ПРАКТИЧЕСКИЕ ЗАНЯТИЯ №8–9

Тема занятий. Полугруппы. Моноиды. Группы. Подгруппы. Циклические группы.

I. Бинарные алгебраические операции. Пусть X – произвольное множество. Бинарной алгебраической операцией (или законом композиции) на X называется отображение $\tau : X \times X \to X$. Таким образом, любой упорядоченной паре $\langle a, b \rangle \in X^2$ ставится в соответствие однозначно определённый элемент $\tau(a, b) \in X$. Вместо $\tau(a, b)$ часто пишут $a \tau b$, и при этом бинарную операцию τ часто обозначают каким-нибудь символом из $*$, $\circ$, $\cdot$, $+$. Будем, кроме того, писать ab без всякого значка. Пусть $*$ – бинарная операция на X, тогда говорят, что $*$ определяет на X алгебраическую структуру, или, что $(X, *)$ – алгебраическая система.

Примеры. 1. Пусть $X = \mathbb{Z}$ (множество целых чисел). Тогда $+$ (сложение чисел), $\cdot$ (умножение чисел), $-$ (вычитание чисел) – бинарные операции на $\mathbb{Z}$, так как эти операции не выводят из класса целых чисел.

2. Более экзотические примеры бинарных операций на $\mathbb{Z}$:

а) $x \circ y = xy + x + y$,

б) $x \circ y = -x - y$,

в) $x \circ y = x$,

г) $x \circ y = y$.

3. С другой стороны операция

$x \circ y = \sqrt{x + y}$

не является бинарной операцией на $\mathbb{Z}$, так как эта операция выводит из класса целых чисел: $1 \circ 2 = \sqrt{3} \notin \mathbb{Z}$. Введённая операция является бинарной операцией на $\mathbb{R}_{\geq} = \{t \in \mathbb{R} \mid t \geq 0\}$.

II. Полугруппы. Моноиды. Бинарная операция $*$ на X называется ассоциативной, если $(a * b) * c = a * (b * c)$ для всех $a, b, c \in X$; она называется коммутативной, если $a * b = b * a$ для всех $a, b \in X$. Те же названия присваиваются и алгебраической системе $(X, *)$. Множество X с заданной на нём ассоциативной бинарной операцией называется полугруппой.

Пример 4. Бинарная операция $\circ$ на множестве $\mathbb{Z}$ в случаях а), б) из примера 2 является коммутативной, а в случаях а), в), г) – ассоциативной. При этом в случае б) имеем коммутативную, но не являющуюся ассоциативной

бинарную операцию на $\mathbb{Z}$, а в случаях в), г) - ассоциативные, но не являющиеся коммутативными бинарные операции на $\mathbb{Z}$, откуда следует независимость этих понятий. Покажем, что операция $\circ$ из б) не является ассоциативной

$$(1\circ 2)\circ 3 = -(-1-2)-3 = 0 \neq 4 = -1-(-2-3) = 1\circ(2\circ 3).$$

Покажем, что операция $\circ$ из в) не является коммутативной

$$1\circ 2 = 1 \neq 2 = 2\circ 1 .$$

Покажем ассоциативность операции $\circ$ из а)

$$(x\circ y)\circ z = (xy+x+y)z + (xy+x+y) + z = \underline{xyz+xy+xz+yz+x+y+z},$$
$$x\circ(y\circ z) = x(yz+y+z) + x + (yz+y+z) = \underline{xyz+xy+xz+yz+x+y+z} .$$

Покажем ассоциативность операции $\circ$ из в)

$$(x\circ y)\circ z = x\circ y = x = x\circ(y\circ z).$$

Пример 5. Пусть $X = \mathbb{Z}$. Тогда $(X , \circ)$, где а) $x\circ y = x + y$, б) $x\circ y = xy$, в) $x\circ y = xy + x + y$, г) $x\circ y = x$, д) $x\circ y = y$ - полугруппы.

Пример 6. Пусть $X = \{0 ; 1\}$. Тогда $(X , \&)$, $(X , \vee)$, $(X , \sim)$, $(X , + \pmod 2)$ - полугруппы.

Элемент $e \in X$ называется единичным (нейтральным) относительно рассматриваемой бинарной операции $*$, если $e * x = x * e = x$ для всех элементов $x \in X$. Если e' - ещё один единичный элемент, то $e' = e' * e = e \Rightarrow e$ - единственный.

Полугруппу с единичным элементом e принято называть моноидом.

Задача 1. Показать, что а) $(\{0 ; 1\} , \&)$, б) $(\{0 ; 1\} , \vee)$, в) $(\{0 ; 1\} , \sim)$, г) $(\{0 ; 1\} , +)$ - моноиды. Найти единичные элементы в указанных моноидах.

Решение. а) $\forall x \in \{0 ; 1\}$ выполняется $1 \& x = x \& 1 = x \Rightarrow 1$ - единичный элемент, следовательно, $(\{0 ; 1\} , \&)$ - моноид.

б) $\forall x \in \{0 ; 1\}$ выполняется $0 \vee x = x \vee 0 = x \Rightarrow 0$ - единичный элемент, следовательно, $(\{0 ; 1\} , \vee)$ - моноид.

в) $\forall x \in \{0 ; 1\}$ выполняется $1 \sim x = x \sim 1 = x \Rightarrow 1$ - единичный элемент, следовательно, $(\{0 ; 1\} , \sim)$ - моноид.

г) $\forall x \in \{0 ; 1\}$ выполняется $0 + x = x + 0 = x \Rightarrow 0$ - единичный элемент, следовательно, $(\{0 ; 1\} , +)$ - моноид.

Задача 2. Показать, что $(\mathbb{Z}, \circ)$, где $x \circ y = xy + x + y$ – моноид. Найти единичный элемент в этом моноиде.

Решение. $\forall x \in \mathbb{Z}$ имеем

$$x \circ 0 = 0 \circ x = x \quad (x \cdot 0 + x + 0 = 0 \cdot x + 0 + x = x),$$

откуда 0 – единичный элемент.

Задача 3. Является ли полугруппа $(\mathbb{Z}, \circ)$, где $x \circ y = x$ моноидом?

Решение. Предположим, что в этой полугруппе существует единичный элемент e, т.е. удовлетворяющий условию $e \circ x = x \circ e = x \quad \forall x \in \mathbb{Z}$. Тогда

$$e = e \circ x = x \quad \forall x \in \mathbb{Z},$$

а следовательно, множество $\mathbb{Z}$ состоит из единственного элемента e. Полученное противоречие показывает, что указанная полугруппа не является моноидом.

Моноиды принято обозначать тройками $(M, *, e)$, где M – множество элементов моноида, $*$ – бинарная операция на M, e – единичный элемент на M относительно $*$. В случае, когда бинарная операция в моноиде обозначается через $+$, такой моноид называется аддитивным (в силу выбора обозначения $+$) и в этом случае единичный элемент обычно обозначается через 0. В случае же, когда бинарная операция в моноиде обозначается через $\cdot$, такой моноид называется мультипликативным и при этом единичный элемент обычно обозначается черех e. Аддитивная запись используется преимущественно в коммутативных моноидах.

Если бинарная операция $\cdot$ на X ассоциативна, то результат её последовательного применения к n элементам множества X не зависит от расстановки скобок. Поэтому можно вводить символы $\prod_{i=1}^{n} x_i$, $x^n = \underbrace{x \ldots x}_{n \text{ раз}}$. Очевидно, что

$$(1) \quad (x^m)^n = x^{mn}, \quad x^m x^n = x^{m+n}$$

для всех $m, n > 0$. Кроме того, в случае существования единичного элемента e обычно полагают $x^0 = e$. При таком обозначении (1) будет справедливо и для всех $m, n \geqslant 0$.

Если используется обозначение $+$ для бинарной ассоциативной операции на X, то совершенно аналогично предыдущему можно использовать символы $\sum_{i=1}^{n} x_i$, $nx = \underbrace{x + \ldots + x}_{n \text{ раз}}$. При этом аналогично (1) при всех $m, n > 0$ выполняется

(2) $n(mx) = (nm)x$, $mx + nx = (m+n)x$.

В случае существования единичного элемента 0 обычно по определению полагают $0x = 0$ (следует различать $0 \in \mathbb{Z}$ слева от $0 \in X$ справа). При таком обозначении, очевидно, (2) сохраняет силу и для всех $m, n \geqslant 0$.

IУ. Обратимые элементы. Элемент a моноида $(M, \cdot, e)$ называется обратимым, если существует элемент $b \in M$ такой, что

(3) $ab = e = ba$.

Понятно, что элемент b тоже тогда будет обратимым. Кроме того, если $ab' = e = b'a$, то

$$b' = eb' = (ba)b' = b(ab') = be = b,$$

т.е. элемент b определяется из (3) единственным образом. Это даёт основание говорить о единственном обратном элементе для a, который обозначается a^{-1}. Очевидно, что $(a^{-1})^{-1} = a$.

Задача 4. Доказать, что если x,y - обратимы, то xy - обратим и $(xy)^{-1} = y^{-1}x^{-1}$.

Решение. Имеем

$$(xy)(y^{-1}x^{-1}) = ((xy)y^{-1})x^{-1} = (x(yy^{-1}))x^{-1} = (xe)x^{-1} = xx^{-1} = e.$$

Аналогично и наоборот $(y^{-1}x^{-1})(xy) = e$.

Задача 5. Найти все обратимые элементы в моноиде $(\mathbb{Z}, \circ, 0)$, где $x \circ y = xy + x + y$ (см. задачу 2).

Решение. Имеем

$$x \circ y = y \circ x = 0 \Leftrightarrow xy + x + y = 0 \Leftrightarrow y(x+1) = -x,$$

откуда при $x \neq -1$ (очевидно, что элемент -1 необратим, так как при $x = -1$ уравнение $y(x+1) = -x$ переходит в $y0 = -1$, которое не имеет решений) получаем

(4) $$y = -\frac{x}{x+1}.$$

Из условия $y \in \mathbb{Z}$ следует, что знаменатель $x + 1$ (в правой части равенства (4)) может принимать лишь значения ± 1, откуда $x = 0$, либо $x = -2$. При этом, соответственно, $y = 0$, либо $y = -2$. Таким образом, обратимыми элементами являются 0, -2, причём обратные к этим элементам совпадают с самими элементами, т.е.

$$0^{-1} = 0 \ , \ (-2)^{-1} = -2 \ .$$

Задача 6. Найти все обратимые элементы в моноидах а) $(\{0;1\}, \&)$, б) $(\{0;1\}, \vee)$, в) $(\{0;1\}, \sim)$, г) $(\{0;1\}, +)$.

Решение. а) В этом случае единичным элементом является 1 (см. задачу 1). Единичный элемент всегда имеет обратный, совпадающий с ним самим. Элемент 0 необратим, так как $0 \& x = 0 \quad \forall x \in \{0;1\}$, а следовательно, ни при каком x не может быть $0 \& x = 1$.

б) В этом случае единичным элементом является 0 (см. задачу 1), следовательно, этот элемент обратим. Элемент 1 необратим, так как $1 \vee x = 1 \quad \forall x \in \{0;1\}$, а следовательно, ни при каком $x \in \{0;1\}$ не может быть $1 \vee x = 0$.

в) В этом случае единичным элементом является 1 (см. задачу 1), следовательно, этот элемент обратим. Обратным к 0 является 0, так как $0 \sim 0 = 1$.

г) В этом случае единичным элементом является 0 (см. задачу 1), следовательно, этот элемент обратим. Обратным к 1 является 1, так как $1 + 1 = 0$.

Задача 7. Показать, что всякий двухэлементный моноид $M = \{a, b\}$ является коммутативным.

Решение. Пусть для определённости a - единичный элемент. Тогда $ab = ba = b$, откуда и следует, что M - коммутативный моноид.

Задача 8. Определить количество попарно различных моноидов с двумя элементами a, b.

Решение. Во-первых, можно двумя способами указать единичный элемент. Пусть, например, a - единичный элемент. Тогда

$$aa = a, \quad ab = b, \quad ba = b$$

и остаётся неопределённым лишь результат bb. Возможны два случая: $bb = b$, $bb = a$. В обоих случаях бинарная операция на $\{a, b\}$ оказывается полностью заданной и как нетрудно видеть в каждом из этих случаев она является ассоциативной. Таким образом, существуют ровно два моноида в случае, когда единичным элементом является a и, очевидно, столько же, когда единичным элементом является b, итого четыре моноида.

У. Группы. Моноид G, все элементы которого обратимы, называется группой. Таким образом, группа удовлетворяет следующим условиям:

$(G1)$ На G определена бинарная операция: $(x, y) \mapsto xy$.

$(G2)$ Эта операция ассоциативна: $(xy)z = x(yz)$ для всех $x, y, z \in G$.

(G3) G обладает единичным элементом e : $xe=ex=x$ для всех $x \in G$.

(G4) Для каждого элемента $x \in G$ существует обратный x^{-1}, удовлетворяющий условию $xx^{-1} = x^{-1}x = e$.

Группа с коммутативной бинарной операцией называется абелевой.

Подмножество $H \subset G$ называется подгруппой в G, если $e \in H$; $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$; $h \in H \Rightarrow h^{-1} \in H$. Подгруппа $H \subset G$ называется собственной, если $H \neq \{e\}$, $H \neq G$.

Число элементов конечной группы G называется её порядком.

Задача 9. Привести примеры групп на $\{0 ; 1\}$.

Указание. См. задачу 6, в), г).

Задача 10. Определить количество попарно различных групп с двумя элементами a, b.

Решение. Можно двумя способами указать единичный элемент. Пусть, например, a - единичный элемент, откуда $aa = a$, $ab = b$, $ba = b$ и остаётся неопределённым лишь результат bb. Заметим, что элемент a не может быть обратным к b, так как $ab = b \neq a$, а следовательно, обратным к b является элемент b, откуда $bb = a$. Таким образом существует единственная группа с заданным единичным элементом a, и, очевидно, единственная группа с заданным элементом b, итого две группы (непосредственной проверкой нетрудно убедиться, что указанные две алгебраические системы являются группами).

Задача 11. Доказать, что любая группа G порядка 3 является коммутативной.

Решение. Пусть $G = \{a, b, c\}$ и для определённости a - единичный элемент. Тогда $ab = ba$, $ac = ca$. Осталось доказать, что $bc = cb$. ~~Очевидно, что $bc \neq b$~~. Очевидно, что $bc \neq b$, так как в случае $bc = b$ имеем $b^{-1}bc = b^{-1}b = a$, откуда $c = a$. Совершенно аналогично получаем $bc \neq c$. Таким образом, остаётся единственная возможность $bc = a$, а следовательно, $b^{-1} = c$, откуда $cb = a = bc$.

Задача 12. Доказать, что любая группа G порядка 4 является коммутативной.

Решение. Пусть $G = \{a, b, c, d\}$ и для определённости a - единич-

ный элемент. Предположим, что группа G не является коммутативной. Пусть для определённости выполняется $bc \neq cb$. Заметим, что $bc \neq b$, $bc \neq c$, а следовательно, $bc \in \{a, d\}$, аналогично $cb \in \{a, d\}$. Пусть для определённости $bc = a$, $cb = d$. Из $bc = a$ следует, что $b^{-1} = c$, откуда $cb = a$, а это противоречит равенству $cb = d$.

Задача I3. Определить количество попарно различных групп с тремя элементами a, b, c.

Решение. Можно тремя способами указать единичный элемент. Пусть, например, a - единичный элемент, откуда $aa = a, ab = b, ac = c$, $ba = b$, $ca = c$ и остаются неопределёнными результаты bb, bc, cb, cc. Очевидно, что $bc \neq b$, $bc \neq c$, откуда $bc = a$. Совершенно аналогично получаем $cb = a$. В силу $b \neq a$ имеем $bb \neq b$, а, используя $b \neq c$, получаем $bb \neq bc = a$, откуда $bb = c$. Аналогично имеем $cc = b$. Таким образом, бинарная операция полностью определена и при этом получаемая в результате алгебраическая система является группой (это доказывается непосредственной проверкой), а следовательно, существует ровно одна группа в случае, когда a - единичный элемент и, очевидно, столько же в случаях, когда единичными элементами являются элементы b, c, итого три группы.

Задача I4. Для любого целого числа $k \geq 2$ привести пример группы порядка k.

Решение. Рассмотрим алгебраическую систему

$$(\{0, 1, \ldots, k-1\}, +(\mathrm{mod}\, k)).$$

Очевидно, что $+(\mathrm{mod}\, k)$ - бинарная операция на $\{0, 1, \ldots, k-1\}$. Эта операция ассоциативна. Единичным элементом является 0. Для каждого числа $i \in \{1, 2, \ldots, k-1\}$ обратным к i является $k - i$. Таким образом, приведённая алгебраическая система удовлетворяет всем свойствам группы.

Задача I5. Доказать, что если $a^2 = e$ для любого элемента a группы G, то эта группа абелева.

Решение. Из условия $a^2 = e$ $\forall a \in G$ имеем $a^{-1} = a$ $\forall a \in G$, откуда $ba = b^{-1}a^{-1} = (ab)^{-1} = ab$ для любых $a, b \in G$, а следовательно, группа G абелева.

Задача I6. Доказать, что множество G, на котором определена ассоци-

ативная бинарная операция и каждое из уравнений $ax = b$, $ya = b$ для любых a и b из G имеет в G не более одного решения, будет группой.

Решение. По условиям для любого элемента $a \in G$ имеем

$$(5)\qquad \begin{aligned} ax_1 &= ax_2 \Rightarrow x_1 = x_2, \\ y_1 a &= y_2 a \Rightarrow y_1 = y_2. \end{aligned}$$

I. Рассмотрим для каждого элемента $a \in G$ элементы $e_a^{\text{л}}$, $e_a^{\text{п}}$, удовлетворяющие равенствам $a e_a^{\text{п}} = a$, $e_a^{\text{л}} a = a$. По условиям задачи такие элементы могут быть определены для каждого $a \in G$ и при том единственным образом. Покажем, что $e_a^{\text{л}} = e_a^{\text{п}}$. Используя (5), имеем

$$(a e_a^{\text{п}})a = aa = a(e_a^{\text{л}} a) = (a e_a^{\text{л}})a \Rightarrow a e_a^{\text{п}} = a e_a^{\text{л}} \Rightarrow e_a^{\text{п}} = e_a^{\text{л}}.$$

В дальнейшем уже обозначаем $e_a = e_a^{\text{л}} = e_a^{\text{п}}$.

2. Покажем теперь, что для любых $a, b \in G$ выполняется $e_a = e_b$. Используя (5), имеем

$$a e_a b = ab = a\, e_b\, b \Rightarrow a e_a = a e_b \Rightarrow e_a = e_b.$$

Таким образом, показано существование элемента $e \in G$ такого, что $e = e_a$ для всякого $a \in G$, откуда $ae = ea = a$ для любого $a \in G$, а следовательно, e – единичный элемент и при этом G – моноид.

3. Покажем, что для всякого элемента $a \in G$ выполняется

$$ax = e,\ ya = e \Rightarrow x = y.$$

Действительно, используя (5), имеем

$$axa = ea = a = ae = aya \Rightarrow ax = ay \Rightarrow x = y.$$

Таким образом, для каждого элемента $a \in G$ существует единственный элемент $x \in G$, удовлетворяющий условиям $ax = xa = e$, т.е. x – обратный к a. Но моноид, в котором для каждого элемента существует обратный, является группой.

УI. Системы образующих. Для любого непустого подмножества S группы G всегда можно указать минимальную подгруппу $H \subseteq G$, содержащую S (т.е. всякая другая подгруппа $H' \subset G$, содержащая S, содержит и H). Такую подгруппу будем обозначать через $\langle S \rangle$. Очевидно, что

$$\langle S\rangle = \bigcap_{S\subseteq H} H .$$

Будем называть $\langle S\rangle$ подгруппой, порождённой множеством S, а S - множеством образующих подгруппы $\langle S\rangle$. Нетрудно показать, что подгруппа $\langle S\rangle$ совпадает с множеством T, состоящим из единичного элемента e и всевозможных произведений

$$t_1 t_2 \cdots t_n , \quad n=1,2,\dots ,$$

где либо $t_i \in S$, либо $t_i^{-1} \in S$, $1 \le i \le n$.

Если множество S состоит из одного элемента, т.е. $S = \{g\}$, где $g \in G$, то подгруппа $\langle g\rangle$ называется циклической.

Будем в дальнейшем под x^{-k} понимать $\left(x^{-1}\right)^k$. Тогда, как нетрудно видеть, в мультипликативной группе G $\forall m,n \in \mathbb{Z}$ выполняется (1). Соответственно, будем в аддитивной группе G через $-x$ обозначать элемент, обратный к $x \in G$ и под $-kx$ будем понимать $k(-x)$. Тогда, как нетрудно видеть, $\forall m,n \in \mathbb{Z}$ справедливо (2).

Из сказанного следует, что любая циклическая группа $\langle a\rangle$ с образующей a является абелевой группой вида $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$ - в случае мультипликативной формы записи бинарной операции, или, соответственно, $\langle a\rangle = \{na \mid n \in \mathbb{Z}\}$ - в случае аддитивной формы записи бинарной операции.

Действительно, в мультипликативной группе G любой элемент $g \in \langle a\rangle$, отличный от $e = a^0$ представим в виде

$$g = a^{i_1} \dots a^{i_k} , \text{ где } k \ge 1,\ i_1,\dots,i_k \in \{1;-1\}.$$

Пусть среди $i_1,\dots,i_k$ ℓ_1 раз встречается 1 и ℓ_2 раз встречается -1, тогда в силу (1) $g = a^{\ell_1-\ell_2}$, т.е. имеет вид a^n, где $n \in \mathbb{Z}$.

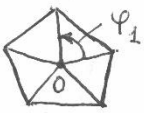
Пример 7. В группе $(\mathbb{Z}, +, 0)$ имеем $\langle 1\rangle = \{n1 \mid n \in \mathbb{Z}\} = \mathbb{Z}$, $\langle 2\rangle = \{n2 \mid n \in \mathbb{Z}\}$ - множество всех чётных чисел из $\mathbb{Z}$, т.е. приведены примеры бесконечных циклических группы и подгруппы.

Пример 8. Для группы $(\{0;1\},+,0)$ имеем $\langle 1\rangle = \{0;1\}$ - пример конечной циклической подгруппы.

Пример 9. Пример циклической группы порядка n (где $n \ge 2$) получится, если рассмотреть все вращения на плоскости вокруг некоторой точки O, совмещающие с собой правильный n-угольник P_n с центром в точке O.

Очевидно, что эти вращения образуют группу; под их произведением следует понимать последовательное выполнение преобразований. Указанная группа C_n содержит вращения $\varphi_0, \varphi_1, \ldots, \varphi_{n-1}$ против часовой стрелки на углы 0, $\frac{2\pi}{n}, \ldots, (n-1)\frac{2\pi}{n}$. При этом $\varphi_s = \varphi_1^s$, $0 \le s \le n-1$, а из геометрических соображений видно, что $\varphi_s^{-1} = \varphi_1^{n-s}$ и $\varphi_1^n = \varphi_0$ (единичное преобразование). Итак $|C_n| = n$, и $C_n = \langle \varphi_1 \rangle$.

$\varphi_1 = \frac{2\pi}{5}$, $n = 5$.

P_5: 

УП. Порядок элемента. Пусть G - произвольная группа, $a \in G$. Возможны два случая: 1) все степени a различны, т.е. $m \neq n \Rightarrow a^m \neq a^n$. В этом случае говорят, что элемент a имеет бесконечный порядок. 2) Имеются совпадения $a^m = a^n$ при $m \neq n$. Тогда в случае $m > n$ (иначе переставим a^m с a^n) имеем $a^{m-n} = e$, где $m-n > 0$, т.е. $\exists$ положительные степени элемента $a \in G$, равные e. Пусть q - наименьший положительный показатель, для которого $a^q = e$. Тогда говорят, что a - элемент конечного порядка q.

Пример I0. В группе $(\mathbb{Z}, +, 0)$ элементы 1,2 имеют бесконечный порядок (см. пример 7).

Пример II. В группе $(\{0;1\}, +, 0\}$ 1 - элемент конечного порядка 2 (см. пример 8).

Заметим, что в конечной группе G, где $|G| \le n$, все элементы будут, очевидно, конечного порядка $\le n$.

Утверждение. Если a - элемент конечного порядка q, то

(6) $\langle a \rangle = \{e, a, \ldots, a^{q-1}\}$;

(7) $a^k = e \Leftrightarrow k = lq$, $l \in \mathbb{Z}$.

Задача I7. Определить порядок элементов в группе $G = (\{0,1,2,3,4,5\}, +(\mathrm{mod}\,6), 0)$.

Решение. Используя (6), имеем

$\langle 1 \rangle = \{0,1,2,3,4,5\}$

(последовательно прибавляем к очередному элементу, начиная с 0, элемент 1 до первого получения элемента 0),

$\langle 2 \rangle = \{0,2,4\}$

(последовательно прибавляем к очередному элементу, начиная с 0, элемент 2 до первого получения элемента 0). Совершенно аналогично получаем: $\langle 3\rangle = \{0,3\}$; $\langle 4\rangle = \{0,4,2\} = \langle 2\rangle$, $\langle 5\rangle = \{0,5,4,3,2,1\} = \langle 1\rangle$. Таким образом, ~~элементы~~ 1 - элемент порядка 5, 2 - порядка 3, 3 - порядка 2, 4 - порядка 3, 5 - порядка 5.

Задача 18. Определить порядок элементов в группах

а) $G = (\{0,1,2,3,4\}, +(mod\ 5), 0)$;

б) $G = (\{0,1,2,3,4,5,6,7\}, +(mod\ 8), 0)$.

Задача 19. Доказать, что если элементы a и b в группе G перестановочны (т.е. $ab = ba$) и имеют конечные взаимно простые порядки r и s (т.е. НОД$(r,s) = 1$), то их произведение ab имеет порядок rs.

Решение. Пусть q - порядок элемента ab. Очевидно, что

$$(8)\quad (ab)^{rs} = a^{rs}b^{rs} = (a^r)^s (b^s)^r = e,$$

а следовательно, в силу (8) число rs делится нацело на q. В силу $(ab)^q = a^q b^q = e$ имеем $a^q = b^{-q}$, откуда $e = (a^r)^q = a^{rq} = b^{-rq}$, а следовательно, в силу (7) получаем $-rq = -ms$, где $m > 0$ (в силу $s>0$, $q>0$, $r>0$). Используя теперь то, что s и r взаимно простые числа, из $rq = ms$ заключаем, что число q делится нацело на s (так как rq делится нацело на s и НОД$(r,s) = 1$). Меняя в приведённых рассуждениях a и b местами, совершенно аналогично получаем, что числю q делится нацело и на r, а следовательно, q делится нацело на rs. Таким образом, получили, что rs делится нацело на q, а q делится нацело на rs, откуда заключаем, что $q = rs$.

Задача 20. Доказать, что если элементы a и b в группе G перестановочны и (имеют конечные порядки r и s соответственно) $\langle a\rangle \cap \langle b\rangle = \{e\}$, то порядок ab равен наименьшему общему кратному r и s, ~~чтд~~ смотри

Решение. Обозначим через q порядок элемента ab, а через k наименьшее общее кратное r и s. Тогда $(ab)^k = a^k b^k = e$, откуда в силу (7) выполняется $k = lq$, где $l \in \mathbb{Z}$, $l > 0$, а следовательно, $q \leq k$. Из $(ab)^q = e$ получаем $a^q b^q = e$, откуда $a^q = b^{-q}$. Используя то, что $\langle a\rangle \cap \langle b\rangle = e$, из последнего равенства имеем $a^q = e = b^{-q}$, откуда $a^q = b^q = e$. Но тогда, используя (7), получаем, что q - общее кратное

чисел r, s, а следовательно, $k \leq q$. Таким образом, получили, что $k \leq q$ $q \leq k$, а следовательно, $k = q$.

Задача 20. Показать, что если порядки r и s элементов a и b группы G взаимно просты, то $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Решение. Предположим, что $\langle a \rangle \cap \langle b \rangle \neq \{e\}$, т.е. найдутся числа k_1, $k_2 \in \mathbb{Z}$ такие, что $a^{k_1} = b^{k_2}$, $1 \leq k_1 \leq r-1$, $1 \leq k_2 \leq s-1$. Но тогда $a^{k_1 s} = b^{k_2 s} = (b^s)^{k_2} = e$, откуда в силу (7) получаем, что $k_1 s$ делится нацело на r, и поскольку НОД$(r, s) = 1$, то это возможно лишь в случае, когда k_1 делится нацело на r, что невозможно, поскольку $1 \leq k_1 \leq r-1$.

Задача 21. Показать, что для любых элементов a, b, с группы G:

а) элементы ab и ba имеют одинаковые порядки;

б) элементы abc, bca и cab имеют одинаковые порядки.

Решение. а) Пусть k_1 и k_2 – порядки элементов ab и ba. Тогда $\underbrace{ab \cdot ab \dots ab}_{k_1 \text{ раз}} = e$, откуда $a^{-1}\underbrace{ab \cdot ab \dots ab}_{k_1 \text{ раз}} a = a^{-1}a = e$, а следовательно, $\underbrace{ba \cdot ba \dots ba}_{k_1 \text{ раз}} = e$. Таким образом, $(ba)^{k_1} = e$, откуда $k_1 \geq k_2$. Меняя в рассуждениях ab и ba местами, получаем противоположное неравенство, откуда и следует, что $k_1 = k_2$.

б) Пусть k_1 и k_2 – порядки элементов abc и bca. Тогда $\underbrace{abc \cdot abc \dots abc}_{k_1 \text{ раз}} = e$, откуда $a^{-1}\underbrace{abc \cdot abc \dots abc}_{k_1 \text{ раз}} a = a^{-1}a = e$, а следовательно, $\underbrace{bca\, bca \dots bca}_{k_1 \text{ раз}} = e$. Таким образом, $(bca)^{k_1} = e$, откуда $k_1 \geq k_2$. Из $\underbrace{bca \cdot bca \dots bca}_{k_2 \text{ раз}} = e$ теперь имеем $(bc)^{-1}\underbrace{bca \cdot bca \dots bca}_{k_2 \text{ раз}} \cdot bc = (bc)^{-1}bc = e$, откуда $\underbrace{abc \cdot abc \dots abc}_{k_2 \text{ раз}} = e$, а следовательно, $k_2 \geq k_1$. Таким образом $k_1 \geq k_2$, $k_2 \geq k_1$, откуда $k_1 = k_2$. Рассмотрение случая с cab аналогично.