МИНИКУРС 'РОЖДЕНИЕ ПОНЯТИЯ ГРУППЫ'. А. Скопенков.

Like the witch, he liked to answer a question with a question; but the answers to Rose's questions were always something she'd always known, while the answers to his questions were things she had never imagined and found startling, unwelcome, even painful, altering her beliefs.
U. K. Le Guin, Dragonfly.

Перестановки. (8-9)

Данная подборка задач посвящена простейшим свойствам перестановок. Эти задачи не требуют для решения каких-либо предварительных знаний. Они подводят читателя к понятию группы, которое явно вводится в параграфе 'Циклические и нециклические группы'.

1-я серия.

1. Пятнадцать школьников сидят на занятии на пятнадцати пронумерованных стульях. Каждую минуту добрый преподаватель пересаживает их по следующей схеме:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 3 & 5 & 10 & 8 & 11 & 14 & 15 & 6 & 13 & 1 & 4 & 9 & 7 & 2 & 12 \end{pmatrix}$$

Через сколько минут все школьники впервые окажутся на своих первоначальных местах? Такое число минут называется *порядком* перестановки.

Перестановкой множества называется запись элементов этого множества в произвольном порядке. Более строго, *перестановкой* множества называется взаимно-однозначное отображение этого множества на себя (биекция). (Перестановку f удобно изображать в виде ориентированного графа, вершины которого — элементы множества, а ребра идут из вершины k в вершину $f(k)$.) Перестановка множества $\{a_1, a_2, \dots, a_n\}$, переводящая a_k в a_{i_k}, записывается в виде $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{i_1} & a_{i_1} & \dots & a_{i_n} \end{pmatrix}$ (обычно $a_k = k$). Обозначим через $(a_1a_2\dots a_n) := \begin{pmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ a_2 & a_3 & \dots & a_n & a_1 \end{pmatrix}$ *цикл.*

Композицией перестановок f и g называется перестановка $f \circ g$, определенная формулой $(f \circ g)(x) := f(g(x))$.

2. Найдите (a) $(12) \circ (13)$; (b) $(12) \circ (23)$; (c) $(23) \circ (12)$; (d) $(123) \circ (132)$; (e) $(12) \circ (13) \circ (12)$; (f) $(12345) \circ (12)$.

3. (a) Придумайте перестановки 9-элементного множества порядков 7, 10, 12, 11.

(b) Чему равен порядок перестановки, являющейся композицией непересекающихся циклов порядков $n_1, ..., n_k$? Такие перестановки $(n_1 + ... + n_k)$-элементного множества называются перестановками *типа* $\langle n_1, ..., n_k\rangle$.

(c) Любые две перестановки a и b одного типа *сопряжены*, т.е. $a = x \circ b \circ x^{-1}$ для некоторой перестановки x.

4. Найдите число перестановок типа
(a) $\langle 2, 3\rangle$; (b) $\langle 3, 3\rangle$; (c) $\langle 1, 2, 3, 4\rangle$.

---

[0]Обновляемую версию см. на www.mccme.ru/circles/oim/materials/groups.pdf. Второй пункт является обновленной версией части статьи *А. Скопенков, Олимпиады и математика, Мат. Просвещение, 10 (2006), 57–63.* В миникурс входят (не включенные в настоящий текст) материал статьи *П. Козлов и А. Скопенков, В поисках утраченной алгебры: в направлении Гаусса (подборка задач), Мат. Просвещение, 12 (2008), 127–144, http://arxiv.org/abs/0804.4357* и пунктов 'Миникурс по геометрическим преобразованиям', 'Малая теорема Ферма', 'Квадратичные вычеты', 'Первообразные корни' сборника *Математика в задачах. Сборник материалов московских выездных математических школ. Под редакцией А. Заславского, Д. Пермякова, А. Скопенкова, М. Скопенкова и А. Шаповалова. Москва, МЦНМО, 2009. www.mccme.ru/circles/oim/materilals/mvz.pdf.* Благодарю М. Скопенкова за полезные замечания.

5. Любую перестановку можно представить в виде композиции

(a) непересекающихся циклов.

(b) транспозиций, т.е. перестановок, каждая из которых меняет местами некоторые два элемента, а остальные оставляет на месте (иными словами, циклов длины 2).

(c) транспозиций $(1i)$, $i = 2, 3, \ldots, n$.

6. Назовите *две* перестановки, композициями которых можно получить любую перестановку n-элементного множества.

7. (a) Любую ли перестановку можно представить в виде композиции нескольких циклов длины 3?

(b) Любую ли перестановку можно представить в виде композиции четного числа транспозиций?

(c) *Игра в 15.* В квадратной коробочке размера 4×4 размещены 15 квадратных фишек размера 1×1 с номерами $1, 2, \ldots, 15$, а одно место осталось свободным. Первоначально фишки расставлены так, как на рисунке справа. Можно ли, последовательно сдвигая фишки на свободное место, получить расстановку фишек на рисунке слева?

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & * \end{bmatrix} \qquad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 15 & 14 & * \end{bmatrix}$$

(d) *Задача для исследования.* Головоломка из $k + l - 1$ разноветных шариков состоит из двух колец по k и l шариков, имеющих один общий шарик (см. рис., который появится позже). При каких k и l можно получить любую расстановку шариков?

Указание к 7: если не получается, читайте дальше.

2-я серия.

Пусть f — перестановка множества $\{1, 2, \ldots, n\}$. Говорят, что пара (i, j), где $1 \leq i, j \leq n$, образует *беспорядок* для перестановки f, если $i < j$, но $f(i) > f(j)$.

Перестановка называется *четной*, если общее число ее беспорядков четно.

8. Четен ли цикл длины n?

9. (a) Композиция четной (нечетной) перестановки и транспозиции нечетна (четна).

(b) Как определить четность композиции перестановок, зная четность сомножителей?

(c) Перестановка четна тогда и только тогда, когда ее можно представить в виде композиции четного числа транспозиций.

(d) Перестановка четна тогда и только тогда, когда любое ее представление в виде композиции транспозиций содержит четное их число.

10. (a) Каких перестановок n-элементного множества больше: четных или нечетных?

(b) Любую четную перестановку можно представить в виде композиции нескольких циклов длины 3.

11. В какое минимальное количество транспозиций раскладывается перестановка n-элементного множества, состоящая из k непересекающихся циклов длины больше 1?

Зачетные задачи по 1-й серии: 2def, 3ab, 4abc, 5ab, 6.
Зачетные задачи по 2-й серии: 7abc, 8, 9abcd, 10ab.

Ответы. 1. 105.
2. (132), (123), (132), e, (23), (1345).
3. (a) Нужной перестановки порядка 11 не существует. (b) НОК$(n_1, \ldots, n_k)$.
4c. $10!/4!$.
6. (12) и $(123\ldots n)$.
7. (a,b,c) Ответ: нет.

Комбинаторика классов эквивалентности. (9–11)

Данная подборка задач посвящена подсчетам числа классов эквивалентости. На примере подсчета числа раскрасок читатель подводится к важным понятиям группы и действия группы на множестве, а также к элементарной формулировке леммы Бернсайда. (Чтобы сделать этот и другие результаты менее доступными, их обычно формулируют и доказывают на языке теории абстрактных групп.)

1-я серия.

(Здесь приведены несложные задачи, которые можно решить без идей, приводящих к лемме Бернсайда.)

1. (a) Сколькими способами можно раскрасить незанумерованные грани куба в красный и серый цвета? Раскраски, совмещающиеся вращением пространства (т.е. движением пространства, сохраняющим ориентацию), считаются одинаковыми.

(b) Сколько существует различных (т.е. неизоморфных) неориентированных графов с 4 вершинами?

(c) Сколькими способами можно раскрасить в a цветов незанумерованные вершины правильного тетраэдра? Здесь раскраски, совмещающиеся движением пространства (не обязательно сохраняющим ориентацию), считаются одинаковыми.

(d) Число из (b) равно числу раскрасок полного графа на 4 вершинах в a цветов, где раскраски, совмещающиеся перестановкой вершин (т.е. автоизоморфизмом) этого графа, считаются одинаковыми.

2. Найдите число раскрасок карусели из n вагончиков в a цветов (т.е. количество раскрасок вершин правильного n-угольника в a цветов, если раскраски, совмещающиеся поворотом, неотличимы) для

(a) $n = 5$; (b) $n = 4$; (c) $n = 6$.

3. Найдите число замкнутых ориентированных связных p-звенных ломаных с вершинами в вершинах данного правильного p-угольника (где p простое). Ломаные, совмещающиеся поворотом, неотличимы.

2-я серия.

Аналогично придуманному Вами способу можно решить задачу 2 для произвольного n, однако решение будет громоздким. Приведем более простой (для "очень непростых" n) способ на примере решения задачи 2c.

Назовем *раскраской поезда* раскраску карусели из шести *занумерованных* вагончиков. (Тогда всего имеется a^6 раскрасок поезда из 6 вагончиков.)

Посчитаем двумя способами число P пар (α, s), в которых $s \in \{0,1,2,3,4,5\}$ и α — раскраска поезда, переходящая в себя при циклическом сдвиге на s вагончиков.

Циклический сдвиг на s переводит в себя ровно $a^{(s,6)}$ раскрасок поезда, поэтому

$$P = a^6 + a + a^2 + a^3 + a^2 + a.$$

С другой стороны, обозначим через $d(\alpha)$ наименьшую положительную величину циклического сдвига, при котором раскраска α поезда переходит в себя. Тогда число тех $s \in \{0,1,2,3,4,5\}$, для которых циклический сдвиг на s вагончиков переводит раскраску α поезда в себя, равно $6/d(\alpha)$. Поэтому

$$P = \sum_{\text{раскраскам } \alpha \text{ поездов}} \frac{6}{d(\alpha)} = \sum_{\text{раскраскам } \beta \text{ каруселей}} d(\beta) \cdot \frac{6}{d(\beta)} = 6X.$$

Здесь X — искомое число раскрасок. Предпоследнее равенство выполнено, поскольку

• для раскрасок α и α' поезда, переводящихся друг в друга циклическими сдвигами, $d(\alpha) = d(\alpha')$ (эти равные числа обозначаются $d(\beta)$, где β — соответствующая раскраска карусели);

• количество раскрасок поезда, получающихся циклическими сдвигами из данной раскраски α поезда (т.е. дающих ту же раскраску карусели), равно $d(\alpha)$.

Итак, $X = \dfrac{1}{6}(a^6 + 2a + 2a^2 + a^3)$.

4. Найдите число

(a) раскрасок карусели из n вагончиков в a цветов.

(b) a-цветных ожерелий из n бус. (Ожерелья считаются одинаковыми, если они совмещаются либо поворотом вокруг центра ожерелья (в плоскости) ожерелья, либо осевой симметрией ожерелья.)

5. Сколькими способами можно раскрасить незанумерованные грани куба в a цветов? Раскраски, совмещающиеся вращением пространства (т.е. движением пространства, сохраняющим ориентацию), считаются одинаковыми.

Указание: если не получается, читайте дальше.

6. Назовем *замороженной раскраской* раскраску незанумерованых граней куба. (Тогда всего имеется a^6 замороженных раскрасок.)

(a) Перечислите все вращения куба (т.е. вращения пространства, переводящие куб в себя).

(b) Как по вращению s куба найти количество $fix(s)$ замороженных раскрасок, переходящих в себя при вращении s?

(c) Найдите число P пар (α, s), в которых

• s — вращение куба и

• α — замороженная раскраска, переходящая в себя при вращении s.

7. Обозначим через $\mathrm{st}\,\alpha$ число вращений s куба, переводящих в себя замороженную раскраску α;

(a) $P = \sum\limits_{\text{замороженным раскраскам } \alpha} \mathrm{st}\,\alpha$.

(b) Для замороженных раскрасок α и α', переходящих друг в друга при некоторых вращениях, $\mathrm{st}\,\alpha = \mathrm{st}\,\alpha'$ (эти равные числа обозначаются $\mathrm{st}\,\beta$, где β — соответствующая незамороженная раскраска, т.е. раскраска незанумерованных граней куба).

(c) $P = \sum\limits_{\text{незамороженным раскраскам } \beta} \mathrm{st}\,\beta \cdot N_\beta$, где N_β — число замороженных раскрасок, отвечающих незамороженной раскраске β.

(d) Число вращений, переводящих замороженную раскраску α в замороженную раскраску α', равно $\mathrm{st}\,\alpha$.

(e) $\mathrm{st}\,\beta \cdot N_\beta = 24$.

3-я серия.

8. (a) Сколькими способами можно раскрасить незанумерованные вершины куба в a цветов? Раскраски, совмещающиеся вращением пространства (т.е. движением пространства, сохраняющим ориентацию), считаются одинаковыми.

(b) Сколькими способами можно раскрасить в a цветов незанумерованные вершины графа $K_{3,3}$? В этом графе 6 вершин, поделенных на 2 группы по 3 вершины. Ребро между двумя вершинами проведено тогда и только тогда, когда эти вершины из разных групп. Раскраски, совмещающиеся изоморфизмом этого графа, считаются одинаковыми.

9. Сформулируйте общую теорему, которую можно было бы применять вместо повторения приведенных решений.

10.* Сколько существует различных (т.е. неизоморфных) неориентированных графов с n незанумерованными вершинами? (Ответ можно оставить в виде суммы.)

11.* Отображения $\{0,1\}^n \to \{0,1\}$ (т.е. функции алгебры логики от n переменных) называются *конгруэнтными*, если они становятся равными после переименования переменных.

(a) Найдите число b_n функций алгебры логики от n переменных с точностью до конгруэнтности.

(b) Докажите, что существует $\lim\limits_{n\to\infty} n!b_n/2^{2^n}$ и найдите этот предел.

Зачетные задачи: 1a, 2a, 4ab, 5, 6abc, 7abcde, 8a.

Ответы. 1. (a) 10. (b) 11. (c) $a(a+1)(a+2)(a+3)/24$.
2. (a) $(a^5-a)/5$.
3. $((p-1)!+1)/p$.
8.a. $\frac{a^8+?a^6+?a^4}{24}$.

9. **Лемма Бернсайда.** *Пусть заданы конечное множество M и семейство $\{g_1 = id\,M, g_2, \ldots, g_n\}$ преобразований этого множества, замкнутое относительно композиции и взятия обратного элемента. Назовем элементы множества M эквивалентными, если один можно перевести в другой одним из данных преобразований, где $id\,M$ – тождественное отображение множества M в себя. Тогда число классов эквивалентности равно $\frac{1}{n}\sum\limits_{k=1}^{n} fix(g_k)$, где $fix(g_k)$ — число элементов множества M, которые преобразование g_k переводит в себя.*

Циклические и нециклические группы. (10–11)

1-я серия.

Назовем *(конечной) группой* (конечное) непустое семейство G преобразований (т.е. перестановок) некоторого множества, замкнутое относительно композиции и взятия обратного элемента (т.е. если $f, g \in G$, то $f^{-1} \in G$ и $f \circ g \in G$).

1. Любая группа содержит тождественное преобразование (оно называется *единичным элементом*).

2. Если в группе G найдется преобразование g, для которого $G = \{g, g^2, \ldots, g^n = id\}$, то группа G называется *циклической*. Любая ли группа из n преобразований является циклической для $n =$

(7) 1,2,3,4,5,6,7; (8) 8; (9) 9; (10) 10; (12) 12; (15)* 15; (21)* 21; (1001)* 1001?

Указание к 2, 3, 5b, 6bg: если не получается, читайте дальше.

3. Если число преобразований в группе является простым, то эта группа циклическая.

Порядком элемента a группы G с единицей e называется наименьшее n, для которого $a^n = e$.

4. (a) Любой элемент группы имеет (конечный) порядок.

(b) Для любого элемента a коммутативной группы G (в которой $xy = yx$) с единицей e выполнено $a^{|G|} = e$.

(c) Если в группе (не обязательно коммутативной) есть элемент порядка 2, то число элеменов группы четно.

(d) Если в группе есть элемент порядка 3, то число элеменов группы делится на 3.

(e) *Теорема Лагранжа.* Число элеменов группы делится на порядок любого ее элемента.

5. (a) Если число n четное составное или делится на квадрат простого, то существует группа из n преобразований, не являющаяся циклической.

(b) *Задача для исследования.* Для каких n любая группа из n преобразований является циклической?

2-я серия.

6. Пусть G — группа из 15 элементов, не являющаяся циклической.

(a) Порядок любого неединичного элемента в G равен 3 или 5.

(b) Может ли каждый неединичный элемент группы G иметь порядок 5?

(c) Если $f, g \in G$ — элементы порядка 5, то множества $\{f, f^2, f^3, f^4\}$ и $\{g, g^2, g^3, g^4\}$ либо не пересекаются, либо совпадают.

(d) Сформулируйте и докажите аналог предыдущего пункта для элементов порядка 3.

(e) Если $f, g \in G$ — элементы порядка 5, то один из них является степенью другого.

(f) Элементы $f, g \in G$ порядков 3 и 5 не коммутируют друг с другом.

(g) Элементы $f, g \in G$ порядка 3, для которых $\{f, f^2\} \neq \{g, g^2\}$, не коммутируют друг с другом.

7. (a) Если в группе есть подмножество из 9 элементов, замкнутое относительно умножения и взятия обратного, то число элементов в группе делится на 9.

(b) *Теорема Лагранжа.* Если H — подгруппа группы G (т.е. подмножество группы G, также являющееся группой), то количество элементов в G делится на количество элементов в H.

8. Пусть G — группа из 15 элементов, не являющаяся циклической, $f \in G$ — элемент порядка 5 и $b \in G$.

(a) порядок элемента $b^{-1}fb$ равен 5. (b) существует $\overline{b} \in \mathbb{Z}_5^*$, для которого $b^{-1}fb = f^{\overline{b}}$.

(c) $\overline{f^n} = 1$. (d) $b^{-1}f^n b = f^{n\overline{b}}$. (e) $\overline{bc} = \overline{b}\overline{c} = \overline{cb}$. (f) $\overline{b^3} = (\overline{b})^3$. (g) Такого не бывает.

9. Не существует нециклической группы из 15 элементов, в которой каждый неединичный элемент имеет порядок 3.

10. (a) Если число преобразований в группе есть произведение pq простых чисел, $p < q$ и $q - 1$ не делится на p, то эта группа циклическая.

(b)* Если p и q простые числа, $p < q$ и $q - 1$ делится на p, то существует нециклическая группа из pq элементов.

11. (Другое окончание доказательства цикличности любой группы из 15 элементов.)

(a) Количество элементов группы G, с которыми коммутирует элемент $f \in G$, равно количеству неподвижных точек преобразования $\varphi_f : G \to G$, определенного формулой $\varphi_f(g) = f^{-1}gf$.

(b) Множество $\{\varphi_f\}_{f \in G}$ является конечной группой (преобразований множества G).

(c) Если в G имеется $4x$ элементов порядка 5 и $2y$ элементов порядка 3, то $20x + 6y$ делится на 15.

12.* *Теоремы Силова.* Пусть p — простое, n делится на p^k и не делится на p^{k+1}, а G — группа из n элементов. Докажите, что

(a) В G имеется подгруппа из p^k элементов.

(b) Число таких подгрупп сравнимо с 1 по модулю p.

(c) Для любых двух таких подгрупп H и H' найдется такое преобразование $g \in G$, что $H' = \{ghg^{-1} \mid h \in H\}$.

Зачетные задачи: 3, 4bc, 5a, 6abcd, 7b, 8abcdefg.

Дальнейшее изучение элементарной теории групп можно продолжить, например, решая задачи из следующих материалов:

[1] В. Б. Алексеев, Теорема Абеля в задачах и решениях, М., МЦНМО, 2001. http://ilib.mirror1.mccme.ru/pdf/alekseev.htm

[2] А. Я. Белов-Канель, И. Иванов-Погодаев, А. Малистов, И. Митрофанов, М. Харитонов, Замощения, раскраски и плиточные группы, материалы летней конференции Турнира городов, 2009, http://turgor.ru/lktg/2009/4/index.php.

[3] Калужнин Л. А., Сущанский В. И. Преобразования и перестановки, Физматлит, 1985. http://lib.mexmat.ru/books/3692

[4] А. Канель-Белов, И. Иванов-Погодаев, А. Малистов, Д. Баранов, И. Митрофанов, Кубик Рубика и проблема Хигмана, материалы летней конференции Турнира городов, 2008, http://olympiads.mccme.ru/lktg/2008/2/index.htm.

[5] А. Я. Канель-Белов, И. А. Иванов-Погодаев, А. С. Малистов, Алгебраические группы и проблема Бернсайда, материалы летней конференции Турнира городов, 2006, http://olympiads.mccme.ru/lktg/2006/2/index.htm.