Содержание

Часть I

3 семестр. Основы теории групп.

1 Самые начала теории групп

1.1 Основные классы алгебраических систем

Для определения группы введем несколько новых страшных понятий.
Группоид — это множество чего угодно +бинарная операция.
Полугруппа — группоид + ассоциативность операции, т.е. $(x * y) * z = x * (y * z)$.
Моноид — полугруппа + нейтральный элемент, т.е. $(e * x = x * e = x)$ или $(0 + x = x + 0 = x)$.
Выдохнули и забыли эти слова до экзамена.

1.2 Группа

Группа — моноид + обратный элемент для каждого жителя нашего множества, т.е. $x * x^{-1} = x^{-1} * x = e$.
Согласно сложившейся традиции будем обозначать произвольную группу латинской G.
Свойства групп:

1. Единственность нейтрального элемента
   ◄ Пусть $\exists e_1, e_2 \in G$. Тогда $e_1 = e_1 * e_2 = e_2$ ►

2. Единственность обратного элемента
   ◄ Пусть $\exists x_1^{-1}, x_2^{-1} \in G : x * x_1^{-1} = e, x * x_2^{-1} = e$. Тогда $x * x_1^{-1} = e = x * x_2^{-1}$. Домножаем слева на x^{-1} и получаем $x_1^{-1} = x_2^{-1}$ ►

3. $(x * y)^{-1} = y^{-1} * x^{-1}$
   Сперва одеваешь рубашку, а потом пиджак; снимаешь наоборот. (c)
   Если более строго, то
   ◄$(x * y)^{-1} * (x * y) = e$, $(y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * x) * y = y^{-1} * y = e \to (x * y)^{-1} = y^{-1} * x^{-1}$►

4. $(x^{-1})^n = (x^n)^{-1}, n \in \mathbb{N}$
   ◀!▶

5. $x^n * x^m = x^{n+m} n, m \in \mathbb{Z}$
   ◀!▶

6. Уравнение $ax = b$ имеет единственное решение $x = a^{-1}b$ $(xa = b \Rightarrow x = ba^{-1})$
   ◀!▶

7. $xy = e \Rightarrow y = x^{-1}$
   ◀!▶

Пожалуйста, обратите внимание на тривиальные доказательства единственности. Всякий уважающий себя студент должен их воспроизвести даже во сне.

Еще несколько полезных определений, которые необходимо знать.
Коммутативная группа(абелева) — группа, в которой есть коммутативноста, т.е. $\forall x, y \in \mathbb{G} \Rightarrow xy = yx)$
Порядок группы $(|\mathbb{G}|)$ -число элементов в группе.
Порядок элемента $(|x|) = min\{n \in \mathbb{N} : x^n = e\}$ (т.е. минимальная натуральная степень, в которую нужно возвести элемент, что бы он превратился в "единицу").

1.3 Подгруппа

Проводим аналогию с подпространствами и радуемся таким знакомым понятиям.
Подмножество H группы G называется **подгруппой** этой группы, если оно само является группой относительно той же операции. $\mathbb{H} \leq \mathbb{G}$; $\mathbb{G} : \mathbb{H}$ является группой относительно той же операции.

Тривиальные подгруппы- это e и $\mathbb{G}$

Если $\mathbb{H} \leq \mathbb{G}$ и $\mathbb{H} \neq \mathbb{G}$, то будем писать $\mathbb{H} < \mathbb{G}$.

Т. о равенстве единичных элементов в группе и подгруппе $H < G \Rightarrow e_H = e_G$ ◀$h \in \mathbb{H} \to he_H = h; he_G = h \Rightarrow e_G g^{-1} he_H = h^{-1}h = e_G e_H \Rightarrow e_H = e_G$▶

Т. о равенстве обратных элементов $H < G, h \in H \Rightarrow h_H^{-1} = h_G^{-1}$ ◀!▶

*!!**Критерий подгруппы:** $\urcorner H < G$ и $H < G \Leftrightarrow$

$$\begin{cases} H \neq \varnothing \\ x \in H \\ y \in H \end{cases}$$

, то $xy = H$

$\urcorner G$ -конечная группа

Пусть $H < G \Rightarrow$

$$\begin{cases} H \neq \varnothing \\ x, y \in H, xy \in H \end{cases}$$

$x \in H \Rightarrow x^k < H, \forall k \in N$, т.к. $|G| < \infty \Rightarrow El, m : x^l = x^m \Rightarrow x^{l-m} \Rightarrow= e \Rightarrow e \in H$!!*

2 Не самые начала теории групп

2.1 Отношение эквивалентности

Отношения на множестве M: $T \leq M * M = \{(a,b) : a, b \in M\}$

$aTb \Leftrightarrow (a,b) \in T$

Примеры:

1. $T = \varnothing$
2. $T = M * M$
3. $M = R, aTb \Leftrightarrow a <= b$
4. $M = R, aTb \Leftrightarrow b = a^2$

T называется **отношением эквивалентности**, если оно удовлетворяет следующим условиям:

1. aTa (рефлексивность)
2. $aTb \to bTa$ (симметричность)
3. $aTb, bTc \to aTc$ (транзитивность)

Будем иметь ввиду вместо $aTb = a \sim b$, $T_a = \{b \in M : a \sim b\}$

Теорема:

1. $a \in T_a$
   ◄!►
2. $\bigcup_{a \in M} T_a = M$
   ◄!►
3. $T_a \bigcap T_b \neq \varnothing \to T_a = T_b$ ◄!►

Итак: M разбито на непересекающиеся подмножества $M \to M/\sim$ (факторизация)

Пара необходимых теорем о отношениях эквивалентности:

1. $\left.\begin{matrix} a \sim a' \\ b \sim b' \end{matrix}\right\} \to \begin{cases} [a'+b'] = [a+b] \\ [a'b'] = [ab] \end{cases}$
   $\blacktriangleleft a' = a + nl; b' = b + nk$
   $a' + b' = a + b + n(l+k) \to [a'+b'] = [a+b]$
   $a'b' = ab + n(ak + bl + nlk) \to [a'b'] = [ab] \blacktriangleright$

2. $H < G, \cdot$

   $|T_x| = |T_z| = |H|$

   $\blacktriangleleft xh_1 = xh_2 \to h_1 = h_2 \blacktriangleright$

Пример: $H < Gx \sim y \leftrightarrow x^{-1}y \in H \leftrightarrow \exists h \in H : x^{-1}y = h \leftrightarrow y = xh, h \in H$; таким образом $T_x = \{y : x \sim y\} = \{y : y = xh\} = xH$;

2.2 Немного(совсем) о кольцах

Если $(Z, +)$ и $(nZ, +)$, то $a \to a + nZ$

Вместо $a \to a + nZ$ будем писать $[a]_n$ или $\bar{a_n}$ или $\bar{a}$ или(like a pro) a

$Z/_\sim = Z/_{nZ} = Z_n$

Кольцо$(A, *, +)$ $\bigoplus$-коммутативность $\bigodot$-дистрибутивность

Бывают кольца коммутативные$(ab = ba)$ и с единицей$(ea = ae = a)$

Подкольцо-это кольцо относительно тех же операций

Поле-коммутативное ассоциативное кольцо с единицей $e \neq 0$.Кроме того, $\forall x \neq 0 \exists x^{-1}(xx^{-1} = x^{-1}x = e)$

$[a]_n + [b]_n = [a+b]_n$ и $[a]_n[b]_n = [ab]_n$

2.3 Циклические группы

Циклическая группа $\mathbb{G}$ - это такая группа, что $\exists a \in \mathbb{G} : \mathbb{G} = \{a^k, k \in \mathbb{Z}\}$ (можно так же сказать, что циклическая подгруппа состоит из всех степеней элемента).

Традиционно обозначается $G =< x >_n$, где n - порядок элемента. Путем нехитрых умозаключений можно сказать, что:

Циклическая группа называется **конечной**, если $|\mathbb{G}| < \infty; |\mathbb{G}| = n \Rightarrow \mathbb{G} = \{e, a, a^2, \ldots, a^{n-1}\}, a^n = e$

Циклическая группа называется **бесконечной**, если $|\mathbb{G}| = \infty \Rightarrow \mathbb{G} = \{e, a, a^{-1}, a^2, a^{-2}, \ldots, a^k, a^{-k}, \ldots\}$

Необходимые формулы и утверждения о циклических группах:

1. $|x^k| = \frac{|x|}{(|x|,k)}$
   ◄!►

2. $x^n x^m = x^{n+m}; (x^n)^m = x^{nm}; x^0 = e$ при $n, m \in \mathbb{Z}$
   ◄!►

3. $G, x \quad < x >= \{x^n,$ где $n \in Z\}$-циклическая подгруппа группы G

Если $|x| = n < \infty \rightarrow < x >= \{e, x, x^2, \ldots, x^{n-1}\}$
Если $|x| = \infty \rightarrow < x >= \{e, x, x^{-1}, x^2, x^{-2}, \ldots\}$
$< x >_n$,т.е. $| < x >_n | = |x| = n$
$< x >_\infty$ т.е. $| < x >_\infty | = |x| = \infty$ См. семинар для св-в (Кострикин)
G-циклическая группа, если $\exists x \in \mathbb{G} : \mathbb{G} =< x >$
Теоремы о циклических группах:

Теорема. У циклической группы все подгруппы циклические, т.е. G-циклическая группа.($H < G \Rightarrow H$-циклическая группа)
◄!►

Теорема. G-циклическая группа, пусть $|\mathbb{G}| = n$и $n \vdots k \Rightarrow \exists! H < G : |H| = k$
◄!►

*!!$\mathbb{Z}_n$-поле $\leftrightarrow$ n-простое
$\mathbb{Z}_n \quad k-$обратим в $\mathbb{Z}_n \leftrightarrow n$ и k-взаимно просты $\{(n, k) = 1\}$
$\phi : G_1 \rightarrow G_2$ называется изоморфизмом, если $\begin{cases} \phi(gh) = \phi(g)\phi(h) \\ \phi\text{-биекция} \end{cases}$
$\urcorner G =< x >, \cdot$
-Если $|G| = \infty \Rightarrow G \cong \mathbb{Z}, + \quad (\mathbb{Z} =< 1 >)(G_1 \cong G_2)$, то группы называются изоморфными.
-Если $|G| = n < \infty \Rightarrow G \cong \mathbb{Z}_n, +$!!*

2.4 Подстановки

S_n-группа подстановок(так же называют симметричной группой)
$x = \{1, 2, 3, \ldots, n\}$, S_n-мн-во биективных функций $\varphi : X \rightarrow X$
$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ \varphi(1) & \varphi(2) & \varphi(3) & \varphi(4) & \ldots & \varphi(n) \end{pmatrix}$

Примеры: $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$
$\varphi(1) = 2, \varphi(2) = 4, \varphi(3) = 3, \varphi(4) = 1$
$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$
$(\varphi\phi)(1) = \varphi(\phi(1)) = \varphi(4) = 1$
$\varphi^{-1}\varphi = \varphi\varphi^{-1} = e$
$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$
$\varphi^{-1} = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 3 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 3 \\ 4 & 1 & 3 & 2 \end{pmatrix}$
S_n-группа $\qquad |S_n| = n!$
Цикл
$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (124)(3) = (3)(124)$
$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34) = (34)(12)$

Независимые циклы - это такие циклы,в которых числа входят в один цикл, но не входят во второй цикл. Например, (123)(456) - независимый.
Более обще: цикл вида $(i_1 i_2 ... i_k)(i_{k+1} ... i_{k+l})...(i_{k+p} ... i_{k+n})$, где все i_j различны, будем называть независимым.
Циклом длины два называется **транспозиция.**

Теоремы:

1. Независимые циклы коммутируют друг с другом (или α, β-независимые циклы $\rightarrow \alpha\beta = \beta\alpha$)

2. Если $\alpha = (i_1, i_2, \dots, i_k)$-цикл длины $k \rightarrow |\alpha| = k$

3. Пусть $\varphi = \alpha_1\alpha_2 \dots \alpha_n$- произведение независимых циклов.
   $\alpha_1 = (i_1, i_2, \dots, i_k)$
   $\alpha_2 = (j_1, j_2, \dots, j_l) \rightarrow |\varphi| =$НОК$(|\alpha_1|, |\alpha_2|, \dots, |\alpha_m|)$

$|G| =$ НОК$(k_1, k_2, \dots, k_m)$
◀!▶

Определение: Инверсия ij - это если $i > j$, но i левее j.

Подстановка $G = \begin{pmatrix} l_1 & l_2 & \dots & l_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$ называется четной, если сумма инверсий в верхней и нижней строках четная. Иначе- нечетная.

Знак подстановки $sgnG = (-1)^{[l_1 l_2 \dots l_n]+[k_1 k_2 \dots k_n]}$

G-четная, если$sgnG = 1$

-нечетная, если$sgnG = -1$

$|\alpha| = k \to sgn\alpha = (-1)^{k-1} \quad (= (-1)^{k+1})$

$\alpha = (ij) = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ 1 & 2 & \dots & j & \dots & i & \dots & n \end{pmatrix}$-нечет

$G = \alpha_1 \alpha_2 \cdot \dots \cdot \alpha_n$-произведение независимых циклов.

$sgnG = (-1)^{n-m} \quad (= (-1)^{n+m})$

3 Какие подгруппы вообще бывают нормальными?

3.1 Классы смежности

$H < G \quad x \sim y \quad x^{-1}y \in H \leftrightarrow y \in xH$(**Левый смежный класс**)

$yx^{-1} \in H \leftrightarrow y \in Hx$(**Правый смежный класс**)

Если G-коммутативна, то $xH = Hx$

Множество левых смежных классов обозначается $G \diagup H$

Множество правых смежных классов обозначается $H \diagdown G$

$|G \diagup H| = |H \diagdown G|$ =индекс подгруппы

3.2 Нормальная подгруппа

Пусть $H < G$

Пытаемся ввести операцию $(xH)(yH) = (xy)H$. Когда она корректна?

Когда $\begin{cases} x \sim x' \\ y \sim y' \end{cases} \rightarrow xy \sim x'y' \; xy \sim x'y' = xh_1yh_2$

$xy = xh_1yh_2h_3 \qquad \Big| \cdot x^{-1}$

$y = h_1yh_4$

$e = y^{-1}h_1yh_4$

$y^{-1}h_1y = h_5 \rightarrow \boxed{y^{-1}Hy \leq H \quad \forall y \in G(1)}$

Из (1) $\rightarrow H \leq yHy^1 \quad \forall y \rightarrow H \leq y^{-1}Hy \leftrightarrow \boxed{y^{-1}Hy = H \quad \forall y \in G(2)} \leftrightarrow$ $\boxed{Hy = yH \quad \forall y \in G(3)}$

(1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (1).

$H < G$ называется **нормальной**, если выполнено любое из 3 равносильных условий.

В этом случае пишут $H \lhd G$

$\rceil H \lhd \rightarrow G/H$-группа относительно $(xH)(yH) = xyH$

Группа G/H называется **фактор-группой** группы G по нормальной подгруппе H.

4 Лагранж гуляет с Эйлером

4.1 Теорема Лагранжа со своими следствиями

Теорема Лагранжа Если $|G| = n < \infty \to |G| \vdots |H|$, что равносильно определению $|G| = |H| \cdot |{}_{G}\diagup^{H}|$где группа G-конечная группа

Следствия из теоремы Лагранжа:

1. $|G| \vdots |x|$

   $\blacktriangleleft x \Rightarrow H =< x >, |H| = |x| \blacktriangleright$

2. $|H| \Big| |G|$

3. $x \in G \to |x| \Big| |G|$

4. $|G| = p -$ простое число $\to G$циклическая группа, причем если$g \neq e \to G =< g >$

5. $|G| = n$
   $g \in G \to g^n = e$

6. **Малая теорема Ферма**
   $a^p \equiv a (mod\, p)$

7. **Теорема Вильсона**

   $(p-1)! + 1 \vdots p \leftrightarrow p -$ простое

4.2 Пара слов об Эйлере

Функция Эйлера$\{\varphi(n)\}$ равна количеству натуральных чисел, меньших чем n и взаимно простых с n.

Теорема Эйлера $a^{\phi(n)} \equiv 1 (mod\, n)$

Свойства $\varphi(n)$**:**

1. $\phi(p) = p - 1, p -$ простое

2. $\phi(p^n) = p^n - p^{n-1}, p -$ простое

3. $\phi(mn) = \phi(m)\phi(n), \qquad (m,n) = 1$

5 Морфизмы

Гомоморфизм $\phi : G_1 \to G_2$ -если $\phi(xy) = \phi(x)\phi(y)$

Мономорфизм — инъективный гоморфизм

Эпиморфизм — сюръективный гомомрфизм.

Эндоморфизм — если $G_1 = G_2$

Автоморфизм — изоморфизм+эндоморфизм

$Ker\phi = \{x \in G_1 : \phi(x) = e_2\} \qquad (= \phi^{-1}(e_2))$ — ядро гомоморфизма.

$Im\phi = \{z \in G_2; \exists x \in G_1 : \phi(x) = z\} = \{\phi(x), x \in G_1\} = \phi(G_1)$ — образ гоморфизма.

Свойства гомоморфизма:

1. $\phi(e_1) = e_2 \qquad$ или $e_G \to e_H$
   ◀▶
2. $\phi(x^{-1}) = (\phi(x))^{-1} \qquad$ или $x \to y$ то $x^{-1} \to y^{-1}$
   ◀▶
3. $|\phi(x)| \,\big|\, |x|$
   ◀!▶
4. $Im\phi < H \qquad Im\phi = \{\phi(x), x \in G\}$
   ◀!▶
5. $Ker\phi < G \qquad Ker\phi = \{\phi^{-1}(e_H)\}$
   ◀!▶
6. $Ker\phi \lhd G$
   ◀!▶
7. $\phi(x_1) = \phi(x_2) \leftrightarrow x_1 \equiv x_2 (mod\, Ker\phi)$
   ◀!▶
8. $\phi -$ мономорфизм $\leftrightarrow Ker\phi = \{e\}$
   ◀!▶
9. $\phi : G \to H, \psi : H \to K -$ гоморфизм $\to \psi \cdot \phi : G \to K -$ гоморфизм
   ◀!▶
10. $\phi : G \to H -$ изомрфизм $\to \phi^{-1} -$ изомрфизм
    ◀!▶

11. ϕ-изоморфизм, то $|\phi(x)| = |x|$
◀!▶

Док-во 6-го св-ва: $\rceil x_1, x_2 \in Ker\phi \to x_1x_2 \in Ker\phi$
$\phi(x_1) = e$
$\phi(x_2) = e$
$\phi(x_1x_2) = \phi(x_1)\phi(x_2) = e \cdot e = e$

6 Прямое произведение

Прямое произведение групп

$G_1, G_2, \dots, G_n$ – группы $(\cdot)$ $\quad G = G_1 \times G_2 \times \dots \times G_n = \{(g_1, g_2, \dots, g_n) : g_i \in G_i, i = 1, \dots, n\}$

Введем операцию $(g_1, g_2, \dots, g_n) \cdot (g_1', g_2', \dots, g_n') = (g_1 g_1', g_2, g_2', \dots, g_n g_n')$

Внешнее прямое произведение: $G = G_1 \times G_2 \times \dots \ (\cdot) \qquad G = G_1 \oplus G_2 \oplus G_3 \oplus \dots \oplus G_n \ (+)$

Свойства внешнего прямого произведения:

1. G-группа
2. $\tilde{G_i} = \{(e_1, e_2, \dots, e_{i-1}, g_i, e_{i+1}, \dots, e_n) < G\} \qquad = \{e_1\} \times \{e_2\} \times \dots \times \{e_{i-1}\} \times G_i \times \{e_{i+1}\} \dots \{e_n\}$
3. $\tilde{G_1} \cong G_i \quad (\phi_i : G_i \to \tilde{G_i} \ \phi_i(g_i)) = (e_1, e_2, \dots, e_{i-1}, g_i, e_{i+1}, \dots e_n)$ – Изоморфизм
4. $\tilde{G_i} \lhd G$
5. $\forall g \in G \, \exists \tilde{g_1} \in \tilde{G_1}, \dots, \ \tilde{g_n} \in \tilde{G_n} : g = \tilde{g_1}\tilde{g_2}\tilde{g_3} \dots \tilde{g_n}$
6. $\forall g \in G \exists! \tilde{g_1} \in \tilde{G_1}, \dots, \ \tilde{g_n} \in \tilde{G_n} : g = \tilde{g_1}\tilde{g_2}\tilde{g_3} \dots \tilde{g_n}$
7. $\tilde{G_i} \cap \tilde{G_j} = \{e\} \quad (i \neq j)$
8. $\tilde{g_1} \in \tilde{G_i}, \tilde{g_j} \in \tilde{G_j} \to \tilde{g_i}\tilde{g_j} \to \tilde{g_j}\tilde{g_i}$
9. $|G| = |G_1||G_2| \dots |G_n|$
10. $|(g_1, g_2, \dots, g_n)| =$ НОК$(|g_1|, |g_2|, \dots, |g_n|)$
11. $\rceil G_1 =< g_1 >_{k_1}, \dots, G_n =< g_n >_{k_n}$ $\qquad$ G-циклическая группа $\Leftrightarrow$ у$k_1, \dots, k_n$нет общих делителей $\quad \lhd$ на дом$\rhd$
    Пример: $C_2 \times C_3 \cong C_6 \, (\cdot)$
    $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \, (+)$

G, $G_1, G_2, \dots, G_n < G$

1. $(6 \Rightarrow 5)$

2. $6 \Rightarrow 7$, то если $\forall g \in G \exists! g_1 \in G_1, \dots, g_n \in G_n : g = g_1 g_2 \dots g_n \Rightarrow G_i \cap G_j = \{e\} \quad (i \neq j)$
   $\lhd$ От противного. Пусть $g \in G_i \cap G_j \Rightarrow g = ee \dots g \dots e \dots e = ee \dots e \dots g \dots e \Rightarrow g = e \Rightarrow G_i \cap G_j = \{e\} \rhd$

3. $\left.\begin{matrix}4\\7\end{matrix}\right\} \Rightarrow 8$ т.е. если $G_i \lhd G_j \quad G_j \lhd G_i, G_i \cap G_j = \{e\} \Rightarrow g_i g_j = g_j g_i (\Leftrightarrow g_i g_j g_i^{-1} g_j^{-1} = e)$

Внутренне прямое произведение:
$G, \quad G_i, \dots, G_n < G$
G – внутренне прямое произведение этих подгрупп, если

1. $\forall g \in G \exists! g_1, \dots, g_n : g = g_1 g_2 \dots g_n$
2. $G_i \lhd G_i; i = 1, \dots n$

Теорема G изоморфно $G_1 \times G_2 \times \dots \times G_n$
(т.е. внутреннее прямое произведние изоморфно внешнему)
$\lhd \phi : G_1 \times \dots \times G_n \to G$
$\phi((g_1, g_2, \dots, g_n)) = g_1 g_2 \dots g_n$
ϕ-гомоморфизм ?$\phi((g_1 \dots, g_n)(h_1, \dots, h_n) = \phi(g_1 h_1, g_2 h_2, \dots, g_n h_n) = g_1 h_1 g_2 h_2 \dots g_n h_n$
$\phi\phi((g_1 \dots, g_n)(h_1, \dots, h_n) = g_1 g_2 \dots g_n h_1 h_2 \dots h_n$Сие выражение выходит из предыдущей строки благодаря свойству 8

ϕ-эпиморфизм. Пусть$g \in G \to \exists g_1, \dots g_n : g = g_1 \dots g_n \to \phi((g_1, \dots, g_n)) = g_1 \dots g_n = g$
ϕ-мономорфизм $\quad Ker\phi = \{((g_1, \dots, g_n) : g_1 g_2 \dots g_n = e)\} \to g_1 = g_2 = \dots = g_n = e$

$$** \begin{cases} \forall g! = g_1 \dots g_n & (1) \\ g_i g_j = g_j g_i & (2) \end{cases} \Leftrightarrow * \begin{cases} \forall g! = g_1 \dots g_n & (1) \\ G_i \lhd G & (2) \end{cases}$$

гдеg_i-элемент i-ой группы, аg_j-элемент j-ой группы $\lhd \to (1) ** \to (1) *$
$(1) ** \to G_i \cap G_j = \{e\} \qquad \rceil g \in G_i \cap G_j \to g = e \cdot e \dots e \cdot g \cdot e \dots e = e \dots ege \dots e \to g = e$
$g g_i g^{-1} = g_1‘ g_2‘ \dots g_n‘ g_i‘ (g_n‘)^{-1} \dots (g_1‘)^{-1} = g_i‘ g_i (g_1‘)^{-1} \in G_i \to G_i \lhd G \rhd$
$\lhd \leftarrow (1)* \to (1) ** \to G_i \cap G_j = \{e\} \qquad G_i \lhd G$
Требуется доказать:$g_i g_j = g_j g_i$, т.е.$g_i g_j g_i^{-1} g_j^{-1} = e$

G-внутреннее прямое произведение, если выполнена (*) ($\Leftrightarrow$ Выполнена (**))

Примеры:

1. $G=\mathbb{Z},+$ не раскладывается в внутренние прямые суммы
$G_n = n\mathbb{Z}$-других подгрупп нет На дом: продумать и записать доказательство.
$nm \in n\mathbb{Z} \cap m\mathbb{Z} \to n\mathbb{Z} \cap m\mathbb{Z} \neq \{0\}$

2. $G=\mathbb{C}^*,\cdot$
$G_1=\mathbb{R}_{>0}=\{x>0, x\in R\}$
$G_2=U=\mathbb{T}=\{z:|z|=1\}=\{z=e^{i\phi}\}$
$G=G_1\times G_2?$ G-коммутативна
$z\in G\to z=|z|e^{i\phi}$ $(|z|>0 \quad e^{i\phi\in U})$
$\rceil z=x_1u_1=x_2u_2 \to ? \begin{cases} x_1=x_2 \\ u_2=u_2 \end{cases} \qquad x_1x_2^{-1}=u_1^{-1}u_2 \to \begin{cases} x_1x_2^{-1}=1 \\ u_1^{-1}u_2=1 \end{cases} \to$
$\begin{cases} x_1=x_2 \\ u_2=u_2 \end{cases}$

$(G_1\times G_2)/G_1\cong G_2$
$\lhd \quad \phi: G_1\times G_2\to G_2$
$\phi((g_1g_2))=g_2$
ϕ-гомоморфизм ? $\phi((g_1,g_2)(g_1`,g_2`))=\phi((g_1g_1`,g_2g_2`))=g_2g_2`$
$\phi((g_1,g_2))\cdot\phi((g_1`,g_2`))=g_2g_2`\to\phi((g_1,g_2)(g_1`,g_2`)$
$Ker\phi=\{(g_1,g_2):\phi(g_1,g_2)=e\}\to Ker\phi=\{(g_1,e)\}=G_1$
$Im\phi=\{\phi((g_1,g_2))\}=\{g_2\}=G_2\to G_1\times G_2/G_1\cong G_2$
Следствия. Если $G_1\lhd G, G/G_1\ncong G_2\to G\ncong G_1\times G_2$
ACHTUNG $G/G_1\cong G_2 \not\to G=G_1\times G_2$
Пример $C_4=\{e,a,a^2,a^3\}$ $\quad C_2=\{e,a^2\}\lhd C_4$
$C_4/C_2=C_2$,но $C_4\neq C_2\times C_2$
т. Кэлли $\forall$ конечная группа $G, |G|=n$ изоморфна подгруппе S_n
$\lhd|G|=n\Rightarrow G=\{g_1,g_2,g_3,\dots,g_n\}$
$S(G)$-все биектифные функции на множестве G $\to S(G)=S_n \quad \phi: G\to S_n \qquad \phi_g=G\to G$ $\quad g$-фиксированный элемент $\in G$

$$\phi_g(x)=g\lambda \quad \begin{Bmatrix} g_1 & g_2 & \dots & g_n \\ \dots & & & \\ g_ig_1 & g_ig_2 & \dots & g_ig_n \end{Bmatrix}$$

7 Интересные моменты, необходимые для решения задач

7.1 Группа диэдра

7.2 Группа кватернионов

7.3 Как определить прямое произведение групп?

8 Вопросы к коллоквиуму

1. Группоид
2. Полугруппа
3. Моноид
4. Группа
5. Порядок группы(|G|)
6. Порядок элемента(|x|)
7. Циклическая группа
8. Определение подгруппы
9. Чему равен $|x^k|$?
10. Критерий подгруппы
11. Отношение эквивалентности
12. Левый и Правый смежные классы
13. Теорема Лагранжа
14. Малая теорема Ферма
15. Функция Эйлера
16. т. Эйлера
17. т. Вильсона
18. Нормальность группы
19. Фактор-группа
20. Автоморфизм
21. AutG
22. Внутренний автоморфизм

23. IntG
24. Гомоморфизм
25. Мономорфизм
26. Эпиморфизм
27. Эндоморфизм
28. Ядро гомоморфизма
29. Образ гомоморфизма
30. Внешнее прямое произведение групп
31. Внутреннее прямое произведение групп
32. т. Кэли
33. Группа подстановок
34. Цикл
35. Независимые циклы
36. Транспозиция
37. Определение полупрямого произведения
38. Четность и нечетность подстановки
39. Знак подстановки
40. Знак произведения подстановок
41. Длина цикла
42. Порядок цикла
43. Порядок произведения независимых циклов