Uvod: pojmovi grupe i polja

Ovo je uvodno poglavlje. U njemu ćemo uvesti neke matematičke pojmove koji će nam biti potrebni tokom kursa *Linearne algebre*.
Skup je jedan od svega nekoliko pojmova u matematici koji se ne definiše. Smatramo da svi podrazumijevamo isto kada koristimo riječ "skup". Skup koji sadrži konačan broj elemenata nazivamo konačnim. Kako bismo stvorili sadržajne matematičke teorije na skupovima uvodimo različite operacije i strukture.
Algebra je široka oblast matematike koja se bavi skupovima i strukturama na skupovima. Slijede dva primjera algebarskih struktura.

Definicija 0.1. *Reći ćemo da je na skupu G uvedena struktura grupe, ako je na G zadata operacija "+", tako da su zadovoljeni sljedeći uslovi:*
1) za $\forall a, b \in G$ važi $a + b \in G$;
2) za $\forall a, b, c \in G$ važi $a + (b + c) = (a + b) + c$;
3) $\exists 0 \in G$ tako da za $\forall a \in G$ važi $a + 0 = 0 + a = a$;
4) za $\forall a \in G \quad \exists(-a) \in G$ tako da $a + (-a) = (-a) + a = 0$.

Takođe ćemo govoriti da skup G sa operacijom "+" čini grupu (ili da je grupa).
Svojstvo 1) naziva se zatvorenost skupa G u odnosu na definisanu operaciju "+", svojstvo 2) asocijativnost, element 0 iz svojstva 3) naziva se neutralnim elementom grupe, a element $(-a)$ iz svojstva 4) inverznim elementom k elementu a.

Definicija 0.2. *Neka je $(G, +)$ grupa. Ako $\forall a, b \in G$ važi $a + b = b + a$ tada se grupa $(G, +)$ naziva komutativnom (Abelovom) grupom.*

Primjer 1. Skup realnih brojeva $\mathbb{R}$ sa standardnom operacijom sabiranja "+" je grupa, $(\mathbb{R}, +)$.
Primjer 2. Skup cijelih brojeva $\mathbb{Z}$ sa standardnom operacijom sabiranja "+" je grupa, $(\mathbb{Z}, +)$.
Primjer 3. Skup prirodnih brojeva sa operacijom sabiranja, $(\mathbb{N}, +)$ nije grupa (npr. neutralni element za sabiranje, 0, nije iz skupa prirodnih brojeva, takođe elementi $\mathbb{N}$ nemaju inverzne elemente).
Primjer 4. Skup cijelih brojeva $\mathbb{Z}$ sa standardnom operacijom množenja "$\cdot$" nije grupa (zadovoljene su sve aksiome, osim 4)).
Primjer 5. Označimo sa H skup svih rotacija geometrijske ravni za uglove $\phi \in [0, 2\pi)$. Na skupu H uvedimo operaciju "$\cdot$" superpozicije (kompozicije) dvije rotacije. Neka su $r_{\phi_1}, r_{\phi_2} \in H$, tada $r_{\phi_1} \cdot r_{\phi_2} = r_{\phi_1 + \phi_2} \in H$. Na ovaj način, superpozicija dvije rotacije je takođe rotacija. Potrebno je provjeriti sve četiri aksiome kako bismo se ubijedili da je $(H, \cdot)$ Abelova grupa.

Primjer 6. Razmotrimo konačan skup M sa n elemenata, recimo riječ LIST (ovaj skup ima $n = 4$ elementa, tj. slova). Označimo sa P skup svih permutacija konačnog skupa M. Skup P sadrži $n!$ elemenata. Na skupu P uvedimo operaciju "$\cdot$" superpozicije dvije permutacije, tj. ako su $p_1, p_2 \in P$, to je $p_1 \cdot p_2$ nova permutacija koja se dobija tako što se na skupu najprije izvede permutacija p_2, a zatim p_1. Recimo, ako je p_1 permutacija koja riječ LIST preslikava u ILST, a p_2 u STLI, to će $p_1 \cdot p_2$ riječ LIST permutovati u TSLI. Kada provjerimo sve aksiome zaključujemo da skup P sa operacijom "$\cdot$" čini grupu. Provjeriti da li je ovo Abelova grupa.

Definicija 0.3. *Reći ćemo da je na skupu P uvedena struktura polja, ako su na skupu P zadate dvije operacije "$+$" i "$\cdot$" tako da su zadovoljeni sljedeći uslovi:*
1. za $\forall a, b \in P$ važi $a + b \in P$ i $a \cdot b \in P$;
2. za $\forall a, b, c \in P$ važi $(a + b) + c = a + (b + c)$ i $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
3. $\exists 0 \in P$ tako da za $\forall a \in P$ važi $a + 0 = a$;
4. za $\forall a \in P \quad \exists(-a) \in P$ tako da $a + (-a) = 0$;
5. za $\forall a, b \in P$ važi $a + b = b + a$ i $a \cdot b = b \cdot a$;
6. $\exists 1 \in P$ tako da za $\forall a \in P \backslash \{0\} \quad a \cdot 1 = a$;
7. za $\forall a \in P \backslash \{0\} \quad \exists a^{-1} \in P \backslash \{0\}$ tako da važi $a \cdot a^{-1} = 1$;
8. za $\forall a, b, c \in P$ važi $a \cdot (b + c) = a \cdot b + a \cdot c$ i $(a + b) \cdot c = a \cdot c + b \cdot c$.

Operacije "$+$" i "$\cdot$" u polju se nazivaju "sabiranjem" i "množenjem". Neutralni element sabiranja, koji smo označili znakom 0, se naziva "nulom". Neutralni element množenja 1 se naziva "jedinicom".
Svojstvo 2.) se naziva asocijativnošću sabiranja i množenja, svojstvo 5.) komutativnošću, a svojstvo 8.) distributivnošću.
Primjer 1. Skup realnih brojeva, $\mathbb{R}$ sa standardnim operacijama sabiranja i množenja, tj. struktura $(\mathbb{R}, +, \cdot)$, čini polje.
Primjer 2. Skup racionalnih brojeva $\mathbb{Q}$ sa standardnim operacijama sabiranja i množenja čini polje.
Dio algebre, koji nam je dobro poznat iz škole, koji se bavi konkretnim skupom racionalnih brojeva sa operacijama sabiranja i množenja (a, dakle, i oduzimanja i dijeljenja) se naziva *Aritmetika*.
Primjer 3. Skup kompleksnih brojeva, $\mathbb{C}$ sa standardnim operacijama sabiranja i množenja, tj. struktura $(\mathbb{C}, +, \cdot)$ čini polje.
Primjer 4. Razmotrimo skup S koji sadrži četiri elementa, označićemo ih simbolima O,I,A i B. Na skupu S uvedimo operacije $+$ i $\cdot$ uz pomoć sljedećih tabela:

+	O	I	A	B	·	O	I	A	B
O	O	I	A	B	O	O	O	O	O
I	I	O	B	A	I	O	I	A	B
A	A	B	O	I	A	O	A	B	I
B	B	A	I	O	B	O	B	I	A

Provjerite da skup S sa ovim operacijama čini polje.
Ovim završavamo uvodno poglavlje u kojem smo uveli neke osnovne pojmove iz *Opšte algebre* koje ćemo dalje koristiti. Primijetimo da ćemo u svim daljim izlaganjima koristiti samo dva polja: to su polje realnih brojeva $\mathbb{R}$ i polje kompleksnih brojeva $\mathbb{C}$. Pri tome pretpostavljamo da

su studenti upoznati sa standardnim operacijama sabiranja i množenja (a znači i oduzimanja i dijeljenja) kako realnih, tako i kompleksnih brojeva.