomorfan prstenu S označavaćemo sa $R \cong S$.

Ako je f epimorfizam prstena R na prsten S , onda se S naziva homomorfna (ili epimorfna) slika prstena R .

Ako postoji monomorfizam prstena R u prsten S , kažemo da se R može potopiti u S .

2.45. Ako je f homomorfizam prstena R u sebe, onda se f naziva endomorfizam, a ako je f izomorfizam prstena R u sebe onda se f naziva automorfizam.

2.46. Ako je f homomorfizam prstena R u prsten S , onda je jezgro $\text{Ker } f$ ideal prstena R a slika $\text{Im } f$ je potprsten prstena S .

2.47. Neka je R prsten i I ideal u R . Ako je $(R/I, +)$ aditivna faktor grupa i ako se na skupu R/I definiše množenje sa

$$(a + I) \cdot (b + J) = ab + I,$$

onda je $(R/I, +, \cdot)$ prsten koji se naziva faktor prsten prstena R po idealu I .

2.48. Ako je R prsten, a I ideal u R , onda faktor prsten $(R/I, +, \cdot)$

(i) je komutativan ako je R komutativan,

(ii) ima jedinicu ako R ima jedinicu.

2.49. Neka je I ideal prstena R . Tada je preslikavanje $\pi : R \rightarrow R/I$ definisano sa $\pi : r \mapsto r + I$ epimorfizam prstena R na prsten R/I čije je jezgro I . π se naziva prirodni epimorfizam (ili prirodni homomorfizam) prstena R na faktor prsten R/I .

2.50. (Prva teorema o izomorfizmu prstena) Ako je $f : R \rightarrow S$ homomorfizam prstena R u prsten S onda je

$$R/\text{Ker } f \cong \text{Im } f.$$

2.51. (Druga teorema o izomorfizmu prstena) Neka su I i J ideali prstena R . Tada je

$$(I + J)/J \cong I/(I \cap J).$$

2.52. (Treća teorema o izomorfizmu prstena) Neka su I i J ideali prstena R i neka je $I \subseteq J$. Tada je J/I ideal u R/I i

$$(R/I)/(J/I) \cong R/J.$$

2.53. Neka je I ideal prstena R . Tada je svaki ideal faktor prstena R/I oblika J/I , gde je J ideal prstena R koji sadrži I . Funkcija f koja preslikava skup svih ideala prstena R koji sadrže I na skup svih ideala prstena R/I , definisana sa

$$f : J \mapsto J/I,$$

je bijekcija.

2.54. U komutativnom prstenu sa jedinicom R ideal P je prost ideal ako i samo ako je R/P domen integriteta.

2.55. U komutativnom prstenu sa jedinicom R ideal M je maksimalan ideal ako i samo ako je R/M polje.

2.56. Ako je M maksimalan ideal komutativnog prstena sa jedinicom R , onda je M prost ideal prstena R .

2.57. Neprazan podskup S komutativnog prstena sa jedinicom se naziva multiplikativno zatvoren (ili zatvoren u odnosu na množenje) ako i samo ako važi:

- (i) $1 \in S$,
- (ii) $a, b \in S \Rightarrow ab \in S$.

2.58. Neka je S multiplikativno zatvoren podskup komutativnog prstena sa jedinicom R .

- (i) Relacija $\sim$ definisana na $R \times S$ sa

$$(r_1, s_1) \sim (r_2, s_2) \iff (\exists s \in S) s(r_1 s_2 - r_2 s_1) = 0,$$

je relacija ekvivalencije.

Skup $(R \times S)/\sim$ označavaćemo sa $S^{-1}R$, a klasu ekvivalencije elementa (r, s) sa r/s .

(ii) $S^{-1}R$ je komutativan prsten sa jedinicom, ako se sabiranje i množenje definišu na sledeći način:

$$\begin{aligned} (r_1/s_1) + (r_2/s_2) &= (r_1 s_2 + r_2 s_1)/s_1 s_2, \\ (r_1/s_1) \cdot (r_2/s_2) &= (r_1 r_2)/(s_1 s_2). \end{aligned}$$

Prsten $S^{-1}R$ se naziva prsten razlomaka prstena R sa imeniocima iz S .

- (iii) Preslikavanje $f : R \rightarrow S^{-1}R$ definisano sa

$$f(r) = r/1$$

je monomorfizam R u $S^{-1}R$, tj. R se može potopiti u $S^{-1}R$.

2.59. Neka je R domen integriteta i $S = R \setminus \{0\}$. $S^{-1}R$ je tada polje koje se naziva polje razlomaka domena R .

U specijalnom slučaju, kada je R prsten celih brojeva $\mathbb{Z}$, polje razlomaka prstena $\mathbb{Z}$ je polje racionalnih brojeva $\mathbb{Q}$.

2.60. Neka je R prsten. Beskonačan niz $(a_0, a_1, \dots)$ elemenata iz R , među kojima je samo konačan broj različit od nule, nazivamo polinom¹ nad R (ili polinom sa koeficijentima iz R). Skup svih takvih polinoma označavaćemo sa $R[x]$. Elemente $a_0, a_1, \dots$ nazivamo koeficijentima polinoma $(a_0, a_1, \dots)$. Polinom $(0, 0, \dots)$ (čiji su svi koeficijenti nule) nazivamo nula-polinom (ili nula).

2.61. Neka je R prsten. Ako se u $R[x]$ definiše sabiranje i množenje polinoma sa

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots),$$

$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (c_0, c_1, \dots),$$

gde je $c_k = \sum_{i=0}^k a_i b_{k-i}$, $k = 0, 1, \dots$, onda je $R[x]$ prsten koji se naziva prsten polinoma nad R (ili prsten polinoma sa koeficijentima iz R).

Ako je R komutativan prsten (ili prsten sa jedinicom ili prsten bez delitelja nule ili domen integriteta), onda odgovarajuće svojstvo ima i prsten polinoma $R[x]$.

Preslikavanje $f : R \rightarrow R[x]$ definisano sa

$$f(r) = (r, 0, 0, \dots)$$

je monomorfizam prstena R u prsten $R[x]$ (tj. prsten R se može izomorfno potopiti u prsten $R[x]$).

2.62. Neka je R prsten sa jedinicom i označimo sa x element

$$x = (0, 1, 0, 0, \dots) \in R[x].$$

Tada je

$$x = (0, 1, 0, 0, \dots),$$

$$x^2 = (0, 0, 1, 0, \dots),$$

.....

¹U 2.62 ćemo definisati polinom x , ali dotle čitalac koji se nije sretao sa ovakvom definicijom polinoma može da posmatra polinom $(a_0, a_1, \dots, a_n, 0, 0, \dots)$ kao formalni izraz $a_0 + a_1x + \dots + a_nx^n$.

$x^n = (0, 0, \dots, 0, 1, 0, \dots)$, gde je $(n+1)$ -va koordinata 1,

Ako se polinom $(r, 0, 0, \dots)$ označi sa r , onda je

$$r(a_0, a_1, \dots) = (r, 0, 0, \dots)(a_0, a_1, \dots) = (ra_0, ra_1, \dots),$$

i

$$rx^n = x^n r = (0, 0, \dots, 0, r, 0, \dots), \text{ gde je } r \text{ } (n+1)\text{-va koordinata.}$$

Tada se svaki polinom $f = (a_0, a_1, \dots, a_n, 0, 0, \dots)$ može napisati u obliku

$$f = a_0 + a_1x + \dots + a_nx^n.$$

Kada polinom f pišemo u ovom obliku, umesto f pisaćemo i $f(x)$.

2.63. Ako je $f = (a_0, a_1, \dots)$ nenula polinom, onda se nenegativan ceo broj n takav da je $a_n \neq 0$ i $a_k = 0$ za svako $k > n$, naziva stepen polinoma f i označava se $\deg f$. a_n se naziva vodeći koeficijent polinoma f , a ako je $a_n = 1$ polinom se naziva normalizovan. a_0 nazivamo konstantni (ili slobodan) član polinoma f . Stepen nula polinoma nije definisan. Polinom stepena 0 nazivamo konstanta.

2.64. Ako je R prsten, a $S = R[x]$, onda se prsten $S[y]$ označava sa $R[x, y]$.

Sa $R[x_1, \dots, x_n]$ označavamo prsten $S[x_n]$, gde je

$$S = R[x_1, \dots, x_{n-1}], \quad n \geq 2.$$

2.65. Polinom $f \in F[x_1, x_2, \dots, x_n]$, gde je F polje, se naziva simetrični polinom ako i samo ako je za svaku permutaciju $p \in S_n$

$$f(x_1, x_2, \dots, x_n) = f(x_{p(1)}, x_{p(2)}, \dots, x_{p(n)}).$$

2.66. Elementarni simetrični polinomi $\sigma_i \in F[x_1, x_2, \dots, x_n]$, $i = 1, 2, \dots, n$, gde je F polje, su polinomi:

$$\sigma_1 = x_1 + x_2 + \dots + x_n = \sum_{i=1}^n x_i,$$

$$\begin{aligned} \sigma_2 &= x_1x_2 + x_1x_3 + \dots + x_1x_n + x_2x_3 + \dots + x_2x_n + \dots + x_{n-1}x_n = \\ &= \sum_{1 \leq i < j \leq n} x_i x_j, \end{aligned}$$

$$\sigma_3 = \sum_{1 \leq i < j < k \leq n} x_i x_j x_k,$$

.....

$$\sigma_n = x_1 x_2 \dots x_n.$$

2.67. Polinom $f \in R[x]$, gde je R komutativan prsten sa jedinicom, se naziva nesvodljiv nad R ako i samo ako je f nesvodljiv element prstena $R[x]$ (v. 2.23).

Ako je F polje, onda je polinom $f(x) \in F[x]$, $\deg f(x) \geq 1$, nesvodljiv nad F ako i samo ako iz $h(x) \mid f(x)$ sledi da je $h(x) = c$ ili $h(x) = cf(x)$, gde je c konstanta (tj. $f(x)$ je nesvodljiv nad F ako i samo ako $f(x)$ nije jednak proizvodu dva polinoma pozitivnog stepena sa koeficijentima iz F).

2.68. (Algoritam deljenja) Neka je R prsten sa jedinicom, $f, h \in R[x]$ nenula polinomi takvi da je vodeći koeficijent polinoma h invertibilan element u R . Tada postoje jedinstveni polinomi $q, r \in R[x]$ takvi da je

$$f = qh + r,$$

gde je $\deg r < \deg h$ ili je r nula.

2.69. Neka je R prsten sa jedinicom i $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$. Tada za svako $c \in R$ postoji jedinstven polinom $q(x) \in R[x]$ takav da je

$$f(x) = q(x)(x - c) + f(c).$$

2.70. Ako je R domen integriteta sa jednoznačnom faktORIZACIJOM, tada je i prsten polinoma $R[x]$ domen integriteta sa jednoznačnom faktORIZACIJOM.

2.71. (Ajzenštajnov (Eisenstein) kriterijum nesvodljivosti) Neka je R domen integriteta sa jednoznačnom faktORIZACIJOM, F polje razlomaka domena R , $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$ a p nesvodljiv element prstena R . Ako važi

- (i) p nije delitelj a_n ,
- (ii) p je delitelj $a_0, a_1, \dots, a_{n-1}$,
- (iii) p^2 nije delitelj a_0 ,

onda je $f(x)$ nesvodljiv nad F .

U specijalnom slučaju, ako je $R = \mathbb{Z}$, nesvodljiv element p je prost broj i ako je $f(x)$ polinom sa celim koeficijentima takav da važi (i), (ii) i (iii), onda je polinom $f(x)$ nesvodljiv nad poljem $\mathbb{Q}$.

2.72. Neka je R potprsten komutativnog prstena S i

$$f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x].$$

Reći ćemo da je element $c \in S$ nula (ili koren) polinoma $f(x)$ (ili da je rešenje jednačine $f(x) = 0$) ako i samo ako je

$$f(c) = a_0 + a_1c + \dots + a_nc^n = 0.$$

2.73. Neka je R komutativan prsten sa jedinicom i $f(x) \in R[x]$. Element $c \in R$ je nula polinoma $f(x)$ ako i samo ako postoji polinom $g(x) \in R[x]$ takav da je

$$f(x) = (x - c)g(x).$$

2.74. Neka je R domen integriteta koji je sadržan u domenu integriteta S i neka je $f \in R[x]$ polinom stepena n . Tada f ima najviše n različitih korena u S .

2.75. Neka je R domen integriteta i $f(x) \in R[x]$. Ako je $c \in R$ koren polinoma $f(x)$, onda postoji najveći nenegativan ceo broj m takav da je

$$f(x) = (x - c)^m g(x),$$

gde je $g(x) \in R[x]$, $g(c) \neq 0$. Pri tom je $0 < m \leq \deg f(x)$.

Nenegativan ceo broj m nazivamo višestrukost korena c . Ako je $m = 1$, onda se c naziva prost (ili jednostruki) koren jednačine $f(x) = 0$, a ako je $m > 1$ c je višestruki koren.

2.76. Neka je R domen integriteta sa jedinstvenom faktORIZACIJOM čije je polje razlomaka F , $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$ i neka je $u = \frac{c}{d} \in F$, pri čemu su c i d uzajamno prosti. Ako je u nula polinoma $f(x)$, onda je c delitelj a_0 , a d delitelj a_n .

2.77. Neka je R domen integriteta i

$$f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x].$$

Sa $f'(x)$ označićemo polinom

$$f'(x) = a_1 + 2a_2x + 3a_3x^2 + \dots + na_nx^{n-1}$$

i nazivamo ga izvod (formalni) polinoma $f(x)$.

2.78. Neka je R domen integriteta. Tada za svako $f, g \in R[x]$ i $c \in R$ važi:

$$(i) (f + g)' = f' + g',$$

$$(ii) (cf)' = cf',$$

$$(iii) (fg)' = f'g + fg'.$$

2.79. Neka je R domen integriteta koji je sadržan u domenu integriteta S , $f \in R[x]$ i $c \in S$.

(i) c je višestruki koren polinoma f ako i samo ako je $f(c) = f'(c) = 0$.

(ii) Ako je R polje i polinom f relativno prost sa f' , onda f nema višestruke korene u S .

2.80. Neka su $x_1, x_2, \dots, x_n$ koreni polinoma $f(x) = a_0 + a_1x + \dots + a_nx^n \in F[x]$, gde je F polje. Tada je

$$\sigma_i = (-1)^i a_{n-i}/a_n, \quad i = 1, 2, \dots, n,$$

gde su σ_i elementarni simetrični polinomi (definicija 2.66).

2.81. Neka je $p(x_1, x_2, \dots, x_n)$ simetrični polinom sa koeficijentima iz polja F . Tada postoji jedinstveni polinom $g(\sigma_1, \sigma_2, \dots, \sigma_n)$ sa koeficijentima iz F , takav da je

$$p(x_1, x_2, \dots, x_n) = g(\sigma_1, \sigma_2, \dots, \sigma_n).$$

2.82. Simetrični polinomi $s_k \in F[x_1, x_2, \dots, x_n]$, $k \in \mathbb{N}$, gde je F polje, definisani sa

$$s_k = x_1^k + x_2^k + \dots + x_n^k, \quad k \in \mathbb{N},$$

se nazivaju Njutnove (Newton) sume.

2.2 Primeri i aksiomatika

365. Ispitati da li sledeći skupovi čine prstene u odnosu na odgovarajuće operacije:

$$a) (\mathbb{Z}, +, \cdot),$$

$$b) (\{2k \mid k \in \mathbb{Z}\}, +, \cdot),$$

c) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$,

d) $(\mathbb{Z}_m, +, \cdot)$.

Rezultat.

a) Komutativan prsten s jedinicom,

b) komutativan prsten bez jedinice,

c) komutativni prsteni s jedinicom,

d) komutativan prsten s jedinicom (v. zadatak 12).

366. Ispitati da li sledeći skupovi čine prstene u odnosu na odgovarajuće operacije:

a) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ u odnosu na uobičajeno sabiranje i množenje racionalnih brojeva.

b) $\{a + bi \mid a, b \in \mathbb{Z}, i^2 = -1\}$ (Gausovi celi brojevi) u odnosu na sabiranje i množenje kompleksnih brojeva.

c) $\{(a, b) \mid a, b \in \mathbb{Z}\}$ u odnosu na operacije $+$ i $\cdot$ definisane sa:

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc).$$

d) Skup svih vektora trodimenzionalnog Euklidovog prostora u odnosu na sabiranje vektora i vektorsko množenje.

Rešenje. a), b), c) Komutativni prsteni sa jedinicom.

d) Ne, jer vektorsko množenje nije asocijativno.

367. Neka je S neprazan skup, $\mathcal{P}(S)$ skup svih podskupova skupa S . Dokazati da je $(\mathcal{P}(S), +, \cdot)$ Bulov prsten ako su $+$ i $\cdot$ definisani sa

$$A + B = (A \setminus B) \cup (B \setminus A),$$

$$A \cdot B = A \cap B.$$

Uputstvo. Koristiti zadatak 38.

368. Dokazati da skup svih matrica formata $n \times n$ sa realnim (kompleksnim) elementima u odnosu na sabiranje i množenje matrica čini nekomutativan prsten sa jedinicom ($n \geq 2$).

369. Neka je $R = \{a, b, c, d\}$ a binarne operacije $+$ i $\cdot$ definisane tabli-

cama

$+$	a	b	c	d		$\cdot$	a	b	c	d
a	a	b	c	d		a	a	a	a	a
b	b	a	d	c	,	b	a	b	c	d
c	c	d	a	b		c	a	a	a	a
d	d	c	b	a		d	a	b	c	d

Dokazati da je $(R, +, \cdot)$ prsten.

Rešenje. $(R, +)$ je Abelova grupa jer je izomorfna sa Klajnovom četvornom grupom $(C_2 \times C_2)$.

Proverićemo da li je množenje asocijativno, tj. da li je za svako $x, y, z \in R$

$$x(yz) = (xy)x.$$

Ako je x jednako a ili c , onda je

$$x(yz) = a = (xy)z.$$

Ako je x jednako b ili d , onda je

$$x(yz) = yz = (xy)z,$$

što znači da je množenje asocijativno.

Na sličan način može se dokazati da važe oba distributivna zakona, pa je $(R, +, \cdot)$ prsten.

Iz tablice kojom je definisano množenje odmah se vidi da je prsten nekomutativan i da nema jedinicu.

370. Dat je skup $R = \{x, y, z, u\}$. Kompletirati tablice operacija $+$ i $\cdot$ tako da $(R, +, \cdot)$ bude prsten

$+$	x	y	z	u		$\cdot$	x	y	z	u
x	x	.	z	.		x	x	x	x	x
y	y	z	.	.	,	y	x	y	.	.
z	.	.	x	.		z	x	.	.	z
u	.	.	.	z		u	x	u	z	.

371. Ako je $(G, +)$ Abelova grupa, $|G| > 1$, i ako u G definišemo množenje sa

$$ab = 0, \quad \text{za svako } a, b \in G,$$

onda je $(G, +, \cdot)$ komutativan prsten bez jedinice. Dokazati.

PRIMEDBA. Prsten sa ovako definisanim množenjem naziva se nula-prsten.

372. Dokazati da je skup $\text{End}(G)$ svih endomorfizama Abelove grupe G , prsten u odnosu na operacije sabiranja, definisanog sa

$$f, g \in \text{End}(G), \quad (f + g)(a) = f(a) + g(a), \quad \text{za svako } a \in G,$$

i množenja, definisanog sa

$$(f \cdot g)(a) = f(g(a)), \quad \text{za svako } a \in G.$$

Rešenje. Neka su $f, g \in \text{End}(G)$. Tada je za svako $a, b \in G$

$$\begin{aligned} (f + g)(a + b) &= f(a + b) + g(a + b) = f(a) + f(b) + g(a) + g(b) = \\ &= f(a) + g(a) + f(b) + g(b) = (f + g)(a) + (f + g)(b), \end{aligned}$$

pa je preslikavanje $f + g$ takođe endomorfizam, tj. operacija sabiranja endomorfizama je unutrašnja. Iz asocijativnosti i komutativnosti sabiranja u G odmah sledi asocijativnost i komutativnost sabiranja u $\text{End}(G)$. Endomorfizam koji sve elemente grupe G preslikava u neutralni element te grupe je neutralni element za sabiranje u $\text{End}(G)$, za endomorfizam f suprotan element je endomorfizam $-f$ definisan sa:

$$(-f)(a) = -f(a), \quad \text{za svako } a \in G.$$

Prema tome, $(\text{End}(G), +)$ je Abelova grupa.

Da je proizvod dva endomorfizma endomorfizam dokazuje se slično kao što je to učinjeno za sabiranje.

Asocijativnost množenja u $\text{End}(G)$ je neposredna posledica asocijativnosti kompozicije preslikavanja, pa preostaje da se dokaže da važe zakoni distributivnosti.

$$\begin{aligned} (f(g + h))(a) &= f((g + h)(a)) = f(g(a) + h(a)) = f(g(a)) + f(h(a)) = \\ &= (fg)(a) + (fh)(a) = (fg + fh)(a) \end{aligned}$$

za svako $a \in G$ i svako $f, g, h \in \text{End}(G)$.

Slično se dokazuje da važi desna distributivnost, pa je $(\text{End}(G), +, \cdot)$ prsten.

Identičko preslikavanje grupe G je endomorfizam te grupe, taj endomorfizam je jedinica u prstenu $\text{End}(G)$, dakle, $\text{End}(G)$ je prsten sa jedinicom.

373. Odrediti prstene endomorfizma za:

- a) cikličku grupu reda n ,
- b) beskonačnu cikličku grupu,
- c) aditivnu grupu racionalnih brojeva.

Rezultat.

- a) $\text{End}(G) \cong (\mathbb{Z}_n, +, \cdot)$,
- b) $\text{End}(G) \cong (\mathbb{Z}, +, \cdot)$,
- c) $\text{End}(G) \cong (\mathbb{Q}, +, \cdot)$.

374. Ako se u prstenu sa jedinicom $(R, +, \cdot)$ definišu operacije $*$ i $\cdot$ sa

$$a * b = a + b - 1, \quad a \cdot b = a + b - ab,$$

dokazati da je $(R, *, \cdot)$ prsten izomorfan prstenu $(R, +, \cdot)$.

375. Neka je R prsten. Označimo sa R' skup svih beskonačnih nizova sa elementima iz R . U skupu R' definišimo operacije $+$ i $\cdot$ na sledeći način:

$$\begin{aligned} (a_0, a_1, \dots, a_k, \dots) + (b_1, b_1, \dots, b_k, \dots) &= \\ &= (a_0 + b_0, a_1 + b_1, \dots, a_k + b_k, \dots), \\ (a_0, a_1, \dots, a_k, \dots) \cdot (b_0, b_1, \dots, b_k, \dots) &= \\ &= (a_0 b_0, a_0 b_1 + a_1 b_0, \dots, a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0, \dots). \end{aligned}$$

Dokazati da je $(R', +, \cdot)$ prsten.

PRIMEDBA. Prsten polinoma $R[x]$ definisan u 2.60, 2.61 i 2.62 je potprsten prstena R' .

376. Neka je R prsten. Označimo sa $R[[x]]$ skup svih formalnih stepenih redova sa koeficijentima R , tj.

$$f \in R[[x]] \iff f = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots = \sum_{k=0}^{\infty} a_k x^k.$$

Neka su $f = \sum_{k=1}^{\infty} a_k x^k$ i $g = \sum_{k=0}^{\infty} b_k x^k$ elementi $R[[x]]$. $f = g$ ako i samo ako je $a_k = b_k$ za svako $k = 0, 1, 2, \dots$.

Na skupu $R[[x]]$ uvedimo operacije $+$ i $\cdot$ na sledeći način:

$$f + g = \sum_{k=0}^{\infty} (a_k + b_k)x^k,$$

$$f \cdot g = \sum_{k=0}^{\infty} c_k x^k, \quad \text{gde je} \quad c_k = \sum_{l=0}^k a_l b_{k-l}.$$

Dokazati da je $(R[[x]], +, \cdot)$ prsten.

377. Dokazati da je prsten $(R', +, \cdot)$ iz zadatka 375 izomorfan prstenu $(R[[x]], +, \cdot)$ iz zadatka 376.

378. Neka je R prsten. Označimo sa $R\langle x \rangle$ skup svih proširenih formalnih stepenih redova sa koeficijentima iz R ,

$$f \in R\langle x \rangle \iff f = a_{-k}x^{-k} + a_{-k+1}x^{-k+1} + \dots + a_{-1}x^{-1} + a_0 + a_1x + \dots + a_nx^n + \dots,$$

(pri čemu k zavisi od f). Uvedimo skraćenu oznaku $f = \sum_{n=-\infty}^{\infty} a_n x^n$, gde se podrazumeva da je samo konačno mnogo koeficijenata sa negativnim indeksima različito od nule.

Ako su

$$f = \sum_{n=-\infty}^{\infty} a_n x^n, \quad g = \sum_{n=-\infty}^{\infty} b_n x^n \in R\langle x \rangle,$$

onda je

$$f = g \iff a_n = b_n \quad \text{za svako} \quad n \in \mathbb{Z}.$$

U skupu $R\langle x \rangle$ uvedimo operacije $+$ i $\cdot$ na sledeći način:

$$f + g = \sum_{n=-\infty}^{\infty} (a_n + b_n)x^n,$$

$$f \cdot g = \sum_{n=-\infty}^{\infty} c_n x^n, \quad \text{gde je} \quad c_n = \sum_{i=-\infty}^n a_i b_{n-i}.$$

Dokazati da je $(R\langle x \rangle, +, \cdot)$ prsten.

379. Ako je R komutativan prsten, tada su i prsteni $R[[x]]$ iz zadatka 376 i $R\langle x \rangle$ iz zadatka 378 komutativni prsteni. Dokazati.

380. Neka su R_1 i R_2 prsteni. U skupu $R_1 \times R_2$ definišemo operacije $+$ i $\cdot$ na sledeći način:

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2),$$

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2).$$

Dokazati da je $(R_1 \times R_2, +, \cdot)$ prsten.

PRIMEDBA. Prsten $R_1 \times R_2$ naziva se direktan proizvod prstena R_1 i R_2 . Analogno se definiše direktan proizvod bilo kog konačnog broja prstena.

381. Neka je $\{R_i \mid i \in \mathbb{N}\}$ familija prstena. Označimo sa $\prod_{i=1}^{\infty} R_i$ skup svih nizova $(a_1, a_2, \dots)$ takvih da je $a_i \in R_i$ za $i = 1, 2, \dots$. Na skupu $\prod_{i=1}^{\infty} R_i$ definišemo operacije $+$ i $\cdot$ na sledeći način:

$$(a_1, a_2, \dots) + (b_1, b_2, \dots) = (a_1 + b_1, a_2 + b_2, \dots),$$

$$(a_1, a_2, \dots) \cdot (b_1, b_2, \dots) = (a_1 b_1, a_2 b_2, \dots).$$

Dokazati da je $(\prod_{i=1}^{\infty} R_i, +, \cdot)$ prsten.

PRIMEDBA. Prsten $\prod_{i=1}^{\infty} R_i$ se naziva direktan proizvod prstena R_i , $i = 1, 2, \dots$.

382. Svako telo, svako polje i svaki Bulov prsten su fon Nojmanovi regularni prsteni. Dokazati.

383. Dokazati da su sledeći prsteni fon Nojmanovi regularni prsteni:

a) Bulov prsten.

b) Prsten matrica formata $n \times n$ nad poljem.

c) $\prod_{i=1}^{\infty} R_i$ (zadatak 381), gde je svaki od prstena R_i , $i = 1, 2, \dots$, fon Nojmanov regularan prsten.

Rešenje. a) U Bulovom prstenu za svaki element x važi

$$x^3 = x^2 x = x^2 = x,$$

pa je za $y = x$, $xyx = x$.

b) Dati prsten matrica je prsten sa jedinicom (jedinična matrica je jedinica prstena). Za svaku matricu A formata $n \times n$ ranga k postoje regularne matrice P i Q takve da je

$$PAQ = \begin{bmatrix} E_k & 0 \\ 0 & 0 \end{bmatrix},$$

gde je E_k jedinična matrica formata $k \times k$. Tada je

$$PAQPAQ = \begin{bmatrix} E_k & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} E_k & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} E_k & 0 \\ 0 & 0 \end{bmatrix} = PAQ,$$

pa pošto su P i Q regularne matrice, sledi da je

$$AQPA = A,$$

tj. za $B = QP$ je

$$ABA = A.$$

c) Neka je $x = (x_1, x_2, \dots) \in \prod_{i=1}^{\infty} R_i$. Za niz $y = (y_1, y_2, \dots) \in \prod_{i=1}^{\infty} R_i$ definisan sa $y_i = x'_i$, gde je $x_i x'_i x_i = x_i$, $i = 1, 2, \dots$, važi $xyx = x$.

384. Dokazati:

a) Prsten celih brojeva $\mathbb{Z}$ je Euklidov prsten (2.25) ako se ϕ definiše sa $\phi(x) = |x|$.

b) Prsten polinoma $F[x]$, gde je F polje, je Euklidov prsten ako se ϕ definiše sa $\phi(f(x)) = \deg f(x)$ (sa $\deg f(x)$ označavamo stepen polinoma $f(x)$).

c) Proizvoljno polje F je Euklidov prsten, ako se ϕ definiše sa $\phi(x) = 1$ za svako $x \neq 0$.

385. Neka je $R = \{a + bi \mid a, b \in \mathbb{Z}\}$ prsten Gausovih celih brojeva (zadatak 366 b). Dokazati da je R Euklidov prsten, ako se ϕ definiše sa $\phi : a + bi \mapsto a^2 + b^2$, $a, b \in \mathbb{Z}$.

Rešenje. Neposredno sledi da je $\phi(a + bi) \geq 1$ za $a + bi \neq 0$ i da je

$$\begin{aligned} \phi((a + bi)(c + di)) &= \phi(ac - bd + (ad + bc)i) = (ac - bd)^2 + (ad + bc)^2 = \\ &= (a^2 + b^2)(c^2 + d^2) = \phi(a + bi)\phi(c + di), \end{aligned}$$

pa sledi da je

$$\phi((a + bi)(c + di)) \geq \phi(a + bi),$$

tj. važi E1 iz 2.25.

Neka su $z_1, z_2 \in R$, $z_2 \neq 0$. Neka je $z_1 z_2^{-1} = s_1 + s_2 i$, gde su s_1 i s_2 racionalni brojevi. Očigledno, postoje celi brojevi n_1 i n_2 takvi da je

$$|s_1 - n_1| \leq \frac{1}{2} \quad \text{i} \quad |s_2 - n_2| \leq \frac{1}{2}.$$

Tada je

$$z_1 = z_2(s_1 + s_2 i) = z_2(n_1 + n_2 i + (s_1 - n_1) + (s_2 - n_2)i) = z_2 q + r,$$

gde je $q = n_1 + n_2 i$, a $r = z_2(s_1 - n_1 + (s_2 - n_2)i)$. $r \in R$ jer je $r = z_1 - z_2 q$.

$$\begin{aligned} \phi(r) &= r\bar{r} = z_2 \bar{z}_2 (s_1 - n_1 + (s_2 - n_2)i) \overline{(s_1 - n_1 + (s_2 - n_2)i)} = \\ &= \phi(z_2) \left((s_1 - n_1)^2 + (s_2 - n_2)^2 \right) \leq \phi(z_2) \left(\frac{1}{4} + \frac{1}{4} \right) \leq \frac{1}{2} \phi(z_2) < \phi(z_2). \end{aligned}$$

Dakle, ili je $r = 0$ ili je $\phi(r) < \phi(z_2)$.

386. Neka je $(R, +, \cdot)$ algebarska struktura koja zadovoljava sve aksiome prstena izuzev komutativnosti sabiranja. Ako R ima desnu jedinicu, dokazati da je R prsten.

Rešenje. Ako je 1 desna jedinica, tada je

$$0 = b(1 + (-1)) = b1 + b(-1) = b + b(-1),$$

pa je

$$-b = b(-1).$$

Dalje je

$$0 = (-b) + (-a) + a + b = b(-1) + a(-1) + a + b = (b + a)(-1) + a + b,$$

tj.

$$a + b = -((b + a)(-1)).$$

Kako je

$$(b + a) + (b + a)(-1) = (b + a)1 + (b + a)(-1) = (b + a)(1 + (-1)) = 0,$$

tj.

$$b + a = -((b + a)(-1)),$$

mora biti

$$a + b = b + a.$$

387. Ako prsten R ima tačno jednu levu jedinicu 1_l , dokazati da je onda 1_l jedinica (dvostrana).

Rešenje. Kako je za svako $a, b \in R$

$$(a1_l - a + 1_l)b = a(1_lb) - ab + 1_lb = b,$$

s obzirom da postoji samo jedna leva jedinica mora biti za svako $a \in R$

$$a1_l - a + 1_l = 1_l,$$

pa je

$$a1_l = a,$$

tj. 1_l je i desna jedinica.

388. Neka je R komutativan prsten bez delitelja nule u kome važi E1 i E2 iz 2.25. Dokazati da je R domen integriteta, tj. da R ima jedinicu.

Rešenje. Neka je a element prstena R , takav da je $\phi(a)$ najmanji prirodan broj skupa nenegativnih celih brojeva $\{\phi(x) \mid x \in R \wedge x \neq 0\}$. Tada je za proizvoljno $b \in R$, $b = aq + r$, gde je $r = 0$ ili je $\phi(r) < \phi(a)$. Pošto ne može da bude $\phi(r) < \phi(a)$, jer je $\phi(a)$ minimum, mora biti $r = 0$. Ako uzmemo da je $b = a$, tada postoji $e \in R$ takvo da je $a = ea = ae$. Neka je b proizvoljan element iz R . Tada je $b = qa$ za neko $q \in R$, pa je

$$be = qae = qa = b = eb,$$

tj. e je jedinica u prstenu R .

389. Dokazati da se u definiciji 2.25 Euklidovog prstena aksioma E2 može zameniti aksiomom

E2'. Za svako $a, b \in R$, ako je $\phi(a) \geq \phi(b)$, onda postoji $c \in R$ takvo da je

$$\phi(a - bc) < \phi(a) \quad \text{ili} \quad a = bc.$$

2.3 Osnovne osobine

390. Dokazati da u prstenu R za svako $a, b \in R$ važi:

$$1) a0 = 0a = 0,$$

$$2) -(-a) = a,$$

$$3) -(a + b) = (-a) + (-b) = -a - b,$$

$$4) (-a)b = a(-b) = -(ab),$$

$$5) (-a)(-b) = ab,$$

$$6) n(ab) = (na)b = a(nb), \text{ za svaki ceo broj } n.$$

Rešenje. 1) $a0 = a(0 + 0) = a0 + a0$, pa sledi da je $a0 = 0$. Slično se dokazuje da je $0a = 0$.

2) i 3) važe u svakoj Abelovoj grupi.

4) $0 = a0 = a(b + (-b)) = ab + a(-b)$, pa sledi da je $a(-b) = -(ab)$. Analogno se dobija $(-a)b = -(ab)$.

U daljem ćemo $-(ab)$ označavati sa $-ab$.

5) Prema prethodnom je

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

6) Po definiciji je $0a = 0$ (ovde je prva nula ceo broj, a druga neutralni element prstena), pa zato za $n = 0$ tvrđenje važi. Pretpostavimo da je

$$k(ab) = (ka)b, \quad k \geq 0.$$

Tada je

$$(k + 1)(ab) = k(ab) + ab = (ka)b + ab = (ka + a)b = ((k + 1)a)b,$$

pa je $n(ab) = (na)b$, za svaki nenegativan ceo broj n . Kako je po definiciji

$$n(ab) = (-n)(-(ab)), \quad \text{za } n < 0,$$

iz prethodnog i 4) sledi da je

$$n(ab) = (na)b,$$

za svaki ceo broj n .

Analogno je i $n(ab) = a(nb)$, za svako $n \in \mathbb{Z}$.

391. Ako neki element prstena sa jedinicom ima multiplikativni inverzni element, onda je taj inverzni element jedinstven. Dokazati.

392. Konačan prsten u kome postoji element a koji nije levi delitelj nule i element b koji nije desni delitelj nule je prsten sa jedinicom. Dokazati.

Rešenje. Preslikavanje $x \mapsto ax$ je injektivno (jer iz $ax = ay$, $x \neq y$, sledi $a(x - y) = 0$, a to protivreči pretpostavci da a nije levi delitelj nule), a kako je prsten konačan to preslikavanje je surjektivno, dakle, ono je bijekcija. Slično, i preslikavanje $x \mapsto xb$ je bijekcija prstena na sebe.

Prema tome, postoje elementi e_1 i e_2 takvi da je $a = ae_1$ i $b = e_2b$. Za svaki element x prstena je

$$ax = ae_1x,$$

pa je

$$a(x - e_1x) = 0,$$

odakle je $x = e_1x$. Slično, iz

$$xb = xe_2b,$$

sledi

$$xe_2 = x.$$

Iz ovih jednakosti za $x = e_1$ i $x = e_2$ dobijamo

$$e_1 = e_1e_2 = e_2,$$

pa je e_1 jedinica prstena.

PRIMEDBA. Primerom pokazati da za beskonačne prstene ovaj stav ne važi.

393. U prstenu R za svako $a, b, c \in R$, $a \neq 0$, važi

$$ab = ac \Rightarrow b = c \quad \text{i} \quad ba = ca \Rightarrow b = c,$$

(tj. važe zakoni kancelacije za množenje elementom različitim od nule) ako i samo ako prsten nema delitelje nule.

394. Neka je R konačan prsten u kome postoji bar jedan element koji nije delitelj nule. Dokazati:

a) R je prsten sa jedinicom.

b) Ako $b \in R$ nema multiplikativni inverzni element, tada je b delitelj nule.

Rešenje. a) Neka je a element koji nije delitelj nule. Tada postoje prirodni brojevi m i n takvi da je $a^m = a^n$, jer je R konačan skup. Neka je $m < n$. Tada je $a^{m-1}(a - a^{n-m+1}) = 0$, pa je $a = a^{n-m+1}$.

Neka je b proizvoljan element iz R . Tada je $ba = ba^{n-m+1}$, što je ekvivalentno sa $(b - ba^{n-m})a = 0$, pa je $b = ba^{n-m}$ jer bi inače a bio delitelj nule.

Analogno se dobija $b = a^{n-m}b$, pa je a^{n-m} jedinica prstena R .

b) Iz a) sledi da svaki element a koji nije delitelj nule ima inverzni element $a^{-1} = a^{n-m-1}$. Ako b nema inverzni element, onda b mora biti delitelj nule.

395. Neka je R prsten sa p elemenata, gde je p prost broj. Ako R sadrži bar jedan proizvod različit od 0, dokazati da je onda prsten R izomorfan prstenu $(\mathbb{Z}_p, +, \cdot)$.

Rešenje. S obzirom da je p prost broj, aditivna grupa $(R, +)$ mora biti ciklička (zadatak 139). Ako je a jedan generator te grupe, onda je

$$R = \{a, 2a, \dots, pa = 0\}.$$

Neka je

$$a^2 = ka, \quad 1 \leq k \leq p.$$

Ukoliko je k jednako p svi proizvodi u prstenu R su jednaki 0, što je protivrečnost, dakle, $k \neq p$. k i p su relativno prosti brojevi, pa postoje celi brojevi l i m tako da je $lk + mp = 1$. Preslikavanje $f : \mathbb{Z}_p \rightarrow R$ definisano sa $f(\bar{i}) = ila$, je izomorfizam prstena $\mathbb{Z}_p$ na prsten R . Zaista, f je injektivno preslikavanje (jer iz $ila = jla$, $\bar{i} \neq \bar{j}$, sledi $(i - j)la = 0$, tj. $(i - j)l \equiv 0 \pmod{p}$, što je kontradikcija), a kako je R konačan skup preslikavanje f je surjektivno, dakle, f je bijekcija. Takođe, za svako $\bar{i}, \bar{j} \in \mathbb{Z}_p$ važi

$$\begin{aligned} f(\bar{i}) + f(\bar{j}) &= ila + jla = (i + j)la = f(\bar{i} + \bar{j}), \\ f(\bar{i}) \cdot f(\bar{j}) &= (ila) \cdot (jla) = ijl^2a^2 = ijl^2ka = \\ &= ijl(1 - mp)a = ijl a = f(\bar{i} \cdot \bar{j}), \end{aligned}$$

pa je f izomorfizam.

PRIMEDBA. Prema tome, svaki prsten sa p elemenata, gde je p prost broj, je izomorfan nula-prstenu (zadatak 371) čija je aditivna grupa ciklička ili prstenu $(\mathbb{Z}_p, +, \cdot)$ (koji je polje).

396. Koliko načina postoji da se na skupu $S = \{0, 1, 2, 3\}$ definiše operacija množenja $\cdot$ tako da $(S, +, \cdot)$ postane prsten, ako je $+$ sabiranje po modulu 4?

Uputstvo. Ako je u nekom prstenu $(R, +, \cdot)$ $(R, +)$ ciklička grupa, i ako je a generator te grupe, onda je množenje potpuno određeno ako se zna a^2 . Zaista, za svako $x, y \in R$ postoje $m, n \in \mathbb{Z}$ tako da je $x = ma$, $y = na$, pa je

$$xy = (ma)(na) = mna^2.$$

Ako sada pođemo od neke cikličke grupe $(C, +)$ sa generatorom a , za a^2 uzmemo neki element te grupe i definišemo množenje gornjom jednakosću, onda se lako proverava da je tako definisano množenje asocijativno i distributivno u odnosu na sabiranje, tj. $(C, +, \cdot)$ je prsten.

Rezultat.

$\cdot_1$	0	1	2	3		$\cdot_2$	0	1	2	3
0	0	0	0	0		0	0	0	0	
1	0	0	0	0	,	1	0	1	2	3
2	0	0	0	0		2	0	2	0	2
3	0	0	0	0		3	0	3	2	1
$\cdot_3$	0	1	2	3		$\cdot_4$	0	1	2	3
0	0	0	0	0		0	0	0	0	
1	0	2	0	2	,	1	0	3	2	1
2	0	0	0	0		2	0	2	0	2
3	0	2	0	2		3	0	1	2	3

397. Odrediti broj neizomorfnih prstena čija je aditivna grupa ciklička grupa reda m .

Rešenje. Neka je R prsten reda m čija je aditivna grupa ciklička grupa reda m i neka je x generator te grupe. R je tada komutativan prsten.

S obzirom na ono što je rečeno u uputstvu za rešavanje prethodnog zadatka, množenje u prstenu R je potpuno određeno ako je poznato x^2 . x^2 može biti svaki od elemenata prstena R , dakle, ne može postojati više od m

neizomorfni prstena čija je aditivna grupa ciklička grupa reda m . Ispitaćemo sada koji od tih prstena su izomorfni.

Neka je u prstenu R $x^2 = nx$, $n \in \mathbb{N}$, i neka je S neki drugi prsten čija je aditivna grupa ciklička grupa reda m sa generatorom y i $y^2 = ry$, $r \in \mathbb{N}$. Razmotrićemo pod kojim uslovima su prsteni R i S izomorfni.

Da bi preslikavanje $f : R \rightarrow S$ bilo izomorfizam potrebno je da se generator aditivne grupe preslikava u generator aditivne grupe, dakle, $f(x) = ky$, za neko $k \in \mathbb{N}$, gde je k uzajamno prost sa m (1.23). Ako je f izomorfizam i multiplikativnih polugrupa, onda je

$$nky = nf(x) = f(nx) = f(x^2) = f(x)^2 = (ky)^2 = k^2y^2 = k^2ry,$$

tj. $n \equiv kr \pmod{m}$. Nije teško proveriti da su ova dva uslova (postoji k takvo da su k i m uzajamno prosti i $n \equiv kr \pmod{m}$) ne samo potrebni nego i dovoljni da preslikavanje f bude izomorfizam prstena R i S . Ako su zadovoljena oba ova dva uslova, onda neposredno sledi da je najveći zajednički delitelj za n i m jednak najvećem zajedničkom delitelju za r i m .

Obrnuto, neka je $\text{nzd}(n, m) = \text{nzd}(r, m)$. Tada je $\frac{r}{\text{nzd}(r, m)}$ uzajamno prost sa $\frac{m}{\text{nzd}(r, m)}$, pa postoje $s, t \in \mathbb{Z}$ tako da je

$$s \frac{r}{\text{nzd}(r, m)} + t \frac{m}{\text{nzd}(r, m)} = 1.$$

Množeći gornju jednakost sa n dobijamo

$$s \frac{n}{\text{nzd}(r, m)} r + t \frac{n}{\text{nzd}(r, m)} m = n,$$

tj.

$$kr \equiv n \pmod{m},$$

pri čemu smo sa k označili broj $s \frac{n}{\text{nzd}(r, m)} = s \frac{n}{\text{nzd}(n, m)}$ koji je relativno prost sa m , jer bi inače bilo $\text{nzd}\left(\frac{n}{\text{nzd}(n, m)}, \frac{m}{\text{nzd}(n, m)}\right) \neq 1$.

Dakle, $R \cong S$ ako i samo ako je $\text{nzd}(n, m) = \text{nzd}(r, m) = l$, pri čemu je l delitelj broja m . Prema tome, postoji onoliko neizomorfni prstena koliko broj m ima različitih delitelja. Ako je $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, gde su p_i $i = 1, \dots, k$, različiti prosti brojevi, onda postoji $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$ različitih neizomorfni prstena čija je aditivna grupa ciklička grupa reda m .

398. Neka je R konačan prsten reda $n > 1$ pri čemu je n proizvod različitih prostih brojeva. Dokazati da je R komutativan prsten.

Rešenje. Ako je $n = p_1 p_2 \dots p_k$, gde su $p_1, p_2, \dots, p_k$ različiti prosti brojevi, onda je Abelova grupa $(R, +)$ reda n ciklička (zadatak 153).

Neka je x generator cikličke grupe $(R, +)$. Tada za svaki element $a \in R$ postoji $m_a \in \mathbb{N}$ takvo da je $a = m_a x$. Neka je $b = m_b x$, onda je

$$ab = (m_a x)(m_b x) = (m_a m_b) x^2 = (m_b m_a) x^2 = (m_b x)(m_a x) = ba,$$

tj. prsten R je komutativan.

PRIMEDBA. U vezi sa zadacima 398, 399 i 400 videti D. B. Erickson, *Orders for finite noncommutative rings*, Amer. Math. Monthly, 73 (1966), 376-377.

399. Dokazati da za svaki prost broj p postoji nekomutativan prsten reda p^2 .

Uputstvo. Neka je $R = \{(x, y) \mid x, y = 0, 1, \dots, p-1\}$. Sabiranje u R definišemo sa $(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$, gde je sabiranje komponentata po modulu p . Množenje definišemo sa $(x_1, x_2) * (y_1, y_2) = (x_1(y_1 + y_2), x_2(y_1 + y_2))$, gde je sabiranje i množenje komponentata po modulu p . Dokazati da je $(R, +, *)$ nekomutativan prsten reda p^2 .

400. Neka je m prirodan broj, $m > 1$. Dokazati da postoji nekomutativan prsten R reda m ako i samo ako je m deljivo kvadratom celog broja ($\neq 1$).

Uputstvo. Neka je $M = p^2 n$, gde je p prost broj. Posmatrati prsten $R_1 \times R_2$ gde je R_1 prsten iz prethodnog zadatka, a $R_2 \cong (\mathbb{Z}_n, +, \cdot)$ i koristiti zadatke 398 i 399.

401. Naći sve neizomorfne prstene koji imaju najviše 7 elemenata.

Delimičan odgovor.

red	1	2	3	4	5	6	7
broj prstena	1	2	2	11	2	4	2

Ovo je detaljno razmotreno u C. R. Fletcher, *Rings of small order*, Math. Gazette, 64 (1980), 9-22.

402. Ako su m i n uzajamno prosti brojevi veći od jedan, dokazati da $\mathbb{Z}_{mn}$ sadrži bar dva idempotentna elementa različita od $\bar{0}$ i $\bar{1}$.

Rešenje. Ako su m i n uzajamno prosti brojevi, onda postoje celi brojevi r i s takvi da je $rm + sn = 1$. Ako ovu jednakost pomnožimo sa rm , dobijamo $(rm)^2 + rsmn = rm$, pa je

$$(rm)^2 \equiv rm \pmod{mn},$$

tj. $(\overline{rm})^2 = \overline{rm}$, i $\overline{rm}$ je idempotent različit od $\overline{0}$ i $\overline{1}$.

Ako bi bilo $rm \equiv 0 \pmod{mn}$, tada bi zbog pretpostavke o m i n , r bilo deljivo sa n , recimo, $r = kn$, $k \in \mathbb{Z}$, pa bi bilo

$$1 = rm + sn = knm + sn = n(km + s),$$

što je protivrečnost.

Analogno se dobija protivrečnost ako se pretpostavi da je $rm \equiv 1 \pmod{mn}$.

Na sličan način se pokazuje da je $\overline{sn}$ takođe idempotent različit od $\overline{0}$ i $\overline{1}$. Iz $rm + sn = 1$ neposredno sledi da je $\overline{sn} \neq \overline{rm}$.

403. Neka je R prsten karakteristike $k > 0$, gde k nije stepen prostog broja. Dokazati da u R postoje bar dva idempotenta e_1 i e_2 različita od nule i jedinice.

Uputstvo. Ako k nije stepen prostog broja tada, postoje dva uzajamno prosta broja s i t takva da je $k = st$. Iskoristiti da je $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ potprsten izomorfni $\mathbb{Z}_k$ i prethodni zadatak.

404. Za koje $n \in \mathbb{N}$ prsten $\mathbb{Z}_n$ nema idempotenta različitih od $\overline{0}$ i $\overline{1}$?

Rezultat. $n = p^k$, gde je p prost broj.

405. Za koje $n \in \mathbb{N}$ prsten $\mathbb{Z}_n$ nema nilpotentnih elemenata različitih od nule?

Rezultat. $n = p_1 p_2 \dots p_k$, gde su p_i različiti prosti brojevi.

406. Dokazati da je neprazan podskup S prstena $(R, +, \cdot)$ potprsten ako i samo ako za svako $a, b \in S$

$$a - b \in S \quad \text{i} \quad a \cdot b \in S.$$

407. Dokazati da je u prstenu $(R, +, \cdot)$ podskup

$$\mathcal{C}(R) = \{x \in R \mid xa = ax, \text{ za svako } a \in R\}$$

potprsten ($\mathcal{C}(R)$ se naziva centar prstena R).

408. Označimo sa $\sum_{i=1}^{\infty} R_i$ podskup onih nizova iz prstena $\prod_{i=1}^{\infty} R_i$ definisanog u zadatku 381 koji imaju samo konačan broj komponenta različitih od nule. Dokazati.

a) $\left(\sum_{i=1}^{\infty} R_i, +, \cdot\right)$ je potprsten prstena $\left(\prod_{i=1}^{\infty} R_i, +, \cdot\right)$.

b) Svaki element prstena $\sum_{i=1}^{\infty} R_i$ različit od nule je delitelj nule.

c) $\sum_{i=1}^{\infty} R_i$ nema jedinicu.

Uputstvo. b) Neka je $f = (f_1, f_2, \dots) \in \sum_{i=1}^{\infty} R_i$. Tada postoji prirodan broj n takav da je $f_k = 0$, za $k > n$. Neka je $g = (g_1, g_2, \dots) \in \sum_{i=1}^{\infty} R_i$ takav da je $g_{n+1} \neq 0$ i $g_k = 0$, za $k \neq n+1$.

Proveriti da je $f \cdot g = 0$.

409. Neka je $\prod_{i=1}^{\infty} R_i$ prsten definisan u zadatku 381, pri čemu je $R_i \cong \mathbb{R}$ za $i = 1, 2, \dots$. Posmatrajmo podskup S skupa $\prod_{i=1}^{\infty} \mathbb{R}$ onih nizova $x = (x_1, x_2, \dots)$ za koje postoji prirodan broj p takav da je $|x_i| < p$ za $i = 1, 2, \dots$ (p zavisi od x) i podskup T onih nizova $y = (y_1, y_2, \dots)$ za koje je $\lim_{n \rightarrow \infty} y_n = 0$. Dokazati:

a) S je potprsten prstena $\prod_{i=1}^{\infty} \mathbb{R}$, a T potprsten prstena S .

b) Svaki od prstena $\prod_{i=1}^{\infty} \mathbb{R}$, S , T sadrži beskonačno mnogo potprstena izomorfnih samom sebi.

c) $\sum_{i=1}^{\infty} \mathbb{R}$ (definisan u prethodnom zadatku) je potprsten i prstena S i prstena T .

410. Neka je R prsten matrica formata $n \times n$ sa elementima iz polja. Dokazati da je skup gornjih (donjih) trougaonih matrica potprsten prstena R .

411. Dokazati:

- (i) Potprsten prstena sa jedinicom ne mora biti prsten sa jedinicom.
- (ii) Potprsten prstena bez jedinice može da ima jedinicu.
- (iii) Potprsten može da ima jedinicu različitu od jedinice prstena.

412. Ako je n prirodan broj, $n \geq 2$, konstruisati prsten sa jedinicom R koji ima niz potprstena $R_1 \supseteq R_2 \supseteq \dots \supseteq R_n$ takvih da R_{2k+1} nema jedinicu, a R_{2k} ima jedinicu, $k = 1, 2, \dots, \left\lfloor \frac{n}{2} \right\rfloor$.

Uputstvo. $n = 2$.

$$R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}, \text{ prsten matrica formata } 2 \times 2,$$

$$R_1 = \left\{ \begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix} \mid b, d \in \mathbb{Z} \right\}, \text{ potprsten bez jedinice,}$$

$$R_2 = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & d \end{bmatrix} \mid d \in \mathbb{Z} \right\}, \text{ potprsten od } R_1 \text{ sa jedinicom.}$$

Za $n > 2$ koristiti blok matrice odgovarajućeg formata.

413. Neka je L potprsten prstena R . Ako L ima jedinični element, a R nema jedinični element, tada R ima delitelje nule.

Rešenje. Neka je e jedinični element prstena L . Tada postoji $a \in R$, $a \notin L$, tako da je $ea = b \neq a$. Kako je

$$eb = e(ea) = (ee)a = ea = b,$$

onda je $ea = eb$, što daje $e(a - b) = 0$. $a \neq b$, $e \neq 0$ (v. 2.3), pa je e delitelj nule u R .

414. a) Dokazati da se svaki prsten R može potopiti u prsten sa jedinicom.

b) Dokazati da se svaki prsten R karakteristike k može potopiti u prsten sa jedinicom karakteristike k .

Uputstvo. a) U skupu uređenih parova $\mathbb{Z} \times R = \{(m, a) \mid m \in \mathbb{Z}, a \in R\}$ definišemo operacije $+$ i $\cdot$ sa

$$(m, a) + (n, b) = (m + n, a + b),$$

$$(m, a) \cdot (n, b) = (mn, ab + na + mb).$$

Dokazati da je $(\mathbb{Z} \times R, +, \cdot)$ prsten sa jedinicom $(1, 0)$ i da je podskup

elemenata oblika $(0, a)$ potprsten prstena $\mathbb{Z} \times R$ izomorfan prstenu R .

b) Ako je karakteristika prstena R nula, tada se primenjuje konstrukcija pod a), a ako je $\text{Char } R = k \neq 0$ primeniti postupak iz a) na $\mathbb{Z}_k \times R$.

415. Konačan domen integriteta D je polje. Dokazati.

Rešenje. Ako je

$$ab = ac, \quad a, b, c \in D, \quad a \neq 0,$$

onda iz

$$ab - ac = a(b - c) = 0,$$

sledi $b = c$. Dakle, u konačnoj komutativnoj polugrupi $(D \setminus \{0\}, \cdot)$ važi zakon kancelacije, pa je na osnovu zadatka 48, $(D \setminus \{0\}, \cdot)$ komutativna grupa.

Prema tome, $(D, +, \cdot)$ je polje.

PRIMEDBA. Prethodno tvrđenje se može dokazati i pod znatno slabijim uslovima (bez pretpostavki o komutativnosti i postojanju jedinice u D). Gornji dokaz se može primeniti i na proizvoljan konačan prsten R bez delitelja nule, pa se dobija da je svaki takav prsten telo. S obzirom na teoremu Vederberna (Wedderburn): svako konačno telo je polje; sledi da je i prsten R polje.

Literatura:

M. Stojaković, *Teorija jednačina*, Naučna knjiga, Beograd, 1973, (str. 130),
V. Perić, *Algebra II*, Svjetlost, Sarajevo, 1980, (str. 100).

416. Neka je R prsten sa jedinicom bez nilpotentnih elemenata. Ako za svako $x \in R$, $x \neq 0$, postoje $a, b \in R$ takvi da je $axb = 1$, tada je R telo. Dokazati.

417. Konstruisati prsten razlomaka $S^{-1}R$ (2.58) ako je $R = \mathbb{Z}$ i

a) $S = \mathbb{Z} \setminus \{0\}$,

b) $S = \{1, p, \dots, p^k, \dots\}$, p je prost broj,

c) $S = \{a \in \mathbb{Z} \mid p \nmid a, \quad p \text{ je prost broj}\}$.

Rešenje. Pošto je $\mathbb{Z}$ domen integriteta, a S u sva tri slučaja ne sadrži 0, uslov 2.58 (i), tj.

$$(r_1, s_1) \sim (r_2, s_2) \iff (\exists s \in S) s(r_1 s_2 - r_2 s_1) = 0,$$

gde $r_1, r_2 \in R$, $s_1, s_2 \in S$, se svodi na

$$(r_1, s_1) \sim (r_2, s_2) \iff r_1 s_2 = r_2 s_1.$$

Detaljno ćemo rešiti a), dok se b) i c) rešavaju analogno.

Lako se proverava da je $\sim$ refleksivna i simetrična relacija, dokažimo da je i tranzitivna. Neka je

$$(r_1, s_1) \sim (r_2, s_2) \quad \text{i} \quad (r_2, s_2) \sim (r_3, s_3),$$

tj. $r_1 s_2 = r_2 s_1$ i $r_2 s_3 = r_3 s_2$, pa je $r_1 s_2 s_3 = r_2 s_1 s_3$ i $r_2 s_3 s_1 = r_3 s_2 s_1$ odakle sledi $r_1 s_2 s_3 = r_3 s_2 s_1$. Kako je $s_2 \neq 0$ važi $r_1 s_3 = r_3 s_1$, tj. $(r_1, s_1) \sim (r_3, s_3)$, pa je $\sim$ tranzitivna relacija, dakle, relacija ekvivalencije. U daljem ćemo klasu u kojoj se nalazi element (r, s) označavati sa r/s .

Treba dokazati da su operacije definisane u 2.58 (i) na skupu $\mathbb{Z} \times S / \sim = S^{-1}\mathbb{Z}$ dobro definisane, tj. da iz

$$(r_1, s_1) \sim (r'_1, s'_1) \quad \text{i} \quad (r_2, s_2) \sim (r'_2, s'_2)$$

sledi

$$(r_1 s_2 + r_2 s_1, s_1 s_2) \sim (r'_1 s'_2 + r'_2 s'_1, s'_1 s'_2)$$

i

$$(r_1 r_2, s_1 s_2) \sim (r'_1 r'_2, s'_1 s'_2),$$

što se lako proverava. Na taj način dobili smo prsten razlomaka $S^{-1}\mathbb{Z}$.

Proverimo da je preslikavanje $f : \mathbb{Z} \rightarrow S^{-1}\mathbb{Z}$ definisano sa $f : r \mapsto r/1$ homomorfizam.

Jasno je da je $r_1 = r_2 \iff (r_1, 1) \sim (r_2, 1) \iff r_1/1 = r_2/1$, pa je f dobro definisano, a i injektivno.

$$f(r_1 + r_2) = (r_1 + r_2)/1 = r_1/1 + r_2/1 = f(r_1) + f(r_2),$$

$$f(r_1 r_2) = (r_1 r_2)/1 = (r_1/1)(r_2/1) = f(r_1)f(r_2),$$

pa je f monomorfizam. Dakle, $S^{-1}\mathbb{Z}$ sadrži potprsten izomorfan sa $\mathbb{Z}$, tj. $\mathbb{Z}$ se može potopiti u $S^{-1}\mathbb{Z}$.

Neposredno se proverava da je $1/1$ jedinica u $S^{-1}\mathbb{Z}$ i da svako $s/1 \in S^{-1}\mathbb{Z}$, (tj. $s \neq 0$), ima mutiplikativni inverzni element $1/s$, tj. $S^{-1}\mathbb{Z}$ je polje i to polje je, što nije teško videti, ustvari polje racionalnih brojeva $\mathbb{Q}$.

U slučaju b) dobija se prsten izomorfan prstenu $\left\{\frac{a}{b} \in \mathbb{Q} \mid b = p^k, k \in \mathbb{N}\right\}$, a u slučaju c) prsten izomorfan prstenu $\left\{\frac{a}{b} \in \mathbb{Q} \mid \text{nzd}(b, p) = 1\right\}$.

418. Dokazati da se svaki domen integriteta R može potopiti u polje.

Uputstvo. Konstruisati $S^{-1}R$, gde je $S = R \setminus \{0\}$.

419. Prsten R je domen integriteta ako i samo ako postoji polje F tako da je R potprsten polja F .

420. Neka je R komutativan prsten sa jedinicom, S multiplikativno zatvoren podskup u R i preslikavanje $f : R \rightarrow S^{-1}R$ dato sa $f : r \mapsto r/1$, gde je $S^{-1}R$ definisano u 2.58. Dokazati:

- a) f je homomorfizam R u $S^{-1}R$.
- b) $\text{Ker } f = \{r \in R \mid \text{postoji } s \in S \text{ tako da je } sr = 0\}$.
- c) Ako S ne sadrži delitelje nule, f je homomorfizam.
- d) Svaki element iz $f(S)$ ima inverzni element u $S^{-1}R$.

421. Konstruisati $S^{-1}R$ (2.58) ako je $R = F[[x]]$, gde je F polje (zadatak 376), a $S = \{1, x, \dots, x^k, \dots\}$.

Rezultat. $S^{-1}R \cong F\langle x \rangle$ (videti zadatak 378).

422. Dokazati da je prsten R komutativan ako i samo ako za svako $a, b \in R$ važi

$$(a + b)^2 = a^2 + 2ab + b^2.$$

423. Dokazati da je svaki Bulov prsten komutativan prsten karakteristike 2.

Rešenje. Ako je R Bulov prsten, onda za svako $a \in R$ važi

$$a + a = (a + a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a,$$

odakle je $a + a = 0$, tj. R ima karakteristiku 2. Iz

$$a + b = (a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2 = a + ab + ba + b$$

sledi $ab + ba = 0$, a kako je $ab + ab = 0$ (jer prsten ima karakteristiku 2) mora biti

$$ab = ba,$$

za svako $a, b \in R$, tj. prsten R je komutativan.

PRIMEDBA. Primer Bulovog prstena je prsten iz zadatka 367.

424. Ako u prstenu sa jedinicom R važi za svako $a, b \in R$ $(a + b)^2 = a^2 + b^2$, tada je R komutativan prsten. Dokazati.

Rešenje. Iz

$$(1 + 1)^2 = 1^2 + 1^2 + 1^2 + 1^2 = 1^2 + 1^2$$

sledi $1 + 1 = 0$, tj. $1 = -1$, pa je $-a = (-1)a = 1a = a$ za svako $a \in R$.

Za svako $a, b \in R$ iz

$$(a + b)^2 = a^2 + ab + ba + b^2 = a^2 + b^2$$

sledi $ab + ba = 0$, pa je $ab = -ba = ba$.

425. Neka je R prsten u kome za svako $x, y \in R$ važi

$$x(y^2 - y) = (y^2 - y)x.$$

Dokazati da je R komutativan prsten.

Rešenje. Za svako $a, b \in R$

$$\begin{aligned} ab &= a(ab + ba - ab - ba) + ab = a(ab + ba) - a^2b - aba + ab = \\ &= a(a^2 + ab + ba + b^2 - a^2 - b^2) - (a^2 - a)b - aba = \\ &= a((a + b)^2 - (a + b) - (a^2 - a) - (b^2 - b)) - (a^2 - a)b - aba = \\ &= ((a + b)^2 - (a + b) - (a^2 - a) - (b^2 - b))a - b(a^2 - a) - aba = \\ &= (ab + ba)a - ba^2 + ba - aba = ba. \end{aligned}$$

426. Neka je R prsten takav da postoji prirodan broj n tako da je $x^n = x$ za svako x iz R . Ako je n neparan broj, karakteristika prstena R je proizvod različitih prostih brojeva, a ako je n paran broj, onda je $\text{Char } R = 2$. Dokazati.

Rešenje. Za svako $x \in R$ i svako $k \in \mathbb{N}$ važi $(kx)^n = kx$, tj. $(k^n - k)x = 0$, pa $\text{Char } R$ deli $k^n - k$ za svaki prirodan broj k . Ako je kvadrat nekog prirodnog broja činilac broja $\text{Char } R$, tada je činilac $\text{Char } R$ i kvadrat nekog prostog broja, recimo p^2 . To znači da p^2 deli $k^n - k$ za svako $k \in \mathbb{N}$, pa i da p^2 deli $p^n - p$, što je nemoguće. Dakle, $\text{Char } R$ je proizvod različitih prostih brojeva.

Ako je n paran broj, onda je $-x = (-x)^n = x$, pa je $2x = 0$ i $\text{Char } R = 2$.

427. Neka je R prsten u kome važi $x^3 = x$ za svako $x \in R$. Dokazati da je R komutativan prsten.

Rešenje. Iz $(x+x)^3 = x+x$ za svako $x \in R$ se neposredno dobija da je za svako $x \in R$ $6x = 0$, a iz

$$x^2 - x = (x^2 - x)^3 = x^6 - 3x^5 + 3x^4 - x^3 = x^2 - 3x + 3x^2 - x,$$

sledi da je $3x^2 = 3x$ za svako $x \in R$.

Neka je $T = \{3x \mid x \in R\}$. Dokazaćemo da je T komutativan potprsten prstena R . Ako su $a, b \in T$, onda postoje $x, y \in R$ tako da je $a = 3x$, $b = 3y$, pa je $a - b = 3(x - y) \in T$ i $ab = 3(3xy) \in T$. Prema tome, na osnovu 2.27, T je potprsten. Kako je

$$a^2 = (3x)^2 = 9x^2 = 3x^2 = 3x = a,$$

na osnovu zadatka 423 T je komutativan prsten. Dakle, $(3x)(3y) = (3y)(3x)$, odakle sledi

$$(1) \quad 3xy = 3yx.$$

Kako je

$$(x+y)^3 = (x^2+xy+yx+y^2)(x+y) = x^3+xyx+yx^2+y^2x+x^2y+xy^2+yxy+y^3,$$

iz $(x+y)^3 = (x+y)$ dobija se

$$(2) \quad xyx + yx^2 + y^2x + x^2y + xy^2 + yxy = 0,$$

a slično iz $(x-y)^3 = (x-y)$ sledi

$$(3) \quad xy^2 - x^2y - xyx - yx^2 + yxy + y^2x = 0.$$

Sabirajući (2) i (3) dobija se

$$(4) \quad 2xy^2 + 2yxy + 2y^2x = 0.$$

Ako jednakost (4) pomnožimo sa y najpre sleva, pa onda zdesna, dobićemo

$$(5) \quad 2yxy^2 + 2y^2xy + 2yx = 0,$$

$$(6) \quad 2xy + 2yxy^2 + 2y^2xy = 0.$$

Oduzimajući (6) od (5) sledi

$$(7) \quad 2xy = 2yx,$$

pa ako od (1) oduzmemo (7) biće $xy = yx$ za svako $x, y \in R$.

428. Neka je R prsten u kome važi $x^4 = x$ za svako $x \in R$. Dokazati da je R komutativan prsten.

Rešenje. Neka je a proizvoljan element iz R . Zbog zadatka 426 a) je $\text{Char } R = 2$, pa je

$$(a + a^2)^2 = a^2 + 2a^3 + a^4 = a + a^2,$$

tj. $a + a^2$ je idempotent. R očigledno ne može da ima nilpotentnih elemenata, pa na osnovu zadatka 437 a) element $a^2 + a$ komutira sa svim elementima prstena. Zbog $\text{Char } R = 2$ važi da je $a^2 + a = a^2 - a$, pa s obzirom na zadatak 425 sledi da je R komutativan prsten.

PRIMEDBA. Zadaci 427 i 428 su specijalni slučajevi teoreme Džekobsona koja je navedena u primedbi iza zadatka 511.

429. Neka je R domen integriteta takav da postoji element $a \in R$, $a \neq 0$ i prirodan broj n , tako da je $na = 0$. Dokazati da je karakteristika domena R prirodan broj d koji je delitelj broja n .

Rešenje. Iz

$$na = n(1_R a) = (n1_R)a = 0$$

i $a \neq 0$ sledi $n1_R = 0$ pošto je R domen. Otuda je za svako $r \in R$

$$nr = n(1_R r) = (n1_R)r = 0r = 0,$$

pa je $\text{Char } R = d$, gde je d prirodan broj manji ili jednak n . Iz pretpostavke da d nije delitelj broja n , tj. da postoje $k, l \in \mathbb{Z}$, $l \neq 0$, $l < d$, tako da je $n = kd + l$, sledi da je $lr = 0$, za svako $r \in R$, što je protivrečnost. Dakle, d je delitelj n .

430. Neka je R prsten sa konačno mnogo elemenata, $a_1, a_2, \dots, a_n$, i neka je n_i red elementa a_i , $i = 1, 2, \dots, n$ u aditivnoj grupi prstena R . Dokazati da je karakteristika prstena R najmanji zajednički sadržalac za n_i , $i = 1, 2, \dots, n$.

431. Neka je R prsten u kome je $xy = yx$ ili $xy = -yx$ za svako $x, y \in R$. Dokazati da je R ili komutativan prsten ili je za svako $x, y \in R$ $xy = -yx$.

Rešenje. Za svako $a \in R$ neka je $C_a = \{x \in R \mid ax = xa\}$ i $A_a = \{x \in R \mid ax = -xa\}$. Po pretpostavci je za svako $a \in R$ $C_a \cup A_a = R$.

Ako je $R \neq C_a$ i $R \neq A_a$, postoje elementi $b \in C_a \setminus A_a$ i $d \in A_a \setminus C_a$. Tada iz $a(b+d) = (b+d)a$ sledi da je $ad = da$, a iz $a(b+d) = -(b+d)a$ sledi da je $ab = -ba$, što su kontradikcije, pa je ili $R = C_a$ ili $R = A_a$.

Označimo sa $U = \{a \in R \mid C_a = R\}$ i $V = \{a \in R \mid A_a = R\}$. Tada je $R = U \cup V$. Ako je $R \neq U$ i $R \neq V$, tada postoje elementi $u \in U \setminus V$ i $v \in V \setminus U$. Posmatrajmo $u+v$. Iz $u+v \in U$ analogno kao i ranije sledi da $v \in U$, a iz $u+v \in V$ sledi da $u \in V$. Prema tome, ili je $R = U$ ili $R = V$, tj. ili je R komutativan prsten ili je $xy = -yx$ za svako $x, y \in R$.

Literatura:

M. Reich, *A commutativity theorem for algebras*, Amer. Math. Monthly, 82 (1975), 377-379.

432. Neka je R prsten sa jedinicom i neka njegovi elementi a, b i $a+b$ imaju multiplikativne inverzne elemente. Dokazati da je $(a+b)^{-1} = a^{-1} + b^{-1}$ ako i samo ako postoji element $p \in R$ takav da je $b = ap$ i $p^2 + p + 1 = 0$.

Rešenje. Pretpostavimo da je $(a+b)^{-1} = a^{-1} + b^{-1}$. Ako tu jednakost pomnožimo sleva sa $a+b$ i zdesna sa b dobijamo

$$b = 2b + a + ba^{-1}b$$

pa je

$$ba^{-1}b + b = -a,$$

što daje, kad se pomnoži sleva sa a^{-1} ,

$$a^{-1}ba^{-1}b + a^{-1}b + 1 = 0.$$

Ako $a^{-1}b$ označimo sa p , vidimo da je $b = ap$ i $p^2 + p + 1 = 0$.

Obrnuto, neka je $p \in R$ takvo da je $b = ap$ i $p^2 + p + 1 = 0$. Tada je

$$p^{-1} = -1 - p = p^2 \quad \text{i} \quad (1+p)^{-1} = -p = 1 + p^2,$$

pa je

$$\begin{aligned} (a+b)^{-1} &= (a+ap)^{-1} = (a(1+p))^{-1} = (1+p)^{-1}a^{-1} = (1+p^2)a^{-1} = \\ &= a^{-1} + p^2a^{-1} = a^{-1} + p^{-1}a^{-1} = a^{-1} + (ap)^{-1} = a^{-1} + b^{-1}. \end{aligned}$$

Literatura:

T.E. Elsner, *The inverse of a sum can be the sum of the inverses*, Math. Mag., 52 (1979), 173-174.

433. Ako u komutativnom prstenu sa jedinicom element a ima multiplikativan inverzni element, a b je nilpotentan element, onda $a + b$ ima multiplikativan inverzni element. Dokazati.

Rešenje. Neka je $b^n = 0$, $n \in \mathbb{N}$. Ako za $a + b$ postoji multiplikativan inverzni element x , onda je $(a + b)x = 1$, odakle je

$$x = a^{-1} - a^{-1}bx.$$

Ako sada x na desnoj strani ove jednačine zamenimo sa $a^{-1} - a^{-1}bx$, biće

$$x = a^{-1} - a^{-1}b(a^{-1} - a^{-1}bx) = a^{-1} - a^{-2}b + a^{-2}b^2x.$$

Produžujući ovaj postupak, posle n koraka dobićemo

$$x = a^{-1} - a^{-2}b + a^{-3}b^2 - \dots + (-1)^{n-1}a^{-n}b^{n-1} + (-1)^na^{-n}b^nx.$$

Kako je $b^n = 0$, poslednji sabirak na desnoj strani ove jednačine jednak je 0, pa je

$$x = \sum_{k=1}^n (-1)^{k-1} a^{-k} b^{k-1}.$$

Množenjem sa $a + b$ se lako proverava da je x zaista multiplikativni inverzni element za $a + b$.

434. Ako su a i b nilpotentni elementi komutativnog prstena R , dokazati da je $a + b$ takođe nilpotentan element.

Rešenje. a i b su nilpotentni elementi, tj. postoje $n, m \in \mathbb{N}$, tako da je

$$a^n = b^m = 0.$$

S obzirom da je prsten komutativan, biće

$$(a + b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^{n+m-k} b^k.$$

Međutim, za $k < m$ je $n + m - k > n$, pa je $a^{n+m-k} = 0$, a za $k \geq m$ je $b^k = 0$. Prema tome,

$$a^{n+m-k} b^k = 0, \quad k = 0, 1, \dots, m + n,$$

tj.

$$(a + b)^{n+m} = 0.$$

PRIMEDBA. Primerom pokazati da gornje tvrđenje ne važi ako prsten nije komutativan.

435. Neka je R komutativan prsten bez nilpotentnih elemenata i neka za elemente $x, y \in R$ važi $x^2 = y^2$ i $x^3 = y^3$. Dokazati da je $x = y$.

Rešenje.

$$(x - y)^3 = x^3 - 3x^2y + 3xy^2 - y^3 = x^3 - 3y^3 + 3x^3 - y^3 = 0,$$

pa pošto R nema nilpotentnih elemenata sledi da je $x - y = 0$, tj. $x = y$.

436. Dokazati da prsten R nema nilpotentnih elemenata ako i samo ako iz $x^2 = 0$ sledi $x = 0$ za svako x iz R .

Rešenje. Pretpostavimo da za svako $x \in R$ iz $x^2 = 0$ sledi $x = 0$ i neka je $a \in R$ nilpotentan element, tj. $a^k = 0$ i $a^{k-1} = b \neq 0$ ($k > 2$). Tada je

$$b^2 = a^{2k-2} = a^k a^{k-2} = 0,$$

tj. $b = 0$, što je protivrečnost.

Obrnuto tvrđenje je direktna posledica definicije nilpotentnog elementa.

437. Ako je prsten R bez nilpotentnih elemenata onda:

a) Za svaki idempotent e i svaki element x prstena R važi $xe = ex$.

c) Ako su $a, b \in R$, onda je $ab = 0$ ako i samo ako je $ba = 0$.

Dokazati.

Rešenje. a) Važi

$$(xe - exe)^2 = xexe - xexe - exexe + exexe = 0,$$

pa je

$$(*) \quad xe - exe = 0.$$

Analogno je

$$(ex - exe)^2 = exex - exexe - exex + exexe = 0,$$

pa je i

$$(**) \quad ex - exe = 0.$$

Ako od (*) oduzmemo (**), dobijamo $xe = ex$.

b) Neka je $ab = 0$. Tada je $(ba)^2 = b(ab)a = 0$, pa je $ba = 0$. Analogno se dokazuje obrnuto tvrđenje.

438. Neka je R prsten u kome za svako $b, c \in R$ za koje je $b^3 = c^2$ sledi da postoji element a takav da je $a^2 = b$ i $a^3 = c$. Dokazati da prsten R nema nilpotentnih elemenata.

Rešenje. Dovoljno je pokazati da iz $b^2 = 0$ sledi $b = 0$ (zadatak 436). Neka je $b^2 = 0$. Tada je $b^3 = 0$, pa je $b^3 = b^2$. Prema tome, postoji element $a \in R$ takav da $a^2 = b$ i $a^3 = b$. Tada je

$$b = a^3 = ab = aa^3 = a^2a^2 = b^2 = 0.$$

439. Neka je R prsten takav da svaki nenula polinom sa koeficijentima iz R ima samo konačno mnogo korena u R . Dokazati da je R konačan prsten ili prsten bez delitelja nule.

Rešenje. Neka je R beskonačan prsten i neka je za neko $a, b \in R$ $ab = 0$, $a \neq 0$, $b \neq 0$. Preslikavanje $f : r \mapsto br$ je endomorfizam aditivne grupe R . Skupovi $\text{Im } f$ i $\text{Ker } f$ ne mogu biti oba konačni zbog prve teoreme o izomorfizmu grupa (1.64).

Neka je $\text{Im } f$ beskonačan skup, tada polinomna jednačina $ax = 0$ ima beskonačno mnogo rešenja, jer je svaki element $c \in \text{Im } f$ oblika $c = bd$ za neko $d \in R$, pa je rešenje jednačine $ax = 0$.

Ako je $\text{Ker } f$ beskonačan skup, onda jednačina $bx = 0$ ima beskonačno mnogo rešenja.

440. Dokazati da je prsten $F[[x]]$ formalnih stepenih redova nad poljem F (zadatak 376) domen integriteta.

441. Neka je R prsten sa jedinicom. Element $f = \sum_{k=0}^{\infty} a_k x^k \in R[[x]]$ (zadatak 376) ima multiplikativni inverzni element u $R[[x]]$ ako i samo ako a_0 ima multiplikativni inverzni element u R . Dokazati.

Rešenje. Neka je $f = \sum_{k=0}^{\infty} a_k x^k$ i $g = \sum_{k=0}^{\infty} b_k x^k$. Ako pretpostavimo da je

$fg = gf = 1$, onda je po definiciji množenja stepenih redova $a_0b_0 = b_0a_0 = 1$, pa je b_0 inverzni element za a_0 .

Obrnuto, pretpostavimo da a_0 ima multiplikativni inverzni element. $fg = 1$ ako i samo ako važe sledeće jednakosti:

$$\begin{aligned} a_0b_0 &= 1, \\ a_0b_1 + a_1b_0 &= 0, \\ a_0b_2 + a_1b_1 + a_2b_0 &= 0, \\ &\dots\dots\dots \\ a_0b_n + a_1b_{n-1} + \dots + a_nb_0 &= 0, \\ a_0b_{n+1} + a_1b_n + \dots + a_nb_1 + a_{n+1}b_0 &= 0, \\ &\dots\dots\dots \end{aligned}$$

Dokažimo indukcijom po n da ovaj sistem ima rešenje po $b_0, b_1, \dots$. Da je tvrđenje tačno za $n = 0$ neposredno sledi iz pretpostavke. Ako su izračunati $b_0, b_1, \dots, b_n$, tada je

$$b_{n+1} = -a_0^{-1}(a_1b_n + \dots + a_nb_1 + a_{n+1}b_0),$$

pa za f postoji desni inverzni element g . Analogno se pokazuje da postoji i levi inverzni element, ako postoje i levi i desni inverzni element tada su oni međusobno jednaki i to je inverzni element za f ($h = h \cdot 1 = h(fg) = (hf)g = 1g = g$).

442. Dokazati da za svaka dva elementa f, g u prstenu $F[[x]]$ formalnih stepenih redova nad poljem F (zadatak 376) važi: f je delitelj g ili je g delitelj f .

Rešenje. Ako su $f, g \in F[[x]]$, neka je f_k koeficijent sa najmanjim indeksom različit od nule u $f = f_0 + f_1x + \dots + f_nx^n + \dots$, a u $g = g_0 + g_1x + \dots + g_nx^n + \dots$ neka je to g_ℓ . Tada f i g mogu da se napišu u obliku

$$f = x^k(f_k + f_{k+1}x + \dots), \quad g = x^\ell(g_\ell + g_{\ell+1}x + \dots),$$

pa za $k \leq \ell$ f deli g , a ako je $\ell \geq k$ tada g deli f , jer na osnovu prethodnog zadatka redovi u zagradama imaju inverzne elemente.

443. Neka je R komutativan prsten bez delitelja nule u kome postoji idempotent a različit od nule. Dokazati da je R domen integriteta čija je jedinica a .

Rešenje. Neka je x proizvoljan element iz R . Kako je $a^2 = a$, biće

$$xa^2 = xa,$$

pa je

$$(xa - x)a = 0,$$

odakle je, zbog $a \neq 0$, $xa - x = 0$, odnosno $xa = ax = x$.

444. Neka je R domen integriteta koji nije polje. Označimo sa $D = \{x \in R \mid x \text{ je invertibilan ili } x = 0\}$. Nazovimo element $u \in R \setminus D$ univerzalnim deliteljem ako za svako $x \in R$ postoje $x^* \in D$ i $y \in R$ takvi da je $x - x^* = uy$.

Ako je R Euklidov prsten, onda u R postoji univerzalni delitelj. Dokazati.

Rešenje. Posmatrajmo neprazan podskup skupa nenegativnih celih brojeva $S = \{\phi(x) \in \mathbb{N} \mid x \in R \setminus D\}$.

Neka je $u \in R \setminus D$ takav da je $\phi(u)$ najmanji prirodan broj u S . Za svaki element $x \in R$ postoje $q, r \in R$ takvi da je $x = qu + r$ i pri tome je $r = 0$ ili $\phi(u) > \phi(r)$.

Ako je $r = 0$, tada možemo uzeti da je $x^* = 0$, a ako je $r \neq 0$ tada $r \notin R \setminus D$, jer je $\phi(u)$ najmanji u S , pa $r \in D$ i možemo uzeti $x^* = r$. Dakle, u je univerzalni delitelj.

Liretarura:

K.S. Williams, *Note on non-Euclidean principal ideal domains*, Math. Mag., 48 (1975), 176-177.

445. Neka je R komutativan prsten sa jedinicom i neka je e idempotent različit od 0 i 1. Dokazati:

- a) $1 - e$ je idempotent,
- b) Re i $R(1 - e)$ su potprsteni sa jedinicom,
- c) $R \cong Re \times R(1 - e)$.

Rešenje. a) $(1 - e)^2 = 1 - 2e + e^2 = 1 - e$.

b) Za svako $xe, ye \in Re$ je

$$xe - ye = (x - y)e \quad \text{i} \quad xeye = xye^2 = xye,$$

pa je Re potprsten (zadatak 406) a njegova jedinica je e .

Analogno se proverava za $R(1 - e)$.

c) Definišimo preslikavanje $f : R \rightarrow Re \times R(1 - e)$ sa

$$f : x \mapsto (xe, x(1 - e)).$$

f je injektivno preslikavanje, jer ako je

$$(xe, x(1 - e)) = (ye, y(1 - e)),$$

tada je

$$xe = ye \quad \text{i} \quad x(1 - e) = y(1 - e),$$

pa kad saberemo dve poslednje jednakosti dobijamo

$$xe + x(1 - e) = ye + y(1 - e),$$

tj. $x = y$.

f je surjektivno preslikavanje, jer ako je $(xe, y(1 - e)) \in Re \times R(1 - e)$ tada je

$$f(xe + y(1 - e)) = (xe, y(1 - e)),$$

pošto je

$$(xe + y(1 - e))e = xe^2 + y(e - e^2) = xe$$

i

$$(xe + y(1 - e))(1 - e) = x(e - e^2) + y(1 - e)^2 = y(1 - e).$$

f je izomorfizam, jer za svako $x, y \in R$ važi

$$\begin{aligned} f(x + y) &= ((x + y)e, (x + y)(1 - e)) = (xe + ye, x(1 - e) + y(1 - e)) = \\ &= (xe, x(1 - e)) + (ye, y(1 - e)) = f(x) + f(y) \end{aligned}$$

i

$$\begin{aligned} f(xy) &= (xye, xy(1 - e)) = (xeye, x(1 - e)y(1 - e)) = \\ &= (xe, x(1 - e))(ye, y(1 - e)) = f(x)f(y). \end{aligned}$$

2.4 Ideali i homomorfizmi

446. Dokazati da je u prstenu svaki ideal potprsten, a da svaki potprsten ne mora da bude ideal.

447. Neka je S neprazan podskup prstena R za koji važi

- a) Iz $a, b \in S$ sledi $a + b \in S$,
- b) Iz $a, b \in S$ i $r \in R$ sledi $ar, ra \in S$.

Dokazati da S ne mora da bude potprsten (a to znači ni ideal) prstena R .

Rešenje. U skupu celih brojeva $\mathbb{Z}$ pored uobičajenog sabiranja, definišemo množenje sa

$$a \cdot b = 0, \quad \text{za svako } a, b \in \mathbb{Z}.$$

Skup $\mathbb{Z}$ je u odnosu na sabiranje i ovako definisano množenje prsten. Tada u skupu $\mathbb{Z}$ podskup nenegativnih celih brojeva zadovoljava date uslove, ali nije potprsten.

448. Neka je $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{Z} \right\}$.

- a) Dokazati da je R prsten u odnosu na sabiranje i množenje matrica.
- b) Dokazati da je $I = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$ ideal u prstenu R .
- c) Naći faktor prsten R/I .

Rešenje. c) Iz

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + I = \begin{bmatrix} 0 & 0 \\ 0 & c \end{bmatrix} + \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} + I = \begin{bmatrix} 0 & 0 \\ 0 & c \end{bmatrix} + I,$$

sledi da je suskup određen matricom $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ jednak suskupu određenom sa $\begin{bmatrix} 0 & 0 \\ 0 & c \end{bmatrix}$, pa je na osnovu definicije operacija u faktor prstenu i definicije matričnih operacija

$$R/I = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & c \end{bmatrix} + I \mid c \in \mathbb{Z} \right\} \cong \mathbb{Z}.$$

449. Ako je $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$, dokazati da je preslikavanje

$$f : \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mapsto a,$$

homomorfizam prstena S na prsten $\mathbb{R}$ realnih brojeva. Odrediti jezgro $\text{Ker } f$ tog homomorfizma i faktor prsten $S/\text{Ker } f$.

450. Neka je D skup svih diferencijabilnih funkcija $f : \mathbb{R} \rightarrow \mathbb{R}$. Dokazati da je $(D, +, \cdot)$ komutativan prsten sa jedinicom ako su operacije $+$ i $\cdot$ definisane sa

$$(f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x), \quad \text{za svako } x \in \mathbb{R}.$$

Ako je $S = \{f \mid f \in D, f(0) = 0\}$ a $T = \{f \mid f \in D, f'(0) = 0\}$, gde je f' izvod funkcije f , dokazati:

- a) S je ideal u D ,
- b) T je potprsten od D , ali nije ideal,
- c) $S \cap T$ je ideal u D .

Rešenje. a) Za svako $f, g \in S$ $(f - g)(0) = f(0) - g(0) = 0$, pa $f - g \in S$. Za svako $h \in D$, $f \in S$,

$$(hf)(0) = h(0)f(0) = 0, \quad (fh)(0) = f(0)h(0) = 0,$$

pa $hf, fh \in S$, što znači da je S ideal u D .

b) Ako $f, g \in T$, onda je

$$(f - g)'(0) = (f' - g')(0) = f'(0) - g'(0) = 0,$$

$$(fg)'(0) = (f'g + fg')(0) = f'(0)g(0) + f(0)g'(0) = 0.$$

Prema tome, T je potprsten od D . T nije ideal u D , jer, na primer, funkcija f definisana sa $(\forall x \in \mathbb{R}) f(x) = 1$ pripada T jer je $f'(0) = 0$, ali za funkciju $g \in D$ definisanu sa $(\forall x \in \mathbb{R}) g(x) = x$ važi $fg = g \notin T$.

c) Pošto su S i T potprsteni i $S \cap T$ je potprsten. Ako je $f \in S \cap T$, onda je $f(0) = 0$ i $f'(0) = 0$, pa je za svako $g \in D$ $(fg)(0) = f(0)g(0) = 0$ i

$$(fg)'(0) = (f'g + fg')(0) = f'(0)g(0) + f(0)g'(0) = 0.$$

451. Neka su R i S prsteni sa bar dva elementa i $f : R \rightarrow S$ epimorfizam (2.44). Odrediti, dajući dokaz ili kontra primer, koja od sledećih tvrđenja su tačna:

- a) Ako je R komutativan prsten i S je komutativan.
- b) Ako R ima jedinicu i S ima jedinicu.
- c) Ako R i S imaju jedinice, onda je $f(1_R) = 1_S$.
- d) Ako R ima delitelje nule i S ima delitelje nule.
- e) Ako je R domen integriteta i S je domen integriteta.
- f) Ako je R polje i S je polje.

Uputstvo. Tvrđenja a), b) i c) su tačna.

d) Netačno. Konstruisati epimorfizam prstena $\mathbb{Z}_6$ na $\mathbb{Z}_2$.

e) Netačno. Konstruisati epimorfizam prstena $\mathbb{Z}$ na $\mathbb{Z}_6$.

f) Tačno. $\text{Ker } f$ je ideal u R , pa ako je R polje mora biti $\text{Ker } f = \{0\}$ ili $\text{Ker } f = R$. Ako bi bilo $\text{Ker } f = R$, onda bi S imao samo 1 element, što je protivrečnost. Dakle, $\text{Ker } f = \{0\}$, što znači da je f izomorfizam.

452. Neka je R komutativan prsten.

a) Dokazati da je skup $N(R)$ svih nilpotentnih elemenata prstena R ideal u R .

b) Dokazati da faktor prsten $R/N(R)$ nema nilpotentnih elemenata.

Rešenje. a) Koristiti postupak primenjen u zadatku 434.

b) Ako je $a + N(R)$ nilpotentan element faktor prstena $R/N(R)$, tj. $(a + N(R))^n = N(R)$, onda je $a^n + N(R) = N(R)$, pa je $a^n \in N(R)$. Dakle, $(a^n)^s = 0$, odnosno $a \in N(R)$, i $a + N(R) = N(R)$, tj. $a + N(R)$ je nula prstena $R/N(R)$.

453. Neka je R komutativan prsten sa jedinicom koji ima $n \in \mathbb{N}$ delitelja nule. Dokazati da prsten R ima najviše $(n + 1)^2$ elemenata.

Rešenje. Neka je d delitelj nule u prstenu R . Označimo sa $A = \{a \in R \mid ad = 0\}$. Očigledno je A ideal u prstenu R i $|A| \leq n + 1$, jer su svi nenula elementi iz A delitelji nule, a njih nema više od n .

Posmatrajmo faktor prsten R/A . Definišimo preslikavanje

$$f : R/A \rightarrow D \quad \text{sa} \quad f : r + A \mapsto rd.$$

Lako se proverava da je f dobro definisano (tj. da iz $r + A = s + A$ sledi $rd = sd$). Preslikavanje f je injektivno, jer

$$\begin{aligned} f(r + A) = f(s + A) &\iff rd = sd \iff (r - s)d = 0 \iff r - s \in A \iff \\ &\iff r \in s + A \iff r + A = s + A \iff r + A = s + A. \end{aligned}$$

Pošto je d delitelj nule, postoji $c \neq 0$, takvo da je $cd = 0$. Tada je za svako $r \in R \setminus A$, $c(rd) = r(cd) = 0$, tj. rd je delitelj nule. Funkcijom f se nula faktor prstena R/A preslikava u $0 \in R$, a slike ostalih elemenata faktor prstena su delitelji nule u R , pa $|R/A| \leq n + 1$. Kako je i $|A| \leq n + 1$ dobija se da je $|R| \leq (n + 1)^2$.

Literatura:

Ganesan, N., *Properties of rings with a finite number of zero divisors*, Math. Ann. 157(1964), 215–218.

454. Dokazati da je prsten celih brojeva $\mathbb{Z}$ prsten glavnih ideala.

Rešenje. Neka je I ideal u prstenu celih brojeva $\mathbb{Z}$. Ako je $I = (0)$, onda je I glavni ideal. Ako je $I \neq (0)$, onda u I mora postojati bar jedan pozitivan ceo broj, pa postoji i najmanji pozitivan ceo broj m . Neka je a bilo koji element ideala I . Tada je

$$a = km + r, \quad 0 \leq r < m.$$

Ako je $r > 0$, onda $r = a - km \in I$, a to je protivrečno sa pretpostavkom da je m najmanji ceo pozitivan broj u I . Dakle, $r = 0$, tj. $a = km$, što znači da su svi elementi ideala I umnošci broja m . I je, prema tome, glavni ideal (m) .

455. Naći sve neizomorfne homomorfne slike prstena celih brojeva $\mathbb{Z}$.

Uputstvo. Koristeći prethodni zadatak i 2.50 dokazati da skup svih neizomorfni homomorfni slika čine svi prsteni $(\mathbb{Z}_m, +, \cdot)$, $m \in \mathbb{N}$ i sam prsten $\mathbb{Z}$.

456. Dokazati da je u prstenu celih brojeva $\mathbb{Z}$ za svako $a, b \in \mathbb{Z}$ ideal generisan sa a i b generisan najvećim zajedničkim deliteljem d brojeva a i b , tj. $(a, b) = (d)$. Generalisati.

Uputstvo. Koristiti zadatak 454.

457. Neka je f endomorfizam prstena R i neka je S skup elemenata prstena R koji su fiksni za f , tj. $S = \{x \in R \mid f(x) = x\}$. Dokazati da je S potprsten od R .

458. Neka je R Euklidov prsten (2.25). Dokazati da je R prsten glavnih ideala.

Rešenje. Neka je I ideal u R različit od (0) . Neka je a element iz I takav da je $\phi(a)$ najmanji prirodan broj u skupu nenegativnih celih brojeva $\{\phi(x) \mid x \in I \wedge x \neq 0\}$. Neka je $b \in I$. Tada je $b = qa + r$, gde je $r = 0$ ili $\phi(r) < \phi(a)$. Pošto $b \in I$ i $qa \in I$, onda i $r = b - qa \in I$, pa ne može biti $\phi(r) < \phi(a)$. Stoga je $r = 0$ i $b = qa$, tj. $I = (a)$.

459. Neka je R prsten bez delitelja nule u kome je svaki potprsten ideal. Dokazati da je R komutativan prsten.

Rešenje. Neka je $a \in R$, $a \neq 0$, i neka je S potprsten generisan sa a . S je očigledno komutativan prsten. Po pretpostavci je S ideal, pa za svako $r \in R$ važi $ar = b \in S$. Tada je $ara = ba = ab$ iz čega sledi da je $a(ra - b) = 0$ pa je $ra = b$, jer R nema delitelje nule. Dakle, $ar = b = ra$.

460. Neka je I ideal fon Nojmanovog regularnog prstena R . Dokazati da je svaki ideal J ideala I (kada se I posmatra kao potprsten od R), ideal u R .

Rešenje. Ideal I kao potprsten je takodje fon Nojmanov regularan prsten, jer ako je $a \in I$ i $aa'a = a$, tada je $b = a'aa' \in I$, pa je

$$aba = a(a'aa')a = (aa'a)a'aa' = aa'a = a.$$

Treba dokazati da za svako $a \in J \subseteq I$ i $r \in R$ važi $ar, ra \in J$. Po pretpostavci $ar \in I$, a pošto je R regularan prsten postoji $x \in R$ tako da je $arxar = ar$. Tada $rx(ar) \in I$, a J je ideal u I pa $ar = a(rxar) \in J$. Analogno se dokazuje da $ra \in J$.

461. Neka su $\prod_{i=1}^{\infty} \mathbb{R}$, $\sum_{i=1}^{\infty} \mathbb{R}$, S i T definisani u zadatku 409. Dokazati:

a) $\sum_{i=1}^{\infty} \mathbb{R}$ je ideal u svakom od prstena $\prod_{i=1}^{\infty} \mathbb{R}$, S i T .

b) T je ideal u S , a nije ideal u $\prod_{i=1}^{\infty} \mathbb{R}$.

462. Neka je R prsten a I ideal u R . Ako je $a \in R$, dokazati da je $A = \{r \in R \mid ra - ar \in I\}$ potprsten.

Rešenje. Neka je $r_1, r_2 \in A$. Na osnovu zadatka 406 je dovoljno da pokažemo da $r_1 - r_2 \in A$ i $r_1 r_2 \in A$.

Ako $r_1, r_2 \in A$, tada $r_1a - ar_1, r_2a - ar_2 \in I$, pa

$$r_1a - ar_1 - (r_2a - ar_2) = (r_1 - r_2)a - a(r_1 - r_2) \in I$$

jer je I ideal, tj. $r_1 - r_2 \in A$. Takođe je

$$r_1r_2a - ar_1r_2 = r_1(r_2a - ar_2) + (r_1a - ar_1)r_2 \in I,$$

pa je $r_1r_2 \in A$.

463. Neka je $\mathcal{C}(R)$ centar prstena R . Dokazati:

a) Ako R nije komutativan i nema jedinicu, onda $\mathcal{C}(R)$ ne mora biti ideal.

b) Ako R ima jedinicu ali nije komutativan, onda centar nikad ne može biti ideal.

464. Neka je R komutativan prsten sa jedinicom u kome je svaki element ili nilpotentan ili ima multiplikativni inverzni element. Dokazati da je $R/N(R)$ polje, gde je sa $N(R)$ označen ideal nilpotentnih elemenata.

Rešenje. Neka je $\bar{x} \in R/N(R)$, $\bar{x} \neq 0$. Tada je $\bar{x} = x + N(R)$ i $x \notin N(R)$, pa x po pretpostavci ima inverzni element x' . Tada je $\bar{x'}$ inverzni element za $\bar{x}$.

465. Neka je $f : R_1 \rightarrow R_2$ homomorfizam prstena R_1 u R_2 . Neka je I ideal u R_1 takav da je $\text{Ker } f \subseteq I$. Dokazati da je $I = f^{-1}(f(I))$, gde je $f^{-1}(A) = \{x \in R_1 \mid f(x) \in A \subseteq R_2\}$.

466. Neka je $f : R_1 \rightarrow R_2$ homomorfizam prstena R_1 u prsten R_2 i neka je $\text{Char } R_1 > 0$. Dokazati da je $\text{Char}(f(R_1)) \leq \text{Char } R_1$.

467. Neka je R prsten sa jedinicom i n prirodan broj. Označimo sa $I_n = \{nx \mid x \in R\}$. Dokazati:

a) I_n je ideal u R .

b) $\text{Char}(R/I_n)$ je delitelj broja n .

Rešenje. b) Ako je 1 jedinica prstena R , onda je $1 + I_n$ jedinica prstena R/I_n . Iz

$$n(1 + I_n) = n1 + I_n = I_n,$$

sledi da je $\text{Char}(R/I_n) \mid n$.

468. Neka su R_1 i R_2 prsteni i neka R_1 sadrži potprsten F_1 koji je polje. Ako je $f : R_1 \rightarrow R_2$ homomorfizam, dokazati da je tada $F_1 \subseteq \text{Ker } f$ ili R_2 sadrži potprsten $F_2 \cong F_1$.

469. Neka su $(R, +, \cdot)$ i $(R', +, \cdot)$ Bulovi prsteni takvi da su polugrupe $(R, \cdot)$ i $(R', \cdot)$ izomorfne. Dokazati da su R i R' izomorfni prsteni.

Rešenje. Neka je $f : R \rightarrow R'$ izomorfizam polugrupa $(R, \cdot)$ i $(R', \cdot)$. Ako su 0 i $0'$ nule prstena R i R' respektivno, tada je $f(0) = 0'$. Zaista, ako je $f(a) = 0'$, onda je

$$f(0) = f(a0) = f(a)f(0) = 0'f(0) = 0'.$$

Neka su a i b proizvoljni elementi iz R . Tada postoji element $x \in R$, $(x = f^{-1}(f(a+b) + f(a) + f(b)))$, takav da je

$$(*) \quad f(a+b) = f(a) + f(b) + f(x).$$

Pomnožimo $(*)$ sa $f(ab)$, biće (pri tom koristimo da je svaki Bulov prsten komutativan i karakteristike 2)

$$f(ab)f(a+b) = f(a)(f(a) + f(b) + f(x)),$$

tj. dobijamo

$$f(ab+ab) = f(ab) + f(ab) + f(abx),$$

odnosno $f(abx) = 0'$ pa je i $abx = 0$ (f je bijekcija).

Ako sad pomnožimo $(*)$ sa $f(ax)$, dobijamo

$$f(ax)f(a+b) = f(ax)(f(a) + f(b) + f(x)),$$

odnosno

$$f(ax+abx) = f(ax) + f(abx) + f(ax),$$

otuda je $f(ax) = 0'$, pa je i $ax = 0$.

Konačno, množeći $(*)$ sa $f(x)$ imamo

$$f(x)f(a+b) = f(x)(f(a) + f(b) + f(x)),$$

$$f(ax+bx) = f(ax) + f(bx) + f(x),$$

$$f(bx) = f(bx) + f(x),$$

pa je

$$f(x) = 0'.$$

Pošto je $f(x) = 0$, $(*)$ postaje

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

što je i trebalo dokazati.

470. Neka je R prsten i $a \in R$. Odrediti minimalan ideal I prstena R koji sadrži element a :

- a) Ako je R komutativan prsten sa jedinicom.
- b) Ako je R komutativan prsten bez jedinice.
- c) Ako je R nekomutativan prsten sa jedinicom.
- d) Ako je R nekomutativan prsten bez jedinice.

Rezultat.

a) $I = Ra = \{ra \mid r \in R\}.$

b) $I = Ra + \mathbb{Z}a = \{ra + na \mid r \in R, n \in \mathbb{Z}\}.$

c) $I = \left\{ \sum_{i=1}^k r_i a s_i \mid r_i, s_i \in R, k \in \mathbb{N} \right\} = RaR.$

d) $I = \left\{ ra + as + na + \sum_{i=1}^k r_i a s_i \mid r, s, r_i s_i \in R, n \in \mathbb{Z}, k \in \mathbb{N} \right\} = \mathbb{Z}a + Ra + aR + RaR.$

471. Neka je R prsten sa jedinicom i neka je I levi ideal koji sadrži jedinicu. Dokazati da je $I = R$.

Rešenje. Iz $1 \in I$ sledi da za svako $r \in R$, $r = r1 \in I$, pa je $R \subseteq I$. Kako je $I \subseteq R$, to je $I = R$.

PRIMEDBA. Analogno se dokazuje odgovarajuće tvrđenje za desni ideal.

472. Neka je R prsten sa jedinicom i I levi ideal u R . Ako neki element $a \in I$ ima levi multiplikativni inverzni element, dokazati da je tada $I = R$.

Uputstvo. Iz $a \in I$ sledi $1 = a^{-1}a \in I$ i primeniti prethodni zadatak.

PRIMEDBA. Analogno se dokazuje odgovarajuće tvrđenje za desne ideale.

473. U komutativnom prstenu sa jedinicom R , element a ima multiplikativan inverzni element ako i samo ako a nije sadržano ni u jednom pravom idealu prstena R .

Rešenje. Neka $a \in R$ ima multiplikativan inverzni element, tada na osnovu zadatka 472 iz $a \in I$ sledi da je $I = R$.

Obrnuto, aR je ideal koji po pretpostavci mora biti ceo prsten R , pa

postoji $y \in R$ tako da je $ay = 1$.

474. Dokazati da telo (a to znači i polje) ima samo trivijalne ideale.

Rešenje. Neka je I ideal tela T . Ako I sadrži element $a \neq 0$, onda je $a^{-1} \in T$, pa je $aa^{-1} = 1 \in T$. Na osnovu zadatka 471 je tada $I = T$.

475. Navesti primer komutativnog prstena koji ima samo trivijalne ideale, a nije polje.

Rešenje. $(R, +, \cdot)$, gde je grupa $(R, +)$ izomorfna grupi $(\mathbb{Z}_p, +)$ za prost broj p , a $a \cdot b = 0$ za svako $a, b \in R$.

476. Neka je R komutativan prsten sa jedinicom koji ima samo trivijalne ideale. Dokazati da je R polje.

Rešenje. Neka je $a \in R$, $a \neq 0$. Tada je glavni ideal $(a) = R$, pa postoji x tako da je $xa = ax = 1$.

477. Dokazati da prsten $F^{n,n}$ matrica formata $n \times n$ ($n \in \mathbb{N}$ i $n \geq 2$) nad poljem F ima samo trivijalne ideale.

Rešenje. Koristićemo činjenicu da se svaka matrica $A = [a_{ij}] \in F^{n,n}$ može izraziti kao zbir matrica $a_{ij}B_{ij}$, $i, j = 1, 2, \dots, n$, gde je B_{ij} matrica koja na (i, j) -om mestu ima 1 a ostali elementi su nule.

Sa E_{ij} označićemo matricu koja nastaje od jedinične matrice kad se u jediničnoj matrici zamene i -ta i j -ta vrsta.

Neka matrica $A = [a_{ij}] \neq 0$ pripada idealu I i neka je $a_{ij} \neq 0$. Tada je $B_{ii}AB_{jj} = a_{ij}B_{ij}$, pa je

$$E_{i1}B_{ii}AB_{jj}E_{j1} = E_{i1}(a_{ij}B_{ij})E_{j1} = a_{ij}B_{11} \in I.$$

Ako je b_{kl} proizvoljan element iz F , onda je i

$$E_{k1} \left(\frac{b_{kl}}{a_{ij}} E \right) (a_{ij}B_{11}) E_{l1} = b_{kl}B_{kl} \in I.$$

Kako se svaka matrica $B = [b_{ij}] \in F^{n,n}$ može prikazati u obliku

$$B = \sum_{k=1}^n \sum_{l=1}^n (b_{kl}B_{kl}),$$

a svaki sabirak na desnoj strani gornje jednakosti je iz I , dobili smo da iz pretpostavke da u I postoji matrica $A \neq 0$ sledi da je $I = F^{n,n}$.

478. Neka je R prsten sa jedinicom, I ideal u R i $I^{n,n}$ prsten matrica formata $n \times n$ sa elementima iz I .

a) Dokazati da je $I^{n,n}$ ideal u $R^{n,n}$.

b) Dokazati da je svaki ideal prstena $R^{n,n}$ oblika $I^{n,n}$ za neki ideal I iz R .

Uputstvo. b) Dokazati, koristeći se postupkom iz prethodnog zadatka, da elementi u preseku prve vrste i prve kolone svih matrica iz ideala J u $R^{n,n}$ obrazuju ideal I u R i da je $J = I^{n,n}$.

479. U prstenu matrica formata $n \times n$ nad poljem F , odrediti sve minimalne leve (desne) ideale.

Uputstvo. Skup matrica koje mogu da imaju elemente različite od nule samo u i -toj koloni je levi ideal I_i . Dokazati da za svaki levi ideal L koji sadrži matricu koja u i -toj i j -toj koloni, $i \neq j$, sadrži bar po jedan element različit od nule, važi $I_i \subseteq L$, $I_i \neq L$.

Pretpostaviti da je levi ideal $J \subseteq I_i$ i elementarnim transformacijama na vrstama, koje mogu da se realizuju množenjem odgovarajućim matricama sleva, pokazati da je $J = I_i$.

480. U prstenu $F[[x]]$ formalnih stepenih redova nad poljem F (zadatak 376) svaki nenula ideal je oblika (x^k) za neki nenegativan ceo broj k . Dokazati.

Rešenje. Neka je $f = \sum_{i=0}^{\infty} a_i x^i$ element ideala I takav da je $a_k \neq 0$, $a_i = 0$, $i = 1, 2, \dots, k-1$ i pri tom je f izabrano tako da je k najmanji među indeksima svih koeficijenata različitih od nule svih stepenih redova iz I .

Ako je $k = 0$, tj. $a_0 \neq 0$, onda f ima multiplikativan inverzni element (zadatak 441) i $I = F[[x]]$.

Ako je $k > 0$, onda je

$$f = x^k(a_k + a_{k+1}x + \dots + a_n x^{n-k} + \dots) = x^k h.$$

Element h ima multiplikativan inverzni element, pa $fh^{-1} = x^k \in I$. Lako se pokazuje da je svako $g \in I$ oblika $x^k g_1$ za neko $g_1 \in F[[x]]$, tj. $I = (x^k)$.

481. Neka je R prsten sa jedinicom. Dokazati da su sledeći uslovi ekvivalentni:

a) R je fon Nojmanov regularan prsten.

b) Svaki glavni levi ideal u R je generisan idempotentom.

c) Svaki konačno generisan levi ideal u R je generisan idempotentom.

Rešenje. a) $\Rightarrow$ b)

Neka je $I = Ra$ glavni levi ideal generisan sa $a \in R$ i neka je element $a' \in R$ takav da je $aa'a = a$. Tada je $e = a'a$ idempotent i $e \in Ra$, pa je $Re \subseteq Ra$. Iz $aa'a = a$ sledi $a \in Ra'a = Re$, pa je $Ra \subseteq Re$, dakle, $Ra = Re$.

b) $\Rightarrow$ c)

Dovoljno je da dokažemo da je svaki konačno generisani levi ideal, glavni levi ideal, a da bismo to dokazali dovoljno je dokazati da je proizvoljan levi ideal generisan sa dva elementa glavni levi ideal. Jednostavno se dokazuje da je levi ideal generisan sa $a, b \in R$ skup $Ra + Rb$.

Neka je e idempotent takav da je $Ra = Re$. Kako je

$$b = be + 1b(1 - e) \in Re + Rb(1 - e),$$

biće

$$Re + Rb(1 - e) \supseteq Ra \quad \text{i} \quad Re + Rb(1 - e) \supseteq Rb,$$

pa je

$$(1) \quad Ra + Rb \subseteq Re + Rb(1 - e).$$

Takođe je

$$(2) \quad Re \subseteq Ra + Rb,$$

a zbog $Re = Ra$ sledi da je $-be = ca$, za neko $c \in R$, pa je

$$b(1 - e) = b - be = ca + 1b \in Ra + Rb$$

i

$$(3) \quad Rb(1 - e) \subseteq Ra + Rb.$$

Iz (2) i (3) sledi

$$(4) \quad Ra + Rb \supseteq Re + Rb(1 - e),$$

a iz (1) i (4) je

$$Ra + Rb = Re + Rb(1 - e).$$

Po pretpostavci postoji idempotent f takav da je $Rb(1 - e) = Rf$, pa je $f = rb(1 - e)$ za neko $r \in R$. Prema tome,

$$fe = rb(1 - e)e = rb(e - e^2) = 0.$$

Neka je $g = (1 - e)f$. Za g važi

$$g^2 = (1 - e)f(1 - e)f = (1 - e)(f - fe)f = (1 - e)f^2 = (1 - e)f = g,$$

tj. g je idempotent, a očigledno je $ge = eg = 0$. Kako je $g \in Rf$, neposredno sledi da je $Rg \subseteq Rf$, a zbog

$$fg = f(1 - e)f = f - (fe)f = f$$

je i $Rf \subseteq Rg$, pa je $Rg = Rf$.

Dokažimo da je

$$Re + Rg = R(e + g) = Ra + Rb.$$

$R(e + g) \subseteq Re + Rg$, a zbog $eg = ge = 0$ je za svako $r, s \in R$

$$re + sg = (re + sg)(e + g) \in R(e + g)$$

tj. $Re + Rg \subseteq R(e + g)$, pa je $Re + Rg = R(e + g)$, odnosno ideal $Ra + Rb = R(e + g)$ je glavni levi ideal generisan idempotentom $e + g$ (da je $e + g$ idempotent neposredno se proverava).

$c) \Rightarrow a)$

Neka je $a \in R$ i neka je e idempotent takav da je $Ra = Re$. Tada je $e = ra$ za neko $r \in R$, pa je $ae = ara$. Iz $a = se$ za neko $s \in R$, sledi da je

$$ae = se^2 = se = a,$$

pa je konačno

$$ara = ae = a,$$

tj. R je fon Nojmanov regularan prsten.

482. Neka je R prsten bez delitelja nule u kome je svaki potprsten ideal. Dokazati da je R komutativan prsten.

Rešenje. Neka je $a \neq 0$, $a \in R$. Posmatrajmo potprsten S generisan elementom a . On je oblika

$$S = \left\{ x \in R \mid x = \sum_{i=1}^n k_i a^i, \quad k_i \in \mathbb{Z}, \quad n \in \mathbb{N} \right\}$$

i S je očigledno komutativan.

Pošto je S ideal, to je $ar \in S$ za svako $r \in R$, pa je $a(ar) = (ar)a$, tj. $a(ar - ra) = 0$. Prema tome, $ar = ra$, jer R nema delitelja nule.

483. Neka je R nula-prsten definisan u zadatku 371. Dokazati da je svaka podgrupa aditivne grupe $(R, +)$ ideal prstena R .

484. Neka su I_1 i I_2 ideali prstena R . Dokazati da su sledeći skupovi takođe ideali prstena R :

- a) $I_1 \cap I_2$,
- b) $I_1 + I_2 = \{a + b \mid a \in I_1, b \in I_2\}$,
- c) $I_1 \cdot I_2 = \{a_1 b_1 + a_2 b_2 + \dots + a_n b_n \mid a_i \in I_1, b_i \in I_2, n \in \mathbb{N}\}$,

(tj. $I_1 \cdot I_2$ je skup svih konačnih suma proizvoda $a_i b_i$, $a_i \in I_1$, $b_i \in I_2$).

485. Dokazati da u prstenu celih brojeva za svaka tri ideala I_1, I_2 i I_3 važi

- a) $I_1 \cdot (I_2 + I_3) = I_1 \cdot I_2 + I_1 \cdot I_3$,
- b) $I_1 \cap (I_2 + I_3) = (I_1 \cap I_2) + (I_1 \cap I_3)$,
- c) $(I_1 \cap I_2) \cdot (I_1 + I_2) = I_1 \cdot I_2$.

PRIMEDBA. U proizvoljnom prstenu a) važi, a b) i c) ne važe.

486. Neka je R komutativan prsten sa jedinicom a I, J i K ideali u R . Dokazati:

- a) $I \cdot J \subseteq I \cap J$.
- b) Ako je $I + J = R$, tada je $I \cdot J = I \cap J$.
- c) Ako je M maksimalan ideal i $I \not\subseteq M$, tada je $M \cdot I = M \cap I$.
- d) Ako su M_1 i M_2 različiti maksimalni ideali, tada je

$$M_1 \cdot M_2 = M_1 \cap M_2.$$

- e) $(I \cdot J) \cdot K = I \cdot (J \cdot K)$.

Rešenje. a) Neposredno sledi iz definicije ideala.

b) S obzirom na a) dovoljno je dokazati da je $I \cap J \subseteq I \cdot J$. Pošto je $I + J = R$, postoje $x_i \in I$ i $x_j \in J$ takvi da je $1 = x_i + x_j$. Neka je $r \in I \cap J$, tada je

$$r = r \cdot 1 = rx_i + rx_j.$$

$rx_j \in I \cdot J$ jer $r \in I$, a $x_j \in J$, analogno važi za $rx_i = x_i r$, pa i $r \in I \cdot J$.

c) Neposredno sledi iz b) i činjenice da je $M + I$ ideal (zadatak 484) i da iz $I \not\subseteq M$ sledi $M + I = R$, jer je M maksimalan ideal.

d) Iskoristiti c) i činjenicu da ako su M_1 i M_2 različiti maksimalni ideali tada $M_1 \not\subseteq M_2$.

487. Neka je R komutativan prsten sa jedinicom. Dokazati da je R fon Nojmanov regularan prsten ako i samo ako za svako $a \in R$ i svaki ideal I u R važi $(a) \cap I = (a) \cdot I$.

Rešenje. Neka je $(a) \cap I = (a) \cdot I$ za svaki ideal u R . Tada za ideal $I = (a)$ sledi da je $(a) = (a) \cap (a) = (a) \cdot (a) = (a^2)$ pa $a \in (a^2)$, tj. postoji $b \in R$ tako da je $a = a^2 b = aba$, jer je R komutativan prsten.

Obrnuto, neka je R fon Nojmanov regularan prsten. Kako za ideale u komutativnom prstenu uvek važi da je $(a) \cdot I \subseteq (a) \cap I$ (zadatak 486 a)) to je dovoljno dokazati da je $(a) \cap I \subseteq (a) \cdot I$. Neka je $x \in (a) \cap I$. Tada je $x = ar$, za neko $r \in R$, jer pripada idealu (a) (zadatak 395), a ako je $b \in R$ takvo da je $aba = a$ onda je

$$x = ar = abar = abx = bax \in (a) \cdot I.$$

488. Neka je R komutativan prsten sa jedinicom i I, J_1 i J_2 ideali u R takvi da je $I + J_1 = I + J_2 = R$. Dokazati da je:

$$\text{a) } I + J_1 \cdot J_2 = I + J_1 \cap J_2 = R.$$

$$\text{b) } I^n + J_1^m = R, \quad n, m \in \mathbb{N}, \quad (I^n = I \cdot I \cdot \dots \cdot I \text{ } n \text{ puta}).$$

Rešenje. a) Iz uslova zadatka sledi da postoje $a', a'' \in I$, $b'_1 \in J_1$ i $b''_2 \in J_2$ takvi da je

$$a' + b'_1 = 1 \quad \text{i} \quad a'' + b''_2 = 1,$$

pa je

$$\begin{aligned} 1 &= (a' + b'_1)(a'' + b''_2) = a'a'' + a'b''_2 + a''b'_1 + b'_1b''_2 = \\ &= a''' + b'_1b''_2 \in I + J_1 \cdot J_2, \quad a''' \in I. \end{aligned}$$

Pošto je $J_1 \cdot J_2 \subseteq J_1 \cap J_2$, sledi da je i $I + J_1 \cap J_2 = R$.

b) Koristiti indukciju po n i m .

489. Neka su u prstenu R , I_1 i I_2 ideali takvi da je

(i) $I_1 + I_2 = R$,

(ii) $I_1 \cap I_2 = \{0\}$.

Dokazati da je prsten R izomorfan sa direktnim proizvodom ideala I_1 i I_2 ,

$$(R, +, \cdot) \cong (I_1 \times I_2, +, \cdot).$$

Rešenje. Definišimo preslikavanje $f : I_1 \times I_2 \rightarrow R$ sa $f : (a_1, a_2) \mapsto a_1 + a_2$.

Zbog uslova (i) f je surjektivno preslikavanje.

Ako su $a_1, b_1 \in I_1$, $a_2, b_2 \in I_2$ takvi da je $f((a_1, a_2)) = f((b_1, b_2))$, onda je $a_1 + a_2 = b_1 + b_2$, $a_1 - b_1 = b_2 - a_2$, pa je

$$a_1 - b_1 = a_2 - b_2 \in I_1 \cap I_2.$$

Prema tome, $a_1 = b_1$, $a_2 = b_2$, pa je f injektivno preslikavanje. Dakle, f je bijekcija.

Ostaje da se dokaže da je f homomorfizam.

$$\begin{aligned} f((a_1, a_2) + (b_1, b_2)) &= f((a_1 + b_1, a_2 + b_2)) = a_1 + b_1 + a_2 + b_2 = \\ &= a_1 + a_2 + b_1 + b_2 = f((a_1, a_2)) + f((b_1, b_2)). \end{aligned}$$

Iz $I_1 \cdot I_2 \subseteq I_1 \cap I_2 = \{0\}$ (zadatak 488) sledi da je $ab = 0$ za svako $a \in I_1$ i $b \in I_2$, pa je

$$\begin{aligned} f((a_1, a_2)(b_1, b_2)) &= f((a_1b_1, a_2b_2)) = a_1b_1 + a_2b_2 = \\ &= a_1b_1 + a_1b_2 + a_2b_1 + a_2b_2 = a_1(b_1 + b_2) + \\ &+ a_2(b_1 + b_2) = (a_1 + a_2)(b_1 + b_2) = f((a_1, a_2))f((b_1, b_2)). \end{aligned}$$

Dakle, f je izomorfizam prstena R i direktnog proizvoda $I_1 \times I_2$.

490. Neka su R_1 i R_2 prsteni sa jedinicom. Dokazati da je u prstenu $R_1 \times R_2$ (zadatak 380) podskup I ideal ako i samo ako je $I = I_1 \times I_2$, gde je I_1 ideal prstena R_1 , a I_2 ideal prstena R_2 .

491. Neka je R komutativan prsten sa jedinicom koji je direktan proizvod konačnog broja polja.

Dokazati da prsten R ima konačno mnogo ideala.

492. Neka je I ideal komutativnog prstena sa jedinicom R . Dokazati da je skup $S = 1 + I$ multiplikativno zatvoren.

493. Neka je R komutativan prsten sa jedinicom i $S_1 \subseteq S_2$ dva multiplikativno zatvorena skupa R . Dokazati da je

$$S_1^{-1}(S_2^{-1}R) = S_2^{-1}(S_1^{-1}R) = S_2^{-1}R.$$

($S^{-1}R$ je definisano u 2.58).

494. Neka je S multiplikativno zatvoren skup komutativnog prstena R , a I i J ideali u R .

Dokazati:

(i) $S^{-1}I + \{x \mid x = a/s, a \in I, s \in S\}$ je ideal u $S^{-1}R$ (2.58),

(ii) $S^{-1}(I + J) = S^{-1}I + S^{-1}J$,

(iii) $S^{-1}(I \cdot J) = (S^{-1}I) \cdot (S^{-1}J)$,

(iv) $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$.

Uputstvo. Koristiti

$$\sum_{i=1}^n (c_i/s) = (\sum_{i=1}^n c_i)/s, \quad \sum_{i=1}^n (a_i b_i/s) = \sum_{i=1}^n (a_i/s)(b_i/s),$$

$$\sum_{i=1}^n (c_i/s_i) = (\sum_{i=1}^n c_i s_1 \dots s_{i-1} s_{i+1} \dots s_k) / s_1 s_2 \dots s_k.$$

2.5 Maksimalni i prosti ideali

495. U prstenu celih brojeva $\mathbb{Z}$ odrediti sve maksimalne ideale.

Rezultat. Ideal I je maksimalan ako i samo ako je $I = (p)$, gde je p prost broj.

496. Neka je R komutativan prsten sa jedinicom, a M njegov ideal. Dokazati da je M maksimalan ideal ako i samo ako je R/M polje.

Rešenje. Neka je M maksimalan ideal prstena R i neka je $a \in R$, $a \notin M$. Jednostavno se proverava da je skup $M + aR$ svih elemenata oblika $m + ax$, $m \in M$, $x \in R$, ideal u R . Taj ideal sadrži M i $a \notin M$, pa kako je M maksimalan ideal sledi da je konstruisani ideal ceo prsten R . Tom idealu pripada i jedinica, pa je za neko $b \in R$

$$1 = m + ab.$$

To znači da je u faktor prstenu R/M ,

$$(a + M)(b + M) = ab + M = 1 - m + M = 1 + M.$$

Dakle, u R/M za bilo koji suskup $a + M \neq M$ postoji multiplikativni inverzni element $b + M$, R/M je komutativan prsten sa jedinicom (jer je R komutativan prsten sa jedinicom), pa je R/M polje.

Obrnuto, pretpostavimo da je R/M polje. Ako M nije maksimalan ideal postoji ideal I različit od M i R koji sadrži M . Ako je a proizvoljan element iz R , a b proizvoljan element iz $I \setminus M$, onda, s obzirom da je R/M polje, postoji suskup $x + M$ takav da je

$$a + M = (b + M)(x + M).$$

Odavde je

$$a - bx \in M,$$

a kako je $M \subseteq I$, sledi da $a - bx \in I$. Međutim, $b \in I$, pa odatle sledi $a \in I$, tj. $I = R$, što je kontradikcija. Prema tome, M je maksimalan ideal.

497. U komutativnom prstenu sa jedinicom R pravi ideal M je maksimalan ako i samo ako za svako $r \notin M$ postoji $x_r \in R$ tako da je $1 + rx_r \in M$. Dokazati.

Rešenje. Neka je M maksimalan ideal. Tada je za $r \notin M$, $M + rR = R$, jer je $M + rR$ ideal koji strogo sadrži M . Tada je za neko $m \in M$ i $x \in R$, $m + rx = 1$, pa je za $x_r = -x$, $1 + rx_r \in M$.

Obrnuto, ako za svako $r \notin M$ postoji $x_r \in R$ takvo da je $1 + rx_r = m \in M$, tada ideal $M + rR$ sadrži 1, pa je $M + rR = R$ na osnovu zadatka 471. Dakle, ako $M \subseteq I$ i $M \neq I$, onda za $R \in I \setminus M$, $rR \subseteq I$ i $M + rR \subseteq I$, tj. $I = R$, pa je M maksimalan ideal.

498. Neka je P pravi ideal komutativnog prstena R . Dokazati da su sledeći uslovi ekvivalentni:

(i) Za svako $a, b \in R$ iz $ab \in P$ sledi $a \in P$ ili $b \in P$.

(ii) Za svaka dva ideala A, B prstena R iz $A \cdot B \subseteq P$ sledi $A \subseteq P$ ili $B \subseteq P$ (v. 2.36 i 2.37).

Rešenje. (i) $\Rightarrow$ (ii) Neka $AB \subseteq P$, ali $A \not\subseteq P$ i $B \not\subseteq P$. Tada postoje $a \in A \setminus P$ i $b \in B \setminus P$, pa zbog (i) $ab \notin P$, no $ab \in AB \subseteq P$, što je kontradikcija.

(ii) $\Rightarrow$ (i) Ako $ab \in P$, tada i $(a)(b) \subseteq P$. Zbog (ii) $(a) \subseteq P$ ili $(b) \subseteq P$, pa $a \in P$ ili $b \in P$ jer $a \in (a)$ i $b \in (b)$.

499. U komutativnom prstenu sa jedinicom, pravi ideal I je prost ako i samo ako je skup $R \setminus I$ multiplikativno zatvoren.

500. Dokazati da je ideal P komutativnog prstena sa jedinicom R prost, ako i samo ako je R/P domen integriteta.

Rešenje. Neka je P prost ideal i neka su $\bar{a}, \bar{b} \in R/P$, $\bar{a} \neq \bar{0}$, $\bar{b} \neq \bar{0}$. Ako je $\bar{a} = a + P$, $\bar{b} = b + P$, pošto je $\bar{a} \neq \bar{0}$ i $\bar{b} \neq \bar{0}$, sledi $a \notin P$ i $b \notin P$. Tada $ab \notin P$, jer je P prost ideal, pa je $\bar{a}\bar{b} \neq \bar{0}$ (videti prethodni zadatak).

Obrnuto, ako je $\bar{a}\bar{b} = \bar{0}$, a $\bar{a} \neq \bar{0}$, $\bar{b} \neq \bar{0}$, to znači da $a \notin P$, $b \notin P$, a $ab \in P$, tj. P nije prost ideal.

501. Dokazati da je u komutativnom prstenu sa jedinicom svaki maksimalan ideal prost.

502. Dokazati da je u domenu integriteta R u kome su svi ideali glavni, svaki prost nenula ideal maksimalan.

Rešenje. Neka je $(x) \neq 0$ prost ideal i $(y) \supseteq (x)$, $(y) \neq (x)$. $x \in (y)$, tj. $x = yz$, a tada i $yz \in (x)$, pa pošto je (x) prost ideal (2.37) to ili $y \in (x)$ ili $z \in (x)$.

Pošto $y \notin (x)$, jer (y) strogo sadrži (x) , to $z \in (x)$ i neka je $z = vx$. Tada je

$$x = yz = yvx,$$

tj.

$$x(1 - yv) = 0.$$

R je domen integriteta pa je $yv = 1$, tj. y ima multiplikativni inverzni element, pa je $(y) = R$.

503. Neka je R domen integriteta u kome svaki skup S ideala sadrži ideal I takav da nijedan drugi ideal $J \in S$ nije sadržan u I (ideal I nazivamo minimalni element skupa S). Dokazati da je R polje.

Rešenje. Neka je $a \in R$, $a \neq 0$. Posmatrajmo skup ideala

$$\{(a), (a^2), \dots, (a^n), \dots\}$$

Očigledno važi $(a) \supseteq (a^2) \supseteq \dots \supseteq (a^n) \supseteq \dots$. Neka je (a^k) minimalni među njima. Tada je $(a^k) \supseteq (a^{k+1})$, međutim, zbog minimalnosti ideala (a^k) mora biti $(a^k) = (a^{k+1})$. Odatle je $a^k = a^{k+1}r$, za neko $r \in R$, pa je $a^k(1-ra) = 0$. R je domen integriteta, pa je $ra = 1$, tj. a ima multiplikativni inverzni element. Prema tome, R je polje.

504. Neka je R komutativan prsten sa jedinicom u kome svaki skup ideala ima minimalan element u odnosu na inkluziju (v. prethodni zadatak). Dokazati da je u R svaki prost ideal maksimalan.

Uputstvo. Dokazati da se uslov o maksimalnosti očuvava u faktor prstenu, formirati faktor prsten R/P , gde je P prost ideal. R/P je domen integriteta (2.54), a na osnovu prethodnog zadatka R/P je polje, pa je zbog zadatka 496 P maksimalan ideal.

505. Neka je R domen integriteta sa konačnim brojem ideala. Dokazati da je R polje.

Uputstvo. Ako je broj ideala u R konačan, tada svaki skup ideala ima minimalan element. Primeniti zadatak 503.

506. Neka je R komutativan prsten sa jedinicom u kome je svaki ideal prost. Dokazati da je R polje.

Rešenje. $(0) = \{0\}$ je prost ideal po pretpostavci, pa iz $ab = 0$ sledi $a = 0$ ili $b = 0$, tj. R je domen integriteta.

Za $a \neq 0$ (a^2) je prost ideal, pa iz $aa = a^2 \in (a^2)$ sledi $a \in (a^2)$. Znači da postoji $x \in R$ takvo da je $a = a^2x$ tj. $a(1-ax) = 0$. R nema delitelje nule, pa je $1-ax = 0$, tj. $ax = 1$ i $x = a^{-1}$.

507. Neka je R komutativan prsten sa jedinicom čija je svaka homomorfna slika domen integriteta. Dokazati da je R polje.

Uputstvo. Koristiti prethodni zadatak, činjenicu da je svaka homomorfna slika prstena R izomorfna faktor prstenu R/I i zadatak 500.

508. Neka je R komutativan prsten i neka su $I_1, I_2, \dots, I_n$ ideali u R , a P prost ideal u R . Dokazati da iz

$$P \supseteq \bigcap_{i=1}^n I_i \quad \text{sledi} \quad P \supseteq I_k, \quad \text{za neko } k = 1, 2, \dots, n.$$

Rešenje. Neka za svako $k = 1, 2, \dots, n$ $I_k \not\subseteq P$, tada postoje $x_k \in I_k$ takvi da je $x_k \notin P$ za $k = 1, 2, \dots, n$. Ali tada

$$x_1 x_2 \dots x_n \in I_1 \cdot I_2 \cdot \dots \cdot I_n \subseteq \bigcap_{i=1}^n I_i \subseteq P,$$

pa pošto je P prost ideal mora biti neki $x_k \in P$, što je kontradikcija.

509. Neka je R komutativan prsten sa jedinicom, I proizvoljan ideal u R , a $P_1, P_2, \dots, P_n$ prosti ideali u R . Dokazati da iz

$$I \subseteq \bigcup_{i=1}^n P_i \text{ sledi } I \subseteq P_j, \text{ za neko } j \in \{1, 2, \dots, n\}.$$

Rešenje. Dokaz ćemo dati indukcijom po broju n prostih ideala.

Za $n = 1$ je tvrđenje očigledno tačno.

Pretpostavimo da je tvrđenje tačno za $n - 1$ i neka je $I \subseteq \bigcup_{i=1}^n P_i$. Pretpostavimo sada da je za svako $j = 1, 2, \dots, n$

$$I \not\subseteq P_1 \cup \dots \cup P_{j-1} \cup P_{j+1} \cup \dots \cup P_n = \bigcup_{\substack{i=1 \\ i \neq j}}^n P_i.$$

Neka je $a_j \in I \setminus \bigcup_{\substack{i=1 \\ i \neq j}}^n P_i$, $j = 1, 2, \dots, n$, a kako $I \subseteq \bigcup_{i=1}^n P_i$ sledi da

$a_j \in P_j$. Posmatrajmo element $z = a_1 + a_2 a_3 \dots a_n \in I \subseteq \bigcup_{i=1}^n P_i$. Pošto $x \in \bigcup_{i=1}^n P_i$, postoji $j \in \{1, 2, \dots, n\}$ tako da je $x \in P_j$.

Ako je $j = 1$ tada $a_2 a_3 \dots a_n = x - a_1 \in P_1$, a pošto je P_1 prost ideal sledi da za neko $k \in \{2, \dots, n\}$ $a_k \in P_1$, što protivreči izboru $a_1, \dots, a_n$.

Ako je $j > 1$, tada $a_1 = x - a_2 a_3 \dots a_n \in P_j$, što je takođe kontradikcija.

Iz ovih protivrečnosti sledi da pretpostavka za svako $j = 1, 2, \dots, n$ $I \not\subseteq \bigcup_{\substack{i=1 \\ i \neq j}}^n P_i$ nije tačna. Prema tome, za neko $j \in \{1, 2, \dots, n\}$ je $I \subseteq \bigcup_{\substack{i=1 \\ i \neq j}}^n P_i$, tj.

I je sadržano u uniji $(n-1)$ -og prostog ideala, pa po indukcijskoj pretpostavci I je sadržano u nekom od tih ideala. Dakle, iz pretpostavke da tvrđenje važi za $n - 1$ dokazali smo da važi za n , pa je time dokaz dovršen.

PRIMEDBA. Za $n = 2$ ne mora da se pretpostavi da su ideali P_1 i P_2 prosti.

510. Neka je u komutativnom prstenu sa jedinicom R , P prost ideal takav da je R/P konačan prsten. Dokazati da je P maksimalan ideal.

Uputstvo. Koristiti zadatke 415 i 500.

511. Neka je R komutativan prsten sa jedinicom takav da za svako $x \in R$ važi $x^n = x$, gde prirodan broj n zavisi od x .

Dokazati da je u prstenu R svaki prost i ideal maksimalan.

Rešenje. Neka je I prost ideal u R . Tada je R/I domen integriteta (zadatak 500). Označimo sa f prirodni homomorfizam $f : R \rightarrow R/I$. Neka je $x \in R$ proizvoljan element takav da je $f(x) \neq 0$ (sa 0 označavamo neutralni element u prstenu R/I , tj. klasu I). U R/I će takođe važiti $(f(x))^n = f(x)$, pa je $f(x)((f(x))^{n-1} - 1) = 0$.

Pošto je R/I domen integriteta i $f(x) \neq 0$ sledi da je $(f(x))^{n-1} - 1 = 0$, pa je za $n > 2$ $f(x)((f(x))^{n-2} - 1) = 0$, tj. $(f(x))^{n-2}$ je multiplikativni inverzni element za $f(x)$ i R/I je polje. Ako je $n = 2$, tada je $f(x) = 1$, pa je i $(f(x))^{-1} = f(x)$ i R/I je opet polje. Na osnovu zadatka 496 sledi da je I maksimalan ideal, što je trebalo dokazati.

(Za prirodni homomorfizam $f : R \rightarrow R/I$ je $f(x) = 0 \iff x \in I$, pa ne može biti za svako $x \in R$ $f(x) = 0$, jer bi to značilo da je $I = R$, a u definiciji prostog ideala se zahteva da je $I \neq R$.)

PRIMEDBA. Da bi se pojednostavilo rešenje ovog zadatka data je pretpostavka da je R komutativan prsten. Međutim, ova pretpostavka je suvišna s obzirom na teoremu N. Džekobsona (N. Jacobson): ako za svaki element x prstena postoji prirodan broj $n(x) > 1$ takav da je $x^{n(x)} = x$, onda je prsten komutativan.

Literatura:

I. Herstein, *An elementary proof of a theorem of Jacobson*, Duke Math. Journal, 21 (1954), 45-48.

512. Neka je $\mathbb{Z}[x]$ prsten polinoma sa celim koeficijentima i p prost broj. Dokazati:

- a) Ideal I generisan sa x i p nije glavni.
- b) I je maksimalan ideal.

c) Glavni ideal (p) je prost, a nije maksimalan.

513. Neka je R komutativan prsten sa jedinicom, a I maksimalan ideal u R .

Dokazati da prsten R/I^k , $k \in \mathbb{N}$, ima tačno jedan maksimalan ideal i to je ideal I/I^k . ($I^k = I \cdot I \cdot \dots \cdot I$, k puta).

Rešenje. Iz definicije ideala neposredno sledi $I \supseteq I^k$. S obzirom na 2.53 dovoljno je dokazati da ne postoji drugi maksimalan ideal u R , različit od I , koji sadrži I^k . Neka je J , $J \neq I$, maksimalan ideal u R koji sadrži I^k . Pošto je maksimalan ideal u komutativnom prstenu prost (zadatak 501) iz karakterizacije prostog ideala (zadatak 498) sledi da je $I \subseteq J$, pa je $I = J$.

514. Neka je R prsten sa jedinicom koji ima tačno jedan maksimalan levi ideal M . Dokazati:

a) M je skup svih elemenata iz R koji nemaju levi multiplikativni inverzni element.

b) Nijedan element iz M nema desni multiplikativni inverzni element.

Rešenje. a) Nijedan element iz M nema levi multiplikativni inverzni element, jer $1 \notin M$. Obrnuto, ako x iz R nema levi multiplikativni inverzni element, tada je $Rx \neq R$, pa je $Rx \subseteq M$ jer se svaki levi ideal sadrži u nekom maksimalnom levom idealu (2.26). No tada je i $1x = x \in M$, pa je M skup svih elemenata iz R koji nemaju leve multiplikativne inverzne elemente.

b) Pretpostavimo da je $xy = 1$ za $x \in M$ i $y \in R$. Tada je

$$(1 - yx)y = y - y(xy) = y - y = 0.$$

S druge strane, $yx \in M$, pa $1 - yx \notin M$ (jer bi inače $yx + (1 - yx) = 1$ pripadalo M), a to znači da $1 - yx$ ima levi multiplikativni inverzni element z . Odatle sledi

$$y = z(1 - yx)y = z0 = 0,$$

što je protivrečno sa $xy = 1$, pa nijedan element $x \in M$ nema desni multiplikativni inverzni element.

PRIMEDBA. Analogno se dokazuju odgovarajuća tvrđenja za desne ideale.

515. Dokazati da prsten sa jedinicom R ima jedinstven maksimalan levi ideal M ako i samo ako je $R \setminus M$ skup svih invertibilnih elemenata u R .

Rešenje. Neka R ima jedinstveni maksimalan levi ideal M i neka je $x \notin M$. Tada, na osnovu prethodnog zadatka, postoji $y \in R$ takvo da je $yx = 1$.

Bar jedan od elemenata xy ili $1 - xy$ ima levi inverzni element, jer bi inače oba pripadala idealu M , pa bi i njihov zbir pripadao M , tj. $1 \in M$, što je protivrečnost. (Iz $1 \in M$ sledi $M = R$ (zadatak 471), a kako je M maksimalan levi ideal mora biti $M \neq R$). $1 - xy$ ne može imati levi multiplikativni inverzni element s , jer bismo imali $s(1 - xy) = 1$, a tada je

$$x = s(1 - xy)x = sx - sx(yx) = sx - sx \cdot 1 = 0 \in M,$$

što protivreči pretpostavci $x \notin M$. Dakle, postoji $z \in R$ tako da je $zxy = 1$, pa je $zxyx = x$, tj. $x = zx(yx) = zx \cdot 1 = zx$, što konačno daje $xy = 1$, pa je x invertibilan element. Na osnovu prethodnog zadatka, u M nema invertibilnih elemenata, pa je $R \setminus M$ skup svih invertibilnih elemenata.

Obrnuto, neka levi ideal M ima osobinu da je $R \setminus M$ skup svih invertibilnih elemenata. Tada iz $J \not\subseteq M$ za neki levi ideal J , sledi da je $J = R$, jer J sadrži element $x \notin M$ tj. invertibilan element (zadatak 472). Prema tome, sem M drugih pravih levih ideala (koji nisu sadržani u M) nema u R , pa je M jedinstven maksimalan levi ideal.

PRIMEDBA. Analogno se dokazuje odgovarajuće tvrđenje za desne ideale.

516. Neka je R prsten sa jedinicom koji ima jedinstven maksimalan levi ideal M . Dokazati:

a) M je dvostrani ideal koji sadrži sve prave leve i sve prave desne ideale prstena R .

b) R/M je telo.

Rešenje. a) Za proizvoljno $r \in R$, Mr je levi ideal, pa pošto je M jedinstven maksimalan levi ideal mora biti $Mr \subseteq M$, tj. M je dvostrani ideal. Preostaje još da dokažemo da M sadrži sve prave desne ideale prstena R .

Ako je I pravi desni ideal u R , onda nijedan element iz I ne može imati desni multiplikativni inverzni element (jer bi na osnovu zadatka 472 bilo $I = R$), a to znači ni multiplikativni inverzni element. Na osnovu prethodnog zadatka sledi da je $I \subseteq M$.

b) Neka je $x + M \in R/M$, $x + m \neq 0 + M = M$, pa $x \notin M$. Na osnovu

zadatka 515 x ima multiplikativni inverzni element y , pa je

$$(x + M)(y + M) = xy + M = 1 + M,$$

što znači da je R/M telo.

517. Neka je R prsten sa jedinicom u kome postoji jedinstven maksimalan ideal M . Dokazati da su u prstenu R jedini idempotenti 0 i 1.

Rešenje. Neka je e idempotent različit od 0 i 1. Tada je $e(1 - e) = 0$, pa su e i $e - 1$ delitelji nule, tj. ideali (e) i $(1 - e)$ su netrivialni ideali prstena R . Svaki pravi ideal je sadržan u maksimalnom idealu (2.35), pa se e i $1 - e$ sadrže u M , jer je M jedinstveni maksimalan ideal. To znači da je $1 = e + (1 - e) \in M$, što je protivrečnost, jer je M pravi ideal u R .

518. Neka je R komutativan prsten sa jedinicom, P prost ideal u R . Dokazati da $S^{-1}R$ ima jedinstven maksimalan ideal $S^{-1}P$, ako je $S = R \setminus P$.

519. Neka je R prsten sa jedinicom u kome zbir dva elementa koji nemaju multiplikativne inverzne elemente takođe nema multiplikativan inverzni element. Dokazati da R ima jedinstven maksimalan levi ideal.

520. Neka je R prsten sa jedinicom koji ima tačno jedan maksimalan levi ideal M . Dokazati da su u R jedini idempotenti 0 i 1.

Rešenje. Neka je $a \in R$, $a \neq 0$, $a \neq 1$, idempotent. Tada je i $1 - a$ takođe idempotent: $(1 - a)^2 = 1 - 2a + a = 1 - a$. Takođe je $a(1 - a) = 0$, tj. a i $1 - a$ su delitelji nule, pa a i $1 - a$ nemaju multiplikativne inverzne elemente. Na osnovu zadatka 515 sledi da $a \in M$ i $1 - a \in M$, pa je i $1 = a + (1 - a) \in M$, tj. $M = R$, što je protivrečnost.

521. Neka je M maksimalan ideal u komutativnom prstenu sa jedinicom R u kome za svako $x \in M$, $1 + x$ ima multiplikativan inverzni element. Dokazati da je M jedinstven maksimalan ideal.

Rešenje. Ako $y \in R \setminus M$, tada je $M + yR = R$ jer je M maksimalan ideal, pa je $x + yt = 1$ za neko $t \in R$, odnosno $yt = 1 - x = 1 + (-x)$. Prema tome, yt ima multiplikativni inverzni element y' , pa je ty' multiplikativni inverzni element za y . Dakle, svaki element iz $R \setminus M$ je invertibilan. U M nema invertibilnih elemenata (jer bi u tom slučaju bilo $M = R$), pa je $R \setminus M$ skup svih invertibilnih elemenata. Na osnovu zadatka 515 M je jedinstven maksimalan ideal.

522. Neka je $F[[x]]$ prsten formalnih stepenih redova nad poljem F (zadatak 376). Dokazati da $F[[x]]$ ima jedinstven maksimalan ideal.

Uputstvo. Koristiti zadatak 480.

2.6 Prsten polinoma

523. Ispitati svodljivost sledećih polinoma nad poljem racionalnih brojeva $\mathbb{Q}$:

$$\begin{array}{ll} a) & x^2 + 4x + 2, \\ c) & x^4 - 10x^2 + 1, \\ e) & x^3 + 3x^2 + 6x + 3, \end{array} \quad \begin{array}{ll} b) & x^3 - x^2 - 4, \\ d) & 4x^3 - 2x^2 + x + 1, \\ f) & x^{50} + 14x - 56. \end{array}$$

Rešenje. a) Ako je polinom drugog stepena svodljiv nad nekim poljem, tada je on proizvod dva linearna polinoma sa koeficijentima iz tog polja, tj. on ima nulu u datom polju. Međutim, $x^2 + 4x + 2$ nema racionalne nule, pa je, prema tome, nesvodljiv nad poljem $\mathbb{Q}$.

b) Slično, ako je polinom trećeg stepena svodljiv nad nekim poljem onda on mora imati bar jedan linearan faktor, tj. bar jednu nulu u tom polju. Jedine moguće racionalne nule polinoma $x^3 - x^2 - 4$ su faktori broja 4, tj. $\pm 1, \pm 2, \pm 4$. Proverom utvrđujemo da je $x_1 = 2$ nula datog polinoma, koji je, prema tome, svodljiv nad $\mathbb{Q}$

$$x^3 - x^2 - 4 = (x - 2)(x^2 + x + 2).$$

c) Ako je polinom četvrtog stepena svodljiv nad nekim poljem, onda postoje dve mogućnosti. Ili dati polinom ima jedan linearan faktor sa koeficijentima iz polja (a to znači da ima nulu u datom polju) ili je jednak proizvodu dva nesvodljiva kvadratna polinoma.

± 1 nisu nule datog polinoma, pa on nema racionalne nule. Prema tome, ako je dati polinom svodljiv, on je proizvod dva polinoma drugog stepena:

$$x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d),$$

gde su $a, b, c, d \in \mathbb{Z}$ (poznato je da ako se polinom čiji su koeficijenti celi brojevi može rastaviti u proizvod polinoma sa racionalnim koeficijentima, onda se on može rastaviti i u proizvod polinoma sa celim koeficijentima). Odatle je

$$a + c = 0, \quad b + ac + d = -10, \quad bc + ad = 0, \quad bd = 1.$$

Iz ovog sistema jednačina lako se dobija da mora biti ili $a^2 = 10 \pm 2$, međutim takav ceo broj a ne postoji, ili je $a = 0$ i $b^2 + 10b + 1 = 0$, što takođe nema rešenje u $\mathbb{Z}$, pa, prema tome, dati polinom je nesvodljiv nad $\mathbb{Q}$.

d) Polinom je nesvodljiv nad $\mathbb{Q}$.

e) Prost broj 3 je delitelj svih koeficijenata polinoma sem vodećeg, 3^2 nije delitelj slobodnog člana, pa je dati polinom nesvodljiv nad $\mathbb{Q}$ na osnovu Ajzenštajnovog kriterijuma (2.71).

f) Nesvodljiv na osnovu Ajzenštajnovog kriterijuma.

524. Polinome

$$f(x) = x^4 - 1 \quad \text{i} \quad g(x) = 4x^5 + 4x^4 - 13x^3 - 11x^2 + 10x + 6$$

rastaviti u proizvod nesvodljivih polinoma nad poljem

a) $\mathbb{Q}$, b) $\mathbb{R}$, c) $\mathbb{C}$.

Rezultat.

$$f(x) = (x-1)(x+1)(x^2+1) \quad \text{nad } \mathbb{Q} \text{ i } \mathbb{R},$$

$$f(x) = (x-1)(x+1)(x+i)(x-i) \quad \text{nad } \mathbb{C}.$$

$$g(x) = (x-1)(2x+1)(2x+3)(x^2-2) \quad \text{nad } \mathbb{Q},$$

$$g(x) = (x-1)(2x+1)(2x+3)(x-\sqrt{2})(x+\sqrt{2}) \quad \text{nad } \mathbb{R} \text{ i } \mathbb{C}.$$

525. Ispitati svodljivost polinoma:

a) $\bar{1}x^3 + \bar{1}x + \bar{1}$,

b) $\bar{2}x^3 + \bar{3}x^2 + \bar{2}x + \bar{3}$

nad poljem $\mathbb{Z}_5$.

Rezultat. a) Nesvodljiv, b) svodljiv.

526. Nad poljem $\mathbb{Z}_5$ polinom $\bar{3}x^3 + \bar{4}x^2 + \bar{3}$ se može rastaviti u proizvod nesvodljivih polinoma na „dva” načina

$$\bar{3}x^3 + \bar{4}x^2 + \bar{3} = (\bar{1}x + \bar{2})^2(\bar{3}x + \bar{2}) = (\bar{1}x + \bar{2})(\bar{1}x + \bar{4})(\bar{3}x + \bar{1}).$$

Objasniti zašto ovo ne protivreči teoremi o jedinstvenoj faktORIZACIJI.

Rešenje. Poznato je da se polinom $f(x)$ nad poljem F može na jedinstven način prikazati kao proizvod nesvodljivih normalizovanih polinoma nad F (tj. polinoma čiji su vodeći koeficijenti jedinice).

Kako je

$$\overline{3}x + \overline{1} = \overline{3}(\overline{1}x + \overline{2}),$$

a

$$\overline{3}x + \overline{2} = \overline{3}(\overline{1}x + \overline{4}),$$

vidimo da se u oba slučaja radi o istoj faktorizaciji:

$$\overline{3}x^3 + \overline{4}x^2 + \overline{3} = \overline{3}(\overline{1}x + \overline{2})^2(\overline{1}x + \overline{4}).$$

527. Primerom pokazati da algoritam deljenja (opisan u 2.68) za polinome $f, h \in R[x]$, gde je R prsten sa jedinicom, ne važi ako vodeći koeficijent polinoma h nije invertibilan element u R .

Rešenje. Neka je $R = \mathbb{Z}$ i $f(z) = x^2$, $h(x) = 2x$ i pretpostavimo da je

$$x^2 = q(x) \cdot 2x + r(x)$$

gde je $\deg r(x) < 1$ ili je $r(x) = 0$. Pošto je $\mathbb{Z}$ domen integriteta mora biti $\deg q(x) = 1$, pa je $q(x) = ax + b$, $a, b \in \mathbb{Z}$, i

$$x^2 = (ax + b) \cdot 2x + r(x).$$

Oдавde sledi da je $2a = 1$, što je protivrečnost jer je a ceo broj.

528. Ako je polinom $p(x)$ nesvodljiv nad poljem F , onda je i polinom $p(x + a)$, za svako $a \in F$, nesvodljiv nad F . Dokazati.

Rešenje. Pretpostavimo da je $p(x + a)$ svodljiv nad F ,

$$p(x + a) = q(x)s(x),$$

gde su $q(x)$ i $s(x)$ polinomi pozitivnog stepena. Ako u gornju jednakost stavimo $x - a$ umesto x , biće

$$p(x) = q(x - a)s(x - a),$$

a polinomi $q(x - a)$ i $s(x - a)$ su pozitivnog stepena, tj. $p(x)$ je svodljiv. Iz ove protivrečnosti sledi da je $p(x + a)$ nesvodljiv nad F .

529. Odrediti za koji racionalan broj a je polinom $x^4 + a$ nesvodljiv nad poljem $\mathbb{Q}$.

Rezultat. Sličnim postupkom kao u zadatku 523 c) se dobija da je $x^4 + a$ nesvodljiv na $\mathbb{Q}$ ako i samo ako je $a \neq -b^2$ i $a \neq \frac{c^2}{4}$, $b, c \in \mathbb{Q}$.

530. Rešiti jednačinu

$$ax^4 + bx^3 + cx^2 + bx + a = 0$$

nad poljem kompleksnih brojeva $\mathbb{C}$ ($a \neq 0$).

Uputstvo. Koristeći smenu $y = x + \frac{1}{x}$ ($y^2 = x^2 + \frac{1}{x^2} + 2$) i deleći jednačinu sa x^2 (pokazati da $x = 0$ nije rešenje) dobija se

$$a(y^2 - 2) + by + c = 0.$$

531. Rastaviti u proizvod nesvodljivih činilaca nad poljem $\mathbb{R}$

$$\begin{array}{ll} \text{a)} & x^4 + 1, \quad \text{c)} \quad x^4 + 4x^3 + 8x^2 + 4x + 1, \\ \text{b)} & x^4 + x^2 + 1, \quad \text{d)} \quad x^4 + x^3 + x^2 + x + 1. \end{array}$$

Rezultat.

$$\begin{array}{l} \text{a)} \quad x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1), \\ \text{b)} \quad x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1), \\ \text{c)} \quad x^4 + 4x^3 + 8x^2 + 4x + 1 = \\ = (x^2 + (2 + \sqrt{2})x + 3 + 2\sqrt{2})(x^2 + (2 - \sqrt{2})x + 3 - 2\sqrt{2}), \\ \text{d)} \quad x^4 + x^3 + x^2 + x + 1 = (x^2 + \frac{1 + \sqrt{5}}{2}x + 1)(x^2 + \frac{1 - \sqrt{5}}{2}x + 1). \end{array}$$

532. Dat je polinom $p(x) = x^5 - 209x + 56$ nad poljem racionalnih brojeva $\mathbb{Q}$. Ako se zna da $p(x)$ ima realne nule x_1 i $\frac{1}{x_1}$ faktorizovati $p(x)$ nad $\mathbb{Q}$.

Rešenje. Podelimo $p(x)$ sa $(x - x_1)(x - \frac{1}{x_1}) = x^2 - \lambda x + 1$ gde je $\lambda = x_1 + \frac{1}{x_1}$ i izjednačimo ostatak sa nulom. Dobija se

$$(\lambda^4 - 3\lambda^2 - 208)x + \lambda^3 - 2\lambda + 56 = 0,$$

a odatle je

$$(*) \quad \lambda^4 - 3\lambda^2 - 208 = 0 \quad \text{i} \quad \lambda^3 - 2\lambda - 56 = 0.$$

Ako drugu jednačinu pomnožimo sa λ i oduzmemo od prve (očigledno je $\lambda \neq 0$), dobijamo

$$\lambda^2 - 56\lambda + 208 = 0.$$

Rešenja poslednje jednačine su $\lambda_1 = 4$ i $\lambda_2 = 52$, od kojih jedino $\lambda = 4$ zadovoljava obe jednačine (*), pa je

$$p(x) = (x^2 - 4x + 1)(x^3 + 4x^2 + 15x + 56).$$

533. Dat je polinom

$$p(x, y) = ax^2 + 2bxy + cy^2 + 2dx + 2ey + f$$

sa realnim koeficijentima.

Koji uslov moraju da zadovoljavaju koeficijenti polinoma $p(x, y)$ da se $p(x, y)$ može rastaviti u proizvod dva linearna faktora u $\mathbb{R}[x, y]$?

Rešenje. Da bi se $p(x, y)$ mogao rastaviti u proizvod dva linearna faktora u $\mathbb{R}[x, y]$ potrebno je i dovoljno da kvadratna jednačina po x

$$ax^2 + 2(by + d)x + cy^2 + 2ey + f = 0$$

čiji su koeficijenti iz $\mathbb{R}[y]$ ima rešenja u $\mathbb{R}[y]$, tj. da je diskriminanta tačan kvadrat:

$$4((by + d)^2 - a(cy^2 + 2ey + f)) = (k(y))^2, \quad k(y) \in \mathbb{R}[y],$$

tj.

$$(b^2 - ac)y^2 + 2(bd - ae)y + d^2 - af = \left(\frac{k(y)}{2}\right)^2.$$

Ovaj kvadratni trinom po y će biti tačan kvadrat ako samo ako je njegova diskriminanta jednaka nuli, što nam daje ekvivalentan uslov

$$(bd - ae)^2 - (b^2 - ac)(d^2 - af) = 0.$$

534. Koji uslov moraju da zadovoljavaju koeficijenti polinoma

$$x^4 + ax^3 + bx^2 + cx + d \in \mathbb{R}[x]$$

da se smenom $x = y + h$ dobije polinom oblika

$$y^4 + py^2 + q.$$

Rezultat. $8c = (4b - a^2)a$.

535. Neka su $f(x), g(x) \in F[x]$, $a \in F$, gde je F polje. Dokazati:

a) $(f(x) + g(x))' = f'(x) + g'(x)$,

b) $(af(x))' = af'(x)$,

c) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$,

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

536. Neka je a nula polinoma $f(x) \in F[x]$, gde je F polje. a je višestruka nula polinoma $f(x)$ ako i samo ako je $f'(x) = 0$. Dokazati.

Rešenje. Neka je $f(a) = f'(a) = 0$. To znači da je $f(x)$ deljiv sa $x - a$, pa je

$$f(x) = (x - a)q(x).$$

Odatle je

$$f'(x) = q(x) + (x - a)q'(x),$$

odnosno

$$f'(a) = q(a) = 0.$$

Dakle, a je nula polinoma $q(x)$, a to znači da je a višestruka nula polinoma $f(x)$.

Pretpostavimo da je a višestruka nula polinoma $f(x)$. Tada je

$$f(x) = (x - a)q(x), \quad q(a) = 0,$$

pa je

$$f'(x) = q(x) + (x - a)q'(x),$$

odakle odmah sledi da je $f'(a) = 0$.

537. Za koje vrednosti $a \in \mathbb{Q}$ polinom $x^5 - 5x - a$ nad poljem racionalnih brojeva ima višestruku nulu?

Rešenje. Ako je b višestruka nula datog polinoma $p(x)$, onda je

$$p(b) = b^5 - 5b - a = 0$$

i

$$p'(b) = 5b^4 - 5 = 0.$$

Iz ovih jednačina sledi $b^4 = 1$ i $a = b^5 - 5b = -4b$, odnosno $a = \pm 4$.

538. Dokazati da u prstenu polinoma $\mathbb{Q}[x]$ važi teorema analogna velikoj Fermaovoj teoremi, tj. ne postoji rešenje jednačine $p^n + q^n = r^n$, $p, q, r \in \mathbb{Q}[x]$, n prirodan broj veći od 2.

Rešenje. Pretpostavimo suprotno. Neka su p, q i r polinomi sa racionalnim koeficijentima za koje je

$$(1) \quad p^n + q^n - r^n = 0, \quad n > 2.$$

Može se pretpostaviti da su ovi polinomi uzajamno prosti po parovima, jer ako dva polinoma imaju zajednički faktor, tada se odmah vidi da je i treći deljiv tim faktorom, pa se zajednički faktor može skratiti.

Neka je a stepen polinoma p , b stepen q , c stepen r i neka je $a \geq b \geq c$. Ako se jednakost (1) diferencira i skрати sa n , dobija se

$$(2) \quad p^{n-1}p' + q^{n-1}q' - r^{n-1}r' = 0.$$

Kada se jednakost (1) pomnoži sa r' , a (2) sa r i oduzmu dobija se da je

$$p^{n-1}(p'r - pr') - q^{n-1}(qr' - q'r) = 0,$$

$$p^{n-1}(p'r - pr') = q^{n-1}(qr' - q'r),$$

pa $p^{n-1} \mid (qr' - q'r)$. Posmatrajući stepene polinoma p, q i r dobija se da je $(n-1)a \leq b+c-1$ što je nemoguće za $n > 2$ i $a \geq b \geq c$.

Dokaz je analogan i za sve ostale međusobne odnose stepena a, b, c .

539. Za koje vrednosti $a, b \in \mathbb{Q}$ je polinom

$$f(x) = ax^{n+1} + bx^n - 1$$

deljiv sa $(x-1)^2$?

Rešenje. Ako je dati polinom deljiv sa $(x-1)^2$, onda je 1 bar dvostruka nula tog polinoma, pa stoga mora biti

$$f(1) = a + b + 1 = 0, \quad f'(1) = (n+1)a + nb = 0.$$

Odavde je

$$a = n, \quad b = -(n+1).$$

540. Naći uslov koji moraju da zadovoljavaju a i b da bi polinom $x^5 + ax^3 + b$, nad poljem racionalnih brojeva $\mathbb{Q}$, imao dvostruki koren različit od nule.

Rezultat. $a \neq 0$ i $3125b^2 + 108a^5 = 0$.

541. Dokazati da je polinom

$$f(x) = 2x^{n+1} - n(n+1)a^{n-1}x^2 + 2(n^2-1)a^nx - n(n-1)a^{n+1}$$

deljiv sa $(x-a)^3$, $n \in \mathbb{N}$.

542. Odrediti polinom $p(x)$ trećeg stepena nad poljem racionalnih brojeva takav da je $p(x)$ deljiv sa $x-1$, a daje međusobno jednake ostatke pri deljenju sa $x-2$, $x-3$ i $x-4$.

Rešenje. Lako se vidi da je

$$p(x) = (x-2)(x-3)(x-4) + a \quad \text{i} \quad p(1) = 0,$$

pa je $a = 6$.

543. Neka su r_a i r_b ostaci pri deljenju polinoma $p(x)$ sa $x-a$ odnosno $x-b$, ($a \neq b$). Koliki je ostatak pri deljenju $p(x)$ sa $(x-a)(x-b)$?

Rešenje. Mora biti

$$(i) \quad p(x) = q(x)(x-a)(x-b) + mx + n,$$

$$(ii) \quad p(x) = q_a(x)(x-a) + r_a,$$

$$(iii) \quad p(x) = q_b(x)(x-b) + r_b.$$

Za $p(a)$ iz (i) i (ii) dobijamo da je

$$ma + n = r_a,$$

a za $p(b)$ iz (i) i (iii) dobijamo

$$mb + n = r_b.$$

Rešavajući sistem jednačina po m i n dobija se da je ostatak pri deljenju $p(x)$ sa $(x-a)(x-b)$

$$r_a \frac{x-b}{a-b} + r_b \frac{x-a}{b-a}.$$

544. Ostaci pri deljenju polinoma $p(x) \in \mathbb{Q}[x]$ sa $x-1$, $x-2$ i $x-3$ su 3, 7 i 13 respektivno. Naći ostatak $r(x)$ pri deljenju $p(x)$ sa $(x-1)(x-2)(x-3)$.

Rezultat. $r(x) = x^2 + x + 1$.

545. Izračunati ostatak pri deljenju polinoma $p(x) \in \mathbb{R}[x]$ sa $x^2 + 1$, ako je

a) $p(x) = (\cos \alpha + x \sin \alpha)^n$,

b) $p(x) = (a + bx)^n$.

Rešenje. a) Ako u

$$(\cos \alpha + x \sin \alpha)^n = (x^2 + 1)q(x) + kx + l$$

stavimo $x = i$ dobićemo ostatak

$$r(x) = x \sin n\alpha + \cos n\alpha.$$

b) Koristiti da je

$$a + bx = \sqrt{a^2 + b^2} \left(\frac{a}{\sqrt{a^2 + b^2}} + x \frac{b}{\sqrt{a^2 + b^2}} \right) = \sqrt{a^2 + b^2} (\cos \phi + x \sin \phi),$$

gde je $\phi = \arctg \frac{b}{a}$.

546. Neka je polinom $p(x) \in F[x]$, F polje, napisan u obliku

$$p(x) = p_0(x^k) + xp_1(x^k) + x^2p_2(x^k) + \dots + x^{k-1}p_{k-1}(x^k),$$

$$p_i(x) \in F[x], \quad i = 0, 1, \dots, k-1.$$

Dokazati da je ostatak pri deljenju $p(x)$ sa $x^k - a$

$$r(x) = p_0(a) + xp_1(a) + \dots + x^{k-1}p_{k-1}(a).$$

Rešenje. Deleći $p_i(x^k)$, $i = 0, 1, \dots, k-1$, sa $x^k - a$ dobijamo

$$p_i(x^k) = (x^k - a)q_i(x^k) + p_i(a).$$

Ako dobijene vrednosti za $p_i(x^k)$ zamenimo u $p(x)$, dobijamo

$$\begin{aligned} p(x) &= (x^k - a)(q_0(x^k) + xq_1(x^k) + \dots + x^{k-1}q_{k-1}(x^k)) + \\ &+ p_0(a) + xp_1(a) + \dots + x^{k-1}p_{k-1}(a). \end{aligned}$$

Kako je ostatak kod deljenja jedinstven, dobija se da je traženi ostatak

$$r(x) = p_0(a) + xp_1(a) + \dots + x^{k-1}p_{k-1}(a).$$

547. Neka je $p(x^n)$ polinom nad poljem racionalnih brojeva $\mathbb{Q}$ koji je deljiv sa $x - 1$. Dokazati da je deljiv i sa $x^n - 1$.

548. Neka je $p(x) = x^{n_1} + x^{n_2} + \dots + x^{n_p}$ gde su $n_1, n_2, \dots, n_p$ prirodni brojevi. Dokazati da je $p(x)$ deljiv sa $q(x) = 1 + x + x^2 + \dots + x^{p-1}$ ako i samo ako je $n_i \not\equiv n_j \pmod{p}$ za $i \neq j$.

Uputstvo. Koristiti činjenicu da je $x^p \equiv 1 \pmod{q(x)}$ i da $q(x)$ deli $p(x)$ ako i samo ako je $p(x) \equiv 0 \pmod{q(x)}$.

549. Neka je R komutativan prsten bez nilpotentnih elemenata i neka je polinom $p = a_0 + a_1x + \dots + a_kx^k$ delitelj nule u $R[x]$. Dokazati da postoji element $b \neq 0$ u R takav da je $ba_0 = ba_1 = \dots = ba_k = 0$.

Rešenje. Neka je $q = b_0 + b_1x + \dots + b_lx^l \in R[x]$ takav da je $pq = 0$. Tada je

$$\begin{aligned} a_0b_0 &= 0, \\ a_1b_0 + a_0b_1 &= 0, \\ a_2b_0 + a_1b_1 + a_0b_2 &= 0, \\ &\dots\dots\dots \\ a_kb_0 + a_{k-1}b_1 + \dots + a_0b_k &= 0. \end{aligned}$$

Ako je $b_0 \neq 0$, onda se množeći drugu jednačinu sa b_0 , treću sa b_0^2 itd., poslednju sa b_0^k , dobija

$$a_0b_0 = 0, \quad a_1b_0^2 = 0, \quad a_2b_0^3 = 0, \quad \dots, \quad a_kb_0^{k+1} = 0,$$

tj. $b_0^{k+1} = 0$ je traženi element.

Ako je $b_0 = 0$, tada se ponavlja opisani postupak koristeći umesto b_0 prvi različit od nule koeficijent b_s u q .

PRIMEDBA. Tvđenje navedeno u prethodnom zadatku može se dokazati i bez pretpostavke da prsten nema nilpotentnih elemenata. Videti: W. R. Scott, *Divisor of zero in polynomial rings*, Amer. Math. Monthly, 61 (1954), 336.

550. Neka je R komutativan prsten sa jedinicom. Dokazati da polinom $f = a_0 + a_1x + \dots + a_kx^k \in R[x]$ ima multiplikativan inverzni element u $R[x]$ ako i samo ako a_0 ima multiplikativan inverzni element u R , a $a_1, a_2, \dots, a_k$ su nilpotentni.

Rešenje. Neka je $fg = 1$, gde je $g = b_0 + b_1x + \dots + b_mx^m$. Neposredno

sledi da je $a_0b_0 = 1$, tj. a_0 je invertibilan element. Pokažimo najpre da je a_k nilpotentan. Iz $fg = 1$ sledi

$$a_kb_m = 0,$$

$$a_kb_{m-1} + a_{k-1}b_m = 0,$$

pa je

$$a_k^2b_{m-1} + a_{k-1}a_kb_m = 0,$$

tj. $a_k^2b_{m-1} = 0$. Iz

$$a_kb_{m-2} + a_{k-1}b_{m-1} + a_{k-2}b_m = 0$$

množenjem sa a_k^2 dobijamo

$$a_k^3b_{m-2} + a_{k-1}a_k^2b_{m-1} + a_{k-2}a_k^2b_m = 0,$$

pa je $a_k^3b_{m-2} = 0$. Nastavljajući ovaj postupak, konačno dobijamo $a_k^{m+1}b_0 = 0$, pa je $a_k^{m+1} = 0$ jer b_0 ima multiplikativni inverzni element a_0 .

Neka je $n < k$ prirodan broj takav da je a_i nilpotentan za $i = n+1, \dots, k$. Posmatrajući koeficijente uz $x^{n+m}, \dots, x^m$ u $fg = 1$ i koristeći činjenicu da je skup $N(R)$ nilpotentnih elemenata iz R , ideal u R , dobijamo da

$$a_nb_m \in N(R),$$

jer je

$$a_nb_m + a_{n+1}b_{m-1} + \dots + a_kb_{m-k} = 0,$$

pa je

$$a_nb_m = -a_{n+1}b_{m-1} - \dots - a_kb_{m-k} \in N(R).$$

Iz $a_nb_{m-1} + a_{n-1}b_m \in N(R)$ sledi

$$a_n(a_nb_{m-1} + a_{n-1}b_m) = a_n^2b_{m-1} + a_{n-1}a_nb_m \in N(R),$$

pa je i $a_n^2b_{m-1} \in N(R)$. Nastavljajući ovaj postupak iz $a_nb_0 + a_{n-1}b_1 + \dots$ dobijamo da $a_n^{m+1}b_0 \in N(R)$ pa i

$$a_0(a_n^{m+1}b_0) = a_n^{m+1}a_0b_0 = a_n^{m+1} \in N(R).$$

Neka je $a_n^{m+1} = c$ i $c^s = 0$. Tada je $a_n^{s(m+1)} = 0$, pa $a_n \in N(R)$. Prema tome, svi elementi $a_k, a_{k-1}, \dots, a_2, a_1$ su nilpotentni.

Obrnuto, pretpostavimo da je a_0 invertibilan u R , a da su $a_1, a_2, \dots, a_k$ nilpotentni. Polinom

$$h = a_1x + a_2x^2 + \dots + a_kx^k$$

je nilpotentan (zadatak 434), pa $f = a_0 + h$ ima multiplikativan inverzni element (zadatak 433).

551. Dokazati da u prstenu polinoma $F[x]$ sa koeficijentima iz polja F važi:

a) Svaki ideal u $F[x]$ je glavni.

b) Ako su $f(x), g(x) \in F[x]$ i $d(x)$ je najveći zajednički delitelj za $f(x)$ i $g(x)$, tada je ideal generisan sa $f(x)$ i $g(x)$ generisan polinomom $d(x)$, tj.

$$(f(x), g(x)) = (d(x)).$$

Generalisati.

Uputstvo. Koristiti postupak sličan postupku koji je primenjen prilikom ispitivanja ideala u prstenu celih brojeva $\mathbb{Z}$ (zadatak 454).

552. Za polinome

$$f(x) = \bar{2}x^3 + \bar{2}x^2 \quad \text{ i } \quad g(x) = \bar{1}x^4 + \bar{2}x^2 + \bar{1}x$$

iz $\mathbb{Z}_3[x]$ naći najveći zajednički delitelj $d(x)$ i izraziti ga u obliku

$$d(x) = s(x)f(x) + t(x)g(x).$$

Rešenje. Najveći zajednički delitelj ćemo odrediti korišćenjem Euklidovog algoritma.

Ako $g(x)$ podelimo sa $f(x)$, dobićemo količnik

$$q_1(x) = \bar{2}x^2 + \bar{2}$$

i ostatak $r_1(x) = \bar{2}x^2 + \bar{1}x$, tj.

$$(1) \quad g(x) = f(x)(\bar{2}x + \bar{2}) + \bar{2}x^2 + \bar{1}x = f(x)q_1(x) + r_1(x).$$

Sada dobijenim ostatkom $r_1(x)$ delimo $f(x)$, dobija se količnik

$$q_2(x) = \bar{1}x + \bar{2}$$

i ostatak $r_2(x) = \bar{1}x$, odnosno

$$(2) \quad f(x) = (\bar{2}x^2 + \bar{1}x)(\bar{1}x + \bar{2}) + \bar{1}x = r_1(x)q_2(x) + r_2(x).$$

Nastavljajući ovaj postupak delimo $r_1(x)$ sa $r_2(x)$, količnik je

$$q_3(x) = \bar{2}x + \bar{1},$$

a ostatak $r_3(x) = \bar{0}$, tj.

$$(3) \quad \bar{2}x^2 + \bar{1}x = \bar{1}x(\bar{2}x + \bar{1}) = r_2(x)q_3(x).$$

Poslednji ostatak različit od nule je $r_2(x) = \bar{1}x$ i to je traženi najveći zajednički delitelj: $d(x) = \bar{1}x$.

(Ukoliko je poslednji ostatak različit od nule polinom koji nije normalizovan, da se dobije najveći zajednički delitelj treba taj polinom normalizovati.)

Iz (2) je

$$(4) \quad d(x) = f(x) - r_1(x)q_2(x),$$

a iz (1) se dobija da je

$$r_1(x) = g(x) = f(x)q_1(x).$$

Zamenjujući ovo u (4) biće

$$d(x) = f(x) - (g(x) - f(x)q_1(x))q_2(x),$$

odakle je konačno

$$d(x) = (\bar{2}x^2 + \bar{2})f(x) + (\bar{2}x + \bar{1})g(x),$$

odnosno

$$s(x) = \bar{2}x^2 + \bar{2}, \quad t(x) = \bar{2}x + \bar{1}.$$

553. Za polinome

$$f(x) = \bar{1}x^4 + \bar{1}x^3 + \bar{1}x + \bar{2} \text{ i } g(x) = \bar{1}x^4 + \bar{2}$$

iz $\mathbb{Z}_3[x]$, naći najveći zajednički delitelj $d(x)$ i izraziti ga u obliku

$$d(x) = s(x)f(x) + t(x)g(x).$$

Rešenje. Najveći zajednički delitelj ćemo odrediti korišćenjem Euklidovog algoritma opisanog u prethodnom zadatku. Ako $f(x)$ podelimo sa $g(x)$, dobijamo da je

$$(*) \quad \bar{1}x^4 + \bar{1}x^3 + \bar{1}x + \bar{2} = (\bar{1}x^4 + \bar{2})\bar{1} + \bar{1}x^3 + \bar{1}.$$

Ako sad $\bar{1}x^4 + \bar{2}$ podelimo ostatkom $\bar{1}x^3 + \bar{1}x$, dobijamo

$$(**) \quad \bar{1}x^4 + \bar{2} = (\bar{1}x^3 + \bar{1}x)\bar{1}x + \bar{2}x^2 + \bar{2}.$$

Nastavljajući ovaj postupak dobijamo

$$\bar{1}x^3 + \bar{1}x = (\bar{2}x^2 + \bar{2})\bar{2}x.$$

Poslednji ostatak različit od nule je $\bar{2}x^2 + \bar{2}$, pa se najveći zajednički delitelj dobija kad se taj ostatak normalizuje. $\bar{2}^{-1}$ u $\mathbb{Z}_3$ je $\bar{2}$, pa je najveći zajednički delitelj $\bar{2}(\bar{2}x^2 + \bar{2}) = \bar{1}x^2 + \bar{1}$. Iz $(**)$ dobijamo

$$\bar{2}x^2 + \bar{2} = \bar{1}x^4 + \bar{2} + (\bar{1}x^3 + \bar{1}x)\bar{2}x,$$

pa kad pomnožimo sa $\bar{2}$

$$\bar{1}x^2 + \bar{1} = \bar{2}(\bar{1}x^4 + \bar{2}) + (\bar{1}x^3 + \bar{1}x)\bar{1}x.$$

Ako se sad $\bar{1}x^3 + \bar{1}x$ zameni vrednošću iz $(*)$, sledi

$$\begin{aligned} \bar{1}x^2 + \bar{1} &= \bar{2}(\bar{1}x^4 + \bar{2}) + \bar{1}x((\bar{1}x^4 + \bar{1}x^3 + \bar{1}x + \bar{2}) + \bar{2}(\bar{1}x^4 + \bar{2})) = \\ &= (\bar{2} + \bar{2}x)(\bar{1}x^4 + \bar{2}) + \bar{1}x(\bar{1}x^4 + \bar{1}x^3 + \bar{1}x + \bar{2}). \end{aligned}$$

554. Odrediti najveći zajednički delitelj za sledeće parove polinoma sa koeficijentima iz odgovarajućeg polja:

a) $f_1(x) = x^3 - x^2 - x + 1,$

$$g_1(x) = x^4 - 3x^2 - 2x + 4, \quad \text{nad } \mathbb{Q}$$

b) $f_2(x) = x^4 + 3x^2 + 4x,$

$$g_2(x) = 2x^2 - 2x - 4, \quad \text{nad } \mathbb{Q}$$

c) $f_3(x) = \bar{1}x^5 + \bar{3}x^3 + \bar{1}x^2 + \bar{2}x + \bar{2},$

$$g_3(x) = \bar{1}x^4 + \bar{3}x^3 + \bar{3}x^2 + \bar{1}x + \bar{2}, \quad \text{nad } \mathbb{Z}_5.$$

Za svaki par polinoma $f_i(x)$, $g_i(x)$ najveći zajednički delitelj prikazati u obliku

$$s_i(x)f_i(x) + t_i(x)g_i(x).$$

Rezultat.

$$\text{a) } x - 1 = \frac{1}{8}(-x^2 + 2x + 4)f_1(x) + \frac{1}{8}(x - 3)g_1(x),$$

$$\text{b) } x + 1 = \frac{1}{48}(x + 2)f_2(x) - \frac{1}{96}(x^3 + 3x^2 + 8x + 24)g_2(x),$$

$$\text{c) } \bar{1}x^2 + \bar{2} = (\bar{4}x + \bar{3})f_3(x) + (\bar{1}x^2 + \bar{4}x + \bar{3})g_3(x).$$

555. Neka su F i K izomorfna polja. Dokazati da su $F[x]$ i $K[x]$ izomorfni prsteni. Da li važi obrnuto?

556. Neka je $(\mathbb{Q}^+, \cdot)$ multiplikativna grupa pozitivnih racionalnih brojeva. Dokazati da je

$$(\mathbb{Q}^+, \cdot) \cong (\mathbb{Z}[x], +).$$

Uputstvo. Dokazati da se svaki element skupa $\mathbb{Q}^+$ može napisati u obliku $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, za različite proste brojeve p_i i jedinstvene cele brojeve α_i .

557. Neka je R komutativan prsten sa jedinicom i neka je I ideal u R . Dokazati da je $I[x]$ ideal u prstenu polinoma $R[x]$.

558. Neka je R komutativan prsten sa jedinicom i neka je $f : R[x] \rightarrow R[x]$ dato sa $f : p(x) \mapsto p(x-a)$, $p(x) \in R[x]$. Dokazati da je f automorfizam prstena $R[x]$.

559. Naći sve automorfizme prstena $\mathbb{Q}[x]$.

Rezultat. Svaki automorfizam f prstena $\mathbb{Q}[x]$ je dat sa $f(\alpha) = \alpha$, za svako $\alpha \in \mathbb{Q}$, i $f(x) = ax + b$, $a, b \in \mathbb{Q}$, $a \neq 0$ i svako takvo preslikavanje je automorfizam.

560. Neka je R komutativan prsten sa jedinicom. Dokazati da prsten polinoma $R[x]$ sadrži beskonačno mnogo potprstena izomorfnih sa $R[x]$.

Uputstvo. $R[x] \cong R[x^k]$, za $k \in \mathbb{N}$.

561. Dokazati da je

$$\text{a) } \mathbb{Z}[x]/(3, x) \cong \mathbb{Z}_3,$$

$$\text{b) } \mathbb{Z}[x]/(6) \cong \mathbb{Z}_6[x].$$

Rešenje. a) Posmatrajmo homomorfizam $f : \mathbb{Z}[x] \rightarrow \mathbb{Z}$ koji svaki polinom iz $\mathbb{Z}[x]$ preslikava u njegov konstantan član i homomorfizam $g : \mathbb{Z} \rightarrow \mathbb{Z}_3$ definisan sa $g(z) = \bar{z}$. gf je homomorfizam $\mathbb{Z}[x]$ u $\mathbb{Z}_3$, a njegovo jezgro $\text{Ker}(gf)$ je ideal koji sačinjavaju svi polinomi čiji je konstantan član deljiv sa 3, tj. ideal $(3, x)$. Na osnovu 2.50 sledi da je

$$\mathbb{Z}[x]/(3, x) \cong \mathbb{Z}_3.$$

b) Posmatrati homomorfizam $f : \mathbb{Z}[x] \rightarrow \mathbb{Z}_6[x]$ definisan sa

$$f(a_0 + a_1x + \dots + a_nx^n) = \bar{a}_0 + \bar{a}_1x + \dots + \bar{a}_nx^n.$$

562. Dokazati:

a) ideal (x) je prost, ali nije maksimalan u $\mathbb{Z}[x]$,

b) ideal (y) je prost, ali nije maksimalan u $\mathbb{Q}[x, y]$.

Rešenje. a) Ideal (x) se sastoji od svih polinoma čiji je konstantni član nula. Ako je proizvod dva polinoma iz $\mathbb{Z}[x]$ polinom čiji je konstantni član nula, onda bar jedan od tih polinoma ima konstantan član nula, dakle, ideal (x) je prost. Međutim, taj ideal nije maksimalan jer je sadržan, na primer, u idealu $(2, x) \neq \mathbb{Z}[x]$.

b) Sličnim zaključivanjem dobija se da je (y) prost ideal. Međutim, taj ideal nije maksimalan jer je sadržan u idealu $(x, y) \neq \mathbb{Q}[x, y]$.

563. Neka je $I = (p(x))$ glavni ideal generisan polinomom $p(x)$ u prstenu $F[x]$, gde je F polje. Dokazati da se polinomi $f(x)$ i $g(x)$ iz $F[x]$ nalaze u istom suskupu faktor prstena $F[x]/I$ ako i samo ako $f(x)$ i $g(x)$ daju isti ostatak pri deljenju sa $p(x)$.

Rešenje. Pretpostavimo da je

$$f(x) + I = g(x) + I.$$

Tada u I postoji polinom $h(x)p(x)$ tako da je

$$f(x) = g(x) + h(x)p(x).$$

Ako je $r(x)$ ostatak pri deobi $g(x)$ sa $p(x)$, tj. ako je

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

onda je

$$f(x) = q(x)p(x) + r(x) + h(x)p(x) = (h(x) + q(x))p(x) + r(x),$$

a to znači da je $r(x)$ ostatak i pri deobi polinoma $f(x)$ sa $p(x)$.

Obrnuto, ako je

$$f(x) = q_1(x)p(x) + r(x)$$

i

$$g(x) = q_2(x)p(x) + r(x),$$

onda je

$$\begin{aligned} f(x) + I &= q_1(x)p(x) + r(x) + I = r(x) + I = \\ &= g(x) - q_2(x)p(x) + I = g(x) + I, \end{aligned}$$

pa $f(x)$ i $g(x)$ pripadaju istom suskupu.

564. Ako je $p(x)$ svodljiv polinom, koji elementi faktor prstena $F[x]/(p(x))$ imaju multiplikativni inverzni element ?

565. Neka je F polje i $p(x) \in F[x]$. Dokazati:

a) Ideal $(p(x))$ je maksimalan u $F[x]$ ako i samo ako je $p(x)$ nesvodljiv nad F .

b) $F[x]/(p(x))$ je polje ako i samo ako je $p(x)$ nesvodljiv nad F .

Uputstvo. Koristiti zadatke 502 i 496.

566. Dokazati da je ideal $(x^2 + 1)$ maksimalan u prstenu $\mathbb{R}[x]$.

Uputstvo. Korsiti prethodni zadatak.

567. U polju $\mathbb{Z}_5[x]/I$, gde je $I = (\bar{1}x^2 + \bar{1}x + \bar{1})$, naći multiplikativan inverzni element za element $\bar{1}x^2 + \bar{2} + I$.

Rešenje. Polinom $\bar{1}x^2 + \bar{1}x + \bar{1}$ je nesvodljiv nad $\mathbb{Z}_5$ (ako bi bio svodljiv imao bi jedan linearan faktor, pa i nulu u $\mathbb{Z}_5$, a lako se proverava da dati polinom nema nulu u $\mathbb{Z}_5$), pa je uzajamno prost sa polinomom $\bar{1}x^2 + \bar{2}$. Prema tome, postoje polinomi $s(x)$ i $t(x)$ takvi da je

$$\bar{1} = s(x)(\bar{1}x^2 + \bar{1}x + \bar{1}) + t(x)(\bar{1}x^2 + \bar{2}).$$

Euklidovim algoritmom se dobija da je

$$s(x) = \bar{3}x + \bar{3} \quad \text{i} \quad t(x) = \bar{2} + \bar{4},$$

pa otuda sledi da je $\overline{2x+4}+I$ multiplikativni inverzni element za $\overline{1x^2+2}+I$.

568. U polju $\mathbb{Q}[x]/(x^3+2x+1)$ naći multiplikativni inverzni element za $\overline{x^2+1}$. (Sa $\overline{x^2+1}$ smo označili suskup kome pripada polinom x^2+1 .)

Rešenje. Jedan od načina da se nađe traženi inverzni element je primena Euklidovog algoritma kao u prethodnom zadatku. Pored toga, taj inverzni element se može odrediti i metodom neodređenih koeficijenata.

Svi suskupovi koji čine dato polje su potpuno određeni ostavima pri deobi sa $p(x)$ (što sledi iz zadatka 563), tj. u svakom suskupu postoji tačno jedan polinom stepena manjeg od 3, odnosno

$$\mathbb{Q}[x]/(x^3+2x+1) = \{\overline{ax^2+bx+c} \mid a, b, c \in \mathbb{Q}\},$$

pa možemo pisati

$$\overline{(x^2+1)} \cdot \overline{(ax^2+bx+c)} = \overline{1},$$

a odatle je

$$\overline{ax^4+bx^3+(a+c)x^2+bx+c} = \overline{1}.$$

S obzirom da je

$$\overline{x^3} = \overline{x^3+2x+1-2x-1} = \overline{-2x-1}, \quad \overline{x^4} = \overline{x \cdot x^3} = \overline{-2x^2-x},$$

biće

$$\begin{aligned} \overline{a(-2x^2-x)+b(-2x-1)+(a+c)x^2+bx+c} &= \\ &= \overline{(c-a)x^2-(a+b)x-b+c} = \overline{1}. \end{aligned}$$

Prema zadatku 563 dva polinoma stepena manjeg od 3 nalaze se u istom suskupu ako i samo ako su jednaki, pa mora biti

$$(c-a)x^2-(a+b)x-b+c=1,$$

odakle se dobija sistem jednačina

$$c-a=0, \quad -(a+b)=0, \quad -b+c=1,$$

čije je rešenje

$$a = \frac{1}{2}, \quad b = -\frac{1}{2}, \quad \text{i} \quad c = \frac{1}{2}.$$

Prema tome, za $\overline{x^2+1}$ u polju $\mathbb{Q}[x]/(x^3+2x+1)$ multiplikativni inverzni element je

$$\overline{\frac{1}{2}(x^2-x+1)}.$$

569. Dokazati da je:

- a) $\mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}[x]/(x^2 - 4)$,
- b) $\mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}[x]/(x^2 + 2x + 2)$,
- c) $\mathbb{Q}[x, y]/(x + y) \cong \mathbb{Q}[x]$.

2.7 Simetrični polinomi

570. U jednačini $x^3 - 7x + \lambda = 0$ odrediti realan parametar λ tako da za rešenja x_1 i x_2 važi $x_1 = 2x_2$.

Rezultat. $\lambda \in \{-6, 6\}$.

571. Polinom

$$p(x) = x^5 - 13x^4 + 67x^3 - 171x^2 + 216x - 108 \in \mathbb{Q}[x]$$

rastaviti na činioce, ako se zna da jednačina $p(x) = 0$ ima jedan trostruki i jedan dvostruki koren.

Rešenje. $p(x) = (x - x_1)^3(x - x_2)^2$, pa je

$$3x_1 + 2x_2 = 13 \quad \text{i} \quad 3x_1^2 + x_2^2 + 6x_1x_2 = 67.$$

Rešavajući ovaj sistem jednačina dobija se $x_1 = 3$ i $x_2 = 2$, pa je $p(x) = (x - 3)^3(x - 2)^2$.

572. U jednačini $x^4 - 9x^3 + mx^2 - 8x + 6 = 0$ odrediti vrednost realnog parametra m tako da zbir dva korena bude jednak zbiru druga dva korena.

Rešenje. Koristeći elementarne simetrične polinome, dobijaju se sledeći uslovi:

$$x_1 + x_2 = x_3 + x_4 = \frac{9}{2}, \quad (x_1 + x_2)(x_3 + x_4) + x_1x_2 + x_3x_4 = m,$$

$$x_1x_2(x_3 + x_4) + x_3x_4(x_1 + x_2) = 8, \quad x_1x_2x_3x_4 = 6,$$

pa je

$$m = \frac{793}{36}.$$

573. Rešiti jednačinu

$$x^4 - 2x^3 + 2x^2 - x - 2 = 0,$$

ako je zbir dva korena jednak jedinici.

574. Ako su sva tri korena polinoma

$$x^3 - px + q, \quad p, q \in \mathbb{R}, \quad p > 0, \quad q > 0,$$

realni, dokazati da za koren r najmanje apsolutne vrednosti važi $\frac{q}{p} < r \leq \frac{3q}{2p}$.

Rešenje. Pošto je zbir korena nula, a proizvod negativan ($q > 0$), (v. 2.80), polinom ima dva pozitivna i jedan negativan koren. Neka su r, s i t koreni tako da je $s \geq r > 0$, a $t = -(r + s)$. Iz

$$(x - r)(x - s)(x + r + s) = x^3 - px + q$$

dobijamo

$$p = r^2 + rs + s^2$$

i

$$q = rs(r + s).$$

Kako je $s^2 \geq rs \geq r^2$, imamo

$$s^2 + rs - 2r^2 \geq 0,$$

pa je

$$3(rs + s^2) \geq 2(r^2 + rs + s^2),$$

tj.

$$\frac{3}{2} (rs + s^2) \geq r^2 + rs + s^2.$$

Ako nejednakosti

$$rs + s^2 < r^2 + rs + s^2 \leq \frac{3}{2} (rs + s^2)$$

pomnožimo sa $\frac{r}{r^2 + rs + s^2} > 0$ dobijamo

$$\frac{rs(r + s)}{r^2 + rs + s^2} < r \leq \frac{3}{2} \frac{rs(r + s)}{r^2 + rs + s^2},$$

odnosno

$$\frac{q}{p} < r \leq \frac{3q}{2p}.$$

575. Neka je $p(x) = x^3 + ay^2 + bx - 1$, $a, b \in \mathbb{Z}$, nesvodljiv polinom nad poljem racionalnih brojeva. Neka je r_1 koren polinoma $p(x)$, a $r_1 + 1$ koren polinoma $q(x) = x^3 + cx^2 + dx + 1$, $c, d \in \mathbb{Z}$. Izraziti korene r_2 i r_3 polinoma $p(x)$ pomoću r_1 .

Rešenje. Pošto je $p(x)$ nesvodljiv nad $\mathbb{Q}$, to je i $p(x-1)$ nesvodljiv nad $\mathbb{Q}$. Kako je $r_1 + 1$ jedan koren polinoma $p(x-1)$, to $p(x-1)$ i $q(x)$ imaju zajednički faktor $(x-r_1)$, a pošto je $p(x-1)$ nesvodljiv, to je $p(x-1) = q(x)$. Otuda dobijamo da su koreni polinoma $q(x)$ $r_1 + 1$, $r_2 + 1$, $r_3 + 1$, pa je

$$r_1 r_2 r_3 = 1 \quad \text{i} \quad (r_1 + 1)(r_2 + 1)(r_3 + 1) = -1.$$

Iz gornjih jednakosti dobija se da su r_2 i r_3 rešenja kvadratne jednačine

$$x^2 + \frac{r_1^2 + 3r_1 + 1}{r_1(r_1 + 1)}x + \frac{1}{r_1} = 0.$$

Rešavanjem gornje kvadratne jednačine dobija se

$$r_2 = -\frac{1}{r_1 + 1} \quad \text{i} \quad r_3 = -\frac{r_1 + 1}{r_1}.$$

(Rešavanje kvadratne jednačine može se izbeći koristeći

$$\frac{r_1^2 + 2r_1 + 1 + r}{r_1(r_1 + 1)} = \frac{r_1 + 1}{r_1} + \frac{1}{r_1 + 1},$$

pa se odmah vidi da su rešenja te jednačine $-\frac{1}{r_1 + 1}$ i $-\frac{r_1 + 1}{r_1}$).

576. Sledeće simetrične polinome prikazati pomoću elementarnih simetričnih polinoma:

a) $(xy + z)(yz + x)(zx + y)$,

b) $(x + y)(y + z)(x + z)$,

c) $x^4 + y^4 + z^4 - 2x^2y^2 - 2x^2z^2 - 2y^2z^2$.

Rešenje. a) Ispitaćemo najpre proizvod datog polinoma $p(x, y, z) = (xy + z)(yz + x)(zx + y)$ i polinoma xyz .

$$\begin{aligned} xyz \cdot p(x, y, z) &= (xyz + z^2)(zyx + x^2)(zxy + y^2) = \\ &= (\sigma_3 + x^2)(\sigma_3 + y^2)(\sigma_3 + z^2) = \sigma_3^3 + (x^2 + y^2 + z^2)\sigma_3^2 + \end{aligned}$$

$$+(x^2y^2 + y^2z^2 + z^2x^2)\sigma_3 + x^2y^2z^2.$$

Kako je

$$x^2 + y^2 + z^2 = (x + y + z)^2 - 2(xy + yz + zx) = \sigma_1^2 - 2\sigma_2,$$

$$\begin{aligned} x^2y^2 + y^2z^2 + z^2x^2 &= (xy + yz + zx)^2 - 2(x + y + z)xyz = \\ &= \sigma_2^2 - 2\sigma_1\sigma_3, \end{aligned}$$

biće

$$\sigma_3 p(x, y, z) = \sigma_3^3 + (\sigma_1^2 - 2\sigma_2)\sigma_3^2 + (\sigma_2^2 - 2\sigma_1\sigma_3)\sigma_3 + \sigma_3^2,$$

odnosno

$$p(x, y, z) = \sigma_3^2 + (\sigma_1^2 - 2\sigma_2)\sigma_3 + (\sigma_2^2 - 2\sigma_1\sigma_3) + \sigma_3.$$

$$\begin{aligned} b) \quad (x + y)(x + z)(y + z) &= (\sigma_1 - x)(\sigma_1 - y)(\sigma_1 - z) = \\ &= \sigma_1^3 - \sigma_1(x + y + z) + \sigma_1(xy + yz + xz) - xyz = \sigma_1\sigma_2 - \sigma_3. \end{aligned}$$

c) Rezultat:

$$\sigma_1^4 - 4\sigma_1^2\sigma_2 + 8\sigma_1\sigma_3.$$

577. Za jednačinu

$$x^3 - 3x + 1 = 0$$

naći Njutnove sume $s_1, s_2, \dots, s_6$, korena x_1, x_2, x_3 (2.82).

Rešenje. Ovde je $\sigma_1 = 0$, $\sigma_2 = -3$, pa će biti

$$s_1 = x_1 + x_2 + x_3 = \sigma_1 = 0,$$

$$s_2 = x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3) = \sigma_1^2 - 2\sigma_2 = 6.$$

Iz date jednačine dobija se $x_i^3 = 3x_i - 1$, $i = 1, 2, 3$, pa je

$$s_3 = x_1^3 + x_2^3 + x_3^3 = 3(x_1 + x_2 + x_3) - 3 = -3,$$

takođe je $x_i^4 = 3x_i^2 - x_i$, $i = 1, 2, 3$, odakle sledi

$$s_4 = x_1^4 + x_2^4 + x_3^4 = 3(x_1^2 + x_2^2 + x_3^2) - (x_1 + x_2 + x_3) = 18.$$

Slično se dobija da je $s_5 = -15$, $s_6 = 57$.

578. Data je jednačina

$$x^3 - 5x^2 + 2x - 4 = 0.$$

a) Naći Njutnove sume s_1, s_2, s_3, s_4 korena jednačine.

b) Naći sume $s_{-1}, s_{-2}, s_{-3}, s_{-4}$ korena jednačine, gde je

$$s_{-k} = x_1^{-k} + x_2^{-k} + x_3^{-k}, \quad k = 1, 2, 3, 4.$$

579. Ako su $x_1, x_2, \dots, x_n$ nule polinoma

$$p(x) = x^n + a_1x^{n-1} + \dots + a_n,$$

a s_k Njutnove sume nula $x_1, x_2, \dots, x_n$, dokazati da tada važi

a) $s_k + a_1s_{k-1} + a_2s_{k-2} + \dots + a_{k-1}s_1 + ka_k = 0$, $k = 1, 2, \dots, n$.

b) $s_k + a_1s_{k-1} + \dots + a_ns_{k-n} = 0$, $k > n$.

580. Ako su $\sigma_1 = x_1 + x_2$, $\sigma_2 = x_1x_2$ i $s_k = x_1^k + x_2^k$, dokazati da je

$$s_k = k \sum_{m=0}^{[k/2]} \frac{(-1)^m (k-m-1)!}{m!(k-2m)!} \sigma_1^{k-2m} \sigma_2^m, \quad \text{za svako } k \in \mathbb{N}.$$

($[a]$ je najveći ceo broj koji nije veći od a).

Uputstvo. Za $k = 1$ i $k = 2$ formula je tačna. Pošto je za $k > 2$, $s_k = \sigma_1 s_{k-1} - \sigma_2 s_{k-2}$, može se primeniti indukcija po k .

PRIMEDBA. Ovo je specijalan slučaj Voringove (Waring) formule kojom se s_k izračunava pomoću $\sigma_1, \sigma_2, \dots, \sigma_n$:

$$s_k = k \sum_{\lambda_1 + 2\lambda_2 + \dots + n\lambda_n = k} (-1)^{k-\lambda_1-\dots-\lambda_n} \frac{(\lambda_1 + \dots + \lambda_n - 1)!}{\lambda_1! \dots \lambda_n!} \sigma_1^{\lambda_1} \dots \sigma_n^{\lambda_n},$$

gde se sumiranje vrši po svim nenegativnim celobrojnim rešenjima jednačine $\lambda_1 + 2\lambda_2 + \dots + n\lambda_n = k$.

581. Formirati kvadratnu jednačinu čiji su koreni treći stepeni korena jednačine $x^2 + 6x + 10 = 0$.

Rešenje. Ovde je $\sigma_1 = x_1 + x_2 = 6$, $\sigma_2 = x_1x_2 = 10$. Tražena jednačina $x^2 + px + q = 0$ ima korene $x'_1 = x_1^3$, $x'_2 = x_2^3$, pa je

$$-p = x'_1 + x'_2 = x_1^3 + x_2^3 = \sigma_1^3 - 3\sigma_1\sigma_2 = -36,$$

$$q = x'_1 x'_2 = x_1^3 x_2^3 = \sigma_2^3 = 1000.$$

Prema tome, tražena jednačina je

$$x^2 + 36x + 1000 = 0.$$

582. Formirati kubnu jednačinu čiji su koreni kvadrati korena jednačine $x^3 - px + q = 0$.

Rezultat. $x^3 + 2px^2 + p^2x - q^2 = 0$.

583. Naći vrednost izraza

$$\frac{x_1}{x_1 + 1} + \frac{x_2}{x_2 + 1} + \frac{x_3}{x_3 + 1} + \frac{x_4}{x_4 + 1},$$

ako su x_1, x_2, x_3, x_4 nule polinoma $x^4 + 9x^3 + 2$.

584. Izraziti elementarne simetrične polinome $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ kao polinome po Njutnovim sumama s_1, s_2, s_3 i s_4 .

Rezultat.

$$\sigma_1 = s_1,$$

$$2\sigma_2 = s_1^2 - s_2,$$

$$6\sigma_3 = s_1^3 - 3s_1s_2 + 2s_3,$$

$$24\sigma_4 = s_1^4 - 6s_1^2s_2 + 8s_1s_3 + 3s_2^2 - 6s_4.$$

585. Rešiti sistem jednačina

$$\begin{aligned} x + y + z + u &= 1, \\ x^2 + y^2 + z^2 + u^2 &= 9, \\ x^3 + y^3 + z^3 + u^3 &= 1, \\ x^4 + y^4 + z^4 + u^4 &= 33. \end{aligned}$$

Rešenje. Ako leve strane datih jednačina izrazimo pomoću elementarnih simetričnih polinoma biće

$$\begin{aligned} \sigma_1 &= 1, \\ \sigma_1^2 - 2\sigma_2 &= 9, \\ \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 &= 1, \\ \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3 - 4\sigma_4 &= 33. \end{aligned}$$

Rešenje ovog sistema se lako određuje:

$$\sigma_1 = 1, \quad \sigma_2 = -4, \quad \sigma_3 = -4, \quad \sigma_4 = 0.$$

Prema tome, da bi rešili dati sistem dovoljno je naći korene jednačine

$$t^4 - t^3 - 4t^2 + 4t = 0.$$

Njeni koreni su $t_1 = 0$, $t_2 = 1$, $t_3 = 2$, $t_4 = -2$, što znači da dati sistem ima 24 rešenja, koja se dobijaju međusobnim permutovanjem korena iz rešenja

$$x = 0, \quad y = 1, \quad z = 2, \quad u = -2.$$

586. U polju realnih brojeva rešiti sisteme jednačina

$$\begin{aligned} a) \quad & x^3 + y^3 + z^3 = a^3, \\ & (y - z)^2 + (z - x)^2 + (x - y)^2 = 2a^2, \\ & x + y + z = a, \\ b) \quad & x + y + z = 9, \\ & x^2 + y^2 + z^2 = 41, \\ & x^2(y + z) + y^2(z + x) + z^2(x + y) = 180. \end{aligned}$$

III

POLJA

3.1 Pregled definicija i teorema

3.1. Neka je $(F, +, \cdot)$ potprsten polja $(K, +, \cdot)$. Potprsten F nazivamo potpolje polja K ako i samo ako je F polje.

3.2. Podskup F polja K je potpolje polja K ako i samo ako F ima bar dva elementa i važi

$$a, b, c \in F, \quad c \neq 0 \Rightarrow a - b, \quad ab, c^{-1} \in F.$$

3.3. Polje K se naziva proširenje (ekstenzija) polja F ako i samo ako je F potpolje polja K .

3.4. Presek proizvoljne familije potpolja polja F je potpolje polja F .

3.5. Prosto polje je polje koje ne sadrži ni jedno pravo potpolje.

3.6. Svako polje F sadrži jedno i samo jedno prosto polje, to prosto polje je presek svih potpolja polja F .

3.7. Karakteristika proizvoljnog polja je 0 ili prost broj p .

3.8. Ako je polje F potpolje polja K , onda polja F i K imaju istu karakteristiku.

3.9. Prosto potpolje polja karakteristike 0 je izomorfno polju $\mathbb{Q}$ racionalnih brojeva.

Prosto potpolje polja karakteristike p je izomorfno polju $\mathbb{Z}_p$ ostataka po

modulu p .

Prema tome, svako polje sadrži potpolje izomorfno polju $\mathbb{Q}$ ili polju $\mathbb{Z}_p$.

3.10. Ako je F konačno polje, onda F ima p^n elemenata, gde je p prost broj, $n \in \mathbb{N}$, a karakteristika polja je p .

3.11. Za svaki prost broj p i svaki prirodan broj n postoji polje sa p^n elemenata.

3.12. Svaka dva konačna polja sa istim brojem elemenata su izomorfna.

3.13. Multiplikativna grupa konačnog polja je ciklička.

3.14. Neka je K polje, a S podskup od K . Presek F svih potpolja polja K koja sadrže S je potpolje polja K koje se naziva potpolje generisano skupom S .

F je minimalno potpolje polja K koje sadrži S .

3.15. Ako je polje K proširenje polja F i $S \subseteq K$, onda se potpolje polja K generisano skupom $F \cup S$ označava sa $F(S)$. Za polje $F(S)$ rećićemo da je dobijeno adjunkcijom skupa S polju F .

Ako je $S = \{a_1, a_2, \dots, a_n\}$, tada ćemo $F(S)$ označavati sa $F(a_1, a_2, \dots, a_n)$.

3.16. Neka je polje K proširenje polja F i $a_1, a_2, \dots, a_n \in K$.

(i) Za svaku permutaciju $\sigma \in S_n$

$$K(a_1, a_2, \dots, a_n) = K(a_{\sigma(1)}, a_{\sigma(2)}, \dots, a_{\sigma(n)}).$$

(ii) $K(a_1, a_2, \dots, a_{n-1})(a_n) = K(a_1, a_2, \dots, a_n)$.

3.17. Ako je polje K proširenje polja F a element $a \in K$, onda se $F(a)$ naziva jednostruko proširenje polja F . Element a nazivamo primitivan element proširenja. $F(a)$ je polje koje se sastoji od svih elemenata oblika $\frac{f(a)}{g(a)}$, gde su $f(x)$ i $g(x)$ polinomi sa koeficijentima iz F i $g(a) \neq 0$.

3.18. Neka je polje K proširenje polja F . Element $a \in K$ se naziva algebarski nad F ako i samo ako postoji nenula polinom $p(x)$ sa koeficijentima iz polja F takav da je $p(a) = 0$. Ako takav polinom ne postoji, a se naziva transcendentan nad F .

3.19. Neka je polje K proširenje polja F . Polje K se naziva algebarsko proširenje polja F ako i samo ako je svaki element iz K algebarski nad F .

Polje K je transcendentno proširenje polja F ako i samo ako je bar jedan element iz K transcendentan nad F .

3.20. Neka je polje K proširenje polja F i neka je element $a \in K$ algebarski nad F . Tada postoji jedinstven normalizovan polinom minimalnog stepena $m(x) \in F[x]$ takav da je $m(a) = 0$. Polinom $m(x)$ se naziva minimalni polinom elemenata a nad F .

Minimalan polinom elemenata a je nesvodljiv nad F . Svaki polinom $q(x) \in F[x]$ takav da je $q(a) = 0$ je deljiv minimalnim polinomom $m(x)$.

Stepen minimalnog polinoma elementa a nad F nazivamo stepen elementa a nad F .

3.21. Ako je polje K proširenje polja F i ako je element $a \in K$ algebarski nad F , onda je

$$F(a) \cong F[x]/(m(x)),$$

gde je $m(x)$ minimalan polinom elementa a nad F .

3.22. Neka je polje K proširenje polja F . Tada se K može posmatrati kao vektorski prostor nad F , pri čemu je sabiranje vektora (elemenata iz K) sabiranje u polju K , a proizvod vektora $a \in K$ i skalara $\alpha \in F$ proizvod αa tih elemenata kao elemenata polja K .

Dimenziju polja K kao vektorskog prostora nad poljem F nazivaćemo stepen K nad F i označavati sa $[K : F]$.

3.23. Polje K se naziva konačno proširenje polja F ako i samo ako je K konačno dimenzionalni vektorski prostor nad F . U suprotnom slučaju, kad je K beskonačno dimenzionalni vektorski prostor nad F , polje K se naziva beskonačno proširenje polja F .

3.24. Neka je $F(a)$ jednostruko proširenje polja F dobijeno adjunkcijom elemenata a .

(i) Ako je a algebarski nad F , onda je

$$[F(a) : F] = n,$$

gde je n stepen elementa a nad F (tj. $n = \deg m(x)$, gde je $m(x)$ minimalni polinom elementa a nad F). Skup

$$\{1, a, a^2, \dots, a^{n-1}\}$$

je baza vektorskog prostora $F(a)$ nad poljem F .

Prema tome, svaki element b polja $F(a)$ može se na jedinstven način prikazati u obliku

$$b = c_0 + c_1 a + \dots + c_{n-1} a^{n-1}, \quad c_0, c_1, \dots, c_{n-1} \in F.$$

(ii) Ako je a transcendentan nad F , onda je

$$[F(a) : F] = \infty.$$

3.25. Svako konačno proširenje polja F je algebarsko proširenje polja F .

3.26. Ako je F polje, onda je $F[x]$ domen integriteta. Polje razlomaka (v. 2.58 i 2.59) domena $F[x]$ označavaćemo sa $F(x)$. Polje $F(x)$ naziva se polje racionalnih funkcija po x nad F i

$$F(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x], g(x) \neq 0 \right\}.$$

Polje $F(x)$ sadrži potpolje izomorfno polju F .

3.27. Ako je a transcendentan element nad poljem F , onda je polje $F(a)$ izomorfno polju $F(x)$ racionalnih funkcija po x nad F i postoji izomorfizam φ takav da je $\varphi(a) = x$ i $\varphi(b) = b$, za svako $b \in F$.

3.28. Ako su F, M i K polja takva da je $F \subseteq M \subseteq K$ (tada se M naziva međupolje za polje F i K), onda je

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

Prema tome, polje M je konačno proširenje polja F , a K konačno proširenje polja M ako i samo ako je K konačno proširenje polja F .

Ako je $\{a_1, a_2, \dots, a_n\}$ baza K nad M , a $\{b_1, b_2, \dots, b_m\}$ baza M nad F , onda mn proizvoda

$$a_i b_j, \quad i = 1, 2, \dots, n, \quad j = 1, 2, \dots, m,$$

čini bazu K nad F .

3.29. Ako je polje K proširenje polja F i element $a \in K$ algebarski nad F , onda je $F(a)$ algebarsko proširenje od F .

3.30. (Teorema o primitivnom elementu) Ako je K konačno proširenje proizvoljnog polja F , onda je K jednostruko proširenje polja F ako i samo ako postoji konačno mnogo međupolja za polja K i F .

Ako je K proširenje polja F karakteristike 0, a $a_1, a_2, \dots, a_n \in K$ elementi algebarski nad F , onda postoji element $\theta \in K$ algebarski nad F , takav da je

$$F(a_1, a_2, \dots, a_n) = F(\theta).$$

3.31. Svaki polinom stepena n nad poljem F može imati najviše n korena u proizvoljnom proširenju polja F .

3.32. Ako je F polje, a $f(x) \in F[x]$ polinom pozitivnog stepena n , onda postoji konačno proširenje K polja F stepena najviše n u kome $f(x)$ ima koren.

3.33. Ako je F polje, a $f(x) \in F[x]$ polinom pozitivnog stepena n , onda postoji konačno proširenje K polja F takvo da se u $K[x]$ polinom $f(x)$ može rastaviti u proizvod linearnih faktora:

$$(*) \quad f(x) = a_0(x - a_1)(x - a_2) \dots (x - a_n), \quad a_i \in K, \quad i = 0, 1, \dots, n,$$

(tj. u polju K polinom $f(x)$ ima n korena, računajući pri tome višestruke korene onoliko puta kolika je njihova višestrukost).

Minimalno proširenje K polja F u kome važi faktorizacija $(*)$ se naziva faktorizacijsko (ili korensko) polje polinoma $f(x)$.

3.34. Neka je $f(x)$ polinom pozitivnog stepena n nad poljem F , a K faktorizacijsko polje polinoma $f(x)$ u kome $f(x)$ ima faktorizaciju $(*)$. Tada je

$$(i) \quad K = F(a_1, a_2, \dots, a_n),$$

$$(ii) \quad [K : F] \leq n!.$$

3.35. Polje F naziva se algebarski zatvoreno ako i samo ako je F faktorizacijsko polje za svaki polinom pozitivnog stepena sa koeficijentima iz F .

3.36. Ako je F proizvoljno polje, onda su sledeći uslovi ekvivalentni:

(i) F je algebarski zatvoreno polje.

(ii) F nema prava algebarska proširenja (tj. svako algebarsko proširenje polja F se poklapa sa F).

(iii) Svaki nesvodljiv polinom nad F je stepena 1.

(iv) Svaki polinom pozitivnog stepena iz $F[x]$ ima koren u F .

3.37. Za svako polje F postoji algebarsko proširenje $\overline{F}$ koje je algebarski zatvoreno. Polje $\overline{F}$ se naziva algebarsko zatvorenje polja F .

3.38. Neka je F polje i n prirodan broj. Element ε polja F se naziva n -ti koren iz jedinice ako i samo ako je $\varepsilon^n = 1$.

Element ε se naziva primitivan n -ti koren iz jedinice ako i samo ako je $\varepsilon^n = 1$ i $\varepsilon^k \neq 1$ za $1 \leq k \leq n-1$.

3.39. Ako je K proširenje polja F , elementi $a, b \in K$ se nazivaju konjugovani nad F ako i samo ako su a i b koreni istog polinoma $p(x) \in F[x]$ nesvodljivog nad F ili su a i b transcendentni nad F .

3.40. Neka su $F(a)$ i $F(b)$ jednostruka proširenja takva da su a i b konjugovani nad F . Polja $F(a)$ i $F(b)$ su izomorfna i postoji izomorfizam tih polja koji preslikava a u b a elemente polja F ostavlja fiksnim (tj. svaki element polja F se preslikava u sebe).

Polja $F(a)$ i $F(b)$ se nazivaju polja konjugovana nad F .

3.41. Svaka dva faktorizacijska polja polinoma $p(x)$ nad poljem F su izomorfna i postoji izomorfizam koji sve elemente polja F ostavlja fiksnim.

3.42. Skup svih automorfizama polja F čini grupu u odnosu na kompoziciju preslikavanja.

3.43. Ako je G neka podgrupa grupe svih automorfizama polja F , onda je skup svih elemenata $a \in F$ takvih da je $\varphi(a) = a$, za svako $\varphi \in G$, potpolje polja F i to potpolje se naziva fiksno polje grupe G .

3.44. Neka je F potpolje polja K . Tada je skup svih automorfizama polja K koji ostavljaju svaki element polja F fiksnim, grupa koju nazivamo grupa Galoa (Galois) polja K nad F i označavamo sa $G(K, F)$. $G(K, F)$ je podgrupa grupe svih automorfizama polja K .

Automorfizmi grupe $G(K, F)$ se nazivaju F -automorfizmi polja K (tj. automorfizam φ polja K se naziva F -automorfizam ako i samo ako je $\varphi(a) = a$ za svako $a \in F$).

3.45. Neka je K konačno proširenje polja F . Svaki automorfizam $\varphi \in G(K, F)$ preslikava proizvoljan element $a \in K$ u element $\varphi(a)$ konjugovan sa a nad F .

3.46. Neka je $f(x) \in F[x]$ a K faktorizacijsko polje polinoma $f(x)$ nad poljem F . Grupa Galoa polinoma $f(x)$ je grupa Galoa $G(K, F)$ polja K nad F .

3.47. Nesvodljiv polinom $f(x)$ stepena n nad poljem F se naziva separabilan ako i samo ako $f(x)$ ima n različitih korena u faktorizacijskom polju (tj. $f(x)$ nema višestrukih korena).

Proizvoljan polinom nad F se naziva separabilan ako i samo ako su svi njegovi nesvodljivi faktori separabilni.

3.48. Svaki polinom nesvodljiv nad poljem F karakteristike 0 je separabilan.

3.49. Neka je $f(x)$ polinom stepena n nad poljem F koji ima tačno k različitih korena $a_1, a_2, \dots, a_k$ u faktorizacijskom polju $K = F(a_1, a_2, \dots, a_k)$. Tada svaki automorfizam φ grupe Galoa $G(K, F)$ određuje jednu permutaciju p_φ

$$a_1 \mapsto \varphi(a_1), \quad a_2 \mapsto \varphi(a_2), \dots, a_k \mapsto \varphi(a_k),$$

skupa $\{a_1, a_2, \dots, a_k\}$. Automorfizam φ je potpuno određen permutacijom p_φ .

Preslikavanje koje svakom automorfizmu grupe $G(K, F)$ pridružuje odgovarajuću permutaciju korena $a_1, a_2, \dots, a_k$ je izomorfizam grupe $G(K, F)$ i neke podgrupe grupe permutacija S_k .

3.50. Proširenje K polja F naziva se normalno ako i samo ako je konačno proširenje F i F je fiksno polje grupe $G(K, F)$ (tj. za svaki element a skupa $K \setminus F$ postoji automorfizam $\varphi \in G(K, F)$ takav da je $\varphi(a) \neq a$).

3.51. Konačno proširenje K polja F je normalno ako i samo ako je

$$[K : F] = |G(K, F)|.$$

3.52. Neka je K konačno proširenje polja F karakteristike 0. Tada su sledeća tvrđenja ekvivalentna:

- (i) K je normalno proširenje polja F .
- (ii) F je faktorizacijsko polje nekog polinoma nad F .
- (iii) Svaki polinom nesvodljiv nad F koji ima jedan koren u K ima sve korene u K .

3.53. (Osnovna teorema teorije Galoa) Neka je K normalno proširenje

polja F i neka je M proizvoljno međupolje za polja K i F (tj. $K \supseteq M \supseteq F$). Tada je preslikavanje

$$M \mapsto G(K, M)$$

bijekcija skupa svih međupolja za polja K i F i skupa svih podgrupa grupe Galoa $G(K, F)$. Pri tome važi

(i) Međupolje M je fiksno polje grupe $G(K, M)$ i

$$[K : M] = |G(K, M)|.$$

(ii) Ako je H proizvoljna podgrupa grupe $G(K, F)$, onda je

$$H = G(K, K_H),$$

gde je K_H fiksno polje grupe H .

(iii) Ako su M_1 i M_2 dva međupolja kojima odgovaraju redom podgrupe $H_1 = G(K, M_1)$ i $H_2 = G(K, M_2)$ grupe $G(K, F)$, onda je

$$M_1 \subseteq M_2 \iff H_1 \supseteq H_2.$$

Ako je $M_1 \subseteq M_2$, onda je

$$[M_2 : M_1] = [H_1 : H_2],$$

(sa $[H_1 : H_2]$ označavamo indeks grupe H_1 po podgrupi H_2).

(iv) M je normalno proširenje polja F ako i samo ako je

$$G(M, F) \cong G(K, F)/G(K, M).$$

3.54. Neka je F polje i $f(x) \in F[x]$. Jednačina $f(x) = 0$ je rešiva radikalima nad F ako i samo ako se svaki koren polinoma $f(x)$ može dobiti konačnim nizom operacija sabiranja, oduzimanja, množenja, deljenja i uzimanja n_i -tih korena (za proizvoljne vrednosti $n_i \in \mathbb{N}$) polazeći od elemenata polja F .

3.55. Neka je F polje karakteristike 0, $f(x) \in F[x]$, a K faktorizacijsko polje polinoma $f(x)$. Jednačina $f(x) = 0$ je rešiva radikalima nad F ako i samo ako je grupa Galoa $G(K, F)$ rešiva grupa.

3.2 Primeri i osnovne osobine

587. Ispitati da li su sledeći prsteni polja:

- a) $(\mathbb{Z}, +, \cdot)$,
- b) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$,
- c) $(\mathbb{Z}_m, +, \cdot)$,
- d) $(\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}, +, \cdot)$,
- e) $\left(\left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}, +, \cdot \right)$.

Rezultat. a) Ne, b) da, c) da, ako je m prost broj; ne, ako je m složen broj (zadatak 12), d) da, e) da.

588. Neka je $(F, +, \cdot)$ polje, a a i b dva različita elementa iz F . Definišimo $*$ i $\circ$ na sledeći način:

$$x * y = x + y - a,$$

$$x \circ y = a + \frac{(x - a)(y - a)}{b - a}.$$

Dokazati da je $(F, *, \circ)$ polje.

589. Ako je R telo, tada je i prsten proširenih formalnih stepenih redova $R\langle x \rangle$ (zadatak 378) takođe telo. Ako je R polje, tada je i $R\langle x \rangle$ polje. Dokazati.

Rešenje. Neka je R telo. Neka je $f = \sum_{h=-\infty}^{\infty} a_h x^h \in R\langle x \rangle$, a r najmanji indeks za koji je $a_r \neq 0$. Tada je $f = x^{-r} h$, gde je

$$h = a_r + a_{r+1}x + \dots + a_n x^{n+r} + \dots \in R[[x]],$$

a_r ima inverzni element, pa na osnovu zadatka 441 postoji $h^{-1} \in R[[x]]$. Tada je $x^r h^{-1}$ inverzni element za f . Prema tome, $R\langle x \rangle$ je telo.

Ako je R polje na osnovu prethodnog neposredno sledi da je i $R\langle x \rangle$ polje.

590. U polju proširenih formalnih stepenih redova $\mathbb{R}\langle x \rangle$ nad poljem realnih brojeva naći inverzne elemente za:

$$a) x^{10}, \quad b) 1 + x, \quad c) \sum_{k=0}^{\infty} 2^k x^k, \quad d) \sum_{k=-3}^{\infty} x^k.$$

Rezultat. a) x^{-10} , b) $\sum_{k=0}^{\infty} (-1)^k x^k$, c) $1 - 2x$, d) $x^3 - x^4$.

591. Neka u prstenu sa jedinicom R za neke elemente a, b važi $aba = a$ i $ba^2b = 1$. Dokazati da je tada $b = a^{-1}$.

Rešenje. Ako se $aba = a$ zdesna pomnoži sa ab , dobija se $aba^2b = a^2b$ pa je $a = a^2b$, tj. $ab = 1$, a ako se $aba = a$ pomnoži sleva sa ba potpuno analogno se dobija da je $ba = 1$.

592. Navesti primer polja karakteristike 5 sa beskonačno mnogo elemenata.

Rešenje. $\mathbb{Z}_5\langle x \rangle$ (zadatak 589).

593. U skupu $\mathbb{Q}^n$ udeđenih n -torki racionalnih brojeva definisane su operacije $+$ i $\cdot$ na sledeći način:

$$(a_0, a_1, \dots, a_{n-1}) + (b_0, b_1, \dots, b_{n-1}) = (a_0 + b_0, a_1 + b_1, \dots, a_{n-1} + b_{n-1}),$$

$$(a_0, a_1, \dots, a_{n-1}) \cdot (b_0, b_1, \dots, b_{n-1}) = (c_0, c_1, \dots, c_{n-1}),$$

gde je

$$c_k = \sum_{j=0}^k a_j b_{k-j} + 2 \sum_{j=k+1}^{n-1} a_j b_{n+k-j}, \quad k = 0, 1, \dots, n-1,$$

(pri čemu se podrazumeva da je $\sum_{j=n}^{n-1} a_j b_{n+k-j} = 0$). Dokazati da je $(\mathbb{Q}^n, +, \cdot)$ polje.

Uputstvo. Dokazati da je $(\mathbb{Q}^n, +, \cdot) \cong \mathbb{Q}[x]/(x^n - 2)$.

594. Dokazati da je karakteristika polja 0 ili prost broj p .

595. Dokazati da polje racionalnih brojeva $\mathbb{Q}$ nema pravih potpolja.

596. Dokazati:

a) Polje karakteristike 0 sadrži potpolje izomorfno polju $\mathbb{Q}$.

b) Polje karakteristike p sadrži potpolje izomorfno polju $\mathbb{Z}_p$.

597. Ako je F polje karakteristike $p \neq 0$, onda za svako $x, y \in F$ važi

$$(x + y)^p = x^p + y^p.$$

Rešenje. Pošto je

$$(x + y)^p = \sum_{k=0}^p \binom{p}{k} x^{p-k} y^k,$$

a prost broj p je delitelj $\binom{p}{k}$ za svako $k \neq 0, p$, s obzirom da je karakteristika polja p , mora biti

$$\binom{p}{k} x^{p-k} y^k = 0$$

za svako $k \neq 0, p$. Dakle, $(x + y)^p = x^p + y^p$.

598. Neka je F konačno polje sa q elementima. Dokazati da za svako $x \in F$ važi

$$x^q = x.$$

Rešenje. Multiplikativna grupa polja F ima $q - 1$ element, pa na osnovu 1.51 za svako $x \neq 0$ mora biti $x^{q-1} = 1$, tj. $x^q = x$. Poslednja jednakost očividno važi i za $x = 0$.

599. Neka je F konačno polje sa q elemenata. Dokazati da je

$$x_1 x_2 \dots x_{q-1} + 1 = 0,$$

gde su $x_1, \dots, x_{q-1}$ svi elementi polja F osim nule.

Uputstvo. Dokazati da je $x^{-1} \neq x$ za svako $x \in F \setminus \{0\}$ osim za $x = \pm 1$.

PRIMEDBA. U specijalnom slučaju, kada je $F = \mathbb{Z}_p$, gde je p prost broj, dobija se da važi teorema Vilsona (Wilson):

$$(p - 1)! \equiv -1 \pmod{p}.$$

600. Neka je F konačno polje sa $q > 2$ elemenata. Dokazati da je

$$\sum_{x \in F} x = 0.$$

Rešenje. Na osnovu zadatka 598 elementi polja F su koreni polinoma $p(x) = x^q - x$. Kako je $q > 2$, to je u $p(x)$ koeficijent uz x^{q-1} nula, pa je na osnovu 2.80 i $\sum_{x \in F} x = 0$.

601. Neka je $f(x) \in \mathbb{Z}_p[x]$ nesvodljiv polinom nad $\mathbb{Z}_p$, $\deg f(x) = n$, p prost broj. Dokazati da je $\mathbb{Z}_p[x]/(f(x))$ polje sa p^n elemenata.

Uputstvo. Videti zadatak 563.

602. Za polje $\mathbb{Z}_3[x]/(\bar{1}x^2 + \bar{1}x + \bar{2})$ formirati aditivnu i multiplikativnu tablicu.

603. Konstruisati polje sa 4, 8 i 9 elemenata.

Uputstvo. Koristiti zadatak 601.

604. Naći generatore multiplikativne grupe polja sa 8, 9 i 13 elemenata.

605. Navesti primere konačnih polja F_1 i F_2 takvih da je aditivna grupa polja F_1 izomorfna multiplikativnoj grupi polja F_2 .

Uputstvo. Problem određivanja parova takvih polja je ekvivalentan sa problemom određivanja prostih brojeva oblika $2^p - 1$, p prost broj. Prosti brojevi ovog oblika nazivaju se Mersenov (Mersenne) prosti brojevi. Da li postoji beskonačno mnogo Mersenovih prostih brojeva je do danas nerešen problem. Detaljnije o ovome može se naći u kursovima teorije brojeva, na primer u: Hardy, G. H., Wright E. M., *An Introduction to the Theory of Numbers*, Oxford, 1960.

606. Neka je $f(x) \in \mathbb{Z}_p[x]$ polinom takav da je $f(a+b) = f(a) + f(b)$ za svako $a, b \in \mathbb{Z}_p$. Dokazati da je $f(x)$ oblika

$$f(x) = a_0x + a_1x^p + a_2x^{p^2} + \dots + a_kx^{p^k}$$

za neki prirodan broj p .

607. Dokazati da u polju F karakteristike p za svako $a, b \in F$, $a \neq b$, važi

$$(a-b)^{p-1} = \sum_{k=0}^{p-1} a^k b^{p-1-k}.$$

Uputstvo. Koristiti činjenicu da je u polju karakteristike p

$$(a-b)^p = a^p - b^p = (a-b) \sum_{k=0}^{p-1} a^k b^{p-1-k}.$$

608. Neka je R domen integriteta koji sadrži polje F .

a) Dokazati da se R može posmatrati kao vektorski prostor nad F , pri čemu je sabiranje vektora (elemenata iz R) sabiranje u domenu R , a proizvod

vektora $a \in R$ i skalara $\alpha \in F$ proizvod αa tih elemenata kao elemenata domena R .

b) Ako je dimenzija vektorskog prostora R nad F konačna, tada je R polje.

Rešenje. b) Neka je $a \in R$ i $a \neq 0$. Definišimo preslikavanje $f_a : R \rightarrow R$ sa $f_a : x \mapsto ax$. Lako se proverava da je preslikavanje f_a linearna transformacija vektorskog prostora R . Pošto je R domen integriteta, f_a je injektivno (jer bi inače iz $x \neq y$ i $ax = ay$ sledilo $a(x-y) = 0$ i R bi sadržavao delitelje nule). Injektivna linearna transformacija konačno dimenzionalnog vektorskog prostora je i surjektivna, pa postoji vektor x takav da je $ax = 1$, tj. a ima inverzni element.

609. Neka su R i S domeni integriteta takvi da je R potprsten prstena S i svaki element $s \in S$ je koren normalizovanog polinoma sa koeficijentima iz R . Dokazati da je R polje ako i samo ako je S polje.

Rešenje. Neka je R polje, neka je $s \in S$, $s \neq 0$, i neka je

$$p = x^n + a_1x^{n-1} + \dots + a_n, \quad a_i \in R, \quad i = 1, 2, \dots, n,$$

normalizovan polinom minimalnog stepena čiji je koren s . Mora biti $a_n \neq 0$, jer bi inače bilo

$$s(s^{n-1} + a_1s^{n-2} + \dots + a_{n-1}) = 0,$$

pa kako je S integralni domen

$$s^{n-1} + a_1s^{n-2} + \dots + a_{n-1} = 0,$$

tj. s bi zadovoljavalo polinom nižeg stepena od $\deg p$.

Neposredno se proverava da je

$$s^{-1} = -a_n^{-1}(s^{n-1} + a_1s^{n-2} + \dots + a_{n-1}) \in S,$$

tj. S je polje.

Neka je S polje i neka je $r \in R$, $r \neq 0$. Tada $r^{-1} \in S$, pa postoji normalizovan polinom

$$q = x^m + b_1x^{m-1} + \dots + b_m, \quad b_i \in R, \quad i = 1, 2, \dots, m,$$

takav da je $q(r^{-1}) = 0$. Otuda sledi da je

$$r^{-1} = -(b_1 + b_2r + \dots + b_mr^{m-1}) \in R,$$

tj. R je polje.

610. Neka je F komutativan prsten sa jedinicom. Dokazati da je F polje ako i samo ako za svaki prsten R svaki homomorfizam $f : F \rightarrow R$, takav da je $f(1) = 1$, mora biti monomorfizam.

611. Neka su $(F, +, \cdot)$ i $(K, +, \cdot)$ polja takva da je $(F, +) \cong (K, +)$ sa izomorfizmom f i važi $f(1_F) = 1_K$, $f(a^{-1}) = (f(a))^{-1}$ za svako $a \in F$, $a \neq 0$. Dokazati da je f izomorfizam polja F i K .

Rešenje. Neka su $a, b \in F \setminus \{0\}$, $a \neq b^{-1}$. Tada važi

$$aba = a - (a^{-1} + (b^{-1} - a)^{-1})^{-1}$$

(tehnički najjednostavnije se proverava tačnosti prethodne jednakosti može izvršiti tako što se inverzni elementi pišu u obliku razlomka ($\frac{1}{a}$ umesto a^{-1}), a zatim primene poznata pravila o računanju sa realnim razlomcima koja važe i u proizvoljnom polju), pa je

$$f(aba) = f(a)f(b)f(a)$$

za svako $a, b \in F$, jer poslednja jednakost očigledno važi i za $a = b^{-1}$, a važi i ako je neki od elemenata a, b jednak je 0_F (jer je f izomorfizam aditivnih grupa, pa je $f(0_F) = 0_K$). Otuda dobijamo da je za svako $a \in F$ (stavljajući $b = 1_F$)

$$f(a^2) = (f(a))^2.$$

Pošto je $(F, +) \cong (K, +)$, sledi da je $\text{Char } F = \text{Char } K$. Neka je $\text{Char } F \neq 2$. Tada iz

$$ab + ab = (a + b)^2 - a^2 - b^2$$

sledi da je

$$\begin{aligned} f(ab) + f(ab) &= f((a + b)^2 - a^2 - b^2) = \\ &= (f(a) + f(b))^2 - (f(a))^2 - (f(b))^2 = 2f(a)f(b), \end{aligned}$$

pa je $f(ab) = f(a)f(b)$.

Ako je $\text{Char } F = 2$, tada je

$$\begin{aligned} (f(ab))^2 &= f((ab)^2) = f(ab^2a) = \\ &= f(a)f(b^2)f(a) = (f(a))^2(f(b))^2 = (f(a)f(b))^2. \end{aligned}$$

Kako je polje K karakteristike 2 iz poslednje jednakosti sledi da mora biti

$$f(ab) = f(a)f(b).$$

612. Neka je R prsten sa jedinicom. R je telo ako i samo ako je u R rešiva jednačina $a + x = ax$ za svako $a \in R$, osim za jedno. Dokazati.

Rešenje. Ako je R telo, onda je $a + x = ax$ ekvivalentno sa $(a - 1)x = a$, pa za svako $a \neq 1$ postoji rešenje $x = (a - 1)^{-1}a$.

Pretpostavimo da jednačina $a + x = ax$ ima rešenje za svako $a \in R$, osim za jedno. Za $a = 1$ data jednačina nema rešenje jer je $1 \neq 0$, pa, prema tome, rešenje postoji za svako $a \neq 1$. Iz $(a - 1)x = a$ sledi $(a - 1)(x - 1) = 1$, tj. svako $b = a - 1 \in R$, $b \neq 0$, ima desni multiplikativni inverzni element.

613. Neka je K telo čiji je centar F (kao centar prstena, videti zadatak 407). Ako za svako $x \in K$ $x^2 \in F$, tada je K polje i $K = F$. Dokazati.

Rešenje. Jednostavno se proverava da je F polje. Neka je karakteristika polja F različita od 2, tj. $2 = 1 + 1 \neq 0$. Tada postoji 2^{-1} , pa je za svako $x \in K$

$$x = ((x + 1)2^{-1})^2 - ((x - 1)2^{-1}) \in F,$$

tj. $K = F$.

Neka je karakteristika F dva i neka $a \in K$, $a \neq F$. Tada postoji $b \in K$ takvo da je $ab \neq ba$. Označimo sa $c = ab - ba \neq 0$. Kako mora biti $\text{Char } K = \text{Char } F = 2$, onda je za svako $x \in K$, $-x = x$, pa je

$$c = ab + ba = (a + b)^2 - a^2 - b^2 \in F,$$

i

$$ac = a(ab) + (ab)a = (a + ab)^2 - a^2 - (ab)^2 \in F,$$

a kako postoji $c^{-1} \in F$, jer je $c \neq 0$, imamo

$$a = (ac)c^{-1} \in F.$$

Dokazali smo da ne postoji $a \in K \setminus F$, dakle $K = F$.

3.3 Proširenja polja

614. Naći potpolja polja kompleksnih brojeva $\mathbb{C}$ generisana sa:

a) $\{0, 1\}$, b) $\{0\}$, c) $\{0, 1, i\}$, d) $\{i, \sqrt{2}\}$,

e) $\{\sqrt{2}, \sqrt{3}\}$, f) $\mathbb{R}$, g) $\mathbb{R} \cup \{i\}$.

Rezultat. a) $\mathbb{Q}$, b) $\mathbb{Q}$, c) $\{a+bi \mid a, b \in \mathbb{Q}\}$, d) $\{a+bi+c\sqrt{2}+di\sqrt{2} \mid a, b, c, d \in \mathbb{Q}\}$, e) $\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$, f) $\mathbb{R}$, g) $\mathbb{C}$.

615. Dokazati da se svaki element polja $F(u)$, gde je u algebarski element stepena n nad poljem F , može prikazati na jedinstven način u obliku

$$a_0 + a_1u + \dots + a_{n-1}u^{n-1}, \quad a_i \in F, \quad i = 0, 1, \dots, n-1.$$

Rešenje. Neka je $f(u)/g(u)$, $g(u) \neq 0$, bilo koji element polja $F(u)$. Ako je $m(x)$ minimalni polinom elementa u nad poljem F , onda su $m(x)$ i $g(x)$ relativno prosti polinomi (jer minimalni polinom mora biti nesvodljiv), pa postoje polinomi $h(x)$ i $k(x)$, takvi da je

$$h(x)g(x) + k(x)m(x) = 1.$$

Odavde je za $x = u$, $h(u)g(u) = 1$ (jer je $m(u) = 0$). Prema tome,

$$\frac{f(u)}{g(u)} = \frac{f(u)}{g(u)} \cdot \frac{h(u)}{h(u)} = f(u)h(u) = f_1(u).$$

Ako je polinom $f_1(x)$ stepena većeg ili jednakog n , onda se deobom sa $m(x)$ dobija

$$f_1(x) = q(x)m(x) + r(x),$$

gde je stepen ostatka $r(x)$ manji od n ili je $r(x) = 0$, pa je odatle za $x = u$

$$f_1(u) = r(u) = a_0 + a_1u + \dots + a_{n-1}u^{n-1}, \quad a_i \in F.$$

Ako pretpostavimo da se $\frac{f(u)}{g(u)}$ može prikazati u navedenom obliku na dva načina:

$$\frac{f(u)}{g(u)} = a_0 + a_1u + \dots + a_{n-1}u^{n-1} = b_0 + b_1u + \dots + b_{n-1}u^{n-1},$$

biće

$$a_0 - b_0 + (a_1 - b_1)u + \dots + (a_{n-1} - b_{n-1})u^{n-1} = 0,$$

a to protivreči pretpostavci da je minimalni polinom elementa u stepena n .

616. U polju $\mathbb{Q}(a)$, gde je a koren jednačine

$$3x^3 - 2x^2 + x + 2 = 0,$$

element $\frac{a-1}{a^2-a+1}$ prikazati u obliku $\alpha a^2 + \beta a + \gamma$, $\alpha, \beta, \gamma \in \mathbb{Q}$.

Rešenje. Koristićemo postupak opisan u zadatku 615. Polinom

$$p(x) = 3x^3 - 2x^2 + x + 2$$

je nesvodljiv nad $\mathbb{Q}$, pa su $p(x)$ i $x^2 - x + 1$ uzajamno prosti polinomi, tj. postoje polinomi $f(x)$ i $g(x)$ takvi da je

$$f(x)p(x) + g(x)(x^2 - x + 1) = 1.$$

Euklidovim algoritmom odredićemo polinome $f(x)$ i $g(x)$. Kako je

$$p(x) = (x^2 - x + 1)(3x + 1) - x + 1,$$

$$x^2 - x + 1 = (-x + 1)(-x) + 1,$$

biće

$$(x^2 - x + 1) - (p(x) - (x^2 - x + 1)(3x + 1))(-x) = 1,$$

odnosno

$$xp(x) + (-3x^2 - x + 1)(x^2 - x + 1) = 1.$$

Iz gornje jednačine za $x = a$ dobijamo da je

$$(-3a^2 - a + 1)(a^2 - a + 1) = 1,$$

pa je, prema tome,

$$\frac{a-1}{a^2-a+1} = \frac{a-1}{a^2-a+1} \cdot \frac{-3a^2-a+1}{-3a^2-a+1} = -3a^3 + 2a^2 + 2a - 1.$$

Iz

$$3a^3 - 2a^2 + a + 2 = 0,$$

je

$$-3a^3 = -2a^2 + a + 2,$$

pa je

$$\frac{a-1}{a^2-a+1} = -2a^2 + a + 2 + 2a^2 + 2a - 1 = 3a + 1.$$

Do ovog rezultata može se doći i metodom neodređenih koeficijenata. Naime, iz jednačine

$$\frac{a-1}{a^2-a+1} = \alpha a^2 + \beta a + \gamma$$

odredićemo koeficijente α, β, γ . Ova jednačina je ekvivalentna sa

$$\begin{aligned} a-1 &= (a^2-a+1)(\alpha a^2 + \beta a + \gamma) = \\ &= \alpha a^4 + (\beta - \alpha)a^3 + (\alpha + \gamma - \beta)a^2 + (\beta - \gamma)a + \gamma, \end{aligned}$$

a kako je

$$\begin{aligned} a^3 &= (2a^2 - a - 2)/3, \\ a^4 &= a \cdot a^3 = (2a^3 - a^2 - 2a)/3 = (a^2 - 8a - 4)/9, \end{aligned}$$

biće

$$a-1 = \left(\frac{4\alpha}{9} - \frac{\beta}{3} + \gamma\right)a^2 + \left(-\frac{5\alpha}{9} + \frac{2\beta}{3} - \gamma\right)a + \left(\frac{2\alpha}{9} - \frac{2\beta}{3} + \gamma\right).$$

Kako je a stepena 3 nad $\mathbb{Q}$, svaki element polja $\mathbb{Q}(a)$ može se na jedinstven način prikazati pomoću $1, a, a^2$, pa mora biti

$$\frac{4\alpha}{9} - \frac{\beta}{3} + \gamma = 0, \quad -\frac{5\alpha}{9} + \frac{2\beta}{3} - \gamma = 1, \quad \frac{2\alpha}{9} - \frac{2\beta}{3} + \gamma = -1,$$

odakle se dobija $\alpha = 0, \beta = 3, \gamma = 1$. Prema tome, dobili smo i na ovaj način da je

$$\frac{a-1}{a^2-a+1} = 3a+1.$$

617. a) U polju $\mathbb{Q}(a)$, gde je a nula polinoma

$$x^4 + x^2 + 1,$$

napisati razlomak $\frac{a}{a-1}$ sa racionalnim imeniocem.

b) U polju $\mathbb{Q}(a)$, gde je a nula polinoma

$$x^3 - 6x^2 + 9x + 3,$$

napisati razlomak $\frac{1}{a^2-6a+8}$ sa racionalnim imeniocem.

618. U polju $\mathbb{Q}(a)$ razlomak $\frac{1}{a+\sqrt{2}}$ napisati sa racionalnim imeniocem, ako je a nula polinoma $x^3 + x + 3$.

619. Odrediti $[K : \mathbb{Q}]$ i naći bazu K nad $\mathbb{Q}$ ako je

a) $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$,

b) $K = \mathbb{Q}(i, \sqrt{3}, \varepsilon)$, gde je $\varepsilon = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$ kompleksan kubni koren iz jedinice,

c) $K = \mathbb{Q}(\sqrt[3]{5}, \sqrt{-2})$,

d) $K = \mathbb{Q}(\sqrt[3]{2}, a)$, gde je $a^4 + 6a + 2 = 0$,

e) $K = \mathbb{Q}(\sqrt{8}, 3 + \sqrt{50})$.

Rešenje. a) $\sqrt{2}$ je nula polinoma $x^2 - 2$ nesvodljivog nad $\mathbb{Q}$, bazu vektorskog prostora $\mathbb{Q}(\sqrt{2})$ nad poljem $\mathbb{Q}$ čine elementi $1, \sqrt{2}$, pa se svaki element iz $\mathbb{Q}(\sqrt{2})$ može prikazati u obliku $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$.

$\sqrt{3}$ je nula polinoma $x^2 - 3$ nesvodljivog nad $\mathbb{Q}(\sqrt{2})$, pa bazu $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ nad $\mathbb{Q}(\sqrt{2})$ čine elementi $1, \sqrt{3}$. Svaki element α polja $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ može se prikazati u obliku

$$\alpha = a + b\sqrt{2} + (c + d\sqrt{2})\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \quad a, b, c, d \in \mathbb{Q}.$$

Dobili smo da se svaki element polja $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ može izraziti kao linearna kombinacija elemenata $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$. Ovi elementi su linearno nezavisni (jer iz pretpostavke da je $\alpha = 0$ dobija se $a + b\sqrt{2} = 0$, $c + d\sqrt{3} = 0$, a odatle $a = b = c = d = 0$), pa prema tome, čine bazu polja $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ nad $\mathbb{Q}$.

Odavde odmah sledi da je

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4.$$

(Kako je $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, a $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, stepen proširenja $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ nad $\mathbb{Q}$ mogli smo odmah dobiti iz

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.)$$

b) Slično kao gore dobija se da je $1, i$ baza $\mathbb{Q}(i)$ nad $\mathbb{Q}$, a $1, i, \sqrt{3}, i\sqrt{3}$ baza $\mathbb{Q}(i, \sqrt{3})$ nad $\mathbb{Q}$.

Kako je

$$\varepsilon = -\frac{1}{2} + \frac{i\sqrt{3}}{2},$$

sledi da $\varepsilon \in \mathbb{Q}(i, \sqrt{3})$, pa se adjungovanjem ε polju $\mathbb{Q}(i, \sqrt{3})$ dobija opet to isto polje.

Dakle,

$$[\mathbb{Q}(i, \sqrt{3}, \varepsilon) : \mathbb{Q}] = 4.$$

620. Odrediti stepen proširenja $\mathbb{Q}(i, \sqrt{-5+12i})$ nad poljem racionalnih brojeva $\mathbb{Q}$.

Rešenje. $[\mathbb{Q}(i, \sqrt{-5+12i}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{-5+12i}) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}]$.
 $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ jer je $p(x) = x^2 + 1$ minimalni polinom za i , a $[\mathbb{Q}(i, \sqrt{-5+12i}) : \mathbb{Q}(i)] = 1$, jer iz formule

$$\sqrt{a+ib} = \pm \left(\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} + i \frac{b}{|b|} \sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}} \right) \text{ za } b \neq 0,$$

sledi

$$\sqrt{-5+12i} = \pm(2+3i) \in \mathbb{Q}(i). \text{ Prema tome,}$$

$$[\mathbb{Q}(i, \sqrt{-5+12i}) : \mathbb{Q}] = 1.$$

621. Naći sva potpolja polja $\mathbb{Q}(\sqrt[4]{-1})$ i odrediti stepen njihovog proširenja u odnosu na $\mathbb{Q}$.

Rešenje. Kako je $\sqrt[4]{-1} = \sqrt{i} = \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}$, sledi da je $\mathbb{Q}(\sqrt[4]{-1}) = \mathbb{Q}(i, \sqrt{2})$. Potpolja polja $\mathbb{Q}(\sqrt[4]{-1})$ su $\mathbb{Q}$, stepena proširenja 1, zatim polja $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ i $\mathbb{Q}(i\sqrt{2})$ od kojih je svako stepena proširenja 2 i samo polje $\mathbb{Q}(i, \sqrt{2})$ stepena proširenja 4 nad $\mathbb{Q}$.

622. Dokazati da je $\mathbb{Q}(\varepsilon_{2k+1}) = \mathbb{Q}(\varepsilon_{4k+2})$ za svako $k \in \mathbb{N}$, gde je ε_{2k+1} primitivan $(2k+1)$ -vi koren iz jedinice (3.38).

Uputstvo. Dokazati da je $-\varepsilon_{2k+1} \in \mathbb{Q}(\varepsilon_{2k+1})$ primitivan $(4k+2)$ -gi koren iz jedinice.

623. Odrediti sva međupolja između polja racionalnih brojeva $\mathbb{Q}$ i polja $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

Rezultat. $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{15})$, $\mathbb{Q}(\sqrt{30})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt{2}, \sqrt{15})$, $\mathbb{Q}(\sqrt{3}, \sqrt{10})$, $\mathbb{Q}(\sqrt{5}, \sqrt{6})$, $\mathbb{Q}(\sqrt{6}, \sqrt{10})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

$\mathbb{Q}(\sqrt{6}, \sqrt{10}) = \mathbb{Q}(\sqrt{6}, \sqrt{15}) = \mathbb{Q}(\sqrt{10}, \sqrt{15})$ jer su elementi svakog od ovih polja oblika $a + b\sqrt{6} + c\sqrt{10} + d\sqrt{15}$.

624. Ako je polje K algebarsko proširenje polja E , a E algebarsko proširenje polja F , onda je K algebarsko proširenje od F . Dokazati.

Rešenje. Neka je a bilo koji element proširenja K polja E i neka je

$$p(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_0, \quad b_k \in E, \quad k = 0, 1, \dots, n,$$

polinom čiji je koren a . Tada je

$$F_1 = F(b_0, b_1, \dots, b_n)$$

konačno proširenje polja F (na osnovu 3.16 (ii), 3.24 i 3.28), pa kako je a algebarski element nad F_1 (jer je koren polinoma $p(x)$ sa koeficijentima iz F_1) mora biti $F_1(a)$ konačno proširenje polja F_1 . Kako je, dakle, F_1 konačno proširenje polja F , a $F_1(a)$ konačno proširenje polja F_1 , sledi da je $F_1(a)$ konačno proširenje polja F . Na osnovu teoreme da je svako konačno proširenje algebarsko, zaključujemo da je $F_1(a)$ algebarsko proširenje polja F , pa je a algebarski element nad F .

Dokazli smo da je svaki element polja K algebarski nad F , a to znači da je K algebarsko proširenje polja F .

625. Neka su $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_{n-1} = F$ polja. Dokazati da važi

$$[F : K] = [K_{n-1} : K_{n-2}] \dots [K_2 : K_1][K_1 : K_0].$$

Uputstvo. Koristiti indukciju.

626. Ako je a algebarski element prostog stepena p nad poljem F , dokazati da ne postoji međupolje između F i $F(a)$ različito od F i od $F(a)$.

627. Neka je a algebarski element neparnog stepena nad poljem F . Dokazati da je $F(a^2) = F(a)$.

Rešenje. S obzirom da je $a^2 \in F(a)$, važi $F \subseteq F(a^2) \subseteq F(a)$.

Pošto je a koren polinoma $p(x) = x^2 - a^2$ stepena 2 sa koeficijentima iz $F(a^2)$, to je $[F(a) : F(a^2)] \leq 2$. Kako je

$$[F(a) : F] = [F(a) : F(a^2)][F(a^2) : F] = 2k + 1,$$

to je $[F(a) : F(a^2)] = 1$, pa je $F(a) = F(a^2)$.

628. Neka je α algebarski element nad poljem $\mathbb{Q}$. Dokazati da postoji ceo broj c takav da je $c\alpha$ nula normalizovanog polinoma sa celim koeficijentima.

Rešenje. Neka je $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Q}[x]$ polinom čija je nula α , i neka je s najmanji zajednički sadržalac imenilaca koeficijenata a_i , $i = 0, 1, \dots, n$. Ako jednakost

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_0 = 0$$

pomnožimo sa s , a sa b_i označimo $a_i s$, $i = 0, 1, \dots, n$, biće

$$(*) \quad b_n \alpha^n + b_{n-1} \alpha^{n-1} + \dots + b_0 = 0,$$

pri čemu su b_i , $i = 0, 1, \dots, n$, celi brojevi.

Množeći $(*)$ sa b_n^{n-1} dobijamo da je

$$(b_n \alpha)^n + b_{n-1} (b_n \alpha)^{n-1} + b_n b_{n-2} (b_n \alpha)^{n-2} + \dots + b_n^{n-2} b_1 (b_n \alpha) + b_n^{n-1} b_0 = 0,$$

pa je $c = b_n$.

629. Ispitati koji od sledećih brojeva su algebarski a koji transcendentni nad poljem racionalnih brojeva:

$$\sqrt[3]{2}, \pi^2, \pi + 2, \sqrt{2} + i\sqrt{3}.$$

Rešenje. $\sqrt[3]{2}$ je koren jednačine $x^3 - 2 = 0$, pa je, prema tome, algebarski element nad poljem $\mathbb{Q}$.

Ako pretpostavimo da je π^2 algebarski element nad $\mathbb{Q}$, onda postoji polinom $p(x)$ sa racionalnim koeficijentima takav da je $p(\pi^2) = 0$. Tada je

$$p(x^2) = q(x),$$

takođe polinom sa racionalnim koeficijentima i

$$p(\pi^2) = q(\pi) = 0,$$

tj. dobijamo da je π algebarski element nad $\mathbb{Q}$ (jer je koren polinoma $q(x)$). Ovo je kontradikcija, jer je poznato da je π transcendentan nad $\mathbb{Q}$, pa odatle zaključujemo da je π^2 transcendentan nad $\mathbb{Q}$.

Na sličan način se može pokazati da je $\pi + 2$ transcendentan, a $\sqrt{2} + i\sqrt{3}$ algebarski element nad poljem racionalnih brojeva.

630. Neka je a realan broj. Dokazati da je bar jedan od brojeva $a + \pi$, $a\pi$, transcendentan nad poljem racionalnih brojeva.

Rešenje. Pretpostavimo da su i $a + \pi$ i $a\pi$ algebarski nad $\mathbb{Q}$. Tada je $F = \mathbb{Q}(a + \pi, a\pi)$ konačno proširenje polja $\mathbb{Q}$, pa je na osnovu 3.25 F algebarsko proširenje polja $\mathbb{Q}$. $((a + \pi)^2 - 4a\pi) \in F$, pa je $(a + \pi)^2 - 4a\pi$ algebarski element nad $\mathbb{Q}$. Tada je i $\pi - a = \sqrt{(a + \pi)^2 - 4a\pi}$ algebarski element nad poljem $\mathbb{Q}$ (ako je neki element b nula polinoma $p(x)$, onda je $\sqrt{b}$ nula polinoma $p(x^2)$). Dakle, $K = \mathbb{Q}(a + \pi, a\pi, \sqrt{(a + \pi)^2 - 4a\pi})$ je konačno, a to znači i algebarsko proširenje polja $\mathbb{Q}$.

Međutim, onda je

$$\frac{1}{2}\sqrt{(a + \pi)^2 - 4a\pi} + \frac{1}{2}(a + \pi) = \frac{1}{2}(\pi - a) + \frac{1}{2}(\pi + a) = \pi \in K,$$

što je protivrečnost, jer je π transcendentan nad $\mathbb{Q}$.

631. Polje $\mathbb{Z}_3$ proširiti do polja K tako da polinom

$$p(x) = \bar{1}x^2 + \bar{1}x + \bar{2} \in \mathbb{Z}_3[x]$$

ima koren u K .

Rešenje. Dati polinom je nesvodljiv nad $\mathbb{Z}_3$, pa je faktor prsten $K = \mathbb{Z}_3[x]/I$, gde je I glavni ideal $(\bar{1}x^2 + \bar{1}x + \bar{2})$, polje. Polje K ima devet elemenata

$$K = \{a + bx + I \mid a, b \in \mathbb{Z}_3\} = \\ = \{I, \bar{1} + I, \bar{2} + I, \bar{1}x + I, \bar{1} + \bar{1}x + I, \bar{2} + \bar{1}x + I, \bar{2}x + I, \bar{1} + \bar{2}x + I, \bar{2} + \bar{2}x + I\}.$$

Preslikavanje $f : \mathbb{Z}_3 \rightarrow K$ definisano sa $f(a) = a + I$ je izomorfizam polja $\mathbb{Z}_3$ i potpolja $\{I, \bar{1} + I, \bar{2} + I\}$ polja K , tj. $\mathbb{Z}_3$ se može potopiti u K , pa ako se svaki element $a \in \mathbb{Z}_3$ identifikuje sa svojim skupom $a + I \in K$ može se smatrati da je K proširenje polja $\mathbb{Z}_3$.

Pokažimo da je $\bar{1}x + I \in K$ koren datog polinoma (s obzirom na navedeni izomorfizam umesto elemenata iz $\mathbb{Z}_3$ za koeficijente polinoma uzimamo njima odgovarajuće elemente iz K). Zaista,

$$\begin{aligned} p(\bar{1}x + I) &= (\bar{1} + I)(\bar{1}x + I)^2 + (\bar{1} + I)(\bar{1}x + I) + \bar{2} + I = \\ &= \bar{1}x^2 + I + \bar{1}x + I + \bar{2} + I = (\bar{1}x^2 + \bar{1}x + \bar{2}) + I = I. \end{aligned}$$

632. Neka je polje K konačno proširenje polja F stepena n . Dokazati da je polje K izomorfno potprstenu K' , koji je polje, prstena $F^{n,n}$ svih matrica formata $n \times n$ nad poljem F .

Uputstvo. K je n -dimenzionalni vektorski prostor nad F , a preslikavanje $f_a : K \rightarrow K$ definisano sa $f_a(x) = ax$, gde je a fiksiran element polja K , je za proizvoljno $a \in K$ linearna transformacija vektorskog prostora K . Ako je uočena neka baza prostora K i sa $[f_a]$ označena matrica linearne transformacije f_a u odnosu na tu bazu, onda je preslikavanje $\varphi : K \rightarrow F^{n,n}$ definisano sa $\varphi : a \mapsto [f_a]$ monomorfizam polja K u prsten $F^{n,n}$, tj. ako uvedemo oznaku $K' = \text{Im } \varphi$, onda je $K' \subseteq F^{n,n}$ polje izomorfno polju K .

PRIMEDBA. Polje K' naziva se matična reprezentacija polja K nad poljem F .

633. Naći matičnu reprezentaciju (prethodni zadatak) polja $K = \mathbb{Z}_2[x]/(\bar{1}x^2 + \bar{1}x + \bar{1})$ nad poljem $\mathbb{Z}_2$.

Rešenje. Elementi polja K su $I, \bar{1} + I, \bar{1}x + I, \bar{1} + \bar{1}x + I$, gde je sa I označen glavni ideal $(\bar{1}x^2 + \bar{1}x + \bar{1})$. Potpolje $F = (I, \bar{1} + I)$ polja K je izomorfno sa $\mathbb{Z}_2$, pa ako se elementi polja F identifikuju sa odgovarajućim elementima polja $\mathbb{Z}_2$, onda je matična reprezentacija polja K nad $\mathbb{Z}_2$ ustvari matična reprezentacija polja K nad F .

Radi jednostavnijeg pisanja u daljem ćemo suskupove koji čine polje K označavati samo pomoću predstavnika tih skupova (suskup $a + I$ označavaćemo samo sa a), onda je $K = \{\bar{0}, \bar{1}, \bar{1}x, \bar{1} + \bar{x}\}$ a operacije u polju K se izводе po modulu $\bar{1}x^2 + \bar{1}x + \bar{1}$. Tako, na primer,

$$\bar{1}x \cdot (\bar{1} + \bar{1}x) = \bar{1}x + \bar{1}x^2 = \bar{1}x + (\bar{1}x + \bar{1}) = \bar{1},$$

gde je korišćeno $\bar{1}x^2 + \bar{1}x + \bar{1} = \bar{0}$.

Polje K posmatrano kao vektorski prostor nad F je dvodimenzionalni prostor sa bazom $e_1 = \bar{1}$ i $e_2 = \bar{1}x$. S obzirom da su elementi i -te kolone matrice koja odgovara jednoj linearnoj transformaciji koordinate slike i -tog bazisnog vektora, biće

$$f_{\bar{0}}(e_1) = \bar{0} \cdot \bar{1} + \bar{0} \cdot x, \quad f_{\bar{0}}(e_2) = \bar{0} \cdot \bar{1} + \bar{0} \cdot x, \quad \text{pa elementu } \bar{0} \text{ odgovara } \begin{bmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{bmatrix},$$

$$f_{\bar{1}}(e_1) = \bar{1} \cdot \bar{1} + \bar{0} \cdot x, \quad f_{\bar{1}}(e_2) = \bar{0} \cdot x + \bar{1} \cdot x, \quad \text{pa elementu } \bar{1} \text{ odgovara } \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix},$$

$$f_{\bar{1}x}(e_1) = \bar{0} \cdot \bar{1} + \bar{1} \cdot x, \quad f_{\bar{1}x}(e_2) = \bar{1} \cdot \bar{1} + \bar{1} \cdot x, \quad \text{pa elementu } \bar{1}x \text{ odgovara } \begin{bmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{bmatrix},$$

$$f_{\bar{1}+\bar{1}x}(e_1) = \bar{1} \cdot \bar{1} + \bar{1} \cdot x,$$

$$f_{\bar{1}+\bar{1}x}(e_2) = (\bar{1} + \bar{1}x) \cdot x = \bar{1}x + \bar{1}x^2 = \bar{1}x + \bar{1} + \bar{1}x = \bar{1} = \bar{1} \cdot \bar{1} + \bar{0} \cdot x,$$

pa elementu $\bar{1} + \bar{1}x$ odgovara $\begin{bmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{bmatrix}$.

Dakle, polje $(K', +, \cdot)$, gde je

$$K' = \left\{ \begin{bmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{bmatrix}, \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{bmatrix} \right\},$$

a operacije polja su sabiranje i množenje matrica, je matrična reprezentacija polja K nad $\mathbb{Z}_2$.

634. Naći matričnu reprezentaciju (v. zadatak 632) polja K iz zadatka 631 nad poljem $\mathbb{Z}_3$.

Rezultat.

$$K' = \left\{ \begin{bmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{bmatrix}, \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{bmatrix}, \begin{bmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{2} \end{bmatrix}, \begin{bmatrix} \bar{0} & \bar{2} \\ \bar{2} & \bar{1} \end{bmatrix}, \right. \\ \left. \begin{bmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{bmatrix}, \begin{bmatrix} \bar{2} & \bar{2} \\ \bar{2} & \bar{0} \end{bmatrix}, \begin{bmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{1} & \bar{2} \\ \bar{2} & \bar{2} \end{bmatrix} \right\}.$$

635. a) Dokazati da je $F = \left\{ \begin{bmatrix} a_1 & 2a_2 \\ a_2 & a_1 \end{bmatrix} \mid a_1, a_2 \in \mathbb{Q} \right\}$ potprsten, koji je polje, prstena matrica $\mathbb{Q}^{2,2}$ i da je F izomorfno polju $\mathbb{Q}(\sqrt{2})$.

b) Neka je d ceo broj koji je proizvod različitih prostih brojeva, $a_k \in \mathbb{Q}$, $k = 0, 1, \dots, n-1$, i neka je $A_{a_1 a_2 \dots a_k} = [a_{ij}] \in \mathbb{Q}^{n,n}$ matrica definisana sa

$$a_{ij} = \begin{cases} a_{i-j} & i \geq j, \\ da_{n+i-j}, & i < j, \end{cases} \quad i, j = 1, 2, \dots, n.$$

Dokazati da je skup matrica

$$F = \{A_{a_1 a_2 \dots a_k} \mid a_1, a_2, \dots, a_k \in \mathbb{Q}\}$$

potprsten koji je polje, prstena matrica $\mathbb{Q}^{n,n}$ i da je F izomorfno polju $\mathbb{Q}(\sqrt[n]{d})$.

636. Dokazati da je polje $\mathbb{Q}(\alpha)$, gde je α nula polinoma $x^3+px+q \in \mathbb{Q}[x]$ nesvodljivog nad $\mathbb{Q}$, izomorfno potpolju

$$F = \left\{ \begin{bmatrix} a_0 & -qa_2 & -qa_1 \\ a_1 & a_0 - pa_2 & -a_1p - a_2q \\ a_2 & a_1 & a_0 - pa_2 \end{bmatrix} \mid a_0, a_1, a_2 \in \mathbb{Q} \right\}$$

prstena $\mathbb{Q}^{3,3}$.

637. Dokazati da polje realnih brojeva $\mathbb{R}$ nije jednostruko proširenje polja racionalnih brojeva.

Uputstvo. S obzirom da je $\mathbb{Q}$ prebrojiv skup, treba dokazati da je svako jednostruko proširenje polja $\mathbb{Q}$ prebrojiv skup. $\mathbb{R}$ je neprebrojiv skup, pa ne može biti jednostruko proširenje polja $\mathbb{Q}$.

638. Neka je $A \subseteq \mathbb{C}$ skup svih algebarskih brojeva nad poljem racionalnih brojeva $\mathbb{Q}$. Dokazati da je A beskonačno proširenje polja $\mathbb{Q}$.

Rešenje. Na osnovu 3.24 i 3.25 kompleksan broj $a \in \mathbb{C}$ pripada A ako i samo ako je stepen proširenja $[\mathbb{Q}(a) : \mathbb{Q}]$ konačan. Ako su $a, b \in A$, onda je na osnovu 3.28

$$[\mathbb{Q}(a, b) : \mathbb{Q}] = [\mathbb{Q}(a, b) : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}].$$

$[\mathbb{Q}(a) : \mathbb{Q}] < \infty$ jer je $a \in A$, element b je algebarski nad $\mathbb{Q}$, pa je algebarski i nad $\mathbb{Q}(a)$, prema tome, $[\mathbb{Q}(a, b) : \mathbb{Q}(a)] < \infty$, dakle, i $[\mathbb{Q}(a, b) : \mathbb{Q}] < \infty$. Pošto $a + b, -a, ab \in \mathbb{Q}(a, b)$ i za $a \neq 0$, $a^{-1} \in \mathbb{Q}(a, b)$, sledi da je svako od polja $\mathbb{Q}(a + b)$, $\mathbb{Q}(-a)$, $\mathbb{Q}(ab)$, $\mathbb{Q}(a^{-1})$ konačno proširenje polja $\mathbb{Q}$. To znači da $a + b, -a, ab, a^{-1}$ pripadaju A , tj. A je potpolje polja $\mathbb{C}$.

Na osnovu Ajzenštajnovog kriterijuma (2.71) može se pokazati da postoje polinomi nesvodljivi nad $\mathbb{Q}$ proizvoljno velikog stepena. Prema tome, na osnovu 3.24 sledi da A ne može biti konačno proširenje polja $\mathbb{Q}$.

639. Neka je $F_k = \mathbb{Q}(\sqrt[k]{2})$, $k = 1, 2, \dots$. Dokazati:

- a) $A = \bigcup_{k=1}^{\infty} F_k$ je polje.
- b) A je algebarsko proširenje polja $\mathbb{Q}$.
- c) A nije konačno proširenje polja $\mathbb{Q}$.

640. Neka je F polje, a $K = F(\alpha)$ i neka je L međupolje ($F \subseteq L \subseteq K$) različito od F . Dokazati da je K konačno proširenje polja L .

Rešenje. Ako je α algebarski element nad F , tvrđenje očigledno važi (3.24, 3.28).

Neka je α transcendentan element nad F . Svaki element polja K je onda oblika $\frac{f(\alpha)}{g(\alpha)}$, gde je $f(x), g(x) \in F[x]$, $g(x) \neq 0$, (3.26, 3.27).

Neka je $\beta = \frac{f(\alpha)}{g(\alpha)} \in L$. Tada α zadovoljava polinomnu jednačinu $\beta g(x) - f(x) = 0$ čiji su koeficijenti iz L , očigledno je $K = L(\alpha)$, pa je K jednostruko algebarsko proširenje polja L , a to znači i konačno proširenje.

641. Neka je u element transcendentan nad poljem racionalnih brojeva $\mathbb{Q}$, $L = \mathbb{Q}(u)$ i $v = \frac{u^3}{u+1}$. Dokazati da je L jednostruko proširenje polja $K = \mathbb{Q}(v)$ i odrediti $[L : K]$.

642. Neka je K proširenje polja F . Ako je $\alpha \in K$ algebarski element nad $F(\beta)$ za neko $\beta \in K$ i ako je α transcendentan element nad F , onda je β algebarski element nad poljem $F(\alpha)$. Dokazati.

643. Neka je a nula polinoma

$$x^3 + x + 3,$$

nesvodljivog nad poljem $\mathbb{Q}$. Polinom $x^2 - 2$ je nesvodljiv nad $\mathbb{Q}$. Da li je $x^2 - 2$ svodljiv nad poljem $\mathbb{Q}(a)$?

Rešenje. Koristićemo teoremu: ako je K proširenje stepena n polja F , onda svaki element $\alpha \in K$ ima nad F stepen koji je delitelj broja n (što neposredno sledi iz $n = [K : F] = [K : F(\alpha)][F(\alpha) : F]$).

a je nula polinoma $x^3 + x + 3$ nesvodljivog nad $\mathbb{Q}$, pa je $[\mathbb{Q}(a) : \mathbb{Q}] = 3$, a ako je b nula polinoma $x^2 - 2$ nesvodljivog nad $\mathbb{Q}$, onda je $[\mathbb{Q}(b) : \mathbb{Q}] = 2$. Pretpostavimo da je $x^2 - 2$ svodljiv nad $\mathbb{Q}(a)$. Tada je taj polinom jednak proizvodu dva linearna polinoma sa koeficijentima iz $\mathbb{Q}(a)$, što znači da $b \in \mathbb{Q}(a)$. Međutim, b je stepena 2 nad $\mathbb{Q}$, $\mathbb{Q}(a)$ je stepena 3 nad $\mathbb{Q}$, a 2 nije delitelj broja 3, pa na osnovu navedene teoreme dolazimo do protivrečnosti.

Ptoma tome, $x^2 - 2$ je nesvodljiv nad $\mathbb{Q}(a)$.

644. Ako je polinom $p(x)$ stepena n nesvodljiv nad poljem F , a K je konačno proširenje od F stepena koji je uzajamno prost sa n , dokazati da je $p(x)$ nesvodljiv nad K .

645. Dokazati da je $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

Rešenje. Očigledno je $\mathbb{Q}(\sqrt{3} + \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5})$. S druge strane,

$$\frac{1}{4}((\sqrt{3} + \sqrt{5})^3 - 14(\sqrt{3} + \sqrt{5})) = \sqrt{3}, \text{ pa } \sqrt{3} \in \mathbb{Q}(\sqrt{3} + \sqrt{5}),$$

a tada i

$$(\sqrt{3} + \sqrt{5}) - \frac{1}{4}((\sqrt{3} + \sqrt{5})^3 - 14(\sqrt{3} + \sqrt{5})) = \sqrt{5} \in \mathbb{Q}(\sqrt{3} + \sqrt{5}),$$

pa je $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

646. Odrediti element a algebarski nad $\mathbb{Q}$ tako da bude

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbb{Q}(a).$$

647. Neka je $p(x)$ polinom sa racionalnim koeficijentima čija je jedna nula a . Naći polinom $q(x) \in \mathbb{Q}[x]$ čija je nula $f(a)$ ako je:

a) $p(x) = x^3 - 2x - 2, \quad f(a) = a^2 - 1,$

b) $p(x) = x^3 + 3x^2 - 3, \quad f(a) = a^2 + a.$

Rešenje. a) Polinom $p(x)$ je nesvodljiv po Ajzenštajnovom kriterijumu (2.71), pa je $\mathbb{Q}(a) = K$ konačno proširenje stepena 3 nad $\mathbb{Q}$. K je trodimenzionalni vektorski prostor nad $\mathbb{Q}$ čija je jedna baza $\{1, a, a^2\}$. Elementi $1, f(a), f^2(a), f^3(a) \in \mathbb{Q}(a)$ moraju biti zavisni (kao vektori), tj.

$$\alpha + \beta f(a) + \gamma f^2(a) + \delta f^3(a) = 0,$$

gde je bar jedan od elemenata $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$ različit od nule, pa je $q(x) = \alpha + \beta x + \gamma x^2 + \delta x^3$.

Za $f(a) = a^2 - 1$, koristeći $a^3 - 2a - 2 = 0$, dobijamo

$$f^2(a) = 2a + 1 \quad \text{ i } \quad f^3(a) = a^2 + 2a + 3,$$

pa je

$$\alpha + \beta(a^2 - 1) + \gamma(2a + 1) + \delta(a^2 + 2a + 3) = 0,$$

tj.

$$(\alpha - \beta + \gamma + 3\delta) \cdot 1 + (2\gamma + 2\delta)a + (\beta + \delta)a^2 = 0.$$

$\{1, a, a^2\}$ je baza od K , pa mora biti

$$\alpha - \beta + \gamma + 3\delta = 0, \quad 2\gamma + 2\delta = 0, \quad \beta + \delta = 0.$$

Jedno netrivialno rešenje ovog sistema je

$$\alpha = -3, \quad \beta = \gamma = -1, \quad \delta = 1,$$

pa je $q(x) = x^3 - x^2 - x - 3$.

648. Ako je a nula polinoma $x^3 - x + 1$ odrediti minimalni polinom elementa $b = 2a^2 - 3a + 2$ nad poljem racionalnih brojeva $\mathbb{Q}$.

Rezultat. $x^3 - 10x^2 + 5x - 1$.

649. Formirati polinome sa racionalnim koeficijentima čije su nule:

$$\begin{array}{ll} a) \quad \sqrt{3}, 2, & e) \quad \sqrt[3]{2} + \sqrt[3]{4}, \\ b) \quad 1, 3 & f) \quad \sqrt{2} + \sqrt{3}, \\ c) \quad -2 + i, 3 - 2i, & g) \quad \sqrt[3]{2} + \sqrt[3]{3}. \\ d) \quad \sqrt[4]{5} + \sqrt{5}, \end{array}$$

Rešenje. a) Ako je $\sqrt{3}$ nula polinoma sa racionalnim koeficijentima, onda njegova nula mora biti i broj $-\sqrt{3}$ koji je konjugovan sa $\sqrt{3}$ nad $\mathbb{Q}$ ($\sqrt{3}$ i $-\sqrt{3}$ su koreni polinoma $x^2 - 3$ nesvodljivog nad $\mathbb{Q}$ (v. 3.39)). Prema tome, traženi polinom je

$$(x - \sqrt{3})(x + \sqrt{3})(x - 2) = x^3 - 2x^2 - 3x + 6.$$

d) Uvedimo oznaku $a = \sqrt[4]{5}$. Potrebno je naći polinom sa racionalnim koeficijentima čija je nula $a + a^2$. Brojevi konjugovani sa a nad poljem $\mathbb{Q}$ su ia , $-a$, $-ia$ (to su nule polinoma $x^4 - 5$ nesvodljivog nad $\mathbb{Q}$), pa su, prema tome, sa $a + a^2$ konjugovani brojevi $ia - a^2$, $-a + a^2$, $-ia - a^2$. Traženi polinom će onda biti

$$\begin{aligned} & (x - a - a^2)(x - ia + a^2)(x + a - a^2)(x + ia + a^2) = \\ & = ((x - a^2)^2 - a^2)((x + a^2)^2 + a^2) = x^4 - 10x^2 - 20x + 20. \end{aligned}$$

Ovaj polinom je nesvodljiv nad $\mathbb{Q}$ po Ajzenštajnovom kriterijumu, pa je to minimalni polinom nad $\mathbb{Q}$ elementa

$$\sqrt[4]{5} + \sqrt{5}.$$

(Do istog rezultata moglo se doći i postupkom opisanom u zadatku 647.)

f) Brojevi konjugovani nad $\mathbb{Q}$ sa $\sqrt{2} + \sqrt{3}$ su

$$\sqrt{2} - \sqrt{3}, \quad -\sqrt{2} + \sqrt{3}, \quad -\sqrt{2} - \sqrt{3},$$

pa je traženi polinom

$$\begin{aligned} (x - \sqrt{2} - \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x + \sqrt{2} - \sqrt{3})(x + \sqrt{2} + \sqrt{3}) = \\ = (x^2 - 5 - 2\sqrt{6})(x^2 - 5 + 2\sqrt{6}) = x^4 - 10x^2 + 1. \end{aligned}$$

Do istog rezultata može se doći i na sledeći način:

Označimo sa $u = \sqrt{2}$, $v = \sqrt{3}$. Tada je $u^2 = 2$, $v^2 = 3$, pa iz $x = u + v$ sledi

$$x^2 = u^2 + 2uv + v^2 = 5 + 2uv.$$

Dalje, iz $x^2 - 5 = 2uv$ sledi

$$x^4 - 10x^2 + 25 = 24,$$

pa je $x^4 - 10x^2 + 1$ polinom čija je nula $\sqrt{2} + \sqrt{3}$.

650. a) Naći polinom sa racionalnim koeficijentima čija je nula

$$\alpha = \sqrt[3]{25} + 4\sqrt[3]{5} - 1.$$

b) Na osnovu rezultata pod a) razlomak

$$\frac{2\sqrt[3]{5}}{\sqrt[3]{25} + 4\sqrt[3]{5} - 1},$$

napisati sa racionalnim imeniocem.

Rešenje. a) Na jedan od ranije navedenih načina odredićemo polinom čija je nula α :

$$p(x) = x^3 + 3x^2 - 57x - 404, \quad p(\alpha) = 0.$$

b) Kako je

$$\alpha^3 + 3\alpha^2 - 57\alpha = 404,$$

odnosno $\alpha(\alpha^2 + 3\alpha - 57) = 404$, biće

$$\frac{2\sqrt[3]{5}}{\sqrt[3]{25} + 4\sqrt[3]{5} - 1} = \frac{2\sqrt[3]{5}}{\alpha} \cdot \frac{\alpha^2 + 3\alpha - 57}{\alpha^2 + 3\alpha - 57} =$$

$$= \frac{2\sqrt[3]{5}(\alpha^2 + 3\alpha - 57)}{404} = \frac{9\sqrt[3]{25} - 19\sqrt[3]{5} + 85}{202}.$$

651. Naći polinom $p(x) \in \mathbb{Q}[x]$ takav da je $p(\sqrt{2} + \sqrt{5}) = 2\sqrt{2} + 5\sqrt{5}$.

Rešenje. Označimo sa $u = \sqrt{2}$, $v = \sqrt{5}$. Tada iz

$$x = u + v$$

sledi

$$x^3 = 17u + 11v.$$

Rešavajući po u i v sistem koji čine poslednje dve jednačine dobijamo

$$u = \frac{x^3 - 11x}{6}, \quad v = \frac{17x - x^3}{6}.$$

Oдавde je

$$2u + 5v = 2 \frac{x^3 - 11x}{6} + 5 \frac{17x - x^3}{6} = \frac{21}{2}x - \frac{1}{2}x^3,$$

pa je

$$p(x) = -\frac{1}{2}x^3 + \frac{21}{2}x.$$

652. Odrediti faktorizacijska polja sledećih polinoma nad $\mathbb{Q}$:

$$\begin{array}{ll} a) & x^3 - 2, \\ b) & x^3 - x^2 - x - 2, \end{array} \quad \begin{array}{ll} c) & x^4 - 5, \\ d) & (x^2 - 2)(x^2 - 3)(x^2 - 5). \end{array}$$

Rešenje. Faktorizacijsko polje polinoma $x^3 - 2$ mora sadržati nulu $\sqrt[3]{2}$. U polju $\mathbb{Q}(\sqrt[3]{2})$ je

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}) = (x - \sqrt[3]{2})p(x).$$

Polinom $p(x)$ nema realne korene, pa je, prema tome, nesvodljiv nad $\mathbb{Q}(\sqrt[3]{2})$.

Koreni polinoma $p(x)$ su $\varepsilon\sqrt[3]{2}$ i $\varepsilon^2\sqrt[3]{2}$, gde je $\varepsilon = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$, pa je faktorizacijsko polje datog polinoma $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$, a stepen proširenja je $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}] = 6$.

b) $x^3 - x^2 - x - 2 = (x - 2)(x^2 + x + 1)$, pa je faktorizacijsko polje tog polinoma $\mathbb{Q}(\varepsilon)$, gde je $\varepsilon = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$, kompleksan kubni koren iz jedinice. Ovde je $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = 2$.

c) Koreni jednačine $x^4 - 5 = 0$ su

$$x_1 = \sqrt[4]{5}, \quad x_2 = -\sqrt[4]{5}, \quad x_3 = i\sqrt[4]{5}, \quad x_4 = -i\sqrt[4]{5},$$

pa je faktorizacijsko polje

$$\mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(\sqrt[4]{5}, -\sqrt[4]{5}, i\sqrt[4]{5}, -i\sqrt[4]{5}) = \mathbb{Q}(\sqrt[4]{5}, i).$$

Stepen proširenja je $[\mathbb{Q}(\sqrt[4]{5}, i) : \mathbb{Q}] = 8$.

d) Faktorizacijsko polje je $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, a stepen proširenja je $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 8$.

653. Jedna nula polinoma $x^4 + 3x^3 + 6x^2 + 12x + 8$ je $-2i$. Naći sve nule tog polinoma.

654. Odrediti a i b u polinomu $p(x) = x^3 - 6x^2 + ax + b$ tako da polinom ima nulu $1 - i\sqrt{5}$, a zatim rešiti jednačinu $p(x) = 0$.

655. Dokazati da konačno polje ne može biti algebarski zatvoreno.

Rešenje. Neka su $a_1, a_2, \dots, a_n$, ($a_1 \neq 0$), svi elementi konačnog polja F . Tada polinom

$$p(x) = (x - a_1)(x - a_2) \dots (x - a_n) + a_1,$$

nema nijednu nulu u F jer je $p(a_i) = a_1$, $i = 1, 2, \dots, n$, pa na osnovu 3.35 F nije algebarski zatvoreno.

656. U polju $\mathbb{C}$, potpolja $\mathbb{Q}(i)$ i $\mathbb{Q}(\sqrt{2})$ su izomorfni vektorski prostori nad poljem $\mathbb{Q}$, ali nisu izomorfna polja. Dokazati.

657. Navesti potpolje polja $\mathbb{C}$ koje nije potpolje polja realnih brojeva, izomorfno polju

$$\text{a) } \mathbb{Q}(\sqrt[3]{2}), \quad \text{b) } \mathbb{Q}(\sqrt[4]{3}).$$

Rešenje. Koristićemo teoremu: ako su a i b nule polinoma nesvodljivog nad poljem F , onda su polja $F(a)$ i $F(b)$ izomorfna.

a) Nule polinoma $x^3 - 2$ nesvodljivog nad $\mathbb{Q}$ su

$$\sqrt[3]{2}, \quad \varepsilon \sqrt[3]{2}, \quad \varepsilon^2 \sqrt[3]{2},$$

gde je $\varepsilon = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$ kompleksan kubni koren iz jedinice.

Prema tome, polje $\mathbb{Q}(\varepsilon \sqrt[3]{2})$ je jedno polje kompleksnih brojeva izomorfno polju $\mathbb{Q}(\sqrt[3]{2})$.

658. Neka je α koren polinoma $x^2 - 2 \in \mathbb{Q}[x]$, a β koren polinoma $x^2 - 4x + 2 \in \mathbb{Q}[x]$. Dokazati da su proširenja $\mathbb{Q}(\alpha)$ i $\mathbb{Q}(\beta)$ izomorfna.

Rešenje. Polinomi $x^2 - 2$ i $x^2 - 4x + 2$ su normalizovani nesvodljivi polinomi nad $\mathbb{Q}$, pa je $x^2 - 2$ minimalni polinom za α nad poljem $\mathbb{Q}$, a $x^2 - 4x + 2$ je minimalni polinom za β nad $\mathbb{Q}$. Prema tome, svaki element polja $\mathbb{Q}(\alpha)$ se na jedinstven način može prikazati u obliku

$$a_0 + a_1\alpha, \quad a_0, a_1 \in \mathbb{Q},$$

a svaki element polja $\mathbb{Q}(\beta)$ se na jedinstven način može prikazati u obliku

$$b_0 + b_1\beta, \quad b_0, b_1 \in \mathbb{Q}.$$

Dokazaćemo da je preslikavanje $\varphi : \mathbb{Q}(\alpha) \rightarrow \mathbb{Q}(\beta)$ definisano sa

$$\varphi(a_0 + a_1\alpha) = a_0 + a_1(\beta - 2)$$

izomorfizam polja $\mathbb{Q}(\alpha)$ i $\mathbb{Q}(\beta)$.

φ je očigledno bijekcija. Ako su $a_0 + a_1\alpha, b_0 + b_1\alpha \in \mathbb{Q}(\alpha)$, neposredno sledi da je $\varphi(a_0 + a_1\alpha + b_0 + b_1\alpha) = \varphi(a_0 + a_1\alpha) + \varphi(b_0 + b_1\alpha)$.

$$\begin{aligned} \varphi((a_0 + a_1\alpha)(b_0 + b_1\alpha)) &= \varphi(a_0b_0 + (a_0b_1 + a_1b_0)\alpha + a_1b_1\alpha^2) = \\ &= \varphi(a_0b_0 + 2a_1b_1 + (a_0b_1 + a_1b_0)\alpha) = a_0b_0 + 2a_1b_1 + (a_0b_1 + a_1b_0)(\beta - 2) = \\ &= a_0b_0 + (a_0b_1 + a_1b_0)(\beta - 2) + a_1b_1(\beta^2 - 4\beta + 4) = \\ &= (a_0 + a_1(\beta - 2))(b_0 + b_1(\beta - 2)) = \varphi(a_0 + a_1\alpha)\varphi(b_0 + b_1\alpha), \end{aligned}$$

pri čemu je korišćeno $\alpha^2 = 2$ i $\beta^2 - 4\beta + 4 = 2$.

659. Dokazati da je jedini automorfizam polja racionalnih brojeva identičko preslikavanje.

Rešenje. Neka je f automorfizam polja $\mathbb{Q}$. Svaki automorfizam polja ostavlja neizmenjene 0 i 1, pa je $f(0) = 0$ i $f(1) = 1$.

Dalje, za svaki prirodan broj n je $f(n) = n$ (što se jednostavno dokazuje indukcijom: tvrđenje važi za $n = 1$, ako pretpostavimo da važi za k , biće $f(k + 1) = f(k) + f(1) = k + 1$).

Takođe je $f(c) = c$ za svaki ceo broj c . Zaista, iz $0 = f(c - c) = f(c) + f(-c)$, sledi

$$-f(c) = f(-c),$$

pa je za svaki prirodan broj n $f(-n) = -f(n) = -n$. Slično, iz

$$1 = f(1) = f\left(c \cdot \frac{1}{c}\right) = f(c) \cdot f\left(\frac{1}{c}\right), \quad c \neq 0,$$

sledi

$$f\left(\frac{1}{c}\right) = \frac{1}{f(c)} = \frac{1}{c},$$

za svaki ceo broj c različit od nule.

Prema tome, za svaki racionalan broj $\frac{p}{q}$ je

$$f\left(\frac{p}{q}\right) = f\left(p \cdot \frac{1}{q}\right) = f(p) \cdot f\left(\frac{1}{q}\right) = p \cdot \frac{1}{q} = \frac{p}{q},$$

što znači da je f identičko preslikavanje.

660. Dokazati da polja $\mathbb{Q}(\sqrt{2})$ i $\mathbb{Q}(\sqrt{3})$ nisu izomorfna.

Rešenje. Pretpostavimo da su data polja izomorfna i neka je f izomorfizam polja $\mathbb{Q}(\sqrt{2})$ na polje $\mathbb{Q}(\sqrt{3})$. Tada se, slično kao u prethodnom zadatku, može pokazati da je za svako $x \in \mathbb{Q}$

$$f(x) = x.$$

Neka je $f(\sqrt{2}) = a + b\sqrt{3}$, $a, b \in \mathbb{Q}$. Tada će biti

$$\begin{aligned} 2 = f(2) &= f(\sqrt{2} \cdot \sqrt{2}) = f(\sqrt{2}) \cdot f(\sqrt{2}) = (a + b\sqrt{3})^2 = \\ &= a^2 + 3b^2 + 2ab\sqrt{3}, \end{aligned}$$

odakle dobijamo sistem jednačina

$$2ab = 0, \quad a^2 + 3b^2 = 2,$$

koji nema racionalna rešenja.

Iz ove protivrečnosti zaključujemo da data polja ne mogu biti izomorfna.

661. Neka je $a = k^2b$, $a, b, k \in \mathbb{Q}$, $k > 0$. Dokazati da je tada

$$\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b}).$$

662. Neka je u transcendentan element nad poljem F . Odrediti sve F -automorfizme polja $F(u)$.

Rešenje. Neka je f F -automorfizam polja $F(u)$. Tada je f potpuno određeno ako je poznato $f(u) = v \in F(u)$, pri čemu $v \notin F$. Na osnovu zadatka 640 $F(u)$ je jednostruko algebarsko proširenje polja $F(v)$, pri čemu je $v = \frac{p(u)}{q(u)}$, $p(x), q(x) \in F[x]$, $q(x) \neq 0$, a u je koren polinoma

$$r(x) = p(x) - vq(x) \in F(v)[x].$$

f je F -automorfizam polja $F(u)$ ako i samo ako je $F(u) = F(v)$, a to važi ako i samo ako je $[F(u) : F(v)] = 1$, ako i samo ako je $r(x)$ linearan polinom, tj.

$$v = \frac{au + b}{cu + d}, \quad a, b, c, d \in F, \quad ad - bc \neq 0.$$

(Ukoliko bi bilo $ad - bc = 0$, onda bi za neko $k \in F$ bilo $ak + b = k(cu + d)$, tj. element v bi bio u F .)

663. Neka je polje K proširenje polja F . Polje K je algebarsko proširenje polja F ako i samo ako za svako međupolje E ($F \subseteq E \subseteq K$) svaki F -monomorfizam $f : E \rightarrow E$ je F -automorfizam polja E . Dokazati.

Rešenje. Neka je K algebarsko proširenje polja F , E međupolje i $f : E \rightarrow E$ F -monomorfizam polja E . Treba da dokažemo da je f epimorfizam, a za to je dovoljno da dokažemo da je f bijekcija, tj. da ima i levo i desno inverzno preslikavanje. f je monomorfizam, pa ima levo inverzno preslikavanje, dakle, preostaje da se dokaže da f ima desno inverzno preslikavanje.

Ako $\alpha \in E$, onda $\alpha \in K$, a kako je K algebarsko proširenje polja F , postoji polinom $p(x) \in F[x]$ takav da je $p(\alpha) = 0$. Pošto je f F -monomorfizam, onda primenom monomorfizma f n puta ($n \in \mathbb{N}$) dobijamo da je

$$f^n(p(\alpha)) = p(f^n(\alpha)) = 0.$$

Polinom $p(x)$ ima najviše $\deg p(x)$ korena (3.31), a f^n za svako $n \in \mathbb{N}$ preslikava koren polinoma $p(x)$ u koren tog polinoma, pa je za neko $k, m \in \mathbb{N}$, $k \neq m$,

$$f^m(\alpha) = f^k(\alpha).$$

Neka je $m > k$. f ima levo inverzno preslikavanje, pa je

$$f^{m-k}(\alpha) = \alpha.$$

Ako je $m - k = 1$ f je identičko preslikavanje na $F(\alpha)$, a ako je $m - k > 1$, tada je f^{m-k-1} desno inverzno preslikavanje za f , pa je f automorfizam polja $F(\alpha)$. α je proizvoljan element iz E , pa je f F -automorfizam polja E .

Za drugi deo dokaza nećemo navoditi kompletno rešenje već samo uputstvo.

Neka je za svako međupolje E ($F \subseteq E \subseteq K$) svaki F -monomorfizam $f : E \rightarrow E$ F -automorfizam polja E . Pretpostavimo da je K transcendentno proširenje polja F i neka je u element polja K transcendentan nad poljem F .

Dokazati da je preslikavanje $f : F(u) \rightarrow F(u)$, međupolja $F(u)$ definisano sa $f : p(u) \mapsto p(u^2)$ F -monomorfizam koji nije F -epimorfizam ($u \in F(u)$ nije slika nijednog elementa iz $F(u)$).

664. Označimo sa K polje svih racionalnih funkcija po x nad poljem racionalnih brojeva $\mathbb{Q}$ (3.26). Neka je L_1 polje koje se dobija kad se polju K adjunguje rešenje jednačine $t^2 - x = 0$, a L_2 polje koje se dobija kad se polju K adjunguje rešenje jednačine $t^3 + x = 0$. Dokazati:

a) L_1 i L_2 nisu izomorfna proširenja polja K .

b) L_1 i L_2 su izomorfna proširenja polja $\mathbb{Q}$.

(Ako su F, L_1 i L_2 polja takva da je $F \subseteq L_1$ i $F \subseteq L_2$, onda se L_1 i L_2 nazivaju izomorfna proširenja polja F ako i samo ako postoji izomorfizam φ polja L_1 na L_2 takav da je $\varphi(a) = a$ za svako $a \in F$.)

Rešenje. a) $[L_1 : K] = 2$, a $[L_2 : K] = 3$, pa L_1 i L_2 nisu izomorfna proširenja polja K .

b) $L_1 = \mathbb{Q}(\sqrt{x})$, a $L_2 = \mathbb{Q}(\sqrt[3]{x})$. Pošto je x transcendentno nad $\mathbb{Q}$, to su $\sqrt{x}$ i $\sqrt[3]{x}$ transcendentni nad $\mathbb{Q}$. Lako se proverava da je preslikavanje $\sigma : L_1 \rightarrow L_2$ takvo da je σ identično preslikavanje skupa $\mathbb{Q}$, a $\sigma(\sqrt{x}) = \sqrt[3]{x}$, izomorfizam L_1 i L_2 .

3.4 Teorija Galoa

665. Dokazati da je algebarsko proširenje K polja F takvo da je $[K : F] = 2$, normalno proširenje.

Rešenje. Neka je $a \in K$, $a \notin F$. Ako je $m(x)$ maksimalni polinom

elementa a nad F , onda iz

$$[K : F] = [K : F(a)][F(a) : F] = 2$$

sledi $[F(a) : F] = 2$, tj. $F(a) = K$, pa je $\deg m(x) = 2$. Pošto polinom $m(x)$ stepena 2 ima jednu nulu u K , on mora imati i drugu nulu u K (2.73).

S obzirom na 3.45 grupa $G(K, F)$ sadrži samo dva automorfizma, $|G(K, F)| = [K : F] = 2$, pa je K normalno proširenje polja F (3.51).

666. Dokazati da polje realnih brojeva $\mathbb{R}$ nije normalno proširenje polja racionalnih brojeva $\mathbb{Q}$.

Rešenje. Polinom $x^3 - 2 \in \mathbb{Q}[x]$ je nesvodljiv nad poljem $\mathbb{Q}$, koren $\sqrt[3]{2}$ tog polinoma je u $\mathbb{R}$, ali ostali koreni su kompleksni brojevi koji ne pripadaju $\mathbb{R}$. Prema tome, na osnovu 3.52 (iii) E nije normalno proširenje polja $\mathbb{Q}$.

667. Dokazati da je polje $\mathbb{Q}\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)$ normalno proširenje polja $\mathbb{Q}$.

Uputstvo. Dokazati da je $\mathbb{Q}\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)$ faktorizacijsko polje polinoma $x^4 + 1 \in \mathbb{Q}[x]$.

668. Odrediti sva polja K , proširenja polja $\mathbb{Q}$, takva da je polje $K(\sqrt[n]{p})$, gde je p prost broj a n prirodan broj, normalno proširenje polja K .

Rešenje. Pošto je $\sqrt[n]{p}$ koren polinoma $f(x) = x^n - p$, faktorizacijsko polje polinoma $f(x)$ je $\mathbb{Q}(\sqrt[n]{p}, \varepsilon)$ gde je ε n -ti primitivni koren iz jedinice. Otuda na osnovu 3.52 sledi da je $K(\sqrt[n]{p})$ normalno proširenje ako i samo ako K sadrži $\mathbb{Q}(\varepsilon)$.

669. Neka je K normalno proširenje polja F , a M međupolje za polja K i F ($F \subseteq M \subseteq K$). Dokazati da je K normalno proširenje polja M . Primerom pokazati da M mora biti normalno proširenje polja F .

Uputstvo. Primer za drugi deo zadatka su polja $\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$, $\varepsilon = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$.

670. Neka su polja F_1, F_2, F_3 takva da je $F_1 \subseteq F_2 \subseteq F_3$, F_2 normalno proširenje polja F_1 i F_3 normalno proširenje F_2 . Da li F_3 mora biti normalno proširenje F_1 ?

Uputstvo. Polje F_3 ne mora da bude normalno proširenje polja F_1 . Dokazati da je polje $\mathbb{Q}(\sqrt{2})$ normalno proširenje polja $\mathbb{Q}$, polje $\mathbb{Q}(\sqrt[4]{2})$ normalno proširenje polja $\mathbb{Q}(\sqrt{2})$, ali $\mathbb{Q}(\sqrt[4]{2})$ nije normalno proširenje polja $\mathbb{Q}$.

671. Od sledećih proširenja odrediti koja su normalna:

a) $\mathbb{Q}(\sqrt{-5})$ nad $\mathbb{Q}$,

b) $\mathbb{Q}(\sqrt[3]{5})$ nad $\mathbb{Q}$,

c) $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ nad $\mathbb{Q}$.

Rezultat. a) Normalno, b) nije normalno, c) normalno.

672. Odrediti sve automorfizme polja $\mathbb{Q}(\sqrt{2})$.

Rešenje. Neka je f automorfizam polja $\mathbb{Q}(\sqrt{2})$. Sličnim postupkom kao u zadatku 659 može se pokazati da je restrikcija f na $\mathbb{Q}$ identičko preslikavanje.

Svaki element polja $\mathbb{Q}(\sqrt{2})$ se na jedinstven način može prikazati u obliku $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$, pa je slika elemenata $a + b\sqrt{2}$ potpuno određena slikom elementa $\sqrt{2}$ (jer je $f(a + b\sqrt{2}) = f(a) + f(b)f(\sqrt{2}) = a + bf(\sqrt{2})$). Kako je $(\sqrt{2})^2 - 2 = 0$, biće $(f(\sqrt{2}))^2 - 2 = 0$.

Dobili smo da je $f(\sqrt{2})$ nula polinoma $x^2 - 2$, pa je, prema tome,

$$f(\sqrt{2}) = \sqrt{2} \quad \text{ili} \quad f(\sqrt{2}) = -\sqrt{2}.$$

U prvom slučaju f je identičko preslikavanje.

Dokažimo da je preslikavanje $f : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$ dato sa

$$f(a + b\sqrt{2}) = a - b\sqrt{2}$$

zaista automorfizam:

$$\begin{aligned} f((a + b\sqrt{2}) + (c + d\sqrt{2})) &= a + c - (b + d)\sqrt{2} = \\ &= f(a + b\sqrt{2}) + f(c + d\sqrt{2}), \\ f((a + b\sqrt{2})(c + d\sqrt{2})) &= (ac + 2bd) - (ad + bc)\sqrt{2} = \\ &= f(a + b\sqrt{2})f(c + d\sqrt{2}). \end{aligned}$$

f je očividno bijekcija polja $\mathbb{Q}(\sqrt{2})$, pa je automorfizam.

Prema tome, jedini automorfizmi polja $\mathbb{Q}(\sqrt{2})$ su identičko preslikavanje i preslikavanje koje $a + b\sqrt{2}$ preslikava u $a - b\sqrt{2}$.

673. Naći grupu svih automorfizama polja $\mathbb{Q}(\sqrt[3]{2})$.

Rešenje. Ranije je dokazano da svaki automorfizam polja koje je proširenje polja racionalnih brojeva ostavlja sve racionalne brojeve neizmenjene. Svaki element polja $\mathbb{Q}(\sqrt[3]{2})$ može se prikazati u obliku

$$a + b\sqrt[3]{2} + c\sqrt[3]{4},$$

pa će slika svakog elementa polja $\mathbb{Q}(\sqrt[3]{2})$ biti potpuno određena slikom elementa $\sqrt[3]{2}$. Ako je f automorfizam, iz $(\sqrt[3]{2})^3 = 2$ sledi $(f(\sqrt[3]{2}))^3 = 2$, što znači da je $f(\sqrt[3]{2})$ takođe treći koren iz 2. Kako je $\sqrt[3]{2}$ jedini realan treći koren iz 2 (ostala dva su kompleksna) sledi da je $f(\sqrt[3]{2}) = \sqrt[3]{2}$, odnosno f je identičko preslikavanje. Prema tome, grupa automorfizama sastoji se samo od identičkog preslikavanja.

PRIMEDBA. Polje $\mathbb{Q}(\sqrt[3]{2})$ nije normalno proširenje polja $\mathbb{Q}$ jer $\mathbb{Q}$ nije fiksno polje grupe automorfizama polja $\mathbb{Q}(\sqrt[3]{2})$ (3.50) (svaki element polja $\mathbb{Q}$ jeste fiksni, međutim, fiksno polje je definisano (3.43) kao skup svih fiksnih elemenata).

674. Neka je F polje, a S proizvoljan skup automorfizama polja F . Dokazati da je skup svih elemenata polja F koji su fiksni za svaki automorfizam skupa S , potpolje polja F .

Rešenje. Ako je f automorfizam polja F , za svako $a, b \in F$ važi

$$\begin{aligned} f(a+b) &= f(a) + f(b), & f(-a) &= -f(a), \\ f(ab) &= f(a)f(b), & f(a^{-1}) &= (f(a))^{-1}, \text{ za } a \neq 0, \\ f(0) &= 0, & f(1) &= 1. \end{aligned}$$

Ako su a i b fiksni elementi za automorfizam f (tj. $f(a) = a$, $f(b) = b$), onda iz gornjih jednakosti na osnovu 3.2 sledi da je skup svih elemenata iz F koji su fiksni u odnosu na f , potpolje F_f polja F . Presek proizvoljne familije potpolja nekog polja je potpolje, prema tome, presek potpolja F_f za $f \in S$ je potpolje polja F .

675. Naći grupu Galoa polinoma

$$a) \quad x^5 - 1, \quad b) \quad x^7 - 1, \quad c) \quad x^5 - 7,$$

u odnosu na polje racionalnih brojeva. Odrediti potpolja faktorizacijskog polja datog polinoma koja odgovaraju podgrupama grupe Galoa.

Rešenje. a) Faktorizacijsko polje polinoma $x^5 - 1$ je $\mathbb{Q}(\alpha)$, gde je $\alpha = e^{2\pi i/5}$ primitivan peti koren iz jedinice. Kako je

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1),$$

a α je nula polinoma

$$p(x) = x^4 + x^3 + x^2 + x + 1$$

nesvodljivog nad $\mathbb{Q}$, grupa Galoa datog polinoma nad $\mathbb{Q}$ (tj. polja $\mathbb{Q}(\alpha)$ nad poljem $\mathbb{Q}$) ima 4 automorfizma (na osnovu 3.51 i 3.52 jer je $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$).

Svaki element polja $\mathbb{Q}(\alpha)$ se može prikazati u obliku

$$a + b\alpha + c\alpha^2 + d\alpha^3, \quad a, b, c, d \in \mathbb{Q},$$

ranije je dokazano da je svaki automorfizam polja $\mathbb{Q}(\alpha)$ potpuno određen ako se zna slika elementa α i da te slike mogu biti samo elementi konjugovani sa α . Elementi konjugovani sa α nad $\mathbb{Q}$, su $\alpha, \alpha^2, \alpha^3, \alpha^4$ (to su nule polinoma $p(x)$ nesvodljivog nad $\mathbb{Q}$), pa ćemo definisati 4 preslikavanja:

$$f_i(a + b\alpha + c\alpha^2 + d\alpha^3) = a + b(\alpha^i) + c(\alpha^i)^2 + d(\alpha^i)^3, \quad i = 1, 2, 3, 4.$$

Na osnovu 3.40 sledi da je svako od preslikavanja f_i automorfizam polja $\mathbb{Q}(\alpha)$ sa fiksnim poljem $\mathbb{Q}$. To su svi automorfizmi polja $\mathbb{Q}(\alpha)$, pa oni čine grupu Galoa polinoma $x^5 - 1$ nad poljem $\mathbb{Q}$. Kako je $f_2^2 = f_4$, $f_2^3 = f_3$, $f_2^4 = f_1$, grupa Galoa $G(\mathbb{Q}(\alpha), \mathbb{Q}) = \{f_1, f_2, f_3, f_4\}$ je ciklička.

Odredimo fiksno polje podgrupe $H = \{f_1, f_4\}$ grupe G . To fiksno polje će se sastojati od svih elemenata x za koje je $f_i(x) = x$, $i = 1, 4$. Iz

$$\begin{aligned} f_4(a + b\alpha + c\alpha^2 + d\alpha^3) &= a + b\alpha^4 + c\alpha^8 + d\alpha^{12} = \\ &= a + b(-\alpha^3 - \alpha^2 - \alpha - 1) + c\alpha^3 + d\alpha^2 = \\ &= (a - b) - b\alpha + (d - b)\alpha^2 + (c - b)\alpha^3 = \\ &= a + b\alpha + c\alpha^2 + d\alpha^3, \end{aligned}$$

(kokristili smo da je $\alpha^5 = 1$, $\alpha^4 = -\alpha^3 - \alpha^2 - \alpha - 1$), sledi $b = 0$, $d = c$, pa je skup svih elemenata oblika

$$a + b(\alpha^2 + \alpha^3), \quad a, b \in \mathbb{Q}$$

fiksno polje podgrupe H .

Za podgrupu $\{f_1\}$ čiji je jedini element identičko preslikavanje, fiksno polje je celo polje $\mathbb{Q}(\alpha)$.

676. Dat je polinom $p(x) \in \mathbb{Q}[x]$,

$$p(x) = x^5 - x^4 - x^3 - x - 2.$$

Naći grupu Galoa polinoma $p(x)$ nad poljem racionalnih brojeva $\mathbb{Q}$.

Uputstvo. $p(x) = (x - 2)(x^4 + x^3 + x^2 + x + 1)$.

677. Dat je polinom

$$p(x) = x^n + 2x^{n-1} + 2x^{n-2} + \dots + 2x^2 + 2x + 1.$$

Naći grupu Galoa polinoma $p(x)$ nad poljem racionalnih brojeva $\mathbb{Q}$.

Rešenje.

$$\begin{aligned} p(x) &= x^n + x^{n-1} + \dots + x^2 + x + x^{n-1} + x^{n-2} + \dots + x^2 + x + 1 = \\ &= (x + 1)(x^{n-1} + x^{n-2} + \dots + x^2 + x + 1). \end{aligned}$$

Nule polinoma $p(x)$ su -1 i n -ti kompleksni koreni iz jedinice $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{n-1}$, pa je faktorizacijsko polje polinoma $p(x)$ $\mathbb{Q}(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{n-1}) = \mathbb{Q}(\varepsilon_1)$, gde je ε_1 primitivan n -ti koren iz jedinice. Svakim $\mathbb{Q}$ -automorfizmom se ε_1 preslikava opet u primitivan koren iz jedinice, pa je grupa Galoa polja $\mathbb{Q}(\varepsilon_1)$ nad $\mathbb{Q}$ izomorfna multiplikativnoj grupi ostataka po modulu n koji su uzajamno prosti sa n .

678. Odrediti grupu Galoa polja $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ nad $\mathbb{Q}$.

679. Odrediti grupu Galoa polinoma

$$x^3 - 2$$

u odnosu na polja $\mathbb{Q}$, $\mathbb{Q}(\varepsilon)$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$, gde je $\varepsilon = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$.

Rešenje. Faktorizacijsko polje polinoma $x^3 - 2$ nad poljem $\mathbb{Q}$ je $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$. Bazu polja $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ nad poljem $\mathbb{Q}$ čine elementi $1, \sqrt[3]{2}, \sqrt[3]{4}, \varepsilon, \varepsilon\sqrt[3]{2}, \varepsilon\sqrt[3]{4}$, pa je, kao što je ranije pokazano, svaki automorfizam polja $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ potpuno određen ako se znaju slike elemenata $\sqrt[3]{2}$ i ε . $\sqrt[3]{2}$ je nula polinoma $x^3 - 2$ nesvodljivog nad $\mathbb{Q}$, a ε je nula polinoma $x^2 + x + 1$ takođe nesvodljivog nad $\mathbb{Q}$, pa se $\sqrt[3]{2}$ može preslikati samo u $\sqrt[3]{2}, \varepsilon\sqrt[3]{2}$ i $\varepsilon^2\sqrt[3]{2}$, a ε u ε i ε^2 .

Kako je $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ proširenje stepena 2 polja $\mathbb{Q}(\sqrt[3]{2})$, postoji automorfizam f takav da je

$$f(\varepsilon) = \varepsilon^2 \text{ i } f(x) = x, \text{ za svako } x \in \mathbb{Q}(\sqrt[3]{2}).$$

Takođe je $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ proširenje stepena tri polja $\mathbb{Q}(\varepsilon)$, pa je preslikavanje g za koje je

$$g(\sqrt[3]{2}) = \varepsilon\sqrt[3]{2}, \quad g(x) = x, \text{ za svako } x \in \mathbb{Q}(\varepsilon)$$

automorfizam polja $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$.

Tada je $f^2 = id$ (identičko preslikavanje), a g^2 je automorfizam takav da je

$$g^2(\varepsilon) = g(g(\varepsilon)) = g(\varepsilon) = \varepsilon,$$

$$g^2(\sqrt[3]{2}) = g(g(\sqrt[3]{2})) = g(\varepsilon\sqrt[3]{2}) = \varepsilon \cdot \varepsilon\sqrt[3]{2} = \varepsilon^2\sqrt[3]{2}.$$

Množenjem automorfizama f i g dobijamo nove automorfizme gf i g^2f , pa se svi dobijeni automorfizmi mogu predstaviti tablicom

	id	f	g	g^2	gf	g^2f
ε	ε	ε^2	ε	ε	ε^2	ε^2
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\varepsilon\sqrt[3]{2}$	$\varepsilon^2\sqrt[3]{2}$	$\varepsilon\sqrt[3]{2}$	$\varepsilon^2\sqrt[3]{2}$

(Ovde se u koloni ispod oznake automorfizma nalazi u prvoj vrsti slika elementa ε a u drugoj vrsti slika elementa $\sqrt[3]{2}$ odgovarajućim automorfizmom.)

S obzirom da se ε mora preslikati u ε ili ε^2 , a $\sqrt[3]{2}$ u $\sqrt[3]{2}$, $\varepsilon\sqrt[3]{2}$ ili $\varepsilon^2\sqrt[3]{2}$, a u gornjoj tablici su navedene sve kombinacije takvih preslikavanja, sledi da, sem navedenih, drugih automorfizama nema. Grupa Galoa polinoma $x^3 - 2$ nad poljem $\mathbb{Q}$ je $G = \{id, f, g, g^2, gf, g^2f\}$ i kako je $f^2 = g^3 = (gf)^2 = id$, grupa G je nekomutativna grupa reda 6 (izomorfna sa grupom S_3).

Potpolju $\mathbb{Q}(\varepsilon)$ polja $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ odgovara podgrupa $H = \{id, g, g^2\}$ grupe G . Automorfizmi iz H ostavljaju sve elemente iz $\mathbb{Q}(\varepsilon)$ nepromenjene.

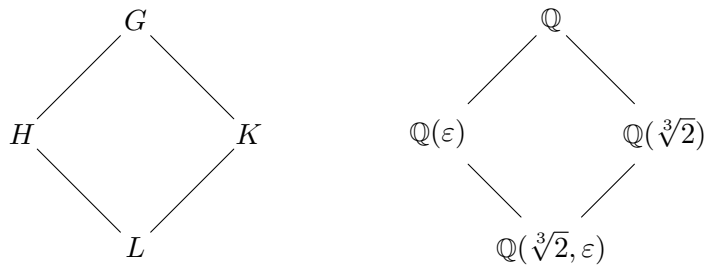
Potpolje $\mathbb{Q}(\sqrt[3]{2})$ je fiksno polje podgrupe $K = \{id, f\}$, a za podgrupu $L = \{id\}$ fiksno polje je celo polje $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$,

Prema tome, u odnosu na polja $\mathbb{Q}$, $\mathbb{Q}(\varepsilon)$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ grupe Galoa polinoma $x^3 - 2$ su respektivno grupe G , H , K i L .

Polje $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ je faktorizacijsko polje polinoma $x^3 - 2$ nesvodljivog nad $\mathbb{Q}$, pa je $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ normalno proširenje polja $\mathbb{Q}$.

H je normalna podgrupa grupe G , pa je polje $\mathbb{Q}(\varepsilon)$ normalno nad $\mathbb{Q}$. Međutim, K nije normalna podgrupa grupe G , pa ni $\mathbb{Q}(\sqrt[3]{2})$ nije normalno proširenje polja $\mathbb{Q}$.

Međusobni odnosi podgrupa grupe G i potpolja polja $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ mogu se prikazati sledećim dijagramom:



Navešćemo i permutacionu grupu polinoma $x^3 - 2$ nad poljem $\mathbb{Q}$ (v. 3.49).

Koreni jednačine $x^3 - 2 = 0$ su

$$x_1 = \sqrt[3]{2}, \quad x_2 = \varepsilon \sqrt[3]{2}, \quad x_3 = \varepsilon^2 \sqrt[3]{2}.$$

Kako je $f(x_1) = x_1$, $f(x_2) = x_3$, $f(x_3) = x_2$, automorfizmu f odgovara permutacija $p_f = (23)$. Iz $g(x_1) = x_2$, $g(x_2) = x_3$, $g(x_3) = x_1$, sledi $p_g = (123)$. Na sličan način dobijamo

$$p_{g^2} = (123), \quad p_{gf} = (12), \quad p_{g^2f} = (13), \quad p_{id} = (1),$$

pa je $\{(1), (12), (13), (23), (123), (132)\}$ permutaciona grupa datog polinoma izomorfna grupi G .

680. Naći grupu Galoa G polinoma

$$p(x) = x^4 - 5x^2 + 6$$

u odnosu na polje racionalnih brojeva $\mathbb{Q}$. Odrediti potpolja faktorizacijskog polja koja odgovaraju podgrupama grupe G .

Rešenje. Koreni polinoma $x^4 - 5x^2 + 6$ su $x_{1,2} = \pm\sqrt{2}$ i $x_{3,4} = \pm\sqrt{3}$, pa je faktorizacijsko polje tog polinoma $\mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Red tražene grupe Galoa G je na osnovu 3.51 i 3.52

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Automorfizmi polja $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ su preslikavanja definisana sa

$$\varphi : \begin{cases} \sqrt{2} \mapsto -\sqrt{2}, \\ \sqrt{3} \mapsto \sqrt{3}, \end{cases} \quad \psi : \begin{cases} \sqrt{2} \mapsto \sqrt{2}, \\ \sqrt{3} \mapsto -\sqrt{3}. \end{cases}$$

Lako se proverava da je $\varphi^2 = id$, $\psi^2 = id$ i $\varphi\psi = \psi\varphi$, pa je skup automorfizama $\{id, \varphi, \psi, \varphi\psi\}$ podgrupa grupe G , a kako je G reda 4, to je $G = \{id, \varphi, \psi, \varphi\psi\}$.

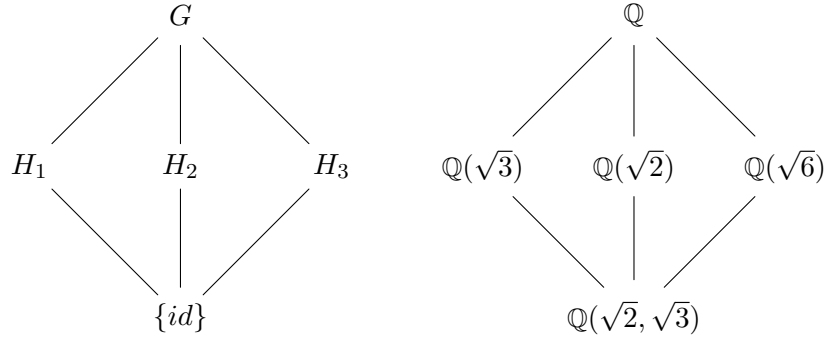
Podgrupe grupe G su

$$H_1 = \{id, \varphi\}, \quad H_2 = \{id, \psi\} \quad \text{i} \quad H_3 = \{id, \varphi\psi\}.$$

Fiksno polje podgrupe H_1 je $\mathbb{Q}(\sqrt{3})$, fiksno polje podgrupe H_2 je $\mathbb{Q}(\sqrt{2})$ a fiksno polje podgrupe H_3 je $\mathbb{Q}(\sqrt{6})$.

Grupa G je komutativna, pa su sve njene podgrupe normalne. Prema tome, i sva navedena polja su normalna proširenja polja $\mathbb{Q}$.

Mreže podgrupa i potpolja su



681. Naći grupu Galoa G polinoma

$$p(x) = x^4 - 2$$

u odnosu na polje racionalnih brojeva $\mathbb{Q}$. Odrediti podgrupe grupe G i potpolja faktorizacijskog polja koja im odgovaraju.

Rešenje. Polinom $p(x)$ je nesvodljiv nad $\mathbb{Q}$ po Ajzenštajnovom kriterijumu. Koreni polinoma su $x_{1,2} = \pm\sqrt[4]{2}$, $x_{3,4} = \pm i\sqrt[4]{2}$, pa je faktorizacijsko polje

$$\mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i).$$

$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 2 \cdot 4 = 8,$$

pa je red grupe G osam.

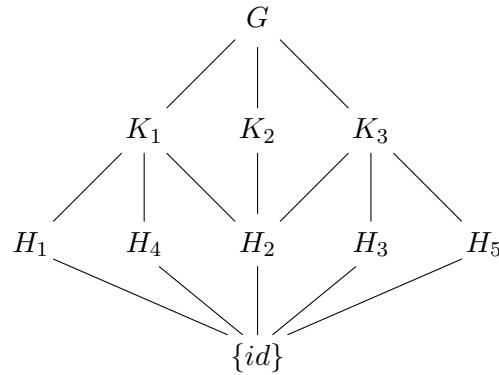
Lako se proverava da su preslikavanja određena sa

$$\psi : \begin{cases} i \mapsto -i, \\ \sqrt[4]{2} \mapsto \sqrt[4]{2}, \end{cases} \quad \text{ i } \quad \varphi : \begin{cases} i \mapsto i, \\ \sqrt[4]{2} \mapsto i\sqrt[4]{2}, \end{cases}$$

automorfizmi polja $\mathbb{Q}(\sqrt[4]{2}, i)$. Polje $\mathbb{Q}(\sqrt[4]{2})$ je fiksno za automorfizam ψ , a polje $\mathbb{Q}(i)$ je fiksno za automorfizam φ . Jednostavno se proverava da je $\psi^2 = id$, $\varphi^4 = id$ i $\psi\varphi = \varphi^3\psi$. Zbog toga je $\{id, \psi, \varphi, \varphi^2, \varphi^3, \varphi\psi, \varphi^2\psi, \varphi^3\psi\}$ podgrupa grupe G reda 8, tj. cela grupa G . Grupa G ima sledeće podgrupe:

$$\begin{aligned} H_1 &= \{id, \psi\}, & K_1 &= \{id, \varphi, \varphi^2, \varphi^3\} \\ H_2 &= \{id, \varphi^2\}, & K_2 &= \{id, \varphi^2, \psi, \varphi^2\psi\}, \\ H_3 &= \{id, \varphi\psi\}, & K_3 &= \{id, \varphi, \varphi\psi, \varphi^3\psi\}. \\ H_4 &= \{id, \varphi^2\psi\}, \\ H_5 &= \{id, \varphi^3\psi\}, \end{aligned}$$

Podgrupe H_2, K_1, K_2, K_3 su normalne podgrupe grupe G , a H_2 je centar te grupe. Mreža podgrupa je



Automorfizmi iz K_1 fiksiraju i , pa je $\mathbb{Q}(i)$ fiksno polje za K_1 .

K_2 fiksira element $\sqrt[4]{2} \cdot \sqrt[4]{2} = \sqrt{2}$, pa je $\mathbb{Q}(\sqrt{2})$ fiksno polje za K_2 .

K_3 fiksira $i\sqrt[4]{2}\sqrt[4]{2} = i\sqrt{2}$, pa je $\mathbb{Q}(i\sqrt{2})$ fiksno polje za K_3 .

H_1 fiksira $\sqrt[4]{2}$, pa je $\mathbb{Q}(\sqrt[4]{2})$ fiksno polje za H_1 .

H_2 fiksira i i $i\sqrt{2}$, pa je $\mathbb{Q}(i, \sqrt{2})$ fiksno polje za H_2 .

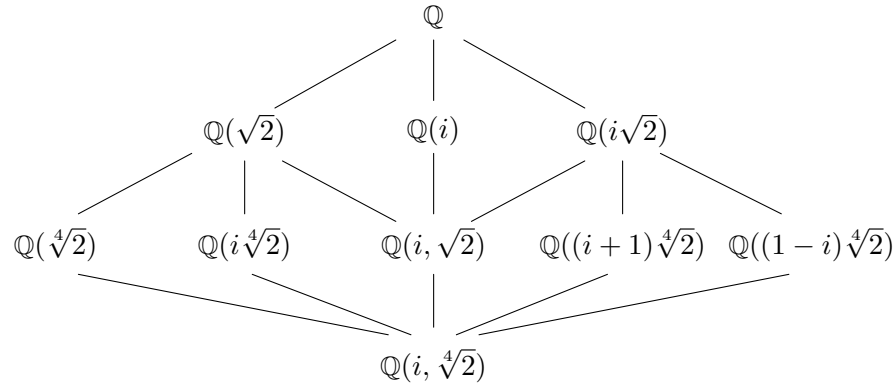
H_3 fiksira $(1+i)\sqrt[4]{2}$, pa je $\mathbb{Q}((1+i)\sqrt[4]{2})$ fiksno polje za H_3 .

H_4 fiksira $i\sqrt[4]{2}$, pa je $\mathbb{Q}(i\sqrt[4]{2})$ fiksno polje za H_4 .

H_5 fiksira $(1-i)\sqrt[4]{2}$, pa je $\mathbb{Q}((1-i)\sqrt[4]{2})$ fiksno polje za H_5 .

Polja $\mathbb{Q}(i, \sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ i $\mathbb{Q}(i\sqrt{2})$ su normalna proširenja polja $\mathbb{Q}$.

Mreža potpolja je



682. Odrediti grupu Galoa G polinoma

$$p(x) = x^4 + 1$$

nad poljem racionalnih brojeva $\mathbb{Q}$. Odrediti podgrupe grupe G i potpolja faktorizacijskog polja koja im odgovaraju.

Rešenje. $x^4 + 1$ je nesvodljiv nad $\mathbb{Q}$. Međutim,

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1),$$

pa su koreni polinoma $x^4 + 1$

$$x_1 = \frac{-\sqrt{2} + i\sqrt{2}}{2}, \quad x_2 = \frac{-\sqrt{2} - i\sqrt{2}}{2}, \quad x_3 = \frac{\sqrt{2} + i\sqrt{2}}{2}, \quad x_4 = \frac{\sqrt{2} - i\sqrt{2}}{2},$$

a faktorizacijsko polje je $\mathbb{Q}(i, \sqrt{2})$. Red grupe G je

$$[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

(Do istog rezultata se moglo doći prikazujući korene u obliku $x_3 = e^{\pi i/4} = \alpha$, $x_1 = \alpha^3$, $x_2 = \alpha^5$, $x_4 = \alpha^7$, faktorizacijsko polje polinoma $x^4 + 1$ je onda $\mathbb{Q}(\alpha)$, a stepen proširenja je $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.)

Preslikavanja definisana sa

$$\varphi : \begin{cases} i \mapsto -i, \\ \sqrt{2} \mapsto \sqrt{2}, \end{cases} \quad \psi : \begin{cases} i \mapsto i, \\ \sqrt{2} \mapsto -\sqrt{2}, \end{cases}$$

su automorfizmi polja $\mathbb{Q}(i, \sqrt{2})$.

Lako se proverava da je $\varphi^2 = id$, $\psi^2 = id$ i $\varphi\psi = \psi\varphi$, pa je $\{id, \varphi, \psi, \varphi\psi\} = G$. Podgrupe grupe G su

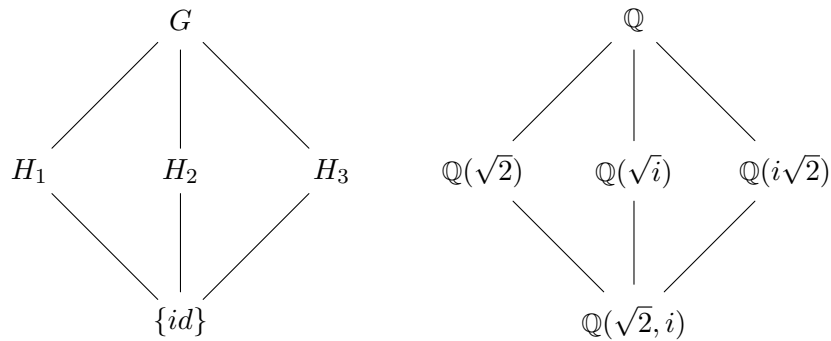
$$H_1 = \{id, \varphi\} \text{ i njoj odgovara potpolje } \mathbb{Q}(\sqrt{2}),$$

$$H_2 = \{id, \psi\} \text{ i njoj odgovara potpolje } \mathbb{Q}(i),$$

$$H_3 = \{id, \varphi\psi\} \text{ i njoj odgovara potpolje } \mathbb{Q}(i\sqrt{2}).$$

G je komutativna grupa pa su sve podgrupe normalne, a odgovarajuća potpolja su normalna proširenja polja $\mathbb{Q}$.

Mreža podgrupa i potpolja je:



683. Odrediti grupu Galoa G polinoma

a) $x^4 + 7x^2 + 4$,

b) $x^4 + 4x^2 + 2$,

c) $x^4 + 6x^2 + 6$,

nad poljem racionalnih brojeva $\mathbb{Q}$. Odrediti podgrupe grupe G i potpolja faktorizacijskog polja koja im odgovaraju.

Rešenje.

a) $x^4 + 7x^2 + 4 = (x^2 + 2)^2 + 3x^2 = (x^2 + \sqrt{-3}x + 2)(x^2 - \sqrt{-3}x + 2),$

pa su koreni datog polinoma

$$\begin{aligned} x_1 &= \frac{\sqrt{-3} + \sqrt{-11}}{2}, & x_2 &= \frac{\sqrt{-3} - \sqrt{-11}}{2}, \\ x_3 &= \frac{-\sqrt{-3} + \sqrt{-11}}{2}, & x_4 &= \frac{-\sqrt{-3} - \sqrt{-11}}{2}. \end{aligned}$$

Faktorizacijsko polje je $\mathbb{Q}(\sqrt{-3}, \sqrt{-11})$, a stepen ekstenzije je

$$[\mathbb{Q}(\sqrt{-3}, \sqrt{-11}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{-3}, \sqrt{-11}) : \mathbb{Q}(\sqrt{-3})][\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}] = 2 \cdot 2 = 4,$$

pa je red grupe G četiri.

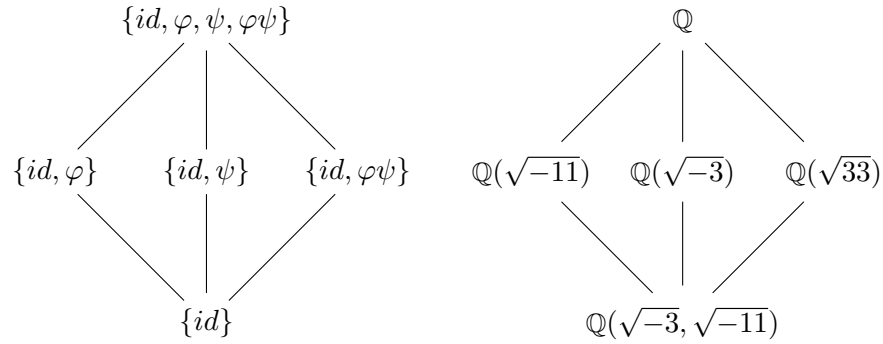
Preslikavanja definisana sa

$$\varphi : \begin{cases} \sqrt{-3} \mapsto -\sqrt{-3}, \\ \sqrt{-11} \mapsto \sqrt{-11}, \end{cases} \quad \text{i} \quad \psi : \begin{cases} \sqrt{-3} \mapsto \sqrt{-3}, \\ \sqrt{-11} \mapsto -\sqrt{-11}, \end{cases}$$

su automorfizmi faktorizacijskog polja.

Lako se proverava da je $\varphi^2 = id$, $\psi^2 = id$ i $\varphi\psi = \psi\varphi$, pa je $G = \{id, \varphi, \psi, \varphi\psi\}$.

Mreža podgrupa i odgovarajućih potpolja je



b) $p(x) = x^4 + 4x^2 + 2 = (x^2 + 2)^2 - 2 = 0$, pa su koreni polinoma $p(x)$

$$x_1 = \sqrt{-2 + \sqrt{2}}, \quad x_2 = -\sqrt{-2 + \sqrt{2}}, \quad x_3 = \sqrt{-2 - \sqrt{2}}, \quad x_4 = -\sqrt{-2 - \sqrt{2}}.$$

Posmatrajmo proširenje $\mathbb{Q}(\sqrt{-2 + \sqrt{2}})$. Polinom $x^4 + 4x^2 + 2$ je nesvodljiv nad $\mathbb{Q}$ po Ajzenštajnovom kriterijumu, pa proizvoljan element $y \in$

$\mathbb{Q}(\sqrt{-2 + \sqrt{2}})$ ima oblik

$$\begin{aligned} y &= a + b\sqrt{-2 + \sqrt{2}} + c(\sqrt{-2 + \sqrt{2}})^2 + d(\sqrt{-2 + \sqrt{2}})^3 = \\ &= (a - 2c) + c\sqrt{2} + (b - 2d + d\sqrt{2})\sqrt{-2 + \sqrt{2}}, \quad a, b, c, d \in \mathbb{Q}. \end{aligned}$$

Iz $x_1 x_3 = \sqrt{-2 + \sqrt{2}} \sqrt{-2 - \sqrt{2}} = \sqrt{2}$, sledi da je

$$\begin{aligned} \sqrt{-2 - \sqrt{2}} &= \frac{\sqrt{2}}{\sqrt{-2 + \sqrt{2}}} = \\ &= \left(2 + \sqrt{-2 + \sqrt{2}}\right)^2 \left(-2\sqrt{-2 + \sqrt{2}} - \frac{1}{2}(\sqrt{-2 + \sqrt{2}})^3\right) = \\ &= -3\sqrt{-2 + \sqrt{2}} - (\sqrt{-2 + \sqrt{2}})^3. \end{aligned}$$

Pri tom je korišćeno

$$\frac{1}{\sqrt{-2 + \sqrt{2}}} = -2\sqrt{-2 + \sqrt{2}} - \frac{1}{2}(\sqrt{-2 + \sqrt{2}})^3$$

(što se dobija metodom neodređenih koeficijenata). Iz svega prethodnog sledi da je faktorizacijsko polje polinoma $p(x)$

$$\mathbb{Q}(\sqrt{-2 + \sqrt{2}}, -\sqrt{-2 + \sqrt{2}}, \sqrt{-2 - \sqrt{2}}, -\sqrt{-2 - \sqrt{2}}) = \mathbb{Q}(\sqrt{-2 + \sqrt{2}}),$$

jer se pomoću nule x_1 racionalno izražavaju sve ostale.

$$[\mathbb{Q}(\sqrt{-2 + \sqrt{2}}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{-2 + \sqrt{2}}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4,$$

pa je red grupe G četiri.

Pošto automorfizmi polja $\mathbb{Q}(\sqrt{-2 + \sqrt{2}})$ permutuju korene polinoma odredimo automorfizam φ koji prevodi x_1 u x_3 . Direktno se proverava da je

$$\begin{aligned} \varphi : \sqrt{-2 + \sqrt{2}} &\mapsto -3\sqrt{-2 + \sqrt{2}} - (\sqrt{-2 + \sqrt{2}})^3, \\ \varphi^2 : \sqrt{-2 + \sqrt{2}} &\mapsto -\sqrt{-2 + \sqrt{2}}, \end{aligned}$$

$$\begin{aligned}\varphi^3 : \sqrt{-2 + \sqrt{2}} &\mapsto 3\sqrt{-2 + \sqrt{2}} + (\sqrt{-2 + \sqrt{2}})^3, \\ \varphi^4 &= id.\end{aligned}$$

Sledi da je grupa G ciklička grupa reda 4. Jedina njena netrivialna podgrupa je $H = \{id, \varphi^2\}$ i njoj odgovara potpolje $\mathbb{Q}(\sqrt{2})$ jer je $\sqrt{2} = 2 + (\sqrt{-2 + \sqrt{2}})^2$ fiksni element za automorfizam φ^2 .

Mreža podgrupa i potpolja je:

$$\begin{array}{ccc} G & & \mathbb{Q} \\ | & & | \\ H & & \mathbb{Q}(\sqrt{2}) \\ | & & | \\ \{id\} & & \mathbb{Q}(\sqrt{-2 + \sqrt{2}}) \end{array}$$

c) Koreni datog polinoma su:

$$x_1 = \sqrt{-3 + \sqrt{3}}, \quad x_2 = -\sqrt{-3 + \sqrt{3}}, \quad x_3 = \sqrt{-3 - \sqrt{3}}, \quad x_4 = -\sqrt{-3 - \sqrt{3}},$$

a njegovo faktorizacijsko polje je

$$\mathbb{Q}(\sqrt{-3 + \sqrt{3}}, -\sqrt{-3 + \sqrt{3}}, \sqrt{-3 - \sqrt{3}}, -\sqrt{-3 - \sqrt{3}}) = \mathbb{Q}(\sqrt{-3 + \sqrt{3}}, \sqrt{2}),$$

jer je

$$x_1 x_3 = \sqrt{6} = \sqrt{3}\sqrt{2} = (x_1^2 + 3)\sqrt{2},$$

pa je $x_3 = \left(x_1 + \frac{3}{x_1}\right)\sqrt{2}$ ili, kad se odredi inverzni element za x_1 , $x_3 = (-2x_1 - \frac{1}{2}x_1^3)\sqrt{2}$.

Red grupe G je

$$\begin{aligned}[\mathbb{Q}(\sqrt{-3 + \sqrt{3}}, \sqrt{2}) : \mathbb{Q}] &= \\ &= [\mathbb{Q}(\sqrt{-3 + \sqrt{3}}, \sqrt{2}) : \mathbb{Q}(\sqrt{-3 + \sqrt{3}})] [\mathbb{Q}(\sqrt{-3 + \sqrt{3}}) : \mathbb{Q}] = 2 \cdot 4 = 8.\end{aligned}$$

Automorfizmi polja $\mathbb{Q}(\sqrt{-3 + \sqrt{3}}, \sqrt{2})$ su:

$$\varphi : \begin{cases} \sqrt{2} \mapsto \sqrt{2}, \\ x_1 \mapsto (2x_1 - \frac{1}{2}x_1^3)\sqrt{2}, \end{cases} \quad \text{i} \quad \psi : \begin{cases} \sqrt{2} \mapsto -\sqrt{2}, \\ x_1 \mapsto x_1. \end{cases}$$

Lako se proverava da je

$$\varphi^2 : \begin{cases} \sqrt{2} \mapsto \sqrt{2}, \\ x_1 \mapsto -x_1, \end{cases} \quad \varphi^3 : \begin{cases} \sqrt{2} \mapsto \sqrt{2}, \\ x_1 \mapsto (2x_1 + \frac{1}{2}x_1^3)\sqrt{2}, \end{cases}$$

$\varphi^4 = id$ i $\psi\varphi = \varphi^3\psi$, pa je $G = \{id, \varphi, \varphi^2, \varphi^3, \psi, \varphi\psi, \varphi^2\psi, \varphi^3\psi\}$.

Slično kao u prethodnim primerima mogu se odrediti podgrupe grupe Galoa G i odgovarajuća potpolja.

684. Neka je $x^4 + ax^2 + b$ nesvodljiv polinom nad poljem $\mathbb{Q}$ čija je grupa Galoa G . Dokazati:

- a) Ako je b kvadrat u $\mathbb{Q}$, tada je G Klajnova grupa $(C_2 \times C_2)$.
- b) Ako b nije kvadrat u $\mathbb{Q}$, ali je $b(a^2 - 4b)$ kvadrat, tada je G ciklička grupa reda 4.
- c) Ako ni b ni $b(a^2 - 4b)$ nisu kvadrati u $\mathbb{Q}$, onda je G diedarska grupa reda 8.

Uputstvo. Generalisati rešenje prethodnog zadatka.

685. Neka je $x^4 + bx^3 + cx^2 + bx + 1$ nesvodljiv polinom nad $\mathbb{Q}$ čija je grupa Galoa G . Dokazati:

- a) Ako je $c^2 + 4c + 4 - 4b^2$ kvadrat u $\mathbb{Q}$, tada je G Klajnova grupa $(C_2 \times C_2)$.
- b) Ako $c^2 + 4c + 4 - 4b^2$ nije kvadrat u $\mathbb{Q}$, ali je

$$(c^2 + 4c + 4 - 4b^2)(b^2 - 4c + 8)$$

kvadrat u $\mathbb{Q}$, tada je G ciklička grupa reda 4.

- c) Ako ni $c^2 + 4c + 4 - 4b^2$ ni $(c^2 + 4c + 4 - 4b^2)(b^2 - 4c + 8)$ nisu kvadrati u $\mathbb{Q}$, tada je G diedarska grupa reda 8.

686. Naći grupu Galoa polinoma

- a) $x^4 - 10x^2 + 1$,

b) $x^3 + 2x^2 - 10x - 15$,

c) $x^5 - 3x^3 - 2x^2 + 6$,

d) $x^5 + x^3 - 2x^2 - 2$,

nad poljem racionalnih brojeva $\mathbb{Q}$.

Uputstvo. a) Nule ovog polinoma su

$$x_1 = \sqrt{2} + \sqrt{3}, \quad x_2 = \sqrt{2} - \sqrt{3}, \quad x_3 = -\sqrt{2} + \sqrt{3}, \quad x_4 = -\sqrt{2} - \sqrt{3},$$

a grupa Galoa je $C_2 \times C_2$,

b) $x^3 + 2x^2 - 10x - 15 = (x - 3)(x^2 + 5x + 5)$,

c) $x^5 - 3x^3 - 2x^2 + 6 = (x^2 - 3)(x^3 - 2)$,

d) $x^5 + x^3 - 2x^2 - 2 = (x^2 + 1)(x^3 - 2)$.

687. Neka je p prost broj, a $f(x)$ polinom stepena p nesvodljiv nad $\mathbb{Q}$. Ako $f(x)$ ima u polju kompleksnih brojeva tačno dva korena koji nisu realni, onda je grupa Galoa polinoma $f(x)$ nad $\mathbb{Q}$ izomorfna simetričnoj grupi S_p . Dokazati.

Rešenje. Neka je G grupa Galoa polinoma $f(x)$ posmatrana kao podgrupa grupe S_p . Ako su $a_1, a_2, \dots, a_n$ koreni polinoma $f(x)$, onda je $F = \mathbb{Q}(a_1, a_2, \dots, a_n)$ faktorizacijsko polje polinoma $f(x)$. Polje $\mathbb{Q}(a_1)$ je potpolje faktorizacijskog polja F , a pošto je $f(x)$ nesvodljiv polinom nad $\mathbb{Q}$, onda je (3.24) $[\mathbb{Q}(a_1) : \mathbb{Q}] = p$. Na osnovu osnovne teoreme teorije Galoa (3.53) potpolju $\mathbb{Q}(a_1)$ polja F odgovara podgrupa H grupe G čiji je indeks u G p . Prema tome, red grupe G je deljiv sa p . Na osnovu Košijeve teoreme (1.97) grupa G sadrži element σ reda p . Permutacija σ mora onda biti ciklus dužine p (zadatak 165).

Preslikavanje definisano sa $\alpha + \beta i \mapsto \alpha - \beta i$ je $\mathbb{R}$ -automorfizam polja $\mathbb{C}$. Ako je $\alpha_1 + \beta_1 i$ kompleksan koren koji nije realan polinoma $f(x)$, onda je $\alpha_1 - \beta_1 i$ drugi kompleksan koren koji nije realan tog polinoma, prema tome, navedeni automorfizam korene koji nisu realni polinoma $f(x)$ preslikava jedan na drugi, a ostale korene ostavlja neizmenjene. Restrikcija tog automorfizma na F je automorfizam polja F , dakle, grupa G sadrži transpoziciju $\tau = (ij)$. S obzirom da se σ može pisati u obliku $\sigma = (ik_2 \dots k_p)$, neki stepen od σ je oblika $\sigma^q = (ijl_3 \dots l_p) \in G$. Permutacije τ i σ^q generišu celu grupu S_p , dakle, $G = S_p$.

PREGLED OZNAKA

U zagradi je navedena stranica na kojoj je nalazi definicija odgovarajuće oznake i broj te definicije.

$\mathbb{N}$	skup prirodnih brojeva
$\mathbb{Z}$	skup celih brojeva
$\mathbb{Q}$	skup racionalnih brojeva
$\mathbb{Q}^+$	skup pozitivnih racionalnih brojeva
$\mathbb{R}$	skup realnih brojeva
$\mathbb{R}^+$	skup pozitivnih realnih brojeva
$\mathbb{C}$	skup kompleksnih brojeva
$\text{nzd}(a, b)$	najveći zajednički delitelj za a i b
$ G $	red grupe G , kardinalni broj skupa G (s. 10 (1.31))
$ a $	red elementa grupe (s. 8 (1.14))
C_n	ciklička grupa reda n (s. 9 (1.24))
$G_1 \cong G_2$	grupe (prsteni, polja) G_1 i G_2 su izomorfne (s. 9 (1.19)), (s. 135 (2.44))
$\text{Ker } f$	jezgro homomorfizma f (s. 8 (1.18), s. 135 (2.43))
$\text{Im } f$	slika homomorfizma f (s. 8 (1.18), s. 135 (2.43))
$\langle a \rangle$	grupa generisana elementom a (s. 9 (1.22))
$\langle S \rangle$	grupa generisana skupom S (s. 9 (1.26))
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$	permutacija $1 \mapsto 4, 2 \mapsto 3, 3 \mapsto 2, 4 \mapsto 1$ (s. 10 (1.33))
$[4 \ 3 \ 2 \ 1]$	permutacija $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ (s. 10 (1.33))
$(1 \ 2 \ 3 \ 4)$	ciklus $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 4, 4 \mapsto 1$ (s. 10 (1.35))
S_n	simetrična grupa stepena n (s. 10 (1.33))
A_n	alternativna grupa stepena n (s. 11 (1.40))
P_n	grupa permutacionih matrica formata $n \times n$ (s. 11 (1.42))
D_n	diedarska grupa reda $2n$ (s. 28 (zad. 16))
$[G : H]$	indeks podgrupe H u grupi G (s. 12 (1.53))
$H \triangleleft G$	H je normalna podgrupa grupe G (s. 12 (1.56))
$G_1 \times G_2$	direktan proizvod grupa (prstena) (s. 14 (1.70)) (s. 148 zad. 380, 381))
$\mathcal{Z}(G)$	centar grupe G (s. 15 (1.74))

$\mathcal{C}(A)$	centralizator skupa A (s. 15 (1.75))
$\mathcal{N}(A)$	normalizator skupa A (s. 16 (1.76))
$[x, y]$	komutator elemenata x, y (s. 16 (1.81))
G'	izvod (komutatorska podgrupa) grupe G (s. 16 (1.82))
$\mathcal{A}(G)$	grupa automorfizama grupe G (s. 18 (1.110))
$\mathcal{U}(G)$	grupa unutrašnjih automorfizama grupe G (s. 18 (1.110))
$\mathbb{Z}_p^\infty$	Priferova grupa (s. 21 (zad. 8))
$a \equiv b \pmod{m}$	a je kongruentno sa b po modulu m (s. 24 (zad. 12))
$\mathbb{Z}_m$	skup ostataka po modulu m (s. 24 (zad. 12))
$\mathbb{Q}_p$	(s. 33 (zad. 36))
$\mathbb{Q}^p$	(s. 34 (zad. 37))
$F^{m,n}$	skup svih matrica formata $m \times n$ nad poljem F
$\text{Char } R$	karakteristika prstena R (s. 131 (2.12))
$\mathcal{C}(R)$	centar prstena R (s. 133 (2.28))
(S)	ideal generisan skupom S (s. 134 (2.38))
(a)	glavni ideal generisan elementom a (s. 135 (2.39))
$S^{-1}R$	prsten razlomaka prstena R sa imeniocima iz S (s. 137 (2.58))
$R[x]$	prsten polinoma nad R (s. 138 (2.61))
$R[x_1, x_1, \dots, x_n]$	(s. 139 (2.64))
$\deg f(x)$	stepen polinoma $f(x)$ (s. 139 (2.63))
σ_i	elementarni simetrični polinom (s. 139 (2.66))
$f'(x)$	izvod polinoma $f(x)$ (s. 141 (2.77))
s_k	Njutnova suma (s. 142 (2.82))
$\text{End}(G)$	prsten endomorfizama Abelove grupe G (s. 145 (zad. 372))
$R[[x]]$	prsten formalnih stepenih redova sa koeficijentima iz R (s. 146 (zad. 376))
$R\langle x \rangle$	prsten proširenih formalnih stepenih redova sa koeficijentima iz R (s. 147 (zad. 378))
$N(R)$	ideal nilpotentnih elemenata prstena R (s. 176 (zad. 452))
$F(S)$	polje generisano sa $F \cup S$ (s. 224 (3.15))
$[K : F]$	stepen proširenja polja K nad poljem F (s. 225 (3.22))
$F(x)$	polje racionalnih funkcija po x nad poljem F (s. 226 (3.26))
$G(K, F)$	grupa Galoa polja K nad poljem F (s. 228 (3.44))

Literatura

- [1] Artin, E., *Galois Theory*, University of Notre Dame Press, Notre Dame, 1971.
- [2] Atiyah, M. F., Macdonald, I. G., *Introduction to Commutative Algebra*, Addison-Wesley, Reading, 1969.
- [3] Baumslag, B., Chandler, B., *Group Theory*, McGraw-Hill, New York, 1968.
- [4] Birkhoff, G., MacLane, S., *A Survey of Modern Algebra (4th ed.)*, Macmillan, New York, 1977.
- [5] Božović, N., Mijajlović Ž., *Uvod u teoriju grupa*, Naučna knjiga, Beograd, 1983.
- [6] Cohn, P. M., *Algebra*, Wiley, Chichester, v. 1, 1974., v. 2. 1977.
- [7] Crvenković, S., Dolinka, I., Madarász, R. Sz., *Odabrana poglavlja opšte algebre*, PMF, Novi Sad, 1998.
- [8] Čupona, G., Trpenovski, B., *Predavanja po algebra*, knjiga II, Skopje, 1973.
- [9] Dašić, V., *Algebra*, Univerzitetska riječ, Titograd, 1987.
- [10] Devidé, V., *Zadaci iz apstraktne algebre*, Naučna knjiga, Beograd, 1971.
- [11] Doroslovački, R., *Elementi opšte i linearne algebre*, FTN-Stylos, Novi Sad, 1997.
- [12] Fang, J., *Abstract algebra*, Schaum, New York, 1963.

- [13] Fraleigh, J., B., *A First Course in Abstract Algebra*, Addison-Wesley, Reading, 1967.
- [14] Gaal, L., *Classical Galois Theory with Examples (2nd ed.)*, Chalsea, New York, 1973.
- [15] Godement, R., *Cours d'algèbre*, Hermann, Paris, 1966.
- [16] Grulović, M. Z., *Osnovi teorije grupa*, Institut za matematiku, Novi Sad, 1997.
- [17] Hall, M., *The Theory of Groups*, Macmillan, New York, 1959.
- [18] Herstein, I. N., *Topics in Algebra (2nd ed.)*, Wiley, New York, 1975.
- [19] Hungerford, T. W., *Algebra*, Springer-Verlag, New York, 1974.
- [20] Jacobson, N., *Basic Algebra*, Freeman, San Francisco, v. I, 1974, v. II, 1980.
- [21] Kalajdžić, G. V., *Algebra – osnovni pojmovi*, BS Procesor - Matematički fakultet, Beograd, 1992.
- [22] Kaplansky, I., *Fields and Rings (2nd ed.)*, The University of Chicago Press, Chicago, 1972.
- [23] Kargapolov, M. I., Merzljakov, Ju. I., *Osnovy teorii grupp*, Nauka, Moskva, 1982.
- [24] Kostrikin, A. I., *Vvedenie v algebru*, Nauka, Moskva, 1977.
- [25] Kuroš, A. G., *Obščaja algebra, lekcii 1969-1970 učebnogo goda*, Nauka, Moskva, 1974.
- [26] Kuroš, A. G., *Teorija grupp*, Nauka, Moskva, 1967.
- [27] Ledermann, W., *Introduction to the Theory of Finite Groups*, Oliver and Boyd, 1973.
- [28] Ljapin, E. C., Aizenštat, A. Ja., Lesohin, M. M., *Upražnenija po teorii grupp*, Nauka, Moskva, 1967.
- [29] Macdonald, D. I., *The Theory of Groups*, Clarendon Press, Oxford, 1968.

- [30] Milić, S., *Elementi opšte algebre*, Institut za matematiku, Novi Sad, 1984.
- [31] Perić, V., *Algebra I, II*, Svjetlost, Sarajevo, 1980.
- [32] Perić, V., *Galoisova teorija*, Prosvetni pregled, Beograd, 1997.
- [33] Prešić, S., *Zbirka zadataka iz apstraktne algebre*, Beograd, 1962.
- [34] Rose, J. S., *A Course on Group Theory*, Cambridge University Press, Cambridge, 1978.
- [35] Rotman, J. J., *The Theory of Groups (2nd ed.)*, Allyn and Bacon, Boston, 1973.
- [36] Samardžiski, A., Celakoski, N., *Rešeni zadaci po algebra II*, Skopje, 1971.
- [37] Stewart, I., *Galois Theory*, Chapman and Hall, London, 1973.
- [38] Stojaković, M., *Teorija jednačina*, Naučna knjiga, Beograd, 1973.
- [39] Ušan, J., Djonin, V., Tošić, R., *Uvod u algebru*, Radivoj Ćirpanov, Novi Sad, 1979.
- [40] van der Waerden, B. L., *Modern Algebra*, Ungar, New York, 1950.
- [41] Weinstein, M., *Examples of Groups*, Polygonal, Passaic, 1977.