# Algebra 2 – radna verzija skripte

Slavko Moconja

2024/25.

## Sadržaj

# 0 Šta je za ispit?

...

# 1 Dejstvo grupe na skup

## A Definicija, primeri, osnovne osobine

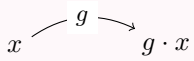
**1/1 Definicija.** Neka je $G$ grupa i $X$ neprazan skup. Dejstvo grupe $G$ na skup $X$ je preslikavanje $\cdot : G \times X \to X$, $(g, x) \mapsto g \cdot x$, koje zadovoljava sledeće dve aksiome:

(d1) $(\forall x \in X)\ \ e \cdot x = x$, gde $e$ označava neutral grupe $G$;

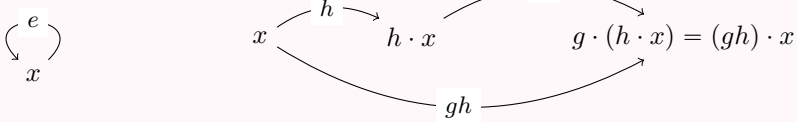
(d2) $(\forall g, h \in G, x \in X)\ \ g \cdot (h \cdot x) = (gh) \cdot x$.

Činjenicu da $G$ deluje na $X$ zapisujemo sa $G \curvearrowright X$.

**1/2 Komentar.** O dejstvu možemo da razmišljamo kao o dinamičkom konceptu: svaki element $g \in G$ deluje na $X$ tako što pomera njegove elemente; $g$ pomera element $x \in X$ u element $g \cdot x$:

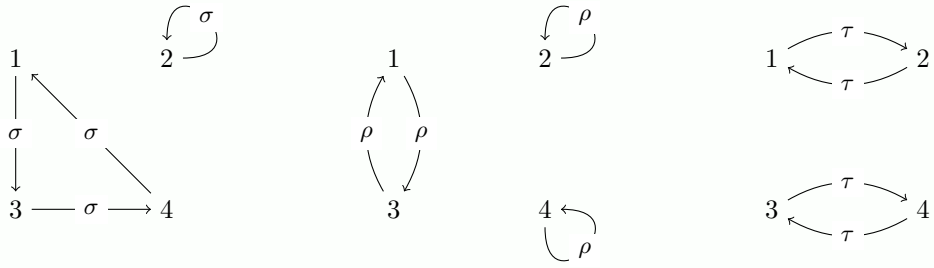



Tada aksiome možemo predstaviti na sledeći način:

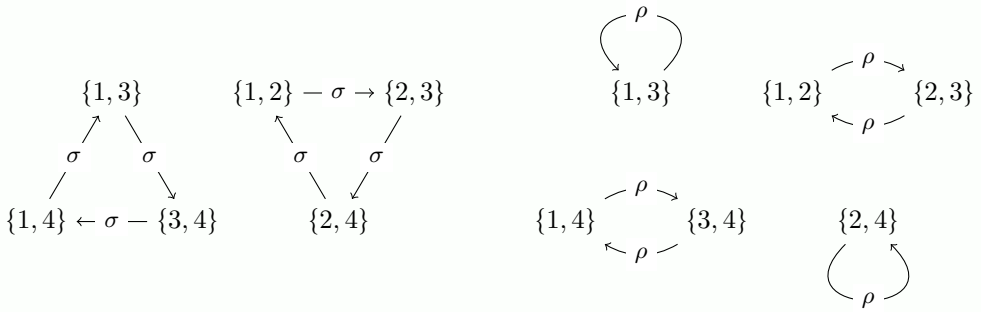



(Primetimo da je redosled nadovezivanja strelica u drugoj aksiomi u saglasnosti sa pravilom za kompoziciju funkcija.) Možemo da imamo u vidu i da je ovo dejstvo elementa $g$ na $X$ permutacija skupa $X$ (bijekcija na $X$), što ćemo kasnije i dokazati.

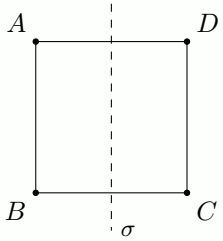
**1/3 Primer.**
Neka je $G = \mathbb{S}_n$ i $X = [n] = \{1, 2, \ldots, n\}$. Imamo prirodno dejstvo $\mathbb{S}_n \curvearrowright [n]$ dato sa $\sigma \cdot i := \sigma(i)$.
Proverimo aksiome dejstva:
(d1) $[] \cdot i = [](i) = i$ (setimo se da je neutral grupe $G$ koincidencija $[]$, tj. identičko preslikavanje skupa $[n]$);
(d2) $\sigma \cdot (\tau \cdot i) = \sigma(\tau \cdot i) = \sigma(\tau(i)) = \sigma \circ \tau(i) = (\sigma \circ \tau) \cdot i$.
Dakle, obe aksiome su zadovoljene.
Pogledajmo specijalan slučaj $\mathbb{S}_4 \curvearrowright [4]$, i nacrtajmo dejstva permutacija $\sigma = [134]$, $\rho = [13]$, $\tau = [12][34]$:



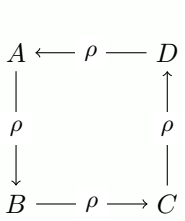

Imamo i prirodno dejstvo $\mathbb{S}_n \curvearrowright [[n]]^2$, gde $[[n]]^2 = \{\{i,j\} \mid i,j \in [n],\ i \neq j\}$ dato sa $\sigma \cdot \{i,j\} := \{\sigma(i), \sigma(j)\}$. Proverićemo aksiome dejstva, ali prvo treba da proverimo da li je ono dobro definisano. Naime, ako $\sigma \in \mathbb{S}_n$ i $\{i,j\} \in [[n]]^2$, treba da proverimo da $\sigma \cdot \{i,j\} \in [[n]]^2$. $\{i,j\} \in [[n]]^2$ znači $i,j \in [n]$ i $i \neq j$, pa kako je $\sigma$ permutacija skupa $[n]$, specijalno 1-1, imamo da je $\sigma(i) \neq \sigma(j)$, i naravno $\sigma(i), \sigma(j) \in [n]$, odakle $\{\sigma(i), \sigma(j)\} \in [[n]]^2$; dakle, $\sigma \cdot \{i,j\} \in [[n]]^2$.
(d1) $[] \cdot \{i,j\} = \{[](i), [](j)\} = \{i,j\}$;
(d2) $\sigma \cdot (\tau \cdot \{i,j\}) = \sigma \cdot \{\tau(i), \tau(j)\} = \{\sigma(\tau(i)), \sigma(\tau(j))\} = \{\sigma \circ \tau(i), \sigma \circ \tau(j)\} = (\sigma \circ \tau) \cdot \{i,j\}$.
Pogledajmo slučaj $\mathbb{S}_4 \curvearrowright [[4]]^2$, i nacrtajmo dejstva permutacija $\sigma = \lfloor 134 \rceil$ i $\rho = \lfloor 13 \rceil$.
Najpre primetimo da je $[[4]]^2 = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}$.
Po definiciji $\lfloor 134 \rceil \cdot \{1,2\} = \{\lfloor 134 \rceil(1), \lfloor 134 \rceil(2)\} = \{3,2\}$, i na sličan način vidimo da su odgovarajaća dejstva data sa:

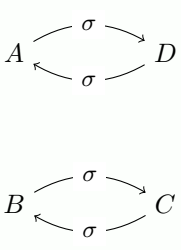


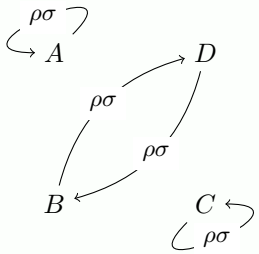

**1/4 Primer.**
Neka je $G = \mathbb{D}_4$ i $X = \{\text{temena kvadrata}\}$; prirodno $\mathbb{D}_4 \curvearrowright X$. Setimo se da je $\mathbb{D}_4$ generisana sa rotacijom $\rho$ za $90^\circ$ oko centra kvadrata u pozitivnom smeru i bilo kojom osnom simetrijom $\sigma$, npr. u odnosu na vertikalnu osu:



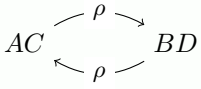

Nacrtajmo dejstva izometrija $\rho$, $\sigma$ i $\rho\sigma$ (primetimo da je $\rho\sigma$ osna simetrija u odnosu na pravu koja sadrži dijagonalu $AC$).

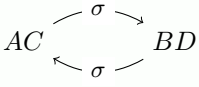


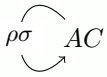


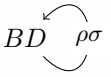



$\mathbb{D}_4$ prirodno deluje i na skup dijagonala kvadrata $\{AC, BD\}$. Nacrtajmo dejstva gornjih elemenata:










**1/5 Primer** (Dejstvo grupe na sebe množenjem sleva)**.**
Posmatrajmo $G \curvearrowright G$ dato sa $g \cdot x := gx$.
Proverimo aksiome dejstva:
(d1) $e \cdot x = ex = x$;
(d2) $g \cdot (h \cdot x) = g \cdot (hx) = g(hx) = (gh)x = (gh) \cdot x$.

**1/6 Primer** (Dejstvo grupe na sebe konjugacijom)**.**
Posmatrajmo $G \curvearrowright G$ dato sa $g \cdot x := gxg^{-1}$.
Proverimo aksiome dejstva:
(d1) $e \cdot x = exe^{-1} = exe = x$;
(d2) $g \cdot (h \cdot x) = g \cdot (hxh^{-1}) = ghxh^{-1}g^{-1} = ghx(gh)^{-1} = (gh) \cdot x$.

Setimo se, ako je $H \leqslant G$, $G/H$ označava skup svih levih koseta podgrupe $H$: $G/H := \{aH \mid a \in G\}$, gde je levi koset $aH := \{ah \mid h \in H\}$. Takođe, setimo se: $aH = bH \iff a^{-1}b \in H$.

**1/7 Primer** (Dejstvo grupe na kosete podgrupe)**.**
Neka je $H \leqslant G$. Posmatrajmo $G \curvearrowright G/H$ dato sa $g \cdot aH := (ga)H$.
Kako smo definisali da $g$ koset predstavljen sa $a$ pomera u koset predstavljen sa $ga$, trebalo bi najpre da dokažemo da je ovako zadato dejstvo dobro definisano. Tj. treba da proverimo da $aH = bH$ povlači $g \cdot aH = g \cdot bH$, tj. $(ga)H = (gb)H$. To možemo da uradimo koristeći gornju napomenu: $aH = bH \iff a^{-1}b \in H \iff a^{-1}g^{-1}gb \in H \iff (ga)^{-1}(gb) \in H \iff (ga)H = (gb)H$. Sada možemo da proverimo aksiome dejstva:
(d1) $e \cdot aH = (ea)H = aH$;
(d2) $g \cdot (h \cdot aH) = g \cdot (ha)H = (g(ha))H = ((gh)a)H = (gh) \cdot aH$.

**1/8 Primer** (Dejstvo grupe na podgrupe konjugacijom)**.**
Neka je $Sub(G)$ familija svih podgrupa od $G$. Posmatrajmo $G \curvearrowright Sub(G)$ dato sa $g \cdot H := gHg^{-1}$.
Poznato nam je da za $H \leqslant G$, takođe $gHg^{-1} \leqslant G$, tj. gornje preslikavanje je dobro definisano. Aksiome dejstva lako možemo da proverimo na sličan način kao u primeru 1/6.

**1/9 Primer.**
Za $\sigma \in \mathbb{S}_n$ i $(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ definišimo: $\sigma \cdot (x_1, x_2, \ldots, x_n) := (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$.
Proverimo aksiome dejstva:
(d1) $[] \cdot (x_1, x_2, \ldots, x_n) = (x_{[](1)}, x_{[](2)}, \ldots, x_{[](n)}) = (x_1, x_2, \ldots, x_n)$.
(d2) Neka su $\sigma, \tau \in \mathbb{S}_n$:

$$\begin{aligned} \sigma \cdot (\tau \cdot (x_1, x_2, \ldots, x_n)) &= \sigma \cdot (x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) \\ &= (x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, \ldots, x_{\sigma(\tau(n))}) \\ &= (x_{\sigma\circ\tau(1)}, x_{\sigma\circ\tau(2)}, \ldots, x_{\sigma\circ\tau}(n)) \\ &= (\sigma \circ \tau) \cdot (x_1, x_2, \ldots, x_n). \end{aligned}$$

**1/10 Zadatak.** (a) Račun u prethodnom primeru je netačan. Gde je greška?

(b) Dokazati da gornja formula ne definiše $\mathbb{S}_n \curvearrowright \mathbb{R}^n$.

(c) Dokazati da sa $\sigma \cdot (x_1, x_2, \ldots, x_n) := (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(n)})$ jeste definisano $\mathbb{S}_n \curvearrowright \mathbb{R}^n$.

**1/11 Primer.**
Neka je $S$ neprazan skup i $X = S^n$. Defnišemo $\mathbb{Z}_n \curvearrowright X$ sa:

$$k \cdot (x_0, x_1, \ldots, x_{n-1}) := (x_{0+k}, x_{1+k}, \ldots, x_{(n-1)+k}),$$

gde $i + k$ računamo u $\mathbb{Z}_n$ (sabiramo modulo $n$).
Proverimo aksiome dejstva:
(d1) $0 \cdot (x_0, x_1, \ldots, x_{n-1}) = (x_{0+0}, x_{1+0}, \ldots, x_{(n-1)+0}) = (x_0, x_1, \ldots, x_{n-1})$;
(d2)

$$\begin{aligned} k \cdot (m \cdot (x_0, x_1, \ldots, x_{n-1})) &= k \cdot (x_{0+m}, x_{1+m}, \ldots, x_{(n-1)+m}) \\ &= k \cdot (y_0, y_1, \ldots, y_{n-1}), \text{ gde } y_i = x_{i+m} \\ &= (y_{0+k}, y_{1+k}, \ldots, y_{(n-1)+k}) \\ &= (x_{0+k+m}, x_{1+k+m}, \ldots, x_{(n-1)+k+m}) \\ &= (k + m) \cdot (x_0, x_1, \ldots, x_{n-1}). \end{aligned}$$

**1/12 Primer.**
Neka je $G$ grupa i $X = \{(g_0, g_1, \ldots, g_{n-1}) \in G^n \mid g_0 g_1 \ldots g_{n-1} = e\}$. Formula iz prethodnog primera definiše $\mathbb{Z}_n \curvearrowright X$. Ako je $G$ konačna, $|X| = |G|^{n-1}$.
Treba samo da proverimo da je dejstvo dobro definisano, tj. da za $k \in \mathbb{Z}_n$ i $(g_0, g_1, \ldots, g_{n-1}) \in X$, $k \cdot (g_0, g_1, \ldots, g_{n-1}) \in X$. Iz $(g_0, g_1, \ldots, g_{k-1}, g_k, g_{k+1} \ldots, g_{n-1}) \in X$ imamo $g_0 g_1 \ldots g_{k-1} g_k g_{k+1} \ldots g_{n-1} = e$. Odavde, množenjem sa $(g_k g_{k+1} \ldots g_{n-1})^{-1}$ zdesna, dobijamo $g_0 g_1 \ldots g_{k-1} = (g_k g_{k+1} \ldots g_{n-1})^{-1}$, pa množenjem sa $g_k g_{k+1} \ldots g_{n-1}$ sleva zaključujemo $g_k g_{k+1} \ldots g_{n-1} g_0 g_1 \ldots g_{k-1} = e$. Dakle, $k \cdot (g_0, g_1, \ldots, g_{n-1}) = (g_k, g_{k+1}, \ldots, g_{n-1}, g_0, g_1, \ldots, g_{k-1}) \in X$. Aksiome dejstva smo već proverili u prethodnom primeru.
Ako je $G$ konačna, dokažimo $|X| = |G|^{n-1}$. Posmatrajmo preslikavanje $X \to G^{n-1}$ dato sa $(g_0, g_1, \ldots, g_{n-1}) \mapsto (g_1, \ldots, g_{n-1})$; dokazaćemo da je u pitanju bijekcija. Preslikavanje je „na" jer za proizvoljno $(g_1, \ldots, g_{n-1}) \in G^{n-1}$ imamo $g_0 g_1 \ldots g_{n-1} = e$ za $g_0 = (g_1, \ldots, g_{n-1})^{-1}$, pa $(g_0, g_1, \ldots, g_{n-1}) \in X$ i $(g_0, g_1, \ldots, g_{n-1}) \mapsto (g_1, \ldots, g_{n-1})$. Ako $(g_0, g_1, \ldots, g_{n-1}), (g_0', g_1, \ldots, g_{n-1}) \in X$, imamo $g_0 =$

$(g_1 \dots g_{n-1})^{-1} = g_0'$, pa imamo da je $(g_0, g_1, \dots, g_{n-1}) = (g_0', g_1, \dots, g_{n-1})$, što dokazuje da je preslikavanje „1-1".

**1/13 Primer.**
Neka $G \curvearrowright X$, i neka je $Y$ skup. Za $g \in G$ i $f \in {}^X Y$ definišemo $G \curvearrowright {}^X Y$ sa $g \cdot f \in {}^X Y$ je funkcija data sa $(g \cdot f)(x) := f(g^{-1} \cdot x)$.
Proverimo aksiome dejstva:
(d1) za svako $x \in X$ imamo $(e \cdot f)(x) = f(e^{-1} \cdot x) = f(e \cdot x) = f(x)$, gde u poslednjem koraku koristimo (d1) za $G \curvearrowright X$, odakle je $e \cdot f = f$;
(d2) za svako $x \in X$ imamo:

$$\begin{aligned}(g \cdot (h \cdot f))(x) &= (h \cdot f)(g^{-1} \cdot x) \\ &= f(h^{-1} \cdot (g^{-1} \cdot x)) \\ &= f((h^{-1}g^{-1}) \cdot x), \text{ gde koristimo (d2) za } G \curvearrowright X \\ &= f((gh)^{-1} \cdot x) \\ &= (gh \cdot f)(x),\end{aligned}$$

odakle $g \cdot (h \cdot f) = (gh) \cdot f$.

**1/14 Definicija.** (a) Neka $G \curvearrowright X$. Za $g \in G$ definišemo $\delta_g : X \to X$ sa $\delta_g(x) := g \cdot x$.

(b) Neka je $X$ neprazan skup. Sa $Sym(X)$ označavamo grupu svih permutacija skupa $X$ (bijekcija $X \to X$) u odnosu na operaciju kompozicije funkcija; $id_X$ je neutral ove grupe; inverz permutacije $\sigma$ je inverzno preslikavanje $\sigma^{-1}$. (**Komentar.** $Sym([n]) = \mathbb{S}_n$.)

**1/15 Tvrđenje** (Osnovne osobine dejstva)**.**
Neka $G \curvearrowright X$, $g, h \in G$ i $x, y \in X$.

(a) $g \cdot x = y \iff g^{-1} \cdot y = x$;

(b) $g \cdot x = g \cdot y \iff x = y$;

(c) $\delta_g \in Sym(X)$;

(d) $\delta_e = id_X$;

(e) $\delta_g \circ \delta_h = \delta_{gh}$;

(f) $\delta_g^{-1} = \delta_{g^{-1}}$;

(g) $\delta : G \to Sym(X)$ dato sa $\delta(g) := \delta_g$ je homomorfizam grupa.

*Dokaz.* (a) ($\Rightarrow$) Pretpostavimo $g \cdot x = y$. Tada je:

$$x \overset{(d1)}{=} e \cdot x = (g^{-1}g) \cdot x \overset{(d2)}{=} g^{-1} \cdot (g \cdot x) = g^{-1} \cdot y.$$

($\Leftarrow$) sada sledi iz ($\Rightarrow$) na sledeći način:

$$g^{-1} \cdot y = x \overset{(\Rightarrow)}{\Longrightarrow} (g^{-1})^{-1} \cdot x = y, \text{ tj. } g \cdot x = y.$$

(b) ($\Rightarrow$) Neka je $g \cdot x = g \cdot y =: z$. Prema (a) imamo $x = g^{-1} \cdot z = y$. Smer ($\Leftarrow$) je očigledan.
(c) Prema (b) $\delta_g$ je „1-1". Kako smo već videli $x = g \cdot (g^{-1} \cdot x) = \delta_g(g^{-1} \cdot x)$; $\delta_g$ je „na".
(d) $\delta_e = id_X$ važi prema (d1).

(e) $\delta_g \circ \delta_h = \delta_{gh}$ važi prema (d2).
(f) Prema (d) i (e) je $\delta_{g^{-1}} \circ \delta_g = id_X = \delta_g \circ \delta_{g^{-1}}$, odakle je $\delta_{g^{-1}} = \delta_g^{-1}$.
(g) Direktno prema (e). □

**1/16 Zadatak.** Neka $G \curvearrowright X$.

(a) Ako $H \leqslant G$, prirodno $H \curvearrowright X$ restrikcijom dejstva.

(b) Prirodno $G \curvearrowright [X]^n = \{n\text{-točlani podskupovi od } X\}$ sa $g \cdot \{x_1, \ldots, x_n\} := \{g \cdot x_1, \ldots, g \cdot x_n\}$.

(c) Prirodno $G \curvearrowright X^n$ – dijagonalno dejstvo sa $g \cdot (x_1, \ldots, x_n) := (g \cdot x_1, \ldots, g \cdot x_n)$.

**Komentar.** Deo (a) je očigledan. Aksiome dejstva u delovima (b) i (c) se direktno proveravaju. U delu (b) potrebno je proveriti i dobru definisanost koja sledi iz prethodnog tvrđenja.

## B Jezgro i slika dejstva, Kejlijeva teorema, $n!$-teorema

**1/17 Komentar.** Neka $G \curvearrowright X$. Prema tvrđenju 1/15(g) imamo pridruženi homomorfizam $\delta : G \to Sym(X)$ dat sa $\delta(g) = \delta_g$, gde $\delta_g(x) = g \cdot x$.

**1/18 Definicija.** Neka $G \curvearrowright X$ i neka je $\delta : G \to Sym(X)$ pridruženi homomorfizam. Definišemo:

(a) $Ker(G \curvearrowright X) := Ker(\delta)$;

(b) $Im(G \curvearrowright X) := Im(\delta)$.

**1/19 Komentar.** (a) Prema prvoj teoremi o izomorfizmu imamo:

$$G/Ker(G \curvearrowright X) \cong Im(G \curvearrowright X) \leqslant Sym(X).$$

(b) $g \in Ker(G \curvearrowright X) \iff \delta_g = id_X \iff (\forall x \in X)\ g \cdot x = x$:

$$Ker(G \curvearrowright X) = \{g \in G \mid (\forall x \in X)\ g \cdot x = x\}.$$

Navešćemo nekoliko primera primene gornje formule na različita dejstva.

**1/20 Teorema** (Kejlijeva teorema)**.**
Svaka grupa $G$ je izomorfna podgrupi neke grupe permutacija. Preciznije, do na izomorfizam, $G \leqslant Sym(G)$.

*Dokaz.* Uočimo dejstvo $G \curvearrowright G$ množenja sleva iz primera 1/5: $g \cdot x := gx$. Kako je $gx = x \iff g = e$, jezgro $Ker(G \curvearrowright G) = \{e\}$ je trivialno. Prema komentaru 1/19(a):

$$G \cong G/Ker(G \curvearrowright G) \cong Im(G \curvearrowright G) \leqslant Sym(G).$$

Dakle, $G \leqslant Sym(G)$. □

**1/21 Teorema.**
$G/Z(G) \cong Inn(G)$.

*Dokaz.* Uočimo dejstvo $G \curvearrowright G$ konjugacijom iz primera 1/6: $g \cdot x := gxg^{-1}$. Najpre, kako je $\delta_g(x) = gxg^{-1}$, $Im(G \curvearrowright G) = \{\delta_g \mid g \in G\} = Inn(G)$ – grupa unutrašnjih automorfizama grupe $G$. Takođe, $g \in Ker(G \curvearrowright G) \iff (\forall x \in X)\ g \cdot x = x \iff (\forall x \in X)\ gxg^{-1} = x \iff (\forall x \in X)\ gx = xg \iff g \in Z(G)$. Teorema direktno sledi prema komentaru 1/19(a). □

**1/22 Definicija.** Neka je $H \leqslant G$. Jezgro podgrupe $H$ je:

$$Core(H) := \bigcap_{a \in G} aHa^{-1}.$$

**1/23 Teorema** ($n!$-teorema)**.**
Neka je $H \leqslant G$ i $|G : H| = n$. Tada $|G : Core(H)| \mid n!$.

*Dokaz.* Uočimo dejstvo $G \curvearrowright G/H$ na kosetima podgrupe $H$ iz primera 1/7: $g \cdot a := gaH$. Izračunajmo $Ker(G \curvearrowright G/H)$: $g \in Ker(G \curvearrowright G/H) \iff (\forall a \in G)\ g \cdot aH = aH \iff (\forall a \in G)\ gaH = aH \iff (\forall a \in G)\ a^{-1}ga \in H \iff (\forall a \in G)\ g \in aHa^{-1} \iff g \in Core(H)$; dakle, $Ker(G \curvearrowright G/H) = Core(H)$. Prema komentaru 1/19(a): $G/Core(H) \leqslant Sym(G/H)$. Kako $|G/H| = |G : H| = n$, $|Sym(G/H)| = n!$, pa po Lagranžovoj teoremi imamo $|G : Core(H)| = |G/Core(H)| \mid n!$. □

**1/24 Komentar.** U dokazu prethodne teoreme smo videli da je $Core(H)$ jezgro izvesnog homomorfizma (datog dejstvom), što znači da je $Core(H) \lhd G$. Kako je $H = eHe^{-1}$, $H$ učestvuje u preseku kojim je definisano jezgro $Core(H)$, pa zaključujujemo $Core(H) \leqslant H$. Prema tome, $Core(H)$ je podgrupa od $H$ koja je normalna u $G$. Štaviše, $Core(H)$ je najveća podgrupa od $H$ koja je normalna u $G$. Da bismo ovo videli, pretpostavimo $K \leqslant H$ i $K \lhd G$. Tada je za svako $a \in G$, $K = aKa^{-1} \leqslant aHa^{-1}$, gde jednakost važi jer $K \lhd G$, a inkluzija jer $K \leqslant H$. Odatle je $K = \bigcap_{a \in G} aKa^{-1} \leqslant \bigcap_{a \in G} aHa^{-1} = Core(H)$.
Primetimo i da odavde imamo $H \lhd G \iff Core(H) = H$.

Dajemo jedan primer primene $n!$-teoreme.

**1/25 Teorema.**
Neka je $G$ konačna grupa i neka je $H \leqslant G$ takva da $|G : H| = p$, gde je $p$ najmanji prost broj koji deli $|G|$. Tada $H \lhd G$.
Specijalno, podgrupa indeksa 2 uvek mora biti normalna.

*Dokaz.* Primetimo da je $(|G|, p!) = p$ jer je $p$ najmanji prost broj koji deli $|G|$. Kako sa jedne strane, po Lagranžovoj teoremi, $|G : Core(H)| \mid |G|$, a sa druge strane, po $n!$-teoremi, $|G : Core(H)| \mid p!$, dobijamo da $|G : Core(H)|$ deli i njihov NZD, tj. $p$. Dakle, ili $|G : Core(H)| = 1$ ili $|G : Core(H)| = p$. Prvi slučaj nije moguć jer $|G : Core(H)| = 1$ znači $G = Core(H)$, a $Core(H) \leqslant H$ i $H \neq G$ (jer $|G : H| = p$). Dakle, $|G : Core(H)| = p$. Sada kako je i $|G : H| = p$ i $Core(H) \leqslant H$, zaključujemo $Core(H) = H$, odakle $H \lhd G$. □

## C Orbite i stabilizatori

**1/26 Definicija.** Neka $G \curvearrowright X$ i $x \in X$.

(a) Orbita elementa $x$ je skup:

$$G \cdot x := \{g \cdot x \mid x \in X\} \subseteq X.^{1}$$

(b) Stabilizator elementa $x$ je skup:

$$G_x := \{g \in G \mid g \cdot x = x\} \subseteq G.^{2}$$

[1] Orbita elementa $x$ se ponekad obeležava i $O(x)$ ili $O_x$.
[2] Stabilizator elementa $x$ se ponekad obeležava i $Stab(x)$ ili $\Sigma_x$.

**1/27 Primer.**
Neka je $G \curvearrowright G$ dejstvo grupe na sebe množenjem sleva iz primera 1/5: $g \cdot x = gx$, i neka je $x \in G$. Primetimo da je $G \cdot x = G$. Zaista, za $y \in G$ imamo $(yx^{-1}) \cdot x = yx^{-1}x = y$, pa $y \in G \cdot x$; dakle, $G \cdot x = G$. Takođe, $g \cdot x = x \iff gx = x \iff g = e$, tj. $G_x = \{e\}$.

**1/28 Primer.**
Neka je $G \curvearrowright G$ dejstvo grupe na sebe konjugacijom iz primera 1/6: $g \cdot x = gxg^{-1}$, i neka je $x \in G$. Tada je $G \cdot x = \{gxg^{-1} \mid g \in G\} =: x^G$ – klasa konjugacije elementa $x$. Primetimo da je $G \cdot x = \{x\} \iff (\forall g \in G)\ gxg^{-1} = x \iff (\forall g \in G)\ gx = xg \iff x \in Z(G)$. Slično, $g \in G_x \iff gxg^{-1} = x \iff gx = xg \iff g \in C(x)$, tj. $G_x = C(x)$ – centralizator elementa $x$ u $G$.

**1/29 Primer.**
Neka je $H \leqslant G$, $G \curvearrowright G/H$ dejstvo grupe na kosetima iz primera 1/7: $g \cdot aH = gaH$, i neka je $aH \in G/H$. Tada je $G \cdot aH = G/H$; zaista, za $bH \in G/H$ imamo $bH = ba^{-1}aH = (ba^{-1}) \cdot aH \in G \cdot aH$. Dakle, $G \cdot aH = G/H$. Takođe, $g \in G_{aH} \iff gaH = aH \iff a^{-1}ga \in H \iff g \in aHa^{-1}$, tj. $G_{aH} = aHa^{-1}$.

**1/30 Primer.**
Neka je $G \curvearrowright Sub(G)$ dejstvo na podgrupa konjugacijom iz primera 1/8: $g \cdot H = gHg^{-1}$. Tada $g \in G_H \iff g \cdot H = H \iff gHg^{-1} = H \iff gH = Hg \iff g \in N(H)$; dakle, $G_H = N(H)$ – normalizator podgrupe $H$ u $G$.

**1/31 Primer.**
Neka je $S$ skup i $\mathbb{Z}_4 \curvearrowright S^4$ dejstvo iz primera 1/11: $k \cdot (x_0, x_1, x_2, x_3) = (x_k, x_{k+1}, x_{k+2}, x_{k+3})$ gde sabiramo u $\mathbb{Z}_4$. Izračunajmo orbitu i satbilizator proizvoljne četvorke.
Pretpostavimo najpre da je $x_0 = x_1 = x_2 = x_3 =: x$. Tada je za svako $k \in \mathbb{Z}_4$, $k \cdot (x, x, x, x) = (x, x, x, x)$, pa je $\mathbb{Z}_4 \cdot (x, x, x, x) = \{(x, x, x, x)\}$ i $(\mathbb{Z}_4)_{(x,x,x,x)} = \mathbb{Z}_4$.
Pretpostavimo sada da su neka tri od $x_0, x_1, x_2, x_3$ jednaki, a četvrti od njih je različit, npr. pretpostavimo $x := x_0 \neq x_1 = x_2 = x_3 =: y$. Tada je $0 \cdot (x, y, y, y) = (x, y, y, y)$, $1 \cdot (x, y, y, y) = (y, y, y, x)$, $2 \cdot (x, y, y, y) = (y, y, x, y)$ i $3 \cdot (x, y, y, y) = (y, x, y, y)$. Dakle, $\mathbb{Z}_4 \cdot (x, y, y, y) = \{(x, y, y, y), (y, y, y, x), (y, y, x, y), (y, x, y, y)\}$, i jedino 0 fiksira element $(x, y, y, y)$, pa je $(\mathbb{Z}_4)_{(x,y,y,y)} = \{0\}$. Isti rezultat dobijamo i ako je neki drugi element $x_i$ različit od preostalih koji su jednaki.
Pretpostavimo sada da među $x_0, x_1, x_2, x_3$ imamo dva para jednakih elemenata. Najpre, neka je $x_0 = x_1 =: x \neq y := x_2 = x_3$. Kao i malopre vidimo da je $\mathbb{Z}_4 \cdot (x, x, y, y) = \{(x, x, y, y), (x, y, y, x), (y, y, x, x), (y, x, x, y)\}$, kao i da jedino 0 fiksira $(x, x, y, y)$, tj. $(\mathbb{Z}_4)_{(x,x,y,y)} = \{0\}$. Isti rezultat dobijamo i ako pođemo od bilo kog elementa iz navedene orbite.
Drugi podslučaj je $x_0 = x_2 =: x \neq y := x_1 = x_3$. Tada je $\mathbb{Z}_4 \cdot (x, y, x, y) = \{(x, y, x, y), (y, x, y, x)\}$, i pored 0, i 2 fiksira element $(x, y, x, y)$, pa je $(\mathbb{Z}_4)_{(x,y,x,y)} = \{0, 2\}$.
U svim preostalim slučajevima, koje ostavljamo za vežbu, dobijamo $\mathbb{Z}_4 \cdot (x_0, x_1, x_2, x_3)\}$ je četvoroelementni skup i $(\mathbb{Z}_4)_{(x_0,x_1,x_2,x_3)} = \{0\}$.

**1/32 Primer.**
Neka je $p$ prost broj, $S$ skup i $\mathbb{Z}_p \curvearrowright S^p$ kao u primeru 1/11. Izračunajmo orbitu i stabilizator proizvoljne $p$-torke.
Podelićemo problem na dva slučaja. Prvo, pretpostavimo $x_0 = x_1 = \cdots = x_{p-1} =: x$. Očigledno $\mathbb{Z}_p \cdot (x, x, \ldots, x) = \{x, x, \ldots, x\}$ i $(\mathbb{Z}_p)_{(x,x,\ldots,x)} = \mathbb{Z}_p$.
Pretpostavimo sada da nisu svi $x_0, x_1, \ldots, x_{p-1}$ jednaki. Tvrdimo da je stabilizator trivijalan. Pret-

postavimo suprotno. Neka je $k \in \mathbb{Z}_p$, $k > 0$, takav da:

$$k \cdot (x_0, x_1, \ldots, x_{p-1}) = (x_0, x_1, \ldots, x_{p-1}).$$

Kako je $(k, p) = 1$ jer je $p$ prost broj, po Bezuovoj lemi postoje brojevi $\alpha, \beta \in \mathbb{Z}$ takvi da je $1 = \alpha k + \beta p$; tada je modulo $p$, $1 = \alpha_p k$, gde je $\alpha_p$ ostatak pri deljenju $\alpha$ sa $p$. Sada imamo:

$$\begin{aligned}(x_1, \ldots, x_{p-1}, x_0) &= 1 \cdot (x_0, x_1 \ldots, x_{p-1}) \\ &= (\alpha_p k) \cdot (x_0, x_1, \ldots, x_{p-1}) \\ &= (\underbrace{k + \cdots + k}_{\alpha_p}) \cdot (x_0, x_1, \ldots, x_{p-1}) \\ &= (x_0, x_1, \ldots, x_{p-1})\end{aligned}$$

gde u poslednjem koraku $\alpha_p$ puta primenjujemo aksiomu (d2) i gornju jednakost. Dakle, dobijamo $(x_0, x_1, \ldots, x_{p-1}) = (x_1, \ldots, x_{p-1}, x_0)$, odakle $x_0 = x_1 = \cdots = x_{p-1}$. Kontradikcija. Dakle, stabilizator je trivijalan.
Sada lako vidimo da orbita ima $p$ različitih elemenata. Naime, ako za $l < k$, $l \cdot (x_0, \ldots, x_{p-1}) = k \cdot (x_0, \ldots, x_{p-1})$, onda je i $0 \cdot (x_0, \ldots, x_{p-1}) = (k - l) \cdot (x_0, \ldots, x_{p-1})$, odakle $k - l$ pripada stabilizatoru; kontradikcija prema prethodnom računu.
Isti rezultat, sa potpuno istim računom, dobijamo i za dejstvo iz primera 1/12.

**1/33 Tvrđenje.**
Neka $G \curvearrowright X$, $a \in G$ i $x \in X$.

(a) $G_x \leqslant G$;

(b) $G_{a \cdot x} = aG_x a^{-1}$; specijalno, elementi u istoj orbiti imaju konjugovane stabilizatore;

(c) $Ker(G \curvearrowright X) = \bigcap_{x \in X} G_x$.

*Dokaz.* (a) Očigledno $e \in G_x$ prema (d1), pa $G_x \neq \varnothing$. Neka $g, h \in G_x$, tj. $g \cdot x = h \cdot x = x$; tada i $g^{-1} \cdot x = x$. Sada i $(g^{-1}h) \cdot x = g^{-1} \cdot (h \cdot x) = g^{-1} \cdot x = x$, odakle $g^{-1}h \in G_x$. Dakle, $G_x \leqslant G$.

(b) Imamo $g \in G_{a \cdot x} \iff g \cdot (a \cdot x) = a \cdot x \iff ga \cdot x = a \cdot x \iff a^{-1}ga \cdot x = x \iff a^{-1}ga \in G_x \iff g \in aG_x a^{-1}$; dakle, $G_{a \cdot x} = aG_x a^{-1}$.

(c) Imamo $g \in Ker(G \curvearrowright X) \iff (\forall x \in X)\ g \cdot x = x \iff (\forall x \in X) g \in G_x \iff g \in \bigcap_{x \in X} G_x$; dakle, $Ker(G \curvearrowright X) = \bigcap_{x \in X} G_x$. □

**1/34 Teorema** (Orbita–stabilizator teorema)**.**
Neka $G \curvearrowright X$ i $x \in X$.

(a) Sa $aG_x \mapsto a \cdot x$ definisana je bijekcija $G/G_x \to G \cdot x$.

(b) $|G : G_x| = |G \cdot x|$.

(c) Ako je $G$ konačna, onda je $|G| = |G_x| \cdot |G \cdot x|$.

*Dokaz.* (a) Uočimo sledeći niz ekvivalencija:

$$aG_x = bG_x \iff b^{-1}a \in G_x \iff b^{-1}a \cdot x = x \iff a \cdot x = b \cdot x.$$

On pokazuje da je dato preslikavanje dobro definisano (smer ($\Rightarrow$)) i da je „1-1" (smer ($\Leftarrow$)). Kako je ono

očigledno „na" (jer se u $a \cdot x$ slika $aG_x$), u pitanju je bijekcija. (b) sada direktno sledi iz (a):

$$|G : G_x| = |G/G_x| = |G \cdot x|,$$

a (c) direktno sledi iz (b) jer je $|G : G_x| = \frac{|G|}{|G_x|}$ ako je $G$ konačna grupa. □

**1/35 Primer.**
Neka je $G$ konačna grupa i neka $H, K \leqslant G$. Od ranije nam je poznata formula $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$. Dokažimo ovu formula koristeći orbita-stabilizator teoremu.
Posmatrajmo dejstvo $H \times K \curvearrowright G$ dato sa $(h, k) \cdot x = hxk^{-1}$. Za vežbu ostavljamo proveru aksioma dejstva. Izračunajmo orbitu od $e$:

$$(H \times K) \cdot e = \{(h, k) \cdot e \mid h \in H,\, k \in K\} = \{hek^{-1} \mid h \in H,\, k \in K\} = \{hk^{-1} \mid h \in H,\, k \in K\} = HK^{-1} = HK,$$

gde $K^{-1} = K$ važi jer je $K$ podgrupa; dakle, $|(H \times K) \cdot e| = |HK|$. Izračunajmo i stabilizator od $e$:

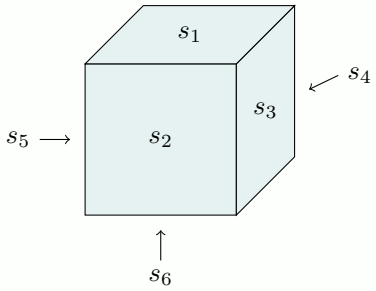
$$(h, k) \in (H \times K)_e \iff (h, k) \cdot e = e \iff hek^{-1} = e \iff h = k \in H \cap K.$$

Dakle, $|(H \times K)_e| = |H \cap K|$. Prema orbita stabilizator teoremi imamo:

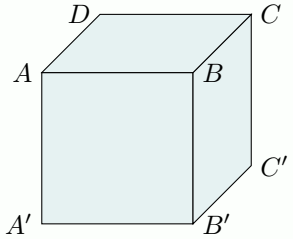
$$|H \times K| = |(H \times K) \cdot e| \cdot |(H \times K)_e| \implies |H| \cdot |K| = |HK| \cdot |H \cap K|,$$

odakle sledi gornja formula.

**1/36 Primer.**
Izračunati koliko grupa prostornih rotacija (bez refleksija) kocke ima elemenata.
Neka je $G$ grupa o kojoj govorimo. Možemo da rešimo ovaj problem na više načina.
I način. Označimo sa $S = \{s_1, \ldots, s_6\}$ skup strana kocke:




Grupa $G$ prirodno deluje na $S$, pri čemu očigledno $G \cdot s_1 = X$, tj. $|G \cdot s_1| = 6$. Sa druge strane, ako $g \in G$ fiksira $s_1$, mora da fiksira i $s_6$, i $g$ je određen sa slikom $s_2$ koja može da bude $s_2, s_3, s_4$ ili $s_5$. Dakle, $|G_{s_1}| = 4$. Prema orbita-stabilizator teoremi $|G| = |G \cdot s_1| \cdot |G_{s_1}| = 6 \cdot 4 = 24$.
II način. Označimo sa $T = \{A, B, C, D, A', B', C', D'\}$ skup temena kocke:




Grupa $G$ prirodno deluje na $T$, pri čemu očigledno $G \cdot A = T$; $|G \cdot A| = 8$. Ako $g \in G$ fiksira $A$, $g$ je određena sa slikom od $B$ koja može da bude $B, D$ ili $A'$; $|G_A| = 3$. Prema orbita stabilizator teoremi $|G| = |G \cdot A| \cdot |G_A| = 8 \cdot 3 = 24$.

III način. Označimo sa $D = \{AC', BD', CA', DB'\}$ skup dijagonala kocke (prethodna slika). Grupa $G$ prirodno deluje na $D$, i očigledno $|G \cdot AC'| = D$, tj. $|G \cdot AC'| = 4$. Neka $g \in G$ fiksira dijagonalu $AC'$. Moguća su dva slučaja. Prvi: $g$ fiksira temena $A$ i $C'$. Tada je $g$ određena sa slikom temena $B$ i imamo tri mogućnosti: $B$ se slika u $B, D$ ili $A'$. Drugi slučaj: $g$ transponuje temena $A$ i $C'$. Ponovo je $g$ određena slikom temena $B$ koje sada može da se slika u $B', C$ ili $D'$. Prema tome, $|G_{AC'}| = 6$. Prema orbita-stabilizator teoremi $|G| = |G \cdot AC'| \cdot |S_{AC'}| = 4 \cdot 6 = 24$.
Ovde možemo da kažemo i više. Nije teško videti da ako $g \in G$ fiksira sve dijagonale, onda $g$ mora biti koincidencija (jedina druga izometrija koja fiksira sve dijagonale je centralna simetrija u odnosu na centar kocke, ali ona je indirektna, tj. ne pripada $G$); dakle, $Ker(G \curvearrowright D)$ je trivijalna. Kako je $G \cong G/Ker(G \curvearrowright D) \cong Im(G \curvearrowright D) \leqslant Sym(D) \cong \mathbb{S}_4$, i kako $|G| = |\mathbb{S}_4| = 24$, zaključujemo $G \cong \mathbb{S}_4$.

**1/37 Zadatak.** Izračunati broj svih izometrija kocke.

**1/38 Teorema.**
Neka $G \curvearrowright X$. Sa $x \sim y :\iff x \in G \cdot y$ definisana je ekvivalencija na $X$, i klasa ekvivalencija elementa $x$, $[x]_\sim$, je orbita elementa $x$: $[x]_\sim = G \cdot x$. Specijalno, orbite dejstva čine particiju skupa $X$.

*Dokaz.* Relacija $\sim$ je refleksivna jer $x = e \cdot x \in G \cdot x$. Pretpostavimo $x \sim y$, tj. $x \in G \cdot y$. Tada $x = g \cdot y$ za neko $g \in G$, pa je $y = g^{-1} \cdot x \in G \cdot x$, tj. $y \sim x$; relacija je simetrična. Konačno, pretpostavimo $x \sim y$ i $y \sim z$, tj. $x \in G \cdot y$ i $y \in G \cdot z$. Tada $x = g \cdot y$ i $y = h \cdot z$ za neke $g, h \in G$, odakle je $x = g \cdot y = g \cdot (h \cdot z) = (gh) \cdot z \in G \cdot z$, tj. $x \sim z$; relacija je tranzitivna.

Po definiciji je $y \in [x]_\sim \iff y \sim x \iff y \in G \cdot x$; dakle, $[x]_\sim = G \cdot x$. □

## D Klasovna jednakost, Košijeva teorema, ostale primene

Prema teoremi 1/38 orbite dejstva $G \curvearrowright X$ čine particiju skupa $X$. Ako su $x_i$, $i \in I$, predstavnici svih orbita (iz svake orbite smo izabrali po jedan element), onda imamo:

$$X = \bigsqcup_{i \in I} G \cdot x_i. \tag{\dagger}$$

Ako je $X$ konačan skup, onda je i $I$ konačan, i iz (†) i orbita-stabilizator teoreme imamo:

$$|X| = \sum_{i \in I} |G \cdot x_i| = \sum_{i \in I} |G : G_{x_i}|. \tag{\ddagger}$$

Ako je i $G$ konačna, prethodnu jednakost možemo da zapišemo i na sledeći način:

$$|X| = |G| \sum_{i \in I} \frac{1}{|G_{x_i}|},$$

jer je $|G : G_{x_i}| = \frac{|G|}{|G_{x_i}|}$. Jednakost (‡) zovemo klasovna jednakost za dejstvo $G \curvearrowright X$.

**1/39 Primer.**
Neka je $G$ konačna grupa. Posmatrajmo dejstvo $G \curvearrowright G$ konjugacijom iz primera 1/6: $g \cdot x = gxg^{-1}$. Neka su $x_i$, $i \in I$, predstavnici netrivijalnih orbita (tj. za $i \in I$, $G \cdot x_i \neq \{x_i\}$). (Primetimo da netrivijlane orbite postoje ako i samo ako je $G$ neabelova.) Tada je:

$$|G| = |Z(G)| + \sum_{i \in I} |G : C(x_i)|.$$

Primetimo da $x \in Z(G) \iff (\forall g \in G)\ gx = xg \iff (\forall g \in G)\ gxg^{-1} = x \iff (\forall g \in G)\ g \cdot x = x \iff G \cdot x = \{x\}$. Dakle, samo centralni elementi imaju trivijalne orbite i moraju biti predstavnici svojih obita.

Prema tome, $Z(G) \cup \{x_i \mid i \in I\}$ je skup predstavnika svih orbita. Prema klasovnoj jednakosti je:

$$|G| = \sum_{x \in Z(G) \cup \{x_i \mid i \in I\}} |G \cdot x| = \sum_{x \in Z(G)} |G \cdot x| + \sum_{i \in I} |G \cdot x_i| = \sum_{x \in Z(g)} 1 + \sum_{i \in I} |G : G_{x_i}| = |Z(G)| + \sum_{i \in I} |G : C(x_i)|,$$

gde poslednja jednakost važi jer je $G_{x_i} = C(x_i)$ prema primeru 1/28.

**1/40 Teorema.**
Neka je $G$ $p$-grupa, tj. $|G| = p^n$, gde je $p$ prost broj i $n \geqslant 1$. Tada $Z(G) \neq \{e\}$.

*Dokaz.* Kao u prethodnom primeru, neka su $x_i$, $i \in I$, predstavnici netrivijalnih orbita dejstva konjugacijom. Tada $x_i \notin Z(G)$ za $i \in I$, pa $C(x_i) \neq G$, odakle je $|G : C(x_i)| > 1$. Kako $|G : C(x_i)| \mid |G| = p^n$, zaključujemo $p \mid |G : C(x_i)|$. Pogledajmo jednakost is prethodnog primera:

$$p^n = |G| = |Z(G)| + \sum_{i \in I} |G : C(x_i)|.$$

Broj $p$ deli levu stranu, i, kako smo upravo videli, deli svaki sabirak sume na desnoj strani; sledi, $p \mid |Z(G)|$. Kako $|Z(G)| \geqslant 1$ jer uvek $e \in Z(G)$, mora biti $|Z(G)| \geqslant p$; centar je netrivijalan. □

**1/41 Posledica.**
Grupa reda $p^2$, $p$ je prost broj, je Abelova.

*Dokaz.* Neka je $|G| = p^2$. Netrivijalni elementi grupe $G$ su ili reda $p$ ili reda $p^2$. Ako postoji element reda $p^2$, $G$ je ciklična reda $p^2$, pa je specijalno Abelova. Preptostavimo da ne postoji element reda $p^2$; svi netrivijalni elmenti su reda $p$. Prema prethodnoj teoremi postoji netrivijalan element $a \in Z(G)$. Kako je $a$ reda $p$, možemo da izaberemo element $b \notin \langle a \rangle$. Kako $ab = ba$ jer $a \in Z(G)$, podgrupa $\langle a, b \rangle$ je Abelova. Takođe, $\langle a, b \rangle$ strogo je veća od $\langle a \rangle$ jer $b \notin \langle a \rangle$. Prema Lagranžovoj teoremi mora biti $|\langle a, b \rangle| = p^2$, odakle $G = \langle a, b \rangle$ je Abelova. □

Neka je $p$ prost broj i neka je $G$ konačna grupa. Neka je $X = \{(g_0, g_1, \ldots, g_{p-1}) \in G^p \mid g_0 g_1 \ldots g_{p-1} = e\}$. Posmatrajmo dejstvo $\mathbb{Z}_p \curvearrowright X$ iz primera 1/12: $k \cdot (g_0, g_1, \ldots, g_{p-1}) = (g_{k+0}, g_{k+1}, \ldots, g_{k+(p-1)})$ gde sabiramo u $\mathbb{Z}_p$. Setimo se da je $|X| = |G|^{p-1}$ (videti primer 1/12). U primeru 1/32 smo videli da za $\vec{g} = (g_0, g_1, \ldots, g_{p-1}) \in X$ imamo dve mogućnosti:

- ako je $g_0 = g_1 = \cdots = g_{p-1}$, $\mathbb{Z}_p \cdot \vec{g} = \{\vec{g}\}$ i $(\mathbb{Z}_p)_{\vec{g}} = \mathbb{Z}_p$;
- ako $g_0, g_1 \ldots, g_{p-1}$ nisu svi jednaki, $|\mathbb{Z}_p \cdot \vec{g}| = p$ i $(\mathbb{Z}_p)_{\vec{g}}$ je trivijalan.

Neka je $X_1 = \{\vec{g} \in X \mid g_0 = g_1 = \cdots = g_{p-1}\}$ skup elemenata sa jednočlanom orbitom, i neka je $X_p$ skup predstavnika svih $p$-točlanih orbita; tada je $X_1 \cup X_p$ skup predstavnika svih orbita. Prema (†) imamo:

$$X = \bigsqcup_{\vec{g} \in X_1} \mathbb{Z}_p \cdot \vec{g} \sqcup \bigsqcup_{\vec{g} \in X_p} \mathbb{Z}_p \cdot \vec{g},$$

odakle je:

$$|G|^{p-1} = |X| = \sum_{\vec{g} \in X_1} 1 + \sum_{\vec{g} \in X_p} p = |X_1| + p|X_p|. \qquad (\star)$$

**1/42 Teorema** (Mala Fermaova teorema)**.**
Ako je $p$ prost broj i $p \nmid n$, onda $n^{p-1} = 1 \mod p$.

*Dokaz.* Uzmimo $G = \mathbb{Z}_n$. Iz $(\star)$ imamo:

$$n^{p-1} = |X_1| \mod p.$$

Dovoljno je da dokažemo $|X_1| = 1$. Neka $\vec{g} \in X_1$. Tada $\vec{g} = (\underbrace{a, a, \ldots, a}_{p})$, gde $a \in \mathbb{Z}_n$, i $a + a + \cdots + a = 0$, tj. $pa = 0$. (Primetite da s obzirom da radimo u grupi $G = \mathbb{Z}_n$, notacija je aditivna.) Međutim, $pa = 0$ znači da red od $a$ u $\mathbb{Z}_n$ deli $p$, a takođe deli i $n$ po Lagranžovoj teoremi, pa kako $p \nmid n$ mora biti da je $a$ element reda 1, tj. $a = 0$. Odavde vidimo da je $X_1 = \{(0, 0, \ldots, 0)\}$, i $|X_1| = 1$. □

**1/43 Teorema** (Vilsonova teorema)**.**
Ako je $p$ prost broj, onda $(p-1)! = -1 \mod p$.

*Dokaz.* Uzmimo $G = \mathbb{S}_p$. Iz $(\star)$ imamo:

$$(p!)^{p-1} = |X| = |X_1| + p|X_p|,$$

odakle $|X_1| = 0 \mod p$. Dovoljno je da izračunamo $X_1$ u ovom slučaju. Primetimo $\vec{g} = (\underbrace{\sigma, \sigma, \ldots, \sigma}_{p}) \in X_1$ ako i samo ako $\sigma^p = [\,]$, ako i samo ako $\sigma = [\,]$ ili $\sigma$ je reda $p$. Jedine permutacije u $\mathbb{S}_p$ reda $p$ su $p$-ciklovi, i njih ima $(p-1)!$. Dakle, $|X_1| = 1 + (p-1)!$, odakle sledi teorema. □

**1/44 Teorema** (Košijeva teorema)**.**
Ako je $p$ prost broj i $p \mid |G|$, onda $G$ ima element reda $p$.

*Dokaz.* Prema $(\star)$, $|G|^{p-1} = |X_1| + p|X_p|$, odakle $p \mid |X_1|$ jer $p \mid |G|$. Primetimo $\vec{g} = (a, a, \ldots, a) \in X_1$ ako i samo ako $a^p = e$, ako i samo ako $a = e$ ili $a$ je reda $p$. Odavde $|X_1| \geqslant 1$ jer $(e, e, \ldots, e) \in X_1$, pa kako $p \mid |X_1|$ mora biti $|X_1| \geqslant p$, a to znači i da za neko $a \neq e$, $(a, a, \ldots, a) \in X_1$, a to znači da je $a$ reda $p$. □

## E Broj orbita, Bernsajdova lema

U ovom delu $G$ i $X$ su konačni.

**1/45 Definicija.** Neka $G \curvearrowright X$ i $g \in G$.

(a) Skup fiksnih tačaka od $g$ je skup:

$$X_g := \{x \in X \mid g \cdot x = x\} \subseteq X.$$

(b) Sa $o(G \curvearrowright X)$ obeležavamo broj orbita dejstva $G \curvearrowright X$.

**1/46 Teorema** (Bernsajdova lema)**.**
Neka $G \curvearrowright X$. Tada:

$$o(G \curvearrowright X) = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

*Dokaz.* Posmatrajmo skup $S = \{(g, x) \in G \times X \mid g \cdot x = x\}$. Skup $S$ možemo da napišemo kao disjunktnu uniju na dva načina:

$$S = \bigsqcup_{g \in G} \{(g, x) \mid x \in X,\ g \cdot x = x\},$$

i kao:

$$S = \bigsqcup_{x \in G} \{(g, x) \mid g \in G,\ g \cdot x = x\}.$$

Primetimo da je $|\{(g,x) \mid x \in X,\, g \cdot x = x\}| = |X_g|$, a daje $|\{(g,x) \mid g \in G,\, g \cdot x = x\}| = |G_x|$. Odatle je:

$$\sum_{g \in G} |X_g| = |S| = \sum_{x \in X} |G_x|.$$

Kako je $|G_x| = \frac{|G|}{|G \cdot x|}$ is orbita-stabilizator teoreme, iz prethodne jednakosti, posle kratkog sređivanja, dobijamo:

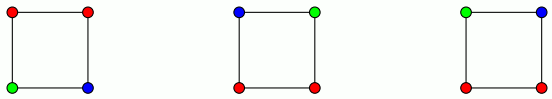
$$\frac{1}{|G|} \sum_{g \in G} |X_g| = \sum_{x \in X} \frac{1}{|G \cdot x|}.$$

Prema tome, dovoljno je da dokažemo da je suma na desnoj strani jednaka $o(G \curvearrowright X)$. Ako sa $\mathcal{O}$ označimo familiju svih orbita, desnu stranu gornje jednakosti računamo na sledeći način:

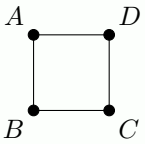
$$\sum_{x \in X} \frac{1}{|G \cdot x|} = \sum_{O \in \mathcal{O}} \sum_{x \in O} \frac{1}{|G \cdot x|} = \sum_{O \in \mathcal{O}} \sum_{x \in O} \frac{1}{|O|} = \sum_{O \in \mathcal{O}} \frac{1}{|O|} \sum_{x \in O} 1 = \sum_{O \in \mathcal{O}} \frac{1}{|O|} |O| = \sum_{O \in \mathcal{O}} 1 = |\mathcal{O}| = o(G \curvearrowright X).$$

Završili smo dokaz. □

**1/47 Primer.**
Na koliko načina možemo da obojimo temena kvadrata u tri boje (crvena, zelena i plava) ako smatramo da su dva kvadrata jednako obojena ako rotacijom ili osnom simetrijom jednog možemo da dobijemo drugi. Npr. sledeća tri kvadrata su isto obojena.

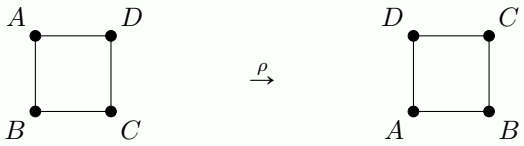


Označimo temena kvadrata sa $A, B, C, D$:

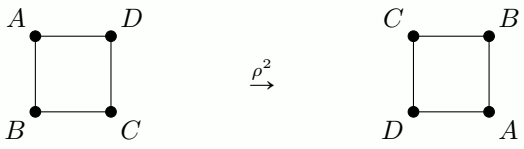



Neka je $X$ skup svih kvadrata sa obojenim temenima u tri boje; primetimo da je $|X| = 3^4 = 81$. Neka $\mathbb{D}_4 \curvearrowright X$ na prirodan način. Po uslovu zadatka dva kvadrata iz $X$ su jednako obojena ako i samo ako se nalaze u istoj orbiti. Prema tome, problem se svodi na računanje broja $o(\mathbb{D}_4 \curvearrowright X)$. Prema Bernsajdovoj lemi potrebno je da izračunamo $|X_g|$ za sve $g \in \mathbb{D}_4$.

- $|X_\varepsilon|$. Svaki kvadrat je fiksiran sa $\varepsilon$, pa je $X_\varepsilon = X$, tj. $|X_\varepsilon| = 81$.
- $|X_\rho|$. Rotacija $\rho$ se ponaša kao cikl $\lfloor ABCD \rceil$:

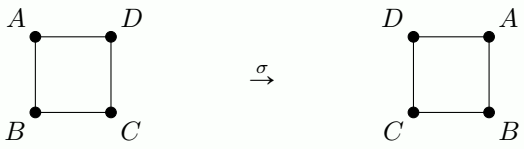



  Da bi $\rho$ fiksirala obojeni kvadrat mora biti boja od $A$ jednaka boji od $D$, boja od $B$ jednaka boji od $A$, boja od $C$ jednaka boji od $B$ i boja od $D$ jednaka boji od $C$; dakle, sva temena moraju biti isto obojena, i imamo samo tri načina za ovo: $|X_\rho| = 3$.
- Slično, $|X_{\rho^3}| = 3$.
- $|X_{\rho^2}|$. Rotacija $\rho^2$ se ponaša kao dupli cikl $\lfloor AC \rceil \lfloor BD \rceil$:



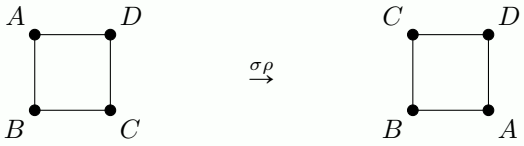

Da bi $\rho^2$ fiksirala obojeni kvadrat moraju $A$ i $C$ biti isto obojeni, i $B$ i $D$ isto obojeni; imamo $3^2$ mogućnosti, tj. $|X_{\rho^2}| = 9$.

- $|X_\sigma|$, gde je $\sigma$ osna simetrija u odnosu na vertikalnu osu; $\sigma$ se ponaša kao dupli cikl $\lfloor AD \rfloor \lfloor BC \rfloor$:




Da bi $\sigma$ fiksirala obojeni kvadrat $A$ i $D$ moraju biti jednako obojeni, i $B$ i $C$ jednako obojeni; $|X_\sigma| = 9$.

- Slično, $|X_{\sigma\rho^2}| = 9$, gde je $\sigma\rho^2$ osna simetrija u odnosu na horizontalnu osu.
- $|X_{\sigma\rho}|$, gde je $\sigma\rho$ osna simetrija u odnosu na dijagonalu $BD$, tj. ponaša se kao transpozicija $\lfloor AC \rfloor$:



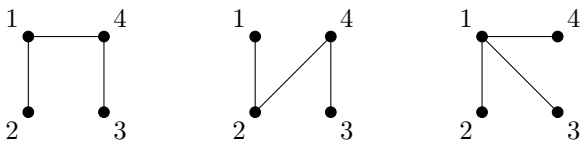

Da bi $\sigma\rho$ fiksirala obojeni kvadrat moraju $A$ i $C$ biti jednako obojeni, a $B$ i $D$ proizvoljno; imamo $3^3$ mogućnosti, tj. $|X_{\sigma\rho}| = 27$.

- Slično, $|X_{\sigma\rho^3}| = 27$.

Iz Bernsajdove leme imamo:

$$o(\mathbb{D}_4 \curvearrowright X) = \frac{1}{8}(81 + 3 + 3 + 9 + 9 + 9 + 27 + 27) = \frac{168}{8} = 21.$$

Graf je skup $V$ na kome je definisana irefleksivna, simetrična relacija $E$; ako su $x, y \in V$ (čvorovi grafa) u relaciji $E$, to crtamo kao liniju između $x$ i $y$ (ivica grafa). Dva grafa na istom skupu su izomorfna ako postoji permutacija čvorova tako da od prvog grafa dobijemo drugi. Npr. prva dva grafa na skupu $V = [4]$ na sledećoj slici su međusobno izomorfna (izomorfizam je dat permutacijom $\lfloor 12 \rfloor$), i neizomorfni su sa trećim:




**1/48 Primer.**
Koliko ima neizomorfnih grafova na četvoroelementnom skupu $V = [4]$?
Neka je $X$ skup svih grafova na $[4]$; kako imamo šest parova čvorova, i za svaki od njih možemo da odlučimo da li postoji ili ne postoji ivica između čvorova tog para, vidimo da je $|X| = 2^6 = 64$. Neka $\mathbb{S}_4 \curvearrowright X$ na prirodan način. Primetimo da su dva grafa izomorfna ako i samo ako prioadaju istoj orbiti, prema tome problem se svodi na računanje $o(\mathbb{S}_4 \curvearrowright X)$, za šta ćemo iskoristiti Bernsajdovu lemu.
Grupa $\mathbb{S}_4$ ima pet tipova permutacija: ima šest 4-cikla, osam 3-cikla, šest transpozicija, dve duple transpozi-

cije i jednu koincidenciju. Nije teško videti da $|X_\sigma|$ zavisi od tipa ciklusne dekompozicije (a ne od konkretne permutacije tog tipa). Tako da nema potrebe da računamo $|X_\sigma|$ za sve permutacije $\sigma$, dovoljno je za pet predstavnika navedenih tipova. Označimo sa $e_{ij}$, $i < j$, ivicu između čvorova $i$ i $j$; $e_{ij}$ može i ne mora da postoji u grafu.

- $\sigma = [1234]$ je 4-cikl. Permutacija $\sigma$ na ivicama grafa deluje kao permutacija $[e_{12}e_{23}e_{34}e_{14}][e_{13}e_{24}]$. Da bi $\sigma$ fiksirala graf ivice iz prvog cikla ili sve postoje ili nijedna ne postoji, i isto važi za ivice drugog cikla. Dakle, imamo dva izbora, tj. $2^2$ grafova koji su fiksirani sa $\sigma$: $|X_\sigma| = 4$.
- $\sigma = [123]$ je 3-cikl. Na ivicama grafa $\sigma$ deluje kao permutacija $[e_{12}e_{23}e_{13}][e_{14}e_{24}e_{34}]$. Kao i malopre, da bi $\sigma$ fiksirala graf, ivice iz prvog cikla ili sve postoje ili nijedna ne postoji, i slično za drugi cikl; imamo dva izbora, tj. $|X_\sigma| = 2^2 = 4$.
- $\sigma = [12]$ je transpozicija. Na ivicama grafa $\sigma$ deluje kao permutacija $[e_{12}][e_{13}e_{23}][e_{14}e_{24}][e_{34}]$. Za svaki od ciklova (njih četiri; dva su trivijalni) imamo mogućnost da izaberemo da li ivice u njemu postoje ili ne; $|X_\sigma| = 2^4 = 16$.
- $\sigma = [12][34]$ je dupla transpozicija. Na ivicama grafa $\sigma$ deluje kao permutacija $[e_{12}][e_{13}e_{24}][e_{14}e_{23}][e_{34}]$. Kao i malopre, $|X_\sigma| = 2^4 = 16$.
- $\sigma = []$ je koincidencija. Kako $\sigma$ fiksira svih šest ivica, za svaku možemo da izaberemo da li postoji ili ne; $|X_\sigma| = 2^6 = 64$.

Prema Bernsajdovoj lemi broj orbita jednak je:

$$o(\mathbb{S}_4 \curvearrowright X) = \frac{1}{24}(6 \cdot 4 + 8 \cdot 4 + 6 \cdot 16 + 3 \cdot 16 + 64) = \frac{264}{24} = 11.$$

Dakle imamo 11 neizomorfnih grafova na četvoroelementnom skupu.

# 2 Teoreme Silova

**2/1 Definicija.** Neka je $G$ konačna grupa i neka $|G| = p^m \cdot n$ gde je $p$ prost broj i $(p, n) = 1$, tj. $p \nmid n$.

(a) Za podgrupu $H \leqslant G$ kažemo da je $p$-podgrupa ako je reda $p^k$ za neko $k \leqslant m$.

(b) Za podgrupu $H \leqslant G$ kažemo da je Silovljeva $p$-podgrupa ili $S_p$-podgrupa ako je reda $p^m$.

(c) Sa $Syl_p(G)$ označavamo skup svih $S_p$-podgrupa od $G$, a sa $s_p$ obeležavamo njihov broj $s_p := |Syl_p(G)|$.

Primetimo da *a priori* ne znamo da li je $Syl_p(G)$ prazna familija.

## A Prva teorema Silova

**2/2 Teorema** (Prva teorema Silova)**.**
Neka $p \mid |G|$, tada $Syl_p(G) \neq \varnothing$.

*Prvi dokaz prve teoreme Silova.* Dokaz izvodimo putpunom indukcijom po $|G|$. Neka je $|G| = p^m \cdot n$, $p \nmid n$. Imamo dva slučaja.

1. slučaj: $p \mid |Z(G)|$. Po Košijevoj teoremi, $Z(G)$ ima element $a$ reda $p$. Tada je $\langle a \rangle \lhd G$ i $G/\langle a \rangle$ je grupa reda $p^{m-1} \cdot n$. Po indukcijskoj hipotezi $G/\langle a \rangle$ ima podgrupu $\tilde{H}$ reda $p^{m-1}$ (ako $m = 1$, ta podgrupa je trivijalna). Tada je $H := \pi^{-1}[\tilde{H}]$ podgrupa od $G$ reda $p^m$, gde je $\pi : G \to G/\langle a \rangle$ kanonska projekcija.

2. slučaj: $p \nmid |Z(G)|$. Posmatrajmo dejstvo konjugacijom $G \curvearrowright G$. Prema primeru 1/39 znamo da je:

$$|G| = |Z(G)| + \sum_{i \in I} |G : G_{x_i}|,$$

gde su $x_i$, $i \in I$, predstavnici netrivijalnih orbita. Kako $p \mid |G|$ i $p \nmid |Z(G)|$, za neko $i \in I$ imamo $p \nmid |G : G_{x_i}|$. Kako je $|G : G_{x_i}| = \frac{|G|}{|G_{x_i}|}$, $p^m \mid |G|$ i $p \nmid |G : G_{x_i}|$, zaključujemo $p^m \mid |G_{x_i}|$. Sa druge strane, kako $x_i$ ima netrivijalnu orbitu, prema orbita-stabilizator teoremi $|G_{x_i}| < |G| = p^m \cdot n$. Dakle, $|G_{x_i}| = p^m \cdot n'$, gde $n' < n$. Po indukcijskoj hipotezi $G_{x_i}$ ima podgrupu $H$ reda $p^m$, a ona je naravno podgrupa i od $G$. Završili smo dokaz. □

Daćemo još jedan dokaz prve teoreme Silova, za koji nam je potrebna sledeća lema.

**2/3 Lema.**
Neka je $p$ prost broj, $m \geqslant 0$ i $n \geqslant 1$. Tada:

$$\binom{p^m \cdot n}{p^m} \equiv n \mod p.$$

*Dokaz.* Primetimo najpre da za $1 \leqslant k \leqslant p$, $p \mid \binom{p}{k}$. Zaista, kako je $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ i $k, p-k < p$, prost broj $p$ iz brojioca se ne skraćuje, pa $p \mid \binom{p}{k}$. Koristeći ovu činjenicu i binomnu teoremu imamo:

$$(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} x^k \equiv x^p + 1 \mod p.$$

Sada indukcijom možemo da vidimo da $(x+1)^{p^m} \equiv x^{p^m} + 1 \mod p$. Zaista, baza $m = 0$ je trivijalna, a u koraku imamo:

$$(x+1)^{p^{m+1}} = \left((x+1)^{p^m}\right)^p \overset{IH}{\equiv} \left(x^{p^m} + 1\right)^p \mod p \equiv x^{p^{m+1}} + 1 \mod p,$$

gde smo u poslednjem koraku iskoristili gornju jednakost.

Nas zanima koeficijent uz $x^{p^m}$ u razvoju $(x+1)^{p^m \cdot n}$ modulo $p$. Prema prethodno dokazanom imamo:

$$(x+1)^{p^m \cdot n} = \left((x+1)^{p^m}\right)^n \equiv \left(x^{p^m} + 1\right)^n \mod p,$$

a koeficijent uz $x^{p^m}$ u razvoju $(x^{p^m} + 1)^n$ je $\binom{n}{1} = n$. Dakle, $\binom{p^m \cdot n}{p^m} \equiv n \mod p$. □

*Drugi dokaz prve teoreme Silova.* Neka je $|G| = p^m \cdot n$, $m \geqslant 1$, $p \nmid n$. Neka je $X = [G]^{p^m}$ – familija svih $p^m$-točlanih podskupova u $G$. Prema prethodnoj lemi, $|X| = \binom{p^m \cdot n}{p^m} \equiv n \mod p$, pa $p \nmid n$ povlači $p \nmid |X|$.

Posmatrajmo dejstvo $G \curvearrowright X$ dato sa $g \cdot S := gS := \{gx \mid x \in S\}$. (Ovo je dejstvo iz zadatka 1/16(b) indukovano dejstvom grupe $G$ na sebe množenjem sleva iz primera 1/5.) Iz klasovne jednakosti znamo da je $|X|$ jednak zbiru kardinalnosti svih orbita; kako $p \nmid |X|$, postoji orbita $G \cdot S$ takva da $p \nmid |G \cdot S|$. Prema orbita-stabilizator teoremi znamo $|G| = |G \cdot S| \cdot |G_S|$, pa kako $p^m \mid |G|$ i $p \nmid |G \cdot S|$, zaključujemo $p^m \mid |G_S|$; specijalno, $|G_S| \geqslant p^m$. Sa druge strane, za fiksirano $x \in S$, za bilo koje $g \in G_S$ imamo $gx \in gS = g \cdot S = S$, pa $G_S x \subseteq S$; odatle, $|G_S| = |G_S x| \leqslant |S| = p^m$. Dakle, $|G_S| = p^m$, pa kako je $G_S \leqslant G$ (tvrđenje 1/33(a)), zaključujemo $G_S \in Syl(G)$. □

**2/4 Komentar.** Primetimo da smo drugi dokaz izveli bez korišćenja Košijeve teoreme. Prateći ovakav pristup, Košijevu teoremu lako možemo da izvedemo iz prve teoreme Silova. Naime, neka $p \mid |G|$. Prema prvoj teoremi Silova izaberimo $H \in Syl_p(G)$, i izaberimo netrivijalan element $a \in H$. Kako je $|H| = p^m$, po Lagranžovoj teoremi red elementa $a$ je $p^k$ za neko $1 \leqslant k \leqslant m$. Tada je $a^{p^{k-1}}$ element reda $p$.

## B Druga i treća teorema Silova

**2/5 Lema.**
Neka $|G| = p^m \cdot n$, $p \nmid n$, i $P \in Syl_p(G)$. Ako je $a$ element reda $p^k$ i $aPa^{-1} = P$, onda $a \in P$.

*Dokaz.* Primetimo da je $k \leqslant m$. Uslov $aPa^{-1} = P$ povlači $\langle a\rangle P = P\langle a\rangle$, što je dovoljno da zaključimo da je $\langle a\rangle P \leqslant G$. Takođe je $|\langle a\rangle \cap P| = p^l$, za neko $l \leqslant k$ jer je $\langle a\rangle \cap P \leqslant \langle a\rangle$. Imamo:

$$|\langle a\rangle P| = \frac{|\langle a\rangle| \cdot |P|}{|\langle a\rangle \cap P|} = \frac{p^k \cdot p^m}{p^l} \geqslant p^m.$$

Dakle, $\langle a\rangle P$ je $p$-nadgrupa $S_p$-podgrupe $P$, pa mora biti $\langle a\rangle P = P$ zbog maksimalnosti $P$. Dakle, $a \in P$. □

**2/6 Definicija.** Neka $p \mid |G|$, $p$ je prost broj, i $P \in Syl_p(G)$. Reći ćemo da je skup $S \subseteq Syl_p(G)$ $P$-invariantan ako je zatvoren za dejstvo $P \curvearrowright Syl_p(G)$ konjugacijom (za $a \in P$ i $Q \in Syl_p(G)$, $a \cdot Q := aQa^{-1}$). Drugim rečima, $Q \in S$ povlači $P \cdot Q \subseteq S$. Trećim rečima, $S$ je unija nekoliko orbita tog dejstva.

**2/7 Lema.**
Neka $p \mid |G|$, $p$ je prost broj, i $P \in Syl_p(G)$. Neka je $S \subseteq Syl_p(G)$ $P$-invarijantan. Tada:

- ako $P \in S$, $|S| = 1 \mod p$;
- ako $P \notin S$, $p \mid |S|$.

*Dokaz.* U skladu sa prethodnom definicijom, govorimo o dejstvu $P \curvearrowright Syl_p(G)$ konjugacijom.

Prvo primetimo $|P \cdot Q| = 1$ ako i samo ako $Q = P$. Smer ($\Leftarrow$) je očigledan. Za ($\Rightarrow$), za svako $a \in P$ imamo $a \cdot Q = Q$, tj. $aQa^{-1} = Q$, pa kako je $a$ element reda $p^k$ jer je iz $P$, prema lemi 2/5, $a \in Q$. Dakle, $P \subseteq Q$, pa kako su obe Silovljeve podgrupe, specijalno istog su reda, važi $P = Q$.

Sa druge strane, ako $|P \cdot Q| > 1$, prema orbita-stabilizator teoremi $|P \cdot Q| = |P : P_Q| \mid |P|$, pa imamo $p \mid |P \cdot Q|$.

Dakle, jedina jednočlana orbita je $P \cdot P = \{P\}$, sve ostale orbite su kardinalnosti deljive sa $p$. Kako je $S$ unija nekoliko orbita, ako $P \in S$, mora biti $|S| = 1 \mod p$, a ako $P \notin S$, mora biti $|S| = 0 \mod p$. □

**2/8 Teorema** (Druga teorema Silova)**.**
Neka $p \mid |G|$, $p$ je prost broj. Svake dve $S_p$-podgrupe su međusobno konjugovane.

*Dokaz.* Posmatrajmo dejstvo $G \curvearrowright Syl_p(G)$ dato konjugacijom: $a \cdot Q = aQa^{-1}$; treba da dokažemo da ovo dejstvo ima jednu orbitu. Pretpostavimo suprotno. Neka $P, Q \in Syl_p(G)$ imaju različite orbite. Primetimo da je orbita $G \cdot P$ i $P$-invarijantna i $Q$-invarijantna. Prema lemi 2/7, $P \in G \cdot P$ povlači $|G \cdot P| = 1 \mod p$, a $Q \notin G \cdot P$ povlači $p \mid |G \cdot P|$. Kontradikcija. □

**2/9 Teorema** (Treća teorema Silova)**.**
Neka $|G| = p^m \cdot n$, $p$ je prost broj, i $p \nmid n$.

(a) $s_p = 1 \mod p$;

(b) za $P \in Syl_p(G)$, $|G : N(P)| = s_p$;

(c) $s_p \mid n$.

*Dokaz.* (a) Neka je $P \in Syl_p(G)$ proizvoljna. Kako je $Syl_p(G)$ očigledno $P$-invarijantan, prema lemi 2/7, $s_p = |Syl_p(G)| = 1 \mod p$.

(b) Posmatrajmo dejstvo $G \curvearrowright Syl_p(G)$ dato konjugacijom: $a \cdot Q = aQa^{-1}$. Neka je $P \in Syl_p(G)$ i izračunajmo $G_P$. Imamo $a \in G_P \iff aPa^{-1} = P \iff a \in N(P)$. Dakle, $G_P = N(P)$, pa je $|G : N(P)| = |G : G_P| = |G \cdot P| = s_p$, gde druga jednakost važi prema orbita-stabilizator teoremi, a poslednja jednakost važi prema drugoj teoremi Silova jer ovo dejstvo ima samo jednu orbitu, pa je $G \cdot P = Syl_p(G)$.

(c) Prema (b), $s_p \mid |G| = p^m \cdot n$, a prema (a), $p \nmid s_p$. Dakle, $s_p \mid n$. □

**2/10 Posledica.**
Neka $p \mid |G|$, $p$ je prost broj, i neka $P \in Syl_p(G)$. Tada $P \lhd G$ ako i samo ako $s_p = 1$.

*Dokaz.* Prema trećoj teoremi Silova, $s_p = 1 \iff |G : N(P)| = 1 \iff G = N(P) \iff P \lhd G$. (Alternativno, prema drugoj teoremi Silova, $P \lhd G \iff Syl_p(G) = \{P\} \iff s_p = 1$.) □

**2/11 Posledica.**
Neka $p \mid |G|$, $p$ je prost broj, i $H \leqslant G$ je $p$-podgrupa od $G$. Tada je $H$ sadržana u nekoj $S_p$-podgrupi od $G$.

*Dokaz.* Posmatrajmo dejstvo $H \curvearrowright Syl_p(G)$ dato konjugacijom: $h \cdot Q = hQh^{-1}$. Neka su $Q_i$, $i \in I$, predstavnici svih orbita. Kako $|H \cdot Q_i| = |H : H_{Q_i}| \mid |H|$ i $H$ je $p$-podgrupa, svaka orbita je kardinalnosti ili 1 ili stepen od $p$. Prema klasovnoj jednakost $s_p = |Syl_p(G)| = \sum_{i \in I} |H \cdot Q_i|$, a prema trećoj teoremi Silova $s_p = 1 \mod p$; dakle, ne mogu svi sabirci na desnoj strani da budu stepeni od $p$. Dakle, postoji $i \in I$ tako da je $H \cdot Q_i = \{Q_i\}$. To znači da za svako $h \in H$ važi $hQ_ih^{-1} = Q_i$, pa prema lemi 2/5, $h \in Q_i$. Prema tome, $H \subseteq Q_i$. □

## C Primene teorema Silova

**2/12 Definicija.** Grupa $G$ je *prosta* ako nema pravu netrivijalnu normalnu podgrupu: ne postoji $H \lhd G$ takva da $\{e\} \lneqq H \lneqq G$.

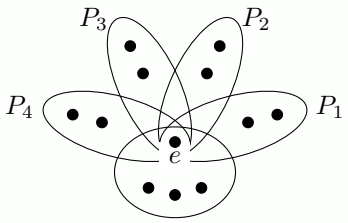
Primeri prostih grupa su grupe prostog reda, tj. ciklične grupe $\mathbb{Z}_p$. One uopšte nemaju pravu netrivijalnu podgrupu, pa nemaju ni normalnu takvu. Abelove grupe, različite od $\mathbb{Z}_p$ nisu proste. Naime, ako je $G$ Abelova grupa koja nije prostog reda, prema Košijevoj teoremi možemo da nađemo element $a \in G$ koji jeste prostog reda; tada je $\langle a \rangle \lhd G$ jer je $G$ Abelova, i $\{e\} \lneqq H \lneqq G$. Dakle, pitanje da li je neka grupa prosta je zanimljivo za neabelove grupe.

**2/13 Primer.**
Grupe reda $p^n$, $p$ je prost broj i $n \geqslant 2$, nisu proste.
Pretpostavimo da je $G$ neabelova grupa reda $p^n$. (Dakle, možemo da kažemo da je i $n \geqslant 3$ prema posledici 1/41.) Videli smo u teoremi 1/40 da je $Z(G)$ netrivijalan, pa kako je on i prava podgrupa jer je $G$ neabelova, našli smo pravu netrivijalnu normalnu podgrupu.

**2/14 Primer.**
Grupe reda $pq^m$, $p < q$ su prosti brojevi i $m \geqslant 1$, nisu proste.
Po trećoj teoremi Silova $s_q = 1 \mod q$ i $s_q \mid p$, pa kako je $p < q$ mora biti $s_q = 1$. Dakle $S_q$-podgrupa od $G$ je prava netrivijalna normalna podgrupa.

**2/15 Primer.**
Grupe reda $p^2q^m$, $p < q$ su prosti brojevi i $m \geqslant 1$, nisu proste.
Po trećoj teoremi Silova $s_q = 1 \mod q$ i $s_q \mid p^2$, pa kako je $p < q$ može biti $s_q = 1$, u kom slučaju smo

završili – $S_q$-podgrupa je prava netrivijalna normalna podgrupa, ili može biti $s_q = p^2$ pod uslovom da $p^2 = 1 \mod q$. Međutim, ovo povlači $q \mid p^2 - 1 = (p-1)(p+1)$, pa kako je $q$ prost i $p < q$ mora biti $q \mid p+1$, a ovo je jedino moguće ako $p = 2$ i $q = 3$.
Pretpostavimo da je $|G| = 2^2 \cdot 3^m$ i $m \geqslant 2$. Prema prethodnom pasusu možemo da pretpostavimo $s_3 = 4$. Neka je $P$ neka $S_3$-podgrupa. Prema trećoj teoremi Silova $|G : N(P)| = s_3 = 4$, pa prema $n!$-teoremi $|G : Core(N(P))| \mid 4! = 24 = 2^3 \cdot 3$. Kako $3^2 \mid |G|$, zaključujemo da $3 \mid |Core(N(P))|$. Dakle, $Core(N(P))$ je netrivijalna podgrupa. Kako je $Core(N(P)) \subseteq N(P) \subsetneq G$ jer $|G : N(P)| = 4$, $Core(N(P))$ je i prava podgrupa. Kako je jezgro uvek normalna podgrupa, završili smo posao.
Dakle, imamo jedan specijalan slučaj da razmotrimo: $|G| = 12 = 2^2 \cdot 3$. Ponovo možemo da pretpostavimo $s_3 = 4$. Neka su $P_1, \ldots, P_4$ sve $S_3$-podgrupe. Kako su sve one reda tri, dakle ciklične prostog reda, međusobno se seku samo po neutralu pa $|P_1 \cup \cdots \cup P_4| = 4 \cdot 2 + 1 = 9$.




Tada preostala tri elementa, zajedno sa neutralom, mogu da formiraju samo jednu podgrupu reda 4, tj. samo jednu $S_2$-podgrupu. Dakle, $s_2 = 1$, odakle je $S_2$-podgrupa prava netrivijalna normalna podgrupa.

**2/16 Primer.**
Grupe reda $2^3 \cdot p^m$, $2 < p$ je prost broj i $m \geqslant 1$, nisu proste.
Kako $s_p \mid 2^3$ imamo $s_p \in \{1, 2, 4, 8\}$, a kako $s_p = 1 \mod p$ imamo sledeće slučajeve.

- Za $p = 5$ ili $p > 7$, $s_p = 1$, pa je $S_p$-podgrupa jedinstvena i normalna, i završili smo.
- Za $p = 7$, $s_7 \in \{1, 8\}$; ako $s_7 = 1$ završavamo kao u prethodnoj tački, pa pretpostavimo $s_7 = 8$.
  - Ako $m \geqslant 2$, uzmimo neku $S_7$-podgrupu $P$, imamo $|G : N(P)| = 8$ prema trećoj teoremi Silova, pa $|G : Core(N(P))| \mid 8!$ prema $n!$-teoremi, odakle $7 \mid |Core(N(P))|$ jer $m \geqslant 2$. Dakle, lako vidimo da je $Core(N(P))$ prava netrivijalna normalna podgrupa, i završili smo.
  - Imamo specijalan slučaj $|G| = 56 = 2^3 \cdot 7$. Neka su $P_1, \ldots, P_8$ sve $S_7$-podgrupe; kako su sve one ciklične prostog reda 7, međusobno se seku samo po neutralu, pa $|P_1 \cup \cdots \cup P_8| = 8 \cdot 6 + 1 = 49$. To znači da u $G$ preostaje sedam elemenata, koji zajedno sa neutralom mogu da formiraju samo jednu $S_2$-podgrupu. Dakle, $s_2 = 1$, pa je $S_2$-podgrupa prava netrivijalna normalna podgrupa.
- Za $p = 3$, $s_3 \in \{1, 4\}$; ako $s_3 = 1$ završavamo kao u prvoj tački, pa pretpostavimo $s_3 = 4$.
  - Ako $m \geqslant 2$, uzmimo neku $S_3$-podgrupu $P$, imamo $|G : N(P)| = 4$ prema trećoj teoremi Silova, pa $|G : Core(N(P))| \mid 4!$ prema $n!$-teoremi, odakle $3 \mid |Core(N(P))|$ jer $m \geqslant 2$. Dakle, $Core(N(P))$ je prava netrivijalna normalna podgrupa.
  - Imamo specijalan slučaj $|G| = 24 = 2^3 \cdot 3$. Možemo da postupimo kao u prethodnom slučaju posmatrajući $S_2$-podgrupu. Ako je $s_2 = 1$, završili smo. Preostala mogućnost je $s_2 = 3$. Neka je $Q$ neka $S_2$-podgrupa; imamo $|G : N(Q)| = 3$ prema trećoj teoremi Silova, pa $|G : Core(N(Q))| \mid 3!$ prema $n!$-teoremi, odakle $4 \mid |Core(N(Q))|$. Dakle, $Core(N(Q))$ je prava netrivijalna normalna podgrupa.

**2/17 Zadatak.** Ako $|G| < 60$ i $|G|$ nije prost broj, dokazati da $G$ nije prosta.

# 3 Alternirajuće grupe

Dokazaćemo da grupe $\mathbb{A}_n$, $n \geqslant 5$, nisu proste. Broj $n \geqslant 5$ je fiksiran.

**3/1 Lema.**
Ako $N \lhd \mathbb{A}_n$ sadrži 3-cikl, onda $N = \mathbb{A}_n$.

*Dokaz.* Nakon prenumeracije skupa $\{1, 2, \ldots, n\}$, možemo da pretpostavimo $\lfloor 123 \rfloor \in N$. Neka su $i, j > 3$ i $i \neq j$; imamo $\lfloor 3ij \rfloor \lfloor 123 \rfloor \lfloor 3ij \rfloor^{-1} = \lfloor 12i \rfloor$, pa kako $\lfloor 3ij \rfloor \in \mathbb{A}_n$ i $N$ je normalna, $\lfloor 12i \rfloor \in N$. Kako ovi 3-ciklovi generišu $\mathbb{A}_n$ zaključujemo $N = \mathbb{A}_n$. □

**3/2 Lema.**
Ako $N \lhd \mathbb{A}_n$, gde $n = 5$ ili $n = 6$, i $N \neq \langle \lfloor \rfloor \rangle$, onda $N = \mathbb{A}_n$.

*Dokaz.* Dovoljno je da nađemo 3-cikl u $N$ prema lemi 3/1. Kako je $N$ netrivijalna mora da sadrži nešto od sledećih permutacija:

(a) 3-cikl;

(b) duplu transpoziciju;

(c) 5-cikl;

(d) dupli 3-cikl u slučaju $n = 6$;

(e) proizvod 4-cikla i 2-cikla u slučaju $n = 6$.

Kao što smo već rekli, slučaj (a) povlači $N = \mathbb{A}_n$.

(b) Pretpostavimo da $N$, posle prenumeracije skupa $\{1, 2, \ldots, n\}$, sadrži $x = \lfloor 12 \rfloor \lfloor 34 \rfloor$. Zbog normalnosti sadrži i $y = \lfloor 125 \rfloor x \lfloor 125 \rfloor^{-1} = \lfloor 25 \rfloor \lfloor 34 \rfloor$, pa sadrži i:

$$xy = \lfloor 12 \rfloor \lfloor 34 \rfloor \lfloor 25 \rfloor \lfloor 34 \rfloor = \lfloor 125 \rfloor,$$

čime smo sveli problem na (a).

(c) Pretpostavimo da $N$, posle prenumeracije skupa $\{1, 2, \ldots, n\}$, sadrži $x = \lfloor 12345 \rfloor$. Zbog normalnosti sadrži i $y = (\lfloor 12 \rfloor \lfloor 34 \rfloor) x (\lfloor 12 \rfloor \lfloor 34 \rfloor)^{-1} = \lfloor 21435 \rfloor$, pa sadrži i:

$$xy = \lfloor 12345 \rfloor \lfloor 21435 \rfloor = \lfloor 153 \rfloor,$$

čime smo sveli problem na (a).

(d) Neka je $n = 6$ i pretpostavimo da $N$, posle prenumeracije skupa $\{1, 2, \ldots, n\}$, sadrži $x = \lfloor 123 \rfloor \lfloor 456 \rfloor$. Zbog normalnosti zadrži i $y = \lfloor 124 \rfloor x \lfloor 124 \rfloor^{-1} = \lfloor 243 \rfloor \lfloor 156 \rfloor$, pa sadrži i:

$$xy = \lfloor 123 \rfloor \lfloor 456 \rfloor \lfloor 243 \rfloor \lfloor 156 \rfloor = \lfloor 16254 \rfloor,$$

čime smo sveli problem na (c).

(e) Neka je $n = 6$ i pretpostavimo da $N$, posle prenumeracije skupa $\{1, 2, \ldots, n\}$, sadrži $x = \lfloor 1234 \rfloor \lfloor 56 \rfloor$. Tada i $x^2 = \lfloor 13 \rfloor \lfloor 24 \rfloor \in N$, čime smo sveli problem na (b). □

**3/3 Lema.**
Ako $N \lhd \mathbb{A}_n$, gde $n \geqslant 7$, i $N \neq \langle \lfloor \rfloor \rangle$, onda $N = \mathbb{A}_n$.

*Dokaz.* Neka je $x \in N$ netrivijalna permutacija, i preptostavimo, posle prenumeracije skupa $\{1, 2, \ldots, n\}$, $x(1) \neq 1$. Neka je $x(1) = i > 1$ i neka su $j, k > 1$ takvi da su $i, j, k$ međusobno različiti. Primetimo da je $\lfloor ijk \rfloor x \lfloor ijk \rfloor^{-1}(1) = \lfloor ijk \rfloor x(1) = \lfloor ijk \rfloor(i) = j \neq i = x(1)$, pa $y := \lfloor ijk \rfloor x \lfloor ijk \rfloor^{-1} \neq x$ i takođe $y \in N$ zbog normalnosti. Neka je $z = yx^{-1} \in N$. Primetimo sledeće:

$$z = \lfloor ijk \rfloor x \lfloor ijk \rfloor^{-1} x^{-1} = \lfloor ijk \rfloor x \lfloor ikj \rfloor x^{-1} = \lfloor ijk \rfloor \lfloor x(i)x(j)x(k) \rfloor.$$

Dakle, $z \in N$ permutuje najviše šest elemenata. Neka je $S$ šestočlani skup koji sadrži $i, j, k, x(i), x(j), x(k)$ i neka je $H$ podgrupa od $\mathbb{A}_n$ koju čine sve parne permutacije koje permutuju skup $S$, a fiksiraju sve brojeve van $S$. Dakle, $z \in H$ i $H \cong \mathbb{A}_6$. Kako je $N \lhd \mathbb{A}_n$, to je $N \cap H \lhd H$, pa kako je $z \in N \cap H$ i kako $H \cong \mathbb{A}_6$, zaključujemo $N \cap H = H$ prema lemi 3/2, tj. $H \subseteq N$. Kako $H$ sadrži 3-ciklove, i $N$ ih sadrži, pa zaključak sledi prema lemi 3/1. □

Kao posledicu prethodne tri leme izvodimo:

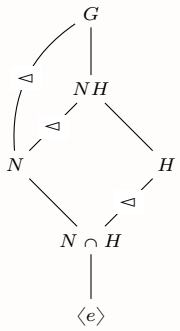
**3/4 Teorema.**
Grupe $\mathbb{A}_n$, $n \geqslant 5$, nisu proste.

**3/5 Zadatak.** Dokazati da je $\mathbb{A}_n$ jedina prava netrivijalna normalna podgrupa od $\mathbb{S}_n$, $n \geqslant 5$.

# 4 Druga i treća teorema o izomorfizmu

## A Druga teorema o izomorfizmu

**4/1 Teorema** (Druga teorema o izomorfizmu)**.**
Neka je $G$ grupa, $N \lhd G$ i $H \leqslant G$. Tada je $N \cap H \lhd H$, $N \lhd NH$ i važi $N/(N \cap H) \cong NH/N$.




*Dokaz.* Kako je $N \lhd G$, znamo da je $NH \leqslant G$. Jasno je $N \leqslant NH$, pa kako je $N$ normalna u većoj grupi $G$, normalna je i u manjoj grupi $NH$: $N \lhd NH$. Takođe, ako $a \in N \cap H$ i $h \in H$ tada $h^{-1}ah \in N$ jer je $N$ normalna u $G$ i $a \in N$, ali i $h^{-1}ah \in H$ jer $a, h \in H$. Dakle, $h^{-1}ah \in N \cap H$, što znači da je $N \cap H \lhd H$. Dakle, količnici $NH/N$ i $H/(N \cap H)$ su definisani.

Uočimo preslikavanje $\varphi : H \to NH/N$ dato sa $\varphi(h) := hN$; primetimo da $h = eh \in NH$, pa $hN$ jeste element količnika $NH/N$, tj, $\varphi$ je dobro definisano preslikavanje. Takođe je $\varphi(h_1h_2) = h_1h_2N = h_1N \cdot h_2N = \varphi(h_1)\varphi(h_2)$, gde druga jednakost važi po definiciji operacije u $NH/N$, pa vidimo da je $\varphi$ homomorfizam.

Odredimo jezgro ovog homomorfizma. Imamo, za $h \in H$, $\varphi(h) = N \iff hN = N \iff h \in N \iff h \in N \cap H$. Dakle, $Ker(\varphi) = N \cap H$.

Dokažimo i da je $\varphi$ na. Neka je $xN$ proizvoljan koset gde $x \in NH$. Zapišimo $x = nh$ za $n \in N$ i $h \in H$. Zbog normalnosti grupe $N$ je $h^{-1}nh = n'$ za neko $n' \in N$, pa je $x = nh = hn'$. Odatle je $xN = hn'N = hN$ jer $n' \in N$, tj. $xN = \varphi(h)$ što dokazuje da je $\varphi$ na. Dakle, $Im(\varphi) = NH/N$.

Prema prvoj teoremi o izomorfizmu $H/Ker(\varphi) \cong Im(\varphi)$, tj. $H/(N \cap H) \cong NH/N$. □

## B Treća teorema o izomorfizmu

**4/2 Teorema** (Treća teorema o izomorfizmu)**.**
Neka su $N, K \lhd G$ i $N \leqslant K$. Tada je $K/N \lhd G/N$ i $(G/N)/(K/N) \cong G/K$.


*Dokaz.* Količnik $G/N$ je definisan jer $N \lhd G$. Takođe, $N \lhd G$ i $N \leqslant K$ povlače $N \lhd K$, pa je i količnik $K/N$ definisan. Očigledno $K/N \subseteq G/N$, pa očigledno $K/N \leqslant G/N$; dokažimo $K/N \lhd G/N$. Za $k \in K$ i $g \in G$ imamo $gN \cdot kN \cdot (gN)^{-1} = (gkg^{-1})N \in K/N$ jer $gkg^{-1} \in K$ zbog $K \lhd G$.

Dakle, $(G/N)/(K/N)$ je definisana. Grupa $G/K$ je definisana jer $K \lhd G$. Posmatrajmo preslikavanje $\varphi : G/N \to G/K$ dato sa $\varphi(gN) = gK$. Moramo da proverimo da je $\varphi$ dobro definisano, tj. da ne zavisi od izbora predstavnika $g$ koseta $gN$. Ako je $g_1N = g_2N$, tada je $g_1^{-1}g_2 \in N$, pa i $g_1^{-1}g_2 \in K$ jer $N \leqslant K$, pa je i $g_1K = g_2K$. Dakle, $\varphi$ jeste dobro definisano.

Dokažimo da je $\varphi$ homomorfizam: $\varphi(g_1N \cdot g_2N) = \varphi(g_1g_2N) = g_1g_2K = g_1K \cdot g_2K = \varphi(g_1N)\varphi(g_2N)$, gde prva i treća jedankost važe po definiciji operacije u odgovarajućem količniku.

Homomorfizam $\varphi$ očigledno je na: koset $gK$ je slika koseta $gN$. Dakle, $Im(\varphi) = G/K$. Izračunajmo jezgro. Imamo da $\varphi(gN) = K \iff gK = K \iff g \in K \iff gN \in K/N$; u poslednjoj ekvivalenciji ($\Leftarrow$) važi jer ako je $gN = kN$ za $k \in K$, onda $g^{-1}k \in N \leqslant K$, odakle, kako $k \in K$, sledi i $g \in K$. Dakle, $Ker(\varphi) = K/N$.

Prema prvoj teoremi o izomorfizmu $(G/N)/(K/N) \cong G/K$. □

# 5 Rešive grupe

## A Digresija: Karakterisične podgrupe

**5/1 Definicija.** Podgrupa $H \leqslant G$ je karakteristična, $H$ char $G$, ako je invariantna u odnosu na sve automorfizme grupe $G$: $(\forall \varphi \in Aut(G))\ \varphi[H] = H$.

**5/2 Komentar.**
1. Primetimo: $H$ char $G \iff (\forall \varphi \in Aut(G))\ \varphi[H] \subseteq H$. Zaista, ako poslednje važi, onda za svako $\varphi$ imamo i $\varphi[H] \subseteq H$ i $\varphi^{-1}[H] \subseteq H$, odakle je i $H = \varphi[\varphi^{-1}[H]] \subseteq \varphi[H]$, pa važi $\varphi[H] = H$.
2. Kako je $Inn(G) \subseteq Aut(G)$, jasno je da $H$ char $G$ povlači $H \lhd G$, jer $H \lhd G$ znači da za svako $g \in G$, $\delta_g[H] \subseteq H$ (pogledati teoremu 1/21 za definiciju $Inn(G)$).

**5/3 Primer.**
$Z(G)$ char $G$.
Neka $a \in Z(G)$ i $\varphi \in Aut(G)$. Neka je $x \in G$ proizvoljno. Tada $a\varphi^{-1}(x) = \varphi^{-1}(x)a$ jer $a \in Z(G)$, pa primenom $\varphi$ dobijamo $\varphi(a)x = x\varphi(a)$. Kako je $x$ bilo proizvoljno zaključujemo $\varphi(a) \in Z(G)$. Dakle $\varphi[Z(G)] \subseteq Z(G)$, pa zaista $Z(G)$ char $G$.

**5/4 Primer.**
Ako je $H \leqslant G$ jedinstvena podgrupa konačnog indeksa $n$, onda je $H$ char $G$ (pa i $H \lhd G$).
Ako je $H$ jedina podgrupa indeksa $n$, kako je za svako $\varphi \in Aut(G)$ tada i $\varphi[H]$ podgrupa indeksa $n$, iz jedinstvenosti sledi $\varphi[H] = H$.
Slično, ako je $H \leqslant G$ jedinstvena podgrupa konačnog reda $n$, onda je $H$ char $G$ i specijalno $H \lhd G$.

Npr. u grupi kvaterniona $Q_8$, $\{-1,1\}$ je jedinstvena podgrupa reda 2 (i jedinstvena podgrupa indeksa 4), pa je $\{-1,1\}$ char $Q_8$ i $\{-1,1\} \lhd Q_8$.

**5/5 Primer.**
U opštem slučaju $H \lhd G$ ne povlači $H$ char $G$.
Npr. u Klajnovoj grupi $V = \mathbb{Z}_2 \times \mathbb{Z}_2$ je $\mathbb{Z}_2 \times \langle 0\rangle \lhd V$ jer je $V$ Abelova, ali nije $\mathbb{Z}_2 \times \langle 0\rangle$ char $V$ jer imamo automorfizam koji transponuje generatore $(1,0)$ i $(0,1)$ pa podgrupu $\mathbb{Z}_2 \times \langle 0\rangle$ slika u podgrupu $\langle 0\rangle \times \mathbb{Z}_2$.

Znamo da $H \lhd K \lhd G$ ne povlači uvek $H \lhd G$. Arhiprimer je grupa $\mathbb{D}_4$ u kojoj je $\langle\sigma\rangle \lhd \langle\sigma, \rho^2\rangle \lhd \mathbb{D}_4$, ali $\langle\sigma\rangle \not\lhd \mathbb{D}_4$.

**5/6 Tvrđenje.**(a) Ako $H$ char $K$ char $G$, onda $H$ char $G$.

(b) Ako $H$ char $K \lhd G$, onda $H \lhd G$.

*Dokaz.* (a) Neka je $\varphi \in Aut(G)$, treba da dokažemo $\varphi[H] = H$. Kako je $K$ char $G$, $\varphi[K] = K$, pa $\varphi_{\restriction K} \in Aut(K)$. Odatle, kako je $H$ char $K$, $\varphi_{\restriction K}[H] = H$, pa je i $\varphi[H] = \varphi_{\restriction K}[H] = H$.

(b) Argument je sličan kao u (a). Neka je $a \in G$ proizvoljno. Kako je $K \lhd G$ to je $\delta_a[K] = K$, tj. $(\delta_a)_{\restriction K} \in Aut(K)$. Kako je $H$ char $K$ to $(\delta_a)_{\restriction K}[H] = H$, pa i $\delta_a[H] = H$. Dakle, $H \lhd G$. □

**5/7 Primer.**
Ako $H$ char $G$ i $H \leqslant K \leqslant G$, ne mora biti $H$ char $K$. (Za razliku od normalnosti, podgrupa može da bude karakteristična u većoj grupi, a da ne bude karakteristična u manjoj.)
Posmatrajmo $G = \mathbb{Z}_4 \times \mathbb{Z}_2$, $K = \langle (2,0), (0,1)\rangle$ i $H = \langle (2,0)\rangle$. Primetimo da $H$ nije karakteristična u $K$; nije teško videti da je sledećom tablicom dat automorfizam grupe $K$ koji očigledno ne fiksira $H$:

| | $(0,0)$ | $(2,0)$ | $(0,1)$ | $(2,1)$ |
|---|---|---|---|---|
| $\varphi(-)$ | $(0,0)$ | $(0,1)$ | $(2,0)$ | $(2,1)$ |

Dokažimo sada $H$ char $G$. Neka je $\varphi \in Aut(G)$. Tada je $\varphi((1,0))$ element reda četiri, tj. jedan od $(1,0), (3,0), (1,1)$ i $(3,1)$. U svakom od ovih slučajeva je: $\varphi((2,0)) = \varphi((1,0)+(1,0)) = \varphi((1,0))+\varphi((1,0)) = (2,0)$, gde se poslednja jednakost lako proveri u sva četiri slučaja. Dakle, $\varphi$ fiksira $H$.

## B Izvod i abelizacija grupe

**5/8 Definicija.** Neka je $G$ grupa, $a, b \in G$, i $A, B \subseteq G$.

(a) Komutator elemenata $a$ i $b$ je element $[a,b] := a^{-1}b^{-1}ab$.

(b) $[A,B] := \langle [a,b] \mid a \in A,\ b \in B\rangle$.

Očigledno $ab = ba \iff [a,b] = e$. Primetimo da je $[a,b]^{-1} = [b,a]$, kao i $g^{-1}[a,b]g = [g^{-1}ag, g^{-1}bg]$, i više $\sigma([a,b]) = [\sigma(a), \sigma(b)]$ za svako $\sigma \in Aut(G)$.

**5/9 Definicija.** Izvod grupe $G$ je podgrupa $G' := [G,G]$ generisana svim komutatorima.

**5/10 Komentar.** Kako je skup svih komutatora zatvoren za inverz (jer $[a,b]^{-1} = [b,a]$), proizvoljni element izvoda $G'$ jednak je konačnom proizvodu komutatora, tj. ako $x \in G'$, onda je $x = [a_1,b_1][a_2,b_2]\dots[a_n,b_n]$.

**5/11 Teorema.**
Neka je $G$ grupa.

(a) $G'$ char $G$, pa je i $G' \lhd G$.

(b) Količnik $G/G'$ je Abelova grupa.

(c) Za $H \lhd G$ važi: $G/H$ je Abelova akko $G' \leqslant H$. Specijalno, izvod $G'$ je najmanja normalna podgrupa $H$ od $G$ takva da je $G/H$ Abelova.

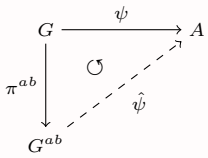
*Dokaz.* (a) Već smo naglasili da za svaki automorfizam imamo $\sigma([a,b]) = [\sigma(a), \sigma(b)]$, pa direktno imamo $\sigma[G'] = G'$, tj. $G'$ char $G$, pa i $G' \lhd G$.

(b) Kako je, u grupi $G/G'$, $[aG', bG'] = [a,b]G' = G'$ jer $[a,b] \in G'$, svi komutatori u $G/G'$ su trivijalni, pa je $G/G'$ Abelova.

(c) Neka je $H \lhd G$ takva da je $G/H$ Abelova. Tada je, za proizvoljne $a, b \in G$, $H = [aH, bH] = [a,b]H$, pa $[a,b] \in H$. Kako $H$ sadrži sve komutatore, sadrži i $G'$: $G' \leqslant H$. Sa druge stane, ako $G' \leqslant H$, tada je i $G' \lhd H$, pa po trećoj teoremi o izomorfizmu imamo $G/H \cong (G/G')/(H/G')$, pa je $G/H$ izomorfna količniku Abelove (prema (b)) grupe $G/G'$, te je i sama Abelova. □

**5/12 Definicija.** Grupa $G/G'$ naziva se abelizacija grupe $G$ i obeležavamo je sa $G^{ab} := G/G'$.

**5/13 Teorema** (Univerzalno svojstvo abelizacije)**.**
Neka je $\pi^{ab} : G \to G^{ab}$ kanonski epimorfizam. Ako je $A$ Abelova grupa i $\psi : G \to A$ homomorfizam, tada postoji jedinstveni homomorfizam $\hat{\psi} : G^{ab} \to A$ takav da $\psi = \hat{\psi} \circ \pi^{ab}$:




*Dokaz.* Dokažimo najpre jedinstvenost. Neka su $\hat{\psi}_1, \hat{\psi}_2 : G^{ab} \to A$ homomorfizmi takvi da $\hat{\psi}_1\pi^{ab} = \psi = \hat{\psi}_2\pi^{ab}$. Tada je $\hat{\psi}_1(gG') = \hat{\psi}_1\pi^{ab}(g) = \psi(g) = \hat{\psi}_2\pi^{ab}(g) = \hat{\psi}_2(gG')$, pa je $\hat{\psi}_1 = \hat{\psi}_2$.

Definišimo $\hat{\psi} : G^{ab} \to A$ sa $\hat{\psi}(gG') = \psi(g)$. Dokažimo da je $\hat{\psi}$ dobro definisano. Neka je $g_1G' = g_2G'$, tj. $g_1^{-1}g_2 \in G'$. Tada, $g_1^{-1}g_2$ je konačan proizvod komutatora. Primetimo da je $\psi([a,b]) = [\psi(a), \psi(b)] = 0$ jer je $A$ Abelova, pa je i $\psi(g_1^{-1}g_2) = 0$, tj. $g_1^{-1}g_2 \in Ker(\psi)$, tj. $\psi(g_1) = \psi(g_2)$. Dakle, $\hat{\psi}$ jeste dobro definisano preslikavanje. Očigledno je $\psi = \hat{\psi} \circ \pi^{ab}$. Konačno $\hat{\psi}$ je homomorfizam jer $\hat{\psi}(g_1G' \cdot g_2G') = \hat{\psi}(g_1g_2G') = \psi(g_1g_2) = \psi(g_1)\psi(g_2) = \hat{\psi}(g_1G')\hat{\psi}(g_2G')$. □

## C Viši izvodi grupe

**5/14 Definicija.** Za $n \geqslant 2$, $n$-ti izvod grupe $G$, $G^{(n)}$ definišemo rekurentno sa $G^{(n)} := (G^{(n-1)})'$.

**5/15 Komentar.** Primetimo da indukcijom, koristeći tvrđenje 5/6(a) i teoremu 5/11(a), lako dokazujemo $G^{(n)}$ char $G$, pa i $G^{(n)} \lhd G$, za sve $n \geqslant 1$.

**5/16 Lema.**
Neka je $G$ grupa, $H \leqslant G$ i $\varphi : G \to K$ epimorfizam grupa. Tada:

(a) $H^{(n)} \leqslant G^{(n)}$ za sve $n \geqslant 1$;

(b) $\varphi[G^{(n)}] = K^{(n)}$ za sve $n \geqslant 1$.

*Dokaz.* (a) Kako je $H \leqslant G$, to je $H' = [H,H] \leqslant [G,G] = G'$. Nastavljamo indukcijom, $H'' = [H',H'] \leqslant [G',G'] = G''$, itd.

(b) Kako je $\varphi[G] = K$ jer je $\varphi$ na, imamo $\varphi[G'] = \varphi[[G,G]] = [\varphi[G],\varphi[G]] = [K,K] = K'$, gde druga jednakost važi jer $\varphi([a,b]) = [\varphi(a),\varphi(b)]$. Dalje nastavljamo indukcijom, $\varphi[G''] = \varphi[[G',G']] = [\varphi[G'],\varphi[G']] = [K',K'] = K''$, itd. □

**5/17 Primer.**
Izračunajmo izvode grupa $\mathbb{S}_n$ i $\mathbb{A}_n$ za $n \geqslant 3$.
Primetimo da je svaki komutator u grupi $\mathbb{S}_n$ parna permutacija, pa $\mathbb{S}_n' \subseteq \mathbb{A}_n$. Primetimo i da je, za $k = 3,4,\ldots,n$, $\lfloor 12k \rceil = \lfloor 1k \rceil \lfloor 2k \rceil \lfloor 1k \rceil \lfloor 2k \rceil = [\ \lfloor 1k \rceil, \lfloor 2k \rceil\ ] \in G'$. Kako znamo da $\lfloor 12k \rceil$ generišu $\mathbb{A}_n$ imamo i $\mathbb{A}_n \subseteq \mathbb{S}_n'$. Dakle, $\mathbb{S}_n' = \mathbb{A}_n$, pa je i $\mathbb{S}_n^{ab} = \mathbb{S}_n/\mathbb{A}_n \cong \mathbb{Z}_2$.
Kako je $\mathbb{A}_3$ Abelova grupa $\mathbb{A}_3' = \langle e \rangle$, pa je $\mathbb{S}_3'' = \langle e \rangle$. Odavde sledi i da su svi viši izvodi grupa $\mathbb{A}_3$ i $\mathbb{S}_3$ trivijalni.
Izračunajmo $\mathbb{A}_4'$. Uočimo $V = \{\lfloor\rceil, \lfloor 12 \rceil \lfloor 34 \rceil, \lfloor 13 \rceil \lfloor 24 \rceil, \lfloor 14 \rceil \lfloor 23 \rceil\}$ – podgrupa duplih transpozicija. Nije teško videti da ovo zaista jeste podgrupa izomorfna Klajnovoj grupi – otud oznaka $V$. Kako konjugat čuva ciklusnu dekompoziciju, a $V$ sadrži sve duple transpozicije, podgrupa $V$ je normalna i njen količnik $\mathbb{A}_4/V$ je reda 3, tj. grupa $\mathbb{Z}_3$. Kako je količnik Abelova grupa, zaključujemo da $\mathbb{A}_4' \subseteq V$. Podgrupa $V$ ima svoje četiri prave podgrupe: trivijalnu i tri ciklične reda 2. Kako $\mathbb{A}_4$ nije Abelova, $\mathbb{A}_4'$ nije trivijalna. Sa druge strane, nije teško videti da nijedna od podgrupa od $V$ reda 2 nije normalna podgrupa od $\mathbb{A}_4$. Prema tome $\mathbb{A}_4' = V$. Kako je $V$ Abelova, $\mathbb{A}_4'' = V' = \langle \lfloor\rceil \rangle$, i viši izvodi su očigledno takođe trivijalni. Dakle, $\mathbb{S}_4'' = V$, $\mathbb{S}_4''' = \langle \lfloor\rceil \rangle$ i viši izvodi su takođe trivijalni.
Izračunajmo sada i $\mathbb{A}_n'$ za $n \geqslant 5$. Fiksirajmo proizvoljno $k$, $3 \leqslant k \leqslant n$. Kako je $n \geqslant 5$, izaberimo $i,j$ takve da $3 \leqslant i < j \leqslant n$ i $i,j \neq k$. Kao u prvom pasusu primetićemo da je:

$$\lfloor 12k \rceil = [\lfloor 1k \rceil \lfloor ij \rceil, \lfloor 2k \rceil \lfloor ij \rceil] \in \mathbb{A}_n'.$$

Kako ovi 3-ciklovi generišu $\mathbb{A}_n$, zaključujemo $\mathbb{A}_n' = \mathbb{A}_n$, pa su očigledno i svi viši izvodi jednaki $\mathbb{A}_n$. Dakle, za $n \geqslant 5$, i $\mathbb{S}_n^{(m)} = \mathbb{A}_n$ za sve $m \geqslant 2$.

## D Rešive grupe

**5/18 Definicija.** Grupa $G$ je *rešiva* ako za neko $n \geqslant 1$ važi $G^{(n)} = \langle e \rangle$. Najmanje takvo $n$ zovemo *stepen rešivosti*.

Jasno je da su sve Abelove grupe rešive jer im je već prvi izvod trivijalan.

**5/19 Primer.**
Kako smo videli u prethodnom odeljku, $\mathbb{S}_3$ i $\mathbb{S}_4$ jesu rešive, dok $\mathbb{S}_n$ za $n \geqslant 5$ nisu rešive.

**5/20 Tvrđenje.**(a) Podgrupa rešive grupe je rešiva.

(b) Homomorfna slika rešive grupe je rešiva. Posebno, količnik rešive grupe je rešiv.

*Dokaz.* (a) Neka je $G$ rešiva i $H \leqslant G$. Neka je $n \geqslant 1$ takav da $G^{(n)} = \langle e \rangle$. Prema lemi 5/16(a), $H^{(n)} \leqslant G^{(n)} = \langle e \rangle$, pa je $H^{(n)} = \langle e \rangle$ i $H$ je rešiva.

(b) Neka je $G$ rešiva i $\varphi : G \to K$ je epimorfizam. Neka je $n \geqslant 1$ takav da $G^{(n)} = \langle e \rangle$. Prema lemi 5/16(b), $K^{(n)} = \varphi[G^{(n)}] = \varphi[\langle e \rangle] = \langle e \rangle$ i $K$ je rešiva.

Ako je $N \lhd G$ i $G$ je rešiva, količnik $G/N$ je rešiv kao homomorfna slika od $G$ pri kanonskom epimorfizmu. □

**5/21 Teorema.**
Neka je $N \lhd G$ i neka su $N$ i $G/N$ rešive. Tada je i $G$ rešiva.

*Dokaz.* Neka su $m, n \geqslant 1$ takvi da $N^{(m)} = \langle e \rangle$ i $(G/N)^{(n)} = \langle N \rangle$. Neka je $\pi : G \to G/N$ kanonski epimorfizam. Prema lemi 5/16(b) je $\langle N \rangle = (G/N)^{(n)} = \pi[G^{(n)}]$, pa je $G^{(n)} \leqslant N$. Prema lemi 5/16(a) sada je $(G^{(n)})^{(m)} \leqslant N^{(m)} = \langle e \rangle$, pa je $(G^{(n)})^{(m)} = \langle e \rangle$. Grupa $G$ je rešiva jer je $(G^{(n)})^{(m)} = G^{(n+m)}$. □

**5/22 Posledica.**
Ako su $G_1$ i $G_2$ rešive, rešiva je i $G_1 \times G_2$.

*Dokaz.* Za $G_1 \times \langle e \rangle \lhd G_1 \times G_2$ imamo da je $G_1 \times \langle e \rangle \cong G_1$ rešiva i $G_1 \times G_2/G_1 \times \langle e \rangle \cong G_2$ rešiva, pa je prema prethodnoj teoremi i $G_1 \times G_2$ rešiva. □

**5/23 Tvrđenje.**
Grupe reda $p^n$ su rešive, gde $p$ je prost i $n \geqslant 1$.

*Dokaz.* Indukcijom po $n$. Za $n = 1$, grupa je ciklična, pa je rešiva. Neka je $|G| = p^n$ za $n > 1$. Setimo se da je centar grupe reda $p^n$ netrivijalan (teorema 1/40), pa je $|Z(G)| = p^m$ za neko $1 < m \leqslant n$. Ako je $m = n$, $G = Z(G)$ je Abelova pa je rešiva. Preptostavimo $m < n$. Tada je $G/Z(G)$ reda $p^{n-m}$ gde $1 < n - m < n$, pa je $G/Z(G)$ rešiva po IH, a $Z(G)$ je rešiva kao Abelova. Po teoremi 5/21, $G$ je rešiva. □

**5/24 Teorema.**
Neka je $G$ grupa. Sledeći iskazi su ekvivalentni:

(1) $G$ je rešiva;

(2) postoji niz podgrupa $G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_n = \langle e \rangle$ takav da je $H_i/H_{i+1}$ Abelova za sve $i < n$.

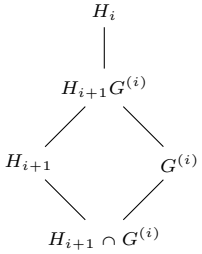
Ako je $G$ konačna, još jedan ekvivalent je i:

(3) postoji niz podgrupa $G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_n = \langle e \rangle$ takav da je $H_i/H_{i+1}$ ciklična prostog reda za sve $i < n$.

*Dokaz.* (1)⇒(2): Neka je $G$ rešiva i $G^{(n)} = \langle e \rangle$. Niz $G \rhd G' \rhd G'' \rhd \cdots \rhd G^{(n)} = \langle e \rangle$ je željeni niz.

(2)⇒(1): Neka je $G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_n = \langle e \rangle$ niz podgrupa takav da je $H_i/H_{i+1}$ Abelova za sve $i < n$. Indukcijom po $i \geqslant 1$ dokazujemo da je $G^{(i)} \leqslant H_i$. (Ovo je dovoljno jer je tada $G^{(n)} \leqslant H_n = \langle e \rangle$ povlači $G^{(n)} = \langle e \rangle$ i $G$ je rešiva.) Za $i = 1$, kako je $G/H_1$ Abelova po teoremi 5/11(c) direktno imamo $G' \leqslant H_1$.

Pretpostavimo da je $G^{(i)} \leqslant H_i$ i dokažimo $G^{(i+1)} \leqslant H_{i+1}$. Kako je $H_{i+1} \lhd H_i$ i $G^{(i)} \leqslant H_i$ po IH, možemo da uočimo dijagram:



Po drugoj teoremi o izomorfizmu $G^{(i)}/(H_{i+1} \cap G^{(i)}) \cong H_{i+1}G^{(i)}/H_{i+1}$, pa je $G^{(i)}/(H_{i+1} \cap G^{(i)})$ izomorfna podgrupi Abelove grupe $H_i/H_{i+1}$, tj. i ona je Abelova. Prema teoremi 5/11(c), $G^{(i+1)} = (G^{(i)})' \leqslant H_{i+1} \cap G^{(i)}$; specijalno, $G^{(i+1)} \leqslant H_{i+1}$, i završili smo dokaz.

Pretpostavimo sada da je $G$ konačna grupa. (3)⇒(2) je očigledno, pa dokazujemo (2)⇒(3). Dovoljno je da dokažemo sledeću lemu: *Ako $H \lhd K$ i $K/H$ je konačna Abelova grupa, onda postoji $L$ takva da $H \lhd L \lhd K$, $L/H$ je ciklična prostog reda i $K/L$ je Abelova reda manjeg od $|K/H|$.* Zaista, ova lema nam očiglendo omogućava da u konačno mnogo koraka „ubacimo" između svakog para $H_i \rhd H_{i+1}$ nove podgrupe takve da novodobijeni niz zadovoljava željeno svojstvo.

Dokažimo lemu. Kako je $K/H$ konačna Abelova grupa, uzmimo prost broj $p$ koji deli $|K/H|$. Po Košijevoj lemi $K/H$ ima element $aH$ reda $p$, pa posmatrajmo podgrupu $\langle aH \rangle$, koja je ciklična reda $p$. Ona je naravno normalna u $K/H$ jer je $K/H$ Abelova. Tada je $L = \pi^{-1}[\langle aH \rangle]$ normalna podgrupa od $K$ takva da $H \subseteq L$ i $\langle aH \rangle = L/H$. Primetimo da jeste $H \lhd L \lhd K$. Takođe, $L/H$ je ciklična prostog reda, a $K/L$ je po trećoj teoremi o izomorfizmu izomorfna sa $(K/H)/(L/H)$ što je količnik konačne Abelove grupe, pa je i sam konačna Abelova grupa. Što se tiče reda, očigledno je $|K/L| = \frac{|K/H|}{|L/H|} = \frac{|K/H|}{p} < |K/H|$. Time smo završili dokaz. □

**5/25 Komentar.** U delu (3) je bitno da je $G$ konačna. Primera radi, grupa $\mathbb{Z}$, iako rešiva jer je Abelova, nema niz opisan u delu (3). Ako imamo niz $\mathbb{Z} \rhd H_1 \rhd \cdots \rhd H_{n-1} \rhd H_n = \langle 0 \rangle$, gde je $H_{n-1}$ netrivijalna, znamo da je $H_{n-1} = k\mathbb{Z}$ za neko $k$, pa $H_{n-1}/H_n = k\mathbb{Z}/\langle 0 \rangle = k\mathbb{Z}$ nije konačna, pa ni prostog reda.

# 6 ((Uglavnom) komutativni) prsteni ((skoro uvek) sa jedinicom)

## A Definicije i primeri

**6/1 Definicija.** Neka je $R$ neprazan skup sa dve binarne operacije $+$ (sabiranje) i $\cdot$ (množenje)[3] na njemu.

(a) $R$ je prsten ako su zadovoljene sledeće aksiome:

- $R$ je Abelova grupa u odnosu na $+$; neutral ove grupe zove se nula prstena $R$, i obeležavamo ga sa 0; inverz elementa $a$ obeležavamo sa $-a$, i zovemo ga aditivni inverz; dakle:
  - $a + (b + c) = (a + b) + c$;
  - $a + 0 = a = 0 + a$;
  - $a + (-a) = 0 = (-a) + a$;[4]
  - $a + b = b + a$;
- $R$ je polugrupa u odnosu na $\cdot$, tj. $\cdot$ je asocijativna operacija:
  - $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
- važe distrubutivni zakoni množenja prema sabiranju:
  - $a \cdot (b + c) = a \cdot b + a \cdot c$;[5]
  - $(a + b) \cdot c = a \cdot c + b \cdot c$.

(b) $R$ je komutativan prsten ako pored uslova iz (a) važi i:

- $a \cdot b = b \cdot a$.

(c) $R$ je prsten sa jedinicom ako pored uslova iz (a) važi i:

- $R$ ima neutral u odnosu na množenje koji se zove jedinica prstena $R$ i obeležavamo ga sa 1:
  - $a \cdot 1 = a = 1 \cdot a$.

(d) Sada je jasno šta znači da je $R$ komutativan prsten sa jedinicom.

[3] Umesto $a \cdot b$ obično ćemo pisati $ab$.
[4] Nadalje ćemo $a + (-b)$ kraće pisati $a - b$.
[5] Kao što je i običaj, množenje je „starije" od sabiranja, pa izraz $a \cdot b + a \cdot c$ znači $(a \cdot b) + (a \cdot c)$.

**6/2 Primer.**(a) Skup $R = \{0\}$ na kome su $+$ i $\cdot$ očigledno definisani jeste prsten, štaviše komutativan prsten sa jedinicom (element 0 je i nula i jedinica prstena). Ovaj prsten zovemo trivijalan prsten. U sledećem tvrđenju ćemo videti da ako prsten sa jedinicom ima bar dva elementa, nula i jedinica su obavezno različiti. Nadalje, za sve prstene o kojima ćemo govoriti, osim ako nije nešto eksplicitno naglašeno, podrazumevamo da su netrivijalni, tj. imaju bar dva elementa.

(b) Osnovni primer prstena je $(\mathbb{Z}, +, \cdot)$. Očigledno je da je u pitanju komutativan prsten sa jedinicom.

(c) Slično, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ i $(\mathbb{C}, +, \cdot)$ očigledno su primeri komutativnih prstena sa jedinicom. Ovi primeri zadovoljavaju i više, u pitanju su polja.

(d) Označimo sa $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$; $\mathbb{Z}[\sqrt{2}]$ je komutativan prsten sa jedinicom u odnosu na uobičajeno sabiranje i množenje. Treba da proverimo da su $+$ i $\cdot$ operacije na $\mathbb{Z}[\sqrt{2}]$. I zaista, ako je $x = a + b\sqrt{2}$ i $y = c + d\sqrt{2}$, onda je $x + y = (a + c) + (b + d)\sqrt{2}$, $a + c, b + d \in \mathbb{Z}$, pa $x + y \in \mathbb{Z}[\sqrt{2}]$. Slično, $xy = (ac + 2bd) + (ad + bc)\sqrt{2}$, $ac + 2bd, ad + bc \in \mathbb{Z}$, pa $xy \in \mathbb{Z}[\sqrt{2}]$. Takođe, očigledno $-x = (-a) + (-b)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, i naglasimo da je nula $0 = 0 + 0 \cdot \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ i jedinica je $1 = 1 + 0 \cdot \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Nema potrebe da proveravamo aksiome jer one važe na većem skupu $\mathbb{R} \supseteq \mathbb{Z}[\sqrt{2}]$.

(e) Za $n \geqslant 2$, $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ u odnosu na standardno sabiranje i množenje modulo $n$ je komutativan prsten sa jedinicom.

(f) Označimo sa $M_n(\mathbb{R})$ skup svih $(n \times n)$-matrica nad $\mathbb{R}$. U odnosu na standardno sabiranje i množenje matrica $M_n(\mathbb{R})$ je (nekomutativan prsten) sa jedinicom (jedinična matrica). Sve aksiome su proverene još u linearnoj algebri. Opštije, ako je $R$ prsten, $M_n(R)$ – skup svih $(n \times n)$-matrica nad $R$ takođe je prsten. Ako $R$ ima jedinicu, i $M_n(R)$ ima jedinicu (dijagonalna matrica sa jedinicom iz $R$ na dijagonali). Ipak, ako $R$ ima jedinicu, $M_n(R)$ je komutativan ako i samo ako $R$ je komutativan i $n = 1$. Dakle, $M_n(R)$ je skoro uvek nekomutativan.

(g) Skup svih polinoma sa realnim koeficijentima po promenljivoj $X$, $\mathbb{R}[X]$, u odnosu na standardno sabiranje i množenje polinoma je komutativan prsten sa jedinicom (jedinica je konstantan polinom 1). Opštije, ako je $R$ prsten, skup svih polinoma sa koeficijentima u $R$ po promenljivoj $X$, $R[X]$, je prsten. $R[X]$ je komutativan ako i samo ako je $R$ komutativan. $R[X]$ ima jedinicu ako i samo ako $R$ ima jedinicu. Odavde, specijalno, je npr. $\mathbb{R}[X, Y]$ – skup polinoma po dve nepoznate $X$ i $Y$, prsten jer je $\mathbb{R}[X, Y] = (\mathbb{R}[X])[Y]$.

(h) Neka su $R_1, R_2$ prsteni. Proizvod $R_1 \times R_2$ sa pokoordinatnim sabiranjem i pokoordinatnim množenjem takođe je prsten. Nula prstena $R_1 \times R_2$ je par $(0_1, 0_2)$, gde su $0_1$ i $0_2$ redom nule prstena $R_1$ i $R_2$; takođe $-(a, b) = (-a, -b)$. Proizvod je komutativan ako i samo ako su oba prstena $R_1$ i $R_2$ komutativni. Proizvod ima jedinicu ako i samo ako oba prstena $R_1$ i $R_2$ imaju jedinicu; u tom slučaju jedinica proizvoda je $(1_1, 1_2)$, gde su $1_1$ i $1_2$ redom jedinice prstena $R_1$ i $R_2$.

(i) Ako je $R$ prsten i $S$ bilo koji neprazan skup, onda je skup svih funkcija $S \to R$, ${}^S R$, prsten u odnosu na operacije $+$ i $\cdot$ definisane na sledeći način:

$$(f + g)(s) := f(s) + g(s) \quad \text{i} \quad (fg)(s) := f(s)g(s).$$

${}^S R$ je komutativan ako i samo ako je $R$ komutativan. ${}^S R$ ima jedinicu ako i samo ako $R$ ima jedinicu.

(j) Parni celi brojevi $2\mathbb{Z}$ u odnosu na uobičajeno sabiranje i množenje čine komutativan prsten bez jedinice. Slično, $R = \{0, 2\}$ sa sabiranjem i množenjem modulo 2 je komutativan prsten bez jedinice.

**6/3 Zadatak.** (a) Neka je $R$ komutativan prsten sa jedinicom, dokazati da za $n \geqslant 2$, $M_n(R)$ nije komutativan.

(b) Naći primer prstena $R$ za koji je $M_2(R)$ komutativan.

**6/4 Tvrđenje** (Osnovne osobine)**.**
Neka je $R$ prsten. Tada:

(a) nula i aditivni inverz elementa $a$ su jedinstveni;

(b) $-(a+b) = (-a) + (-b)$ i $-(-a) = a$;

(c) $a \cdot 0 = 0 = 0 \cdot a$;

(d) ako $R$ ima jedinicu, ona je jedinstvena;

(e) ako $R$ ima jedinicu i $|R| \geqslant 2$, onda $1 \neq 0$;

(f) $-(ab) = (-a)b = a(-b)$ i $ab = (-a)(-b)$.

*Dokaz.* (a) i (b) važe jer je $R$ Abelova grupa u odnosu na $+$. (Primetimo $-(-a) = a$ je aditivno zapisan zakon $(a^{-1})^{-1} = a$ koji važi u grupama; $-(a+b) = (-a) + (-b)$ je aditivno zapisan zakon $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$ koji važi u Abelovim grupama.)

(c) Imamo $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$, pa skraćivanjem $a \cdot 0$ u grupi $(R, +)$ dobijamo $a \cdot = 0$. Slično, $0 \cdot a = 0$.

(d) Neka su $1$ i $1'$ jedinice. Tada $1 = 1 \cdot 1' = 1'$, gde prva jednakost važi jer je $1'$ (desna) jedinica, a druga jer je $1$ (leva) jedinica.

(e) Ako $1 = 0$, onda za svako $a \in R$ je $a = a \cdot 1 = a \cdot 0 \overset{(c)}{=} 0$, odakle $R = \{0\}$ i $|R| = 1$.

(f) Iz $(-a)b + ab = ((-a) + a)b = 0 \cdot b = 0$ sledi $-(ab) = (-a)b$; slično važi i $-(ab) = a(-b)$. Odatle je $(-a)(-b) = -((-a)b) = -(-(ab)) = ab$. □

**6/5 Definicija.** Neka je $R$ prsten sa jedinicom. Element $u \in R$ je invertibilan ako ima multiplikativan inverz, tj. ako postoji element, koga obeležavamo sa $u^{-1}$, takav da $u \cdot u^{-1} = 1 = u^{-1} \cdot u$.

Skup svih invertibilnih elemenata u $R$ obeležavamo sa $R^\times$.

Primetimo da 0 nikad nije invertibilna (ako je prsten netrivijalan), jer ako postoji $0^{-1}$ tada je $1 = 0 \cdot 0^{-1} = 0$, gde druga jednakost važi prema prethodnom tvrđenju, a $1 = 0$ povači trivijalnost prstena.

**6/6 Primer.**(a) Očigledno, $\mathbb{Z}^\times = \{-1, 1\}$, $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.

(b) $\mathbb{Z}_n^\times = \{k < n \mid nzd(k, n) = 1\}$. Da bismo ovo dokazali, pretpostavimo da je za $k < n$, $nzd(k, n) = 1$; po Bezuovoj lemi tada postoje celi brojevi $x, y$ takvi da $kx + ny = 1$. Uzimajući ovu jednakost modulo $n$ vidimo da je $k\hat{x} = 1$ u $\mathbb{Z}_n$ (gde je $\hat{x}$ ostatak pri deljenju $x$ sa $n$); dakle, $\hat{x}$ je multiplikativan inverz od $k$, pa $k \in \mathbb{Z}_n^\times$. Sa druge strane, ako $k \in \mathbb{Z}_n$ ima multiplikativni inverz $l$, tada iz $kl = 1$ u $\mathbb{Z}_n$ sledi da je $kl - sn = 1$ za neko $s$; kako $nzd(k, n)$ očigledno deli levu stranu jednakosti, mora da deli i 1; dakle, $nzd(k, n) = 1$.

(c) Iz linearne algebre znamo da matrica $A \in M_n(\mathbb{R})$ ima inverz ako i samo ako $det(A) \neq 0$; dakle, $M_n(\mathbb{R})^\times = \{A \in M_n(\mathbb{R}) \mid det(A) \neq 0\}$. Opštije, ako je $R$ komutativan prsten sa jedinicom, ispostavi se da je $A \in M_n(R)$ invertibilna ako i samo ako je $det(A)$ invertibilna u $R$: $M_n(R)^\times = \{A \in M_n(R) \mid det(A) \in R^\times\}$. Dokaz ove činjenice je suštinski isti kao u linearnoj algebri za $\mathbb{R}$. Naime, i u ovom slučaju važi jednakost: $det(A)\ E = adj(A)\ A = A\ adj(A)$, odakle je jasno da je $A$ invertibilna ako je $det(A) \in R^\times$; sa druge strane, zbog multiplikativnosti determinante, $AA^{-1} = E$ povlači $det(A)\ det(A^{-1}) = 1$, odakle $det(A) \in R^\times$.

(d) Nije teško videti da je polinom $p(X) \in \mathbb{R}[X]$ invertibilan ako i samo ako je nenula i konstantan: $\mathbb{R}[X]^\times = \mathbb{R} \setminus \{0\}$.

(e) Lako $(R_1 \times R_2)^\times = R_1^\times \times R_2^\times$.

**6/7 Zadatak.** Izračunati $\mathbb{Z}[\sqrt{2}]^\times$.

**6/8 Tvrđenje.**
Neka je $R$ prsten sa jedinicom. Tada je $R^\times$ grupa u odnosu na množenje.

*Dokaz.* Očigledno $1 \in R^\times$. Dokažimo da $u, v \in R^\times$ povlači $uv \in R^\times$. Zaista, označimo $(uv)^{-1} := v^{-1}u^{-1}$; tada je $(uv)(uv)^{-1} = uvv^{-1}u^{-1} = 1$ i $(uv)^{-1}(uv) = v^{-1}u^{-1}uv = 1$, odakle $uv \in R^\times$. Takođe, $u \in R^\times$ povlači $u^{-1} \in R^\times$ jer očigledno $(u^{-1})^{-1} = u$. Već znamo da je množenje asocijativno, 1 je neutralni element, i po definiciji svaki element $u \in R^\times$ ima inverz. Dakle, $R^\times$ je grupa u odnosu na množenje. □

Primetimo da prethodno tvrđenje sada povlači da je multiplikativni inverz elementa $u \in R^\times$ jedinstven.

**6/9 Definicija.** (a) Polje je komutativan prsten sa jedinicom $F$ u kome je $F^\times = F \setminus \{0\}$.

(b) Prsten sa deljenjem je prsten sa jedinicom $R$ u kome je $R^\times = R \setminus \{0\}$.

Dakle, u polju i prstenu sa deljenjem svi nenula elementi imaju multiplikativne inverze; jedina razlika je što zahtevamo od polja da bude komutativno. Samim tim, svako polje je i prsten sa deljenjem.

**6/10 Primer.**
Arhiprimer prstena sa deljenjem koji nije polje su kvaternioni. Ovaj primer možemo opisati na sledeći način. Neka je $\mathbb{C}$ polje kompleksnih brojeva. Izgradićemo kvaternione $\mathbb{H}$[a], tako što ćemo proširiti $\mathbb{C}$ uvođenjem još jedne imaginarne jedinice $j$. Dakle, neka je $j$ simbol za još jednu imaginarnu jedinicu: znači, $j \notin \mathbb{C}$ i $j^2 = -1$. Neka je $\mathbb{H} = \{z + wj \mid z, w \in \mathbb{C}\}$[b] na kome sabiramo i množimo na sledeći način:

$$(z_1 + w_1 j) + (z_2 + w_2 j) = (z_1 + z_2) + (w_1 + w_2)j \quad \text{i} \quad (z_1 + w_1 j)(z_2 + w_2 j) = (z_1 z_2 - w_1 \overline{w_2}) + (z_1 w_2 + w_1 \overline{z_2})j.$$

Nije teško proveriti da je $\mathbb{H}$ Abelova grupa u odnosu na sabiranje; primetimo da je $0 = 0 + 0 \cdot j$, i aditivni inverz $-(z + wj) = (-z) + (-w)j$. Dokažimo asocijativnost množenja:

$$\begin{aligned}
& (z_1 + w_1 j)[(z_2 + w_2 j)(z_3 + w_3 j)] \\
= \; & (z_1 + w_1 j)[(z_2 z_3 - w_2 \overline{w_3}) + (z_2 w_3 + w_2 \overline{z_3})j] \\
= \; & [z_1(z_2 z_3 - w_2 \overline{w_3}) - w_1 \overline{(z_2 w_3 + w_2 \overline{z_3})}] + [z_1(z_2 w_3 + w_2 \overline{z_3}) + w_1 \overline{(z_2 z_3 - w_2 \overline{w_3})}]j \\
= \; & [z_1 z_2 z_3 - z_1 w_2 \overline{w_3} - w_1 \overline{z_2} \, \overline{w_3} - w_1 \overline{w_2} z_3] + [z_1 z_2 w_3 + z_1 w_2 \overline{z_3} + w_1 \overline{z_2} \, \overline{z_3} - w_1 \overline{w_2} w_3]j.
\end{aligned}$$

Sa druge strane:

$$\begin{aligned}
& [(z_1 + w_1 j)(z_2 + w_2 j)](z_3 + w_3 j) \\
= \; & [(z_1 z_2 - w_1 \overline{w_2}) + (z_1 w_2 + w_1 \overline{z_2})j](z_3 + w_3 j) \\
= \; & [(z_1 z_2 - w_1 \overline{w_2}) z_3 - (z_1 w_2 + w_1 \overline{z_2}) \overline{w_3}] + [(z_1 z_2 - w_1 \overline{w_2}) w_3 + (z_1 w_2 + w_1 \overline{z_2}) \overline{z_3}]j \\
= \; & [z_1 z_2 z_3 - w_1 \overline{w_2} z_3 - z_1 w_2 \overline{w_3} - w_1 \overline{z_2} \, \overline{w_3}] + [z_1 z_2 w_3 - w_1 \overline{w_2} w_3 + z_1 w_2 \overline{z_3} + w_1 \overline{z_2} \, \overline{z_3}]j.
\end{aligned}$$

Primetimo da smo dobili isti rezultat, tj. definisano množenje je asocijativno. Jedinica za množenje je $1 = 1 + 0 \cdot j$, što se lako vidi. Distributivni zakoni se direktno proveravaju na sličan način. Primetimo da množenje nije komutativno:

$$ji = (0 + 1 \cdot j)(i + 0 \cdot j) = (0 \cdot i - 1 \cdot \overline{0}) + (0 \cdot 0 + 1 \cdot \overline{i})j = (-i)j \neq ij.$$

Dakle, $\mathbb{H}$ nije polje. Ostaje da proverimo da svaki nenula element ima multiplikativni inverz. Neka je $z + wj \neq 0$. Rešimo jednačinu $(z' + w'j)(z + wj) = 1$ po $z'$ i $w'$, tj. sistem $z'z - w'\overline{w} = 1$ i $z'w + w'\overline{z} = 0$.

Determinanta sistema jednaka je $\Delta = \begin{vmatrix} z & -\overline{w} \\ w & \overline{z} \end{vmatrix} = z\overline{z} + w\overline{w} = |z|^2 + |w|^2$; primetimo da je $\Delta \neq 0$ jer je bar jedan od $z$ i $w$ nenula kompleksan broj. Dalje je $\Delta_{z'} = \begin{vmatrix} 1 & -\overline{w} \\ 0 & \overline{z} \end{vmatrix} = \overline{z}$ i $\Delta_{w'} = \begin{vmatrix} z & 1 \\ w & 0 \end{vmatrix} = -w$. Po Kramerovom pravilu je $z' = \frac{\overline{z}}{|z|^2+|w|^2}$ i $w' = -\frac{w}{|z|^2+|w|^2}$. Dakle, $\frac{\overline{z}}{|z|^2+|w|^2} - \frac{w}{|z|^2+|w|^2}j$ je levi inverz od $z + wj$; direktnim računom nije teško videti da je i desni inverz.

[a] Oznaka $\mathbb{H}$ za kvaternione je u čast Hamiltona koji ih je prvi opisao.

[b] Zbir $z + wj$ je formalan, što znači da dva elementa $z_1 + w_1 j$ i $z_2 + w_2 j$ smatramo jednakim ako i samo ako $z_1 = z_2$ i $w_1 = w_2$.

Napomenimo i sledeće. Svaki konačan prsten sa deljenjem jeste polje. Ovo tvrđenje je poznato kao Mala Vederburnova teorema, i ovde je nećemo dokazivati, navodimo je samo kao informaciju.

**6/11 Definicija.** Element $a \in R$ je levi (desni) delitelj nule ako postoji $x \in R$, $x \neq 0$, takav da $ax = 0$ ($xa = 0$); $a$ je obostrani delitelj nule ako je i levi i desni delitelj nule. Očigledno, ako je $R$ komutativan, $a$ je levi delitelj nule ako i samo ako $a$ je desni delitelj nule, ako i samo ako $a$ je obostrani delitelj nule; u tom slučaju kažemo samo delitelj nule.

U skladu sa prethodnom definicijom, 0 je uvek i delitelj nule. (Ponekad se definiše da je delitelj nule obavezno nenula element, ali to je samo stvar definicije koja nije bitna.) Dakle, kada govorimo o deliteljima nule, jedino je zanimljivo da govorimo da li je nenula element delitelj nule.

Ako $R$ ima jedinicu, napomenimo da ona nikad nije delitelj nule jer za svako $x \neq 0$, $1 \cdot x = x \cdot 1 = x \neq 0$. Slično, invertibilan element $u \in R^\times$ nikad nije delitelj nule jer ako $ux = 0$ za neko $x \neq 0$ (ili $xu = 0$), onda imamo $0 \neq x = 1 \cdot x = u^{-1}ux = u^{-1} \cdot 0 = 0$, što je nemoguće. Kontrapozicijom sada možemo da zaključimo da netrivijalni delitelji nule nikada nisu invertibilni.

**6/12 Primer** (Primeri delitelja nule).(a) Videli smo da u $\mathbb{Z}_n$, $k \in \mathbb{Z}_n$ je invertibilan ako i samo ako $nzd(k, n) = 1$. Dokažimo $k \in \mathbb{Z}_n$ je delitelj nule ako i samo ako $nzd(k, n) > 1$. Smer ($\Rightarrow$) je očigledan, jer, kako smo već napomenuli, delitelj nule nije invertibilan. Pretpostavimo da je $k \in \mathbb{Z}_n$ takav da $nzd(k, n) = d > 1$; zapišimo $k = k'd$ i $n = n'd$, i primetimo $n' \neq 0$ u $\mathbb{Z}_n$ jer $n' < n$. Tada je $kn' = k'dn' = k'n = 0$ u $\mathbb{Z}_n$, pa je $k$ delitelj nule.

(b) Slično, u prstenu $M_n(\mathbb{R})$, ako matrica nije invertibilna ona je delitelj nule. Pretpostavimo da $A$ nije invertibilna, što znači da je $det(A) = 0$. Međutim, to znači da je 0 jedna od sopstvenih vrednosti matrice $A$, pa postoji nenula vekotor $v$ koji je sopstveni za 0, tj. $Av = 0 \cdot v = 0$. Sada možemo da napravimo matricu $B$ tako što poređamo $n$ puta vektor $v$ u nju: $B = \begin{pmatrix} v & v & \dots & v \end{pmatrix}$; očigledno, $B$ je nenula matrica i $AB = 0$. Ovo pokazuje da je $A$ levi delitelj nule. Da bismo videli da je $A$ desni delitelj nule, primetimo da je $det(A^T) = 0$ takođe, pa nađemo sopstveni vektor $w$ za $A^T$ koji odovara sopstvenoj vrednosti 0: $A^T w = 0 \cdot w = 0$. Odatle je $w^T A = 0$, pa ako napravimo matricu $C$ tako što poređamo $n$ puta vrstu $w^T$ u nju: $C = \begin{pmatrix} w^T \\ w^T \\ \vdots \\ w^T \end{pmatrix}$, jasno dobijamo nenula matricu $C$ takvu da $CA = 0$; dakle, $A$ je i desni delitelj nule.

**6/13 Zadatak.** Ako je $det(A) = 0$ naći matricu $D$ takvu da $AD = DA = 0$.

(c) Ako su $R_1$ i $R_2$ prsteni, $R_1 \times R_2$ uvek ima netrivijalne delitelje nule (specijalno, nikad nije prsten sa deljenjem ili polje, jer delitelji nule nisu invertibilni). Naime, za $x \in R_1$ i $y \in R_2$, $x, y \neq 0$, $(x, 0) \cdot (0, y) = (0, 0) = (0, y) \cdot (x, 0)$, pa su elementi oblika $(x, 0)$ i $(0, y)$ uvek deliteji nule.

(d) Neka je $\mathbb{R}^\infty$ beskonačno dimenzioni vektorski prostor nizova $(a_0, a_1, a_2, \dots)$, i neka je $R$ skup svih linearnih preslikavanja $\mathbb{R}^\infty \to \mathbb{R}^\infty$. Nije teško proveriti da je $R$ prsten u kome sabiramo na sledeći

način: $(f+g)(\vec{x}) := f(\vec{x}) + g(\vec{x})$, a množenje je obična kompozicija preslikavanja. Nula je samo konstantno nula-preslikavanje, a jedinica je naravno $id_{\mathbb{R}^\infty}$. Uočimo sledeća tri elementa prstena $R$: levi šift $\lambda(a_0, a_1, a_2, \dots) := (a_1, a_2, a_3, \dots)$, desni šift $\delta(a_0, a_1, a_2, \dots) = (0, a_0, a_1, \dots)$ i prvu „projekciju" $\pi(a_0, a_1, a_2, \dots) = (a_0, 0, 0, \dots)$. Primetimo $\lambda\delta = id$, tj. $\delta$ je desni inverz za $\lambda$, odnosno $\lambda$ je levi inverz za $\delta$. Odavde sledi da $\lambda$ ne može biti desni delitelj nule: ako je $f\lambda = 0$, onda je $f = f\ id = f\lambda\delta = 0\ \delta = 0$, tj. $f = 0$. Slično, $\delta$ ne može biti levi delitelj nule. Sa druge strane, $\lambda\pi = 0$ i $\pi\delta = 0$, pa $\lambda$ jeste levi, a $\delta$ jeste desni delitelj nule.

**6/14 Definicija.** Komutativan prsten sa jedinicom $R$ je domen ako nema netrivijalne delitelje nule. (Drugim rečima, $R$ je domen ako u njemu važi popularan zakon: $ab = 0 \implies a = 0 \vee b = 0$.)

**6/15 Primer** (Primeri domena)**.**(a) $\mathbb{Z}$ je domen.

(b) Polja su domeni (jer su svi nenula elementi invertibilni, pa ne mogu biti delitelji nule).

(c) $\mathbb{Z}_n$ je domen ako i samo ako je $n$ prost broj. Ako ne $n$ prost broj, onda za $k \in \mathbb{Z}_n$, $k \neq 0$, imamo $nzd(k, n) = 1$, pa je $k$ invertibilan (kako smo već videli), pa je $\mathbb{Z}_n$ polje, pa i domen. Ako $n$ nije prost, imamo $1 < k < n$ u $\mathbb{Z}_n$ tako da $k \mid n$, odakle je $nzd(k, n) = k > 1$, pa je $k$ delitelj nule (što smo takođe već videli), odakle $\mathbb{Z}_n$ nije domen (pa ni polje).

> **6/16 Komentar.** Primetimo da smo zaključili $\mathbb{Z}_n$ je polje ako i samo ako $n$ je prost broj.

(d) Ako je $R$ domen, onda je i prsten polinoma nad $R$, $R[X]$, takođe domen. Ako je $p(X)$ nenula polinom sa vodećim koeficijentom $a \neq 0$, i ako je $q(X)$ nenula polinom sa vodećim koeficijentom $b$, onda je $p(X)q(X)$ polinom sa vodećim koeficijentom $ab \neq 0$ (jer je $R$ domen), odakle, $p(X)q(X) \neq 0$. Dakle, $R[X]$ nema netrivijalne delitelje nule.

U prethodnom primeru smo naglasili da je polje uvek domen, kao i da je prsten $\mathbb{Z}_n$ domen ako i samo ako je polje. Ovo je zapravo tačno za sve konačne prstene.

**6/17 Teorema.**
Neka je $R$ konačan domen. Tada je $R$ polje.

*Dokaz.* Neka je $x \in R$ nenula element. Treba da nađemo njegov multiplikativan inverz. Posmatrajmo niz $x, x^2, x^3, \dots$. Kako je $R$ konačan, ovaj niz nije beskonačan; specijalno, postoje $m < n$ takvi da $x^m = x^n$. Odavde je $x^m(1 - x^{n-m}) = 0$. Kako je $R$ domen imamo dve mogućnosti: $x^m = 0$ ili $1 - x^{n-m} = 0$.

Neka je $x^m = 0$. Tada postoji najmanje $k$ tako da $x^k = 0$. Kako $x \neq 0$, $k > 1$ i očigledno $k \leqslant m$. Međutim tada je $0 = x^k = xx^{k-1}$, pa kako $x \neq 0$ i $R$ je domen, mora biti $x^{k-1} = 0$; ovo protivreči pretpostavci da je $k$ bio najmanji za koji je $x^k = 0$. Dakle, ovaj slučaj nije moguć.

Neka je $1 - x^{n-m} = 0$, tj. $x^{n-m} = 1$. Odatle je $xx^{n-m-1} = 1$, i našli smo inverz od $x$. Dakle, $R$ je polje. □

## B Homomorfizmi prstena

**6/18 Definicija.** Neka su $R$ i $S$ prsteni i $\varphi : R \to S$. Preslikavanje $\varphi$ je homomorfizam prstena ako zadovoljava sledeće aksiome:

- $\varphi(x +_R y) = \varphi(x) +_S \varphi(y)$;
- $\varphi(x \cdot_R y) = \varphi(x) \cdot_S \varphi(y)$.

Ako $R$ i $S$ imaju jedinicu, zahtevamo i da je:

- $\varphi(1_R) = 1_S$.

**6/19 Komentar.** Neka je $\varphi : R \to S$ homomorfizam prstena. Zbog prve aksiome, $\varphi$ je specijalno homomorfizam Abelovih grupa $\varphi : (R, +_R, 0_R) \to (S, +_S, 0_S)$, pa iz Algebre 1 znamo da je:

- $\varphi(0_R) = 0_S$, i
- $\varphi(-x) = -\varphi(x)$ za sve $x \in R$.

**6/20 Komentar.** Sledeće stvari su lake:

(a) $id_R : R \to R$ je uvek homomorfizam prstena.

(b) Ako su $\varphi : R \to S$ i $\psi : S \to T$ homomorfizmi prstena, onda je i $\psi \circ \varphi : R \to T$ homomorfizam prstena.

(c) Ako je $\varphi : R \to S$ homomorfizam i bijekcija, onda je i $\varphi^{-1} : S \to R$ homomorfizam (i bijekcija). (Ovakve homomorfizme zovemo izomorfizmi; vidi sledeću definiciju.)

**6/21 Definicija.** Neka je $\varphi : R \to S$ homomorfizam prstena.

(a) Ako je $R = S$, za $\varphi$ kažemo da je endomorfizam.

(b) Ako je $\varphi$ 1-1, za $\varphi$ kažemo da je monomorfizam.

(c) Ako je $\varphi$ na, za $\varphi$ kažemo da je epimorfizam.

(d) Ako je $\varphi$ bijekcija, za $\varphi$ kažemo da je izomorfizam.

(e) Ako je $R = S$ i $\varphi$ je bijekcija, za $\varphi$ kažemo da je automorfizam.

**6/22 Primer.**(a) Preslikavanje $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ dato sa $\varphi(x) =$ „ostatak pri deljenju $x$ sa $n$" je epimorfizam prstena; $\varphi$ nije 1-1.

(b) Preslikavanje $\pi_1 : R \times S \to R$ dato sa $\pi_1(x, y) = x$ je epimorfizam prstena; $\pi_1$ nije 1-1 ako je $S$ netrivijalan. Slično i $\pi_2 : R \times S \to S$ dato sa $\pi_1(x, y) = y$ je epimorfizam prstena.

(c) Neka je $R$ prsten i $c \in R$. Preslikavanje $\varphi_c : R[X] \to R$ dato sa $\varphi(p(X)) = p(c)$ je epimorfizam prstena.

(d) Konjugacija $\mathbb{C} \to \mathbb{C}$, data sa $z \to \bar{z}$, je automorfizam prstena $\mathbb{C}$.

(e) Neka je $U_2(\mathbb{R})$ prsten gornje trougaonih $2 \times 2$ matrica nad $\mathbb{R}$:

$$U_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}.$$

(Proveriti da je ovo zaista prsten (nekomutativan sa jedinicom).) Definišemo $\varphi : U_2(\mathbb{R}) \to \mathbb{R} \times \mathbb{R}$ sa $\varphi \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = (a, c)$. Tada je $\varphi$ epimorfizam prstena. Očigledno je da je $\varphi$ na, da se slaže sa sabiranjem, i da jedinicu slika u $(1, 1)$, što je jedinica u $\mathbb{R} \times \mathbb{R}$. Proveravamo i da se slaže sa množenjem:

$$\varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\right) = \varphi \begin{pmatrix} ax & ay + bz \\ 0 & cz \end{pmatrix} = (ax, cz) = (a, c)(x, z) = \varphi \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \varphi \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}.$$

**6/23 Definicija.** Neka je $\varphi : R \to S$ homomorfizam prstena.

(a) Jezgro homomorfizma $\varphi$ je $ker(\varphi) = \{x \in R \mid \varphi(x) = 0_S\}$.

(b) Slika homomorfizma $\varphi$ je $im(\varphi) = \{\varphi(x) \mid x \in R\} \subseteq S$.

**6/24 Primer.**(a) Jezgro epimorfizam $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ datog sa $\varphi(x) =$ „ostatak pri deljennju $x$ sa $n$" je $ker(\varphi) = n\mathbb{Z}$.

(b) Jezgro epimorfizma $\pi_1 : R \times S \to R$ datog sa $\pi_1(x, y) = x$ je $ker(\pi_1) = 0 \times S$.

(c) Neka je $c \in \mathbb{R}$. Izračunajmo jezgro epimorfizma $\varphi_c : \mathbb{R}[X] \to \mathbb{R}$ datog sa $\varphi_c(p(X)) = p(c)$. Znamo da je $p(c) = 0$ ako i samo ako je $p(X)$ deljiv sa $X - c$, pa je $ker(\varphi_c) = \{(X - c)q(X) \mid q(X) \in \mathbb{R}[X]\}$.

(d) Neka je $\varphi_i : \mathbb{R}[X] \to \mathbb{C}$ preslikavanje dato sa $\varphi_i(p(X)) = p(i)$. Nije teško videti da je $\varphi_i$ epimorfizam prstena. Izračunajmo jezgro. Znamo $p(i) = 0$ ako i samo ako $p(-i) = 0$ (kompleksne nule kod polinoma sa realnim koeficijentima se javljaju po konjugovanim parovima), pa odatle, $p(i) = 0$ ako i samo ako $p(X)$ je deljiv sa $(X - i)(X + i) = X^2 + 1$. Dakle, $ker(\varphi_i) = \{(X^2 + 1)q(X) \mid q(X) \in \mathbb{R}[X]\}$.

(e) Jezgro epimorfizma $\varphi : U_2(\mathbb{R}) \to \mathbb{R} \times \mathbb{R}$ datog sa $\varphi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = (a, c)$, očigledno je $ker(\varphi) = \left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{R}\right\}$.

Očigledno je $\varphi$ na ako i samo ako $im(\varphi) = S$. Kao i kod grupa, $\varphi$ je 1-1 ako i samo ako je jezgro trivijalno: $ker(\varphi) = \{0_R\}$.

**6/25 Tvrđenje.**
Neka je $\varphi : R \to S$ homomorfizam prstena. Tada je $\varphi$ 1-1 ako i samo ako $ker(\varphi) = \{0_R\}$.

*Dokaz.* Kako smo već komentarisali, $\varphi$ je specijalno homomorfizam Abelovih grupa $\varphi : (R, +_R, 0_R) \to (S, +_S, 0_S)$, pa iz Algebre 1 znamo da je $\varphi$ 1-1 ako i samo ako $ker(\varphi) = \{0_R\}$. □

**6/26 Zadatak.** Neka je $R$ prsten i $a \in R$. Definišemo oznaku $n \cdot a$, $n \in \mathbb{Z}$, na sledeći način:

- $0 \cdot a := 0_R$;
- $n \cdot a := \underbrace{a + a + \cdots + a}_{n}$ za $n \geqslant 1$;
- $n \cdot a := -((-n) \cdot a)$ za $n \leqslant -1$.

Za $m, n \in \mathbb{Z}$ i $a \in R$ dokazati:

(a) $m \cdot a + n \cdot a = (m + n) \cdot a$;

(b) $m \cdot (n \cdot a) = (mn) \cdot a$.

Dalje definišemo oznaku $a^n$ na sledeći način:

- $a^n := \underbrace{aa \ldots a}_{n}$ za $n \geqslant 1$;
- ako $R$ ima jedinicu i $a \neq 0$, $a^0 := 1_R$;
- ako $a \in R^\times$, $a^n := (a^{-1})^{-n}$ za $n \leqslant -1$.

Kada je definisan odgovarajući izraz, dokazati:

(c) $a^m a^n = a^{m+n}$;

(d) $(a^n)^{-1} = a^{-n}$;

(e) $(a^m)^n = a^{mn}$.

**6/27 Primer** (Karakteristika prstena)**.**
Neka je $R$ prsten sa jediniciom. Primetimo da postoji jedinstveni homomorfizam $\chi : \mathbb{Z} \to R$. Zaista, najpre mora biti $\chi(0) = 0_R$ i $\chi(1) = 1_R$, a onda poštujući sabiranje mora biti:

$$\chi(n) = \chi(\underbrace{1 + 1 + \cdots + 1}_{n}) = \underbrace{\chi(1) + \chi(1) + \cdots + \chi(1)}_{n} = \underbrace{1_R + 1_R + \cdots + 1_R}_{n} = n \cdot 1_R,$$

za $n \geqslant 2$, gde je $n \cdot 1_R$ samo oznaka za zbir $n$-mnogo $1_R$. Dalje, poštujući sabiranje vidimo:

$$0_R = \chi(0) = \chi(n + (-n)) = \chi(n) + \chi(-n) = n \cdot 1_R + \chi(-n),$$

odakle je $\chi(-n) = -(n \cdot 1_R) = -n \cdot 1_R$ za $n \geqslant 1$. Sada nije teško videti da ovo preslikavanje zaista jeste homomorfizam prstena (koristeći prethodni zadatak npr.).
Jezgro homomorfizma $\chi$ je aditivna podgrupa od $\mathbb{Z}$, tj. $ker(\chi) = n\mathbb{Z}$ za neko $n \geqslant 0$. Broj $n$ se zove karakteristika prstena $R$, i obeležava se sa $char(R)$. Primetimo:

- $char(R) \neq 1$ jer u suprotnom $1 \in ker(\chi)$, pa je $0_R = \chi(1) = 1_R$ (setimo se da implicitno pretpostavljamo $0_R = 1_R$);
- ako je $char(R) = n \geqslant 2$, onda je $n$ najmanji pozitivan broj takav da $n \cdot 1_R = 0_R$; ovo je slučaj npr. u prstenu $\mathbb{Z}_n$: $char(\mathbb{Z}_n) = n$;
- ako je $char(R) = 0$, onda je $\chi$ 1-1, i ne postoji pozitivno $n$ takvo da $n \cdot 1_R = 0_R$; npr. $char(\mathbb{Z}) = 0$, $char(\mathbb{R}[X]) = 0$, $char(M_n(\mathbb{R})) = 0$ itd.

**6/28 Zadatak.** Ako je $R$ domen (ili samo sa jedinicom bez delitelja nule), dokazati $char(R) = 0$ ili $char(R) = p$ za neki prost broj $p$. Specijalno, ovo je tačno za polja.

## C Potprsteni i ideali

**6/29 Definicija** (Potprsten)**.** Neka je $R$ prsten i $S \subseteq R$. $S$ je potprsten od $R$, $S \leqslant R$, ako važe sledeće aksiome:

- $(S, +)$ je podgrupa od $(R, +)$, tj.:
  - $0 \in S$;
  - ako $x \in S$ onda i $-x \in S$;
  - ako $x, y \in S$ onda i $x + y \in S$.

  Iz Algebre 1 znamo da je ekvivalentan uslov da je $S \neq \varnothing$, i $x, y \in S$ povlači $x - y \in S$.
- ako $x, y \in S$ onda i $xy \in S$.

Ako $R$ ima jedinicu tražimo i:

- $1 \in S$.

**6/30 Primer** (Primeri potprstena)**.**(a) Jedini potprsten od $\mathbb{Z}$ je sam $\mathbb{Z}$. Zaista, ako $S \leqslant \mathbb{Z}$, kako $1 \in S$ i kako je $S$ aditivna podgrupa od $\mathbb{Z}$, $S$ mora da sadrži i aditivnu podgrupu generisanu sa 1, a to je celo $\mathbb{Z}$.

(b) U prstenu $2\mathbb{Z}$, potprsteni su svi podskupovi $2n\mathbb{Z}$, što se lako vidi.

(c) Primetimo $\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C}$.

**6/31 Definicija** (Ideal)**.** Neka je $R$ prsten i $I \subseteq R$. $I$ je ideal od $R$, $I \lhd R$, ako važe sledeće aksiome:

- $(I, +)$ je podgrupa od $(R, +)$, dakle, $I \neq \varnothing$, i $x, y \in I$ povlači $x - y \in I$.

- ako $x \in I$ i $r \in R$, onda $xr, rx \in I$.[6]

**6/32 Komentar.** Ako $R$ nema jedinicu, onda je svaki ideal i potprsten od $R$ (i potprsten i ideal su aditivne podgrupe od $R$, potprsten, ako $R$ nema jedinicu, treba samo da bude zatvoren za množnje, dok ideal mora da zadovoljava i više, mora da bude zatvoren i za množenje elementima iz $R$.) Ako $R$ ima jedinicu, onda je samo $R$ istovremeno i potprsten i ideal od sebe. Naime, svaki potprsten mora da sadrži jedinicu, dok pravi ideali (ideali strogo manji od $R$) nikada ne sadrže jedinicu, što sledi iz sledećeg tvrđenja.

**6/33 Tvrđenje.**
Neka je $R$ prsten sa jedinicom i $I \lhd R$. Sledeći iskazi su ekvivalentni:

(1) $I = R$;

(2) $1 \in I$;

(3) $R^\times \cap I \neq \varnothing$.

*Dokaz.* (1) $\Rightarrow$ (2) i (2) $\Rightarrow$ (3) su očigledni, pa dokazujemo (3) $\Rightarrow$ (1). Neka $u \in R^\times \cap I$. Tada za svako $r \in R$ imamo i $(ru^{-1})u \in I$, tj. $r \in I$; dakle, $R \subseteq I$, odakle $R = I$. □

Dakle, pravi ideali u prstenima sa jedinicama nikada ne sadrže invertibilne elemente.

**6/34 Primer** (Primeri ideala)**.**(a) U svakom prstenu, $0 := \{0\}$ je ideal: nula-ideal.

(b) Ideali prstena $\mathbb{Z}$ su tačno skupovi $n\mathbb{Z}$. Zaista, ovo su jedine aditivne podgrupe od $\mathbb{Z}$, ali zadovoljavaju i uslov da za $r \in \mathbb{Z}$ i $nk \in n\mathbb{Z}$, $rnk = n(rk) \in n\mathbb{Z}$.

(c) U prstenu $2\mathbb{Z}$, podskup $2n\mathbb{Z}$ je ideal, što lako vidimo na sličan način.

(d) Ako je $F$ polje, jedini pravi ideal je nula ideal, što sledi iz prethodnog tvrđenja, jer su svi nenula elementi invertibilni.

**6/35 Tvrđenje** (Presek ideala je ideal)**.**
Neka je $R$ prsten, i $I_\lambda$, $\lambda \in \Lambda$, familija ideala od $R$. Tada je i $I := \bigcap_{\lambda\in\Lambda} I_\lambda$ ideal od $R$.

*Dokaz.* Kako je presek podgrupa – podgrupa, $I$ jeste aditivna podgrupa od $R$. Neka $x \in I$, tj. $(\forall\lambda \in \Lambda)\ x \in I_\lambda$, i neka $r \in R$. Tada $(\forall\lambda \in \Lambda)\ rx, xr \in I_\lambda$ jer $I_\lambda \lhd R$, odakle $rx, xr \in I$. Dakle, $I \lhd R$. □

Primetimo da je, očigledno, presek ideal najveći ideal koji je sadržan u svakom članu preseka.

**6/36 Primer** (Glavni ideal)**.**
Neka je $R$ prsten sa jedinicom i $a \in R$. Glavni ideal generisan sa $a$, u oznaci $\langle a\rangle$, je najmanji ideal od $R$ koji sadrži $a$. Primetimo najpre da takav ideal postoji prema prethodnom tvrđenju, jer je najmanji ideal koji sadrži $a$ upravo presek svih ideala koji sadrže $a$ (primetimo da uvek postoji ideal koji sadrži $a$, a to je ceo prsten $R$).
Opišimo $\langle a\rangle$ na lepši način (i za to nam je potrebno da $R$ ima jedinicu). Tvrdimo:

$$\langle a\rangle = RaR := \{r_1ar_1' + r_2ar_2' + \cdots + r_nar_n' \mid n \geqslant 1,\ r_1, r_1', r_2, r_2', \ldots, r_n, r_n' \in R\}.$$

Nije teško videti da $RaR$ jeste ideal (direktan račun); takođe, $a \in RaR$ jer možemo zapisati $a = 1 \cdot a \cdot 1$. Dakle, po definiciji, $\langle a\rangle \subseteq RaR$. Sa druge strane, $a \in \langle a\rangle$ povlači $ra \in \langle a\rangle$ jer je $\langle a\rangle$ ideal, što dalje povlači $rar' \in \langle a\rangle$ iz istog razloga, pa i sume ovakvih elemenata pripadaju $\langle a\rangle$ jer je ideal zatvoren za sabiranje.

[6] Ako je $R$ komutativan, dovoljno je samo da tražimo $rx \in I$. U nekomutativnom slučaju možemo da definišemo posebno leve ideale, one koji zadovoljavaju $rx \in I$, i desne ideale, one koji zadovoljavaju $xr \in I$, i oni ne moraju biti isti. Nas ovde zanimaju obostrani ideali, tj. ideali u smislu naše definicije.

Dakle, važi i $RaR \subseteq \langle a \rangle$, čime smo završili dokaz jednakosti.
U slučaju komutativnog prstena sa jedinicom, $\langle a \rangle$ zaista ima lep opis: $\langle a \rangle = Ra := \{ra \mid r \in R\}$. To sledi jer u slučaju komutativnog prstena imamo:

$$r_1 a r_1' + r_2 a r_2' + \cdots + r_n a r_n' = r_1 r_1' a + r_2 r_2' a + \cdots + r_n r_n' a = \underbrace{(r_1 r_1' + r_2 r_2' + \cdots + r_n r_n')}_{=r} a = ra,$$

odakle direktno sledi $RaR = Ra$.

Primetili smo da je presek ideala najveći ideal koji je sadržan u svakom idealu koji učestvuje u preseku. Postoji i najmanji ideal koji sadrži neku familiju ideala: njena suma.

**6/37 Tvrđenje** (Suma ideala)**.**
Neka je $R$ prsten, i $I_\lambda$, $\lambda \in \Lambda$, familija idela od $R$. Tada je:

$$I = \sum_{\lambda \in \Lambda} I_\lambda := \{x_1 + x_2 + \cdots + x_n \mid n \geqslant 1,\ \lambda_i \in \Lambda,\ x_i \in I_{\lambda_i}\}$$

najmanji ideal od $R$ koji sadrži sve $I_\lambda$. (Da bude jasno, u sumi su sve moguće konačne sume elemenata iz ideala u familiji.)

*Dokaz.* Direktan račun za vežbu. □

Konkretno, ako $I, J \lhd R$, onda je $I + J = \{i + j \mid i \in I,\ j \in J\}$. Primetimo, ako je $R$ komutativan, onda je $\langle x \rangle + \langle y \rangle = \{rx + r'y \mid r, r' \in R\}$; ovaj ideal označavamo i sa $\langle x, y \rangle$.

**6/38 Zadatak.** Izračunati $m\mathbb{Z} \cap n\mathbb{Z}$ i $m\mathbb{Z} + n\mathbb{Z}$ u $\mathbb{Z}$.

**6/39 Definicija.** Neka je $R$ prsten.

(a) Ideal $M \lhd R$ je maksimalan ako je $M \subsetneq R$ i ne postoji $N \lhd R$ takav da $M \subsetneq N \subsetneq R$.

(b) Ako je $R$ komutativan, ideal $P \lhd R$ je prost ako zadovoljava $xy \in P$ povlači $x \in P$ ili $y \in P$.

Naglasimo da pojam prostog ideala nismo definisali za nekomutativne prstene.

**6/40 Primer.**(a) $R$ je očigledno uvek prost ideal od sebe; ovo nije zanimljivo.

(b) 0 je prost ideal ako i samo ako $R$ nema delitelje nule.

(c) U $\mathbb{Z}$ su prosti ideali 0 i $p\mathbb{Z}$, gde je $p$ prost broj. U $\mathbb{Z}$ su maksimalni ideali $p\mathbb{Z}$, gde je $p$ prost broj.

(d) Maksimalni ideali u $\mathbb{C}[X]$ su tačno glavni ideali generisani polinomom stepena 1: $X - z$. Najpre, da bismo videli da je $\langle X - z \rangle$ maksimalan, pretpostavimo $\langle X - z \rangle \subsetneq N$ i dokažimo $N = \mathbb{C}[X]$. Postoji polinom $p(X) \in N \setminus \langle X - z \rangle$; specijalno, $p(X)$ nije deljiv sa $X - z$, pa kada ga podelimo sa $X - z$ dobijamo nenula konstantni ostatak: $p(X) = (X - z)q(X) + w$, $w \in \mathbb{C}^\times$. Odatle, $w = p(X) - (X - z)q(X) \in N$ jer $p(X) \in N$ i $(X - z)q(X) \in \langle X - z \rangle \subseteq N$. Kako $N$ sadrži invertibilan element $w$, $N = \mathbb{C}[X]$.

Dokažimo sada da nemamo druge maksimalne ideale. Neka je $M$ maksimalan; očigledno $M \neq 0$ i $M \cap \mathbb{C}^\times = \varnothing$. Izaberimo polinom $a(X) \in M$ najmanjeg stepena (dakle, on je stepena bar jedan). Neka je $X - z$ linearan faktor od $a(X)$, pa $a(X) \in \langle X - z \rangle$. Dokazujemo $M = \langle X - z \rangle$. Zbog maksimalnosti, dovoljno je da dokažemo $M \subseteq \langle X - z \rangle$. Neka je $p(X) \in M$, i podelimo $p(X)$ sa $a(X)$ sa ostatkom: $p(X) = a(X)q(X) + r(X)$, gde je $r(X)$ stepena manjeg od $a(X)$. Primetimo da $r(X) = p(X) - a(X)q(X) \in M$, pa kako smo izabrali $a(X)$ da bude najmanjeg mogućeg stepena u $M$, i kako je $r(X)$ manjeg stepena, i kako $M \cap \mathbb{C}^\times = \varnothing$, mora biti $r(X) = 0$. Dakle, $p(X) = a(X)q(X) \in \langle X - z \rangle$ jer $a(X) \in \langle X - z \rangle$.

**6/41 Zadatak.** Dokazati da su maksimalni ideali u $\mathbb{R}[X]$ glavni ideali generisani linearnim polinomom, i glavni ideali generisani kvadratnim polinomom sa negativnom diskriminantom.

**6/42 Tvrđenje.**
Neka je $R$ komutativan prsten sa jedinicom. Ako je $M \lhd R$ maksimalan, onda je on i prost.

*Dokaz.* Pretpostavimo $x, y \notin M$. Tada, zbog maksimalnosti, $\langle x \rangle + M = R$ i $\langle y \rangle + M = R$, pa možemo zapisati $rx + m = 1$ i $r'y + m' = 1$ za neke $r, r' \in R$ i $m, m' \in M$. Odavde je množenjem $1 = rr'(xy) + \underbrace{(rxm' + r'ym + mm')}_{\in M}$, pa ako bi bilo $xy \in M$ dobili bismo i da $1 \in M$, što nije; dakle, $xy \notin M$. Prema tome, $M$ je prost. □

**6/43 Primer.**
Primetimo dve stvari:

(a) Prethodno tvrđenje ne važi ako $R$ nema jedinicu. Naime, posmatrajmo prsten $R = 2\mathbb{Z}$ i ideal $M = 4\mathbb{Z}$. Primetimo da $M$ nije prost jer $2 \cdot 2 = 4 \in M$, ali $2 \notin M$. Međutim, $M$ jeste maksimalan. Pretpostavimo da je $M \subsetneq N$ i $n \in N \setminus M$; tada je $n$ oblika $n = 4k + 2$, pa $2 = n - 4k \in N$ jer $n \in N$ i $4k \in M \subseteq N$. Kako $2 \in N$, sada nije teško videti da je $N = R$, što dokazuje da $M$ jeste maksimalan.

(b) Primetimo i da obratno ne važi, prost ideal ne mora biti maksimalan. Najjednostavniji primer je npr. ideal 0 u $\mathbb{Z}$, koji jeste prost jer $\mathbb{Z}$ nema delitelje nule, ali nije maksimalan – sadržan je u svim idealima $n\mathbb{Z}$.

Nešto netrivijalniji primer je sledeći. Neka je $P = \langle X \rangle$ u prstenu $R = \mathbb{Z}[X]$; dakle, $P$ je skup svih polinoma čiji je konstantan koeficijent nula. Ideal $P$ jeste prost: ako $p(X), q(X) \notin P$, to znači da $p(X)$ i $q(X)$ imaju nenula konstantne koeficijente, npr. $a$ i $b$; tada je i konstantan koeficijent $ab$ polinoma $p(X)q(X)$ takođe nenula, pa $p(X)q(X) \notin P$. Dakle, $P$ je prost. Sa druge strane, $P$ nije maksimalan. Npr. $M = \langle 2 \rangle + P$ je strogo veći od $P$ jer $2 \in M \setminus P$, ali $M$ nije ceo $R$. Zaista, nije teško videti da proizvoljan element u $M$, koji je oblika $2f(X) + Xg(X)$, ima paran konstantan koeficijent, pa $M \neq R$. Prema tome, našli smo strogo veći pravi ideal od $P$, i $P$ nije maksimalan.

**6/44 Zadatak.** Dokazati da je $\langle 2, X \rangle$ maksimalan u $\mathbb{Z}[X]$, i dokazati da ovaj ideal nije glavni.

U prstenima sa jedinicom maksimalni ideali uvek postoje. Za dokaz nam je potrebna aksioma izbora:

**6/45 Teorema** (Hauzdorfov princip maksimalnosti (aksioma izbora)).
Svaka neprazna familija skupova $\mathcal{F}$ ima maksimalan lanac u odnosu na $\subseteq$, tj. postoji potfamilija $\mathcal{L} \subseteq \mathcal{F}$ takva da:

- $A, B \in \mathcal{L}$ povlači $A \subseteq B$ ili $B \subseteq A$, i ($\mathcal{L}$ je lanac)
- ako $A \in \mathcal{F} \setminus \mathcal{L}$ onda postoji $B \in \mathcal{L}$ takav da $A \not\subseteq B$ i $B \not\subseteq A$. ($\mathcal{L}$ je maksimalan lanac)

**6/46 Tvrđenje.**
Neka je $R$ prsten sa 1. Tada $R$ ima maksimalan ideal.

*Dokaz.* Neka je $\mathcal{I}$ familija svih pravih (različitih od $R$) ideala u $R$; $\mathcal{I}$ je neprazna jer $0 \in \mathcal{I}$. Prema Hauzdorfovom principu maksimalnosti izaberimo neki maksimalni lanac $\mathcal{L} \subseteq \mathcal{I}$. Tvrdimo da je $M := \bigcup \mathcal{L}$ maksimalan ideal.

Prvo dokazujemo da je $M$ ideal. Jasno je da $\mathcal{L} \neq \varnothing$ jer $\mathcal{I} \neq \varnothing$, pa $0 \in M$ jer pripada svakom članu unije. Neka $x, y \in M$; tada $x \in I$ i $y \in J$ za neke $I, J \in \mathcal{I}$. Kako je $\mathcal{L}$ lanac, $I$ i $J$ su uporedivi, npr. $I \subseteq J$. Tada $x, y \in J$, pa i $x - y \in J$, pa $x - y \in M$. Dakle, $M$ jeste aditivna podgrupa od $R$. Neka $x \in M$ i $r \in R$. Ponovo $x \in I$ za neko $I \in \mathcal{I}$, pa $xr, rx \in I$, odakle i $xr, rx \in M$. Dakle, $M$ jeste ideal.

$M$ je i pravi ideal jer $1 \notin M$ (jer 1 ne pripada nijednom članu unije; jedino u ovom trenutku korstimo da $R$ ima jedinicu). Dakle, $M \in \mathcal{I}$.

Dokažimo da je $M$ maksimalan ideal. Pretpostavimo suprotno, $M \subsetneq N \subsetneq R$ i $N \lhd R$. Tada $N \in \mathcal{I}$ i $N$ je strogi nadskup svih ideala iz $\mathcal{L}$ jer je strogi nadskup njihove unije. To znači da se $\mathcal{L}$ može produžiti do lanca $\mathcal{L} \cup \{N\}$, što protivreči činjenici da je $\mathcal{L}$ bio maksimalan lanac. Završili smo dokaz. □

**6/47 Zadatak.** Neka je $R$ prsten sa jedinicom.

(a) Neka je $I \lhd R$ pravi ideal. Dokazati da postoji maksimalan ideal $M \lhd R$ takav da $I \subseteq M$.

(b) Neka $a \in R$ nije invertibilan. Dokazati da postoji maksimalan ideal $M \lhd R$ takav da $a \in M$.

(Adaptirati prethodni dokaz.)

U dokazu prethodnog tvrđenja koristili smo da $R$ ima jedinicu. Postavlja se prirodno pitanje da li prsten bez jedinice mora da ima maksimalan ideal (videli smo da može da ima: $4\mathbb{Z}$ u $2\mathbb{Z}$ jeste maksimalan). Odgovor je u opštem slučaju negativan:

**6/48 Primer** (Primer prstena koji nema maksimalan ideal)**.**
Ovo pitanje nije lako. Daćemo jedan veštački primer, a kasnije ćemo videti i jedan prirodniji.
Posmatrajmo aditivnu grupu $\mathbb{Q}$ i definišimo novo množenje na njoj sa $a * b := 0$ za sve $a, b \in \mathbb{Q}$; nije teško videti da je ovo komutativan prsten bez jedinice. Dokazaćemo da on nema makismalan ideal. Kako je množenje trivijalno, jasno je da je $I \subseteq \mathbb{Q}$ ideal ako i samo ako je aditivna podgrupa od $\mathbb{Q}$; prema tome, problem se svodi na dokaz da $\mathbb{Q}$ nema maksimalnu podgrupu. Pretpostavimo suprotno, neka je $M \leqslant \mathbb{Q}$ maksimalna podgrupa; jasno $M \neq 0$. Izaberimo $\frac{p}{q} \in \mathbb{Q} \setminus M$ i $\frac{m}{n} \in M \setminus \{0\}$; tada i $\frac{1}{q} \in \mathbb{Q} \setminus M$ i $m \in M$. Kako je $M$ maksimalna, $\mathbb{Q} = M + \langle \frac{1}{q} \rangle$, pa je $\frac{1}{mq^2} = u + k\frac{1}{q}$ za neko $u \in M$ i $k \in \mathbb{Z}$. Množenjem sa $mq$ dobijamo $\frac{1}{q} = (mq)u + km$, što pripada $M$ jer $u$, pa i umnožak $(mq)u$, pripada $M$, kao i $m$, pa i umnožak $km$, pripada $M$. Kontradikcija.

Nadovezujći se na prethodni primer možemo da primetimo da svaku Abelovu grupu možemo da da pretvorimo u prsten sa trivijalnim množenjem: $a * b := 0$. Primetimo da ovakav prsten nema prave proste ideale.

## D Količnički prsten

**6/49 Definicija.** Neka je $I \lhd R$. Na $R$ definišemo relaciju jednakosti modulo $I$, $\equiv_I$, sa:

$$x \equiv_I y \ :\iff \ x - y \in I.$$

$x \equiv_I y$ još se obeležava i sa $x \equiv y \mod I$.

Primetimo dva trivijalna slučaja: $\equiv_0$ je samo relacija jednakosti $=$ na $R$, dok je $\equiv_R$ puna relacija $R \times R$.

**6/50 Tvrđenje.**
Neka je $I \lhd R$. Relacija $\equiv_I$ je kongruencija prstena $R$, tj.:

(a) $\equiv_I$ je ekvivalencija prstena $R$, i $[a]_{\equiv_I} = a + I := \{a + x \mid x \in R\}$;

(b) $\equiv_I$ poštuje operacije, tj. ako $a \equiv_I a'$ i $b \equiv_I b'$, onda:

- $a + b \equiv_I a' + b'$, i
- $ab \equiv_I a'b'$.

*Dokaz.* (a) Refleksivnost važi jer $a \equiv_I a \iff a - a \in I \iff 0 \in I$, a desna strana je tačna. Simetričnost: Pretpostavimo $a \equiv_I b$, tj. $a - b \in I$; tada i $b - a = -(a - b) \in I$, pa $b \equiv_I a$. Tranzitivnost: Pretpostavimo $a \equiv_I b$ i $b \equiv_I c$, tj. $a - b, b - c \in I$; tada i $a - c = (a - b) + (b - c) \in I$, pa $a \equiv_I c$.

Izračunajmo klasu $[a]_{\equiv_I}$: $x \in [a]_{\equiv_I} \iff x \equiv_I a \iff x - a \in I \iff (\exists i \in I)\ x = a + i \iff x \in a + I$.

(b) Pretpostavimo $a - a', b - b' \in I$. Tada i $(a + b) - (a' + b') = (a - a') + (b - b') \in I$, pa $a + b \equiv a' + b'$. Takođe, $ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I$, pa $aa' \equiv_I bb'$. □

Naglasimo da smo samo u posledenjoj rečenici dokaza koristili da je $I$ dvostrani ideal; u svim ostalim delovima smo koristili samo da je $I$ Abelova grupa u odnosu na $+$.

**6/51 Definicija.** Neka je $I \lhd R$. Količnički prsten $R$ po $I$, u oznaci $R/I$, je količnički skup $R/I := R/_{\equiv_I} = \{a + I \mid a \in R\}$ sa operacijama $+$ i $\cdot$ definisanim sa:

$$(a + I) + (b + I) := (a + b) + I \quad \text{i} \quad (a + I) \cdot (b + I) := ab + I.$$

**6/52 Komentar.** Prema prethodnom tvrđenju, definisane operacije u dobro definisane (ne zavise od izbora predstavnika klasa $\equiv_I$). Direktno se proverava da je $R/I$ prsten u odnosu na ove operacije. Lako vidimo da je nula u $R/I$ klasa $0 + I = I$. Takođe, aditivni inverz od $a + I$ je $(-a) + I$. Ako je $R$ imao jedinicu, onda je $1 + I$ jedinica prstena $R/I$ (obratno nije tačno: $R/I$ može da ima jedinicu, a da je $R$ nije imao). Ako je $R$ bio komutativan, onda je i $R/I$ komutativan (obratno nije tačni: $R/I$ može da bude komutativan, a da $R$ nije bio).

**6/53 Primer** (Primer komutativnog količnika nekomutativnog prstena)**.**
Najjednostavnije je da uzmemo komutativan prsten $R$ i nekomutativan prsten $S$, i da posmaramo nekomutativan prsten $R \times S$. Tada je $I = 0 \times S$ ideal prstena $R \times S$, i $(R \times S)/I$ je izomorfan sa $R$, pa je $(R \times S)/I$ komutativan. Detalje ostavljamo čitaocu, a mi ćemo da pogledamo konkretan primer.
Neka je $U_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$ prsten svih gornje trougaonih $2 \times 2$ matrica nad $\mathbb{R}$. Nije teško videti da je $U_2(\mathbb{R})$ zaista prsten (sa jedinicom). Ovaj prsten je nekomutativan; npr.:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Posmatrajmo skup $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{R} \right\}$; dokažimo da je $I$ ideal u $U_2(\mathbb{R})$. Jasno je da nula matrica pripada $I$, kao i da je $I$ zatvoren za sabiranje. Dokažimo zatvorenost za spoljno množenje:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ad \\ 0 & 0 \end{pmatrix} \in I \quad \text{i} \quad \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & dc \\ 0 & 0 \end{pmatrix} \in I.$$

Sada možemo da posmatramo $U_2(\mathbb{R})/I$, i dokažimo da je u pitanju komutativan prsten. Neka su $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ i $B = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$. Tada su:

$$AB = \begin{pmatrix} ax & ay + bz \\ 0 & cz \end{pmatrix}, \quad BA = \begin{pmatrix} xa & xb + yc \\ 0 & zc \end{pmatrix}, \quad \text{i} \quad AB - BA = \begin{pmatrix} 0 & (a + c)y + b(x + z) \\ 0 & 0 \end{pmatrix} \in I.$$

Dakle, $AB \equiv BA \mod I$, tj. $(A + I)(B + I) = AB + I = BA + I = (B + I)(A + I)$, što dokazuje komutativnost.

**Zadatak.** Dokazati da je $U_2(\mathbb{R})/I \cong D_2(\mathbb{R})$, gde je $D_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{R} \right\}$ prsten dijagonalnih matrica.

**6/54 Primer** (Primer količnika sa jedinicom prstena bez jedinice)**.**
Najjednostavnije je da posmatramo prsten sa jedinicom $R$ i prsten bez jedinice $S$; tada je $R \times S$ prsten bez jedinice, $I = 0 \times S$ je ideal, i $(R \times S)/I \cong R$ ima jedinicu. Detalje ostavljamo za vežbu, a ovde dajemo konkretan primer.
Posmatrajmo prsten polinoma $\mathbb{Z}_2[X]$ i skup $R = \{p(X) \in \mathbb{Z}_2[X] \mid p(0) = 0\}$; dakle, $R$ je skup svih polinoma nad $\mathbb{Z}_2$ čiji je konstantan član jednak 0. Mošemo da primetimo da je $R$ zapravo ideal $\langle X \rangle$ u $\mathbb{Z}_2[X]$, što specijalno znači da je $R$ zatvoren za sabiranje i množenje, tj. sam po sebi je prsten. Jasno je da $R$ nema jedinicu: naime, ako je $p(X)$ nenula polinom iz $R$, onda je $deg(p) \geqslant 1$, pa je npr. $deg(p \cdot X) = deg(p) + deg(X) \geqslant 1 + 1 = 2$, odakle sledi da $p \cdot X \neq X$; dakle, $p$ ne može biti jedinica.
Neka je $I = \langle X^2 + X \rangle$ ideal generisan u $R$. Očigledno $X^2 \equiv X \mod I$ jer $X^2 - X = X^2 + X \in I$ (u $\mathbb{Z}_2$ plus i minus su jednaki). Takođe, primetimo da je za svako $n \geqslant 3$:

$$\begin{aligned} X^n &= X^n + X^{n-1} + \ldots + X^3 \\ &\quad + X^{n-1} + \ldots + X^3 + X^2 + X^2 \\ &= (X^2 + X)(X^{n-2} + X^{n-3} + \ldots + X) + X^2, \end{aligned}$$

odakle sledi $X^n \equiv X^2 \equiv X \mod I$. Odavde, za svaki $p(X) \in R$ je $p(X) \equiv 0 \mod I$ (ako $p(X)$ ima paran broj sabiraka) ili $p(X) \equiv X \mod I$ (ako $p(X)$ ima neparan broj sabiraka).
Dakle, postoje samo dva elementa u $R/I$: $I$ i $X + I$. Kako je $(X + I)(X + I) = X^2 + I = X + I$, $X + I$ je jedinica prstena $R/I$. (Štaviše, očigledno je $R/I \cong \mathbb{Z}_2$).

U slučaju komutativnog prstena sa jedinicom, prost/maksimalan ideal možemo da okarakterišemo na sledeći način:

**6/55 Tvrđenje.**
Neka je $R$ komutativan prsten sa jedinicom, i $I \lhd R$. Tada:

(a) $I$ je prost ako i samo ako $R/I$ je domen;

(b) $I$ je maksimalan ako i samo ako $R/I$ je polje.

*Dokaz.* (a) Primetimo da $I$ nije prost ako i samo ako postoje $x, y \notin I$ takvi da $xy \in I$, ako i samo ako u $R/I$ postoje elementi $x + I, y + I \neq I$ takvi da $xy + I = I$; kako je $xy + I = (x + I)(y + I)$, poslednje je ekvivalentno sa $R/I$ ima netrivijalne delitelje nule, tj. $R/I$ nije domen.

(b) Ideal $I$ je maksimalan ako i samo ako za svako $x \notin I$, $I + \langle x \rangle = R$, ako i samo ako za svako $x \notin I$, $1 \in I + \langle x \rangle$, ako i samo ako za svako $x \notin I$, postoji $i \in I$ i $r \in R$ tako da $1 = i + rx$, ako i samo ako za svako $x \notin I$, postoji $r \in R$ tako da $rx = 1 \mod I$, ako i samo ako za svako $x + I \neq I$ u $R/I$, postoji $r + I$ tako da $(x + I)(r + I) = 1 + I$, ako i samo ako svako $x + I \neq I$ u $R/I$ ima multiplikativan inverz, ako i samo ako $R/I$ je polje. □

Primetimo da odavde direktno sledi da je makismalan ideal u komutativnom prstenu sa jedinicom uvek i prost. Takođe, primetimo da u dokazu dela (a) smo zapravo dokazali jače tvrđenje $I$ je prost ako i samo ako $R/I$ nema delitelje nule, i za ovu ekvivalenciju nije bilo bitno da li $R$ ima ili nema jedinicu (i dalje je bitno da je komutativan, jer pojam prostog ideala nismo definisale za nekomutativne prstene).

**6/56 Primer.**
U prethodnom tvrđenju (b) bilo je bitno da $R$ ima jedinicu. Npr. videli smo da u prstenu $2\mathbb{Z}$ imamo maksimalan ideal $4\mathbb{Z}$. Lako vidimo da je $2\mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 2 + 4\mathbb{Z}\}$, na kome množimo $(2 + 4\mathbb{Z})(2 + 4\mathbb{Z}) = 4 + 4\mathbb{Z} = 4\mathbb{Z}$, pa $2\mathbb{Z}/4\mathbb{Z}$ nema jedinicu, tj. $2\mathbb{Z}/4\mathbb{Z}$ nije polje (nije ni domen).

## E Teoreme o korespondenciji i izomorfizmu

**6/57 Teorema** (Teorema o korespondenciji)**.**
Neka je $R$ prsten i $I \lhd R$.

(a) Ako je $J \lhd R$ takav da $I \subseteq J$, onda je $J/I := \{j + I \mid j \in J\} \lhd R/I$. Štaviše, ako je $\hat{J} \lhd R/I$, onda je $\hat{J} = J/I$ za neki $J \lhd R$ takav da $I \subseteq J$.

(b) Korespondencija iz (a) verno čuva poredak, tj. za $J, J' \lhd R$ takve da $I \subseteq J, J'$, $J \subseteq J'$ ako i samo ako $J/I \subseteq J'/I$, i $J = J'$ ako i samo ako $J/I = J'/I$.

(c) Ako je $R$ komutativan, u prethodnoj korespondenciji $J$ je prost (maksimalan) u $R$ ako i samo ako je $J/I$ prost (maksimalan) u $R/I$.

*Dokaz.* (a) Prvi deo je direktan. Neka je $J \lhd R$ takav da $I \subseteq J$, i neka je $J/I = \{j + I \mid j \in J\}$. Nula u $R/I$, $I = 0 + I \in J/I$ jer $0 \in J$. Za $x, y \in J$ treba proveriti $(x + I) - (y + I) = (x - y) + I \in J/I$, i za $x \in J, r \in R$ treba proveriti $(x + I)(r + R) = xr + I, (r + I)(x + I) = rx + I \in J/I$. Obe provere su direktne.

Pretpostavimo sada da je $\hat{J} \lhd R/I$. Neka je $J := \{x \in R \mid x + I \in \hat{J}\}$. Očigledno $I \subseteq J$, jer $i + I = I \in \hat{J}$ jer $\hat{J}$ sadrži nulu u $R/I$. Treba proveriti da je $J$ ideal. Jasno, $0 \in J$ jer $I \subseteq J$. Neka $x, y \in J$, tj. $x + I, y + I \in \hat{J}$; tada $(x - y) + I = (x + I) - (y + I) \in \hat{J}$, odakle $x - y \in J$; dakle, $J$ je aditivna podgrupa od $R$. Neka $x \in J$, tj. $x + I \in \hat{J}$, i neka $r \in R$; tada $rx + I = (r + I)(x + I) \in \hat{J}$, i slično $xr + I \in \hat{J}$, pa $rx, xr \in J$, i završili smo dokaz da je $J$ ideal. Sada $x + I \in \hat{J}$ ako i samo ako $x \in J$ po definiciji, ako i samo ako $x + I \in J/I$. U poslednjoj ekvivalenciji, smer ($\Rightarrow$) je direktno po definiciji $J/I$, a za smer ($\Leftarrow$) primetimo ako $x + I \in J/I$, onda je $x + I = j + I$ za neko $j \in J$, pa je $x - j \in I \subseteq J$, odakle, $x \in J$. Dakle, dokazali smo i da je $\hat{J} = J/I$.

(b) Direktan račun, ostavljamo za vežbu.

(c) Prema (a) i (b) je sada očigledno da je $J \lhd R$ takav da $I \subseteq J$ maksimalan ako i samo ako je $J/I$ maksimalan u $R/I$ (bez obzira da li je prsten komutativan).

Da bismo uradili isto za proste ideale, pretpostavimo da je $R$ komutativan. Primetimo $(x + I)(y + I) \in J/I$ ako i samo ako $xy + I \in J/I$, ako i samo ako (slično kao malopre) $xy \in J$. Odavde sada sledi da je $J/I$ prost ako i samo ako je $J$ prost (jer isto $x + I \in J/I$ ako i samo ako $x \in J$, i $y + I \in J/I$ ako i samo ako $y \in J$). □

**6/58 Teorema** (Prva teorema o izomorfizmu)**.**
Neka je $\varphi : R \to S$ homomorfizam prstena. Tada je $ker(\varphi) := \{x \in R \mid \varphi(x) = 0_S\} \lhd R$, $im(\varphi) := \{\varphi(x) \mid x \in R\} \leqslant S$, i $R/ker(\varphi) \cong im(\varphi)$.

*Dokaz.* Dokažimo najpre da je $ker(\varphi) \lhd R$. Kako $\varphi(0_R) = 0_S$, $0_R \in ker(\varphi)$. Pretpostavimo $x, y \in ker(\varphi)$, tj. $\varphi(x) = \varphi(y) = 0_S$; tada je $\varphi(x - y) = \varphi(x) - \varphi(y) = 0_S - O_S = 0_S$, pa $x - y \in ker(\varphi)$. Konačno, ako $x \in ker(\varphi)$ i $r \in R$, tada je $\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r) \cdot 0_S = 0_S$ i slično $\varphi(xr) = 0_S$, tj. $rx, xr \in ker(\varphi)$.

Dalje dokazujemo $im(\varphi) \leqslant S$. Neka $a, b \in im(\varphi)$, i neka je $a = \varphi(x)$ i $b = \varphi(y)$. Tada $0_S = \varphi(0_R) \in im(\varphi)$; $a - b = \varphi(x) - \varphi(y) = \varphi(x - y) \in im(\varphi)$; $ab = \varphi(x)\varphi(y) = \varphi(xy) \in im(\varphi)$. Dodatno, ako $R$ i $S$ imaju jedinicu, onda $1_S = \varphi(1_R) \in im(\varphi)$.

Posmatrajmo preslikavanje $\Phi : R/ker(\varphi) \to im(\varphi)$ dato sa $\Phi(x + ker(\varphi)) = \varphi(x)$. Jasno je da je $\Phi(x + ker(\varphi)) \in im(\varphi)$. Primetimo:

$$x \equiv y \mod ker(\varphi) \iff x - y \in ker(\varphi) \iff \varphi(x - y) = 0_S \iff \varphi(x) - \varphi(y) = 0_S \iff \varphi(x) = \varphi(y).$$

Prethodni niz ekvivalencija pokazuje da je $\Phi$ dobro definisano preslikavanje (smer $\Rightarrow$) koje je 1-1 (smer $\Leftarrow$). Dodatno, $\Phi$ je očigledno na jer $\varphi(x) = \Phi(x + ker(\varphi))$.

Ostaje da proverimo da je $\Phi$ homomorfizam prstena. Najpre, $\Phi((x + ker(\varphi)) + (y + ker(\varphi))) = \Phi((x + y) + ker(\varphi)) = \varphi(x + y) = \varphi(x) + \varphi(y) = \Phi(x + ker(\varphi)) + \Phi(y + ker(\varphi))$. Slično, $\Phi((x + ker(\varphi))(y + ker(\varphi))) = \Phi((xy) + ker(\varphi)) = \varphi(xy) = \varphi(x)\varphi(y) = \Phi(x + ker(\varphi))\Phi(y + ker(\varphi))$. Konačno, ako $R$ i $S$ imaju jedinice, imamo da je $\Phi(1_R + ker(\varphi)) = \varphi(1_R) = 1_S$. □

**6/59 Primer.**
Neka je $R$ prsten i $I \lhd R$. Posmatrajmo prsten polinoma sa koeficijentima u $R$. Označimo sa $I[X]$ podskup svih polinoma čiji koeficijenti pripadaju idealu $I$. Tada je $I[X] \lhd R[X]$ i $R[X]/I[X] \cong (R/I)[X]$.
Posmatrajmo preslikavanje $\varphi : R[X] \to (R/I)[X]$ dato sa $\varphi(\sum_{i=0}^{n} r_i X^i) := \sum_{i=0}^{n} (r_i + I)X^i$. Tvrdimo da je $\varphi$ homomorfizam prstena. Jasno $\varphi(0) = 0 + I = I$. Za zbir imamo:

$$\sum_{i=0}^{n} r_i X^i + \sum_{i=0}^{m} s_i X^i = \sum_{i=0}^{max\{n,m\}} (r_i + s_i)X^i \overset{\varphi}{\mapsto} \sum_{i=0}^{max\{n,m\}} ((r_i + s_i) + I)X^i =$$

$$= \sum_{i=0}^{max\{n,m\}} ((r_i + I) + (s_i + I))X^i = \sum_{i=0}^{n} (r_i + I)X^i + \sum_{i=0}^{m} (s_i + I)X^i,$$

gde smo stavili $r_i = 0$ za $i > n$ i $s_i > 0$ za $i > m$. Za proizvod imamo:

$$\left(\sum_{i=0}^{n} r_i X^i\right)\left(\sum_{i=0}^{m} s_i X^i\right) = \sum_{i=0}^{mn} \left(\sum_{j+k=i} r_j s_k\right) X^i \overset{\varphi}{\mapsto} \sum_{i=0}^{mn} \left(\sum_{j+k=i} r_j s_k + I\right) X^i =$$

$$= \sum_{i=0}^{mn} \left(\sum_{j+k=i} (r_j + I)(s_k + I)\right) X^i = \left(\sum_{i=0}^{n} (r_i + I)X^i\right)\left(\sum_{i=0}^{m} (s_i + I)X^i\right),$$

gde smo ponovo stavili $r_i = 0$ za $i > n$ i $s_i > 0$ za $i > m$. Ako $R$ ima jedinicu, jasno $\varphi(1) = 1 + I$.
Dakle, $\varphi$ jeste homomorifzam prstena. Štaviše, $\varphi$ je očigledno na, tj. $im(\varphi) = (R/I)[X]$. Izračunajmo $ker(\varphi)$:

$$\sum_{i=0}^{n} r_i X^i \in ker(\varphi) \iff \sum_{i=0}^{n} (r_i + I)X^i = I \iff (\forall i = 0, \ldots, n)\ r_i + I = I \iff (\forall i = 0, \ldots, n)\ r_i \in I.$$

Dakle, $ker(\varphi) = I[X]$, pa je prema prvoj teoremi o izomorfizmu, $I[X] \lhd R[X]$, i $R[X]/I[X] \cong im(\varphi) = (R/I)[X]$.

**6/60 Teorema** (Druga teorema o izomorfizmu)**.**
Neka je $R$ prsten, $S \leqslant R$ i $I \lhd R$. Tada je $S + I := \{s + i \mid s \in S,\ i \in I\} \leqslant R$, $S \cap I \lhd S$ i $(S + I)/I \cong S/(S \cap I)$.

*Dokaz.* Najpre dokazujemo $S + I \leqslant R$. Kako $0 \in S, I$, to $0 = 0 + 0 \in S + I$. Neka $x, y \in S + I$, $x = s + i$ i $y = s' + i'$. Tada $x - y = s + i - s' - i' = (s - s') + (i - i') \in S + I$ jer $s - s' \in S$ i $i - i' \in I$. Slično, $xy = (s + i)(s' + i') = ss' + (si' + is' + ii') \in S + I$ jer $ss' \in S$ i $si', is', ii' \in I$, pa i $si' + is' + ii' \in S$. Ako $R$ ima jedinicu, tada $1 \in S$, pa $1 = 1 + 0 \in S + I$.

Dokaz za $S \cap I \lhd S$ je direktan. Jasno $0 \in S \cap I$. Za $x, y \in S \cap I$ treba proveriti $x - y \in S \cap I$. Za $x \in S \cap I$ i $s \in S$ treba proveriti $sx, xs \in S \cap I$. Sve provere su direktne.

Primetimo da je dodatno $I \lhd S + I$; jasno, za svaki $i \in I$ imamo $i = 0 + i \in S + I$, tj. $I \subseteq S + I$, i $I$ jeste ideal u ovom potprstenu jer je ideal u većem prstenu.

Posmatrajmo $\varphi : S \to (S + I)/I$ dato sa $\varphi(s) = s + I$. Direktno se vidi da je $\varphi$ homomorfizam. Primetimo da je $\varphi$ na: zaista, za $s \in S$ i $i \in I$ imamo $(s + i) + I = s + I = \varphi(s)$, gde prva jednakost važi jer očigledno $s + i \equiv s \mod I$. Dakle, $im(\varphi) = (S + I)/I$. Izračunajmo jezgro. Za $s \in S$, $s \in ker(\varphi) \iff s + I = I \iff s \in I$. Dakle, $ker(\varphi) = S \cap I$. Tvrđenje sledi prema prvoj teoremi o izomorfizmu. □

**6/61 Teorema** (Treća teorema o izomorfizmu)**.**
Neka $I, J \lhd R$ i $I \subseteq J$. Tada $J/I := \{j + I \mid j \in J\} \lhd R/I$ i $(R/I)/(J/I) \cong R/J$.

*Dokaz.* Prema teoremi o korespondenciji $J/I \lhd R/I$. Posmatrajmo preslikavanje $\varphi : R/I \to R/J$ dato sa $\varphi(x+I) = x+J$. Primetimo da je ovo preslikavanje dobro definisano jer $x+I = y+I \implies x-y \in I \implies x-y \in J$ jer $I \subseteq J$; poslednje povlači $x+J = y+J$. Dakle, $\varphi$ jeste dobro definisano preslikavanje. Takođe, $\varphi$ je očigledno na: $im(\varphi) = R/J$, i direktno vidimo da je $\varphi$ homomorfizam. Izračunajmo $ker(\varphi)$. Imamo $x+I \in ker(\varphi) \iff x+J = J \iff x \in J \iff x+I \in J/I$. (U poslednjoj ekvivalenciji, implikacija $\Leftarrow$, važi jer: $x+I \in J/I$ povlači $x+I = j+I$ za neko $j \in J$, tj. $x-j \in I \subseteq J$, odakle i $x = (x-j)+j \in J$.) Dakle, $ker(\varphi) = J/I$, i teorema sledi prema prvoj teoremi o izomorfizmu. □

## F Digresija: Primer prstena bez maksimalnog ideala

*Ovaj odeljak je za zainteresovane studente.*

Definišemo:

- $R$ je skup svih konvergentnih realnih nizova: $R = \{(a_n) \mid \lim\limits_{n\to\infty} a_n \text{ postoji (i konačan je)}\}$;
- $R_0$ je skup svih realnih nizova koji teže nuli: $R_0 = \{(a_n) \mid \lim\limits_{n\to\infty} a_n = 0\}$;
- $R_e$ je skup svih realnih nizova koji su eventualno nula: $R_e = \{(a_n) \mid (\exists N)(\forall n > N)\ a_n = 0\}$.

Primetimo da je očigledno $R_e \subseteq R_0 \subseteq R$.

Na $R$ možemo prirodno da definišemo sabiranje i množenje na sledeći način:

$$(a_n) + (b_n) := (a_n + b_n) \quad \text{i} \quad (a_n)(b_n) := (a_n b_n).$$

Primetimo da su ovako definisane operacije zaista operacije na $R$ jer zbir i proizvod dva konvergentna niza jeste konvergentan (i teži zbiru, odnosnu proizvodu limesa polaznih nizova). Nije teško videti da je $R$ komutativan prsten sa nulom $0 = (0)$, aditivnim inverzom $-(a_n) = (-a_n)$ i jedinicom $1 = (1)$.

Primetimo sada da je $R_0 \lhd R$. Jasno je da $0 \in R_0$. Neka $(a_n), (b_n) \in R_0$, tada $\lim\limits_{n\to\infty} a_n - b_n = \lim\limits_{n\to\infty} a_n - \lim\limits_{n\to\infty} b_n = 0 - 0 = 0$, pa i $(a_n) - (b_n) = (a_n - b_n) \in R_0$. Konačno, ako $(a_n) \in R_0$ i $(r_n) \in R$, $\lim\limits_{n\to\infty} r_n = r$, tada $\lim\limits_{n\to\infty} r_n a_n = \lim\limits_{n\to\infty} r_n \ \lim\limits_{n\to\infty} a_n = r \cdot 0 = 0$, pa $(r_n)(a_n) = (r_n a_n) \in R_0$. Može da se vidi i više:

**6/62 Zadatak.** Dokazati da je $R_0 \lhd R$ maksimalan ideal.

Lako možemo da vidimo i da je $R_e \lhd R$.

Ideal $R_0$ nije potprsten od $R$, ali jeste prsten (bez jedinice) sam za sebe, i važi $R_e \lhd R_0$ (jer je $R_e$ zatvoren za množenje iz $R$ pa i iz $R_0$). Nadalje nas ne zanima prsten $R$; posmatramo prsten $R_0$ i njegov ideal $R_e$. Cilj je da dokažemo:

**6/63 Tvrđenje.**
$R_0/R_e$ nema maksimalne ideale.

Prema teoremi o korespondenciji dovoljno je da dokažemo da $R_0$ nema maksimalne ideale koji sadrže $R_e$. Dakle, sledeći korak je da opišemo maksimalne ideale od $R_0$.

Za svako $k \in \mathbb{N}$ uočimo:

- $M_k = \{(a_n) \in R_0 \mid a_k = 0\}$.

Nije teško videti da je $M_k \lhd R_0$. Dokazujemo da $M_k$ jeste maksimalan ideal od $R_0$. Jasno je da $M_k \subsetneq R_0$. Uočimo proizvoljan niz $(r_n) \in R_0 \setminus M_k$; dakle, $r_k \neq 0$. Dokazujemo $R_0 = M_k + \langle (r_k) \rangle$. Uočimo niz $(r'_n)$ za koji je $r'_k = \frac{1}{r_k}$ i $r'_n = 0$ za $n \neq k$; jasno $(r'_n) \in R_0 \setminus M_k$. Dakle, niz $(r'_n)(r_n)$ je nula-niz, osim što je njegov $k$-ti član jednak 1. Neka je sada $(a_n) \in R_0$ proizvoljan niz, i neka je $(a'_n)$ niz dat sa $a'_k = 0$ i $a'_n = a_n$ za $n \neq k$; jasno, $(a'_n) \in M_k$. Očigledno je $(a_n) = (a'_n) + ((a_n)(r'_n))(r_n)$, pa $(a_n) \in M + \langle (r_n) \rangle$. Dakle, $R_0 = M + \langle (r_n) \rangle$, i kako je $(r_n)$ bio proizvoljan, zaključujemo da je $M_k$ maksimalan ideal.

Sledeći korak je da dokažemo da $R_0$ nema više maksimalnih ideala. Primetimo da time završavamo posao jer očigledno $R_e \nsubseteq M_k$ za sve $k$ (očigledno postoje eventualno nula-nizovi $(a_n)$ za koje je $a_0 \neq 0$, npr. stavimo $a_k = 1$ i $a_n = 0$ za $n \neq k$).

Pretpostavimo suprotno, $M \lhd R_0$ je maksimalan ideal takav da $M \neq M_k$ za sve $k$.

Neka je $(e_n^k)$ niz dat sa: $e_k^k = 1$ i $e_n^k = 0$ za $n \neq k$.

**Lema.** Za sve $k$, $(e_n^k) \in M$.

Za dokaz leme, fiksirajmo $k$. Kako $M \neq M_k$, $M$ je maksimalan i $M_k \neq R_0$, imamo $M \nsubseteq M_k$. To znači da imamo niz $(a_n) \in M \setminus M_k$; specijalno, $a_k \neq 0$. Uočimo niz $(b_n)$ dat sa $b_k = \frac{1}{a_k}$ i $b_n = 0$ za $n \neq k$. Jasno, $(b_n) \in R_0$ i $(e_n^k) = (b_n)(a_n) \in M$. Ovim smo dokazali lemu.

**6/64 Komentar.** Da bismo nastavili, moramo malo da skrenemo sa puta. Naime, mi smo opisali kako izgleda glavni ideal $\langle a \rangle$ ako je $R$ (komutativan) prsten sa jedinicom; u slučaju komutativnog prestena sa jedinicom, opis je vrlo jednostavan: $\langle a \rangle = Ra$. Međutim, nama ovde treba opis u slučaju komutativnog prstena bez jedinice. Problem je u sledećem. Po definiciji $\langle a \rangle$ je najmanji ideal koji sadrži $a$ (koji postoji kao presek svih ideala koji sadrže $a$). To specijalno znači da mora biti $Ra = \{ra \mid r \in R\} \subseteq \langle a \rangle$, međutim, ako $R$ nema jedinicu, obratna inkluzija ne mora da važi. Npr. u $R = 2\mathbb{Z}$, $R \cdot 2 = 4\mathbb{Z}$, dok je $\langle 2 \rangle = 2\mathbb{Z}$.
U svakom slučaju, nije teško videti da je opis sledeći:

**6/65 Zadatak.** Neka je $R$ komutativan prsten bez jedinice i $a \in R$. Tada je $\langle a \rangle = Ra + \mathbb{Z}a = \{ra + \lambda a \mid r \in R,\ \lambda \in \mathbb{Z}\}$.

Neka je $(a_n) \in R_0 \setminus M$; zbog maksimalnosti $M$, $R_0 = M + \langle (a_n) \rangle$. Primetimo da $(|a_n|) \in R_0$, kao i da $(\sqrt{|a_n|}) \in R_0$. Tada postoje $(b_n) \in M$, $(r_n) \in R_0$ i $\lambda \in \mathbb{Z}$ takvi da:

$$(\sqrt{|a_n|}) = (b_n) + (r_n)(a_n) + \lambda(a_n). \qquad (*)$$

Dalje primetimo i da $(sgn(a_n)\sqrt{|a_n|}) \in R_0$, pa i $(sgn(a_n)\sqrt{|a_n|}r_n), (sgn(a_n)\sqrt{|a_n|}\lambda) \in R_0$, pa možemo da nađemo $N$ takvo da za $n > N$, $|sgn(a_n)\sqrt{|a_n|}r_n|,\ |sgn(a_n)\sqrt{|a_n|}\lambda| < \frac{1}{4}$, odakle sledi $\frac{1}{2} < 1 - sgn(a_n)\sqrt{|a_n|}r_n - sgn(a_n)\sqrt{|a_n|}\lambda < \frac{3}{2}$. Uočimo niz $(c_n)$ dat sa $c_n = 0$ za $n \leqslant N$ i:

$$c_n = \frac{sgn(a_n)\sqrt{|a_n|}}{1 - sgn(a_n)\sqrt{|a_n|}r_n - sgn(a_n)\sqrt{|a_n|}\lambda}, \quad \text{za } n > N.$$

Po izboru $N$, ovaj niz je definisan, za $n > N$ imenilac je ograničen, pa vidimo da $(c_n) \in R_0$.

Dokažimo da je za $n > N$, $c_n b_n = a_n$. Ako je $a_n = 0$, jasno je po definiciji da je i $c_n = 0$, pa jednakost $c_n b_n = a_n$ važi. Pretpostavimo da $a_n \neq 0$. Tada je:

$$c_n b_n = \frac{1}{\frac{1}{sgn(a_n)\sqrt{|a_n|}} - r_n - \lambda} b_n = \frac{b_n}{\frac{\sqrt{|a_n|}}{a_n} - r_n - \lambda} \overset{(*)}{=} \frac{\sqrt{|a_n|} - r_n a_n - \lambda a_n}{\frac{\sqrt{|a_n|}}{a_n} - r_n - \lambda} = a_n.$$

Dakle, $c_n b_n = a_n$ za $n > N$. Odatle imamo:

$$(a_n) = (a_n) \sum_{k=0}^{N} (e_n^k) + (c_n)(b_n) \in M,$$

jer $\sum_{k=0}^{N} (e_n^k) \in M$ prema lemi. Prema tome, $(a_n) \in M$; kontradikcija.

## G Kineska teorema o ostacima

**6/66 Definicija.** Ideali $I, J \lhd R$ su uzajamno prosti ako $I + J = R$.

**6/67 Zadatak.** Neka je $R$ komutativan prsten sa jedinicom, i neka su $I_1, I_2, \ldots, I_n \lhd R$ po parovima uzajamno prosti. Dokazati $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 I_2 \ldots I_n$.

**6/68 Teorema** (Kineska teorema o ostacima)**.**
Neka $R$ ima jedinicu, i neka su $I_1, \dots, I_n \lhd R$ po parovima uzajamno prosti ideali. Tada je sa:

$$\varphi(x + J) = (x + I_1, x + I_2, \dots, x + I_n)$$

definisan izomorfizam:

$$\varphi : R/J \to R/I_1 \times R/I_2 \times \cdots \times R/I_n,$$

gde je $J = \bigcap_{i=1}^{n} I_n$.

*Dokaz.* Prvo primetimo da je $\varphi$ dobro definisano preslikavanje jer $J \subseteq I_k$ za sve $1 \leqslant k \leqslant n$, pa $x+J = y+J \implies x - y \in J \implies (\forall k = 1, \dots, n)\ x - y \in I_k \implies (\forall k = 1, \dots, n)\ x + I_k = y + I_k$. Direktno se vidi da $\varphi$ jeste homomorfizam prstena.

Dokažimo da je $\varphi$ 1-1, tj. da je $ker(\varphi)$ trivijalno. Imamo $x + J \in ker(\varphi) \iff (\forall k = 1, \dots, n)\ x + I_k = I_k \iff (\forall k = 1, \dots, n)\ x \in I_k \iff x \in \bigcap_{k=1}^{n} I_k \iff x \in J \iff x + J = J$; dakle, $ker(\varphi)$ je trivijalno.

Konačno, treba da dokažemo da je $\varphi$ na. Primetimo da za $k \neq l$ imamo element $a_{k,l} \in R$ takav da $a_{k,l} \equiv 0 \mod I_k$ i $a_{k,l} \equiv 1 \mod I_l$. Zaista, kako su $I_k$ i $I_l$ uzajamno prosti, $I_k + I_l = R$, pa postoje $a \in I_k$ i $b \in I_l$ takvi da $a + b = 1$; jasno je da $a_{k,l} = a$ zadovoljava željene uslove. Za svako $l$, neka je $A_l$ proizvod svih $a_{k,l}$ za $k \neq l$ (u proizvoljnom poretku). Kako je svaki činilac u proizvodu $\equiv 1 \mod I_l$, i $A_l \equiv 1 \mod I_l$. Sa druge strana, za svako $k \neq l$ u proizvodu učestvuje činilac $\equiv 0 \mod I_k$, pa $A_l \equiv 0 \mod I_k$ za sve $k \neq l$.

Neka je $\vec{y} = (x_1 + I_1, x_2 + I_2, \dots, x_n + I_n)$ proizvoljan element kodomena. Posmatrajmo element $x = x_1A_1 + x_2A_2 + \cdots + x_nA_n$. Fiksirajmo $l$. Kako za $k \neq l$, $A_k \equiv 0 \mod I_l$, $x \equiv x_lA_l \mod I_l$, a kako je $A_l \equiv 1 \mod I_l$ dobijamo $x \equiv x_l \mod I_l$. Ovo važi za sve $l$, pa je $\varphi(x) = \vec{y}$; $\varphi$ je na. □

# 7 Domeni

Podsetimo se definicije domena.

**7/1 Definicija.** Domen je komutativan prsten sa jedinicom bez delitelja nule.

Prva stvar koju treba da primetimo je da je u domenima dozvoljeno skraćivanje:

**7/2 Lema.**
Neka je $D$ domen, $a, b, c \in D$, i $a \neq 0$. Tada $ab = ac$ povlači $b = c$.

*Dokaz.* Jednakost $ab = ac$ možemo zapisati sa $a(b - c) = 0$. Kako $D$ nema delitelje nule i $a \neq 0$, mora biti $b - c = 0$, tj. $b = c$. □

**7/3 Zadatak.** Neka je $D$ komutativan prsten sa jedinicom koji zadovoljava zakon skraćivanja. Dokazati da je $D$ domen.

## A Polje razlomaka

Na isti način kao što u matematici gradimo polje racionalnih brojeva kao skup razlomaka celih brojeva, možemo od bilo kog domena $D$ da napravimo njegovo polje razlomaka $F(D)$.

Neka je $D$ domen i neka je $D_0 = D \setminus \{0\}$. Na skupu $D \times D_0$ definišemo relaciju $\approx$ sa:

$$(a, b) \approx (x, y) :\iff ay = bx, \quad \text{gde } a, b, x, y \in D,\ b, y \neq 0.$$

**7/4 Lema.**
$\approx$ je ekvivalencija.

*Dokaz.* Refleksivnost i simetričnost su očigledne. Tranzitivnost: Neka $(a,b) \approx (x,y) \approx (u,v)$, tj. $ay = bx$ i $xv = yu$. Množenjem prve jednakosti sa $v$ dobijamo $ayv = bxv$, pa iz druge dobijamo $ayv = byu$. Skraćivanjem sa $y \neq 0$, dobijamo $av = bu$, odakle $(a,b) \approx (u,v)$. □

Označimo klasu elementa $(a,b)$ sa $\frac{a}{b}$: $\frac{a}{b} := [(a,b)]_{\approx}$; dakle:

$$\frac{a}{b} = \frac{x}{y} \iff (a,b) \approx (x,y) \iff ay = bx.$$

Primetimo dakle da ovako, formalno definisan razlomak $\frac{a}{b}$, $a, b \in D$ i $b \neq 0$, zadovoljava uobičajenu jednakost razlomaka. Označimo sa $F(D)$[7] količnički skup:

$$F(D) := (D \times D_0)/_{\approx} = \left\{ \frac{a}{b} \mid a \in D,\ b \in\ D_0 \right\}.$$

Na skupu $F(D)$ definišemo strukturu prstena sa jedinicom na sledeći način:

$$\frac{a}{b} + \frac{x}{y} := \frac{ay + bx}{by}, \quad -\frac{a}{b} := \frac{-a}{b}, \quad \frac{a}{b} \cdot \frac{x}{y} := \frac{ax}{by}, \quad 0 := \frac{0}{1}, \quad 1 := \frac{1}{1}.$$

**7/5 Lema.**
$F(D)$ je dobro definisan domen.

*Dokaz.* Najpre ćemo dokazati da su operacije dobro definisane. Pretpostavimo $\frac{a}{b} = \frac{a'}{b'}$ i $\frac{x}{y} = \frac{x'}{y'}$, tj. $ab' = ba'$ i $xy' = yx'$. Prvo dokazujemo $\frac{a}{b} + \frac{x}{y} = \frac{a'}{b'} + \frac{x'}{y'}$, tj. $\frac{ay+bx}{by} = \frac{a'y'+b'x'}{b'y'}$, tj. treba da pokažemo $(ay+bx)b'y' = (a'y'+b'x')by$. Prethodna jednakost svodi se na: $ab'yy'+bb'xy' = a'byy'+bb'yx'$, tj. na: $(ab'-a'b)yy'+bb'(xy'-yx') = 0$. Međutim, kako su obe zagrade jednake 0, završili smo posao.

Dalje, pokazujemo $-\frac{a}{b} = -\frac{a'}{b'}$, tj. $\frac{-a}{b} = \frac{-a'}{b'}$, odnosno $(-a)b' = (-a')b$; ovo je očigledno iz $ab' = a'b$.

Konačno, pokazujemo $\frac{a}{b} \cdot \frac{x}{y} = \frac{a'}{b'} \cdot \frac{x'}{y'}$, tj. $\frac{ax}{by} = \frac{a'x'}{b'y'}$, odnosno $axb'y' = a'x'by$. Poslednja jednakost ekvivalentna je sa $axb'y' - a'x'by = 0$, tj. sa $axb'y' - ax'b'y + ax'b'y - a'x'by = 0$, odnosno sa $ab'(xy' - x'y) + (ab' - a'b)x'y = 0$; kako su obe zagrade očiglendo 0, završili smo posao.

Dakle, operacije na $F(D)$ zaista jesu dobro definisane.

Asocijativnost sabiranja:

$$\frac{a}{b} + \left(\frac{x}{y} + \frac{u}{v}\right) = \frac{a}{b} + \frac{xv + yu}{yv} = \frac{a(yv) + b(xv + yu)}{b(yv)} = \frac{(ay + bx)v + (by)u}{(by)v} = \frac{ay + bx}{by} + \frac{u}{v} = \left(\frac{a}{b} + \frac{x}{y}\right) + \frac{u}{v}.$$

Komutativnost sabiranja sledi vrlo slično. 0 jeste neutral za sabiranje jer $0 + \frac{a}{b} = \frac{0}{1} + \frac{a}{b} = \frac{0 \cdot b + 1 \cdot a}{1 \cdot b} = \frac{a}{b}$.

Da bismo videli da je $F(D)$ aditivna abelova grupa, treba još da dokažemo da $-\frac{a}{b}$ jeste inverz od $\frac{a}{b}$. To sledi iz: $-\frac{a}{b} + \frac{a}{b} = \frac{-a}{b} + \frac{a}{b} = \frac{-ab+ab}{b^2} = \frac{0}{b^2}$, a $\frac{0}{b^2} = \frac{0}{1}$ direktno iz definicije jer $0 \cdot 1 = 0 = b^2 \cdot 0$.

Proveru ostalih aksioma ostavljamo za vežbu. Ostaje da se proveri da množenje jeste asocijativno i komutativno, i da je 1 neutral za množenje, kao i da je množenje distributivno prema sabiranju. Svi delovi slede na sličan način kao i gore.

Konačno, treba da dokažemo da $F(D)$ nema netrivijalne delitelje nule. Preptostavimo $\frac{a}{b} \cdot \frac{x}{y} = 0$, tj. $\frac{ax}{by} = \frac{0}{1}$. To znači da je $ax \cdot 1 = by \cdot 0$, tj. $ax = 0$, odakle je $a = 0$ ili $x = 0$. Bez umanjenja opštosti, $a = 0$. Dovoljno je da zaključimo $\frac{a}{b} = 0$, a to sada sledi jer $a \cdot 1 = 0 \cdot 1 = 0 = b \cdot 0$, pa je $\frac{a}{b} = \frac{0}{1}$. □

Već smo u prethodnom dokazu primetili da je $\frac{a}{b} = 0$ ako i samo ako $a = 0$. Za $a \in D_0$, primetimo da je $\frac{a}{a} = 1$ jer je $a \cdot 1 = a \cdot 1$. Sada ako je $\frac{a}{b} \neq 0$, tj. $a \neq 0$, tada je $\frac{b}{a}$ definisan element od $F(D)$, i $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = 1$, što znači da svaki nenula element $\frac{a}{b}$ ima multiplikativni inverz i $(\frac{a}{b})^{-1} = \frac{b}{a}$. Dakle:

**7/6 Lema.**
$F(D)$ je polje.

[7] Oznaka $F(D)$ dolazi od *Fractions in D*.

Polje $F(D)$ se zove polje razlomaka domena $D$.

Formalno, $D \not\subseteq F(D)$. Međutim, $D$ se može identifikovati sa potprstenom od $F(D)$, pa u tom smislu $D \subseteq F(D)$ ima smisla.

**7/7 Lema.**
Sa $\iota : a \mapsto \frac{a}{1}$ definisan je monomorfizam $\iota : D \to F(D)$.

*Dokaz.* Jasno $\iota(0) = \frac{0}{1} = 0$ i $\iota(1) = \frac{1}{1} = 1$. Za sabiranje: $\iota(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \iota(a) + \iota(b)$. Za množenje: $\iota(ab) = \frac{ab}{1} = \frac{a}{1}\frac{b}{1} = \iota(a)\iota(b)$. Dakle, $\iota$ jeste homomorfizam prstena.

Da bismo videli da je $\iota$ 1-1, primetimo $a \in ker(\iota) \iff \frac{a}{1} = 0 \iff a = 0$. Dakle, $\iota$ je 1-1. □

Prema prvoj teoremi o izmorfizmu znamo $D \cong im(\iota) \leqslant F(D)$, pa $D$ možemo posmatrati kao potprsten od $F(D)$, gde smo $a \in D$ identifikovali sa $\frac{a}{1}$.

**7/8 Primer.**(a) Ako je $D = \mathbb{Z}$, onda je $F(D) = \mathbb{Q}$.

(b) Ako je $D$ polje, onda je $F(D) = D$. Zaista, monomorfizam $\iota$ je u ovom slučaju izomorfizam. Da bismo videli da je na, uzmimo $\frac{a}{b} \in F(D)$. Tada, kako je $b$ nenula i $D$ je polje, $b$ je invertibilan, pa možemo da vidimo da je $\frac{a}{b} = \frac{ab^{-1}}{1}$: poslednje sledi jer $a \cdot 1 = ab^{-1} \cdot b$. Prema tome, $\frac{a}{b} = \iota(ab^{-1})$ i $\iota$ zaista jeste na.

(c) Ako je $D = \mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$, onda je $F(D) = \mathbb{Q}[\sqrt{2}] := \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$. Inkluzija ($\supseteq$) je jasna: ako $x + y\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ gde $x = \frac{a}{b}$ i $y = \frac{c}{d}$, imamo $x + y\sqrt{2} = \frac{a}{b} + \frac{c}{d}\sqrt{2} = \frac{ad+bc\sqrt{2}}{bd}$, a broj na desnoj strani očigledno pripada $F(\mathbb{Z}[\sqrt{2}])$. Sa druge stane, za ($\subseteq$), uzmimo razlomak $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$. Posle racionalisanja imamo:

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{-ad + bc}{c^2 - 2d^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

(Primetimo da je $c^2 - 2d^2 \neq 0$ ako $c + d\sqrt{2} \neq 0$, tj. ako $c \neq 0$ ili $d \neq 0$.)

## B Prosti i nerastavljivi elementi

$D$ je sve vreme domen.

**7/9 Definicija.** (a) Element $a \in D$ deli element $b \in D$, oznaka $a \mid b$, ako postoji $c \in D$ tako da $b = ac$.

(b) Elementi $a, b \in D$ su konjugovani, oznaka $a \sim b$, ako $b = ua$ za neki $u \in D^\times$.

(c) Element $d \in D$ je NZD elemenata $a, b \in D$, oznaka $d = nzd(a, b)$, ako $d \mid a, b$, i $e \mid a, b$ povlači $e \mid d$.

(d) Element $a \in D$ je prost ako $a \notin D^\times \cup \{0\}$, i $a \mid bc$ povlači $a \mid b$ ili $a \mid c$.

(e) Element $a \in D$ je nerastavljiv ako $a \notin D^\times \cup \{0\}$, i $a = bc$ povlači $b \in D^\times$ ili $c \in D^\times$.

(f) Element $a \in D$ ima prostu faktorizaciju ako je $a = p_1 p_2 \dots p_n$ za neke proste $p_1, p_2, \dots, p_n \in D$.

(g) Element $a \in D$ ima nerastavljivu faktorizaciju ako je $a = p_1 p_2 \dots p_n$ za neke nerastavljive $p_1, p_2, \dots, p_n \in D$.

(h) Dve faktorizacije (proste ili nerastavljive) $a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$ su konjugovane ako važi $m = n$, i postoji $\sigma \in \mathbb{S}_n$ tako da $p_i \sim q_{\sigma(i)}$ za sve $i = 1, 2, \dots, n$.

(i) Element $a \in D$ ima jednoznačnu faktorizaciju, ako ima nerastavljivu faktorizaciju, i ako su svake dve nerastavljive faktorizacije konjugovane.

Nula i invertibilni elementi očigledno nikada nemaju prostu (nerastavljivu) faktorizaciju, pa kada govorimo o tome da li element $a$ ima prostu (nerastavljivu) faktorizaciju uvek podrazumevamo da govorimo o $a \notin D^\times \cup \{0\}$.

Sledeće tvrđenje nabraja osnovne osobine prethodnih pojmova.

**7/10 Tvrđenje.**(a) Relacija $\mid$ je refleksivna i tranzitivna. Takođe, $a \mid b$ ako i samo ako $b \in \langle a \rangle$.

(b) Relacija $\sim$ je ekvivalencija.

(c) $a \sim b$ ako i samo ako $a \mid b$ i $b \mid a$.

(d) $a \notin D^\times \cup \{0\}$ je prost ako i samo ako je $\langle a \rangle$ prost ideal.

(e) Prost element je uvek nerastavljiv. Dakle, prosta fakotirzacija je uvek i nerastavljiva.

(f) Ako $a \notin D^\times$, $a \mid b$ i $b$ je nerastavljiv, onda $a \sim b$.

(g) Ako $a$ ima prostu faktorizaciju, onda ima i jednoznačnu faktorizaciju.

(h) Ako $d \mid p_1 p_2 \dots p_n$ i $p_1, \dots, p_n$ su prosti, onda $d \in D^\times$ ili $d$ je konjugovan sa proizvodom nekih $p$-ova.

(i) Ako dva elementa imaju prostu faktorizaciju, onda imaju i NZD.

*Dokaz.* (a), (b) i (c) su laki, i ostavljamo za vežbu.

(d) Neka je $a \notin D^\times \cup \{0\}$. Kako $a \mid x \iff x \in \langle a \rangle$, definicije prostog elementa i prostog ideala se prevode jedna na drugu.

(e) Neka je $a \notin D^\times \cup \{0\}$ prost element, i neka $a = bc$. Tada očigledno $a \mid bc$, pa kako je $a$ prost, $a \mid b$ ili $a \mid c$. Bez umanjenja opštosti, neka $a \mid b$, i neka je $b = ad$. Tada je $a = bc = adc$, pa skraćivanjem sa $a$ dobijamo $dc = 1$, odakle $c \in D^\times$. Dakle, $a$ je nerastavljiv.

(f) Neka $a \notin D^\times$, $a \mid b$ i $b$ je nerastavljiv. Zapišimo $b = ac$. Kako je $b$ nerastavljiv i $a \notin D^\times$, to $c \in D^\times$; dakle, $a \sim b$.

(g) Neka je $a = p_1 p_2 \dots p_n$ prosta faktorizacije (onda je ona i nerastavljiva), i neka je $a = q_1 q_2 \dots q_m$ nerastavljiva faktorizacije elementa $a$. Dovoljno je da dokažemo da su one konjugovane. Kako $p_1 \mid q_1 q_2 \dots q_m$ i $p_1$ je prost, $p_1$ deli neki od činilaca, i bez umanjenja opštosti $p_1 \mid q_1$. Kako je $q_1$ nerastavljiv, $p_1 \sim q_1$ prema (f). Zapišimo $q_1 = u p_1$ gde $u \in D^\times$. Podelimo $p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$ sa $p_1$; dobijamo $p_2 \dots p_n = u q_2 \dots q_m$. Kako prosti elementi ne dele invertibilne (jer su sami neinvertibilni), postupak možemo da nastavimo sa $p_2$, itd. Može da se desi da je $m = n$, i kroz postupak vidimo da su $p$-ovi i $q$-ovi po parovima konjugovani, čimo smo završili dokaz jednoznačnosti. Ako je $n < m$, onda ćemo posle $n$-tog koraka imati $1 = v q_{i_1} \dots q_{i_{m-n}}$ za neko $v \in D^\times$, što povlači da su $q_{i_1}, \dots, q_{i_{n-m}}$ invertibilni; kontradikcija. Ako je $m < n$, posle $m$-tog koraka ćemo imati $p_{m+1} \dots p_n = v$ za neko $D^\times$, što povlači da su $p_{m+1}, \dots, p_n$ invertibilni; opet kontradikcija. Dakle, završili smo dokaz.

(h) Dokaz ćemo izvesti indukcijom po $n$. Za bazu, pretpostavimo da $d \mid p$ i $p$ je prost; kako je $p$ nerastavljiv prema (e), $d \in D^\times$ ili $d \sim p$ prema (f). Ovo završava dokaz baze.

Pretpostavimo da tvrđenje važi za proizvod $n$ prostih, i pretpostavimo $d \mid p_1 \dots p_n p_{n+1}$. Zapišimo $p_1 \dots p_n p_{n+1} = dx$. Kako $p_{n+1} \mid dx$ i kako je $p_{n+1}$ prost, $p_{n+1} \mid d$ ili $p_{n+1} \mid x$.

Prvi slučaj. Ako $p_{n+1} \mid d$, zapišimo $d = p_{n+1} d'$ i podelimo polaznu jednakost sa $p_{n+1}$; dobijamo $p_1 \dots p_n = p_{n+1} d' x$, odakle $d' \mid p_1 \dots p_n$, pa je prema IH $d' \in D^\times$ ili je $d'$ konjugovan sa proizvodom nekih od $p_1, \dots, p_n$. U prvom slučaju je $d = p_{n+1} d' \sim p_{n+1}$, a u drugom vidimo da je $d$ proizvod nekih od $p_1, \dots, p_n$ i $p_{n+1}$.

Drugi slučaj. Ako $p_{n+1} \mid x$, zapišimo $x = p_{n+1} x'$ i podelimo polaznu jednakost sa $p_{n+1}$; dobijamo $p_1 \dots p_n = d p_{n+1} x'$, odakle $d \mid p_1 \dots p_n$, pa prema IH direktno završavamo.

(i) Neka su $a = p_1 p_2 \dots p_n$ i $b = q_1 q_2 \dots q_m$ proste faktorizacije elemenata $a$ i $b$. Izaberimo maksimalan skup konjugovanih parova $p$-ova i $q$-ova; bez umanjenja opštosti neka su $p_1 \sim q_1, p_2 \sim q_2, \dots, p_k \sim q_k$, i $p_{k+1}, \dots, p_n$ i $q_{k+1}, \dots, q_m$ su po parovima nekonjugovani. Tvrdimo da je $d := p_1 p_2 \dots p_k$ NZD od $a$ i $b$ (ako ne postoji konjugovani par $p$-ova i $q$-ova, $d = 1$). Jasno je da $d \mid a$ i $d \mid b$ ($d \mid b$ jer je $d$ konjugovan sa $q_1 q_2 \dots q_k$). Pretpostavimo $e \mid a$ i $e \mid b$; dokazujemo $e \mid d$. Možemo da pretpostavimo $e \notin D^\times$; u suprotnom $e \mid d$ trivijalno. Prema (h), kako $e \mid a$ i $e \mid b$, $e$ je konjugovan proizvodu nekih od $p$-ova i proizvodu nekih od $q$-ova. To specijalno znači da $e$ ima prostu faktorizaciju, pa prema (g) ima i jednoznačnu faktorizaciju. Odatle, njegove dve nađene faktorizacije (jedna preko $p$-ova i druga preko $q$-ova) su konjugovane. Odatle, prema izboru $d$, sada lako možemo da vidimo da $e \mid d$.

TREBA NAĆI BOLjI NAČIN DA SE ZAPIŠE POSLEDNjE □

**7/11 Primer.**
Posmatrajmo domen $\mathbb{Z}[i\sqrt{3}] := \{a+bi\sqrt{3} \mid a,b \in \mathbb{Z}\}$. Nije teško videti da je $\mathbb{Z}[i\sqrt{3}]$ potprsten od $\mathbb{C}$ (zatvoren za sabiranje i množenje), pa samim tim jeste i domen.
U ovom i sličnim primerima primetimo sledeće. Za $z, w \in \mathbb{Z}[i\sqrt{3}]$ i $z \neq 0$, $z \mid w$ u $\mathbb{Z}[i\sqrt{3}]$ ako i samo ako količnik $\frac{w}{z}$ izračunat u $\mathbb{C}$ pripada $\mathbb{Z}[i\sqrt{3}]$: $\frac{w}{z} \in \mathbb{Z}[i\sqrt{3}]$. Zaista, množenje je nasleđeno iz $\mathbb{C}$, pa ako $z \mid w$ u $\mathbb{Z}[i\sqrt{3}]$, i $w = zx$ za neko $x \in \mathbb{Z}[i\sqrt{3}]$, onda je i $w = zx$ u $\mathbb{C}$, pa je $x = \frac{w}{z}$ u $\mathbb{C}$. Obratno je, takođe, očigledno.
Druga korisna stvar u analizi ovakvih primera je kvadrat modula: $|z|^2 = a^2 + 3b^2 \in \mathbb{N}$, za $z = a + bi\sqrt{3} \in \mathbb{Z}[i\sqrt{3}]$.
Npr. možemo da primetimo da je $\mathbb{Z}[i\sqrt{3}]^\times = \{-1, 1\}$. Zaista, $-1$ i $1$ očigledno jesu invertibilni. Sa druge strane, ako je $z$ invertibilan, i ako $zw = 1$ u $\mathbb{Z}[i\sqrt{3}]$, uzimajući kvarat modula imamo $|z|^2|w|^2 = |zw|^2 = 1$, pa je $|z|^2 = 1$. Kako $1 = |z|^2 = a^2 + 3b^2 \in \mathbb{N}$, sada je lako da vidimo da je $z = 1$ ili $z = -1$. Zapravo, primetimo da odavde možemo da zaključimo da je $z \in \mathbb{Z}[i\sqrt{3}]$ invertibilan ako i samo ako $|z|^2 = 1$.

(a) Element 2 nije prost, ali jeste nerastavljiv. Jasno $2 \notin \mathbb{Z}[i\sqrt{3}]^\times \cup \{0\}$. Primetimo da $2 \mid 2 \cdot 2 = 4 = (1 - i\sqrt{3})(1 + i\sqrt{3})$, ali $2 \nmid 1 - i\sqrt{3}$ i $2 \nmid 1 + \sqrt{3}$. Dakle, 2 nije prost.

Da bismo videli da 2 jeste nerastavljiv, pretpostavimo $2 = zw$. Uzimajući kvadrat modula imamo $4 = |z|^2|w|^2$. Imamo tri sučaja: $|z|^2 = 1$ i $|w|^2 = 4$ (u ovom služaju $z$ je invertibilan i završili smo), $|z|^2 = 4$ i $|w|^2 = 1$ (u ovom slučaju $w$ je invertibilan i završili smo), ili $|z|^2 = |w|^2 = 2$. Poslednji slučaj nije moguć jer za $z = a + bi\sqrt{3}$, $|z|^2 = a^2 + 3b^2$ očigledno ne može da bude 2. Dakle, 2 je nerastavljiv.

> **7/12 Komentar.** Dakle, u opštem slučaju, nerastavljiv element ne mora biti prost.

(b) Na sličan način kao za 2, možemo da vidimo da su $1 - i\sqrt{3}$ i $1 + i\sqrt{3}$ nerastavljivi elementi. Dakle imamo dve nerastavljive faktorizacije broja 4: $2 \cdot 2 = 4 = (1 - i\sqrt{3})(1 + i\sqrt{3})$, koje nisu konjugovane jer $2 \neq \pm(1 - i\sqrt{3})$ i $2 \neq \pm(1 + i\sqrt{3})$.

> **7/13 Komentar.** Dakle, u opštem slučaju, nerastavljive faktorizacije ne moraju biti konjugovane, tj. element ne mora da ima jednoznačnu faktorizaciju. Odatle sledi i da prosta faktorizacija ne mora da postoji.

(c) Brojevi $z = 4$ i $w = 2(1 - i\sqrt{3})$ nemaju NZD. Kako smo videli $z = 2 \cdot 2 = (1 - i\sqrt{3})(1 + i\sqrt{3})$, pa vidimo da su 2 i $1 - i\sqrt{3}$ zajednični delioci od $z$ i $w$. Nije teško da vidimo da su 2 i $1 - i\sqrt{3}$ maksimalni zajednički delioci, u smislu da ne postoji $d$ tako da $2 \mid d \mid z, w$, kao i da ne postoji $d$ tako da $1 - i\sqrt{3} \mid d \mid z, w$. Međutim, kako $2 \not\sim 1 - i\sqrt{3}$, ovo znači da $nzd(z, w)$ ne postoji.

> **7/14 Komentar.** Dakle, u opštem slučaju, dva elementa ne moraju da imaju NZD.

**7/15 Primer.**
Kompleksan broj $z \in \mathbb{C}$ je algebarski ceo broj ako postoji moničan (vodeći koeficijent je 1) polinom $p(X) \in \mathbb{Z}[X]$ takav da $p(z) = 0$; dakle, postoje celi brojevi $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{Z}$ takvi da:

$$\alpha_0 + \alpha_1 z + \cdots + \alpha_{n-1} z^{n-1} + z^n = 0.$$

Npr. $z \in \mathbb{Z}$ jeste algebarski ceo broj jer zadobvoljava moničan linearan polinom $X - z$ nad $\mathbb{Z}$. Sa druge strane, npr. $z \in \mathbb{Q} \setminus \mathbb{Z}$ nije algebraski ceo broj: ako zapišemo $z = \frac{p}{q}$ gde su $p$ i $q$ uzajamno pstoji, i ako:

$$\alpha_0 + \alpha_1 \frac{p}{q} + \cdots + \alpha_{n-1} \frac{p^{n-1}}{q^{-1}} + \frac{p^n}{q^n} = 0,$$

množenjem sa $q^n$ dobijamo:

$$\alpha_0 q^n + \alpha_1 p q^{n-1} + \cdots + \alpha_{n-1} p^{n-1} q + p^n = 0.$$

Kako $q$ deli prvih $n$ sabiraka, mora da deli i poslednji: $q \mid p^n$; kako su $p$ i $q$ uzajamno prosti, to je moguće jedino ako $q = \pm 1$, pa je $z = \frac{p}{q} = \pm p \in \mathbb{Z}$; kontradikcija.

Označimo sa $D \subseteq \mathbb{C}$ skup svih algebraskih celih brojeva. Tvrdimo da je $D$ potprsten od $\mathbb{C}$. Već smo videli $0, 1 \in D$, pa treba samo da dokažemo da je $D$ zatvoren za aditivni inverz, sabiranje i množenje. Što se tiče aditivnog inverza, stvar je laka: pretpostavimo da za $z \in D$ imamo:

$$\alpha_0 + \alpha_1 z + \alpha_2 z^2 + \alpha_3 z^3 + \cdots + \alpha_{n-1} z^{n-1} + z^n = 0,$$

gde su $\alpha$-e celi brojevi. Tada je:

$$\alpha_0 - \alpha_1(-z) + \alpha_2(-z)^2 - \alpha_3(-z)^3 + \cdots + (-1)^{n-1}\alpha_{n-1}(-z)^{n-1} + (-1)^n(-z)^n = 0,$$

pa množenjem sa $-1$ ako je potrebno (tj. ako je $n$ neparno), dobijamo relaciju koja pokazuje da $-z \in D$.

Dokažimo zatvorenost za sabiranje i množenje. Neka $z, w \in D$. Iz definicije algebarskog celog broja vidimo da možemo da zapišemo $z^n = -\sum_0^{n-1} \alpha_i z^i$ i $w^m = -\sum_{j=0}^{m-1} \beta_j w^j$, gde su $\alpha$-e i $\beta$-e celi. Posmatrajmo vektor-kolonu $\vec{v}$ dužine $mn$ čiji su unosi brojevi $z^k w^l$, $0 \leqslant k < n$ i $0 \leqslant l < m$, u nekom poretku. Primetimo da je $(z+w)z^k w^l$ linearna kombinacija nad $\mathbb{Z}$ unosa vektora $\vec{v}$. Zaista, $(z+w)z^k w^l = z^{k+1}w^l + z^k w^{l+1}$, pa ako $k+1 < n$ i $l+1 < m$, ovo je već željena linearna kombinacija. Ako je $k+1 = n$ i $l+1 < m$, onda je $(z+w)z^k w^l = z^n w^l + z^k w^{l+1} = (-\sum_{i=0}^{n-1} \alpha_i z^i) w^l + z^k w^{l+1}$, odakle dobijamo željenu linearnu kombinaciju. Na sličan način postupamo i u ostalim slučajevima. Šta to znači? Svaki unos vektora $(z+w)\vec{v}$ je celobrojna linearna kombinacija unosa vektora $\vec{v}$, tj. postoji celobrojna matrica $A$ takva da $(z+w)\vec{v} = A\vec{v}$. Linearna algebra nam kaže da je $z+w$ sopstvena vrednost matrice $A$ (i da je $\vec{v}$ odgovarajući sopstveni vektor). Linearna algebra nam još kaže da je $z+w$ onda nula karakterističnog polinoma matrice $A$. Kako je karakteristični polinom celobrojne matrice polinom sa celobrojnim koeficijentima, i kako je on do na znak moničan, zaključujemo $z+w \in D$. Na sličan način, $zw \in D$.

Da ne ostane misteriozno, pogledajmo konkretan primer prethodnog objašnjenja. Broj $z = \sqrt{5}$ je algebarski ceo jer $-5 + z^2 = 0$, tj. $z^2 = 5$. Takođe, broj $w = \frac{-1+i\sqrt{3}}{2}$ je algebraski ceo jer $1 + w + w^2 = 0$, tj. $w^2 = -1-w$. Posmatrajmo vektor $\vec{v} = \begin{pmatrix} 1 & z & w & zw \end{pmatrix}^T$. Konstruišemo matricu $A$ takvu da $A\vec{v} = (z+w)\vec{v}$. Imamo: $(z+w)\cdot 1 = z+w$, $(z+w)z = z^2 + zw = 5 + zw$, $(z+w)w = zw + w^2 = zw - 1 - w$ i $(z+w)zw = z^2 w + zw^2 = 5w - z - zw$; kad stavimo u matricu, dobijamo:

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 5 & 0 & 0 & 1 \\ -1 & 0 & -1 & 1 \\ 0 & -1 & 5 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ z \\ w \\ zw \end{pmatrix} = (z+w) \begin{pmatrix} 1 \\ z \\ w \\ zw \end{pmatrix}$$

Iz ove jednakosti sledi da je $z+w = \sqrt{5} + \frac{-1+i\sqrt{3}}{2}$ nula karakterističnog polinoma matrice na levoj strani, koji je moničan i nad $\mathbb{Z}$, pa je $z+w$ algebarski ceo broj. Slično, nameštanjem matrice $B$ tako da $B\vec{v} = (zw)\vec{v}$, dokazujemo $zw$ je algebarski ceo broj.

Sada znamo da je $D$ potprsten od $\mathbb{C}$, pa je on i domen. Već smo videli da $D$ nije zatvoren za inverze (npr. $2 \in D$, ali $\frac{1}{2} \notin D$), pa $D^\times \cup \{0\} \subsetneq D$.

Primetimo da je $D$ zatvoren za koren. Naime, ako:

$$\alpha_0 + \alpha_1 z + \cdots + \alpha_{n-1} z^{n-1} + z^n = 0,$$

onde je:

$$\alpha_0 + \alpha_1(\sqrt{z})^2 + \cdots + \alpha_{n-1}(\sqrt{z})^{2(n-1)} + (\sqrt{z})^{2n} = 0,$$

odakle $\sqrt{z} \in D$. (Ovde bi trebalo da smo precizniji, tj. trebalo bi da kažemo šta mislimo pod korenom kompleksnog broja. Ako zapišemo u trigonometrijskom obliku $z = r(\cos\theta + i\sin\theta)$, pod korenom mislimo $\sqrt{z} := \sqrt{r}(\cos\frac{\theta}{2} + i\sin\frac{\theta}{2})$; iz De Moavrove formule znamo $(\sqrt{z})^2 = z$.)
Odavde sledi da $z \in D \setminus (D^\times \cup \{0\})$ nije nerastavljiv (pa ni prost) jer možemo da zapišemo $z = \sqrt{z} \cdot \sqrt{z}$ u domenu $D$, a $\sqrt{z} \notin D^\times$ (jer $z \notin D^\times$).

**7/16 Komentar.** Dakle, u opštem slučaju, domen ne mora da ima nerastavljive elemente. Specijalno, nerastavljive faktorizacije ne moraju da postoje.

**7/17 Definicija** (Broj prostih faktora)**.** Neka je $a \in D$. Za $a$ definišemo njegov broj prostih faktora, $\#a \in \mathbb{N} \cup \{\infty\}$, na sledeći način:

- $\#0 := \infty$;
- ako $a \in D^\times$, $\#a := 0$;
- ako $a \notin D^\times \cup \{0\}$ ima prostu faktorizaciju $a = p_1 \dots p_n$, $\#a := n$;
- ako $a \notin D^\times \cup \{0\}$ nema prostu faktorizaciju, $\#a := \infty$.

**7/18 Komentar.** Primetimo nekoliko činjenica:

(a) Očigledno, $\#a = 0$ ako i samo ako $a \in D^\times$.

(b) Ako svi elementi van $D^\times \cup \{0\}$ imaju prostu faktorizaciju, onda $\#a = \infty$ ako i samo ako $a = 0$.

(c) Ako $a \notin D^\times \cup \{0\}$ ima prostu faktorizaciju, onda je broj $\#a$ dobro definisan, tj. ne zavisi od izbora faktorizacije. Zaista, prema tvrđenju 7/10(g) ako $a$ ima prostu faktorizaciju, onda ima jednoznačnu faktorizaciju; specijalno, svake dve proste faktorizacije su međusobno konjugovane, pa imaju jednak broj prostih faktora.

(d) Ako $a \sim b$ (tj. ako $\langle a\rangle = \langle b\rangle$), onda $\#a = \#b$. Ovo sledi direktno razmatrajući sve slučajeve. Ako $a = 0$, onda i $b = 0$, pa $\#a = \#b = \infty$. Ako $a \in D^\times$, onda i $b \in D^\times$, pa $\#a = \#b = 0$. Ako $a \notin D^\times \cup \{0\}$ ima prostu faktorizaciju $a = p_1p_2 \dots p_n$, i $b = ua$ za $u \in D^\times$, tada je $b = (up_1)p_2 \dots p_n$ prosta faktorizacijaod $b$, pa $\#a = \#b = n$. Ako $a \notin D^\times \cup \{0\}$ nema prostu faktorizaciju, onda, prema prethodna tri slučaja, ni $b$ nema prostu faktorizaciju; opet, $\#a = \#b = \infty$.

(e) Ako $b \mid a$ (tj. ako $\langle a\rangle \subseteq \langle b\rangle$), onda $\#b \leqslant \#a$. Ponovo diskutujemo sve slučajeve. Ako $a = 0$ ili $a \notin D^\times \cup \{0\}$ nema prostu faktorizaciju, onda $\#a = \infty$, pa trivijalno $\#b \leqslant \#a$. Ako $a \in D^\times$, onda $b \mid a$ povlači da i $b \in D^\times$, pa $\#b = 0 \leqslant 0 = \#a$. Konačno, ako $a \notin D^\times \cup \{0\}$ ima prostu faktorizaciju $a = p_1 \dots p_n$, kako $b \mid a$, prema tvrđenju 7/10(h), $b \in D^\times$ ili $b$ je konjugovan sa proizvodom nekih $p$-ova; u oba slučaja je $\#b \leqslant \#a$.

(f) Prema prethodne dve tačke, $\langle a\rangle \subsetneq \langle b\rangle$ povlači $\#b < \#a$.

**7/19 Primer.**
Primetimo da potencijalna analogna funkcija broja nerastavljivih faktora u opštem slučaju nije dobro definisana. Slično kao u primeru domena $\mathbb{Z}[i\sqrt{3}]$, možemo da posmatramo domen $\mathbb{Z}[i\sqrt{29}] = \{a + bi\sqrt{29} \mid a, b \in \mathbb{Z}\}$. U njemu je:

$$30 = 2 \cdot 3 \cdot 5 = (1 - i\sqrt{29})(1 + i\sqrt{29}),$$

gde su svi elementi 2, 3, 5, $1 - i\sqrt{29}$ i $1 + i\sqrt{29}$ nerastavljivi. Dakle, 30 ne samo da nema jednoznačnu faktorizaciju, nego ima i nerastavljive faktorizacije različitih dužina. Proveru detalja ostavljamo za vežbu.

**7/20 Definicija.** Kažemo da domen $D$ zadovoljava uslov rastućeg lanca na glavnim idealima ili ACCP[8] ako ne postoji beskonačan strogo rasući lanac glavnih idela, tj. ne postoje elementi $a_0, a_1, a_2, \ldots$ takvi da $\langle a_0\rangle \subsetneq \langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \ldots$.

**7/21 Primer.**
Skoro svi primeri koji nas zanimalju će zadovoljavati ACCP. Međutim, primetimo da u opštem slučaju $D$ ne mora da zadovoljava ACCP. Ako se vratimo na domen $D$ svih algebarskih celih brojeva, možemo da primetimo da imamo:

$$\langle 2\rangle \subsetneq \langle \sqrt{2}\rangle \subsetneq \langle \sqrt[4]{2}\rangle \subsetneq \langle \sqrt[8]{2}\rangle \subsetneq \ldots$$

pa $D$ ne zadovoljava ACCP.

## C Nerastavljivi polinomi

Posebno zanačajan pojam kasnije biće nam pojam nerastavljivog polinoma. On se ne poklapa u potpunosti sa pojmom nerastavljivog elementa koji smo uveli, pa ćemo mu posvetiti posebnu pažnju.

**7/22 Definicija** (Slabo nerastavljiv polinom)**.** Neka je $D[X]$ domen polinoma nad domenom $D$, i neka je $p(X) \in D[X]$ nekonstantan polinom. Polinom $p(X)$ je slabo nerastavljiv ako nije proizvod dva nekonstantna polinoma, tj. ako nije $p(X) = f(X)g(X)$, gde $f(X), g(X) \in D[X]$ i $deg(f), deg(g) \geqslant 1$.

Jasno je da ako je nekonstantan polinom $p(X) \in D[X]$ nerastavljiv element u $D[X]$, onda nije proizvod dva neinvertibilna elementa, pa specijalno nije ni proizvod dva nekonstanta polinoma, tj. $p(X)$ jeste i slabo nerastavljiv. Obratno međutim nije tačno.

**7/23 Primer.**
U prstenu $\mathbb{Z}[X]$, polinom $2X$ se ne može zapisati kao proizvod dva nekonstanta polinoma (jer bi u suprotnom bio bar stepena dva), pa, dakle, jeste slabo nerastavljiv, ali nije nerastavljiv element u $\mathbb{Z}[X]$ jer $2X$ je očigledno proizvod dva neinvertibilna elementa 2 i $X$.

Ipak, treba imati u vidu sledeće:

**7/24 Komentar.** Ako je $F$ polje, onda je nekonstantan polinom $p(X) \in F[X]$ nerastavljiv ako i samo ako je slabo nerastavljiv. Zaista, ako je $p(X)$ slabo nerastavljiv i $p(X) = f(X)g(X)$, onda je npr. $f(X)$ konstantan (i nenula), pa je invertibilan jer su svi nenula elementi u polju invertibilni.

Završićemo ovaj odeljak sa teoremom koju ćemo često kasnije koristiti.

**7/25 Teorema** (Ajzenštajnov kriterijum)**.**
Neka je $D$ domen i neka je $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in D[X]$. Ako postoji prost element $p \in D$ takav da $p \mid a_0, a_1, \ldots, a_{n-1}$, $p \nmid a_n$ i $p^2 \nmid a_0$, onda je $f(X)$ slabo nerastavljiv.

*Dokaz.* Pretpostavimo suprotno, $f(X) = g(X)h(X)$, $g(X) = b_mX^m + \cdots + b_1X + b_0$, $h(X) = c_kX^k + \cdots + c_1X + c_0$, gde $1 \leqslant k, m < n$ i $k + m = n$. Kako $p \mid a_0 = b_0c_0$ i $p$ je prost, bez umanjenja opštosti možemo da pretpostavimo $p \mid b_0$. Sa druge strane, kako $p \nmid a_n = b_mc_k$, sigurno $p \nmid b_m$. Dakle, postoji najmanje $i \leqslant m$ takvo da $p \mid b_0, b_1, \ldots, b_i$ i $p \nmid b_i$; primetimo $i < n$. Posmatrajmo, $a_i$:

$$a_i = b_0c_i + b_1c_{i-1} + \cdots + b_{i-1}c_1 + b_ic_0.$$

(Ovde ako $i > k$, stavimo $c_i = 0$.) Kako $p \mid b_0, \ldots, b_{i-1}$, deli i zbir $b_0c_i + b_1c_{i-1} + \cdots + b_{i-1}c_1$, pa kako $p \mid a_i$ jer $i < n$, zaključujemo da mora $p \mid b_ic_0$. Po izboru $i$, $p \nmid b_i$, pa kako je prost zaključujemo $p \mid c_0$. Sada iz $p \mid b_0$ i $p \mid c_0$ sledi $p^2 \mid b_0c_0 = a_0$. Kontradikcija. □

[8] Skraćenica ACCP dolazi od *Ascending Chain Condition on Principal ideals*

Ajzenštajnov kriterijum važi i u opštijem obliku:

**7/26 Zadatak.** Neka je $D$ domen i neka je $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in D[X]$. Ako postoji prost ideal $P \lhd D$ takav da $a_0, a_1, \ldots, a_{n-1} \in P$, $a_n \notin P$ i $a_0 \notin P^2$[a], onda je $f(X)$ slabo nerastavljiv.

[a]Ovde $P^2$ je ideal $P^2 = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid n \geqslant 1,\ a_1, b_1, a_2, b_2, \ldots, a_n, b_n \in P\}$.

Ako je $P$ u zadatku glavni ideal, onda je Ajzenštajnov kriterijum u obliku koji je iskazan u gornjoj teoremi.

## D Euklidski domeni (ED)

**7/27 Definicija.** Neka je $D$ domen.

(a) Euklidska norma na $D$ je funkcija $N : D \setminus \{0\} \to \mathbb{N}$ koja zadovljava sledeći uslov:

- za sve $a, b \in D$, $b \neq 0$, postoje $q, r \in D$ takvi da $a = bq + r$, i $r = 0$ ili $N(r) < N(b)$.

(b) Domen $D$ je Euklidski domen (ED) ako postoji euklidska norma na $D$.

**7/28 Primer.**(a) Svako polje $F$ je ED. Norma na $F$ je data npr. sa $N(x) = 1$ za sve $x \neq 0$. Zaista, za $a, b \in F$, $b \neq 0$ imamo $a = (\underbrace{ab^{-1}}_{=q})b + \underbrace{0}_{=r}$.

(b) $\mathbb{Z}$ je ED. Norma na $\mathbb{Z}$ je data sa $N(x) = |x|$.

**7/29 Primer** (Prsten polinoma nad poljem)**.**
Neka je $F$ polje, $F[X]$ je ED. Norma je data sa $N(a) = deg(a)$ za $a(X) \neq 0$.[a]
Dokazujemo da $N$ zaista jeste norma. Pretpostavimo suprotno, $N$ nije norma. To znači da je skup:

$$S = \{(a, b) \mid a, b \in F[X], b \neq 0,\ \text{ne postoje } q, r \in F[X] \text{ takvi da } a = bq + r, \text{ i } r = 0 \text{ ili } deg(r) < deg(b)\}$$

neprazan. Primetimo da ako $(a, b) \in S$ onda, očigledno $b \neq 0$, ali i $a \neq 0$; zaista, ako je $a = 0$, onda je $a = bq + r$ za $q = r = 0$, što protivreči $(a, b) \in S$. Dakle, za $(a, b) \in S$, $deg(a)$ i $deg(b)$ su definisani, pa je definisan i $deg(a) + deg(b)$. Fiksirajmo bilo koji par $(a, b) \in S$ takav da je zbir $deg(a) + deg(b)$ minimalan moguć. Zapišimo $a(X) = a_nX^n + a'(X)$ i $b(X) = b_mX^m + b'(X)$ gde su $a_n, b_m \neq 0$, i $a'(X)$ i $b'(X)$ su sume članova stepena manjeg od $n$ odnosno $m$. Naglasimo da možda jeste $n = 0$ ili $m = 0$. Posmatrajmo dva slučaja:
Prvi slučaj: $n < m$. Tada možemo zapisati $a = bq + r$ za $q = 0$ i $r = a$, i kako $deg(r) = deg(a) = n < m = deg(b)$, zaključujemo $(a, b) \notin S$. Kontradikcija.
Drugi slučaj: $n \geqslant m$. Tada možemo da zapišemo sledeće:

$$a(X) = a_nX^n + a'(X) = \underbrace{a_nb_m^{-1}X^{n-m}}_{=q(X)}(\underbrace{b_mX^m + b'(X)}_{=b(X)}) + (\underbrace{-a_nb_m^{-1}X^{n-m}b'(X) + a'(X)}_{=r(X)}).$$

Primetimo dve stvari. Prvo, kako $(a, b) \in S$, sigurno $r(X) \neq 0$; dakle, $deg(r)$ je definisan. Drugo, očigledno $deg(r) < n$, pa je i $deg(r) + deg(b) < deg(a) + deg(b)$ odakle $(r, b) \notin S$ jer je po izboru $(a, b)$ bio par sa najmanjim zbirom stepena u $S$. Kako $(r, b) \notin S$, to znači da postoje $q', r' \in F[X]$ takvi da $r = bq' + r'$, i $r' = 0$ ili $deg(r') < deg(b)$. Odatle je $a = bq + r = bq + bq' + r' = b(q + q') + r'$, gde $r' = 0$ ili $deg(r') < deg(b)$. Dakle, $(a, b) \notin S$. Kontradikcija.
Kako nijedan slučaj nije moguć, završili smo posao: $N$ zaista jeste norma, i $F[X]$ je ED.

[a]Naglasimo da $deg(0)$ ne definišemo. U literaturi se ponekad definiše $deg(0) = -1$ ili $deg(0) = -\infty$.

**7/30 Primer** (Gausovi celi brojevi)**.**
Domen Gausovih celih brojeva je potprsten $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ od $\mathbb{C}$. Nije teško videti da je $\mathbb{Z}[i]$ zaista domen – proveru ostavljamo za vežbu. Definišemo normu na $\mathbb{Z}[i]$ sa: $N(a+bi) := a^2+b^2$. Primetimo

da je zapravo $N(z) = |z|^2$. (Primetimo da je u ovom slučaju i $N(0)$ definisano.)
Dokažimo da je $N$ zaista norma na $\mathbb{Z}[i]$. Neka $z, w \in \mathbb{Z}[i]$, $w \neq 0$. U $\mathbb{C}$ računamo $\frac{z}{w} = \frac{z}{w}\frac{\overline{w}}{\overline{w}} = \frac{z\overline{w}}{|w|^2} = a + bi$, i primetimo da kako $z, w \in \mathbb{Z}[i]$, to $a, b \in \mathbb{Q}$. Izaberimo cele brojeve $u, v \in \mathbb{Z}$ takve da $|a-u| \leqslant \frac{1}{2}$ i $|b-v| \leqslant \frac{1}{2}$; posmatrajmo $q = u + vi \in \mathbb{Z}[i]$ i $r = z - wq \in \mathbb{Z}[i]$; jasno, $z = wq + r$, pa treba još da dokažemo $r = 0$ ili $N(r) < N(w)$. Najpre primetimo $|\frac{z}{w} - q|^2 = |(a-u) + (b-v)i|^2 = (a-i)^2 + (b-v)^2 \leqslant \frac{1}{4} + \frac{1}{4} < 1$. Sada je $N(r) = N(z - wq) = |z - wq|^2 = |w|^2|\frac{z}{w} - q|^2 < |w|^2 = N(w)$. Završili smo dokaz.

**7/31 Primer** (Ajzenštajnovi celi brojevi)**.**
Domen Ajzenštajnovih celih brojeva je potprsten $\mathbb{Z}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Z}\}$ od $\mathbb{C}$, gde je $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Nije teško sračunati da je $\omega^2 = -1 - \omega$, pa nije teško videti da je $\mathbb{Z}[\omega]$ zaista potprsten od $\mathbb{C}$ – proveru ostavljamo za vežbu. Definišemo normu na $\mathbb{Z}[\omega]$ sa: $N(a + b\omega) := a^2 - ab + b^2$. Primetimo da je i ovde zapravo $N(a + b\omega) = |a + b\omega|^2$: $|a + b\omega|^2 = |(a - \frac{b}{2}) + \frac{b\sqrt{3}}{2}i|^2 = (a - \frac{b}{2})^2 + (\frac{b\sqrt{3}}{2})^2 = a^2 - ab + b^2$.
Da bismo videli da je $N$ zaista norma na $\mathbb{Z}[\omega]$, postupićemo kao u prethodnom primeru. Uzmimo $z, w \in \mathbb{Z}[\omega]$, $w \neq 0$, i u $\mathbb{C}$ zapišimo $\frac{z}{w} = \frac{z\overline{w}}{|w|^2} = a + b\omega$, gde $a, b \in \mathbb{Q}$. Izaberimo cele brojeve $u, v \in \mathbb{Z}$ takve da $|a-u| \leqslant \frac{1}{2}$ i $|b-v| \leqslant \frac{1}{2}$; posmatrajmo $q = u+v\omega \in \mathbb{Z}[\omega]$ i $r = z-wq \in \mathbb{Z}[\omega]$; jasno, $z = wq+r$, pa treba da dokažemo $r = 0$ ili $N(r) < N(w)$. Primetimo $|\frac{z}{w}-q|^2 = |(a-u)+(b-v)\omega|^2 = (a-i)^2-(a-u)(b-v)+(b-v)^2 \leqslant \frac{1}{4}+\frac{1}{4}+\frac{1}{4} < 1$. Sada je $N(r) = N(z - wq) = |z - wq|^2 = |w|^2|\frac{z}{w} - q|^2 < |w|^2 = N(w)$.

**7/32 Zadatak.** Dokazati da su sledeći domeni euklidski:

(a) $\mathbb{Z}[i\sqrt{2}] := \{a + bi\sqrt{2} \mid a, b \in \mathbb{Z}\}$ sa normom $N(a + bi\sqrt{2}) = a^2 + 2b^2$;

(b) $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ sa normom $N(a + b\sqrt{2}) = |a^2 - 2b^2|$;

(c) $\mathbb{Z}[\sqrt{3}] := \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ sa normom $N(a + b\sqrt{3}) = |a^2 - 3b^2|$.

## E Glavnoidealski domeni (PID)

**7/33 Definicija.** Domen $D$ je glavnoidealski domen (PID)[9] ako je svaki ideal u $D$ glavni, tj. za svaki $I \lhd D$ postoji $a \in I$ tako da $I = \langle a \rangle$.

**7/34 Teorema.**
ED je PID.

*Dokaz.* Neka je $D$ ED sa normom $N$. Neka je $I \lhd D$. Možemo da pretpostavimo da $I$ nije trivijalan: $I \neq 0$. Neka je $b \in I$ bilo koji nenula element sa minimalnom normom. Tvrdimo $I = \langle b \rangle$. Treba samo da dokažemo $(\subseteq)$, pa uzmimo proizvoljno $a \in I$. Zapišimo $a = qb + r$, gde je $r = 0$ ili $N(r) < N(b)$. Kako $r = a - qb \in I$ i $b$ je bio nenula element u $I$ minimalne norme, $r$, ako je nenula, ne može imati manju normu od $b$. Zaključujemo, mora biti $r = 0$. Dakle, $a = qb$, odakle $a \in \langle b \rangle$. □

Dakle, svi primeri za koje smo videli da su ED, su i primeri PID.

**7/35 Zadatak.** Dokazati da $\mathbb{Z}[i\sqrt{3}] := \{a + bi\sqrt{3} \mid a, b \in \mathbb{Z}\}$ nije glavnoidealski, pa ni euklidski.

Obrat gornje teoreme ne važi, ali dati primer PID koji nije ED nije trivijalno. Jedan takav primer dajemo u odeljku H.

## F Domeni sa jednoznačnom faktorizacijom (UFD)

**7/36 Definicija.** Domen $D$ je domen sa jednoznačnom faktorizacijom (UFD)[10] ako svaki element $a \notin D^\times \cup \{0\}$ ima jednoznačnu faktorizaciju.

[9] Skraćenica PID dolazi od *Principal Ideal Domain*.
[10] Skraćenica UFD dolazi od *Unique Factorization Domain*.

Videli smo da su prosti elementi uvek nerastavljivi, i da obratno ne važi u opštem slučaju. Kod UFD-a je situacija bolja.

**7/37 Lema.**
Neka je $D$ UFD. Svaki nerastavljiv element je prost.

*Dokaz.* Neka je $a \notin D^\times \cup \{0\}$ nerastavljiv, i neka $a \mid bc$; treba da dokažemo $a \mid b$ ili $a \mid c$. Ako je neki od $b$ i $c$ invertibilan, odmah vidimo da $a$ deli onog drugog, pa pretpostavimo da $b$ i $c$ nisu invertibilni. Zapišimo $bc = ad$, i primetimo da ni $d$ nije invertibilan, jer bismo u suprotnom dobili faktorizaciju nerastavljivog elementa $a$. Zapišimo nerastavljive faktorizacije $b$, $c$ i $d$: $b = p_1 \dots p_n$, $c = q_1 \dots q_m$ i $d = r_1 \dots r_k$. Sada je $p_1 \dots p_n q_1 \dots q_m = ar_1 \dots r_k$. Iz jednoznačnosti faktorizacije mora biti $n+m = 1+k$, i nerastavljivi faktori sa leve i sa desne strane su po parovima konjugovani. Specijalno, $a$ je konjugovano sa nekim $p_i$ ili sa nekim $q_j$. U prvom slučaju $a \mid b$, u drugom $a \mid c$. Završili smo dokaz. □

**7/38 Teorema** (Karakterizacija UFD-a)**.**
Sledeći iskazi su ekvivalentni:

(1) $D$ je UFD;

(2) svaki $a \notin D^\times \cup \{0\}$ ima nerastavljivu faktorizaciju, i svaki nerastavljiv je prost;

(3) svaki $a \notin D^\times \cup \{0\}$ ima prostu faktorizaciju;

(4) svaki $a \notin D^\times \cup \{0\}$ ima nerastavljivu faktorizaciju, i svaka dva elementa imaju NZD;

(5) $D$ zadovoljava ACCP, i svaki nerastavljiv je prost;

(6) (Teorema Kaplanskog) svaki nenula pravi prost ideal sadrži prost element.

*Dokaz.* (1)⇔(2) Smer ⇒ sledi iz definicije UFD i leme 7/37. Smer ⇐ sledi iz tvrđenja 7/10(g): svaki $a \notin D^\times \cup \{0\}$ ima nerastavljivu faktorizaciju, pa kako je svaki nerastavljiv prost, $a$ ima prostu faktorizaciju; prema tvrđenju 7/10(g), $a$ ima jednoznačnu faktorizaciju.

(2)⇒(3) je očigledno.

(3)⇒(4) Prvi deo je očigledan, pa dokazujemo drugi. Neka $a, b \in D$. Ako je neki od njih invertibilan lako vidimo da je $nzd(a,b) = 1$; pretpostavimo da nijedan nije invertibilan. Ako je neki od njih nula, lako vidimo da je $nzd(a,b) = 0$; pretpostavimo da su oba nenula. Sada prema (3) i tvrđenju 7/10(i), $nzd(a,b)$ postoji.

(4)⇒(2) Treba samo da dokažemo da je svaki nerastavljiv prost. Neka je $p$ nerastavljiv, i neka $p \mid ab$; dokazujemo $p \mid a$ ili $p \mid b$. Možemo da pretpostavimo da $a, b \neq 0$, jer u suprotnom završavamo posao trivijalno. Uočimo, prema (4), $d = nzd(ab, pb)$. Kako $p \mid ab, pb$ to $p \mid d$, i kako $b \mid ab, pb$, to $b \mid d$. Zapišimo $d = pu = bv$. Sada kako $bv = d \mid pb$, skraćivanjem sa $b \neq 0$ imamo $v \mid p$; kako je $p$ nerastavljiv, prema tvrđenju 7/10(f) imamo dva slučaja: $v \in D^\times$ i $v \sim p$. Ako $v \in D^\times$, onda iz $bv = d = pu$ imamo $b = puv^{-1}$, pa zaključujemo $p \mid b$ Ako $v \sim p$, kako iz $bv = d \mid ab$ skraćivanjem sa $b \neq 0$ sledi $v \mid a$, zaključujemo $p \mid a$.

(3)⇒(5) Kako smo već dokazali (3)⇒(4)⇒(2), svaki nesvodljiv element jeste prost. Ako pretpostavimo da imamo strogo rastući niz glavnih ideala $\langle a_0 \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \dots$, prema komentaru 7/18(f) imamo $\#a_0 > \#a_1 > \#a_2 > \dots$, pa kako ovaj niz ne može beskonačno da opada, ni polazni niz ideala ne može beskonačno da raste. Dakle, $D$ ima ACCP.

(5)⇒(6) Neka je $P \lhd D$ nenula prost ideal. Kako je prema (5) svaki nerastavljiv prost, dovoljno je da nađemo nerastavljiv element u $P$. Pretpostavimo suprotno, $P$ ne sadrži nerastavljive elemente. Dokazaćemo sledeće: za svaki nenula $a \in P$ postoji nenula $b \in P$ takav da $\langle a \rangle \subsetneq \langle b \rangle$. Neka je $a \in P$ nenula. Kako $a$ nije nerastavljiv možemo da zapišemo $a = bc$ tako da $b, c \notin D^\times$; očigledno $b, c \neq 0$. Kako je $P$ prost i $bc = a \in P$, bar jedan od $b$ i $c$ pripada $P$. Bez umanjenja opštosti, $b \in P$. Iz $a = bc$ sledi $a \in \langle b \rangle$, pa $\langle a \rangle \subseteq \langle b \rangle$, iz $c \notin D^\times$ sledi $\langle a \rangle \subsetneq \langle b \rangle$. Sada je lako da konstruišemo beskonačan rastući niz glavnih ideal, što je kontradikcija sa ACCP: izberemo bilo koje nenula $a_0 \in P$. Prema prethodnom tvrđenju, izaberemo nenula $a_1 \in P$ tako da $\langle a_0 \rangle \subsetneq \langle a_1 \rangle$. Ponovo, prema prethodnom tvrđenju izaberemo nenula $a_2 \in P$ tako da $\langle a_1 \rangle \subsetneq \langle a_2 \rangle$. I nastavimo ovaj postupak.

(6)⇒(3) Neka je $S$ skup svih invertibilnih i skup svih konačnih proizvoda prostih elemenata. Dovoljno je da dokažemo $S^c = \{0\}$. Pretpostavimo suprotno, $a \in S^c$ je nenula element. Primetimo da je $\langle a\rangle \subseteq S^c$. Ako $\langle a\rangle \cap S \neq \varnothing$, onda $\langle a\rangle$ sadrži invertibilan element ili neki proizvod prostih. Ako $\langle a\rangle$ sadrži invertibilan element, onda je i $a$ invertibilan, tj. $a \in S$, što je suprotno izboru $a$. Ako $\langle a\rangle$ sadrži proizvod prostih $p_1 \dots p_n$, onda $a \mid p_1 \dots p_n$, pa je i $a$ proizvod prostih prema tvrđenju 7/10(h) (jer nije invertibilan), što opet protivreči izboru elementa $a$. Dakle, $\langle a\rangle \subseteq S^c$.

Neka je $\mathcal{F} := \{I \lhd D \mid \langle a\rangle \subseteq I \subseteq S^c\}$. Koristeći Hauzdorfov princip maksimalnosti vidimo da $\mathcal{F}$ sadrži maksimalan element $P$. Zaista, unija $P$ bilo kog maksimalnog lanca u $\mathcal{F}$ je ideal za koji je $\langle a\rangle \subseteq P \subseteq S^c$, odakle sledi da je $P$ u $\mathcal{F}$, pa je i maksimalan u $\mathcal{F}$ jer bismo u suprotnom mogli produžiti lanac. (Za vežbu, razjasniti detalje.) Tvrdimo da je $P$ prost ideal.

Neka $b, c \notin P$. Tada su $P + \langle b\rangle$ i $P + \langle c\rangle$ strogo veći od $P$, pa, zbog maksimalnosti $P$ u $\mathcal{F}$, oni seku $S$. Neka je $x + rb, y + sc \in S$, gde $x, y \in P$. Tada očigledno i $(x + rb)(y + sc) \in S$, tj. $(xy + (sc)x + (rb)y) + (rs)bc \in S$. Kako prvi sabirak pripada $P$ i kako $P \cap S = \varnothing$, mora da bude $bc \notin P$. Dakle, $P$ je prost ideal.

Kako je $P$ nenula jer sadrži $a$, prema (6) sadrži i prost element. To znači $P \cap S \neq \varnothing$. Kontradikcija. □

**7/39 Teorema.**
PID je UFD. Specijalno, ED je UFD.

*Dokaz.* Neka je $D$ PID. Najkraći dokaz je da proverimo uslov (6) u teoremi 7/38. Neka je $P \lhd D$ pravi nenula prost ideal. Kako je $D$ PID, $P = \langle p\rangle$. Očigledno, $p \notin D^\times \cup \{0\}$, i kako je $\langle p\rangle$ prost, $p$ je prost prema tvrđenju 7/10(d).

Klasični dokaz je ipak da proverimo uslov (5) u teoremi 7/38. Dajemo i taj dokaz. Dokažimo najpre ACCP. Neka je $\langle a_0\rangle \subseteq \langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \dots$ rastući niz glavnih ideala. Tada je i $I = \bigcup_{n=0}^{\infty} \langle a_n\rangle$ ideal, pa kako je $I$ glavnoidealski, $I = \langle a\rangle$ za neko $a$. Po definiciji $I$, postoji $n$ tako da $a \in \langle a_n\rangle$. Kako sa druge strane, $a_n \in I = \langle a\rangle$, zaključujemo $I = \langle a\rangle = \langle a_n\rangle$. Odatle, za $k \geqslant n$, $\langle a_n\rangle \subseteq \langle a_k\rangle \subseteq I = \langle a_n\rangle$, pa polazni niz postaje konstantan posle $n$-tog člana, tj. nije beskonačno strogo rastući.

Ostaje da proverimo da su nerastavljivi elementi prosti. Neka je $a \in D$ nerastavljiv element, i neka $a \mid bc$; dokazujemo $a \mid b$ ili $a \mid c$. Posmatrajmo $\langle a, b\rangle$, i zapišimo $\langle a, b\rangle = \langle d\rangle$; to je moguće jer je $D$ PID. Tada $d \mid a$, pa kako je $a$ nerastavljiv, $d \in D^\times$ ili $d \sim a$ prema tvrđenju 7/10(f). Ako je $d$ invertibilan, onda $1 \in \langle d\rangle = \langle a, b\rangle$, pa možemo da zapišemo $1 = xa + yb$, pa množenjem sa $c$ dobijamo $c = (xc)a + y(bc) \in \langle a\rangle$, tj. $a \mid c$. Ako $d \sim a$, onda $\langle a\rangle = \langle d\rangle = \langle a, b\rangle$, odakle $b \in \langle a\rangle$, tj. $a \mid b$. Završili smo dokaz. □

Dakle, svi primeri za koje smo videli da su ED ili PID su i UFD. Obrat prethodne teoreme ne važi, tj. postoji UFD koji nije PID.

**7/40 Primer.**
Arhiprimer domena koji je UFD, ali nije PID je $\mathbb{Z}[X]$. Da bismo dokazali da $\mathbb{Z}[X]$ nije PID, dokažimo da ideal $I = \langle 2, X\rangle$ nije glavni. Primetimo, kako je proizvoljan element u $I$ oblika $2p(X) + Xq(X)$, $I$ je skup svih polinoma čiji je konstantan koeficijent paran. Specijalno, $I \neq \mathbb{Z}[X]$. Pretpostavimo suprotno, $I$ je glavni ideal $I = \langle a(X)\rangle$. Kako $a(X) \mid 2$ jer $2 \in I$, $a(X) = a$ je konstantan polinoma, i mora biti $a = \pm 1$ ili $a = \pm 2$; ako $a = \pm 1$, onda je $a$ invertibilan, što nije slučaj. Dakle, $a = \pm 2$, i odatle $I = \langle 2\rangle$. Kako $X \in I = \langle 2\rangle$, $2 \mid X$, što je očigledno kontradikcija.

Ostaje da vidimo da $\mathbb{Z}[X]$ jeste UFD. Ovo sledi direktno iz Gausove leme, koju ćemo dokazati u odeljku G, a u ovom konkretnom slučaju možemo da izvedemo direktan dokaz. Proverimo uslov (6) iz teoreme 7/38. Neka je $P \lhd \mathbb{Z}[X]$ pravi nenula prost ideal; treba da nađemo prost element $p(X) \in P$. Primetimo najpre da je $P \cap \mathbb{Z} \lhd \mathbb{Z}$ prost ideal. Ovo je prilično očigledno i direktno (Za vežbicu.), a možemo da vidimo i ovako: prema drugoj teoremi o izomorfizmu $\mathbb{Z}/(P \cap \mathbb{Z}) \cong (\mathbb{Z} + P)/P \leqslant \mathbb{Z}[X]/P$, pa kako je $\mathbb{Z}/(P \cap \mathbb{Z})$ izomorfan potprstenu domena $\mathbb{Z}[X]/P$ (domen je jer je $P$ prost), i $\mathbb{Z}/(P \cap \mathbb{Z})$ je domen, pa je $P \cap \mathbb{Z}$ prost ideal u $P$.

Ako je $P \cap \mathbb{Z} = p\mathbb{Z}$ za neki prost broj $p$, onda je $p$ prost (u $\mathbb{Z}[X]$) element od $P$, što završava posao. I ovo lako možemo da vidimo direktno (Za vežbu.), a možemo da vidimo i ovako: u $\mathbb{Z}[X]$, $\langle p\rangle = p\mathbb{Z}[X]$, a prema primeru 6/59, $\mathbb{Z}[X]/p\mathbb{Z}[X] \cong (\mathbb{Z}/p\mathbb{Z})[X]$; kako je prsten na desnoj strani domen, $p\mathbb{Z}[X]$ je prost u $\mathbb{Z}[X]$.

Dakle, ostaje nam slučaj $P \cap \mathbb{Z} = 0$. (Primetimo da ne može biti $P \cap \mathbb{Z} = \mathbb{Z}$, jer to znači da $1 \in P$, pa $P = \mathbb{Z}[X]$ nije pravi ideal.) Uzmimo $p(X) \in P$ da bude polinom minimalnog mogućeg stepena, i među takvim polinomima, uzmimo $p(X)$ da bude, po apsolutnoj vrednosti, minimalnog mogućeg vodećeg koeficijenta. Primetimo da ne postoji prost broj $q$ koji deli sve koeficijente polinoma $p(X)$ (takve polinom ćemo kasnije zvati primitivni). Zaista, ako postoji prost broj $q$ koji deli sve koeficijente polinoma $p(X)$, onda je $p(X) = qp'(X)$, pa kako $q \notin P$ i $P$ je prost, $p'(X) \in P$, i kako $p'(X)$ ima isti stepen kao $p(X)$ i po apsolutnoj vrednosti manji vodeći koeficijent od $p(X)$, dobijamo kontradikciju sa izborom polinoma $p(X)$.

Tvrdimo $P = \langle p(X) \rangle$, odakle $p(X)$ je prost, što završava posao. Pretpostavimo suprotno, i neka je $f(X) \in P$ najmanjeg mogućeg stepena takav da $p(X) \nmid f(X)$. Zapišimo $p(X) = \sum_{i=0}^{k} p_i X^i$ i $f(X) = \sum_{i=0}^{n} f_i X^i$; po izboru polinoma $p(X)$, $k \leqslant n$. Izaberimo nenula cele brojeve $a, b \in \mathbb{Z}$ takve da $ap_k = bf_n$, i posmatrajmo polinom $g(X) := aX^{n-k}p(X) - bf(X)$. Jasno $g(X) \in P$ i $deg(g) < deg(f)$. Po izboru polinoma $f(X)$ sledi $p(X) \mid g(X)$, odakle direktno sledi $p(X) \mid aX^{n-k}p(X) - g(X) = bf(X)$.

Izaberimo sada po apsolutnoj vrednosti najmanje nenula $b$ tako da $p(X) \mid bf(X)$; takav izbor je moguć jer bar jedno takvo $b$ postoji prema prethodnom zaključku. Ako je $|b| = 1$, završili smo posao: $p(X) \mid f(X)$, tj. $f(X) \in \langle p(X) \rangle$. Ostaje nam slučaj $|b| > 1$, i dokazaćemo da on nije moguć. Pretpostavimo $|b| > 1$. Tada postoji prost broj $q$ takav da $q \mid b$. Dokazaćemo da $p(X) \mid \frac{b}{q} f(X)$, što će biti kontradikcija sa izborom broja $b$ jer $|\frac{b}{q}| < |b|$. Kako $p(X) \mid bf(X)$, zapišimo $bf(X) = p(X)s(X)$ i $s(X) = \sum_{i=0}^{l} s_i X^i$ gde $l = n - k$. Setimo se da $q$ ne deli sve koeficijente polinoma $p(X)$; pa neka je $i \leqslant k$ najmanji takav da $q \nmid p_i$. Tvrdimo da $q$ deli sve koeficijente polinoma $s(X)$. Pretpostavimo suprotno, $q$ ne deli sve koeficijente polinoma $s(X)$, i neka je $j \leqslant l$ najmanji takav da $q \nmid s_j$. U jednakosti $bf(X) = p(X)s(X)$ posmatrajmo koeficijent uz $X^{i+j}$:

$$bf_{i+j} = \underbrace{p_0 s_{i+1} + \cdots + p_{i-1} s_{j+1}}_{=A} + p_i s_j + \underbrace{p_{i+1} s_{j-1} + \cdots + p_{i+j} s_0}_{=B}.$$

Kako $q \mid bf_{i+j}$ jer $q \mid b$, $q \mid A$ prema izboru broja $i$, i $q \mid B$ prema izboru broja $j$, zaključujemo $q \mid p_i s_j$, što je u suprotnosti sa $q \nmid p_i$ i $q \nmid s_j$. Dakle, $q$ deli sve koeficijente polinoma $s(X)$, pa možemo zapisati $s(X) = qs'(X)$. Vraćanjem u gornju jednakost dobijamo: $bf(X) = p(X)s(X) = qp(X)s'(X)$, odakle je $\frac{b}{q} f(X) = p(X)s'(X)$, odakle $p(X) \mid \frac{b}{q} f(X)$. Završili smo posao.

**7/41 Zadatak.** Dokazati da je $\mathbb{R}[X, Y]$ UFD koji nije PID.

Među UFD-ovima, PID-ove možemo prepoznati na sledeći način:

**7/42 Teorema.**
Neka je $D$ UFD. Sledeći iskazi su ekvivalentni:

(1) $D$ je PID;

(2) svaki pravi nenula prost ideal je maksimalan;

(3) prosti ideali su glavni;

(4) maksimalni ideali su glavni;

(5) ako $nzd(a, b) = 1$, onda $\langle a, b \rangle = D$, za sve $a, b \in D$;

(6) $\langle a, b \rangle = \langle nzd(a, b) \rangle$, za sve $a, b \in D$;

(7) ideali $\langle a, b \rangle$ su glavni, za sve $a, b \in D$.

*Dokaz.* (1)⇒(2) Neka je $D$ PID, i neka je $P$ nenula pravi prost ideal. Pretpostavimo $P \subseteq Q \subsetneq D$, i, kako je $D$ PID, zapišimo $P = \langle a \rangle$ i $Q = \langle b \rangle$. Kako je $P$ prost, $a$ je prost element, a kako je $Q \neq D$, $b \notin D^\times$. Kako $a \in \langle b \rangle$, to $b \mid a$. Kako je $a$ prost (pa i nerastavljiv) i $b \notin D^\times$, to je $b \sim a$. Dakle, $P = Q$, odakle sledi da je $P$ maksimalan.

(2)⇒(3) Neka je $P$ nenula pravi prost ideal. Uzmimo nenula element $x \in P$, i, kako je $D$ UFD, posmatrajmo njegovu prostu faktorizaciju: $x = p_1 p_2 \dots p_n$. Kako je $P$ prost, $p_i \in P$ za neko $I$. Tada je $\langle p_i \rangle$ prost ideal, pa je prema (2) maksimalan. Kako je $\langle p_i \rangle \subseteq P \neq D$, iz maksimalnosti sledi $P = \langle p_i \rangle$.

(3)⇒(4) je očigledno jer su maksimalni ideali uvek prosti.

(4)⇒(5) Pretpostavimo $nzd(a,b) = 1$. Ako $\langle a, b \rangle \neq D$, onda postoji maksimalan ideal $M$ takav da $\langle a, b \rangle \subseteq M$; prema (4) $M = \langle c \rangle$, i očigledno $c \notin D^\times$. Sada $a, b \in \langle c \rangle$ povlači $c \mid a, b$, pa $c \mid nzd(a,b) = 1$. Odavde, $c \in D^\times$; kontradikcija.

(5)⇒(6) Pretpostavimo $nzd(a,b) = c$ (NZD postoji jer je $D$ UFD). Jasno $\langle a, b \rangle \subseteq \langle c \rangle$. Zapišimo $a = ca'$ i $b = cb'$. Tada lako vidimo da je $nzd(a', b') = 1$, pa prema (5), $\langle a', b' \rangle = D$, odakle možemo da zapišemo $1 = ra' + sb'$. Množenjem sa $c$ dobijamo: $c = ra + sb \in \langle a, b \rangle$. Dakle, $\langle a, b \rangle = \langle c \rangle$.

(6)⇒(7) Očigledno.

(7)⇒(1) Pretpostavimo suprotno, $D$ nije PID, i neka $I$ nije glavni. Naći ćemo beskonačan strogo rastući lanac glavnih ideala što protivreči ACCP s obzirom da je $D$ UFD. Neka je $a_0 \in I$ proizvoljno. Pretpostavimo da smo konstruisali strogo rastući lanac glavnih podideala od $I$:

$$\langle a_0 \rangle \subsetneq \langle a_1 \rangle \subsetneq \cdots \subsetneq \langle a_n \rangle \subseteq I,$$

i pokažimo da ga uvek možemo produžiti za još jedan član. Kako $I$ nije glavni, $I \neq \langle a_n \rangle$, pa izaberimo $b \in I \setminus \langle a_n \rangle$. Tada $\langle a_n \rangle \subsetneq \langle a_n, b \rangle \subseteq I$, i, prema (7), $\langle a_n, b \rangle = \langle a_{n+1} \rangle$ za neko $a_{n+1}$. Završili smo posao. □

**7/43 Primer.**
Imajući u vidu prethodnu teoremu, ako znamo da je domen UFD, često lako možemo da prepoznamo da li je PID. Npr. ako $D$ jeste UFD, ali nije polje, po Gausovoj lemi (odeljak G) $D[X]$ jeste UFD. Posmatramo preslikavanje $\varphi : D[X] \to D$ dato sa $\varphi(f(X)) := f(0)$. Lako možemo da vidimo da je $\varphi$ epimorfizam prstena, pa je po prvoj teoremi o izomorfizmu $D[X]/ker(\varphi) \cong D$, tj. $D[X]/ker(f)$ je domen koji nije polje, tj. $ker(f)$ je ideal koji je prost ali nije maksimalan. Dakle, $D[X]$ nije PID.
Dodatno, lako možemo da izračunamo $ker(\varphi) = \langle X \rangle$, jer $f(0) = 0$ ako i samo ako $f(X)$ ima nula konstantni koeficijent, ako i samo ako $X \mid f(X)$.

## G Gausova teorema

U ovom odeljku dokazaćemo sledeće dve teoreme:

**7/44 Teorema** (Gausova lema)**.**
Neka je $D$ UFD, $F = F(D)$, i $f(X) \in D[X]$ nenula polinom. Tada $f(X)$ je nerastavljiv u $D[X]$ ako i samo ako $f(X)$ je primitivan i $f(X)$ je nerastavljiv u $F[X]$.

**7/45 Teorema** (Gausova teorema)**.**
Ako je $D$ UFD, onda je i $D[X]$ UFD.

Gausova lema je rezultat koji se se često koristi u zadacima. Moramo najpre da defišemo pojam primitivnog polinoma i da dokažemo da je skup primitivnih polinoma zatvoren za množenje.

**7/46 Definicija.** Neka je $D$ UFD, i neka je $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in D[X]$ nekonstantan polinom. Kažemo da je polinom $f(X)$ primitivan ako ne postoji prost element $p \in D$ takav da $p \mid a_0, a_1, \dots, a_n$.

**7/47 Primer.**
Moničan polinom $f(X)$ (dakle, ako $a_n = 1$) je primitivan.

**7/48 Zadatak.** Neka je $D$ UFD, i $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in D[X]$ nekonstantan polinom. Dokazati da su sledeći iskazi ekvivalentni:

(1) $f(X)$ je primitivan;

(2) $nzd(a_0, a_1, \ldots, a_n) = 1$;

(3) $\langle a_0, a_1, \ldots, a_n \rangle = D$.

**7/49 Komentar.** Neka je $D$ UFD. Primetimo da je nekonstantan polinom $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in D[X]$ nerastavljiv ako i samo ako je primitivan i slabo nerastavljiv. Za ($\Rightarrow$) treba samo da dokažemo da nerastavljiv povlači primitivan (jer već znamo da povlači slabo nerastavljiv). Ako $f(X)$ nije primitivan, postoji prost $p$ koji deli sve koeficijente $a_i$; zapišimo $a_i = pa_i'$. Tada $f(X) = p(a_n' X^n + \cdots + a_1' X + a_0')$ svedoči rastavljivost polinoma $f(X)$ u $D[X]$.
($\Leftarrow$) Pretpostavimo sada da je $f(X)$ primitivan i slabo nerastavljiv. Zapišimo $f(X) = g(X)h(X)$. Kako je $f(X)$ slabo nerastavljiv, jedan od $g(X)$ i $h(X)$ je konstantan, npr. $g(X) = c$; dakle, $f(X) = ch(X)$. Ako je $c$ invertibilan, završili smo posao. Dakle, treba da odbacimo slučaj da je $c$ neinvertibilan. Pretpostavimo suprotno, $c$ je neinvertibilan. Kako je $D$ UFD, $c$ se može napisati kao proizvod prostih, i neka je $p$ jedan od njegovih faktora. Ali sada očigledno iz $f(X) = cg(X)$ sledi da $p$ deli sve koeficijente polinoma $f(X)$, što protivreči primitivnosti.

Za dokaz Gausove leme, potrebna nam je kratka priprema.

**7/50 Lema.**
Neka je $D$ UFD.

(a) Ako je $f(X) \in D[X]$ nekonstantan polinom, onda postoje $d \in D$ i primitivan polinoma $f'(X)$ takvi da $f(X) = df'(X)$.

(b) Ako su $f(X), g(X) \in D[X]$ primitivni polinomi i $a, b \in D \setminus \{0\}$, onda $af(X) = bg(X)$ povlači $a \sim b$ u $D$ i $f(X) \sim g(X) \in D[X]$.

*Dokaz.* (a) Zapišimo $f(X) = a_n X^n + \cdots + a_1 X^n + a_0$. Neka je $d = nzd(a_0, a_1, \ldots, a_n)$; primetimo da $d$ postoji jer je $D$ UFD. Zapišimo $a_i = da_i'$ za sve $i = 0, 1, \ldots, n$, i stavimo $f'(X) = a_n' X^n + \cdots + a_1' X + a_0'$. Očigledno $f(X) = df'(X)$, pa ostaje da dokažemo da je $f'(X)$ primitivan. Ako imamo prost element $p$ takav da $p \mid a_0', a_1', \ldots, a_n'$, onda $pd \mid a_0, a_1, \ldots, a_n$, pa $pd \mid d$; odatle $p \sim 1$, što protivreči činjenici da je $p$ prost. Dakle, $f'(X)$ je primitivan.

(b) Pretpostavimo da je $af(X) = bg(X)$, gde su $f(X)$ i $g(X)$ primitivni, i $a, b \neq 0$. Neka je $d = nzd(a, b)$ (postoji jer smo u UFD-u), i zapišimo $a = da'$ i $b = db'$. Deljenjem sa $d$ dobijamo $a'f(X) = b'g(X)$. Ako su $a'$ i $b'$ invertibilni, onda smo završili posao: tada očigledno $a = da' \sim db' = b$ i $f(X) = (a'^{-1}b')g(X) \sim g(X)$. Dakle, pretpostavimo da bar jedan od $a'$ i $b'$, bez umanjenja opštosti $a'$, nije invertibilan; dokazujemo da ovaj slučaj nije moguć. Neka je $p$ neki njegov prost faktor. Tada $p \mid a'f(X) = b'g(X)$, tj. $p$ deli sve koeficijente polinoma $b'g(X)$. Kako je $g(X)$ primitivan, $p$ ne deli neki koeficijent $g_i$ polinoma $g(X)$. Dakle, $p \nmid g_i$, $p \mid b'g_i$ i $p$ je prost povlače $p \mid b'$. Odatle $p \mid a', b'$, pa $pd \mid a, b$, odakle $pd \mid d$. Dakle, $p \sim 1$, što je u suprotnosti sa činjenicom da je $p$ prost. Završili smo dokaz. □

**7/51 Lema.**
Neka je $D$ UFD, i neka su $f(X), g(X) \in D[X]$ nekonstantni polinomi. Ako su $f(X)$ i $g(X)$ primitivni, onda je i $f(X)g(X)$ primitivan.

*Dokaz.* Zapišimo $f(X) = a_n X^n + \cdots + a_1 X + a_0$ i $g(X) = b_m X^m + \cdots + b_1 X + b_0$, gde $n, m \geqslant 1$, $a_n, b_m \neq 0$; zapišimo $f(X)g(X) = c_k X^k + \cdots + c_1 X + c_0$, gde $k = m + n$. Neka je $p \in D$ proizvoljan prost element. Kako $p$ nedeli sve koeficijente polinoma $f(X)$ i $g(X)$ jer su oni primitivni, postoje najmanji $i \leqslant n$ i $j \leqslant m$ takvi da

$p \nmid a_i$ i $p \nmid b_j$ (dakle, $p \mid a_0, \ldots, a_{i-1}$ ako $i > 0$, i $p \mid b_0, \ldots, b_{j-1}$ ako $j > 0$). Posmatrajmo koeficijent $c_{i+j}$:

$$c_{i+j} = \underbrace{a_0 b_{i+j} + \cdots + a_{i-1} b_{j+1}}_{=A} + a_i b_j + \underbrace{a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0}_{=B}.$$

(Ovde podrazumevamo da smo stavili $a_l = 0$ za $l > n$ i $b_l = 0$ za $l > m$, ako se takvi indeksi pojavljuju.) Primetimo da $p \mid A$ jer deli $a$-ove u svim sabircima, i $p \mid B$ jer deli $b$-ove u svim sabircima. Međutim, kako $p \nmid a_i$, $p \nmid b_j$ i $p$ je prost, $p \nmid a_i b_j$, pa $p \nmid c_{i+j}$. Dakle, $p$ ne deli sve koeficijente polinoma $f(X)g(X)$. Kako je $p$ bio proizvoljan, zaključujemo da ne postoji prost element koji deli sve koeficijente polinoma $f(X)g(X)$, pa je on primitivan. □

**7/52 Komentar.** Prethodni dokaz je prilično elementaran. Dokažimo prethodnu lemu na još jedan, nešto neelementarniji način.
Pretpostavimo suprotno, $f(X)g(X)$ nije primitivan. To znači da postoji prost element $p$ koji deli sve njegove koeficijente, tj. pravi prost ideal $\langle p \rangle \lhd D$ sadrži sve koeficijente polinoma $f(X)g(X)$. Setimo se da je $D/\langle p \rangle$ domen jer je $\langle p \rangle$ prost. Prema primeru 6/59, $D[X]/\langle p \rangle[X] \cong (D/\langle p \rangle)[X]$, pa je $D[X]/\langle p \rangle[X]$ domen (jer je izomorfan prstenu polinoma nad domenom). U domenu $D[X]/\langle p \rangle[X]$ je $f(X)g(X) + \langle p \rangle[X] = \langle p \rangle[X]$ jer svi koeficijenti polinoma $f(X)g(X)$ pripadaju $\langle p \rangle$. Dakle, $(f(X) + \langle p \rangle[X])(g(X) + \langle p \rangle[X]) = \langle p \rangle[X]$, pa kako je $D[X]/\langle p \rangle[X]$ domen, jedan od činilaca je nula, npr. $f(X) + \langle p \rangle[X] = \langle p \rangle[X]$. To znači da svi koeficijenti polinoma $f(X)$ pripadaju $\langle p \rangle$, pa $p$ deli sve koeficijente polinoma $f(X)$, odakle $f(X)$ nije primitivan. Kontradikcija.

*Dokaz teoreme 7/44 (Gausove leme).* Neka je $D$ UFD, $F = F(D)$, i $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in D[X]$ nenula polinom.

($\Rightarrow$) Neka je $f(X)$ nerastavljiv u $D[X]$. Prema komentaru 7/49 znamo da je $f(X)$ primitivan i slabo nerastavljiv. Pretpostavimo da u $F[X]$ važi $f(X) = g(X)h(X)$. Ako je $g(X)$ ili $h(X)$ konstantan, završili smo posao. Dakle, treba da odbacimo slučaj $g(X), h(X)$ su nekonstantni. Izaberimo nenula $a \in D$ tako da $ag(X) \in D[X]$; primetimo da je ovo moguće – npr., uzmimo za $a$ proizvod svih imenilaca koeficijenata polinoma $g(X)$. Slično, nađimo nenula $b \in D$ tako da $bh(X) \in D[X]$. Koristeći lemu 7/50(a), nađimo $a', b' \in D$ i primitivne polinome $g'(X), h'(X) \in D[X]$ takve da $ag(X) = a'g'(X)$ i $bh(X) = b'h'(X)$. Tada je $abf(X) = abg(X)bh(X) = a'b'g'(X)h'(X)$. Kako su $f(X)$ i $g'(X)h'(X)$ primitivni (drugi prema lemi 7/51), prema lemi 7/50(b), $ab \sim a'b'$ i $f(X) \sim g'(X)h'(X)$. Druga od ovih činjenica povlači $f(X) = ug'(X)h'(X)$ za neko $u \in D[X]^\times = D^\times$, što je u suprotnosti sa slabom nerastavljivošću polinoma $f(X)$.

($\Leftarrow$) Ako je $f(X)$ rastavljiv u $D[X]$, onda prema komentaru 7/49, $f(X)$ nije primitivan ili $f(X)$ nije slabo rastavljiv. U prvom slučaju nemamo šta da dokažemo, a u drugom je dovoljno da primetimo da ako zapišemo $f(X)$ kao proizvod dva nekonstanta polinoma nad $D$, to je specijalno i rastavljanje $f(X)$ nad $F$ jer $D \subseteq F$; odatle, $f(X)$ je rastavljiv nad $F$. □

Gausovu teoremu sada izvodimo kao posledicu.

*Dokaz teoreme 7/45 (Gausove teoreme).* Neka je $D$ UFD, dokazujemo $D[X]$ je UFD. Proverićemo uslov (5) iz teoreme 7/38. Dokažimo prvo da $D[X]$ zadovoljava ACCP. Neka je $\langle a_0(X) \rangle \subseteq \langle a_1(X) \rangle \subseteq \langle a_2(X) \rangle \subseteq \ldots$ beskonačan lanac glavih idela; dokazaćemo da ne može biti strogo rastući. Najpre primetimo da je $deg(a_0) \geqslant deg(a_1) \geqslant deg(a_2) \geqslant \ldots$, pa kako ovaj niz ne može beskonačno da strogo opada, u originalnom nizu, počeši od nekog člana, svi polinomi su istog stepena. Bez umanjenja opštosti, odbacivanjem nekog početnog dela niza, možemo da pretpostavimo da su svi polinomi $a_0(X), a_1(X), a_2(X), \ldots$ istog stepena. Označimo da $a_n^*$ vodeći koeficijent polinoma $a_n(X)$. Primetimo da $\langle a_n \rangle \subseteq \langle a_{n+1} \rangle$ povlači $\langle a_n^* \rangle \subseteq \langle a_{n+1}^* \rangle$ u $D$, pa u $D$ imamo rastući niz glavnih idela. Kako je $D$ UFD, ovaj niz glavnih ideala u $D$ nije beskonačno strogo rastući, pa ponovo odbacivanjem nekog početnog dela, možemo da pretpostavimo da je $\langle a_n^* \rangle = \langle a_0^* \rangle$ za sve $n$, tj. $a_n^* \sim a_0^*$ za sve $n$. Sada, iz $a_n(X) \mid a_0(X)$ i $deg(a_n) = deg(a_0)$ sledi $a_0(X) = da_n(X)$. Specijalno, $a_0^* = da_n^*$, pa kako $a_0^* \sim a_n^*$, to je $d \in D^\times$. Dakle, $a_0(X) = da_n(X) \sim a_n(X)$, odakle $\langle a_0(X) \rangle = \langle a_n(X) \rangle$ za sve $n$. Ovim smo dokazali da $D[X]$ zadovoljava ACCP.

Ostaje da dokažemo da je svaki nerastavljiv polinom $f(X)$ prost u $D[X]$. Prema Gausovoj lemi $f(X)$ je primitivan i $f(X)$ je nerastavljiv u $F[X]$, gde je $F = F(D)$. Kako je $F[X]$ UFD (jer je ED prema primeru 7/29), $f(X)$ jeste prost u $F[X]$. Pretpostavimo $f(X) \mid g(X)h(X)$ u $D[X]$. Tada je ovo tačno i u $F[X]$, pa, bez umanjenja opštosti, $f(X) \mid g(X)$ u $F[X]$. Zapišimo $g(X) = f(X)q(X)$ gde $q \in F[X]$. Izaberimo $a \in D$ tako da $aq(X) \in D[X]$, i izaberimo $b, c \in D$ i primitivne polinome $g'(X), q'(X) \in D[X]$ tako da $g(X) = bg'(X)$ i $aq(X) = cq'(X)$; poslednje je moguće prema lemi 7/50(a). Sada je $abg'(X) = ag(X) = af(X)q(X) = cf(X)q'(X)$. Prema lemi 7/51, $f(X)q'(X)$ je primitivan, pa prema lemi 7/50(b), $g'(X) \sim f(X)q'(X)$. Odavde lako sledi $f(X) \mid g'(X) \mid g(X)$. Završili smo dokaz. □

## H Primer PID-a koji nije ED

Neka je $\xi = \frac{1+i\sqrt{19}}{2}$; posmatrajmo $\mathbb{Z}[\xi] := \{a + b\xi \mid a, b \in \mathbb{Z}\}$. Primetimo da je:

$$\xi^2 = \frac{1 + 2i\sqrt{19} - 19}{4} = \frac{2 + 2i\sqrt{19}}{4} - \frac{20}{4} = \xi - 5,$$

odakle lako vidimo da je $\mathbb{Z}[\xi]$ zatvoren za množenje, i da je $\xi$ potprsten od $\mathbb{C}$. Dokazačemo da je $\mathbb{Z}[\xi]$ PID koji nije euklidski. Najpre ćemo da dokažemo sledeću lemu:

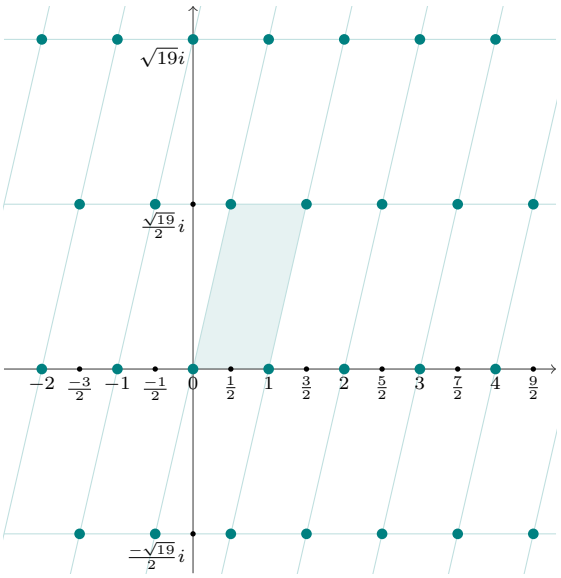
**7/53 Lema.**(a) Za svako $z \in \mathbb{C}$ važi bar jedan od sledeća dva uslova:

(1) postoji $s \in \mathbb{Z}[\xi]$ tako da $|z - s| < 1$;

(2) postoji $s \in \mathbb{Z}[\xi]$ tako da $|2z - s| < 1$.

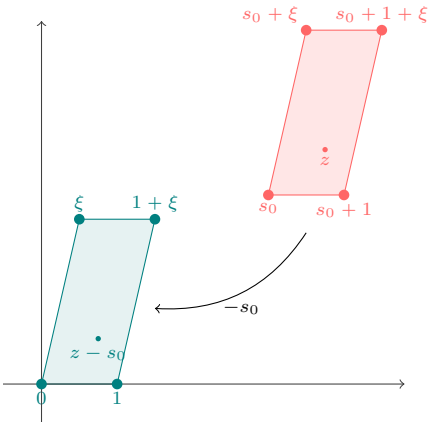
(b) Ako $z \in \mathbb{C} \setminus \mathbb{Z}[\xi]$, postoje $r, s \in \mathbb{Z}[\xi]$ tako da $0 < |rz - s| < 1$.

*Dokaz.* (a) Primetimo da je $a + b\xi = \frac{2a+b}{2} + \frac{b}{2}i\sqrt{19}$. Takođe, primetimo da je $2a + b$ parno ako i samo ako je $b$ parno, pa su elementi prstena $\mathbb{Z}[\xi]$ oblika $m + ni\sqrt{19}$ ili $(m + \frac{1}{2}) + (n + \frac{1}{2})i\sqrt{19}$, gde su $m, n \in \mathbb{Z}$. Dakle, $\mathbb{Z}[\xi]$ u $\mathbb{C}$ izgleda ovako:



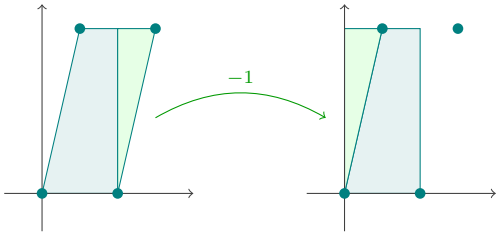

Slika $\mathbb{Z}[\xi]$ u $\mathbb{C}$

Kao što je prikazano na slici, $\mathbb{Z}[\xi]$ određuje pokrivanje kompleksne ravni $\mathbb{C}$ paralelogramima čija su temena elementi iz $\mathbb{Z}[\xi]$. Primetimo da za svako $z \in \mathbb{Z}$ postoji $s_0 \in \mathbb{Z}[\xi]$ tako da $z - s_0 \in P$, gde je $P$ označeni paralelogram sa temenima $0, 1, 1 + \omega, \omega$; zaista, ako se $z$ nalazi u paralelogramu sa donjim levim temenom $s_0$ (paralelogramu sa temenima $s_0, s_0 + 1, s_0 + \omega + 1, s_0 + \omega$), translacijom za $-s_0$ taj paralelogram se slika u $P$, pa $z - s_0 \in P$:




(Formalno, ako zapišemo $z = x + iy = x + \frac{2y}{\sqrt{19}}\frac{\sqrt{19}i}{2} = (x - \frac{y}{\sqrt{19}}) + \frac{2y}{\sqrt{19}}\frac{1+\sqrt{19}i}{2} = (x - \frac{y}{\sqrt{19}}) + \frac{2y}{\sqrt{19}}\xi$, ako uzmemo $m = \lfloor x - \frac{y}{\sqrt{19}} \rfloor$, $n = \lfloor \frac{2y}{\sqrt{19}} \rfloor$ i $s_0 = m + n\xi$, dobijamo $z - s_0 \in P$.)

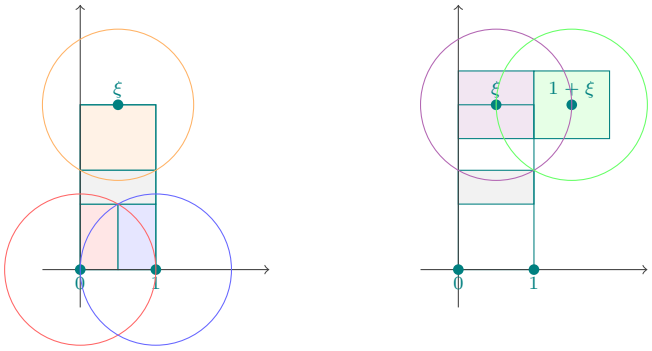
Štaviše, možemo da nađemo $s_1 \in \mathbb{Z}[\xi]$ tako da $z - s_1 \in Q$ gde je $Q$ pravougaonik sa temenima $0, 1, \xi + \frac{1}{2}, \xi - \frac{1}{2}$:




Kao što slika sugeriše, za $z - s_0 \in P$, ako $z - s_0$ pripada plavom trapezu stavimo $s_1 = s_0$, a ako $z - s_0$ pripada zelenom trouglu stavimo $s_1 = s_0 + 1$ (transliramo $z - s_0$ za $-1$). (Formalno, ako $Re(z - s_0) < 1$ stavimo $s_1 = s_0$, a ako $Re(z - s_0) \geqslant 1$ stavimo $s_1 = s_0 + 1$.) Dakle, sada znamo da $z$ možemo da transliramo za $s_1 \in \mathbb{Z}[\xi]$, tako da $z - s_1 \in Q$.

Tvrdimo sledeće: dovoljno je da za $w \in Q$ nađemo $t \in \mathbb{Z}[\xi]$ tako da $|w - t| < 1$ ili $|2w - t| < 1$. Zaista, primenom ovog na $t = z - s_1$ imamo $|z - (s_1 + t)| < 1$ ili $|2z - (2s_1 + t)| < 1$, pa možemo uzeti željeno $s$ da bude $s = s_1 + t$, odnosno $s = 2s_1 + t$.

Dakle, na dalje, za $w \in Q$ tražimo $t \in \mathbb{Z}[\xi]$ tako da $|w - t| < 1$ ili $|2w - t| < 1$. Geometrijski to znači da $w$ pripada jediničnom krugu sa centrom $t$, odnosno da $2w$ pripada jediničnom krugu sa centrom $t$. Posmatrajmo sledeću sliku (levo):




Na slici levo su jedinični krugovi sa centrima 0, 1 i $\xi$. Ako $w$ pripada crvenom pravougaoniku, tj. ako $0 \leqslant Re(w) \leqslant \frac{1}{2}$ i $0 \leqslant Im(w) < \frac{\sqrt{3}}{2}$, jasno je da treba da uzmemo $t = 0$. Ako $w$ pripada plavom pravougaoniku, tj. ako $\frac{1}{2} \leqslant Re(w) \leqslant 1$ i $0 \leqslant Im(w) < \frac{\sqrt{3}}{2}$, jasno je da treba da uzmemo $t = 1$. Konačno, ako $w$ pripada narandžastom pravougaoniku, tj. ako $0 \leqslant Re(w) \leqslant 1$ i $\frac{\sqrt{19}-\sqrt{3}}{2} < Im(w) \leqslant \frac{\sqrt{19}}{2}$, jasno je da treba da uzmemo $t = \xi$. Konkretne račune ostavljamo za vežbu. Dakle, ostaje nam sivi pravougaonik, $0 \leqslant Re(w) \leqslant 1$ i $\frac{\sqrt{3}}{2} \leqslant Im(w) \leqslant \frac{\sqrt{19}-\sqrt{3}}{2}$, koji nije u potpunosti pokriven sa ova tri kruga.

Posmatrajmo homotetiju sa centrom 0 i koeficijentom 2 (slika desno). Za $w$ iz sivog pravougaonika imamo $0 \leqslant Re(2w) \leqslant 2$ i $\sqrt{3} \leqslant Im(2w) \leqslant \sqrt{19} - \sqrt{3}$. Sliku sivog pravougaonika možemo da podelimo na dva kao na slici: ljubičasti u kome je $0 \leqslant Re(2w) \leqslant 1$ i zeleni u kome je $1 \leqslant Re(2w) \leqslant 2$. Ako je $2w$ u ljubičastom pravougaoniku, uzimajući $t = \xi$ dobijamo $|2w - t| < 1$, a ako je $2w$ u zelenom, uzimajući $t = 1 + \xi$ dobijamo $|2w - t| < 1$. I ovaj račun je direktan i ostavljamo ga za vežbu.

Ovime smo završili dokaz dela (a).

(b) Neka $z \in \mathbb{C} \setminus \mathbb{Z}[\xi]$. Opšti slučaj u (b) sledi iz (a). Preciznije, ako postoji $s \in \mathbb{Z}[\xi]$ tako da $|z - s| < 1$, tada je odmah $|z - s| > 0$ jer $z \notin \mathbb{Z}[\xi]$, pa uzimajući ovo $s$ i $r = 1$ završavamo posao. Pretpostavimo sada da postoji $s \in \mathbb{Z}[\xi]$ tako da $|2z - s| < 1$. Ako se desilo da je $|2z - s| > 0$, opet smo završili uzimajući ovo $s$ i $r = 2$.

Dakle, ostaje nam slučaj da smo našli $s \in \mathbb{Z}[\xi]$, tako da $|2z - s| < 1$, ali $|2z - s| = 0$, tj. $2z = s$. Kako $z \notin \mathbb{Z}[\xi]$, $2 \nmid s$ u $\mathbb{Z}[\xi]$, tj. ako zapišemo $s = a + b\xi$, bar jedan od $a$ i $b$ je neparan. Imamo tri partikularna slučaja:

1. slučaj: $a$ je neparan i $b$ je paran. Tada je $s = 1 + (2a' + 2b'\xi)$, pa je $z = \frac{1}{2} + (a' + b'\xi)$, odakle je $z - (a' + b'\xi) = \frac{1}{2}$. Dakle, $|z - (a' + b'\xi)| = \frac{1}{4}$ što je stogo veće od nule i strogo manje od jedinice, i završili smo.

2. slučaj: $a$ je neparan i $b$ je neparan. Tada je $s = 1 + \xi + (2a' + 2b'\xi)$, pa je $z - (a' + b'\xi) = \frac{1+\xi}{2}$. Množenjem sa $\xi$ dobijamo $\xi z - \xi(a' + b'\xi) = \frac{\xi+\xi^2}{2} = \frac{2\xi-5}{2} = (\xi - 2) - \frac{1}{2}$. Dakle, $\xi z - [\xi(a' + b'\xi) - (\xi - 2)] = -\frac{1}{2}$, pa za $r = \xi$ i (novo) $s = \xi(a' + b'\xi) - (\xi - 2)$ dobijamo $0 < |rz - s| < 1$.

3. slučaj: $a$ je paran i $b$ je neparan. Tada je $s = \xi + (2a' + 2b'\xi)$, pa je $z - (a' + b'\xi) = \frac{\xi}{2}$. Množenjem sa $1 + \xi$ dobijamo $(1+\xi)z - (1+\xi)(a' + b'\xi) = \frac{\xi+\xi^2}{2} = \frac{2\xi-5}{2} = (\xi-2) - \frac{1}{2}$. ponovo, $(1+\xi)z - [(1+\xi)(a' + b'\xi) - (\xi-2)] = -\frac{1}{2}$, pa za $r = 1 + \xi$ i (novo) $s = (1 + \xi)(a' + b'\xi) - (\xi - 2)$ dobijamo $0 < |rz - s| < 1$.

Završili smo dokaz. □

Da bismo dokazali da je $\mathbb{Z}[\xi]$ PID koristićemo karakterizacu iz sledeće teoreme, ali prvo nam je potreban sledeći pojam.

**7/54 Definicija** (Dedekind–Haseova norma)**.** Neka je $D$ domen. Dedekind–Haseova norma na $D$ je preslikavanje $N : D \to \mathbb{N}$ koje zadovoljava:

- $N(x) = 0$ ako i samo ako $x = 0$;
- za sve $a, b \in D$, $a, b \neq 0$, važi:
  - $b \mid a$, ili
  - postoje $r, s \in D$ takvi da $0 < N(ra + sb) < N(b)$.

**7/55 Komentar.** Primetimo da ako $D$ ima euklidsku normu, onda ima i Dedekind–Haseovu normu. Neka je $N_e$ euklidska norma na $D$. Definišimo $N : D \to \mathbb{N}$ sa: $N(0) := 0$ i $N(x) := 2^{N_e(X)}$ za $x \neq 0$. Da bismo proverili da je $N$ Dedekind-Haseova norma, najpre jasno je da $N(x) = 0 \iff x = 0$, pa uzmimo nenula $a, b \in D$, i pretpostavimo $b \nmid a$. Zapišimo $a = bq + r$, gde, kako $b \nmid a$, $N_e(r) < N_e(b)$. Kako je $0 \leqslant N_e(r) < N_e(b)$, imamo $0 < 2^{N_e(R)} < 2^{N_e(b)}$, tj. $0 < N(r) < N(b)$, i kako je $r = a - qb = 1 \cdot a + (-q) \cdot b$, to je $0 < N(1 \cdot a + (-q) \cdot b) < N(b)$, i završili smo posao.

Dakle, euklidski domeni imaju Dedekind–Haseovu normu. Međutim, tačno je i više: domeni koju imaju Dedekind–Haseovu normu su tačno PID-ovi.

**7/56 Teorema.**
Neka je $D$ domen. Tada $D$ je PID ako i samo ako postoji Dedekind–Haseova norma na $D$.

*Dokaz.* ($\Rightarrow$) Neka je $D$ PID. Specijalno, $D$ je UFD, pa svaki nenula i neinvertibilan element $x$ ima prostu faktorizaciju, i broj prostih faktora $\#x$ je definisan. Definišimo $N : D \to \mathbb{N}$ sa:

- $N(0) := 0$;
- $N(x) := 2^{\#x}$ za $x \neq 0$.

(Ako promenimo definiciju 7/17 da definišemo $\#0 := -\infty$, onda je $N(x) = 2^{\#x}$ za sve $x \in D$.)

Dokazaćemo da je $N$ Dedekind–Haseova norma na $D$; jasno je $N(x) = 0 \iff x = 0$. Pretpostavimo $a, b \in D$, $a, b \neq 0$, i pretpostavimo $b \nmid a$. Neka je $c = nzd(a, b)$. Prema teoremi 7/42(6), $\langle a, b\rangle = \langle c\rangle$; odatle, $c = ra + sb$ za neke $r, s \in D$, i jasno $c \neq 0$. Kako $a \in \langle c\rangle \setminus \langle b\rangle$, to $\langle b\rangle \subsetneq \langle c\rangle$, pa $\#c < \#b$ prema komentaru 7/18. Odatle imamo $0 < N(c) < N(b)$, tj. $0 < N(ra + sb) < N(b)$, što dokazuje da je $N$ Dedekind–Haseova norma na $D$.

($\Leftarrow$) Neka je $N : D \to \mathbb{N}$ Dedekind–Haseova norma na $D$; dokazujemo da je $D$ PID. Dokaz je sličan dokazu teoreme 7/34. Neka je $I \lhd D$ pravi nenula ideal, i neka je $b \in I$ nenula element najmanje moguće norme. Tvrdimo $I = \langle b\rangle$, i dovoljno je da dokažemo $I \subseteq \langle b\rangle$. Neka je $a \in I$ nenula element. Ako $b \mid a$ završili smo posao, pa treba da eliminišemo slučaj $b \nmid a$. Ako $b \nmid a$, postoje $r, s \in D$ takvi da za $x = ra + sb$ važi $0 < N(x) < N(b)$. Kako jasno $x \in I$, kako $N(x) > 0$ povlači $x \neq 0$, i kako $N(x) < N(b)$, dobili smo kontradikciju sa izborom elementa $b$. Završili smo dokaz. □

Sada možemo da dokažemo:

**7/57 Tvrđenje.**
$\mathbb{Z}[\xi]$ je PID.

*Dokaz.* Dovoljno je da nađemo Dedekind–Haseovu normu na $\mathbb{Z}[\xi]$. Definišimo $N(a + b\xi) := a^2 + ab + 5b^2$. Kao i u mnogim ranijim sličnim primerima (npr. kod prstena Gausovih celih brojeva i Ajzenštajnovih celih brojeva) u pitanju je funkcija $N(z) = |z|^2$:

$$|a + b\xi|^2 = \left|\frac{2a + b}{2} + \frac{b\sqrt{19}}{2}i\right|^2 = \left(\frac{2a + b}{2}\right)^2 + \left(\frac{b\sqrt{19}}{2}\right)^2 = \frac{4a^2 + 4ab + b^2 + 19b^2}{4} = a^2 + ab + 5b^2.$$

Proveravamo da je $N$ Dedekind–Haseova norma na $\mathbb{Z}[\xi]$. Najpre, jasno $N(z) = |z|^2 = 0 \iff z = 0$. Proverimo drugi uslov. Neka su $z, w \in \mathbb{Z}[\xi]$ nenula elementi, i pretpostavimo $w \nmid z$. Posmatrajmo $\frac{z}{w} \in \mathbb{C}$; kako $w \nmid z$ u $\mathbb{Z}[\xi]$, $\frac{z}{w} \notin \mathbb{Z}[\xi]$. Prema lemi 7/53(b), postoje $r, s \in \mathbb{Z}[\xi]$ tako da $0 < |r\frac{z}{w} - s| < 1$. Odatle je $0 < |r\frac{z}{w} - s|^2 < 1$, pa je $0 < |r\frac{z}{w} - s|^2|w|^2 < |w|^2$, tj. $0 < |rz - sw|^2 < |w|^2$. Dakle, $0 < N(rz - sw) < N(w)$, i završili smo dokaz. □

**7/58 Zadatak.** Imajući u vidu lemu 7/53 i dokaz prethodnog tvrđenja, geometrijski objasniti zašto sa $N(z) = |z|^2$ nije definisana Dedekind–Haseova norma na $\mathbb{Z}[i\sqrt{3}]$. (Setimo se da $\mathbb{Z}[i\sqrt{3}]$ nije UFD, pa ni PID, pa svakako ne može da ima Dedekind–Haseovu normu.)

Dalje dokazujemo da $\mathbb{Z}[\xi]$ nije euklidski domen. Iskoristićemo sledeću lemu.

**7/59 Lema.**(a) $\mathbb{Z}[\xi]^\times = \{\pm 1\}$;

(b) 2 i 3 su nerastavljivi;

(c) ni 2 ni 3 ne deli nijedan od $\xi - 1$, $\xi$ i $\xi + 1$.

*Dokaz.* Setimo se da je za $a + b\xi \in \mathbb{Z}[\xi]$, $|a + b\xi|^2 = a^2 + ab + 5b^2$ (ovo smo videli u dokazu prethodnog tvrđenja).

(a) Neka je $a + b\xi$ invertibilan; tada postoji $x + y\xi$ tako da $(a + b\xi)(x + y\xi) = 1$. Uzimajući kvadrat modula dobijamo:

$$1 = |(a + b\xi)(x + y\xi)|^2 = |(a + b\xi)|^2|x + y\xi|^2 = (a^2 + ab + 5b^2)(x^2 + xy + 5xy^2).$$

Odavde je $a^2 + ab + 5b^2 = 1$. Ako je $b = 0$, mora biti $a = \pm 1$, odakle nalazimo dva invertibilna elementa $\pm 1$. Dovoljno je još da dokažemo da je $b \neq 0$ nemoguće. Zaista, imamo da je $1 = a^2 + ab + 5b^2 = (a + \frac{b}{2})^2 + \frac{19}{4}b^2 \geqslant 0 + \frac{19}{4}$ ako $b \neq 0$; kako $1 \not\geqslant \frac{19}{4}$, zaključujemo da ne može biti $b \neq 0$.

(b) Zapišimo $2 = (a + b\xi)(c + d\xi)$ i uzmimo kvadrat modula:

$$4 = (a^2 + ab + 5b^2)(c^2 + cd + 5d^2).$$

Ako je neka zagrada na desnoj strani jednaka 1, npr. $a^2+ab+5b^2=1$, kao u (a) zaključujemo $a+b\xi=\pm 1$ je invertibilan, što završava posao. Dakle, ostaje samo da eliminišemo slučaj da su obe zagrade u gornjem proizvodu jednake 2. Pretpostavimo $a^2+ab+5b^2=2$. Kao i u (a), kako je $a^2+ab+5b^2=(a+\frac{b}{2})^2+\frac{19}{4}b^2$ i kako je $\frac{19}{4}>2$, mora biti $b=0$, pa se jednakost svodi na $a^2=2$. Kako ova jednakost ne važi ni za jedno celo $a$, završili smo posao.

Na potpuno isti način vidimo da je 3 nerastavljiv.

(c) Ovo je očigledno. □

**7/60 Tvrđenje.**
$\mathbb{Z}[\xi]$ nije ED.

*Dokaz.* Pretpostavimo suprotno, $\mathbb{Z}[\xi]$ je euklidski domen sa normom $N$. Izaberimo $d\in\mathbb{Z}[\xi]\setminus(\mathbb{Z}[\xi]^\times\cup\{0\})$ minimalne moguće norme.

Prvo, primetimo da za svako $x\in\mathbb{Z}[\xi]$ važi bar jedno od $d\mid x-1$, $d\mid x$ i $d\mid x+1$. Zaista, kako je $\mathbb{Z}[\xi]$ euklidski, možemo da zapišemo $x=dq+r$ gde $r=0$ ili $N(r)<N(d)$. Po izboru $d$, $N(r)<N(d)$ znači $r\in\mathbb{Z}[\xi]^\times\cup\{0\}$, pa, imajući u vidu lemu 7/59(a), zaključujemo $r\in\{-1,0,1\}$. Dakle, važi bar jedno od $x=dq-1$, $x=dq$ i $x=dq+1$, odakle sledi željeno tvrđenje: važi bar jedno od $d\mid x-1$, $d\mid x$ i $d\mid x+1$.

Primenimo prethodni pasus na $x=2$; zaključujemo $d\mid 2-1=1$ ili $d\mid 2$ ili $d\mid 2+1=3$. Kako $d$ nije invertibilan, $d\mid 1$ je nemoguće. Kako su prema lemi 7/59(b), 2 i 3 nerastavljivi, $d\mid 2$ povlači $d\sim 2$, a $d\mid 3$ povlači $d\sim 3$; kako su prema lemi 7/59(a), $\pm 1$ jedini invertibilni, zaključujemo da je $d=-2$ ili $d=2$ ili $d=-3$ ili $d=3$.

Primenimo sada gornje zapažanje na $x=\xi$; zaključujemo $d\mid\xi-1$ ili $d\mid\xi$ ili $d\mid\xi+1$. Međutim, znajući da je $d=\pm 2$ ili $d=\pm 3$, nijedna opcija nije moguća prema lemi 7/59(c). Ova kontradikcija završava dokaz. □

# 8 Polja

Da podsetimo, polje je domen u kome su svi elementi invertibilni. S tim u vezi, jedini pravi ideal u polju je nula ideal. U analizi polja $F$, često će nam biti bitan prsten polinoma nad $F$, $F[X]$, pa ćemo da se podsetimo nekoliko njegovih osobina.

Najpre, $F[X]$ je ED (primer 7/29) u kome je norma data sa $N(p(X))=deg(p(X))$ za $p(X)\neq 0$. (Setimo se da $deg(0)$ ne definišemo, ili možemo da ga definišemo kao $deg(0)=-1$, ili kao $deg(0)=-\infty$.) To znači da za svaka dva polinoma $p(X),q(X)\in F[X]$, $q(X)\neq 0$, postoje polinomi $b(X),r(X)\in F[X]$ takvi da $p(X)=q(X)b(X)+r(X)$, i $r(X)=0$ ili $deg(r(X))<deg(q(X))$.

Kako je $F[X]$ ED, on je i PID (teorema 7/34), pa i UFD (teorema 7/39). Specijalno, to znači da se u $F[X]$ pojmovi prost i nerastavljiv element poklapaju (tvrđenje 7/10(e) i lema 7/37). Sa druge strane, polinom u $F[X]$ je nerastavljiv ako i samo ako je slabo nerastavljiv (komentar 7/24), pa dakle u $F[X]$ važi:

$$\text{prost polinom} = \text{nerastavljiv polinom} = \text{slabo nerastavljiv polinom}.$$

Takođe, svaki pravi nenula prost ideal je maksimalan (teorema 7/42), i obratno važi prema 6/42, pa u $F[X]$ važi:

$$\text{pravi nenula prost ideal} = \text{maksimalan ideal}.$$

Kako je $F[X]$ PID, svi ideali su glavni, pa su pravi nenula prosti ideali glavni ideali generisani prostim elementom (tvrđenje 7/10(d)). Prema svemu rečenom, prethodnoj jednakosti možemo da dodamo i:

$$\text{maksimalan ideal} = \langle\text{nerastavljiv polinom}\rangle.$$

## A Karakteristika polja

Podsetimo se da je polje domen u kome je svaki nenula element invertibilan.

Neka je $F$ polje. U primeru 6/27 videli smo da postoji jedinstveni homomorfizam prstena $\chi : \mathbb{Z} \to F$ koji je definisan sa $\chi(n) = n \cdot 1_F$. Prema prvoj teoremi o izomorfizmu, $\mathbb{Z}/ker(\chi) \cong im(\chi) \leqslant F$. Kako je $\mathbb{Z}/ker(\chi)$ izomorfan potprstenu polja $F$, u pitanju je domen, pa je $ker(\chi)$ prost ideal od $\mathbb{Z}$: dakle, $ker(\chi) = 0$ ili $ker(\chi) = p\mathbb{Z}$, gde je $p$ prost broj (ovo je bio zadatak 6/28). Definisali smo da je $char(F) = 0$ ako je $ker(\chi) = 0$, i $char(F) = p$ ako je $ker(\chi) = p$.

Ako je $ker(\chi) = 0$, tada je $\chi$ 1-1, pa vidimo da $F$ sadrži izomorfnu kopiju celih brojeva; u ovom slučaju, po definiciji $\chi$, konačni zbirovi $1_F$ nikada nisu jednaki nula. Dodatno, s obzirom da je $\mathbb{Z} \leqslant F$, i da u $F$ nenula elementi imaju inverze, direktno vidimo da je i $\mathbb{Q} \leqslant F$. Za $\mathbb{Q}$ kažemo da se prosto potpolje od $F$.

Sa druge strane, ako je $ker(\chi) = p\mathbb{Z}$, onda je $\mathbb{Z}/p\mathbb{Z}$ sadržano u $F$. Kako je $p$ prost, $p\mathbb{Z}$ je i maksimalan ideal od $\mathbb{Z}$, pa je $\mathbb{Z}/p\mathbb{Z}$ polje. U ovom slučaju kažemo da je $\mathbb{Z}/p\mathbb{Z}$ prosto potpolje od $F$. U ovom slučaju, po definiciji $\chi$, $p$ je najmanji pozitivan ceo broj za koji je $\underbrace{1_F + \cdots + 1_F}_{p} = 0_F$.

Da rezimiramo. Kada govorimo o polju $F$, uvek je slučaj da ono sadrži ili potpolje izomorfno sa $\mathbb{Q}$ ili potpolje izomorfno sa $\mathbb{Z}/p\mathbb{Z}$, $p$ je prost broj, i u oba slučaja je u pitanju potpolje generisano sa jedinicom.

**8/1 Tvrđenje.**
Neka je $F$ polje, $R$ prsten sa jedinicom i $\varphi : F \to R$ homomorfizam. Tada je $f$ monomorfizam.

*Dokaz.* Jezgro $ker(\varphi)$ je ideal od $F$, pa je ili $ker(\varphi) = 0$ ili $ker(\varphi) = F$, jer su ovo jedini ideali polja $F$. Kako je $\varphi(1) = 1$, $ker(\varphi) \neq F$, odakle preostaje samo da je $ker(\varphi) = 0$, tj. $\varphi$ je 1-1. □

**8/2 Tvrđenje.**
Neka je $\varphi : F \to E$ homomorfizam polja. Tada je $char(F) = char(E)$, i $\varphi$ je identiteta na prostom potpolju.

*Dokaz.* Prema prethodnom tvrđenju, $\varphi$ je 1-1. Neka je $\chi_F : \mathbb{Z} \to F$ dato sa $\chi_F(n) = n \cdot 1_F$ i $\chi_E : \mathbb{Z} \to E$ dato sa $\chi_E(n) = n \cdot 1_E$. S obzirom da je $\varphi$ homomorfizam, nije teško videti da je $\chi_E = \varphi \circ \chi_F$. Odatle je $\chi_E(x) = 0_E \iff \varphi(\chi_F(x)) = 0_E \iff \chi_F(x) = 0_F$ jer je $\varphi$ 1-1. Dakle, $ker(\chi_E) = ker(\chi_F)$, pa je $char(E) = char(F)$. Prema tome, $E$ i $F$ imaju isto prosto potpolje.

Primetimo da je $\varphi$ identiteta na $im(\chi_F)$; pod ovim mislimo da je $\varphi(n \cdot 1_F) = n \cdot 1_E$, što je očigledno. Prema tome, ako su $F$ (pa i $E$) proste karaketristike, $\varphi$ jeste identiteta na prostom potpolju od $F$. Ako su $F$ (i $E$) karakteristike nula, treba još da proverimo da je $\varphi(\frac{m \cdot 1_E}{n \cdot 1_E}) = \frac{m \cdot 1_E}{n \cdot 1_E}$, gde $n \neq 0$. Ovo sada direktno sledi iz $\varphi(\frac{m \cdot 1_E}{n \cdot 1_E}) = \varphi((m \cdot 1_F)(n \cdot 1_F)^{-1}) = \varphi(m \cdot 1_F)\varphi(n \cdot 1_F)^{-1} = (m \cdot 1_E)(n \cdot 1_E)^{-1} = \frac{m \cdot 1_E}{n \cdot 1_E}$. □

## B Raširenje polja

**8/3 Definicija.** Neka su $F$ i $E$ polja. Za $E$ kažemo da je raširenje polja $F$ ako je $F$ potpolje od $E$: $F \leqslant E$. Sa $E/F$ zapisujemo iskaz „$E$ je raširenje polja $F$".

**8/4 Tvrđenje** (Osnovna zapažanja o raširenju)**.**
Neka je $E/F$. Tada:

(a) $char(F) = char(E)$;

(b) $E$ je vektorski prostor nad poljem $F$ (u odnosu na sabiranje u $E$ i množenje u $E$ elementom iz $F$).

*Dokaz.* (a) Ako je $char(F) = 0$, onda $\mathbb{Q} \leqslant F$, pa kako $F \leqslant E$, to i $\mathbb{Q} \leqslant E$, odakle $char(E) = 0$. Ako je $char(F) = p$, onda $\mathbb{Z}_p \leqslant F$, pa opet kako $F \leqslant E$, to i $\mathbb{Z}_p \leqslant E$, odakle $char(E) = p$. Dakle, u svakom slučaju, $char(F) = char(E)$.

(b) Treba da proverimo da $E$ zadovoljava aksiome vektorskog prostora nad poljem $F$, a to znači:

- $E$ je Abelova grupa u odnosu na sabiranje, što jeste tačno;
- za $f \in F$ i $e \in E$, važi $fe \in E$, što takođe jeste tačno jer $F \subseteq E$;

- za $f, f' \in F$ i $e, e' \in E$ važe jednakosti: $f(f')e = (ff')e$, $1 \cdot e = e$, $f(e+e') = fe+fe'$ i $(f+f')e = fe+f'e$, što takođe jeste tačno zbog osobina množenja u $E$.

Dakle, direktno (i trivijalno), $E$ jeste vektorski prostor nad $F$. □

**8/5 Komentar.** Neka je $E/F$.

(a) Kako je $E$ vektorski prostor nad $F$, iz linearne algebre znamo da postoji baza $B \subseteq E$ za $E$ nad $F$.

(b) Podsetimo, ako je baza $B = \{b_1, b_2, \ldots, b_n\}$ konačna, biti baza znači:

- za svako $e \in E$ postoje koeficijenti $f_1, f_2, \ldots, f_n \in F$ takvi da $e = f_1b_1 + f_2b_2 + \cdots + f_nb_n$;

(uslov generatrise)

- ako za $f_1, f_2, \ldots, f_n \in F$, $f_1b_1 + f_2b_2 + \cdots + f_nb_n = 0$, onda je $f_1 = f_2 = \cdots = f_n = 0$.

(uslov linearne nezavisnosti)

Ekvivalentno, za svako $e \in E$ postoje jedinstveni koeficijenti $f_1, f_2, \ldots, f_n \in F$ takvi da $e = f_1b_1 + f_2b_2 + \cdots + f_nb_n$.

(c) Iz linearne algebre je manje poznato, pa naglasimo, ako je baza $B$ beskonačna, biti baza znači:

- za svako $e \in E$ postoji konačno mnogo $b_1, b_2, \ldots, b_n \in B$ i koeficijenti $f_1, f_2, \ldots, f_n \in F$ takvi da $e = f_1b_1 + f_2b_2 + \cdots + f_nb_n$ (dakle, svako $e \in E$ je generisano nad $F$ sa konačno mnogo elemenata baze);
- za proizvoljan izbor konačno mnogo $b_1, b_2, \ldots, b_n \in B$, ako za $f_1, f_2, \ldots, f_n \in F$, $f_1b_1 + f_2b_2 + \cdots + f_nb_n = 0$, onda je $f_1 = f_2 = \cdots = f_n = 0$ (dakle, svaki konačan podskup od $B$ je linearno nezavisan nad $F$).

(d) Iz linearne algebre takođe znamo da su svake dve baze jednake kardinalnosti, tj. da je dobro definisan pojam dimenzije: $dim_F(E) = |B|$.

**8/6 Definicija** (Stepen raširenja)**.** Neka je $E/F$. Stepen raširenja $E/F$ je $[E : F] := dim_F(E)$. Raširenje $E/F$ je konačno ako je $[E : F]$ konačan broj; u suprotnom je beskonačno.

**8/7 Primer.**(a) Označimo $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Nije teško videti da je $\mathbb{Q}[\sqrt{2}]$ potprsten od $\mathbb{C}$ (ili $\mathbb{R}$). Međutim, važi i više, u pitanju je potpolje. Ako je $a + b\sqrt{2} \neq 0$, onda je i $a - b\sqrt{2} \neq 0$ (Zašto?), pa racionalisanjem imamo:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

Dakle, $\mathbb{Q}[\sqrt{2}]$ sadrži i inverze, pa je polje.

Očigleno, $\mathbb{Q} \leqslant \mathbb{Q}[\sqrt{2}]$, pa posmatrajmo $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$. Iz same definicije se vidi da je $\{1, \sqrt{2}\}$ generatrisa za $\mathbb{Q}[\sqrt{2}]$ nad $\mathbb{Q}$. Da bismo videli da je ovo i baza, proverimo linearnu nezavisnost. Neka $a + b\sqrt{2} = 0$, $a, b \in \mathbb{Q}$. Ako je $b = 0$, direktno je $a = 0$, i završili smo. Ako je $b \neq 0$, onda je $\sqrt{2} = -\frac{a}{b} \in \mathbb{Q}$; kontradikcija.

Dakle, $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, i baza ovog raširenja je $\{1, \sqrt{2}\}$.

(b) Označimo $\mathbb{Q}[\sqrt[3]{2}] := \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$. Dokazaćemo da je $\mathbb{Q}[\sqrt[3]{2}]$ polje, takvo da $[\mathbb{Q}\sqrt[3]{2} : \mathbb{Q}] = 3$, i da je baza ovog raširenja $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.

Da je $\mathbb{Q}[\sqrt[3]{2}]$ Abelova grupa je prilično očigledno. Treba da dokažemo zatvorenost za množenje kako bismo dokazali da je prsten. Imamo:

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4})(x + y\sqrt[3]{2} + z\sqrt[3]{4}) = (ax + 2bz + 2cy) + (ay + bx + 2cz)\sqrt[3]{2} + (az + by + cx)\sqrt[3]{4} \in \mathbb{Q}[\sqrt[3]{2}],$$

pa je $\mathbb{Q}[\sqrt[3]{2}]$ zaista zatvoreno za množenje. Da bi smo dokazali da je polje, treba da dokažemo da je zatvoreno za inverze. Neka je $a+b\sqrt[3]{2}+c\sqrt[3]{4} \neq 0$. Želimo da dokažemo da postoji $x+y\sqrt[3]{2}+z\sqrt[3]{4} \in \mathbb{Q}[\sqrt[3]{2}]$ tako da $(a+b\sqrt[3]{2}+c\sqrt[4]{2})(x+y\sqrt[3]{2}+z\sqrt[3]{4}) = 1$. Imajući u vidu prethodni račun, dovoljno je da imamo $x, y, z \in \mathbb{Q}$ tako da $ax + 2bz + 2cy = 1$, $ay + bx + 2cz = 0$ i $az + by + cx = 0$. Ovo možemo da kažemo i na sledeći način: dovoljno je da sledeća matrična jednačina ima rešenje:

$$\begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Dakle, jasno je da je dovoljno (a što će se ispostaviti i potrebnim) da je matrica na levoj strani invertibilna. Ona je invertibilna ako i samo ako joj je determinanta $a^3 + 2b^3 + 4c^3 - 6abc \neq 0$.

Dakle, ima smisla da ispitamo racionalna rešenja jednačine $a^3 + 2b^3 + 4c^3 - 6abc = 0$. Jedno rešenje je naravno $(a, b, c) = (0, 0, 0)$; ovo zovemo trivijalno rešenje, i dokazaćemo da je ono i jedino rešenje. Pretpostavimo da postoji $(a, b, c)$ netrivijalno rešenje. Tada postoji i netrivijalno celobrojno rešenje, jer ako uzmemo $s$ za bude NZS imenilaca od $a$, $b$, $c$, množeći sa $s^3$ imamo $(sa)^3 + 2(bs)^3 + 4(sc)^2 - 6(sa)(sb)(sc) = 0$, pa je i $(sa, sb, sc)$ netrivijalno celobrojno rešenje.

Dakle, pretpostavimo da je $(a, b, c)$ netrivijalna celobrojna trojka takva da $a^3 + 2b^3 + 4c^3 - 6abc = 0$. Možemo da pretpostavimo da je $nzd(a, b, c) = 1$. Zaista, ako je $d = nzd(a, b, c)$, deleći sa $d^3$ dobijamo $(\frac{a}{d})^3 + 2(\frac{b}{d})^3 + 4(\frac{c}{d})^3 - 6\frac{a}{d}\frac{b}{d}\frac{c}{d} = 0$, pa imamo i celobrojno rešenje $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ za koje je NZD ovih brojeva jedan. Dakle, bez umanjenja opštosti, pretpostavimo da je $nzd(a, b, c) = 1$. Posmatrajmo sada jednakost:

$$a^3 + 2b^3 + 4c^3 - 6abc = 0.$$

Kako su poslednja tri sabirka parna, mora i $a^3$ da bude paran, pa i $a$ je paran: zapišimo $a = 2a'$. Vraćajući u jednakost imamo:

$$8a'^3 + 2b^3 + 4c^3 - 12a'bc = 0,$$

i deleći sa dva dobijamo:

$$4a'^3 + b^3 + 2c^3 - 6a'bc = 0.$$

Slično kao malopre, $b$ je parno, pa ako zapišemo $b = 2b'$, ubacimo u jednakost i podelimo sa dva dobijamo:

$$2a'^3 + 4b'^3 + c^3 - 6a'b'c = 0.$$

Odavde je i $c$ parno. Međutim, to je kontradikcija jer $nzd(a, b, c) = 1$ specijalno znači da ne mogu sva tri da budu parna.

Dakle, $(0, 0, 0)$ je jedino racionalno rešenje jednačine $a^3 + 2b^3 + 4c^3 - 6abc = 0$. Vraćajući se u polazni problem, gornja matrica ima inverz ako i samo ako determinanta $a^3 + 2b^3 + 4c^3 - 6abc \neq 0$, ako i samo ako $(a, b, c) \neq (0, 0, 0)$. Dakle, ako $a + b\sqrt[3]{2} + c\sqrt[3]{4} \neq 0$, specijalno $(a, b, c) \neq (0, 0, 0)$, pa prethodna analiza pokazuje da ovaj element ima inverz u $\mathbb{Q}[\sqrt[3]{2}]$.

Dakle, $\mathbb{Q}[\sqrt[3]{2}]$ jeste polje. Skup $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ očigledno je generatrisa za $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$. Da li je ovaj skup linearno nezavisan nad $\mathbb{Q}$? Ako je bar jedan koeficijent u linearnoj kombinaciji $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ nenula, onda, kao što smo videli, taj element ima inverz, pa je i sam nenula. Dakle, $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ je linearno nezavisan nad $\mathbb{Q}$. Prema tome u pitanju je baza, i odatle $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$.

Mi ćemo razviti teoriju koja će nam omogućiti da prethodne primer brže rešimo, ali do tada pokušajte da uradite sledeći zadatak direktno elementarnim metodama:

**8/8 Zadatak.** Dokazati da je $\mathbb{Q}[\sqrt[4]{2}] := \{a+b\sqrt[4]{2}+c\sqrt[4]{4}+d\sqrt[4]{8} \mid a, b, c, d \in \mathbb{Q}\}$ je polje, i $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}$ je raširenje stepena četiri sa bazom $\{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}\}$.

Osnovna osobina stepena raširenja je:

**8/9 Teorema** (Lančano pravilo)**.**
Neka je $F \leqslant E \leqslant K$ lanac polja (dakle, ovde imamo tri raširenja: $E/F$, $K/E$ i $K/F$).

(a) Ako je $B$ baza za $E/F$ i $C$ baza za $K/E$, onda je, onda je $BC := \{bc \mid b \in B,\ c \in C\}$ baza za $K/F$.

(b) $[K : F] = [K : E] \cdot [E : F]$.

Specijalno, $K/F$ je konačno ako i samo ako su $K/E$ i $E/F$ konačni, i tada $[K : E], [E : F] \mid [K : F]$.

*Dokaz.* (a) Da bismo dokazali da je $BC$ generatorni skup za $K/F$, uzmimo $k \in K$. Kako je $C$ baza za $K/E$, možemo zapisati $k = \sum_{i=1}^{n} e_i c_i$ za neke $e_i \in E$ i $c_i \in C$. Kako je $B$ baza za $E/F$, možemo zapisati $e_i = \sum_{j=1}^{m} f_{ij} b_j$ za neke $f_{ij} \in F$ i $b_j \in B$. Sada je:

$$k = \sum_{i=1}^{n} e_i c_i = \sum_{i=1}^{n} \left( \sum_{j=1}^{m} f_{ij} b_j \right) c_i = \sum_{i=1}^{n} \sum_{j=1}^{m} f_{ij} (b_j c_i).$$

Dakle, $k$ smo zapisali kao konačnu linearnu kombinaciju elemenata iz $BC$ sa koeficijentima iz $F$, što znači da je $BC$ generatorni skup za $K$ nad $F$.

Dalje treba da proverimo da su konačni podskupovi od $BC$ linearno nezavisni, pa uzmimo konačno mnogo elemenata iz $BC$. Možemo da pretpostavimo da smo uzeli $b_j c_i$ za sve $1 \leqslant j \leqslant m$ i $1 \leqslant i \leqslant n$. Pretpostavimo da je $\sum_{i=1}^{n} \sum_{j=1}^{m} f_{ij} (b_i c_j) = 0$. Ovu sumu možemo da zapišemo kao $\sum_{i=1}^{n} \left( \sum_{j=1}^{m} f_{ij} b_j \right) c_i = 0$, što je, primetićemo, linerna kombinacija $c$-ova nad $E$, odakle je zbog linearne nezavisnosti $C$ nad $E$, koeficijent $\sum_{j=1}^{m} f_{ij} b_j = 0$ za svako $i$. Poslednje je linearna kombinacija $b$-ova nad $F$, pa, za svako $i$, zbog linearne nezavisnosti $B$ nad $F$, $f_{ij} = 0$ za svako $j$. Dakle, svi koeficijenti su nula, pa zaključujemo da je $\{b_j c_i \mid j \leqslant m,\ i \leqslant n\}$ linearno nezavisan nad $F$.

(b) Uz oznake iz (a), po definiciji stepena, $[E : F] = |B|$, $[K : E] = |C|$, i, prema (a), $[K : F] = |BC|$. Dakle, treba samo proveriti da li je $|BC| = |B| \cdot |C|$. Dovoljno je da za različite parove $(b, c) \neq (b', c')$ važi $bc \neq b'c'$. Neka $(b, c) \neq (b', c')$. Ako je $c = c'$, onda je $b \neq b'$, pa je $bc \neq b'c'$ očigledno. Ako $c \neq c'$, onda $bc = b'c' \iff bc - b'c' = 0 \iff b = b' = 0$ zbog linearne nezavisnosti $C$ nad $E$; međutim kako $b, b'$ pripadaju bazi $B$ nad $F$, oni su nenula, pa ponovo zaključujemo $bc \neq b'c'$. □

**8/10 Zadatak.** Uraditi zadatak 8/8 koristeći prethodnu teoremu.
[*Uputstvo*: Uočiti lanac $\mathbb{Q} \leqslant \mathbb{Q}[\sqrt{2}] \leqslant \mathbb{Q}[\sqrt[4]{2}]$.]

## C Prosta raširenja polja

**8/11 Definicija** (Prosto raširenje)**.** Neka je $E/F$.

(a) Za $a \in E$, sa $F[a]$ označavamo najmanji potprsten od $E$ koji sadrži $F$ i $a$.

(b) Za $a \in E$, sa $F(a)$ označavamo najmanje potpolje od $E$ koje sadrži $F$ i $a$.

(c) Raširenje $E/F$ je prosto ako je $E = F(a)$ za neko $a \in E$. U tom slučaju kažemo da je $a$ primitivan element raširenja $E/F$.

Skupovi $F[a]$ i $F(a)$ imaju jednostavan opis:

**8/12 Tvrđenje.**
Neka je $E/F$ i $a \in E$. Tada:

(a) $F[a] = \{p(a) \mid p(X) \in F[X]\}$;

(b) $F(a) = \{\frac{p(a)}{q(a)} \mid p(X), q(X) \in F[X],\ q(a) \neq 0\}$.

*Dokaz.* (a) S obzirom da $F[a]$ sadrži i $F$ i $a$, i s obzirom da je $F[a]$ zatvoren za množenje i sabiranje, jasno je da $\{p(a) \mid p(X) \in F[X]\} \subseteq F[a]$. Sa druge strane, nije teško videti da $\{p(a) \mid p(X) \in F[X]\}$ jeste potprsten od $F$, pa kako je $F[a]$ najmanji potprsten od $F$ koji sadrži $F$ i $a$ zaključujemo da mora biti $F[a] = \{p(a) \mid p(X) \in F[X]\}$.
(b) Slično kao (a). □

**8/13 Definicija.** Neka je $E/F$ i $a \in E$.

(a) Element $a$ je algebarski nad $F$ ako postoji nenula polinom $p(X) \in F[X]$ takav da je $p(a) = 0$. U suprotnom, $a$ je transcendentan nad $F$.

(b) Ako je $a$ algebarski nad $F$, minimalan polinom za $a$ nad $F$ je nenula polinom $\mu_{a,F}(X) \in F[X]$ koji zadovoljava sledeće uslove:

- $\mu_{a,F}(a) = 0$;
- $\mu_{a,F}(X)$ je moničan (vodeći koeficijent je 1);
- $\mu_{a,F}(X)$ je nerastavljiv nad $F$.

**8/14 Tvrđenje.**
Neka je $E/F$ i $a \in E$ algebarski nad $F$. Tada:

(a) $\mu_{a,F}(X)$ postoji i jedinstven je;

(b) ako za $p(X) \in F[X]$ važi $p(a) = 0$, onda $\mu_{a,F}(X) \mid p(X)$;

(c) $F(a) = F[a]$;

(d) $\{1, a, a^2, \ldots, a^{n-1}\}$ je baza za $F(a)/F$, gde je $n = deg(\mu_{a,F})$;

(e) specijalno, $[F(a) : F] = deg(\mu_{a,F})$.

*Dokaz.* (a) Neka je $m(X) \in F[X]$ nenula polinom najmanjeg mogućeg stepena (recimo $n$) takav da $m(a) = 0$; primetimo da $m(X)$ postoji jer je $a$ algebarski element. Ako je $m_n$ vodeći koeficijent polinoma $m(X)$, zamenom $m(X)$ sa $\frac{1}{m_n}m(X)$, možemo da pretpostavimo da je $m(X)$ moničan polinom. Da bismo dokazali da je $m(X)$ minimalan za $a$ nad $F$, dovoljno je još da dokažemo da je $m(X)$ nerastavljiv nad $F$. Pretpostavimo $m(X) = p(X)q(X)$ gde su $p(X), q(X) \in F[X]$ nekonstantni polinomi. Kako je $0 = m(a) = p(a)q(a)$, mora biti $p(a) = 0$ i $q(a) = 0$. Kako su oba polinoma $p(X)$ i $q(X)$ stepena manjeg od $m(X)$, ovo je kontradikcija. Dakle, $m(X)$ je nerastavljiv. Ovime smo dokazali da minimalan polinom postoji.

Pre jedinstvenosti dokažimo (b). Neka je $p(X) \in F[X]$ takav da $p(a) = 0$. Kako je $F[X]$ euklidski domen, možemo da zapišemo $p(X) = m(X)q(X) + r(X)$ gde je $r(X) = 0$ ili $deg(r) < deg(m)$. Kako je $r(a) = p(a) - m(a)q(a) = 0 - 0 \cdot q(a) = 0$, po izboru $m(X)$ ne može biti $deg(r) < deg(m)$, pa zaključujemo $r(X) = 0$. Dakle, $p(X) = m(X)q(X)$, tj. $m(X) \mid p(X)$.

Vratimo se na jedinstvenost minimalnog polinoma. Neka je $m'(X) \in F[X]$ još jedan minimalan polinom za $a$ nad $F$. Kako je $m'(X) = 0$, prema prethodnom $m(X) \mid m'(X)$. Kako je $m'(X)$ nerastavljiv, $m(X) \sim m'(X)$; specijalno, $deg(m) = deg(m')$ jer $F[X]^\times = F \setminus \{0\}$. Kako su $m(X)$ i $m'(X)$ monični, mora biti $m'(X) = m(X)$.

(c) Jasno je da $F[a] \subseteq F(a)$, pa je potrebno da dokažemo obratnu inkluziju. Neka je $b \in F(a)$; tada je $b = \frac{p(a)}{q(a)}$, gde $p(X), q(X) \in F[X]$ i $q(a) \neq 0$. Neka je $d(X) = nzd(q(X), \mu_{a,F}(X))$ u $F[X]$. Zbog nerastavljivosti polinoma $\mu_{a,F}(X)$, ili je $d(X) = 1$ ili $d(X) = \mu_{a,F}(X)$; kako $q(a) \neq 0$ i $d(X) \mid q(X)$, vidimo da $d(X) \neq \mu_{a,F}(X)$. Dakle, $d(X) = 1$. Možemo da zapišemo $1 = d(X) = u(X)q(X) + v(X)\mu_{a,F}(X)$ za neke $u(X), v(X) \in F[X]$. Za $X = a$ dobijamo $1 = u(a)q(a)$. Sada je $b = \frac{p(a)}{q(a)} \cdot \frac{u(a)}{u(a)} = p(a)u(a) \in F[X]$, i završili smo dokaz.

(d) Neka je $n = deg(\mu_{a,F})$. Najpre primetimo da je $\{1, a, \ldots, a^{n-1}\}$ linearno nezavisan nad $F$. Zaista, ako je $\lambda_0 + \lambda_1 a + \cdots + \lambda_{n-1}a^{n-1} = 0$, gde $\lambda_i \in F$, dobijamo polinom $p(X) = \lambda_0 + \lambda_1 X + \cdots + \lambda_{n-1}X^{n-1} \in F[X]$ za koji je $p(a) = 0$, pa prema (b), $\mu_{a,F}(X) \mid p(X)$. Međutim kako je $p(X)$ stepena manjeg od $n$, mora biti $p(X) = 0$, tj. sve $\lambda$-e su nula.

Videli smo u (c) da je proizvoljan nenula element $x \in F(a)$ oblika $x = p(a)$ za neki $p(X) \in F[X]$. Ako zapišemo $p(X) = \mu_{a,F}(X)q(X) + r(X)$, gde $r(X) = 0$ ili $deg(r) < deg(\mu_{a,F}) = n$, dobijamo $x = p(a) = r(a)$.

Kako $x \neq 0$, $r(X) \neq 0$, pa je $deg(r) < n$. Iz $x = r(a)$ i $deg(r) < n$ sledi da je $x$ zapisan kao linearna kombinacija $\{1, a, \ldots, a^{n-1}\}$.

(e) Direktno iz (d). □

**8/15 Posledica.**
Neka je $F \leqslant K \leqslant E$ lanac polja, i $a \in E$ algebarski nad $F$. Tada:

(a) $a$ je algebraski nad $K$;

(b) $\mu_{a,K}(X) \mid \mu_{a,F}(X)$.

*Dokaz.* (a) je očigledno. Naime, $\mu_{a,F}(X) \in K[X]$ jer $F \leqslant K$, pa $a$ anulira bar jedan polinom ($\mu_{a,F}(X)$) nad $K$. Deo (b) sada sledi direktnom primenom prethodnog tvrđenja (b). □

**8/16 Primer.**
Posmatrajmo potpolje $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ od $\mathbb{C}$. (Po analogiji sa ranijim definicijama, mislimo na najmanje raširenje od $\mathbb{Q}$ koje sadrži $\sqrt{2}$ i $\sqrt{3}$.) Analizirajmo $F/\mathbb{Q}$.
Izračunajmo najpre $[F : \mathbb{Q}]$. Uočimo lanac polja: $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt{2}) \leqslant (\mathbb{Q}(\sqrt{2}))(\sqrt{3}) = F$. Primetimo da $\sqrt{2}$ zadovoljava polinom $X^2 - 2$ nad $\mathbb{Q}$. Da li je ovo $\mu_{\sqrt{2},\mathbb{Q}}(X)$? Pitanje je samo da li je rastavljiv nad $\mathbb{Q}$. I odgovor je: nije. Ovo možemo lako da vidimo na sledeći način. S obzirom da je u pitanju polinom drugog stepena, on je rastavljiv nad $\mathbb{Q}$ ako i samo ako je proizvod dva linearna polinoma nad $\mathbb{Q}$, ako i samo ako ima racionalnu nulu. Kako su nule od $X^2 - 2$ $\pm\sqrt{2}$, i kako znamo da $\sqrt{2}$ nije racionalan, zaključujemo da je $X^2 - 2$ nerastavljiv nad $\mathbb{Q}$, pa je $\mu_{\sqrt{2},\mathbb{Q}}(X) = X^2 - 2$. Primetimo još jedan način da zaključimo nerastavljivost $X^2 - 2$ nad $\mathbb{Q}$. Naime, kako je ovaj polinom moničan, on je i primitivan, pa po Gausovoj lemi je rastavljiv nad $\mathbb{Q}$ ako i samo ako je rastavljiv nad $\mathbb{Z}$. A za nerastavljivost nad $\mathbb{Z}$ možemo da iskoristimo Ajzenštajnov kriterijum: za prost broj 2 vidimo da 2 deli sve koeficijente polinoma $X^2 - 2$ osim najstarijeg, kao i da $4 = 2^2$ ne deli najmlađi koeficijent. U svakom slučaju, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = deg(X^2 - 2) = 2$. Takođe, $\{1, \sqrt{2}\}$ je baza za $\mathbb{Q}(\sqrt{2})$ nad $\mathbb{Q}$.
Da bismo izarčunali $[F : \mathbb{Q}]$, prema lančanom pravilu dovoljno je da izračunamo $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$. Za ovo nam je potreban $\mu_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(X)$. Jedan kandidat nam je svakako $X^2 - 3$. Ovaj polinom je nerastavljiv nad $\mathbb{Q}$ (isti argumenti kao u prethodnom pasus), međutim pitanje je da li je rastavljiv nad $\mathbb{Q}(\sqrt{2})$. S obzirom da je stepena 2, on je nerastavljiv nad $\mathbb{Q}(\sqrt{2})$ ako i samo ako nema koren u $\mathbb{Q}(\sqrt{2})$. Njegovi koreni su $\pm\sqrt{3}$, pa pitamo se da li $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$? Pretpostavimo da ovo jeste slučaj, i zapišimo $\sqrt{3}$ u bazi za $\mathbb{Q}(\sqrt{2})$ nad $\mathbb{Q}$: $\sqrt{3} = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$. Jasno $b \neq 0$ jer znamo $\sqrt{3} \notin \mathbb{Q}$. Kvadriranjem $\sqrt{3} - b\sqrt{2} = a$ dobijamo $3 + 2b^2 - 2b\sqrt{6} = a^2$, tj. $\sqrt{6} = \frac{3+2b^2-a^2}{2b} \in \mathbb{Q}$, što je kontradikcija. Dakle, $X^2 - 3$ jeste nerastavljiv nad $\mathbb{Q}(\sqrt{2})$, pa je $\mu_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(X) = X^2 - 3$, $\{1, \sqrt{3}\}$ je baza za $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ nad $\mathbb{Q}(\sqrt{2})$, i $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. Prema lančanom pravilu je $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$. Štaviše, baza za $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ nad $\mathbb{Q}$ dobija se množenjem baza u lancu, tj. $\{1, \sqrt{3}\} \cdot \{1, \sqrt{2}\} = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Dakle, elementi $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ na jedinstven način zapisuju se u obliku $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, gde $a, b, c, d \in \mathbb{Q}$.
Dokažimo i da je $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ prosto raširenje. Za to bi trebalo da nađemo neki primitivan element. I tvrdimo sledeće: $\alpha = \sqrt{2} + \sqrt{3}$ je primitivan element za $F/\mathbb{Q}$. Najpre, očigledno $\alpha \in F$, pa imamo lanac $\mathbb{Q} \leqslant \mathbb{Q}(\alpha) \leqslant F$. Probajmo da nađemo $\mu_{\alpha,\mathbb{Q}}(X)$. Kvadriranjem $\alpha = \sqrt{2} + \sqrt{3}$ dobijamo $\alpha^2 = 5 + 2\sqrt{6}$, odakle je $\alpha^2 - 5 = 2\sqrt{6}$, pa ponovnim kvadriranjem dobijamo $\alpha^4 - 10\alpha^2 + 25 = 24$, tj. $\alpha$ zadovoljava $X^4 - 10X^2 + 1 = 0$. Ovo nam je kandidat za minimalni polinom nad $\mathbb{Q}$. Pitanje je samo da li je nerastavljiv. Nažalost, Ajzenštajnov kriterijum nam ne pomaže, ali možemo da iskoristimo Gausovu lemu i da dokažemo da je nerastavljiv nad $\mathbb{Z}$. S obzirom da je polinom četvrtog stepena, ako je rastavljiv on je ili proizvod linearnog i kubnog polinoma, ili proizvod dva kvadratna polinoma. U oba slučaja možemo da pretpostavimo da je rastav moničan jer u proizvodu moraju da daju moničan polinom, a jedini načini da u proizvodu dobijemo 1 u $\mathbb{Z}$ su $1 = 1 \cdot 1 = (-1) \cdot (-1)$. Ako je $X^4 - 10X^2 + 1$ proizvod linearnog i kubnog moničnog polinoma nad $\mathbb{Z}$, on mora da ima celobrojnu nulu, kandidati su $\pm 1$, i vidimo da ovo nije slučaj. Ostaje da

dokažemo da $X^4 - 10X^2 + 1$ nije proizvod dva monična kvadratna polinoma nad $\mathbb{Z}$. Pretpostavimo:

$$X^4 - 10X^2 + 1 = (X^2 + aX + b)(X^2 + cX + d),\ a, b, c, d \in \mathbb{Z}.$$

Tada je $a + c = 0$, $b + d + ac = -10$, $ad + bc = 0$ i $bd = 1$. Dakle, $c = -a$, pa se druga jednakost svodi na $b + d - a^2 = -10$. Iz $bd = 1$ je $b = d = 1$ ili $b = d = -1$. U prvom slučaju $b + d - a^2 = -10$ postaje $a^2 = 12$, a u drugom $a^2 = 8$; u oba slučaja $a$ nije ceo broj. Ova kontradikcija završava dokaz nerastavljivosti.
Dakle, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = deg(X^4 - 10X^2 + 1) = 4$. Iz lančanog pravila na $\mathbb{Q} \leqslant \mathbb{Q}(\alpha) \leqslant F$ imamo: $[F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$, tj. $4 = [F : \mathbb{Q}(\alpha)] \cdot 4$, odakle je $[F : \mathbb{Q}(\alpha)] = 1$, tj. $F = \mathbb{Q}(\alpha)$.
U prethodnom postupku smo dokazali nerastavljivost $X^4 - 10X^2 + 1$ nad $\mathbb{Q}$, pa smo zaključili $F = \mathbb{Q}(\alpha)$. Mogli smo da dokažemo i $F = \mathbb{Q}(\alpha)$ direktno, pa da lančano pravilo iskoristimo kao dokaz nerastavljivosti. Naime, iz $\alpha = \sqrt{2} + \sqrt{3}$ imamo $\alpha - \sqrt{2} = \sqrt{3}$, odakle kvadriranjem dobijamo $\alpha^2 - 2\alpha\sqrt{2} + 2 = 3$, odakle $\sqrt{2} = \frac{\alpha^2 - 1}{2\alpha} \in \mathbb{Q}(\alpha)$. Sada i $\sqrt{3} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$, pa konačno i $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \leqslant \mathbb{Q}(\alpha)$. Kako smo već imali $\mathbb{Q}(\alpha) \leqslant \mathbb{Q}(\sqrt{2}, \sqrt{3})$, zaključujemo $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Imajući u vidu prvi deo analize, ovo znači $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, tj. minimalni polinom za $\alpha$ nad $\mathbb{Q}$ je stepena četiri. Kako je naš kandidat $X^4 - 10X^2 + 1$ stepena četiri, on mora biti željeni minimalni polinom (zbog jedinstvenosti minimalnog polinoma), što specijalno znači da je on nerastavljiv nad $\mathbb{Q}$.

**8/17 Primer.**
Neka je $\alpha = \sqrt[3]{7} + \sqrt[3]{49}$; analizirajmo raširenje $\mathbb{Q}(\alpha)/\mathbb{Q}$.
Odredimo prvo minimalni polinom za $\alpha$ nad $\mathbb{Q}$. Kubiranjem $\alpha = \sqrt[3]{7} + \sqrt[3]{49}$ dobijamo:

$$\alpha^3 = 7 + 3\sqrt[3]{7^2}\sqrt[3]{49} + 3\sqrt[3]{7}\sqrt[3]{49^2} + 49 = 56 + 21(\sqrt[3]{7} + \sqrt[3]{49}) = 56 + 21\alpha.$$

Dakle, $\alpha$ zadovoljava polinom $X^3 - 21X - 56$. Primetimo da ovaj polinom jeste nerastavljiv nad $\mathbb{Z}$ po Ajzenštajnovom kriterijumu za prost broj 7; prema Gausovoj lemi, on je nerastavljiv i nad $\mathbb{Q}$. Dakle, $\mu_{\alpha,\mathbb{Q}}(X) = X^3 - 21X - 56$. Odatle $\{1, \alpha, \alpha^2\}$ je baza za $\mathbb{Q}(\alpha)$ nad $\mathbb{Q}$, i $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.
Dokažimo da je $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{7})$. Jasno je da $\alpha \in \mathbb{Q}(\sqrt[3]{7})$, pa je $\mathbb{Q}(\alpha) \leqslant \mathbb{Q}(\sqrt[3]{7})$. Iz lančanog pravila imamo jednakost:

$$[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}(\alpha)] \cdot 3.$$

Nije teško videti da je i $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 3$: $\sqrt[3]{7}$ zadovoljava polinom $X^3 - 7$ nad $\mathbb{Q}$, i ovaj polinom jeste nerastavljiv nad $\mathbb{Q}$ prema Ajzenštajnovom kriterijumu (za prost broj 7) i Gausovoj lemi, tj. $\mu_{\sqrt[3]{7},\mathbb{Q}}(X) = X^3 - 7$. Dakle, $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}(\alpha)] = 1$, odakle sledi $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{7})$.
Primetimo da smo jednakost mogli da dokažemo i direktno, ali je račun malo nezgodniji. Na primer, kvadriranjem $\alpha = \sqrt[3]{7} + \sqrt[3]{49}$ dobijamo $\alpha^2 = \sqrt[3]{49} + 2 \cdot 7 + 7\sqrt[3]{7} = 14 + \alpha + 6\sqrt[3]{7}$, odakle je $\sqrt[3]{7} = \frac{\alpha^2 - \alpha - 14}{6} \in \mathbb{Q}(\alpha)$, pa je i $\mathbb{Q}(\sqrt[3]{7}) \leqslant \mathbb{Q}(\alpha)$.
Primetimo još da je $\mathbb{Q}(\sqrt[3]{7}) = \mathbb{Q}(\sqrt[3]{49})$. Ovo je zapravo lako: $\geqslant$ važi jer $\sqrt[3]{49} = (\sqrt[3]{7})^2 \in \mathbb{Q}(\sqrt[3]{7})$, a $\leqslant$ važi jer $\sqrt[3]{7} = \frac{(\sqrt[3]{49})^2}{7} \in \mathbb{Q}(\sqrt[3]{49})$.
Međutim, da smo direktno dokazivali $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{49})$, ponovo bismo mogli da primetimo $\alpha \in \mathbb{Q}(\sqrt[3]{49})$ (mada je to manje očigledno nego $\alpha \in \mathbb{Q}(\sqrt[3]{7})$), i da uočimo lanac $\mathbb{Q} \leqslant \mathbb{Q}(\alpha) \leqslant \mathbb{Q}(\sqrt[3]{49})$, pa da dokažemo $[\mathbb{Q}(\sqrt[3]{49}) : \mathbb{Q}] = 3$. Međutim, ovde bismo naišli na još jedan problem. Naime, $\sqrt[3]{49}$ zadovoljava polinoma $X^3 - 49$, čija nesvodljivost ne sledi direktno prema Ajzenštajnovom kriterijumu. Međutim, tada možemo da kažemo da polinom trećeg stepena jeste rastavljiv ako i samo ako ima racionalnu nulu, a kandidati za nju su $\pm 1$, $\pm 7$ i $\pm 49$; dakle, direktnim računom dobijamo nerastavljivost.
Ovde bi možda bilo manje zamorno direktno dokazati $\mathbb{Q}(\sqrt[3]{49}) \leqslant \mathbb{Q}(\alpha)$ (ostavljamo za vežbu).

**8/18 Primer.**
Neka je $F$ najmanje potpolje od $\mathbb{C}$ koje sadrži sve korene polinoma $X^3 - 5$ ($F$ se zove korensko polje polinoma $X^3 - 5$ nad $\mathbb{Q}$). Izračunati $[F : \mathbb{Q}]$.
Nađimo najpre sve korene polinoma $X^3 - 5$, tj. rešimo jednačinu $X^3 = 5$. Jedno rešenje svakako je $x_1 = \sqrt[3]{5}$.

Ako podelimo $X^3-5$ sa $X-\sqrt[3]{5}$ dobijamo:

$$X^3-5=(X-\sqrt[3]{5})(X^2+\sqrt[3]{5}X+\sqrt[3]{25}).$$

Preostala dva korena možemo da dobijemo iz formule za korene kvadratne funkcije:

$$x_{2,3}=\frac{-\sqrt[3]{5}\pm\sqrt{\sqrt[3]{25}-4\sqrt[3]{25}}}{2}=\frac{-\sqrt[3]{5}\pm\sqrt[3]{5}i\sqrt{3}}{2}=\sqrt[3]{5}\left(-\frac{1}{2}\pm i\frac{\sqrt{3}}{2}\right).$$

Dakle, željeno polje je $F=\mathbb{Q}(\sqrt[3]{5},\sqrt[3]{5}(-\frac{1}{2}+i\frac{\sqrt{3}}{2}),\sqrt[3]{5}(-\frac{1}{2}-i\frac{\sqrt{3}}{2}))$. Lako vidimo da je $F=\mathbb{Q}(\sqrt[3]{5},-\frac{1}{2}+i\frac{\sqrt{3}}{2},-\frac{1}{2}-i\frac{\sqrt{3}}{2})$; zaista, ovo sledi jer su polja zatvorena za množenje i deljenje (u konkretnom slučaju sa $\sqrt[3]{5}$). Odatle je dalje lako $F=\mathbb{Q}(\sqrt[3]{5},i\sqrt{3})$. Da bismo izračunali $[F:\mathbb{Q}]$, možemo da idemo na lančano pravilo na dva lanca: $\mathbb{Q}\leqslant\mathbb{Q}(\sqrt[3]{5})\leqslant F$ i $\mathbb{Q}\leqslant\mathbb{Q}(i\sqrt{3})\leqslant F$. Dobijamo:

$$[F:\mathbb{Q}]=deg(\mu_{\sqrt[3]{5},\mathbb{Q}})\cdot deg(\mu_{i\sqrt{3},\mathbb{Q}(\sqrt[3]{5})})\quad\text{i}\quad[F:\mathbb{Q}]=deg(\mu_{i\sqrt{3},\mathbb{Q}})\cdot deg(\mu_{\sqrt[3]{5},\mathbb{Q}(i\sqrt{3})}).$$

Direktno možemo da vidimo da je $\mu_{\sqrt[3]{5},\mathbb{Q}}(X)=X^3-5$ i $\mu_{i\sqrt{3},\mathbb{Q}}(X)=X^2+3$; nerastavljivost oba opravdava se Ajzenštajnovim kriterijumom. Sada možemo da nastavimo na dva načina.
Prvi način. Koristeći samo prvo navedeno lančano pravilo, dovoljno je da nađemo $\mu_{i\sqrt{3},\mathbb{Q}(\sqrt[3]{5})}(X)$. Kandidat je svakako i ovde $X^2+3$, pa se postavlja pitanje njegove nerastavljivosti nad $\mathbb{Q}(\sqrt[3]{5})$. S obzirom da je stepena dva, dovoljno je da vidimo da nema koren u $\mathbb{Q}(\sqrt[3]{5})$, i to zaista jeste tačno. Naime, koreni $\pm i\sqrt{3}$ od $X^2+3$ nisu realni, dok je polje $\mathbb{Q}(\sqrt[3]{5})$ očigledno potpolje od $\mathbb{R}$ (setimo se da je baza nad $\mathbb{Q}$ jednaka $\{1,\sqrt[3]{5},\sqrt[3]{25}\}$); dakle, $X^2+3$ nema korene u $\mathbb{Q}(\sqrt[3]{5})$, pa je nerastavljiv nad njim, i $\mu_{i\sqrt{3},\mathbb{Q}(\sqrt[3]{5})}(X)=X^2+3$. Korišćenjem prvog lančanog pravila dobijamo $[F:\mathbb{Q}]=3\cdot 2=6$.
Drugi način. Znamo da $\mu_{i\sqrt{3},\mathbb{Q}(\sqrt[3]{5})}(X)\mid\mu_{i\sqrt{3},\mathbb{Q}}(X)=X^2+3$, kao i $\mu_{\sqrt[3]{5},\mathbb{Q}(i\sqrt{3})}(X)\mid\mu_{\sqrt[3]{5},\mathbb{Q}}(X)=X^3-5$, pa imamo $deg(\mu_{i\sqrt{3},\mathbb{Q}(\sqrt[3]{5})})(X)\leqslant 2$ i $deg(\mu_{\sqrt[3]{5},\mathbb{Q}(i\sqrt{3})})(X)\leqslant 3$. Dakle, iz gornja dva lančana pravila imamo: $3\mid[F:\mathbb{Q}]$, $2\mid[F:\mathbb{Q}]$ i $[F:\mathbb{Q}]\leqslant 6$; sledi $[F:\mathbb{Q}]=6$.

**8/19 Komentar.** Iskoristimo priliku da kažemo nešto više o rešavanju jednačine $X^n=a$, $a\in\mathbb{C}$, $a\neq 0$. Pretpostavimo da je $x_0$ jedno rešenje. Tada sva rešenja možemo da opišemo sa: $x_0\xi$, gde je $\xi$ rešenje jednačine $X^n=1$. Zaista, ako je $x$ rešenje $X^n=a$ iz $x^n=a$ i $x_0^n=a$ sledi $(x/x_0)^n=1$, pa možemo da zapišemo $x=x_0(x/x_0)$ gde je $x/x_0$ rešenje $X^n=1$. Sa druge strane, ako je $\xi$ rešenje $X^n=1$, onda je $(x_0\xi)^n=x_0^n\xi^n=a\cdot 1=a$, tj. $x_0\xi$ je rešenje jednačine $X^n=a$. Dakle, ako imamo partikularno rešenje $x_0$, problem se svodi na rešavanje jednačine $X^n=1$.
Označimo sa $\omega_n=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$. Prema De Moavrovoj formuli znamo da je $\omega_n^k=\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}$ za svako $k=0,1,\ldots,n-1$ (i za druge $k$-ove, ali nas ovi zanimaju). Primetimo da su svi ovi elementi različiti (zato i uzimamo $k=0,1,\ldots,n-1$, od $n$ počinju periodično da se ponavljaju). Ponovo prema De Moavrovoj formuli imamo da je $(\omega_n^k)^n=\cos 2\pi k+i\sin 2\pi k=1$. Dakle, rešenja jednačine $X^n=1$ su $1=\omega_n^0,\omega_n,\omega_n^2,\ldots,\omega_n^{n-1}$. Prema tome, rešenja $X^n=a$ su $x_0,x_0\omega_n,x_0\omega_n^2,\ldots,x_0\omega_n^{n-1}$.
Korensko polje od $X^n-a$ nad $\mathbb{Q}$ stoga je $\mathbb{Q}(x_0,x_0\omega_n,x_0\omega_n^2,\ldots,x_0\omega_n^{n-1})=\mathbb{Q}(x_0,\omega_n)$ (poslednja jednakost lako se vidi). U prethodnom primeru je dakle $F=\mathbb{Q}(\sqrt[3]{5},\omega_3)$, gde je $\omega_3=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$. Ovo smo u primeru dobili direktno, ali sada znamo da ovakve primere možemo na sistematičniji način raditi.

## D Konstrukcije lenjirom i šestarom

U ovoj lekciji bavićemo se geometrijskim konstrukcijama (neoznačenim) lenjirom i šestarom iz algebarskog ugla. Geometrijske konstrukcije dešavaju se u realnoj ravni $\mathbb{R}^2$. Pretpostavljamo na početku da su nam date dve tačke $O=(0,0)$ i $E=(1,0)$ u ravni, odnosno da nam je poznata jedinična duž. Podrazumevamo da nam je iz geometrije poznato da su neke osnovne konstrukcije izvodive koristeći lenjir i šestar, kao npr. konstrukcija simetrale date duži, konstrukcija simetrale datog ugla, konstrukcija prave kroz tačku paralelna sa datom pravom, itd.

**8/20 Definicija.** Ako je $\mathcal{S} \subseteq \mathbb{R}^2$ skup tačaka, kažemo da je tačka $X$ *konstruktibilna u jednom koraku iz* $\mathcal{S}$ ako se $X$ može dobiti u preseku $\Phi_1$ i $\Phi_2$, gde je svaka od $\Phi_i$ jedna od sledećih figura:

- prava $AB$, gde $A, B \in \mathcal{S}$;
- krug sa centrom $C$ poluprečnika $AB$, gde $A, B, C \in \mathcal{S}$.

(Ako su nam tačke skupa $\mathcal{S}$ poznate (date ili već konstruisane), jasno je da prethodne figure možemo konstruisati lenjirom, odnosno šestarom.)

**8/21 Definicija.** Neka je $\mathcal{S} \subseteq \mathbb{R}^2$ skup tačaka, $X \in \mathbb{R}^2$ i $a \in \mathbb{R}^2$.

(a) Tačka $X$ je *konstruktibilna iz* $\mathcal{S}$ ako postoji konačan niz tačaka $X_1, X_2, \ldots, X_n = X$ takvi da je za svako $i \geqslant 1$ tačka $X_i$ konstruktibilna u jednom koraku iz $\mathcal{S} \cup \{X_j \mid j < i\}$.

(b) Tačka $X$ je *konstruktibilna* ako je konstruktibilna iz $\{O, E\}$.

(c) Broj $a$ je *konstruktibilan (iz* $\mathcal{S}$*)* ako je tačka $(a, 0)$ konstruktibilna (iz $\mathcal{S}$).

**8/22 Definicija.** Sa $\mathcal{K} \subseteq \mathbb{R}^2$ obeležavamo skup svih konstruktibilnih tačaka. Sa $K \subseteq \mathbb{R}$ obeležavamo skup svih konstruktibilnih brojeva.

Sledeća lema je laka:

**8/23 Lema.**
Tačka $(a, b)$ je konstsruktibilna akko su brojevi $a$ i $b$ konstruktibilni. □

Dakle:

**8/24 Posledica.**
$\mathcal{K} = K^2$. □

**8/25 Teorema.**
$K$ je prebrojivo potpolje od $\mathbb{R}$ koje sadrži $\mathbb{Q}$.

*Dokaz.* Dokaz da je $K$ polje (samim tim potpolje od $\mathbb{R}$, samim tim sadrži $\mathbb{Q}$) je lak. Treba da se proveri da za $a, b \in K$ važi $-a, a + b, ab \in K$, i ako $b \neq 1$ da $1/b \in K$. Ovo su sve jednostavne konstrukcije (neke koriste Talesovu teoremu).

Dokažimo da je $K$ prebrojiv; dovoljno je da dokažemo da je $\mathcal{K}$ prebrojiv. Označimo sa $\mathcal{K}_n$ skup svih tačaka koje su konstruktibilne u najviše $n$ koraka. Indukcijom po $n$ vidimo da je svaki od skupova $\mathcal{K}_n$ konačan. Zaista, za $n = 1$, iz skupa $\{O, E\}$ konstruktibilna je jedna prava i dva kruga, pa lako vidimo da u jednom koraku možemo da dobijemo samo četiri nove tačke, tj. $\mathcal{K}_1$ je konačan. Pretpostavimo da je $\mathcal{K}_n$ konačan sa $t$ tačaka. Tada tačke skupa $\mathcal{K}_n$ određuju najviše $\binom{t}{2}$ različitih pravih i najviše $t\binom{t}{2}$ različitih krugova. Kada sve ovo ispresecamo, vidimo da možemo da konstruišemo samo konačno mnogo novih tačaka u još jednom koraku, pa je $\mathcal{K}_{n+1}$ konačan. Kako je $\mathcal{K} = \bigcup_{n=1}^{\infty} \mathcal{K}_n$, $\mathcal{K}$ je prebrojiv unija konačnih skupova, dakle prebrojiv skup. □

**8/26 Definicija.** Polje $K$ naziva se *polje konstruktibilnih brojeva.*

**8/27 Posledica.**
Tačka $X$ je konstruktibilna akko je konstruktibilna iz skupa $\mathbb{Q}^2$.

*Dokaz.* Smer ($\Rightarrow$) je očigledan jer $O, E \in \mathbb{Q}^2$.

($\Leftarrow$) sledi jer $\mathbb{Q} \subseteq K$. Preciznije, pretpostavimo da je $X_1, X_2, \ldots, X_n = X$ niz tačaka koji svedoči da je $X$ konstruktibilna iz $\mathbb{Q}^2$. U konstrukciji svake tačke $X_i$ koristimo (možda) nekoliko tačaka iz $\mathbb{Q}^2$; pretpostavimo da za konstrukciju tačke $X_i$ koristimo $Y_{i,1}, \ldots, Y_{i,k_i} \in \mathbb{Q}^2$. Kako je $\mathbb{Q} \subseteq K$, za sve $i, j$ imamo niz $Z_{i,j,1}, \ldots, Z_{i,j,l_{i,j}} = Y_{i,j}$ koji svedoči da je $Y_{i,j}$ konstruktibilna iz $\{O, E\}$. Sada kada spojimo sve ove nizove i nadovežemo polazni niz jasno je da smo dobili niz koji svedoči da je $X$ konstruktibilna iz $\{O, E\}$. □

Kao još jednu posledicu prethodne teoreme imamo da „većina" tačaka u ravni zapravo nije konstruktibilna (s obzirom da je $K$ prebrojiv, a $\mathbb{R}$ neprebrojiv). Teorija polja nam omogućava da izvršimo i precizniju analizu (ne)konstruktibilnih brojeva.

**8/28 Lema.**
Neka je $F \leqslant \mathbb{R}$ i neka je tačka $X(a,b)$ konstruktibilna u jednom koraku iz $F^2$. Tada je $|F(a,b) : F| \leqslant 2$.

*Dokaz.* Treba da razmotrimo tri slučaja.

1. slučaj: tačka $X$ je u preseku pravih $AB$ i $CD$ gde $A, B, C, D \in F^2$. Jednačina prave $AB$ je:

$$(x_B - x_A)(y - y_A) = (y_B - y_A)(x - x_A),$$

pa kako $X \in AB$ imamo $(x_B - x_A)(b - y_A) = (y_B - y_A)(a - x_A)$, i slično $X \in CD$ povlači $(x_D - x_C)(b - y_C) = (y_D - y_C)(a - x_C)$, pa direktno vidimo da $a, b$ dobijamo kao rešenje $2 \times 2$ sistema linearnih jednačina sa koeficijentima u $F$, odakle $a, b \in F$, odakle $[F(a,b) : F] = 1$.

2. slučaj: tačka $X$ je u preseku prave $AB$ i kruga $k(C, DE)$, gde $A, B, C, D, E \in F^2$. Neka je $r$ dužina duži $DE$; primetimo $r^2 \in F$. Jednačina kruga je:

$$(x - x_C)^2 + (y - y_C)^2 = r^2,$$

a jednačina prave je $(x_B - x_A)(y - y_A) = (y_B - y_A)(x - x_A)$, pa $a, b$ dobijamo kao rešenja ovog sistema. Kako $A \neq B$, bez umanjenja opštosti pretpostavimo $x_A \neq x_B$. Tada jednačinu gornje prave možemo zapisati u obliku $y = \alpha x + \beta$, gde jasno $\alpha, \beta \in F$. Zamenom u jednačinu kruga dobijamo da $a$ zadovoljava polinom drugog stepena nad $F$, pa $[F(a) : F] \leqslant 2$, a kako je $b = \alpha a + \beta$, $[F(a,b) : F(a)] = 1$. Dakle, $[F(a,b) : F] = [F(a,b) : F(a)] \cdot [F(a) : F] \leqslant 2$.

3. slučaj: tačka $X$ je u preseku krugova $k_1(A, BC)$ i $k_2(P, QR)$, gde sve tačke pripadaju $F^2$. Neka su $r_1^2, r_2^2 \in F$ redom kvadrati dužina duži $BC$ i $QR$. Tada $a, b$ dobijamo rešavanjem sistema:

$$(x - x_A)^2 + (y - y_A)^2 = r_1^2,$$

$$(x - x_P)^2 + (y - y_P)^2 = r_2^2.$$

Oduzimanjem ove dve jednačine dobija se jednačina prave (radikalne ose ovih krugova) oblika $\alpha x + \beta y = \gamma$, gde $\alpha, \beta, \gamma \in F$, pa rešavamo sistem u kojem učestvuje jednačina prvog kruga i jednačina ove prave. Kao u drugom slučaju dobijamo $[F(a,b) : F] \leqslant 2$. □

**8/29 Lema.**
Ako je $[E : F] = 2$, tada je svaka tačka iz $E^2$ konstruktibilna iz $F^2$.

*Dokaz.* Neka je $X(a,b)$ tačka iz $E^2$; dovoljno je da dokažemo da su brojevi $a$ i $b$, tj. tačke $(a,0)$ i $(b,0)$ konstruktibilne iz $F^2$. Naravno, dokazujemo samo za $(a,0)$. Ako je $a \in F$, nemamo šta da dokazujemo, pa pretpostavimo $a \notin F$. Tada $F < F(a) \leqslant E$, pa iz $2 = [E : F] = [E : F(a)] \cdot [F(a) : F]$ i $[F(a) : F] > 1$ vidimo $E = F(a)$ i $[F(a) : F] = 2$, što znači da $a$ zadovoljava polinom $x^2 + \alpha x + \beta = 0$ nad $F$. Neka je $\alpha \neq 0$. Primetimo da tačka $(a,0)$ zadovoljava jednačinu:

$$(x + \frac{\alpha}{2})^2 + (y + \frac{\beta}{\alpha})^2 = (\frac{\alpha}{2} - \frac{\beta}{\alpha})^2.$$

Ovo je očigledno jednačina kruga $k(A, OB)$ gde $A(-\frac{\alpha}{2}, -\frac{\beta}{\alpha})$ i $B = (\frac{\alpha}{2} - \frac{\beta}{\alpha})$ su iz $F^2$. Dakle, $(a,0)$ dobijamo u preseku ovog kruga i prave $OE$, te je $(a,0)$ konstruktibilna.

Ako je gore $\alpha = 0$, tj. $a$ zadovoljava polinom $x^2 + \beta = 0$ nad $F$, tada $a+1$ zadovoljava polinom $x^2 - 2x + 1 + \beta = 0$ nad $F$, pa prema prethodnom pasusu $(a+1, 0)$ je konstruktibilna, a odatle i $(a,0)$. □

**8/30 Teorema.**
Neka je $F \leqslant \mathbb{R}$. Tačka $X(a,b)$ je konstruktibilna iz $F^2$ akko postoji niz polja $F = F_0 \leqslant F_1 \leqslant \cdots \leqslant F_n$ takvih da $[F_{i+1} : F_i] = 2$ za sve $i < n$ i $a, b \in F_n$.

*Dokaz.* ($\Rightarrow$) Neka je $X_1, X_2, \ldots, X_n = X$ niz tačaka preko kojih vršimo konstrukciju tačke $X$ iz $F^2$; neka je $X_i(a_i, b_i)$. Ako stavimo $F_0 = F$ i $F_{i+1} = F_i(a_{i+1}, b_{i+1})$ direktno prema lemi 8/28 dobijamo niz polja $F = F_0 \leqslant F_1 \leqslant \cdots \leqslant F_n$ takvih da $[F_{i+1} : F_i] \leqslant 2$ i $a, b \in F_n$. Ako izbacimo iz niza nepotrebna ponavljanja dobijamo novi niz u kome je $[F_{i+1} : F_i] = 2$ za sve $i < n$.

($\Leftarrow$) Pretpostavimo da imamo niz polja $F = F_0 \leqslant F_1 \leqslant \cdots \leqslant F_n$ takvih da $[F_{i+1} : F_i] = 2$ za sve $i < n$ i $a, b \in F_n$. Prema lemi 8/29, $X$ je konstruktibilno iz $F_{n-1}^2$. Svaka tačka iz $F_{n-1}^2$ potrebna za konstrukciju $X$ je, ponovo prema lemi 8/29, konstruktibilna iz $F_{n-2}^2$, itd. Dakle, $X$ je konstruktibilna iz $F^2$. □

**8/31 Posledica** (Potreban uslov za konstruktibilnost iz $F^2$).
Ako je tačka $X(a,b)$ konstruktibilna iz $F^2$, onda je $[F(a,b) : F] = 2^n$ za neko $n \in \mathbb{N}$.

*Dokaz.* Prema prethodnoj teoremi možemo da nađemo niz polja $F = F_0 \leqslant F_1 \leqslant \cdots \leqslant F_n$ takvih da $[F_{i+1} : F_i] = 2$ za sve $i < n$ i $a, b \in F_n$. Primetimo da je $[F_n : F] = 2^n$ i da je $F \leqslant F(a,b) \leqslant F_n$, pa je po lančanom pravilu $[F(a,b) : F] = 2^m$ za neko $m \leqslant n$. □

Imajući u vidu posledicu 8/27 direktno izvodimo:

**8/32 Posledica** (Potreban i dovoljan uslov za konstruktibilnost).(a) Tačka $X(a,b)$ je konstruktibilna akko postoji niz polja $\mathbb{Q} = F_0 \leqslant F_1 \leqslant \cdots \leqslant F_n$ takvi da $[F_{i+1} : F_i] = 2$ za sve $i < n$ i $a, b \in F_n$.

(b) Broj $a$ je konstruktibilan akko postoji niz polja $\mathbb{Q} = F_0 \leqslant F_1 \leqslant \cdots \leqslant F_n$ takvi da $[F_{i+1} : F_i] = 2$ za sve $i < n$ i $a \in F_n$. □

**8/33 Posledica** (Potreban uslov za konstruktibilnost).

(a) Ako je tačka $X(a,b)$ konstruktibilna onda je $[\mathbb{Q}(a,b) : \mathbb{Q}] = 2^n$ za neko $n \in \mathbb{N}$.

(b) Ako je broj $a$ konstruktibilan onda je $[\mathbb{Q}(a) : \mathbb{Q}] = 2^n$ za neko $n \in \mathbb{N}$. □

**8/34 Primer** (Duplikacija kocke je nemoguća).
Problem duplikacije kocke je sledeći. Ako nam je data kocka stranice 1, konstruisati kocku duplo veće zapremine. Dakle, treba da konstruišemo duž dužine $\sqrt[3]{2}$. Ovo nije moguće prema posledici 8/33 jer $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

**8/35 Primer** (Kvadratura kruga je nemoguća).
Problem kvadrature kruga je sledeći. Ako nam je dat krug poluprečnika 1, konstruisati kvadrat jednake površine. Dakle, treba da konstruišemo kvadrat površine $\pi$, tj. stranice $\sqrt{\pi}$. Ovo nije moguće prema posledici 8/33 jer $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$ jer je $\pi$ transcendentan broj.

**8/36 Primer** (Tricekcija ugla je nemoguća).
Problem trisekcije ugla je sledeći. Za zadati ugao konstruisati ugao jednak njegovoj trećini. Dokazaćemo da ugao od $20^\circ$ nije konstruktibilan, pa trisekcija ugla od $60^\circ$ nije moguća. Očigledno, ugao od $20^\circ$ je konstruktibilan akko i samo ako je konstruktibilan $\cos 20^\circ$. Primetimo:

$\cos 60^\circ + i \sin 60^\circ = (\cos 20^\circ + i \sin 20^\circ)^3 =$

$$= (\cos^3 20^\circ - 3\cos 20^\circ \sin^2 20^\circ) + i(3\cos^2 20^\circ \sin 20^\circ - \sin^3 20^\circ),$$

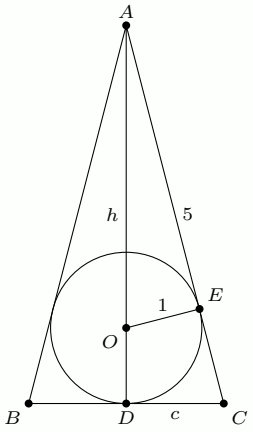
pa je $\frac{1}{2} = \cos 60^\circ = \cos^3 20^\circ - 3\cos 20^\circ(1 - \cos^2 20^\circ) = 4\cos^3 20^\circ - 3\cos 20^\circ$. Dakle, $\cos 20^\circ$ zadovoljava polinom $x^3 - \frac{3}{4}x - \frac{1}{8} = 0$. Ovaj polinom nema racionalan koren (direktna provera svih mogućnosti), pa je nerastavljiv nad $\mathbb{Q}$, odakle $[\mathbb{Q}(\cos 20^\circ) : \mathbb{Q}] = 3$, pa $\cos 20^\circ$ nije konstruktibilan prema posledici 8/33.

**8/37 Lema.**
Ugao od $n^\circ$, $n \in \mathbb{N}$, je konstuktibilan akko $3 \mid n$.

*Dokaz.* Prema prethodnom primeru uglovi od $1^\circ$ i $2^\circ$ ne mogu biti konstruktibilni (u suprotnom, dovoljnim brojem nadovezivanja konstruisali bismo ugao od $20^\circ$). Iz geometrije znamo da je pravilan petougao konstruktibilan, pa je konstruktibilan njegov centralni ugao od $72^\circ$. Ako oduzmemo konstruktibilan ugao od $60^\circ$, dobijamo da je ugao od $12^\circ$ konstruktibilan. Polovljenjem dva puta konstruišemo ugao od $3^\circ$. Dakle, ugao od $1^\circ$ i $2^\circ$ nisu, a ugao od $3^\circ$ jeste konstruktibilan. Sada tvrđenje leme direktno sledi. □

**8/38 Primer.**
Konstrukcija pravilnog 9-tougla je nemoguća. U suprotnom konstruisali bismo i njegov centralni ugao od $40^\circ$, a $3 \nmid 40$. (Ili bismo polovljenjem dobili ugao od $20^\circ$, a videli smo da je to nemoguće.)

**8/39 Primer.**
U opštem slučaju nije moguće konstruisati jednakokraki trougao ako su dati krak $b$ i poluprečnik upisanog kruga $r$. Dokažimo da jednakokraki trougao čiji je krak $b = 5$ i poluprečnik upisanog kruga $r = 1$ nije konstruktibilan. (Treba naglasiti da ovaj trougao zaista postoji.) Pogledajmo sliku:




Iz $\triangle ADC \sim \triangle AEO$ imamo $\frac{AC}{DC} = \frac{AO}{EO}$, tj. $\frac{b}{c} = \frac{h-r}{r}$, tj. $\frac{5}{c} = h - 1$, odakle je $c = \frac{5}{h-1}$. Po Pitagorinoj teoremi je $h^2 + c^2 = b^2$, pa je $h^2 + \frac{25}{(h-1)^2} = 25$, odnosno $h^2(h-1)^2 - 25(h-1)^2 + 25 = 0$. Sređivanjem dobijamo da $h$ zadovoljava polinom $x^3 - 2x^2 - 24x + 50 = 0$, koji je po Ajzenštajnovom kriteriju nerastavljiv. Dakle, $|\mathbb{Q}(h) : \mathbb{Q}| = 3$, pa visina $h$ nije konstruktibilan broj prema posledici 8/33, pa ni trougao ne može biti konstruktibilan.

Za kraj bez dokaza navodimo i sledeću teoremu:

**8/40 Teorema.**
Pravilan $n$-tougao je konstruktibilan akko $n = 2^k p_1 p_2 \dots p_m$, gde $k, m \geqslant 0$ i $p_1, \dots, p_m$ su različiti Fermaovi prosti brojevi (prosti brojevi oblika $2^{2^l} + 1$, gde $l \in \mathbb{N}$). □