Алгебра 2(P)– вежбе

Никола Лелас

Садржај

1 Теореме о изоморфизмима група

Нека је $\phi : G \to H$ хомоморфизам група. Дефинишемо:

$$\ker \phi = \{g \in G \mid \phi(g) = e\} \quad \text{језгро хомоморфизма } \phi.$$
$$\operatorname{im} \phi = \{\phi(g) \mid g \in G\} \quad \text{слика хомоморфизма } \phi.$$

Приметимо да важи:

$$\phi \text{ је 1-1 ако и само ако је } \ker \phi = \{e\}.$$
$$\phi \text{ је на ако и само ако је } \operatorname{im} \phi = H.$$

Теорема 1.1 (Прва теорема о изоморфизму)**.** Нека је $\phi : G \to H$ хомоморфизам група. Тада је $\ker \phi \triangleleft G$ и важи

$$G/\ker \phi \cong \operatorname{im} \phi.$$

Прву теорему о изоморфизму ћемо најчешће користити у случају када је хомоморфизам ϕ сурјективан и тада имамо

$$G/\ker \phi \cong H.$$

Задатак 1. Доказати да за све $n \geq 2$ важи $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^\times$.

Решење. Посматрајмо пресликавање детерминанте $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$. То пресликавање је на (сваки ненула реалан x број је детерминанта нпр. дијагоналне матрице са једним x и све остало јединицама по дијагонали) и хомоморфизам на основу Бине-Кошијеве теореме,

$$\det(AB) = \det A \cdot \det B \quad \text{за } A, B \in \mathrm{GL}_n(\mathbb{R}).$$

Његово језгро је

$$\ker \det = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det A = 1\} = \mathrm{SL}_n(\mathbb{R}).$$

На основу Прве теореме о изоморфизму онда следи тражено

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^\times.$$

□

Задатак 2. Показати да је за све $n \geq 2$ испуњено $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Решење. Посматрајмо пресликавање $\phi : \mathbb{Z} \to \mathbb{Z}_n$ дефинисано са $\phi(x) = x \pmod n$, $x \in \mathbb{Z}$. Ово пресликавање је очигледно на. Такође, за све $x, y \in \mathbb{Z}$ важи

$$\begin{aligned}\phi(x+y) &= (x+y) \pmod n \\ &= x \pmod n +_n y \pmod n \\ &= \phi(x) +_n \phi(y),\end{aligned}$$

чиме је показано да је ϕ хомоморфизам. Његово језгро је:

$$\begin{aligned}\ker\phi &= \{x \in \mathbb{Z} \mid \phi(x) = 0\} \\ &= \{x \in \mathbb{Z} \mid x \pmod n = 0\} \\ &= \{x \in \mathbb{Z} \mid x = na \text{ за неко } a \in \mathbb{Z}\} = n\mathbb{Z}.\end{aligned}$$

На основу Прве теореме о изоморфизму следи тражено $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.
□

Задатак 3. Нека је $U = \{z \in \mathbb{C} \mid |z| = 1\}$. Тада је U група у односу на множење комплексних бројева. Доказати да је $\mathbb{R}/\mathbb{Z} \cong U$.

Решење. Посматрајмо пресликавање $\phi : \mathbb{R} \to U$ дефинисано са $\phi(x) = e^{ix} = \cos x + i\sin x$, $x \in \mathbb{R}$. Тригонометријски облик произвољног комплексног броја из U је $\cos\theta + i\sin\theta$ за неко $\theta \in \mathbb{R}$, па је пресликавање које посматрамо на. За произвољне $x, y \in \mathbb{R}$ важи

$$\begin{aligned}\phi(x+y) &= e^{i(x+y)} \\ &= e^{ix}e^{iy} = \phi(x)\phi(y),\end{aligned}$$

чиме је показано да је ϕ хомоморфизам. На основу Прве теореме о изоморфизму онда следи $\mathbb{R}/\ker\phi \cong U$.

Одредимо још $\ker\phi$:

$$\begin{aligned}\ker\phi &= \{x \in \mathbb{R} \mid \phi(x) = 1\} \\ &= \{x \in \mathbb{R} \mid e^{ix} = 1\} \\ &= \{\alpha \in \mathbb{R} \mid \alpha = 2k\pi, k \in \mathbb{Z}\} = \{2k\pi \mid k \in \mathbb{Z}\}.\end{aligned}$$

Сада нисмо баш добили $\ker\phi = \mathbb{Z}$, али важи $\ker\phi \cong \mathbb{Z}$ (један изоморфизам $\ker\phi \to \mathbb{Z}$ је одређен са $2k\pi \to k$, $k \in \mathbb{Z}$). Одатле следи тражено $\mathbb{R}/\mathbb{Z} \cong U$.
□

Задатак 4. Нека је G Абелова група.
а) Доказати да су $K = \{g \in G \mid g^2 = e\}$ и $H = \{g^2 \mid g \in G\}$ две подгрупе од G.
б) Доказати да је $G/K \cong H$.

Решење. а) За произвољне g_1 и g_2 из K имамо $g_1^2 = g_2^2 = e$, одакле је

$$\begin{aligned}(g_1g_2)^2 &= g_1^2g_2^2 \text{ (јер је } G \text{ Абелова група)} \\ &= e,\end{aligned}$$

одакле следи $g_1g_2 \in K$. Такође је и

$$(g_1^{-1})^2 = \left(g_1^2\right)^{-1} = e,$$

па зато $g_1^{-1} \in K$. Закључујемо да је K подгрупа од G.

Слично, за произвољне h_1 и h_2 из H имамо $h_1 = t_1^2$ и $h_2 = t_2^2$ за неке $t_1, t_2 \in G$. Одатле је

$$h_1 h_2 = t_1^2 t_2^2 = (t_1 t_2)^2 \in H$$
$$h_1^{-1} = (t_1^2)^{-1} = \left(t_1^{-1}\right)^2 \in H.$$

Тако добијамо да је и H подгрупа од G.
б) Посматрајмо пресликавање $\phi : G \to G$ дефинисано са $\phi(g) = g^2$, $g \in G$. По дефиницији је $\operatorname{im}\phi = H$. Такође, за све $g_1, g_2 \in G$ важи

$$\begin{aligned}\phi(g_1 g_2) &= (g_1 g_2)^2 \\ &= g_1^2 g_2^2 \\ &= \phi(g_1)\phi(g_2),\end{aligned}$$

па је ϕ хомоморфизам. Његово језгро је:

$$\begin{aligned}\ker\phi &= \{g \in G \mid \phi(g) = e\} \\ &= \left\{g \in G \mid g^2 = e\right\} = K.\end{aligned}$$

Из Прве теореме о изоморфизму онда следи $G/K \cong H$.
□

Теорема 1.2 (Друга теорема о изоморфизму)**.** Нека је $H \leq G$ и $K \triangleleft G$. Тада је $HK \leq G$, $K \triangleleft HK$, $H \cap K \triangleleft H$ и имамо изоморфизам

$$H/H \cap K \cong HK/K.$$

Теорема 1.3 (Трећа теорема о изоморфизму)**.** Нека је H и K нормалне подгрупе од G такве да је $H \leq K$. Тада је $H \triangleleft K$, $K/H \triangleleft G/H$ и важи

$$(G/H)/(K/H) \cong G/K.$$

Задатак 5. Нека је $H \leq G$ и $K \triangleleft G$. Ако је $G = HK$ и $H \cap K = \langle e\rangle$, показати да је $G/K \cong H$.

Решење. На основу Друге теореме о изоморфизму имамо

$$H/H \cap K \cong HK/K.$$

Пошто је $H \cap K = \langle e\rangle$, следи $H/H \cap K \cong H$, што уз $G = HK$ даје тражено тврђење.
□

Задатак 6. Нека је H подгрупа од $\mathbb{S}_n$ која садржи барем једну непарну пермутацију. Доказати да је

$$H/H \cap \mathbb{A}_n \cong \mathbb{S}_n/\mathbb{A}_n.$$

Решење. Применимо Другу теорему о изоморфизму на $H \leq \mathbb{S}_n$ и $\mathbb{A}_n \triangleleft \mathbb{S}_n$. Тако добијамо

$$H/H \cap \mathbb{A}_n \cong H\mathbb{A}_n/\mathbb{A}_n.$$

Како је H са особином да садржи барем једну непарну пермутацију, важи да је $H\mathbb{A}_n = \mathbb{S}_n$ (зато што у $H\mathbb{A}_n$ имамо барем једну непарну и све парне пермутације, а стога и све пермутације). Одатле директно следи тражено тврђење.
□

Задатак 7. Доказати да за све природне бројеве m, n важи

$$(m, n)[m, n] = mn,$$

при чему је (m, n) ознака за НЗД, а $[m, n]$ ознака за НЗС бројева m и n.

Решење. Посматрајмо подгрупе $m\mathbb{Z}$ и $n\mathbb{Z}$ од $\mathbb{Z}$. Група $\mathbb{Z}$ је Абелова, па су обе ове подгрупе свакако нормалне. Због тога можемо применити Другу теорему о изоморфизму да добијемо

$$m\mathbb{Z}/m\mathbb{Z} \cap n\mathbb{Z} \cong m\mathbb{Z} + n\mathbb{Z}/n\mathbb{Z}.$$

Сада је

$$m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$$
$$m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z},$$

што даје

$$m\mathbb{Z}/[m, n]\mathbb{Z} \cong (m, n)\mathbb{Z}/n\mathbb{Z}.$$

Изједначавањем редова посматраних група коначно добијамо $\frac{[m,n]}{m} = \frac{n}{(m,n)}$ тј. $(m, n)[m, n] = mn$.
□

Задатак 8. Група G се назива метаабеловом ако постоји $N \triangleleft G$ таква да су групе G/N и N Абелове. Доказати да је свака подгрупа метаабелове групе и сама метаабелова.

Решење. Нека је G метаабелова група и $H \leq G$. Тада постоји $N \triangleleft G$ таква да су групе G/N и N Абелове. Из Друге теореме о изоморфизму знамо да је $H \cap N \triangleleft H$, као и да важи

$$H/H \cap N \cong HN/N. \tag{1}$$

Приметимо да је $H \cap N$ Абелова група, јер је садржана у Абеловој групи N. Такође, HN/N је подгрупа Абелове групе G/N, па је и она Абелова. На основу изоморфизма (1) закључујемо да је Абелова и група $H/H \cap N$.

Дакле, за подгрупу H постоји нормална подгрупа $M := H \cap N$ таква да су H/M и M Абелове. По дефиницији је онда H метаабелова.
□

2 Решиве групе

Дефиниција 2.1. Нека је G група и $x, y \in G$. Комутатор елемената x и y, у ознаци $[x, y]$ је дефинисан са

$$[x, y] = xyx^{-1}y^{-1}.$$

Дефиниција 2.2. Подгрупа групе G генерисана комутаторима свих елемената из G се назива извод групе G и означава се G'.

Пример 2.3. Нека је G Абелова група. Тада сви елементи из G међусобно комутирају, па за све $x, y \in G$ важи

$$[x, y] = xyx^{-1}y^{-1} = xx^{-1}yy^{-1} = e.$$

Одатле закључујемо да је $G' = \langle e \rangle$.
□

Задатак 9. Одредити извод симетричне групе $\mathbb{S}_n$, $n \geq 3$.

Решење. Приметимо прво да је за произвољне $\pi, \sigma \in \mathbb{S}_n$ испуњено

$$\operatorname{sgn}[\pi, \sigma] = \operatorname{sgn}\left(\pi\sigma\pi^{-1}\sigma^{-1}\right) = 1.$$

Како су производи и инверзи парних пермутација поново парне пермутације, закључујемо да је $\mathbb{S}_n' \subseteq \mathbb{A}_n$.

Покажимо да важи и обратна инклузија $\mathbb{A}_n \subseteq \mathbb{S}_n'$. Пошто 3-циклови генеришу $\mathbb{A}_n$, довољно је да покажемо да се произвољни 3-цикл може представити преко комутатора неких елемената из $\mathbb{S}_n$. Заиста, за произвољни 3-цикл $\lceil a, b, c \rfloor$ имамо:

$$\begin{aligned}
\lceil a, b, c \rfloor &= \lceil a, b \rfloor \lceil b, c \rfloor \\
&= \lceil a, b \rfloor \lceil a, c \rfloor \lceil a, b \rfloor \lceil a, c \rfloor \\
&= \lceil a, b \rfloor \lceil a, c \rfloor \lceil a, b \rfloor^{-1} \lceil a, c \rfloor^{-1} \\
&= \left[\lceil a, b \rfloor, \lceil a, c \rfloor\right].
\end{aligned}$$

Према томе, добијамо $\mathbb{S}_n' = \mathbb{A}_n$.
□

Задатак 10. Одредити извод алтернирајуће групе $\mathbb{A}_n$, $n \geq 5$.

Решење. Свакако имамо да је $\mathbb{A}_n' \subseteq \mathbb{A}_n$. Докажимо да важи обратна инклузија. Слично као у претходном задатку, довољно је да произвољни 3-цикл представимо преко комутатора неких пермутација. Једина разлика је што сада те пермутације морају бити парне, па представљање из претходног задатка не можемо директно да искористимо.

Уочимо произвољни 3-цикл $\lceil a, b, c \rfloor$. Пошто је $n \geq 5$, постоје $d, e \notin \{a, b, c\}$ такви да је $d \neq e$. Означимо:

$$f = \lceil a, b \rfloor \lceil d, e \rfloor \quad \text{и} \quad g = \lceil a, c \rfloor \lceil d, e \rfloor.$$

Приметимо да су пермутације f и g парне, као и да важи

$$\begin{aligned}[f,g] &= \lceil a,b\rfloor\lceil d,e\rfloor\lceil a,c\rfloor\lceil d,e\rfloor\lceil a,b\rfloor\lceil d,e\rfloor\lceil a,c\rfloor\lceil d,e\rfloor \\ &= \lceil a,b\rfloor\lceil a,c\rfloor\lceil a,b\rfloor^{-1}\lceil a,c\rfloor^{-1} \\ &= [\lceil a,b\rfloor,\lceil a,c\rfloor] \\ &= \lceil a,b,c\rfloor.\end{aligned}$$

Добијамо $\mathbb{A}_n \subseteq \mathbb{A}_n'$, што даје $\mathbb{A}_n' = \mathbb{A}_n$.
□

Напомена. Приметимо да је при решавању претходног задатка био кључан услов $n \geq 5$. Наравно, у случајевима $n = 2$ и $n = 3$ је група $\mathbb{A}_n$ Абелова, па одмах користећи Пример 2.3 добијамо $\mathbb{A}_n' = \langle e\rangle$. Зато нам остаје само нетривијалан случај $n = 4$ којим ћемо се позабавити мало касније.

Задатак 11. Одредити извод диедарске групе $\mathbb{D}_n$, $n \geq 3$.

Решење. Одредимо за почетак комутаторе произвољних елемената из $\mathbb{D}_n$. Како ти елементи могу бити ротације и рефлексије издвајамо следеће случајеве:

- Комутатор две ротације ρ^i и ρ^j:

$$\left[\rho^i,\rho^j\right] = \rho^i\rho^j\rho^{-i}\rho^{-j} = \varepsilon$$

- Комутатор ротације ρ^i и рефлексије $\sigma\rho^j$:

$$\left[\rho^i,\sigma\rho^j\right] = \rho^i\sigma\rho^j\rho^{-i}\rho^{-j}\sigma = \rho^i\sigma\rho^{-i}\sigma = \rho^i\rho^i\sigma\sigma = \rho^{2i} \in \langle\rho^2\rangle. \tag{2}$$

- Комутатор две рефлексије $\sigma\rho^i$ и $\sigma\rho^j$:

$$\left[\sigma\rho^i,\sigma\rho^j\right] = \sigma\rho^i\sigma\rho^j\rho^{-i}\sigma\rho^{-j}\sigma = \rho^{-i}\rho^{j-i}\rho^j = \rho^{2(j-i)} \in \langle\rho^2\rangle.$$

Закључујемо да су комутатори произвољних елемената из $\mathbb{D}_n$ садржани у подгрупи $\langle\rho^2\rangle$, па је $\mathbb{D}_n' \subseteq \langle\rho^2\rangle$. Са друге стране, из (2) имамо $\rho^2 = [\rho,\sigma]$, што даје обратну инклузију $\langle\rho^2\rangle \subseteq \mathbb{D}_n'$. Према томе, $\mathbb{D}_n' = \langle\rho^2\rangle$. Приметимо још и да за непарно n важи $\langle\rho^2\rangle = \langle\rho\rangle$, па добијамо и мало прецизније

$$\mathbb{D}_n' = \begin{cases} \langle\rho\rangle, & \text{ако је } n \text{ непарно} \\ \langle\rho^2\rangle, & \text{ако је } n \text{ парно.}\end{cases}$$

□

Задатак 12. Одредити извод групе $\mathrm{GL}_2(\mathbb{R})$.

Решење. За произвољне матрице $A, B \in \mathrm{GL}_2(\mathbb{R})$ важи

$$\det[A,B] = \det(ABA^{-1}B^{-1}) = 1.$$

Одатле закључујемо да је $\mathrm{GL}_2(\mathbb{R})' \subseteq \mathrm{SL}_2(\mathbb{R})$. Покажимо још и обратну инклузију.

За почетак, уочимо произвољну матрицу $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ из $\mathrm{SL}_2(\mathbb{R})$. Детерминанта посматране матрције је једнака 1, па важи $ad - bc = 1$.

Ако је $a \neq 0$, важи

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & ab \\ \frac{c}{a} & ad \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & \frac{1}{a} \end{bmatrix}.$$

Ослањајући се на услов $ad - bc = 1$, даље добијамо

$$\begin{aligned} \begin{bmatrix} a & b \\ c & d \end{bmatrix} &= \begin{bmatrix} 1 & ab \\ \frac{c}{a} & bc+1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & \frac{1}{a} \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ \frac{c}{a} & 1 \end{bmatrix} \begin{bmatrix} 1 & ab \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & \frac{1}{a} \end{bmatrix}. \end{aligned}$$

Ако је $a = 0$, онда мора бити $b \neq 0$ и важи $bc = -1$. Сличо као за $a \neq 0$ у овом случај имамо

$$\begin{bmatrix} 0 & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -\frac{d}{b} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{b} & 0 \\ 0 & b \end{bmatrix}.$$

Према томе, да бисмо показали да је $\mathrm{SL}_2(\mathbb{R}) \subseteq \mathrm{GL}_2(\mathbb{R})'$, довољно је да произвољне матрице $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}$ за $x \in \mathbb{R}$, $\begin{bmatrix} y & 0 \\ 0 & \frac{1}{y} \end{bmatrix}$ за $y \in \mathbb{R} \setminus \{0\}$ и $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ изразимо преко комутатора елемената из $\mathrm{GL}_2(\mathbb{R})$. Имамо прво

$$\begin{aligned} \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^{-1} &= \begin{bmatrix} 2 & 2x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}, \end{aligned}$$

а транспоновањем претходног рачуна добијамо и израз за $\begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}$.

Даље се слично показује да важи

$$\begin{bmatrix} y & 0 \\ 0 & \frac{1}{y} \end{bmatrix} = \begin{bmatrix} y & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} y & 0 \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{-1}$$

и

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} -1 & 0 \\ 1 & 2 \end{bmatrix}^{-1},$$

што завршава задатак уз закључак $\mathrm{GL}_2(\mathbb{R})' = \mathrm{SL}_2(\mathbb{R})$.
□

Задатак 13. Нека је H подгрупа групе G. Тада H садржи комутаторе свих $g_1, g_2 \in G$ ако и само ако је $H \triangleleft G$ и G/H Абелова група.

Решење. Претпоставимо да H садржи комутаторе произвољних елемената из G. Покажимо прво да је $H \triangleleft G$. Пошто је H подгрупа од G, довољно је да покажемо да је она инваријантна у односу на конјугацију произвољним елементима из G. Уочимо произвољно $x \in H$ и $g \in G$. Тада је

$$gxg^{-1} = gxg^{-1}x^{-1}x = \underbrace{[g,x]}_{\in H}\underbrace{x}_{\in H} \in H,$$

одакле следи $H \triangleleft G$. Остаје још да покажемо да је група G/H Абелова. Уочимо произвољна два косета g_1H и g_2H из G/H. Њихов комутатор је

$$[g_1H, g_2H] = g_1Hg_2H(g_1H)^{-1}(g_2H)^{-1} = g_1Hg_2Hg_1^{-1}Hg_2^{-1}H = [g_1,g_2]H = H,$$

јер је $[g_1, g_2] \in H$. Закључујемо да g_1H и g_2H комутирају, па је због њихове произвољности група G/H Абелова.

Нека је сада $H \triangleleft G$ и G/H Абелова група. Тада за свака два косета g_1H и g_2H важи

$$[g_1H, g_2H] = H.$$

Пошто, као што смо већ видели, важи $[g_1H, g_2H] = [g_1, g_2]H$, закључујемо да је

$$[g_1, g_2]H = H.$$

Према томе, за произвољне елементе g_1 и g_2 из G важи $[g_1, g_2] \in H$.
□

Како је, по дефиницији, извод групе G једна њена подгрупа која садржи све комутаторе елемената из G, одмах добијамо следећу последицу.

Последица. Нека је G група. Тада је $G' \triangleleft G$ и G/G' Абелова група.

Дефиниција 2.4. Количничка група G/G' се назива абелизација групе G и означава се са G^{ab}.

Пример 2.5. За $n \geq 3$, из Задатка 9 имамо да је $\mathbb{S}_n' = \mathbb{A}_n$. Како је $[\mathbb{S}_n : \mathbb{A}_n] = 2$, добијамо

$$\mathbb{S}_n^{\mathrm{ab}} = \mathbb{S}_n/\mathbb{A}_n \cong \mathbb{Z}_2.$$

Слично, за $n \geq 5$, из Задатка 10 имамо да је $\mathbb{S}_n' = \mathbb{A}_n$, па је

$$\mathbb{A}_n^{\mathrm{ab}} = \langle \varepsilon \rangle.$$

□

Пример 2.6. Из Задатка 12 имамо да је $\mathrm{GL}_2(\mathbb{R})' = \mathrm{SL}_2(\mathbb{R})$. Зато је

$$\mathrm{GL}_2(\mathbb{R})^{\mathrm{ab}} = \mathrm{GL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{R}) \cong \mathbb{R}^\times,$$

на основу Задатка 1.
□

Задатак 14. Одредити извод групе $\mathbb{A}_4$.

Решење. Посматрајмо подскуп

$$V = \left\{ \varepsilon, \underbrace{\lceil 1,2 \rfloor \lceil 3,4 \rfloor}_{f}, \underbrace{\lceil 1,3 \rfloor \lceil 2,4 \rfloor}_{g}, \underbrace{\lceil 1,4 \rfloor \lceil 2,3 \rfloor}_{h} \right\}$$

групе $\mathbb{A}_4$. Приметимо, да су осим неутрала ε, сви елементи из V реда 2, као и да важи

$$fg = gf = h, gh = hg = f \text{ и } hf = fh = g.$$

Због тога је V подгрупа од $\mathbb{A}_4$. Пошто се конјугацијом не мења облик цикличне декомпозиције пермутације и f, g и h су (једине) дупле транспозиције из $\mathbb{A}_4$, важи да је та подгрупа нормална. Приметимо и да је

$$[\mathbb{A}_4 : V] = \frac{|\mathbb{A}_4|}{|V|} = \frac{12}{4} = 3,$$

па је $\mathbb{A}_4/V \cong \mathbb{Z}_3$. Дакле, важи $V \triangleleft \mathbb{A}_4$ и $\mathbb{A}_4/V$ је Абелова група. На основу Задатка 13 онда следи $\mathbb{A}_4' \subseteq V$.

Са друге стране, група $\mathbb{A}_4$ је неабелова, па је $\mathbb{A}_4' \neq \langle \varepsilon \rangle$. То значи да постоји барем једна нетривијална пермутација у $\mathbb{A}_4'$. Како је $\mathbb{A}_4' \subseteq V$, та пермутација мора бити дупла транспозиција. Међутим, $\mathbb{A}_4' \triangleleft \mathbb{A}_4$, па се у $\mathbb{A}_4'$ морају налазити и сви конјугати те дупле транспозиције, што су управо све преостале дупле транспозиције из $\mathbb{A}_4$. Одатле закључујемо да је $\mathbb{A}_4' = V$.
□

Напомена. Приметимо да је група V Абелова, изоморфна Клајновој групи, $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Изводе вишег реда групе G дефинишемо индуктивно са $G'' = (G')'$, $G''' = (G'')'$ и генерално,

$$G^{(n+1)} = \left(G^{(n)}\right)' \quad \text{за } n \in \mathbb{N}.$$

На овај начин добијамо низ нормалних подгрупа

$$G \triangleright G' \triangleright G'' \triangleright \ldots G^{(n)} \triangleright \ldots \tag{3}$$

Дефиниција 2.7. Ако постоји (најмањи) природан број n такав да за низ (3) важи

$$G \triangleright G' \triangleright G'' \triangleright \ldots G^{(n)} = \langle e \rangle$$

за групу G се каже да је решива. У супротном, за групу се G каже да није решива.

Пример 2.8. Нека је $n \geq 5$. На основу Задатака 9 и 10 имамо да су низови извода за $\mathbb{S}_n$ и $\mathbb{A}_n$ редом

$$\mathbb{S}_n \triangleright \mathbb{A}_n \triangleright \mathbb{A}_n \triangleright \mathbb{A}_n \triangleright \ldots$$
$$\mathbb{A}_n \triangleright \mathbb{A}_n \triangleright \mathbb{A}_n \triangleright \mathbb{A}_n \triangleright \ldots$$

Због тога групе $\mathbb{S}_n$ и $\mathbb{A}_n$ нису решиве.

Слично, за $n = 4$ се ослањамо још на Задатак 14 и Пример 2.3 да добијемо низове извода за $\mathbb{S}_4$ и $\mathbb{A}_4$:

$$\mathbb{S}_4 \triangleright \mathbb{A}_4 \triangleright V \triangleright \langle e \rangle$$
$$\mathbb{A}_4 \triangleright V \triangleright \langle e \rangle.$$

Такође, низ извода групе $\mathbb{S}_3$ је $\mathbb{S}_3 \triangleright \mathbb{A}_3 \triangleright \langle e \rangle$, а за $\mathbb{A}_3$, $\mathbb{S}_2$ и $\mathbb{A}_2$ се одмах тривијално завршава неутралом, пошто су те групе Абелове. Дакле, групе $\mathbb{S}_4$, $\mathbb{S}_3$, $\mathbb{S}_2$, $\mathbb{A}_4$, $\mathbb{A}_3$ и $\mathbb{A}_2$ су решиве.

Да сумирамо, групе $\mathbb{S}_n$ и $\mathbb{A}_n$ су решиве ако и само ако је $n \leq 4$.

□

Пример 2.9. Нека је $n \geq 3$. На основу Задатка 11 и Примера 2.3 имамо да је низ извода за $\mathbb{D}_n$

$$\mathbb{D}_n \triangleright \langle \rho^2 \rangle \triangleright \langle e \rangle.$$

Закључујемо да су групе $\mathbb{D}_n$ решиве.

□

Овај одељак завршавамо једном теоремом која је често корисна за показивање да је нека група решива.

Теорема 2.10. Група G је решива ако и само ако постоји $H \triangleleft G$ таква да су H и G/H решиве групе.

3 Дејства група

Дефиниција 3.1. Дејство групе G на скуп S је пресликавање $\cdot : G \times S \to S$ са особинама:

- $e \cdot x = x$ за све $x \in S$.
- $g \cdot (h \cdot x) = (gh) \cdot x$ за све $g, h \in G$ и $x \in S$.

Имамо и еквивалентну дефиницију: Дејство групе G на скуп S је хомоморфизам из G у групу $\operatorname{Sym} S$, где је

$$\operatorname{Sym} S = \{f : S \to S \mid f \text{ је бијекција}\}.$$

Уз дејство групе G на скуп S дефинишемо следеће скупове:

$$\mathcal{O}_x = \{g \cdot x \mid g \in G\} \quad \text{орбита елемента } x \in S.$$
$$\operatorname{Stab}(x) = \{g \in G \mid g \cdot x = x\} \quad \text{стабилизатор елемента } x \in S.$$
$$\operatorname{Fix}(g) = \{x \in S \mid g \cdot x = x\} \text{ фиксни скуп елемента } g \in G.$$

Скуп свих орбита означавамо са S/G.

Задатак 15. Показати да је са $n \cdot (a, b) = (n +_{10} a, n +_8 b)$, $n \in \mathbb{Z}, a \in \mathbb{Z}_{10}, b \in \mathbb{Z}_8$ дефинисано дејство групе $\mathbb{Z}$ на скуп $\mathbb{Z}_{10} \times \mathbb{Z}_8$ и испитати који се од елемената $(1, 0)$ и $(1, 3)$ налази у орбити за $(2, 3)$ при овом дејству.

Решење. Докажимо прво да је $\cdot$ дејство. За произвољне $m, n \in \mathbb{Z}$ и $(a, b) \in \mathbb{Z}_{10} \times \mathbb{Z}_8$ имамо:

$$\begin{aligned} 0 \cdot (a, b) &= (0 +_{10} a, 0 +_8 b) = (a, b) \\ n \cdot (m \cdot (a, b)) &= n \cdot (m +_{10} a, m +_8 b) \\ &= (n +_{10} (m +_{10} a), n +_8 (m +_8 b)) \\ &= ((n +_{10} m) +_{10} a, (n +_8 m) +_8 b) \\ &= ((n + m) +_{10} a, (n + m) +_8 b) \\ &= (n + m) \cdot (a, b). \end{aligned}$$

Овим смо показали да $\cdot$ јесте дејство.

Даље је по дефиницији

$$\begin{aligned} \mathcal{O}_{(2,3)} &= \{n \cdot (2, 3) \mid n \in \mathbb{Z}\} \\ &= \{(n +_{10} 2, n +_8 3) \mid n \in \mathbb{Z}\} \\ &= \{(x, y) \in \mathbb{Z}_{10} \times \mathbb{Z}_8 \mid x = n +_{10} 2, y = n +_8 3 \text{ за неко } n \in \mathbb{Z}\}. \end{aligned}$$

Према томе, $(1, 0)$ се налази у $\mathcal{O}_{(2,3)}$ ако постоји $n \in \mathbb{Z}$ такво да је $1 = n +_{10} 2$ и $0 = n +_8 3$. Одавде добијамо систем:

$$\begin{aligned} n + 2 &\equiv 1 \pmod{10} \\ n + 3 &\equiv 0 \pmod{8}. \end{aligned}$$

Он је еквивалентан са

$$\begin{aligned} n &\equiv 9 \pmod{10} \\ n &\equiv 5 \pmod{8}. \end{aligned}$$

Из прве једначине имамо $n = 10k + 9$ за неко $k \in \mathbb{Z}$. Враћањем у другу једначину онда добијамо

$$\begin{aligned} 10k + 9 &\equiv 5 \pmod{8} \\ 2k &\equiv 4 \pmod{8}. \end{aligned}$$

Имамо да је једно решење ове једначине $k = 2$, одакле је $n = 29$ једно решење система (није неопходно да нађемо сва решења, пошто нас суштински само занима да ли систем има решења). Закључујемо да је $(1, 0) \in \mathcal{O}_{(2,3)}$.

Слично, за $(1, 3)$ имамо систем

$$\begin{aligned} n &\equiv 9 \pmod{10} \\ n &\equiv 0 \pmod{8}. \end{aligned}$$

Из друге једначине следи да је број n дељив са 8, па је, специјално, паран. Међутим, прва једначина имплицира да се n завршава цифром 9, што није могуће истовремено са тим. Дакле, закључујемо да систем нема решења, па $(1, 3) \notin \mathcal{O}_{(2,3)}$.

□

Задатак 16. Посматрајмо групу $G = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid a, b, d \in \mathbb{R}, ad = 1 \right\}$ у односу на уобичајено множење матрица. Доказати да је са

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \cdot z = \frac{az + b}{d}, \ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in G, z \in \mathbb{C}$$

дефинисано једно дејство групе G на скуп комплексних бројева $\mathbb{C}$. Одредити орбиту и стабилизатор за елемент $i \in \mathbb{C}$ при овом дејству.

Решење. За произвољне матрице $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, $\begin{bmatrix} e & f \\ 0 & h \end{bmatrix}$ из G и $z \in \mathbb{C}$ имамо:

$$\begin{aligned}
\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot z &= \frac{1 \cdot z + 0}{1} = z \\
\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \cdot \left(\begin{bmatrix} e & f \\ 0 & h \end{bmatrix} \cdot z \right) &= \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \cdot \frac{ez + f}{h} \\
&= \frac{a\frac{ez+f}{h} + b}{d} \\
&= \frac{aez + af + bh}{dh} \\
&= \begin{bmatrix} ae & af + bh \\ 0 & dh \end{bmatrix} \cdot z \\
&= \left(\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} e & f \\ 0 & h \end{bmatrix} \right) \cdot z.
\end{aligned}$$

Добијено показује да је $\cdot$ дејство. Сада је по дефиницији:

$$\begin{aligned}
\mathcal{O}_i &= \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \cdot i \,\middle|\, \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in G \right\} \\
&= \left\{ \frac{ai + b}{d} \mid a, b, d \in \mathbb{R}, ad = 1 \right\} \\
&= \left\{ a^2 i + ab \mid a, b \in \mathbb{R}, a \neq 0 \right\} \\
&= \left\{ z \in \mathbb{C} \mid \Im(z) > 0 \right\}.
\end{aligned}$$

Слично, за стабилизатор имамо:

$$\begin{aligned}
\mathrm{Stab}(i) &= \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in G \,\middle|\, \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \cdot i = i \right\} \\
&= \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in G \,\middle|\, \frac{ai + b}{d} = i \right\} \\
&= \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in G \,\middle|\, \frac{a}{d} = 1, b = 0 \right\} \\
&= \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \in G \,\middle|\, a = d \right\} \\
&= \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} \text{ (пошто имамо и услов } ad = 1 \text{ за матрице из } G).
\end{aligned}$$

□

Задатак 17. Посматрајмо подгрупу G групе $\mathbb{S}_8$ генерисану пермутацијама $\lceil 1,2,3\rfloor\lceil 7,8\rfloor$ и $\lceil 4,5\rfloor$ која дејствује на скуп $S=\{1,2,\ldots,8\}$ као група пермутација,

$$\sigma\cdot n=\sigma(n),\ \ \sigma\in G, n\in S.$$

Одредити $\mathcal{O}_1,\mathcal{O}_6,\mathcal{O}_7$, $\mathrm{Stab}(2),\mathrm{Stab}(4)$, као и $\mathrm{Fix}(\lceil 4,5\rfloor)$ и $\mathrm{Fix}(\lceil 1,2,3\rfloor\lceil 7,8\rfloor)$ при овом дејству.

Решење. Прво можемо одредити све елементе групе G,

$$\begin{aligned}G=\{&\varepsilon,\lceil 1,2,3\rfloor\lceil 7,8\rfloor,\lceil 1,3,2\rfloor,\lceil 7,8\rfloor,\lceil 1,2,3\rfloor,\lceil 1,3,2\rfloor\lceil 7,8\rfloor,\\ &\lceil 4,5\rfloor,\lceil 1,2,3\rfloor\lceil 4,5\rfloor\lceil 7,8\rfloor,\lceil 1,3,2\rfloor\lceil 4,5\rfloor,\lceil 4,5\rfloor\lceil 7,8\rfloor,\lceil 1,2,3\rfloor\lceil 4,5\rfloor,\lceil 1,3,2\rfloor\lceil 4,5\rfloor\lceil 7,8\rfloor\}.\end{aligned}$$

Сада по дефиницији имамо

$$\begin{aligned}\mathcal{O}_1&=\{\sigma\cdot 1\mid\sigma\in G\}\\&=\{\sigma(1)\mid\sigma\in G\}\\&=\{1,2,3\}.\end{aligned}$$

Слично је онда

$$\mathcal{O}_6=\{6\}\quad\text{и}\quad\mathcal{O}_7=\{7,8\}.$$

Даље за стабилизаторе имамо

$$\begin{aligned}\mathrm{Stab}(2)&=\{\sigma\in G\mid\sigma\cdot 2=2\}\\&=\{\sigma\in G\mid\sigma(2)=2\}\\&=\{\varepsilon,\lceil 7,8\rfloor,\lceil 4,5\rfloor,\lceil 4,5\rfloor\lceil 7,8\rfloor\}\\&=\langle\lceil 4,5\rfloor,\lceil 7,8\rfloor\rangle,\end{aligned}$$

као и

$$\begin{aligned}\mathrm{Stab}(4)&=\{\varepsilon,\lceil 1,2,3\rfloor\lceil 7,8\rfloor,\lceil 1,3,2\rfloor,\lceil 7,8\rfloor,\lceil 1,2,3\rfloor,\lceil 1,3,2\rfloor\lceil 7,8\rfloor\}\\&=\langle\lceil 1,2,3\rfloor\lceil 7,8\rfloor\rangle.\end{aligned}$$

Коначно за фиксне скупове имамо

$$\mathrm{Fix}(\lceil 4,5\rfloor)=\{n\in S\mid\lceil 4,5\rfloor\cdot n=n\}=\{1,2,3,6,7,8\}$$

и

$$\mathrm{Fix}(\lceil 1,2,3\rfloor\lceil 7,8\rfloor)=\{4,5,6\}.$$

□

Задатак 18. Нека је G група која дејствује на скупове X и Y. Тада је са

$$g\cdot(x,y)=(g\cdot x,g\cdot y),\ \ g\in G, x\in X, y\in Y$$

дефинисано једно дејство групе G на Декартов производ $X\times Y$ које се назива дијагонално дејство. Одредити стабилизатор за $(x,y)\in X\times Y$ при овом дејству.

Решење. Рачунамо директно по дефиницији:

$$\begin{aligned}\operatorname{Stab}(x,y) &= \{g \in G \mid g \cdot (x,y) = (x,y)\} \\ &= \{g \in G \mid (g \cdot x, g \cdot y) = (x,y)\} \\ &= \{g \in G \mid g \cdot x = x, g \cdot y = y\} \\ &= \{g \in G \mid g \in \operatorname{Stab}(x), g \in \operatorname{Stab}(y)\} \\ &= \operatorname{Stab}(x) \cap \operatorname{Stab}(y).\end{aligned}$$

□

Нека је $\cdot$ дејство групе G на скуп S. Тада је за произвољне $x, y \in S$ са $x \sim y$ ако и само ако постоји $g \in G$ такво да је $y = g \cdot x$ дефинисана једна релација на S. Штавише, та релација је релација еквиваленције, чије су класе орбите при дејству које посматрамо. Одатле закључујемо да скуп свих орбита чини једну партицију скупа S. Ако је T једна трансверзала те партиције (то је скуп који садржи тачно по једног представника сваке класе тј. орбите), онда из претходног закључка имамо:

$$\sum_{x \in T} |\mathcal{O}_x| = |S| \quad \text{(класна једначина)}.$$

Тврђење 3.2 (Теорема о орбити и стабилизатору)**.** Нека је G група која дејствује на скуп S. Тада за свако $x \in S$ важи:

- $\operatorname{Stab}(x)$ је подгрупа од G.
- $[G : \operatorname{Stab}(x)] = |\mathcal{O}_x|$.
- Ако је G коначна група, онда је $|G| = |\operatorname{Stab}(x)||\mathcal{O}_x|$.

Тврђење 3.3 (Бернсајдова лема)**.** Нека је G коначна група која дејствује на коначан скуп S. Тада важи:

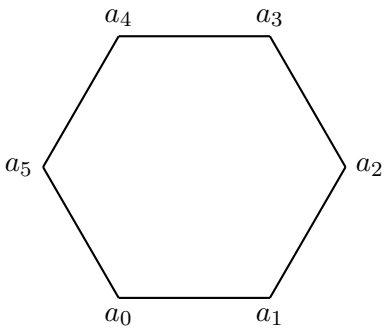
$$|S/G| = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|.$$

Задатак 19. Одредити на колико начина се могу обојити темена правилног шестоугла са n боја ако су два бојења иста када се једног од другог може добити:
а) ротацијом шестоугла.
б) произвољном изометријом шестоугла.

Решење. а) Нека је S скуп свих могућих бојења темена шестоугла. Тада можемо записати:

$$S = \{(a_0, a_1, a_2, a_3, a_4, a_5) \mid 1 \leq a_i \leq n\},$$

при чему $a_i = k$ значи да је i-то теме обојено k-том бојом. Приметимо да је $|S| = n^6$. Ситауацију можемо представити и шестоуглом на слици:



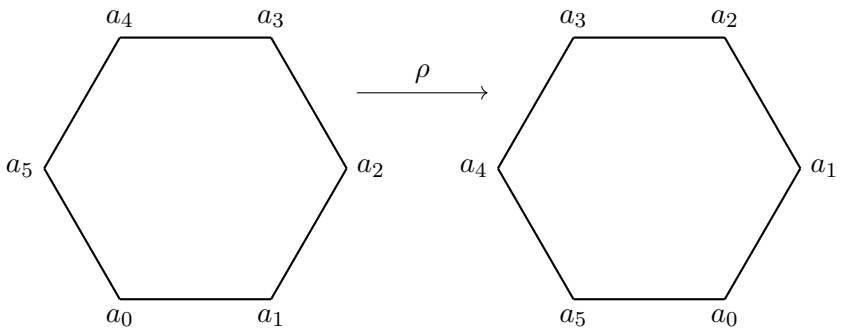
Подгрупа свих ротација $\langle\rho\rangle$ групе $\mathbb{D}_6$ дејствује на скуп S ротирајући темена шестоугла. При томе су два бојења иста ако и само ако се налазе у истој орбити при овом дејству. Дакле, треба да израчунамо број орбита $|S/\langle\rho\rangle|$. Из Бернсајдове леме је

$$\begin{aligned}|S/\langle\rho\rangle| &= \frac{1}{|\langle\rho\rangle|}\sum_{g\in\langle\rho\rangle}|\operatorname{Fix}(g)| \\ &= \frac{1}{6}\sum_{i=0}^{5}\left|\operatorname{Fix}(\rho^i)\right|.\end{aligned}$$

Све што је још потребно да урадимо је да израчунамо колико се елемената налази у фиксним скуповима које смо добили.

За $i = 0$ имамо да је $\rho^i = \varepsilon$, па сви елементи скупа S остају фиксирани. Дакле, $|\operatorname{Fix}(\varepsilon)| = n^6$.

За $i = 1$ имамо елемент ρ који представља ротацију за $60°$ око центра шестоугла у смеру супротном од смера кретања казаљке на сату. Његово дејство можемо представити сликом испод. Бојења у фиксном скупу су она која при овом дејству остају



инваријантна. То значи да прва и друга слика морају бити исте, одакле добијамо услове

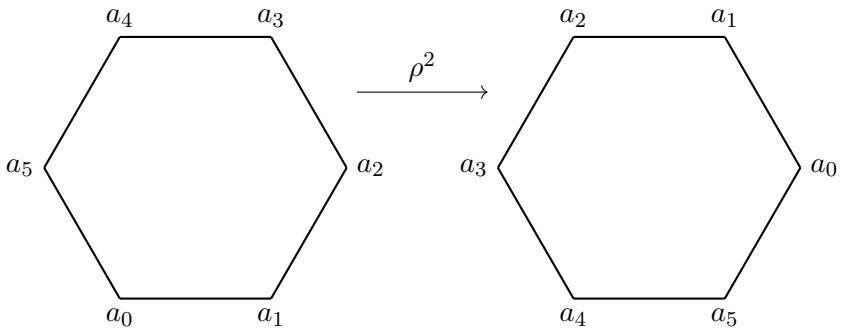
$$a_0 = a_5, a_1 = a_0, a_2 = a_1, a_3 = a_2, a_4 = a_3, a_5 = a_4.$$

Закључујемо да важи

$$a_0 = a_1 = a_2 = a_3 = a_4 = a_5 = \alpha,\ 1 \leq \alpha \leq n,$$

па је $|\mathrm{Fix}(\rho)| = n$.

Слично даље за $n = 2$, имамо дејство елемента ρ^2 кога представљамо сликом:



Из једнакости прве и друге слике добијамо услове

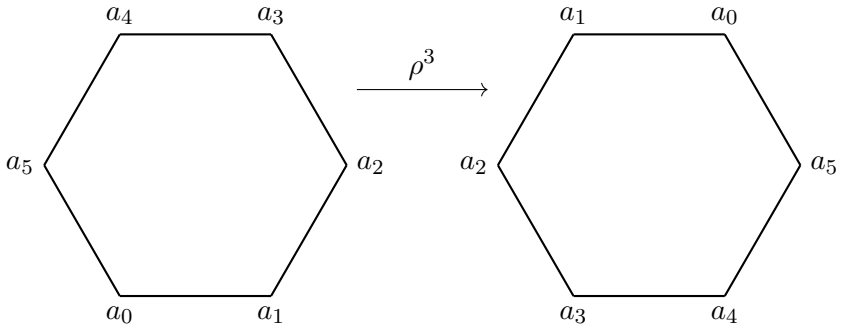
$$a_0 = a_4, a_1 = a_5, a_2 = a_0, a_3 = a_1, a_4 = a_2, a_5 = a_3.$$

Закључујемо да је

$$a_0 = a_2 = a_4 = \alpha,\ \ a_1 = a_3 = a_5 = \beta,\ \ 1 \leq \alpha, \beta \leq n,$$

па је $|\mathrm{Fix}(\rho^2)| = n^2$.

За $n = 3$ је дејство елемента ρ^3 представљено сликом:



Из једнакости прве и друге слике добијамо услове

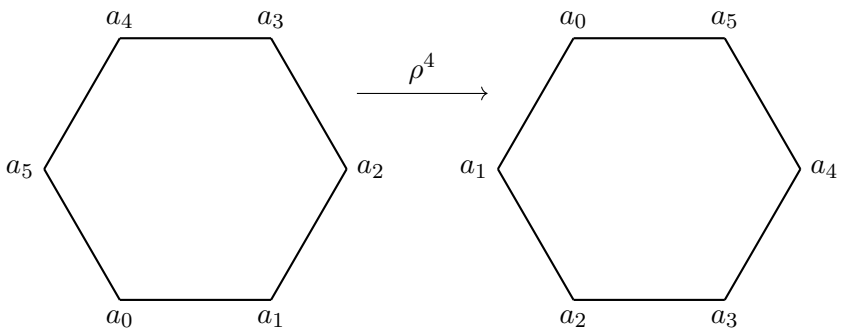
$$a_0 = a_3, a_1 = a_4, a_2 = a_5, a_3 = a_0, a_4 = a_1, a_5 = a_2.$$

Закључујемо да је

$$a_0 = a_3 = \alpha,\ \ a_1 = a_4 = \beta, a_2 = a_5 = \gamma\ \ 1 \leq \alpha, \beta, \gamma \leq n,$$

па је $|\mathrm{Fix}(\rho^3)| = n^3$.

За $n = 4$ је дејство елемента ρ^4 представљено сликом:



Из једнакости прве и друге слике добијамо услове

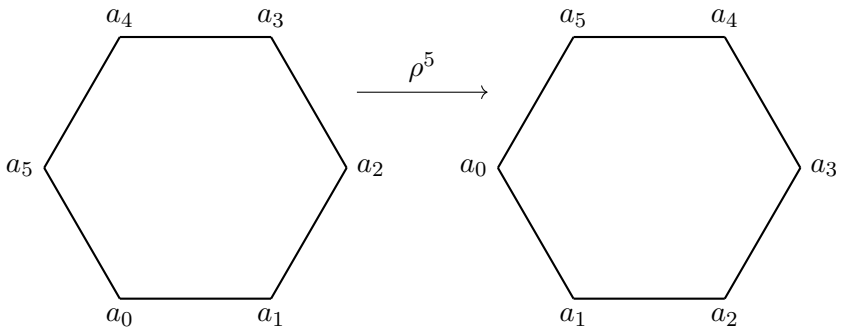
$$a_0 = a_2, a_1 = a_3, a_2 = a_4, a_3 = a_5, a_4 = a_0, a_5 = a_1.$$

Закључујемо да је

$$a_0 = a_2 = a_4 = \alpha,\ \ a_1 = a_3 = a_5 = \beta,\ \ 1 \leq \alpha, \beta \leq n,$$

па је $|\operatorname{Fix}(\rho^4)| = n^2$.

Коначно за $n = 5$ је дејство елемента ρ^5 представљено сликом:



Из једнакости прве и друге слике добијамо услове

$$a_0 = a_1, a_1 = a_2, a_2 = a_3, a_3 = a_4, a_4 = a_5, a_5 = a_0.$$

Закључујемо да важи

$$a_0 = a_1 = a_2 = a_3 = a_4 = a_5 = \alpha,\ \ 1 \leq \alpha \leq n,$$

па је $|\operatorname{Fix}(\rho^5)| = n$.

Када све сумирамо, добијамо да је број тражених бојења једнак

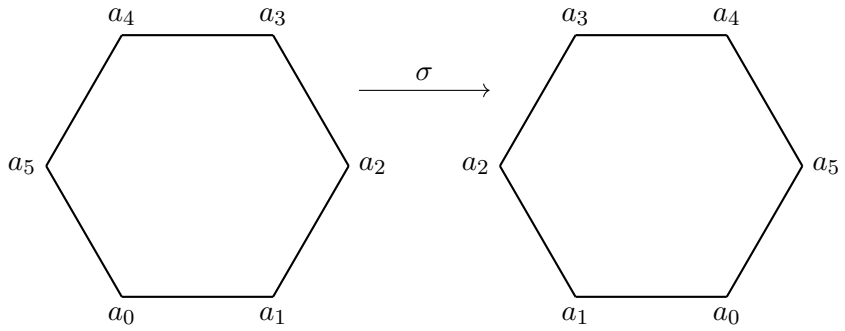
$$\frac{1}{6}\left(n^6 + n^3 + 2n^2 + 2n\right).$$

б) Све је исто као у делу а), само што сада уместо дејства подгрупе $\langle\rho\rangle$, посматрамо дејство целе групе $\mathbb{D}_6$. На основу Бернасајдове леме добијамо да је број тражених бојења једнак

$$\frac{1}{|\mathbb{D}_6|}\sum_{g\in\mathbb{D}_6}|\operatorname{Fix}(g)| = \frac{1}{12}\sum_{g\in\mathbb{D}_6}|\operatorname{Fix}(g)|.$$

Кардиналности фиксних скупова ротација смо већ одредили у делу а), па остаје само још да их одредимо за рефлексије.

Рефлексија σ је у односу на вертикалну осу шестоугла, па је њено дејство представљено сликом:

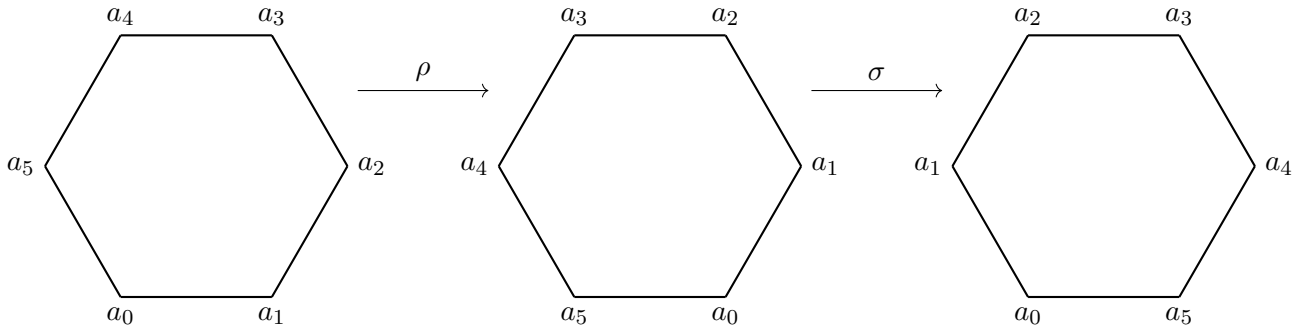


Из једнакости прве и друге слике закључујемо да важи

$$a_0 = a_1 = \alpha,\ \ a_2 = a_5 = \beta,\ \ a_3 = a_4 = \gamma,\ \ 1 \le \alpha, \beta, \gamma \le n,$$

па је $|\operatorname{Fix}(\sigma)| = n^3$.

Дејство рефлексије $\sigma\rho$ је представљено сликом:

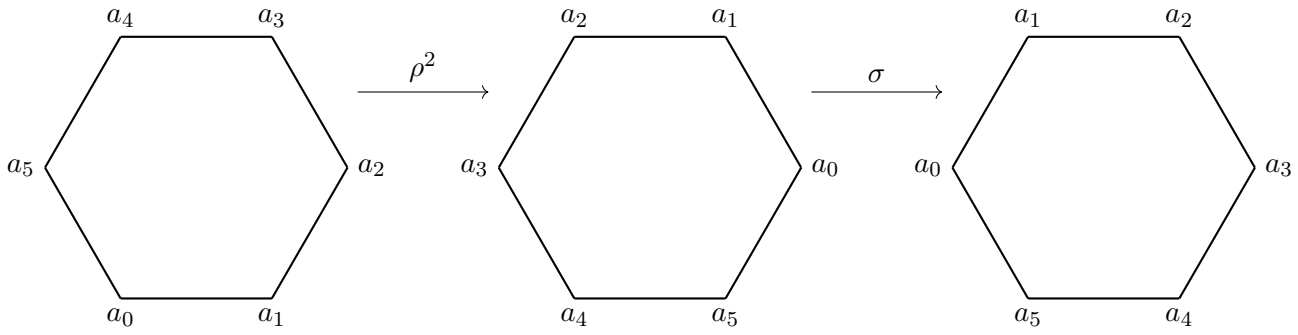


Из једнакости прве и *треће* слике закључујемо да важи

$$a_0 = \alpha,\ \ a_1 = a_5 = \beta,\ \ a_2 = a_4 = \gamma,\ \ a_3 = \delta,\ \ 1 \le \alpha, \beta, \gamma, \delta \le n,$$

па је $|\operatorname{Fix}(\sigma\rho)| = n^4$.

Дејство рефлексије $\sigma\rho^2$ је представљено сликом:

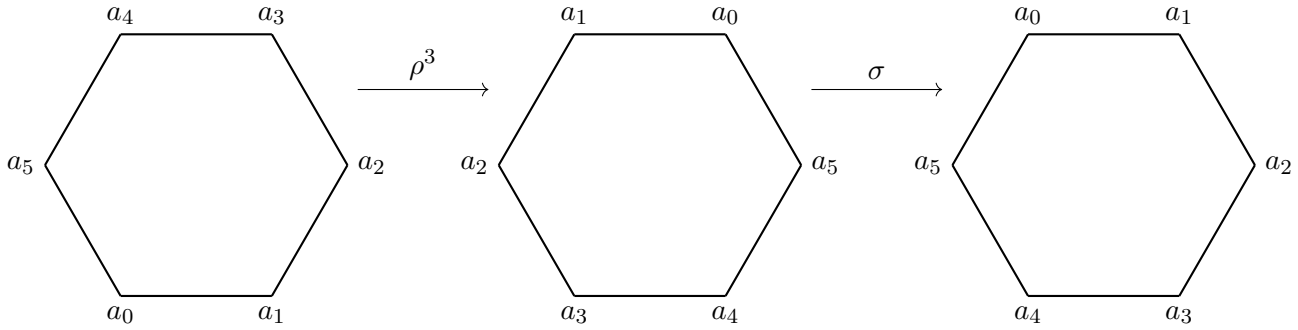


Из једнакости прве и треће слике закључујемо да важи

$$a_0 = a_5 = \alpha,\ \ a_1 = a_4 = \beta,\ \ a_2 = a_3 = \gamma,\ \ 1 \leq \alpha, \beta, \gamma \leq n,$$

па је $|\operatorname{Fix}(\sigma\rho^2)| = n^3$.

Дејство рефлексије $\sigma\rho^3$ је представљено сликом:

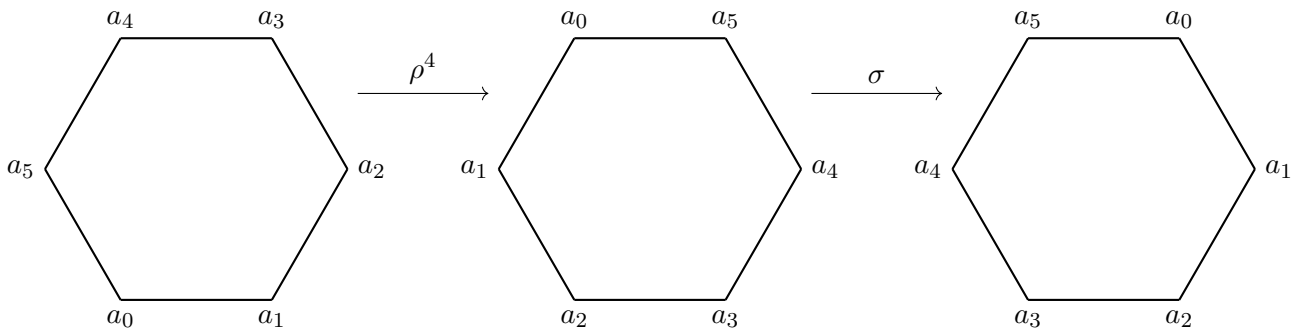


Из једнакости прве и треће слике закључујемо да важи

$$a_0 = a_4 = \alpha,\ \ a_1 = a_3 = \beta,\ \ a_2 = \gamma,\ \ a_5 = \delta,\ \ 1 \leq \alpha, \beta, \gamma, \delta \leq n,$$

па је $|\operatorname{Fix}(\sigma\rho^3)| = n^4$.

Дејство рефлексије $\sigma\rho^4$ је представљено сликом:

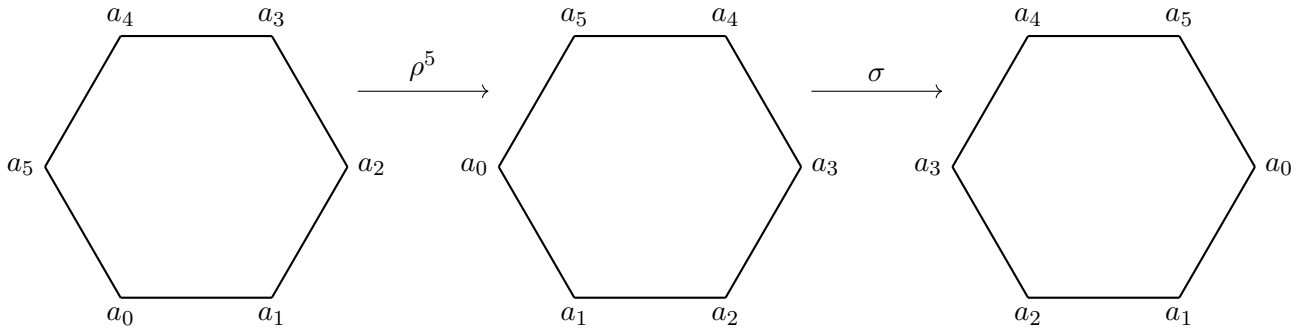


Из једнакости прве и треће слике закључујемо да важи

$$a_0 = a_3 = \alpha,\ \ a_1 = a_2 = \beta,\ \ a_4 = a_5 = \gamma,\ \ 1 \leq \alpha, \beta, \gamma \leq n,$$

па је $|\operatorname{Fix}(\sigma\rho^4)| = n^3$.

Коначно, дејство рефлексије $\sigma\rho^5$ је представљено сликом:



Из једнакости прве и треће слике закључујемо да важи

$$a_0 = a_2 = \alpha,\ \ a_1 = \beta,\ \ a_3 = a_5 = \gamma,\ \ a_4 = \delta,\ \ 1 \leq \alpha, \beta, \gamma, \delta \leq n,$$

па је $|\operatorname{Fix}(\sigma\rho^5)| = n^4$.

Када све сумирамо, добијамо да је број тражених бојења једнак

$$\frac{1}{12}\left(n^6 + 3n^4 + 4n^3 + 2n^2 + 2n\right).$$

□

Задатак 20. Нека је G коначна група која дејствује на коначан скуп S, $|S| \geq 2$, при чему при том дејству постоји само једна орбита. Доказати да постоји $g \in G$ такво да је $\operatorname{Fix}(g) = \emptyset$.

Решење. Из Бернсајдове леме имамо

$$|S/G| = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|.$$

Како је само једна орбита при дејству које посматрајмо, из претходног добијамо

$$|G| = \sum_{g \in G} |\operatorname{Fix}(g)|. \tag{4}$$

Ако би за све $g \in G$ било $\operatorname{Fix}(g) \neq \emptyset$, онда би сваки од сабирака са десне стране једнакости (4) био барем 1. Како је тих сабирака тачно $|G|$, то је могуће само ако су сви једнаки 1. Међутим, за $g = e$ имамо $\operatorname{Fix}(e) = S$, па је $|\operatorname{Fix}(e)| = |S| \geq 2$. Одатле закључујемо да је немогуће да за све $g \in G$ важи $\operatorname{Fix}(g) \neq \emptyset$, па постоји барем једно $g \in G$ такво да је $\operatorname{Fix}(g) = \emptyset$.
□

Задатак 21. Нека је G група реда 21 која дејствује на скуп X кардиналности 11. Доказати да постоји $x \in X$ такво да је $g \cdot x = x$ за све $g \in G$.

Решење. Претпоставимо супротно, нека за свако $x \in X$ постоји $g \in G$ такво да је $g \cdot x \neq x$. То значи да при овом дејству нема једночланих орбита. Из Теореме о орбити и стабилизатору следи да за све $x \in X$ важи:

$$|\mathcal{O}_x| \mid |G| \quad \text{тј.} \quad |\mathcal{O}_x| \mid 21.$$

Већ смо видели да орбите не могу бити једночлане, а пошто је свака орбита садржана у скупу X кардиналност 11, оне не могу имати ни 21 елемент. Закључујемо да орбите могу имати 3 или 7 елемената.

Из класне једначине добијамо даље

$$\sum_{x \in T} |\mathcal{O}_x| = |X| \quad \text{тј.} \quad \sum_{x \in T} |\mathcal{O}_x| = 11.$$

Према томе, добили смо да се број 11 може представити као нека сума тројки и седмица. То је немогуће, па добијена контрадикција показује да постоји тражено $x \in X$ такво да је $g \cdot x = x$ за све $g \in G$.
□

Задатак 22. Доказати да за произвољну коначну групу G важи

$$|G| = |Z(G)| + \sum_{\substack{a \in T \\ a \notin Z(G)}} \frac{|G|}{|C_G(a)|},$$

где је T трансверзала партиције групе G на класе конјугације, $Z(G)$ центар групе G и $C_G(a) = \{g \in G \mid ag = ga\}$ централизатор елемента $a \in G$.

Решење. Посматрајмо дејство групе G на саму себе конјугацијом,

$$g \cdot a = g^{-1}ag, \;\; g, a \in G.$$

Орбита и стабилизатор за произвољно $a \in G$ при овом дејству су редом

$$\begin{aligned}
\mathcal{O}_a &= \{g \cdot a \mid g \in G\} \\
&= \{g^{-1}ag \mid g \in G\} \ \rightarrow \text{ класа конјугације за } a \\
\mathrm{Stab}(a) &= \{g \in G \mid g \cdot a = a\} \\
&= \{g \in G \mid g^{-1}ag = a\} \\
&= \{g \in G \mid ag = ga\} = C_G(a).
\end{aligned}$$

Из класне једначине имамо

$$|G| = \sum_{a \in T} |\mathcal{O}_a|,$$

где је T трансверзала партиције групе G на класе конјугације. Приметимо да су класе конјугације елемената из центра једночлане, пошто они комутирају са свим елементима из G. Зато даље имамо

$$\begin{aligned}
|G| &= \sum_{a \in Z(G)} 1 + \sum_{\substack{a \in T \\ a \notin Z(G)}} |\mathcal{O}_a| \\
&= |Z(G)| + \sum_{\substack{a \in T \\ a \notin Z(G)}} |\mathcal{O}_a|.
\end{aligned}$$

Коначно, из теореме о орбити и стабилизатору важи $|\mathcal{O}_a| = \frac{|G|}{|\mathrm{Stab}(a)|} = \frac{|G|}{|C_G(a)|}$, што заменом у последњу једнакост даје тражено тврђење.
□

Дефиниција 3.4. Нека је p прост број. Група реда p^n, $n \in \mathbb{N}$ се назива p-група.

Задатак 23. Доказати да p-групе имају нетривијалан центар.

Решење. Нека је G једна p-група, $|G| = p^n$ за неко $n \in \mathbb{N}$. Из претходног задатка имамо

$$p^n = |Z(G)| + \sum_{\substack{a \in T \\ a \notin Z(G)}} \frac{p^n}{|C_G(a)|}. \tag{5}$$

Приметимо да за све елементе $a \notin Z(G)$ важи $C_G(a) \neq G$. Како је и сваки централизатор подгрупа од G, закључујемо да су редови свих централизатора $C_G(a)$ за $a \notin Z(G)$ неки степени броја p, мањи од p^n. Према томе, у суми

$$\sum_{\substack{a \in T \\ a \notin Z(G)}} \frac{p^n}{|C_G(a)|}$$

су сви чланови дељиви са p, па је и та сума дељива са p. Из (5) онда следи да и $p \mid |Z(G)|$. Због тога је $Z(G)$ нетривијалан.
□

Дефиниција 3.5. Група се назива простом ако нема правих нормалних подгрупа.

Тврђење 3.6 (Кошијева лема)**.** Нека је G коначна група и p прост број који дели $|G|$. Тада у G постоји елемент реда p.

Задатак 24. Нека је G једна p-група таква да је $|G| \geq p^2$. Доказати да G није проста.

Решење. На основу Задатка 23 имамо да је $|Z(G)| > 1$. Зато, у случају да је $Z(G) \neq G$, имамо да је $Z(G)$ права нормална подгрупа од G. Према томе, у том случају група G није проста.

Остаје још да испитамо шта се дешава када је $Z(G) = G$. У том случају је G Абелова група, па је свака њена подгрупа нормална. На основу Кошијеве леме можемо пронаћи елемент a реда p у G. Тада је подгрупа $H = \langle a \rangle$ од G реда p, па представља једну праву нормалну подгрупу од G. Дакле, ни у овом случају група G није проста.
□

Задатак 25. Доказати да су p-групе решиве.

Решење. Нека је G једна p-група, $|G| = p^n$ за неко $n \in \mathbb{N}$. Доказ изводимо индукцијом по n.
база индукције:
За $n = 1$, имамо да је $|G| = p$, па је $G \cong \mathbb{Z}_p$. Зато је, специјално, G Абелова група, а тиме и решива.
индукцијска хипотеза: Претпоставимо да су све групе реда p^k решиве за све $1 \leq k \leq n$.
индукцијски корак: Доказујемо да је онда и произвољна група G реда p^{n+1} решива. На основу Задатка 23 имамо да је $|Z(G)| > 1$.

Ако је $Z(G) = G$, онда је G Абелова група, па је и решива.

Ако је $Z(G) \neq G$, из Лагранжеве теореме имамо да је $|Z(G)| = p^k$ за неко $1 \leq k \leq n$. На основу индукцијске хипотезе онда следи да је $Z(G)$ решива група. Такође,

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^{n+1}}{p^k} = p^{n+1-k}.$$

Како је $1 \leq k \leq n$, следи $1 \leq n+1-k \leq n$, па је и група $G/Z(G)$ решива на основу индукцијске хипотезе. Према томе, групе $Z(G)$ и $G/Z(G)$ су решиве, па је на основу Теореме 2.10 решива и група G.

На основу принципа математичке индукције закључујемо да су све p-групе решиве.
□

Задатак 26. Нека је p прост број. Одредити, до на изоморфизам, све групе реда p^2.

Решење. Нека је $|G| = p^2$. На основу Задатка 23 знамо да је $|Z(G)| > 1$, па нам остаје $|Z(G)| \in \{p, p^2\}$.

Претпоставимо прво да је $|Z(G)| = p$. Тада је и $|G/Z(G)| = p$, па је та количничка група циклична. Означимо са $aZ(G)$, $a \notin Z(G)$ неки њен генератор. За произвољно $y \in G$, онда постоји $k \in \mathbb{Z}$ такво да је $yZ(G) = a^k Z(G)$. Одатле можемо закључити да $y^{-1}a^k \in Z(G)$. Сада, за комутатор елемената y и a имамо:

$$yay^{-1}a^{-1} = ya\underbrace{y^{-1}a^k}_{\in Z(G)}a^{-k}a^{-1} = yy^{-1}a^k aa^{-k-1} = e.$$

Закључујемо да елементи y и a комутирају. Због произвољности елемента y онда следи да је $a \in Z(G)$. То даје контрадикцију која показује да је немогуће да $Z(G)$ има p елемената.

Остаје нам само могућност $|Z(G)| = p^2$. Тада је $Z(G) = G$, па је G Абелова група. Због тога добијамо да, до на изоморфизам, постоје тачно две групе реда p^2 и то су

$$\mathbb{Z}_{p^2} \quad \text{и} \quad \mathbb{Z}_p \times \mathbb{Z}_p.$$

□

Дефиниција 3.7. Нека је G група. Језгро подгрупе H од G дефинишемо са

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

Тврђење 3.8. Нека је H подгрупа групе G. Тада:

- $\operatorname{Core} H \leq H$
- $\operatorname{Core} H \triangleleft G$
- Ако је $N \leq H$ и $N \triangleleft G$, онда је $N \leq \operatorname{Core} H$.

Приметимо да из претходног тврђења следи да је подгрупа H нормална у G ако и само ако је $H = \operatorname{Core} H$.

Теорема 3.9 ($n!$- теорема)**.** Нека је H подгрупа групе G таква да је индекс $[G : H] = n$ коначан. Тада $[G : \operatorname{Core} H] \mid n!$.

Тврђење 3.10. Нека је H подгрупа групе G, таква да је индекс $[G : H]$ најмањи прост број који дели $|G|$. Тада је $H \triangleleft G$.

Задатак 27. Нека је G група реда pq, где су $p < q$ прости бројеви. Доказати да G није проста.

Решење. На основу Кошијеве леме можемо пронаћи елемент a реда q у G. Означимо $H = \langle a \rangle$. Тада је H подгрупа реда q од G, чији је индекс

$$[G : H] = \frac{|G|}{|H|} = \frac{pq}{q} = p.$$

Како је p најмањи прост број који дели $|G|$, закључујемо да је $H \triangleleft G$. Због тога група G није проста.
□

4 Теореме Силова

Дефиниција 4.1. Нека је G коначна група и p прост број који дели $|G|$. Подгрупа од реда p^k, где $p^k \mid |G|$ и $p^{k+1} \nmid |G|$ се назива Силовљева p-подгрупа или S_p подгрупа од G.

Пример 4.2. У групи реда $500 = 2^2 \cdot 5^3$ можемо посматрати S_2 и S_5 подгрупе. Под условом да постоје, S_2 подгрупе су реда 4, а S_5 подгрупе су реда 125.
□

Пример 4.3. У цикличној групи $\mathbb{Z}_{12}$ постоји јединствена S_2 подгрупа која је реда 4 и једнака $\{0, 3, 6, 9\}$, као и јединствена S_3 подгрупа која је реда 3 и једнака $\{0, 4, 8\}$.
□

Теорема 4.4 (Прва теорема Силова)**.** Нека је G коначна група и p прост број који дели $|G|$. Тада постоји S_p подгрупа од G.

Теорема 4.5 (Друга теорема Силова)**.** Нека је G коначна група и p прост број који дели $|G|$. Тада:

- Свака p-подгрупа од G је садржана у некој S_p подгрупи од G.
- Сваке две S_p подгрупе од G су међусобно конјуговане.

Друга теорема Силова ће нам бити од највећег значаја у једном специјалном случају. Претпоставимо да за неку групу G постоји јединствена S_p подгрупа H. Тада нам Друга теорема Силова говори да се конјугацијом подгрупе H увек добија нека S_p подгрупа од G, што у овом случају мора бити поново H. Према томе, подгрупа H је инваријантна у односу на конјугацију, па имамо $H \triangleleft G$. Тиме смо показали следећу значајну последицу коју ћемо често користити.

Последица. Нека је G коначна група и p прост број који дели $|G|$. Ако је S_p подгрупа H од G јединствена, онда је $H \triangleleft G$.

Теорема 4.6 (Трећа теорема Силова)**.** Означимо са s_p број S_p подгрупа коначне групе G и запишимо $|G| = p^k m$, $p \nmid m$. Тада:

- $s_p \equiv 1 \pmod{p}$.
- $s_p \mid m$.

Задатак 28. Испитати да ли Силовљеве подгрупе од $\mathbb{S}_4 \times \mathbb{Z}_3$ могу бити цикличне.

Решење. Имамо да је $|\mathbb{S}_4 \times \mathbb{Z}_3| = 72 = 2^3 \cdot 3^2$, па можемо посматрати S_2 и S_3 подгрупе од $\mathbb{S}_4 \times \mathbb{Z}_3$. Прво, S_2 подгрупе (које постоје на основу Прве теореме Силова) су реда 8, па ће бити цикличне ако у групи $\mathbb{S}_4 \times \mathbb{Z}_3$ постоје елементи реда 8. Слично, S_3 подгрупе су реда 9, па ће оне бити цикличне ако у $\mathbb{S}_4 \times \mathbb{Z}_3$ постоје елементи реда 9. Међутим, редови елемената у $\mathbb{S}_4 \times \mathbb{Z}_3$ могу бити $\{1, 2, 3, 4, 6, 12\}$, па закључујемо да $\mathbb{S}_4 \times \mathbb{Z}_3$ нема цикличних Силовљевих подгрупа.
□

Задатак 29. Нека је G група реда pq^k где су p и q прости бројеви такви да је $p < q$. Доказати да група G није проста.

Решење. На основу Прве теореме Силова можемо уочити S_q подгрупу H од G. Тада је $|H| = q^k$, па је $[G : H] = p$. Пошто је p најмањи прост број који дели $|G|$ закључујемо да је $H \triangleleft G$. Одатле следи да група G није проста.
□

Задатак 30. Одредити, до на изоморфизам, све групе реда pq, где су p и q различити прости бројеви такви да је $p < q$ и $p \nmid q - 1$.

Решење. Нека је $|G| = pq$. На основу Прве теореме Силова можемо уочити S_q подгрупу H од G. Тада је $|H| = q$, па је $H \cong \mathbb{Z}_q$. Приметимо и да је $[G : H] = p$, па пошто је p најмањи прост број који дели $|G|$ закључујемо да је $H \triangleleft G$.

Даље из Треће теореме Силова имамо

$$\begin{aligned} s_p &\equiv 1 \pmod{p} \\ s_p &\mid q. \end{aligned}$$

Пошто је q прост број из другог услова имамо $s_p \in \{1, q\}$. Ако би било $s_p = q$, из првог услова бисмо добили $q \equiv 1 \pmod{p}$, одакле би следило $p \mid q - 1$. То је немогуће из претпоставке задатка, па закључујемо да је $s_p = 1$. На основу Друге теореме Силова (прецизније на основу њене последице коју смо видели), добијамо да је јединствена S_p подгрупа K нормална у G. Приметимо и да је $|K| = p$, па важи $K \cong \mathbb{Z}_p$.

Даље, можемо посматрајмо подгрупу $H \cap K$ од H и K. На основу Лагранжеве теореме следи

$$|H \cap K| \mid |H|, |K| \quad \text{тј.} \quad |H \cap K| \mid q, p.$$

Како су p и q различити прости бројеви, они су узајамно прости, па добијамо $|H \cap K| = 1$ тј. $H \cap K = \langle e \rangle$.

Посматрајмо сада подгрупу HK од G (штавише, ова подгрупа је нормална, јер су и H и K нормалне у G). Имамо

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{qp}{1} = pq = |G|.$$

Можемо закључити да важи $HK = G$.

Дакле, да сумирамо, имамо $H \triangleleft G$, $K \triangleleft G$, $H \cap K = \langle e \rangle$ и $HK = G$. На основу Теореме о разлагању следи

$$G \cong H \times K \cong \mathbb{Z}_q \times \mathbb{Z}_p \cong \mathbb{Z}_{pq}.$$

Према томе, под датим условима, до на изоморфизам, постоји само једна група реда pq и она је циклична.
□

Задатак 31. Нека је G група реда p^2q, где су p и q различити прости бројеви. Доказати да група G није проста.

Решење. Разликујемо два случаја у зависности од тога да ли је $p > q$ или $p < q$. У првом случају имамо да група G није проста на основу Задатка 29, па остаје само да се позабавимо другим случајем.

Из Треће теореме Силова имамо:

$$\begin{aligned} s_q &\equiv 1 \pmod{q} \\ s_q &\mid p^2. \end{aligned}$$

Пошто је p прост број из другог услова добијамо $s_q \in \{1, p, p^2\}$.

Ако је $s_q = 1$, на основу Друге теореме Силова следи да је јединствена S_q подгрупа нормална у G, па одмах имамо да група G није проста.

Ако је $s_q = p$, из првог услова следи $p \equiv 1 \pmod{q}$. Одавде добијамо $q|p-1$, што није могуће, јер је $p < q$.

Препоставимо да је $s_q = p^2$. Онда је $p^2 \equiv 1 \pmod{q}$, одакле следи $q|p^2 - 1$ тј. $q|(p-1)(p+1)$. Пошто је q прост број закључујемо да $q|p-1$ или $q|p+1$. Већ смо видели да $q \nmid p-1$, па нам остаје $q|p+1$. Још једном се ослањајући на чињеницу да су p и q прости бројеви такви да је $p < q$, добијамо да је $p = 2$ и $q = 3$.

Да сумирамо, имамо да или група G није проста или је $|G| = 12$, па задатак завршавамо да докажемо да група реда 12 не може бити проста. То ћемо издовијити у посебан задатак.

□

Задатак 32. Доказати да група реда 12 није проста.

Решење. Нека је G група реда 12. Означимо са H неку њену S_2 подгрупу. Тада је $|H| = 4$, па је $[G : H] = 3$. На основу $n!$-теореме онда следи

$$[G : \operatorname{Core} H] \mid 3! = 6.$$

Ако би било $\operatorname{Core} H = \langle e \rangle$, онда би важило $[G : \operatorname{Core} H] = |G| = 12$, па бисмо добили $12|6$. То је наравно немогуће, па закључујемо да је $\operatorname{Core} H$ једна права, нормална подгрупа од G. Због тога група G није проста.

□

Задатак 33. Нека су $p < q < r$ различити прости бројеви. Доказати да група G реда pqr није проста.

Решење. Из Треће теореме Силова имамо:

$$\begin{aligned} &s_p \equiv 1 \pmod{p} \\ &s_p \mid qr \end{aligned} \tag{6}$$

$$\begin{aligned} &s_q \equiv 1 \pmod{q} \\ &s_q \mid pr \end{aligned} \tag{7}$$

$$\begin{aligned} &s_r \equiv 1 \pmod{r} \\ &s_r \mid pq. \end{aligned} \tag{8}$$

Пошто су бројеви q и r прости, из услова (6) добијамо $s_p \in \{1, q, r, qr\}$. Слично, из услова (7) добијамо $s_q \in \{1, p, r, pr\}$. Међутим, ако би било $s_q = p$, онда би важило $p \equiv 1 \pmod{q}$. Одатле би следило $q \mid p-1$, што није могуће, јер је $p < q$. Према томе, остаје нам само $s_q \in \{1, r, pr\}$. На потпуно исти начин добијамо $s_r \in \{1, pq\}$.

Претпоставимо сада да је група G проста. Тада мора бити $s_p, s_q, s_r > 1$, па закључујемо да важи $s_p \geq q, s_q \geq r$ и $s_r = pq$. Означимо са H_i све S_p, са K_i све S_q и са L_i све S_r подгрупе од G. Приметимо да је за све i испуњено $|H_i| = p, |K_i| = q$ и $|L_i| = r$, а имамо и да важи следеће:

- $H_i \cap H_j = K_i \cap K_j = L_i \cap L_j = \langle e \rangle$ за све $i \neq j$
  Свакако важи да је $H_i \cap H_j$ подгрупа и од H_i и од H_j. Како су H_i и H_j обе реда p, њихове једине подгрупе су тривијална подгрупа $\langle e \rangle$ и оне саме. Пошто је $H_i \neq H_j$, друго је немогуће, па следи $H_i \cap H_j = \langle e \rangle$. Потпуно аналогно се ради за $K_i \cap K_j$ и $L_i \cap L_j$.

- $H_i \cap K_j = K_i \cap L_j = L_i \cap H_j = \langle e \rangle$ за све i и j
  Важи да је $H_i \cap K_j$ подгрупа од H_i и K_j, па на основу Лагранжеве теореме следи

  $$|H_i \cap K_j| \mid |H_i|, |K_j| \quad \text{тј.} \quad |H_i \cap K_j| \mid p, q.$$

  Како су p и q различити прости бројеви, они су узајамно прости, па добијамо $|H_i \cap K_j| = 1$ тј. $H_i \cap K_j = \langle e \rangle$. На потпуно исти начин радимо и за $K_i \cap L_j$ и $L_i \cap H_j$.

Посматрајмо сада скуп $\mathcal{S}$ у којем су сви елементи групе G који се налазе у једној од подгрупа H_i, K_i или L_i. Са једне стране, свакако је $\mathcal{S} \subseteq G$, па важи $|\mathcal{S}| \leq |G|$. Са друге стране, пошто смо видели да се све подгрупе H_i, K_i и L_i међусобно секу тривијално, добијамо да је

$$\begin{aligned} |\mathcal{S}| &= s_p(p-1) + s_q(q-1) + s_r(r-1) + 1 \\ &\geq q(p-1) + r(q-1) + pq(r-1) + 1 \\ &= pq - q + qr - r + pqr - pq + 1 \\ &= pqr + (q-1)(r-1) \\ &> pqr = |G|. \end{aligned}$$

Према томе, добили смо контрадикцију и она управо показује да група G није проста. □

Задатак 34. Нека је G група реда p^2q^2, где су $p < q$ прости бројеви. Доказати да група G није проста.

Решење. Из Треће теореме Силова имамо:

$$\begin{aligned} s_q &\equiv 1 \pmod{q} \\ s_q &\mid p^2. \end{aligned}$$

Пошто је p прост број из другог услова добијамо $s_q \in \{1, p, p^2\}$.

Ако је $s_q = 1$, на основу Друге теореме Силова следи да је јединствена S_q подгрупа нормална у G, па одмах имамо да група G није проста.

Ако је $s_q = p$, из првог услова следи $p \equiv 1 \pmod{q}$. Одавде добијамо $q|p-1$, што није могуће, јер је $p < q$.

Препоставимо да је $s_q = p^2$. Онда је $p^2 \equiv 1 \pmod{q}$, одакле следи $q|p^2 - 1$ тј. $q|(p-1)(p+1)$. Пошто је q прост број закључујемо да $q|p-1$ или $q|p+1$. Већ смо видели да $q \nmid p-1$, па нам остаје $q|p+1$. Још једном се ослањајући на чињеницу да су p и q прости бројеви такви да је $p < q$, добијамо да је $p = 2$ и $q = 3$.

Да сумирамо, имамо да или група G није проста или је $|G| = 36$, па задатак завршавамо да докажемо да група реда 36 не може бити проста. То ћемо издовијити у посебан задатак.
□

Задатак 35. Доказати да група реда 36 није проста.

Решење. Нека је G група реда 36. Означимо са H неку њену S_3 подгрупу. Тада је $|H| = 9$, па је $[G : H] = 4$. На основу $n!$-теореме онда следи

$$[G : \operatorname{Core} H] \mid 4! = 24.$$

Ако би било $\operatorname{Core} H = \langle e \rangle$, онда би важило $[G : \operatorname{Core} H] = |G| = 36$, па бисмо добили $36|24$. То је наравно немогуће, па закључујемо да је $\operatorname{Core} H$ једна права, нормална подгрупа од G. Због тога група G није проста.
□

Задатак 36. Нека је p непаран прост број. Доказати да група G реда $8p$ није проста.

Решење. Из Треће теореме Силова имамо:

$$\begin{aligned} s_p &\equiv 1 \pmod{p} \\ s_p &\mid 8. \end{aligned}$$

Из другог услова добијамо могућности $s_p \in \{1, 2, 4, 8\}$.

Ако је $s_p = 1$, на основу Друге теореме Силова следи да је јединствена S_p подгрупа нормална у G, па одмах имамо да група G није проста.

Ако је $s_p = 2$, из првог услова имамо да је $2 \equiv 1 \pmod{p}$, што није могуће.

Ако је $s_p = 4$, из првог услова имамо да је $4 \equiv 1 \pmod{p}$, што нам даје $p = 3$.

Ако је $s_p = 8$, из првог услова имамо да је $8 \equiv 1 \pmod{p}$, што нам даје $p = 7$.

Дакле, или група G није проста или је $|G| \in \{24, 56\}$. Преостала два случаја $|G| = 24$ и $|G| = 56$ издвајамо у посебне задатке.
□

Задатак 37. Доказати да група реда 24 није проста.

Решење. Нека је G група реда 24. Означимо са H неку њену S_2 подгрупу. Тада је $|H| = 8$, па је $[G : H] = 3$. На основу $n!$-теореме онда следи

$$[G : \operatorname{Core} H] \mid 3! = 6.$$

Ако би било $\operatorname{Core} H = \langle e \rangle$, онда би важило $[G : \operatorname{Core} H] = |G| = 24$, па бисмо добили $24|6$. То је наравно немогуће, па закључујемо да је $\operatorname{Core} H$ једна права, нормална подгрупа од G. Због тога група G није проста.
□

Задатак 38. Доказати да група реда 56 није проста.

Решење. Нека је $|G| = 56$. Из Треће теореме Силова имамо

$$\left.\begin{array}{ll} s_2 \equiv 1 & (\mathrm{mod}\ 2) \\ s_2 \mid 7 & \end{array}\right\} \longrightarrow s_2 \in \{1, 7\}$$
$$\left.\begin{array}{ll} s_7 \equiv 1 & (\mathrm{mod}\ 7) \\ s_7 \mid 8 & \end{array}\right\} \longrightarrow s_7 \in \{1, 8\}.$$

Претпоставимо да је група G проста. Тада мора бити $s_2 = 7$ и $s_7 = 8$. Означимо са H_i све S_7 подгрупе од G. Поред њих ћемо посматрати и две S_2 подгрупе K_1 и K_2 од G. Приметимо да је $|H_i| = 7$ и $|K_i| = 8$ за све i. Имамо следеће:

- $H_i \cap K_j = \langle e \rangle$ за све i и j
  Важи да је $H_i \cap K_j$ подгрупа од H_i и K_j, па на основу Лагранжеве теореме следи
  $$|H_i \cap K_j| \mid |H_i|, |K_j| \quad \text{тј.} \quad |H_i \cap K_j| \mid 7, 8.$$
  Како су бројеви 7 и 8 узајамно прости, следи $|H_i \cap K_j| = 1$ тј. $H_i \cap K_j = \langle e \rangle$.

- $H_i \cap H_j = \langle e \rangle$ за све $i \neq j$
  Важи да је $H_i \cap H_j$ подгрупа и од H_i и од H_j. Како су H_i и H_j обе реда 7, њихове једине подгрупе су тривијална подгрупа $\langle e \rangle$ и оне саме. Пошто је $H_i \neq H_j$, друго је немогуће, па следи $H_i \cap H_j = \langle e \rangle$.

Приметимо да пресек подгрупа K_1 и K_2 не мора бити тривијалан, пошто оне нису простог реда. Оне су реда 8 и различите, па из Лагранжеве теореме следи $|K_1 \cap K_2| \in \{1, 2, 4\}$. Пошто је $|K_1 \cup K_2| = |K_1| + |K_2| - |K_1 \cap K_2|$, добијамо

$$|K_1 \cup K_2| \geq 8 + 8 - 4 = 12.$$

Означимо сада са $\mathcal{S}$ скуп елемената из G који се налазе у некој од погрупа H_1, K_1 или K_2. Тада је $\mathcal{S} \subseteq G$, па имамо $|\mathcal{S}| \leq |G|$. Са друге стране, пошто се подгупе H_i међусобно и са подгрупама K_1 и K_2 секу тривијално, имамо да је

$$\begin{aligned} |\mathcal{S}| &= s_7(7-1) + |K_1 \cup K_2| \\ &\geq 8 \cdot 6 + 12 \\ &= 60 > |G|. \end{aligned}$$

Добијамо контрадикцију која показује да група G није проста.
□

Задатак 39. Доказати да група реда 48 није проста.

Решење. Нека је G група реда 48. Означимо са H неку њену S_2 подгрупу. Тада је $|H| = 16$, па је $[G : H] = 3$. На основу $n!$-теореме онда следи

$$[G : \operatorname{Core} H] \mid 3! = 6.$$

Ако би било $\operatorname{Core} H = \langle e \rangle$, онда би важило $[G : \operatorname{Core} H] = |G| = 48$, па бисмо добили $48|6$. То је наравно немогуће, па закључујемо да је $\operatorname{Core} H$ једна права, нормална подгрупа од G. Због тога група G није проста.
□

Последица (Последица до сада урађених задатака)**.** Ако је G група таква да је $|G| < 60$ и $|G|$ није прост број, онда група G није проста.

Из претходне последице закључујемо да, осим тривијалних случајева, међу групама реда мањег од 60 нема простих. Најмања проста група која није простог реда је алтернирајућа група $\mathbb{A}_5$ и она је управо реда 60.

Задатак 40. Нека је G група реда $5 \cdot 7 \cdot 17$. Доказати да је група G циклична.

Решење. Из Треће теореме Силова имамо:

$$\left.\begin{array}{l} s_5 \equiv 1 \pmod 5 \\ s_5 \mid 7 \cdot 17 \end{array}\right\} \longrightarrow s_5 = 1$$

$$\left.\begin{array}{l} s_7 \equiv 1 \pmod 7 \\ s_7 \mid 5 \cdot 17 \end{array}\right\} \longrightarrow s_7 \in \{1, 85\}$$

$$\left.\begin{array}{l} s_{17} \equiv 1 \pmod{17} \\ s_{17} \mid 5 \cdot 7 \end{array}\right\} \longrightarrow s_{17} \in \{1, 35\}.$$

Одмах можемо закључити да је јединствена S_5 подгрупа H нормална у G. Приметимо да је $|H| = 5$, па је $H \cong \mathbb{Z}_5$.

Докажимо још да мора бити $s_7 = 1$ или $s_{17} = 1$. За почетак ћемо претпоставити супротно; тада је $s_7 = 85$ и $s_{17} = 35$. Означимо са K_i све S_7 подгрупе и са L_i све S_{17} подгрупе од G. Тада је $|K_i| = 7$ и $|L_i| = 17$. Имамо и следеће:

- $K_i \cap L_j = \langle e \rangle$ за све i и j
  Важи да је $K_i \cap L_j$ подгрупа од K_i и L_j, па на основу Лагранжеве теореме следи

  $$|K_i \cap L_j| \mid |K_i|, |L_j| \quad \text{тј.} \quad |K_i \cap L_j| \mid 7, 17.$$

  Како су бројеви 7 и 17 узајамно прости, следи $|K_i \cap L_j| = 1$ тј. $K_i \cap L_j = \langle e \rangle$.

- $K_i \cap K_j = L_i \cap L_j = \langle e \rangle$ за све $i \neq j$
  Важи да је $K_i \cap K_j$ подгрупа и од K_i и од K_j. Како су K_i и K_j обе реда 7, њихове једине подгрупе су тривијална подгрупа $\langle e \rangle$ и оне саме. Пошто је $K_i \neq K_j$, друго је немогуће, па следи $K_i \cap K_j = \langle e \rangle$. Потпуно слично радимо и за $L_i \cap L_j$.

Означимо са $\mathcal{S}$ скуп елемената из G који се налазе у некој од погрупа K_i или L_i. Тада је $\mathcal{S} \subseteq G$, па имамо $|\mathcal{S}| \leq |G|$. Са друге стране, пошто се све подгупе K_i и L_i међусобно секу тривијално, добијамо да је

$$\begin{aligned} |\mathcal{S}| &= s_7(7-1) + s_{17}(17-1) + 1 \\ &= 85 \cdot 6 + 35 \cdot 16 + 1 \\ &= 1071 > |G|. \end{aligned}$$

Добијена контрадикција показује да је $s_7 = 1$ или $s_{17} = 1$. Фиксирајмо сада једну S_7 подгрупу K и S_{17} подгрупу L од G. Из претходног знамо да је барем једна од њих

јединствена, а тиме и нормална у G. Због тога је $M := KL$ подгрупа од G. Приметимо да је

$$|M| = |KL| = \frac{|K||L|}{|K \cap L|} = \frac{7 \cdot 17}{1} = 7 \cdot 17.$$

Како су 7 и 17 прости бројеви такви да $7 \nmid 17 - 1$ закључујемо да је подгрупа M циклична, $M \cong \mathbb{Z}_{7 \cdot 17}$ (на основу Задатка 30). Такође, важи да је $[G : M] = 5$, па како је 5 најмањи прост број који дели $|G|$, добијамо да је $M \triangleleft G$.

Испитајмо још однос подгрупе M са H. Пошто је $H \cap M$ подгрупа од H и M, из Лагранжеве теореме следи

$$|H \cap M| \mid |H|, |M| \quad \text{тј.} \quad |H \cap M| \mid 5, 7 \cdot 17.$$

Бројеви 5 и $7 \cdot 17$ су узајамно прости, одакле закључујемо $|H \cap M| = 1$ тј. $H \cap M = \langle e \rangle$. Можемо закључити и

$$|HM| = \frac{|H||M|}{|H \cap M|} = \frac{5 \cdot 7 \cdot 17}{1} = 5 \cdot 7 \cdot 17 = |G|.$$

Пошто је $HM \leq G$, добијамо $HM = G$. Дакле, да сумирамо, имамо да су $H, M \triangleleft G$, $H \cap M = \langle e \rangle$ и $HM = G$. Из Теореме о разлагању онда следи

$$G \cong H \times M \cong \mathbb{Z}_5 \times \mathbb{Z}_{7 \cdot 17} \cong \mathbb{Z}_{5 \cdot 7 \cdot 17}.$$

Према томе, доказали смо да је група G циклична.
□

Задатак 41. Нека је G група реда $2^2 \cdot 19 \cdot 37$. Доказати да тада:
а) G има нормалну подгрупу реда $19 \cdot 37$.
б) G има подгрупу индекса 2.

Решење. а) Из Треће теореме Силова имамо:

$$\left.\begin{array}{l} s_{19} \equiv 1 \pmod{19} \\ s_{19} \mid 2^2 \cdot 37 \end{array}\right\} \longrightarrow s_{19} = 1.$$

Закључујемо да је јединствена S_{19} подгрупа H нормална у G. Означимо са K неку S_{37} подгрупу од G. Тада је $HK \leq G$. Из Лагранжеве теореме, пошто је $H \cap K \leq H, K$ закључујемо

$$|H \cap K| \mid |H|, |K| \quad \text{тј.} \quad |H \cap K| \mid 19, 37.$$

Добијамо да је $|H \cap K| = 1$, одакле следи

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{19 \cdot 37}{1} = 19 \cdot 37.$$

Према томе, $M := HK$ је тражена подгрупа, уколико покажемо да је она нормална у G. Приметимо да је $[G : M] = 4$, па на основу $n!$-теореме следи

$$[G : \operatorname{Core} M] | 4!.$$

Дакле, имамо

$$\frac{|G|}{|\operatorname{Core} M|} \mid 24 \quad \text{тј.} \quad \frac{2^2 \cdot 19 \cdot 37}{|\operatorname{Core} M|} \mid 24.$$

Из последњег закључујемо да $19 \cdot 37 \mid |\operatorname{Core} M|$, па како је $\operatorname{Core} M \leq M$, добијамо $\operatorname{Core} M = M$. Због тога је подгрупа M нормална у G.
б) На основу Кошијеве леме у групи G можемо уочити елемент a реда 2. Означимо са L цикличну подгрупу од G генерисану са a. Тада је $|L| = 2$. Поред L посматрајмо подгрупу M из дела а). Како смо показали да је $M \triangleleft G$, важи да је $LM \leq G$.

Из Лагранжеве теореме, пошто је $L \cap M \leq L, M$ закључујемо

$$|L \cap M| \mid |L|, |M| \quad \text{тј.} \quad |L \cap M| \mid 2, 19 \cdot 37.$$

Добијамо да је $|L \cap M| = 1$, одакле следи

$$|LM| = \frac{|L||M|}{|L \cap M|} = \frac{2 \cdot 19 \cdot 37}{1} = 2 \cdot 19 \cdot 37.$$

Зато је LM индекса 2 у G и представља тражену подгрупу.
□

Задатак 42. Нека је G група реда $1947 = 3 \cdot 11 \cdot 59$.
а) Доказати да G има нормалну подгрупу реда 3 или реда 11.
б) Доказати да G има подгрупу реда $3 \cdot 11$. Да ли је она циклична?
в) Доказати да G има подгрупу реда $11 \cdot 59$. Да ли је она нормална?

Решење. а) Из Треће теореме Силова имамо:

$$\left.\begin{array}{l} s_3 \equiv 1 \pmod 3 \\ s_3 \mid 11 \cdot 59 \end{array}\right\} \longrightarrow s_3 \in \{1, 11 \cdot 59\}$$

$$\left.\begin{array}{l} s_{11} \equiv 1 \pmod{11} \\ s_{11} \mid 3 \cdot 59 \end{array}\right\} \longrightarrow s_{11} \in \{1, 3 \cdot 59\}.$$

Докажимо да мора бити $s_3 = 1$ или $s_{11} = 1$. У супротном је $s_3 = 11 \cdot 59$ и $s_{11} = 3 \cdot 59$. Означимо са H_i све S_3 подгрупе и са K_i све S_{11} подгрупе од G. Тада је $|H_i| = 3$ и $|K_i| = 11$. Имамо и следеће:

- $H_i \cap K_j = \langle e \rangle$ за све i и j
  Важи да је $H_i \cap K_j$ подгрупа од H_i и K_j, па на основу Лагранжеве теореме следи

  $$|H_i \cap K_j| \mid |H_i|, |K_j| \quad \text{тј.} \quad |H_i \cap K_j| \mid 3, 11.$$

  Како су бројеви 3 и 11 узајамно прости, следи $|H_i \cap K_j| = 1$ тј. $H_i \cap K_j = \langle e \rangle$.

- $H_i \cap H_j = K_i \cap K_j = \langle e \rangle$ за све $i \neq j$
  Важи да је $H_i \cap H_j$ подгрупа и од H_i и од H_j. Како су H_i и H_j обе реда 3, њихове једине подгрупе су тривијална подгрупа $\langle e \rangle$ и оне саме. Пошто је $H_i \neq H_j$, друго је немогуће, па следи $H_i \cap H_j = \langle e \rangle$. Потпуно слично радимо и за $K_i \cap K_j$.

Означимо са $\mathcal{S}$ скуп елемената из G који се налазе у некој од погрупа H_i или K_i. Тада је $\mathcal{S} \subseteq G$, па имамо $|\mathcal{S}| \leq |G|$. Са друге стране, пошто се све подгрупе H_i и K_i међусобно секу тривијално, добијамо да је

$$\begin{aligned} |\mathcal{S}| &= s_3(3-1) + s_{11}(11-1) + 1 \\ &= 11 \cdot 59 \cdot 2 + 3 \cdot 59 \cdot 10 + 1 \\ &= 3069 > |G|. \end{aligned}$$

Добијена контрадикција показује да је $s_3 = 1$ или $s_{11} = 1$. То значи да је барем једна од S_3 или S_{11} подгрупа јединствена, а тиме и нормална у G. Оне су управо реда 3 или 11, чиме завршавамо овај део.
б) Уочимо сада произвољну фиксирану S_3 подгрупу H и S_{11} подгрупу K од G. Тада је $|H| = 3$ и $|K| = 11$, а из дела а) знамо да је барем једна од њих нормална у G, као и да је $|H \cap K| = 1$. Због тога је $HK \leq G$ и

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{3 \cdot 11}{1} = 3 \cdot 11.$$

Дакле, HK представља тражену подгрупу. Пошто су 3 и 11 различити прости бројеви такви да $3 \nmid 11 - 1$, закључујемо да она јесте циклична (на основу Задатка 30).
в) Ослонимо се још једном на трећу теорему Силова да добијемо

$$\left.\begin{aligned} &s_{59} \equiv 1 \pmod{59} \\ &s_{59} \mid 3 \cdot 11 \end{aligned}\right\} \longrightarrow s_{59} = 1.$$

Закључујемо да је јединствена S_{59} подгрупа L нормална у G. Због тога је $KL \leq G$, где је K S_{11} подгрупа од G из дела б). Из Лагранжеве теореме, пошто је $K \cap L \leq K, L$ добијамо

$$|K \cap L| \mid |K|, |L| \quad \text{тј.} \quad |K \cap L| \mid 11, 59.$$

Добијамо да је $|K \cap L| = 1$, одакле следи

$$|KL| = \frac{|K||L|}{|K \cap L|} = \frac{11 \cdot 59}{1} = 11 \cdot 59.$$

Дакле, KL је тражена подгрупа. Пошто је њен индекс у G једнак 3, што је најмањи прост број који дели $|G|$, закључујемо да та подгрупа јесте нормална.
□

Наредних пар задатака ће нам дати још један метод за показивање да нека група није проста, који често ради у ситуацији када не функционише ништа што смо до сада видели.

Задатак 43. Нека је G проста група и H подгрупа од G индекса k. Тада је $G \leq \mathbb{S}_k$.

Решење. Посматрајмо дејство групе G на скуп G/H дефинисано са

$$g \cdot aH = gaH, \;\; g, a \in G.$$

Подсетимо се да ово дејство можемо видети и као хомоморфизам $\phi : G \to \mathrm{Sym}(G/H)$ дефинисан са

$$\phi(g) = \tau_g, \quad \text{где је } \tau_g : G/H \to G/H,\ \tau_g(aH) = gaH, a \in G.$$

Одредимо језгро овог хомоморфизма,

$$\begin{aligned}
\ker \phi &= \{g \in G \mid \phi(g) = \mathrm{id}_{G/H}\} \\
&= \{g \in G \mid \tau_g = \mathrm{id}_{G/H}\} \\
&= \{g \in G \mid gaH = aH \text{ за све } a \in G\} \\
&= \{g \in G \mid a^{-1}gaH = H \text{ за све } a \in G\} \\
&= \{g \in G \mid a^{-1}ga \in H \text{ за све } a \in G\} \\
&= \{g \in G \mid g \in aHa^{-1} \text{ за све } a \in G\} \\
&= \mathrm{Core}\, H.
\end{aligned}$$

Пошто је група G проста и $\mathrm{Core}\, H \leq H$, закључујемо да је $\mathrm{Core}\, H = \langle e \rangle$. Према томе, хомоморфизам ϕ има тривијално језгро, па је утапање. Због тога можемо сматрати да је $G \leq \mathrm{Sym}(G/H)$. Коначно, пошто је $[G : H] = k$, важи $\mathrm{Sym}(G/H) \cong \mathbb{S}_k$, чиме добијамо тражено $G \leq \mathbb{S}_k$.
□

Наредно тврђење је последица доказа треће теореме Силова.

Тврђење 4.7. Нека је K једна S_p подгрупа групе G и $N_G K$ нормализатор за G у K. Тада је

$$[G : N_G K] = s_p.$$

Задатак 44. Нека је p прост број такав да $p \mid k!$ и $p^2 \nmid k!$ и H једна S_p подгрупа од $\mathbb{S}_k$. Тада важи:

$$|N_{\mathbb{S}_k} H| = p(p-1)(k-p)!.$$

Решење. На основу Тврђења 4.7 имамо

$$[\mathbb{S}_k : N_{\mathbb{S}_k} H] = s_p,$$

одакле је

$$|N_{\mathbb{S}_k} H| = \frac{|\mathbb{S}_k|}{s_p} = \frac{k!}{s_p}. \tag{9}$$

Према томе, све што треба да одредимо је број s_p Силовљевих p-подгрупа од G. Пошто $p \mid k!$ и $p^2 \nmid k!$ имамо да су S_p подгрупе од G реда p. Оне су стога цикличне, генерисане елементима реда p.

Вративши се на услове $p \mid k!$ и $p^2 \nmid k!$ закључујемо да је $p \leq k < 2p$, па су p-циклови једини елементи реда p у $\mathbb{S}_k$. Одредимо њихов број m.

Пре свега, сваки p-цикл можемо видети као уређењу p-торку неких p изабраних елемената из скупа $\{1, 2, \ldots, k\}$. Број свих таквих p-торки је $\binom{k}{p}p!$. Међутим, ако се сви

елементи у некој p-торци ротирају за $1, 2, \ldots, p$ места удесно, одговарајући цикл остаје исти. То значи да сваком p-циклу одговара p различитих p-торки, па је

$$m = \binom{k}{p}\frac{p!}{p} = \binom{k}{p}(p-1)!.$$

Вратимо се сада на S_p подгрупе. Оне су цикличне, реда p и број њихових генератора је $p-1$. Наравно, сви њихови генератори су p-циклови, па закључујемо да свакој фиксираној S_p подгрупи одговара $p-1$ различит p-цикл. Због тога је

$$s_p = \frac{m}{p-1} = \frac{\binom{k}{p}(p-1)!}{p-1} = \frac{k!}{(k-p)!p!}(p-2)! = \frac{k!}{(k-p)!p(p-1)}.$$

Враћањем у (9) добијамо

$$|N_{\mathbb{S}_k}H| = \frac{k!}{\frac{k!}{(k-p)!p(p-1)}} = p(p-1)(k-p)!,$$

чиме добијамо тражено.
□

Задатак 45. Нека је p прост број, $k \in \{p, p+1\}$ и H једна S_p подгрупа од $\mathbb{S}_k$. Тада важи:

$$|N_{\mathbb{S}_k}H| = p(p-1).$$

Решење. Ово је само директна последица претходног задатка.
□

Задатак 46. Доказати да група реда $2^3 \cdot 3 \cdot 7^2$ није проста.

Решење. Нека је $|G| = 2^3 \cdot 3 \cdot 7^2$. Из Треће теореме Силова имамо:

$$\left.\begin{array}{l} s_2 \equiv 1 \pmod 2 \\ s_2 \mid 3 \cdot 7^2 \end{array}\right\} \longrightarrow s_2 \in \{1, 3, 7, 21, 49, 147\}$$

$$\left.\begin{array}{l} s_3 \equiv 1 \pmod 3 \\ s_3 \mid 2^3 \cdot 7^2 \end{array}\right\} \longrightarrow s_3 \in \{1, 4, 7, 28, 49, 192\}$$

$$\left.\begin{array}{l} s_7 \equiv 1 \pmod 7 \\ s_7 \mid 2^3 \cdot 3 \end{array}\right\} \longrightarrow s_7 \in \{1, 8\}.$$

Претпоставимо да је група G проста. Тада мора бити $s_7 = 8$. Означимо са K једну S_7 подгрупу од G. На основу Тврђења 4.7 имамо

$$[G : N_G K] = s_7 = 8,$$

па нам Задатак 43 омогућава да сматрамо $G \leq \mathbb{S}_8$. Из Лагранжеве теореме онда следи

$$2^3 \cdot 3 \cdot 7^2 \mid 8!,$$

што је контрадикција, јер $7^2 \nmid 8!$. Према томе, група G не може бити проста.
□

Задатак 47. Доказати да група реда 396 није проста.

Решење. Нека је $|G| = 396$. Из Треће теореме Силова имамо:

$$\left.\begin{array}{ll} s_2 \equiv 1 & (\text{mod } 2) \\ s_2 \mid 99 & \end{array}\right\} \longrightarrow s_2 \in \{1, 3, 9, 11, 33, 99\}$$
$$\left.\begin{array}{ll} s_3 \equiv 1 & (\text{mod } 3) \\ s_3 \mid 44 & \end{array}\right\} \longrightarrow s_3 \in \{1, 4, 22\}$$
$$\left.\begin{array}{ll} s_{11} \equiv 1 & (\text{mod } 11) \\ s_{11} \mid 36 & \end{array}\right\} \longrightarrow s_{11} \in \{1, 12\}.$$

Претпоставимо да је група G проста. Тада мора бити $s_{11} = 12$. Означимо са H једну S_{11} подгрупу од G. На основу Тврђења 4.7 имамо

$$[G : N_G H] = s_{11} = 12,$$

па нам Задатак 43 омогућава да сматрамо $G \leq \mathbb{S}_{12}$. Приметимо да, пошто $11 \mid |\mathbb{S}_{12}| = 12!$ и $11^2 \nmid |\mathbb{S}_{12}| = 12!$, можемо сматрати да је H и једна S_{11} подгрупа од $\mathbb{S}_{12}$. Како је $G \leq \mathbb{S}_{12}$, онда је и $N_G H \leq N_{\mathbb{S}_{12}} H$, па из Лагранжеве теореме следи

$$|N_G H| \mid |N_{\mathbb{S}_{12}} H|. \tag{10}$$

Остаје само још да израчунамо редове нормализатора који се појављују. Са једне стране, како смо већ видели, важи $[G : N_G H] = 12$, одакле је

$$|N_G H| = \frac{|G|}{12} = \frac{396}{12} = 33.$$

Са друге стране, из Задатка 45 директно следи $|N_{\mathbb{S}_{12}} H| = 11 \cdot (11 - 1) = 110$.

Враћањем у (10)добијамо контрадикцију

$$33 \mid 110,$$

која показује да група G није проста.
□

5 Прстени

5.1 Дефиниција и основне особине прстена

Дефиниција 5.1. Прстен је алгебарска структура $(P, +, \cdot)$, где је P непразан скуп, а $+$ и $\cdot$ бинарне операција на P такве да важи

1. Структура $(P, +)$ је Абелова група:
   - За све $x, y, z \in P$ важи $(x + y) + z = x + (y + z)$.
   - Постоји елемент $0 \in P$ такав да за све $x \in P$ важи $x + 0 = 0 + x = x$.

- За свако $x \in P$ постоји $-x \in P$ такво да је $x + (-x) = -x + x = 0$.
- За све $x, y \in P$ важи $x + y = y + x$.

2. Операција $\cdot$ је асоцијативна:
   - За све $x, y, z \in P$ важи $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
3. Дистрибутивност $\cdot$ према $+$:
   - За све $x, y, z \in P$ важи $x \cdot (y + z) = x \cdot y + x \cdot z$ и $(x + y) \cdot z = x \cdot z + y \cdot z$.

Дефиниција 5.2. Прстен $(P, +, \cdot)$ у коме постоји елемент $1 \in P$ такав да за све $x \in P$ важи $x \cdot 1 = 1 \cdot x = x$ се назива прстен са јединицом.

Дефиниција 5.3. Прстен $(P, +, \cdot)$ такав да за све $x, y \in P$ важи $x \cdot y = y \cdot x$ се назива комутативни прстен.

Надаље ћемо се бавити само комутатитвним прстенима са јединицом и ако не нагласимо другачије, под термином прстен ће се подразумевати комутативни прстен са јединицом.

Дефиниција 5.4. Комутатитвни прстен са јединицом $(P, +, \cdot)$ у коме је $0 \neq 1$ и за свако $x \in P \setminus \{0\}$ постоји $x^{-1} \in P$ такво да је $x \cdot x^{-1} = x^{-1} \cdot x = 1$ се назива поље.

Задатак 48. Нека је $C(\mathbb{R})$ скуп непрекидних реалних функција реалне променљиве на коме су дефинисане операције сабирања и множења са

$$(f + g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x)g(x), \quad f, g \in C(\mathbb{R}), x \in \mathbb{R}.$$

Доказати да је $C(\mathbb{R})$ комутативни прстен са јединицом у односу на ове операције.

Решење. За почетак имамо да је збир и производ две непрекидне функције такође непрекидна функција, па су операција сабирања и одузимања које посматрамо коректно дефинисане. Уочимо произвољне $f, g, h \in C(\mathbb{R})$ и $x \in \mathbb{R}$. Тада је

$$\begin{aligned}(f + (g + h))(x) &= f(x) + (g + h)(x) \\ &= f(x) + (g(x) + h(x)) \\ &= (f(x) + g(x)) + h(x) \\ &= (f + g)(x) + h(x) \\ &= ((f + g) + h)(x),\end{aligned}$$

па следи $f + (g + h) = (f + g) + h$.

Дефинишимо функцију $\mathbf{0} \in C(\mathbb{R})$ са $\mathbf{0}(x) = 0$ за све $x \in \mathbb{R}$. Онда за све $x \in \mathbb{R}$ важи

$$(f + \mathbf{0})(x) = f(x) + \mathbf{0}(x) = f(x) + 0 = f(x) \quad \text{и} \quad (\mathbf{0} + f)(x) = \mathbf{0}(x) + f(x) = 0 + f(x) = f(x),$$

што показује да је $\mathbf{0}$ неутрал за операцију $+$.

За сваку функцију $f \in \mathbb{C}(\mathbb{R})$ можемо дефинисати функцију $-f \in C(\mathbb{R})$ са $(-f)(x) = -f(x)$ за све $x \in \mathbb{R}$. Онда за све $x \in \mathbb{R}$ важи

$$(f + (-f))(x) = f(x) - f(x) = 0 = \mathbf{0}(x) \quad \text{и} \quad (-f + f)(x) = -f(x) + f(x) = 0 = \mathbf{0}(x),$$

што показује да је $-f$ инверз за проивољно f при операцији $+$.

Додатно, за све $f, g \in C(\mathbb{R})$ и $x \in \mathbb{R}$ важи

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x),$$

што даје $f + g = g + f$.

Приметимо још да за произвољне $f, g, h \in C(\mathbb{R})$ и $x \in \mathbb{R}$ имамо

$$\begin{aligned}(f \cdot (g \cdot h))(x) &= f(x) \cdot (g \cdot h)(x) \\ &= f(x) \cdot (g(x) \cdot h(x)) \\ &= (f(x) \cdot g(x)) \cdot h(x) \\ &= (f \cdot g)(x) \cdot h(x) \\ &= ((f \cdot g) \cdot h)(x),\end{aligned}$$

$$\begin{aligned}((f + g) \cdot h))(x) &= (f + g)(x) \cdot h(x) \\ &= (f(x) + g(x)) \cdot h(x) \\ &= f(x) \cdot h(x) + g(x) \cdot h(x) \\ &= (f \cdot h)(x) + (g \cdot h)(x) \\ &= (f \cdot h + g \cdot h)(x),\end{aligned}$$

$$\begin{aligned}(f \cdot (g + h))(x) &= f(x) \cdot (g + h)(x) \\ &= f(x) \cdot (g(x) + h(x)) \\ &= f(x) \cdot g(x) + f(x) \cdot h(x) \\ &= (f \cdot g)(x) + (f \cdot h)(x) \\ &= (f \cdot g + f \cdot h)(x),\end{aligned}$$

одакле следи $f \cdot (g \cdot h) = (f \cdot g) \cdot h$, $(f + g) \cdot h = f \cdot h + g \cdot h$ и $f \cdot (g + h) = f \cdot g + f \cdot h$. Дакле, доказали смо да је $C(\mathbb{R})$ прстен.

Пошто за све $f, g \in C(\mathbb{R})$ и $x \in \mathbb{R}$ важи

$$(f \cdot g)(x) = f(x) \cdot g(x) = g(x) \cdot f(x) = (g \cdot f)(x),$$

имамо $f \cdot g = g \cdot f$. Тиме је показано да је прстен $C(\mathbb{R})$ комутативан.

Коначно, можемо дефинисати функцију $\mathbf{1} \in C(\mathbb{R})$ са $\mathbf{1}(x) = 1$ за све $x \in \mathbb{R}$. Онда је

$$(f \cdot \mathbf{1})(x) = f(x) \cdot \mathbf{1}(x) = f(x) \cdot 1 = f(x) \quad \text{и} \quad (\mathbf{1} \cdot f)(x) = \mathbf{1}(x) \cdot f(x) = 1 \cdot f(x) = f(x),$$

што показује да је $\mathbf{1}$ неутрал за операцију $\cdot$. Тиме смо показали да је прстен $C(\mathbb{R})$ са јединицом и завршили задатак.

□

Задатак 49. Нека је R скуп свих матрица $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$, где су $a, b \in \mathbb{R}$. Доказати да је R комутативни прстен са јединицом у односу на уобичајене операције сабирања и множења матрица.

Решење. Прво, за матрице $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ и $\begin{bmatrix} c & -d \\ d & c \end{bmatrix}$ из R имамо

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} a+c & -b-d \\ b+d & a+c \end{bmatrix} \in R$$
$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{bmatrix} \in R, \tag{11}$$

што показује да су операције сабирања и множења матрица коректно дефинисане на R. Већ знамо да је R прстен у односу на те операције, па то нећемо показивати. Све што још треба да покажемо је да је прстен R комутативан и са јединицом.

За јединицу одмах знамо да постоји– то је управо јединична матрица $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in R$. Такође, важи

$$\begin{bmatrix} c & -d \\ d & c \end{bmatrix} \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{bmatrix},$$

што уз (11) показује да је прстен R комутативан.
□

5.2 Потпрстени

Дефиниција 5.5. Нека је R прстен. Подскуп $A \subseteq R$ је потпрстен од R ако за све $a, b \in A$ важи:

- $a + b \in A$.
- $-a \in A$.
- $ab \in A$.
- $1 \in A$.

Задатак 50. Посматрајмо прстен $\mathbb{Z} \times \mathbb{Z}$ свих уређених парова $(a, b), a, b \in \mathbb{Z}$ у односу на операције

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b)(c, d) = (ac, bd), \quad a, b, c, d \in \mathbb{Z}.$$

Доказати да је $A = \{(a, a) \mid a \in \mathbb{Z}\}$ потпрстен од $\mathbb{Z} \times \mathbb{Z}$.

Решење. За произвољне (a, a) и (b, b) из A имамо

$$(a, a) + (b, b) = (a + b, a + b) \in A$$
$$-(a, a) = (-a, -a) \in A$$
$$(a, a)(b, b) = (ab, ab) \in A$$
$$(1, 1) \in A,$$

одакле следи да је A потпрстен од $\mathbb{Z} \times \mathbb{Z}$.
□

Задатак 51. Нека је $S = \{x2^y \mid x, y \in \mathbb{Z}\}$. Показати да је S потпрстен поља реалних бројева $\mathbb{R}$.

Решење. Уочимо произвољне елементе $z_1 = x_1 2^{y_1}$ и $z_2 = x_2 2^{y_2}$ из S. По дефиницији су онда $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. Означимо са $m = \min\{y_1, y_2\}$. Тада имамо

$$z_1 + z_2 = x_1 2^{y_1} + x_2 2^{y_2} = 2^m \left(x_1 2^{y_1 - m} + x_2 2^{y_2 - m}\right).$$

Свакако је $m \in \mathbb{Z}$, а такође због $m \leq y_1, y_2$ важи и $x_1 2^{y_1-m} + x_2 2^{y_2-m} \in \mathbb{Z}$. Одатле закључујемо да $z_1 + z_2 \in S$. Слично је онда и

$$\begin{aligned} -z_1 &= (-x_1)2^{y_1} \in S \\ z_1 z_2 &= x_1 2^{y_1} x_2 2^{y_2} = (x_1 x_2) 2^{y_1 + y_2} \in S \\ 1 &= 1 \cdot 2^0 \in S, \end{aligned}$$

чиме је показано да је S потпрстен од $\mathbb{R}$.
□

5.3 Хомоморфизми прстена

Дефиниција 5.6. Нека су R и S два прстена. Пресликавање $f : R \to S$ такво да за све $x, y \in R$ важи

- $f(x + y) = f(x) + f(y)$
- $f(xy) = f(x)f(y)$
- $f(1) = 1$

се назива хомоморфизам прстена.

Слично као у теорији група, сурјективни хомоморфизмам се назива епиморфизам, инјективни хомоморфизам се назива мономорфизам или утапање, док се бијективни хомоморфизам назива изоморфизам. Ако постоји изоморфизам између нека два прстена R и S за њих се каже да су изоморфни и пише се $R \cong S$.

Нека је $f : R \to S$ хомоморфизам прстена. Дефинишемо:

$$\begin{aligned} &\ker f = \{a \in R \mid f(a) = 0\} \quad \text{језгро хомоморфизма } f. \\ &\operatorname{im} f = \{f(a) \mid a \in R\} \quad \text{слика хомоморфизма } f. \end{aligned}$$

Слично као и код група, имамо:

$$\begin{aligned} &f \text{ је 1-1 ако и само ако је } \ker f = \{0\}. \\ &f \text{ је на ако и само ако је } \operatorname{im} f = S. \end{aligned}$$

Задатак 52. Посматрајмо пресликавање $f : \mathbb{Z}[X] \to \mathbb{R}$ дефинисано са $f(p(X)) = p(\sqrt{2})$, $p(X) \in \mathbb{Z}[X]$. Доказати да је f хомоморфизам прстена.

Решење. Уочимо произвољне полиноме $p(X)$ и $q(X)$ из $\mathbb{Z}[X]$, као и мултипликативни неутрал $\mathbf{1}(X) \equiv 1$ тог прстена. Тада је

$$f((p+q)(X)) = (p+q)(\sqrt{2}) = p(\sqrt{2}) + q(\sqrt{2}) = f(p(X)) + f(q(X))$$
$$f((p\cdot q)(X)) = (p\cdot q)(\sqrt{2}) = p(\sqrt{2})\cdot q(\sqrt{2}) = f(p(X))\cdot f(q(X))$$
$$f(\mathbf{1}(X)) = 1,$$

чиме је показано да је f хомоморфизам.
□

Задатак 53. Дати су прстен $R_1 = \left\{a + b\frac{1+\sqrt{13}}{2} \mid a, b \in \mathbb{Z}\right\}$ у односу на сабирање и множење реалних бројева и прстен $R_2 = \left\{\begin{bmatrix} a & b \\ 3b & a+b \end{bmatrix} \mid a, b \in \mathbb{Z}\right\}$ у односу на сабирање и множење матрица. Доказати да је $R_1 \cong R_2$.

Решење. Посматрајмо пресликавање $\phi : R_1 \to R_2$ дефинисано са

$$\phi\left(a + b\frac{1+\sqrt{13}}{2}\right) = \begin{bmatrix} a & b \\ 3b & a+b \end{bmatrix}, \ a, b \in \mathbb{Z}.$$

Ово пресликавање је очигледно сурјективно. Докажимо да је хомоморфизам.

За произвољне $a, b, c, d \in \mathbb{Z}$ важи

$$\phi\left(a + b\frac{1+\sqrt{13}}{2} + c + d\frac{1+\sqrt{13}}{2}\right) = \phi\left(a + c + (b+d)\frac{1+\sqrt{13}}{2}\right)$$
$$= \begin{bmatrix} a+c & b+d \\ 3(b+d) & a+c+b+d \end{bmatrix} = \begin{bmatrix} a & b \\ 3b & a+b \end{bmatrix} + \begin{bmatrix} c & d \\ 3d & c+d \end{bmatrix}$$
$$= \phi\left(a + b\frac{1+\sqrt{13}}{2}\right) + \phi\left(c + d\frac{1+\sqrt{13}}{2}\right),$$

$$\phi\left(\left(a + b\frac{1+\sqrt{13}}{2}\right)\left(c + d\frac{1+\sqrt{13}}{2}\right)\right) = \phi\left(ac + (ad+bc)\frac{1+\sqrt{13}}{2} + +bd\left(\frac{1+\sqrt{13}}{2}\right)^2\right)$$
$$= \phi\left(ac + 3bd + (ad+bc+bd)\frac{1+\sqrt{13}}{2}\right) = \begin{bmatrix} ac+3bd & ad+bc+bd \\ 3(ad+bc+bd) & ac+3bd+ad+bc+bd \end{bmatrix}$$
$$= \begin{bmatrix} a & b \\ 3b & a+b \end{bmatrix}\begin{bmatrix} c & d \\ 3d & c+d \end{bmatrix} = \phi\left(a + b\frac{1+\sqrt{13}}{2}\right)\phi\left(c + d\frac{1+\sqrt{13}}{2}\right),$$

$$\phi(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

што показује да је ϕ хомоморфизам.

Остаје само још да покажемо да је ϕ инјективно пресликавање. То можемо урадити директно по дефиницији, а можемо и показати да је $\ker\phi = \{0\}$, што је у овом случају једноставније. Имамо

$$\begin{aligned}
\ker\phi &= \left\{ a + b\frac{1+\sqrt{13}}{2} \in R_1 \mid \phi\left(a + b\frac{1+\sqrt{13}}{2}\right) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\} \\
&= \left\{ a + b\frac{1+\sqrt{13}}{2} \in R_1 \mid \begin{bmatrix} a & b \\ 3b & a+b \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\} \\
&= \left\{ a + b\frac{1+\sqrt{13}}{2} \in R_1 \mid a = b = 0 \right\} \\
&= \{0\}.
\end{aligned}$$

Закључујемо да је ϕ изоморфизам, чиме добијамо тражено $R_1 \cong R_2$.
□

5.4 Идеали и количнички прстени

Дефиниција 5.7. Подскуп I прстена R се назива идеал и означава $I \triangleleft R$ ако важи:

- за све $x, y \in I : x + y \in I$
- за све $x \in I$ и $a \in R : ax \in I$.

Дефиниција 5.8. Коначан скуп $S = \{x_1, x_2, \ldots x_n\} \subseteq R$ генерише идеал I прстена R ако се сваки елемент из I може записати у облику $a_1x_1 + a_2x_2 + \ldots a_nx_n$ за неке $a_1, a_2, \ldots, a_n \in R$. У том случају пишемо $I = \langle S \rangle$.

Дефиниција 5.9. Идеал I прстена R је главни ако је генерисан само једним елементом из R, $I = \langle a \rangle$ за неко $a \in R$.

Задатак 54. Посматрајмо прстен полинома $\mathbb{Z}[X]$ и у њему подскуп

$$I = \{2f(X) + Xg(X) \mid f(X), g(X) \in \mathbb{Z}[X]\}.$$

Показати да је I идеал прстена $\mathbb{Z}[X]$. Да ли је тај идеал главни?

Решење. Покажимо прво да је I идеал. Уочимо произвољне $u(X)$ и $v(X)$ из I. Тада постоје полиноми $f_1(X), f_2(X), g_1(X), g_2(X) \in \mathbb{Z}[X]$ такви да је

$$\begin{aligned}
u(X) &= 2f_1(X) + Xg_1(X) \\
v(X) &= 2f_2(X) + Xg_2(X).
\end{aligned}$$

Одатле је

$$u(X) + v(X) = 2\underbrace{(f_1(X) + f_2(X))}_{\in\mathbb{Z}[X]} + X\underbrace{(g_1(X) + g_2(X))}_{\in\mathbb{Z}[X]} \in I.$$

Слично за произвољно $\alpha(X) \in \mathbb{Z}[X]$ имамо

$$\alpha(X)u(X) = 2\underbrace{\alpha(X)f_1(X)}_{\in\mathbb{Z}[X]} + X\underbrace{\alpha(X)g_1(X)}_{\in\mathbb{Z}[X]} \in I.$$

Овим смо показали да је I идеал прстена $\mathbb{Z}[X]$.

Остаје још да испитамо да ли је овај идеал главни. За почетак можемо приметити да је $I = \langle 2, X\rangle$. Ако би овај идеал био главни, важило би $I = \langle f(X)\rangle$ за неки полином $f(X) \in \mathbb{Z}[X]$. Одатле би важило $\langle 2, X\rangle = \langle f(X)\rangle$, што имплицира постојање полинома $a(X), b(X) \in \mathbb{Z}[X]$ таквих да важи

$$2 = f(X)a(X) \tag{12}$$
$$X = f(X)b(X). \tag{13}$$

Из (12) следи да је $f(X) = 1$ или $f(X) = 2$. Ако би било $f(X) = 2$, из (13) би следило $X = 2b(X)$, што није могуће, пошто је $b(X) \in \mathbb{Z}[X]$. Дакле, остаје нам $f(X) = 1$. Онда је $I = \langle 1\rangle = \mathbb{Z}[X]$, па добијамо $\langle 2, X\rangle = \mathbb{Z}[X]$. Специјално, одатле следи да постоје полиноми $m(X), n(X) \in \mathbb{Z}[X]$ такви да је

$$2m(X) + Xn(X) = 1.$$

Добијамо да мора бити $n(X) = 0$ и $2m(X) = 1$. Међутим, како је $m(X) \in \mathbb{Z}[X]$ ни ово није могуће, па закључујемо да идеал I није главни.
□

Задатак 55. Посматрајмо комутативни потпрстен $K = \left\{ \begin{bmatrix} a & b \\ -5b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$ прстена матрица $M_2(\mathbb{Z})$.
а) Доказати да је $I = \left\{ \begin{bmatrix} 5a & b \\ -5b & 5a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$ идеал прстена K.
б) Доказати да је $I = \left\langle \begin{bmatrix} 0 & 1 \\ -5 & 0 \end{bmatrix} \right\rangle$.

Решење. а) Уочимо произвољне елементе $\begin{bmatrix} 5a & b \\ -5b & 5a \end{bmatrix}$ и $\begin{bmatrix} 5c & d \\ -5d & 5c \end{bmatrix}$ из I, као и $\begin{bmatrix} m & n \\ -5n & m \end{bmatrix}$ из K. Тада је

$$\begin{bmatrix} 5a & b \\ -5b & 5a \end{bmatrix} + \begin{bmatrix} 5c & d \\ -5d & 5c \end{bmatrix} = \begin{bmatrix} 5(a+c) & b+d \\ -5(b+d) & 5(a+c) \end{bmatrix} \in I$$

$$\begin{bmatrix} m & n \\ -5n & m \end{bmatrix} \begin{bmatrix} 5a & b \\ -5b & 5a \end{bmatrix} = \begin{bmatrix} 5am - 5bn & bm + 5an \\ -25an - 5bm & -5bn + 5am \end{bmatrix} = \begin{bmatrix} 5(am - bn) & bm + 5an \\ -5(bn + 5an) & 5(am - bn) \end{bmatrix} \in I.$$

Из добијеног следи да је I идеал прстена K.
б) Приметимо да за произвољно $\begin{bmatrix} a & b \\ -5b & a \end{bmatrix} \in K$ важи

$$\begin{bmatrix} a & b \\ -5b & a \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -5 & 0 \end{bmatrix} = \begin{bmatrix} -5b & a \\ -5a & -5b \end{bmatrix}.$$

Због тога, за произвољно $\begin{bmatrix} 5a & b \\ -5b & 5a \end{bmatrix} \in I$ имамо

$$\begin{bmatrix} 5a & b \\ -5b & 5a \end{bmatrix} = \begin{bmatrix} b & -a \\ 5a & b \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -5 & 0 \end{bmatrix},$$

чиме је показано да важи $I = \left\langle \begin{bmatrix} 0 & 1 \\ -5 & 0 \end{bmatrix} \right\rangle$.
□

Количнички прстен

Нека је I идеал прстена R. На скупу $R/I = \{a + I \mid a \in R\}$ свих левих косета дефинишемо операције сабирања и множења са:

- $(a + I) + (b + I) = (a + b) + I$
- $(a + I) \cdot (b + I) = ab + I, \ \ a, b \in R.$

Уз овако дефинисане операције R/I је комутативни прстен са јединицом који се назива количнички прстен прстена R по идеалу I.

Приметимо да је у прстену R/I неутрал за операцију сабирања I, а за операцију множења $1 + I$.

Слично као и код група, веома применљив метод одређивања количничког прстена је коришћење Прве теореме о изоморфизму.

Теорема 5.10 (Прва теорема о изоморфизму прстена)**.** Нека је $f : R \to S$ хомоморфизам прстена. Тада је $\ker f$ један идеал прстена R и важи

$$R/\ker f \cong \operatorname{im} f.$$

Од интереса ће нам бити две класе идеала описане наредним дефиницијама.

Дефиниција 5.11. Идеал I прстена R је прост ако за све $a, b \in R$ из $ab \in I$ следи $a \in I$ или $b \in I$.

Дефиниција 5.12. Идеал I прстена R је максималан ако није садржан ни у једном правом[1] идеалу од R.

У вези простих идеала, значајан ће нам бити појам домена који је описан у наредној дефиницији.

Дефиниција 5.13. Прстен R је домен ако у њему нема правих делитеља нуле тј. ако за све $a, b \in R$ из $ab = 0$ следи $a = 0$ или $b = 0$.

[1] прави идеал прстена R је сваки идеал тог прстена различит од $\{0\}$ и R

Пример 5.14. Посматрајмо поље F и претпоставимо да за неке $a, b \in F$ важи $ab = 0$. Ако је $a \neq 0$ онда у F постоји инверз a^{-1} за a, па добијамо

$$a^{-1}ab = a^{-1} \cdot 0 \longrightarrow b = 0.$$

Закључујемо да у пољу нема правих делитеља нуле, па је свако поље домен.
□

Приметимо да директно на основу Дефиниција 5.11 и 5.12 није баш једноставно испитати да ли је неки идеал прост/максималан. Посао нам знатно може олакшати наредно тврђење.

Тврђење 5.15.

- Идеал I прстена R је прост ако и само ако је количнички прстен R/I домен.
- Идеал I прстена R је максималан ако и само ако је количнички прстен R/I поље.

Пошто је свако поље домен, одмах имамо наредну последицу.

Последица. Сваки максималан идеал је прост.

Задатак 56. Посматрајмо прстен $R = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mid a, b \in \mathbb{Q} \right\}$ у односу на множење и сабирање матрица.
а) Доказати да је подскуп $J = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \mid b \in \mathbb{Q} \right\}$ идеал прстена R.
б) Доказати да је $R/J \cong \mathbb{Q}$.

Решење. За произвољне матрице $\begin{bmatrix} 0 & b_1 \\ 0 & 0 \end{bmatrix}$ и $\begin{bmatrix} 0 & b_2 \\ 0 & 0 \end{bmatrix}$ из J и $\begin{bmatrix} \alpha & \beta \\ 0 & \alpha \end{bmatrix}$ из R важи

$$\begin{bmatrix} 0 & b_1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & b_2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & b_1 + b_2 \\ 0 & 0 \end{bmatrix} \in J$$
$$\begin{bmatrix} \alpha & \beta \\ 0 & \alpha \end{bmatrix} \begin{bmatrix} 0 & b_1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & \alpha b_1 \\ 0 & 0 \end{bmatrix} \in J.$$

Одатле закључујемо да је J идеал прстена R.
б) Посматрајмо пресликавање $\phi : R \to \mathbb{Q}$ дефинисано са

$$\phi\left(\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \right) = a, \quad \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \in R.$$

Ово пресликавање је очигледно на. Такође, за произвољне матрице $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$ и $\begin{bmatrix} c & d \\ 0 & c \end{bmatrix}$ из

R важи

$$\phi\left(\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} + \begin{bmatrix} c & d \\ 0 & c \end{bmatrix}\right) = \phi\left(\begin{bmatrix} a+c & b+d \\ 0 & a+c \end{bmatrix}\right)$$
$$= a + c = \phi\left(\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\right) + \phi\left(\begin{bmatrix} c & d \\ 0 & c \end{bmatrix}\right)$$
$$\phi\left(\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\begin{bmatrix} c & d \\ 0 & c \end{bmatrix}\right) = \phi\left(\begin{bmatrix} ac & ad+bc \\ 0 & ac \end{bmatrix}\right)$$
$$= ac = \phi\left(\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\right)\phi\left(\begin{bmatrix} c & d \\ 0 & c \end{bmatrix}\right)$$
$$\phi\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = 1.$$

Одатле закључујемо да је ϕ хомоморфизам прстена.

Из Прве теореме о изоморфизму онда следи

$$R/\ker\phi \cong \mathbb{Q}.$$

Одредимо још $\ker\phi$:

$$\ker\phi = \left\{\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \in R \mid \phi\left(\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}\right) = 0\right\}$$
$$= \left\{\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \in R \mid a = 0\right\}$$
$$= \left\{\begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \mid b \in \mathbb{Q}\right\} = J.$$

Дакле, добијамо тражено $R/J \cong \mathbb{Q}$.
□

Задатак 57. Нека је S прстен реалних функција реалне променљиве у односу на операције сабирања и множења тачку по тачку и $I = \{f \in S \mid f(0) = 0\}$ један подскуп од S.
а) Показати да је I идеал прстена S.
б) Испитати да ли је идеал I прост/максималан.

Решење. а) Уочимо произвољне функције $f, g \in I$. Тада је $f(0) = g(0) = 0$. Одатле следи

$$(f+g)(0) = f(0) + g(0) = 0 + 0 = 0,$$

па добијамо да је $f + g \in I$. Слично, за произвољну функцију $\alpha \in S$ имамо

$$(\alpha f)(0) = \alpha(0)f(0) = \alpha(0) \cdot 0 = 0,$$

па је $\alpha f \in I$. Тиме је показано да је I идеал прстена S.
б) Посматрајмо пресликавање $\phi : S \to \mathbb{R}$ дефинисано са

$$\phi(f) = f(0), \quad f \in S.$$

Како за произвољне функције $f, g \in S$ важи

$$\begin{aligned}
&\phi(f+g) = (f+g)(0) = f(0) + g(0) = \phi(f) + \phi(g) \\
&\phi(fg) = (fg)(0) = f(0)g(0) = \phi(f)\phi(g) \\
&\phi(\mathbf{1}) = \mathbf{1}(0) = 1,
\end{aligned}$$

имамо да је ϕ хомоморфизам прстена. Тај хомоморфизам је очигледно сурјективан, па на основу Прве теореме о изоморфизму следи

$$S/\ker\phi \cong \mathbb{R}.$$

Пошто је по дефиницији

$$\begin{aligned}
\ker\phi &= \{f \in S \mid \phi(f) = 0\} \\
&= \{f \in S \mid f(0) = 0\} \\
&= I,
\end{aligned}$$

добијамо

$$S/I \cong \mathbb{R}.$$

Дакле, количнички прстен S/I је поље, па закључујемо да је идеал I максималан, а тиме и прост.
□

Задатак 58. Посматрајмо прстен полинома $R[X,Y]$ са две неодређене над прстеном R. Доказати да је $R[X,Y]/\langle X\rangle \cong R[Y]$.

Решење. Посматрајмо пресликавање $\psi : R[X,Y] \to R[Y]$ дефинисано са

$$\psi(f(X,Y)) = f(0,Y), \;\; f(X,Y) \in R[X,Y].$$

Ово пресликавање је на, пошто за свако $g(Y) \in R[Y]$ можемо дефинисати $f(X,Y) \in R[X,Y]$ са $f(X,Y) = g(Y)$ и онда је $\psi(f(X,Y)) = f(0,Y) = g(Y)$.

Покажимо да је ψ хомоморфизам прстена. За произвољне $f_1(X,Y)$ и $f_2(X,Y)$ из $R[X,Y]$ важи

$$\begin{aligned}
\psi((f_1+f_2)(X,Y)) &= (f_1+f_2)(0,Y) \\
&= f_1(0,Y) + f_2(0,Y) \\
&= \psi(f_1(X,Y)) + \psi(f_2(X,Y)) \\
\psi((f_1f_2)(X,Y)) &= (f_1f_2)(0,Y) \\
&= f_1(0,Y)f_2(0,Y) \\
&= \psi(f_1(X,Y))\psi(f_2(X,Y)) \\
\psi(\mathbf{1}(X,Y)) &= \mathbf{1}(0,Y) = \mathbf{1}(Y).
\end{aligned}$$

Закључујемо да ψ јесте хомоморфизам прстена. Одредимо још његово језгро. Важи:

$$\begin{aligned}\ker\psi &= \{f(X,Y) \mid \psi(f(X,Y)) = \mathbf{0}(Y)\}\\ &= \{f(X,Y) \mid f(0,Y) = \mathbf{0}(Y)\}\\ &= \{f(X,Y) \mid f(0,Y) = 0 \text{ за све } Y\}\\ &= \{f(X,Y) \mid X \text{ дели } f(X,Y)\}\\ &= \{f(X,Y) \mid f(X,Y) = Xf'(X,Y) \text{ за неко } f'(X,Y) \in R[X,Y]\}\\ &= \langle X\rangle.\end{aligned}$$

Из Прве теореме о изоморфизму прстена онда следи

$$R[X,Y]/\langle X\rangle \cong R[Y].$$

□

Задатак 59. Испитати да ли је главни идеал $\langle X\rangle$ прост/максималан у прстену полинома $\mathbb{Q}[X,Y]$.

Решење. Из претходног задатка имамо да је $\mathbb{Q}[X,Y]/\langle X\rangle \cong \mathbb{Q}[Y]$. Како је $\mathbb{Q}[Y]$ домен, а није поље, закључујемо да је идеал $\langle X\rangle$ прост, али није максималан.
□

5.5 Главноидеалски домени

Дефиниција 5.16. Домен у коме је сваки прави идеал главни се назива главно идеалски домен.

Најзначајнији пример главноидеалског домена који ћемо посматрати је прстен полинома $\mathbb{F}[X]$ над произвољним пољем $\mathbb{F}$. У њему није тешко препознати максималне идеале: они су генерисани несводљивим полиномима.

Пример 5.17 (Конструкција поља комплексних бројева)**.** Посматрајмо полином $X^2+1 \in \mathbb{R}[X]$ који је несводљив над пољем реалних бројева $\mathbb{R}$. Због тога је главни идеал $\langle X^2+1\rangle$ максималан у прстену $\mathbb{R}[X]$, па количнички прстен $\mathbb{R}[X]/\langle X^2+1\rangle$ мора бити поље. Одредимо то поље.

Директно по дефиницији количничког прстена имамо:

$$\begin{aligned}\mathbb{R}[X]/\langle X^2+1\rangle &= \{f(X) + \langle X^2+1\rangle \mid f(X) \in \mathbb{R}[X]\}\\ &= \{q(X)(X^2+1) + r(X) + \langle X^2+1\rangle \mid q(X), r(X) \in \mathbb{R}[X], \deg r(X) < 2\}\\ &= \{r(X) + \langle X^2+1\rangle \mid r(X) \in \mathbb{R}[X], \deg r(X) < 2\}\\ &= \{a + bX + \langle X^2+1\rangle \mid a, b \in \mathbb{R}\}\\ &\cong \mathbb{C},\end{aligned}$$

при чему је последњи изоморфизам одређен са $a + bX + \langle X^2+1\rangle \to a + bi$, $a, b \in \mathbb{R}$. Дакле, можемо приметити да претходна конструкција преставља један експлицитан

начин добијања поља комплексних бројева од поља реалних бројева. Приметимо још и да за елемент $X + \langle X^2 + 1\rangle$ који одговара елементу $i \in \mathbb{C}$ важи

$$\big(X + \langle X^2 + 1\rangle\big)^2 = X^2 + \langle X^2 + 1\rangle = -1 + \langle X^2 + 1\rangle \longleftrightarrow -1,$$

па он заиста преставља (конкретно) решење једначине $t^2 = -1$ (кога нема у пољу $\mathbb{R}$). □

Задатак 60. Показати да је количнички прстен $\mathbb{Z}_3[X]/\langle 2X^3 + X + 1\rangle$ једно поље, одредити број његових елемената и израчунати мултипликативни инверз за $X^2 + 1 + \langle 2X^3 + X + 1\rangle$ у том пољу.

Решење. Да бисмо доказали да је $\mathbb{Z}_3[X]/\langle 2X^3 + X + 1\rangle$ поље, довољно је да покажемо да је идеал $\langle 2X^3 + X + 1\rangle$ максималан. Пошто је $\mathbb{Z}_3$ поље, то се своди на показивање несводљивости полинома $f(X) = 2X^3 + X + 1$ над $\mathbb{Z}_3$. Овде имамо једну олакшавајућу околност– полином $f(X)$ је степена (највише) 3, па ће он бити несводљив над $\mathbb{Z}_3$ ако и само ако нема нула над $\mathbb{Z}_3$. То није тешко да проверимо:

$$f(0) = 1, f(1) = 2 \cdot 1 + 1 + 1 = 1, f(2) = 2 \cdot 2^3 + 2 + 1 = 1.$$

Закључујемо да је полином $f(X)$ несводљив над $\mathbb{Z}_3$, па је количнички прстен $\mathbb{Z}_3[X]/\langle 2X^3 + X + 1\rangle$ једно поље.

Одредимо број елемената тог поља. По дефиницији је

$$\begin{aligned}
\mathbb{Z}_3[X]/\langle 2X^3 + X + 1\rangle &= \mathbb{Z}_3[X]/\langle f(X)\rangle = \{g(X) + \langle f(X)\rangle \mid g(X) \in \mathbb{Z}_3[X]\} \\
&= \{q(X)f(X) + r(X) + \langle f(X)\rangle \mid q(X), r(X) \in \mathbb{Z}_3[X], \deg r(X) < 3\} \\
&= \{r(X) + \langle f(X)\rangle \mid r(X) \in \mathbb{Z}_3[X], \deg r(X) < 3\} \\
&= \left\{a + bX + cX^2 + \langle f(X)\rangle \mid a, b, c \in \mathbb{Z}_3\right\}.
\end{aligned}$$

Закључујемо да посматрано поље има $3 \cdot 3 \cdot 3 = 27$ елемената.

Остаје још да одредимо мултипликативни инверз за $X^2 + 1 + \langle 2X^3 + X + 1\rangle$. Пошто је полином $2X^3 + X + 1$ несводљив и не дели $X^2 + 1$, имамо да су $2X^3 + X + 1$ и $X^2 + 1$ узајамно прости. Због тога постоје полиноми $f_1(X)$ и $f_2(X)$ из $\mathbb{Z}_3[X]$ такви да је

$$f_1(X)(2X^3 + X + 1) + f_2(X)(X^2 + 1) = 1.$$

Полиноме $f_1(X)$ и $f_2(X)$ налазимо Еуклидовим алгоритмом:

$$\begin{aligned}
2X^3 + X + 1 &= (X^2 + 1) \cdot 2X + 2X + 1 \\
X^2 + 1 &= (2X + 1)(2X + 1) + 2X \\
2X + 1 &= 2X \cdot 1 + 1.
\end{aligned}$$

Враћањем на горе добијамо:

$$\begin{aligned}
1 &= 2X + 1 - 2X \\
1 &= 2X + 1 - \big(X^2 + 1 - (2X + 1)(2X + 1)\big) \\
1 &= -(X^2 + 1) + (2X + 2)(2X + 1) \\
1 &= -(X^2 + 1) + (2X + 2)\big(2X^3 + X + 1 - 2X \cdot (X^2 + 1)\big) \\
1 &= (2X + 2)(2X^3 + X + 1) - (X^2 + X + 1)(X^2 + 1).
\end{aligned}$$

Добијамо $f_1(X) = 2X + 2$ и $f_2(X) = -(X^2 + X + 1)$. Одатле је

$$\begin{aligned} 1 + \langle 2X^3 + X + 1\rangle &= (2X+2)(2X^3 + X + 1) - (X^2 + X + 1)(X^2 + 1) + \langle 2X^3 + X + 1\rangle \\ &= -(X^2 + X + 1)(X^2 + 1) + \langle 2X^3 + X + 1\rangle \\ &= \left(-(X^2 + X + 1) + \langle 2X^3 + X + 1\rangle\right)\left(X^2 + 1 + \langle 2X^3 + X + 1\rangle\right). \end{aligned}$$

Закључујемо да је мултипликативни инверз за $X^2 + 1 + \langle 2X^3 + X + 1\rangle$ једнак

$$-(X^2 + X + 1) + \langle 2X^3 + X + 1\rangle = 2X^2 + 2X + 2 + \langle 2X^3 + X + 1\rangle.$$

□

Задатак 61. Одредити све елементе $a \in \mathbb{Z}_3$ за које је количнички прстен $\mathbb{Z}_3[X]/\langle X^3 + X^2 + aX + 1\rangle$ поље.

Решење. Посматрани количнички прстен је поље ако и само ако је главни идеал $\langle X^3 + X^2 + aX + 1\rangle$ максималан. Пошто је $\mathbb{Z}_3$ поље, тај идеал ће бити максималан ако је полином $f(X) = X^3 + X^2 + aX + 1$ несводљив над $\mathbb{Z}_3$. Слично као у претходном задатку, довољно је да нађемо све вредности $a \in \mathbb{Z}_3$ за које полином $f(X)$ нема нула над $\mathbb{Z}_3$. Имамо:

$$\begin{aligned} &f(0) = 1 \ \rightarrow \text{ ово је у реду.} \\ &f(1) = 3 + a = a \ \rightarrow \text{ ово је различито од нуле за } a \neq 0. \\ &f(2) = 8 + 4 + 2a + 1 = 2a + 1 \ \rightarrow \text{ ово је различито од нуле за } a \neq 1. \end{aligned}$$

Закључујемо да постоји само једна тражена вредност и то је $a = 2$.
□

Задатак 62. Испитати да ли је идеал $\langle X^2 + Y^2 - 1, X\rangle$ прост/максималан у прстену $\mathbb{C}[X, Y]$.

Решење. Испитајмо какав је количнички прстен $\mathbb{C}[X, Y]/\langle X^2 + Y^2 - 1, X\rangle$. За почетак, потпуно аналогно као у Задатку 58 имамо да је

$$\mathbb{C}[X, Y]/\langle X^2 + Y^2 - 1, X\rangle \cong \mathbb{C}[Y]/\langle Y^2 - 1\rangle.$$

Зато се наше почетно питање своди на испитивање да ли је количнички прстен $\mathbb{C}[Y]/\langle Y^2 - 1\rangle$ домен/поље.

Приметимо да су у том прстену елементи $Y - 1 + \langle Y^2 - 1\rangle$ и $Y + 1 + \langle Y^2 - 1\rangle$ различити од нуле (тј. од $\langle Y^2 - 1\rangle$). При томе, имамо

$$\left(Y - 1 + \langle Y^2 - 1\rangle\right)\left(Y + 1 + \langle Y^2 - 1\rangle\right) = Y^2 - 1 + \langle Y^2 - 1\rangle = \langle Y^2 - 1\rangle.$$

Дакле, у прстену $C[Y]/\langle Y^2 - 1\rangle$ постоје прави делитељи нуле, па он није домен, а стога ни поље. Закључујемо да идеал $\langle X^2 + Y^2 - 1, X\rangle$ прстена $\mathbb{C}[X, Y]$ није ни максималан, нити је прост.
□

Још један значајан пример главноидеалског домена је прстен Гаусових целих $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ у односу на операције сабирања и множења комплексних бројева. Ово је такође и један пример еуклидског домена. На еуклидским доменима је дефинисана тзв. еуклидска норма која омогућава да се изврши дељење са остатком. Онда можемо извршити и Еуклидов алгоритам да нађемо НЗД два елемента, па отуда и назив еуклидски домен. Конкретно, у $\mathbb{Z}[i]$ је еуклидска норма дефинисана са

$$N(a + bi) = a^2 + b^2, \;\; a, b \in \mathbb{Z}.$$

Задатак 63. Одредити НЗД$(11 + 7i, 18 - i)$ у прстену Гаусових целих $\mathbb{Z}[i]$.

Решење. Спроводимо Еуклидов алгоритам вршећи узастопна дељења са остатком слично као и у класичном случају над $\mathbb{Z}$. При томе се алгоритам завршава када стигнемо или до остатка једнаког нули или остатка норме 1 (дакле до неког од елемената $\pm 1, \pm i$).

Пре него што почемо прво дељење, морамо да знамо који је елемент већи да бисмо њега поделили мањим елементом. То одређујемо на основу норми

$$N(11 + 7i) = 11^2 + 7^2 = 121 + 49 = 170$$
$$N(18 - i) = 18^2 + 1^2 = 324 + 1 = 325,$$

па је за наше потребе елемент $18 - i$ већи. Сада свакако можемо поделити $18 - i$ са $11 + 7i$ у $\mathbb{C}$:

$$\frac{18 - i}{11 + 7i} = \frac{(18 - i)(11 - 7i)}{170} = \frac{191 - 137i}{170} = \frac{191}{170} - \frac{137}{170}i.$$

За количник у $\mathbb{Z}[i]$ бирамо онај елемент који је најближи броју $\frac{191}{170} - \frac{137}{170}i$. При томе је шта тачно значи "најближи" одређено управо еуклидском нормом. У прстену Гаусових целих који посматрамо норма је квадрат (уобичајеног) еуклидског растојања у $\mathbb{C}$, па ће се појам најближег поклапати са нашом интуитивном представом. То значи да ће количник у $\mathbb{Z}[i]$ бити елемент чији је реални део најближи цео број броју $\frac{191}{170}$, а имагинарни део броју $-\frac{137}{170}$. Добијамо да је тражени количник $1 - i$. Онда је остатак једнак

$$18 - i - (11 + 7i)(1 - i) = 18 - i - 11 + 11i - 7i - 7 = 3i.$$

Дакле, успели смо да поделимо са остатком у $\mathbb{Z}[i]$:

$$18 - i = (11 + 7i)(1 - i) + 3i.$$

Како нисмо добили остатак 0, нити норме 1, поступак настављамо за $11 + 7i$ и $3i$. Имамо:

$$\frac{11 + 7i}{3i} = \frac{11}{3i} + \frac{7}{3} = \frac{7}{3} - \frac{11}{3}i.$$

Најближи цео број броју $\frac{7}{3}$ је 2, а броју $-\frac{11}{3}$ је -4, па је количник у $\mathbb{Z}[i]$ једнак $2 - 4i$. Остатак је онда

$$11 + 7i - 3i(2 - 4i) = 11 + 7i - 6i - 12 = -1 + i.$$

Поново нисмо добили остатак 0, нити норме 1, па поступак настављамо за $3i$ и $-1+i$. Добијамо:

$$\frac{3i}{-1+i} = \frac{3i(-1-i)}{2} = \frac{3}{2} - \frac{3}{2}i.$$

Сада смо у ситуацији да постоје два подједнако удаљена цела броја броју $\frac{3}{2}$, а то су 1 и 2. Можемо се одлучити за било који од њих. Слично и за $-\frac{3}{2}$ можемо одабрати било који од бројева -1 и -2. Одаберимо зато за количних елемент $1-i$. Остатак је онда

$$3i - (-1+i)(1-i) = 3i + 1 - i - i - 1 = i.$$

Приметимо да је сада норма остатка једнака 1, што завршава наш поступак, уз закључак

$$\text{НЗД}(11+7i, 18-i) = i.$$

Пошто смо добили да је њихов НЗД норме 1, за елементе $11+7i$ и $18-i$ можемо казати и да су узајамно прости.
□

6 Поља

Дефиниција 6.1. Нека су K и F поља таква да је $F \subseteq K$. У том случају кажемо да је K раширење поља F и пишемо $F \leq K$ или K/F.

Кључна за изучавање поља ће нам бити следећа једноставна особина: Ако је K/F раширење поља, онда је K векторски простор над F. Ова особина омогућава да се доста теорије поља изрази једноставним језиком линеарне алгебре.

Дефиниција 6.2. Степен раширења поља K над пољем F се дефинише као димензија за K посматраног као векторски простор над F,

$$[K : F] = \dim_F K.$$

Претходна дефиниција нам омогућава да уведемо једну једноставну класификацију раширења поља: за раширење K/F кажемо да је коначно (бесконачно) ако је степен раширења $[K : F]$ коначан (бесконачан). Надаље ћемо се бавити само коначним раширењима поља.

Посматрајмо сада неко коначно раширење поља K/F и уочимо произвољни елемент $a \in K$. Дефинишемо два подскупа од K:

$$F[a] = \{f(a) \mid f(X) \in F[X]\}$$
$$F(a) = \left\{ \frac{f(a)}{g(a)} \mid f(X), g(X) \in F[X], g(a) \neq 0 \right\}.$$

Важи да је $F[a]$ комутативни прстен са јединицом и $F(a)$ поље.

Задатак 64. Посматрајмо домен целих $\mathbb{Q}[\sqrt{2}]$.

а) Показати да је $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

б) Показати да је $\mathbb{Q}[\sqrt{2}]$ поље.

в) Одредити степен раширења $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}]$.

Решење. а) По дефиницији је $\mathbb{Q}[\sqrt{2}] = \{f(\sqrt{2}) \mid f \in \mathbb{Q}[X]\}$. Одатле је јасно да је

$$\mathbb{Q}[\sqrt{2}] \supseteq \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\},$$

па је све што треба да покажемо друга инклузија. Уочимо произвољно $z \in \mathbb{Q}[\sqrt{2}]$. Тада постоји полином $f(X) \in \mathbb{Q}[X]$ такав да је $z = f(\sqrt{2})$. Када распишемо

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \;\; a_i \in \mathbb{Q}, a_n \neq 0$$

добијамо да је

$$z = a_n(\sqrt{2})^n + a_{n-1}(\sqrt{2})^{n-1} + \cdots + a_1(\sqrt{2}) + a_0.$$

Групишући чланове са парним индексима $0 \leq i \leq n$, као и оне са непарним добијамо

$$z = (a_0 + 2a_2 + 4a_4 + \dots) + \sqrt{2}(a_1 + 2a_3 + 4a_5 + \dots).$$

Како су сви бројеви a_i рационални, такви су и бројеви $a_0 + 2a_2 + 4a_4 + \dots$ и $a_1 + 2a_3 + 4a_5 + \dots$, па можемо записати

$$z = a + b\sqrt{2},$$

где су $a, b \in \mathbb{Q}$. На тај начин добијамо да $z \in \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, чиме је показана и инклузија

$$\mathbb{Q}[\sqrt{2}] \subseteq \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\},$$

а тиме и завршен први део.
б) Пошто знамо да је $\mathbb{Q}[\sqrt{2}]$ домен целих, да би смо показати да је поље, све што треба да покажемо је да за свако ненула $z \in \mathbb{Q}[\sqrt{2}]$ постоји мултипликативни инверз. Због дела а) можемо произвољно $z \in \mathbb{Q}[\sqrt{2}]$, $z \neq 0$ записати у облику $z = a + b\sqrt{2}$ за неке $a, b \in \mathbb{Q}$, $a^2 + b^2 \neq 0$. Одатле је

$$\begin{aligned} z^{-1} &= \frac{1}{a + b\sqrt{2}} \\ &= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\ &= \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \end{aligned}$$

Пошто су бројеви a и b рационални, такви су и бројеви $A = \frac{a}{a^2-2b^2}$ и $B = \frac{-b}{a^2-2b^2}$ (и наравно, $a^2 - 2b^2$ не може бити једнако нули због $a^2 + b^2 \neq 0$). Закључујемо да је

$$z^{-1} = A + B\sqrt{2}, \;\; A, B \in \mathbb{Q},$$

што значи да $z^{-1} \in \mathbb{Q}[\sqrt{2}]$. Тиме је показано да је $\mathbb{Q}[\sqrt{2}]$ поље.
в) Из дела а) имамо да скуп $\{1, \sqrt{2}\}$ генерише $\mathbb{Q}[\sqrt{2}]$ над пољем $\mathbb{Q}$. Ако покажемо да је тај скуп линеарно независан над $\mathbb{Q}$, добићемо да чини једну базу за $\mathbb{Q}[\sqrt{2}]$ над $\mathbb{Q}$, па следи да је $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.

Претпоставимо да постоје рационални бројеви c_1 и c_2 такви да је

$$c_1 + c_2\sqrt{2} = 0.$$

Ако је било који од c_1 и c_2 једнак нули, онда такав мора бити и други, па можемо сматрати да су ти бројеви различити од нуле. Тако добијамо да је

$$\sqrt{2} = -\frac{c_1}{c_2} \in \mathbb{Q},$$

а то је контрадикција. Дакле, мора бити $c_1 = c_2 = 0$, што значи да је скуп $\{1, \sqrt{2}\}$ линеарно независан над $\mathbb{Q}$. Одатле закључујемо и тражено

$$[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2.$$

□

Дефиниција 6.3. Нека је K/F раширење поља. Елемент $a \in K$ се назива алгебарским над F ако анулира барем један полином $f(X) \in F[X]$. У супротном се a назива трансцендентним.

Пример 6.4. Елемент $\sqrt{5} \in \mathbb{R}$ је алгебарски над $\mathbb{Q}$ зато што анулира полином $X^2 - 5 \in \mathbb{Q}[X]$. Слично је и $i \in \mathbb{C}$ алгебарски над $\mathbb{Q}$ пошто анулира полином $X^2 + 1 \in \mathbb{Q}[X]$.

Пример 6.5. Реални бројеви e и π су трансцендентни над $\mathbb{Q}$ (ово је мало теже доказати).

Задатак 65. Нека је K/F раширење поља и $a \in K$ трансцендентан елемент над F. Показати да тада $F[a]$ није поље.

Решење. Претпоставимо супротно, нека је $F[a]$ поље. Тада, специјално, за елемент $a \in F[a]$ постоји мултипликативни инверз, $a^{-1} = f(a)$, где је $f(X) \in F[X]$. Одатле је онда $1 = af(a)$, односно $af(a) - 1 = 0$. Добијамо да a анулира полином $Xf(X) - 1 \in F[X]$, што је контрадикција са чињеницом да је a трансцендентан над пољем F. Дакле, немогуће је да $F[a]$ буде поље.
□

Тврђење 6.6. Нека је K/F раширење поља и $a \in K$ алгебарски елемент над F. Тада постоји јединствени полином $\mu_{a,F}(X) \in F[X]$ такав да је:

- $\mu_{a,F}(X) \neq 0$
- $\mu_{a,F}(a) = 0$
- $\mu_{a,F}(X)$ је моничан и несводљив над пољем F.

Полином $\mu_{a,F}(X)$ се назива минималним полиномом елемента a над пољем F.

Тврђење 6.7. Нека је K/F раширење поља $a \in K$ алгебарски елемент над F, чији је минимални полином степена $n \in \mathbb{N}$. Тада је $F[a]$ коначно раширење поља F степена n и $\{1, a, a^2, \ldots, a^{n-1}\}$ је једна база за $F[a]$ над F.

Задатак 66. Доказати да је $\mathbb{Q}[\sqrt[3]{2}]$ поље, одредити степена раширења $\left[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}\right]$ и наћи једну базу за $\mathbb{Q}[\sqrt[3]{2}]$ над $\mathbb{Q}$.

Решење. Приметимо да $\sqrt[3]{2}$ анулира $f(X) = X^3 - 2 \in \mathbb{Q}[X]$. Зато је $\sqrt[3]{2}$ алгебарски елемент над $\mathbb{Q}$, па је $\mathbb{Q}[\sqrt[3]{2}]$ поље. Додатно, нуле полинома $f(X)$ (над пољем $\mathbb{C}$) су $\sqrt[3]{2}$, $\varepsilon\sqrt[3]{2}$ и $\varepsilon^2\sqrt[3]{2}$, где је $\varepsilon = e^{2\pi i/3}$. Закључујемо да $f(X)$ нема нула над $\mathbb{Q}$, па је несводљив над тим пољем (пошто је степена ≤ 3). Тај полином је и моничан, па представља минимални полином за $\sqrt[3]{2}$ над $\mathbb{Q}$. Зато је

$$\left[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}\right] = \deg f(X) = 3$$

и $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ је једна база за $\mathbb{Q}[\sqrt[3]{2}]$ над $\mathbb{Q}$.
□

Задатак 67. Доказати да је реалан број $\alpha = \sqrt{3+\sqrt{13}}$ алгебарски над пољем $\mathbb{Q}$. Затим наћи једну базу за $K = \mathbb{Q}[\alpha]$ над $\mathbb{Q}$ и изразити елемент $\frac{1}{\alpha+2}$ у добијеној бази.

Решење. Директан рачун показује да важи

$$\begin{aligned}
\alpha^2 &= 3 + \sqrt{13} \\
\alpha^2 - 3 &= \sqrt{13} \\
\alpha^4 - 6\alpha^2 + 9 &= 13 \\
\alpha^4 - 6\alpha^2 - 4 &= 0.
\end{aligned}$$

Дакле, α анулира полином $f(X) = X^4 - 6X^2 - 4 \in \mathbb{Q}[X]$, па је алгебарски елемент над пољем $\mathbb{Q}$.

Докажимо сада да је $f(X)$ минимални полином за α над $\mathbb{Q}$. Како је тај полином моничан, све што треба да покажемо је да је несводљив над пољем $\mathbb{Q}$. Претпоставимо супротно, нека је $f(x)$ сводљив над $\mathbb{Q}$. Тада постоје полиноми $g(X)$ и $h(X)$ са рационалним коефицијентима такви да је

$$f(X) = g(X)h(X),$$

при чему је $1 \leq \deg g, \deg h \leq 3$. То значи да имамо само две суштински различите могућности:

$$\deg g = 1, \deg h = 3 \quad \text{или} \quad \deg g = 2, \deg h = 2.$$

Прва могућност одмах отпада, јер имплицира да полином $f(X)$ има рационалне нуле, што није тачно (нуле полинома $f(X)$ су $\pm\sqrt{3 \pm \sqrt{13}}$). Зато, испитајмо другу могућност. Пошто је полином $f(X)$ моничан, можемо сматрати да су такви и полиноми $g(X)$ и $h(X)$. Када запишемо $g(X) = X^2 + aX + b$ и $h(X) = X^2 + cX + d$, где су $a, b, c, d \in \mathbb{Q}$ добијамо

$$\begin{aligned}
f(X) &= (X^2 + aX + b)(X^2 + cX + d) \\
X^4 - 6X^2 - 4 &= X^4 + (a+c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd.
\end{aligned}$$

Последња једначина омогућава да коефицијенте a, b, c и d изразимо као решења система

$$\begin{aligned} a + c &= 0 \\ b + d + ac &= -6 \\ ad + bc &= 0 \\ bd &= -4. \end{aligned}$$

Из прве једначине имамо $c = -a$, одакле заменом у трећу једначину добијамо

$$a(d - b) = 0.$$

Одавде добијамо два случаја $a = 0$ или $b = d$.

Ако је $a = 0$, онда је и $c = 0$, а почетни систем се своди на

$$\begin{aligned} b + d &= -6 \\ bd &= -4. \end{aligned}$$

Изражавањем $d = -6 - b$ добијамо квадратну једначину

$$b(-6 - b) = -4 \quad \text{односно} \quad b^2 + 6b - 4 = 0.$$

Ова једначина нема рационалних решења, што уз услов да је $b \in \mathbb{Q}$ даје контрадикцију. Дакле, овај случај је немогућ.

Претпоставимо сада да је $b = d$. Онда четврта једначина полазног система даје $b^2 = -4$, што одмах даје контадикцију, пошто је $b \in \mathbb{Q}$. На тај начин одмах одбацујемо и овај случај.

Закључујемо да је полином $f(X)$ несводљив над $\mathbb{Q}$, па је и минималан полином за α над $\mathbb{Q}$. Због тога је $\{1, \alpha, \alpha^2, \alpha^3\}$ једна база за $K = \mathbb{Q}[\alpha]$ над $\mathbb{Q}$, а такође добијамо и $[K : \mathbb{Q}] = 4$.

Остало је још да изразимо елемент $\frac{1}{\alpha+2}$ у добијеној бази. Другим речима, оно што тражимо су рационални бројеви A, B, C и D такви да је

$$\frac{1}{\alpha + 2} = A + B\alpha + C\alpha^2 + D\alpha^3.$$

Множењем претходне једнакости са $\alpha + 2$ добијамо

$$\begin{aligned} A(\alpha + 2) + B\alpha(\alpha + 2) + C\alpha^2(\alpha + 2) + D\alpha^3(\alpha + 2) &= 1 \\ A\alpha + 2A + B\alpha^2 + 2B\alpha + C\alpha^3 + 2C\alpha^2 + D\alpha^4 + 2D\alpha^3 &= 1 \\ A\alpha + 2A + B\alpha^2 + 2B\alpha + C\alpha^3 + 2C\alpha^2 + D\alpha^4 + 2D\alpha^3 - 1 &= 0 \end{aligned} \tag{14}$$

Приметимо је једнакост (14) расписана у односу на скуп $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ који није линеарно независан, па не можемо одмах тврдити да су одговарајући коефицијенти уз $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ једнаки нули. Тај проблем решавамо враћајући се на минимални полином $f(X) = X^4 - 6X^2 - 4$. Пошто је $f(\alpha) = 0$, следи да је испуњено $\alpha^4 - 6\alpha^2 - 4 = 0$, одакле добијамо потребни израз за α^4,

$$\alpha^4 = 6\alpha^2 + 4.$$

Враћањем у једнакост (14) добијамо

$$A\alpha + 2A + B\alpha^2 + 2B\alpha + C\alpha^3 + 2C\alpha^2 + D(6\alpha^2 + 4) + 2D\alpha^3 - 1 = 0$$
$$(2A + 4D - 1) + (A + 2B)\alpha + (B + 2C + 6D)\alpha^2 + (C + 2D)\alpha^3 = 0.$$

Сада, пошто скуп $\{1, \alpha, \alpha^2, \alpha^3\}$ јесте линеарно независан, можемо последњу једнакост заменити еквивалентним системом линеарних једначина

$$\begin{aligned} 2A + 4D - 1 &= 0 \\ A + 2B &= 0 \\ B + 2C + 6D &= 0 \\ C + 2D &= 0. \end{aligned}$$

Решавањем овог система добијамо $A = \frac{1}{3}$, $B = -\frac{1}{6}$, $C = -\frac{1}{6}$ и $D = \frac{1}{12}$. Дакле, тражени израз је

$$\frac{1}{\alpha + 1} = \frac{1}{3} - \frac{1}{6}\alpha - \frac{1}{6}\alpha^2 + \frac{1}{12}\alpha^3.$$

□

Задатак 68. Нека је $\alpha = \sqrt{2} + \sqrt{5}$. Доказати да је α алгебарски елемент над $\mathbb{Q}$, наћи $\mu_{\alpha,\mathbb{Q}}(X)$, степен раширења $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ и одредити једну базу за $\mathbb{Q}[\alpha]$ над $\mathbb{Q}$. Затим изразити елемент $\frac{1}{\alpha - 1}$ у добијеној бази.

Решење. Слично као у претходном задатку, прво имамо

$$\begin{aligned} \alpha^2 &= 7 + 2\sqrt{10} \\ \alpha^2 - 7 &= 2\sqrt{10} \\ \alpha^4 - 14\alpha^2 + 49 &= 40 \\ \alpha^4 - 14\alpha^2 + 9 &= 0. \end{aligned}$$

Закључујемо да α анулира полином $f(X) = X^4 - 14X^2 + 9 \in \mathbb{Q}[X]$, па је алгебарски елемент над пољем $\mathbb{Q}$.

Сада доказујемо да је $f(X)$ минимални полином за α над $\mathbb{Q}$. Како је тај полином моничан, све што треба да покажемо је да је несводљив над пољем $\mathbb{Q}$. Претпоставимо супротно, нека је $f(x)$ сводљив над $\mathbb{Q}$. Тада постоје полиноми $g(X)$ и $h(X)$ са рационалним коефицијентима такви да је

$$f(X) = g(X)h(X),$$

при чему је $1 \leq \deg g, \deg h \leq 3$. То значи да имамо само две суштински различите могућности:

$$\deg g = 1, \deg h = 3 \quad \text{или} \quad \deg g = 2, \deg h = 2.$$

Прва могућност одмах отпада, јер имплицира да полином $f(X)$ има рационалне нуле, што није тачно (нуле полинома $f(X)$ су $\pm(\sqrt{2} \pm \sqrt{5})$). Зато, испитајмо другу могућност. Пошто је полином $f(X)$ моничан, можемо сматрати да су такви и полиноми $g(X)$ и

$h(X)$. Када запишемо $g(X) = X^2 + aX + b$ и $h(X) = X^2 + cX + d$, где су $a, b, c, d \in \mathbb{Q}$ добијамо

$$f(X) = (X^2 + aX + b)(X^2 + cX + d)$$
$$X^4 - 14X^2 + 9 = X^4 + (a + c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd.$$

Последња једначина омогућава да коефицијенте a, b, c и d изразимо као решења система

$$\begin{aligned} a + c &= 0 \\ b + d + ac &= -14 \\ ad + bc &= 0 \\ bd &= 9. \end{aligned}$$

Из прве једначине имамо $c = -a$, одакле заменом у трећу једначину добијамо

$$a(d - b) = 0.$$

Одавде добијамо два случаја $a = 0$ или $b = d$.

Ако је $a = 0$, онда је и $c = 0$, а почетни систем се своди на

$$\begin{aligned} b + d &= -14 \\ bd &= 9. \end{aligned}$$

Изражавањем $d = -14 - b$ добијамо квадратну једначину

$$b(-14 - b) = 9 \quad \text{односно} \quad b^2 + 14b + 9 = 0.$$

Ова једначина нема рационалних решења, што уз услов да је $b \in \mathbb{Q}$ даје контрадикцију. Дакле, овај случај је немогућ.

Претпоставимо сада да је $b = d$. Онда четврта једначина полазног система даје $b^2 = 9$, одакле је $b = \pm 3$. Друга једначина полазног система онда постаје

$$a^2 \pm 6 = 14.$$

Одавде је $a^2 = 20$ или $a^2 = 8$. Ни једна од добијених могућности не допушта $a \in \mathbb{Q}$, што је контрадикција. На тај начин одбацујемо и овај случај.

Закључујемо да је полином $f(X)$ несводљив над $\mathbb{Q}$, па је и минималан полином за α над $\mathbb{Q}$. Због тога је $\{1, \alpha, \alpha^2, \alpha^3\}$ једна база за $K = \mathbb{Q}[\alpha]$ над $\mathbb{Q}$, а такође добијамо и $[K : \mathbb{Q}] = 4$.

Остало је још да изразимо елемент $\frac{1}{\alpha - 1}$ у добијеној бази. Треба да нађемо рационалне бројеве A, B, C и D такве да је

$$\frac{1}{\alpha - 1} = A + B\alpha + C\alpha^2 + D\alpha^3.$$

Множењем претходне једнакости са $\alpha - 1$ добијамо

$$\begin{aligned} A(\alpha-1) + B\alpha(\alpha-1) + C\alpha^2(\alpha-1) + D\alpha^3(\alpha-1) &= 1 \\ A\alpha - A + B\alpha^2 - B\alpha + C\alpha^3 - C\alpha^2 + D\alpha^4 - D\alpha^3 &= 1 \\ A\alpha - A + B\alpha^2 - B\alpha + C\alpha^3 - C\alpha^2 + D\alpha^4 - D\alpha^3 - 1 &= 0. \end{aligned} \tag{15}$$

Слично као у претходном задатку, враћамо се на минимални полином $f(X) = X^4 - 14X^2 + 9$ за α да решимо проблем чињенице да је једнакост (15) расписана у односу на скуп $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ који није линеарно независан . Пошто је $f(\alpha) = 0$, следи да је испуњено $\alpha^4 - 14\alpha^2 + 9 = 0$, одакле добијамо израз за α^4,

$$\alpha^4 = 14\alpha^2 - 9.$$

Враћањем у једнакост (15) добијамо

$$\begin{aligned} A\alpha - A + B\alpha^2 - B\alpha + C\alpha^3 - C\alpha^2 + D(14\alpha^2 - 9) - D\alpha^3 - 1 &= 0 \\ (-A - 9D - 1) + (A - B)\alpha + (B - C + 14D)\alpha^2 + (C - D)\alpha^3 &= 0. \end{aligned}$$

Пошто скуп $\{1, \alpha, \alpha^2, \alpha^3\}$ јесте линеарно независан, можемо последњу једнакост заменити еквивалентним системом линеарних једначина

$$\begin{aligned} -A - 9D - 1 &= 0 \\ A - B &= 0 \\ B - C + 14D &= 0 \\ C - D &= 0. \end{aligned}$$

Решавањем овог система добијамо $A = -\frac{13}{4}$, $B = -\frac{13}{4}$, $C = \frac{1}{4}$ и $D = \frac{1}{4}$. Дакле, тражени израз је

$$\frac{1}{\alpha - 1} = -\frac{13}{4} - \frac{13}{4}\alpha + \frac{1}{4}\alpha^2 + \frac{1}{4}\alpha^3.$$

□

Тврђење 6.8 (Гаусова лема)**.** Нека је $f(X) \in \mathbb{Z}[X]$. Тада је $f(X)$ несводљив над $\mathbb{Q}$ ако и само ако је несводљив над $\mathbb{Z}$.

Тврђење 6.9 (Ајзенштајнов критеријум)**.** Нека је $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$. Ако постоји прост број p такав да:

- $p \mid a_0, a_1, \ldots, a_{n-1}$
- $p \nmid a_n$
- $p^2 \nmid a_0$,

онда је $f(X)$ несводљив над $\mathbb{Z}$ (а тиме и над $\mathbb{Q}$ због Гаусове леме).

Пример 6.10. Полином $X^n - 2$ је несводљив над $\mathbb{Q}$ за све $n \in \mathbb{N}$ према Ајзенштајновом критеријуму примењеном за $p = 2$.
□

Задатак 69. Нека је θ једна нула полинома $f(X) = X^7 + 3X^5 + 18X^4 - 33X^2 + 6X - 3 \in \mathbb{Z}[X]$. Одредити степен раширења $[\mathbb{Q}[\theta] : \mathbb{Q}]$ и наћи једну базу за $\mathbb{Q}[\theta]$ над $\mathbb{Q}$.

Решење. Приметимо да је полином $f(X)$ несводљив над $\mathbb{Q}$ према Ајзенштајновом критеријуму примењеном за $p = 3$. Како је $f(X)$ моничан и $f(\theta) = 0$ закључујемо да је минимални полином за θ над $\mathbb{Q}$. Због тога је $[\mathbb{Q}[\theta] : \mathbb{Q}] = \deg f(X) = 7$ и скуп $\{1, \theta, \theta^2 \ldots, \theta^6\}$ представља једну базу за $\mathbb{Q}[\theta]$ над $\mathbb{Q}$.
□

Дефиниција 6.11. Нека је K/F раширење поља и $a, b \in K$ алгебарски елементи над F. Дефинишемо

$$F[a, b] = F[a][b] \leq K.$$

Слично, за сваких n алгебарских елемената $a_1, a_2, \ldots, a_n$ дефинишемо индуктивно

$$F[a_1, a_2, \ldots, a_n] = F[a_1, a_2, \ldots, a_{n-1}][a_n].$$

Тврђење 6.12. Нека је $F \leq E \leq K$ ланац коначних раширења. Тада је и раширење K/F коначно и важи

$$[K : F] = [K : E][E : F].$$

Прецизније, ако је $\{a_i \mid 1 \leq i \leq m\}$ база за K над E и $\{b_j \mid 1 \leq j \leq n\}$ база за E над F, онда је $\{a_i b_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ база за K над F.

Задатак 70. Посматрајмо поље $K = \mathbb{Q}[\sqrt{3}, i]$.
а) Наћи $\alpha \in \mathbb{C}$ такво да је $K = \mathbb{Q}[\alpha]$.
б) Одредити степен раширења $[K : \mathbb{Q}]$ и наћи једну базу за K над $\mathbb{Q}$.

Решење. а) Означимо $\alpha = \sqrt{3} + i$. Тада је $\alpha \in K$ као збир два елемента из K, па имамо да је $\mathbb{Q}[\alpha] \subseteq K$. Докажимо још обратну инклузију. Приметимо прво да је:

$$\frac{1}{\alpha} = \frac{1}{\sqrt{3} + i} = \frac{\sqrt{3} - i}{3 + 1} = \frac{1}{4}(\sqrt{3} - i) \in \mathbb{Q}[\alpha].$$

Онда и $4 \cdot \frac{1}{4}(\sqrt{3} - i) = \sqrt{3} - i \in \mathbb{Q}[\alpha]$. Коначно, одатле и $\sqrt{3} = \frac{1}{2}\left(\sqrt{3} + i + \sqrt{3} - i\right) \in \mathbb{Q}[\alpha]$, па и $i = \sqrt{3} + i - \sqrt{3} \in \mathbb{Q}[\alpha]$. Дакле, $\sqrt{3}, i \in \mathbb{Q}[\alpha]$, због чега је $K = \mathbb{Q}[\sqrt{3}, i] \subseteq \mathbb{Q}[\alpha]$. Према томе, добили смо тражену обратну инклузију, што омогућава да закључимо да је $K = \mathbb{Q}[\alpha]$.
б) Из низа међураширења $\mathbb{Q} \leq \mathbb{Q}[\sqrt{3}] \leq K$ имамо да је

$$[K : \mathbb{Q}] = [K : \mathbb{Q}[\sqrt{3}]] \cdot [\mathbb{Q}[\sqrt{3}] : \mathbb{Q}].$$

Степен раширења $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}]$ је једнак степену минималног полинома $\mu_{\sqrt{3},\mathbb{Q}}(X)$ за $\sqrt{3}$ над $\mathbb{Q}$. Како је $\sqrt{3}$ нула моничног полинома $X^2 - 3 \in \mathbb{Q}[X]$, несводљивог на основу Ајзенштајновог критеријума примењеног за $p = 3$, закључујемо да је $\mu_{\sqrt{3},\mathbb{Q}}(X) = X^2 - 3$. Због тога је $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 2$, а добијамо да је и $\{1, \sqrt{3}\}$ једна база за $\mathbb{Q}[\sqrt{3}]$ над $\mathbb{Q}$.

Слично, како је $K = \mathbb{Q}[\sqrt{3}][i]$, степен раширења $[K : \mathbb{Q}[\sqrt{3}]]$ је једнак степену минималног полинома $\mu_{i,\mathbb{Q}[\sqrt{3}]}(X)$ за i над $\mathbb{Q}[\sqrt{3}]$. Приметимо да i анулира полином

$X^2+1 \in \mathbb{Q}[\sqrt{3}][X]$. Због тога је $\deg \mu_{i,\mathbb{Q}[\sqrt{3}]}(X) \in \{1,2\}$. Ако би било $\deg \mu_{i,\mathbb{Q}[\sqrt{3}]}(X) = 1$, онда би следило да $i \in \mathbb{Q}[\sqrt{3}]$. Међутим, у пољу $\mathbb{Q}[\sqrt{3}]$ се налазе само реални бројеви, па је то немогуће. Закључујемо да је $\deg \mu_{i,\mathbb{Q}[\sqrt{3}]}(X) = 2$ и прецизније $\mu_{i,\mathbb{Q}[\sqrt{3}]}(X) = X^2+1$, пошто је полином X^2+1 моничан. Због тога је $[K : \mathbb{Q}[\sqrt{3}]] = 2$ и $\{1, i\}$ је једна база за K над $\mathbb{Q}[\sqrt{3}]$.

Коначно, добијамо да је $[K : \mathbb{Q}] = 2 \cdot 2 = 4$, као и да је $\{1, \sqrt{3}, i, i\sqrt{3}\}$ једна база за K над $\mathbb{Q}$.
□

Коренско поље

Нека је F поље и $f(X)$ полином са коефицијентима у F. Претпоставимо да $f(X)$ има све нуле $a_1, a_2, \ldots, a_n$ у неком раширењу K поља F. Коренско поље полинома $f(X)$ над пољем F је $F[a_1, a_2, \ldots, a_n]$.

Пример 6.13. Нуле полинома $f(X) = X^3 - 2 \in \mathbb{Q}[X]$ над пољем комплексних бројева $\mathbb{C}$ су једнаке $\sqrt[3]{2}, \varepsilon\sqrt[3]{2}$ и $\varepsilon^2\sqrt[3]{2}$, где је $\varepsilon = e^{\frac{2\pi i}{3}}$. Зато је коренско поље полинома $f(X)$ над $\mathbb{Q}$ једнако $\mathbb{Q}\left[\sqrt[3]{2}, \varepsilon\sqrt[3]{2}, \varepsilon^2\sqrt[3]{2}\right] = \mathbb{Q}[\sqrt[3]{2}, \varepsilon]$.
□

Задатак 71. Наћи број $\alpha \in \mathbb{C}$ такав да је коренско поље K полинома $f(X)$ над $\mathbb{Q}$ једнако $\mathbb{Q}[\alpha]$ ако је:
а) $f(X) = X^4 - 6X^2 + 4$.
б) $f(X) = X^4 + X^3 - X^2 - 2X - 2$.

Решење. а) Одредимо сва решења једначине $x^4 - 6x^2 + 4 = 0$ над пољем комплексних бројева $\mathbb{C}$. Увођењем смене $x^2 = t$ она се своди на квадратну једначину $t^2 - 6t + 4 = 0$. Њена решења су $t_1 = 3 + \sqrt{5}$ и $t_2 = 3 - \sqrt{5}$. Зато су решења полазне једначине

$$x_1 = \sqrt{3+\sqrt{5}},\ \ x_2 = -\sqrt{3+\sqrt{5}},\ \ x_3 = \sqrt{3-\sqrt{5}},\ \ x_4 = -\sqrt{3-\sqrt{5}}.$$

Према томе, важи $K = \mathbb{Q}[x_1, x_2, x_3, x_4] = \mathbb{Q}\left[\sqrt{3+\sqrt{5}}, \sqrt{3-\sqrt{5}}\right]$. Приметимо још да је

$$\sqrt{3+\sqrt{5}} \cdot \sqrt{3-\sqrt{5}} = \sqrt{9-5} = 2,$$

па важи $\sqrt{3-\sqrt{5}} = \frac{2}{\sqrt{3+\sqrt{5}}}$. Због тога је $K = \mathbb{Q}\left[\sqrt{3+\sqrt{5}}\right]$.
б) Одредимо сва решења једначине $x^4 + x^3 - x^2 - 2x - 2 = 0$ над пољем комплексних бројева $\mathbb{C}$. У ту сврху имамо

$$\begin{aligned}
&x^4 + x(x^2-2) - (x^2-2) - 4 = 0\\
&(x^2-2)(x^2+2) + x(x^2-2) - (x^2-2) = 0\\
&(x^2-2)(x^2+2+x-1) = 0\\
&(x^2-2)(x^2+x+1) = 0,\ \text{па је } x^2-2=0 \text{ или } x^2+x+1=0.
\end{aligned}$$

Закључујемо да су решења наше једначине $x_1 = \sqrt{2}$, $x_2 = -\sqrt{2}$, $x_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ и $x_4 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$, при чему је $x_3 x_4 = 1$. Због тога је

$$K = \mathbb{Q}[x_1, x_2, x_3, x_4] = \mathbb{Q}\left[\sqrt{2}, -\frac{1}{2} + i\frac{\sqrt{3}}{2}\right] = \mathbb{Q}\left[\sqrt{2}, i\sqrt{3}\right].$$

Означимо $\alpha = \sqrt{2} + i\sqrt{3}$. Одмах имамо да $\alpha \in K$, па важи $\mathbb{Q}[\alpha] \subseteq K$. Са друге стране,

$$\frac{1}{\alpha} = \frac{\sqrt{2} - i\sqrt{3}}{2+3} = \frac{1}{5}\left(\sqrt{2} - i\sqrt{3}\right).$$

Одатле је $\sqrt{2} - i\sqrt{3} = \frac{5}{\alpha} \in \mathbb{Q}[\alpha]$. Даље онда и

$$\sqrt{2} = \frac{1}{2}\left(\sqrt{2} + i\sqrt{3} + \sqrt{2} - i\sqrt{3}\right) \in \mathbb{Q}[\alpha],$$

као и

$$i\sqrt{3} = \frac{1}{2}\left(\sqrt{2} + i\sqrt{3} - (\sqrt{2} - i\sqrt{3})\right) \in \mathbb{Q}[\alpha].$$

Дакле, $\sqrt{2}, i\sqrt{3} \in \mathbb{Q}[\alpha]$, па је $K \subseteq \mathbb{Q}[\alpha]$. Закључујемо да је $K = \mathbb{Q}[\alpha]$ за $\alpha = \sqrt{2} + i\sqrt{3}$. □

7 Пример писменог испита са решењима

1. а) Показати да је са

$$a \cdot (u_1, u_2, u_3) = (u_1, au_1 + u_2, a^2u_1 + 2au_2 + u_3), \;\; a \in \mathbb{Z}, (u_1, u_2, u_3) \in \mathbb{R}^3$$

дефинисано једно дејство групе $(\mathbb{Z}, +)$ на скуп $\mathbb{R}^3$.
б) Одредити орбите за $(1,0,0)$ и $(0,0,3)$ при овом дејству.

Решење. а) За произвољне $a, b \in \mathbb{Z}$ и $(u_1, u_2, u_3) \in \mathbb{R}^3$ имамо:

$$\begin{aligned}
0 \cdot (u_1, u_2, u_3) &= (u_1, 0 \cdot u_1 + u_2, 0^2 \cdot u_1 + 2 \cdot 0 \cdot u_2 + u_3) = (u_1, u_2, u_3) \\
a \cdot (b \cdot (u_1, u_2, u_3)) &= a \cdot (u_1, bu_1 + u_2, b^2u_1 + 2bu_2 + u_3) \\
&= (u_1, au_1 + bu_1 + u_2, a^2u_1 + 2a(bu_1 + u_2) + b^2u_1 + 2bu_2 + u_3) \\
&= (u_1, (a+b)u_1 + u_2, a^2u_1 + 2abu_1 + 2au_2 + b^2u_1 + 2bu_2 + u_3) \\
&= (u_1, (a+b)u_1 + u_2, (a^2 + 2ab + b^2)u_1 + 2(a+b)u_2 + u_3) \\
&= (u_1, (a+b)u_1 + u_2, (a+b)^2u_1 + 2(a+b)u_2 + u_3) \\
&= (a+b) \cdot (u_1, u_2, u_3).
\end{aligned}$$

Овим смо показали да $\cdot$ јесте дејство.
б) По дефиницији је

$$\begin{aligned}
\mathcal{O}_{(1,0,0)} &= \{a \cdot (1,0,0) \mid a \in \mathbb{Z}\} \\
&= \left\{(1, a \cdot 1 + 0, a^2 \cdot 1 + 2a \cdot 0 + 0) \mid a \in \mathbb{Z}\right\} \\
&= \{(1, a, a^2) \mid a \in \mathbb{Z}\}.
\end{aligned}$$

Слично налазимо и да је

$$\begin{aligned}\mathcal{O}_{(0,0,3)} &= \{a \cdot (0,0,3) \mid a \in \mathbb{Z}\} \\ &= \left\{(0, a \cdot 0 + 0, a^2 \cdot 0 + 2a \cdot 0 + 3) \mid a \in \mathbb{Z}\right\} \\ &= \{(0,0,3) \mid a \in \mathbb{Z}\},\end{aligned}$$

што завршава задатак.
□

2. Нека је G група реда 2552.
а) Доказати да G има нормалну подгрупу реда 11 или реда 29.
б) Доказати да G има подгрупу реда $11 \cdot 29$. Да ли она мора бити циклична?

Решење. а) Из Треће теореме Силова имамо:

$$\left.\begin{aligned} s_{11} &\equiv 1 \pmod{11} \\ s_{11} &\mid 232 \end{aligned}\right\} \longrightarrow s_{11} \in \{1, 232\}$$

$$\left.\begin{aligned} s_{29} &\equiv 1 \pmod{29} \\ s_{29} &\mid 88 \end{aligned}\right\} \longrightarrow s_{29} \in \{1, 88\}.$$

Докажимо да мора бити $s_{11} = 1$ или $s_{29} = 1$. У супротном је $s_{11} = 232$ и $s_{29} = 88$. Означимо са H_i све S_{11} подгрупе и са K_i све S_{29} подгрупе од G. Тада је $|H_i| = 11$ и $|K_i| = 29$. Имамо и следеће:

- $H_i \cap K_j = \langle e \rangle$ за све i и j
  Важи да је $H_i \cap K_j$ подгрупа од H_i и K_j, па на основу Лагранжеве теореме следи

  $$|H_i \cap K_j| \mid |H_i|, |K_j| \quad \text{тј.} \quad |H_i \cap K_j| \mid 11, 29.$$

  Како су бројеви 11 и 29 узајамно прости, следи $|H_i \cap K_j| = 1$ тј. $H_i \cap K_j = \langle e \rangle$.

- $H_i \cap H_j = K_i \cap K_j = \langle e \rangle$ за све $i \neq j$
  Важи да је $H_i \cap H_j$ подгрупа и од H_i и од H_j. Како су H_i и H_j обе реда 11, њихове једине подгрупе су тривијална подгрупа $\langle e \rangle$ и оне саме. Пошто је $H_i \neq H_j$, друго је немогуће, па следи $H_i \cap H_j = \langle e \rangle$. Потпуно слично радимо и за $K_i \cap K_j$.

Означимо са $\mathcal{S}$ скуп елемената из G који се налазе у некој од погрупа H_i или K_i. Тада је $\mathcal{S} \subseteq G$, па имамо $|\mathcal{S}| \leq |G|$. Са друге стране, пошто се све подгрупе H_i и K_i међусобно секу тривијално, добијамо да је

$$\begin{aligned}|\mathcal{S}| &= s_{11}(11-1) + s_{29}(29-1) + 1 \\ &= 232 \cdot 10 + 88 \cdot 28 + 1 \\ &= 4785 > |G|.\end{aligned}$$

Добијена контрадикција показује да је $s_{11} = 1$ или $s_{29} = 1$. То управо значи да је барем једна од S_{11} или S_{29} подгрупа јединствена, а тиме и нормална у G. Како су оне реда 11 или 29, добијамо тражено тврђење.

б) Уочимо сада произвољну фиксирану S_{11} подгрупу H и S_{29} подгрупу K од G. Тада је $|H| = 11$ и $|K| = 29$, а из дела а) знамо да је барем једна од њих нормална у G, као и да је $|H \cap K| = 1$. Због тога је $HK \leq G$ и

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{11 \cdot 29}{1} = 11 \cdot 29.$$

Дакле, HK представља тражену подгрупу. Пошто су 11 и 29 различити прости бројеви такви да $11 \nmid 29 - 1$, закључујемо да она јесте циклична (на основу Задатка 30).
□

3. Посматрајмо скуп

$$S = \left\{ \frac{a}{b} \in \mathbb{Q} \mid \text{НЗД}(a, b) = 1,\ 5 \nmid b \right\}.$$

а) Доказати да је S комутативни прстен са јединицом у односу на операције сабирања и множења рационалних бројева.
б) Испитати да ли је S домен, односно поље.

Решење. а) Уочимо произвољна два елемента $\frac{a}{b}$ и $\frac{c}{d}$ из S. Тада знамо да $5 \nmid b, d$, као и

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Бројилац $ad + bc$ и именилац bd добијеног збира не морају бити узајамно прости. Међутим, како $5 \nmid b, d$, важи да и $5 \nmid bd$, што значи да ни после евентуалног скраћивања у разломку $\frac{ad+bc}{bd}$ именилац не може бити дељив са 5. Одатле следи да $\frac{a}{b} + \frac{c}{d} \in S$, чиме смо показали да је сабирање рационалних бројева коректно дефинисана операција на S.

Из потпуно истих разлога, пошто је

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

имамо да је и множење рационалних бројева коректно дефинисана операција на S.

Познато нам је да сабирање и множење рационалних бројева чине један комутативни прстен са јединицом на скупу рационалних бројева $\mathbb{Q}$. Као што смо већ видели, те две операције коректно су дефинисане на скупу S, што уз очигледну чињеницу да $0, 1 \in S$ омогућава да закључимо да је и S комутативни прстен са јединицом (у односу на операције сабирања и множења рационалних бројева).
б) Одмах можемо закључити да S јесте домен. Разлог томе је што би постојање правих делитеља нуле у S одмах имплицирало и постојање правих делитеља нуле у $\mathbb{Q}$, а то није могуће, јер је $\mathbb{Q}$ поље (у односу на операције сабирања и множења рационалних бројева које посматрамо).

Са друге стране, S није поље, јер у њему постоје ненула елементи који немају мултипликативни инверз. Пример једног таквог елемента је $\frac{5}{7}$, због чињенице да $\frac{7}{5} \notin S$.
□

4. Одредити НЗД$(11 - 14i, 19 + 7i)$ у прстену Гаусових целих $\mathbb{Z}[i]$.

Решење. За почетак имамо да су норме посматраних елемената редом:

$$N(11-14i) = 11^2 + 14^2 = 121 + 196 = 317$$
$$N(19+7i) = 19^2 + 7^2 = 361 + 49 = 410.$$

Закључујемо да је $19+7i$ веће норме, па ћемо га поделити бројем $11-14i$ у $\mathbb{C}$:

$$\frac{19+7i}{11-14i} = \frac{(19+7i)(11+14i)}{317} = \frac{111+343i}{317} = \frac{111}{317} + \frac{343}{317}i.$$

Количник у $\mathbb{Z}[i]$ ће бити елемент чији је реални део најближи цео број броју $\frac{111}{317}$, а имагинарни део броју $\frac{343}{317}$, што је $0 + 1 \cdot i = i$. Онда је остатак једнак

$$19 + 7i - i(11 - 14i) = 19 + 7i - 11i - 14 = 5 - 4i.$$

Како нисмо добили остатак 0, нити норме 1, поступак настављамо за $11-4i$ и $5-4i$. Имамо:

$$\frac{11-4i}{5-4i} = \frac{(11-4i)(5+4i)}{41} = \frac{71+24i}{41} = \frac{71}{41} + \frac{24}{41}i.$$

Најближи цео број броју $\frac{71}{41}$ је 2, а броју $\frac{24}{41}$ је 1, па је количник у $\mathbb{Z}[i]$ једнак $2+i$. Остатак је онда

$$11 - 4i - (5 - 4i)(2 + i) = 11 - 4i + 3i - 14 = -3 - i.$$

Поново нисмо добили остатак 0, нити норме 1, па поступак настављамо за $5-4i$ и $-3-i$. Добијамо:

$$\frac{5-4i}{-3-i} = \frac{(5-4i)(-3+i)}{10} = \frac{-11+17i}{10} = -\frac{11}{10} + \frac{17}{10}i.$$

Најближи цео број броју $-\frac{11}{10}$ је -1, а броју $\frac{17}{10}$ је 2, па је количник у $\mathbb{Z}[i]$ једнак $-1+2i$. Остатак је онда

$$5 - 4i - (-3 - i)(-1 + 2i) = 5 - 4i - 5 + 5i = i.$$

Приметимо да је сада норма остатка једнака 1, што завршава наш поступак, уз закључак

$$\text{НЗД}(11 - 4i, 19 + 7i) = i.$$

□

5. Нека је K коренско поље полинома $X^4+2X^2-15 \in \mathbb{Q}[X]$ над пољем $\mathbb{Q}$. Одредити степен раширења $[K : \mathbb{Q}]$, наћи једну базу за K над $\mathbb{Q}$, као и број $\alpha \in \mathbb{C}$ такав да је $K = \mathbb{Q}[\alpha]$.

Решење. Прво одређујемо сва решења једначине $x^4 + 2x^2 - 15 = 0$ над пољем комплексних бројева $\mathbb{C}$. Увођењем смене $x^2 = t$ она се своди на квадратну једначину $t^2 + 2t - 15 = 0$, чија су решења $t_1 = 3$ и $t_2 = -5$. Зато су решења полазне једначине $\pm\sqrt{3}$ и $\pm i\sqrt{5}$, па налазимо да је $K = \mathbb{Q}[\pm\sqrt{3}, \pm i\sqrt{5}] = \mathbb{Q}\left[\sqrt{3}, i\sqrt{5}\right]$.

Посматрајући сада низ међупроширења $\mathbb{Q} \leq \mathbb{Q}[\sqrt{3}] \leq K$, добијамо да је

$$[K : \mathbb{Q}] = [K : \mathbb{Q}[\sqrt{3}]] \cdot [\mathbb{Q}[\sqrt{3}] : \mathbb{Q}].$$

Степен проширења $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}]$ је једнак степену минималног полинома $\mu_{\sqrt{3},\mathbb{Q}}(X)$ за $\sqrt{3}$ над $\mathbb{Q}$. Како је $\sqrt{3}$ нула моничног полинома $X^2 - 3 \in \mathbb{Q}[X]$, несводљивог на основу Ајзенштајновог критеријума примењеног за $p = 3$, закључујемо да је $\mu_{\sqrt{3},\mathbb{Q}}(X) = X^2 - 3$. Због тога је $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 2$, а добијамо да је и $\{1, \sqrt{3}\}$ једна база за $\mathbb{Q}[\sqrt{3}]$ над $\mathbb{Q}$.

Слично, како је $K = \mathbb{Q}[\sqrt{3}][i\sqrt{5}]$, степен проширења $[K : \mathbb{Q}[\sqrt{3}]]$ је једнак степену минималног полинома $\mu_{i\sqrt{5},\mathbb{Q}[\sqrt{3}]}(X)$ за $i\sqrt{5}$ над $\mathbb{Q}[\sqrt{3}]$. Приметимо да $i\sqrt{5}$ анулира полином $X^2 + 5 \in \mathbb{Q}[\sqrt{3}][X]$. Због тога је $\deg \mu_{i\sqrt{5},\mathbb{Q}[\sqrt{3}]}(X) \in \{1, 2\}$. Ако би било $\deg \mu_{i\sqrt{5},\mathbb{Q}[\sqrt{3}]}(X) = 1$, онда би следило да $i\sqrt{5} \in \mathbb{Q}[\sqrt{3}]$. Међутим, у пољу $\mathbb{Q}[\sqrt{3}]$ се налазе само реални бројеви, па је то немогуће. Закључујемо да је $\deg \mu_{i\sqrt{5},\mathbb{Q}[\sqrt{3}]}(X) = 2$ и прецизније $\mu_{i\sqrt{5},\mathbb{Q}[\sqrt{3}]}(X) = X^2 + 5$, пошто је полином $X^2 + 5$ моничан. Због тога је $[K : \mathbb{Q}[\sqrt{3}]] = 2$ и $\{1, i\sqrt{5}\}$ је једна база за K над $\mathbb{Q}[\sqrt{3}]$.

Коначно, добијамо да је $[K : \mathbb{Q}] = 2 \cdot 2 = 4$, као и да је $\{1, \sqrt{3}, i\sqrt{5}, i\sqrt{15}\}$ једна база за K над $\mathbb{Q}$.

Означимо још $\alpha = \sqrt{3} + i\sqrt{5}$. Тада је $\alpha \in K$ као збир два елемента из K, па имамо да је $\mathbb{Q}[\alpha] \subseteq K$. Докажимо још обратну инклузију. Приметимо прво да је:

$$\frac{1}{\alpha} = \frac{1}{\sqrt{3} + i\sqrt{5}} = \frac{\sqrt{3} - i\sqrt{5}}{3 + 5} = \frac{1}{8}(\sqrt{3} - i\sqrt{5}) \in \mathbb{Q}[\alpha].$$

Онда и $8 \cdot \frac{1}{8}(\sqrt{3} - i\sqrt{5}) = \sqrt{3} - i\sqrt{5} \in \mathbb{Q}[\alpha]$. Коначно, одатле и $\sqrt{3} = \frac{1}{2}\left(\sqrt{3} + i\sqrt{5} + \sqrt{3} - i\sqrt{5}\right) \in \mathbb{Q}[\alpha]$, па и $i\sqrt{5} = \sqrt{3} + i\sqrt{5} - \sqrt{3} \in \mathbb{Q}[\alpha]$. Дакле, $\sqrt{3}, i\sqrt{5} \in \mathbb{Q}[\alpha]$, због чега је $K = \mathbb{Q}[\sqrt{3}, i\sqrt{5}] \subseteq \mathbb{Q}[\alpha]$. Према томе, добили смо тражену обратну инклузију, што омогућава да закључимо да је $K = \mathbb{Q}[\alpha]$.

□