Разбор задач домашнего задания по алгебре на 22.01 для группы БПИ209
3 модуль
Автор: vk.com/yourkumir

1* Пусть H - подгруппа группы G и e_H - нейтральный элемент в H. Докажите (*не пользуясь критерием подгруппы*), что e_H - нейтральный элемент в G.

Пусть e_G - нейтральный элемент в группе G и $x = e_H$, тогда $x * x = x$ по определению нейтрального элемента. В группе G все элементы обратимы, поэтому x имеет обратный элемент x^{-1} и, домножив наше равенство справа на x^{-1} получим $x * x * x^{-1} = x * x^{-1}$
Воспользуемся полученными результатами: $x = x * e_G = x * x * x^{-1} = x * x^{-1} = e_G$, то есть $e_H = e_G$, что и требовалось доказать.
Примечание. Утверждение кажется очевидным, но это та тонкость, которая требует доказательства. В доказательстве мы считаем, что подгруппа - это подмножество группы, которое является группой относительно той же операции, и используем определение нейтрального элемента для e_G и e_H и существование обратного элемента для элементов группы G.

56.15 б),в) В циклической группе $\langle a \rangle$ порядка n найти все элементы g, удовлетворяющие условию $g^k = e$, и все элементы порядка k при: б) $n = 24, k = 4$; в) $n = 100, k = 20$

б) $\langle a \rangle = \{e, a, a^2, ..., a^{22}, a^{23}\}$
1) Пусть $g = a^i$, тогда $g^4 = e \Rightarrow a^{4i} = e$, тогда необходимо найти такие i, что $4i$ делится нацело на 24, то есть i делится нацело на 6. Получим $g: e, a^6, a^{12}, a^{18}$
2) Для того чтобы найти такие g, что $ord(g) = 4$ воспользуемся формулой $ord(a^i) = \dfrac{n}{\text{НОД}(n, i)}$.
Тогда необходимо найти такие i, что НОД$(24, i)$=6. Получим $g: a^6, a^{18}$

в) $\langle a \rangle = \{e, a, a^2, ..., a^{22}, a^{99}\}$
1) Пусть $g = a^i$, тогда $g^{20} = e \Rightarrow a^{20i} = e$, тогда необходимо найти такие i, что $20i$ делится нацело на 100, то есть i делится нацело на 5. Получим $g: e, a^5, a^{10}, a^{15}, a^{20}, a^{25}, a^{30}, a^{35}, a^{40}, a^{45}, a^{50}, a^{55}, a^{60}, a^{65}, a^{70}, a^{75}, a^{80}, a^{85}, a^{90}, a^{95}$
2) Для того чтобы найти такие g, что $ord(g) = 20$ воспользуемся формулой $ord(a^i) = \dfrac{n}{\text{НОД}(n, i)}$.
Тогда необходимо найти такие i, что НОД$(100, i)$=5. Получим $g: a^5, a^{15}, a^{35}, a^{45}, a^{55}, a^{65}, a^{85}, a^{95}$

Ответ: б) $g: e, a^6, a^{12}, a^{18}$ и $g: a^6, a^{18}$;
в) $g: e, a^5, a^{10}, a^{15}, a^{20}, a^{25}, a^{30}, a^{35}, a^{40}, a^{45}, a^{50}, a^{55}, a^{60}, a^{65}, a^{70}, a^{75}, a^{80}, a^{85}, a^{90}, a^{95}$ и $g: a^5, a^{15}, a^{35}, a^{45}, a^{55}, a^{65}, a^{85}, a^{95}$

56.16 г),д) Найти все подгруппы в циклической группе порядка: г) 125; д) p^n (p — простое число).

г) $\langle a \rangle_{125}$
Порядок подгруппы делит порядок группы, поэтому выпишем все делители 125 (это и будут порядки всех подгрупп): $1, 5, 25, 125$. Теперь выпишем наши подгруппы:
порядок $1 - \{e\}$
порядок $5 - \{e, a^{25}, a^{50}, a^{75}, a^{100}\} \Leftrightarrow \langle a^{25} \rangle$
порядок $25 - \{e, a^5, a^{10}, a^{15}, a^{20}, a^{25}, a^{30}, a^{35}, ..., a^{100}, a^{105}, a^{110}, a^{115}, a^{120}\} \Leftrightarrow \langle a^5 \rangle$
порядок 125 – вся группа

д) $\langle a \rangle_{p^n}$ (p — простое число)
Порядок подгруппы делит порядок группы, поэтому выпишем все делители p^n (это и будут порядки всех подгрупп): $1, p, p^2, ..., p^{n-1}, p^n$. Теперь выпишем наши подгруппы (чтобы понять, как мы это получаем, посмотрите предыдущий пункт):
порядок $1 - \{e\}$
порядок $p - \langle a^{p^{n-1}} \rangle$
порядок $p^2 - \langle a^{p^{n-2}} \rangle$
...
порядок $p^i - \langle a^{p^{n-i}} \rangle$
...
порядок $p^{n-1} - \langle a^p \rangle$
порядок p^n – вся группа

56.13 Найти число элементов порядка p^m в циклической группе порядка p^n, где p—простое число, $0 < m \le n$.

Пусть $\langle a \rangle_{p^n}$ -исходная циклическая группа, тогда необходимо найти такие g, что $ord(g) = p^m$
Воспользуемся утверждением $ord(x) = n \Rightarrow ord(x^k) = \dfrac{n}{\text{НОД}(n,k)}$:
$ord(a) = p^n \Rightarrow ord(g) = ord(a^k) = \dfrac{p^n}{\text{НОД}(p^n,k)} = p^m \Rightarrow \text{НОД}(p^n,k) = \dfrac{p^n}{p^m} = p^{n-m}$
Найдем k: k имеет вид $p^{n-m} * t$, где t находится в диапазоне от 1 до p^m $(k \le p^n)$ и не делится на p (можно записать это как $k = \{p^{n-m} * t, t = \overline{1, p^m}\} \backslash t : \text{НОД}(p,t) \ne 1)$
Тогда количество таких $k (\Rightarrow a^k)$ равно $p^m - p^{m-1}$ (p^m чисел в диапазоне от 1 до p^m минус p^{m-1} чисел, которые делятся в этом диапазоне на p, так как мы идём по диапазону с шагом p).

Ответ: $p^m - p^{m-1} = p^{m-1}(p-1)$

56.37 а), г), е), ж), л) Найти смежные классы: а) аддитивной группы $\mathbb{Z}$ по подгруппе $n\mathbb{Z}$, n — натуральное число; г) аддитивной группы $\mathbb{C}$ по подгруппе $\mathbb{R}$; е) мультипликативной группы $\mathbb{C}^*$ по подгруппе $\mathbb{R}^*$; ж) мультипликативной группы $\mathbb{C}^*$ по подгруппе положительных вещественных чисел; л) циклической группы $\langle a \rangle_6$ по подгруппе $\langle a \rangle_4$.

Вспомним определение смежного класса: левым смежным классом элемента g группы G по подгруппе H называют множество $g = \{gh \mid h \in H\}$

а) $G = (\mathbb{Z}, +)$, $H = (n\mathbb{Z}, +)$
$n\mathbb{Z}$ - это целые числа, кратные n. Если мы возьмём целое число и сложим с целыми числами, кратными n, то получим следующие смежные классы:

$$\begin{cases} n\mathbb{Z} & \text{g\%n=0} \\ 1 + n\mathbb{Z} & \text{g\%n=1} \\ 2 + n\mathbb{Z} & \text{g\%n=2} \\ ... & \\ (n-1) + n\mathbb{Z} & \text{g\%n=n-1} \end{cases}$$

г) $G = (\mathbb{C}, +)$, $H = (\mathbb{R}, +)$
Если мы рассмотрим комплексные числа на комплексной плоскости, то сложение комплексного числа с вещественным числом даст нам сдвиг точки, соответствующей данному комплексному числу, на величину вещественного числа параллельно действительной оси. Смежный класс для комплексного числа - прямая, параллельная действительной оси. Тогда смежные классы - это множество прямых, которые параллельны действительной оси Rez на комплексной плоскости, включая саму действительную ось (для комплексных чисел, у которых мнимая часть равна 0).
Примечание. $H = (\mathbb{R}, +)$ - это действительная ось на комплексной плоскости.

е) $G = (\mathbb{C}^*, \cdot)$, $H = (\mathbb{R}^*, \cdot)$
Вспомним, что $\mathbb{R}^* = \mathbb{R} \backslash \{0\}$
Опять же рассмотрим комплексную плоскость, но вместо точки сопоставим каждому комплексному числу радиус-вектор (вектор с началом в начале координат и с концом в точке нашего комплексного числа). При умножении комплексного числа на ненулевое вещественное число, его координаты (действительная и мнимая часть) пропорционально увеличатся или уменьшатся, то есть произойдёт растяжение, сжатие или даже поворот (при умножении на отрицательное число) радиус-вектора данного комплексного числа. Смежный класс для ненулевого комплексного числа - прямая, которая проходит через начало координат и точку, соответствующую данному комплексному числу на комплексной плоскости. Тогда смежные классы - это множество прямых, проходящих через начало координат, но не включая саму точку начала координат (выколота).
Примечание. $H = (\mathbb{R}^*, \cdot)$ - это действительная ось на комплексной плоскости с выколотой точкой (0,0).

ж) $G = (\mathbb{C}^*, \cdot)$, $H = (\mathbb{R}^+, \cdot)$
Вспомним, что $\mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$
Задание аналогичное предыдущему, только теперь мы комплексное число умножаем на положительные вещественные числа, т.е. не можем его отобразить (развернуть) относительно начала координат, а можем только сжать или растянуть, не меняя его направления. Смежный класс для ненулевого комплексного числа - луч, который имеет начало в точке начала координат (но эта точка выколота) и проходит через точку, соответствующую данному комплексному числу на комплексной плоскости. Тогда смежные классы - это множество лучей, имеющих начало в точке начала координат, но не включая саму точку начала координат (выколота).

л) $G = \langle a \rangle_6 = \{e, a, a^2, a^3, a^4, a^5\}$, $H = \langle a^4 \rangle = \{e, a^2, a^4\}$
Предлагаю просто взять каждый элемент группы и умножить его на все элементы подгруппы, так мы найдём все смежные классы:
$e: \ \{e * e, e * a^2, e * a^4\} = \{e, a^2, a^4\}$
$a: \ \{a * e, a * a^2, a * a^4\} = \{a, a^3, a^5\}$
$a^2: \ \{a^2 * e, a^2 * a^2, a^2 * a^4\} = \{a^2, a^4, e\} = \{e, a^2, a^4\}$
$a^3: \ \{a^3 * e, a^3 * a^2, a^3 * a^4\} = \{a^3, a^5, a\} = \{a, a^3, a^5\}$
$a^4: \ \{a^4 * e, a^4 * a^2, a^4 * a^4\} = \{a^4, e, a^2\} = \{e, a^2, a^4\}$
$a^5: \ \{a^5 * e, a^5 * a^2, a^5 * a^4\} = \{a^5, a, a^3\} = \{a, a^3, a^5\}$
Таким образом, у нас всего два смежных класса: $\{e, a^2, a^4\}$ и $\{a, a^3, a^5\}$, то есть четные и нечетные степени a.

Примечание. Как можно проверить смежные классы для конечных случаев:
1) Порядок подгруппы делит порядок группы. Если вы в задании поняли $\langle a^4 \rangle$ как $\langle a \rangle_4 = \{e, a, a^2, a^3\}$, то вас должна остановить мысль, что 6 не делится на 4.
2) Количество элементов в смежном классе равно количеству элементов в подгруппе.
3) Смежные классы или совпадают, или не имеют общих элементов. Если вы получили, что в двух смежных классах у вас есть общий элемент, но при этом они не совпадают, то вы что-то делаете не так.
4) Можно проверить количество смежных классов, их должно быть $\dfrac{|G|}{|H|}$ штук.

56.38 Пусть g — невырожденная матрица из $GL_n(\mathbb{C})$ и $H = SL_n(\mathbb{C})$. Доказать, что смежный класс gH состоит из всех матриц $a \in GL_n(\mathbb{C})$, определитель которых равен определителю матрицы g.

Вспомним общую и специальную линейную группу: GL_n - множество всех невырожденных ($det \neq 0$) матриц размера $n*n$ с операцией матричного умножения, L_n - множество всех матриц размера $n*n$ с определителем, равным 1, с операцией матричного умножения.

Так как при перемножении матриц, перемножаются их определители ($det(AB) = detA * detB$), то смежный класс матрицы g будет состоять из матриц с определителем, равным определителю матрицы g ($det(g * s) = detg * dets = detg * 1 = detg$), что и требовалось доказать.

56.17 Предположим,что в некоторой неединичной группе все неединичные элементы имеют одинаковый порядок p. Доказать,что p является простым числом.

Неединичный элемент - это элемент, который не является нейтральным. Неединичная группа - это группа, в которой есть хотя бы один неединичный элемент.

Докажем от противного. Пусть p - это составное число, то есть $p = mn$, $1 < m, n < p$, тогда по условию неединичный элемент g нашей группы будет иметь порядок mn: $g^{mn} = e$, и значит, что существует неединичный элемент g^m порядка n: $g^{mn} = (g^m)^n = e$, n - наименьшее такое натуральное число. Получаем противоречие, так как $n \neq p$, следовательно p - простое, что и требовалось доказать.

56.19 Существует ли бесконечная группа, все элементы которой имеют конечный порядок?

Да, существует. $G = (\{g \mid g \in \sqrt[n]{1},\ n \in \mathbb{N}\}, \cdot)$
1) G - замкнута
2) $|G| = \infty$
3) $\forall g \in G \ ord(g) < \infty$

56.14 г) Пусть $G = \langle a \rangle$ — циклическая группа порядка n. Доказать, что г) для всякого делителя d числа n существует единственная подгруппа H порядка d.

Нам понадобятся два вспомогательных утверждения: (1) любая подгруппа циклической группы являтся циклической, (2) Если $k \in \mathbb{Z}$, $d = \text{НОД}(n, k)$, то $\langle a^k \rangle = \langle a^d \rangle$

Будем считать, что (1) вы доказали, поэтому докажем (2):
Пусть $G = \langle a \rangle$, $|G| = n$, $k \in \mathbb{Z}$, $d = \text{НОД}(n, k)$, тогда $\langle a^k \rangle = \langle a^d \rangle$.
Пусть $k = dk'$, $n = dn'$ и по свойству НОДа $uk + vn = d$, тогда
$a^k = (a^d)^{k'} \in \langle a^d \rangle \Rightarrow \langle a^k \rangle \subseteq \langle a^d \rangle$
$a^d = a^{uk+vn} = (a^k)^u * (a^n)^v = (a^k)^u \in \langle a^k \rangle \Rightarrow \langle a^d \rangle \subseteq \langle a^k \rangle$
Доказано включение с обоих сторон, то есть $\langle a^k \rangle = \langle a^d \rangle$, что и требовалось доказать.

Теперь перейдём к основному утверждению. Все подгруппы циклической группы - циклические (1), поэтому чтобы перебрать все подгруппы, нам достаточно рассмотреть каждый элемент a^k группы G (он является порождающим своей циклической группы). По утверждению (2) $\langle a^k \rangle = \langle a^{\text{НОД}(n,k)} \rangle$ нам достаточно рассмотреть лишь $\langle a^d \rangle$, где d - делитель n, то есть для каждого делителя n существует лишь одна подгруппа порядка d, что и требовалось доказать.

Примечание. Попрошу вас обратить внимание на все пункты этого номера, так как эти утверждения важны.
Пусть $G = \langle a \rangle$ — циклическая группа порядка n.
а)элементы a^k и a^l имеют одинаковые порядки тогда и только тогда, когда $\text{НОД}(k, n) = \text{НОД}(l, n)$
б)элемент a^k является порождающим элементом G тогда и только тогда, когда k и n взаимно просты
в)всякая подгруппа H порождается элементом вида a^d, где $d|n$
г)для всякого делителя d числа n существует единственная подгруппа H порядка d