Algebra 2 – radna verzija skripte

Slavko Moconja

2024/25.

Sadržaj

I Dejstvo grupe na skup

A Definicija, primeri, osnovne osobine

I–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 $G \rightharpoondown X$.

I–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 $g \cdot x$:

$$x \xrightarrow{g} g \cdot x$$

Tada aksiome možemo predstaviti na sledeći način:

$$
\begin{tikzcd}
x \arrow[loop above, "e"]
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
x \arrow[r, "h"] \arrow[rr, bend right, "gh"'] & h \cdot x \arrow[r, "g"] & g \cdot (h \cdot x) = (gh) \cdot x
\end{tikzcd}
$$

(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.

I–3 Primer. Neka je $G = \mathbb{S}_n$ i $X = [n] = \{1, 2, \dots, n\}$. Imamo prirodno dejstvo $\mathbb{S}_n \curvearrowright [n]$ dato sa $\sigma \cdot i := \sigma(i)$.

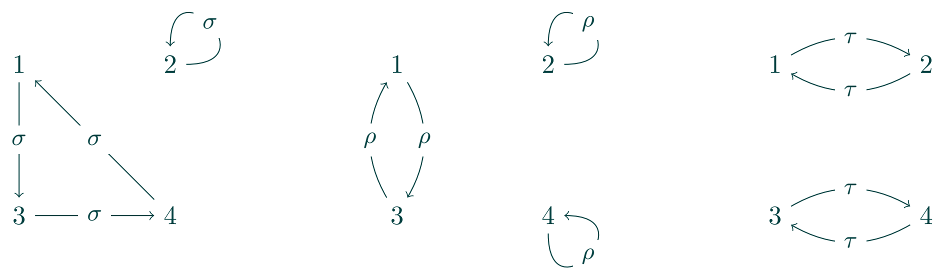
Proverimo aksiome dejstva:

(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 σ 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, $\sigma \cdot \{i, j\} \in [[n]]^2$.

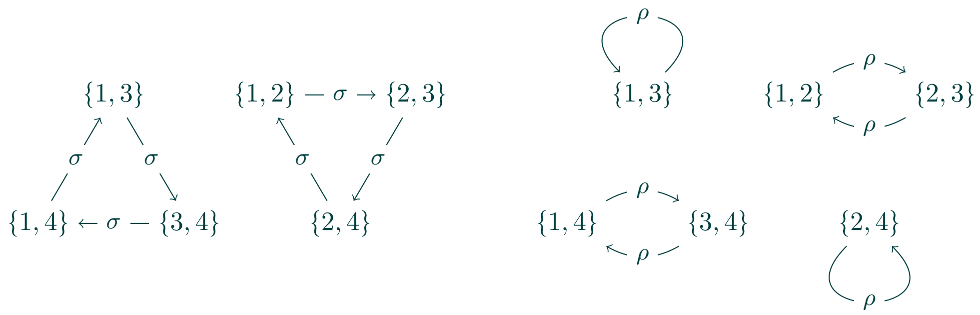
(d1) $[] \cdot \{i, j\} = \{[](i), [](j)\} = \{i, j\}$;

(d2) $\sigma \cdot (\tau \cdot \{i, j\}) = \sigma \cdot \{\tau(i), \tau(j)\} = \{\sigma(\tau(i)), \sigma(\tau(j))\} = \{\sigma \circ \tau(i), \sigma \circ \tau(j)\} = (\sigma \circ \tau) \cdot \{i, j\}$.

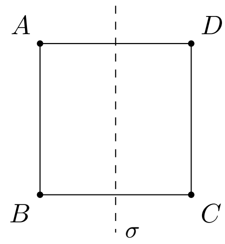
Pogledajmo slučaj $\mathbb{S}_4 \curvearrowright [[4]]^2$, i nacrtajmo dejstva permutacija $\sigma = [134]$ i $\rho = [13]$.

Najpre primetimo da je $[[4]]^2 = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$.

Po definiciji $[134] \cdot \{1, 2\} = \{[134](1), [134](2)\} = \{3, 2\}$, i na sličan način vidimo da su odgovarajauća dejstva data sa:



I–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 ρ za 90° oko centra kvadrata u pozitivnom smeru i bilo kojom osnom simetrijom σ, npr. u odnosu na vertikalnu osu:



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

$$
\begin{tikzcd}
A \arrow[d, "\rho"] & D \arrow[l, "\rho"'] \\
B \arrow[r, "\rho"] & C \arrow[u, "\rho"]
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, bend left, "\sigma"] & D \arrow[l, bend left, "\sigma"] \\
B \arrow[r, bend left, "\sigma"] & C \arrow[l, bend left, "\sigma"]
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[loop left, "\rho\sigma"] & D \arrow[dl, bend left, "\rho\sigma"] \\
B \arrow[ur, bend left, "\rho\sigma"] & C \arrow[loop right, "\rho\sigma"]
\end{tikzcd}
$$

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

$$
\begin{tikzcd}
AC \arrow[r, bend left, "\rho"] & BD \arrow[l, bend left, "\rho"]
\end{tikzcd}
\qquad
\begin{tikzcd}
AC \arrow[r, bend left, "\sigma"] & BD \arrow[l, bend left, "\sigma"]
\end{tikzcd}
\qquad
\begin{tikzcd}
AC \arrow[loop left, "\rho\sigma"]
\end{tikzcd}
\qquad
\begin{tikzcd}
BD \arrow[loop right, "\rho\sigma"]
\end{tikzcd}
$$

I–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) $g \cdot (h \cdot x) = g \cdot (hx) = g(hx) = (gh)x = (gh) \cdot x$.

I–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: $aH = bH \iff a^{-1}b \in H$.

I–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) $g \cdot (h \cdot aH) = g \cdot (ha)H = (g(ha))H = ((gh)a)H = (gh) \cdot aH$.

I–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 I–6.

I–9 Primer. Za $\sigma \in \mathbb{S}_n$ i $(x_1, x_2, \dots, x_n) \in \mathbb{R}^n$ definišimo: $\sigma \cdot (x_1, x_2, \dots, x_n) := (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$.

Proverimo aksiome dejstva:

(d1) $[] \cdot (x_1, x_2, \dots, x_n) = (x_{[](1)}, x_{[](2)}, \dots, x_{[](n)}) = (x_1, x_2, \dots, x_n)$.

(d2) Neka su $\sigma, \tau \in \mathbb{S}_n$:

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

I–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 $\sigma \cdot (x_1, x_2, \dots, x_n) := (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \dots, x_{\sigma^{-1}(n)})$ jeste definisano $\mathbb{S}_n \curvearrowright \mathbb{R}^n$.

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

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

gde $i + k$ računamo u $\mathbb{Z}_n$ (sabiramo modulo n).

Proverimo aksiome dejstva:

(d1) $0 \cdot (x_0, x_1, \dots, x_{n-1}) = (x_{0+0}, x_{1+0}, \dots, x_{(n-1)+0}) = (x_0, x_1, \dots, x_{n-1})$;

(d2)

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

I–12 Primer. Neka je G grupa i $X = \{(g_0, g_1, \dots, g_{n-1}) \in G^n \mid g_0 g_1 \dots g_{n-1} = e\}$. 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 $(g_0, g_1, \dots, g_{n-1}) \in X$, $k \cdot (g_0, g_1, \dots, g_{n-1}) \in X$. Iz $(g_0, g_1, \dots, g_{k-1}, g_k, g_{k+1} \dots, g_{n-1}) \in X$ imamo $g_0 g_1 \dots g_{k-1} g_k g_{k+1} \dots g_{n-1} = e$. Odavde, množenjem sa $(g_k g_{k+1} \dots g_{n-1})^{-1}$ zdesna, dobijamo $g_0 g_1 \dots g_{k-1} = (g_k g_{k+1} \dots g_{n-1})^{-1}$, pa množenjem sa $g_k g_{k+1} \dots g_{n-1}$ sleva zaključujemo $g_k g_{k+1} \dots g_{n-1} g_0 g_1 \dots g_{k-1} = e$. Dakle, $k \cdot (g_0, g_1, \dots, g_{n-1}) = (g_k, g_{k+1}, \dots, g_{n-1}, g_0, g_1, \dots, g_{k-1}) \in X$. 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 $(g_0, g_1, \dots, g_{n-1}) \mapsto (g_1, \dots, g_{n-1})$; dokazaćemo da je u pitanju bijekcija. Preslikavanje je „na" jer za proizvoljno $(g_1, \dots, g_{n-1}) \in G^{n-1}$ imamo $g_0 g_1 \dots g_{n-1} = e$ za $g_0 = (g_1, \dots, g_{n-1})^{-1}$, pa $(g_0, g_1, \dots, g_{n-1}) \in X$ i $(g_0, g_1, \dots, g_{n-1}) \mapsto (g_1, \dots, g_{n-1})$. Ako $(g_0, g_1, \dots, g_{n-1}), (g_0', g_1, \dots, g_{n-1}) \in X$, 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".

I–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 korisimo (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 $g \cdot (h \cdot f) = (gh) \cdot f$.

I–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 σ je inverzno preslikavanje σ^{-1}. (**Komentar.** $Sym([n]) = \mathbb{S}_n$.)

I–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) δ_g je „1-1". Kako smo već videli $x = g \cdot (g^{-1} \cdot x) = \delta_g(g^{-1} \cdot x)$; δ_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). □

I–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

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

I–18 Definicija. Neka $G \rightharpoonup X$ i neka je $\delta : G \to Sym(X)$ pridruženi homomorfizam. Definišemo:

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

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

I–19 Komentar. (a) Prema prvoj teoremi o izomorfizmu imamo:

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

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

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

Navešćemo nekoliko primera primene gornje formule na različita dejstva.

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

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

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

Dakle, $G \leqslant Sym(G)$. □

I–21 Teorema. $G/Z(G) \cong Inn(G)$.

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

I–22 Definicija. Neka je $H \leqslant G$. Jezgro podgrupe H je:

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

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

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

I–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 zaključujemo $Core(H) \leqslant H$. 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.

I–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 $H \lhd G$. $\square$

C Orbite i stabilizatori

I–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]

I–27 Primer. Neka je $G \curvearrowright G$ dejstvo grupe na sebe množenjem sleva iz primera I–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. $G_x = \{e\}$.

I–28 Primer. Neka je $G \curvearrowright G$ dejstvo grupe na sebe konjugacijom iz primera I–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.

I–29 Primer. Neka je $H \leqslant G$, $G \curvearrowright G/H$ dejstvo grupe na kosetima iz primera I–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. $G_{aH} = aHa^{-1}$.

I–30 Primer. Neka je $G \curvearrowright Sub(G)$ dejstvo na podgrupa konjugacijom iz primera I–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.

I–31 Primer. Neka je S skup i $\mathbb{Z}_4 \curvearrowright S^4$ dejstvo iz primera I–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 $0 \cdot (x, y, y, y) = (x, y, y, y)$, $1 \cdot (x, y, y, y) = (y, y, y, x)$, $2 \cdot (x, y, y, y) =$

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

(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 $(\mathbb{Z}_4)_{(x_0,x_1,x_2,x_3)}=\{0\}$.

I–32 Primer. Neka je p prost broj, S skup i $\mathbb{Z}_p\rightharpoondown S^p$ kao u primeru I–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. Pretpostavimo 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 α_p ostatak pri deljenju α 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 α_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 I–12.

I–33 Tvrđenje. Neka $G\rightharpoondown X$, $a\in G$ i $x\in X$.

(a) $G_x\leqslant G$;

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

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

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

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

I–34 Teorema (Orbita–stabilizator teorema)**.** Neka $G\rightharpoondown X$ 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. □

I–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:

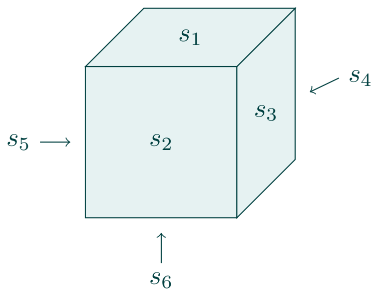
$$|H \times K| = |(H \times K) \cdot e| \cdot |(H \times K)_e| \implies |H| \cdot |K| = |HK| \cdot |H \cap K|,$$

odakle sledi gornja formula.

I–36 Primer. Izračunati koliko grupa prostornih rotacija (bez refleksija) kocke ima elemenata.

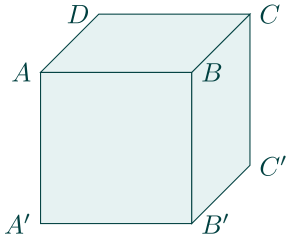
Neka je G grupa o kojoj govorimo. Možemo da rešimo ovaj problem na više načina.

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, $Ker(G \rightharpoonup D)$ je trivijalna. Kako je $G \cong G/Ker(G \rightharpoonup D) \cong Im(G \rightharpoonup D) \leqslant Sym(D) \cong \mathbb{S}_4$, i kako $|G| = |\mathbb{S}_4| = 24$, zaključujemo $G \cong \mathbb{S}_4$.

I–37 Zadatak. Izračunati broj svih izometrija kocke.

I–38 Teorema. Neka $G \rightharpoonup X$. 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 I–38 orbite dejstva $G \rightharpoonup X$ čine particiju skupa X. Ako su x_i, $i \in I$, predstavnici svih orbita (iz svake orbite smo izabrali po jedan element), onda imamo:

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

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

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

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 $G \rightharpoonup X$.

I–39 Primer. Neka je G konačna grupa. Posmatrajmo dejstvo $G \curvearrowright G$ konjugacijom iz primera I–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:

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

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

I–40 Teorema. Neka je G $\underline{p\text{-grupa}}$, 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 $|G : C(x_i)| \bigm| |G| = p^n$, zaključujemo $p \bigm| |G : C(x_i)|$. 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, $p \bigm| |Z(G)|$. Kako $|Z(G)| \geqslant 1$ jer uvek $e \in Z(G)$, mora biti $|Z(G)| \geqslant p$; centar je netrivijalan. $\square$

I–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. $\square$

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

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

Neka je $X_1 = \{\vec{g} \in X \mid g_0 = g_1 = \dots = g_{p-1}\}$ 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:

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

I–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 $|X_1| = 1$. $\square$

I–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 σ 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. $\square$

I–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. $\square$

E Broj orbita, Bernsajdova lema

U ovom delu G i X su konačni.

I–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 $G \curvearrowright X$.

I–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:

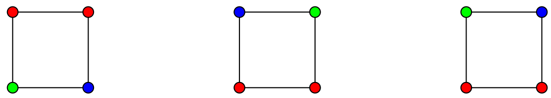
$$\frac{1}{|G|}\sum_{g\in G}|X_g| = \sum_{x\in X}\frac{1}{|G\cdot x|}.$$

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

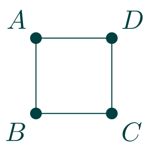
$$\sum_{x\in X}\frac{1}{|G\cdot x|} = \sum_{O\in\mathcal{O}}\sum_{x\in O}\frac{1}{|G\cdot x|} = \sum_{O\in\mathcal{O}}\sum_{x\in O}\frac{1}{|O|} = \sum_{O\in\mathcal{O}}\frac{1}{|O|}\sum_{x\in O}1 = \sum_{O\in\mathcal{O}}\frac{1}{|O|}|O| = \sum_{O\in\mathcal{O}}1 = |\mathcal{O}| = o(G \rightharpoondown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

Završili smo dokaz. $\square$

I–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.

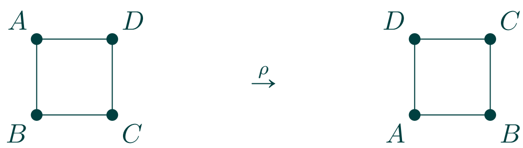


Označimo temena kvadrata sa A, B, C, D:



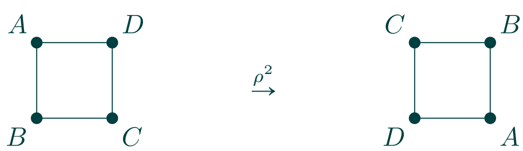
Neka je X skup svih kvadrata sa obojenim temenima u tri boje; primetimo da je $|X| = 3^4 = 81$. Neka $\mathbb{D}_4 \rightharpoondown X$ na prirodan način. Po uslovu zadatka dva kvadrata iz X su jednako obojena ako i samo ako se nalaze u istoj orbiti. Prema tome, problem se svodi na računanje broja $o(\mathbb{D}_4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

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



Da bi ρ 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 ρ^2 se ponaša kao dupli cikl $[AC][BD]$:



Da bi ρ^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 σ osna simetrija u odnosu na vertikalnu osu; σ se ponaša kao dupli cikl $\lfloor AD\rceil\lfloor BC\rceil$:

  Da bi σ 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 $\lfloor AC\rceil$:

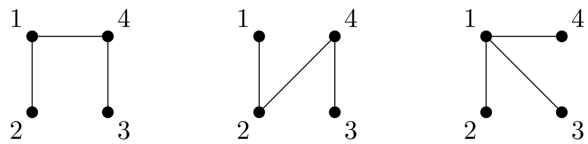
  Da bi $\sigma\rho$ fiksirala obojeni kvadrat moraju A i C biti jednako obojeni, a B i D proizvoljno; imamo 3^3 mogućnosti, tj. $|X_{\sigma\rho}| = 27$.

- 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 $\lfloor 12\rceil$), i neizomorfni su sa trećim:



I–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 transpozicije 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 σ, 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.

- $\sigma = \lfloor 1234\rceil$ je 4-cikl. Permutacija σ na ivicama grafa deluje kao permutacija $\lfloor e_{12}e_{23}e_{34}e_{14}\rceil\lfloor e_{13}e_{24}\rceil$. Da bi σ 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 σ: $|X_\sigma| = 4$.

- $\sigma = \lfloor 123\rceil$ je 3-cikl. Na ivicama grafa σ deluje kao permutacija $\lfloor e_{12}e_{23}e_{13}\rceil\lfloor e_{14}e_{24}e_{34}\rceil$. Kao i malopre, da bi σ fiksirala graf, ivice iz prvog cikla ili sve postoje ili nijedna ne postoji, i slično za drugi cikl; imamo dva izbora, tj. $|X_\sigma| = 2^2 = 4$.

- $\sigma = \lfloor 12 \rceil$ je transpozicija. Na ivicama grafa σ deluje kao permutacija $\lfloor e_{12} \rceil \lfloor e_{13} e_{23} \rceil \lfloor e_{14} e_{24} \rceil \lfloor e_{34} \rceil$. Za svaki od ciklova (njih četiri; dva su trivijalni) imamo mogućnost da izaberemo da li ivice u njemu postoje ili ne; $|X_\sigma| = 2^4 = 16$.
- $\sigma = \lfloor 12 \rceil \lfloor 34 \rceil$ je dupla transpozicija. Na ivicama grafa σ deluje kao permutacija $\lfloor e_{12} \rceil \lfloor e_{13} e_{24} \rceil \lfloor e_{14} e_{23} \rceil \lfloor e_{34} \rceil$. Kao i malopre, $|X_\sigma| = 2^4 = 16$.
- $\sigma = \lfloor \rceil$ je koincidencija. Kako σ 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.

II Teoreme Silova

II–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

II–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 I–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. $\square$

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

II–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, $\binom{p^m \cdot n}{p^m} \equiv n \mod p$. $\square$

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 I–16(b) indukovano dejstvom grupe G na sebe množenjem sleva iz primera I–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 I–33(a)), zaključujemo $G_S \in Syl(G)$. $\square$

II–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

II–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, $a \in P$. $\square$

II–6 Definicija. Neka $p \mid |G|$, p je prost broj, i $P \in Syl_p(G)$. Reći ćemo da je skup $S \subseteq Syl_p(G)$ $\underline{P\text{-invariantan}}$ 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.

II–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 II–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 $|S| = 0 \mod p$. □

II–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 II–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. □

II–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 II–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, $s_p \mid n$. □

II–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, $P \lhd G \iff Syl_p(G) = \{P\} \iff s_p = 1$.) □

II–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 II–5, $h \in Q_i$. Prema tome, $H \subseteq Q_i$. □

C Primene teorema Silova

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

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 $\{e\} \subsetneq H \subsetneq G$. Dakle, pitanje da li je neka grupa prosta je zanimljivo za neabelove grupe.

II–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 I–41.) Videli smo u teoremi I–40 da je $Z(G)$ netrivijalan, pa kako je on i prava podgrupa jer je G neabelova, našli smo pravu netrivijalnu normalnu podgrupu.

II–14 Primer. Grupe reda pq^m, $p < q$ su prosti brojevi i $m \geqslant 1$, nisu proste.

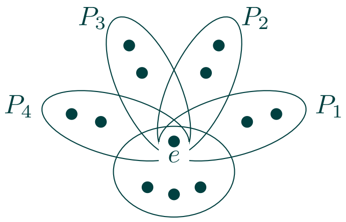
Po trećoj teoremi Silova $s_q = 1 \mod q$ i $s_q \mid p$, pa kako je $p < q$ mora biti $s_q = 1$. Dakle S_q-podgrupa od G je prava netrivijalna normalna podgrupa.

II–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.

II–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 $|G : Core(N(P))| \,\big|\, 8!$ prema $n!$-teoremi, odakle $7 \,\big|\, |Core(N(P))|$ 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 $P_1, \dots, P_8$ sve S_7-podgrupe; kako su sve one ciklične prostog reda 7, međusobno se seku samo po neutralu, pa $|P_1 \cup \dots \cup P_8| = 8 \cdot 6 + 1 = 49$. 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.

II–17 Zadatak. Ako $|G| < 60$ i $|G|$ nije prost broj, dokazati da G nije prosta.

III Alternirajuće grupe

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

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

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

III–2 Lema. Ako $N \lhd \mathbb{A}_n$, gde $n = 5$ ili $n = 6$, i $N \neq \langle[]\rangle$, onda $N = \mathbb{A}_n$.

Dokaz. Dovoljno je da nađemo 3-cikl u N prema lemi III–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 $\{1, 2, \dots, n\}$, sadrži $x = [12][34]$. Zbog normalnosti sadrži i $y = [125]x[125]^{-1} = [25][34]$, pa sadrži i:

$$xy = [12][34][25][34] = [125],$$

čime smo sveli problem na (a).

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

$$xy = [12345][21435] = [153],$$

čime smo sveli problem na (a).

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

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

čime smo sveli problem na (c).

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

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

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

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

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 III–2, tj. $H \subseteq N$. Kako H sadrži 3-ciklove, i N ih sadrži, pa zaključak sledi prema lemi III–1. $\square$

Kao posledicu prethodne tri leme izvodimo:

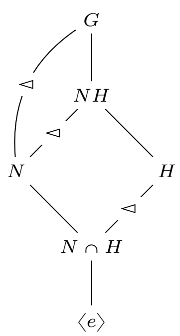
III–4 Teorema. Grupe $\mathbb{A}_n$, $n \geqslant 5$, nisu proste.

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

IV Druga i treća teorema o izomorfizmu

A Druga teorema o izomorfizmu

IV–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, φ 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 φ homomorfizam.

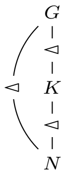
Odredimo jezgro ovog homomorfizma. Imamo, za $h \in H$, $\varphi(h) = N \iff hN = N \iff h \in N \iff h \in N \cap H$. Dakle, $Ker(\varphi) = N \cap H$.

Dokažimo i da je φ 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 φ 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

IV–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 φ 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, φ jeste dobro definisano.

Dokažimo da je φ 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 φ 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 $(G/N)/(K/N) \cong G/K$. □

V Rešive grupe

A Digresija: Karakterisične podgrupe

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

V–2 Komentar.

1. Primetimo: H char $G \iff (\forall \varphi \in Aut(G))\ \varphi[H] \subseteq H$. Zaista, ako poslednje važi, onda za svako φ 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 I–21 za definiciju $Inn(G)$).

V–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 φ 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.

V–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 $\{-1, 1\} \lhd Q_8$.

V–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 $\langle \sigma \rangle \ntriangleleft \mathbb{D}_4$.

V–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 $\varphi_{\upharpoonright K} \in Aut(K)$. Odatle, kako je H char K, $\varphi_{\upharpoonright K}[H] = H$, pa je i $\varphi[H] = \varphi_{\upharpoonright K}[H] = H$.

(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. $(\delta_a)_{\upharpoonright K} \in Aut(K)$. Kako je H char K to $(\delta_a)_{\upharpoonright K}[H] = H$, pa i $\delta_a[H] = H$. Dakle, $H \lhd G$. □

V–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, φ fiksira H.

B Izvod i abelizacija grupe

V–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 $\sigma \in Aut(G)$.

V–9 Definicija. Izvod grupe G je podgrupa $G' := [G, G]$ generisana svim komutatorima.

V–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 $x = [a_1, b_1][a_2, b_2] \ldots [a_n, b_n]$.

V–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. $\square$

V–12 Definicija. Grupa G/G' naziva se <u>abelizacija</u> grupe G i obeležavamo je sa $G^{ab} := G/G'$.

V–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 $\psi = \hat{\psi} \circ \pi^{ab}$:

$$\begin{tikzcd}
G \arrow[r, "\psi"] \arrow[d, "\pi^{ab}"'] \arrow[dr, phantom, "\circlearrowleft"] & A \\
G^{ab} \arrow[ur, dashed, "\hat{\psi}"'] &
\end{tikzcd}$$

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 $g_1 G' = g_2 G'$, 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 $\hat{\psi}(g_1 G' \cdot g_2 G') = \hat{\psi}(g_1 g_2 G') = \psi(g_1 g_2) = \psi(g_1)\psi(g_2) = \hat{\psi}(g_1 G')\hat{\psi}(g_2 G')$. $\square$

C Viši izvodi grupe

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

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

V–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 φ 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. $\square$

V–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 $k = 3, 4, \ldots, n$, $\lfloor 12k \rfloor = \lfloor 1k \rfloor \lfloor 2k \rfloor \lfloor 1k \rfloor \lfloor 2k \rfloor = [\ \lfloor 1k \rfloor, \lfloor 2k \rfloor\ ] \in G'$. Kako znamo da $\lfloor 12k \rfloor$ 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 $V = \{\lfloor\rfloor, \lfloor 12 \rfloor \lfloor 34 \rfloor, \lfloor 13 \rfloor \lfloor 24 \rfloor, \lfloor 14 \rfloor \lfloor 23 \rfloor\}$ – 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, $\mathbb{A}_4'' = V' = \langle \lfloor\rfloor \rangle$, i viši izvodi su očigledno takođe trivijalni. Dakle, $\mathbb{S}_4'' = V$, $\mathbb{S}_4''' = \langle \lfloor\rfloor \rangle$ 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:

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

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

V–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.

V–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.

V–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 V–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 V–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. $\square$

V–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 V–16(b) je $\langle N \rangle = (G/N)^{(n)} = \pi[G^{(n)}]$, pa je $G^{(n)} \leqslant N$. Prema lemi V–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 $(G^{(n)})^{(m)} = G^{(n+m)}$. $\square$

V–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. $\square$

V–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 I–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 V–21, G je rešiva. $\square$

V–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 V–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:

$$\begin{tikzcd}
& H_i \arrow[d, dash] & \\
& H_{i+1}G^{(i)} \arrow[dl, dash] \arrow[dr, dash] & \\
H_{i+1} \arrow[dr, dash] & & G^{(i)} \arrow[dl, dash] \\
& H_{i+1} \cap G^{(i)} &
\end{tikzcd}$$

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 V–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. $\square$

V–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.