КОГДА ЛЮБАЯ ГРУППА ИЗ N ЭЛЕМЕНТОВ ЦИКЛИЧЕСКАЯ?

представляют Д. Баранов, А. Клячко, К. Кохась, А. Скопенков и М. Скопенков

Назовем *группой* непустое семейство G преобразований (т.е. перестановок) некоторого множества, замкнутое относительно композиции и взятия обратного преобразования (т.е. если $f, g \in G$, то $f \circ g \in G$ и $f^{-1} \in G$). [1] Если в группе G найдется преобразование g, для которого $G = \{g, g^2, \dots, g^n, \dots\}$, то группа G называется *циклической*.

Этот цикл задач посвящен следующему интригующему вопросу:

Для каких n любая группа из n перестановок циклическая?

В настоящем цикле задач намечено более простое решение этого вопроса, чем в [В]. Оно не претендует на новизну.

Примеры конечных групп.

(1) Группа S_n *всех* перестановок n-элементного множества.

(2) Группа перестановок $\{\mathrm{id} = (1)(2)(3)(4), (13)(24), (1234), (1432)\}$ множества из четырех элементов.

(3) Рассмотрим квадрат на плоскости и все движения плоскости, переводящие его в себя. Это тождественное преобразование, 3 поворота и 4 симметрии. Всего 8 преобразований. Возьмем группу из 8 перестановок множества вершин квадрата, происходящих при применении перечисленных восьми преобразований плоскости.

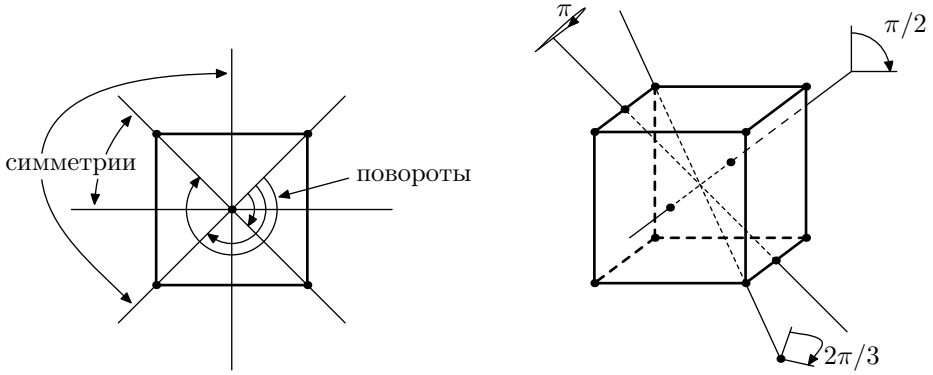

Рисунок: движения квадрата и куба

(4) Рассмотрим куб в пространстве и все вращения пространства (включая тождественное), переводящие его в себя.

(a) Возьмем группу из всех перестановок множества *вершин* куба, происходящих при применении таких вращений.

(b) Возьмем группу из всех перестановок множества *середин ребер* куба, происходящих при применении таких вращений.

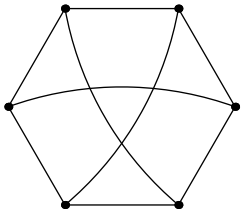

Рисунок: граф $K_{3,3}$

[1] « ...Обычно определяют группу как множество с двумя операциями, удовлетворяющими набору аксиом вроде $f(gh) = (fg)h$. Эти аксиомы автоматически выполняются для групп преобразований. В действительности эти аксиомы означают просто, что группа образована из некоторой группы преобразований забыванием преобразуемого множества. Такие аксиомы, наряду с другими немотивированными определениями, служат математикам главным образом для того, чтобы затруднить непосвященным овладение своей наукой и тем самым повысить ее авторитет.» (В.И. Арнольд.) При этом на примере решения данного цикла задач школьники увидят, что общее понятие группы все-таки полезно для изучения групп преобразований.

(5) Группа всех перестановок 6-элементного множества, являющихся изоморфизмами графа $K_{3,3}$.

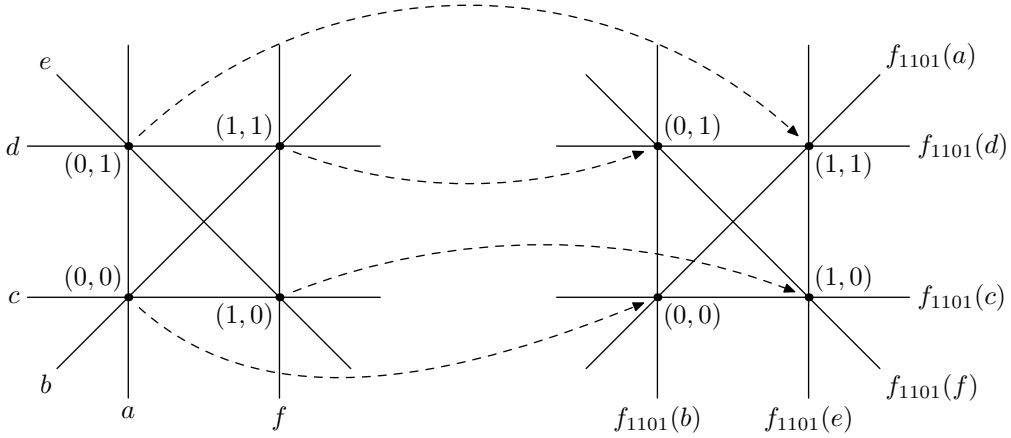

Рисунок: линейное преобразование $f_{1101} : \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$

(6) Рассмотрим множество $\mathbb{Z}_2^2 = \{(0,0),(0,1),(1,0),(1,1)\}$ упорядоченных пар вычетов по модулю 2. Для любых четырех вычетов a, b, c, d по модулю 2 рассмотрим отображение $f_{abcd} : \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$, заданное формулой $f_{abcd}(x, y) = (ax + by, cx + dy)$. Среди всех таких отображений выберем взаимно-однозначные. Они образуют группу.

Зачем? На примере исследования этого вопроса мы покажем, как появляются некоторые основные понятия теории групп. Основные идеи будут представлены на «олимпиадных» примерах: на простейших частных случаях и со сведением к необходимому минимуму алгебраического языка. [2]

«Новичку». За счет принятого стиля изложения Вам *не будет сложнее* решать приведенные задачи, чем школьникам, уже знакомым с основами теории групп. Вы освоите необходимые идеи на примере решения задач 1-й серии, которые все равно просты. Веселые задачи 3-й серии также помогут Вам освоиться.

Школьнику, уже знакомому с основами теории групп. Конечно, Вам будет *интереснее* решать приведенные задачи. Вы можете не разбирать все предлагаемые частные случаи, а сразу доказывать общий результат, из которого они вытекают, чтобы потом сконцентрироваться на новых для Вас задачах. Они имеются уже в самом начале — см. общий вопрос и некоторые пункты задачи 1.5. Если Вы используете другое определение группы, то нужно доказать его эквивалентность вышеприведенному.

Общие замечания к формулировкам задач. Если условие задачи является утверждением, то в задаче требуется это утверждение доказать. Если некоторая задача не получается, то читайте дальше — соседние задачи могут оказаться подсказками.

Звездочки. За каждое верное ($\geqslant +.$) письменное решение школьник или команда получает звездочку. По усмотрению жюри звездочка может дополнительно выдаваться за красивые решения, за решения сложных задач и за некоторые решения, набранные в tex'е. Число звездочек у жюри не ограничено. Одну звездочку можно потратить на одну попытку устной сдачи одной из задач.

Благодарим С.А. Дориченко и Г.Р. Челнокова за полезные замечания.

[2] Это не только сделает материал более доступным, но поможет тем, кто привык к абстрактному изложению, развить математический вкус. Благодаря этому они смогут разумно выбирать проблемы для исследования и ясно излагать собственные открытия, не скрывая ошибок (или известности полученного результата) за чрезмерным формализмом. К сожалению, такое (бессознательное) сокрытие ошибки часто происходит с молодыми математиками, воспитанными на чрезмерно формальных курсах.

1. ДО. 1-я серия.

Через $|X|$ обозначается число элементов в множестве X.

1.1. (a) Код для замка состоит из упорядоченного набора девяти различных ненулевых цифр. Известно следующее правило: если коды A и B открывают замок (допускается возможность $A = B$), то код, полученный заменой каждой цифры k в коде A на цифру, стоящую на k-м месте в коде B, тоже открывает замок. Известно, что замок открывает только код 856291473 и все коды, полученные из него многократным применением указанного правила. Сколько всего кодов открывают замок?

(b) Тот же вопрос для следующего правила: если код A открывает замок и B — произвольный код (допускается возможность $A = B$), то код, полученный заменой
каждой цифры в коде A, равной номеру места цифры k в коде B,
на цифру, стоящую на k-м месте в коде B,
тоже открывает замок.

1.2. (a) Докажите, что множество из примера 6 действительно является группой.

(b) Какие из приведенных примеров групп являются циклическими?

(c) Любая группа содержит тождественное преобразование (оно называется *единичным элементом* и обозначается e).

1.3. (a) Придумайте группу и в ней две перестановки a и b, для которых $ab = b^{-1}a$.

(b) В языке племени Абаба 2 буквы: «а» и «б». Если в любом месте любого слова этого языка вставить или вычеркнуть буквосочетание «ааб» или буквосочетание «бба», то смысл слова от этого не изменится. На скале нацарапано 4 слова на языке Абаба. Докажите, что среди них есть два, совпадающих по смыслу.

1.4. (a) Придумайте группу из 17 перестановок, которые можно так занумеровать числами $0, 1, 2, \ldots, 16$, чтобы номер композиции был бы равен *сумме* номеров 'сомножителей' по модулю 17.

(b) Придумайте группу из 16 перестановок, которые можно так занумеровать числами $1, 2, \ldots, 16$, чтобы номер композиции был бы равен *произведению* номеров 'сомножителей' по модулю 17.

(c) Существует ли группа из 8 перестановок, которые можно так занумеровать числами $1, 2, 4, 7, 8, 11, 13, 14$, чтобы номер композиции был бы равен *произведению* номеров 'сомножителей' по модулю 15?

1.5. Любая ли группа из n преобразований является циклической для следующих значений n:

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

> Группа G называется *коммутативной*, если $xy = yx$ для любых $x, y \in G$.
> *Порядком* $\operatorname{ord} a$ элемента a группы G с единичным элементом e называется наименьшее целое положительное n, для которого $a^n = e$ (если такое n существует).

1.6. (a) *Теорема Ферма-Эйлера.* Для любого элемента a конечной коммутативной группы G с единичным элементом e выполнено $a^{|G|} = e$.

(b) Любая циклическая группа является коммутативной.

(c) Верно ли обратное?

1.7. Если количество элементов в группе является простым числом, то эта группа циклическая.

1.8. (a) Найдите порядок каждого элемента в группе S_4.

(b) Любой элемент конечной группы имеет (конечный) порядок.

(c) Если в конечной группе есть элемент порядка 2, то число элементов группы четно.

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

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

(f) В любой группе из четного числа элементов есть элемент порядка 2.

1.9. (a) Если число n четное составное, то существует группа из n преобразований, не являющаяся циклической.

(b) Если число n делится на квадрат простого, то существует группа из n преобразований, не являющаяся циклической.

1.10. (a) Любая коммутативная группа из 10 элементов является циклической.

(b) То же для 21 элемента.

(c) То же для 1001 элемента.

(d) Для каких n любая коммутативная группа из n элементов является циклической?

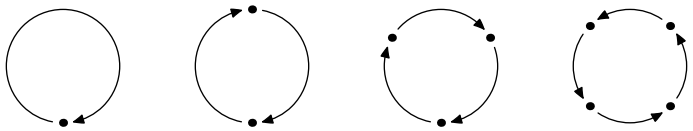

Рисунок: перестановка типа $\langle 1, 2, 3, 4\rangle$

1.11. Перестановка $(n_1 + ... + n_k)$-элементного множества, являющаяся композицией непересекающихся циклов порядков $n_1, ..., n_k$, называется перестановкой *типа* $\langle n_1, ..., n_k\rangle$.

(a) Докажите, что любые две перестановки f и g одного типа *сопряжены* в группе S_n, т.е. $g = b^{-1}fb$ для некоторой перестановки $b \in S_n$.

(b) Докажите обратное.

(c) Порядки сопряженных перестановок равны.

1.12. Пусть G — группа из 15 элементов.

(a) В G есть элемент порядка 3.

(b) Любой элемент порядка 5 в G сопряжен только со своими степенями.

2. ДО. 2-я серия.

Некоторые решения.

Решение задачи 1.2. (c) $\quad f \in G \quad \Rightarrow \quad f^{-1} \in G \quad \Rightarrow \quad ff^{-1} = e \in G.$

Решение задачи 1.5-7 для $n = 3$. Пусть, напротив, имеется нециклическая группа G из трех перестановок. Обозначим через a нетождественную перестановку в ней. Если $a^2 \neq e$, то перестановки a, a^2, a^3 различны и группа циклическая. Если же $a^2 = e$, то рассмотрим перестановку $b \in G$, отличную от e и a. Тогда перестановка ab отлична от e, a, b. (Действительно $ab \neq a$ и $ab \neq b$ очевидно. Если $ab = e$, то $b = a^2b = a$ — противоречие.) Противоречие.

Решение задачи 1.5-10. Рассмотрим правильный пятиугольник на плоскости. Рассмотрим все движения плоскости, переводящие его в себя. Это тождественное преобразование, 4 поворота и 5 симметрий. Всего 10 преобразований. Нужную группу образуют 10 перестановок множества вершин правильного пятиугольника, происходящих при применении перечисленных десяти преобразований плоскости. Эта группа нециклическая, поскольку для двух перестановок s и t, «пришедших из симметрий», $st \neq ts$. А если бы $s = g^k$ и $t = g^l$ для некоторой перестановки g, то $st = ts$.

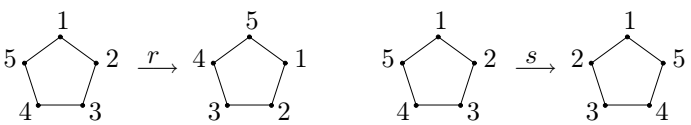

Рисунок: движения правильного 5-угольника

Другое решение задачи 1.5-10. Оно более сложное, чем предыдущее, но зато может помочь Вам в решении задачи 2.1. Рассмотрим перестановки r и s 5-элементного множества вершин правильного 5-угольника, «пришедшие» из поворота на $2\pi/5$ и из симметрии; см. рисунок. Тогда $r^5 = e = s^2$ и $sr = r^{-1}s$. Рассмотрим 10 перестановок $r^k s^l$, $k, l \in \mathbb{Z}$. Из соотношения $sr = r^{-1}s$ можно получить, что это множество является группой. (Именно в этом отличие приводимого решения от предыдущего — мы получили замкнутость относительно композиции и взятия обратного не из геометрических соображений, а из комбинаторных. Поэтому появилась возможность обобщать это доказательство на случаи, когда геометрической интерпретации не видно.) Из этого же соотношения вытекает, что эта группа не является циклической.

Новые задачи.

2.1. (a) Существует нециклическая группа из 21 элемента.

(b) Существует нециклическая группа из 55 элементов.

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

Указание к 2.1a. См. вышеприведенное другое решение задачи 1.5-10. Попробуйте сообразить, каким соотношениям должны удовлетворять перестановки r и s, чтобы множество $r^k s^l$, $k, l \in \mathbb{Z}$, образовывало бы нециклическую группу из 21 перестановки. А потом попробуйте придумать такие перестановки.

Подгруппой группы G называется подмножество группы G, также являющееся группой.

2.2. (a) Может ли в коммутативной группе из 10 элементов быть два различных элемента порядка 2? (Это подсказка к задаче 1.10a.)

(b) *Теорема Лагранжа.* Число элементов в конечной группе делится на число элементов в любой ее подгруппе.

2.3. (Это подсказка к задаче 1.12b.) Пусть G — группа из 15 элементов и $f, g \in G$ — элементы порядка 5.

(a) Множества $\{f, f^2, f^3, f^4\}$ и $\{g, g^2, g^3, g^4\}$ либо не пересекаются, либо совпадают.

(b) Один из элементов f, g является степенью другого.

2.4. Пусть G — группа из 15 элементов, $f \in G$ — элемент порядка 5, $b \in G$, $b^{-1}fb = f^m$ и $k \in \mathbb{Z}$, $k > 0$. Тогда $b^{-1}f^k b = f^{km}$ и $b^{-k}fb^k = f^{m^k}$.

2.5. Пусть G — группа из 15 элементов, в которой каждый неединичный элемент имеет порядок 3. Пусть $f, g \in G - e$.

(a) Множества $\{f, f^2\}$ и $\{g, g^2\}$ либо не пересекаются, либо совпадают.

(b) Если $\{f, f^2\} \neq \{g, g^2\}$, то $fg \neq gf$.

(c) С каждым неединичным элементом сопряжено ровно 4 других элемента.

2.6. (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) Пусть G — группа из 1001 элемента и $f \in G - \{e\}$. Докажите, что G циклическая, если f сопряжен только со своими степенями.

3. ДО. 3-я серия

Веселые задачи этой серии на более абстрактном языке описывают важную идею, приведенную в указании к задаче 2.1a. Формально, они не нужны для нашей главной цели.

3.1. [3] В языке Велосипедистов (англ. Cyclists) имеется две буквы a и a^{-1}. Они называются *противоположными*.

В этом и других рассматриваемых языках *словами* называются все конечные упорядоченные наборы из букв; в частности, имеется *пустое* слово, в котором нет букв (т.е. молчание тоже имеет значение).

Слово «восьмерка», состоящее из восьми букв a подряд, считается *неприличным*. Слово, состоящее из двух противоположных букв подряд, называется *запинкой*.

В этом и других рассматриваемых языках смысл слова не меняется от

• зачеркивания в любом месте любого неприличного подслова или запинки, а также от

• добавления в любое месте любого неприличного подслова или запинки.

(Научно выражаясь, смысл — класс эквивалентности слов относительно операций вставки и удаления неприличных слов или запинок).

Например, на языке Велосипедистов слова $aaaa^{-1}a$ и aaa различны, но имеют одинаковый смысл.

(a) У Велосипедистов имеется всего 8 смыслов.

(b) Велосипедисты разговаривают о вычетах по модулю 8. Иными словами, множество смыслов с операцией приписывания *изморфно* множеству вычетов по модулю 8 с операцией суммы по модулю 8. Приведем четкую формулировку этого утверждения. Слова можно приписывать одно к другому: из слов X и Y получается слово XY. (Например, из слов aa и $aa^{-1}a$ получается слово $aaaa^{-1}a$.) Эта операция на множестве слов задает операцию «приписывания» на множестве смыслов. Так вот, восемь смыслов можно занумеровать вычетами по модулю 8 так, что номер смысла слова XY равен сумме (по модулю 8) номера смысла слова X и номера смысла слова Y.

3.2. Для обеспечения секретности сотрудники Пентагона придумали специальный язык. В нем имеются четыре буквы a, b, a^{-1} и b^{-1}. Буквы a и a^{-1} называются *противоположными*. Буквы b и b^{-1} тоже. Пять букв a подряд или две буквы b подряд образуют неприличное слово. Еще одно неприличное слово — ... В нем 4 буквы, первые три из которых — такие же, как в слове $abab$, а последние три из которых — такие же, как в слове $a^{-1}bbab^{-1}$.

(a) У сотрудников Пентагона имеется всего 10 смыслов.

(b) Сотрудники Пентагона разговаривают о движениях множества вершин правильного пятиугольника на плоскости. Дайте сами четкую формулировку этого утверждения!

3.3. В языке Ценителей Совершенства также четыре буквы a, b, a^{-1} и b^{-1}. Три буквы a подряд или две буквы b подряд образуют неприличное слово. Еще одно неприличное слово — ... В нем 10 букв, и оно получается записыванием пять раз подряд слова ba.

(a) У Ценителей Совершенства имеется конечное количество смыслов.

(b) Ценители Совершенства разговаривают о некоторой группе. Дайте сами четкую формулировку этого утверждения!

3.4. (a) В языке Алгебраистов также четыре буквы a, b, a^{-1} и b^{-1}. Неприличные слова настолько неприличны, что в этом тексте неуместно не только описывать их, но даже говорить, конечно ли их число. Докажите, что Алгебраисты разговаривают о некоторой группе. Дайте сами четкую формулировку этого утверждения! (Эта группа может оказаться бесконечной, даже если неприличных слов конечное число.)

(b) Если в язык Алгебраистов добавить новые буквы c и c^{-1} и некоторые новые неприличные слова, то Алгебраисты по-прежнему будут разговаривать о некоторой группе.

---

[3] Это — пример *некрасивой* задачи по математике. Понять ее условие сложнее, чем придумать решение (понимая условие). Однако нам эта задача нужна, чтобы на простейшем примере показать важную конструкцию.

4. ПОСЛЕ. 4-я серия.

Некоторые решения.

1.8. (d) Пусть a — элемент порядка 3. Выпишем все элементы группы. Теперь будем постепенно зачеркивать их следующим образом: на каждом шаге выбираем произвольным образом незачеркнутый элемент x и зачеркиваем 3 элемента x, xa, xa^2. При этом никакой элемент мы не зачеркнем больше одного раза: действительно, предположим, что, например, зачеркиваемый элемент xa уже был зачеркнут. Тогда либо $xa = y$, либо $xa = ya$, либо $xa = ya^2$ для некоторого ранее выбранного элемента y. Но тогда либо $x = ya^2$, либо $x = y$, либо $x = ya$. Таким образом, элемент x уже был зачеркнут. Полученное противоречие доказывает, что на каждом шаге зачеркивается ровно 3 новых элемента. В конце будут зачеркнуты все элементы. Значит, число элементов группы делится на 3.

(e) *Теорема Лагранжа.* Для $x \in G$ рассмотрим множество $\{x, xf, xf^2, \dots, xf^{\operatorname{ord} f - 1}\}$. По определению порядка указанные элементы различны. Значит, в этом множестве $\operatorname{ord} f$ элементов. Если $xf^k = yf^l$, то $y = xf^{k-l}$. Поэтому для разных x эти множества либо не пересекаются, либо совпадают. Значит, $|G|$ делится на $\operatorname{ord} f$.

1.10. (a) Обозначим через p порядок неединичного элемента f. Если $p = 10$, то группа циклична. Пусть теперь $p < 10$. По теореме Лагранжа $p \in \{5, 2\}$. Если есть элемент g порядка $10/p$, то $G = \{fg, (fg)^2, \dots, (fg)^{10}\}$. Иначе есть элемент $g \notin \{f, f^2, \dots, f^p\}$ порядка p. Тогда $\{f^k g^l\}_{k,l \in \mathbb{Z}}$ есть подгруппа порядка p^2. Противоречие с теоремой Лагранжа.

1.11. *Указание.* Перенумеруем элементы множества так, чтобы f перешла в g. Эта перенумерация задает требуемую перестановку b.

2.3. (a) Предположим, что эти множества пересекаются. Тогда существуют такие натуральные числа $1 \leq k, l \leq 4$, что $f^k = g^l$. Так как НОД$(k, 5) = 1$, то существует такое целое число m, что $5 \,|\, km - 1$. Тогда $f = f^{km} = (f^k)^m = (g^l)^m = g^{lm}$. Отсюда следует, что эти множества совпадают.

(b) Рассмотрим 25 элементов $f^k g^l$ для $1 \leq k, l \leq 5$. Так как в группе всего 15 элементов, то существуют $1 \leq k, l, m, n \leq 5$ такие, что $(k, l) \neq (m, n)$ и $f^k g^l = f^m g^n$. Домножая на f^{-m} слева и на g^{-l} справа, получаем $f^{k-m} = g^{n-l}$. Так как f и g — элементы порядка 5, то множества $\{f, f^2, f^3, f^4\}$ и $\{g, g^2, g^3, g^4\}$ пересекаются. Из (a) получаем, что они совпадают.

2.5. (c) *Указание.* Рассмотрим элемент $f \neq e$. Обозначим число сопряженных с ним элементов $c(f)$ (вместе с самим элементом f). Рассмотрим множество

$$Z(f) := \{g \in G : fg = gf\}$$

. Из (b) следует, что $Z(f) = \{e, f, f^2\}$. Теперь из того, что $c(f) \cdot |Z(f)| = |G|$ получаем $c(f) = 15/3 = 5$.

2.1. (a) *Новое указание.* Искомая группа является группой некоторых перестановок 49-элементного множества $\mathbb{Z}_7^2$. Для описания группы представим его элементы как пары (x, y) вычетов по модулю 7. Для любых целых неотрицательных k, l определим преобразование

$$f_{k,l} : \mathbb{Z}_7^2 \to \mathbb{Z}_7^2 \quad \text{формулой} \quad f_{k,l}(x, y) := (2^k x, lx + y).$$

Проверьте, что

- таких преобразований ровно 21;
- они образуют группу;
- эта группа не является циклической.

2.1. (b) *Указание.* Воспользуйтесь тем, что $2^5 = 33 - 1$. Для любых целых неотрицательных k, l определим преобразование $f_{k,l} : \mathbb{Z}_{11}^2 \to \mathbb{Z}_{11}^2$ формулой $f_{k,l}(x, y) := (4^k x, lx + y)$.

3.3. *Указание.* Проще всего использовать то, что Ценители Совершенства являются Алгебраистами.

3.4. *Указание.* Сопоставьте каждому смыслу преобразование множества смыслов, определяемое как «приписывание данного смысла слева».

Новые задачи.

4.1. Существует нециклическая группа из 39 элементов.

4.2. Пусть G — группа из 1001 элемента и $f \in G - \{e\}$. Предположим, что f сопряжен только с некоторыми своими степенями. Пусть $h \notin \langle f\rangle := \{f, f^2, \dots, f^n, \dots\}$. Обозначим через q наименьшее из целых положительных n, для которых $h^n \in \langle f\rangle$.

(a) q делит $\operatorname{ord} h$.

(b) Если $h^{-1}fh = f^k$, то $h^{-n}fh^n = f^{k^n}$.

(c) $h^{-1}fh = f$.

(d) $\{fh, (fh)^2, (fh)^3, \dots, (fh)^{q \operatorname{ord} f}\}$ подгруппа в G.

4.3. Пусть G — группа из 1001 элемента, не являющаяся циклической.

(a) Каждый элемент содержится в максимальной по включению подгруппе, не совпадающей со всей G.

Такие подгруппы будем сокращенно называть *максимальными подгруппами.*

(b) Каждая максимальная подгруппа является циклической.

4.4. Назовем *коммутативизатором* группы G множество

$$Z = Z(G) := \{a \in G \ : \ ga = ag \text{ для любого } g \in G\}$$

тех элементов, которые коммутируют со всеми. (Мы надеемся, что использование слова *коммутативизатор* вместо общепринятого *центр* более удобно для начинающих.)

(a) Найдите $Z(S_n)$ для каждого $n = 2, 3, 4, \dots$

(b) Коммутативизатор группы является подгруппой.

4.5. Пусть G — группа из 1001 элемента, не являющаяся циклической. Пусть порождающий элемент любой максимальной подгруппы сопряжен не только со своими степенями.

(a) Любая максимальная подгруппа содержит коммутативизатор.

(b) Выразите через $|F|$ и $|Z|$ число элементов, сопряженных элементам максимальной подгруппы F.

5. ПОСЛЕ. 5-я серия

Указание к задаче 1.4c. Такую группу удобно придумывать как подгруппу в группе перестановок множества $\{1, 2, 4, 7, 8, 11, 13, 14\}$

5.1. (a) Для любых группы G и элемента $g \in G$ множество

$$N(g) = N_G(g) := \{a \in G \ : \ ga = ag^k \text{ для некоторого } k\}$$

является подгруппой.

(b) Найдите $N_{S_3}(g)$ для каждого $g \in S_3$.

(c) Число различных подгрупп, сопряженных с $\langle g\rangle$, равно $|G|/|N(g)|$.

5.2. Пусть G — группа из 1001 элемента, не являющаяся циклической. Предположим, что порождающий элемент любой максимальной подгруппы (напомним, что по утверждению задачи 4.3b она циклическая) сопряжен не только со своими степенями.

(a) Пересечение двух максимальных подгрупп равно коммутативизатору.

(b) Число различных подгрупп, сопряженных с максимальной подгруппой F, равно $1001/|F|$.

(c) Для числа $\widehat{F}$ элементов, сопряженных элементам максимальной подгруппы F и не лежащих в коммутативизаторе, справедливы неравенства $500 < \widehat{F} \leq 1000 - |Z|$.

Теорема о первообразном корне. Для любого простого p существует число g, для которого остатки от деления на p чисел $g^1, g^2, g^3, \dots, g^{p-1} \equiv 1 \mod p$ различны.

5.3. *Доказательство теоремы о первообразном корне.* Здесь латинскими буквами обозначаются целые неотрицательные числа. Пусть p простое и a не делится на p.

(a) $p-1$ делится на наименьшее $k>0$, для которого $a^k \equiv 1 \bmod p$.

Указание: используйте малую теорему Ферма.

(b) Для любых целых n и a сравнение $x^n \equiv a \bmod p$ имеет не более n решений.

(c) Если $p-1$ делится на d, то сравнение $x^d \equiv 1 \bmod p$ имеет ровно d решений.

(d) Докажите теорему о первообразном корне для $p = 2^m + 1$.

(e) Докажите теорему о первообразном корне для $p = 2^m \cdot 3^n + 1$.

(f) Докажите теорему о первообразном корне для *произвольного* простого p.

(g)* Верно ли, что число 3 является первообразным корнем по модулю любого простого числа вида $p = 2^m + 1$?

5.4. Для каких n любая группа из n элементов является коммутативной?

6. Указания и решения, выдаваемые после окончательного финиша

2.1c. По теореме о первообразном корне существует элемент $a \in \mathbb{Z}_q$ порядка p. Для любых целых неотрицательных k, l определим преобразование $f_{k,l} : \mathbb{Z}_q^2 \to \mathbb{Z}_q^2$ формулой $f_{k,l}(x,y) := (a^k x, lx + y)$. Нетрудно проверить, что

- таких преобразований ровно pq;
- они образуют группу;
- эта группа не является циклической.

3.1. *Указание.* Положим *номер смысла* данного слова равным разности между числом букв a и a^{-1} в этом слове по модулю 8.

3.2. *Указание.* Биекция между смыслами и движениями правильного пятиугольника строится следующим образом: букве a поставим в соответствие поворот на 72° против часовой стрелки с центром в центре пятиугольника. Букве b поставим в соответствие такое отражение, что выполняется $a \circ b \circ a \circ b^{-1} = id$; смыслу слова будет соответствовать композиция движений, соответствующих его буквам.

3.3b. *Первое решение.* Следует из задачи 3.4a.

3.3b. *Второе решение.* Ценители Совершенства разговаривают о группе всех таких перестановок вершин правильного икосаэдра, которые получены из вращений трехмерного пространства, переводящих икосаэдр в себя. То есть о группе A_5.

4.2. (b) Утверждение доказывается индукцией по n.

5.3. *Указания.* (b) Докажем более общее утверждение: *многочлен степени n не может иметь более n корней в множестве $\mathbb{Z}/p\mathbb{Z}$ вычетов по модулю p (в котором имеются операции сложения и умножения по модулю p).* Здесь многочленом называется бесконечный упорядоченный набор $(a_0, \dots, a_n, \dots)$ вычетов по модулю p, в котором лишь конечное число элементов отлично от нуля. Обычно многочлен записывается в виде $a_0 + a_1 x + \dots + a_k x^k$ (если $a_{k+1} = a_{k+2} = \dots = 0$). Эта запись дает отображение $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Будьте осторожны: разным многочленам может соответствовать одно и то же отображение. *Корнем* многочлена $a_0 + a_1 x + \dots + a_k x^k$ называется такой вычет x_0 по модулю p, что выполнено

$$a_0 + a_1 x_0 + \dots + a_k x_0^k = 0.$$

Пусть многочлен $P(x)$ степени n имеет в $\mathbb{Z}_p$ различные корни $x_1, \dots, x_n, x_{n+1}$. Представьте его в виде

$$P(x) = b_n(x - x_1)\dots(x - x_n) + b_{n-1}(x - x_1)\dots(x - x_{n-1}) + \dots + b_1(x - x_1) + b_0$$

('*интерполяция Ньютона*'). Последовательно подставляя в сравнение $P(x) \equiv 0 \bmod p$ вычеты $x_1, \dots, x_n, x_{n+1}$, получим $b_0 \equiv b_1 \equiv \dots \equiv b_{n-1} \equiv b_n \equiv 0 \bmod p$.

То же самое решение можно записать и так. Пусть P — многочлен. Тогда $P - P(a) = (x-a)Q$ для некоторого многочлена Q степени меньше $\deg P$. Поэтому если $P(a) = 0$, то

$P = (x - a)Q$ для некоторого многочлена Q степени меньше $\deg P$. Теперь требуемое в задаче утверждение доказывается индукцией по степени многочлена P с использованием простоты числа p.

(c) *Первое указание.* Заметьте, что многочлен $x^{p-1} - 1$ имеет ровно $p - 1$ корень в множестве $\mathbb{Z}/p\mathbb{Z}$ и делится на $x^d - 1$. Докажите, что если многочлен степени a имеет ровно a корней и делится на многочлен степени b, то этот многочлен степени b имеет ровно b корней.

(c) *Второе указание.* Если $p = kd$, то для любого a сравнение $y^k \equiv a \bmod p$ имеет не более k решений.

(d) Если первообразного корня нет, то по (a) сравнение $x^{2^{m-1}} \equiv 1 \bmod p$ имеет $p - 1 = 2^m > 2^{m-1}$ решений.

(e,f) Аналогично (d).

5.4. *Указание.* Все группы порядка n абелевы тогда и только тогда, когда в разложении числа n на простые сомножители $n = p_1^{k_1} \dots p_l^{k_l}$

- $k_i < 3$;
- p_i не делит $p_j^{k_j} - 1$.

Доказывается это примерно так же, но в случае 1 надо воспользоваться тем, что любая конечная абелева группа раскладывается в прямое произведение циклических подгрупп.

Остальные задачи тривиальны или покрываются прилагаемым текстом [BKS].

Литература

[A] В.И. Арнольд, Обыкновенные дифференциальные уравнения, М, Наука, 1984.

[B] Ken Brown, Mathematics 4340, When are all groups of order n cyclic? Cornell University, March 2009, http://www.cornell.edu/ kbrown/4340/cyclic_only_orders.pdf

[BKS] В. Брагин, А. Клячко, А. Скопенков. Когда любая группа из n элементов циклическая?

[KS] Л.А. Калужнин, В.И. Слущанский, Преобразования и перестановки. М.: 1979, 112 стр.

[KM] Каргаполов М.И., Мерзляков Ю.И., Основы теории групп, М., Наука, 1982. http://arhivknig.com/obrazovanie/87077-osnovy-teorii-grupp.html

[K] А.И. Кострикин, Введение в алгебру. Основы алгебры. 1994.