Георгий Потошин, 2024

Алгебра I, листочек 3

1. **Есть ли в группе $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ подгруппа, изоморфная $\mathbb{Z}_4 \times \mathbb{Z}_4$? Изоморфная $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$?**

   Посчитаем количество элементов порядка 4 в обоих группах. Как нетрудно заметить $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_{16}$ имеет порядок 4, если его имеет b, в противном случае порядок либо 2, либо 1, таких пар всего 4 $(0, 4)$, $(1, 4)$, $(0, 12)$ et $(1, 12)$. Но $(a, b) \in \mathbb{Z}_4 \times \mathbb{Z}_4$ имеет порядок 4, когда хотя бы одна компонента его имеет. Таких пар после нетрудного подсчета оказывается $4 * 2 + 2 * 4 - 2 * 2 = 12$, и их больше, чем в группе куда мы хотим устроить вложение, а значит оно не удастся.

   Аналогично в $\mathbb{Z}_2^3$ мы обнаружим 7 инволюций, а в $\mathbb{Z}_2 \times \mathbb{Z}_{16}$ их всего 3 и вложение не удастся.

2. **(Теорема Нетер) Если $K, H \leq G$ и $H \leq N_K$, докажите, что $H/(H \cap K) \cong HK/K$, где HK – подгруппа, порожденная элементами вида $h \cdot k, h \in H, k \in K$.**

   Покажем, что HK в данном случае совпадает с произведением по Минковскому. Пусть $h, h' \in H$ и $k, k', k'' \in K$, тогда $hkh'k' = hh'k''k$, так как $h' \in H \subseteq N_K$. Тогда $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k''$, и $e = ee \in HK$ есть нейтральный элемент. Ещё можно заметить, что $H, K \leq N_K$, а тогда $K \trianglelefteq HK \subset N_K$. Построим гомоморфизм $\varphi : H \longrightarrow HK/K, h \mapsto hK$. Он очевидно сюръективен. Посчитаем его ядро $(h \in \operatorname{Ker}(\varphi)) \Leftrightarrow (hK = K \;\&\; h \in H) \Leftrightarrow (h \in K \cap H)$. Тогда применим теорему о сюрьективном гомеоморфизме, $H/(H \cap K) \cong HK/K$.

3. **Опишите все перестановки, которые могут быть разложены в произведение циклов длины три.**

   Разобьём перестановку на дизъюнктивные циклы. Назовём дискриминантом перестановки сумму длин её дизъюнктивных циклов, уменьшенных на 1. Покажем, что умножение на транспозицию меняет четность дискриминанта.

   - Если транспозиция дизъюнктивна с существующими индексами, то умножение на неё добавит к дискриминанту 1.
   - Если транспозиция пересекается с 1 циклом по 1 индексу, то $(ab)(ac \dots d) = (abc \dots d)$ или $(d \dots ca)(ba) = (d \dots cba)$ один цикл увеличится на 1.
   - Если транспозиция пересекается с 1 циклом по 2 индексам, то $(ab)(ad \dots ebc \dots f) = (ac \dots f)(bd \dots e)$ или $(f \dots cbe \dots da)(ba) = (e \dots db)(f \dots ca)$ и цикл разобьется на 2, а дискриминант уменьшится на 1.
   - Если транспозиция пересекается с 2 циклами по 1 индексу, то $(ab)(ac \dots e)(bd \dots f) = (ad \dots fbc \dots e)$ или $(f \dots db)(e \dots ca)(ba) = (e \dots cbf \dots da)$ циклы слипнутся, а дискриминант увеличится на 1.

   Зная также, что перестановка раскладывается по циклам на транспозиции, которых будет ровно дискриминант штук, мы получаем, что домножение на четную перестановку не меняет четности. В частности это означает, что все четные перестановки образуют знакопеременную группу, так как () четна, обратная получается переворачиванием циклов, что тоже не меняет четность, а произведение четных четно.

   Тогда покажем, что циклы длинны три порождают знакопеременную группу. Знакопеременная группа состоит из элементов в которых при разложении получается четное число нечетных перестановок. Заметим, что мы можем всегда добавить к циклу 2 любых буквы $(a \dots bc)(dec) = (a \dots bdec)$. Так же мы можем создать пару любых дизъюнктивных транспозиций $(abc)(bcd) = (ac)(bd)$. Из этого мы делаем вывод, что всегда можно из 3-х циклов собрать четный цикл или четное количество нечетных. Перемножив их можно получить любой четный элемент. Но так как 3-циклы сами по себе четные, то их произведение всегда таким и останется. Тогда $\langle 3\text{-циклы} \rangle = A$.

4. **Постройте сюръективный гомоморфизм $S_n \longrightarrow \mathbb{Z}_2$ для любого $n \geq 2$.**

   Отправим нечетную перестановку в 1, а четную в 0. Исходя из рассуждений прошлой задачи, получится сюрьекивный гомоморфизм, так как четность ведёт себя мультипликативно.

5. **Постройте сюръективный гомоморфизм $S_4 \longrightarrow S_3$.**

   Как мы видели в задаче 3 листочка 2 $V_4 \trianglelefteq S_4$, где нетривиальными элементами V_4 являются (2,2)-циклы. Там я проверил все возможные сопряжения, то тогда можно построить фактор-группу S_4/V_4, её порядок равен $24/4 = 6$, так что она изоморфна либо $\mathbb{Z}_6$, либо S_3. Но в S_4 все элементы были порядка меньшего 6, то значит и в фактор-группе их порядок меньше $(gA)^n = g^n A = A$. Тогда $S_4/V_4 \cong S_3$, осталось построить гомоморфизм. Транспозиции должна перейти в инволюцию, которыми в S_3 могут быть только инволюции. Тогда например $(12) \mapsto (12)$. Так как ядром является V_4, то $(12)(34) \mapsto (12)(??) = e$, а значит $(34) \mapsto (12)$. Также $(12)V_4 = \{(12), (43), (1324), (1423)\}$, в нём нет (23), а значит её образ должен отличатся от (12), пусть им будет (23), аналогично поймём и зададим образ (13) равный (13). Тогда аналогично прошлому рассуждению поймём, что дополнение к траноспозиции до 2-цикла из ядра должно переходить в тот же элемент, то есть $(24) \mapsto (13)$ и $(14) \mapsto (23)$. Так как мы построили отображение порождающих элементов в порождающие, то если можно корректно дополнить гомоморфизм, то это делается единственным способом через разложение на порождающие. И так как гомоморфизм существует, в чем мы убедились, построив фактор-группу, то построение продолжится корректно, потому как в этом алгоритме все выборы привели бы к симметричной ситуации с точностью до переименования. Одна из ситуаций подошла бы нам, но так как они эквивалентны, то подходят все.

6. **Докажите, что любую перестановку из S_n можно получить, перемножая транспозицию $(1, n)$ и цикл $(1, 2, 3, \dots, n)$.**

   Имея два элемента (a, b) и $(a, a+1, \dots, b-1, b)$ можно их перемножить $(a, b)(a, a+1, \dots, b-1, b) = (a+1, \dots, b-1, b)$ или $(a, a+1, \dots, b-1, b)(a, b) = (a, a+1, \dots, b-1)$. Обратные к элементам равняются некоторой степени этого элемента, а значит мы можем брать обратные. Тогда продолжив дальше перемножение мы сможем выразить $(a, a+1, \dots, b-1)(b, b-1, \dots, a+1) = (a, b, b-1)$, а также $(b, b-1, \dots, a+1)(a, a+1, \dots, b-1) = (b, a, a+1)$, пройдя ещё чуть дальше мы получи $(a, b)(b, a, a+1) = (a+1, b)$ и $(a, b)(a, b, b-1) = (a, b-1)$. Тогда мы вновь получили 2 пары $(a, b-1)$ и $(a, a+1, \dots, b-1)$ и вторую пару $(a+1, b)$ и $(a+1, a+2, \dots, b)$, так что мы можем продолжить рекурсию. В итоге мы сможем выразить любую транспозицию, а значит и любой элемент симметрической группы.

7. **Пусть перестановка $\sigma \in S_n$ разложена в произведение l независимых циклов длин $\rho_1 \geq \dots \geq \rho_l \geq 1$. Выпишите формулу для:**

   - **четности σ**

     Как мы видели в 3 задаче этого листочка, это четность её дискриминант. Так что формула $(\sum_i (\rho_i - 1)) \bmod 2$.

   - **порядка перестановки σ**

     Степень перестановки это в точности произведение степеней её циклов. Каждый цикл редуцируется, если степень делит его порядок. Наименьшее число удовлетворяющее этому свойству это в точности наименьшее общее кратное, то есть $\rho_1 \vee \dots \vee \rho_l$.

   - **порядка класса сопряженности σ**

     Заметим, что сопряжение по транспозиции не меняет численный тип разбиения на циклы, так как $(ab)(ad \dots c)(ab) = (bd \dots c)$, $(ab)(c \dots eabf \dots k)(ab) = (af \dots kc \dots eb)$ и $(ab)(ad \dots c)(bd' \dots c')(ab) = (bd \dots c)(ad' \dots c')$. Это достаточно проверить для транспозиций, так как остальные элементы группы раскладываются через них. Более того одна перестановка может быть получена из другой того же типа через переименование индексов, а это как мы видели в 7 задаче 1 листочка является сопряжением по перестановке индексов. Так что размер класса сопряженности это в точности размер типового класса. Сначала выберем упорядоченные наборы, чтобы потом на них надеть скобки и получить циклы, это можно сделать $n!/(n - (\rho_1 + \dots + \rho_l))!$ количеством способов. Дальше расставим скобки в порядке убывания. Сначала самые длинные циклы, потом меньшие итд. Это делается 1 способом. В итоге для каждого элемента мы получим повторения, одно получается из другого через циклическую перестановку внутри одних скобок. Тогда у нас будет $\prod_i \rho_i$ перестановок и конечная формула равняется $\frac{n!}{(n-(\rho_1+\dots+\rho_l))! \prod_i \rho_i}$

   - **порядок централизатора σ**

     Зададим действии $* \; G = S_n$ на G через сопряжение. Тогда орбитой σ по этому действию будет его класс $G * \sigma = [\sigma]$, а стабилизатором – централизатор $G_\sigma = Z_\sigma$. Тогда $h * \sigma = g * \sigma$ тогда и только тогда, когда $g^{-1}h * \sigma = \sigma$ тогда и только тогда, когда $g^{-1}h \in G_\sigma$ тогда и только тогда, когда $h \in gG_\sigma = gZ_\sigma$. Это означает, что каждое значение из орбиты получается через действие элементов одного класса, а значит $|G * \sigma| = |G|/|G_\sigma|$, или $|Z_\sigma| = |G|/|G * \sigma|$. Тогда формула будет следующей $(n - (\rho_1 + ... + \rho_l))! \prod_i \rho_i$.

8. **Найдите центр группы перестановок S_n. Найдите центр группы невырожденных матриц $\mathrm{GL}_2(\mathbb{C})$.**

   Центр группы S_n уже был мной посчитан в листочке 2 задаче 6.

   Обозначим за $e_{i,j}$ матричные единицы. Тогда очевидно, что матрицы вида $k(e_{1,1} + e_{2,2})$ входят в центр. Возьмём тогда матрицу из центра.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} a & 2b \\ c & 2d \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 2c & 2d \end{pmatrix}$$

   Тогда мы получим $2b = b$ и $2c = c$, а значит они нули.

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & d \\ a & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & a \\ d & 0 \end{pmatrix}$$

   А значит, что a=d. Тогда $\mathbb{C}^*(e_{1,1} + e_{2,2})$ – весь центр.

9. **Докажите, что подгруппа внутренних автоморфизмов** $\mathrm{Inn}(G)$ **нормальна в группе автоморфизмов** $\mathrm{Aut}(G)$**. Докажите, что** $\mathrm{Inn}(G) \cong G/Z_G$**.**

   Проверим нормальность, пусть S_s – сопряжение по s, а f - автоморфизм. Тогда сопряжем $f \circ S_s \circ f^{-1}(x) = f(sf^{-1}(x)s) = f(s)xf(s)^{-1}$, получилось сопряжение по $f(s)$. А значит $\mathrm{Inn}(G)$ нормальна в $\mathrm{Aut}(G)$.

   Сопоставим элементу группы сопряжение по нему, получится сюрьективный гомоморфизм. g лежит в его ядре равносильно $gsg^{-1} = s$ или $gs = sg$ для любого s, что равносильно $g \in Z_G$. Тогда по теореме о гомоморфизме $\mathrm{Inn}(G) = \mathrm{Im}(f) \cong G/\mathrm{Ker(f)} = G/Z_G$.

10. **Докажите, что если $|G| = p^n$, где p – простое, то $|Z_G| = p^k$ для $k > 0$.**

    Центр группы – подгруппа, а значит её порядок делит порядок группы. В данном случае её порядок может быть только степенью p. Осталось показать, что она не тривиальна. Разобьем G на классы сопряженности. Как мы видели в задаче 7, порядок класса сопряженности делит порядок группы. Классы элементов не из центра имеют размер больший 1, а значат должны делится на p. Если у элемента класс состоит из него самого, то это эквивалентно тому, что он лежит в центре. Тогда будет иметь место равенство $|G| = |Z_G| + \sum[g]$, где все слагаемые кроме $|Z_G|$ делятся на p, а значит должно делится и $|Z_G|$, но это и означает, что центр не тривиален.

11. **Покажите, что невырожденные 2×2 матрицы с коэффициентами из $\mathbb{Z}_2$ образуют группу. Обозначим ее $\mathrm{GL}_2(\mathbb{Z}_2)$. Докажите, что она изоморфна S_3.**

    Как мы видели на первом листочке умножение матриц коммутативно. В данном случае, $\mathbb{Z}_2$ - поле, а значит обращение матриц определено корректно. Над данным полем оно $(ae_{1,1} + be_{1,2} + ce_{2,1} + de_{2,2})^{-1} = de_{1,1} - be_{1,2} - ce_{2,1} + ae_{2,2}$. Посчитаем порядки элементов

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

    Такие порядки у элементов группы порядка 6 могут быть только у S_3. Так что эта группа изоморфна S_3.