Uređeni prsteni

Prekpaljaj, Teuta

Uređeni prsteni

Prekpaljaj, Teuta

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Teuta Prekpaljaj

UREĐENI PRSTENI

Diplomski rad

Voditelj rada:
izv.prof.dr.sc. Zvonko Iljazović

Zagreb, srpanj 2020.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Zahvaljujem svom mentoru, izv. prof. dr. sc. Zvonku Iljazoviću na izuzetnom trudu, vremenu i strpljenju koje je uložio u izradu ovog diplomskog rada, kao i na svemu što me naučio. Ovaj rad posvećujem svojoj obitelji koja me uvijek podržavala.

Sadržaj

Uvod

U ovom diplomskom radu ćemo proučavati uređene prstene. Neki osnovni pojmovi s kojima ćemo se upoznati su grupe, prsteni i prerezi te razne binarne operacije i relacije povezane s njima. Rad je podijeljen na tri poglavlja, prsteni i prerezi, pravi prerezi i dobri prerezi.

U prvom poglavlju ćemo definirati pojmove grupa, prsten, polje, uređaj na nekom skupu, uređeni prsten, potpolje, homomorfizam grupa i prerez. Dokazat ćemo, između ostalog, da je skup svih prereza u nekom uređenom skupu uz binarnu relaciju $\preceq$ potpuno uređen skup i navesti nekoliko primjera potpuno uređenih skupova. Na kraju poglavlja ćemo na skupu prereza definirati binarnu operaciju $\oplus$, tj. zbrajat ćemo prereze.

U drugom poglavlju ćemo definirati prave prereze, guste uređene grupe, Arhimedove grupe kao i binarne operacije i relacije vezane uz njih. Definirat ćemo i množenje prereza, nakon što smo u prethodnom poglavlju definirali zbrajanje. Dokazat ćemo i neka svojstva množenja prereza.

U trećem poglavlju ćemo definirati još jednu vrstu prereza, a to su dobri prerezi. Pokazat ćemo kako su povezani dobri i pravi prerezi. Na kraju ćemo definirati zbrajanje i množenje dobrih prereza.

Poglavlje 1

Prsteni i prerezi

1.1 Prsteni

Definicija 1.1.1. *Neka je G skup. Za svaku funkciju $G \times G \to G$ kažemo da je binarna operacija na G. Ako je $\cdot$ binarna operacija na G (dakle, $\cdot : G \times G \to G$), onda ćemo za $a, b \in G$ umjesto $\cdot(a, b)$ pisati $a \cdot b$.*

Definicija 1.1.2. *Za binarnu operaciju $\cdot$ na skupu G kažemo da je asocijativna ako za sve $a, b, c \in G$ vrijedi $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*

Ako je $\cdot$ asocijativna binarna operacija na skupu G onda za uređeni par $(G, \cdot)$ kažemo da je polugrupa.

Definicija 1.1.3. *Neka je $\cdot$ binarna operacija na skupu G te neka je $e \in G$. Pretpostavimo da je $e \cdot x = x$ i $x \cdot e = x$ za svaki $x \in G$. Tada za e kažemo da je neutralan element za operaciju $\cdot$.*

Propozicija 1.1.4. *Pretpostavimo da je $\cdot$ binarna operacija na G te da su e i f neutralni elementi za operaciju $\cdot$. Tada je $e = f$.*

Dokaz. Budući da je e neutralni element, za svaki $x \in G$ vrijedi $e \cdot x = x$. Posebno, za $x = f$ vrijedi

$$e \cdot f = f. \tag{1}$$

Budući da je f neutralni element, za svaki $x \in G$ vrijedi $x \cdot f = x$, pa posebno za $x = e$ dobivamo

$$e \cdot f = e. \tag{2}$$

Iz (1) i (2) slijedi tvrdnja propozicije. □

Definicija 1.1.5. *Neka je $(G, \cdot)$ polugrupa takva da postoji neutralni element za operaciju $\cdot$. Tada za $(G, \cdot)$ kažemo da je monoid. Ako je e neutralni element za operaciju $\cdot$ onda za e kažemo da je neutralni element u monoidu $(G, \cdot)$.*

Definicija 1.1.6. *Neka je $(G, \cdot)$ monoid. Neka je e neutralni element u $(G, \cdot)$. Neka su $x, y \in G$ takvi da je $x \cdot y = e$ i $y \cdot x = e$. Tada za y kažemo da je inverzni element od x u $(G, \cdot)$.*

Propozicija 1.1.7. *Neka je $(G, \cdot)$ monoid te neka je $x \in G$. Pretpostavimo da su $y, z \in G$ inverzni elementi od x u $(G, \cdot)$. Tada je $y = z$.*

Dokaz. Imamo $x \cdot y = e$, pri čemu je e neutralni element u $(G, \cdot)$. Slijedi $(y \cdot x) \cdot z = e \cdot z$ pa je $y \cdot (x \cdot z) = z$, tj. $y \cdot e = z$. Dakle, $y = z$. □

Ako je $(G, \cdot)$ monoid i $x \in G$ takav da x ima inverzni element, onda taj inverzni element (koji je jedinstven prema prethodnoj propoziciji) obično označavamo sa x^{-1}.
Dakle, $x \cdot x^{-1} = e$ i $x^{-1} \cdot x = e$ pri čemu je e neutralni element u $(G, \cdot)$.

Definicija 1.1.8. *Za binarnu operaciju $\cdot$ na skupu G kažemo da je komutativna ako za sve $a, b \in G$ vrijedi $a \cdot b = b \cdot a$.*

Definicija 1.1.9. *Neka je $(G, \cdot)$ monoid takav da svaki $x \in G$ ima inverzni element u $(G, \cdot)$. Tada za $(G, \cdot)$ kažemo da je grupa.*

Ako je $(G, \cdot)$ grupa takva da je binarna operacija $\cdot$ komutativna onda za $(G, \cdot)$ kažemo da je komutativna ili Abelova grupa.
Ako koristimo oznaku $+$ za binarnu operaciju na skupu G, pri čemu je $(G, +)$ Abelova grupa, onda neutralni element u $(G, +)$ obično označavamo sa 0, a za $x \in G$ inverzni element od x u $(G, +)$ označavamo sa $-x$. Dakle, ako je $(G, +)$ Abelova grupa onda za svaki $x \in G$ vrijedi $x + (-x) = 0$ i $(-x) + x = 0$.

Definicija 1.1.10. *Neka je P skup te neka su $+$ i $\cdot$ binarne operacije na P sa sljedećim svojstvima:*

1. *$(P, +)$ je Abelova grupa*
2. *$(P, \cdot)$ je polugrupa*
3. *Za sve $x, y, z \in P$ vrijedi*
   $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
   $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$ (distributivnost operacije $\cdot$ prema $+$)

Tada za uređenu trojku $(P, +, \cdot)$ kažemo da je prsten.

Definicija 1.1.11. *Neka je $(P, +, \cdot)$ prsten takav da je binarna operacija $\cdot$ komutativna. Tada za $(P, +, \cdot)$ kažemo da je komutativan prsten.*

Definicija 1.1.12. *Neka je $(P, +, \cdot)$ prsten takav da binarna operacija $\cdot$ ima neutralni element. Tada za $(P, +, \cdot)$ kažemo da je prsten s jedinicom.*

Ako je $(P, +, \cdot)$ prsten s jedinicom onda neutralni element za operaciju $\cdot$ obično označavamo s 1.

Napomena 1.1.13. *Ako je $(P, +, \cdot)$ prsten onda ćemo neutralni element za operaciju $+$, u skladu sa ranijim dogovorom označiti s 0.*

Propozicija 1.1.14. *Neka je $(P, +, \cdot)$ prsten. Neka je $x \in P$. Tada je $x \cdot 0 = 0$ i $0 \cdot x = 0$.*

Dokaz. Imamo $0 \cdot x = (0 + 0) \cdot x = (0 \cdot x) + (0 \cdot x)$. Definiramo $z = 0 \cdot x$. Dobili smo da je $z = z + z$. Slijedi $z + (-z) = (z + z) + (-z)$, tj. $0 = z + (z + (-z))$ pa je $0 = z$. Dakle, $0 \cdot x = 0$. Analogno dobijemo da je $x \cdot 0 = 0$. □

Definicija 1.1.15. *Neka je $(P, +, \cdot)$ komutativan prsten s jedinicom takav da P ima bar dva elementa. Pretpostavimo da za svaki $x \in P$ takav da je $x \neq 0$ vrijedi da x ima inverzni element u monoidu $(P, \cdot)$. Tada za $(P, +, \cdot)$ kažemo da je polje.*

Napomena 1.1.16. *Ako je $(P, +, \cdot)$ prsten onda ćemo u pisanju kao i inače smatrati da operacija $\cdot$ "ima veći prioritet" od operacije $+$. Tako npr. za $x, y, z \in P$, $z + x \cdot y$ zapravo znači $z + (x \cdot y)$.*

Propozicija 1.1.17. *Neka je $(P, +, \cdot)$ prsten te neka su $x, y \in P$. Tada vrijedi*

1. $x \cdot (-y) = -(x \cdot y)$
2. $(-x) \cdot y = -(x \cdot y)$
3. $(-x) \cdot (-y) = x \cdot y$

Dokaz.

1. Koristeći propoziciju 1.1.14 dobivamo $x \cdot (-y) + x \cdot y = x \cdot ((-y) + y) = x \cdot 0 = 0$, dakle, $x \cdot (-y) + x \cdot y = 0$ pa je, po definiciji, $x \cdot (-y)$ inverzni element od $x \cdot y$ u $(P, +)$. Dakle, $x \cdot (-y) = -(x \cdot y)$.

2. Ovu tvrdnju dokazujemo analogno.

3. Za svaki $a \in P$ vrijedi $-(-a) = a$ (po definiciji inverznog elementa u monoidu). Koristeći tvrdnje 1. i 2. dobivamo
   $(-x) \cdot (-y) = -((-x) \cdot y) = -(-(x \cdot y)) = x \cdot y$.
   Dakle, tvrdnja 3. vrijedi.

□

Definicija 1.1.18. *Neka je $(P, +, \cdot)$ prsten. Za $x, y \in P$ definiramo $x - y = x + (-y)$.*

Propozicija 1.1.19. *Neka je $(P, +, \cdot)$ prsten te neka su $x, y, z \in P$. Tada vrijedi:*

1. $x \cdot (y - z) = x \cdot y - x \cdot z$
2. $(x - y) \cdot z = x \cdot z - y \cdot z$.

Dokaz. 1. Koristeći prethodnu propoziciju dobivamo:
$x \cdot (y - z) = x \cdot (y + (-z)) = x \cdot y + x \cdot (-z) = x \cdot y + (-(x \cdot z)) = x \cdot y - x \cdot z$. Dakle, jednakost 1. vrijedi.

2. Analogno dokazujemo tvrdnju 2.

□

1.2 Uređeni prsteni

Definicija 1.2.1. *Neka je S skup. Svaki podskup od $S \times S$ nazivamo binarna relacija na skupu S.*

Ako je ρ binarna relacija na skupu S (dakle, $\rho \subseteq S \times S$) onda za $x, y \in S$ takve da je $(x, y) \in \rho$ pišemo $x\rho y$.

Definicija 1.2.2. *Za binarnu relaciju ρ na skupu S kažemo da je refleksivna ako za svaki $x \in S$ vrijedi $x\rho x$.*
Za binarnu relaciju ρ na skupu S kažemo da je antisimetrična ako za sve $x, y \in S$ takve da je $x\rho y$ i $y\rho x$ vrijedi $x = y$.
Za binarnu relaciju ρ na skupu S kažemo da je tranzitivna ako za sve $x, y, z \in S$ takve da je $x\rho y$ i $y\rho z$ vrijedi $x\rho z$.

Definicija 1.2.3. *Neka je ρ binarna relacija na skupu S. Pretpostavimo da je ρ refleksivna, antisimetrična i tranzitivna relacija te da za sve $x, y \in S$ vrijedi $x\rho y$ ili $y\rho x$. Tada za ρ kažemo da je uređaj na skupu S.*

Definicija 1.2.4. *Ako je $\leq$ uređaj na skupu S, onda za $(S, \leq)$ kažemo da je uređen skup.*

Definicija 1.2.5. *Neka je $(S, \leq)$ uređen skup. Pretpostavimo da za sve $A, B \subseteq S$, $A \neq \emptyset$, $B \neq \emptyset$, takve da je $a \leq b$, $\forall a \in A$, $\forall b \in B$, postoji $c \in S$ takav da je $a \leq c$, $\forall a \in A$ i $c \leq b$, $\forall b \in B$. Tada za $(S, \leq)$ kažemo da je potpuno uređen skup.*

Primjer 1.2.6. *Neka je $\leq$ standardni uređaj na $\mathbb{N}$. Tada je $(\mathbb{N}, \leq)$ uređen skup. Tvrdimo da je $(\mathbb{N}, \leq)$ potpuno uređen skup. Neka su $A, B \subseteq \mathbb{N}$, $A \neq \emptyset$, $B \neq \emptyset$ takvi da je $a \leq b$, $\forall a \in A$, $\forall b \in B$. Budući da svaki neprazan podskup od $\mathbb{N}$ ima najmanji element, postoji $c \in B$ takav da je $c \leq b$, $\forall b \in B$. Nadalje, zbog $c \in B$, vrijedi $a \leq c$, $\forall a \in A$.*
Zaključak: $(\mathbb{N}, \leq)$ je potpuno uređen skup.

Primjer 1.2.7. *Neka je $\leq$ standardni uređaj na $\mathbb{Z}$. Tvrdimo da je $(\mathbb{Z}, \leq)$ potpuno uređen skup. Neka su $A, B \subseteq \mathbb{Z}$, $A \neq \emptyset$, $B \neq \emptyset$ takvi da je $a \leq b$, $\forall a \in A$, $\forall b \in B$. Odaberimo $a_0 \in A$. Slijedi $a_0 \leq b$, $\forall b \in B$, što povlači da je*

$$b - a_0 + 1 \geq 1, \tag{1}$$

za svaki $b \in B$. Definirajmo $B' = \{b - a_0 + 1 \mid b \in B\}$. Očito je $B' \subseteq \mathbb{Z}$, a iz $(*)$ slijedi da je $B' \subseteq \mathbb{N}$. Stoga B' ima najmanji element, označimo ga s c'. Iz $c' \in B'$ slijedi da postoji $c \in B$ takav da je $c' = c - a_0 + 1$. Neka je $b \in B$. Imamo $b - a_0 + 1 \in B'$ pa je $c' \leq b - a_0 + 1$, tj. $c - \cancel{a_0 + 1} \leq b - \cancel{a_0 + 1}$. Slijedi $c \leq b$, $\forall b \in B$. Zbog $c \in B$ vrijedi $a \leq c$, $\forall a \in A$.
Zaključak: $(\mathbb{Z}, \leq)$ je potpuno uređen skup.

Primjer 1.2.8. *Neka je $\leq$ standardni uređaj na $\mathbb{Q}$. Tada $(\mathbb{Q}, \leq)$ nije potpuno uređen skup. Naime, promotrimo skupove $A = \{x \in \mathbb{Q} \mid x < \sqrt{2}\}$ i $B = \{x \in \mathbb{Q} \mid x > \sqrt{2}\}$. Za svaki $a \in A$ i za svaki $b \in B$ očito vrijedi $a < b$. Pretpostavimo da postoji $c \in \mathbb{Q}$ takav da je*

$$a \leq c, \tag{1}$$

za svaki $a \in A$ i

$$c \leq b, \tag{2}$$

za svaki $b \in B$. Budući da je $c \in \mathbb{Q}$ vrijedi $c \neq \sqrt{2}$ pa imamo dva slučaja:

1. *slučaj: $c < \sqrt{2}$*
   Odaberimo $x \in \mathbb{Q}$ takav da je
   $$c < x < \sqrt{2}. \tag{3}$$
   Slijedi da je $x \in A$ pa prema (1) *vrijedi $x \leq c$. Ovo je u kontradikciji s* (3).

2. *slučaj: $\sqrt{2} < c$*
   Odaberimo $x \in \mathbb{Q}$ takav da je
   $$\sqrt{2} < x < c. \tag{4}$$
   Slijedi da je $x \in B$ pa prema (2) *vrijedi $c \leq x$. To je u kontradikciji s* (4).

Oba slučaja vode u kontradikciju pa zaključujemo da ne postoji $c \in \mathbb{Q}$ takav da je $a \leq c$, $\forall a \in A$ i $c \leq b$, $\forall b \in B$. Prema tome $(\mathbb{Q}, \leq)$ nije potpuno uređen skup.

Definicija 1.2.9. *Neka je $(P, +, \cdot)$ prsten te neka je $\leq$ uređaj na P. Pretpostavimo da vrijedi sljedeće:*

1. *Ako su $x, y \in P$ takvi da je $x \leq y$, onda za svaki $z \in P$ vrijedi $x + z \leq y + z$.*
2. *Ako su $x, y \in P$ takvi da je $0 \leq x$ i $0 \leq y$, onda je $0 \leq x \cdot y$.*

Tada za $(P, +, \cdot, \leq)$ kažemo da je uređeni prsten.

Neka je $\leq$ uređaj na skupu S. Za $x, y \in S$ pišemo $x < y$ ako je $x \leq y$ i $x \neq y$.

Napomena 1.2.10. *Neka je $(S, \leq)$ uređen skup. Ako su $x, y \in S$ takvi da ne vrijedi $x \leq y$, onda pišemo $x \not\leq y$. Ako su $x, y \in S$ takvi da ne vrijedi $x < y$, onda pišemo $x \not< y$.*

Propozicija 1.2.11. *Neka je $(S, \leq)$ uređen skup. Neka su $x, y, z \in S$. Tada vrijede sljedeće tvrdnje:*

1. $x \not< x$,
2. $x \leq y \ i \ y < z \Rightarrow x < z$,
3. $x < y \ i \ y \leq z \Rightarrow x < z$,
4. $x < y \ i \ y < z \Rightarrow x < z$,
5. $x \not\leq y \Leftrightarrow y < x$
6. $y \not< x \Leftrightarrow x \leq y$.

Dokaz. 1. Očito vrijedi.

2. Pretpostavimo da je $x \leq y$ i $y < z$. Iz $y < z$ slijedi $y \leq z$, a ovo zajedno s $x \leq y$ daje $x \leq z$. Dokazujemo da je $x \neq z$. Pretpostavimo suprotno, tj. da je $x = z$. Tada polazne pretpostavke možemo zapisati ovako: $x \leq y$ i $y < x$. Posebno, $y \leq x$ pa antisimetričnost relacije $\leq$ daje $x = y$. No, to je u kontradikciji s $y < x$. Prema tome, $x \neq z$, dakle, $x < z$.

3. Ovu tvrdnju dokazujemo analogno.

4. Ova tvrdnja slijedi iz 2. i 3.

5. $\Rightarrow$ Pretpostavimo da $x \not\leq y$. Iz definicije uređaja slijedi da je $x \leq y$ ili $y \leq x$. Dakle, mora vrijediti da je $y \leq x$. Kada bi vrijedilo $y = x$ onda bismo imali $x \leq y$ što je nemoguće zbog $x \not\leq y$. Prema tome, $y \neq x$ pa zaključujemo da je $y < x$.
   $\Leftarrow$ Pretpostavimo sada da je $y < x$. Kada bi vrijedilo $x \leq y$, onda bi tvrdnja 2. povlačila da je $x < x$ što je nemoguće prema tvrdnji 1. Dakle, $x \not\leq y$. Time je tvrdnja 5. dokazana.

6. Ova tvrdnja slijedi iz tvrdnje 5.

□

Definicija 1.2.12. *Neka su* $(P, +', \cdot')$ *i* $(R, +, \cdot)$ *polja. Kažemo da je* $(P, +', \cdot')$ *potpolje od* $(R, +, \cdot)$ *ako je* $P \subseteq R$ *te ako za sve* $x, y \in P$ *vrijedi* $x +' y = x + y$ *i* $x \cdot' y = x \cdot y$.

Propozicija 1.2.13. *Neka je* $(P, +', \cdot')$ *potpolje od* $(R, +, \cdot)$. *Neka je* $0'$ *neutralni element za* $+'$ *te neka je* $1'$ *neutralni element za operaciju* $\cdot'$. *Vrijedi sljedeće:*

1. *0'=0. Nadalje, ako je* $x \in P$ *onda je inverzni element od x u monoidu* $(P, +')$ *jednak inverznom elementu od x u monoidu* $(R, +)$.

2. *1'=1. Nadalje, ako je* $x \in P$, $x \neq 0$, *onda je inverzni element od x u monoidu* $(P, \cdot')$ *jednak inverznom elementu od x u monoidu* $(R, \cdot)$.

Dokaz. 1. Odaberimo bilo koji $a \in P$. Imamo $a +' 0' = a$, tj. $a + 0' = a$. Neka je b inverzni element od a u $(R, +)$. Slijedi $b + (a + 0') = b + a$, tj. $(b + a) + 0' = 0$, dakle, $0 + 0' = 0$, pa je $0' = 0$. Neka je $x \in P$. Neka je y inverzni element od x u $(P, +')$. Tada vrijedi $x +' y = 0'$, tj. $x + y = 0$. Zbog komutativnosti operacije + vrijedi i $y + x = 0$, što znači da je y inverzni element od x u $(R, +)$.

2. Odaberimo neki $a \in P$, $a \neq 0$. Imamo $a \cdot' 1' = a$, tj. $a \cdot 1' = a$. Neka je b inverz od a u $(R, \cdot)$. Slijedi $b \cdot (a \cdot 1') = b \cdot a$ pa dobivamo da je $1' = 1$. Neka je $x \in P$, $x \neq 0$. Neka je y inverzni element od x u $(P, +')$. Tada vrijedi $x \cdot' y = 1'$, tj. $x \cdot y = 1$. Iz ovoga zaključujemo da je y inverzni element od x u $(R, \cdot)$.

□

Propozicija 1.2.14. *Neka je* $(R, +, \cdot)$ *polje te neka je* $P \subseteq R$ *takav da ima bar dva elementa. Tada postoje +' i* $\cdot'$ *takvi da je* $(P, +', \cdot')$ *potpolje od* $(R, +, \cdot)$ *ako i samo ako vrijedi sljedeće:*

1. $x - y \in P, \forall x, y \in P,$

2. $x \cdot y \in P, \forall x, y \in P,$

3. $x^{-1} \in P, \forall x \in P, x \neq 0.$

Dokaz. Pretpostavimo da postoje $+'$ i $\cdot'$ takve da je $(P, +', \cdot')$ potpolje od $(R, +, \cdot)$. Neka su $x, y \in P$. Imamo $x \cdot y = \text{x} \cdot' \text{y}$ pa je očito da je $x \cdot y \in P$. Isto tako, očito je $x + y \in P$. Iz $y \in P$ i prethodne propozicije (tvrdnja 1.) slijedi da je $-y \in P$. Stoga je $x + (-y) \in P$, tj. $x - y \in P$.

Neka je $x \in P$, $x \neq 0$. Iz prethodne propozicije (tvrdnja 2.) slijedi da je $x^{-1} \in P$. Obratno, pretpostavimo da vrijede svojstva 1., 2. i 3. Dokažimo da postoje $+'$ i $\cdot'$ takve da je $(P, +', \cdot')$ potpolje od $(R, +, \cdot)$. Odaberimo $a \in P$. Prema tvrdnji 1. vrijedi $a - a \in P$, tj.

$0 \in P$. Neka je $x \in P$. Imamo $0, x \in P$ pa iz tvrdnje 1. slijedi $0 - x \in P$, tj. $-x \in P$. Neka su $x, y \in P$. Slijedi $x, -y \in P$ pa prema tvrdnji 1. imamo $x - (-y) \in P$, tj. $x + y \in P$.

Definiramo binarne operacije $+'$ i $\cdot'$ na P sa $x +' y = x + y$ i $x \cdot' y = x \cdot y$, za sve $x, y \in P$. Tvrdimo da je $(P, +', \cdot')$ potpolje od $(R, +, \cdot)$. Dovoljno je provjeriti da je $(P, +', \cdot')$ polje.

Neka su $x, y, z \in P$. Vrijedi $(x +' y) +' z = x +' (y +' z)$ jer je $(x +' y) +' z = (x + y) + z$, $x +' (y +' z) = x + (y + z)$, a operacija $+$ je asocijativna. Znamo da je $0 \in P$. Za svaki $x \in P$ vrijedi $x +' 0 = x + 0 = x$. Stoga je 0 neutralni element za operaciju $+'$.

Neka je $x \in P$. Znamo da je $-x \in P$. Imamo $x +' (-x) = x + (-x) = 0$. Zaključujemo da je $(P, +')$ grupa. Operacija $+'$ je komutativna jer je operacija $+$ komutativna. Prema tome, $(P, +')$ je Abelova grupa.

Operacija $\cdot'$ je asocijativna jer je operacija $\cdot$ asocijativna. Svojstva distributivnosti množenja u odnosu na zbrajanje za operacije $+'$ i $\cdot'$ slijede iz činjenice da operacije $+$ i $\cdot$ imaju ta svojstva. Prema tome, $(P, +', \cdot')$ je prsten. Komutativnost operacije $\cdot$ povlači komutativnost operacije $\cdot'$. Stoga je $(P, +', \cdot')$ komutativni prsten.

Budući da P ima bar dva elementa, postoji $a \in P$ takav da je $a \neq 0$. Iz tvrdnje 3. slijedi da je $a^{-1} \in P$ pa iz tvrdnje 2. slijedi da je $a \cdot a^{-1} \in P$, tj. $1 \in P$. Sada je očito da je 1 neutralni element za operaciju $\cdot'$. Stoga je $(P, +', \cdot')$ komutativni prsten s jedinicom.

Neka je $x \in P$, $x \neq 0$. Prema tvrdnji 3. vrijedi $x^{-1} \in P$ pa imamo $x \cdot' x^{-1} = x \cdot x^{-1} = 1$. Dakle, svaki element od P različit od 0 ima inverzni element u monoidu $(P, \cdot')$. Stoga je $(P, +', \cdot')$ polje.

Time je tvrdnja propozicije dokazana. □

Definicija 1.2.15. *Neka su $(G, \cdot)$ i $(H, *)$ grupe. Za funkciju $f : G \to H$ kažemo da je homomorfizam ako vrijedi $f(x \cdot y) = f(x) * f(y)$, $\forall x, y \in G$.*

Propozicija 1.2.16. *Neka su $(G, \cdot)$ i $(H, *)$ grupe. Neka je e_G neutralni element u grupi $(G, \cdot)$ te neka je e_H neutralni element u grupi $(H, *)$. Neka je $f : G \to H$ homomorfizam ovih grupa. Tada je $f(e_g) = e_H$.*

Dokaz. Odaberimo neki $x \in G$. Označimo $y = f(x)$. Imamo $y = f(x) = f(x \cdot e_G) = f(x) * f(e_G) = y * f(e_G)$. Dakle, $y = y * f(e_G)$. Neka je y^{-1} inverzni element od y u $(H, *)$. Iz prethodne jednakosti slijedi da je $y^{-1} * y = y^{-1} * (y * f(e_G))$ pa je $e_H = f(e_G)$. □

1.3 Prerezi

Definicija 1.3.1. *Neka je $(S, \leq)$ uređen skup. Neka su $A, B \subseteq S$, $A \neq 0$, $B \neq 0$ takvi da je $A \cap B = \emptyset$, $A \cup B = S$ te takvi da je $x \leq y$, $\forall x \in A$, $\forall y \in B$. Tada za uređeni par (A,B) kažemo da je prerez u $(S, \leq)$.*
Skup svih prereza u $(S, \leq)$ označavamo s $\Omega(S, \leq)$.

Na skupu $\Omega(S, \leq)$ *definiramo binarnu relaciju* $\preceq$ *na sljedeći način:*

$$(A, B) \preceq (C, D) \Leftrightarrow A \subseteq C.$$

Propozicija 1.3.2. *Neka je* $(S, \leq)$ *uređeni skup. Tada je* $(\Omega(S, \leq), \preceq)$ *uređeni skup.*

Dokaz. Dakle, treba dokazati da je $\preceq$ uređaj na skupu $\Omega(S, \leq)$. Očito je $\preceq$ refleksivna relacija na $\Omega(S, \leq)$. Pretpostavimo da su $(A, B), (C, D) \in \Omega(S, \leq)$ takvi da je $(A, B) \preceq (C, D)$ i $(C, D) \preceq (A, B)$. Tada je $A \subseteq C$ i $C \subseteq A$. Stoga je $A = C$. Iz definicije prereza je očito da je $B = S \setminus A$ i $D = S \setminus C$. Stoga je $B = D$. Dakle, $(A, B) = (C, D)$ pa zaključujemo da je relacija $\preceq$ antisimetrična. Lako zaključujemo da je relacija $\preceq$ tranzitivna.

Neka su $(A, B), (C, D) \in \Omega(S, \leq)$. Ako je $A \subseteq C$ onda je $(A, B) \preceq (C, D)$. Pretpostavimo da $A \not\subseteq C$. Tada postoji $a_0 \in A$ takav da $a_0 \notin C$. Budući da je $C \cup D = S$ zaključujemo da je $a_0 \in D$. Dokažimo da je $C \subseteq A$.

Neka je $c \in C$. Iz $a_0 \in D$ i definicije prereza slijedi da je $c \leq a_0$. Pretpostavimo da $c \notin A$. Tada je $c \in B$. Iz $a_0 \in A$ i $c \in B$ te definicije prereza slijedi $a_0 \leq c$. Ovo, zajedno s $c \leq a_0$ daje $c = a_0$. No ovo je nemoguće jer je $c \in B$, $a_0 \in A$ i $A \cap B = \emptyset$. Zaključak: $c \in A$. Dakle, dokazali smo da za svaki $c \in C$ vrijedi $c \in A$, prema tome imamo $C \subseteq A$ pa je $(C, D) \preceq (A, B)$.

Zaključak: $\preceq$ je uređaj na $\Omega(S, \leq)$. □

Teorem 1.3.3. *Neka je* $(S, \leq)$ *uređen skup. Tada je* $(\Omega(S, \leq), \preceq)$ *potpuno uređen skup.*

Dokaz. Prema prethodnoj propoziciji, $(\Omega(S, \leq), \preceq)$ je uređen skup. Pretpostavimo da su $X, Y \subseteq \Omega(S, \leq)$ takvi da je $X \neq \emptyset$, $Y \neq \emptyset$ te da za svaki $(A, B) \in X$ i svaki $(C, D) \in Y$ vrijedi $(A, B) \preceq (C, D)$. Neka je $\mathcal{A}$ unija svih $A \subseteq S$ za koje postoji $B \subseteq S$ takav da je $(A, B) \in X$ (uočimo da za takav B vrijedi $B = S \setminus A$). Dakle, $\mathcal{A} = \bigcup_{(A, S\setminus A) \in X} A$.

Tvrdimo da je $(\mathcal{A}, S \setminus \mathcal{A})$ prerez u $(S, \leq)$. Budući da je $X \neq \emptyset$, postoji $(A_0, B_0) \in X$. Iz definicije od $\mathcal{A}$ je očito da je $A_0 \subseteq \mathcal{A}$. Budući da je (A_0, B_0) prerez u $(S, \leq)$, imamo da je $A_0 \neq \emptyset$ pa slijedi da je $\mathcal{A} \neq \emptyset$. Budući da je $Y \neq \emptyset$, postoji $(C_0, D_0) \in Y$. Ako je $A \subseteq S$ takav da postoji $B \subseteq S$ sa svojstvom da je $(A, B) \in X$ onda je $(A, B) \preceq (C_0, D_0)$ što povlači da je $A \subseteq C_0$. Iz ovoga i definicije skupa $\mathcal{A}$ zaključujemo da je $\mathcal{A} \subseteq C_0$.

Budući da je (C_0, D_0) prerez u $(S, \leq)$, imamo da je $D_0 \neq \emptyset$ pa možemo odabrati neki $x \in D_0$. Slijedi da $x \notin C_0$, pa posebno $x \notin \mathcal{A}$. Dakle, $x \in S \setminus \mathcal{A}$. Stoga je $S \setminus \mathcal{A} \neq \emptyset$. Pretpostavimo da je $x \in \mathcal{A}$ te da je $y \in S \setminus \mathcal{A}$. Slijedi da postoji $A \subseteq S$ takav da je $x \in A$ te da je $(A, B) \in X$ za neki $B \subseteq S$. Uočimo da $y \notin A$ (jer bi inače vrijedilo $y \in \mathcal{A}$) pa budući da je (A, B) prerez u $(S, \leq)$ imamo da je $y \in B$. Stoga je $x \leq y$ (po definiciji prereza). Zaključak: $(\mathcal{A}, S \setminus \mathcal{A})$ je prerez u $(S, \leq)$, tj. $(\mathcal{A}, S \setminus \mathcal{A}) \in \Omega(S, \leq)$.

Neka je $(A, B) \in X$. Očito je $A \subseteq \mathcal{A}$ pa je $(A, B) \preceq (\mathcal{A}, S \setminus \mathcal{A})$. Uočimo da smo zapravo već dokazali sljedeću činjenicu: za svaki $(C_0, D_0) \in Y$ vrijedi $\mathcal{A} \subseteq C_0$. Dakle, za svaki $(C_0, D_0) \in Y$ vrijedi $(\mathcal{A}, S \setminus \mathcal{A}) \preceq (C_0, D_0)$.

Zaključak: Ako označimo $W = (\mathcal{A}, S \setminus \mathcal{A})$, onda imamo $W \in \Omega(S, \leq)$ te je $U \preceq W$, za svaki $U \in X$ i $W \preceq V$, za svaki $V \in Y$.

Time smo dokazali da je $(\Omega(S, \leq), \preceq)$ potpuno uređen skup. □

Definicija 1.3.4. *Neka su $(S, \leq)$ i $(T, \leq')$ uređeni skupovi. Za funkciju $f : S \to T$ kažemo da je rastuća (s obzirom na uređaje $\leq$ i $\leq'$) ako za sve $x, y \in S$ takve da je $x \leq y$ vrijedi $f(x) \leq' f(y)$.*

Propozicija 1.3.5. *Neka su $(S, \leq)$ i $(T, \leq')$ uređeni skupovi te neka je $f : S \to T$ funkcija. Tada je f rastuća injekcija ako i samo ako za sve $x, y \in S$ takve da je $x < y$ vrijedi $f(x) <' f(y)$.*

Dokaz. Pretpostavimo da je f rastuća injekcija. Neka su $x, y \in S$ takvi da je $x < y$. Tada je $x \leq y$ i $x \neq y$ pa iz činjenice da je f rastuća injekcija slijedi da je $f(x) \leq' f(y)$ i $f(x) \neq f(y)$. Stoga je $f(x) <' f(y)$.

Obratno, pretpostavimo da za sve $x, y \in S$ takve da je $x < y$ vrijedi $f(x) <' f(y)$. Neka su $x, y \in S$ takvi da je $x \leq y$. Ako je $x = y$ onda je $f(x) = f(y)$ pa je $f(x) \leq' f(y)$ (jer je $\leq'$ refleksivna relacija na T). Ako je $x \neq y$, onda imamo $x < y$ pa je $f(x) <' f(y)$ što povlači $f(x) \leq' f(y)$. Prema tome, funkcija f je rastuća.

Pretpostavimo da su $x, y \in S$ takvi da je $x \neq y$. Budući da je $\leq$ uređaj na S, vrijedi $x \leq y$ ili $y \leq x$. Iz $x \neq y$ slijedi $x < y$ ili $y < x$. Prema pretpostavci vrijedi $f(x) <' f(y)$ ili $f(y) <' f(x)$. U oba slučaja imamo da je $f(x) \neq f(y)$. Dakle, f je injekcija. □

Definicija 1.3.6. *Neka je $(S, \leq)$ uređen skup. Za $x_0 \in S$ kažemo da je najveći element u $(S, \leq)$ ako za svaki $x \in S$ vrijedi $x \leq x_o$.*

Propozicija 1.3.7. *Neka je $(S, \leq)$ uređen skup koji nema najvećeg elementa. Neka je $f : S \to \Omega(S, \leq)$ funkcija definirana s $f(x) = (\{y \in S \mid y \leq x\}, \{y \in S \mid x < y\})$. Tada je f rastuća injekcija s obzirom na $\leq$ i $\preceq$.*

Dokaz. Uočimo da je funkcija f dobro definirana. Naime, definiramo prije svega za $x \in S$ skupove $A_x = \{y \in S \mid y \leq x\}$ i $B_x = \{y \in S \mid x < y\}$. Očito je $A_x \cap B_x = \emptyset$ i $A_x \cup B_x = S$.

Neka su $y \in A_x$ i $y' \in B_x$. Tada je $y \leq x$ i $x < y'$ pa je $y < y'$, posebno $y \leq y'$. Vrijedi $x \in A_x$ pa je $A_x \neq \emptyset$. Kada bi vrijedilo $B_x = \emptyset$, onda bismo imali da je $A_x = S$ što bi značilo da je x najveći element u $(S, \leq)$, a to je nemoguće prema pretpostavci propozicije. Stoga je $B_x \neq \emptyset$. Zaključak: (A_x, B_x) je prerez u $(S, \leq)$, tj. $(A_x, B_x) \in \Omega(S, \leq)$. Prema tome, funkcija f je dobro definirana.

Neka su $x, y \in S$ takvi da je $x < y$. Dokažimo da je $f(x) <' f(y)$. Imamo $f(x) = (A_x, B_x)$ i $f(y) = (A_y, B_y)$. Neka je $z \in A_x$. Tada je $z \leq x$ pa zbog $x \leq y$ imamo $z \leq y$. Stoga je $z \in A_y$. Time smo dokazali da je $A_x \subseteq A_y$, a to povlači da je $f(x) \preceq f(y)$. Očito je $y \in A_y$, a imamo da $y \notin A_x$ (jer je $x < y$). Stoga je $A_x \neq A_y$. Prema tome, $f(x) \neq f(y)$. Dakle, $f(x) \prec f(y)$.

Dokazali smo sljedeće: Ako su $x, y \in S$ takvi da je $x < y$, onda je $f(x) \prec f(y)$. Iz prethodne propozicije slijedi da je f rastuća injekcija. □

Korolar 1.3.8. *Za svaki uređen skup $(S, \leq)$ koji nema najveći element postoji potpuno uređen skup $(T, \leq')$ i rastuća injekcija $f : S \to T$.*

Dokaz. Ovo slijedi iz prethodne propozicije i teorema. □

Definicija 1.3.9. *Neka je $(G, +)$ Abelova grupa te neka je $\leq$ uređaj na G takav da za sve $x, y, z \in G$ takve da je $x \leq y$ vrijedi $x + z \leq y + z$. Tada za $(G, +, \leq)$ kažemo da je uređena grupa.*

Napomena 1.3.10. *Ako je $(G, +, \leq)$ uređena grupa onda ćemo s 0 označavati neutralni element u $(G, +)$, a za $x \in G$ ćemo sa $-x$ označavati inverzni element od x u $(G, +)$.*

Definicija 1.3.11. *Za grupu $(G, +)$ kažemo da je trivijalna ako je G jednočlan skup.*
Za uređenu grupu $(G, +, \leq)$ kažemo da je trivijalna ako je grupa $(G, +)$ trivijalna.
Za prsten $(P, +, \cdot)$ kažemo da je trivijalan ako je P jednočlan skup.

Propozicija 1.3.12. *Neka je $(G, +, \leq)$ uređena grupa. Neka su $x, y \in G$ takvi da je $x < y$ te neka je $z \in G$. Tada je $x + z < y + z$.*

Dokaz. Iz $x < y$ slijedi $x \leq y$ i $x \neq y$. Iz $x \leq y$ i definicije uređene grupe slijedi $x+z \leq y+z$. Pretpostavimo da je $x + z = y + z$. Tada je $x + z + (-z) = (y + z) + (-z)$, tj. $x + (z + (-z)) = y + (z + (-z))$ pa je $x + 0 = y + 0$, tj. $x = y$. No ovo je nemoguće zbog $x < y$. Prema tome, $x + z \neq y + z$ i time smo dokazali da je $x + z < y + z$. □

Propozicija 1.3.13. *Neka je $(G, +, \leq)$ netrivijalna uređena grupa. Tada $(G, \leq)$ nema najveći element.*

Dokaz. Odaberimo $x \in G$ takav da je $x \neq 0$. Iz $x \leq 0$ ili $0 \leq x$ slijedi $x < 0$ ili $0 < x$. Ako je $x < 0$ onda iz prethodne propozicije slijedi $x + (-x) < 0 + (-x)$, tj. $0 < -x$. U svakom slučaju, postoji $\lambda \in G$ takav da je $0 < \lambda$. Pretpostavimo da $(G, \leq)$ ima najveći element, neka je to $x_0 \in G$. Iz $0 < \lambda$ i prethodne propozicije slijedi da je $x_0 < x_0 + \lambda$. Ovo je u kontradikciji s činjenicom da je x_0 najveći element u $(G, \leq)$. Time je tvrdnja propozicije dokazana. □

Propozicija 1.3.14. *Neka je $(S, \leq)$ uređeni skup te neka je $A \subseteq S$. Pretpostavimo da je $A \neq \emptyset$, $S \setminus A \neq \emptyset$ te da vrijedi sljedeće: ako su $x \in A$ i $y \in S$ takvi da je $y \leq x$, onda je $y \in A$. Tada je $(A, S \setminus A)$ prerez.*

Dokaz. Dovoljno je dokazati da za svaki $x \in A$ i svaki $y \in S \setminus A$ vrijedi $x \leq y$. Neka su $x \in A$ i $y \in S \setminus A$. Tada je $x \leq y$ ili $y \leq x$. No $y \leq x$ ne može vrijediti jer bi u suprotnom iz pretpostavke propozicije slijedilo $y \in A$, što je u kontradikciji s $y \in S \setminus A$. Prema tome, $x \leq y$. Zaključak: $(A, S \setminus A)$ je prerez. □

Propozicija 1.3.15. *Neka je $(S, \leq)$ uređeni skup te neka je (A, B) prerez u $(S, \leq)$. Pretpostavimo da su $x \in A$ i $y \in S$ takvi da je $y \leq x$. Tada je $y \in A$.*

Dokaz. Pretpostavimo suprotno. Tada je $y \in B$ pa iz definicije prereza slijedi da je $x \leq y$. Ovo, zajedno s $y \leq x$ daje $x = y$, što povlači da je $x \in A \cap B$. Dakle, $A \cap B \neq \emptyset$ što je u kontradikciji s činjenicom da je (A, B) prerez. Zaključak: $y \in A$. □

1.4 Zbrajanje prereza

Definicija 1.4.1. *Neka je $(G, +)$ Abelova grupa te neka su $A, C \subseteq G$. Definiramo $A + C = \{a + c \mid a \in A, c \in C\}$.*

Korolar 1.4.2. *Neka je $(G, +, \leq)$ uređena grupa te neka su $a, b, c, d \in G$ takvi da je $a < b$ i $c < d$. Tada je $a + c < b + d$.*

Dokaz. Iz $a < b$ i propozicije 1.3.12 slijedi $a + c < b + c$. Iz $c < d$ i propozicije 1.3.12 slijedi $b + c < b + d$. Iz 4. točke propozicije 1.1.19 slijedi $a + c < b + d$. □

Propozicija 1.4.3. *Neka je $(G, +, \leq)$ uređena grupa te neka su (A, B) i (C, D) prerezi u $(G, \leq)$. Tada je $(A + C, G\backslash(A + C))$ prerez u $(G, \leq)$.*

Dokaz. Iz $A \neq \emptyset$ i $C \neq \emptyset$ slijedi da je $A + C \neq \emptyset$. Odaberimo $b \in B$ i $d \in D$ (to možemo jer je $B \neq \emptyset$ i $D \neq \emptyset$). Neka su $a \in A$ i $c \in C$. Tada je $a < b$ i $c < d$ pa je prema prethodnom korolaru $a + c < b + d$. Dakle, za svaki $x \in A + C$ vrijedi $x < b + d$. Iz ovoga zaključujemo da $b + d \notin A + C$. Prema tome, $G\backslash(A + C) \neq \emptyset$.

Pretpostavimo da su $x \in A + C$ i $y \in G$ takvi da je $y \leq x$. Iz $x \in A + C$ slijedi da postoje $a \in A$ i $c \in C$ takvi da je $x = a + c$. Imamo $y \leq a + c$ pa iz definicije uređene grupe slijedi da je $y + (-c) \leq (a + c) + (-c)$, tj. $y + (-c) \leq a$. Iz propozicije 1.3.15 slijedi da je $y + (-c) \in A$. Označimo $a' = y + (-c)$. Dakle, $a' \in A$ te slijedi $y = a' + c$. Stoga je $y \in A + C$.

Iz svega ovoga i propozicije 1.3.14 slijedi da je $(A + C, G\backslash(A + C))$ prerez u $(G, \leq)$. □

Lema 1.4.4. *Neka je $(G, \leq)$ Abelova grupa te neka su $A, B, C \subseteq G$. Tada je*

$$(A + B) + C = A + (B + C). \tag{1}$$

Dokaz. Neka je $x \in (A + B) + C$. Tada postoje $y \in A + B$ i $c \in C$ takvi da je $x = y + c$. Iz $y \in A + B$ slijedi da postoje $a \in A$ i $b \in B$ takvi da je $y = a + b$. Stoga je $x = (a + b) + c$. Iz činjenice da je operacija + asocijativna slijedi da je $x = a + (b + c)$. Očito je $b + c \in B + C$ pa vidimo da je $x \in A + (B + C)$. Time smo dokazali da je $(A + B) + C \subseteq A + (B + C)$. Analogno dobijemo da je $A + (B + C) \subseteq (A + B) + C$.

Dakle, (1) vrijedi. □

Lema 1.4.5. *Neka je* $(G, +, \leq)$ *uređena grupa te neka je* (A, B) *prerez u* $(G, \leq)$*. Neka je* $C = \{x \in G \mid x \leq 0\}$*. Tada je* $A + C = A$*.*

Dokaz. Neka je $a \in A$. Imamo $a = a + 0$. Uočimo da je $0 \in C$. Stoga je $a \in A + C$. Time smo dokazali da je $A \subseteq A + C$.

Obratno, neka je $x \in A + C$. Tada postoje $a \in A$ i $c \in C$ takvi da je $x = a + c$. Imamo $c \leq 0$ što povlači da je $a + c \leq a + 0$, tj. $a + c \leq a$. Prema propoziciji 1.3.15 vrijedi $a + c \in A$, tj. $x \in A$. Time smo dokazali da je $A + C \subseteq A$. Dakle, vrijedi $A + C = A$. □

Sljedeću lemu dokazujemo analogno lemi 1.4.4.

Lema 1.4.6. *Neka je* $(G, +)$ *Abelova grupa te neka su* $A, C \subseteq G$*. Tada je* $A + C = C + A$*.*

Definicija 1.4.7. *Neka je* $(G, +, \leq)$ *uređena grupa. Na skupu* $\Omega(G, \leq)$ *definiramo binarnu operaciju* $\oplus$ *sa* $(A, B) \oplus (C, D) = (A + C, G\backslash(A + C))$*. Uočimo da je ova definicija dobra prema propoziciji 1.4.3.*

Definicija 1.4.8. *Ako je* $(G, \cdot)$ *monoid takav da je binarna operacija* $\cdot$ *komutativna onda za* $(G, \cdot)$ *kažemo da je komutativan monoid.*

Propozicija 1.4.9. *Neka je* $(G, +, \leq)$ *uređena grupa, pri čemu je* $(G, +)$ *netrivijalna grupa. Tada je* $(\Omega(G, \leq), \oplus)$ *komutativan monoid.*

Dokaz. Neka su (A, B), (C, D) i (E, F) prerezi u $(G, \leq)$. Tada je $((A, B) \oplus (C, D)) \oplus (E, F) = (A + C, G\backslash(A + C)) \oplus (E, F) = ((A + C) + E, G\backslash((A + C) + E))$. S druge strane, vrijedi $(A, B) \oplus ((C, D) \oplus (E, F)) = (A + (C + E), G\backslash(A + (C + E))$ pa iz leme 1.4.4 slijedi da je $((A, B) \oplus (C, D)) \oplus (E, F) = (A, B) \oplus ((C, D) \oplus (E, F))$. Prema tome, binarna operacija $\oplus$ je asocijativna. Analogno vidimo da je $\oplus$ komutativna binarna operacija.

Neka je $\mathbf{O} = \{x \in G \mid x \leq 0\}$. Očito je $\mathbf{O} \neq \emptyset$. Nadalje, prema propoziciji 1.3.13 0 nije najveći element u $(G, \leq)$ pa zaključujemo da je $\mathbf{O} \neq G$. Stoga je $G\backslash\mathbf{O} \neq \emptyset$. Očito vrijedi sljedeće: ako su $x \in \mathbf{O}$ i $y \in G$ takvi da je $y \leq x$, onda je $y \in \mathbf{O}$. Iz propozicije 1.3.14 slijedi da je $(\mathbf{O}, G\backslash\mathbf{O})$ prerez u $(G, \leq)$. Neka je $(A, B) \in \Omega(G, \leq)$. Prema lemi 1.4.5 vrijedi $A + \mathbf{O} = A$. Stoga je $(A, B) \oplus (\mathbf{O}, G\backslash\mathbf{O}) = (A + \mathbf{O}, G\backslash(A + \mathbf{O})) = (A, G\backslash A) = (A, B)$. Dakle, $(A, B) \oplus (\mathbf{O}, G\backslash\mathbf{O}) = (A, B)$.

Zaključak: $(\mathbf{O}, G\backslash\mathbf{O})$ je neutralni element za operaciju $\oplus$. Time je tvrdnja propozicije dokazana. □

Definicija 1.4.10. *Neka je* $(G, \cdot)$ *komutativan monoid te neka je* $\leq$ *uređaj na* G *takav da za sve* $x, y, z \in G$ *vrijedi sljedeće: ako je* $x \leq y$*, onda je* $x \cdot z \leq y \cdot z$*. Tada za uređenu trojku* $(G, \cdot, \leq)$ *kažemo da je uređeni monoid.*

Propozicija 1.4.11. *Neka je* $(G, +, \leq)$ *uređena grupa. Tada je* $(\Omega(G, \leq), \oplus, \leq)$ *uređeni monoid.*

Dokaz. Znamo da je $(\Omega(G,\leq),\oplus)$ komutativni monoid (prema propoziciji 1.4.9) te da je $\preceq$ uređaj na $\Omega(G,\leq)$ (prema propoziciji 1.3.2). Preostaje dokazati da za sve $\alpha,\beta,\gamma\in\Omega(G,\leq)$ takve da je $\alpha\preceq\beta$ vrijedi $\alpha\oplus\gamma\preceq\beta\oplus\gamma$.

Neka su $(A,B),(C,D),(E,F)\in\Omega(G,\leq)$ takvi da je

$$(A,B)\preceq(C,D). \tag{1}$$

Želimo dokazati da je

$$(A,B)\oplus(E,F)\preceq(C,D)\oplus(E,F), \tag{2}$$

tj. $(A+E,G\backslash(A+E))\preceq(C+E,G\backslash(C+E))$. Dakle, treba dokazati da je $A+E\subseteq C+E$. Neka je $x\in A+E$. Tada postoje $a\in A$ i $e\in E$ takvi da je $x=a+e$. Iz (1) slijedi da je $A\subseteq C$. Stoga je $a\in C$ pa je $a+e\in C+E$, tj. $x\in C+E$. Time smo dokazali da je $A+E\subseteq C+E$ pa vrijedi (2).

Time je tvrdnja propozicije dokazana. □

Definicija 1.4.12. *Neka su $(G,\cdot)$ i $(H,*)$ monoidi te neka je $f:G\to H$ funkcija. Kažemo da je f homomorfizam monoida $(G,\cdot)$ i $(H,*)$ ako za sve $x,y\in G$ vrijedi $f(x\cdot y)=f(x)*f(y)$.*

Napomena 1.4.13. *Neka je $(S,\leq)$ uređeni skup te neka su (A,B) i (C,D) prerezi u $(S,\leq)$. Tada je $B=S\backslash A$ i $D=S\backslash C$. Stoga je $(A,B)=(C,D)\Leftrightarrow A=C$.*

Napomena 1.4.14. *Neka je $(G,\cdot,\leq)$ uređeni monoid te neka su $a,b,c,d\in G$ takvi da je $a\leq b$ i $c\leq d$. Tada je $a\cdot c\leq b\cdot d$. Naime, iz definicije uređenog monoida dobivamo da je $a\cdot c\leq b\cdot c$ i $b\cdot c\leq b\cdot d$ pa iz tranzitivnosti relacije $\leq$ slijedi da je $a\cdot c\leq b\cdot d$.*

Propozicija 1.4.15. *Neka je $(G,+,\leq)$ uređena grupa, $(G,+)$ netrivijalna te neka je $f:G\to\Omega(G,\leq)$ funkcija definirana s $f(x)=(\{z\in G\,|\,z\leq x\},\{z\in G\,|\,x<z\})$. Tada je f homomorfizam monoida $(G,+)$ i $(\Omega(G,\leq),\oplus)$.*

Dokaz. Neka su $x,y\in G$. Želimo dokazati da je

$$f(x+y)=f(x)\oplus f(y). \tag{1}$$

Imamo $f(x+y)=(\{z\in G\,|\,z\leq x+y\},\{z\in G\,|\,x+y<z\})$, $f(x)=(\{z\in G\,|\,z\leq x\},\{z\in G\,|\,x<z\})$, $f(y)=(\{z\in G\,|\,z\leq y\},\{z\in G\,|\,y<z\})$. Imamo $f(x)\oplus f(y)=(C,D)$, gdje je $C=\{z\in G\,|\,z\leq x\}+\{z\in G\,|\,z\leq y\}$, a $D=G\backslash C$. Da bismo dokazali da vrijedi (1) dovoljno je prema napomeni 1.4.13 dokazati da je

$$\{z\in G\,|\,z\leq x+y\}=C. \tag{2}$$

Neka je $z\in C$. Tada postoje $z_1,z_2\in G$ takvi da je $z_1\leq x$, $z_2\leq y$ i $z=z_1+z_2$. Iz napomene 1.4.14 slijedi da je $z_1+z_2\leq x+y$, tj. $z\leq x+y$. Obratno, pretpostavimo da je

$z \in G$ takav da je $z \leq x + y$. Želimo dokazati da je $z \in C$. Imamo $z + (-x) \leq y$. Definirajmo $z_2 = z + (-x)$. Tada je $z_2 \leq y$ i $x + z_2 = z$. Vrijedi $x \in \{a \in G \mid a \leq x\}$ i $z_2 \in \{a \in G \mid a \leq y\}$. Stoga je $x + z_2 \in C$, tj. $z \in C$. Time smo dokazali da vrijedi (2).

Dakle, vrijedi (2) i propozicija je dokazana. □

Definicija 1.4.16. *Neka su $(G, +, \leq)$ i $(H, *, \leq)$ uređeni monoidi. Za funkciju $f : G \to H$ kažemo da je morfizam ovih uređenih monoida ako je f homomorfizam monoida $(G, +)$ i $(H, *)$ te ako je f rastuća funkcija s obzirom na uređaje $\leq$ i $\leq$.*

Definicija 1.4.17. *Neka je $(G, \cdot, \leq)$ uređeni monoid. Kažemo da je $(G, \cdot, \leq)$ potpuno uređeni monoid ako je $(G, \leq)$ potpuno uređen skup.*

Teorem 1.4.18. *Neka je $(G, +, \leq)$ netrivijalna uređena grupa. Tada postoje potpuno uređeni monoid $(H, *, \leq)$ i injekcija $f : G \to H$ koja je morfizam uređenih monoida $(G, +, \leq)$ i $(H, *, \leq)$.*

Dokaz. Prema propoziciji 1.4.11 $(G, \leq)$ nema najveći element. Neka je $f : G \to \Omega(G, \leq)$ funkcija definirana s $f(x) = (\{y \in G \mid y \leq x\}, \{y \in G \mid x < y\})$. Prema propoziciji 1.3.7 funkcija f je injekcija te je rastuća s obzirom na $\leq$ i $\leq$. Prema prethodnoj propoziciji funkcija f je homomorfizam monoida $(G, +)$ i $(\Omega(G, \leq), \oplus)$. Prema propoziciji 1.3.14, $(\Omega(G, \leq), \oplus, \leq)$ je uređeni monoid. Prema tome, f je morfizam uređenih monoida $(G, +, \leq)$ i $(\Omega(G, \leq), \oplus, \leq)$. Iz teorema 1.3.3 slijedi da je $(\Omega(G, \leq), \leq)$ potpuno uređen skup. Stoga je $(\Omega(G, \leq), \oplus, \leq)$ potpuno uređen monoid.

Time je tvrdnja teorema dokazana. □

Poglavlje 2

Pravi prerezi

2.1 Pravi prerezi

Definicija 2.1.1. *Neka je $(S, \leq)$ uređeni skup te neka je $A \subseteq S$. Za $a_0 \in A$ kažemo da je najveći element od A u $(S, \leq)$ ako za svaki $a \in A$ vrijedi da je $a \leq a_0$.*

Definicija 2.1.2. *Neka je $(S, \leq)$ uređeni skup te neka je (A, B) prerez u $(S, \leq)$. Kažemo da je (A, B) pravi prerez u $(S, \leq)$ ako skup A nema najveći element u $(S, \leq)$.*

Skup svih pravih prereza u $(S, \leq)$ označavamo s $\Omega'(S, \leq)$. Očito je $\Omega'(S, \leq) \subseteq \Omega(S, \leq)$.

Definicija 2.1.3. *Neka su X i Y skupovi takvi da je $Y \subseteq X$. Pretpostavimo da je ρ binarna relacija na X. Neka je $\rho' = \{(a, b) \in Y \times Y \mid (a, b) \in \rho\}$. Očito je ρ' binarna relacija na Y. Za ρ' kažemo da je binarna relacija na Y određena s ρ. Uočimo da je $\rho' = (Y \times Y) \cap \rho$. Nadalje, ako su $a, b \in Y$, onda je $a\rho' b \Leftrightarrow a\rho b$.*

Napomena 2.1.4. *Neka je ρ binarna relacija na skupu X, neka je $Y \subseteq X$, te neka je ρ' binarna relacija na Y određena s ρ. Pretpostavimo da je ρ refleksivna na X. Tada je ρ' refleksivna na Y. Naime, za svaki $y \in Y$ vrijedi $y\rho y$ pa je i $y\rho' y$. Pretpostavimo sada da je ρ antisimetrična na X. Tada je ρ' antisimetrična na Y. Naime, ako su $a, b \in Y$ takvi da je $a\rho' b$ i $b\rho' a$ onda je $a\rho b$ i $b\rho a$ pa je $a = b$.*

Slično zaključujemo da je ρ' tranzitivna relacija na Y ako je ρ tranzitivna relacija na X te da je ρ' uređaj na Y ako je ρ uređaj na X. Ako je ρ uređaj na X onda za ρ' kažemo da je uređaj na Y određen s ρ.

Definicija 2.1.5. *Neka je $(S, \leq)$ uređeni skup. Podsjetimo se da smo na skupu $\Omega(S, \leq)$ definirali binarnu relaciju $\preceq$. Označimo sa $\preceq'$ binarnu relaciju na $\Omega'(S, \leq)$ određenu s $\preceq$. Iz propozicije 1.3.2 slijedi da je $\preceq'$ uređaj na $\Omega'(S, \leq)$, tj. da je $(\Omega'(S, \leq), \preceq')$ uređen skup.*

Teorem 2.1.6. *Neka je $(S, \leq)$ uređen skup. Tada je $(\Omega'(S, \leq), \preceq')$ potpuno uređen skup.*

Dokaz. Pretpostavimo da su $X, Y \subseteq \Omega'(S, \leq)$ takvi da je $X \neq 0$ i $Y \neq 0$ te da za svaki $(A, B) \in X$ i za svaki $(C, D) \in Y$ vrijedi $(A, B) \leq' (C, D)$. Neka je

$$\mathcal{A} = \bigcup_{(A, S\setminus A)\in X} A$$

U dokazu teorema 1.3.3 smo vidjeli da je $(\mathcal{A}, S\setminus\mathcal{A})$ prerez u $(S, \leq)$ takav da je $U \leq (\mathcal{A}, S\setminus\mathcal{A})$ za svaki $U \in X$ i $(\mathcal{A}, S\setminus\mathcal{A}) \leq V$ za svaki $V \in Y$. Dokažimo da je $(\mathcal{A}, S\setminus\mathcal{A})$ pravi prerez u $(S, \leq)$.

Pretpostavimo suprotno. Tada $\mathcal{A}$ ima najveći element u $(S, \leq)$, tj, postoji $a_0 \in \mathcal{A}$ takav da je $a \leq a_0$ za svaki $a \in \mathcal{A}$. Iz definicije od $\mathcal{A}$ slijedi da postoji A takav da je $a_0 \in A$ te takav da je $(A, S\setminus A) \in X$. Za svaki $a \in A$ očito vrijedi $a \in \mathcal{A}$ pa je $a \leq a_0$. Iz ovoga zaključujemo da je a_0 najveći element od A u $(S, \leq)$.

No $(A, S\setminus A) \in X$ i $X \subseteq \Omega'(S, \leq)$ povlači da je $(A, S\setminus A)$ pravi prerez u $(S, \leq)$, što je u kontradikciji s tvrdnjom da A ima najveći element. Prema tome, $(\mathcal{A}, S\setminus\mathcal{A})$ je pravi prerez u $(S, \leq)$. Označimo $W = (\mathcal{A}, S\setminus\mathcal{A})$. Imamo $W \in \Omega'(S, \leq)$ te $U \leq' W$ za svaki $U \in X$ i $W \leq' V$ za svaki $V \in Y$.

Zaključak: $(\Omega'(S, \leq), \leq')$ je potpuno uređen skup. □

Propozicija 2.1.7. *Neka je $(G, +, \leq)$ uređena grupa te neka su (A, B) i (C, D) pravi prerezi u $(G, \leq)$. Tada je $(A, B) \oplus (C, D)$ pravi prerez u $(G, \leq)$.*

Dokaz. Vrijedi $(A, B) \oplus (C, D) = (A + C, G\setminus(A + C))$. Dokažimo da $A + C$ nema najveći element u $(G, \leq)$.

Neka su $a \in A$ i $c \in C$. Budući da A nema najveći element, postoji $a' \in A$ takav da $a' \not\leq a$ pa slijedi $a < a'$. Isto tako zaključujemo da postoji $c' \in C$ takav da je $c < c'$. Iz korolara 1.4.2 slijedi da je $a + c < a' + c'$. Ovim smo pokazali sljedeće: Za svaki $x \in A + C$ postoji $x' \in A + C$ takav da je $x < x'$. Iz ovoga zaključujemo da $A + C$ nema najveći element.

Time je tvrdnja propozicije dokazana. □

Definicija 2.1.8. *Neka je $(G, +, \leq)$ uređena grupa. Na $\Omega'(G, \leq)$ definiramo binarnu operaciju $\oplus'$ na sljedeći način: $\alpha \oplus' \beta = \alpha \oplus \beta$, za sve $\alpha, \beta \in \Omega'(G, \leq)$.*

Uočimo da je prema propoziciji 2.1.7 ova definicija dobra.

Uočimo da je $\oplus'$ asocijativna binarna operacija na $\Omega'(G, \leq)$. Naime, za sve $\alpha, \beta, \gamma \in \Omega'(G, \leq)$, koristeći asocijativnost binarne operacije $\oplus$ dobivamo $\alpha \oplus' (\beta \oplus' \gamma) = \alpha \oplus (\beta \oplus \gamma) = (\alpha \oplus \beta) \oplus \gamma = (\alpha \oplus' \beta) \oplus' \gamma$.

Analogno zaključujemo da je $\oplus'$ komutativna binarna operacija.

Primjer 2.1.9. *Neka je $\leq$ standardni uređaj na $\mathbb{Z}$. Tvrdimo da u uređenom skupu $(\mathbb{Z}, \leq)$ nema pravih prereza. Pretpostavimo suprotno, da postoji pravi prerez (A, B) u $(\mathbb{Z}, \leq)$.*

Odaberimo $a \in A$ i $b \in B$. Tada je $a < b$ pa je $b-a \in \mathbb{N}$. Neka je $S = \{k \in \mathbb{N} \mid a+k \in B\}$. Vrijedi $b-a \in S$, dakle S je neprazan podskup od $\mathbb{N}$ pa stoga ima najmanji element. Neka je k_0 najmanji element od S. Dakle, $k_0 \in \mathbb{N}$ i $a + k_0 \in B$. Tvrdimo da $a + k_0 - 1 \notin B$.

Pretpostavimo suprotno, tj. da je $a + k_0 - 1 \in B$. Ako je $k_0 \geq 2$, onda je $k_0 - 1 \in \mathbb{N}$ pa zbog $a + (k_0 - 1) \in B$ imamo da je $k_0 - 1 \in S$, što je nemoguće jer je k_0 najmanji element od S. Stoga je $k_0 = 1$ pa je $a + k_0 - 1 = a$, dakle $a \in B$. No to je nemoguće jer je $A \cap B = \emptyset$. Dakle, $a + k_0 - 1 \notin B$. Slijedi da je $a + k_0 - 1 \in A$.

Označimo $z = a + k_0 - 1$. Imamo $z \in A$ i $z + 1 \in B$. Neka je $x \in A$. Tada je $x < y$, za svaki $y \in B$ pa je posebno $x < z + 1$. Stoga je $x \leq z$. Zaključujemo da je z najveći element od A. Ovo je u kontradikciji s činjenicom da je (A, B) pravi prerez u $(\mathbb{Z}, \leq)$.

2.2 Guste uređene grupe

Definicija 2.2.1. *Za uređen skup $(S, \leq)$ kažemo da je netrivijalan ako S ima bar 2 elementa.*

Definicija 2.2.2. *Za netrivijalni uređeni skup $(S, \leq)$ kažemo da je gust ako za sve $x, y \in S$ takve da je $x < y$ postoji $z \in S$ takav da je $x < z < y$.*

Primjer 2.2.3. *Neka je $(S, \leq)$ gust uređen skup. Odaberimo $a, b \in S$ takve da je $a < b$ (to možemo napraviti jer S ima bar 2 elementa).*

Neka je $A = \{x \in S \mid x < b\}$, $B = \{x \in S \mid b \leq x\}$. Tvrdimo da je (A, B) pravi prerez u $(S, \leq)$. Za svaki $x \in A$ i $y \in B$ očito vrijedi $x \leq y$. Nadalje, imamo $A \cup B = S$, $A \cap B = \emptyset$, $A \neq \emptyset$ (jer je $a \in A$) i $B \neq \emptyset$ (jer je $b \in B$). Stoga je (A, B) prerez u $(S, \leq)$.

Pretpostavimo da A ima najveći element u $(S, \leq)$, neka je to x. Iz $x \in A$ slijedi da je $x < b$. Gustoća uređenog skupa $(S, \leq)$ povlači da postoji $z \in S$ takav da je $x < z < b$. Iz $z < b$ slijedi da je $z \in A$, no to je zajedno s $x < z < b$ u kontradikciji s činjenicom da je x najveći element od A.

Prema tome, (A, B) je pravi prerez u $(S, \leq)$.

Definicija 2.2.4. *Za uređenu grupu $(G, +, \leq)$ kažemo da je gusta ako je $(G, \leq)$ gust uređen skup.*

Lema 2.2.5. *Neka je $(G, +, \leq)$ uređena grupa. Neka je (A, B) pravi prerez u $(G, \leq)$. Tada je*

$$A = A + \{x \in G \mid x < 0\}. \tag{1}$$

Dokaz. Neka su $a \in A$ i $x \in G$ takvi da je $x < 0$. Iz $x < 0$ i propozicije 1.3.12 slijedi da je $a + x < a + 0$, tj. $a + x < a$. Prema propoziciji 1.3.14 vrijedi $a + x \in A$. Time smo dokazali da je $A + \{x \in G \mid x < 0\} \subseteq A$.

Obratno, neka je $a \in A$. Budući da A nema najveći element, postoji $a' \in A$ takav da je $a < a'$. Slijedi $a + (-a') < 0$. Definiramo $x = a - a'$. Tada je $x \in G$ i $x < 0$. Iz definicije od x slijedi da je $x + a' = a$. Time smo pokazali da je $A \subseteq A + \{x \in G \mid x < 0\}$.

Dakle, vrijedi (1). □

Propozicija 2.2.6. *Neka je $(G, +, \leq)$ gusta uređena grupa. Neka je $\Theta = (\{x \in G \mid x < 0\}, \{x \in G \mid 0 \leq x\})$. Tada je Θ neutralni element za binarnu operaciju $\oplus'$ (u $\Omega'(G, \leq)$).*

Dokaz. Budući da je $(G, \leq)$ gust uređen skup, vrijedi da je $(G, \leq)$ netrivijalan uređen skup, dakle, G ima bar 2 elementa. Stoga postoji $x \in G$ takav da je $x \neq 0$. Slijedi $x < 0$ ili $0 < x$. Ako je $0 < x$ onda je $-x < 0$. Zaključak: postoji $a \in G$ takav da je $a < 0$. Iz prethodnog primjera slijedi da je Θ pravi prerez u $(G, \leq)$, dakle, $\Theta \in \Omega'(G, \leq)$.

Neka je $(A, B) \in \Omega'(G, \leq)$. Koristeći prethodnu lemu dobivamo $(A, B) \oplus' \Theta = (A + \{x \in G \mid x < 0\}, G \backslash (A + \{x \in G \mid x < 0\})) = (A, G \backslash A) = (A, B)$.

Dakle, $(A, B) \oplus' \Theta = (A, B)$ pa iz činjenice da je $\oplus'$ komutativna binarna operacija slijedi da je Θ neutralni element za $\oplus'$. □

Korolar 2.2.7. *Neka je $(G, +, \leq)$ gusta uređena grupa. Tada je $(\Omega'(G, \leq), \oplus', \leq')$ uređeni monoid.*

Dokaz. Neka su $\alpha, \beta, \gamma \in \Omega'(G, \leq)$ takvi da vrijedi $\alpha \leq' \beta$. Tada je $\alpha \leq \beta$ pa iz činjenice da je $(\Omega(G, \leq), \oplus, \leq)$ uređeni monoid (prema propoziciji 1.4.11) slijedi da je $\alpha \oplus \gamma \leq \beta \oplus \gamma$. Prema tome $\alpha \oplus' \gamma \leq' \beta \oplus' \gamma$. Time je tvrdnja korolara dokazana. □

Definicija 2.2.8. *Neka je $(G, \cdot)$ grupa te $g \in G$. Za $n \in \mathbb{N}$ definiramo g^n induktivno na sljedeći način: neka je $g^1 = g$; pretpostavimo da smo definirali g^n za neki $n \in \mathbb{N}$. Definiramo $g^{n+1} = g^n \cdot g$. Definiramo $g^0 = e$, gdje je e neutralni element u $(G, \cdot)$. Ako je $m \in \mathbb{Z}$, $m < 0$, definiramo $g^m = (g^{-m})^{-1}$. Ako je $g \in G$ i $m \in \mathbb{Z}$, onda za g^m kažemo da je m-ta potencija od g u grupi $(G, \cdot)$.*

Napomena 2.2.9. *Ako je $(G, +)$ Abelova grupa, $g \in G$ i $m \in \mathbb{Z}$, onda m-tu potenciju od g u $(G, +)$ obično označavamo sa $m \cdot g$. Dakle, $1 \cdot g = g$, $0 \cdot g = 0_G$, gdje je 0_G neutralni element u $(G, +)$. Nadalje, za svaki $n \in \mathbb{N}$ vrijedi $(n + 1)g = ng + g$ te $(-n)g = -(ng)$.*

2.3 Arhimedova grupa

Definicija 2.3.1. *Neka je $(G, +, \leq)$ uređena grupa. Za $(G, +, \leq)$ kažemo da je Arhimedova grupa ako za svaki $x \in G$ takav da je $0 < x$ i svaki $y \in G$ postoji $n \in \mathbb{N}$ takav da je $y < nx$.*

Definicija 2.3.2. *Neka je $(G, \cdot)$ monoid te neka je $x \in G$. Pretpostavimo da x ima inverzni element u $(G, \cdot)$. Tada za x kažemo da je invertibilan element u $(G, \cdot)$.*

Propozicija 2.3.3. *Neka je $(G, \cdot)$ monoid te neka su x i y invertibilni elementi u $(G, \cdot)$. Tada je $x \cdot y$ invertibilan element u $(G, \cdot)$ te vrijedi $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.*

Dokaz. Neka je e neutralni element u $(G, \cdot)$. Vrijedi $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = x \cdot ((y \cdot y^{-1}) \cdot x^{-1}) = x \cdot x^{-1} = e$. Analogno dobivamo da je $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = e$ pa zaključujemo da tvrdnja propozicije vrijedi. □

Napomena 2.3.4. *Neka je $(G, +)$ Abelova grupa te neka su $x, y \in G$. Tada je $-(x + y) = -x + (-y)$. To slijedi direktno iz prethodne propozicije.*

Propozicija 2.3.5. *Neka je $(G, +, \leq)$ Arhimedova grupa te neka je (A, B) prerez u $(G, \leq)$. Neka je $x \in G$ takav da je $0 < x$. Tada postoje $a \in A$ i $b \in B$ takvi da je $b - a = x$.*

Dokaz. Odaberimo $a_0 \in A$ i $b_0 \in B$. Iz definicije Arhimedove grupe slijedi da postoji $n \in \mathbb{N}$ takav da je $b_0 - a_0 < nx$. Iz ovoga slijedi da je $b_0 < a_0 + nx$. Iz činjenice da je (A, B) prerez slijedi da je $a_0 + nx \in B$. Neka je $k = \min\{n \in \mathbb{N} \mid a_0 + nx \in B\}$.

1. slučaj: $k = 1$
   Tada je $a_0 + 1 \cdot x \in B$. Označimo $a = a_0$ i $b = a_0 + x$. Imamo $a \in A$, $b \in B$ i $b - a = x$.

2. slučaj: $k > 1$
   Tada postoji $m \in \mathbb{N}$ takav da je $k = m+1$. Imamo $a_0 + kx \in B$, tj. $a_0 + (m+1)x \in B$, no $a_0 + mx \notin B$ zbog definicije od k. Definiramo $a = a_0 + mx$ i $b = a_0 + (m+1)x$. Vrijedi $a \notin B$ pa je $a \in A$. Očito je $b \in B$. Koristeći prethodnu napomenu dobivamo $b - a = b + (-a) = (a_0 + (m+1)x) + (-a_0 + (-mx)) = (m+1)x + (-mx) = mx + x + (-mx) = x$.

   Dakle, $b - a = x$.

Time je tvrdnja propozicije dokazana. □

Korolar 2.3.6. *Neka je $(G, +, \leq)$ gusta Arhimedova grupa te neka je (A, B) prerez u $(G, \leq)$. Pretpostavimo da je $x \in G$ takav da je $0 < x$. Tada postoje $a \in A$ i $b \in B$ takvi da je $b - a < x$.*

Dokaz. Iz činjenice da je $(G, +, \leq)$ gusta grupa slijedi da postoji $x' \in G$ takav da je $0 < x' < x$. Prema propoziciji 2.3.5 postoje $a \in A$ i $b \in B$ takvi da je $b - a = x'$. Slijedi $b - a < x$. □

Teorem 2.3.7. *Neka je $(G, +, \leq)$ gusta Arhimedova grupa. Tada je $(\Omega'(G, \leq), \oplus')$ grupa.*

Dokaz. Znamo da je $(\Omega'(G, \leq), \oplus')$ monoid (prema propoziciji 2.2.6) te da je $\Theta = (\{x \in G \mid x < 0\}, \{x \in G \mid 0 \leq x\})$ neutralni element za $\oplus'$. Neka je $(A, B) \in \Omega'(G, \leq)$.

Definiramo $C = \{y \in G \mid \exists b \in B, b < -y\}$. Tvrdimo da je $C \neq \emptyset$. Odaberimo neki $b \in B$. Prema propoziciji 1.3.13, $(G, \leq)$ nema najveći element pa postoji $b' \in G$ takav da je $b < b'$. Definiramo $y = -b'$. Tada je $y \in G$ i $-y = b'$ pa je $b < -y$. Stoga je $y \in C$. Dakle, $C \neq \emptyset$.

Odaberimo neki $a \in A$. Pretpostavimo da je $-a \in C$. Tada postoji $b \in B$ takav da je $b < -(-a)$, tj. $b < a$. Ovo je nemoguće prema definiciji prereza. Stoga $-a \notin C$ pa zaključujemo da je $G\backslash C \neq \emptyset$. Pretpostavimo da je $x \in C$ te da je $y \in G$ takav da je $y \leq x$. Zbog $x \in C$ postoji $b \in B$ takav da je $b < -x$. Iz $y \leq x$ slijedi $-x \leq -y$ pa je $b < -y$, što povlači da je $y \in C$. Iz propozicije 1.3.12 slijedi da je $(C, G\backslash C)$ prerez u $(G, \leq)$. Dokažimo da je $(C, G\backslash C)$ pravi prerez u $(G, \leq)$.

Neka je $c \in C$. Tada postoji $b \in B$ takav da je $b < -c$. Iz činjenice da je $(G, \leq)$ gust skup slijedi da postoji $x \in G$ takav da je $b < x < -c$. Iz $b < x$ slijedi da je $-x \in C$. Iz $x < -c$ slijedi $c < -x$. Ovim smo pokazali da za svaki $c \in C$ postoji $c' \in C$ takav da je $c < c'$. Prema tome, C nema najveći element u $(G, \leq)$ pa je, dakle, $(C, G\backslash C)$ pravi prerez u $(G, \leq)$. Tvrdimo da je

$$(A, B) \oplus' (C, G\backslash C) = \Theta. \tag{1}$$

Jednakost (1) je ekvivalentna s $(A + C, G\backslash(A + C)) = \Theta$, a ovo je ekvivalentno s $A + C = \{x \in G \mid x < 0\}$. Neka su $a \in A$ i $c \in C$. Tada postoji $b \in B$ takav da je $b < -c$. Budući da je (A, B) prerez, vrijedi da je $a < b$ pa je $a < -c$, što povlači da je $a + c < 0$. Time smo dokazali da je $A + C \subseteq \{x \in G \mid x < 0\}$.

Neka je $x \in G$ takav da je $x < 0$. Tada je $0 < -x$ pa iz korolara 2.3.6 slijedi da postoje $a \in A$ i $b \in B$ takvi da je $b - a < -x$. Slijedi da je $b < -x + a$. Definiramo $c = -(-x + a)$. Tada je $-c = -x + a$ pa je $b < -c$. Stoga je $c \in C$. Nadalje, iz definicije od c slijedi da je $c = x - a$ pa je $x = a + c$. Dakle, $x \in A + C$. Prema tome, $\{x \in G \mid x < 0\} \subseteq A + C$.

Time smo dokazali da vrijedi $A + C = \{x \in G \mid x < 0\}$. Stoga vrijedi (1). Iz činjenice da je $\oplus'$ komutativna binarna operacija slijedi da je $(C, G\backslash C) \oplus' (A, B) = \Theta$.

Zaključak: $(\Omega'(G, \leq), \oplus')$ je grupa. □

Korolar 2.3.8. *Neka je $(G, +, \leq)$ gusta Arhimedova grupa. Tada je $(\Omega'(G, \leq), \oplus', \leq')$ uređena grupa.*

Dokaz. Ovo slijedi iz prethodnog teorema i korolara 2.2.7. □

Definicija 2.3.9. *Neka je $(G, +, \leq)$ uređena grupa takva da je $(G, \leq)$ potpuno uređen skup. Tada za $(G, +, \leq)$ kažemo da je potpuno uređena grupa.*

Korolar 2.3.10. *Neka je $(G, +, \leq)$ gusta Arhimedova grupa. Tada je $(\Omega'(G, \leq), \oplus', \leq')$ potpuno uređena grupa.*

Dokaz. Ovo slijedi iz prethodnog korolara i teorema 2.1.6. □

Definicija 2.3.11. *Neka su $(G, +, \leq)$ i $(H, +', \leq')$ uređene grupe. Za funkciju $f : G \to H$ kažemo da je morfizam uređenih grupa ako za sve $x, y \in G$ vrijedi:*

1. $f(x + y) = f(x) +' f(y)$

2. *ako je* $x \leq y$ *onda je* $f(x) \leq f(y)$.

Uočimo da je f *morfizam ovih uređenih grupa ako i samo ako je* f *morfizam uređenih monoida* $(G, +, \leq)$ *i* $(H, +', \leq')$.

Propozicija 2.3.12. *Neka je* $(G, +, \leq)$ *gusta Arhimedova grupa. Neka je* $f : G \to \Omega'(G, \leq)$ *funkcija definirana s* $f(g) = (\{x \in G \mid x < g\}, \{x \in G \mid g \leq x\})$. *Tada je* f *injektivni morfizam uređenih grupa* $(G, +, \leq)$ *i* $(\Omega'(G, \leq), \oplus', \leq')$.

Dokaz. Uočimo prvo da je f dobro definirana funkcija. Naime, neka je $g \in G$. Prema prethodnoj lemi $(G, \leq)$ nema najveći element pa stoga postoji $z \in G$ takav da je $-g < z$, što povlači da je $-z < g$. Prema tome, $\{x \in G \mid x < g\} \neq \emptyset$. Stoga je $(\{x \in G \mid x < g\}, \{x \in G \mid g \leq x\})$ prerez u $(G, \leq)$.

Neka je $x \in G$ takav da je $x < g$. Budući da je uređeni skup $(G, \leq)$ gust, postoji $y \in G$ takav da je $x < y < g$. Ovo pokazuje da skup $\{x \in G \mid x < g\}$ nema najveći element u $(G, \leq)$. Prema tome, $(\{x \in G \mid x < g\}, \{x \in G \mid g \leq x\})$ je pravi prerez u $(G, \leq)$. Dakle, funkcija f je dobro definirana.

Neka su $g_1, g_2 \in G$, $g_1 \neq g_2$. Tada je $g_1 < g_2$ ili $g_2 < g_1$. Pretpostavimo da je $g_1 < g_2$. Tada je $g_1 \in \{x \in G \mid x < g_2\}$ i očito $g_1 \notin \{x \in G \mid x < g_1\}$. Stoga je $\{x \in G \mid x < g_2\} \neq \{x \in G \mid x < g_1\}$ pa je $f(g_1) \neq f(g_2)$. Do istog zaključka dolazimo u slučaju $g_2 < g_1$. Prema tome, f je injekcija.

Neka su $g_1, g_2 \in G$. Tvrdimo da je

$$f(g_1 + g_2) = f(g_1) \oplus' f(g_2). \tag{1}$$

Vrijedi $f(g_1 + g_2) = (\{x \in G \mid x < g_1 + g_2\}, \{x \in G \mid g_1 + g_2 \leq x\})$. S druge strane imamo

$$f(g_1) \oplus' f(g_2) = (\{y \in G \mid y < g_1\} + \{z \in G \mid z < g_2\}, G \backslash (\{y \in G \mid y < g_1\} + \{z \in G \mid z < g_2\})). \tag{2}$$

Stoga je, da bismo dokazali (1), dovoljno dokazati da je $\{x \in G \mid x < g_1 + g_2\} = \{y \in G \mid y < g_1\} + \{z \in G \mid z < g_2\}$.

Neka je $a \in \{y \in G \mid y < g_1\} + \{z \in G \mid z < g_2\}$. Tada je $a = y + z$, gdje su $y, z \in G$ takvi da je $y < g_1$ i $z < g_2$. Iz korolara 1.4.2 slijedi da je $y + z < g_1 + g_2$, tj. $a < g_1 + g_2$. Stoga je $a \in \{x \in G \mid x < g_1 + g_2\}$.

Obratno, neka je $x \in G$ takav da je $x < g_1 + g_2$. Tada je $x - g_1 < g_2$ (prema propoziciji 1.3.12). Budući da je $(G, \leq)$ gust uređen skup, postoji $z \in G$ takav da je $x - g_1 < z < g_2$. Iz $x - g_1 < z$ slijedi $x - z < g_1$. Definiramo $y = x - z$. Tada je $y < g_1$ i $x = y + z$. Također znamo da je $z < g_2$ pa je $x \in \{y \in G \mid y < g_1\} + \{z \in G \mid z < g_2\}$. Time smo dokazali da vrijedi jednakost (2). Stoga vrijedi i (1).

Neka su $g_1, g_2 \in G$ takvi da je $g_1 \leq g_2$. Ako je $x \in G$ takav da je $x < g_1$, onda je $x < g_2$ (prema propoziciji 1.1.19). Prema tome, vrijedi $\{x \in G \mid x < g_1\} \subseteq \{x \in G \mid x < g_2\}$ pa imamo, po definiciji, da je $f(g_1) \leq' f(g_2)$.

Zaključak: f je injektivni morfizam uređenih grupa. □

Definicija 2.3.13. *Neka je $(S, \leq)$ uređeni skup te neka je $A \subseteq S$. Kažemo da je A gust skup u $(S, \leq)$ ako za sve $x, y \in S$ takve da je $x < y$ postoji $a \in A$ takav da je $x < a < y$.*

Uočimo sljedeće: ako je $(S, \leq)$ netrivijalan uređen skup, onda je $(S, \leq)$ gust uređen skup ako i samo ako je S gust skup u $(S, \leq)$.

Uočimo i sljedeće: ako je A gust skup u $(S, \leq)$ te $B \subseteq S$ takav da je $A \subseteq B$, onda je i B gust skup u $(S, \leq)$. Posebno, ako je A gust skup u $(S, \leq)$, onda je S gust skup u $(S, \leq)$.

Propozicija 2.3.14. *Neka je $(G, +, \leq)$ gusta Arhimedova grupa te neka je $f : G \to \Omega'(G, \leq)$ funkcija iz prethodne propozicije. Tada je $f(G)$ gust skup u $(\Omega'(G, \leq), \preceq')$.*

Dokaz. Neka su $(A, B), (C, D) \in \Omega'(G, \leq)$ takvi da je $(A, B) \prec' (C, D)$. Iz toga slijedi da je $A \subseteq C$ i $A \neq C$. Zaključujemo da postoji $c \in C$ takav da $c \notin A$. Budući da je (C, D) pravi prerez u $(G, \leq)$, C nema najveći element pa postoji $c' \in C$ takav da je $c < c'$. Tvrdimo da je

$$A \subseteq \{x \in G \mid x < c'\}. \tag{1}$$

Neka je $a \in A$. Pretpostavimo da je $c' \leq a$. Tada, zbog $c < c'$, imamo $c < a$. Iz propozicije 1.3.14 slijedi da je $c \in A$, kontradikcija. Stoga ne vrijedi $c' \leq a$ pa je $a < c'$. Time smo dokazali da vrijedi (1).

Nadalje, vrijedi $A \neq \{x \in G \mid x < c'\}$ jer $c \notin A$ i $c \in \{x \in G \mid x < c'\}$. Iz ovoga i (1) slijedi da je $(A, B) \prec' f(c')$. Ako je $x \in G$ takav da je $x < c'$, onda je $x \in C$ (prema propoziciji 1.3.14). Stoga je $\{x \in G \mid x < c'\} \subseteq C$.

Nadalje, $\{x \in G \mid x < c'\} \neq C$ jer $c' \notin \{x \in G \mid x < c'\}$ i $c' \in C$. Stoga je $f(c') \prec' (C, D)$. Dakle, $(A, B) \prec' f(c') \prec' (C, D)$. Time je tvrdnja propozicije dokazana. □

2.4 Uređene grupe i proširenje množenja

Teorem 2.4.1. *Neka je $(G, +, \leq)$ uređena grupa te neka je $G^+ = \{x \in G | 0 \leq x\}$. Pretpostavimo da je $*$ asocijativna binarna operacija na G^+ takva da je*

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

$$i \;\; z * (x + y) = z * x + z * y, \forall x, y, z \in G. \tag{1}$$

Tada postoji binarna operacija $\cdot$ na G takva da je $x \cdot y = x * y, \forall x, y \in G^+$ te takva da je $(G, +, \cdot, \leq)$ uređeni prsten.

Dokaz. Neka je $z \in G^+$. Tvrdimo da je $0 * z = 0$. Imamo $0 * z = (0 + 0) * z = 0 * z + 0 * z$. Dakle, $0 * z = 0 * z + 0 * z$ pa slijedi da je $0 * z = 0$. Analogno dobivamo da je $z * 0 = 0$.

Definirajmo binarnu operaciju $\cdot$ na G na sljedeći način: Neka su $x, y \in G$. Imamo 4 slučaja.

(i) $0 \leq x, 0 \leq y$
Definiramo $x \cdot y = x * y$

(ii) $x \leq 0, 0 \leq y$
Definiramo $x \cdot y = -((-x) * y)$

(iii) $0 \leq x, y \leq 0$
Definiramo $x \cdot y = -(x * (-y))$

(iv) $x \leq 0, y \leq 0$
Definiramo $x \cdot y = (-x) * (-y)$

Tvrdimo da je $\cdot$ asocijativna binarna operacija na G. Neka su $a, b, c \in G$. Imamo 8 slučajeva.

1) $a, b, c \in G^+$

Koristeći asocijativnost binarne operacije $*$ dobivamo

$$a \cdot (b \cdot c) = a \cdot (b * c) = a * (b * c) = (a * b) * c = (a \cdot b) \cdot c$$

Dakle, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

2) $a \leq 0, b, c \in G^+$
Imamo: $a \cdot (b \cdot c) = a \cdot (b * c) = -((-a) * (b * c)) = -((-a) * b) * c)$.
S druge strane imamo: $(a \cdot b) \cdot c = (-((-a) * b)) \cdot c = \mu \cdot c$, gdje je $\mu = -((-a) * b)$.
Budući da je $\mu \leq 0$ imamo $\mu \cdot c = -((-\mu) * c) = -(((-a) * b) * c)$.

Dakle, $(a \cdot b) \cdot c = -(((-a) * b) * c)$. Prema tome, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

3) $b \leq 0, a, c \in G^+$
Imamo: $a \cdot (b \cdot c) = a \cdot (-(-b) * c) = a \cdot v$, gdje je $v = -((-b) * c)$.
Budući da je $v \leq 0$ imamo $a \cdot v = -(a * (-v)) = -(a * ((-b) * c))$. Dakle,

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

S druge strane imamo $(a \cdot b) \cdot c = (-(a * (-b))) \cdot c = \mu \cdot c$, gdje je $\mu = -(a * (-b))$.
Budući da je $\mu \leq 0$ imamo $\mu \cdot c = -((-\mu) * c) = -((a * (-b)) * c)$.

Dakle,

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

Iz (2) i (3) te asocijativnosti $*$ slijedi $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

4) $c \leq 0, a, b \in G^+$
Imamo $a \cdot (b \cdot c) = a \cdot (-(b * (-c))) = a \cdot v$, gdje je $v = -(b * (-c))$.
Budući da je $v \leq 0$ imamo $a \cdot v = -(a * (-v)) = -(a * (b * (-c)))$.
Dakle,
$$a \cdot (b \cdot c) = -(a * (b * (-c))). \tag{4}$$
S druge strane imamo $(a \cdot b) \cdot c = (a * b) \cdot c = -((a * b) * (-c))$.
Dakle,
$$(a \cdot b) \cdot c = -((a * b) * (-c)). \tag{5}$$
Iz (4) i (5) te asocijativnosti $*$ slijedi $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

5) $a, b \leq 0, c \in G^+$
Imamo $a \cdot (b \cdot c) = a \cdot (-((-b) * c)) = a \cdot \mu$, gdje je $\mu = -((-b) * c))$. Budući da je $a \leq 0$ $\mu \leq 0$ imamo $a \cdot \mu = (-a) * (-\mu) = (-a) * ((-b) * c)$.
Dakle,
$$a \cdot (b \cdot c) = (-a) * (-\mu) = (-a) * ((-b) * c). \tag{6}$$
S druge strane imamo $(a \cdot b) \cdot c = ((-a) * (-b)) \cdot c = ((-a) * (-b)) * c$.
Dakle,
$$(a \cdot b) \cdot c = ((-a) * (-b)) * c. \tag{7}$$
Iz (6) i (7) te asocijativnosti $*$ slijedi $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

6) $a, c \leq 0, b \in G^+$
Imamo $a \cdot (b \cdot c) = a \cdot (-(b * (-c))) = (-a) * (b * (-c))$.
Dakle,
$$a \cdot (b \cdot c) = (-a) * (b * (-c)). \tag{8}$$
S druge strane imamo $(a \cdot b) \cdot c = (-((-a) * b)) \cdot c = ((-a) * b) * (-c)$.
Dakle,
$$(a \cdot b) \cdot c = ((-a) * b) * (-c). \tag{9}$$
Iz (8) i (9) te asocijativnosti $*$ slijedi $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

7) $a \in G^+, b, c \leq 0$
Imamo $a \cdot (b \cdot c) = a * ((-b) * (-c))$.
Dakle,
$$a \cdot (b \cdot c) = a * ((-b) * (-c)). \tag{10}$$
S druge strane imamo $(a \cdot b) \cdot c = (-(a * (-b))) \cdot c = (a * (-b)) * (-c)$.

Dakle,

$$(a \cdot b) \cdot c = (a * (-b)) * (-c). \tag{11}$$

Iz (10) i (11) te asocijativnosti $*$ slijedi $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

8) $a, b, c \leq 0$
Imamo $a \cdot (b \cdot c) = a \cdot ((-b) * (-c)) = -((-a) * ((-b) * (-c)))$.

Dakle,

$$a \cdot (b \cdot c) = -((-a) * ((-b) * (-c))). \tag{12}$$

S druge strane imamo $(a \cdot b) \cdot c = ((-a) * (-b))) \cdot c = -(((-a) * (-b)) * (-c))$.

Dakle,

$$(a \cdot b) \cdot c = -(((-a) * (-b)) * (-c)). \tag{13}$$

Iz (12) i (13) te asocijativnosti $*$ slijedi $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Zaključak:$\cdot$ je asocijativna binarna operacija.
Neka su $a, b, c \in G$. Tvrdimo da je

$$-(a \cdot b) = (-a) \cdot b. \tag{14}$$

Imamo 4 slučaja.

1. $a, b \in G^+$

   Tada je $-(a \cdot b) = -(a * b)$. S druge strane, vrijedi $(-a) \cdot b = -(-(-a) * b) = -(a * b)$. Dakle, $-(a \cdot b) = (-a) \cdot b$.

2. $a \leq 0, b \in G^+$

   Tada je $-(a \cdot b) = -(-((-a) * b)) = (-a) * b = (-a) \cdot b$. Dakle, $-(a \cdot b) = (-a) \cdot b$.

3. $a \in G^+, b \leq 0$

   Imamo $-(a \cdot b) = -(-(a * (-b)) = a * (-b) = a \cdot (-b)$. S druge strane, zbog $-a \leq 0$ imamo $(-a) \cdot b = a * (-b)$. Stoga je $-(a \cdot b) = (-a) \cdot b$.

4. $a, b \leq 0$

   Imamo $-(a \cdot b) = -((-a) * (-b))$. S druge strane, imamo $(-a) \cdot b = -((-a) * (-b))$. Dakle, $-(a \cdot b) = (-a) \cdot b$.

Zaključak: (14) vrijedi za sve $a, b \in G$.
Neka su $a, b \in G$. Tvrdimo da je

$$-(a \cdot b) = a \cdot (-b). \tag{15}$$

Imamo 4 slučaja.

1. $a, b \in G^+$

   Imamo $-(a \cdot b) = -(a * b)$. S druge strane, imamo $a \cdot (-b) = -(a * b)$. Dakle, $-(a \cdot b) = a \cdot (-b)$.

2. $a \leq 0, b \in G^+$

   Imamo $-(a \cdot b) = (-a) * b$. S druge strane, imamo $a \cdot (-b) = (-a) * b$. Dakle, $-(a \cdot b) = a \cdot (-b)$.

3. $a \in G^+, b \leq 0$

   Imamo $-(a \cdot b) = a * (-b)$. S druge strane, imamo $a \cdot (-b) = a * (-b)$. Dakle, $-(a \cdot b) = a \cdot (-b)$.

4. $a, b \leq 0$

   Imamo $-(a \cdot b) = -((-a) * (-b))$. S druge strane, imamo $a \cdot (-b) = -((-a) * (-b))$. Dakle, $-(a \cdot b) = a \cdot (-b)$.

Zaključak: (15) vrijedi za sve $a, b \in G$.

Neka su $a, b \in G$. Koristeći (14) i (15) dobivamo $(-a)\cdot(-b) = -(a\cdot(-b)) = -(-(a\cdot b)) = a \cdot b$. Dakle, $(-a) \cdot (-b) = a \cdot b$ za sve $a, b \in G$.

Pomoćna tvrdnja 1. *Neka su $x, y, z \in G$ takvi da je $x, z \in G^+, y \leq 0$ i $x + y \geq 0$. Tada je $(x + y) \cdot z = x \cdot z + y \cdot z$. Naime, koristeći pretpostavku teorema dobivamo da je $(x + y) * z + (-y) * z = ((x + y) + (-y)) * z = x * z$. Dakle, $(x + y) * z + (-y) * z = x * z$ pa je $(x + y) * z = x * z + (-((-y) * Z))$, tj. $(x + y) \cdot z = x \cdot z + y \cdot z$.*

Pomoćna tvrdnja 2. *Neka su $x, y, z \in G$ takvi da je $x, z \in G^+, y \leq 0$ i $x + y \leq 0$. Tada je $(x + y) \cdot z = x \cdot z + y \cdot z$. Naime, označimo $A = (x + y) \cdot z$ i $B = x \cdot z + y \cdot z$. Želimo dokazati da je $A = B$, a za to je dovoljno dokazati da je $-A = -B$.*

Imamo $-A = -((x + y) \cdot z) = (-(x + y)) \cdot z = (-x + (-y)) \cdot z$. Vrijedi $-x \leq 0, -y \in G^+$ te $-x + (-y) \in G^+$ jer je $x + y \leq 0$. Koristeći prvu pomoćnu tvrdnju dobivamo $-A = (-x + (-y)) \cdot z = (-x) \cdot z + (-y) \cdot z = -(x \cdot z) + (-(y \cdot z)) = -(x \cdot z + y \cdot z) = -B$.

Dakle, $-A = -B$ pa je pomoćna tvrdnja 2 dokazana.

Neka su $a, b, c \in G$. Dokažimo da je

$$(a + b) \cdot c = a \cdot c + b \cdot c. \tag{16}$$

1. slučaj: $c \in G^+$

   a) $a, b \in G^+$

      Imamo $(a + b) \cdot c = (a + b) * c = a * c + b * c = a \cdot c + b \cdot c$. Dakle, (16) vrijedi

b) $a \in G^+, b \leq 0$

Tada iz pomoćne tvrdnje 1 i 2 slijedi da vrijedi (16).

c) $a \leq 0, b \in G^+$

Tada iz pomoćne tvrdnje 1 i 2 slijedi da vrijedi (16).

d) $a, b \leq 0$

Označimo $A = (a + b) \cdot c$ i $B = a \cdot c + b \cdot c$. Imamo $-a, -b \in G^+$ pa koristeći podslučaj a) dobivamo $-A = -(a + b) \cdot c = (-(a + b)) \cdot c = (-a + (-b)) \cdot c = (-a) \cdot c + (-b) \cdot c = -(a \cdot c) + (-(b \cdot c)) = -(a \cdot c + b \cdot c) = -B$.

Dakle, $-A = -B$ pa je $A = B$, tj. vrijedi (16).

2. slučaj: $c \leq 0$

Označimo $A = (a + b) \cdot c$ i $B = a \cdot c + b \cdot c$. Imamo $-c \in G^+$ pa koristeći 1. slučaj dobivamo $-A = -((a+b)\cdot c) = (a+b)\cdot(-c) = a\cdot(-c)+b\cdot(-c) = -(a\cdot c)+(-(b\cdot c)) = -(a \cdot c + b \cdot c) = -B$.

Dakle, $-A = -B$ pa je $A = B$, tj. vrijedi (16).

Pomoćna tvrdnja 3. *Neka su $x, y, z \in G$ takvi da je $x, z \in G^+, y \leq 0$ i $x + y \geq 0$. Tada je $z \cdot (x + y) = z \cdot x + z \cdot y$. Naime, koristeći pretpostavku teorema, dobivamo da je $z * (x + y) + z * (-y) = z * ((x + y) + (-y)) = z * x$. Dakle, $z * (x + y) + z * (-y) = z * x$ pa je $z * (x + y) = z * x + (-(z * (-y)))$, tj. $z \cdot (x + y) = z \cdot x + z \cdot y$.*

Pomoćna tvrdnja 4. *Neka su $x, y, z \in G$ takvi da je $x, z \in G^+, y \leq 0$ i $x + y \leq 0$. Tada je $z\cdot(x+y) = z\cdot x+z\cdot y$. Naime, označimo $A = z\cdot(x+y)$ i $B = z\cdot x+z\cdot y$. Imamo $-x \leq 0, -y \in G^+$ i $-x+(-y) \in G^+$ pa, koristeći pomoćnu tvrdnju 3, dobivamo $-A = -(z\cdot(x+y)) = z\cdot(-(x+y)) = z \cdot (-x + (-y)) = z \cdot (-x) + z \cdot (-y) = -(z \cdot x) + (-(z \cdot y)) = -(z \cdot x + z \cdot y) = -B$. Dakle, $-A = -B$ pa je $A = B$, tj. vrijedi pomoćna tvrdnja.*

Neka su $a, b, c \in G$. Tvrdimo da je

$$c \cdot (a + b) = c \cdot a + c \cdot b. \tag{17}$$

1. slučaj: $c \in G^+$

a) $a, b \in G^+$

Tada iz (1) slijedi da vrijedi (17).

b) $a \in G^+, b \leq 0$ ili $a \leq 0$ i $b \in G^+$

Tada (17) slijedi iz pomoćnih tvrdnji 3. i 4.

c) $a, b \leq 0$

Označimo $A = c \cdot (a + b)$ i $B = c \cdot a + c \cdot b$. Imamo $-a, -b \in G^+$ pa koristeći podslučaj a) dobivamo $-A = -(c \cdot (a + b)) = c \cdot (-(a + b)) = c \cdot ((-a) + (-b)) = c \cdot (-a) + c \cdot (-b) = -(c \cdot a) + (-(c \cdot b)) = -(c \cdot a + c \cdot b) = -B$.

Dakle, $-A = -B$ pa je $A = B$, tj. vrijedi (17).

2. $c \leq 0$

Označimo $A = c \cdot (a + b)$ i $B = c \cdot a + c \cdot b$. Imamo $-c \in G^+$ pa koristeći prvi slučaj dobivamo $-A = -(c \cdot (a+b)) = (-c) \cdot (a+b) = (-c) \cdot a + (-c) \cdot b = -(c \cdot a) + (-(c \cdot b)) = -(c \cdot a + c \cdot b) = -B$.

Dakle, $-A = -B$ pa je $A = B$, tj. vrijedi (17).

Iz (16) i (17) zaključujemo da je $(G, +, \leq)$ prsten.

Neka su $x, y, z \in G$ takvi da je $x \leq y$. Tada je $x + z \leq y + z$ jer je $(G, +, \leq)$ uređena grupa. Nadalje, pretpostavimo da su $x, y \in G$ takvi da je $0 \leq x$ i $0 \leq y$. Tada su $x, y \in G^+$ pa je $x \cdot y = x * y$ te je očito $x \cdot y \in G^+$, dakle $0 \leq x \cdot y$.

Zaključak: $(G, +, \cdot, \leq)$ je uređeni prsten. □

2.5 Množenje prereza

Definicija 2.5.1. *Neka je $(P, +, \cdot, \leq)$ uređeni prsten takav da je $(P, +, \leq)$ gusta Arhimedova grupa. Tada za $(P, +, \cdot, \leq)$ kažemo da je gust Arhimedov prsten.*

Pretpostavimo da je $(P, +, \cdot, \leq)$ gust Arhimedov prsten. Tada je $(P, +, \leq)$ gusta Arhimedova grupa pa je prema 2.3.8 $(\Omega'(P, \leq), \oplus', \preceq')$ uređena grupa.

Definicija 2.5.2. *Podsjetimo se da je Θ neutralni element za $\oplus'$. Definiramo $\Omega^+(P, \leq) = \{(A, B) \in \Omega'(P, \leq) \mid \Theta \preceq' (A, B)\}$.*

Propozicija 2.5.3. *Neka je $(S, \leq)$ uređeni skup te neka je $B \subseteq S$ takav da je $B \neq \emptyset$ i $S \setminus B \neq \emptyset$. Pretpostavimo da za svaki $x \in B$ i svaki $y \in S$ takav da je $x \leq y$ vrijedi $y \in B$. Tada je $(S \setminus B, B)$ prerez u $(S, \leq)$.*

Dokaz. Očito su $S \setminus B$ i B disjunktni neprazni skupovi takvi da je $(S \setminus B) \cup B = S$. Neka je $x \in S \setminus B$ i $y \in B$. Tada je $x < y$. Naime, u suprotnom bi vrijedilo da je $y \leq x$, a što bi prema prethodnoj propoziciji povlačilo da je $x \in B$, a to je nemoguće jer je $x \in S \setminus B$.

Prema tome, $(S \setminus B, B)$ je prerez u $(S, \leq)$. □

Definicija 2.5.4. *Neka je $(P, +, \cdot)$ prsten. Za $A, B \subseteq P$ definiramo*

$$A \cdot B = \{x \cdot y \mid x \in A, y \in B\}.$$

Propozicija 2.5.5. *Neka je* $(P, +, \cdot)$ *prsten te neka su* $A, B, C \subseteq P$. *Tada je*

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

Dokaz. Neka je $x \in (A \cdot B) \cdot C$. Tada postoje $z \in A \cdot B$ i $c \in C$ takvi da je $x = z \cdot c$. Iz $z \in A \cdot B$ slijedi da postoje $a \in A$ i $b \in B$ takvi da je $z = a \cdot b$. Stoga je $x = (a \cdot b) \cdot c = a \cdot (b \cdot c)$ pa je $x \in A \cdot (B \cdot C)$. Stoga je $(A \cdot B) \cdot C \subseteq A \cdot (B \cdot C)$.

Analogno vidimo da je $A \cdot (B \cdot C) \subseteq (A \cdot B) \cdot C$. □

Lema 2.5.6. *Neka je* $(P, +, \cdot)$ *uređeni prsten. Neka su* $a, b \in P$ *takvi da je* $a \leq b$ *te neka je* $c \in P$ *takav da je* $0 \leq c$. *Tada je* $ca \leq cb$ *i* $ac \leq bc$.

Dokaz. Iz $a \leq b$ slijedi $0 \leq b - a$. Iz ovoga, $0 \leq c$ i definicije uređenog prstena slijedi da je $0 \leq c \cdot (b - a)$. Koristeći propoziciju 1.1.19 dobivamo $0 \leq c \cdot b - c \cdot a$ pa je $c \cdot a \leq c \cdot b$.

Analogno dobivamo da je $a \cdot c \leq b \cdot c$. □

Propozicija 2.5.7. *Neka je* $(G, +, \leq)$ *uređena grupa. Neka su* (A, B) *i* (C, D) *prerezi u* $(G, \leq)$. *Tada je* $(G \backslash (B + D), B + D)$ *prerez u* $(G, \leq)$.

Dokaz. Očito je $B + D \neq \emptyset$. Odaberimo $a \in A$ i $c \in C$. Tvrdimo da $a + c \notin B + D$. Pretpostavimo suprotno. Tada postoje $b \in B$ i $d \in D$ takvi da je $a + c = b + d$. Budući da su (A, B) i (C, D) prerezi vrijedi $a < b$ i $c < d$ pa korolar 1.4.2 povlači da je $a + c < b + d$. Ovo je u kontradikciji s $a + c = b + d$. Prema tome, $a + c \notin B + D$ pa je $G \backslash (B + D) \neq \emptyset$.

Pretpostavimo da je $x \in B + D$ te da je $y \in G$ takav da je $x \leq y$. Postoje $b \in B$ i $d \in D$ takvi da je $x = b + d$. Iz $b + d \leq y$ slijedi da je $d \leq y - b$. Ovo povlači da $y - b \notin C$ pa je $y - b \in D$. Označimo $d' = y - b$. Imamo $d' \in D$ i $y = b + d'$. Stoga je $y \in B + D$. Iz propozicije 2.5.3 slijedi da je $(G \backslash (B + D), B + D)$ prerez u $(G, \leq)$. □

Propozicija 2.5.8. *Neka je* $(P, +, \cdot, \leq)$ *uređeni prsten takav da je* $(P, +, \cdot)$ *prsten s jedinicom. Tada je* $0 \leq 1$.

Dokaz. Vrijedi $0 \leq 1$ ili $1 \leq 0$. Pretpostavimo da je $1 \leq 0$. Tada je $0 \leq -1$ pa iz definicije uređenog prstena slijedi da je $0 \leq (-1) \cdot (-1)$. No, $(-1) \cdot (-1) = 1 \cdot 1 = 1$. Dakle, $0 \leq 1$.

Time je tvrdnja propozicije dokazana. □

Korolar 2.5.9. *Neka je* $(P, +, \cdot, \leq)$ *uređeno polje. Tada je* $0 < 1$.

Dokaz. Prema prethodnoj propoziciji vrijedi $0 \leq 1$. Pretpostavimo da je $0 = 1$. Neka je $x \in P$. Imamo $x = 1 \cdot x = 0 \cdot x = 0$. Dakle, $x = 0$ za svaki $x \in P$ pa je $P = \{0\}$. Ovo je nemoguće, naime skup P, prema definiciji polja, ima bar 2 elementa. Stoga je $0 \neq 1$ pa je $0 < 1$. □

Propozicija 2.5.10. *Neka je* $(P, +, \cdot)$ *polje. Neka su* $x, y \in P$ *takvi da je* $x \neq 0$ *i* $y \neq 0$. *Tada je* $x \cdot y \neq 0$. *Nadalje, vrijedi* $-x \neq 0$ *te* $(-x)^{-1} = -x^{-1}$.

Dokaz. Pretpostavimo da je $x \cdot y = 0$. Tada je $x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0$. Stoga je $(x^{-1} \cdot x) \cdot y = 0$, tj. $1 \cdot y = 0$. To je u kontradikciji s pretpostavkom propozicije. Iz $-x = 0$ bi zbog $x + (-x) = 0$ slijedilo $x = 0$ što je nemoguće. Prema tome, $-x = 0$. Imamo $(-x) \cdot (-x^{-1}) = x \cdot x^{-1} = 1$.

Dakle, $(-x) \cdot (-x^{-1}) = 1$ pa je $-x^{-1} = (-x)^{-1}$. □

Propozicija 2.5.11. *Neka je* $(P, +, \cdot, \leq)$ *uređeno polje.*

1) Neka su $x, y \in P$ *takvi da je* $0 < x$ *i* $0 < y$. *Tada je* $0 < x \cdot y$.

2) Neka su $a, b, c \in P$ *takvi da je* $a < b$ *i* $0 < c$. *Tada je* $ac < bc$.

3) Neka je $x \in P$ *takav da je* $0 < x$. *Tada je* $0 < x^{-1}$.

4) Neka je $x \in P$ *takav da je* $x < 0$. *Tada je* $x^{-1} < 0$.

Dokaz. 1) Iz definicije uređenog prstena slijedi $0 \leq x \cdot y$, a iz prethodne propozicije slijedi da je $0 \neq x \cdot y$. Prema tome, $0 < x \cdot y$.

2) Koristeći propoziciju 1.1.19 dobivamo da je $0 < b - a$. Ovo, zajedno s $0 < c$ i tvrdnjom 1), daje $0 < c \cdot (b - a)$, tj. $0 < c \cdot b - c \cdot a$ pa je $ca < cb$.

3) Pretpostavimo suprotno. Tada je $x^{-1} \leq 0$. Kada bi vrijedilo $x^{-1} = 0$ onda bi slijedilo $x \cdot x^{-1} = x \cdot 0$, tj. $1 = 0$ što je nemoguće. Prema tome, $x^{-1} < 0$. Sada iz tvrdnje 2) slijedi $x^{-1} < x \cdot 0$, tj. $1 < 0$, što je u kontradikciji s korolarom 2.5.9.

4) Iz $x < 0$ slijedi $0 < -x$ pa tvrdnja 3) povlači $0 < (-x)^{-1}$. Stoga je, prema propoziciji 2.5.10, $0 < -x^{-1}$. Slijedi $x^{-1} < 0$.

□

Propozicija 2.5.12. *Neka je* $(P, +, \cdot, \leq)$ *uređeno polje te neka su* (A_1, A) *i* (B_1, B) *prerezi u* $(P, \leq)$ *takvi da je* $0 \leq x$, *za svaki* $x \in A \cup B$. *Tada je* $(P \backslash (A \cdot B), A \cdot B)$ *prerez u* $(P, \leq)$.

Dokaz. Imamo $A \neq \emptyset$ i $B \neq \emptyset$ pa je očito $A \cdot B \neq \emptyset$. Iz prethodnog korolara slijedi da je $0 < 1$ pa je $-1 < 0$. Za svaki $a \in A$ i za svaki $b \in B$ vrijedi $0 \leq a$ i $0 \leq b$ pa je $0 \leq a \cdot b$. Prema tome, $0 \leq x$ za svaki $x \in A \cdot B$. Iz ovoga zaključujemo da $-1 \notin A \cdot B$.

Prema tome, $A \cdot B \neq P$ pa je $P \backslash (A \cdot B) \neq \emptyset$. Pretpostavimo da je $x \in A \cdot B$ te da je $y \in P$ takav da je $x \leq y$. Tvrdimo da je $y \in A \cdot B$. Vrijedi $x = a \cdot b$, gdje je $a \in A, b \in B$. Imamo 3 slučaja.

1. $0 < a$

   Tada je, prema prethodnoj propoziciji, $0 < a^{-1}$. Iz $a \cdot b \leq y$ i leme 2.5.6 slijedi $a^{-1}(a \cdot b) \leq a^{-1} \cdot y$, tj. $b \leq a^{-1} \cdot y$. Budući da je (B_1, B) prerez i $b \in B$ imamo $a^{-1} \cdot y \in B$. Označimo $b' = a^{-1} \cdot y$. Tada je $b' \in B$ i $y = a \cdot b'$ pa zaključujemo da je $y \in A \cdot B$.

2. $0 < b$

   Analogno zaključujemo da je $y \in A \cdot B$.

3. $a = 0$ i $b = 0$

   Tada je $a \cdot b = 0$ pa je $0 \leq y$, tj. $a \leq y$. Budući da je (A_1, A) prerez, imamo $y \in A$. Nadalje, zbog $0 < 1$ vrijedi $b < 1$ pa je $1 \in B$. Stoga je $y \cdot 1 \in A \cdot B$, tj. $y \in A \cdot B$.

U svakom slučaju vrijedi $y \in A \cdot B$. Iz propozicije 2.5.3 slijedi da je $(P\backslash(A \cdot B), A \cdot B)$ prerez u $(P, \leq)$. □

Propozicija 2.5.13. *Neka je $(P, +, \cdot)$ uređeno polje. Neka su $(A_1, A), (B_1, B)$ i (C_1, C) prerezi u $(P, \leq)$ takvi da je $0 \leq x$, za svaki $x \in A \cup B \cup C$. Tada je $C \cdot (A + B) = C \cdot A + C \cdot B$.*

Dokaz. Neka je $x \in C \cdot (A + B)$. Tada postoje $c \in C, a \in A$ i $b \in B$ takvi da je $x = c \cdot (a + b)$. Slijedi $x = c \cdot a + c \cdot b$ pa je $x \in C \cdot A + C \cdot B$. Dakle, $C \cdot (A + B) \subseteq C \cdot A + C \cdot B$.

Obratno, neka je $x \in C \cdot A + C \cdot B$. Tada postoje $u \in C \cdot A$ i $v \in C \cdot B$ takvi da je $x = u + v$. Slijedi da postoje $c_1 \in C$ i $a \in A$ takvi da je $u = c_1 \cdot a$ te da postoje $c_2 \in C$ i $b \in B$ takvi da je $v = c_2 \cdot b$.

Imamo 2 slučaja.

1. $c_1 \leq c_2$

   Imamo $0 \leq b$ pa iz leme 2.5.6 slijedi $c_1 \cdot b \leq c_2 \cdot b$. Imamo $c_1 \cdot (a + b) = c_1 \cdot a + c_1 \cdot b \leq c_1 \cdot a + c_2 \cdot b = u + v = x$. Dakle, $c_1 \cdot (a + b) \leq x$. Po propoziciji 2.5.7, $(P\backslash(A + B), A + B)$ je prerez u $(P, \leq)$. Iz propozicije 2.5.12 slijedi da je $(P\backslash(C \cdot (A + B)), C \cdot (A + B))$ prerez. Očito je $c_1 \cdot (a + b) \in C \cdot (A + B)$ pa iz $c_1 \cdot (a + b) \leq x$ slijedi da je $x \in C \cdot (A + B)$.

2. $c_2 \leq c_1$

   Dokazuje se analogno prvom slučaju.

Time smo dokazali da je $C \cdot A + C \cdot B \subseteq C \cdot (A + B)$. Stoga je $C \cdot (A + B) = C \cdot A + C \cdot B$.
□

Poglavlje 3

Dobri prerezi

3.1 Veza pravih i dobrih prereza

Definicija 3.1.1. *Neka je* $(S, \leq)$ *uređeni skup,* $A \subseteq S$ *te* $a_0 \in A$. *Kažemo da je* a_0 *najmanji element skupa* A *u* $(S, \leq)$ *ako je* $a_0 \leq a$, *za svaki* $a \in A$.

Definicija 3.1.2. *Neka je* $(S, \leq)$ *uređeni skup te neka je* (A, B) *prerez u* $(S, \leq)$. *Kažemo da je* (A, B) *dobar prerez u* $(S, \leq)$ *ako* B *nema najmanji element u* $(S, \leq)$.

Propozicija 3.1.3. *Neka je* $(G, +, \leq)$ *uređena grupa. Neka su* (A, B) *i* (C, D) *dobri prerezi u* $(G, \leq)$. *Tada je* $(G\backslash(B + D), B + D)$ *dobar prerez u* $(G, \leq)$.

Dokaz. Znamo da je $(G\backslash(B + D), B + D)$ prerez u $(G, \leq)$ (prema propoziciji 2.5.7). Pretpostavimo da $B + D$ ima najmanji element u $(G, \leq)$. Tada postoje $b_0 \in B$ i $d_0 \in D$ takvi da je $b_0 + d_0$ najmanji element od $B + D$ u $(G, \leq)$. Neka je $b \in B$. Tada je $b + d_0 \in B + D$. Stoga je $b_0 + d_0 \leq b + d_0$, Što povlači da je $b_0 \leq b$. Ovo znači da je b_0 najmanji element od B što je nemoguće.

Zaključak: $B + D$ nema najmanji element pa je $(G\backslash(B + D), B + D)$ dobar prerez u $(G, \leq)$. □

Definicija 3.1.4. *Neka je* $(S, \leq)$ *uređeni skup. Tada sa* $\Gamma(S, \leq)$ *označavamo skup svih dobrih prereza u* $(S, \leq)$.

Ako je $(G, +)$ *Abelova grupa i* $A \subseteq G$, *Onda definiramo* $-A = \{-a \,|\, a \in A\}$. *Uočimo da je* $-(-A) = A$.

Lema 3.1.5. *Neka je* $(G, +, \leq)$ *uređena grupa.*

1) Pretpostavimo da je (A, B) *pravi prerez u* $(G, \leq)$. *Tada je* $(-B, -A)$ *dobar prerez u* $(G, \leq)$.

2) Neka je (C, D) dobar prerez u $(G, \leq)$. Tada postoji pravi prerez (A, B) takav da je $(-B, -A) = (C, D)$.

Dokaz. 1) Budući da su A i B neprazni skupovi, imamo da su $-A$ i $-B$ neprazni skupovi. Neka su $a \in A$ i $b \in B$. Tada je $a < b$ pa je $-b < -a$. Dakle, za svaki $x \in -B$ i za svaki $y \in -A$ vrijedi $x < y$. Ovo također povlači da je $A \cap B = \emptyset$. Neka je $x \in G$. Tada je $-x \in G$ pa je $-x \in A$ ili $-x \in B$, što povlači da je $x \in -B$ ili $x \in -A$. Ovo pokazuje da je $G = (-B) \cup (-A)$. Zaključak: $(-B, -A)$ je prerez u $(G, \leq)$.

Dokažimo da je $(-B, -A)$ dobar prerez. Pretpostavimo da $-A$ ima najmanji element. Dakle, postoji $a_0 \in A$ takav da je $-a_0$ najmanji element od $-A$. Za svaki $a \in A$ vrijedi $-a \in -A$ pa je $-a_0 \leq a$, što povlači da je $a \leq a_0$. Iz ovoga slijedi da je a_0 najveći element od A, što je u kontradikciji s činjenicom da je (A, B) pravi prerez.

Prema tome, $-A$ nema najmanji element, dakle, $(-B, -A)$ je dobar prerez.

2) Neka je (C, D) dobar prerez u $(G, \leq)$. Definiramo $A = -D$ i $B = -C$. Tvrdimo da je (A, B), tj. $(-D, -C)$ pravi prerez u $(G, \leq)$. Na isti način kao u 1) dobivamo da je $(-D, -C)$ prerez.

Pretpostavimo da $-D$ ima najveći element. Dakle, postoji $d_0 \in D$ takav da je $-d_0$ najveći element od $-D$. Stoga za svaki $d \in D$ vrijedi $-d \leq -d_0$ pa je $d_0 \leq d$. Dakle, d_0 je najmanji element od D, što je nemoguće jer je (C, D) dobar prerez. Prema tome, $-D$ nema najveći element pa je $(-D, -C)$ pravi prerez u $(G, \leq)$.

Dakle, (A, B) je pravi prerez u $(G, \leq)$ i očito je $(-B, -A) = (C, D)$.

□

Propozicija 3.1.6. *Neka je $(G, +, \leq)$ uređena grupa te neka je $\gamma : \Omega'(G, \leq) \to \Gamma(G \leq)$ funkcija definirana s $\gamma(A, B) = (-B, -A)$. Tada je γ bijekcija.*

Dokaz. Uočimo prije svega da je prema tvrdnji 1) prethodne propozicije γ dobro definirana funkcija. Neka je $(C, D) \in \Gamma(G, \leq)$. Prema tvrdnji 2) prethodne propozicije postoji $(A, B) \in \Omega'(G, \leq)$ takav da je $(-B, -A) = (C, D)$, tj. $\gamma(A, B) = (C, D)$. Prema tome, γ je surjekcija.

Neka su $(A_1, B_1), (A_2, B_2) \in \Omega'(G, \leq)$ takvi da je $\gamma(A_1, B_1) = \gamma(A_2, B_2)$. Tada je $(-B_1, -A_1) = (-B_2, -A_2)$ pa je $-B_1 = -B_2$ i $-A_1 = -A_2$. Stoga je $B_1 = B_2$ i $A_1 = A_2$, dakle, $(A_1, B_1) = (A_2, B_2)$. Prema tome, γ je injekcija.

Zaključak: γ je bijekcija. □

Napomena 3.1.7. *Neka je $(G, +)$ grupa te neka su $A, B \subseteq G$. Tada je $-(A + B) = -A + (-B)$. Naime, ako je $x \in -(A + B)$ onda postoje $a \in A$ i $b \in B$ takvi da je $x = -(a + b)$. Slijedi $x = -a + (-b)$ pa je očito $x \in -A + (-B)$. Prema tome, $-(A + B) \subseteq -A + (-B)$. Na sličan način vidimo da je $-A + (-B) \subseteq -(A + B)$.*

Definicija 3.1.8. *Neka je $\cdot$ binarna operacija na skupu G. Tada za uređeni par $(G, \cdot)$ kažemo da je grupoid.*

Definicija 3.1.9. *Neka su $(G, \cdot)$ i $(H, *)$ grupoidi. Za funkciju $f : G \to H$ kažemo da je morfizam grupoida ako za sve $x, y \in G$ vrijedi $f(x \cdot y) = f(x) * f(y)$.*

Ako je f još i bijekcija onda kažemo da je f izomorfizam grupoida $(G, \cdot)$ i $(H, *)$.

Propozicija 3.1.10. *Neka su $(G, \cdot)$ i $(H, *)$ grupoidi te neka je $f : G \to H$ izomorfizam ovih grupoida.*

1) Ako je $(G, \cdot)$ polugrupa onda je $(H, *)$ polugrupa.

2) Ako je $(G, \cdot)$ monoid onda je $(H, *)$ monoid. Pri tome je $f(e)$ neutralni element za operaciju $*$ ako je e neutralni element za operaciju $\cdot$.

3) Ako je $(G, \cdot)$ grupa onda je $(H, *)$ grupa.

4) Ako je $\cdot$ komutativna operacija onda je $*$ komutativna operacija.

Dokaz. 1) Pretpostavimo da je $(G, \cdot)$ polugrupa. Neka su $h_1, h_2, h_3 \in H$. Tada postoje $g_1, g_2, g_3 \in G$ takvi da je $h_1 = f(g_1), h_2 = f(g_2)$ i $h_3 = f(g_3)$. Znamo da je $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$, stoga je $f((g_1 \cdot g_2) \cdot g_3) = f(g_1 \cdot (g_2 \cdot g_3))$ pa je $f(g_1 \cdot g_2) * f(g_3) = f(g_1) * f(g_2 \cdot g_3)$, tj. $(f(g_1) * f(g_2)) * f(g_3) = f(g_1) * (f(g_2) * f(g_3))$. Prema tome, $(h_1 * h_2) * h_3 = h_1 * (h_2 * h_3)$.

Zaključujemo da je $(H, *)$ polugrupa.

2) Pretpostavimo da je $(G, \cdot)$ monoid. Tada je $(G, \cdot)$ polugrupa pa iz 1) slijedi da je $(H, *)$ polugrupa. Neka je e neutralni element za operaciju $\cdot$. Neka je $h \in H$. Tada postoji $g \in G$ takav da je $h = f(g)$. Vrijedi $h * f(e) = f(g) * f(e) = f(g \cdot e) = f(g) = h$, dakle, $h * f(e) = h$. Analogno dobivamo da je $f(e) * h = h$. Prema tome, $f(e)$ je neutralni element za operaciju $*$.

3) Pretpostavimo da je $(G, \cdot)$ grupa. Neka je e neutralni element za $\cdot$. Znamo da je tada $f(e)$ neutralni element za $*$. Nadalje, znamo da je $(H, *)$ monoid. Neka je $h \in H$. Tada postoji $g \in G$ takav da je $h = f(g)$. Definiramo $h' = f(g^{-1})$. Imamo $h * h' = f(g) * f(g^{-1}) = f(g \cdot g^{-1}) = f(e)$, dakle, $h * h' = f(e)$. Analogno dobivamo da je $h' * h = f(e)$. Prema tome, h' je inverzni element od h u monoidu $(H, *)$.

Zaključak: $(H, *)$ je grupa.

4) Pretpostavimo da je operacija $\cdot$ komutativna. Neka su $h_1, h_2 \in H$. Tada postoje $g_1, g_2 \in G$ takvi da je $h_1 = f(g_1), h_2 = f(g_2)$. Imamo $h_1 * h_2 = f(g_1) * f(g_2) = f(g_1 \cdot g_2) = f(g_2 \cdot g_1) = f(g_2) * f(g_1) = h_2 * h_1$, dakle, $h_1 * h_2 = h_2 * h_1$.

Prema tome, operacija $*$ je komutativna.

□

3.2 Zbrajanje dobrih prereza

Definicija 3.2.1. *Neka je* $(G, +, \leq)$ *uređena grupa. Na* $\Gamma(G, \leq)$ *definiramo binarnu operaciju* $+$ *sa* $(A, B) + (C, D) = (G\backslash(B + D), B + D)$. *Ova definicija je dobra prema propoziciji 3.1.3*

Propozicija 3.2.2. *Neka je* $(G, +, \leq)$ *uređena grupa. Tada je funkcija* $\gamma : \Omega'(G, \leq) \to \Gamma(G, \leq)$ *definirana s* $\gamma(A, B) = (-B, -A)$ *izomorfizam grupoida* $(\Omega'(G, \leq), \oplus')$ *i* $(\Gamma(G, \leq), +)$.

Dokaz. Prema propoziciji 3.1.6 funkcija γ je bijekcija. Neka su $(A, B), (C, D) \in \Omega'(G, \leq)$. Imamo $\gamma((A, B) \oplus' (C, D)) = \gamma((A + C, G\backslash(A + C))) = (-G\backslash(A + C), -(A + C))$. S druge strane,

$$\gamma(A, B) + \gamma(C, D) = (-B, -A) + (-D, -C) = (G\backslash(-A + (-C)), -A + (-C)). \tag{1}$$

Tvrdimo da je $\gamma((A, B) \oplus' (C, D)) = \gamma(A, B) + \gamma(C, D)$. Prema prethodnim jednakostima dovoljno je dokazati da je $(-G\backslash(A + C), -(A + C)) = (G\backslash(-A + (-C)), -A + (-C))$. Budući da je riječ o prerezima, dovoljno je dokazati da je

$$-(A + C) = -A + (-C). \tag{2}$$

Pretpostavimo da je $x \in -(A + C)$. Tada postoje $a \in A$ i $c \in C$ takvi da je $x = -(a + c)$. Slijedi $x = -a + (-c)$ pa je očito $x \in -A + (-C)$. Prema tome $-(A + C) \subseteq -A + (-C)$. Analogno dobivamo da je $-A + (-C) \subseteq -(A + C)$. Prema tome, vrijedi (2). Stoga je γ morfizam grupoida $(\Omega'(G, \leq), \oplus')$ i $(\Gamma(G, \leq), +)$.

Time je tvrdnja dokazana. □

Korolar 3.2.3. *Neka je* $(G, +, \leq)$ *gusta Arhimedova grupa. Tada je* $(\Gamma(G, \leq), +)$ *Abelova grupa. Neka je* $\Theta' = (\{y \in G \mid y \leq 0\}, \{y \in G \mid 0 < y\})$. *Tada je* Θ' *neutralni element za operaciju* $+$.

Dokaz. Prema teoremu 2.3.7, $(\Omega'(G, \leq), \oplus')$ je grupa. Očito je operacija $\oplus'$ komutativna. Neka je $\gamma : \Omega'(G, \leq) \to \Gamma(G, \leq)$ funkcija definirana s $\gamma(A, B) = (-B, -A)$. Prema prethodnoj propoziciji γ je izomorfizam grupoida $(\Omega'(G, \leq), \oplus')$ i $(\Gamma(G, \leq), +)$. Iz propozicije 3.1.10 slijedi da je $(\Gamma(G, \leq), +)$ grupa te da je $+$ komutativna operacija na $\Gamma(G, \leq)$. Stoga je $(\Gamma(G, \leq), +)$ Abelova grupa.

Znamo da je $\Theta = (\{x \in G \mid x < 0\}, \{x \in G \mid 0 \leq x\})$ neutralni element za operaciju $\oplus'$. Iz tvrdnje 2) propozicije 3.1.10 slijedi da je $\gamma(\Theta)$ neutralni element za operaciju $+$. Dokažimo da je $\gamma(\Theta) = \Theta'$.

Vrijedi $\gamma(\Theta) = (-\{x \in G \mid 0 \leq x\}, -\{x \in G \mid x < 0\})$. Budući da su $\gamma(\Theta)$ i Θ' prerezi dovoljno je dokazati da su im prve komponente jednake, tj.

$$-\{x \in G \mid 0 \leq x\} = \{y \in G \mid y \leq 0\}. \tag{1}$$

Neka je $z \in -\{x \in G \mid 0 \leq x\}$. Tada postoji $x \in G$ takav da je $0 \leq x$ te da je $z = -x$. Iz $0 \leq x$ slijedi $-x \leq 0$, tj. $z \leq 0$. Stoga je $z \in \{y \in G \mid y \leq 0\}$.

Obratno, pretpostavimo da je $z \in \{y \in G \mid y \leq 0\}$. Tada je $z \leq 0$ pa je $0 \leq -z$. Definiramo $x = -z$. Tada je $0 \leq x$, a iz $z = -(-z)$ slijedi $z = -x$. Stoga je $z \in -\{x \in G \mid 0 \leq x\}$.

Time smo dokazali da (1) vrijedi pa je tvrdnja korolara dokazana. □

Lema 3.2.4. *Neka je X skup te neka su $A, B \subseteq X$. Tada je $A \subseteq B \Leftrightarrow X\backslash B \subseteq X\backslash A$.*

Dokaz. Pretpostavimo da je $A \subseteq B$. Neka je $y \in X\backslash B$. Tada $y \notin A$ (kada bi vrijedilo $y \in A$ onda bi zbog $A \subseteq B$ vrijedilo $y \in B$, što je nemoguće). Stoga je $y \in X\backslash A$. Prema tome, $X\backslash B \subseteq X\backslash A$.

Obratno, pretpostavimo da je $X\backslash B \subseteq X\backslash A$. Pretpostavimo da je $y \in A$. Kada bi vrijedilo $y \notin B$, onda bismo imali $y \in X\backslash B$ pa bi slijedilo $y \in X\backslash A$, tj. $y \notin A$, što je nemoguće.

Prema tome, $y \in B$ i time smo dokazali da je $A \subseteq B$. □

Propozicija 3.2.5. *Neka je $(S, \leq)$ uređeni skup te neka su (A, B) i (C, D) prerezi u $(S, \leq)$. Tada je $(A, B) \leq (C, D)$ ako i samo ako je $D \subseteq B$.*

Dokaz. Vrijedi $B = S\backslash A$ i $D = S\backslash C$. Koristeći prethodnu lemu dobivamo

$$(A, B) \leq (C, D) \Leftrightarrow A \subseteq C \Leftrightarrow S\backslash C \subseteq S\backslash A \Leftrightarrow D \subseteq B.$$

□

Definicija 3.2.6. *Neka je $(S, \leq)$ uređeni skup. Neka je $\leq''$ binarna relacija na $\Gamma(S, \leq)$ određena sa $\leq$ (podsjetimo se da je $\leq$ binarna relacija na $\Omega(S, \leq)$). Iz napomene 2.1.4 slijedi da je $\leq''$ uređaj na $\Gamma(S, \leq)$.*

Propozicija 3.2.7. *Neka je $(G, +, \leq)$ gusta Arhimedova grupa. Tada je $(\Gamma(G, \leq), +, \leq'')$ uređena grupa.*

Dokaz. Znamo da je $(\Gamma(G, \leq), +)$ Abelova grupa. Preostaje dokazati da za sve $a, b, c \in \Gamma(G, \leq)$ takve da je $a \leq'' b$ vrijedi $a + c \leq'' b + c$. Neka su $(A, B), (C, D), (E, F) \in \Gamma(G, \leq)$ takvi da je $(A, B) \leq'' (C, D)$. Tada iz prethodne propozicije slijedi da je $D \subseteq B$. Lako se vidi (kao u dokazu propozicije 1.4.11) da je $D + F \subseteq B + F$. Imamo $(A, B) + (E, F) = (G\backslash(B + F), B + F)$ i $(C, D) + (E, F) = (G\backslash(D + F), D + F)$ pa iz prethodne propozicije slijedi da je $(A, B) + (E, F) \leq'' (C, D) + (E, F)$.

Prema tome, $(\Gamma(G, \leq), +, \leq'')$ je uređena grupa. □

3.3 Množenje dobrih prereza

Propozicija 3.3.1. *Neka je $(P, +, \cdot, \leq)$ uređeno polje. Neka su $a, b, c, d \in P$ takvi da je $0 \leq a < b$ i $0 \leq c < d$. Tada je $a \cdot c < b \cdot d$.*

Dokaz. Iz $a < b$ i $0 \leq c$ te leme 2.5.6 slijedi $a \cdot c \leq b \cdot c$. Nadalje, iz $0 < b$ i $c < d$ te tvrdnje 2) propozicije 2.5.11 slijedi $b \cdot c < b \cdot d$. Stoga je $a \cdot c < b \cdot d$. □

Definicija 3.3.2. *Neka je $(G, +, \leq)$ uređena grupa. Definiramo*

$$\Gamma^+(G, +, \leq) = \{(A_1, A) \in \Gamma(G, \leq) \mid \Theta' \preceq'' (A_1, A)\}.$$

Podsjetimo se da je $\Theta' = (\{y \in G \mid y \leq 0\}, \{y \in G \mid 0 < y\})$. Stoga iz propozicije 3.2.5 zaključujemo da za svaki $(A_1, A) \in \Gamma(G, \leq)$ vrijedi sljedeće:

$$(A_1, A) \in \Gamma^+(G, +, \leq) \Leftrightarrow A \subseteq \{y \in G \mid 0 < y\}. \tag{1}$$

Propozicija 3.3.3. *Neka je $(P, +, \cdot, \leq)$ uređeno polje. Neka su $(A_1, A), (B_1, B) \in \Gamma^+(P, +, \leq)$. Tada je $(P \backslash (A \cdot B), A \cdot B) \in \Gamma^+(P, +, \leq)$.*

Dokaz. Prema (1) dovoljno je dokazati sljedeće:

$$(P \backslash A \cdot B, A \cdot B) \in \Gamma(P, \leq) \tag{2}$$

i

$$A \cdot B \subseteq \{y \in P \mid 0 < y\}. \tag{3}$$

Iz (1) slijedi da je $A \subseteq \{y \in P \mid 0 < y\}$ i $B \subseteq \{y \in P \mid 0 < y\}$. Neka su $a \in A$ i $b \in B$. Tada je $0 < a$ i $0 < b$ pa iz tvrdnje 1) propozicije 2.5.11 slijedi da je $0 < a \cdot b$. Time smo dokazali da vrijedi (3).

Dokažimo sada (2). Iz propozicije 2.5.12 slijedi da je $(P \backslash (A \cdot B), A \cdot B)$ prerez u $(P, \leq)$. Preostaje dokazati da je to dobar prerez u $(P, \leq)$. Pretpostavimo suprotno. Tada $A \cdot B$ ima najmanji element u $(P, \leq)$ pa postoji $m \in A \cdot B$ takav da je

$$m \leq x \text{ za svaki } x \in A \cdot B. \tag{4}$$

Iz $m \in A \cdot B$ slijedi da je $m = a_0 \cdot b_0$ za neke $a_0 \in A$ i $b_0 \in B$. Budući da je (A_1, A) dobar prerez u $(P, \leq)$, skup A nema najmanji element pa postoji $a \in A$ takav da je $a < a_0$. Na isti način zaključujemo da postoji $b \in B$ takav da je $b < b_0$. Znamo da je $0 < a$ i $0 < b$. Iz prethodne propozicije slijedi da je $a \cdot b < a_0 \cdot b_0$, tj. $a \cdot b < m$, a očito je $a \cdot b \in A \cdot B$. Ovo je u kontradikciji s (4). Prema tome, $(P \backslash (A \cdot B), A \cdot B)$ je dobar prerez u $(P, \leq)$.

Dakle, vrijedi (2). Time je tvrdnja propozicije dokazana. □

Propozicija 3.3.4. *Neka je $(P, +, \cdot, \leq)$ uređeno polje. Neka je $*$ binarna operacija na $\Gamma^+(P, +, \leq)$ definirana s $(A_1, A) * (B_1, B) = (P\backslash(A \cdot B), A \cdot B)$. Tada je binarna operacija $*$ asocijativna.*

Dokaz. Neka su $(A_1, A), (B_1, B), (C_1, C) \in \Gamma^+(P, +, \leq)$. Imamo

$$((A_1, A) * (B_1, B)) * (C_1, C) = (P\backslash(A \cdot B), A \cdot B) * (C_1, C) = (P\backslash((A \cdot B) \cdot C), (A \cdot B) \cdot C),$$

$$(A_1, A) * ((B_1, B) * (C_1, C)) = (A_1, A) * (P\backslash(B \cdot C), B \cdot C) = (P\backslash(A \cdot (B \cdot C)), A \cdot (B \cdot C)).$$

Prema propoziciji 2.5.5 vrijedi $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ pa je

$$(P\backslash((A \cdot B) \cdot C), (A \cdot B) \cdot C) = (P\backslash(A \cdot (B \cdot C)), A \cdot (B \cdot C)).$$

Time je tvrdnja dokazana. □

Propozicija 3.3.5. *Neka je P skup, neka su $+, \cdot$ i $\cdot'$ binarne operacije na skupu P te neka je $\leq$ uređaj na P. Pretpostavimo da su $(P, +, \cdot, \leq)$ i $(P, +, \cdot', \leq)$ uređeni prsteni. Nadalje, pretpostavimo da za sve $x, y \in P$ takve da je $0 \leq x$ i $0 \leq y$ vrijedi $x \cdot y = x \cdot' y$. Pri tome je 0 neutralni element za operaciju $+$. Tada su binarne operacije $\cdot$ i $\cdot'$ jednake.*

Dokaz. Neka su $x, y \in P$. Tvrdimo da je

$$x \cdot y = x \cdot' y. \tag{1}$$

Imamo nekoliko slučajeva:

1) $0 \leq x$ i $0 \leq y$

   Tada (1) vrijedi prema pretpostavci.

2) $x \leq 0$ i $0 \leq y$

   Tada je $0 \leq -x$ i $0 \leq y$ pa, koristeći propoziciju 1.1.17, dobivamo

   $$-(x \cdot y) = (-x) \cdot y = (-x) \cdot' y = -(x \cdot' y).$$

   Dakle, $-(x \cdot y) = -(x \cdot' y)$ pa je $x \cdot y = x \cdot' y$.

3) $0 \leq x$ i $y \leq 0$

   Tada je $0 \leq -y$ pa imamo $-(x \cdot y) = x \cdot (-y) = x \cdot' (-y) = -(x \cdot' y)$ pa je $-(x \cdot y) = -(x \cdot' y)$.

4) $x \leq 0$ i $y \leq 0$

   Tada je $0 \leq -x$ i $0 \leq -y$. Vrijedi

   $$x \cdot y = (-x) \cdot (-y) = (-x) \cdot' (-y) = x \cdot' y.$$

Time je tvrdnja propozicije dokazana. □

Teorem 3.3.6. *Neka je* $(P,+,\cdot,\leq)$ *uređeno polje takvo da je* $(P,+,\leq)$ *gusta Arhimedova grupa. Tada postoji jedinstvena binarna operacija* $\cdot$ *na* $\Gamma(P,\leq)$ *takva da je* $(\Gamma(P,\leq),+,\cdot,\leq'')$ *uređeni prsten te takva da je* $(A_1,A)\cdot(B_1,B)=(P\backslash(A\cdot B),A\cdot B)$*, za sve* $(A_1,A),(B_1,B)\in\Gamma^+(P,+,\leq)$.

Dokaz. Prema propoziciji 3.2.7, $(\Gamma(P,\leq),+,\leq'')$ je uređena grupa. Nadalje, prema propoziciji 3.3.4 binarna operacija $*$ na $\Gamma^+(P,+,\leq)$ definirana s $(A_1,A)*(B_1,B)=(P\backslash(A\cdot B),A\cdot B)$ je asocijativna.

Neka su $\alpha,\beta,\gamma\in(P\backslash A\cdot B,A\cdot B)$. Imamo $\alpha=(A_1,A),\beta=(B_1,B),\gamma=(C_1,C)$. Dokažimo da je

$$(\alpha+\beta)*\gamma=\alpha*\gamma+\beta*\gamma. \tag{1}$$

Vrijedi

$$(\alpha+\beta)*\gamma=(P\backslash(A+B),A+B)*\gamma=(P\backslash(A+B)\cdot C,(A+B)\cdot C). \tag{2}$$

S druge strane imamo

$$\alpha*\gamma+\beta*\gamma=(P\backslash(A\cdot C),A\cdot C)+(P\backslash(B\cdot C),B\cdot C)=(P\backslash(A\cdot B+B\cdot C),A\cdot B+B\cdot C).$$

Dakle,

$$\alpha*\gamma+\beta*\gamma=(P\backslash(A\cdot C+B\cdot C),A\cdot C+B\cdot C). \tag{3}$$

Da bismo dokazali (1) dovoljno je, prema (2) i (3) dokazati da je $(A+B)\cdot C=A\cdot C+B\cdot C$. Iz $(A_1,A)\in\Gamma^+(P,+,\leq)$ imamo $\Theta'\leq''(A_1,A)$ pa je prema propoziciji 3.2.5 $A\subseteq\{x\in P\,|\,0<x\}$. Analogno dobivamo da su i skupovi B i C podskupovi od $\{x\in P\,|\,0<x\}$.

Dakle, za svaki $x\in A\cup B\cup C$ vrijedi $0<x$. Iz propozicije 2.5.13 slijedi da je $(A+B)\cdot C=A\cdot C+B\cdot C$. Prema tome, vrijedi (1).

Operacija $*$ je očito komutativna pa vrijedi

$$\gamma*(\alpha+\beta)=(\alpha+\beta)*\gamma=\alpha*\gamma+\beta*\gamma=\gamma*\alpha+\gamma*\beta.$$

Dakle, $\gamma*(\alpha+\beta)=\gamma*\alpha+\gamma*\beta$.

Iz teorema 2.4.1 slijedi da postoji binarna operacija $\cdot$ na $\Gamma(P,\leq)$ takva da je $(\Gamma(P,\leq),+,\cdot,\leq'')$ uređeni prsten te $\alpha\cdot\beta=\alpha*\beta$, za sve $\alpha,\beta\in\Gamma^+(P,+,\leq)$.

Time je tvrdnja propozicije dokazana. □

Ubuduće ćemo kada govorimo o uređenom polju $(P,+,\cdot,\leq)$ takvom da je $(P,+,\leq)$ gusta Arhimedova grupa, sa $\cdot$ označavati binarnu operaciju na $\Gamma(P,\leq)$ iz prethodnog teorema.

Propozicija 3.3.7. *Neka je* $(P,+,\cdot,\leq)$ *uređeno polje takvo da je* $(P,+,\leq)$ *gusta Arhimedova grupa. Neka je* $B_1=\{x\in P\,|\,x\leq 1\}$ *i* $B=\{x\in P\,|\,1<x\}$*. Neka je* $\mathbf{1}=(B_1,B)$*. Tada je* $\mathbf{1}$ *neutralni element za operaciju* $\cdot$ *na* $\Gamma(P,\leq)$.

Dokaz. Očito su skupovi B_1 i B disjunktni te je očito da je $B_1 \cup B = P$. Nadalje, za svaki $x \in B_1$ i za svaki $y \in B$ vrijedi $x \leq y$. Vrijedi $1 \in B_1$, dakle, $B_1 \neq \emptyset$. Prema korolaru 2.5.9 vrijedi $0 < 1$ pa iz propozicije 1.3.12 slijedi da je $0 + 1 < 1 + 1$, tj. $1 < 1 + 1$. Zaključujemo da je $B \neq \emptyset$. Dakle, (B_1, B) je prerez u $(P, \leq)$.

Neka je $x \in B$. Tada je $1 < x$ pa, budući da je $(P, +, \leq)$ gusta grupa, postoji $x' \in P$ takav da je $1 < x' < x$. Slijedi $x' \in B$ i $x' < x$. Ovo pokazuje da B nema najmanji element. Prema tome, $\mathbf{1}$ je dobar prerez u $(P, \leq)$, tj. $\mathbf{1} \in \Gamma(P, \leq)$. Uočimo da je $\Theta' \preceq'' \mathbf{1}$. Neka je $\gamma \in \Gamma(P, \leq)$. Tvrdimo da je $\gamma \cdot \mathbf{1} = \gamma$. Imamo 2 slučaja: $\Theta' \preceq'' \gamma$ ili $\gamma \preceq'' \Theta'$.

1) $\Theta' \preceq'' \gamma$

   Imamo $\gamma = (A_1, A)$. Prema definiciji operacije $\cdot$ vrijedi

   $$\gamma \cdot \mathbf{1} = (P \backslash (A \cdot \{x \in P \mid 1 < x\}), A \cdot \{x \in P \mid 1 < x\}) \tag{1}$$

   Tvrdimo da je

   $$A \cdot \{x \in P \mid 1 < x\} = A. \tag{2}$$

   Neka je $a \in A$ te neka je $x \in P$ takav da je $1 < x$. Iz $\Theta' \preceq'' \gamma$ i propozicije 3.2.5 slijedi da je $A \subseteq \{x \in P \mid 0 < x\}$. Stoga je $0 < a$, pa iz $1 < x$ i tvrdnje 2) propozicije 2.5.11 slijedi $a < a \cdot x$. Budući da je (A_1, A) prerez, imamo da je $a \cdot x \in A$. Time smo dokazali da je $A \cdot \{x \in P \mid 1 < x\} \subseteq A$.

   Obratno, neka je $a \in A$. Budući da je (A_1, A) dobar prerez, A nema najmanji element pa postoji $b \in A$ takav da je $b < a$. Iz $b \in A$ slijedi $0 < b$. Prema tvrdnji 3) propozicije 2.5.11 vrijedi $0 < b^{-1}$. Iz ovoga i $b < a$ te tvrdnje 2) propozicije 2.5.11 slijedi $b \cdot b^{-1} < a \cdot b^{-1}$, tj. $1 < a \cdot b^{-1}$.

   Definiramo $x_0 = a \cdot b^{-1}$. Dakle, $1 < x_0$ i $a = b \cdot x_0$. Stoga je $A \subseteq A \cdot \{x \in P \mid 1 < x\}$. Prema tome, vrijedi (2). Iz (1) sada slijedi da je $\gamma \cdot \mathbf{1} = (P \backslash A, A)$, tj. $\gamma \cdot \mathbf{1} = (A_1, A)$ pa je $\gamma \cdot \mathbf{1} = \gamma$.

2) $\gamma \preceq'' \Theta'$

   Znamo da je $(\Gamma(P, \leq), +, \cdot, \preceq'')$ uređeni prsten te da je Θ' neutralni element za $+$. Stoga je $\Theta' \preceq'' -\gamma$. Prema slučaju 1) vrijedi $(-\gamma) \cdot \mathbf{1} = -\gamma$. Koristeći propoziciju 1.1.14 zaključujemo da vrijedi $-(\gamma \cdot \mathbf{1}) = -\gamma$ pa je $\gamma \cdot \mathbf{1} = \gamma$.

Time je tvrdnja propozicije dokazana. □

Propozicija 3.3.8. *Neka je $(P, +, \cdot, \leq)$ uređeni prsten. Pretpostavimo da za sve $x, y \in P$ takve da je $0 \leq x$ i $0 \leq y$ vrijedi $x \cdot y = y \cdot x$. Tada je $\cdot$ komutativna binarna operacija.*

Dokaz. Neka su $x, y \in P$. Imamo 4 slučaja.

1) $0 \leq x$ i $0 \leq y$

   Tada je prema pretpostavci propozicije $x \cdot y = y \cdot x$.

2) $x \leq 0$ i $0 \leq y$

   Tada je $0 \leq -x$ pa prema pretpostavci propozicije vrijedi $(-x) \cdot y = y \cdot (-x)$. Dakle, $-(x \cdot y) = -(y \cdot x)$ pa je $x \cdot y = y \cdot x$.

3) $0 \leq x$ i $y \leq 0$

   Tada je $0 \leq -y$ pa prema pretpostavci propozicije vrijedi $x \cdot (-y) = (-y) \cdot x$. Dakle, $-(x \cdot y) = -(y \cdot x)$ pa je $x \cdot y = y \cdot x$.

4) $x \leq 0$ i $y \leq 0$

   Tada je $0 \leq -x$ i $0 \leq -y$ pa prema pretpostavci propozicije vrijedi $(-x) \cdot (-y) = (-y) \cdot (-x)$. Dakle, $x \cdot y = y \cdot x$.

U svakom slučaju vrijedi $x \cdot y = y \cdot x$. Time je tvrdnja propozicije dokazana. □

Korolar 3.3.9. *Neka je* $(P, +, \cdot, \leq)$ *uređeno polje takvo da je* $(P, +, \leq)$ *gusta Arhimedova grupa. Tada je* $\cdot$ *komutativna binarna operacija na* $\Gamma(P, \leq)$.

Dokaz. Znamo da je $(\Gamma(P, \leq), +, \cdot, \leq'')$ uređeni prsten (prema teoremu 3.3.6). Nadalje, znamo da je Θ' neutralni element za $+$. Stoga je, prema prethodnoj propoziciji, dovoljno dokazati da za sve $\alpha, \beta \in \Gamma(P, \leq)$ takve da je $\Theta' \leq'' \alpha$ i $\Theta' \leq'' \beta$ vrijedi $\alpha \cdot \beta = \beta \cdot \alpha$. Neka su $\alpha, \beta \in \Gamma(P, \leq)$ takvi da je $\Theta' \leq'' \alpha$ i $\Theta' \leq'' \beta$. Imamo $\alpha = (A_1, A), \beta = (B_1, B)$. Vrijedi $\alpha \cdot \beta = (P \setminus (A \cdot B), A \cdot B)$ i $\beta \cdot \alpha = (P \setminus (B \cdot A), B \cdot A)$. Iz činjenice da je binarna operacija $\cdot$ na P komutativna lako zaključujemo da je $A \cdot B = B \cdot A$.

Stoga je $\alpha \cdot \beta = \beta \cdot \alpha$ i time je korolar dokazan. □

Bibliografija

[1] S. Kurepa, *Matematička analiza 2*, Školska knjiga, Zagreb, 1997.

[2] S. Mardešić, *Matematička analiza 1*, Školska knjiga, Zagreb, 1991.

[3] B. Pavković, D. Veljan, *Elementarna matematika 1*, Tehnička knjiga, Zagreb, 1992

Sažetak

U ovom diplomskom radu proučavali smo uređene prstene. Kroz tri poglavlja smo definirali pojmove grupa, prsten, polje, uređeni skup, uređeni prsten, potpolje, homomorfizam grupa, gusta i Arhimedova grupa, pravi i dobar prerez. Veliki dio rada posvećen je zbrajanju i množenju prereza te pravih i dobrih prereza uz dokazivanje nekih svojstava tih binarnih operacija.

Summary

In this paper we studied ordered rings. Through three chapters we defined the notions group, ring, field, ordered set, ordered ring, subfield, group homomorphism, dense and Archimedean group, proper and good cut. Big part of this paper is dedicated to adition and multiplication of regular, proper and good cuts with proving some of the properties of those binary operations.

Životopis

Rođena sam 4. kolovoza 1992. godine u Zagrebu. Pohađala sam OŠ Antuna Mihanovića i Prvu ekonomsku školu u Zagrebu. U srpnju 2011. godine sam upisala Prirodoslovno-matematički fakultet u Zagrebu. Godine 2017. završila sam preddiplomski studij Matematika, nastavnički smjer i iste godine upisala diplomski studij Matematika, nastavnički smjer na istom fakultetu.