Групи.

Разглеждаме непразното множество $G \neq \varnothing$, затворено относно някаква бинарна операция $*$. Бинарната операция е изображение

$$* : G \times G \longrightarrow G,$$

действащо по правилото $(a, b) \mapsto c$ за $\forall a, b \in G$ и някакъв елемент $c \in G$. С други думи бинарната операция съопставя по един елемент от G на всяка нарадена двойка елементи от $G \times G$. За по-кратко записваме $a * b = c \in G$.

Казваме, че G е група относно операцията $*$ и за удобство пишем $(G, *)$ (наредена двойка от множеството и операцията, спрямо която то е група), ако са изпълнени следните три аксиоми:

1) Дадената операция е асоциативна, т.е.

$$(a * b) * c = a * (b * c)$$

за всеки три елемента $a, b, c \in G$.

2) Съществува неутрален елемент $e \in G$, такъв че

$$a * e = e * a = a$$

за всеки елемент $a \in G$. Когато операцията е събиране $+$, обикновено този елемент се нарича нулев елемент и пишем 0; ако операцията е умножение $\cdot$, обикновено този елемент се нарича единичен и се бележи с 1.

3) За всеки елемент $a \in G$ съществува обратен елемент $a^{-1} \in G$, такъв че

$$a * a^{-1} = a^{-1} * a = e.$$

Типични примери за групи са групата на целите числа относно събирането $(\mathbb{Z}, +)$; групата $\mathbb{Z}^* = \mathbb{Z} \backslash \{0\}$ относно умножението – $(\mathbb{Z}^*, \cdot)$; групата

$GL_n(F)$, състояща се от всички неособени матрици от ред n с елементи от поле F, относно умножението; групата $\mathbb{C}_n$ на n-тите комплексни корени на единицата относно умножението; групата $\mathbb{Z}_n$ на остатъците по модул n относно събирането.

Ако освен трите аксиоми е изпълнено още и че

4) $a * b = b * a$

за произволни два елемента $a, b \in G$, то казваме, че групта G е абелева или комутативна. Очевдино групите $(\mathbb{Z}, +), (\mathbb{Z}^*, \cdot), (\mathbb{C}_n, \cdot)$ и $(\mathbb{Z}_n, +)$са абелеви, но $GL_n(F)$ не е.

Задача 1. *Опишете адитивната група $\mathbb{Z}_6$.*

Решение. Достатъчно е да покажем кой елемент се съпоставя на всеки два елемнта от $\mathbb{Z}_6$ под действието на операцията $+$. Ще използваме таблицата на Кейли за по-лесно описание.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Да забележим, че абелевостта на групата се отразява като симетрия на таблицата спрямо „главния диагонал“. $\square$

<u>Забележка 1:</u>

Обратимите елементи относно операцията умножение в $\mathbb{Z}_n$ също образуват група.

<u>Забележка 2:</u>

В $\mathbb{Z}_n$ са обратими тези $\overline{k}$, за които $(k, n) = 1$. Наистина от тъждеството на Безу следва, че за тях съществуват елементи $u, v \in \mathbb{Z}$, такива че $uk + vn = 1$ и взимайки това равенство по модул n получаваме

$$uk \equiv 1 (\operatorname{mod} n)$$

или с други думи $\overline{k}^{-1} = \overline{u}$.

<u>Забележка 3:</u>

Ако n е просто число, то обратимите елементи спрямо умножението са $\{\overline{1}, \overline{2}, \dots, \overline{n-1}\} = \mathbb{Z}_n^*$.

Задача 2. *Опишете $\mathbb{Z}_5^*$ и решете уравнението $\overline{3}x = \overline{2}$.*

Решение. Съставяме таблицата на Кейли

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

от която става ясно, че $\overline{3}^{-1} = \overline{2}$ (защото според таблицата $\overline{3} \cdot \overline{2} = \overline{1}$). Умножаваме двете страни на уравнението с $\overline{3}^{-1} = \overline{2}$, за да получим, че

$$x = \overline{2} \cdot \overline{2} = \overline{4}.$$

$\square$

Ако $(G, *)$ е група, а $H \subseteq G$, то казваме, че H е подгрупа на G и пишем $H \leq G$ (или по-подробно $(H, *) \leq (G, *)$), ако $ab^{-1} \in H$ за всеки два елемента $a, b \in H$. Алтернативно може да се провери последователно, че $ab \in H$ и $b^{-1} \in H$.

Задача 3. *Покажете, че множеството*

$$M = \left\{ \begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix} \mid a, b \in \mathbb{Q}, a \neq 0 \right\}$$

е група относно умножението на матрици, а подмножеството

$$N = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{Q}, a \neq 0 \right\}$$

е негова подгрупа.

Решение. Започваме от провекрата затвореността на M относно операцията и на асоциативността на самата операцията. Нека

$$A = \begin{pmatrix} a_1 & 0 \\ b_1 & a_1^{-1} \end{pmatrix}, B = \begin{pmatrix} a_2 & 0 \\ b_2 & a_2^{-1} \end{pmatrix}, C = \begin{pmatrix} a_3 & 0 \\ b_3 & a_3^{-1} \end{pmatrix}$$

са три произволни елемента на групата G. Тогава

$$AB = \begin{pmatrix} a_1a_2 & 0 \\ a_2b_1 + a_1^{-1}b_2 & (a_1a_2)^{-1} \end{pmatrix} \in M,$$

което означава, че M е затворено относно умножението на матрици. Още

$$(AB)C = \begin{pmatrix} a_1a_2a_3 & 0 \\ a_2a_3b_1 + a_1^{-1}a_3b_2 + a_1^{-1}a_2^{-1}b_3 & (a_1a_2a_3)^{-1} \end{pmatrix}.$$

От друга страна

$$BC = \begin{pmatrix} a_2a_3 & 0 \\ a_3b_2 + a_2^{-1}b_3 & (a_2a_3)^{-1} \end{pmatrix}$$

и

$$A(BC) = \begin{pmatrix} a_1a_2a_3 & 0 \\ a_2a_3b_1 + a_1^{-1}a_3b_2 + a_1^{-1}a_2^{-1}b_3 & (a_1a_2a_3)^{-1} \end{pmatrix}.$$

По този начин директно проверихме, че $(AB)C = A(BC)$, т.е. показахме асоциативността на операцията.

Очевидно единичната матрица

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$$

и играе ролята на неутрален елемент.

Матрицата

$$A^{-1} = \begin{pmatrix} a_1^{-1} & 0 \\ -b_1 & a_1 \end{pmatrix} \in M$$

за вска матрица $A \in M$ е съответстващата обратна матрица и играе ролята на обратен елемент в M. С това трите аксиоми са проверени и $(M, \cdot)$ е група.

Нека сега

$$N_1 = \begin{pmatrix} a_1 & 0 \\ 0 & a_1^{-1} \end{pmatrix}, N_2 = \begin{pmatrix} a_2 & 0 \\ 0 & a_2^{-1} \end{pmatrix}$$

са прозиволни елементи от N. Тогава

$$N_1N_2 = \begin{pmatrix} a_1a_2 & 0 \\ 0 & (a_1a_2)^{-1} \end{pmatrix} \in N$$

и

$$N_2^{-1} = \begin{pmatrix} a_2^{-1} & 0 \\ 0 & a_2 \end{pmatrix} \in N,$$

което доказва, че $(N, \cdots) \leq (M, \cdot)$. Еквивалентно можеше да проверим единствено, че

$$N_1 N_2^{-1} = \begin{pmatrix} a_1 a_2^{-1} & 0 \\ 0 & a^{-1} a_2 \end{pmatrix} \in N.$$

□

Задача 4. *Разглеждаме реалната права $\mathbb{R}$ и множеството от реални фунцкии*

$$G = \{f \mid f(x) = ax + b, a, b \in \mathbb{R}\}.$$

Докажете, че G е група относно операцията композиция на изображения, а подмножествата

$$K_1 = \{f \mid f(x) = ax, a \in \mathbb{R}, a \neq 0\}, K_2 = \{f \mid f(x) = x + b, b \in \mathbb{R}\}$$

са нейни подрупи.

Решение. Имайки предивд, че за всеки две функции $f_1(x) = a_1 x + b_1$ и $f_2(x) = a_2 x + b_2$ е в сила $(f_2 f_1)(x) = f_2(f_1(x)) = a_2(a_1 x + b_1) + b_2 = a_1 a_2 x + a_2 b_1 + b_2 \in G$, то доказваме, че множеството G е затворено относно композицията на функции.

Докажете директно, че

$$(f_3 f_2)(f_1(x)) = f_3((f_2 f_1)(x)),$$

за да покажете асоциативността на операцията.

Търсим единичен елемент $e(x) = ax + b \in G$. За да го определим, ще намерим коефициентите a и b чрез проверка на втората аксиома за група. За произволна функция $f = a_1 x + b_1 \in G$ тябва да е изпълнено, че

$$(fe)(x) = f(x).$$

Имаме, че $(fe)(x) = f(e(x)) = a_1(ax+b)+b_1 = a_1 ax + a_1 b + b_1$ и $f(x) = a_1 x + b_1$. Приравняваме коефициентите, т.е. търсим решения на уравненията

$$a_1 a = a_1$$

и

$$a_1 b + b_1 = b_1.$$

Ясно е, че те са изпълнени за произволна функция f_1 само при $a = 1$ и $b = 0$. С други думи открихме, че единичният елемент е $e(x) = x \in G$.

За произволна функция $f(x) = ax + b \in G$ търсим обратен елемент $f^{-1} = a_1 x + b_1$, така че да е изпълнена третата аксиома за група, а именно

$$(f^{-1} f)(x) = e(x).$$

От една страна имаме, че $(f^{-1} f)(x) = f^{-1}(f(x)) = a_1(ax + b) + b_1 = a_1 ax + a_1 b + b_1$, а от друга $e(x) = x$. Отново, приравнявайки коефициентите на двата израза получаваме уравненията

$$a_1 a = 1$$

и

$$a_1 b + b_1 = 0.$$

Те са изпълени едновременно, точно когато $a_1 = \dfrac{1}{a} = a^{-1}$ и $b_1 = -a_1 b = \dfrac{b}{a}$ или с други думи за произволен елемент $f(x) = ax + b \in G$ съответният му обратен елемент е $f^{-1}(x) = \dfrac{1}{a}x - \dfrac{b}{a}$. Очевидно $f^{-1} \in G$, което доказва окончателно, че G е група.

По познатия вече начин покажете, че $K_1, K_2 \leq G$. $\square$

Да разгледаме някои по-интересни примери за групи.

Нека $n \in \mathbb{N}$, $n \geq 3$. Нека φ е ротация на равнината около центъра на координатната ситема Oxy на ъгъл $\dfrac{2\pi}{n}$ в положителна посока. Нека σ е симетрия спрямо оста Ox. Аналитично може да представим φ и σ като линейни оператори по следния начин:

$$\varphi = \begin{pmatrix} \cos\dfrac{2\pi}{n} & -\sin\dfrac{2\pi}{n} \\ \sin\dfrac{2\pi}{n} & \cos\dfrac{2\pi}{n} \end{pmatrix}, \sigma \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Тогава множеството

$$D_n = \{\varphi^i \sigma^j \mid i = 0, 1, \ldots, n-1; j = 0, 1\}$$

е група относно операцията умножение на линейни оператори наречена диедрална група. Тя всъщност изчерпва всички симетрии на правилен n-ъгълник в равнината. Лесно се вижда, че $|D_n| = 2n$.

Нека разгледаме множеството

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\},$$

в което е въведена операция умножение по правилата

$$i^2 = j^2 = k^2 = -1; ij = -ji = k; jk = -kj = i; ki = -ik = j.$$

Спрямо тази операция множеството Q_8 е група, наречена група на кватернионите.

Нека Ω е множество от n елемента. С S_Ω означаваме множеството от всички взаимно еднозначни изображения на Ω в себе си. Без ограничение може да считаме, че

$$\Omega = \{1, 2, \dots, n\}$$

и тогава означаваме с S_n множеството от всички пермутации на числата от 1 до n. Ако например пермутацията σ пермутира числата от 1 до n в $i_1, i_2, \dots, i_n$,то записваме

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix},$$

т.е. 1 отива в i_1, 2 отива в i_2 и т.н. n отива в i_n. Всъщност, редът на целите колони в този начин на записване на пермутации очевидно няма значение. Ако

$$\tau = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$$

е друга пермутация, в която за удобство сме разменили колоните така, че първият ѝ ред да съвпада с втория ред на σ, то произведението

$$\tau\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

се проследява в обратен ред, т.е. от σ към τ. Имаме, че 1 отива в i_1, а след това i_1 отива в j_1 – следователно в $\tau\sigma$ числото 1 отива в j_1. Имаме, че 2 отива в i_2, а след това i_2 отива в j_2 – следователно в $\tau\sigma$ числото 2 отива в j_2. И така нататък, накрая получаваме, че в $\tau\sigma$ числото n отива в j_n. Записано като пермутация имаме, че

$$\tau\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}.$$

Директно се проверява, че това умножение на пермутации е асоциативно.

Ясно е, че

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

оставя всяко от числата на мястото му и това всъщност е главната пермутация на числата от 1 до n. Очевидно $\sigma e = e\sigma = \sigma$ за всяка пермутация $\sigma \in S_n$.

Ако

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

е произволна пермутация на числата от 1 до n, то пермутацията, която ги връща обратно в главната е

$$\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

С това вече е ясно, че S_n е група относно умножението на пермутации, наречена симетрична група от ред n.

Всяка пермутация от S_n се разлага в произведение на независими цикли. Цикъл е подмножество $\{c_1, c_2, \dots, c_k\}$, $k \leq n$ на числата от 1 до n от дадена пермутация, в което например c_1 отива в c_2, c_2 отива в c_3 и т.н. c_{n-1} отива в c_n, а c_n се връща обратно в c_1. Записваме $(c_1, c_2, \dots, c_n)$. Два цикъла $(c_1, c_2, \dots, c_k)$ и $(b_1, b_2, \dots, b_l)$ са независими, ако $\{c_1, c_2, \dots, c_k\} \cap \{b_1, b_2, \dots, b_l\} = \varnothing$. Да вземем един нагледен пример. В пермутацията

$$\zeta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 2 & 7 & 6 & 1 & 4 & 5 \end{pmatrix}$$

имаме че 1 отива в 3, 3 отива в 2, 2 отива в 8, 8 отива в 5, 5 отива в 6, а 6 се връща в 1. Следователно получихме цикъла $(1, 3, 2, 8, 5, 6)$. Остана да проследим, че 4 отива в 7, а 7 се връща в 4. Това изчерпва всички числа от 1 до 8 и получихме разлагане на пермутацията

$$\zeta = (1, 3, 2, 8, 5, 6)(4, 7).$$

Ясно е, че числата, които остават на място под действието на дадена пермутация, не участват в разлагането й на цикли.

Задача 5. *Пресметнете произведението на циклите*

$$(1,5,6)(2,3,5,4).$$

Решение. Първото нещо, което забелязваме е, че двата цикъла не са независими. Т.к. най-голямото число, което се среща в тях е 6, без ограничение можем да разглеждаме пермутациите само на числата от 1 до 6. За всеки цикъл ще възстановим съответстваща му пермутация и след това ще умножим двете пермутации. Накрая ще разложим резултатната пермутация на цикли. И така, в

$$(2,3,5,4)$$

имаме, че 2 отива в 3, 3 отива в 5, 5 отива в 4, а 4 се връща в 2. Останалите числа 1 и 6 остават на място. Следователно получихме, че

$$(2,3,5,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 2 & 4 & 6 \end{pmatrix} = \sigma.$$

По същата процедура намираме, че

$$(1,5,6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 4 & 6 & 1 \end{pmatrix} = \tau.$$

Сега

$$(1,5,6)(2,3,5,4) = \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 4 & 6 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 2 & 4 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 2 & 4 & 1 \end{pmatrix} = (1,5,4,2,3,6).$$

□

Цикъл с дължина 2 се нарича транспозиция. Очевидно е, че ако (α_1, α_2) е транспозиция, то транспозицията (α_2, α_1) връща числата обратно в изходно положение. Всяка пермутация се разлага в произведение на транспозиции, но не независими и не по единствен начин. Един начин да разложим пермутация е да я разложим в неазависими цикли, а след това всеки цикъл да разложим в произведение от транспозиции например по правилото

$$(i_1, i_2, \ldots, i_m) = (i_m, i_{m-1}) \ldots (i_m, i_2)(i_m, i_1).$$

Една пермутация се нарича четна/нечетна, ако се разлага в произведение на четен/нечетен брой транспозиции. Ясно е, че произведението на четни пермутации също е четна пермутация. Освен това в главната пермутация e има 0 на брой транспозиции и тя също е четна. Също така се вижда и че обратната на всяка четна пермутация е четна. И така четните пермутации образуват подгрупа $A_n < S_n$, наречена алтернативна група от ред n. Лесно се вижда, че всеки цикъл от нечетен/четен ред е четна/нечетна пермутация.

Ако дадена група G съдържа краен брой елементи, то числото $|G|=$ броя на елементите се нарича ред на G. Например, ако G има $n \in \mathbb{N}$ на брой елемента, то казваме че G е група от ред n и пишем $|G| = n$. Ако G съдържа безбройно много елементи, то казваме че тя е група от безкраен ред и пишем $|G| = \infty$.

Нека $a \in G$ е произволен елемент на групата G. Най-малкото естествено число r, ако изобщо съществува такова, за което е изпълнено, че $a^r = e$ се нарича ред на елемента a. Записваме $|a| = r$. Ясно е, че ако $a^k = e$ за някое естествено число k, то $r \mid k$. За произволен елемент от краен ред $a \in G$ е в сила, че $a^{|G|} = e$. Следователно $|a| \mid |G|$ за всеки елемент от краен ред a.

Нека $a \in G$ е произволен елемент и $|a| = r$. Множеството

$$\langle a \rangle = \{a^0 = e, a^1, \ldots, a^{r-1}\}$$

е подгрупа на G, наречена циклична подгрупа, породена от a. В сила е, че $|\langle a \rangle| = |a|$.

Нека $H \leq G$ е произволна подгрупа на G. Множествата $gH = \{gh \mid h \in H\}$ за $\forall g \in G$ се наричат леви съседни класове на G по H с представители g. Аналогично, $Hg = \{hg \mid h \in H\}$ са десните съседни класове. Броят на левите съседни класове на G по H е равен на броят на десните съседни класове и се нарича индекс на H в G; означението е $|G : H|$.

Теорема на Лагранж. *Нека G е крайна група и $H \leq G$ е нейна подгрупа. В такъв случай*

$$|G| = |H|.|G : H|.$$

Нека за пример разгледаме групата $\mathbb{C}_6$, състояща се от комплексните корени на уравнението $x^6 = 1$. По-конкретно

$$\mathbb{C}_6 = \left\{1, \varepsilon = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6}, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5\right\}.$$

Понеже $1 = \varepsilon^0$, то всъщност $\mathbb{C}_6 = \langle\varepsilon\rangle$ е циклична група. Директно се проверява, че $|1| = 1, |\varepsilon| = 6, |\varepsilon^2| = 3, |\varepsilon^3| = 2, |\varepsilon^4| = 3, |\varepsilon^5| = 6$. Всъщност, от $|\mathbb{C}_6| = 6 = |\varepsilon^5| = |\langle\varepsilon^5\rangle|$ и $\langle\varepsilon^5\rangle \le \mathbb{C}_6$ следва, че още е изпълнено и $\langle\varepsilon^5\rangle = \mathbb{C}_6$.

Да разгледаме цикличната група $H = \langle\varepsilon^3\rangle$, породена от елемента ε^3. Имаме, че $H \le G$ и $|H| = |\varepsilon^3| = 2$. По-конкретно $H = \{1, \varepsilon^3\}$. Да видим всевъзможните съседни класове gH на G по H. За $g = 1$ имаме, че $1H = \{1.1, 1.\varepsilon^3\} = \{1, \varepsilon^3\} = H$. За $g = \varepsilon$ имаме, че $\varepsilon H = \{\varepsilon, \varepsilon^4\}$. За $g = \varepsilon^2$ имаме, че $\varepsilon^2 H = \{\varepsilon^2, \varepsilon^5\}$. За $g = \varepsilon^3$ имаме, че $\varepsilon^3 H = \{\varepsilon^3, \varepsilon^6\} = \{\varepsilon^3, 1\} = 1H = H$. За $g = \varepsilon^4$ имаме, че $\varepsilon^4 H = \{\varepsilon^4, \varepsilon^7\} = \{\varepsilon^4, \varepsilon\} = \varepsilon H$. За $g = \varepsilon^5$ имаме, че $\varepsilon^5 H = \varepsilon^2 H$. И така всички различни съседни класове са $H, \varepsilon H$ и $\varepsilon^2 H$. Тогава е в сила разбиването

$$G = H \cup \varepsilon H \cup \varepsilon^2 H$$

и ествествно е изпълнено и равенството от теоремата на Лагранж.

Казваме, че подгрупата $H \le G$ е нормална и пишем $H \trianglelefteq G$, ако левите и десните класове на G по H съвпадат, т.е. $gH = Hg$ за $\forall g \in G$. Ясно е, че ако G е абелева група, то комутативността на операцията в нея води до това, че всяка подгрупа $H \trianglelefteq G$ е нормална.

Нека G е група. Множеството

$$Z(G) = \{x \in G \mid xa = ax \text{ за } \forall a \in G\}$$

се нарича център на G.

Задача 6. *Покажете, че $Z(G) \trianglelefteq G$.*

Решение. Процедираме по познатия метод за проверка дали едно подмножество е подгрупа.

1. $Z(G) \neq \varnothing$, защото очевидно $e \in Z(G)$.

2. Множеството $Z(G)$ е затворено относно груповата операция в G. Наистина, ако $x, y \in Z(G)$, то $xy \in Z(G)$, защото

$$xya = xay = axy$$

за всяко $a \in G$, т.к. по начало $x, y \in Z(G)$.

3. Ако $y \in Z(G)$, то $y^{-1} \in Z(G)$. Наистина от

$$ya = ay$$

след ляво умножение с y^{-1} получаваме

$$a = y^{-1}ay,$$

а сега, след дясно умножение с y^{-1} имаме

$$ay^{-1} = y^{-1}a$$

и това е изпълнено за всяко $a \in G$.

По този начин $Z(G) \leq G$. Нормалността на $Z(G)$ като подгрупа следва от това, че всеки от елементите на $Z(G)$ комутира с всеки от елементите на G по определени и оттам левите и десните съседни класове съвпадат. $\square$

Елементът a се нарича спрегнат на елемента b в G, ако съществува елемент $x \in G$, такъв че $a = x^{-1}bx$.

Свойства:

1. Всеки елемент $a \in G$ е спрегнат на себе си чрез $a = e^{-1}ae$.

2. Ако a е спрегнат на b, то и b е спрегнат на a. Наистина от $a = x^{-1}bx$ след ляво умножение с x и дясно умножение с x^{-1} получаваме, че $b = xax^{-1} = (x^{-1})^{-1}ax^{-1}$.

3. Ако a е спрегнат на b и b е спрегнат на c, то a е спрегнат на c. Наистина, от $a = x^{-1}bx$ и $b = y^{-1}cy$ следва, че $a = x^{-1}bx = x^{-1}y^{-1}cyx = (yx)^{-1}cyx$.

Тези три свойства означават, че релацията един елемент да е спрегнат на друг е ралация на еквивалентност. Тогава групата G се разбива на непресичащи се класове спрегнати елементи.

Задача 7. *Опишете групата S_3. Намерете редовете на елементите и опишете подгрупите и класовете спрегнати елементи.*

Решение. Симетричната група от ред 3 се състои от всички пермутации на числата 1,2,3. Техният брой е $3! = 6$. Изброяваме шестте различни пермутации като същевременно ги разлагаме в цикли:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2) = a, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3) = b,$$

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(1,2)=c,\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=(2,3)=d,\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=(1,3)=p.$$

Редът на произволен цикъл е равен на дължината му. Следователно $a^3=e$, а оттук и $a^{-1}=a^2=(1,3,2)(1,3,2)=(1,2,3)=b$. Също така $b^2=b^{-1}=a$. Имаме още, че $ac=(1,2,3)(1,2)=(2,3)=d$ и $a^2c=bc=(1,2,3)(1,2)=(1,3)=p$. По този начин изразихме всички пермутации, различни от главната, чрез пермутациите a и c, а именно

$$a=a,b=a^2,c=c,d=ac,p=a^2c.$$

Съставяме таблицата на Кейли

$\cdot$	e	a	a^2	c	ac	a^2c
e	e	a	a^2	c	ac	a^2c
a	a	a^2	e	ac	a^2c	c
a^2	a^2	e	a	a^2c	c	ac
c	c	a^2c	ac	e	a^2	a
ac	ac	c	a^2c	a	e	a^2
a^2c	a^2c	ac	c	a^2	a	e

Разглеждаме всевъзможните циклични подгрупи и тривиалните подгрупи

$$H_1=\langle c\rangle=\{e,c\},H_2=\langle ac\rangle=\{e,ac\},H_3=\langle a^2c\rangle=\{e,a^2c\},$$

$$H_4=\langle a\rangle=\{e,a,a^2\}=\{e,b,b^2\},H_5=\{e\},H_6=S_3,$$

които всъщност изчерпват всички подгрупи на S_3.

За класовете спрегнати елементи: e сам образува цял клас $\{e\}$; всевъзможните спрегнати на a са

$$b^{-1}ab=a^2ab=b;$$

$$c^{-1}ac=cac=a^2cc=a^2c^2=a^2=b,$$

$$d^{-1}ad=dad=acaac=aca^2c=a^2=b,$$

$$p^{-1}ap=a^2caa^2c=a^2ca^3c=a^2cc=a^2c^2=a^2=b$$

и следователно друг клас от спрегнати елементи е $\{a,b\}$; всевъзможните спрегнати на c са

$$a^{-1}ca=a^2ca=ac=d,$$

$$b^{-1}cb = acb = aca^2 = a^2c = p,$$

$$d^{-1}cd = accac = a^2c = p,$$

$$p^{-1}cp = pcp = a^2cca^2c = ac = d$$

и следователно третият и последен съседен клас е $\{c, d, p\}$. □

Задача 8. *Покажете, че*

а) $|x| = |x^{-1}|$,

б) Спрегнатите елементи имат еднакви редове,

в) $|ab| = |ba|$.

Решение. а) Нека $|x| = r$, а $|x^{-1}| = m$. Умножаваме двете страни на равенството

$$x^r = e$$

с x^{-r}, което по дефиниция е равно на $(x^{-1})^r$. И така

$$e = x^{-r} = (x^{-1})^r,$$

откъдето следва, че $m \mid r$. От друга страна умножаваме двете страни на равенството

$$(x^{-1})^m = e$$

с x^m, откъдето получаваме, че

$$e = x^m.$$

От последното равенство следва, че също $r \mid m$, което доказва, че $r = m$.

б) Нека $|a| = r$, $c = x^{-1}ax$ и $|c| = m$. Имаме, че

$$c^r = \underbrace{x^{-1}axx^{-1}ax \dots x^{-1}ax}_{r \text{ пъти}} = x^{-1}a^rx = x^{-1}x = e$$

и следователно $m \mid r$. Повтаряйки аналогично разсъждение за $a = xcx^{-1}$ покажете, че $r \mid m$, откъдето ще следва, че $r = m$.

в) Имаме, че $ab = b^{-1}bab$, което означава, че ab и ba са спрегнати. Сега твърдението следва от подточка б). □

Задача 9. *Покажете, че ако в групата G съществува единствен елемент a от ред 2, то $a \in Z(G)$.*

Решение. Ако $|a| = 2$, то за всеки спрегнат на a с произволен $b \in G$ имаме, че $|b^{-1}ab| = 2$. От единствеността на a следва, че $b^{-1}ab = a$ за произволен елемент $b \in G$, което е еквивалентно на $ab = ba$ за произволен $b \in G$. Последното означава точно, че $a \in Z(G)$. □

Задача 10. *Покажете, че всяка подгрупа $H \leq G$ с индекс 2 е нормална.*

Решение. Щом индексът на H в G е равен на 2, то G притежава точно два леви съседни класа по H. Единият задължително е $eH = H$, а нека другият е gH за някакъв елемент $g \in G$. Тогава $G = H \cup gH$. По аналогични причини $G = H \cup Hg$, откъдето следва, че $gH = Hg$. □

Нека са дадени две групи $(G_1, *)$ и $(G_2, \circ)$. Изображението

$$\varphi : G_1 \longrightarrow G_2$$

се нарича хомоморфизъм на групи, ако

$$\varphi(a * b) = \varphi(a) \circ \varphi(b)$$

за произволни два елемента $a, b \in G_1$. Смисълът на това е, че изображението φ запазва операциите между елементите в двете групи. Ако допълнително φ е биекция, то то се нарича изоморфизъм на групи, а групите G_1 и G_2 се наричат изоморфни и пишем $G_1 \cong G_2$.

Ако G е група и $H \trianglelefteq G$ е нормална нейна подгрупа, то множеството

$$G/H = \{gH \mid g \in G\}$$

от съседните класове на G по H има групова структура спрямо операцията, наследена от G, и се нарича факторгрупа на G по H. Ясно е, че $|G/H| = |G : H|$.

Задача 11. *Опишете факторгрупата $\mathbb{C}_8/H$, където $H = \{1, -1\}$.*

Решение. Понеже групата $\mathbb{C}_8$ е абелева, то задължително подгрупата $H \trianglelefteq \mathbb{C}_8$ е нормална. Следователно е коректно да разглеждаме факторгрупата $\mathbb{C}_8/H$. Според теоремата на Лагранж очакваме

$$|\mathbb{C}_8/H| = |\mathbb{C}_8 : H| = \frac{|\mathbb{C}_8|}{|H|} = \frac{8}{2} = 4$$

на брой различни съседни класа или с други думи това са четирите елемента на разглежданата факторгрупа. Имаме, че

$$\mathbb{C}_8 = \left\{1, \varepsilon = \cos\frac{2\pi}{8} + i\sin\frac{2\pi}{8}, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5, \varepsilon^6, \varepsilon^7\right\}.$$

Т.к. $\varepsilon^4 = -1$ следва, че $H = \langle\varepsilon^4\rangle = \{1, \varepsilon^4\}$. Ясно е, че H е един от съседните класове и точно той играе ролята на единияен елемент във факторгрупата. Както преди, намираме останалите три съседни класа на $\mathbb{C}_8$ по H, а именно

$$\varepsilon H = \{\varepsilon, \varepsilon^5\}, \varepsilon^2 H = \{\varepsilon^2, \varepsilon^6\}, \varepsilon^3 H = \{\varepsilon^3, \varepsilon^7\}.$$

Според правилото за пресмятане на произведенията в мултипликативно записана факторгрупа

$$aH \cdot bH = (ab)H$$

попълваме таблицата на Кейли

$\cdot$	H	εH	$\varepsilon^2 H$	$\varepsilon^3 H$
H	H	εH	$\varepsilon^2 H$	$\varepsilon^3 H$
εH	εH	$\varepsilon^2 H$	$\varepsilon^3 H$	H
$\varepsilon^2 H$	$\varepsilon^2 H$	$\varepsilon^3 H$	H	εH
$\varepsilon^3 H$	$\varepsilon^3 H$	H	εH	$\varepsilon^2 H$

□

Задача 12. *Покажаете, че ако факторгрупата $G/Z(G)$ е циклична, то групата G е абелева.*

Решение. Щом $G/Z(G)$ е циклична, то тя има вида

$$G/Z(G) = \{Z(G), gZ(G), g^2Z(G), \dots, g^nZ(G)\}$$

за някой елемент $g \in G$. Тогава имаме разбиването

$$G = Z(G) \cup gZ(G) \cup g^2Z(G) \cup \dots \cup g^nZ(G).$$

Нека $x, y \in G$ са произволни елементи. Тогава всеки от тях попада в някой от горните съседни класове. Нека $x \in g^kZ(G)$ за $0 \le k \le n$ и $y \in g^lZ(G)$ за $0 \le l \le n$. Това означава, че $x = g^kz_1$ за $z_1 \in Z(G)$ и

$y = g^l z_2$ за $z_2 \in Z(G)$. Тогава от свойствата на центъра на група имаме, че

$$xy = g^k z_1 g^l z_2 = g^k g^l z_1 z_2 = g^{k+l} z_2 z_1 = g^l g^k z_2 z_1 = g^l z_2 g^k z_1 = yx.$$

Последното доказва, че G е абелева. $\square$

Задача 13. *Кои от изображенията*
а) $f : (\mathbb{R}^+, \cdot) \longrightarrow (\mathbb{R}, +)$, *такова че* $f(x) = \ln x$,
б) $g : GL_n(\mathbb{R}) \longrightarrow (\mathbb{R}, +)$, *такова че* $g(A) = \det A$,
в) $h : (\mathbb{C}^*, \cdot) \longrightarrow (\mathbb{R}^*, \cdot)$, *такова че* $h(z) = |z|$
са хомоморфизми на групи?

Решение. а) Според свойствата на логаритмите имаме, че за всеки две положителни реални числа е изпълнено

$$\ln(xy) = \ln(x) + \ln(y).$$

Записано с нашите означения това означава, че

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

за $\forall x, y \in \mathbb{R}^+$, което означава, че f е хомоморфизъм на групи.
б) Отговор: g е хомоморфизъм на групи.
в) Отговор: h е хомоморфизъм на групи. $\square$

Нека $\varphi : G_1 \longrightarrow G_2$ е хомоморвизъм на групи. Множеството

$$\operatorname{Ker} \varphi = \{x \in G_1 \mid \varphi(x) = e_2\},$$

където e_2 е единичният елемент на G_2, се нарича ядро на хомоморфизма φ. Имаме, че $\operatorname{Ker} \varphi \leq G_1$. Нещо повече - съществува взаимно еднозначно съответствие между нормалните подгрупи на G_1 и ядрата на хомоморфизмите, действащи върху G_1, т.е. $\operatorname{Ker} \varphi \trianglelefteq G_1$. Множеството

$$\operatorname{Im} \varphi = \{y \in G_2 \mid \exists x \in G_1 : \varphi(x) = y$$

се нарича образ на хомоморфизма φ. Имаме, че $\operatorname{Im} \varphi \leq G_2$.

Теорема за хомоморфизмите. *Нека G_1 и G_2 са групи, а изображението*

$$\varphi : G_1 \longrightarrow G_2$$

е хомоморфизъм на групи. Тогава

$$G_1 / \operatorname{Ker} \varphi \cong \operatorname{Im} \varphi.$$

Задача 14. *Нека* $H = \{A \in \mathbb{R}_{n\times n} \mid \det A > 0\}$. *Покажете, че* $GL_n(\mathbb{R})/H \cong \mathbb{C}_2$.

Решение. Построяваме изображението

$$\varphi : GL_n(\mathbb{R}) \longrightarrow \mathbb{C}_2$$

по правилото $\varphi(A) = \dfrac{\det A}{|\det A|}$ за $\forall A \in GL_n(\mathbb{R})$. Понеже за всеки две матрици $A, B \in GL_n(\mathbb{R})$ имаме, че

$$\varphi(AB) = \frac{\det(AB)}{|\det(AB)|} = \frac{\det A \det B}{|\det A \det B|} =$$

$$= \frac{\det A \det B}{|\det A||\det B|} = \frac{\det A}{|\det A|} \cdot \frac{\det B}{|\det B|} = \varphi(A)\varphi(B),$$

то изображението φ е хомоморфизъм на групи.

Ще докажем, че $\operatorname{Im}\varphi = \mathbb{C}_2$. Наистина, $1 \in \operatorname{Im}\varphi$, защото матрицата $A = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \ddots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix} \in GL_n(\mathbb{R})$ и $\varphi(A) = \dfrac{1}{|1|} = 1$. Също така $-1 \in \operatorname{Im}\varphi$, защото матрицата $B = \begin{pmatrix} -1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \ddots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix} \in GL_n(\mathbb{R})$ и $\varphi(B) = \dfrac{-1}{|-1|} = -1$. По този начин $\mathbb{C}_2 \subseteq \operatorname{Im}\varphi$. За обратното включване разглеждаме произволна матрица $C \in GL_n(\mathbb{R})$. Тогава $\varphi(C) \in \operatorname{Im}\varphi$ е произволен елемент от образа. Да намерим $\varphi(C)$. Ясно е, че $\det C = \varepsilon|\det C|$, където $\varepsilon = \pm 1$ в зависимост от това дали $\det C > 0$ или $\det C < 0$. Тогава $\varphi(C) = \dfrac{\det C}{|\det C|} = \dfrac{\varepsilon|\det C|}{|\det C|} = \varepsilon = \pm 1$. Следователно $\operatorname{Im}\varphi \subseteq \mathbb{C}_2$ и окончателно $\operatorname{Im}\varphi = \mathbb{C}_2$.

Ще покажем, че $\operatorname{Ker}\varphi = H$. Наистина, нека $A \in \operatorname{Ker}\varphi$. Това означава, че $\varphi(A) = 1$. Разписвайки лявата страна на това равенство получаваме, че

$$\frac{\det A}{|\det A|} = 1,$$

което е еквивалентно на равенството

$$\det A = |\det A|.$$

Понеже $\det A \neq 0$, последното е вярно точно когато $\det A > 0$, т.е. тогава и само тогава, когато $A \in H$. С това $\operatorname{Ker} \varphi \subseteq H$. Обратно, нека $B \in H$ – това означава, че $\det B > 0$. Тогава от дефиницията на абсолютна стойност имаме, че

$$\varphi(B) = \frac{\det B}{|\det B|} = \frac{\det B}{\det B} = 1$$

и $B \in \operatorname{Ker} \varphi$. С това $H \subseteq \operatorname{Ker} \varphi$ и окончателно получаваме, че $\operatorname{Ker} \varphi = H$. От взаимно еднозначното съответстиве между ядрата на хомоморфизмите върху $GL_n(\mathbb{R})$ и нормалните ѝ подгрупи следва, че $H \trianglelefteq GL_n(\mathbb{R})$.

Остава единствено да приложим теоремата за хомоморфизмите. Имаме, че

$$GL_n(\mathbb{R}) / \operatorname{Ker} \varphi \cong \operatorname{Im} \varphi.$$

От равенствата, които доказахме горе следва

$$GL_n(\mathbb{R})/H \cong \mathbb{C}_2,$$

което искахме да покажем. □

Задача 15. *Нека* $H = \{A \in \mathbb{C}_{n\times n} \mid \det A \in \mathbb{R}^{>0}\}$, *а* $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ *е единичната окръжност в комплексната равнина. Покажете, че* $GL_n(\mathbb{C})/H \cong \mathbb{U}$.

Решение. В общия случай, детерминантата на матрица $A \in GL_n(\mathbb{C})$ е ненулево комплексно число. Т.к. всяко комплексно число $a \in \mathbb{C}$ може да се представи във вида

$$a = r(\cos\theta + i\sin\theta),$$

където $r = |a|$, а $\theta \in [0, 2\pi)$ е ъгълът, който радиус вектора на a сключва с реалната ос, то разгледайте изображението

$$f : GL_n(\mathbb{C}) \longrightarrow \mathbb{U},$$

дефинирано с

$$f(A) = \frac{\det A}{|\det A|} \quad \left(= \frac{r(\cos\theta + i\sin\theta)}{r} = \cos\theta + i\sin\theta \in \mathbb{U} \right).$$

Докажете, че f е хомоморфизъм на групи и използвайте вече познатия метод и теоремата за хомоморфизмите, за да решите задачата. □

Задача 16. *В множеството*

$$G = \{(a, b, c) \mid a, b, c \in \mathbb{R}\}$$

е въведена бинарната операция $\circ$ *по правилото*

$$(a_1, b_1, c_1) \circ (a_1, b_2, c_2) = (a_1 + a_2, b_1 + a_1 c_2 + b_2, c_1 + c_2).$$

Докажете, че

а) G *е група относно операцията* $\circ$,

б) $H = \{(0, b, 0) \mid b \in \mathbb{R}\}$ *е нормална подгрупа на* G, *изоморфна на* $(\mathbb{R}, +)$, *а* $G/H \cong (\mathbb{R}^2, +)$, *където* $+$ *е стандартното събиране на наредени двойки реални числа.*

Решение. а) Покажете, че G е група по познатия начин чрез директна проверка на трите аксиоми.

б) Покажете, че $H \leq G$ по познатия вече начин. Първоначално докажете, че $G/H \cong (\mathbb{R}^2, +)$ като построите подходящ хомоморфизъм на групи

$$\varphi : G \longrightarrow (\mathbb{R}^2, +)$$

с образ $\operatorname{Im} \varphi = \mathbb{R}^2$ и ядро $\operatorname{Ker} \varphi = H$. От последното ще следва, че $H \trianglelefteq G$. Накрая постройте подходящ хомоморфизъм на групи

$$\psi : H \longrightarrow \mathbb{R}$$

и директно покажете, че ψ е биекция (т.е. че едновременно е инекция и сюрекция). $\square$