МАТЕРИАЛЫ К ЭКЗАМЕНУ ПО ЛИНЕЙНОЙ АЛГЕБРЕ (III СЕМЕСТР)

1. Бинарная алгебраическая операция.

Бинарная алгебраическая операция – это операция, принимающая два аргумента и возвращающая один результат. Если A, B, C – непустые множества, то отображение $P \to C$, где $P \in A \times B$ называется бинарной операцией. Если $A = B = C$, то действие операции называется внутренним. Если $A = C$ или $B = C$, то действие операции называется внешним.

2. Определение группы. Абелева группа. Примеры групп.

0) $\forall g_1, g_2 \in G \to g_1 * g_2 \in G$;
1) $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)\ \forall g_1, g_2, g_3 \in G$ (ассоциативность);
2) $\exists e \in G : g * e = e * g = g\ \forall g \in G$ (нейтральный эл-т);
3) $\forall g \in G\ \exists g^{-1} \in G : g * g^{-1} = g^{-1} * g = e$ (обратный эл-т);
0),1),2),3) $\Rightarrow$ $(G,*)$ – группа.
4) $g_1 * g_2 = g_2 * g_1\ \forall g_1, g_2 \in G$ (коммутативность)
0),1),2),3),4) $\Rightarrow$ $(G,*)$ – абелева группа.
Примеры: $(\mathbb{Z},+)$ – группа, $(\mathbb{Z},*)$ – не группа ($\nexists g^{-1}\ \forall g$)

3. Аддитивная и мультипликативная запись операции.

То же, что в пункте 2, но вместо операции $*$ операция $+$, в пункте 2) e замегяется на 0, в пункте 3) g^{-1} заменяется на $-g$.

4. Единственность нейтрального элемента в группе.

Пусть $\exists e_1, e_2 \in G : e_1 * g = g * e_1 = g, e_2 * g = g * e_2 = g\ \forall g \in G$. Тогда $e_1 * g = e_2 * g \Rightarrow e_1 * g * g^{-1} = e_2 * g * g^{-1} \Rightarrow e_1 = e_2 \Rightarrow \overset{\text{o}}{\text{X}} \Rightarrow \exists!\ e \in G : e * g = g * e = g$.

5. Единственность обратного элемента для каждого элемента группы.

Пусть $\forall g \in G\ \exists g_1^{-1}, g_2^{-1} \in G : g * g_1^{-1} = g_1^{-1} * g = e, g * g_2^{-1} = g_2^{-1} * g = e$. Тогда $g_1^{-1} * g = g_2^{-1} * g \Rightarrow g_1^{-1} * (g * g_1^{-1}) = g_2^{-1} * (g * g_2^{-1}) \Rightarrow g_1^{-1} = g_2^{-1} \Rightarrow \overset{\text{o}}{\text{X}} \Rightarrow \forall g \in G\ \exists!\ g^{-1} \in G : g * g^{-1} = g^{-1} * g = e$.

6. Определение подгруппы.

G – группа, H – непустое подмножество G, называется подгруппой G, если H является группой относительно операции группы G, ограниченной на H. Обозначается $H < G$.

7. Критерий того, что подмножество группы является подгруппой.

$(G,*)$ группа, $H \subset G$
1) $e \in H$
2) $\forall h_1, h_2 \in H \Rightarrow h_1 * h_2 \in H$
3) $\forall h \in H \Rightarrow h^{-1} \in H$

8. Порядок группы.

Количество элементов в группе $(G,*)$ называется её порядком $|G|$.

9. Порядок элемента группы.

$(G,*)$ – группа, $g \in G$, тогда порядком элемента $ord(g) = |g|$ называется минимальное натуральное число $m : \underbrace{g * g * \ldots * g}_{m} = g^m = e$.

10. Изоморфизм групп.

$(G,*), (H,+)$ – группы, тогда $\varphi: G \to H$ – изоморфизм групп, если
1) φ – биекция
2) $g_1, g_2 \in G, \varphi(g_1 * g_2) = \varphi(g_1) + \varphi(g_2) \in H$
$G \cong H \Leftrightarrow \exists \varphi: G \to H$ – изоморфизм.

11. Свойства изоморфизма.

$(G,*), (H,+)$ – группы, $\varphi: G \to H$ – изоморфизм, тогда верно следующее:
1) $e_G \in G$ переходит в $e_H \in H$

2) $g \in G, \varphi(g^{-1}) = \varphi(g)^{-1}$
3) $\varphi^{-1}: H \to G$ – тоже изоморфизм

12. Примеры изоморфных и неизоморфных групп.

Группы порядка 20, неизоморфные между собой:
$\mathbb{Z}_{20} \cong \mathbb{Z}_5 \times \mathbb{Z}_4$ – абелевы, максимальный порядок элемента 20
$\mathbb{Z}_{10} \times \mathbb{Z}_2 \cong \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ – абелевы, максимальный порядок элемента 10
D_{10} – не абелева

Стоит также знать группы $\mathbb{C}_n = \{z \in \mathbb{C} : z^n = 1\} = \left\{z = e^{i\frac{2\pi k}{n}}, k = 0, \dots, n-1\right\}$, $\mathbb{U} = \mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$

Чтобы найти все подгруппы группы G стоит искать циклические подгруппы порядков, являющихся делителями порядка группы G. Если G абелева, то найдётся ровно одна подгруппа подходящего порядка, если неабелева, некоторые подгруппы могут не найтись.

13. Определения кольца, поля, области целостности. Примеры.

$(K, +, *)$ – кольцо, если выполняются следующие утверждения:
0) $a, b \in K \Rightarrow a + b \in K, a * b \in K$
1) $a + b = b + a \; \forall a, b \in K$
2) $(a + b) + c = a + (b + c) \; \forall a, b, c \in K$
3) $\exists 0 : a + 0 = 0 + a = a \; \forall a \in K$
4) $\forall a \in K \; \exists (-a) \in K : a + (-a) = (-a) + a = 0$
5) $a * (b + c) = a * b + a * c \; \forall a, b, c \in K$
6) $(b + c) * a = b * a + c * a \; \forall a, b, c \in K$

Если выполняются также следующие утверждения, то $(K, +, *)$ – поле:
7) $(a * b) * c = a * (b * c)$ – ассоциативность
8) $\exists 1 \in K : 1 * a = a * 1 = a \; \forall a \in K$ – существование единичного элемента
9) $a * b = b * a \; \forall a, b \in K$ – коммутативность
10) $\forall a \in K : a \neq 0 \Rightarrow \exists a^{-1} \in K : a * a^{-1} = a^{-1} * a = 1$ – обратимость
11) $0 \neq 1$ (в поле есть два различных элемента)

Областью целостности (целостным кольцом) называется коммутативное ассоциативное кольцо с единицей, в котором нет делителей нуля и которое не является полем (элементы $a, b \in K$ называются делителями нуля, если $a \neq 0, b \neq 0$, но $a * b = 0$). В поле делителей нуля нет (док-во через умножение на обратный).

14. Кольцо целых чисел и кольцо многочленов над полем.

Кольцом целых чисел называется кольцо, элементами которого являются натуральные числа, им противоположные и 0 (и только они).

Кольцом многочленов над полем называется кольцо, образованное многочленами от одной или нескольких переменных с коэффициентами из данного кольца.

15. Наибольший общий делитель двух элементов целостного кольца.

Пусть K – область целостности, $a, b \in K$. Говорят, что b делит a ($b|a$), если $\exists c \in K : a = b * c$. Ассоциированными называются $a, b \in K : a \vdots b, b \vdots a$, т.е. $a = b * c, b = a * d$. Элемент d называется общим делителем a и b, если верно, что $d|a$ и $d|b$. Наибольшим общим делителем a и b ($\text{НОД}\{a, b\} = (a, b)$) называется их общий делитель, который делится на любой их общий делитель.

16. Взаимно простые элементы, обратимые элементы, простые элементы целостного кольца.

Элементы кольца называются взаимно простыми, они не имеют никаких общих делителей, кроме 1 и (-1). Элемент кольца a называется обратимым,

если для него существует обратный элемент $a^{-1} : a * a^{-1} = a^{-1} * a = 1$. Ненулевой необратимый элемент называется простым, если его нельзя представить в виде произведения двух необратимых элементов.

17. Алгоритм Евклида, выражение НОД двух элементов через них, теорема о разложении любого необратимого элемента на простые множители в кольце целых чисел.

Деление с остатком в $\mathbb{Z}$: $\forall a, b \in \mathbb{Z}\ \exists q, r \in \mathbb{Z} : a = b * q + r, 0 \leq |r| < |b|$. Если $r = 0$, то $a = b * q$, т.е. $b|a$ или $a \vdots b$ (делится без остатка). Алгоритм Евклида: $\forall a, b \in \mathbb{Z}\ \exists (a, b) \in \mathbb{Z}$, причём $\exists u, r \in \mathbb{Z} : (a, b) = a * u + b * v$.

1) $b = 0 \Rightarrow (a, b) = a = a * 1 + b * 0$
2) $a \vdots b \Rightarrow (a, b) = b = a * 0 + 1 * b$
3) $a = b * q_1 + r_1, 0 < |r_1| < |b|$
   $b = r_1 * q_2 + r_2, 0 < |r_2| < |r_1|$
   $r_1 = r_2 * q_3 + r_3, 0 < |r_3| < |r_2|$
   $\ldots r_{n-1} = r_n * q_n$, тогда $r_n = \text{НОД}\{a, b\} = (a, b)$ – общий делитель a и b. Кольцо, в котором определено деление с остатком, называется евклидовым.

$(a, b) = 1 \Leftrightarrow \exists x, y : ax + by = 1$, но $(a, b) = d \Rightarrow \exists x, y : ax + by = d$ (доказывается алгоритмом Евклида, x, y ищутся с помощью преобразования матрицы $\begin{pmatrix} a & b \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$).

18. Наименьшее общее кратное двух элементов, выражение для НОД и НОК двух элементов кольца целых чисел через их простые множители (делители).

$a, b \in K$ – область целостности. $\text{НОК}\{a, b\} = [a, b]$ – элемент, который делит любое общее кратное a, b. НОД – это произведение множителей, входящих в разложение обоих чисел. $\text{НОК}\{a, b\} = [a, b] = \frac{a*b}{(a,b)}$.

19. Циклическая группа. Порядок ее элементов.

Циклической называется группа, все элементы которой порождаются одним элементом, этот элемент называется образующим. Порядок циклической группы является порядком образующего элемента. Циклическая группа всегда абелева.

$(G,*)$ – группа, $g \in G \Rightarrow g^m = \underbrace{g * g * \ldots * g}_{m}, g^{-m} = \underbrace{g^{-1} * g^{-1} * \ldots * g^{-1}}_{m}, m \in \mathbb{Z}$, $g^0 = e, (g^m)^k = g^{mk}$. Каждая конечная циклическая группа порядка n изоморфна группе $\mathbb{Z}_n$. $G =< g >, ord(g) = n \Rightarrow ord(g^k) = \frac{n}{(n,k)}$.

20. Свойства порядка элемента группы. Бесконечные и конечные циклические группы.

$(G,*)$ – группа, $g \in G$, тогда $ord(g)$ – минимальное $n \in \mathbb{N} : g^n = e$, если такое существует. Иначе $ord(g) = \infty$. $ord(g) = \infty \Rightarrow g^m \neq g^l\ (m \neq l)$, т.к. $g^m = g^l \Rightarrow g^{m-l} = e \Rightarrow m - l = 0 \Rightarrow m = l \Rightarrow \overset{o}{X}$ или $m - l = ord(g) = \infty \Rightarrow \overset{o}{X}$.

$ord(g) = n < \infty$, $g^m = e \Rightarrow n|m$. $ord(g) = n, g^m = g^k \Leftrightarrow m \equiv k\ (mod\ n)$.

21. Циклическая подгруппа, порожденная данным элементом.

$(G,*)$ – группа, $g \in G \Rightarrow < g >$ – подгруппа G.

22. Подгруппы циклической группы.

Подгруппа циклической группы – тоже циклическая группа.

23. Отношение эквивалентности на множестве.

Отношение эквивалентности на множестве G – это бинарное отношение, для которого выполнены следующие условия:

1) $a \sim a\ \forall a \in G$ (рефлексивность)

2) $\forall a, b \in G : a \sim b \Rightarrow b \sim a$ (симметричность)
3) $\forall a, b, c \in G : a \sim b, b \sim c \Rightarrow a \sim c$ (транзитивность)

24. Классы эквивалентных элементов.

Классом эквивалентности $\bar{a} \in G$ элемента $a \in G$ называется подмножество элементов ему эквивалентных: $\bar{a} = \{g \in G : g \sim a\}$. Классы эквивалентности либо не пересекаются, либо полностью совпадают.

25. Фактор множество.

Фактор множество – это множество всех классов эквивалентности заданного множества G по заданному отношению $\sim$, обозначается $G/\sim$.

26. Отношение сравнимости по модулю n в множестве целых чисел.

$a, b \in \mathbb{Z}$, тогда $a \sim b \ (mod\ n) \Leftrightarrow a \equiv b \ (mod\ n) \Leftrightarrow a - b \vdots n$ (имеют одинаковые остатки при делении на n).

27. Кольцо вычетов по модулю n.

$(\mathbb{Z}_n, +, *)$ – кольцо вычетов по модулю n, разбивается на классы эквивалентности отношением сравнимости по модулю n: $\mathbb{Z}_n = \{\overline{0}_n, \overline{1}_n, \dots, \overline{\overline{n-1}_n}\}$.

28. Его обратимые элементы.

У каждого ненулевого элемента кольца $\mathbb{Z}_n$ есть обратный. Док-во: пусть $m \in \mathbb{Z}_n$, тогда произведения $m * 0, m * 1, \dots, m * (n-1)$ – это n различных чисел, а т.к. в кольце $\mathbb{Z}_n$ ровно n классов эквивалентности, у нас есть по представителю от каждого класса, значит среди них найдётся $\overline{1}$, значит m - обратим. Исключением являются делители нуля, т.к. тогда мы получим меньше, чем n различных значений и среди них не найдётся $\overline{1}$ (сначала возьмём из разложения m те множители, которые не входят в разложение n, умножим их на числа $0, 1, \dots, n-1$ и получим n различных значений, затем умножим все эти значения на оставшиеся множители m, фактически на $\text{НОД}\{m, n\}$, тогда все значения будут кратны $\text{НОД}\{m, n\}$, значит среди них точно не найдётся $\overline{1}$). Таким образом, обратимыми являются все элементы кольца, кроме делителей нуля и, собственно, нуля.

Число обратимых элементов в кольце $\mathbb{Z}_n$ можно вычислить с помощью функции Эйлера $\varphi(n) = n * \left(1 - \frac{1}{p_1}\right) * \dots * \left(1 - \frac{1}{p_k}\right), n = p_1^{s_1} * \dots * p_k^{s_k}$ – количество натуральных чисел, взаимно простых с n, меньших n.

29. Критерий того, что это кольцо является полем.

Кольцо $\mathbb{Z}_n$ является полем, если и только если n – простое число. В этом случае в кольце нет делителей нуля, т.е. все элементы кольца обратимы.

30. Конечнопорождённые группы.

Конечнопорождённая группа – это группа, порождаемая конечной системой образующих. $(G, *)$ – группа, $S \subset G, < S > = \left\{g_1^{\varepsilon_{11}}, \dots g_1^{\varepsilon_{1s_1}}, \dots, g_k^{\varepsilon_{k1}}, \dots g_1^{\varepsilon_{ks_1}}, g_i \in S, \varepsilon_{ij} = \pm 1, i, j = \overline{1, k}, k \in \mathbb{N}\right\}$ – называется системой порождающих. Если $G =< S >$, говорят, что G порождается множеством элементов S.

31. Группа диэдра.

D_n – повороты правильного n-угольника вокруг центра на углы, кратные $\frac{2\pi}{n}$ и симметрии относительно осей, проходящих через центр и вершины или центр и середины сторон. $|D_n| = 2n, D_n =< u_{\frac{2\pi}{n}}, s >, ord\left(u_{\frac{2\pi}{n}}\right) = n, ord(s) = 2, s u_{\frac{2\pi}{n}} s = u_{-\frac{2\pi}{n}} = u_{\frac{2\pi}{n}}^{-1}$.

32. Критерий того, что группа, порожденная двумя элементами, изоморфна группе диэдра.

$G =< a, b >, ord(a) = n, ord(b) = 2\ (b = b^{-1}), b * a * b = a^{-1} \Rightarrow G \cong D_n$. Док-во: $b * a * b = a^{-1} \Rightarrow a * b = b * a^{-1}, b * a = a^{-1} * b$, кроме того $b * b = b * b^{-1} = id$, тогда $\forall g \in G =< a, b >, ord(a) = n, ord(b) = 2 :\ b * a * b = a^{-1} \Rightarrow \begin{cases} g = a^k, k \in \mathbb{Z} \\ g = b * a^k \end{cases}$ (если в выражении g через пораждающие есть b, то его можно вытащить вперёд) $\Rightarrow g_1 = a^k, g_2 = a^m \Rightarrow g_1 g_2 = a^{k+m}; g_1 = a^k, g_2 = b * a^m \Rightarrow g_1 g_2 = a^k * b * a^m = b * a^{-k} * a^m = b * a^{m-k};\ g_1 = b * a^k, g_2 = b * a^m \Rightarrow g_1 g_2 = b * a^k * b * a^m = b * b * a^{-k} * a^m = a^{m-k}$. Таблицы Кэли совпадают, значит это изоморфизм.

33. Группа кватернионов.

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}, i^2 = j^2 = k^2 = 1, ord(1) = 1, ord(-1) = 2$, для остальных $ord = 4$. Можно представить в матричном виде, как $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \in \mathbb{C}^{2\times 2}$. Умножение происходит так же, как векторное произведение базисных векторов правой тройки.

34. Критерий того, что группа, порожденная двумя элементами, изоморфна группе кватернионов.

$G =< a, b >, ord(a) = 4, a^2 = b^2, b^{-1} * a * b = a^{-1} \Rightarrow G \cong Q_8$. Док-во: $b^{-1} * a * b = a^{-1} \Rightarrow a * b = b * a^{-1}, a^{-1} b = b^{-1} * a * b * b = b^{-1} * a * b^2 = b^{-1} * a^3 = b^{-1} * a^{-1}$. Если в записи элемента через образующие есть b, то его можно вынести вперёд, тогда общий вид элемента $g = b^{\varepsilon} a^k, \varepsilon = \{-1, 0, 1\}, k \in \mathbb{Z}$, т.е. таблица Кэли определена однозначно.

35. Симметрическая группа. Ее порядок.

$S_n = \left\{\alpha = \begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix}\right\} = S(X), |S_n| = n!$ – её порядок, $S(X)$ – множество биективных отображений $X \to X, X = \{1, \dots, n\}$.

36. Умножение подстановок.

Справа налево. Стоит заметить, что $\alpha(i_1, \dots, i_k)\alpha^{-1} = \big(\alpha(i_1), \dots, \alpha(i_k)\big)$.

37. Разложение подстановки в произведение независимых циклов.

Любую подстановку можно разложить в произведение независимых циклов единственным образом, с точностью до перестановки сомножителей (независимые цикли перестановочны).

38. Цикленный тип подстановки.

Цикленный тип подстановки – набор чисел $(s_1, \dots s_l)$, каждое их которых соответствует длине независимого цикла, в произведение которых разлагается данная подстановка. Для подсчёта количества различных циклов из S_n длины k используется формула $C_n^k (k-1)!$.

39. Четность, нечетность, знак подстановки. Знак произведения подстановок.

$\alpha = \begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix} = \begin{pmatrix} l_1 & \cdots & l_n \\ s_1 & \cdots & s_n \end{pmatrix}$. Чётностью подстановки называется чётность числа, равного $[l_1, \dots, l_n] + [s_1, \dots, s_n]$, где $[l_1, \dots, l_n]$ – число транспозиций, требующихся для приведения $[l_1, \dots, l_n]$ к виду $[1, \dots, n]$. Знак подстановки – это $(-1)^{[l_1,\dots,l_n]+[s_1,\dots,s_n]}$. Причём $sgn(\alpha * \beta) = sgn(\alpha) * sng(\beta)$. Знак независимого цикла длины n определяется по формуле $(-1)^{n-1}$. Знак подстановки $\alpha \in S_n$ с цикленным типом $(k_1, \dots, k_m), k_1 + \cdots + k_m = n$ равен $(-1)^{n-m}$.

40. Порождаемость симметрической группы транспозициями.

$S_n =< (i,j) >, i,j = \overline{1,n}\,(i \neq j), (i,j)^{-1} = (i,j)$. Доказывается через последовательное выделение из некоторой подстановки транспозиций и постепенное приведение к виду Id.

41. Знакопеременная группа. Ее порядок.

$A_n \trianglelefteq S_n$ – группа чётных подстановок. $|A_n| = \frac{n!}{2}$.

42. Порождаемость знакопеременной группы тройными циклами.

$\forall \alpha \in A_n \Rightarrow \alpha$ - произведение чётного числа транспозиций $\Rightarrow A_n =< (i,j), (k,l) >\Rightarrow A_n =< (i,j,k) >$, т.к. $(i,j) * (j,k) = (i,j,k)$, а $(i,j)(k,l) = (i,j) * (j,k) * (j,k) * (k,l) = (i,j,k) * (j,k,l) \Rightarrow A_n =< (i,j,k) >$.

43. Сравнение элементов группы по модулю подгруппы. Левые и правые смежные классы группы по подгруппе.

$H < G, g_1, g_2 \in G$, говорят, что $g_1 \equiv g_2\ (mod\ H)$, если $g_1^{-1} g_2 \in H$. Это отношение эквивалентности (доказательство проверкой). Классы этого отношения эквивалентности называются левыми смежными классами группы G по подгруппе H. $Lg = \{g' \in G : g \equiv g' (mod\ H)\} = gH$ ($g \equiv g' (mod\ H) \Leftrightarrow g^{-1} g' \in H \Leftrightarrow \exists h \in H : g^{-1} g' = h \Leftrightarrow \exists h \in H : g' = gh$). Правые смежные классы задаются другим отношением эквивалентности: $g_1 \equiv g_2 (mod\ H) \Leftrightarrow g_1 g_2^{-1} H$, обозначается $Rg = Hg$.

44. Разбиение группы на смежные классы.

Множество левых смежных классов группы G по подгруппе H обозначается G/H, правых – $H\backslash G$. Если группа абелева, левые и правые смежные классы совпадают. Существует взаимно-обратное соответствие между G/H и $H\backslash G$ ($f(g) = g^{-1}, f: G \to G$ – биекция, тогда $f(gH) = Hg^{-1}$).

45. Индекс подгруппы в конечной группе.

Количество левых (правых) смежных классов группы G по подгруппе H называется индексом подгруппы H в группе G и обозначается $|G:H|$.

46. Теорема Лагранжа.

$|G| < \infty, H < G \Rightarrow |G| = |H| * |G:H|$. Док-во: $|Lg| = |gH| = |H|, gh_1 = gh_2 \Leftrightarrow h_1 = h_2$, т.е. G разбивается на непересекающееся левое множество классов $|G| = |H| * |G:H|$.

47. Следствия теоремы Лагранжа: о порядке подгруппы, о порядке элемента группы, о цикличности группы простого порядка, малая теорема Ферма, теорема Эйлера, теорема Вильсона.

О порядке группы: $|G| < \infty, H < G \Rightarrow |G| \vdots |H|$

О порядке элемента группы: $|G| < \infty, \forall g \in G \Rightarrow |G| \vdots ord(g)$, т.к. можно рассмотреть подгруппу $H =< G >, |H| = ord(g)$

О цикличности группы простого порядка: $|G| = p$ – простое, тогда G – циклическая группа, т.к. $\forall g \in G \Rightarrow \begin{cases} ord(g) = 1 \Leftrightarrow g \equiv e \\ ord(g) = p \Leftrightarrow ord(g) = |G| \Leftrightarrow G =< g > \end{cases}$

Малая теорема Ферма: p – простое, $(a,p) = 1 \Rightarrow a^{p-1} = 1 (mod\ p)$, т.к. $a \in \mathbb{Z}_p^*$, $\left|\mathbb{Z}_p^*\right| = p - 1, a^{|\mathbb{Z}_p^*|} = 1$ в $\mathbb{Z}_p^* \Rightarrow a^{p-1} = 1\ (mod\ p)$ (всегда справедливо, что $g \in G, g^{|G|} = e$, т.к. $|G| \vdots ord(g)$).

Теорема Эйлера: $(a,n) = 1 \Rightarrow a^{\varphi(n)} = 1\ (mod\ n)$, т.к. можно рассмотреть a как элемент кольца $\mathbb{Z}_n^* : |\mathbb{Z}_n^*| = \varphi(n)$.

Теорема Вильсона: p – простое число, тогда $(p-1)! = -1\ (mod\ p)$. Док-во: рассмотрим $\mathbb{Z}_p$: $\forall x \in \mathbb{Z}_p^* \Rightarrow x^{|\mathbb{Z}_p^*|} = x^{p-1} = 1 \Rightarrow x^{p-1} - 1 = 0 \Rightarrow (x - \overline{1}) * (x - \overline{2}) * \ldots * (x - \overline{p-1}) = 0 \Rightarrow (p-1)! = -1\ (mod\ p)$.

48. Действие группы на множестве.

G – группа преобразований множества $X, x, y \in X$. Говорят, что $x \underset{G}{\sim} y \Leftrightarrow \exists g \in G : y = gx$. Причём $x \underset{G}{\sim} y$ – отношение эквивалентности:

1) $x \underset{G}{\sim} x$, т.к. $x = ex$

2) $x \underset{G}{\sim} y \Rightarrow y = gx \Rightarrow g^{-1}y = x \Rightarrow y \underset{G}{\sim} x$

3) $\begin{cases} x \underset{G}{\sim} y \Rightarrow y = gx, g \in G \\ y \underset{G}{\sim} z \Rightarrow z = hy, h \in G \end{cases} \Rightarrow z = h(gx) = (hg)x, hg \in G \Rightarrow x \underset{G}{\sim} z$

X разбивается на непересекающиеся (смежные) классы эквивалентности.

49. Орбита и стабилизатор данной точки. Транзитивное действие группы.

Класс эквивалентности элемента $x \in X$ называется его орбитой $Gx = \{y \in X : y = gx\}$. Если имеется только одна орбита группы G, т.е. $X = Gx$, то группа (действие группы) называется транзитивной.

Стабилизатором элемента x в группе G называется $G_x = \{g \in G : gx = x\}$. Note: $G_x < G \ \forall x$ ($ex = x \Rightarrow x \in G_x; g_1 \in G_x, g_2 \in G_x \Rightarrow g_1x = x, g_2x = x \Rightarrow g_1g_2x = x \Rightarrow g_1g_2 \in G_x; g \in G_x \Rightarrow gx = x \Rightarrow x = g^{-1}x \Rightarrow g^{-1} \in G_x$).

50. Биективное соответствие между элементами орбиты точки и множеством левых смежных классов группы по стабилизатору этой точки.

Существует взаимно-однозначное соответствие между левыми смежными классами G/G_x и точками орбиты $gx \in Gx$. Док-во: $gG_x \longmapsto gx \in Gx, h \in G_x \Rightarrow gG_x \ni gh \longmapsto gx \in Gx \Rightarrow gG_x = ghG_x \longmapsto ghx = gx \in Gx$. Это отображение сюръективно, т.к. всегда $\exists gG_x : gG_x \longmapsto gx \in G$, и инъективно, т.к. если $g_1G_x \longmapsto gx, g_2G_x \longmapsto gx \Rightarrow g_1x = g_2x \Rightarrow g_1^{-1}g_1x = g_1^{-1}g_2x \Rightarrow x = g_1^{-1}g_2x \Rightarrow g_1^{-1}g_2 \in G_x \Rightarrow g_1 = g_2 (mod\ G_x) \Rightarrow g_1G_x = g_2G_x$.

51. Следствие теоремы Лагранжа о порядках конечной группы, орбиты и стабилизатора точки.

$G \subset S(x), |G| < \infty \Rightarrow |G| = |Gx| * |G_x| \ \forall x \in X$, т.к. $|Gx| = |G : G_x|$.

52. Группы симметрий и вращений правильных многогранников.

$G = SymT \Rightarrow |G| = |Gv| * |G_v| = |Gv| * |G_{v^r}| * |G_{v_r}|$ (число вершин, число рёбер, выходящих из каждой вершины и число преобразований, оставляющих некоторое ребро на месте соответственно). Для тетраэдра $|G| = |SymT| = 4 * 3 * 2$ (преобразования: id и симметрия относительно плоскости, проходящей через центр противолежащего ребра). $Sym_+F = RotF \ \forall F$. Соответственно $|RotT| = 4 * 3 * 1$ (только id). Группы симметрий куба и октаэдра, додекаэдра и икосаэдра попарно изоморфны между собой. $SymT \cong S_4, Sym_+T \cong A_4$.

53. Лемма Бернсайда. Примеры ее применения.

$g \in G, Fix(g) = \{x \in X : gx = x\}$, X/G – множество орбит Gx, тогда $|X/G| = \frac{1}{|G|} * \sum_{g \in G} |Fix(g)|$. Док-во: $\sum_{g \in G} |Fix(g)| = |\{(g, x) \in G \times X : gx = x\}| = \sum_{x \in X} |G_x| = \sum_{Gx \in X/G} |Gx| * |G_x| = \sum_{Gx \in X/G} |G| = |G| * |X/G|$.

54. Критерий согласованности сравнимости элементов по модулю подгруппы с операцией умножения в группе.

$H < G, G/H = \{gH\}$. Определим операцию: $(g_1H) * (g_2H) = (g_1g_2H)$. Тогда $g_1 = g_1' (mod\ H), g_2 = g_2' (mod\ H) \Rightarrow g_1 * g_2 = g_1' * g_2' (mod\ H) \Rightarrow g_1' = g_1 * h_1, g_2' = g_2 * h_2, h_1, h_2 \in H$. Умножение корректно, т.к. $\forall g_1, g_2 \in G, \forall h_1, h_2 \in H \Rightarrow g_1 * g_2 = (g_1 * h_1) * (g_2 * h_2) \ (mod\ H) \Leftrightarrow (g_1 * g_2)^{-1} * g_1 * h_1 * g_2 * h_2 \in H \Leftrightarrow g_2^{-1} * g_1^{-1} * g_1 * h_1 * g_2 * h_2 \in H \Leftrightarrow g_2^{-1} * h_1 * g_2 * h_2 \in H \Leftrightarrow g_2^{-1} * h_1 * g_2' \in H \Leftrightarrow g_2^{-1} * h_1 * g_2 \in H \Leftrightarrow g^{-1} * h * g \in H \ \forall g \in G, \forall h \in H$.

55. Определение нормальной подгруппы. Примеры.

$H < G$ называется нормальной подгруппой G, если $\forall g \in G, \forall h \in H \Rightarrow g * h * g^{-1} \in H$, обозначается $H \trianglelefteq G$. В этом случае правые и левые классы совпадают ($g * H * g^{-1} = H \Rightarrow gH = Hg \Rightarrow H = g^{-1} * H * g$).

56. Нормальность подгруппы абелевой группы и подгруппы индекса два.

Все подгруппы абелевой группы – нормальные (т.к. умножение коммутативно). $H < G, |G:H| = 2 \Rightarrow H \trianglelefteq G$, т.к. $G/H = H\backslash G \Leftrightarrow gH = Hg$.

57. Фактор группа. Примеры.

$H \trianglelefteq G$, тогда G/H с операцией $(g_1H) * (g_2H) = (g_1g_2H)$ является группой, называется факторгруппой. Док-во:

1) $\big((g_1 * H) * (g_2 * H)\big) * (g_3 * H) = \big((g_1 * g_2) * H\big) * (g_3 * H) = (g_1 * g_2) * g_3 * H = g_1 * (g_2 * g_3) * H = (g_1 * H) * \big((g_2 * H) * (g_3 * H)\big)$ – ассоциативность

2) $e * H = H, (g * H) * (e * H) = g * H, (e * H) * (g * H) = g * H \Rightarrow e * H \in G/H$

3) $\forall g * H \in \frac{G}{H} \exists (g * H)^{-1} \in G/H$, т.к. $(g * H)^{-1} = g^{-1} * H \Rightarrow (g * H) * (g^{-1} * H) = g * g^{-1} * H = e * H = H; (g^{-1} * H) * (g * H) = g^{-1} * g * H = e * H = H$

58. Гомоморфизм групп. Примеры.

$(G,*), (H,+)$ – группы, тогда $f: G \to H$ – гомоморфизм, если $f(g_1 * g_2) = f(g_1) + f(g_2)$.

59. Свойства гомоморфизма.

$(G,*), (H,\circ)$ – группы, $f: G \to H$ – гомоморфизм, тогда $f(e_G) = e_H$, т.к. $f(e_G) = f(e_G * e_G) = f(e_G) \circ f(e_G), \exists \big(f(e_G)\big)^{-1} \in H \Rightarrow f(e_G) \circ \big(f(e_G)\big)^{-1} = f(e_G) \circ f(e_G) \circ \big(f(e_G)\big)^{-1} \Rightarrow e_H = f(e_G)$. Для всех $g \in G, ord(g) < \infty \Rightarrow ord\big(f(g)\big) \mid ord(g)$, например, при $ord(g) = n \Rightarrow \big(f(g)\big)^n = f(g^n) = f(e_G) = e_H \Rightarrow n \vdots ord\big(f(g)\big) \Rightarrow ord\big(f(g)\big) \mid ord(g)$ (при изоморфизме порядки совпадают).

60. Ядро и образ гомоморфизма.

$(G,*), (H,\circ)$ – группы, $f: G \to H$ – гомоморфизм, тогда $Im(f) = \{h \in H : \exists g \in G : f(g) = h\}$ – образ гомоморфизма, $Ker(f) = \{g \in G : f(g) = e_H\}$ – ядро гомоморфизма. $Im(f) < H, Ker(f) < G$ – проверяется непосредственно (невыход за пределы множества, наличие единичного элемента и обратимость всех элементов).

61. Ядро гомоморфизма – нормальная подгруппа.

$Ker(f) \trianglelefteq G$. Док-во: $g' \in Ker(f) \Rightarrow f(g') = e_H \Rightarrow \forall g \in G, f(g * g' * g^{-1}) = f(g) * f(g' * g^{-1}) = f(g) * f(g') * f(g^{-1}) = f(g) * e_H * f(g^{-1}) = e_H \Rightarrow g * g' * g^{-1} \in Ker(f) \Rightarrow Ker(f) \trianglelefteq G$

62. Теорема о гомоморфизме. Примеры.

$(G,*), (H,\circ)$ – группы, $f: G \to H$ – гомоморфизм, тогда $G/Ker(f) \cong Im(f)$. Док-во: $Ker(f) \trianglelefteq G \Rightarrow \exists$ факторгруппа $G/Ker(f)$. Рассмотрим отображение $F: G/Ker(f) \to H$, положим $F\big(gKef(f)\big) = f(g) \in H$, тогда $g_1Ker(f) = g_2Ker(f) \Rightarrow g_1 = g_2 \ \big(mod\ Ker(f)\big) = f(g_1) = f(g_2) \Rightarrow F\big(g_1Ker(f)\big) = F\big(g_2Ker(f)\big)$ (это корректно, т.к. $f(g_1) = f(g_2) \Leftrightarrow \big(f(g_1)\big)^{-1} f(g_1) = \big(f(g_1)\big)^{-1} f(g_2) \Leftrightarrow e_H = f(g_1^{-1}) f(g_2) = f(g_1^{-1}g_2) \Leftrightarrow g_1^{-1}g_2 \in Ker(f) \Leftrightarrow g_1 = g_2 \ \big(mod\ Ker(f)\big)$).

Сохранение операции: $F\Big(\big(g_1Ker(f)\big)\big(g_2Ker(f)\big)\Big) = F\big(g_1g_2Ker(f)\big) = f(g_1g_2) = f(g_1)f(g_2) = F\big(g_1Ker(f)\big)F\big(g_2Ker(f)\big)$. Инъекция: $F\big(g_1Ker(f)\big) = F\big(g_2Ker(f)\big) \Leftrightarrow f(g_1) = f(g_2) \Leftrightarrow g_1 = g_2 \ \big(mod\ Ker(f)\big) \Leftrightarrow g_1Ker(f) = g_2Ker(f)$.

Сюръекция: $\forall h \in Im(f)\ \exists g : f(g) = h \Rightarrow F\big(gKer(f)\big) = f(g) = h \Rightarrow Im(f) = Im(F)$.

Следствие: $|Im(f)| = |G/Ker(f)| = |G{:}\,Ker(f)| = \frac{|G|}{|Ker(f)|} \Rightarrow |G| = |Ker(f)||Im(f)|$

63. Теорема Кэли.

Любая конечная группа изоморфна некоторой подгруппе группы перестановок множества элементов этой группы. Док-во: построим $f{:}\,G \to S(G)$, тогда $f(g){:}\,G \to G, \big(f(g)\big)(x) = gx$. Тогда $f(g)$ – биекция, т.к. $\forall y \in G\ \exists x \in G : \big(f(g)\big)(x) = y : x = g^{-1}y \Rightarrow \big(f(g)\big)(g^{-1}y) = g(g^{-1}y) = y$ (сюръекция) и $\big(f(g)\big)(x_1) = \big(f(g)\big)(x_2) \Rightarrow gx_1 = gx_2 \Rightarrow g^{-1}gx_1 = g^{-1}gx_2 \Rightarrow x_1 = x_2$ (инъекция), а f – гомоморфизм с инъекцией, т.к. $\big(f(g_1g_2)\big)(x) = (g_1g_2)(x) = g_1(g_2x) = \big(f(g_1)\big)\Big(\big(f(g_2)\big)(x)\Big) = \Big(\big(f(g_1)\big)\big(f(g_2)\big)\Big)(x) \Rightarrow \big(f(g_1g_2)\big) = \Big(\big(f(g_1)\big)\big(f(g_2)\big)\Big)$ (гомоморфизм) и $f(g_1) = f(g_2) \Rightarrow \big(f(g_1)\big)(x) = \big(f(g_2)\big)(x)\ \forall x \in G \Rightarrow g_1x = g_2x \Rightarrow g_1xx^{-1} = g_2xx^{-1} \Rightarrow g_1 = g_2 \Rightarrow Ker(f) = \{e\}$ (инъекция).

64. Внешнее прямое произведение групп.

$G_1, \dots, G_k$ – группы, тогда $G_1\times \dots \times G_k = \{(g_1, \dots, g_k), g_i \in G_i, i = \overline{1,k}\}$ – прямое произведение групп с операцией $(g_1, \dots, g_k)(g_1', \dots, g_k') = (g_1g_1', \dots, g_kg_k')$.

65. Внешнее прямое произведение групп – группа, её порядок, порядок её элемента.

$G_1\times \dots \times G_k$ – группа, т.к. умножение в каждой группе ассоциативно, а для прямого произведения групп определено поэлементно, $(e_1, \dots, e_k)$ – нейтральный элемент, $\forall (g_1, \dots, g_k) \in G_1\times \dots \times G_k \Rightarrow (g_1^{-1}, \dots, g_k^{-1}) = (g_1, \dots, g_k)^{-1}$. Если все группы абелевы, то их прямое произведение тоже абелево (т.к. операции определены поэлементно). $G = G_1\times \dots \times G_k \Rightarrow |G| = |G_1| * \dots * |G_k|$. Для $(g_1, \dots, g_k) \in G_1\times \dots \times G_k \Rightarrow ord(g_1, \dots, g_k) = \text{НОК}\{ord(g_1), \dots, ord(g_k)\}$ (т.к. возведение в степень определено поэлементно).

66. Следствие о прямом произведении циклических групп, порядки которых взаимно просты.

$G_1 =< g_1 >, ord(g_1) = m, G_2 =< g_2 >, ord(g_2) = n \Rightarrow G_1\times G_2 =< (g_1, g_2) >,$ $ord(g_1, g_2) = mn$, если $(m, n) = 1$, т.к. $|G_1\times G_2| = |G_1| * |G_2| = mn = ord(g_1, g_2)$.

67. Определение того, что группа является внутренним прямым произведением своих подгрупп.

G – группа, $G_1, \dots, G_k < G$. Говорят, что G является внутренним прямым произведением своих подгрупп $G_1, \dots, G_k$, если $\forall g \in G$ единственным образом представляется в виде $g = g_1 * \dots * g_k, g_i \in G_i, i = \overline{1,k}$ и $g_i * g_j = g_j * g_i\ \forall i, j = \overline{1,k}, i \neq j$.

68. Критерий того, что группа является внутренним прямым произведением своих подгрупп, критерий для случая двух подгрупп.

Если $\forall i = \overline{(1,k)} \Rightarrow G_i \cong G_i' = \{e_1\}\times \dots \times\{e_{i-1}\}\times G_i\times\{e_{i+1}\}\times \dots \times\{e_k\} < G$, то G является внутренним прямым произведением подгрупп $G_1', \dots, G_k'$. Док-во: рассмотрим $f{:}\,G_i \to G = G_1\times \dots \times G_k, f(g_i) = (e_1, \dots, e_{i-1}, g_i, e_{i+1}, \dots, e_k)$, это гомоморфизм, поскольку $f(g_ig_i') = (e_1, \dots, e_{i-1}, g_ig_i', e_{i+1}, \dots, e_k) = (e_1, \dots, e_{i-1}, g_i, e_{i+1}, \dots, e_k) * (e_1, \dots, e_{i-1}, g_i', e_{i+1}, \dots, e_k) = f(g_i)f(g_i')$. $Ker(f) = \{e_i\}$, $Im(f) = G_i'$, $G_i/Ker(f) \cong Im(f)$, $G_i \cong G_i' < G$. Кроме того, $\forall (g_1, \dots, g_k)$ единственным образом представляется в виде $(g_1, e_2, \dots, e_k) * \dots * (e_1, \dots, e_{k-1}, g_k)$ с точностью до перестановки (т.к. операции определены поэлементно).

Группа является прямым произведением своих подгрупп, если $\forall g \in G$ единственным образом представляется в виде $g = g_1 * \ldots * g_k, g_i \in G_i, i \in \overline{1,k}$ и $G_i \trianglelefteq G, i \in \overline{1,k}$. Док-во: требуется проверить, что g единственным образом представляется в виде $(g_1, \ldots, g_k), g_i \in G_i, G_i \cap G_j = \{e\}, i \neq j$ и что $g_i g_j = g_j g_i, i \neq j$. Проверка: если $g_i g_j = g_j g_i, i \neq j$, то $\forall g = g_1 * \ldots * g_k, g_i' \in G_i \Rightarrow g g_i g^{-1} = g_1 * \ldots * g_k * g_i' * g_1^{-1} * \ldots * g_k^{-1} = g_i * g_i' * g_i^{-1} \in G_i \Rightarrow G_i \trianglelefteq G$. Пусть $g \in G_i \cap G_j, g \neq e \Rightarrow g = g_i e_j = e_i g_j \Rightarrow g = g_i = g_j = e \Rightarrow G_i \cap G_j = \{e\}$. В обратную сторону: $G_i \trianglelefteq G, i \in \overline{1,k} \Rightarrow g_i g_j g_i^{-1} g_j^{-1} = \left(g_i g_j g_i^{-1}\right) g_j^{-1} \in G_j = g_i\left(g_j g_i^{-1} g_j^{-1}\right) \in G_i \Rightarrow g_i g_j g_i^{-1} g_j^{-1} \in G_i \cap G_j = \{e\} \Rightarrow g_i g_j g_i^{-1} g_j^{-1} = e \Rightarrow g_i g_j g_i^{-1} g_j^{-1} g_j = g_j \Rightarrow g_i g_j g_i^{-1} = g_j \Rightarrow g_i g_j g_i^{-1} g_i = g_j g_i \Rightarrow g_i g_j = g_j g_i$.

G является прямым произведением двух своих подгрупп, если $g = g_1 g_2, g_1 \in G_1, g_2 \in G_2$ представляется единственным образом, $G_1 \cap G_2 = \{e\}, G_1 \trianglelefteq G, G_2 \trianglelefteq G$. Проверка: пусть $g = g_1 g_2 = g_1' g_2', g_1, g_1' \in G_1, g_2, g_2' \in G_2 \Rightarrow g_1^{-1} g_1 g_2 g_2'^{(-1)} = g_1^{-1} g_1' g_2' g_2'^{(-1)} \Rightarrow G_2 \ni g_2 g_2'^{(-1)} = g_1^{-1} g_1' \in G_1 \Rightarrow G_1 \cap G_2 \ni g_2 g_2'^{(-1)} = g_1^{-1} g_1' = \{e\} \Rightarrow g_1 = g_1', g_2 = g_2'$.

69. Связь между внутренним и внешним прямыми произведениями. Примеры.

Если группа является внутренним прямым произведением своих подгрупп, то она является и их внешним произведением. Док-во: рассмотрим $f: G_1 \times \ldots \times G_k \to G, f(g_1, \ldots, g_k) = g_1 * \ldots * g_k \in G$. Это гомоморфизм, т.к. $f\left((g_1, \ldots, g_k)(g_1', \ldots, g_k')\right) = f(g_1 g_1', \ldots, g_k g_k') = g_1 g_1' * \ldots * g_k g_k' = g_1 * \ldots * g_k * g_1' * \ldots * g_k' = f(g_1, \ldots, g_k) f(g_1', \ldots, g_k')$, сюръекция, т.к. $\forall g \in G \; \exists g_1, \ldots, g_k : g = g_1 * \ldots * g_k, g_i \in G_i, i = \overline{1,k} \Rightarrow g = f(g_1, \ldots, g_k)$, инъекция, т.к. $f(g_1, \ldots, g_k) = f(g_1', \ldots, g_k') \Rightarrow g_1 * \ldots * g_k = g_1' * \ldots * g_k' \Rightarrow (g_1, \ldots, g_k) = (g_1', \ldots, g_k')$.

70. Изоморфизм колец. Примеры.

$G = G_1 \times G_2 \Rightarrow G/G_1 \cong G_2, G/G_2 \cong G_1$. Док-во: $f: G \to G_2, f\left((g_1, g_2)\right) = g_2$

1) $f\left((g_1, g_2)(g_1', g_2')\right) = f\left((g_1 g_1', g_2 g_2')\right) = g_2 g_2' = f\left((g_1, g_2)\right) f\left((g_1', g_2')\right)$
2) $Ker(f) = \{(g_1, g_2) : f(g_1, g_2) = e_2\} = \{(g_1, e_2), g_1 \in G_1, e_2 \in G_2\} = G_1 \times \{e_2\} \cong G_1$
3) $Im(f) = G_2$, т.к. $\forall g_2 \in G_2 \; \exists (e_1, g_2) \in G_1 \times G_2 : f\left((e_1, g_2)\right) = g_2$

По теореме о гомоморфизме $G/Ker(f) \cong Im(f) \Rightarrow G_1 \times G_2/G_1 \cong G_2$.

Отображение $f: K_1 \to K_2$ называется изоморфизмом колец, если это биекция и $f(a+b) = f(a) + f(b), f(ab) = f(a) f(b) \; \forall a, b \in K_1$

71. Функция Эйлера, её свойства, формула для вычисления её значений.

$\varphi(n) = |\mathbb{Z}_n^*|$. Если $n = mk, (m,k) = 1 \Rightarrow \varphi(n) = \varphi(m) * \varphi(k)$. Если $n = p_1^{k_1} * \ldots * p_s^{k_s}, p_i$ – простые, то $\varphi(n) = \varphi\left(p_1^{k_1}\right) * \ldots * \varphi\left(p_s^{k_s}\right)$, т.к. $\left(p_1^{k_1}, \left(p_2^{k_2}, \ldots, p_s^{k_s}\right)\right) = 1 \Rightarrow \varphi(n) = \varphi\left(p_1^{k_1}\right) * \varphi\left(p_2^{k_2} * \ldots * p_s^{k_s}\right)$ и т.д. Причём $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$, т.к. значение функции Эйлера – это количество чисел, взаимно простых с данным и не превосходящих его, не взаимно просты с простым числом p только числа кратные ему, они имеют вид $p, 2p, 3p, \ldots, (p^{k-1} - 1)p$, таких чисел $p^{k-1} - 1$, тогда $\varphi(k) = p^k - 1 - (p^{k-1} - 1) = p^k - p^{k-1}$.

72. Примарные группы.

Примарная группа – это группа, порядок которой равен степени простого числа.

73. Теорема о разложении конечной циклической группы в прямую сумму (произведение) примарных циклических групп. Примеры.

$n = p_1^{k_1} * \dots * p_s^{k_s} \Rightarrow \mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_s^{k_s}}$, т.к. $\left(p_1^{k_1}, \left(p_2^{k_2}, \dots, p_s^{k_s}\right)\right) = 1 \Rightarrow \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2} * \dots * p_s^{k_s}}$ и т.д.

74. Теорема о строении конечнопорождённой абелевой группы.

Любая конечнопорождённая абелева группа является прямым произведением бесконечных и примарных циклических групп, набор порядков этих групп определён однозначно.

75. Теорема о разложении конечной абелевой группы в прямую сумму (произведение) примарных циклических групп. Примеры.

Любая конечная абелева группа является прямым произведением примарных циклических групп (нет бесконечных слагаемых, как $\mathbb{Z}$), набор порядков этих групп определён однозначно.

76. Автоморфизмы группы. Примеры.

Автоморфизм – это изоморфизм группы в себя. Например, для матрицы автоморфизмы $f(A) = A^T, f(A) = (A^T)^{-1}$.

77. Группа автоморфизмов.

Множество всех автоморфизмов $Aut(G)$ – группа. Док-во: $Aut(g) < S(G)$,

1) $id \in Aut(G)$
2) $f_1, f_2 \in Aut(G) \Rightarrow f_1 f_2(x_1 x_2) = f_1\big(f_2(x_1) f_2(x_2)\big) = f_1\big(f_2(x_1)\big) f_1\big(f_2(x_2)\big) = f_1 f_2(x_1) f_1 f_2(x_2) \Rightarrow f_1 f_2 \in Aut(G)$
3) $f^{-1}\big(f(x_1) f(x_2)\big) = f^{-1}\big(f(x_1 x_2)\big) = x_1 x_2 = f^{-1}\big(f(x_1)\big) f^{-1}\big(f(x_2)\big) \Rightarrow f^{-1} \in Aut(G)\ \forall f \in Aut(G)$

78. Группа автоморфизмов циклической группы конечного порядка.

$G = \mathbb{Z}_n \Rightarrow Aut(G) = Aut(\mathbb{Z}_n), \mathbb{Z}_n = <\bar{1}>, f(\bar{1}) = \bar{k}, f\big(\bar{l}\big) = f\left(\underbrace{\bar{1} + \dots + \bar{1}}_{l}\right) = \overline{lk}$,

$\exists f^{-1} :\ f^{-1}(\bar{1}) = \bar{m} \Rightarrow f^{-1}\big(\bar{l}\big) = \bar{m}\bar{l} \Rightarrow f^{-1} f = \bar{m}\bar{k} = \bar{1} \Rightarrow \bar{k} \in \mathbb{Z}_n^* \Rightarrow Aut(G) \cong \mathbb{Z}_n^*$.

79. Внутренние автоморфизмы группы.

$f(g) = gxg^{-1}$ – внутренний автоморфизм, т.к. $\forall y \in G\ \exists x \in G : gxg^{-1} = y, x = g^{-1}yg$ (сюръекция), $\big(f(g)\big)(x_1) = \big(f(g)\big)(x_2) \Rightarrow gx_1g^{-1} = gx_2g^{-1} \Rightarrow x_1 = x_2$ (инъекция), $\big(f(g)\big)(x_1x_2) = g(x_1x_2)g^{-1} = gx_1g^{-1}gx_2g^{-1} = \big(f(g)\big)(x_1)\big(f(g)\big)(x_2)$ (гомоморфизм).Обозначаются $Int(G)$, $Int(G) < Aut(G)$.

80. Центр группы.

$Z(G) = \{h : hg = gh\ \forall g\} = \{h : hgh^{-1} = g\}$ – центр группы.

81. Фактор группа по центру группы.

$Z(G) \trianglelefteq G, G/Z(G) \cong Int(G)$. Док-во: $f: G \to Aut(G)$, тогда $f(g)$ – внутренний автоморфизм, $\big(f(g)\big)(x) = gxg^{-1}$, $f: g \to f(g)$ – гомоморфизм, т.к. $\big(f(g_1g_2)\big)(x) = (g_1g_2)x(g_1g_2)^{-1} = g_1g_2xg_2^{-1}g_1^{-1} = g_1\big(f(g_2)\big)(x)g_1^{-1} = \big(f(g_1)\big)\big(f(g_2)\big)(x)$, причём $Ker(f) = \{g \in G : f(g) = Id\} = \{g \in G : gxg^{-1} = x\ \forall x\} = Z(G) \Rightarrow Z(G) \trianglelefteq G$. Тогда $Im(f) = Int(G) \Rightarrow Int(G) < Aut(G)$

82. Группа внутренних автоморфизмов симметрической группы.

$G = S_3 = <(1,2),(1,3),(2,3)>$, тогда $f \in Aut(G)$ осуществляет подстановку этих транспозиций, тогда $f \in S_3 = Int(S_3) < Aut(S_3) \subset S_3 \Rightarrow Int(S_3) = Aut(S_3) = S_3$.

83. Действие группы на себе сопряжениями. Классы сопряженных элементов, стабилизаторы.

Действие сопряжения: $\big(f(g)\big)(x) = gxg^{-1}$, орбита $Gx = \{gxg^{-1}\ \forall g \in G\} = C(x)$ – класс элементов, сопряжённых с x, стабилизатор $G_x = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} = Z(x)$ – централизатор $x, Z(x) < G$. Тогда $|G| < \infty \Rightarrow |G| =$

$|Gx| * |G_x| = |C(x)| * |Z(x)|, Gx = x \Leftrightarrow gxg^{-1} = x\ \forall g \in G \Leftrightarrow x \in Z(G) \Leftrightarrow Z(x) = G,$
$G = Z(G) \cup C(x_1) \cup \ldots \cup C(x_k), C(x_i) \cap C(x_j) = \emptyset.$

84. Теорема о центре примарной группы.

Центр примарной группы нетривиален. Док-во: $|G| = p^m, p$ – простое, тогда

1) $m = 1 \Rightarrow |G| = p \Rightarrow G$ – циклическая $\Rightarrow G = Z(G)$
2) $m > 1 \Rightarrow G = Z(G) \cup C(x_1) \cup \ldots \cup C(x_k), x_i \notin Z(x), |C(x_i)| = |G|/|Z(x_i)|,$ где $Z(x_i) < G \Rightarrow |Z(x_i)| = p^{l_i}, l < m \Rightarrow |C(x_i)| = p^{m-l_i}, |G| = |Z(G)| + \sum_{i=1}^{k} |C(x_i)|, x_i \notin Z(G) \Rightarrow p^m = |Z(G)| + \sum_{i=1}^{k} p^{m-l_i} \Rightarrow |Z(G)| \vdots p \Rightarrow Z(G) \neq \{e\}$

85. Теорема о фактор группе неабелевой группы по её центру.

Если группа G не абелева, то $G/Z(G)$ – не циклическая группа. Док-во: пусть $G/Z(G) =< gZ(G) >, \quad G = \cup_{k=0}^{m-1} g^k Z(G), g \in G, g \notin Z(G).$ Тогда $\forall h \in G : h = g^k z, z \in Z(G) \Rightarrow h_1 h_2 = g^{k_1} z_1 g^{k_2} z_2 = g^{k_1+k_2} z_1 z_2 = g^{k_2} z_2 g^{k_1} z_1 = h_2 h_1 \Rightarrow$ группа G – абелева, пришли к противоречию.

86. Теорема о группе, порядок которой является квадратом простого числа.

$|G| = p^2, p$ – простое, тогда G – абелева группа. Док-во: $Z(G) < G, |G| \vdots |Z(G)| \Rightarrow \begin{cases} |Z(G)| = 1 \\ |Z(G)| = p \end{cases}, Z(G) \neq \{e\} \Rightarrow |Z(G)| = p \Rightarrow |G/Z(G)| = p \Rightarrow G/Z(G) \cong \mathbb{Z}_p \Rightarrow$
G – абелева, либо $|Z(G)| = p^2 \Rightarrow G = Z(G) \Rightarrow G$ – абелева.

Следствие: $|G| = p^2 \Rightarrow G \cong \mathbb{Z}_{p^2}$ или $\cong \mathbb{Z}_p \times \mathbb{Z}_p$.

87. Теорема о неабелевой группе, порядок которой является удвоеннным простым числом.

$|G| = 2p, p$ – простое, G – неабелева, тогда $G \cong D_p$. Док-во: $\forall g \in G \Rightarrow 2p = |G| \vdots ord(g)$

1) $\forall g \in G, g \neq e : ord(g) = 2 \Rightarrow G$ – абелева $\Rightarrow \overset{o}{X}$
2) $\exists g \in G : ord(g) = 2p \Rightarrow G$ – циклическая $\Rightarrow \overset{o}{X}$
3) $\exists g \in G : ord(g) = p$

Рассмотрим $H =< g >, |H| = p,$ тогда $|G:H| = 2 \Rightarrow H \trianglelefteq G. \ G = H \cup sH, s \notin H \Rightarrow G/H \cong \mathbb{Z}_2, (sH)^2 = H \Rightarrow s^2 = H,$ т.е. $s^2 = g^k.$

1) Пусть $ord(s) = p \Rightarrow s = s * s^p = s^{p+1} = s^{2m} = (s^2)^m = g^{km} \in H \Rightarrow \overset{o}{X}$
2) $ord(s) = p^2 \Rightarrow G$ – абелева $\Rightarrow \overset{o}{X}$
3) $ord(s) = 2$

88. Теорема о неабелевой группе порядка восемь.

$|G| = 8, G$ – неабелева, тогда $G = D_4$ или $G = Q_8$. Док-во:

1) $\forall g \in G, g \neq e : ord(g) = 2 \Rightarrow G$ – абелева $\Rightarrow \overset{o}{X}$
2) $\exists g \in G : ord(g) = 8 \Rightarrow G$ – циклическая $\Rightarrow \overset{o}{X}$
3) $\exists g \in G : ord(g) = 4$

Рассмотрим $H =< g >, |H| = 4,$ тогда $|G:H| = 2 \Rightarrow H \trianglelefteq G. \ G = H \cup sH, s \notin H \Rightarrow G/H \cong \mathbb{Z}_2, (sH)^2 = H \Rightarrow s^2 = H,$ т.е. $s^2 = g^k.$

1) $ord(s) = 2 \Rightarrow G \cong D_4 \Rightarrow s^2 = g^k, s^2 = e$
2) $ord(s) = 4 \Rightarrow G \cong Q_8 \Rightarrow s^2 = g^k, s = g$ или $s = g^3$

Проверка:

1) $sgs = sgs^{-1} \Rightarrow ord(g) = ord(sgs^{-1}) = 4 \Rightarrow sgs = \begin{cases} g \Rightarrow sg = gs \Rightarrow \overset{o}{X} \\ g^{-1} \Rightarrow G = D_4 \end{cases}$

2) $ord(s^{-1}gs) = ord(g) = 4 \Rightarrow s^{-1}gs = \begin{cases} g \Rightarrow sg = gs \Rightarrow \overset{o}{X} \\ g^{-1} \Rightarrow G = Q_8 \end{cases}$