Садржај

Предговор

Овај уџбеник базиран је на предавањима и вежбама које су аутори више година држали из предмета Алгебра, и касније Алгебра 1, у четвртом семестру студија смера Информатика на Математичком факултету. Основне алгебарске структуре које се овде обрађују, деценијама се на Математичком факултету изучавају на целогодишњем курсу у оквиру смера Математика, а последњих десетак година у два једносеместрална курса. Имајући то у виду, а и посебне потребе студената Информатике, нешто од важног материјала је морало да буде изостављено, али се ипак водило рачуна о томе да се најосновнији резултати и конструкције ипак обраде.

Главни део текста књиге подељен је у пет поглавља. Прво поглавље је посвећено основама теорије група. Ту су обрађене све основне теореме, али неки од напреднијих садржаја попут Силовљевих теорема, дубљег испитивања група малог реда, решивих група, је ипак морало бити изостављено. У другом поглављу, које је посвећено коначно генерисаним Абеловим групама, материјал је стандардно обрађен, осим што је изостављен доказ јединствености нормалне форме, али је детаљно обрађен метод како се до ове форме долази. Треће поглавље је посвећено основама теорије комутативних прстена са јединицом, али се није улазило дубље у теорију идеала. Користећи идеале у прстену $\mathbb{Z}$ доказана је Кинеска теорема о остацима, а на самом крају је дискутована и мултипликативна група коначног поља са посебним нагласком на примену у елементарној теорији бројева. Четврто поглавље је посвећено проширењима поља. Овде је дата стандардна Кронекерова конструкција, илустрована на основним примерима, а приказана је и конструкција коначних поља што је посебно важно за студенте смера Информатика. Како се у оквиру књиге појављује и немали број задатака, пето поглавље је посвећено детаљном решењу свих задатака.

После решења задатака дата су и четири (кратка) додатка. Први представља прецизну конструкцију прстена полинома, еуклидског дељења, као и Еуклидовог алгоритма за прстен полинома над пољем, са којим се студенти срећу и раније, али ипак без праве математичке конструкције. Остала три додатка се тичу неких додатних питања и намењена су, пре свега, знатижељнијим студентима.

Препорука је аутора ове књиге читаоцима да пажљиво прођу кроз текст пре него што се позабаве задацима и да свакако најпре покушају да задатке реше сами, а не да одмах гледају решења. То је добро проверен начин да од материјала којим располажете стекнете највише користи. Алгебра је специфична по томе што се задаци не разликују битно од теорије, па вам добро разумевање теорије омогућује да и задатке успешно урадите уз мало труда.

За крај, аутори желе да изразе захвалност рецензентима др Зорану Пуцановићу, ванредном професору Грађевинског факултета у Београду и др Тањи Стојадиновић, доценту Математичког факултета у Београду, на низу веома корисних сугестија које су дали и захваљујући чијем залагању у овој књизи има значајно мање штампарских, па и других грешака него што би иначе било. А свакако, за све преостале грешке, одговорност преузимају аутори на себе.

У Београду, септембра 2021. Аутори

За елемент axa^{-1} кажемо да је конјугован елементу x. Са овим појмом касније ћемо се често сретати.

Степен елемента x^m може се дефинисати и за негативне m:

$$x^{-n} := (x^{-1})^n, \text{ за } n \geqslant 1.$$

Наравно, ако је $n = 0$ узимамо $x^0 = e$. Може се доказати да овако дефинисана степена функција (у групи) има следеће особине (погледати задатак 1.7).

Став 1.4 Нека је G група, $x \in G$ и $m, n \in \mathbb{Z}$. Тада важи:

$$1)\ x^{-n} = (x^n)^{-1}; \qquad 2)\ x^m x^n = x^{m+n}; \qquad 3)\ (x^m)^n = x^{mn}.$$

Коначна група G може се задати њеном таблицом множења, тзв. Кејлијевом таблицом. Ову таблицу задајемо тако што врсте и колоне означимо елементима групе, а затим у пресеку врсте означене са a и колоне означене са b записујемо елемент ab. У наставку овог поглавља даћемо Кејлијеве таблице за неколико група.

Напомена. Кејлијеву таблицу заправо можемо формирати за сваку бинарну операцију задату на неком коначном скупу (што ћемо и чинити у неколико задатака).

Пређимо сада на примере група.

Групе формиране од бројева

Први и најједноставнији примери група су групе које формирају бројеви. То су групе $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, а такође и $(\mathbb{Q}\setminus\{0\}, \cdot)$, $(\mathbb{Q}^+, \cdot)$, $(\mathbb{R}\setminus\{0\}, \cdot)$, $(\mathbb{R}^+, \cdot)$, као и $(\mathbb{C}\setminus\{0\}, \cdot)$. Наравно, овде су $+$ и $\cdot$ уобичајене операције сабирања и множења бројева, док су са $\mathbb{Q}^+$ (односно $\mathbb{R}^+$) означени сви позитивни рационални (односно реални) бројеви.

Нешто сложенији је следећи пример. Нека је $n \geqslant 2$ природан број. Посматрајмо скуп свих n-тих корена из јединице:

$$\mathbb{C}_n = \{z \in \mathbb{C} : z^n = 1\}.$$

Подсетимо се кратко тригонометријског облика комплексних бројева. Уколико $z = a + bi \in \mathbb{C}\setminus\{0\}$, $a, b \in \mathbb{R}$, онда се он може написати у облику

$$z = |z|(\cos\theta + i\sin\theta),$$

при чему је $|z| = \sqrt{a^2 + b^2}$ модул комплексног броја, док је θ његов аргумент и он је јединствено одређен захтевом да $\theta \in [0, 2\pi)$. Уколико је и $w \in \mathbb{C}\setminus\{0\}$, њега можемо такође записати у тригонометријском облику:

$$w = |w|(\cos\phi + i\sin\phi),$$

где $\phi \in [0, 2\pi)$. Тада је

$$\begin{aligned} z \cdot w &= |z||w|(\cos\theta + i\sin\theta)(\cos\phi + i\sin\phi) \\ &= |z||w|((\cos\theta\cos\phi - \sin\theta\sin\phi) + i(\sin\theta\cos\phi + \cos\theta\sin\phi)) \\ &= |z||w|(\cos(\theta+\phi) + i\sin(\theta+\phi)). \end{aligned}$$

Наравно, може се десити да је $\theta+\phi \geqslant 2\pi$, то је сасвим у реду, формула је тачна. Такође (присетимо се Муаврове формуле[2]):

$$z^n = |z|^n(\cos\theta + i\sin\theta)^n = |z|^n(\cos n\theta + i\sin n\theta).$$

Уколико је $|z| = 1$, онда је $z = \cos\theta + i\sin\theta$, за неко θ. Посебно, сваки елемент из $\mathbb{C}_n$ је овог облика (пошто је $z^n = 1$, то је и $|z|^n = 1$, те је $|z| = 1$). Покажимо да је $(\mathbb{C}_n, \cdot)$ једна комутативна група (дакле група у којој елементи комутирају). Знамо да је операција множења комплексних бројева и асоцијативна и комутативна. Такође, како је $1^n = 1$, $1 \in \mathbb{C}_n$. Остаје само да се провери да сваки елемент из $\mathbb{C}_n$ има инверз који такође припада $\mathbb{C}_n$. Но, ако је $z = \cos\theta + i\sin\theta \in \mathbb{C}_n$, онда је $z^n = \cos n\theta + i\sin n\theta = 1$. Следи $1 = z^n = z^{n-1}z = zz^{n-1}$, па је $z^{-1} = z^{n-1} = \cos(n-1)\theta + i\sin(n-1)\theta = 1$. Уз то, $(z^{n-1})^n = (z^n)^{n-1} = 1$, па је $z^{-1} = z^{n-1} \in \mathbb{C}_n$, што је и требало доказати. Коначно, можемо се запитати чему је једнак аргумент инверза z^{-1}. Ако је $\theta = 0$, тј. $z = 1$, тада је $z^{-1} = 1$, тј. аргумент броја z^{-1} је такође 0. Нека је даље $\theta > 0$. Како важи

$$(\cos\theta + i\sin\theta)(\cos(2\pi-\theta) + i\sin(2\pi-\theta)) = \cos(2\pi) + i\sin(2\pi) = 1,$$

из јединствености инверза следи да је $z^{-1} = \cos(2\pi-\theta) + i\sin(2\pi-\theta)$, па је аргумент броја z^{-1} једнак $2\pi - \theta$ (јер је $2\pi - \theta \in (0, 2\pi)$).

Коначно, размотримо случај $n = 4$. Није тешко утврдити да је $\mathbb{C}_4 = \{1, -1, i, -i\}$, а ову групу можемо представити њеном Кејлијевом таблицом.

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Групе формиране од бијекција

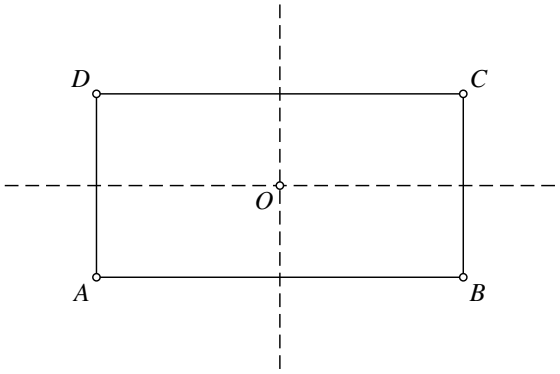
Наравно да појам групе није уведен због група које чине бројеви.

Размотримо следећи пример. Посматра се непразан скуп X и све бијекције скупа X у самог себе. Скуп свих тих бијекција, уз операцију

[2]Ова формула се може доказати применом математичке индукције и претходне формуле за множење комплексних бројева.

композиције пресликавања, чини групу ПЕРМУТАЦИЈА скупа X. Овој групи ће бити посвећен посебан одељак, а ми ћемо се овде позабавити неким једноставним примерима група које чине симетрије неких геометријских објеката.

Посматрајмо неки правоугаоник, који није квадрат.



Слика 1. Осне рефлексије правоугаоника.

Сем идентичне трансформације, овај правоугаоник има још само три симетрије: две осне рефлексије (у односу на осе које су симетрале наспрамних страница) и једну централну рефлексију (у односу на центар правоугаоника, тј. тачку O). Јасно је да композиција те две осне рефлексије даје централну рефлекцију. Означимо ову групу и њене елементе са

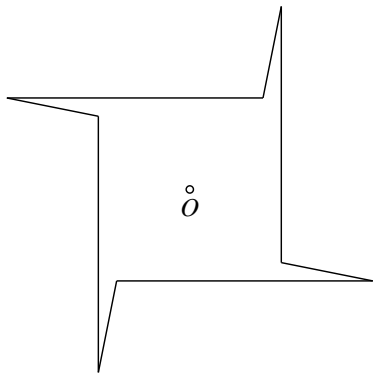
$$V = \{\varepsilon, \sigma_1, \sigma_2, \rho\},$$

где је са ε означена идентичка трансформација равни, σ_1 и σ_2 су осне рефлексије, а ρ централна рефлексија. Није тешко саставити таблицу множења у овој групи.

$\circ$	ε	σ_1	σ_2	ρ
ε	ε	σ_1	σ_2	ρ
σ_1	σ_1	ε	ρ	σ_2
σ_2	σ_2	ρ	ε	σ_1
ρ	ρ	σ_2	σ_1	ε

Приметимо да за сваки елемент x ове групе важи: $x^2 = \varepsilon$ и да је група комутативна. Касније ћемо видети да из прве чињенице следи и друга. Група V зове се и Клајнова група, а V долази од првог слова у немачкој речи „Vier”, што значи „четири”.

Посматрајмо следећи квадрат ’са прилозима’.



Слика 2. Квадрат 'са прилозима'.

Квадрат је веома симетрична фигура, има више оса симетрије, но због додатних дужи, добијена фигура има само ротације око центра O за симетрије. Ради се наравно о ротацијама (у смеру супротном од кретања казаљке на часовнику) за 90°, 180°, 270°, као и о ротацији за 0°, која је заправо идентичка трансформација (њу увек морамо да имамо ако желимо да добијемо групу). Ако са ρ означимо ту ротацију за 90°, онда је јасно да је одговарајућа ротација за 180° заправо $\rho \circ \rho = \rho^2$, ротација за 270° је ρ^3, док је ρ^4 ротација за 360°, што је наравно идентичка трансформација коју ћемо, као и горе, означити са ε.

Сада можемо формирати и таблицу за ову групу.

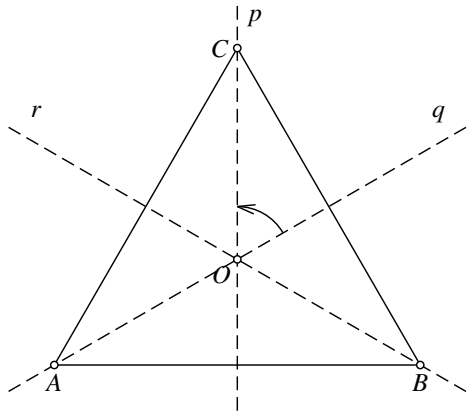
$\circ$	ε	ρ	ρ^2	ρ^3
ε	ε	ρ	ρ^2	ρ^3
ρ	ρ	ρ^2	ρ^3	ε
ρ^2	ρ^2	ρ^3	ε	ρ
ρ^3	ρ^3	ε	ρ	ρ^2

Зашто је, на пример, $\rho^3 \circ \rho^2 = \rho$? Имамо да је

$$\rho^3 \circ \rho^2 = \rho^5 = \rho^4 \circ \rho = \varepsilon \circ \rho = \rho.$$

Јасно је да правоугаоник и овај квадрат са додацима нису подударне фигуре (нису ни сличне), но оне ипак имају исти број симетрија. Али, комплетну информацију о „симетричности" неког објекта не можемо добити само из броја његових симетрија, јер је битно и како се оне компонују, тј. битна је сама ГРУПА симетрија. А видимо да се ове групе ипак суштински разликују. У случају Клајнове групе, квадрат сваког елемента једнак је неутралу, док у другом случају имамо елемент чији квадрат није једнак неутралу, заправо сваки елемент те групе је степен елемента ρ. Групе за које је то случај називају се цикличне групе и њима ћемо се ускоро више позабавити.

За крај одељка проверимо која је група симетрија једнакостраничног троугла.



Слика 3. Осне рефлексије једнакостраничног троугла.

Троугао има три осе симетрије: p, q, r и стога имамо три одговарајуће осне рефлексије σ_p, σ_q, σ_r. Осим ових, троугао има и три ротационе симетрије: ротације око центра O у смеру супротном кретању казаљке на часовнику за углове $0°$, $120°$ и $240°$. Наравно ротација за угао од $0°$ је идентичка трансформација ε. Ако са ρ означимо наведену ротацију за $120°$, онда је јасно да је трећа ротација заправо ρ^2. Да би се формирала таблица множења (тј. Кејлијева таблица), корисно је знати везу између ротација и осних рефлексија. Наиме, трансформација која се добија као композиција две осне рефлексије у односу на праве које се секу је заправо ротација за двоструки (оријентисани) угао који те праве заклапају (погледати слику 3). Смер ротације наравно зависи од поретка компоновања рефлексија. Стога имамо $\rho = \sigma_q \circ \sigma_r = \sigma_r \circ \sigma_p = \sigma_p \circ \sigma_q$, док је $\rho^2 = \rho^{-1} = \sigma_r \circ \sigma_q = \sigma_p \circ \sigma_r = \sigma_q \circ \sigma_p$. У то се можемо уверити и директном провером на теменима:

$$A \overset{\sigma_r}{\longmapsto} C \overset{\sigma_q}{\longmapsto} B, \quad B \overset{\sigma_r}{\longmapsto} B \overset{\sigma_q}{\longmapsto} C, \quad C \overset{\sigma_r}{\longmapsto} A \overset{\sigma_q}{\longmapsto} A,$$

$$A \overset{\rho}{\longmapsto} B \overset{\rho}{\longmapsto} C \overset{\rho}{\longmapsto} A.$$

Напишимо сада таблицу множења у овој групи.

$\circ$	ε	ρ	ρ^2	σ_p	σ_q	σ_r
ε	ε	ρ	ρ^2	σ_p	σ_q	σ_r
ρ	ρ	ρ^2	ε	σ_r	σ_p	σ_q
ρ^2	ρ^2	ε	ρ	σ_q	σ_r	σ_p
σ_p	σ_p	σ_q	σ_r	ε	ρ	ρ^2
σ_q	σ_q	σ_r	σ_p	ρ^2	ε	ρ
σ_r	σ_r	σ_p	σ_q	ρ	ρ^2	ε

Видимо да ова група није комутативна (јер њена Кејлијева таблица није симетрична у односу на главну дијагоналу), да у њој имамо три елемента, сем неутрала, чији је квадрат једнак неутралу, а и два елемента чији је трећи степен једнак неутралу. Не постоји елемент тако да је сваки елемент неки степен тог изабраног елемента – ова група није циклична.

Група симетрија једнакостраничног троугла је специјалан случај из низа група, које се називају ДИЕДАРСКЕ групе и које представљају групе симетрија правилних n-тоуглова. Ова група се означава са $\mathbb{D}_3$, јер је једнакостранични троугао заправо правилни n-тоугао, за $n = 3$. Овим важним групама ћемо се више позабавити у посебном одељку.

Задаци

1.7 Доказати став 1.4.

1.8 Нека је $A = \{(a, b) : a, b \in \mathbb{Q},\, a \neq 0\}$. Доказати да је $(A, \circ)$ група, при чему је $\circ$ задато са $(a, b) \circ (c, d) = (ac, bc + d)$.

1.9 Доказати да скуп

$$M = \left\{ \begin{bmatrix} x & y \\ 0 & 1/x \end{bmatrix} : x \in \mathbb{R} \setminus \{0\},\, y \in \mathbb{R} \right\}$$

чини (некомутативну) групу у односу на множење матрица.

1.10 Доказати да скуп

$$G = \left\{ \begin{bmatrix} a & 0 \\ a - b & b \end{bmatrix} : a, b \in \mathbb{R} \setminus \{0\} \right\}$$

чини групу у односу на множење матрица.

1.11 Доказати да скуп

$$SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z},\, ad - bc = 1 \right\}$$

чини (некомутативну) групу у односу на множење матрица.

1.12 Доказати да скуп

$$G = \left\{ \begin{bmatrix} 2a & -a & -a \\ -a & 2a & -a \\ -a & -a & 2a \end{bmatrix} : a \in \mathbb{R} \setminus \{0\} \right\}$$

чини комутативну групу у односу на множење матрица.

1.13 Нека је са $M_n(\mathbb{R})$ означен скуп свих матрица димензије $n \times n$ са елементима из $\mathbb{R}$. Доказати да скуп

$$G = \left\{ \begin{bmatrix} a & a & \dots & a \\ a & a & \dots & a \\ \vdots & \dots & \ddots & \vdots \\ a & a & \dots & a \end{bmatrix} : a \in \mathbb{R} \setminus \{0\} \right\} \subseteq M_n(\mathbb{R})$$

чини комутативну групу у односу на множење матрица.

1.14 Нека је са $M_n(\mathbb{R})$ означен скуп свих матрица димензије $n \times n$ са елементима из $\mathbb{R}$. Претпоставимо да је $G \subseteq M_n(\mathbb{R})$ такав да је G група у односу на множење матрица. Доказати да су или све матрице из G сингуларне[3] или су све матрице из G несингуларне.

1.15 Нека је $G = \mathbb{Q} \cap [0, 1)$. На скупу G дефинисана је операција $\oplus$ са:

$$x \oplus y = \begin{cases} x + y, & 0 \leqslant x + y < 1 \\ x + y - 1, & x + y \geqslant 1. \end{cases}$$

Доказати да је $(G, \oplus)$ Абелова група.

1.16 Нека је $G = \bigcup_{n=1}^{\infty} \{z \in \mathbb{C} : z^n = 1\}$. Доказати да G чини групу у односу на операцију множења комплексних бројева.

1.17 Нека је $c > 0$ и $V = (-c, c)$. На скупу V дефинисана је операција $\oplus$ са:

$$v_1 \oplus v_2 = \frac{v_1 + v_2}{1 + \frac{v_1 v_2}{c^2}}.$$

Доказати да је $(G, \oplus)$ Абелова група.

1.18 Нека је за $a, b \in \mathbb{R}$, $a \neq 0$, функција $f_{a,b} : \mathbb{R} \longrightarrow \mathbb{R}$ дефинисана са $f_{a,b}(x) = ax + b$. Доказати да $G = \{f_{a,b} : a, b \in \mathbb{R}, a \neq 0\}$ чини групу у односу на композицију функција.

1.19 Да ли је $(G, \cdot_{14})$ група, ако је: а) $G = \{1, 3, 5\}$; б) $G = \{1, 3, 5, 7\}$; в) $G = \{1, 9, 11, 13\}$; г) $G = \{1, 3, 5, 9, 11, 13\}$?

1.20 Доказати да подскуп од $\{1, 2, 3, \dots, 21\}$ који садржи неки паран број и број 11 не може чинити групу у односу на операцију множења бројева по модулу 22.

1.21 Нека је g елемент групе G. Доказати да је $G = \{gx : x \in G\}$ и да за $x \neq y$ важи $gx \neq gy$.

1.22 Нека је G група чији је носач скуп $\{e, a, b, c\}$. Написати Кејлијеву таблицу ове групе ако је познато да је e неутрал и да важи $a^2 = b^2 = e$.

[3] Матрица димензије $n \times n$ је сингуларна акко је њен ранг мањи од n.

$$|\Omega((1,2,1,2,1,2))| = 2, \quad |\Omega((2,2,2,2,2,2))| = 1,$$

што се директно проверава (погледати и наредни доказ). ♣

Искористимо добијене резултате за доказ Кошијеве теореме.

Доказ Кошијеве теореме. Дакле, нека је G коначна група и p прост број који дели ред групе G. Треба доказати да у G постоји елемент реда p. У ту сврху, нека је $H = \langle a \rangle$ нека циклична група реда p и

$$X = \{(x_1, x_2, \ldots, x_p) \in G^p : x_1 x_2 \cdots x_p = e\}.$$

Приметимо пре свега да је $|X| = |G|^{p-1}$. Наиме, $x_1, \ldots, x_{p-1}$ могу бити ма који елементи групе G, а тада је $x_p = (x_1 \cdots x_{p-1})^{-1}$. Стога $p \mid |X|$. Дејство групе H на X задато је са:

$$a \cdot (x_1, x_2, \ldots, x_p) := (x_2, \ldots, x_p, x_1).$$

Дакле, дејство одговара цикличном пермутовању дате p-торке. Приметимо да је довољно задати дејство генератора пошто је H циклична група (дејство осталих елемената је јединствено одређено условом б) из дефиниције 1.93). Проверимо да је $(x_2, \ldots, x_p, x_1) \in X$. Ово следи из

$$\begin{aligned} x_2 \cdots x_{p-1} x_p x_1 &= x_2 \cdots x_{p-1} (x_1 x_2 \cdots x_{p-1})^{-1} x_1 \\ &= x_2 \cdots x_{p-1} x_{p-1}^{-1} \cdots x_2^{-1} x_1^{-1} x_1 = e. \end{aligned}$$

Дакле, дејство је добро дефинисано. Како број елемената орбите ма ког елемента дели ред групе H, закључујемо да је број елемената ма које орбите или 1 или p. Приметимо да је орбита елемента $(e, e, \ldots, e)$ једночлана. Како је X дисјунктна унија различитих орбита, тј.

$$X = \Omega_1 \sqcup \Omega_2 \sqcup \cdots \sqcup \Omega_k,$$

за орбите $\Omega_1, \ldots, \Omega_k$, и како постоји бар једна једночлана орбита закључујемо да мора постојати бар још једна таква. Наиме, уколико је нпр. Ω_1 једина једночлана орбита, добили бисмо једнакост

$$|G|^{p-1} = 1 + p(k-1).$$

Но, ово није могуће пошто $p \mid |G|$. Нека је $\Omega_2 = \{(x_1, x_2, \ldots, x_p)\}$ једночлана орбита различита од $\{(e, e, \ldots, e)\}$. Тада мора бити

$$a \cdot (x_1, x_2, \ldots, x_p) = (x_1, x_2, \ldots, x_p),$$

тј.

$$(x_2, \ldots, x_p, x_1) = (x_1, x_2, \ldots, x_p).$$

Добијамо да је $x_1 = x_2 = \cdots = x_p$. Означимо тај елемент са g. По претпоставци, $g \neq e$, а осим тога, како $(g, g, \ldots, g) \in X$, мора бити $g^p = e$. По (1.9) закључујемо да је g тражени елемент реда p. □

Видели смо да је број елемената у орбити неког елемента једнак индексу стабилизатора тог елемента. Да ли постоји веза између стабилизатора два елемента из исте орбите? Важи следећи став.

Став 1.104 Нека група G дејствује на скупу X. Ако су елементи x и y из исте орбите, онда су њихови стабилизатори конјуговане подгрупе, тј. постоји елемент $g \in G$ такав да је $\Sigma_y = g\Sigma_x g^{-1}$.

Доказ. По претпоставци постоји елемент $g \in G$ такав да је $y = g \cdot x$. Покажимо да је

$$\Sigma_y = g\,\Sigma_x\,g^{-1}.$$

$\subseteq$: Нека је $h \in \Sigma_y$. Како је $y = g \cdot x$, то је $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = e \cdot x = x$. Добијамо

$$(g^{-1}hg) \cdot x = g^{-1} \cdot (h \cdot (g \cdot x)) = g^{-1} \cdot (h \cdot y) = g^{-1} \cdot y = x.$$

Дакле, $g^{-1}hg \in \Sigma_x$, па $h \in g\,\Sigma_x\,g^{-1}$.

$\supseteq$: Нека је $h \in \Sigma_x$. Тада је

$$(ghg^{-1}) \cdot y = g \cdot (h \cdot (g^{-1} \cdot y)) = g \cdot (h \cdot x) = g \cdot x = y.$$

Дакле, $g\,\Sigma_x\,g^{-1} \subseteq \Sigma_y$. □

Нека G дејствује на X и нека је g елемент из G. Скуп свих фиксних тачака елемента g, у ознаци X^g задаје се са:

$$X^g := \{x \in X : g \cdot x = x\}.$$

Приметимо да важи следеће:

$$x \in X^g \quad \text{ако и само ако} \quad g \in \Sigma_x.$$

Став 1.105 Нека G дејствује на X. Ако су елементи g и h конјуговани, онда постоји бијекција између скупова X^g и X^h.

Доказ. Нека је $g = khk^{-1}$. Дефинишимо пресликавање $f\colon X \to X$ са $f(x) = k \cdot x$. Покажимо да f успоставља бијекцију између X^h и X^g.

Нека је $x \in X^h$. Тада је $h \cdot x = x$, па следи

$$\begin{aligned} g \cdot f(x) &= g \cdot (k \cdot x) = k \cdot (h \cdot (k^{-1} \cdot (k \cdot x))) \\ &= k \cdot (h \cdot ((k^{-1}k) \cdot x)) = k \cdot (h \cdot (e \cdot x)) = k \cdot (h \cdot x) = k \cdot x = f(x). \end{aligned}$$

Дакле, $f\left[X^h\right] \subseteq X^g$. Са друге стране, ако $y \in X^g$, тада је $g \cdot y = y$, па како је $h = k^{-1}gk$, следи

$$h \cdot (k^{-1} \cdot y) = (k^{-1}gk) \cdot (k^{-1} \cdot y) = (k^{-1}gkk^{-1}) \cdot y = k^{-1} \cdot (g \cdot y) = k^{-1} \cdot y,$$

тј. $k^{-1} \cdot y \in X^h$. Како је $f(k^{-1} \cdot y) = y$, следи $X^g \subseteq f\left[X^h\right]$, па f заиста успоставља тражену бијекцију. □

Формула која одређује број различитих орбита је веома корисна у разним применама. Дајемо је у оквиру наредне теореме.

Теорема 1.106 Нека коначна група G дејствује на коначном скупу X. Тада је број различитих орбита једнак броју

$$\frac{1}{|G|}\sum_{g\in G}|X^g|\,.$$

Доказ. Означимо тражени број различитих орбита са k. Дакле,

$$X=\Omega_1\sqcup\cdots\sqcup\Omega_k,$$

где су Ω_i различите орбите. Посматрајмо скуп E задат са

$$E=\{(g,x)\in G\times X : g\cdot x=x\}.$$

Приметимо да

$$x\in X^g \text{ акко } (g,x)\in E \text{ акко } g\in\Sigma_x.$$

„Пребројаћемо" елементе у E на два начина. Приметимо најпре да је

$$E=\bigsqcup_{g\in G}\{g\}\times X^g.$$

Дакле,

$$|E|=\sum_{g\in G}|X^g|\,. \tag{1.20}$$

С друге стране,

$$E=\bigsqcup_{x\in X}\Sigma_x\times\{x\}.$$

Према томе,

$$|E|=\sum_{x\in X}\Sigma_x=\sum_{i=1}^{k}\sum_{x\in\Omega_i}|\Sigma_x|.$$

Како елементи из исте орбите имају конјуговане стабилизаторе (по ставу 1.104), то је $|\Sigma_x|=|\Sigma_y|$ уколико су x и y у истој орбити. Изаберимо по један елемент x_i из сваке од орбита Ω_i. По ставу 1.101 добијамо

$$|E|=\sum_{i=1}^{k}\sum_{x_i\in\Omega_i}|\Sigma_{x_i}|=\sum_{i=1}^{k}|\Omega_i||\Sigma_{x_i}|=\sum_{i=1}^{k}[G:\Sigma_{x_i}]|\Sigma_{x_i}|=\sum_{i=1}^{k}|G|=k|G|.$$

Из (1.20) и претходне једнакости следи тражени резултат. □

За крај наводимо два примера примене управо доказане формуле.

Пример 1.107 Темена квадрата бојимо са две боје. На колико се начина то може извести?

$x'y + y'/x = 0$. Није тешко проверити да овај систем има (јединствено) решење $x' = 1/x$ и $y' = -y$ $(x \neq 0)$ и важи $x' \neq 0$. Дакле, A' је инверз матрице A.

1.10 Докажимо прво да је множење матрица операција на скупу G. Нека је $A, B \in G$. Тада за неке $a_1, b_1, a_2, b_2 \in \mathbb{R} \setminus \{0\}$, важи

$$A = \begin{bmatrix} a_1 & 0 \\ a_1 - b_1 & b_1 \end{bmatrix}, \qquad B = \begin{bmatrix} a_2 & 0 \\ a_2 - b_2 & b_2 \end{bmatrix},$$

па је

$$AB = \begin{bmatrix} a_1 & 0 \\ a_1 - b_1 & b_1 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ a_2 - b_2 & b_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 & 0 \\ a_1a_2 - b_1b_2 & b_1b_2 \end{bmatrix}.$$

Како је $a_1a_2 \neq 0$ и $b_1b_2 \neq 0$, то је $AB \in G$.

Асоцијативност се поново „преноси" из $M_2(\mathbb{R})$, а неутрал је матрица

$$E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 - 1 & 1 \end{bmatrix}.$$

Одредимо инверз матрице $A = \begin{bmatrix} a & 0 \\ a - b & b \end{bmatrix} \in G$. Нека је то матрица $A' = \begin{bmatrix} a' & 0 \\ a' - b' & b' \end{bmatrix}$. Тада важи $AA' = A'A = E$, тј.

$$\begin{bmatrix} aa' & 0 \\ aa' - bb' & bb' \end{bmatrix} = \begin{bmatrix} a'a & 0 \\ a'a - b'b & b'b \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Изједначавањем одговарајућих елемената ових матрица добијамо следеће једнакости: $aa' = a'a = 1$, $aa' - bb' = 0$ и $bb' = 1$, па је $a' = 1/a$ и $b' = 1/b$, односно

$$A' = \begin{bmatrix} 1/a & 0 \\ 1/a - 1/b & 1/a \end{bmatrix} \in G$$

је инверз матрице A.

1.11 Приметимо да је $SL_2(\mathbb{Z})$ скуп матрица из $M_2(\mathbb{Z})$ чија је детерминанта једнака 1.

Нека је $A, B \in SL_2(\mathbb{Z})$. Тада је $AB \in M_2(\mathbb{Z})$, тј. сви елементи матрице AB су цели бројеви. Како је по Бине-Кошијевој теореми $\det(AB) = \det(A)\det(B)$, то је и $\det(AB) = 1$, па важи $AB \in SL_2(\mathbb{Z})$.

Као у претходном задатку закључујемо да је операција асоцијативна и да је њен неутрал E (јер је $E \in SL_2(\mathbb{Z})$).

Докажимо и да матрица $A \in SL_2(\mathbb{Z})$ има инверз у $SL_2(\mathbb{Z})$. Нека је $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Знамо да инверз матрице, тј. A^{-1}, можемо одредити по формули

$$A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A),$$

па како је $\det(A) = 1$, то је

$$A^{-1} = \operatorname{adj}(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Дакле, $A^{-1} \in M_2(\mathbb{Z})$, па како је $\det(A^{-1}) = da - (-b)(-c) = \det(A) = 1$, закључујемо да важи $A^{-1} \in SL_2(\mathbb{Z})$.

1.12 Означимо $M_a = \begin{bmatrix} 2a & -a & -a \\ -a & 2a & -a \\ -a & -a & 2a \end{bmatrix}$ (за $a \in \mathbb{R} \setminus \{0\}$).

Множење матрица је операција на G, јер за $a, b \in \mathbb{R} \setminus \{0\}$ важи

$$\begin{bmatrix} 2a & -a & -a \\ -a & 2a & -a \\ -a & -a & 2a \end{bmatrix} \begin{bmatrix} 2b & -b & -b \\ -b & 2b & -b \\ -b & -b & 2b \end{bmatrix} = \begin{bmatrix} 6ab & -3ab & -3ab \\ -3ab & 6ab & -3ab \\ -3ab & -3ab & 6ab \end{bmatrix},$$

тј. $M_a \cdot M_b = M_{3ab} \in G$.

Множење матрица је асоцијативна операција на $M_3(\mathbb{R})$, па и на G, а по претходној једнакости и комутативна на G.

Неутрал је матрица M_e ($e \neq 0$) таква да за све $a \in \mathbb{R} \setminus \{0\}$ важи

$$M_a \cdot M_e = M_e \cdot M_a = M_a.$$

По претходном ово важи ако и само ако је $M_{3ae} = M_{3ea} = M_a$. Дакле, неутрал је матрица $M_{\frac{1}{3}}$.

Матрица M_b је инверз матрице M_a (за $a \in \mathbb{R} \setminus \{0\}$) ако и само ако је $b \neq 0$ и важи

$$M_a \cdot M_b = M_b \cdot M_a = M_{\frac{1}{3}}.$$

Како је $M_a \cdot M_b = M_b \cdot M_a = M_{3ab}$, инверз матрице M_a је матрица $M_{\frac{1}{9a}}$.

Коментар. Приметимо да неутрал није јединична матрица, иако је операција у групи множење матрица. Погледати и наредна два задатка.

1.13 Означимо $M_a = \begin{bmatrix} a & a & \dots & a \\ a & a & \dots & a \\ \vdots & \dots & \ddots & \vdots \\ a & a & \dots & a \end{bmatrix}$ (за $a \in \mathbb{R} \setminus \{0\}$).

Множење матрица је операција на G, јер за $a, b \in \mathbb{R} \setminus \{0\}$ важи

$$\begin{bmatrix} a & a & \dots & a \\ a & a & \dots & a \\ \vdots & \dots & \ddots & \vdots \\ a & a & \dots & a \end{bmatrix} \begin{bmatrix} b & b & \dots & b \\ b & b & \dots & b \\ \vdots & \dots & \ddots & \vdots \\ b & b & \dots & b \end{bmatrix} = \begin{bmatrix} nab & nab & \dots & nab \\ nab & nab & \dots & nab \\ \vdots & \dots & \ddots & \vdots \\ nab & nab & \dots & nab \end{bmatrix},$$

тј. $M_a \cdot M_b = M_{nab} \in G$.

Множење матрица је асоцијативна операција на $M_n(\mathbb{R})$, па и на G, а по претходној једнакости и комутативна на G.

Неутрал је матрица M_e $(e \neq 0)$ таква да за све $a \in \mathbb{R} \setminus \{0\}$ важи

$$M_a \cdot M_e = M_e \cdot M_a = M_a.$$

По претходном ово важи ако и само ако је $M_{nae} = M_{nea} = M_a$, па је неутрал матрица $M_{\frac{1}{n}}$.

Матрица M_b је инверз матрице M_a (за $a \in \mathbb{R} \setminus \{0\}$) ако и само ако је $b \neq 0$ и важи

$$M_a \cdot M_b = M_b \cdot M_a = M_{\frac{1}{n}}.$$

Како је $M_a \cdot M_b = M_b \cdot M_a = M_{nab}$, инверз за M_a је матрица $M_{\frac{1}{n^2 a}}$.

Коментар. Приметимо да неутрал није јединична матрица, иако је операција у групи множење матрица. Погледати и претходни, као и наредни задатак.

1.14 Елементе групе G означаваћемо малим словима (да их не бисмо помешали са истакнутим елементима скупа $M_n(\mathbb{R})$); између осталог, неутрал групе G ћемо означити са e.

Подсетимо се да је матрица сингуларна ако и само ако је њена детерминанта једнака 0. Размотримо сада следеће случајеве.

1° e је сингуларна. Тада је $\det(e) = 0$. Нека је $a \in G$ произвољно. Како је e неутрал групе G важи $a \cdot e = e \cdot a = a$, па је по Бине-Кошијевој теореми

$$\det(a) = \det(a \cdot e) = \det(a) \cdot \det(e) = 0,$$

односно a је сингуларна, што је и требало доказати.

2° e је несингуларна. Тада је $\det(e) \neq 0$. Нека је $a \in G$ произвољно. Довољно је доказати да $\det(a) \neq 0$. Претпоставимо супротно. Тада за инверз a^{-1} елемента a важи $a \cdot a^{-1} = a^{-1} \cdot a = e$, па је по Бине-Кошијевој теореми

$$\det(e) = \det(a \cdot a^{-1}) = \det(a) \cdot \det(a^{-1}) = 0,$$

што је контрадикција.

1.15 Нека је $x, y \in G$. Јасно је да је тада $x \oplus y \in \mathbb{Q}$. Проверимо да је и $x \oplus y \in [0, 1)$. Ако је $0 \leqslant x + y < 1$, тада је $x \oplus y = x + y \in [0, 1)$; ако је $x + y \geqslant 1$, тада је $x \oplus y = x + y - 1$, па како је $x + y < 2$ (јер је $x, y < 1$), то је и у овом случају $x \oplus y \in [0, 1)$. Дакле, $\oplus$ је операција на G.

Докажимо да је $\oplus$ асоцијативна операција (погледати и коментар). Нека је $x, y, z \in G$. Приметимо да у дефиницији операције $\oplus$ имамо „два случаја". То нам сугерише да ћемо и приликом доказивања асоцијативности имати неколико случајева, које разликујемо како бисмо израчунали $(x \oplus y) \oplus z$ и $x \oplus (y \oplus z)$.

Случај 1. $0 \leqslant x + y < 1$ и $0 \leqslant y + z < 1$.

Додатак II

Ред производа елемената

У овом делу показаћемо да за свака три природна броја m, n, r који су сви већи од 1, постоји група G и елементи a и b из G такви да је $\omega(a) = m$, $\omega(b) = n$ и $\omega(ab) = r$.

Пођимо од групе $\mathrm{SL}_2(\mathbb{C})$:

$$\mathrm{SL}_2(\mathbb{C}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{C}, ad - bc = 1 \right\}.$$

Докажимо најпре да је $-I$ једини елемент ове групе који је реда 2 (овде I означава јединичну матрицу). Наиме, уколико је $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ реда 2, онда је

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

те добијамо

$$a^2 + bc = 1, \quad ab + bd = 0, \quad ca + dc = 0, \quad cb + d^2 = 1. \qquad (\mathbf{II}.1)$$

Претпоставимо да је $a + d = 0$. Тада из једнакости $ad - bc = 1$ добијамо $a^2 + bc = -1$, што противречи првој једнакости у ($\mathbf{II}$.1). Дакле, $a + d \neq 0$ и из друге и треће једнакости у ($\mathbf{II}$.1) добијамо $b = c = 0$. Следи да је $a^2 = d^2 = 1$ и $ad = 1$. Према томе $a = d \in \{-1, 1\}$. С обзиром да је A реда 2, дакле, $A \neq I$, добијамо да је $A = -I$, што смо и желели да докажемо.

Нека су сада u, v, w елементи из $\mathbb{C} \setminus \{0\}$ редом редова $2m, 2n, 2r$. Посматрајмо матрице

$$A = \begin{bmatrix} u & 1 \\ 0 & u^{-1} \end{bmatrix}, \quad B = \begin{bmatrix} v & 0 \\ t & v^{-1} \end{bmatrix},$$