Конспект по Алгебре

Коченюк Анатолий

25 октября 2018 г.

Глава 1

1 четверть

03.09.2018
06.09.2018
12.09.2018

Теорема 1.1. *$f : X \to Y$ – инъективно $\iff \forall y, h : Y \to X : f \circ g = f \circ h \Rightarrow g = h$*

Доказательство. $\Rightarrow$:
фиксируем $g, h : f \circ g = f \circ h$. Нужно доказать, что $\forall y \quad g(y) = h(y)$
фиксируем $y \in Y$. $\sqsupset g(y) \neq h(y) \Rightarrow f \circ g(y) \neq f \circ h(y)$?!!
$\Leftarrow$:
фиксируем $x_1, x_2 : f(x_1) = f(x_2) \quad x_1 = x_2$?
фиксируем $g(y) = x_1 . h(y) = x_2$
$f \circ g(y) = f(x_1)$
$f \circ h(y) = f(x_2)$
$g(y) = h(y) \Rightarrow x_1 = x_2$ □

Теорема 1.2. *$f : x \to Y$ – сюръективна $\iff \forall g.h : Y \to X : g \circ f = h \circ f \Rightarrow g = h$*

Доказательство. $\Rightarrow$:
фиксируем $g, h : g \circ f = h \circ f \quad \forall y \quad h(y) = g(y)$?
фиксируем $y \quad \sqsupset$: $h(y) \neq g(y) \quad \forall y \in Y \exists x \in X : f(x) = y$
$(g \circ f)(x) = g(f(x)) = g(y) \neq h(y) = h(f(x)) = (h \circ f)(x)$, т.е. $g \circ f \neq h \circ f$?!!
$\Leftarrow$:
h/w □

$\mathbb{R}^2 \to \mathbb{R}^2$
$(x, y) \mapsto (2x + y - 3, x - y - 1)$
Инъективна: фиксируем $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2 \quad \sqsupset f(x_1, y_1) = f(x_2, y_2)$
$f(x_1, y_1) = (2x_1 + y_1 - 3, x_1 - y_1 - 1)$
$f(x_2, y_2) = (2x_2 + y_2 - 3, x_2 - y_2 - 1)$
$(2x_1 + y_1 - 3, x_1 - y_1 - 1) = (2x_2 + y_2 - 3, x_2 - y_2 - 1)$
$2x_1 + y_1 - 3 = 2x_2 + y_2 - 3 \quad x_1 - y_1 - 1 = x_2 - y_2 - 1$
$3x_1 - 4 = 3x_2 - 4$
$x_1 = x_2 \Rightarrow y_1 = y_2$

1.1 Преобразования конечных множеств.

A – конечна $A = \{1, \ldots, n\} \quad |A| = n$

Определение 1.1. *$F(A) = F_n$ – совокупность преобразований A*

$\alpha : A \to A$ – пеобразование
$\alpha = \begin{pmatrix} 1 & \cdots & n \\ a_1 & \cdots & a_n \end{pmatrix}$ – перестановка $\iff \forall i \neq j \quad a_i \neq a_j$

$\beta = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$

$\beta \circ \alpha = \begin{pmatrix} 1 & \cdots & n \\ a_1 & \cdots & a_n \\ b_1 & \cdots & b_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$

Д/З:

1. $\mathbb{R}^2 \to \mathbb{R}^2 \quad (x, y) \mapsto (x - y + 2, 2x + y)$
2. $\mathbb{R}^3 \to \mathbb{R}^3 \quad (x, y, z) \mapsto (2x - y, 7y + 3x, 0))$
3. $\mathbb{R}^3 \to \mathbb{R}^3 \quad (x, y, z) \mapsto (x - 5 + y + z, x - y + z + 4, 2(x + 1) + 2z - 3)$
4. При каких $a, b, c \in \mathbb{R}$
   $f : \mathbb{R} \to \mathbb{R} \quad x \mapsto ax + b$
   $g : \mathbb{R} \to \mathbb{R} \quad x \mapsto cx^2$
   $f(g(x)) = g(f(x))$
5. При каких $a, b \in \mathbb{R} \quad f(x) = ax + b$
   $f(\sin(x)) = \sin(f(x))$

14.09.2018

Глава 2

Теория Групп

2.1 Алгебраические операции

Определение 2.1. *Алгебраическая операция на множестве* A *– отображение* $f : AxA \to A$

Примеры:

- $''+'' : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
- $''\cdot'' : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
- на 2^M операция объединения. $X \cup Y = \{x | x \in X$ или $x \in Y\}$
- $\circ : F(A) \times F(A) \to F(A) \quad (f, g) \mapsto f \circ g$
- $A = \{0, 1, 2, 3\} \quad a, b \in A \quad a \triangle b = a + b (mod 4)$

$\triangle$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Определение 2.2. $(A, *)$ *– группоид, если* A*–множество и* $*$ *– операция на* A

$(\mathbb{N}, \div)$ – не группоид
$(\mathbb{R}, \div)$ – группоид

Определение 2.3. $(A, *)$ *– коммутативный, если* $\forall a, b \in A \quad a * b = b * a$

$(\mathbb{R}, -)$ – не коммутативный
$(F(A), \circ)$ – не коммутативный
$(\mathbb{R}, \cdot)$

Определение 2.4. $(A, *$ *– ассоциативный, если* $\forall a, b, c \in \quad (a * b) * c = a * (b * c)$

$(\mathbb{N}, +)$ – ассоциативный
$(\mathbb{R}, -)$ – не ассоциативный

Определение 2.5. $(A, *)$ *– группоид с сокращением (левым, правым).* $\forall a, b, c \in A$
$q * b = q * c \Rightarrow b = c$*(лев)*
$b * a = c * a \Rightarrow b = c$*(прав)*

$\rhd : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \quad (n, m) \mapsto m$
$(\mathbb{N}, \rhd)$ – не сократим справа $2 \rhd 2 = 5 \rhd 3, \quad 2 \neq 5$
Сократим справа.

Определение 2.6. $(A, *)$ *– инверсивный, если* $\forall a, b \in A \exists x, y \in A : a * x = b, y * a = b$

$(\mathbb{N},+)$ – не инверсивный. $5,5 \in \mathbb{N} \quad 5+x=5, y+5=y \quad x,y \notin \mathbb{N}$
$(\mathbb{Z},-)$ – инверсивный.$a,b \in \mathbb{Z} \quad a+(b-a)=b \quad (b-a)+a=b$

Определение 2.7. $(A,*)$ *– группоид. a– идемпотент, если $a*a=a$*

$(\mathbb{N},\triangleright)$ – любой элемент – идемпотент

Определение 2.8. $(A,*) \ni \theta$ *– аннулятор, если $\forall a \in A$*
$a*\theta=\theta$
$\theta*a=\theta$

Определение 2.9. $(A,*)$ *с нейтральным элементом $a' \in A$ называется обратным к a*
$a*a'=e$
$a'*a=e$

Определение 2.10. $(A,*)$ *– группоид. $B \subseteq A$ и $\forall a,b \in B \quad a*b \in B$. Тогда $(B,*)$ – подгруппоид группоида A*

$(\mathbb{N},+)$ – подгруппоид $(\mathbb{Z},+)$

Лемма 2.1. $(A,*)$ *– ассоциативный, инверсивный группоид с нейтральным элементом$\Rightarrow$ $(A,*)$ – сократимый*

Доказательство. $a*y=a*x$
По инверсивности $\exists a' \in A : a'*a=e$
$a'*(a*x)=a'*(a*y)$
$(a'*a)*x=(a'*a)*y$
$e*x=e*y$
$x=y$ □

Д/З:

Письменно(на листочке, подписанном с табличкой):

1. .

*	1	2	3
1	2	3	1
2	3	3	2
3	1	2	1

Проверить Коммутативность, Ассоциативность, Сократимость, Инверсивность, Нейтральный элемент

2. группоид поворотов квадрата
3. $(\mathbb{N}, \text{НОК})$
4. $(\mathbb{N}, \text{НОД})$

   Устно:

5. $|A|=3 \quad (F(A),\circ)$ найти все подгруппоиды
6. $(M,*) \quad M$ – конечный, ассоциативный, сократимый. Существует ли нейтральный элемент
7. $(A,*)$ – ассоциативное с нейтральным элементом. ? $(A',\circ)$ – подгруппоид (A' – множество обратимых элементов)

18.09.2018
ДЗ:

1. найти все подгруппоиды группоида $(F(A),\circ), |A|=3$ (их строго больше 6?) – устно
2. Составить таблицу Кэли, где $A=\{a,b\}$, для:
   - $(2^A,\cap)$
   - $(2^A,\triangle)$

3. $M_{2x2}(\mathbb{R})$ – множество матриц

   $A = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{R} \right\} \subseteq M_{2x2}(\mathbb{R})$

   $b = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in \mathbb{R} \backslash \{0\} \right\} \subseteq M_{2x2}(\mathbb{R})$

   $(M_{2x2}(\mathbb{R}), \cdot), (A, \cdot), (B, \cdot)$ – все свойства

4. $(\mathbb{Z}, *) \quad a * b = |a - b|$ – все свойства

5. $f(x) = \sqrt{x^2 - 1}$ – инъективность, сюръективность. Построить обратное, если возможно.

   $f^n = \underbrace{f \circ f \circ \ldots \circ f}_{n}$ — ?

Теорема 2.1. *M – конечно $(M, *)$ – асс, сокр $\Rightarrow \exists e$*

Доказательство. фиксируем $a \in quad a^2 \in M$

$n > i \quad a^n = a^i$, т.к. M – конечно

$a^{n-i} a^i = a^i \Rightarrow a^{n-i} * a = a$

a^{n-i} – нейтральный?

фиксируем $x \in M \quad x * a = x * a = z * a^{n-i} * a \Rightarrow x = x a^{n-i}$ Таким образом a^{n-i} – правый нейтральный. То, что он также и левый нейтральный доказывается аналогично.

$a * x = a * a^{n-i} * x$

$a * x = a a^{n-i} * x$ □

2.2 Группы. Основные понятия

Определение 2.11. *$(G, *)$ – группоид называется полугруппа, если выполняется ассоциативность*

Определение 2.12. *$(G, *)$ – группоид называется группой, если выполняется:*

1. *Ассоциативность:* $\forall a, b, c \in G \quad (a * b) * c = a * (b * c)$

2. *Существование нейтрального элемента* $\exists e \in G \quad \forall g \in G \quad e * g = g * e = g$

3. *Существование обратного элемента* $\forall a \in G\ \exists b \in G \quad a * b = b * a = e$

   e – единица. $b =: a - 1$

Альтернативное определение: группа – множество и 3 операции:

1. *бинарная операция* $*$

2. *унарная операция* $.^{-1}$

3. *нульарная операция* e

Утверждение 2.1. *1. e – единственное*

2. a^{-1} – единственный

Доказательство. б $\sqsupset \exists a_1$ и a_2:

$$a * a_1 = a_1 * a = e$$
$$a * a_2 = a_2 * a = e$$

$(a_2 * a) * a_1 = e * a_1 = a_1$

$a_2 * (a * a_1) = a_2 * e = a_2$

$a_1 = a_2$ по ассоциативности

□

Определение 2.13. $(G, *)$ – *группа называется абелевой, если выполняется коммутативность.* $\forall a, b \quad a * b = b * a$

Примеры:

1. $(\mathbb{Z}, +)$ – абелева группа
2. $(S(A), \circ) = S_n, n = |A|$ – не абелева группа при $n \geqslant 3$

Определение 2.14 (центр группы)**.** $Z(G) = \{z \in G | zg = gz \forall g \in G\}$

Замечание 2.1. $(G, \cdot)$ – *абелева* $\Rightarrow Z(G) = G$

Определение 2.15. G – *конечно* $\Rightarrow (G, *)$ – *конечна*
G – *бесконечно* $\Rightarrow (G, *)$ – *бесконечно*

Теорема 2.2. *конечная полугруппа* $(S, *)$ *является группой* $\Longleftrightarrow$ *выполняется сократимость.*

Доказательство. .

$\Rightarrow$ $\sqsupset a * x = b * a$
$\exists x^{-1} : a * x * x^{-1} = b * x * x^{-1}$
$a = b$ ч.т.д.

$\Leftarrow$ (S, *) – ассоциативна, сократима и S – конечно $\overset{\text{Упр}}{\Rightarrow}$ существует нейтральный элемент, $(S, *)$ – обратима $\Rightarrow (S, *)$ – группа

□

Замечание 2.2. *обратный переход неверен, если* S – *бесконечно. Пример* – $(\mathbb{N}, +)$

Определение 2.16. *порядок элемента* $g \in (G, *)$ – *наименьший* $n \in N : f^n = e$*. Если такого* n *не существует, то элемент называется элементом бесконечного порядка.*

Утверждение 2.2. $a \in (G, *)$ – *конечного порядка* n
Тогда $e, a, a^2, \ldots, a^{n-1}$ – *различные элементы и* $\forall m \in \mathbb{Z} \quad a^m$ *совпадает с одним из них*

Доказательство. $\sphericalangle a^i = a^j \quad i > jquada^{i-j} = e \ i - j < n$, n – минимальное такое число, что $a^n = e$??!
$\forall m \in \mathbb{Z} \exists i : a^m = a^i \quad m = n * q + r \quad a^m = a^{n*q+r} = e * a^r$ □

Замечание 2.3. *В конечной группе у всех элементов конечный порядок*

Определение 2.17. *Если* $H \subseteq G \neq \emptyset \Rightarrow (H, *)$ – *подгруппоид, если:*

- $\forall a, b \in H \quad a * b \in H$
- $\forall a \in H \quad a^{-1} \in H$

Упражнение 2.1. $(H, *)$ – *подгруппа группы* $(G, *)$ – *группа*

Определение 2.18. $\{e\}, G$ – *несобственные подгруппы, все остальные собственные.*
$H \leqslant G$ – H *подгруппа* G
$H < G$ – H *собственная подгруппа* G

Теорема 2.3. $B \subset A \quad (A, *)$ – *конечная группа* $\quad e \in B, B$ *замкнута относительно* $* \Rightarrow (B, *)$ – *подгруппа*

Доказательство. из определения подгруппы нам осталось проверить только обратимость
фиксируем $b \in B$. Так как B – конечно, то порядок b конечен $\Rightarrow \exists n : b^n = e \Rightarrow b * b^{n-1} = e = b^{n-1} * b \Rightarrow b^{-1} = b^{n-1}$ □

Теорема 2.4. $\{(B_\alpha, *)\}_{\alpha \in I}$ – *семейство подгрупп* $(G, *)$
$B = \bigcap\limits_{\alpha \in I} = B_\alpha \Rightarrow (B, *)$ – *подгруппа*

Доказательство. фиксируем $a, b \in B \Rightarrow a?b \in B_\alpha \forall \alpha \Rightarrow a * b \in B_\alpha \forall \alpha \Rightarrow a * b \in B$
$\forall a \in B \quad a^{-1} \in B$ аналогично □

Определение 2.19. $S \subset G$
$C_G(S) = \{g \in G | sg = gs \forall s \in S\}$ - *централизатор*
$N_G(S) = \{g \in G | gS = Sg\}$

ДЗ:

1. 2.1 (ссылка)
2. на $\mathbb{R}_+$ ограниченные функции:
   - $f_1(x) = x$
   - $f_2(x) = -x$
   - $f_3(x) = \dfrac{1}{x}$
   - $f_4(x) = -\dfrac{1}{x}$

   – группа относительно композиции? Абелева группа?
3. (!)Любая группа третьего порядка – абелева
4. (!)Если $\forall g \in G \quad g \leqslant 2 \Rightarrow G$ – абелева
5. (!)$C_G(S) \leqslant G$
6. (!)$\mathbb{Z}(G) = \bigcup\limits_{g \in G} C_G(g)$
7. (!)$\mathbb{N}_G(S) \leqslant G$

ДЗ (на 2 октября):

1. $H \leqslant G \Longleftrightarrow HH \subseteq H$ и $H^{-1} \subseteq H$
2. Множество функций $f(x) = \dfrac{ax+b}{cx+d} \quad a, b, c, d \in \mathbb{R} \quad ad - bc \neq 0$ — группа относительно композиции
3. (!)$F \leqslant H \leqslant G \Rightarrow F \leqslant G$
4. (!)$A, B, C \leqslant G$ и $C \subseteq A \cap B \Rightarrow C \leqslant A$ или $C \leqslant B$

Определение 2.20. $S \subset G, S \neq \emptyset \Rightarrow \langle S \rangle = \bigcap\limits_{S \subseteq H \leqslant G}$ – *подгруппа, порождённая* S

Замечание 2.4. *Это наименьшая подгруппа, содержащаяся в* S

Определение 2.21. *Подгруппа* $H \leqslant G$ *– называется циклической, если* $\exists g \in G : \quad H = \langle \{g\} \rangle$

Пример: $(\mathbb{Z}, +) \quad 1$ – порождающий элемент

Теорема 2.5. $\forall S \subset G \quad \langle S \rangle = \{S_i \dots S_n | S_i \in S \cup S^{-1}, i \in \mathbb{N}_0\} =: T$

Доказательство. .

$\subseteq$ $T \leqslant G$ т.к. $T \neq \emptyset$:

- $\forall t_1, t_2 \in T \quad t_1 \cdot t_2 \in T$
- $\forall t_1, t_2 \in T \quad t^{-1} \in T$

$\langle S \rangle \subseteq T$ т.к. T входит в пересечение

$\supseteq$ $t \in T \quad t = s_1 \dots s_n \in \langle S \rangle$
$\forall S \subset H \leqslant G$ т.к. $S_1 \dots S_n \in H$

□

2.3 Примеры групп

1. Группа вычетов по модулю n

   $n \in \mathbb{N} \quad \mathbb{Z}_n$ – группа вычетов по модулю n

   $[a]_m = \{b \in \mathbb{Z} : b \equiv a(mod\ n)\}$

   $[a]_m + [b]_m = [a+b]_m$

   Упражнение 2.2. $(\mathbb{Z}_n, +)$ – *абелева группа*

2. Группа Матриц

   2.1 Полная линейная группа

   F – поле $\quad GL_n(F) = \{A \in M_{n\times n}(F) | detA \neq 0\}$

   2.2 Специальная линейная группа

   F – поле $\quad SL_n(F) = \{A \in M_{n\times n}(F) | detA = 1\}$

   $det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$

   Утверждение 2.3. $A \in M_{n\times n}(F) \quad \exists A^{-1} \Longleftrightarrow detA \neq 0$

   Упражнение 2.3. $Aff_1(\mathbb{R}) = \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} | a \in \mathbb{R}\backslash\{0\} \quad b \in \mathbb{R}\}$

   (1) $\quad Aff_1(\mathbb{R}) \subset SL_2(\mathbb{R})$

3. Группа биективных преобразований множества $A \quad (B(A), \circ)$

4. Группа биективных преобразований конечного множества $A \quad S_n$

   Определение 2.22. $\alpha \in S_n$ *называется циклом длины* k*, если она перемещает ровно* k *элементов*
   $i-1, i_2 \dots i_k : \quad \alpha(i_1) = i_2, \alpha(I-2) = i_3, \dots, \alpha(i_k) = i_1$

   Пример: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix} = (1324)$

   Теорема 2.6. *Любая перестановка разлагается однозначно с точностью до порядка на произведение попарно независимых циклов*

   Доказательство. $\alpha \in S_n \quad i_1$ – первый перемещаемый элемент

   $i_2 = \alpha(i_1) \quad i_3 = \alpha(i_2) \quad i_k = i_j$

   $j = 1$ т.к. α – биективно

   Остались недвинутые элементы.

   Возьмём следующий наименьший, который α перемещает. $i_k + 1$ и продолжим

   Т.к. α – конечно, то мы однажды переберём их все. $\alpha = (i_1 \dots i_l)(i_{k+1} \dots i_{k+l}) \dots$

   Возьмём следующий □

   Определение 2.23. *цикл длины* 2 *называется транспозицией*

   Утверждение 2.4. *Любой цикл можно разложить в произведение транспозиций*

   Доказательство. $(i_1 \dots i_k) = (i_1 i_k) \dots (i_1 i_3)(i_1 i_2)$ □

   Определение 2.24. $\alpha \in S_n \quad \alpha = \tau_1 \dots \tau_n$ – *разложение в транспозицию*
   Тогда $sgn\ \alpha = (-1)^m$

   Теорема 2.7. *Определение* sgn *корректно*

Замечание 2.5. *Знак транспозиции* $= -1$

Определение 2.25. $\alpha \in S_n$ *– чётная, если* $sgn\ \alpha = 1$.

Нечётная, если $sgn\ \alpha = -1$

Определение 2.26. $A_n = \{\alpha \in S_n | \alpha - \text{чёт}\}$

Упражнение 2.4. *(a)* $(!) A_n \leqslant S_n$

(b) множество нечётных перестановок не подгруппа

Утверждение 2.5. *Всякую транспозицию можно представить в виде произведения траспозиций вида:*

(1) $(i, i+1), \quad i \in \{1, \dots, n-1\}$

Доказательство. (1) $(i, j) = (1, i)(1, j)(1, i)$

(2) Упражнение . Подсказка $(i, i+1)$ в виде произведения $(1, k)$

□

5. Группа движений плоскости

Определение 2.27. *Движение плоскости* f *– симметрия фигуры* $F, f(F) = F$

Пример – группа симметрий треугольника

Определение 2.28. *Диэдральная группа – группа симметрий правильного* n *- угольника*

Дз:
Письменно:

1. (!) D_n – не абелева
2. (!) $!\langle\{(1,2); (12\dots n)\}\rangle = S_n$
3. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 1 & 2 & 5 & 7 & 6 & 9 & 8 \end{pmatrix}$ В виде цикла; разложить в транспозиции; вычислить знак.

Устно (список ссылок на упражнения):

1. 2.2
2. 2.4
3. 4

2.4 Теоретико-групповые конструкции

G – группа, $H \leqslant G$
$R \subseteq G \times G : (x, y) \in R \Longleftrightarrow x * y^{-1} \in H$

Упражнение 2.5. *Упр:* R *– рефлексивно, симметрично и транзитивно, т.е. отношение эквивалентности*

Определение 2.29. *Классы эквивалентности отношения* R *называются правыми смежными классами по подгруппе* $H \quad Ha = \{ha | h \in H\}$

Утверждение 2.6. $\forall Ha, Hb$ *либо не пересекаются* ($Ha \cap Hb = \emptyset$)*, либо совпадают* ($Ha = Hb$)

Доказательство. $\exists\, x \in Ha \cap Hb$, тогда $x = h_a \cdot a = h_b \cdot b, h_a, h_b \in H$
$h_a a = h_b b$
$a = h_a h_b b$
$a \in Hb$, т.к. $h_a h_b \in H$
ф. $y \in Ha \quad y = h_y \cdot a = h_y h_a h_b b \in Hb$

□

Замечание 2.6. *Аналогично определяется левый смежный класс.*

Следствие 2.1. $G = \bigsqcup\limits_{H_a \leqslant G} H_{a_i}$

Доказательство. $g \in G \quad \exists Hg \ni g$ □

Упражнение 2.6. *Если* G *– абелева, то* $\forall Ha \exists b \neq a : H : Ha = bH$

Упражнение 2.7. G *– группа,* $H \leqslant G$
Тогда $H \to aH \quad h \mapsto ah$ *– биекция*

Доказательство.

- Иньективность $\forall h_i, h_j \quad ah_u = ah_j \Rightarrow h_i = h_j$
- Сюръективность $x \in aH \quad x = ah_a, h_a \in H \quad h_a \mapsto x$

□

Теорема 2.8. *Порядок любой подгруппы конечной группы делит порядок группы.*

G *– конечная группа* $n = |G| \quad m = |H| \Rightarrow n \vdots m$

Доказательство. $G = a_1 H \bigsqcup a_2 H \bigsqcup \cdots \bigsqcup a_i H$
$\forall aH \quad |aH| = H$ ($H \to aH$ – биекция) $G = i \cdot m$ чтд □

Определение 2.30. *Число левых смежных классов группы* G *по подгруппе* H *называется индексом подгруппы* H *в группе* G
$|G : H|$
G/H *– множество левых смежных классов*
$H \backslash G$ *– множество правых смежных классов*

Упражнение 2.8. $H \leqslant G$ *тогда* $H \backslash G \to G/H \quad Hx \mapsto x^{-1}H$

Определение 2.31. $H \leqslant G$ *– называется нормальной, если* $\forall a \in G \quad aH = Ha$
$H \trianglelefteq G$

Примеры:

1. $G \trianglelefteq G$ т.к. $\forall a \quad aG = G = Ga$
2. $\{e\} \trianglelefteq G \quad a\{e\} = \{a\} = \{e\}a$
3. **Теорема 2.9.** *Если* $|G : H| = 2 \Rightarrow H \trianglelefteq G$

   Доказательство. $H \bigsqcup Hb = G = H \bigsqcup aH \quad Hb = aH$
   Если $xH = H = Hx$
   Если $xH = aH = Ha \quad aH \neq H$ □
4. **Упражнение 2.9.** $H \trianglelefteq G$ *и* $K \trianglelefteq H$ *тогда* $K \trianglelefteq G$

Определение 2.32. *Гамильтонова группа – не абелева группа такая, что выполняется* $\forall H \leqslant G \quad H \trianglelefteq G$

Определение 2.33. *Группа называется простой если у неё только 2 нормальные подгруппы*

A_n – простая

Лемма 2.2. *Если* $H \trianglelefteq G$ *то* $\forall h \in H, a \in G \quad aha^{-1} \in H$

Доказательство. фиксируем $h \in H, a \in G \quad ah \in aH$
$aH = Ha$, т.к. $H \trianglelefteq G$
$ah = xa$, где $x \in H$
$aha^{-1} = x \in H$ □

Теорема 2.10. $(G, \cdot)$ - *группа* $H \trianglelefteq G$
Тогда $(G/H, \cdot)$ – *группа*

Доказательство. $aH \cdot bH = (ab)H$ – определения операции

1. Корректность определения. $\sqsupset a_1H = a_2H \quad b_1H = b_2H$
   $a_1b_1 = (a_2h_a)(b_2h_b) = a_2(b_2b_2^{-1})h_ab_2h_b = a_2b_2h, h \in H$. По лемме $b_2^{-1}h_ab_2 \in H$
   $\Rightarrow a_1b_1 \in a_2b_2H \Rightarrow a_1b_1Ha_2b_2H$

2. ассоциативность $aH \cdot (bH \cdot cH) = aH(bc)H = a(bc)H = (ab)cH = (ab)H \cdot cH = (aH \cdot bH) \cdot cH$

3. нейтральный элемент $eH = H$

4. обратный к ah– $a^{-1}H$

□

ДЗ на 16.10.2018

1. $A \trianglelefteq G, B \trianglelefteq G \Rightarrow AB \trianglelefteq G$

2. найти все нормальные подгруппы в S_3

3. Написать таблицу Кэли для $\mathbb{Z}/D \quad D = \{0, 2\}$

4. Доказать, что $A_n \trianglelefteq S_n$

Определение 2.34. *Группа* G/H – *фактор группа по подгруппе* H

Примеры:

1. $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ т.к. $\mathbb{Z}$ – абелева
   Тогда $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$

Определение 2.35 (Прямое произведение групп)**.** $(G, *), (F, \circ)$ – *группы*
$(G \times F, \square)$ – *прямое произведение*
$(g_1, f_1)\square(g_2, f_2) = (g_1 * g_2, f_1 \circ f_2)$

Утверждение 2.7. *Прямое произведение является группой:*

Доказательство. 1. корректность очевидна

2. ассоциативность (Упр!)

3. нейтральный элемент (e_G, e_F)

4. обратный к (g_1, f_1) – (g^{-1}, f^{-1}) (Упр!)

□

Упражнение 2.10. F – *циклическая группа порядка* p
G – *циклическая группа порядка* q
p, q – *простые* $\Rightarrow F \times G$ – *циклическая группа порядка* pq

Упражнение 2.11. F, G – *конечные группы* $\Rightarrow |F \times G| = |F| \cdot |G|$

2.5 Отображения групп

Определение 2.36. *гомоморфизм группы* $(A, *)$ *в группу* $(B, \circ)$ *называется отображение* $f : A \to B : f(a_1 * a_2) = f(a_1) \circ f(a_2)$

Утверждение 2.8. *1.* $f(e_B) = e_B$

2. $f(a^{-1}) = (f(a))^{-1}$ *f:A*

Определение 2.37. .
f:A $Ker\ f = \{a \in A | f(a) = e_B\}$
$Im\ f = \{f(a) | a \in A\}$

3. $Ker\ f \trianglelefteq A$

4. $Im\ f \leqslant B$

5. f *– инъективна* $\Longleftrightarrow Ker\ f = \{e\}$

6. f *– сюръектина* $\Longleftrightarrow Im\ f = B$

Доказательство. 1. Пусть $x = f(e_A)$

$x = f(e_A) = f(e_a * e_a) = f(e_a) \circ f(e_A) = x \circ x$

ф. $b \in B \quad x \circ b = (x \circ x) \circ b$

$b = x \circ b$ аналогично $b = b \circ x \Rightarrow x = e_B$

2. Упр
3. Упр
4. Упр
5. Упр
6. Очевидно

□

Определение 2.38. *Изоморфизм групп – биективный гомоморфизм*
„A изоморфна B” A $\cong$

Теорема 2.11. *Изоморфность групп – отношение эквивалентности на множестве всевозможных групп*

Доказательство.

Рефлективность $G \cong G \quad id : G \to G \quad l2018.10.16.3 g \mapsto g$ – изоморфизм

Симметричность $(G, *) \quad (F, \circ)$ Пусть G изоморфна F т.е. $f : G \to F$ – биективный гомоморфизм
$f^{-1} : F \to G$ – биективный гомоморфизм.

Транзитивность. $f_1 : G \to F \quad f_2 : F \to H \quad f_3 = f_2 \circ f_1 : G \to H$ – биективный гомоморфизм.
$f_3(g_1 * g_2) = f_2(f_1(g_1 * g_2)) = f_2(f_1(g_1) \circ f_1(g_2)) = f_2(f_1(g_1)) \square f_2(f_1(g_2)) = f_3(g_1) \square f_3(g_2)$ □

Определение 2.39. *Абстрактная группа – множество всех классов эквивалентности по отношению изоморфности.*

Примеры:

1. $S_2 \cong \mathbb{Z}$
2. $\mathbb{Z} \cong n\mathbb{Z} \quad x \mapsto nx$

   понятно, что это биективное отображение. Докажем, что это гомоморфизм.

   $x_1, x_2 \in \mathbb{Z} \quad f(x_1 + x_2) = n(x_1 + x_2) = nx_1 + nx_2 = f(x_1) + f(x_2)$
3. $D_3 \cong S_3$

4. $(\mathbb{R},+) \cong (\mathbb{R}_{>0},\cdot)$ $\quad exp : \mathbb{R} \to \mathbb{R}_{>}$ $\quad x \mapsto e^x$
   exp – биективна
   ф. $x_1, x_2 \in \mathbb{R}$ $\quad e^{x_1+x_2} = e^{x_1} \cdot e^{x_2}$

   Замечание 2.7. *Основание может быть любым* $\neq 1, > 0$

Утверждение 2.9. *Любые две группы простого порядка изоморфны*

Доказательство. $|G| = p$

1. Любая группа простого порядка циклическая.
   ф. $g \in G$ $\quad < x >=: H$

   $|G| \vdots |H|$ по теореме Лагранжа $\Rightarrow |H| = 1 \vee |H| = p$
   т.е. $H = \{e\} \vee |H| = G$
   любой элемент порождает нашу группу $\Rightarrow$ она циклическая
2. $|G| = p = |H|$ $\quad (G, \circ)$ $\quad (H, *)$
   $< g >= G$ $\quad < h >= H$
   $f : G \to H$ $\quad g^i \mapsto h^i$
   (a) f – биективно
   $h_1, h_2 \in H, h_1 \neq h_2$ $\quad h_1 = h^i$ $\quad h^2 = h^j$ т.к. $h^i \neq h^j$ то $i \not\equiv j(mod\ p) \Rightarrow g^i \neq g^j \Rightarrow$ выполняется инъективность.
   G, H – конечны $\Rightarrow f$ – биективна
   (b) f – гомомрфизм
   ф $g^i, g^j \in G$ $\quad f(h^i \circ g^j) = f(g^{i+j}) = h^{i+j} = h^i * h^j = f(g^i) * f(g^j)$

□

Упражнение 2.12. $G_1 \times \{e_2\} \leqslant G_1 \times G_2$
Тогда доказать, что это нормальная подгруппа и $G_1 \times G_2 / G_1 \times \{e_2\} \cong G_1$

Теорема 2.12. A, B *– две группы* $f : A \to B$ *– гомоморфизм.*
Тогда:

1. $Ker\ f \trianglelefteq A$
2. $Im\ f \leqslant B$
3. $Im\ f \cong A/Ker\ f$

Доказательство. 1. $e_A \in Ker\ f$
   $a, b \in Ker\ f$ тогда $f(a * b) = f(a) \circ f(b) = e_B \circ e_B = e_B \Rightarrow a * b \in Ker\ f$
   $a \in Ker\ f$ $\quad f(a^{-1}) = f(a)^{-1} = e_B^{-1} = e_B \Rightarrow a^{-1} \in Ker\ f$
   Т.О. $Ker\ f \leqslant A$
   $(!)a(ker\ f) = (Ker\ f)a$
   ф. $ak \in aKer\ f \Rightarrow aka^{-1} \in Ker\ f \Rightarrow (aka^{-1})a \in Ker\ fa \Rightarrow ak \in Ker\ fa$
   Т.О. $Ker\ f \trianglelefteq A$

2. (a) $f(e_A) = e_B \Rightarrow e_B \in Im\ f \Rightarrow Im\ f \neq \emptyset$
   (b) ф. $b_1, b_2 \in Im\ f$ $\quad b_1 \circ b_2 = f(a_1) \circ f(a_2) = f(a_1 * a_2) \in Im\ f$
   (c) ф. $b \in \Im\ f$ $\quad b = fa)$ $\quad f(a^{-1}) = b^{-1} \Rightarrow b^{-1} \in \Im\ f$
   Т.О. $Im\ f \leqslant B$

3. $\varphi : A/Ker\ f \to Im\ f \quad a(Ker\ f) \mapsto f(a)$

   Докажем, что φ изоморфизм

   (a) Корректность
   Пусть $a(Ker\ f) = b(Ker\ f) \Rightarrow a \in b(Ker\ f) \quad a = b * k, k \in Ker\ f$
   $f(a) = f(b * k) = f(b) circ f(k) = f(b) \circ e_B = f(b)$

   (b) Сюръективность очевидна (у каждого образа действительно есть прообраз)

   (c) Инъективность Пусть $f(a) = f(b)$ Тогда $f^{-1}(a) \circ f(b) = e_B$
   $f(a^{-1}) \circ f(b) = e_B \quad f(a^{-1} * b) = e_B$
   $a^{-1} * b \in Ker\ f \Rightarrow a(Ker\ f) = b(Ker\ f)$

   (d) φ – гомоморфизм
   $\varphi(a(ker\ f) * b(Ker\ f)) = \varphi((a * b)(ker\ f)) = f(a * b) = f(a) \circ f(b) = \varphi(a(Ker\ f)) \circ \varphi(b(Ker\ f))$

   Т.О. φ – изоморфизм, что и требовалось доказать

□

Теорема 2.13 (Кэли). *Всякая конечная группа порядка n изоморфна подгруппе S_n*

Доказательство. $|G| = n = \{a_1 \dots a_n\}$, где $a_1 = e$

$g \in G$ тогда $\alpha_g := \begin{pmatrix} a_1 & \dots & a_n \\ g * a_1 & \dots & g * a_n \end{pmatrix}$

α_g – перестановка $a_i \neq a_j$ тогда $g * a_i \neq g * a_j$

$H = \{\alpha_{a_1}, \alpha_{a_2}, \dots, \alpha_{a_n}\} \subseteq S_n$

Композиция перестановок такого вида – перестановка такого вида.

ф. $\alpha_g, \alpha_f \in H$

ф. $x \in G \quad \alpha_g \circ \alpha_f(x) = \alpha_g(\alpha_f(x)) = \alpha_g(f * x) = g * (f * x) = (g * f) * x = \alpha_{g*f}(x)$

$\alpha_g \in H$ Тогда $\alpha_{g^{-1}}$ будет обратным.

Т.О. $H \leqslant S_n$

Докажем, что $H \cong G$

$\varphi : G \to H \quad g \mapsto \alpha g$

Сюръективность очевидна

Инъективность $\alpha_{g_1} = \alpha_{g_2} \Rightarrow \alpha_{g(1)}(a_1) = \alpha_{g_2}(a_1) \Rightarrow g_1 * e = g_2 * e \Rightarrow g_1 = g_2$

Гомоморфизм ф. $x \in G \quad \alpha_{g-1*g_2}(x) = g_1 * g_2 * x = (\alpha_{g_1} \circ \alpha_{g_2})(x)$

Т.О. φ – изоморфизм □