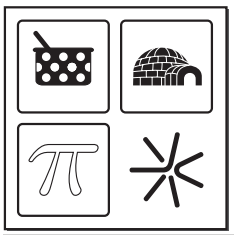

IS Petnica, seminar MATEMATIKE
Zimski MAT1, 2019
Branislav Šobot
Predavanje

# Šta će nama algebarske strukture?

## 1 Grupice

**Definicija.** ***Grupa*** $\mathbb{G}$ *je uređeni par* $(G, *)$*, gde je* $G$ *neprazan skup,* $* : G \times G \to G$ *operacija na* $G$ *i važi*

*(G1) (asocijativnost)* $(x * y) * z = x * (y * z)$ *za sve* $x, y, z \in G$*;*

*(G2) (neutralni element) postoji* $a \in G$ *takav da je* $x * a = a * x = x$ *za sve* $x \in G$ *i nadalje ga obeležavamo sa* $1$*;*

*(G3) (inverzni element) za sve* $g \in G$ *postoji neko* $h \in G$ *tako da je* $h * g = g * h = 1$ *i nadalje označavamo* $h = g^{-1}$*.*

*Grupa* $\mathbb{G}$ *je* ***komutativna*** *(Abelova) ako za sve* $x, y \in G$ *važi* $x * y = y * x$*.*

**Primer.** $(\mathbb{Z}, +)$ *je komutativna grupa;* $(\mathbb{Q}, +)$ *je komutativna grupa;* $(\mathbb{N}, +)$ *nije grupa;* $(\mathbb{R} \setminus \{0\}, \cdot)$ *je komutativna grupa;* $(\mathbb{Z}, -)$ *nije grupa; Nekomutativna grupa simetrija pravilnog* $n$*-tougla* $\mathbb{D}_n$*; Nekomutativna grupa permutacija* $\mathbb{S}_n$*; Ako je* $\mathbb{G}$ *grupa, onda imamo grupu svih matrica* $GL_n(\mathbb{G})$ *formata* $n \times n$ *čija su polja elementi skupa* $G$*, a operacija je po koordinatama; grupa* $\mathbb{Z}_n$ *svih ostataka po modulu* $n$ *gde je operacija* $+_n$ *sabiranje po modulu* $n$*.*

**Definicija.** *Neka su* $\mathbb{G} = (G, *)$ *i* $\mathbb{H} = (H, \cdot)$ *grupe. Funkcija* $f : G \to H$ *se naziva* ***izomorfizam*** *ako je bijekcija i za sve* $x, y \in G$ *važi* $f(x * y) = f(x) \cdot f(y)$*. Ako postoji izomorfizam između dve grupe, onda pišemo* $\mathbb{G} \cong \mathbb{H}$ *i nama su te grupe suštinski iste, samo što smo odlučili da različito zovemo elemente i operacije.*

**Primer.** *Trivijalno je* $\mathbb{Z}_1 \cong \mathbb{S}_1$*; Grupa rotacija pravilnog* $n$*-tougla je izomorfna sa* $\mathbb{Z}_n$*.*

**Definicija.** *Neka je* $\mathbb{G} = (G, \cdot)$ *grupa i* $H \subseteq G$*. Kažemo da je* $\mathbb{H} = (H, \cdot)$ ***podgrupa*** *grupe* $\mathbb{G}$*, i to pišemo* $\mathbb{H} \leq \mathbb{G}$*, ako za sve* $a, b \in H$ *važi* $a \cdot b^{-1} \in H$*. Ovo je samo jedan od načina da se kaže:* $\mathbb{G}$ *i* $\mathbb{H}$ *su grupe i* $\mathbb{H}$ *je sadržana u* $\mathbb{G}$*.*

**Primer.** *Trivijalno je* $\mathbb{G}, \{0\} \leq \mathbb{G}$ *uvek;* $(\mathbb{Q}, +)$ *je podgrupa od* $(\mathbb{R}, +)$*;* $(\mathbb{N}, +)$ *nije podgrupa od* $(\mathbb{Z}, +)$ *jer nije grupa;* $(\mathbb{Z}_n, +_n)$ *nije podgrupa grupe* $(\mathbb{Z}, +)$ *jer nije ista operacija; Ako je* $a$ *elment grupe* $G$*, onda je* $\{a^n : n \in \mathbb{Z}\}$ *podgrupa grupe* $\mathbb{G}$*.*

**Definicija.** ***Red grupe*** *je broj elemenata te grupe. Neka je* $\mathbb{G} = (G, \cdot)$ *grupa i* $a \in G$*.* ***Red elementa*** $a$ *u grupi* $\mathbb{G}$ *je najmanji prirodan broj* $n \in \mathbb{N}$ *takav da je* $a^n = 1$*. Ako takav broj ne postoji, kažemo da je* $a$ *beskonačnog reda.*

**Primer.** *Grupa* $\mathbb{S}_n$ *je reda* $n!$*; Red svake osne simetrije u* $\mathbb{D}_n$ *je 2; U konačnoj grupi, red svakog elementa je konačan; U grupi* $(\mathbb{Z}, +)$ *red svakog elementa (sem* $0$*) je beskonačan.*

**Teorema 1.** *(Lagranžova teorema) Neka je* $\mathbb{G}$ *konačna grupa i* $\mathbb{H} \leq \mathbb{G}$*. Tada red grupe* $\mathbb{H}$ *deli red grupe* $\mathbb{G}$*. Specijalno, red svakog elementa grupe* $\mathbb{G}$ *deli red grupe* $\mathbb{G}$*.*

1. Neka je $F$ neki neprazan skup. Dokazati da skup svih bijekcija na skupu $F$ čini grupu sa operacijom kompozicije. Ta grupa se naziva grupa simetrija skupa $F$. Vidite li vezu sa permutacijama?

2. Posmatrajmo ponovo $\mathbb{Z}_n$, tj. ostatke po modulu $n$. Obeležimo sa $\mathbb{Z}_n^\times$ podskup svih ostataka uzajamno prostih sa $n$ (npr. $\mathbb{Z}_6^\times = \{1, 5\}$). Dokazati da je $(\mathbb{Z}_n^\times, \cdot_n)$ grupa, gde je $\cdot_n$ množenje po modulu $n$. Zašto smo baš uzeli samo one uzajmno proste sa $n$, a ne recimo sve ostatke?

3. Dokazati da sva rešenja jednačine $x^n = 1$ čine grupu, ako znamo da ih ima $n$ različitih.

4. Označimo sa $\rho$ i $\sigma$ redom proizvoljnu rotaciju i proizvoljnu osnu simetriju pravilnog 2019-ugla. Dokazati da je $(\sigma \circ \rho)^{-1} = \rho^{-1} \circ \sigma^{-1}$.

5. Dokazati da skup svih polinoma sa realnim koeficijentima (tj. izraza oblika $a_n x^n + ... + a_1 x + a_0$ gde $a_0, a_1, ..., a_n \in \mathbb{R}$) sa uobičajenom operacijom sabiranja polinoma čini grupu.

6. Dokazati da je $\mathbb{S}_2 \cong \mathbb{Z}_2$ i da je $\mathbb{S}_3 \cong \mathbb{D}_3$.

7. Obeležimo sa $\mathbb{V}_4$ grupu sa elementima $1, a, b, c$ u kojoj je operacija $\cdot$ definisana sa $a \cdot a = b \cdot b = c \cdot c = 1$, $a \cdot b = b \cdot a = a \cdot c = c \cdot a = b \cdot c = c \cdot b$ i $1 \cdot x = x \cdot 1 = x$ za sve $x \in \{a, b, c\}$ (ovo se inače zove Klajnova grupa). Dalje, obeležimo sa $\mathbb{Z}_2 \times \mathbb{Z}_2$ grupu sa elementima $(0, 0), (0, 1), (1, 0), (1, 1)$ i sabiranjem po koordinatama po modulu 2 (ovo ima neke veze sa proizvodom grupa). Dokazati da je $\mathbb{V}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

8. Da li je $(\mathbb{R} \setminus \{0\}, \cdot)$ podgrupa grupe $(\mathbb{R}, +)$?

9. Naći sve podgrupe grupa $\mathbb{S}_3$ i $\mathbb{D}_4$.

10. Neka je $\mathbb{G}$ grupa i neka je $a \in G$ element konačnog reda $n$. Dokazati da ako je $a^m = 1$, onda $n|m$.

11. Dokazati da grupa $(\mathbb{Z}_p, +_p)$ nema netrivijalnih podgrupa.

12. Dokazati

    - (Ojlerova teorema) Neka $\varphi(n)$ označava broj prirodnih brojeva manjih od $n$ koji su uzajamno prosti sa $n$ (npr. $\varphi(6) = 2$). Ako su $a$ i $m$ uzajamno prosti brojevi, dokazati da $m|a^{\varphi(m)} - 1$.
    - (Mala Fermaova teorema) Ako je $p$ prost broj i $a$ prirodan koji nije deljiv sa $p$, dokazati da $p|a^{p-1} - 1$.

13. Neka nam je data rubikova kocka u početnoj poziciji. Dokazati da ako uzmemo bilo koji partern (neki niz poteza) i ponavljamo ga dovoljno dugo vratićemo se u početnu poziciju.

14. Kažemo da je broj $a < p$ primitivni koren po prostom modulu $p$ ako je najmanji prirodan broj $n$ takav da $p|a^n - 1$ upravo $p - 1$.

    - Dokazati da je $a$ primitivni koren po modulu $p$ ako i samo ako je broj $a$ reda $p-1$ u grupi $(\mathbb{Z}_p^\times, \cdot_p)$ (videti zadatak 2).
    - Dokazati da postoji tačno $\varphi(p-1)$ primitivnih korena po modulu $p$ ako je $p$ prost.

15. - Neka su $p$ i $q$ prosti. Ako je $q|2^p - 1$, onda $p|q - 1$ (dakle, $p < q$).
    - Dokazati da prostih brojeva ima beskonačno mnogo koristeći prethodnu tufnu.

# 2 Prstenčići i poljica

**Definicija.** ***Prsten*** *je uređena trojka $(R, +, \cdot)$, gde su $+$ i $\cdot$ operacije na $R$ takve da važi*

*(R1) $(R, +)$ je komutativna grupa;*

*(R2) (asocijativnost za $\cdot$) Za sve $x, y, z \in R$ važi $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;*

*(R3) (distributivnosti) Za sve $x, y, z \in R$ važi $x \cdot (y + z) = x \cdot y + x \cdot z$ i $(y + z) \cdot x = y \cdot x + z \cdot x$.*

**Primer.** *$(\mathbb{Z}, +, \cdot)$ je prsten; $(\mathbb{Q}, +, \cdot)$ je prsten; Ako posmatramo sve funkcije $f : [0, 1] \to \mathbb{R}$ sa operacijama $+$ i $\cdot$ po tačkama, one čine prsten; $(\mathbb{Z}, \cdot, +)$ nije prsten; $(\mathbb{Z}_n, +_n, \cdot_n)$ je prsten.*

**Definicija.** ***Polje*** *je uređena trojka $\mathbb{F} = (F, +, \cdot)$, gde su $+$ i $\cdot$ operacije na $F$ takve da važi*

*(F1) $(F, +)$ je komutativna grupa;*

*(F2) $(F \setminus \{0\}, \cdot)$ je komutativna grupa;*

*(F3) Važe distributivni zakoni.*

**Primer.** *$(\mathbb{Q}, +, \cdot)$ je polje; $(\mathbb{R}, +, \cdot)$ je polje; $(\mathbb{Z}, +, \cdot)$ nije polje; ako je $p$ prost, onda je $(\mathbb{Z}_p, +_p, \cdot_p)$ je polja; $(\mathbb{Z}_4, +_4, \cdot_4)$ nije polje; Ako je $\mathbb{F}$ polje, onda je $\mathbb{F}[x]$ prsten polinoma nad $\mathbb{F}$.*

U nastavku šta je sve sposobna teorija polja da dokaže:

**Teorema 2.** *(Abel-Ruffini) Postoji polinom petog stepena koji ima nulu koja se ne može izraziti koristeći se celim brojevima i operacijama sabiranja, oduzimanja, množenja, deljenja i korenovanja.*

**Teorema 3.** *(Trisekcija ugla) Ugao od $\frac{\pi}{3}$ se ne može podeliti na tri jedanka dela koristeći se samo šetarom i lenjirom.*

**Teorema 4.** *(Kvadratura kruga) Ako je dat krug, onda je nemoguće konstruisati kvadrat jednake površine koristeći samo šestar i lenjir.*

**Teorema 5.** *(Dublikacija kocke) Ako je data kocka, nemoguće je konstruisati kocku duplo veće zapremine koristeći se samo šestarom i lenjirom.*

Kako se pokazuju ove stvari? Pretpostavimo da na početku imamo koordinatni početak i tačku $(1, 0)$. Kažemo da je neki broj $x \in \mathbb{R}$ **konstruktibilan** ako se tačka $(x, 0)$ može konstruisati pomoću šestara i lenjira. Vrlo zamornim osnovnoškolskim konstrukcijama pokaže se da je ustvari skup svih konstruktabilnih brojeva jedno polje (sa operacijama sabiranja i množenja realnih brojeva) koje je sadržano u $\mathbb{R}$. Zatim se pokaže da je broj konstruktabilan ako i samo ako mu je stepen ekstenzije broj oblika $2^k$ (šta god bio taj stepen ekstenzije). Kao završni udarac imamo da u sva tri problema iz pretpostavke da su pomenute konstrukcije moguće dobijamo da su konstruktabilni brojevi čiji stepeni ekstenzije svakako nisu stepeni dvojke.

**Teorema 6.** *Za svaki prost broj $p$ i svako $n \in \mathbb{N}$ postoji jedinstveno (do na izomorfizam) polje reda $p^n$.*

1. Neka je $(G, +)$ komutativna grupa. Dokazati da ako definišemo $x \cdot y = 0$ za sve $x, y \in G$ dobijamo da je $(G, +, \cdot)$ prsten.
2. Obeležimo sa $2\mathbb{Z}$ skup svih parnih celih brojeva. Dokazati da je $(2\mathbb{Z}, +, \cdot)$ prsten u kojem ne postoji neutralni element za drugu operaciju.
3. Neka je $A$ neprazan skup i neka je $X \Delta Y = (X \setminus Y) \cup (Y \setminus X)$ za sve $X, Y \subseteq A$ (dakle simetrična razlika). Dokazati da je $(\mathcal{P}(A), \Delta, \cap)$ prsten.
4. Neka je $F = \{0, 1, x, 1+x\}$ (dakle skup nekih polinoma). Dokazati da je $(F, +_2, \cdot_2)$ polje, gde polinome sabiramo tako što njihove koeficijente sabiramo po modulu 2 (i za množenje slično). Po uzoru na ovaj primer, naći primer polja sa 8 elemenata.
5. Uvedimo oznaku $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b : a, b \in \mathbb{Q}\}$. Dokazati da je $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ polje.
6. Sad generalno, ako $x \in \mathbb{R}$, onda sa $\mathbb{Q}[x]$ obeležimo najmanje polje koje sadrži $\mathbb{Q}$ i broj $x$ (primetimo da je bilo $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ jer zaista sve brojeve tog oblika moramo imati da bi bilo zatvoreno za operacije polja, a da je zaista polje to je zadatak broj 5). Dokazati da je $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[1 + \sqrt{2}]$.
7. Neka je $\mathbb{F}$ konačno polje sa elementima $0, x_1, ..., x_n$ (znači jedan od ovih $x_i$ je 1). Dokazati da je $1 + x_1x_2...x_n = 0$. Kakve ovo ima veze sa malom Fermaovom teoremom?
8. (Vilsonova teorema) Ako je $p$ prost, dokazati da je $(p-1)! \equiv -1 (\mathrm{mod}\, p)$.
9. **Karakteristika** polja $\mathbb{F} = (F, +, \cdot)$ je najmanji broj $p \in \mathbb{N}$ takav da je $p \cdot a = 0$ za sve $a \in F$. Ukoliko taj broj ne postoji, kažemo da je polje karakteristike 0.
   - Dokazati da je svako konačno polje ima nenula karakteristiku.
   - Dokazati da je karakteristika konačnog polja prost broj(Hint: posmatrati potpolje generisano sa 1).