Algebarske strukture:

1. Definicija operacije i binarne operacije. Cayleyeva tablica. Primjeri operacija.

Funkcija f_1: $S_1 x S_2 \rightarrow S_3$ zove se binarna operacija.
f_1:SxS $\rightarrow$ S zove se binarna operacija na skupu S
Vidimo da je binarna funkcija funkcija 2 argumenta (varijable).

z=x+y
Zapis binarne funkcije je cesto infiksan, ali ne uvijk (npr. nzv(6,15) $\rightarrow$ prefiksno).
Operacija može biti unarna, ternarna, ili opženito n-arna.
- unarna f:S$\rightarrow$S (npr. x^2)
- ternarna f:SxSxS$\rightarrow$S (npr. u=xyz)
- n-arna f:(x_1 x x_2 x x_3 x…x x_n)$\rightarrow$x (x_1+x_2+x_3+…)

Od ranije znamo da se funkcija može zadavati tablično, ali nam je poznat slučaj samo jedne varijable:

x	f(x)
1	2
2	4
0	0

Kako su operacije specijalne funkcije, ako je skup na kojem se definira konačan, tada se binarna operacija može zadati dvodimenzionalnom tablicom, koja se naziva Cayleyeva tablica. U slučaju ternarne operacije, “tablica” bi trebala biti trodimenzionalna, pa se tablični prikaz od 3 ili više argumenata ne koristi.
Primjer:
NZD (x,y), S={1,2,3}

NZD	1	2	3
1	1	1	1
2	1	2	1
3	1	1	3

Operacija može biti i teoretkska:
a*b ili *(a,b), S={a,b}

*	a	b
a	a	a
b	b	b

Za ovu operaciju se ne može zadati formula operacije, jedino tablica.
Ako je zadana binarna operacija $f: A \times A \rightarrow A$ i ako je skup A konačan i ima n elemenata, tada broj različitih operacija na skupu A iznosi n^{n^2}.

Primjeri operacija: neke temeljne binarne operacije na skupu G:
- operacija zbrajanja realnih brojeva (G=R, a+b)
- množenje realnih brojeva (G=R, a*b)
- najveća zajednička mjera dvaju prirodnih brojeva (G=N, Nzm(a,b))
- zbrajanje I množenje kompleksnih brojeva, zbrajanje vektora, kompozicija dviju funkcija,zbrajanje pravokutnih matrica, itd.

2. Osnovna svojstva binarnih operacija. Vanjska i unutarnja operacija. Grupoid.

Skup na kojem je definirana neka operacija naziva se operacijska struktura.
Primjer: (R,+), (N,+,·) ili općenito (S,*) ili (S,*,○)
* i ○ – hipotetske operacije
Nas zanimaju one operacijske strukture čije operacije imaju neka "lijepa" svojstva:
a) svojstvo zatvorenosti:
(za svaki a,b $\in$ S) (a*b $\in$ S)
b) svojstvo komutativnosti:
(za svaki a,b $\in$ S) a*b=b*a
c) svostvo asocijativnosti
(za svaki a,b,c $\in$ S) a*(b*c)=(a*b)*c
d) neutralni element
(za svaki x $\in$ S) (postoji e $\in$ S) (x*e = e*x = x), e-neutralni element
e) inverzni element
(za svaki x $\in$ S) (postoji y $\in$ S) (x*y = y*x = e), y-inverzni element elementa x, općenito se označava sa x^{-1}

Vanjska i unutarnja operacija???

Struktura (S,*) se naziva grupoid ako operacija * ima svojstvo zatvorenosti.
Primjer:
(N,+) je grupoid
(V, ·) nije grupoid (jer dobijemo broj, a ne vektor).

3. Definicija polugrupe i monoida. Dajte primjere.

Grupoid (S,*) sa svojstovom asocijativnosti za operaciju * naziva se polugrupa.
Primjeri: (N, +) je polugrupa
(V, x) nije polugrupa jer x nije asocijativno (napisat primjer)
Ako u polugrupi (S,*) postoji element e takav da (za svaki x $\in$ S) (x*e = e*x = x), tada se struktura naziva monoid (polugrupa s jedinicom).
e – jedinica polugrupe ili neutralni element polugrupe
Primjer:
(N,+) – grupoid, polugrupa
x+e = e+x = x → nema takvoga e, pa ovo nije monoid
(N_0,+) → onda ima e, koji je jednak 0
(N,·) – grupoid, polugrupa, monoid → e=1

Napomena: ako je binarna operacija zapisana aditivno, kao +, onda se neutralni element zove *nula* (nul-element) i označava sa 0.

4. Pojam slobodne polugrupe.

Neka je Y bilo koji skup simbola, koje interpretiramo kao *slova*. **Riječ** na X je konačan slijed elemenata skupa X. Npr. ako je X={a,b,c}, onda su S=aaac, T=ababba, U= abacbb riječi na X. Skup svih riječi označavamo sa X*.
Definirajmo sada binarnu operaciju · na skupu X*. Ako su S i T dvije riječi, onda neka je ST riječ dobivena tako da najprije napišemo redom sva slova riječi S i odmah do njih desno nadovežemo slova riječi T. U gornjem primjeru je ST=aaacababba. Ovakva binarna operacija zove se konkatenacija (ulančavanje, nadovezivanje) riječi.
Lako je provjeriti da je konkatenacija asocijativna operacija. Provjeri se najlakše na primjeru T(SU)=(TS)U. Time smo dobili polugrupu (X*.·) svih riječi koja se zove **slobodna polugrupa**.
Slobodnoj polugrupi X* možemo pridružiti još jedan element (riječ) λ koji se zove *prazna riječ*. Jasno je da se konkatenacijom s praznom riječi ništa ne mijenja: λT=T λ=T za svaki T iz X*, uključujući i T= λ. Prema tome, λ je neutralni element, čime X* postaje monoid s obzirom na operaciju konkatenacije.

5. Definicija grupe. Abelova grupa. Aditivna i multiplikativna grupa.

Struktura (S,*) se zove **grupa** ako je monoid u kojem
(za svaki x $\in$ S) (postoji $x^{-1} \in$ S) ($x*x^{-1}=x^{-1}*x=e$)
x^{-1} – inverzni element elementa x
Primjer: (Z,+) → $x+x^{-1}=0$

U slučaju da je zapis aditivni (S,+), inverzni element se označava sa –x, a ako je zapis multiplikativni ili opći, inverzni element se označava s x^{-1}. Ako element x strukture ima inverzni element, tada za x kažemo da je invertibilan.
Ako je uz sva svojstva grupe operacija * komutativna, za grupu (S,*) kažemo da je komutativna grupa ili **Abelova grupa**.
Ako je u nekoj Abelovoj grupi (S,*) binarna operacija zapisana multiplikativno, tj. ako je zadana grupa (S,·), onda grupu nazivamo **multiplikativnom grupom**. U njoj operaciju · zovemo množenjem.
Ako je u nekoj Abelovoj grupi (S,*) binarna operacija zapisana aditivno, tj. ako je zadana grupa (S,+), onda grupu nazivamo **aditivnom grupom**. Po dogovoru, svaka aditivna grupa je Abelova grupa. Neutralni element aditivne grupe zovemo **nula** (i označavamo s 0), a inverzni element od a označavamo sa –a umjesto a^{-1} i zovemo **suprotni element**.
Inverzni element a^{-1} od a je jedincat, tj. ne moegu postojati dva različita inverzna elementa od a. Vrijedi $(a^{-1})^{-1}=a$.
Neka je (S, ·) grupa.

a) (invertiranje produkta) Za sve a,b $\in$ S vrijedi:

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

b) (pravilo skraćivanja) Za sve a,b,c $\in$ S iz uvjeta ac=bc slijedi a=b. Na sličan način iz ca=cb slijedi a=b.

6. Potencije a^n i a^{-n} u grupi. Teorem o potencijama u multiplikativnom i aditivnom obliku.

Ako je *n* prirodan broj, onda se u svakoj grupi definira potencija elementa:
$x^n = x*x*x*...*x$
$x^{-n} = x^{-1}*x^{-1}*...*x^{-1}$
$(x^{-1})^n = x^{-n}$
$a^0 = e$

Ako je zapis grupe aditivan, tada se x^n zapisuje:
$x^n = n\cdot x = x+x+x+x+x+...+x$
Ako je zapis multiplikativan:
$x^n = x\cdot x\cdot x... \cdot x$

Teoremi o potencijama u multiplikativnom obliku, u grupi (S, ·):

a) $x^m\cdot y^n = x^{m+n} = x^n\cdot x^m$ (komutativnost vrijedi zobg operacije +, a ne ·)
b) $x^n\cdot y^n = (x\cdot y)^n \neq (y\cdot x)^n$
c) $(x^m)^n = x^{m\cdot n}$

Teoremi o potencijama u aditivnom obliku , u grupi (S,+):

a) $mx+nx = (m+n)\cdot x = nx+mx$
b) $nx+ny = n(x+y) \neq n(y+x)$
c) $n\cdot(mx) = (n\cdot m)x = (m\cdot n)x$

7. Pojam podgrupe i reda grupe.

Ako su (S,*) i (T,*) dvije grupe sa istom operacijom, i pritom je S podskup od T, tada kažemo da je (S,*) podgrupa grupe (T,*), što se označava: (S,*) ≤ (T,*). Ako je pritom S pravi podskup od T, onda pišemo (S,*) < (T,*).

({e},*) – trivijalna podgrupa (ima svojstva I zatvorenosti I asocijativnosti)

Ako je (S,*) grupa, i k(S)=n (k-kardinalni broj) konačan broj, tada kažemo da je grupa konačna. Broj *n* se naziva red grupe.
Ako je broj elemenata skupa S beskonačan, tada kažemo da je grupa (S,*) beskonačna ili beskonačnog reda.

8. Primjeri konačne i beskonačne Abelove i ne-Abelove grupe.

Primjeri konačnih Abelovih grupa:
a) Grupa samo s jednim elementom zove se *trivijalna grupa* ({e},*). To su npr. ({1},·) ili ({0},+)
b) Grupa ({-1,1},·) je reda dva. Skup {1,-1,i,-i} je grupa s obzirom na množenje kompleksnih brojeva, i njen red je četiri.

Primjeri beskonačnih Abelovih grupa:
a) **Z** ≤ **Q** ≤ **R** ≤ **C**   Svaka podgrupa aditivne grupe cijelih brojeva **Z** ima oblik n**Z** = 0,1,2, ...
b) Skup $\mathbf{R}^n$ svih poredanih n-teraca realnih brojeva je grupa s obzirom na zbrajanje vektora (koje se definira kao zbrajanja po komponentama). Očito je $\mathbf{R}^n \leq \mathbf{R}^{n+1}$, jer $\mathbf{R}^n$ možemo shvatiti kao podskup $\mathbf{R}^{n+1}$ tako da element vektor $(x_1, \ldots ,x_n) \in \mathbf{R}^n$ poistovjetimo s vektorom $(x_1, \ldots , x_n , 0) \in \mathbf{R}^{n+1}$
c) Skup svih kompleksnih brojeva na jediničnoj kružnici u **C** je grupa s obzirom na množenje. Označava se sa S^1. Očito je $\mathbf{C_n} \leq S^1$ za svaki n iz **N**.

Primjeri beskonačnih nekomutativnih grupa:
a) Skup svih regularnih (invertibilnih) kvadratnih matrica s realnim koeficijentima reda n≥2 je grupa s obziromna množenje matrica. Označava se sa GL(n, R) i zove se opća linearna grupa. Neutralni element je jedinična matrica *I*. Svojstvo grupoidnosti je posljedica činjenice da je produkt regularnih matrica opet regularna matrica. Ova grupa je beskonačna i nekomutativna. Neke podgrupe su grupa regularnih gornjih trokutastih matriva, grupa matrica čija je determinanta jednaka 1, itd.
b) Neka je zadan skup X i neka je G skup svih bijekcija f:X→X. Taj skup je grupa s obzirom na kompoziciju funkcija kao binarnu operaciju u zove se grupa permutacija skupa X. Elementi se zovu permutacije skupa X. Neutralni element

je identična funkcija, a inverzni element je inverzna funkcija f^{-1}. Ta grupa je općenito nekomutativna, već kad je X tročlan skup.

9. Podgrupa generirana elementom *a*. Ciklička grupa.

U grupi (S,*) uzmimo element *a* i promatrajno skup $\{a^k : k \in \mathbf{Z}\}$. TO je podgrupa grupe S: Označavamo ju sa:

$$<a> = \{a^k : k \in \mathbf{Z}\}$$

To je najmanja (s obzirom na inkluziju) podgrupa grupe S koja sadrži *a* kao svoj element. Podgrupu $<a>$ zovemo podgrupom **generiranom** elementom *a*. Element *a* zovemo generatorom te podgrupe.

Neka je (S,*) grupa i $a \in S$, $a \neq e$. Ako za neki prirodni broj *n* vrijedi $a^n=e$, onda najmanji takav *n* zovemo **redom elementa a** i označavamo sa $n = |a|$.

Ako je *a* reda *n*, onda je inverz elementa a^k jednak a^{n-k}, jer je $a^k a^{n-k} = e$.

$$(a^k)^{-1} = a^{n-k}$$

Za grupu (S,*) kažemo da je **ciklička grupa** ako postoji element $a \in S$ takav da je $S = <a>$, tj. svaki $x \in S$ se može napisati u obliku potencije $x = a^k$ za neki $k \in Z$:

$$S = \{a^k : k \in Z\}$$

Element *a* se zove **generator** cikličke grupe S. Kažemo da je ciklička grupa S generirana elementom *a*.

Ako je generator *a* konačnog reda *n*, onda je ciklička grupa reda *n*:

$$S = \{e,a,a^2, \dots , a^{n-1}\}$$

Ako je $a^k \neq e$ za svaki $k \in N$, onda je S **beskonačna ciklička grupa**:

$$S = \{\dots, a^{-2},a^{-1},e,a,a^2, \dots\}$$

Primjer toga je aditivna grupa cijlih brojeva Z, koja je generirana elementom 1:

$$S = \{\dots, -2,-1,0,1,2, \dots\} = <1>$$

10. O grupi n-tih korjena iz jedinice Cn.

Koji su to elementi konačne cikličke grupe koji generiraju cijelu grupu? Grupu C_n čine svi n-ti korijeni iz jedinice. Ima ih ukupno n, i u Gaussovoj ravnini predstavljaju one kompleksne brojeve koji leže u vrhovima pravilnog n-terokuta upisanog u jediničnu kružnicu oko ishodišta:

$$\cos(2k\pi/n)+i\sin(2k\pi/n),\ k = 0,1, \dots , n-1$$

Svaki n-ti korijen iz jedinice koji je generator cikličke grupe C_n zove se **primitivni n-ti korijen** iz jedinice.

Primjer: Element $\varepsilon = \cos(2\pi/n)+ i\sin(2\pi/n)$ je primitivni n-ti korijen iz jedinice.

Sljedeći teorem opisuje koji još elementi cikličke grupe C_n mogu biti primitivni korijeni:

a) Element $\varepsilon^k \in C_n$ je primitivni n-ti korijen iz jedinice onda I samo onda ako su *n* i *k* relativno prosti. Primitivnih korijena ima $\varphi(n)$, gdje je $\varphi(n)$ Eulerova funkcija.
b) Neka je *n* prost broj. Svi elementi iz C_n koji su $\neq 1$ su primitivni korijeni.

Element $k \in Z_n$ je generator aditivne grupe Z_n onda i samo onda ako su *k* i *n* relativno prosti. Ako je *n* prost broj, onda je svaki njegov element koji je $\neq 1$, ujedno i generator grupe Z_n.
Primjer:
Vrijedi $\varphi(20)=8$ jer su brojevi k = 1,3,7,9,11,13,17,19 manji od 20 i relativno prosti sa 20. Ti brojevi su generatori grupe Z_{20}, a isto tako ε^k su primitivni korijeni iz jedinice u grupi C_{20}, $\varepsilon = \cos(2\pi/n)+ i\sin(2\pi/n)$.

11. Primjeri konačnih i beskonačnih cikličkih grupa.

Primjeri konačnih cikličkih grupa:
a) $<e> = (\{e\},+)$
b) $<-1> = (\{-1,1\},\cdot)$

Primjer beskonačnih cikličkih grupa:
a) $<1> = (Z,+)$

To je valjda to, nisam siguran.

12. Simetrična grupa. Dokaz svojstava grupe za S_2.

Neka je zadan neki konačan skup od n elemenata $S = \{a_1,a_2, \dots , a_n\}$.
Svaka bijekcija skupa S na samog sebe $f:S\rightarrow S$ naziva se **permutacija**. Skup svih permutacija (svih bijekcija skupa S na samog sebe) označava se sa S_n. Ako uvedemo uobičajenu operaciju $\circ$ (kompozicija funkcija), tada imamo strukturu $(S_n, \circ)$. Može se pokazati da je ta struktura grupa i naziva se grupa permutacija ili **simetrična grupa**. Ova grupa ima red n! ili n! elemenata:
$k(S_n) = n!$
U toj grupi je e = i, tj, neutralni element je identična funkcija (ili identiteta).
$f\circ i = i\circ f = f$

Svojstva i dokazi???

13. Morfizmi grupe. Cayleyev teorem.

Neka su $(G,\cdot)$ i $(H,\cdot)$ dvije grupe. Preslikavanje $f : G \rightarrow H$ zove se **homomorfizam grupa** ako za sve $a,b \in G$ vrijedi:

$$f(ab)=f(a)f(b)$$

Ako je $f : G \rightarrow H$ homomorfizam grupa, onda je:

a) f(e) = e
b) $f(a)^{-1} = f(a^{-1})$
Homomorfizam f : X → Y dviju grupa X i Y zovemo **izomorfizam** ako je f bijekcija. Kažemo da su grupe X i Y **izomorfne** i pišemo $X \cong Y$.
Grupe G i H koje su međusobno izomorfne možemo smatrati "jednakima". Poistovjećivanje vrši upravo funkcija f:
a) G i H imaju isti kardinalni broj (f je bijekcija)
b) množenje u grupama G i H vrši se na potpuno isti način, dotično umnošku *ab* u grupi G će odgovarati upravo umnožak f(a)f(b) u grupi H.
Ako su dvije konačne grupe G i H izomorfne, onda su pripadne Cayleyeve tablice množenja "iste". Točnije, umnošku *ab* u tablici množenja grupe G će odgovarati upravo umnožak f(a)f(b) u tablici množenja grupe H.
Ako je f : G → H surjektivni homomorfizam grupa, onda kažemo da je f **epimorfizam**. Injektivni homomorfizam zove se **monomorfizam**.
Ako je G=H (grupe su (G,*) i (H,○)), tada kažemo da su grupe (G,*) i (G,○) **automorfne** (izomorfizam na samoga sebe se zove automorfizam).
Cayleyev teorem:
Može se pokazati da je svaka konačna grupa (G,*), k(G)=n izomorfna jednoj grupi permutacija skupa n elemenata. (G,*) je izomorfno sa $(S_n, \circ)$.

14. Definicija prstena i podprstena.

Grupa (S,*, ○) (znači, ima 2 operacije koje zovemo zbrajanje i množenje elemenata prstena) se naziva prsten ako vrijedi:
a) (S,*) je Abelova grupa
b) (S \ {e} ,○) je polugrupa (○ je asocijativno)
c) vrijede oba zakona distributivnosti (npr. za (R,+,·) vrijedi a(b+c)=ab+ac i (a+b)c=ac+bc)

Primjer:
(Z,+,·)
(Z,+) je Abelova grupa
(Z \ {0}, ·) je polugrupa

a) Ako se u definiciji prstena pod b) traži da struktura (S\{e},○) bude monoid, tu strukturu nazivamo prsten s jedinicom.
b) Ako se u definiciji prstena pod b) traži da je struktura (S\{e},○) grupa, tada se nova struktura naziva tijelo.
c) Ako se u definicij prstena pod b) traži da je struktura (S\{e},○) komutativna polugrupa, tada kažemo da je struktura komutativni prsten.
d) Ako se u definiciji prstena pod b) traži da je struktura (S\{e},○) komutativna grupa, tada se struktura naziva komutatuivno tijelo ili polje.

Ako je jasno koje su operacije na prstenu definirane, govorimo samo o prstenu S. Isto tako kažemo da je R **potprsten** prstena S ako je R podskup od S i R je prsten s operacijama naslijeđenim iz S. Svaki prsten S ima dva trivijalna potprstena: {0} i S. Ako prsten sadrži jedinični element e s obzirom na množenje(tj. za sve a iz R je e·a=a·e=e), onda ga zovemo **prstenom s jedinicom**.

15. Primjeri konačniih i beskonačnih prstena.

Primjer konačnog prstena: Ako je *n* pozitivan cijeli broj, onda skup $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ cijelih brojeva modulo *n* (koji je kao aditivna grupa ciklička grupa reda *n*) tvori prsten s *n* elemenata.
Primjer beskonacnog: ???

16. Dokažite da je skup svih polinoma R[x] s koeficijentina nad poljem R i uobičajenim operacijama + i • jedan prsten. Pojam iredicibilnog polinoma.

Neka je R komutativan prste s jedinicom i $a_0, a_1, \ldots, a_n \in R$. Izraz:

$$f(x) = a_0+a_1x+\ldots+a_nx^n$$

zove se **formalni polinom** s koeficijentima iz prstena R, ili polinom nad R.
Ako u polinomu $f(x) = a_0+a_1x+\ldots+a_nx^n$ vrijedi $a_n \neq 0$, onda kažemo da je f(x) polinom n-tog stupnja i a_n je vodeći koeficijent polinoma. Skup svih formalnih polinoma s koeficijentima iz R označavamo sa R[x]. Za dva polinoma iz R[x] kažemo da su jednaki ako su im koeficijenti uz odgovarajuće potencije od x isti. Skup polinoma R[x] uvijek sadrži R kao svoj podskup.
Cilj nam je sada da R[x] organiziramo u prsten, tj. uvedemo operacije zbrajanja množenja polinoma. Dva polinoma iz R[x] zbrajamo tako da zbrojimo odgovarajuće koeficijente uz iste potencije od x. Ako je $f(x) = a_0+a_1x+\ldots+a_mx^m$ i $g(x) = b_0+b_1x+\ldots+b_nx^n$ onda definiramo:

$$f(x)+g(x) = \sum_{j=1}^{\max\{m,n\}} (a_j+b_j)x^j$$

gdje stavljamo $a_j=0$ ako je $j>m$ i $b_j=0$ za $j>n$.
Na sličan način definiramo i množenje polinoma:

$$f(x)g(x) = a_0b_0+(a_1b_0+a_0b_1)x+\ldots+a_mb_nx^{m+n}$$

Pri tome je koeficijent uz x^k jednak:

$$a_0b_k+a_1b_{k-1}+\ldots+a_kb_0 = \sum_{j=0}^{k} a_jb_{k-j}$$

Na ovako definirano zbrajanje i množenje polinoma, skup svih polinoma R[x] je prsten.

Neka je (F,+,·) bilo koje polje. Za dva polinoma f(x) i g(x) $\in$ F[x] kažemo da su **proporcionalni** nad F ako postoji konstanta $c \in F$, $c \neq 0$, takva da je $f(x)=c \cdot g(x)$.
Za polinom f(x) $\in$ F[x] koji je barem prvoga stupnja, kažemo da je **ireducibilan** (nerastavljiv) ako iz rastava f(x)=g(x)h(x) slijedi da je jedan od polinoma g(x), h(x) nultoga stupnja (tj. konstanta iz F). Dakle, drugi je onda proporcionalan sa f(x).

Ako polinom f(x) nije ireducibilan, kažemo da je **reducibilan**, tj. rastavljiv na produkt dvaju polinoma od kojih niji jedan nije konstantan.

17. Definicija tijela i polja. Primjeri konačnih i beskonačnih polja.

Grupa (S,*, ○) (znači, ima 2 operacije koje zovemo zbrajanje i množenje elemenata prstena) se naziva prsten ako vrijedi:
a) (S,*) je Abelova grupa
b) (S \ {e} ,○) je polugrupa (○ je asocijativno)
c) vrijede oba zakona distributivnosti (npr. za (R,+,·) vrijedi a(b+c)=ab+ac i (a+b)c=ac+bc)

Ako se u definiciji prstena pod b) traži da je struktura (S\{e},○) grupa, tada se nova struktura naziva **tijelo**.
Ako se u definiciji prstena pod b) traži da je struktura (S\{e},○) komutativna grupa, tada se struktura naziva komutatuivno tijelo ili **polje**.

Primjer konačnih polja:
Skup Z_n je polje onda i samo onda ako je *n* prost broj: Z_2={0,1}, Z_3, Z_5, Z_7, ... Sva ova polja su konačna.
Primjeri beskonačnih polja su Q, R, C, i mnoga druga.

Nadam se da se na to mislilo.

18. Primjeri ostalih algebarskih struktura

a) Booleova algebra

Bilo koji primjer, npr. A v B

b) Vektorski prostor

Vektorski ili linearni prostor je algebarski pojam u matematici koji nalazi primjenu u svim glavnim granama matematike, među kojima su linearna algebra, analiza i analitička geometrija. Definira se na sljedeći način: neka skup V ima strukturu Abelove grupe u odnosu na zbrajanje. Elemente skupa V zovemo vektori. Neutralni element označujemo sa 0 i zovemo nulti vektor. Neka skup F ima strukturu polja. Elemente skupa F zovemo skalari, a neutralne elemente u odnosu na dvije binarne operacije označujemo sa 0 i 1. Na skupu F × V definirano je množenje vektora skalarom, tj. preslikavanje F × V → V, koje svakom skalaru $\alpha \in F$ i svakom vektoru $x \in V$ pridružuje vektor $\alpha x \in V$, tako da vrijede sljedeći aksiomi:

(I) $\alpha(\beta x) = (\alpha\beta)x, \forall\alpha, \beta \in F, \forall x \in V$

(II) $\alpha(x + y) = \alpha x + \alpha y, \forall\alpha \in F, \forall x, y \in V$

(III) $(\alpha + \beta)x = \alpha x + \beta x, \forall\alpha, \beta \in F, \forall x \in V$

(IV) $1x = x, \forall x \in V$

Ovako se definisano preslikavanje zove množenje vektora skalarom, dok se V naziva vektorski prostor nad poljem F i piše V(F).

c) Petllja
d) Kvazigrupa

Generalizacija pojma grupe u kojoj se izostavlja svojstvo asocijativnosti naziva se petlja, a u još općenitijoj situaciji kada nema jedinice kvazigrupa.