ЛЕКЦИЯ 21
ПОДГРУПИ. ЦИКЛИЧНИ ПОДГРУПИ. РЕД НА ЕЛЕМЕНТ НА ГРУПА.

Определение. *Нека G е група и $H \neq \emptyset$ е подмножество на G. Казваме, че H е подгрупа на групата G, ако са изпълнени следните условия:*

(1) Ако $x, y \in H$, тогава $xy \in H$ $(x + y \in H)$.

(2) Ако $x \in H$, тогава $x^{-1} \in H$ $(-x \in H)$.

Твърдение 1. *Подгрупите наследяват операцията на групата и относно наследената операция също са групи.*

Доказателство:

Операцията се наследява съгласно (1). Ясно е, че наследената операция е асоциативна. От $H \neq \emptyset$ следва, че съществува $h \in H$. Съгласно (2), имаме $h^{-1} \in H$. От (1) следва $hh^{-1} = e \in H$. Следователно H има неутрален елемент. От (2) следва, че всеки елемент от H има обратен елемент също в H. Доказателството, че H е група е завършено.

Примери.

1. Всяка група е подгрупа на себе си. Неутралният елемент сам по себе си също е подгрупа. Тези две подгрупи се наричат несобствени подгрупи.

2. Разглеждаме групата на обратимите квадратни матрици от n-ти ред с елементи от полето F $\mathrm{GL}_n(F)$. В нея множеството

$$\mathrm{SL}_n(F) = \{A \in \mathrm{GL}_n(F) \mid \det(A) = 1\}$$

е подгрупа. Тази подгрупа се нарича *специална линейна група.*

3. В мултипликативната група на полето на комплексните числа, множеството

$$\{z \in \mathbb{C} \mid z^n = 1, \text{ където } n \text{ е фиксирано естествено число}\}$$

е подгрупа. Също множеството

$$\{z \in \mathbb{C} \mid z^n = 1, \text{ за някое естествено число } n\}$$

е подгрупа. Първата от тези подгрупи е крайна, а втората безкрайна (защо?).

4. В адитивната група на целите числа, четните числа образуват подгрупа. По-общо всички числа, които се делят на дадено естествено число n образуват подгрупа, която се бележи с $n\mathbb{Z}$.

Задача. *Да се докаже, че за всяка подгрупа H на адитивната група на $\mathbb{Z}$ съществува неотрицателно цяло число n, такова че $H = n\mathbb{Z}$.*

5. Във всяко линейно пространство подпространствата са подгрупи на неговата адитивна група. В пръстените подпръстените са подгрупи на адитивната група.

6. В мултипликативната група на реалните числа положителните числа образуват подгрупа. Същото е вярно и за мултипликативната група на рационалните числа.

Твърдение 2. *Сечението на произволна фамилия от подгрупи на дадена група също е подгрупа.*

Доказателство:

Същото както за подпространства.

Определение. *Нека G е група и $g \in G$.*

1. *Ако n е естествено число и операцията е мултипликативна, дефинираме*

$$g^n = \underbrace{gg \dots g}_{n}.$$

Елементът g^n се нарича n-та степен на g.

Ако операцията е адитивна дефинираме

$$ng = \underbrace{g + g + \cdots + g}_{n}.$$

Елементът ng се нарича n-то кратно на g.

2. *Ако операцията е мултипликативна нулевата степен на елемента g се дефинира с равенството $g^0 = e$.*

   Ако операцията е адитивна нулевото кратно на елемента g се дефинира с равенството $0g = o$ (нулевият елемент на G).

3. *Нека n е цяло отрицателно число и $n = -n'$.*

   Ако операцията е мултипликативна n-тата степен на елемента g се дефинира чрез равенството

$$g^n = \underbrace{g^{-1}g^{-1}\dots g^{-1}}_{n'}.$$

   Ако операцията е адитивна, n-тото кратно на g дефинираме чрез равенството

$$ng = \underbrace{(-g) + (-g) + \dots + (-g)}_{n'}.$$

Забележка. *Понеже произведението (сумата) на краен брой елементи не зависи от начина, по който са поставени скобите, степените (кратното) на елементите са дефинирани коректно*

Твърдение 3. *Нека G е мултипликативна група и $a \in G$. Тогава е вярно равенството*

$$a^n a^m = a^{n+m}, \quad \forall n, m \in \mathbb{Z}. \tag{*}$$

Доказателство:

Ако $m = 0$ или $n = 0$ равенството (*) е очевидно. Поради това ще предполагаме, че $m \neq 0$ и $n \neq 0$ и ще разгледаме останалите възможни ситуации както следва.

Случай 1 $m > 0$ и $n > 0$. Имаме

$$a^m a^n = \underbrace{aa\dots a}_{m}\underbrace{aa\dots a}_{n} = \underbrace{aa\dots a}_{m+n} = a^{m+n}.$$

Случай 2 $m > 0$ и $n < 0$. Полагаме $n' = -n$. Тогава

$$a^m a^n = \underbrace{aa\dots a}_{m}\underbrace{a^{-1}a^{-1}\dots a^{-1}}_{n'}. \tag{**}$$

Ако $m > n'$ тогава от (**) следва

$$a^m a^n = \underbrace{aa\ldots a}_{m-n'} = a^{m-n'} = a^{m+n}.$$

Ако $m = n'$ тогава в дясната част на (**) всичките множители се съкращават и получаваме

$$a^m a^n = e = a^0 = a^{m+n}.$$

Ако $m < n'$ тогава от (**) получаваме

$$a^m a^n = \underbrace{a^{-1}a^{-1}\ldots a^{-1}}_{n'-m} = (a^{-1})^{n'-m} = a^{m-n'} = a^{m+n}.$$

Случай 3 $m < 0$ и $n > 0$. Да се направи самостоятелно.

Случаи 4 $m < 0$ и $n < 0$. Нека $m' = -m$ и $n' = -n$. Тогава

$$a^m a^n = \underbrace{a^{-1}a^{-1}\ldots a^{-1}}_{m'}\underbrace{a^{-1}a^{-1}\ldots a^{-1}}_{n'} = \underbrace{a^{-1}a^{-1}\ldots a^{-1}}_{m'+n'} =$$
$$(a^{-1})^{m'+n'} = a^{-(m'+n')} = a^{m+n}.$$

Твърдението е доказано.

В адитивен вариант равенството (*) има вида

$$(m+n)a = ma + na, \quad \forall n, m \in \mathbb{Z}.$$

Задача. *Да се провери, че във всяка мултипликативна група е вярно равенството*

$$(a^n)^m = a^{nm}, \quad \forall n, m \in \mathbb{Z}.$$

(в адитивен вариант това равенство е $m(na) = (mn)a$, $\forall n$, $m \in \mathbb{Z}$).

Определение. *Нека G е мултипликативна група и $g \in G$. Дефинираме*

$$\langle g \rangle = \{h \in G \mid \exists n \in \mathbb{Z} \text{ такова, че } h = g^n\}.$$

Забележка. *По принцип равенството*

$$\langle g\rangle = \{e = g^0, g^{\pm 1}, \dots, g^{\pm k}, \dots\}$$

не е вярно тъй като отдясно може да има повторения (в групите е възможно две различни степени на даден елемент да са равни). Ако всеки две цели степени на елемента g обаче са различни, тогава това равенство е вярно.

При адитивна група имаме

$$\langle g\rangle = \{h \in G \mid \exists n \in \mathbb{Z} \text{ такова, че } h = ng\}.$$

Твърдение 4. *Нека G е група и $g \in G$. Тогава подмножеството $\langle g\rangle$ е подгрупа на G.*

Доказателство:

Нека h, $t \in \langle g\rangle$. Тогава $h = g^m$ и $t = g^n$ и съгласно равенството (*) $ht = g^{m+n}$. Следователно $ht \in \langle g\rangle$. Също от (*) имаме $g^{-m}h = hg^{-m} = e$, поради това $h^{-1} = g^{-m} \in \langle g\rangle$.

Подгрупата $\langle g\rangle$ се нарича циклична подгрупа на групата G породена от елемента g.

Тъй като $g^n g^m = g^{n+m}$ и $g^m g^n = g^{m+n}$, имаме че

$$g^n g^m = g^m g^n, \quad \forall n, m \in \mathbb{Z}.$$

Следователно $\langle g\rangle$ е комутативна подгрупа.

Определение. *Казваме, че групата G е циклична, ако съществува елемент $g \in G$, такъв че $\langle g\rangle = G$.*

Примери.

1. Адитивната група на $\mathbb{Z}$ е циклична, защото $\mathbb{Z} = \langle 1\rangle$.
2. Мултипликативната група $\mathbb{C}_n = \{z \in \mathbb{C} \mid z^n = 1\}$ е циклична, защото
$$\mathbb{C}_n = \left\langle \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \right\rangle.$$

Определение. *Нека G е мултипликативна група и $g \in G$. Казваме, че елементът g има краен ред, ако съществува естествено число n, такова че $g^n = e$. Най-малкото естествено число n, за което $g^n = e$ се нарича ред на елемента g и се бележи $|g|$. Ако $g^n \neq e$ за всяко естествено число n, казваме че g има безкраен ред и пишем $|g| = \infty$.*

Забележка. *При адитивна операция, това че елементът g има краен ред равен на k означава, че $kg = 0$ и $sg \neq 0$ при $0 < s < k$. Елементът g има безкраен ред, ако $ng \neq 0$ за всяко естествено число n.*

Примери.

1. Нека $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in S_4$. Тогава $\varphi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, $\varphi^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ и $\varphi^4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$. Следователно $|\varphi| = 4$.
2. В адитивната група на целите числа, всяко ненулево число има безкраен ред.

Твърдение 5. *Нека G е група, $g \in G$ и $|g| = k < \infty$. Тогава е вярно равенството*

$$\langle g \rangle = \{g^0 = e, g, g^2, \ldots, g^{k-1}\}.$$

Поради това редът на цикличната подгрупа $\langle g \rangle$ е равен на реда на g.

Доказателство:

Да припомним, че равенството $|g| = k$ означава, че

$$g^k = e \text{ и } g^s \neq e, \quad o < s < k. \tag{\#}$$

Нека $h \in \langle g \rangle$, т. е. $h = g^n$. Ако $n = kq + r$, $0 \leq r < k$, тогава

$$h = g^n = g^{kq+r} = (g^k)^q g^r = g^r.$$

Тъй като $0 \leqq r < k$ доказахме, че

$$\langle g \rangle \subseteq \{e = g^0, g, g^2, \ldots, g^{k-1}\}.$$

За да докажем, че в това включване имаме равенство, трябва да проверим, че в дясната част няма повторения. Да допуснем противното и нека $g^n = g^m$, $n > m$, $0 \leq m < k$, $0 \leq n < k$. Тогава получаваме, че $g^{n-m} = e$. Понеже $o < n - m < k$ това противоречи на (#). Полученото противоречие доказва Твърдение 5.

Твърдение 6. *Нека G е мултипликативна група и $g \in G$. Ако $|g| = \infty$, тогава всеки две цели степени на елемента g са различни и следователно в тази ситуация е вярно равенството*

$$\langle g \rangle = \{e = g^0, g^{\pm 1}, \ldots, g^{\pm k}, \ldots\}.$$

Доказателство:

Да допуснем противното, т. е. $g^n = g^m$ и $n > m$. Тогава $g^{n-m} = e$, което е противоречие.