Групи

Определение.
Нека $G \neq \emptyset$ е множество, в което е зададена бинарна операция. Казваме, че относно тази операция G е група ако са изпълнени слидните условия:

(1) операцията е асоциативна, т.е. G е полугрупа;

(2) съществува неутрален елемент:
При мултипликативна операция това означава, че $\exists\, e \in G$ такъв, че $eg = ge = g$.
При адитивна операция това означава, че $\exists\, o \in G$, тъкъв че $o + g = g + o = g$.

(3) всеки елемент на G е обратим:
При мултипликативна операция това означава, че за всеки елемент $g \in G$ съществува $g^{=1} \in G$, тъкъв че $gg^{-1} = g^{-1}g = e$.
При адитивна операция това означава, че за всеки елемент $g \in G$ съществува $-g \in G$, тъкъв че $g + (-g) = (-g) + g = o$.

Ако операциятя е комутативна тогава групата се нарича комутативна или абелева. Броят на елементите на дадена група (или нейната мощност) се нарича *ред* на групата G и се бележи с $|G|$.

Примери:

1) Относно събирането линейните пространства и пръстените са абелеви групи.
2) Ненулевите елементи на всяко поле относно умножението образуват абелева група. Тази група се нарича мултипликативна група на полето.
3) Обратимите квадратни матрици от даден ред над полето F относно умножението образуват група, която се нача пълна линейна група и се бележи с $GL_n(F)$. Тази група не е абелева.
4) В Z числата 1 с –1 относно умножението образуват група от два елемента.

Непосредствени следствия от аксиомите на група

Следствие 1.
Единственост на неутралния елемент.

Следствие 2.
Единственост на обратния елемент.

Следствие 3.
Произведението(сумата) на краен брой елемнти не зависи от начина, по който са поставени скобите.

Следствие 4.
Вярно е равенството

$$(a_1 a_2 .....a_k)^{-1} = a_k{}^{-1} .....a_2{}^{-1} a_1{}^{-1}.$$

Следствие 5.
От $ax = ay$ *или* $xa = ya$ *следва* $x = y$.

Следствие 6.
$(a^{-1})^{-1} = a$.

Симетрична група на дадено множество

Нека $\Omega \neq \varnothing$ е дадено множество. Разглеждаме полугрупата $M(\Omega)$ на всичките изображения на Ω в Ω. Множеството на всичките 1-1 изображения от $M(\Omega)$ означаваме със $S(\Omega)$.

Твърдение.
$S(\Omega)$ *наследява операцията на* $M(\Omega)$ *и относно наследената операция е група.*

Доказателство:
Нека $\varphi, \psi \in S(\Omega)$. Тогава

$$\varphi(\Omega) = \Omega \quad \text{и} \quad \psi(\Omega) = \Omega .$$

Следователно $\varphi\psi(\Omega) = \varphi(\Omega) = \Omega$, т.е. $\varphi\psi$ е изображение "върху".
Нека $u, v \in \Omega$ и $u \neq v$. Тогава $\psi(u) \neq \psi(v)$. Следователно $\varphi(\psi(u)) \neq \varphi(\psi(v))$, т.е. $\varphi\psi$ изобразява различните елементи в различни. Доказанме, че $\varphi\psi \in S(\Omega)$, което означава че $S(\Omega)$ наследява операцията на $M(\Omega)$. Очевидно е, че тъждесвиното изображение $\varepsilon(x) = x, \forall x \in \Omega$ е неутрален елемент на тази операция в $S(\Omega)$. Ако $\varphi \in S(\Omega)$ и $\varphi(x) = x'$, тогава дефинираме

$$\varphi^{-1}(x') = x .$$

Понеже $\varphi \in S(\Omega)$, изображението φ^{-1} е дефинирано коректно и $\varphi^{-1} \in S(\Omega)$. Ясно е, че

$$\varphi\varphi^{-1} = \varphi^{-1}\varphi = \varepsilon .$$

С това проверката, че $S(\Omega)$ е група е завършена.□

Определение.
Групата $S(\Omega)$ *се нарича симетрична група на множеството* Ω.

Нека да разгледаме специалната ситуация, когато $\Omega = \{1, 2, ..., n\}$. В тази ситуация групата $S(\Omega)$ се нарича симетрична група от n-та степен и се бележи с S_n. Полугрупата $M(\Omega)$ се нарича симетрична полугрупа от n-та степен и се бележи с M_n.

Нека $\varphi \in M_n$ и $\varphi(1) = i_1, \varphi(2) = i_2, ..., \varphi(n) = i_n$. Тогава изображението φ ще записваме пос ледния начин

$$\varphi = \begin{pmatrix} 1 & 2 & ..... & n \\ i_1 & i_2 & ..... & i_n \end{pmatrix}.$$

При това представяне на φ очевидно е вядно, че

$$\varphi \in S(\Omega) \Leftrightarrow \begin{pmatrix} i_1 & i_2 & ..... & i_n \end{pmatrix} \text{ е пермутация на числата от 1 до } n.$$

Следователно броят на елементите на групата S_n е равен на $n!$.

Подгрупи

Определение.
Нека G е група и $H \neq \varnothing$ е подмножество но 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.
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 $H \neq \varnothing \Rightarrow \exists h \in H$. 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 подгрупата $GL_n(F)$. В нея множеството

$$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1\}$$

е подгрупа. Тази подгрупа се нарича специална линейна група.

3) В мултипликативната група на полето на комплексните числа. Множеството

$$\{z \in C \mid z^n = 1, \textit{за } n \textit{ фиксирано естествено число}\}$$

е подгрупа. Също множеството

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

е подгрупа.

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 nZ.
5) Във всяко линеино пространство подпространствата са подгрупи на неговата адитивна група.

Твърдение.
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*

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

Елементът g^n се нарича n-та степен на g.
Ако операцията е адитивна дефинираме

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

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 $og = 0$ (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

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

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

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

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

$$a^n a^m = a^{n+m},\ \forall n,m \in Z. \qquad (*)$$

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

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

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

$$a^m a^n = \underbrace{aa.....a}_{m}\ \underbrace{a^{-1}a^{-1}.....a^{-1}}_{n'}. \qquad (**)$$

Ако $m > n'$ тогава от (**) следва

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

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

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

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

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

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

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

Твърдението е доказано.□

В адитивен вариант равенството (*) има вида

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

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

$$(g^n)^m = g^{nm}, \ \forall n, m \in Z$$

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

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

$$< g >= \{h \in G \mid \exists\, n \in Z \text{ такова, че } h = g^n\}.$$

Забележка. *По принцип равенството*

$$< g >= \{e = g^0, g^{\pm 1}, ..., g^{\pm k}, ...\}$$

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

$$< g >= \{h \in G \mid \exists\, n \in Z \text{ такова, че } h = ng\}.$$

твърдение.
Нека G е група. За всеки елемент g принадлежащ на G имаме подмножеството $< g >$ е подгрупа на G.

Д-во:

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

Подгрупата $< g >$ се нарича циклична подгрупа на групата G породена от елемента g.
Тъй като $g^n g^m = g^{n+m}$ и $g^m g^n = g^{n+m}$, имаме че

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

Следователно $< g >$ е комутативна подгрупа.

Определение.
Казваме, че групата G е циклична, ако $\exists\, g \in G$, такъв че $< g > = G$.

Примери:

1. Адитивната група на Z е циклична, защото $Z = < 1 >$.
2. Мултипликативната група $C_n = \{z \in \mathbb{C} \mid z^n = 1\}$ е циклична, защото

$$C_n = < \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} > .$$

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 ред равен на k означава, че $kg = 0$ и $sg \neq 0$ при $0 < s < k$.

Твърдение.
Нека G е група $g \in G$ е $|g| < \infty$. Тогава редът на цикличната подгрупа $|< g >|$ е равен на реда $|g|$ на елемента g.

Доказателство:
Ще предполагаме, че групата G е мултипликативна. Нека $|g| = k$, тогава

$$g^k = e \quad \text{и} \quad g^s \neq e, \quad 0 < s < k. \qquad (\#)$$

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

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

Тъй като $0 \leq r < k$ доказахме, че

$$< g > \subseteq \{e = g^o, g, ..., g^{k-1}\}.$$

За да докажем, че е вярно равенството

$$< g > = \{e = g^o, g, ..., g^{k-1}\} \qquad (\#\#)$$

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

Твърдение.
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

$$< g > = \{e = g^0, g^{\pm 1}, ..., g^{\pm k}, ...\}.$$

Доказателство:

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