1

Дејство групе на скуп

1.1 Теоријски увод

Дефиниција Нека је G група и S скуп. Дејство групе G на скуп S је пресликавање $\cdot : G \times S \longrightarrow S$, које задовољава две аксиоме:

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

(Овде је $g \cdot x$ ознака за $\cdot(g, x)$.)

Ако G делује на скуп S, пишемо $G \circlearrowleft S$, и кажемо да је S један G-скуп.

Тврђење 1 Нека $G \circlearrowleft S$. Тада:

1. $g \cdot x = y$ ако и само ако $x = g^{-1} \cdot y$;
2. пресликавање $g \cdot : S \longrightarrow S$, дато са $x \mapsto g \cdot x$, је пермутација скупа S;
3. пресликавање $\phi : S \longrightarrow \mathrm{Sym}(S)$, дато са $\phi(g) = g\cdot$, је хомоморфизам група.

Обратно, ако је $\phi : G \longrightarrow \mathrm{Sym}(S)$ неки хомоморфизам група, тада је са $g \cdot x = \phi(g)(x)$ дефинисано једно дејство $G \circlearrowleft S$.

Дакле, постоји природна *бијективна кореcподенција* између скупа свих различитих дејстава групе G на скупу S и скупа свих хомоморфизама из G у $\mathrm{Sym}(S)$, где је $\mathrm{Sym}(S)$ група свих бијективних пресликавања из S у S.

Дефиниција Нека $G \circlearrowleft S$. *Орбита* елемента $x \in S$ је скуп $\mathcal{O}(x) = \{g \cdot x \mid g \in G\} \subseteq S$. Кардиналност орбите $|\mathcal{O}(x)|$, зовемо ред орбите. Скуп свих орбита означавамо са S/G.

Тврђење 2 Нека $G \circlearrowleft S$. Дефинишимо на S релацију $\sim$ са: $x \sim y$ ако и само ако постоји $g \in G$ тако да $g \cdot x = y$. Тада:

1. $\sim$ је еквиваленција на скупу S;
2. класа еквиваленције елемента x је $x/\sim = \mathcal{O}(x)$;
3. S/G је партиција скупа S.
4. **(Класна једнакост)** Ако је S коначан скуп и T скуп представника партиције S/G, тада $|S| = \sum_{x \in T} |\mathcal{O}(x)|$.

Дефиниција Нека $G \circlearrowleft S$. *Стабилизатор* елемента $x \in S$ је скуп $\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\} \subseteq G$.

Тврђење 3 Нека $G \circlearrowleft S$, и нека је $x \in S$ произвољно. Тада:

1. $\mathrm{Stab}(x) \leq G$;
2. додељивање $g \cdot x \mapsto g\,\mathrm{Stab}(x)$ је добро дефинисана бијекција $\mathcal{O}(x) \longrightarrow G/\mathrm{Stab}(x)$ ($G/\mathrm{Stab}(x)$ је ознака за скуп левих косета подгрупе $\mathrm{Stab}(x)$);
3. $|G : \mathrm{Stab}(x)| = |\mathcal{O}(x)|$;
4. ако је G коначна, $|G| = |\mathrm{Stab}(x)| \cdot |\mathcal{O}(x)|$. Одавде специјално важи да ред орбите дели ред групе.

Дефиниција Нека $G \circlearrowleft S$. *Фиксни скуп* елемента $g \in G$ је скуп $\mathrm{Fix}(g) = \{x \in S \mid g \cdot x = x\} \subseteq S$.

Тврђење 4 (Бернсајдова лема) Нека је G коначна група и $G \circlearrowleft S$. Тада $|S/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$.

Дефиниција Нека група G дејствује на скуповима X и Y. За пресликавање $\phi : X \longrightarrow Y$ кажемо да је *хомоморфизам G-скупова* ако оно комутира са дејством групе G, тј. ако за свако $g \in G$ и $x \in X$ важи $\phi(g \cdot x) = g \cdot \phi(x)$. Ако је ϕ и бијективно, зовемо га *изоморфизам G-скупова*.

Дефиниција Дејство $G \circlearrowleft S$ је *транзитивно* ако постоји $x \in S$ тако да за свако $y \in S$ постоји $g \in G$ тако да важи $y = g \cdot x$. Еквивалентно, $|S/G| = 1$. Еквивалентно, за све $x \in S$ и све $y \in S$ постоји $g \in G$ тако да $y = g \cdot x$.

Дефиниција Дејство $G \circlearrowleft S$ је *дупло транзитивно* ако постоје $x_1, x_2 \in S$, $x_1 \neq x_2$, тако да за све $y_1, y_2 \in S$, $y_1 \neq y_2$, постоји $g \in G$ тако да важи $y_1 = g \cdot x_1$ и $y_2 = g \cdot x_2$. Еквивалентно, за све $x_1, x_2 \in S$, $x_1 \neq x_2$, и све $y_1, y_2 \in S$, $y_1 \neq y_2$, постоји $g \in G$ тако да $y_1 = g \cdot x_1$ и $y_2 = g \cdot x_2$.

Дупло транзитивно дејство је наравно и транзитивно.

1.2 Решени задаци

1. Означимо са $\mathbb{H} = \{z = x + iy \mid x \in \mathbb{R}, y \in \mathbb{R}_{>0}\} \subseteq \mathbb{C}$ такозвану *горњу полураван*. Доказати да је са

$$(\gamma, z) \mapsto \gamma \cdot z = \frac{az+b}{cz+d}, \qquad \text{где је } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{R}), \tag{1.1}$$

задато једно дејство *специјалне линеарне групе* $\mathrm{SL}_2(\mathbb{R})$ на $\mathbb{H}$.

Решење. Најпре трансформишимо

$$\frac{az+b}{cz+d} = \frac{(az+b)(c\overline{z}+d)}{|cz+d|^2} = \frac{ac|z|^2 + bd + (ad+bc)x + i(ad-bc)y}{|cz+d|^2},$$

па за $z \in \mathbb{H}$, за које је дакле $\Im(z) = y > 0$, важи

$$\Im\left(\frac{az+b}{cz+d}\right) = \frac{y}{|cz+d|^2} > 0,$$

тј. $\gamma \cdot z \in \mathbb{H}$, за свако $\gamma \in \mathrm{SL}_2(\mathbb{R})$. Другим речима, са (1.1) је добро дефинисано једно пресликавање из $\mathrm{SL}_2(\mathbb{R}) \times \mathbb{H}$ у $\mathbb{H}$.

Сада проверавамо две аксиоме дејства. За неутрал $\gamma = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ и произвољну тачку $z \in \mathbb{H}$ имамо да је $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot z = \frac{1z+0}{0z+1} = z$, па важи прва аксиома.

Нека су сада $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ и $\gamma_1 = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ две произвољне матрице из групе $\mathrm{SL}_2(\mathbb{Z})$ и $z \in \mathbb{H}$ произвољна тачка у горњој полуравни. Директно рачунамо

$$\begin{aligned}
\gamma \cdot (\gamma_1 \cdot z) &= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \frac{a_1 z + b_1}{c_1 z + d_1} = \frac{a\frac{a_1 z + b_1}{c_1 z + d_1} + b}{c\frac{a_1 z + b_1}{c_1 z + d_1} + d} \\
&= \frac{(aa_1 + bc_1)z + ab_1 + bd_1}{(ca_1 + dc_1)z + cb_1 + dd_1} = \begin{bmatrix} aa_1 + bc_1 & ab_1 + bd_1 \\ ca_1 + dc_1 & cb_1 + dd_1 \end{bmatrix} \cdot z \\
&= \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \right) \cdot z = (\gamma\gamma_1) \cdot z,
\end{aligned}$$

што значи да важи и друга аксиома.

2. Нека је V векторски простор над пољем F. Онда мултипликативна група $F^{\times}$ поља F делује на V скаларним множењем.

Решење. Дакле пресликавање $F^{\times} \times V \longrightarrow V$ је дато са $x \cdot v = xv$, где је на десној страни множење вектора $v \in V$ скаларом x у F-векторском простору V. Онда за $v \in V$, $x, y \in F^{\times}$, формуле

$$1 \cdot v = 1v = v \quad \text{и} \quad (xy) \cdot v = (xy)v = x(yv) = x \cdot (y \cdot v)$$

следе из аксиома векторског простора, па $F^{\times} \circlearrowleft V$.

3. Нека је $\mathcal{Q} = \{aX^2 + bXY + cY^2 \mid a, b, c \in \mathbb{Z}\}$ скуп свих *бинарних квадратних форми* (хомогених полинома степена 2, са две неодређене X и Y) са коефицијентима у прстену $\mathbb{Z}$. Ако за $\gamma = \begin{bmatrix} t & u \\ v & w \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ и квадратну форму $q(X, Y) = aX^2 + bXY + cY^2$ дефинишемо

$$(\gamma \cdot q)(X, Y) = q([X, Y]\gamma) = q(tX + vY, uX + wY),$$

доказати да је $\cdot$ једно дејство групе $\mathrm{SL}_2(\mathbb{Z})$ на скуп $\mathcal{Q}$.

Нека је $\mathcal{Q}_d = \{aX^2 + bXY + cY^2 \mid a, b, c \in \mathbb{Z},\ b^2 - 4ac = d\} \subseteq \mathcal{Q}$ скуп свих бинарних квадратних форми *дискриминанте* $b^2 - 4ac$ једнаке неком фиксираном $d \in \mathbb{Z}$. Доказати да је рестрикција пресликавања $\cdot : \mathrm{SL}_2(\mathbb{Z}) \times \mathcal{Q} \longrightarrow \mathcal{Q}$ на $\mathrm{SL}_2(\mathbb{Z}) \times \mathcal{Q}_d$ једно дејство групе $\mathrm{SL}_2(\mathbb{Z})$ на скуп $\mathcal{Q}_d$.

Решење. Најпре, $q(tX + vY, uX + wY)$ је једнако

$$= a(tX + vY)^2 + b(tX + vY)(uX + wY) + c(uX + wY)^2$$

$$= (at^2 + btu + cu^2)X^2 + (2atv + btw + buv + 2cuw)XY + (av^2 + bvw + cw^2)Y^2, \tag{1.2}$$

што је такође једна бинарна квадратна форма са целобројним коефицијентима, тј. елемент из $\mathcal{Q}$.

Проверимо прву аксиому дејства: за произвољну квадратну форму $q \in \mathcal{Q}$ имамо

$$\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot q \right)(X, Y) = q([X, Y] \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}) = q(X, Y),$$

тј. важи да је $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot q = q$, за све q.

Нека су γ и γ_1 две произвољне матрице из $\mathrm{SL}_2(\mathbb{Z})$. Онда је

$$\begin{aligned} ((\gamma\gamma_1) \cdot q)(X, Y) &= q([X, Y](\gamma\gamma_1)) = q([X, Y]\gamma\gamma_1) \\ &= (\gamma_1 \cdot q)([X, Y]\gamma) = (\gamma \cdot (\gamma_1 \cdot q))(X, Y), \end{aligned}$$

па важи и друга аксиома.

За други део задатка, довољно је показати да је $\gamma \cdot q \in \mathcal{Q}_d$, за произвољне $\gamma = \begin{bmatrix} t & u \\ v & w \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ и $q \in \mathcal{Q}_d$, јер аксиоме дејства аутомацки важе. Међутим, из (1.2) видимо да је дискриминанта квадратне форме $(\gamma \cdot q)(X, Y)$ дата са

$$(2atv + btw + buv + 2cuw)^2 - 4(at^2 + btu + cu^2)(av^2 + bvw + cw^2)$$

$$= (b^2 - 4ac)(t^2w^2 + u^2v^2 - 2tuvw) = d(tw - uv)^2 = d,$$

јер је дискриминанта од q једнака $b^2 - 4ac = d$, а $\det(\gamma) = 1$.

4. Доказати Тврђење 1.

Решење. Нека $G \circlearrowright S$.

1. Ако је $g \cdot x = y$, тада је $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot y$. По другој аксиоми је даље $(g^{-1}g) \cdot x = g^{-1} \cdot y$, тј. $e \cdot x = g^{-1} \cdot y$, одакле на основу прве аксиоме важи $x = g^{-1} \cdot y$.

   Аналогно, ако је $x = g^{-1} \cdot y$, тада је $g \cdot x = g \cdot (g^{-1} \cdot y)$. На основу друге аксиоме је $g \cdot x = (gg^{-1}) \cdot y$, тј. $g \cdot x = e \cdot y$, одакле је по првој аксиоми $g \cdot x = y$.

2. Докажимо да је пресликавање $g\cdot$ 1-1. Ако је $g \cdot x_1 = g \cdot x_2$, тада је, користећи аксиоме 2 и 1, редом, $x_1 = g^{-1} \cdot (g \cdot x_2) = (g^{-1}g) \cdot x_2 = e \cdot x_2 = x_2$.

   Како је за свако y тачно $g^{-1} \cdot y = g^{-1} \cdot y$, према 1. важи $g \cdot (g^{-1} \cdot y) = y$, што показује да је $g\cdot$ на.

3. Према 2, $\phi : G \longrightarrow \mathrm{Sym}(S)$ је добро дефинисана функција. Приметите да за све $g, h \in G$ и све $x \in S$ важи $\phi(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot (\phi(h)(x)) = \phi(g)(\phi(h)(x)) = (\phi(g) \circ \phi(h))(x)$, одакле је $\phi(gh) = \phi(g) \circ \phi(h)$, што доказује да је ϕ хомоморфизам група.

4. Нека је $\phi : G \longrightarrow \mathrm{Sym}(S)$ хомоморфизам група, и нека је $g \cdot x = \phi(g)(x)$. Докажимо да ово јесте дејство. Најпре, $e \cdot x = \phi(e)(x) = \mathrm{id}_S(x) = x$, где је id_S идентичка пермутација на S, а $\phi(e) = \mathrm{id}_S$ јер је ϕ хомоморфизам. Такође, $(gh) \cdot x = \phi(gh)(x) = (\phi(g) \circ \phi(h))(x) = \phi(g)(\phi(h)(x)) = \phi(g)(h \cdot x) = g \cdot (h \cdot x)$. Дакле, обе аксиоме су испуњене.

5. Доказати Тврђење 2.

Решење. Нека $G \circlearrowleft S$ и нека је на S: $x \sim y$ ако и само ако постоји $g \in G$ тако да $g \cdot x = y$.

1. $\sim$ је рефлексивна јер је $e \cdot x = x$, за све x. Ако је $g \cdot x = y$, тада је $g^{-1} \cdot y = x$, што доказује симетричност релације $\sim$. Коначно, ако је $g \cdot x = y$ и $h \cdot y = z$, тада је $(hg) \cdot x = h \cdot (g \cdot x) = h \cdot y = z$, одакле следи транзитивност релације $\sim$.

2. Приметите да $y \in x/\sim$ ако и само ако $x \sim y$, што важи ако и само ако постоји $g \in G$ тако да $g \cdot x = y$, тј. ако и само ако $y \in \{g \cdot x \mid g \in G\} = \mathcal{O}(x)$.

3. Према 2. је $S/G = S/\sim$, а количнички скуп еквиваленције је увек партиција.

4. Ако је T скуп представника партиције S/G, тада је $S = \bigsqcup_{x \in T} \mathcal{O}(x)$, па ако је S коначан, тада је $|S| = \sum_{x \in T} |\mathcal{O}(x)|$.

6. Доказати Тврђење 3.

Решење. Нека $G \circlearrowleft S$.

1. Како је $e \cdot x = x$, то $e \in \mathrm{Stab}(x)$. Ако $g \in \mathrm{Stab}(x)$, тј. ако $g \cdot x = x$, тада је $x = g^{-1} \cdot x$, па и $g^{-1} \in \mathrm{Stab}(x)$. Коначно, ако $g, h \in \mathrm{Stab}(x)$, тада $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$, одакле $gh \in \mathrm{Stab}(x)$. Дакле, $\mathrm{Stab}(x) \leq G$.

2. Докажимо најпре да је додељивање $g \cdot x \mapsto g\mathrm{Stab}(x)$ добро дефинисано, тј. ако је $g_1 \cdot x = g_2 \cdot x$ тада је и $g_1\mathrm{Stab}(x) = g_2\mathrm{Stab}(x)$. Нека је $g_1 \cdot x = g_2 \cdot x$. Тада $(g_2^{-1}g_1) \cdot x = x$, тј. $g_2^{-1}g_1 \in \mathrm{Stab}(x)$, па је $g_2^{-1}g_1\mathrm{Stab}(x) = \mathrm{Stab}(x)$, одакле је $g_1\mathrm{Stab}(x) = g_2\mathrm{Stab}(x)$.

   Ако је $g_1\mathrm{Stab}(x) = g_2\mathrm{Stab}(x)$, тада је $g_2^{-1}g_1\mathrm{Stab}(x) = \mathrm{Stab}(x)$, па $g_2^{-1}g_1 \in \mathrm{Stab}(x)$. Тада $(g_2^{-1}g_1) \cdot x = x$, тј. $g_1 \cdot x = g_2 \cdot x$, што доказује да је дато додељивање 1-1.

   Коначно у косет $g\mathrm{Stab}(x)$ се слика елемент $g \cdot x \in \mathcal{O}(x)$, одакле следи да је додељивање на.

3. Према 2. важи $|G/\mathrm{Stab}(x)| = |\mathcal{O}(x)|$, а по дефиницији је $|G : \mathrm{Stab}(x)| = |G/\mathrm{Stab}(x)|$.

4. Ако је G коначна, тада је $|G| = |\mathrm{Stab}(x)| \cdot |G : \mathrm{Stab}(x)|$, па је према 3. $|G| = |\mathrm{Stab}(x)| \cdot |\mathcal{O}(x)|$.

7. Описати орбиту и стабилизатор матрице $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ при дејству коњугацијом у групи $\mathrm{GL}(2, \mathbb{R})$. Колико елемената има орбита матрице A при дејству коњугацијом у $\mathrm{GL}(2, \mathbb{F}_3)$?

Решење. Нека је $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}(\mathbb{R})$, тј. детерминанта $ad - bc \neq 0$. Тада је $X^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ и:

$$X \cdot A = XAX^{-1} = \frac{1}{ad-bc} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} =$$

$$= \frac{1}{ad-bc} \begin{bmatrix} a & 2b \\ c & 2d \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad-bc} \begin{bmatrix} ad-2bc & ab \\ -cd & 2ad-bc \end{bmatrix}.$$

Одредимо $\mathrm{Stab}(A)$. Матрица X је у $\mathrm{Stab}(A)$ ако и само ако $X \cdot A = A$, тј.

$$\frac{1}{ad-bc} \begin{bmatrix} ad-2bc & ab \\ -cd & 2ad-bc \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

Одавде имамо да је $ad - 2bc = ad - bc$, $ab = cd = 0$ и $2ad - bc = 2ad - 2bc$. Прва и трећа једначина се своде на $bc = 0$, па како $ad - bc \neq 0$, то $ad \neq 0$, и $a \neq 0$, $d \neq 0$. Из $ab = cd = 0$ даље следи $b = c = 0$. Дакле,

$$\mathrm{Stab}(A) = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \middle| \, a, d \in \mathbb{R}, \, a \neq 0, \, d \neq 0 \right\}.$$

Орбита је скуп $\mathcal{O}(A) = \{X \cdot A \mid X \in \mathrm{GL}(\mathbb{R})\} = \{XAX^{-1} \mid X \in \mathrm{GL}(\mathbb{R})\}$. Сетимо се из линеарне алгебре да коњуговање чува траг и детерминанту матрице, тј. за свако $X \in \mathrm{GL}(\mathbb{R})$ важи $\mathrm{tr}(XAX^{-1}) = \mathrm{tr}(A) = 3$ и $\det(XAX^{-1}) = \det(A) = 2$. Дакле, $\mathcal{O}(A) \subseteq \{B \mid \mathrm{tr}(B) = 3, \det(B) = 2\}$. Докажимо да у конкретном случају важи и обратно.

Нека је $B = \begin{bmatrix} x & y \\ u & v \end{bmatrix}$, таква да је $\mathrm{tr}(B) = x + v = 3$ и $\det(B) = xv - uy = 2$. Карактеристични полином матрице B је тада $\chi_B(x) = x^2 - \mathrm{tr}(B)x + \det(B) = x^2 - 3x + 2 = (x-1)(x-2)$. Како је карактеристични полином производ линеарних фактора, то је он једнак минималном полиному матрице B, па како је минимални полином производ линеарних фактора, то је матрица B дијагонализабилна, и дијагонална матрица којој је B коњуговна на дијагонали има сопствене вредности 1 и 2, што ће рећи то је баш A. Дакле, постоји матрица $X \in \mathrm{GL}(\mathbb{R})$ таква да је $X^{-1}BX = A$, па је $B = XAX^{-1}$, одакле $B \in \mathcal{O}(A)$.

Дакле, орбита је $\mathcal{O}(A) = \{B \mid \mathrm{tr}(B) = 3, \det(B) = 2\}$. Читалац сам може даље да опише $\mathcal{O}(A)$.

Посматрајмо сада дејство групе $\mathrm{GL}(\mathbb{F}_3)$ на матрицу A. Рачун је потпуно исти, па према томе:

$$\mathrm{Stab}(A) = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \middle| a, d \in \mathbb{F}_3,\, a \neq 0,\, d \neq 0 \right\} \text{ и}$$

$$\mathcal{O}(A) = \{B \in \mathrm{M}_2(\mathbb{F}_3) \mid \mathrm{tr}(B) = 3 = 0,\, \det(B) = 2\}.$$

Нас занима колико је $|\mathcal{O}(A)|$. Број елемената $|\mathcal{O}(A)|$ можемо израчунати на два начина. Први је да елементарно опишемо матрице над $\mathbb{F}_3$ чији је траг једнак 0, а детерминанта једнака 2 (што је лако и остављамо читаоцу).

Други начин је да се сетимо да важи формула $|\mathrm{GL}(\mathbb{F}_3)| = |\mathcal{O}(A)| \cdot |\mathrm{Stab}(A)|$. Очигледно $|\mathrm{Stab}(A)| = 4$. Група $\mathrm{GL}(\mathbb{F}_3)$ има 48 елемената, што није тешко проверити и остављамо читаоцу да то уради. Према томе $|\mathcal{O}(A)| = 12$.

8. Нека је G коначна група и H и K неке њене две *произвољне* подгрупе. Доказати да је онда

$$|HK| \cdot |H \cap K| = |H| \cdot |K|.$$

Решење. Нека је $X = \{Hg \mid g \in G\}$ скуп десних косета подгрупе H. Онда подгрупа K делује на X пресликавањем дефинисаним за $k \in K$ и $g \in G$, са

$$k \cdot (Hg) = Hgk^{-1}.$$

Ово је дејство, јер је $e \cdot (Hg) = Hge^{-1} = Hge = Hg$ и за произвољне $k, k_1 \in K$ имамо $(kk_1) \cdot (Hg) = Hg(kk_1)^{-1} = Hgk_1^{-1}k^{-1} = k \cdot (Hgk_1^{-1}) = k \cdot (k_1 \cdot (Hg))$.

Орбита $\mathcal{O}(H)$ косета $H = He \in X$ при овом дејству је једнака $\{Hk^{-1} \ : \ k \in K\} = \{Hk \ : \ k \in K\}$. Дакле, унија свих елемената који припадају неком косету из орбите $\mathcal{O}(H)$ је тачно скуп HK, а како сваки косет Hk има $|H|$ елемената, закључујемо да је $|HK| = |\mathcal{O}(H)| \cdot |H|$.

Са друге стране, стабилизатор елемента H је $\mathrm{Stab}(H) = \{k \in K \mid k \cdot H = H\}$. Како је $k \cdot H = H \Leftrightarrow Hk^{-1} = H \Leftrightarrow k^{-1} \in HH = H \Leftrightarrow k \in H$, закључујемо да је $\mathrm{Stab}(H) = H \cap K$. Сада на основу Тврђења 3 о орбити и стабилизатору, добијамо да је

$$|\mathcal{O}(H)| = \frac{|K|}{|\mathrm{Stab}(H)|} = \frac{|K|}{|H \cap K|},$$

што заједно са закључком претходног параграфа даје тражену једнакост.

Напомена: Задатак се могао решити и посматрањем дејства подгрупе H на скуп левих косета $Y = \{gK \mid g \in G\}$ подгрупе K. Онда је дејство дефинисано са $h \cdot gK = (hg)K$, за $h \in H$ и $gK \in Y$. Нека читалац провери детаље и размисли зашто су ова дејства дефинисана на различите начине.

Задатак смо могли да решимо и користећи треће дејство. Директни производ $H \times K$ делује на скуп HK на следећи начин: за $x \in HK$ и $(h,k) \in H \times K$, $(h,k) \cdot x = hxk^{-1}$. Доказати да је и ово једно добро дефинисано дејство и да Тврђење о орбити и стабилизатору примењено на тачку $e = ee \in HK$ води до исте формуле.

9. Доказати Тврђење 4.

Решење. Нека је G коначна група и нека $G \circlearrowleft S$. Уочимо скуп $A = \{(g,x) \in G \times S \mid g \cdot x = x\}$. Приметимо да је $\bigcup_{g \in G} \{g\} \times \mathrm{Fix}(g) = A$, као и да је $\bigcup_{x \in S} \mathrm{Stab}(x) \times \{x\} = A$. Одатле је

$$\sum_{g \in G} |\mathrm{Fix}(g)| = |A| = \sum_{x \in S} |\mathrm{Stab}(x)|.$$

Даље је према Тврђењу 3

$$\sum_{x \in S} |\mathrm{Stab}(x)| = \sum_{x \in S} \frac{|G|}{|\mathcal{O}(x)|} = |G| \sum_{x \in S} \frac{1}{|\mathcal{O}(x)|}.$$

Остаје да докажемо да је $\sum_{x \in S} \frac{1}{|\mathcal{O}(x)|} = |S/G|$.

Како орбите чине партицију скупа S, то је

$$\sum_{x \in S} \frac{1}{|\mathcal{O}(x)|} = \sum_{O \in S/G} \sum_{x \in O} \frac{1}{|\mathcal{O}(x)|} = \sum_{O \in S/G} \sum_{x \in O} \frac{1}{|O|} = \sum_{O \in S/G} 1 = |S/G|.$$

10. На колико начина се могу обојити темена правилног p-тоугла (p је прост број) са n боја, ако два бојења сматрамо истим ако ротацијом једног обојеног p-тоугла добијамо други. Доказати Малу Фермаову теорему: $n^p =_p n$, а ако $p \nmid n$ тада $n^{p-1} =_p 1$.

Решење. Означимо темена p-тоугла и уочимо скуп свих бојења $S = \{(a_0, a_1, \ldots, a_{p-1}) \mid 1 \leq a_i \leq n\}$. (Ово значи да је i-то теме обојено бојом a_1.) Уочимо даље дејство групе $\mathbb{Z}/p\mathbb{Z}$ на скуп S, дато на очигледан начин: $k \cdot (a_0, a_1, \ldots, a_{p-1}) = (a_{0+k}, a_{1+k}, \ldots, a_{p-1+k})$, где је сабирање у индексу по модулу p. Дакле, елемент $k \in \mathbb{Z}/p\mathbb{Z}$ ротира p-тоугао за угао $2k\pi/p$. Према томе, два бојења су иста ако и само ако су у истој орбити овог дејства, тј. различитих бојења има колико и орбита овог дејства. Према Бернсајдовој леми је $|S/(\mathbb{Z}/p\mathbb{Z})| = \frac{1}{|\mathbb{Z}/p\mathbb{Z}|} \sum_{k=0}^{p-1} |\mathrm{Fix}(k)|$.

Елемент $0 \in \mathbb{Z}/p\mathbb{Z}$ фиксира свако бојење, па је $\mathrm{Fix}(0) = S$, тј. $|\mathrm{Fix}(0)| = n^p$.

Нека је $1 \le k \le p-1$. Приметите да је тада k генератор групе $\mathbb{Z}/p\mathbb{Z}$, па је $\{0, k, 2k, \ldots, (p-1)k\} = \{0, 1, \ldots, p-1\}$, по модулу p. Елемент $(a_0, \ldots, a_{p-1}) \in \mathrm{Fix}(k)$ ако и само ако $(a_{0+k}, \ldots, a_{p-1+k}) = (a_0, \ldots, a_{p-1})$, одакле је $a_0 = a_{0+k} = a_{0+2k} = a_{0+3k} = \ldots = a_{0+(p-1)k}$, па према претходном запажању важи $a_0 = a_1 = a_2 = \ldots = a_{p-1}$. Дакле, $\mathrm{Fix}(k) = \{(a, a, \ldots, a) \mid 1 \le a \le n\}$, тј. $|\mathrm{Fix}(k)| = n$.

Дакле, $|S/\mathbb{Z}/p\mathbb{Z}| = \dfrac{1}{p}\,(n^p + (p-1)n)$.

Специјално то значи да $p \mid n^p + (p-1)n$. Тада је $n^p = n^p + (p-1)n - (p-1)n =_p n$, или $p \mid n^p - n$. Ако $p \nmid n$, тада из $p \mid n(n^{p-1} - 1)$ следи $p \mid n^{p-1} - 1$, или $n^{p-1} =_p 1$.

11. Нека је G коначна група и нека је p прост број такав да $p \mid |G|$. Уочимо скуп $S = \{(a_0, a_1, \ldots, a_{p-1}) \in G^p \mid a_0 a_1 \ldots a_{p-1} = e\}$. Нека је $k \cdot (a_0, a_1, \ldots, a_{p-1}) = (a_k, a_{1+k}, \ldots, a_{p-1+k})$, за $k \in \mathbb{Z}/p\mathbb{Z}$, где је сабирање у индексима по модулу p. Доказати да је овим дефинисано дејство групе $\mathbb{Z}/p\mathbb{Z}$ на скуп S. Одредити орбите овог дејства.

Доказати Кошијеву лему: у групи G постоји елемент реда p.

Решење. Ако $k \in \mathbb{Z}/p\mathbb{Z}$ и $(a_0, a_1, \ldots, a_{p-1}) \in S$, докажимо најпре да $k \cdot (a_0, a_1, \ldots, a_{p-1}) \in S$. Како $(a_0, a_1, \ldots, a_{p-1}) \in S$, то $a_0 a_1 \ldots a_{k-1} a_k \ldots a_{p-1} = e$, па је $a_k \ldots a_{p-1} = (a_0 a_1 \ldots a_{k-1})^{-1}$, одакле је $a_k \ldots a_{p-1} a_0 a_1 \ldots a_{k-1} = e$, па је $(a_k, a_{1+k}, \ldots, a_{p-1+k}) = k \cdot (a_0, a_1, \ldots, a_{p-1}) \in S$.

Како је очигледно још $0 \cdot (a_0, \ldots, a_{p-1}) = (a_0, \ldots, a_{p-1})$ и $(k + l) \cdot (a_0, \ldots, a_{p-1}) = k \cdot (l \cdot (a_0, \ldots, a_{p-1}))$, то је овим заиста дефинисано дејство групе $\mathbb{Z}/p\mathbb{Z}$ на S.

Одредимо $|S|$. Приметите да из $a_0 a_1 \ldots a_{p-1} = e$ следи $a_0 = (a_1 \ldots a_{p-1})^{-1}$, и такође ако изаберемо произвољно елементе $a_1, \ldots, a_{p-1}$, тада је $((a_1 \ldots a_{p-1})^{-1}, a_1, \ldots, a_{p-1}) \in S$. Према томе $|S| = |G|^{p-1}$.

Опишимо сада орбите. Како ред орбите дели ред групе $\mathbb{Z}/p\mathbb{Z}$, а ред групе је прост број p, то је $|\mathcal{O}(a_0, a_1, \ldots, a_{p-1})| \in \{1, p\}$. Дакле, $|\mathcal{O}(a_0, a_1, \ldots, a_{p-1})| = 1$ ако и само ако $1 \cdot (a_0, a_1, \ldots, a_{p-1}) = (a_0, a_1, \ldots, a_{p-1})$, тј. $(a_1, a_2, \ldots, a_0) = (a_0, a_1, \ldots, a_{p-1})$, одакле је $a_0 = a_1 = a_2 = \ldots = a_{p-1} = a$, тј. $(a_0, a_1, \ldots, a_{p-1}) = (a, a, \ldots, a)$.

Нека је n_1 број једночланих орбита, а n_p број орбита са p елемената. Приметите да је $n_1 \ge 1$, јер $(e, e, \ldots, e) \in S$ има једночлану орбиту. Према класној једнакости важи $|G|^{p-1} = |S| = n_1 + p n_p$. Како $p \mid |G|$, одавде закључујемо да $p \mid n_1$. Дакле, $p \mid n_1$ и $n_1 \ge 1$, па је $n_1 \ge p$. Према томе постоји елемент $a \in G$, $a \ne e$, такав да $(a, a, \ldots, a) \in S$, што значи да је $a^p = e$. Како је $a \ne e$, и како је p прост број, следи да је a реда p.

12. Нека је G коначна p-група. Доказати да је центар $Z(G) \ne \langle e \rangle$.

Решење. Уочимо дејство коњугацијом групе G на себе. Нека $|G| = p^n$.

Докажимо најпре да је $\mathrm{Stab}(x) = C_G(x)$. Елемент $g \in \mathrm{Stab}(x)$ ако и само ако $gxg^{-1} = x$, тј. $gx = xg$, што важи ако и само ако $g \in C_G(x)$.

Приметимо да $|\mathcal{O}(x)| \in \{1, p, p^2, \ldots, p^n\}$, јер ред орбите дели ред групе G. Приметите још да $|\mathcal{O}(x)| = 1$ ако и само ако $|G| = |\mathrm{Stab}(x)|$, тј. $G = \mathrm{Stab}(x)$, што је према претходном еквивалентно са $G = C_G(x)$. Дакле $|\mathcal{O}(x)| = 1$ ако и само ако $x \in Z(G)$.

Нека је T' скуп представника партиције G/G. Тада је $Z(G) \subseteq T'$, па запишимо $T' = Z(G) \sqcup T$. Ако $x \in T$, како $x \notin Z(G)$, тада $p \mid |\mathcal{O}(x)|$. Класна једнакост има облик $p^n = |G| = |Z(G)| + \sum_{x \in T} |\mathcal{O}(x)|$, при чему је сума на десној страни дељива са p.

Према томе, $p \mid |Z(G)|$. Како је још $|Z(G)| \geq 1$, јер $e \in Z(G)$, закључујемо да $|Z(G)| \geq p$. Дакле, $Z(G) \neq \langle e \rangle$.

13. Нека су S и T скупови, $|S| = m$, и $G \circlearrowleft T$. Група G делује на скуп функција $S^T = \{f \mid f : T \longrightarrow S\}$ са: $(g \cdot f)(t) = f(g^{-1} \cdot t)$. Доказати да је овим заиста дефинисано једно дејство $G \circlearrowleft S^T$. Доказати да је $|\mathrm{Fix}_{S^T}(g)| = m^{|T/\langle g \rangle|}$. (Овде је $\mathrm{Fix}_{S^T}(g)$ фиксни скуп при дејству $G \circlearrowleft S^T$, а $|T/\langle g \rangle|$ је број орбита при дејству $\langle g \rangle \circlearrowleft T$, које је рестрикција дејства $G \circlearrowleft T$ на цикличну подгрупу $\langle g \rangle$.)

Решење. Проверимо најпре да јесмо дефинисали дејство $G \circlearrowleft S^T$. Ако $g \in G$, $f \in S^T$, приметите да је тада $g \cdot f = f \circ (g^{-1} \cdot \ )$, па $g \cdot f \in S^T$.

Нека су $f \in S^T$ и $t \in T$ произвољни. Тада је $(e \cdot f)(t) = f(e^{-1} \cdot t) = f(e \cdot t) = f(t)$, па је $e \cdot f = f$. Ако су $g, h \in G$ произвољни, тада $((gh) \cdot f)(t) = f((gh)^{-1} \cdot t) = f((h^{-1}g^{-1}) \cdot t) = f(h^{-1} \cdot (g^{-1} \cdot t)) = (h \cdot f)(g^{-1} \cdot t) = (g \cdot (h \cdot f))(t)$, одакле је $(gh) \cdot f = g \cdot (h \cdot f)$.

Функција $f \in \mathrm{Fix}_{S^T}(g)$ ако и само ако $g \cdot f = f$, тј. ако и само ако за све $t \in T$ важи $(g \cdot f)(t) = f(t)$, тј. $f(g^{-1} \cdot t) = f(t)$. Како је t произвољно то значи $f(t) = f(g^{-1} \cdot t) = f(g^{-2} \cdot t) = f(g^{-3} \cdot t) = \ldots$, тј. f је константна на орбити $\mathcal{O}_{\langle g \rangle}(t)$.

Према томе, $f \in \mathrm{Fix}_{S^T}(g)$ је у потпуности одређена на представницима партиције $T/\langle g \rangle$, а пресликавања из скупа представника партиције $T/\langle g \rangle$ у скуп S има $m^{|T/\langle g \rangle|}$. Дакле, $|\mathrm{Fix}_{S^T}(g)| = m^{|T/\langle g \rangle|}$.

14. Доказати да подгрупа од $\mathbb{S}_n$, $n \geq 3$, генерисана са $n-2$ транспозиције не делује транзитивно на скуп $\{1, 2, \ldots, n\}$.

Решење. Докажимо тврђење индукцијом по n. Ако је $n = 3$ тврђење је очигледно: једна транспозиција, нпр. $(1,2)$, генерише $G = \{(), (1,2)\}$, па $\mathcal{O}(1) = \mathcal{O}(2) = \{1, 2\}$ и $\mathcal{O}(3) = \{3\}$. Дакле, имамо две орбите, па дејство није транзитивно.

Претпоставимо да смо тврђење доказали за $n-1$ и докажимо га за n. Нека је $G = \langle (a_1, b_1), (a_2, b_2), \ldots, (a_{n-2}, b_{n-2}) \rangle$. Претпоставимо супротно, тј. да G делује транзитивно на $\{1, 2, \ldots, n\}$. Уочимо скуп $I = \{a_1, a_2, \ldots, a_{n-2}, b_1, b_2, \ldots, b_{n-2}\}$.

Приметимо најпре да за свако $a \in \{1, 2, \ldots, n\}$ важи $a \in I$. У супротном, a се не појављује у транспозицијама које генеришу G, тј. a је фиксна тачка за групу G. Одатле је $\mathcal{O}(a) = \{a\}$, па имамо бар две орбите, у супротности са претпоставком о транзитивности дејства.

Како $|I| \leq 2n-4$, и како се сваки елемент из $\{1, 2, \ldots, n\}$ појављује бар једном у I, то постоји елемент $a \in \{1, 2, \ldots, n\}$ који се појављује само једном у скупу I. Другим речима постоји тачно једна транспозиција (a, b), за неко b, у генераторном скупу за G, у којој се појављује a. Нека је H група генерисана са преосталих $n-3$ транспозиција.

Тада је a фиксна тачка за H, па је H изоморфна подгрупи од $\mathbb{S}_{n-1}$, генерисаној са $n-3$ транспозиције, одакле по индукцијској хипотези следи да дејство H на $\{1, 2, \ldots, n\} - \{a\}$ није транзитивно. Уочимо орбите овог дејства $\mathcal{O}_H(b)$ и $\mathcal{O}_H(c)$ које су различите.

Како је $G = \langle H, (a, b) \rangle$, како H пермутује $\mathcal{O}_H(c)$, и како (a, b) фиксира све тачке у $\mathcal{O}_H(c)$, закључујемо да G пермутује $\mathcal{O}_H(c)$, тј. $\mathcal{O}(c) = \mathcal{O}_H(c)$. Према томе $a \notin \mathcal{O}(c)$ и очигледно $a \in \mathcal{O}(b)$, па и дејство групе G има бар две орбите, одакле закључујемо да није транзитивно. Контрадикција.

15. Описати сва дејства групе $\mathbb{D}_3$ на четворочлани скуп. Да ли постоји такво дејство које је транзитивно?

Решење. Нека је $\mathbb{D}_3 = \langle \rho, \sigma \mid \rho^3 = \sigma^2 = \varepsilon, \rho\sigma = \sigma\rho^{-1} \rangle$ и нека је $S = \{a, b, c, d\}$. Одмах можемо да дамо одговор на друго питање. Наиме, како ред орбите дели ред групе, то не можемо имати само једну орбиту, тј. транзитивно дејство $\mathbb{D}_3$ на S не постоји.

Проблем описа свих дејстава $\mathbb{D}_3 \circlearrowleft S$ је еквивалентан опису свих хомоморфизама $\phi : \mathbb{D}_3 \longrightarrow \mathrm{Sym}(S)$. Довољно је одредити слике $f(\rho)$ и $f(\sigma)$ тако да $f(\rho)f(\sigma) = f(\sigma)f(\rho)^{-1}$. Како ред $r(f(\rho))$ мора да дели ред $r(\rho) = 3$, то је $f(\rho) = \lfloor \rceil$ или је $f(\rho)$ неки 3–цикл. Такође, како $r(f(\sigma)) \mid r(\sigma) = 2$, то је $f(\sigma) = \lfloor \rceil$ или је $f(\sigma)$ транспозиција или је $f(\sigma)$ дупла транспозиција.

Ако је $f(\rho) = f(\sigma) = \lfloor \rceil$, тада је дато дејство тривијално (сваки елемент групе $\mathbb{D}_3$) фиксира сваки елемент из S.

Нека је $f(\rho) = \lfloor \rceil$ и нека је $f(\sigma)$ транспозиција. Без умањења општости претпоставимо да је $f(\sigma) = \lfloor a, b \rceil$. Тада је очигледно испуњено $(f\rho)f(\sigma) = f(\sigma)f(\rho)^{-1}$, па f индукује хомоморфизам. Одговарајуће дејство има три орбите, једну двочлану $\{a, b\}$ и две једночлане $\{c\}$ и $\{d\}$. У овом дејству ротације тривијално делују на сваки елемент скупа S, док све симетрије пермутују a и b, а фиксирају c и d.

Нека је $f(\rho) = \lfloor\rceil$ и нека је $f(\sigma)$ дупла транспозиција. Без умањења општости претпоставимо да је $f(\sigma) = \lfloor a, b\rceil\lfloor c, d\rceil$. И тада је очигледно испуњено $(f\rho)f(\sigma) = f(\sigma)f(\rho)^{-1}$, па f индукује хомоморфизам. Одговарајуће дејство има две орбите: $\{a, b\}$ и $\{c, d\}$. У овом дејству ротације тривијално делују на сваки елемент скупа S, док све симетрије пермутују a и b, и c и d.

Нека је надаље $f(\rho)$ 3–цикл; без умањења општости претпоставимо да је $f(\rho) = \lfloor a, b, c\rceil$. Из услова $f(\rho)f(\sigma) = f(\sigma)f(\rho)^{-1}$ имамо $f(\rho) = f(\sigma)f(\rho)^{-1}f(\sigma)^{-1}$, тј.

$$\lfloor a, b, c\rceil = f(\sigma)\lfloor a, c, b\rceil f(\sigma)^{-1} = \lfloor f(\sigma)(a), f(\sigma)(c), f(\sigma)(b)\rceil.$$

Одавде закључујемо да је или $f(\sigma) = \lfloor b, c\rceil$ или $f(\sigma) = \lfloor a, c\rceil$ или $f(\sigma) = \lfloor a, b\rceil$. Без умањења општости можемо претпоставити да је $f(\sigma) = \lfloor a, b\rceil$, јер је тада $f(\sigma\rho) = \lfloor b, c\rceil$ и $f(\sigma\rho^2) = \lfloor a, c\rceil$, па променом генераторне симетрије у $\mathbb{D}_3$ добијамо остале случајеве. У овом случају дато дејство има две орбите: $\{a, b, c\}$ и $\{d\}$.

Дакле, имамо четири нееквивалентна начина да дефинишемо дејство $\mathbb{D}_3$ на скуп S. Једно је тривијално, тј. имамо четири једночлане орбите. У другом имамо једну двочлану и две једночлане орбите. У трећем имамо две двочлане орбите. У последњем имамо једну трочлану и једну једночлану орбиту.

1.3 Задаци за самосталан рад

16. Нека је $F[X_1, X_2, \ldots, X_n]$ прстен полинома са n неодређених над неким пољем F. За $\sigma \in \mathbb{S}_n$ и $f \in F[X_1, X_2, \ldots, X_n]$, нека је

$$\sigma \cdot f(X_1, X_2, \ldots, X_n) = f(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}).$$

Доказати да је $\cdot$ једно дејство симетричне групе $\mathbb{S}_n$ на скуп полинома $F[X_1, X_2, \ldots, X_n]$.

У случају $n = 4$, одредити кардиналности орбита и стабилизатора полинома $X_1 + X_2$, $X_1X_2 + X_3X_4$ и $(X_1 + X_2)(X_3 + X_4)$, редом.

17. Нека је $\mathrm{Aff}(\mathbb{R}) = \{f : \mathbb{R} \longrightarrow \mathbb{R} \mid f(x) = ax + b, a, b \in \mathbb{R}, a \neq 0\}$ група (у односу на композицију пресликавања) афиних транформација реалне праве $\mathbb{R}$. Доказати да је за $f \in \mathrm{Aff}(\mathbb{R})$ и $x \in \mathbb{R}$, са $f \cdot x = f(x)$ задато једно дејство и да је то дејство дупло транзитивно.

18. За пермутацију $\sigma \in \mathbb{S}_n$ и вектор $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{R}^n$ дефинишимо

$$\sigma \cdot \mathbf{v} = (v_{\sigma^{-1}(1)}, v_{\sigma^{-1}(2)}, \ldots, v_{\sigma^{-1}(n)}).$$

Доказати да је овим дефинисано једно дејство симетричне групе $\mathbb{S}_n$ на векторски простор $\mathbb{R}^n$.

19. Група $\mathrm{GL}_2(\mathbb{R})$ делује на колона-векторе из $\mathbb{R}^2$ матричним множењем слева. Проверити да је ово једно дејство и одредити орбите и стабилизаторе елемената $\mathbf{v}_0 = (0,0)^t$ и $\mathbf{v}_1 = (1,0)^t$ при овом дејству.

20. Група $\mathrm{GL}_2(\mathbb{Z})$ инвертибилних 2×2 матрица са коефицијентима у прстену $\mathbb{Z}$ делује (матричним множењем слева) на Абелову групу $\mathbb{Z}^2$ чији елементи су представљени векторима-колонама. Одредити орбите овог дејства, за сваку орбиту наћи по једног представника и одредити његов стабилизатор.

21. Доказати да дејство $\mathrm{GL}_2(\mathbb{R}) \circlearrowleft \mathbb{R}^2 \setminus \{(0,0)^t\}$ матричним множењем слева *није* дупло транзитивно.

22. Нека је $G \circlearrowleft X$ неко дејство. Ако са $\Delta = \{(x,x) \mid x \in X\}$ означимо дијагоналу Декартовог квадрата $X \times X$, и приметимо да G делује и на $(X \times X) - \Delta$ са $g \cdot (x_1, x_2) = (g \cdot x_1, g \cdot x_2)$, доказати да је дејство $G \circlearrowleft X$ дупло транзитивно ако и само ако је дејство $G \circlearrowleft (X \times X) - \Delta$ транзитивно.

23. Нека је G коначна група и $H, K < G$. Онда за произвољно $x \in G$ имамо следеће формуле за кардиналност дуплог косета:

$$|HxK| = \frac{|H||K|}{|H \cap xKx^{-1}|} = \frac{|H||K|}{|x^{-1}Hx \cap K|}.$$

24. Доказати да су централизатори елемената у истој класи коњугације међусобно коњуговани. Ако су $n_1, n_2, \ldots, n_r$ кардиналности централизатора представника свих различитих класа коњугације неке коначне групе G, доказати да је

$$\frac{1}{n_1} + \frac{1}{n_2} + \ldots + \frac{1}{n_r} = 1.$$

25. На колико начина се могу обојити темена правилног шестоугла са n боја, ако два бојења сматрамо истим ако:

    (а) ротацијом једног обојеног шестоугла добијамо други;

    (б) изометријом једног обојеног шестоугла добијамо други.

26. Нека је p прост број. На кружници је правилно распоређено p тачака. Колико има полигона чија су темена дате тачке, при чему су два полигона једнака ако се ротацијом једног добија други. Доказати Вилсонову теорему: $(p-1)! =_p -1$.

27. На колико начина можемо обојити стране коцке са n боја, при чему су два бојења једнака ако "окретањем" једне обојене коцке добијамо другу.

28. Доказати $\sum\limits_{\substack{1\le a\le n\\(a,n)=1}} (a-1,n)=\varphi(n)\tau(n)$.

29. Доказати $\sum\limits_{a=0}^{n-1} m^{(a,n)} =_n 0$.

30. Нека је G коначна група која транзитивно делује на коначан скуп S, $|S|>1$. Доказати да постоји елемент $g\in G$ такав да $\mathrm{Fix}(g)=\emptyset$.

31. Нека је G коначна група и H права подгрупа. Доказати да је $\bigcup\limits_{g\in G} gHg^{-1} \subsetneq G$.

32. **($n!$ – теорема)** Нека је $H\le G$, коначног индекса $|G:H|=n$. Доказати да $|G:\mathrm{Core}(H)| \mid n!$.

33. Нека је G група која садржи подгрупу коначног индекса у G. Доказати да G садржи нормалну подгрупу коначног индекса.

34. Нека је p прост, нека $G\le \mathbb{S}_p$ делује транзитивно на $\{1,2,\ldots,p\}$ и нека је $\langle()\rangle \ne H \lhd G$. Доказати да и H делује транзитивно на $\{1,2,\ldots,p\}$.

35. Нека је G коначна p-група која делује на коначан скуп S, $|S|=n$, $p\nmid n$. Доказати да постоји $x\in S$ тако да за све $g\in G$ важи $g\cdot x=x$.

36. Доказати да је дејство алтернирајуће групе $\mathbb{A}_n \circlearrowleft \{1,2,\ldots,n\}$ транзитивно ако је $n\ge 3$. Доказати да је ово дејство и дупло транзитивно ако је $n\ge 4$. Зашто $\mathbb{A}_3$ не делује дупло транзитивно на $\{1,2,3\}$?

37. Нека је $O(2)$ ортогонална група коју чине реалне 2×2 матрице A такве да је $A\cdot A^t = A^t\cdot A = \begin{bmatrix} 1 & 0\\ 0 & 1\end{bmatrix}$. Група $O(2)$ делује на колона-векторе из $\mathbb{R}^2\setminus\{(0,0)^t\}$ матричним множењем. Да ли је ово дејство транзитивно?

38. Нека коначна група G делује транзитивно на неки скуп X и нека је $N\lhd G$. Онда за рестрикцију дејства на $N\circlearrowleft X$ важи да све орбите од N на X имају исту кардиналност.

39. Нека група G делује дупло транзитивно на неки скуп X и нека је $N\lhd G$. Онда је дејство $N\circlearrowleft X$ или тривијално или транзитивно.

40. Нека је $G\circlearrowleft X$ транзитивно дејство групе G на скуп X и нека је $x\in X$ произвољно. Онда група G дејствује (множењем слева) и на скуп левих косета $G/\mathrm{Stab}(x)$ стабилизатора $\mathrm{Stab}(x)$ елемента x. Доказати да су X и $G/\mathrm{Stab}(x)$ изоморфни G-скупови.

41. Нека $G \circlearrowleft X$ и $G \circlearrowleft Y$ и нека је $\phi : X \longrightarrow Y$ хомоморфизам G-скупова. Ако је $x \in X$, онда је $\mathrm{Stab}(x) \leq \mathrm{Stab}(\phi(x))$. Ако је ϕ и изоморфизам G-скупова, онда је $\mathrm{Stab}(x) = \mathrm{Stab}(\phi(x))$.

42. Нека су H и K подгрупе групе G. Група G делује левим множењем на скупове левих косета G/H и G/K. Доказати да су G-скупови G/H и G/K изоморфни (тј. постоји изоморфизам G-скупова између њих) ако и само ако су подгрупе H и K коњуговане у G.

43. За сваку групу G имамо природно дејство $\mathrm{Aut}(G) \circlearrowleft G$ њене групе аутоморфизама на њу саму: за $f \in \mathrm{Aut}(G)$ и $g \in G$, $f \cdot g = f(g)$. Нека је G коначна група са бар 2 елемента. Доказати да ако $\mathrm{Aut}(G)$ делује транзитивно на $G \backslash \{e\}$, онда мора бити $G \cong (\mathbb{Z}/p\mathbb{Z})^n$, за неки прост број p.

44. Нека је G коначна група са бар 2 елемента, таква да $\mathrm{Aut}(G)$ делује дупло транзитивно на $G \setminus \{e\}$. Доказати да је онда $G \cong (\mathbb{Z}/2\mathbb{Z})^n$, за неко $n \in \mathbb{N}$, или $G \cong \mathbb{Z}/3\mathbb{Z}$.

45. Нека је $G \circlearrowleft X$ дупло транзитивно дејство и нека је $x \in X$, произвољно. Доказати да је $\mathrm{Stab}(x)$ максимална подгрупа од G (тј. да не постоји нека права подгрупа $K < G$ за коју је $\mathrm{Stab}(x) \subsetneq K$).

46. Дато је дејство $G \circlearrowleft X$, при чему је $|X| \geq 3$. Доказати да је дејство дупло транзитивно ако и само ако група $\mathrm{Stab}(x)$ делује транзитивно на скуп $X - \{x\}$, за свако $x \in X$.

1.4 Упутства

16. Лако налазимо да је $\mathrm{Stab}(X_1 + X_2) = \{(), (1,2), (3,4), (1,2)(3,4)\}$, па је према Тврђењу о орбити и стабилизатору $|\mathcal{O}(X_1 + X_2)| = |\mathbb{S}_4|/4 = 6$. Експлицитно, $\mathcal{O}(X_1 + X_2) = \{X_i + X_j \mid 1 \leq i,j \leq 4, i \neq j\}$. Слично се раде и остали случајеви.

17. За парове (x_1, x_2) и (y_1, y_2) у $\mathbb{R}^2$, за које је $x_1 \neq x_2, y_1 \neq y_2$, решите систем једначина $ax_1 + b = y_1$, $ax_2 + b = y_2$, по a и b.

18. За проверу $\sigma \cdot (\tau \cdot \mathbf{v}) = (\sigma\tau) \cdot \mathbf{v}$, искористимо да је $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$. Означимо $\tau \cdot \mathbf{v} = (u_1, u_2, ..., u_n)$, тј. нека је $u_i = v_{\tau^{-1}(i)}$. Онда је $\sigma \cdot (\tau \cdot \mathbf{v}) = \sigma \cdot (u_1, u_2, ..., u_n) = (u_{\sigma^{-1}(1)}, u_{\sigma^{-1}(2)}, ..., u_{\sigma^{-1}(n)}) = (v_{\tau^{-1}(\sigma^{-1}(1))}, v_{\tau^{-1}(\sigma^{-1}(2))}, ..., v_{\tau^{-1}(\sigma^{-1}(n))}) = (v_{(\sigma\tau)^{-1}(1)}, v_{(\sigma\tau)^{-1}(2)}, ..., v_{(\sigma\tau)^{-1}(n)})$.

19. Ако је $(a,b)^t \neq (0,0)^t$, онда је

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a & 1 \\ b & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{и} \quad \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a & 0 \\ b & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix},$$

одакле закључујемо да је $\mathcal{O}(\mathbf{v}_0) = \{\mathbf{v}_0\}$ и $\mathcal{O}(\mathbf{v}_1) = \mathbb{R}^2 \backslash \{\mathbf{v}_0\}$, тј. ово дејство има тачно две орбите; $\mathrm{Stab}(\mathbf{v}_0) = \mathrm{GL}_2(\mathbb{R})$, $\mathrm{Stab}(\mathbf{v}_1) = \{\begin{bmatrix} 1 & x \\ 0 & y \end{bmatrix} : y \neq 0\}$.

20. Ово дејство ће имати бесконачно много орбита. Означимо $X_0 = \{(0,0)^t\}$ и за све $d \in \mathbb{Z}_{\geq 1}$, нека је $X_d = \{(a,b)^t \in \mathbb{Z}^2 \mid \text{НЗД}(a,b) = d\}$. Ако означимо за $d \in \mathbb{Z}_{\geq 0}$, елемент $\mathbf{v}_d = (d,0)^t$, онда је $\mathcal{O}(\mathbf{v}_d) = X_d$. За доказ овога искористити да ако су $a, b \in \mathbb{Z}$ узајамно прости, постоје неки цели бројеви x, y такви да је $ax + by = 1$. Али онда је $\begin{bmatrix} a & -y \\ b & x \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. У општем случају, ако је НЗД$(a,b) = d$, применити исти аргумент за целе бројеве a/d, b/d који су узајамно прости. Стабилизатори су $\mathrm{Stab}(\mathbf{v}_0) = \mathrm{GL}_2(\mathbb{Z})$ и за $d > 0$, $\mathrm{Stab}(\mathbf{v}_d) = \{\begin{bmatrix} 1 & x \\ 0 & y \end{bmatrix} \mid x \in \mathbb{Z}, y = \pm 1\}$.

21. Нека су v_1, v_2, v_3 три различита ненула вектора у $\mathbb{R}^2$, при чему су вектори v_2 и v_3 линеарно независни. Да ли овим дејством можемо да пошаљемо пар $(v_1, -v_1)$ у пар (v_2, v_3)?

22. По дефиницији.

23. Посматрајмо дејство (множењем слева) подгрупе H на скуп левих косета G/K подгрупе K. Стабилизатор косета xK при овом дејству је $H \cap xKx^{-1}$, а дупли косет HxK је унија косета који леже у орбити косета xK. Применити Тврђење о орбити и стабилизатору.

24. Применити класну једнакост.

25. У првом случају посматрати дејство групе $\mathbb{Z}/6\mathbb{Z}$, а у другом случају дејство $\mathbb{D}_6$ на скуп S свих обојених шестоуглова, па применити Бернсајдову лему. Решења: $|S/\mathbb{Z}/6\mathbb{Z}| = \frac{1}{6}(n^6 + n^3 + 2n^2 + 2n)$ и $|S/\mathbb{D}_6| = \frac{1}{12}(n^6 + 3n^4 + 4n^3 + 2n^2 + 2n)$.

26. Уочити дејство групе $\mathbb{Z}/p\mathbb{Z}$ на скуп S свих полигона. (Ово дејство ротира темена једног полигона у други.) Доказати да $|S| = (p-1)!/2$. Доказати да $k \neq 0$ фиксира $(p-1)/2$ полигон, па применити Бернсајдову лему.

27. Одредити групу G ротација коцке, па применити Бернсајдову лему. $|G| = 24$ и може се доказати да је $G \cong \mathbb{S}_4$.

28. Посматрајте дејство групе $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ на $\mathbb{Z}/n\mathbb{Z}$. Израчунајте број орбита овог дејства и $|\mathrm{Fix}(g)|$, за $g \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, па приметите да тврђење Бернсајдове леме даје тражену једнакост.

29. Посматрајте дејство $\mathbb{Z}/n\mathbb{Z} \circlearrowleft \mathbb{Z}/n\mathbb{Z}$ дато са $a \cdot b = a + b$. Посматрајте одговарајуће дејство $\mathbb{Z}/n\mathbb{Z} \circlearrowleft S^{\mathbb{Z}/n\mathbb{Z}}$, где је S m–точлани скуп. Даље искористите задатак 13. и Бернсајдову лему.

30. Запишите Бернсајдову лему за транзитивно дејство. Како је $|\mathrm{Fix}(e)| \geq 2$, закључите да постоји $g \in G$ тако да $\mathrm{Fix}(g) = \emptyset$.

31. Приметите да је дејство левим множењем групе G на леве косете подгрупе H увек транзитивно. Докажите да $gH \in \mathrm{Fix}(a)$ ако и само ако $a \in gHg^{-1}$. Сада примените претходни задатак.

32. Посматрати дејство левим множењем групе G на скуп левих косета подгрупе H. Уочите хомоморфизам $\phi : G \longrightarrow \mathrm{Sym}(G/H) \cong \mathbb{S}_n$, који одговара том дејству. Докажите да је $\ker(\phi) = \mathrm{Core}(H)$, па примените прву теорему о изоморфизму.

33. Ако је H коначног индекса, искористите $n!$ – теорему да докажете да је $\mathrm{Core}(H)$ тражена подгрупа.

34. Нека су $a, b \in \{1, 2, \ldots, p\}$ произвољни и нека је $g \in G$такво да $g \cdot a = b$. Докажите да $g^{-1} \cdot \mathcal{O}_H(b) \subseteq \mathcal{O}_H(a)$. Докажите да $|\mathcal{O}_H(a)| = |\mathcal{O}_H(b)|$, па из класне једнакости закључите да постоји само једна орбита.

35. Примените класну једнакост на задату ситуацију, и докажите да мора постојати једночлана орбита.

36. За доказ транзитивности, уочите циклове $(1, 2, n), (1, 3, n), \ldots, (1, n-1, n), (1, n, 2)$ који сви припадају групи $\mathbb{A}_n$. За доказ дупле транзитивности, приметите да пар елемента i, k можемо послати у пар j, l пермутацијом $(i, j)(k, l) \in \mathbb{A}_n$. Нађите 3-цикл који ће пар i, k сликати у пар i, l.

37. Није. Докажите да је сваки круг са центром у $(0, 0)$ једна орбита, па је ово пример дејства са бесконачно много орбита.

38. Ако су x, y две тачке у X, треба показати да је $|N \cdot x| = |N \cdot y|$. За то је довољно показати да су орбите $N \cdot x$ и $N \cdot y$ у бијекцији; али због транзитивности, $y = g \cdot x$, за неко $g \in G$, па је $N \cdot y = N \cdot g \cdot x = g \cdot N \cdot x$.

39. Ако N не делује тривијално на X, постоји неко $n \in N, n \neq e$ и неко $x \in X$ такви да је $n \cdot x \neq x$. Сада за произвољна два различита елемента $x_1, x_2 \in X$ примените дуплу транзитивност за пар $(x, n \cdot x)$ и пар (x_1, x_2) и нормалност подгрупе N да бисте показали да су x_1 и x_2 у истој N-орбити.

40. Дефинишимо пресликавање $\phi : G/\mathrm{Stab}(x) \longrightarrow X$ са $\phi(g\ \mathrm{Stab}(x)) = gx$. Доказати да је ово пресликавање добро дефинисано (да не зависи од избора представника косета), да је хомоморфизам G-скупова, да је инјективно и да је сурјективно (за шта искористимо услов да је дејство $G \circlearrowleft X$ транзитивно).

41. Први део се проверава директно по дефиницији. За други део, приметити да ако је ϕ бијективни хомоморфизам G-скупова, онда је инверзно пресликавање $\phi^{-1} : Y \longrightarrow X$ такође хомоморфизам G-скупова, па применити први део и за ϕ^{-1}.

42. За свако дејство $G \circlearrowleft X$ и свако $g \in G$ и $x \in X$ важи $\mathrm{Stab}(g \cdot x) = g\mathrm{Stab}(x)g^{-1}$. Како је дејство $G \circlearrowleft G/H$ транзитивно, скуп свих стабилизатора тачака из G/H се поклапа са скупом свих коњугата подгрупе H. Слично и скуп свих стабилизатора дејства $G \circlearrowleft G/K$ се поклапа са свим коњугатима подгрупе K. Сада, ако су G/H и G/K изоморфни G-скупови, њихови скупови стабилизатора се морају поклапати према претходном задатку. У обрнутом смеру искористити ♣♣ задатак.

43. За сваки аутоморфизам $f \in \mathrm{Aut}(G)$, елементи g и $f(g)$ су истог реда у групи G. Нека је p неки прост делитељ од $|G|$; применом Кошијеве леме налазимо неки елемент у G реда p; због транзитивности дејства, сви елементи $\neq e$ су истог реда p. Искористити да G има нетривијалан центар да би се закључило да G мора бити Абелова. Видети G као $\mathbb{Z}/p\mathbb{Z}$-векторски простор.

44. Према претходном задатку, знамо да мора бити $G \cong (\mathbb{Z}/p\mathbb{Z})^n$, за неки прост p, при чему $(\mathbb{Z}/p\mathbb{Z})^n$ можемо видети и као $\mathbb{Z}/p\mathbb{Z}$-векторски простор. Ако би било $p > 2$ и $n \geq 2$, онда за било која два линеарно независна вектора $v, w \in (\mathbb{Z}/p\mathbb{Z})^n$ не бисмо могли да нађемо аутоморфизам $A \in \mathrm{Aut}(G) \cong \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ (овај изоморфизам следи из Линеарне алгебре) који пар вектора $(v, -v)$ пресликава у пар (v, w). (Зашто ово неће бити контрапример ако је $p = 2$?). Ако је $n = 1$, искористити да сваки аутоморфизам групе $\mathbb{Z}/p\mathbb{Z}$ који фиксира неки ненула елемент фиксира и све остале, да би се закључило да у овом случају мора бити $p \leq 3$.

45. Најпре, како је дејство и транзитивно, G-скупови X и $G/\mathrm{Stab}(x)$ су изоморфни, па је специјално и дејство $G \circlearrowleft G/\mathrm{Stab}(x)$ дупло транзитивно. Претпоставимо да $\mathrm{Stab}(x)$ није максимална подгрупа, тј. да постоји нека подгрупа K таква да је $\mathrm{Stab}(x) < K < G$, где $<$ значи "права подгрупа". Онда изаберимо неко $g \in G - K$ и неко $k \in K - \mathrm{Stab}(x)$. Због дупле транзитивности, постоји неко $h \in G$ такво да је $h \cdot \mathrm{Stab}(x) = \mathrm{Stab}(x)$ и $h \cdot (k\mathrm{Stab}(x)) = g\mathrm{Stab}(x)$. Одавде извести контрадикцију.

46. Смер ($\Rightarrow$) следи директно по дефиницији. Смер ($\Leftarrow$): пар (x_1, x_2) можемо пресликати у пар (y_1, y_2), где су $x_1 \neq x_2$ и $y_1 \neq y_2$ нпр. користећи одговарајуће елементе из $\mathrm{Stab}(x_1)$ и $\mathrm{Stab}(y_2)$ на следећи начин: $(x_1, x_2) \mapsto (x_1, y_2) \mapsto (y_1, y_2)$. Ово "не ради" само ако је $x_1 = y_2$, али у том случају изаберите неко $z \neq x_1, y_1$ (зато нам је требао услов $|X| \geq 3$) и пређите из првог у други пар у 3 корака.