МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ)

В. В. Беляев

ЗАДАЧИ
ПО ТЕОРИИ ГРУПП

МОСКВА
МФТИ
2013

УДК 512.54
ББК 22.144

Рецензент:
Кандидат физико-математических наук *Чубаров И. А.*

Беляев, В. В.
Задачи по теории групп. – М.: МФТИ, 2013. – 42 с.
ISBN

Сборник задач по теории групп предназначен для студентов второго курса ФИВТ, направление 010400 «Прикладная математика и информатика», слушающих курс лекций «Теория групп». В него входят задачи, закрепляющие понимание основных понятий теории групп, а также некоторые комбинаторные задачи, требующие знания этой теории.

Сборник может использоваться студентами первого курса для формирования навыков работы с основными алгебраическими понятиями. С этой целью в сборник включен ряд дополнительных задач.

Кроме того, данное пособие дополнено программой курса «Теория групп» и экзаменационными вопросами.

Содержание

Введение

На сегодняшний день теория групп, а точнее, групповой язык, применяется практически во всех областях математики: геометрии и топологии, теории дифференциальных уравнений и функциональном анализе, дискретной математике и компьютерных науках и т.д. В каком объеме студент младших курсов должен знать теорию групп? Что может он усвоить за 15 лекций, которые предлагаются ему по учебному плану? Ответ на эти вопросы зависит от многих условий: от уровня математической культуры студентов, научных интересов преподавателей, читающих лекции и ведущих семинарские занятия, от специализации студента, от востребованности языка теории групп в других математических курсах лекций и еще от многих других причин.

Данный сборник задач по теории групп составлен из реальных задач, которые предлагались студентам второго курса ФИВТ в осеннем семестре 2011–2012 учебного года. Задачи составлялись сразу после чтения соответствующего теоретического материала и предназначались для закрепления на практике некоторых базисных понятий теории групп.

Должен сказать, что исходная программа курса, которая также помещена в это пособие, несколько раз корректировалась по ходу чтения лекций, так как некоторые понятия оказались слишком сложными для их усвоения в таком кратком курсе, и окончательный итог всех изменений программы в какой-то степени отражен в экзаменационных вопросах, также представленных в конце пособия. Говорю «в какой-то степени», так как мной было принято решение не выносить на экзамен некоторые сложные теоретические результаты из курса лекций. Таким образом, курс лекций и, следовательно, подбор задач к нему находятся в состоянии развития, и данное пособие отражает лишь его первоначальное состояние.

Какие же наиболее существенные изменения произошли в курсе лекций по сравнению с исходной программой? На лекциях не рассматривались последние два раздела программы:

примитивные групповые пространства и базисные идеи теории Галуа. Последние — основы теории Галуа — были удалены из курса по следующим причинам. Во-первых, их трудно изложить в кратком курсе теории групп, и, во-вторых, они не являются важным материалом для будущих специалистов в области дискретной математики и компьютерных наук. В моей программе курса теория Галуа появилась лишь по просьбе некоторых сильных студентов и планировалась для краткого изложения в случае свободного времени. Что касается темы примитивных групповых пространств, то ее сокращение, особенно понятие орбитала, в будущем нежелательно, так как в этом разделе закладываются основы связи между группами и симметрическими графами.

Вместо удаленных двух разделов были прочитаны лекции по раскрашиванию групповых пространств, доказаны теоремы Силова и основная теорема о строении конечной абелевой группы. Если тема раскрашиваний была выбрана в связи с общей комбинаторной направленностью курса лекций, то теоремы Силова излагались по просьбе преподавателей, ведущих семинары. Структурная теорема теории конечных абелевых групп оказалась удобным материалом как с лекционной точки зрения, так и с точки зрения ведения семинарских занятий. Основная идея доказательства этой теоремы знакома студентам с первого курса: они сталкиваются с ней при изучении действия нильпотентного оператора векторного пространства, а на семинарах эта теорема хорошо усваивается с помощью простых комбинаторных задач.

Кроме задач по теории групп, данное пособие включает в себя раздел дополнительных задач, которые предлагались студентам еще на первом курсе. Хотя большинство из этих задач и не имеет групповой формулировки, но знание и понимание данного дополнительного материала активно использовалось нами как на лекциях, так и на семинарах по теории групп. Поэтому считаю полезным включить в данное пособие некоторые задачи первого семестра.

В. В. Беляев

ЧАСТЬ I. **Задачи по теории групп**

§ 1. Подстановки

1.1. Для каких действительных a, b и c отображение $f\colon \mathbb{R} \to \mathbb{R}$, заданное многочленом

$$f(x) = x^3 + ax^2 + bx + c,$$

является подстановкой множества $\mathbb{R}$?

1.2. Для каких целых a и b отображение $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$, заданное как

$$f(x) = ax + b,$$

является подстановкой множества $\mathbb{Z}_n$?

1.3. Доказать, что число различных подстановок степени n равно $n!$.

1.4. Подстановка g множества $\{1, 2, \ldots, 9\}$ определена равенством

$$g(i) = 10 - i.$$

Найти циклический тип подстановки и построить её граф.

1.5. Найти число различных циклических типов подстановок степени n для $n = 1, 2, \ldots, 10$.

1.6. Найти циклические типы всех подстановок множеств $\mathbb{Z}_6$, $\mathbb{Z}_7$ и $\mathbb{Z}_{11}$, заданных следующим образом:

а) $f(x) = x + a$,

б) $f(x) = ax$,

где a — целое число.

1.7. Найти число подстановок степени 6, имеющих циклический тип 2^3, и выписать все эти подстановки.

1.8. Найти число транспозиций степени n для произвольного n.

1.9. Найти число 3-циклов степени n для произвольного n.

1.10. Найти число подстановок степени n, имеющих циклический тип 2^2.

1.11. Найти число подстановок степени $2n$, имеющих циклический тип 2^n.

1.12. Для $1 \leqslant r \leqslant n$ показать, что существует точно $\dfrac{n!}{r \cdot (n-r)!}$ r-циклов степени n.

1.13. Какие подстановки множества $\{x_1, x_2, x_3, x_4\}$ не изменяют многочлен $x_1 + x_2 - x_3 - x_4$?

1.14. Найти многочлен $f(x_1, x_2, x_3, x_4) \in \mathbb{R}[x_1, \ldots, x_4]$, который не изменяется под действием подстановок (x_1, x_2, x_3, x_4) и (x_2, x_4), но не является симметрическим многочленом.

1.15. Попытаться решить задачу Лагранжа для $n \leqslant 5$: сколько различных многочленов можно получить из многочлена от n переменных, переставляя переменные произвольным образом?

§ 2. Произведения подстановок, четные и нечетные подстановки

2.1. Определите четность подстановки (т. е. знак подстановки) для подстановок из задач 1.4 и 1.6.

2.2. Доказать, что число четных подстановок конечного множества мощности $\geqslant 2$ равно числу нечетных подстановок.

2.3. Будем говорить, что подстановки g и h не пересекаются, если $\mathrm{supp}(g) \cap \mathrm{supp}(h) = \varnothing$. Доказать:

а) любая нетождественная подстановка конечного множества представима в виде произведения непересекающихся циклов;

б) любой нетривиальный n-цикл представим в виде произведения $(n-1)$-й транспозиции;

в) подстановка конечного множества является нечетной $\Leftrightarrow$ число её циклов четной длины нечетно.

2.4. Доказать, что для любой подстановки g число циклов длины $2n$ её квадрата g^2 есть четное число для любого $n \in$ $\in \mathbb{N}$.

2.5. Пусть $\Omega = \{-n, \ldots, -1, 0, 1, \ldots, n\}$ и g — подстановка Ω, удовлетворяющая условию

$$g(-i) = -g(i)$$

для любого $i \in \Omega$. Доказать, что g — четная подстановка $\Leftrightarrow$ множество

$$\{i \in \Omega \mid i > 0 \ \ \& \ \ g(i) < 0\}$$

содержит четное число чисел.

2.6. Найти подстановку, обратную к

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 5 & 4 & 2 & 8 & 6 & 7 \end{pmatrix}.$$

2.7. Как связаны между собой графы подстановок g и g^{-1}? В частности, как связаны циклические типы этих подстановок?

2.8. Пусть g и h — подстановки, носители которых имеют лишь одну общую точку. Доказать, что $g^{-1}h^{-1}gh$ есть 3-цикл.

2.9. Исследовать строение графа произведения двух подстановок, носители которых имеют точно одну общую точку.

2.10. Доказать, что графы подстановок g и h изоморфны $\Leftrightarrow$ найдется такая подстановка a, что $a^{-1}ga = h$.

2.11. Доказать, что для любой подстановки g найдется такая подстановка a, что $(ga)^2 = a^2$.

2.12. Доказать, что подстановка g конечного множества является квадратом другой подстановки $\Leftrightarrow$ для любого четного n число n-циклов подстановки g четно.

2.13. Пусть g — подстановка конечного множества, квадрат которой есть тождественная подстановка. Доказать:

$$g \text{ — нечетная подстановка} \Leftrightarrow |\operatorname{supp}(g)| \equiv 2 \pmod 4.$$

2.14. Пусть $\mathbb{Q}^+$ — множество всех положительных рациональных чисел. Функция $f\colon \mathbb{Q}^+ \to \mathbb{Q}^+$ удовлетворяет тождеству

$$f(xf(y)) = \frac{f(x)}{y}$$

для любых $x, y \in \mathbb{Q}^+$. Доказать, что f — подстановка множества $\mathbb{Q}^+$ и $f(xy) = f(x) \cdot f(y)$ для любых $x, y \in \mathbb{Q}^+$. Какой циклический тип имеет подстановка f? Построить такую функцию.

(Эта задача является вариацией одной задачи из Международной математической олимпиады 1990 года.)

§ 3. Порождающие множества $\mathbf{Sym}(\Omega)$ и $\mathbf{Alt}(\Omega)$

3.1. Пусть T — некоторое множество транспозиций из S_n. Показать, что $\langle T\rangle = S_n \Leftrightarrow$ граф T связен. Вывести отсюда, что граф минимального порождающего множества транспозиций является деревом и, следовательно, имеет $n-1$ ребро.

3.2. Найти необходимые и достаточные условия на пары i, j для того, чтобы
$$\langle (12\ldots n), (ij)\rangle = S_n.$$

3.3. Показать, что для всех i, $1 < i < n$,
$$\langle (23\ldots n), (1i)\rangle = S_n.$$

3.4. Показать, что множество всех 3-циклов порождает A_n для $n \geqslant 3$.

3.5. Показать, что S_n порождается тремя инволюциями ($n > 1$).

3.6. Пусть g и h — циклы, причем:
1) $|\operatorname{supp}(g) \cap \operatorname{supp}(h)| = 1$;
2) $\operatorname{supp}(g) \cup \operatorname{supp}(h) = \Omega$.

Доказать:
1) если по крайней мере один из циклов g или h имеет четную длину, то $\langle g, h\rangle = \operatorname{Sym}(\Omega)$;
2) если длины циклов g и h нечетны, то $\langle g, h\rangle = \operatorname{Alt}(\Omega)$.

§ 4. Понятия группы и подгруппы

4.1. Доказать, что пересечение любого семейства подгрупп есть подгруппа.

4.2. В каком случае объединение двух подгрупп является подгруппой?

4.3. Доказать: группа G содержит ровно две подгруппы $\Leftrightarrow$ G — циклическая группа простого порядка.

4.4. Доказать, что любая подгруппа циклической группы является также циклической.

4.5. Доказать, что любая конечнопорожденная подгруппа аддитивной группы $\mathbb{Q}$ является циклической.

4.6. Найти все подгруппы в циклической группе порядка p^n, где p — простое число. Найти число порождающих эту группу элементов.

4.7. Элемент порядка 2 называется *инволюцией.* Найти все инволюции в S_n для $n \leqslant 5$.

4.8. Доказать, что конечная группа четного порядка содержит инволюцию.

4.9. Доказать, что порядок любой подстановки конечного множества равен наименьшему общему кратному длин циклов подстановки.

4.10. Найти порядки подстановок из S_n для $n \leqslant 5$.

4.11. Найти порядки всех подгрупп из S_n для $n \leqslant 4$.

4.12. Доказать:

а) S_n — неабелева группа $\Leftrightarrow$ $n \geqslant 3$;

б) A_n — неабелева группа $\Leftrightarrow$ $n \geqslant 4$.

Говорят, что подгруппы $G_1, \ldots, G_n$ образуют *расщепление* группы G, если

$$\bigcup_{i=1}^{n} G_i = G \quad \text{и} \quad G_i \cap G_j = 1 \text{ для } i \neq j.$$

Подгруппы G_i называются *компонентами расщепления.*

4.13. Доказать, что порядок группы, обладающей расщеплением с n компонентами, не превосходит $(n-1)^2$.

4.14. Описать расщепляемые группы с тремя компонентами расщепления.

4.15. Пусть $x^2 = 1$ для любого $x \in G$. Доказать, что группа G абелева.

§ 5. Смежные классы и классы сопряженных элементов

5.1. Найти $|S_n : A_n|$.

5.2. Доказать, что пересечение подгрупп взаимно простых порядков тривиально.

5.3. Показать, что для любого делителя m порядка конечной циклической группы G существует подгруппа порядка m.

5.4. Пусть $|G : H_i| = n_i$, $i = 1, 2$. Доказать, что

$$|G : H_1 \cap H_2| \leqslant n_1 n_2.$$

5.5. Пусть индексы подгрупп H_1 и H_2 в группе G являются взаимно простыми числами. Доказать, что $G = H_1 H_2$, т. е.

$$G = \{xy \mid x \in H_1,\, y \in H_2\}.$$

5.6. Найти мощности всех классов сопряженных элементов в S_5.

5.7. Найти число классов сопряженных элементов в S_6.

5.8. Доказать, что группа порядка 15 абелева.

5.9. Доказать, что в S_5 нет подгрупп порядка 15.

5.10. Пусть $|G| = p^n$, где p — простое и $n > 0$. Доказать, что $Z(G) \neq 1$.

5.11. Найти все решения в натуральных числах уравнения классов для $m = 1, 2, 3$:

$$\frac{1}{x_1} + \ldots + \frac{1}{x_m} = 1.$$

5.12. Описать все конечные группы, имеющие не более трех классов сопряженных элементов.

5.13. Пусть G — объединение трех собственных подгрупп H_1, H_2 и H_3. Доказать:

а) $H_1 \cap H_2 = H_1 \cap H_3 = H_2 \cap H_3$;

б) $|G : H_i| = 2, \quad i = 1, 2, 3$.

§ 6. Нормальные подгруппы

6.1. Доказать, что пересечение нормальных подгрупп — нормальная подгруппа.

6.2. Доказать, что любой класс сопряженных элементов порождает нормальную подгруппу.

6.3. Пусть H и K — нормальные в G подгруппы. Доказать, что множество

$$HK = \{xy \mid x \in H,\, y \in K\}$$

является нормальной подгруппой в G.

6.4. Доказать, что любая подгруппа индекса 2 является нормальной.

6.5. Пусть G — абелева группа. Доказать, что G — простая группа $\Leftrightarrow$ $|G|$ — простое число.

6.6. Доказать, что любая подгруппа из $Z(G)$ является нормальной в G.

6.7. Пусть $H \lhd S_n$ и $n \geqslant 5$. Доказать, что $H = 1$, $H = A_n$ или $H = S_n$.

6.8. Найти все нормальные подгруппы в S_n для $n \leqslant 4$.

6.9. Доказать, что $Z(S_n) = 1$ для $n \geqslant 3$.

§ 7. Факторгруппы, морфизмы, теоремы об изоморфизмах, прямые произведения

7.1. Доказать, что мультипликативная группа положительных действительных чисел изоморфна аддитивной группе всех действительных чисел.

7.2. Доказать, что мультипликативная группа всех ненулевых действительных чисел изоморфна прямому произведению циклической группы порядка 2 и мультипликативной группе положительных действительных чисел. Вывести отсюда, что мультипликативная группа всех ненулевых действительных чисел неизоморфна мультипликативной группе всех положительных действительных чисел.

7.3. Доказать, что мультипликативная группа всех положительных рациональных чисел изоморфна аддитивной группе всех целочисленных финитарных строк, т. е. строк с конечным числом ненулевых координат,

$$\{(x_1, x_2, \ldots) \mid x_i \in \mathbb{Z}\},$$

с покоординатной операцией сложения.

7.4. Доказать, что мультипликативная группа комплексных чисел с модулем, равным 1,

$$T = \{z \in \mathbb{C} \mid |z| = 1\},$$

изоморфна факторгруппе $\mathbb{R}/\mathbb{Z}$, аддитивной группы $\mathbb{R}$ по группе целых чисел $\mathbb{Z}$.

7.5. Доказать, что группа вращений куба изоморфна S_4, а группа всех симметрий куба изоморфна $\mathbb{Z}_2 \times S_4$.

7.6. Доказать, что группа вращений правильного тетраэдра изоморфна A_4, а группа всех симметрий тетраэдра изоморфна S_4.

7.7. Доказать, что группа симметрий куба изоморфна группе симметрий правильного октаэдра.

7.8. Доказать, что циклическая группа порядка n изоморфна $\mathbb{Z}_n$, а бесконечная циклическая группа изоморфна $\mathbb{Z}$.

7.9. Доказать, что прямое произведение конечного набора групп является циклической группой $\Leftrightarrow$ все прямые сомножители являются циклическими группами взаимно простых порядков.

7.10. Доказать, что прямое произведение групп есть абелева группа $\Leftrightarrow$ все прямые сомножители — абелевы группы.

7.11. Доказать, что центр прямого произведения групп совпадает с произведением центров координатных подгрупп.

7.12. Пусть p — простое число. Группа G называется *элементарной абелевой p-группой*, если она, во-первых, абелева, и, во-вторых, для любого $x \in G \quad x^p = 1$.

Доказать, что G есть конечная элементарная абелева p-группа $\Leftrightarrow$ G есть прямое произведение конечного числа циклических групп порядка p.

7.13. Пусть $H \leqslant G$ и для любого $x \in G \quad x^2 \in H$. Доказать, что $H \lhd G$, и G/H — элементарная абелева 2-группа.

7.14. Классифицировать, с точностью до изоморфизма, все группы порядков $\leqslant 5$.

7.15. Пусть $V = \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle$. Доказать, что

1) $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$,
2) $V \lhd S_4$,
3) $S_4/V \cong S_3$,
4) $A_4/V \cong \mathbb{Z}_3$.

7.16. Пусть $f\colon G \to H$ — гомоморфизм. Доказать:

1) образ любой подгруппы из G есть подгруппа в H;
2) образ любой нормальной подгруппы из G есть нормальная подгруппа в $f(G)$;
3) полный прообраз любой подгруппы из $f(G)$ есть подгруппа в G;
4) полный прообраз любой нормальной подгруппы из $f(G)$ есть нормальная подгруппа в G;
5) образ любой циклической подгруппы из G есть циклическая группа;
6) образ абелевой подгруппы из G есть абелева группа.

7.17. Попытаться самостоятельно доказать вторую и третью теоремы об изоморфизмах.

7.18. Пусть G — абелева группа и $n \in \mathbb{Z}$. Доказать, что отображение $f\colon G \to G$, определенное по правилу

$$f(x) = x^n,$$

есть эндоморфизм группы G.

7.19. Пусть G — произвольная группа и $g \in G$. Доказать, что отображение $f\colon G \to G$, определенное по правилу

$$f(x) = g^{-1}xg,$$

есть автоморфизм группы G.

Замечание. Этот автоморфизм называется *внутренним.*

7.20. Пусть G — произвольная группа и $g \in G$. Допустим, что $gZ(G) \in Z(G/Z(G))$. Доказать, что отображение $f : G \to G$, определенное по правилу

$$f(x) = x^{-1}g^{-1}xg,$$

есть эндоморфизм группы G. Найти $\operatorname{Ker} f$.

§ 8. Действие группы. Орбиты и стабилизаторы

8.1. Объяснить, почему мы не можем определить действие группы G на себе левым сдвигом, полагая $a^x = xa$. Показать, как можно определить действие G сдвигом на множестве левых смежных классов $\{aH \mid a \in G\}$ подгруппы G.

8.2. Пусть группа G действует на Ω, $x, y \in G$ и $\alpha, \beta \in \Omega$. Доказать:

1) орбиты α^G и β^G либо совпадают, либо не имеют общих точек;
2) если $\beta = \alpha^x$, то $G_\beta = x^{-1}G_\alpha x$;
3) $\alpha^x = \alpha^y \;\Leftrightarrow\; G_\alpha x = G_\alpha y$.

8.3. Пусть группа G действует транзитивно на Ω. Доказать, что стабилизаторы G_α точек $\alpha \in \Omega$ образуют класс сопряженных в G подгрупп и $|G : G_\alpha| = |\Omega|$ для любого $\alpha \in \Omega$.

8.4. *Нормализатором* подмножества H в группе G называется множество

$$N_G(H) = \left\{x \in G \mid x^{-1}Hx = H\right\}.$$

Доказать, что $N_G(H)$ — подгруппа в G, причем, если H — подгруппа, то $H \leqslant N_G(H)$.

8.5. Пусть $H \leqslant G$. Доказать, что число сопряженных с H подгрупп равно $|G : N_G(H)|$.

8.6. Пусть $H \leqslant G$, $|G : H| = n$ и $K = \bigcap\limits_{x \in G} H^x$. Доказать:

1) K — наибольшая нормальная в G подгруппа, содержащаяся в H;
2) индекс $|G : K|$ является делителем $n!$;
3) K совпадает с ядром действия группы G сдвигом на правых смежных классах подгруппы H.

8.7. Пусть p — минимальное простое число, делящее порядок G. Доказать, что любая подгруппа индекса p из G является нормальной. В частности, если $|G| = p^n$, то любая подгруппа индекса p нормальна.

8.8. Пусть $H < G$ и $|G| = p^n$, p — простое. Доказать, что $H < N_G(H)$. В частности, каждая максимальная подгруппа из G является нормальной и её индекс равен p.

8.9. Пусть $|G| = p^n$, p — простое. Доказать, что для любого делителя m порядка G найдется подгруппа порядка m.

8.10. *Централизатором* подмножества $\mathcal{M}$ из группы G называется множество

$$C_G(\mathcal{M}) = \{x \in G \mid xm = mx \text{ для любого } m \in \mathcal{M}\}.$$

Доказать, что $C_G(\mathcal{M})$ — подгруппа в G и $C_G(\mathcal{M}) \leqslant N_G(\mathcal{M})$.

8.11. Пусть $a \in G$. Доказать:

$$C_G(a^G) = \bigcap_{x \in G} x^{-1}C_G(a)x.$$

8.12. Доказать, что ядро действия сопряжением группы G на классе a^G сопряженных с a элементов совпадает с централизатором $C_G(a^G)$.

8.13. Пусть Ω — G-пространство и $g, h \in G$. Доказать:

1) $\mathrm{Supp}(g^h) = (\mathrm{Supp}(g))^h$; 2) $\mathrm{Fix}(g^h) = (\mathrm{Fix}(g))^h$.

8.14. Доказать, что группа порядка $4n + 2$ имеет подгруппу индекса 2.

8.15. Доказать, что S_6 не имеет подгрупп порядков 30 и 40.

8.16. Доказать, что действие группы симметрий куба на множестве его шести граней транзитивно. Вывести отсюда, что группа симметрий куба имеет подгруппу индекса 6.

8.17. Пусть G_A — стабилизатор вершины A в группе симметрий куба. Найти все орбиты группы G_A на множестве ребер куба.

8.18. Найти порядок группы симметрий правильного додекаэдра.

8.19. Доказать, что число различных многочленов, которые можно получить из многочлена f перестановками переменных, равно индексу стабилизатора f в симметрической группе всех перестановок переменных. Вывести отсюда, что это число не может быть равно 8, 4 или 3, если f — многочлен с 5 переменными.

§ 9. Раскрашивание групповых пространств

Групповая формулировка задачи. Для данного G-пространства Ω найти число орбит действия группы G на пространстве функций $\Phi = \mathrm{Fun}(\Omega, C)$.

Любой элемент множества C называется *цветом*, а элементы из Φ, т. е. отображения множества Ω в множество цветов C, называется *раскраской* Ω. Две раскраски называются одинаковыми, если они лежат в одной орбите действия G на Φ.

Число различных раскрасок G-пространства Ω можно вычислить по следующей формуле.

Основная формула

$$n = \frac{\sum\limits_{x \in G} q^{\mathrm{cyc}(x)}}{|G|},$$

где n — число различных раскрасок,

q — число цветов, т. е. мощность множества C,

$\mathrm{cyc}(x)$ — число циклов подстановки, индуцируемой действием x на Ω.

Наряду с основной формулой используется упрощенная формула, вытекающая из основной.

Упрощенная формула

$$n = \sum_{i=1}^{m} \frac{q^{\mathrm{cyc}(x_i)}}{|C_G(x_i)|}\,,$$

где $x_1, \ldots, x_m$ — представители всех классов сопряженных элементов в группе G.

Кроме основной и упрощенной формул существует ещё несколько формул, уменьшающих объем вычислений. Все эти формулы получаются из основной формулы с помощью следующих соображений: если подстановки a и b множества Ω сопряжены в $\mathrm{Sym}(\Omega)$, то $\mathrm{cyc}(a) = \mathrm{cyc}(b)$. В частности, если элементы x и y из G сопряжены в G, то $\mathrm{cyc}(x) = \mathrm{cyc}(y)$, что и позволяет сократить вычисления в упрощенной формуле.

Замечание. В решении задач, приведенных ниже, разрешается использовать только основную и упрощенную формулы. Если студент применяет другую формулу, то он должен пояснить её.

9.1. Данный круг разбит на m равных секторов для $m \in \in \{6, 7, 8, 9, 10, 11, 12\}$ (см. рис. 1). Найти число различных раскрасок секторов круга в два цвета, считая раскраски одинаковыми, если одну из них можно получить из другой с помощью вращений круга.

9.2. Найти число различных ожерелий, сделанных из m бусинок двух цветов, для $m \in \{6, 7, 8, 9\}$ (см. рис. 2).

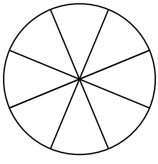


Рис. 1

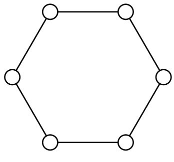


Рис. 2

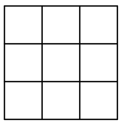


Рис. 3

Замечание. Два ожерелья считаются одинаковыми, если из них одно можно получить из другого с помощью вращения и переворачивания.

9.3. Подсчитать число различных 01-слов длины p^2 или pq, где p и q — различные простые числа, считая два слова одинаковыми, если одно из них можно получить из другого с помощью циклического сдвига.

9.4. Найти число различных раскрасок клеток квадрата 3×3 (см. рис. 3) в два цвета, считая две раскраски одинаковыми, если одну из них можно получить из другой с помощью

а) перестановки строк и столбцов квадрата,

б) поворотов квадрата на угол 90°,

в) транспонирования квадрата,

г) перестановки столбцов и строк квадрата, а также поворотов квадрата на 90°,

д) перестановки строк и столбцов квадрата, а также его транспонирования,

е) перестановки строк квадрата,

ж) четных перестановок строк и столбцов квадрата.

9.5. Найти число различных 01-матриц размеров 2×3, 2×4, 3×4, считая две матрицы одинаковыми, если одну из них можно получить из другой с помощью перестановки строк и столбцов.

$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$ — пример 01-матрицы размера 2×4.

9.6. Подсчитать число различных раскрасок граней куба:

а) в два цвета,

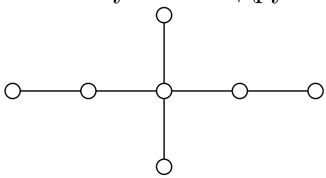
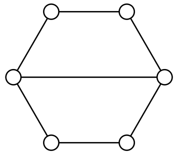
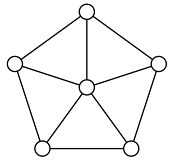
б) точно в два цвета,

в) точно в три цвета,

считая две раскраски одинаковыми, если одну из них можно получить из другой с помощью вращений куба (в пространстве).

9.7. Найти число различных раскрасок граней правильного октаэдра в два цвета, считая две раскраски одинаковыми, если одну из них можно получить из другой с помощью вращений октаэдра (в пространстве).

9.8. Найти число различных раскрасок вершин графа в два цвета, считая две раскраски одинаковыми, если одну из них можно получить из другой с помощью автоморфизма графа:

а)  б)  в) 

9.9. Найти число различных раскрасок ребер графов из задачи 119 в два цвета.

§ 10. Теоремы Силова

10.1. Доказать, что любая силовская p-подгруппа прямого произведения конечных групп A и B является произведением силовских p-подгрупп сомножителей A и B.

10.2. Пусть G — конечная группа, P — силовская p-подгруппа группы G и $H \lhd G$. Доказать, что $H \cap P$ — силовская p-подгруппа группы H и HP/H — силовская p-подгруппа факторгруппы G/H.

10.3. Доказать, что конечная группа G порождается своими силовскими p-подгруппами, взятыми по одному экземпляру для каждого простого делителя p порядка группы G.

10.4. Доказать, что силовская p-подгруппа в конечной группе G единственна тогда и только тогда, когда она нормальная в группе G.

10.5. Доказать, что силовская p-подгруппа единственна тогда и только тогда, когда произведение любых p-элементов в группе есть также p-элемент.

10.6. Доказать, что

а) в конечной абелевой группе силовская p-подгруппа единственна для любого простого делителя p порядка группы,

б) конечная абелева группа есть прямое произведение всех своих силовских подгрупп, в) если конечная группа G имеет единственную силовскую p-подгруппу для каждого простого делителя p порядка G, то G есть прямое произведение своих силовских подгрупп.

10.7. Доказать, что число различных силовских 2-подгрупп в A_5 равно 5.

10.8. Найти число силовских p-подгрупп в A_5 для $p = 3$ и $p = 5$.

10.9. Найти все силовские p-подгруппы ($p = 2, 3$) в группах S_3 и A_4.

10.10. В скольких силовских 2-подгруппах группы S_4 содержатся подстановки

а) $(1\,3\,2\,4)$, б) $(1\,3)$, в) $(1\,2)(3\,4)$?

10.11. Пусть $g = (1\,2\,3\,4\,5)$, $P = \langle g \rangle \leqslant S_5$, $G = S_5$ и $N = N_G(P)$. Показать, что $|N| = 20$ и $N = \langle g,\, a \rangle$, где $a = (2\,3\,5\,4)$.

10.12. Доказать, что любая группа порядка 15, 35, 175, 185, 99, 255 является абелевой.

10.13. Доказать, что любая силовская 2-подгруппа группы S_4 изоморфна группе диэдра D_8 (т. е. порождается двумя инволюциями и имеет порядок 8).

10.14. Доказать, что силовская 2-подгруппа S_5 изоморфна D_8.

10.15. Доказать, что силовская 2-подгруппа S_6 изоморфна $D_8 \times \mathbb{Z}_2$.

10.16. Доказать, что в S_n, $n \leqslant 7$, нет подгрупп порядка 15. Показать, что S_8 содержит подгруппу порядка 15.

10.17. (Аргумент Фраттини.) Пусть H — нормальная подгруппа конечной группы G и P — силовская подгруппа конечной группы H. Доказать, что $G = H \cdot N_G(P)$.

10.18. Пусть P — силовская p-подгруппа конечной группы G и H — подгруппа, содержащая $N_G(P)$. Доказать, что $H = N_G(H)$.

10.19. Если Q — нормальная p-подгруппа конечной группы G, то Q содержится в любой силовской p-подгруппе группы G.

10.20. Пусть

$$P = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Z}_p,\ p \text{ — простое} \right\}.$$

Доказать, что P — силовская p-подгруппа в $SL(2, \mathbb{Z}_p)$.

§ 11. Основная теорема о конечных абелевых группах

11.1. Доказать, что группы $\mathbb{Z}$ и $\mathbb{Q}$ не разлагаются в прямую сумму ненулевых подгрупп.

11.2. Доказать, что конечная циклическая группа является прямой суммой примарных циклических подгрупп.

11.3. Пользуясь основной теоремой о конечных абелевых группах, найти с точностью до изоморфизма все абелевы группы порядков:

а) 2; б) 6; в) 8; г) 12;
д) 16; е) 24; ж) 36; з) 48.

11.4. Говорят, что абелева группа имеет тип $(n_1, n_2, \ldots, n_k)$, если она является прямой суммой циклических групп порядков $n_1, n_2, \ldots, n_k$.

Есть ли в абелевой группе типа (2, 16) подгруппы типа:

а) (2, 8); б) (4, 4); в) (2, 2, 2)?

11.5. Сколько подгрупп

а) порядков 2 и 6 в нециклической абелевой группе порядка 12?

б) порядков 3 и 6 в нециклической абелевой группе порядка 18?

в) порядков 5 и 15 в нециклической абелевой группе порядка 75?

11.6. Сколько элементов

а) порядка 2, 4 и 6 в группе $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3$;

б) порядка 2, 4, и 5 в группе $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5$?

§ 12. Инволютивное исчисление

12.1. Доказать, что S_3 — группа диэдра.

12.2. D_{2n} — абелева группа $\Leftrightarrow$ $n = 2$.

12.3. Доказать:

а) центр бесконечной группы диэдра тривиален;

б) центр группы D_{2n} тривиален $\Leftrightarrow$ $n \equiv 1 \pmod 2$;

в) центр группы D_{2n} имеет порядок 2 $\Leftrightarrow$ $n \neq 2$ и $n \equiv 0 \pmod 2$.

12.4. Группа D_{2n} содержит два перестановочных различных отражения $\Leftrightarrow$ $n \equiv 0 \pmod 2$.

12.5. Группа D_{2n} содержит два перестановочных сопряженных отражения $\Leftrightarrow$ $n \equiv 0 \pmod 4$.

12.6. Доказать, что если два отражения r_1 и r_2 сопряжены в группе диэдра, то для некоторого отражения r выполнено равенство $rr_1r = r_2$.

12.7. Пусть (G, H) — конечная пара Фробениуса с подгруппой H четного порядка. Показать, что ядро Фробениуса $K = \left(G - \bigcup\limits_{x \in G} H^x\right) \cup \{1\}$ является абелевой группой нечетного порядка.

12.8. Пусть $G = \langle a, b, c\rangle$, причем $a^2 = b^2 = c^2 = (ab)^n = (ac)^m = (bc)^n = 1$. Доказать:

а) если $(n, m, k) = (2, 3, 3)$, то $|G| \leqslant 24$;
б) если $(n, m, k) = (2, 3, 4)$, то G конечна;
в) если $(n, m, k) = (2, 3, 5)$, то G конечна;
г) если $(n, m, k) = (2, 2, k)$, то $|G| \leqslant 4k$.

12.9. Показать, что существует бесконечная группа G, для которой

а) $|ab| = 2$, $|ac| = 3$, $|bc| = 6$, $|a| = |b| = |c| = 2$;
б) $|ab| = |a| = |b| = |c|$, $|ac| = |bc| = 4$.

12.10. Пусть любой элемент, лежащий вне подгруппы $H < G$, является инволюцией. Доказать, что справедлив один из двух случаев:

1) любой неединичный элемент из G является инволюцией. В частности, G — абелева группа;
2) H — абелева подгруппа индекса 2 в G.

12.11. Пусть $G = \langle a, b, c\rangle$, причем $a^2 = b^2 = c^2 = (abc)^2 = 1$. Доказать, что все произведения четного числа элементов a, b, c образуют абелеву подгруппу индекса 2 в группе G.

§ 13. Функции длины

Пусть ℓ_i — функция длины на группе G, Gr_i — функция роста G относительно ℓ_i, $i = 1,\ 2$, т. е.

$$\mathrm{Gr}_i(n) = |\{x \in G \mid \ell_i(x) \leqslant n\}|,$$

$d_i = d(G, \ell_i)$ — диаметр G относительно ℓ_i.

Доказать следующие утверждения.

13.1. $\ell_1 + \ell_2$ — функция длины на G.

13.2. $\lambda\ell_i$ — функция длины на G для любого $\lambda > 0$.

13.3. Если $\ell_1(x) \leqslant \ell_2(x)$ для любого $x \in G$, то $\mathrm{Gr}_1(n) \geqslant \mathrm{Gr}_2(n)$ для любого $n \in \mathbb{N}$.

13.4. Если $\ell_1(x) \leqslant \ell_2(x)$ для любого $x \in G$, то $d_1 \leqslant d_2$.

13.5. Пусть ℓ_2 — функция длины относительно порождающего множества $S \subseteq G$, причем $\ell_1(x) \leqslant \ell_2(x)$ для любого $x \in S$. Тогда $\ell_1(x) \leqslant \ell_2(x)$ для любого $x \in G$.

13.6. Пусть ℓ_2 — функция длины относительно конечного порождающего множества $S \subseteq G$ и ℓ_1 — произвольная функция длины. Тогда найдется такое $\lambda > 0$, что $\ell_1(x) \leqslant \lambda\ell_2(x)$ для любого $x \in G$.

13.7. Пусть Ω — метрическое пространство конечного диаметра с метрикой d и $G \leqslant \mathrm{Sym}(\Omega)$. Тогда $\ell(x) = \sup\limits_{\alpha\in\Omega} d(\alpha, \alpha^x)$ является функцией длины на G.

13.8. Найти диаметр группы $\mathbb{Z}_{100}$ относительно порождающего множества S:

а) $S = \{1\}$, б) $S = \{1, 5\}$,
в) $S = \{1, 10\}$, г) $S = \{1, 20\}$.

13.9. Найти минимальный диаметр группы $\mathbb{Z}_{100}$ относительно двухэлементных порождающих множеств.

13.10. Вычислить функцию роста группы $\mathbb{Z}$ относительно порождающих 3 и 5.

13.11. Вычислить послойную функцию роста группы $G = \langle a\rangle \times \langle b\rangle$ относительно порождающего множества $\{a, b\}$, если $|a| = 5$ и $|b| = 10$.

13.12. Найти диаметр группы S_n относительно порождающего множества T:

а) T — множество всех транспозиций,

б) T — множество транспозиций, граф которых образует цепь длины $n-1$.

13.13. Вычислить послойную функцию роста группы S_n, $n = 3, 4, 5$, относительно порождающего множества транспозиций, граф которых образует цепь.

13.14. Построить граф Кэли группы диэдра $D = \langle a, b\rangle$ относительно порождающего множества S:

а) $S = \{a, b\}$, б) $S = \{a, ab\}$.

13.15. Построить граф Кэли группы S_4 относительно порождающего множества транспозиций $T = \{(12), (23), (34)\}$.

13.16. Показать, что граф Кэли группы $\mathbb{Z}_{11}$ относительно порождающего множества $S = \{3, 5\}$ является плоским.

ЧАСТЬ II. **Дополнительные задачи**

§ 14. Семейства множеств

Определение 14.1. Множество всех подмножеств множества M называется *булеаном* и обозначается через 2^M. Любое подмножество булеана 2^M будем называть *семейством подмножеств* из M.

Определение 14.2. Через $\binom{M}{k}$, где $k \in \mathbb{N}$, будем обозначать множество всех k-элементных подмножеств из M.

Задачи

14.1. Доказать, что для любого конечного множества M справедливо равенство

$$|2^M| = 2^{|M|}.$$

14.2. Доказать, что для любого конечного множества M справедливо равенство

$$\left|\binom{M}{k}\right| = \binom{|M|}{k},$$

где $1 \leqslant k \leqslant M$.

Замечание. Через $\binom{m}{k}$ обозначается число $\frac{m!}{k!(m-k)!}$. Это число называется *биномиальным коэффициентом.* Наряду с обозначением $\binom{m}{k}$ часто используется обозначение C_m^k.

Определение 14.3. Семейство $\mathcal{L} \subset 2^M$ называется *покрытием* множества M, если любой элемент из M принадлежит хотя бы одному X из $\mathcal{L}$, т.е.

$$M = \bigcup_{x \in \mathcal{L}} X.$$

Покрытие $\mathcal{L}$ называется *разбиением* множества M, если элементы покрытия $\mathcal{L}$ попарно не пересекаются, т.е. для любых $X, Y \in \mathcal{L}$

$$X \cap Y \neq \varnothing \Rightarrow X = Y.$$

Определение 14.4 (Пространства прямых). Пусть M — непустое множество, элементы которого мы будем в дальнейшем называть *точками* и $\mathcal{L}$ — некоторое семейство подмножеств из M, которые мы будем называть *прямыми*. Множество M вместе с семейством $\mathcal{L}$ мы будем называть *пространством прямых*, если выполнены следующие условия.

1. Любые две точки лежат на единственной прямой.
2. Любая прямая содержит по крайней мере три точки.
3. Точки из M не коллинеарны, т.е. не лежат на одной прямой.

Задачи

14.3. Доказать, что в любом пространстве прямых через любую точку проходят по крайней мере три прямые.

14.4. Доказать, что в любом пространстве прямых найдутся 4 точки такие, что никакие три из них не лежат на одной прямой.

14.5. Описать, с точностью до обозначения точек, все пространства прямых, содержащие не более 10 точек.

Определение 14.5. Пространство прямых будем называть *аффинной плоскостью*, если через любую точку, не лежащую на прямой, проходит единственная прямая, параллельная данной (т.е. не имеющая с ней общих точек).

Пространство прямых будем называть *проективной плоскостью*, если любые две прямые имеют хотя бы одну общую точку.

Задачи

14.6. Доказать, что если некоторая прямая в аффинной плоскости состоит из n точек, то

а) любая другая прямая содержит ровно n точек;

б) аффинная плоскость содержит ровно n^2 точек.

14.7. Доказать, что если некоторая прямая в проективной плоскости содержит n точек, то

а) любая другая прямая содержит ровно n точек;

б) проективная плоскость содержит ровно $n^2 - n + 1$ точку.

§ 15. Отношения

Определение 15.1. Пусть A и B — два множества. *Прямым произведением* множеств A и B называется множество всех упорядоченных пар, в которых первый элемент принадлежит A, а второй — B:

$$A \times B = \{(a, b) \mid \ a \in A \quad \& \quad b \in B\}.$$

Степенью множества A называется его прямое произведение самого на себя:

$$A^n = \underbrace{A \times A \times \ \ldots \times A}_{n} = \{(a_1, \ldots, a_n) \mid \ a_i \in A, \ i = 1, \ldots, n\}.$$

Задачи

15.1. Доказать, что для любых конечных множеств A и B справедливо равенство $|A \times B| = |A| \cdot |B|$.

15.2. Доказать, что для любого конечного множества A и произвольного натурального n справедливо равенство $|A^n| = |A|^n$.

Определение 15.2 (Отношения «между»). Пусть A и B — два непересекающихся множества. Любое подмножество $R \subset A \times B$ называется *отношением между* A и B. Любой элемент из R называется *инцидентностью.* Если $(a, b) \in R$, то мы будем говорить, что элементы a и b *инцидентны.*

Очевидно, любому семейству $\mathcal{L} \subset 2^M$ можно поставить в соответствие отношение R между M и $\mathcal{L}$, определив инцидентность следующим образом: для любых $m \in M$ и $L \in \mathcal{L}$

$$(m, L) \in R \ \Leftrightarrow \ m \in L.$$

Обратно, для любого отношения $R \subset A \times B$ можно построить семейство подмножеств $\mathcal{L}$ из A, определив их следующим образом:

$$(b) = \{a \in A \mid \ (a, b) \in R\}.$$

Если для любых b_1, $b_2 \in B$ выполнено условие

$$(b_1) = (b_2) \Rightarrow b_1 = b_2,$$

т.е. любой элемент из B однозначно определён множеством инцидентных с ним элементов из A, то данное отношение восстанавливается однозначно с точностью до обозначения элементов из B, по системе подмножеств $\mathcal{L} = \{(b) \mid \; b \in B\}$.

Аналогично можно построить семейство $\mathcal{L}^*$ подмножеств из B, полагая

$$(a) = \{b \in B \mid \; (a, b) \in R\}.$$

Семейство $\mathcal{L}^* = \{(a) \mid \; a \in A\}$ будем называть *двойственным* к семейству $\mathcal{L}^* = \{(b) \mid \; b \in B\}$.

Таким образом, для любого семейства подмножеств $\mathcal{L}$ из 2^M можно определить двойственное семейство подмножеств $\mathcal{L}^* \subset 2^{\mathcal{L}}$, в котором элементу $m \in M$ ставят в соответствие множество элементов из $\mathcal{L}$, содержащих m.

Задачи

15.3. Доказать, что пространство прямых является проективной плоскостью тогда и только тогда, когда двойственная система подмножеств образует также пространство прямых.

15.4. Пусть M — множество, элементы которого будем называть точками, и $\mathcal{L}$ — семейство подмножеств из M, которые будем называть блоками. Предположим, что выполнены два условия:

а) любые два блока имеют ровно одну общую точку,

б) любая точка принадлежит ровно 2-м блокам.

Может ли M состоять из 10 точек? Какое число точек может быть в M?

Теорема (двойной подсчёт инцидентностей). *Для любого отношения $R \subset A \times B$ справедливы равенства:*

$$|R| = \sum_{a \in A} |(a)| = \sum_{b \in B} |(b)|.$$

Доказательство. Для каждых $a \in A$ и $b \in B$ положим

$$R_a = \{(a, b) \mid \; (a, b) \in R\} \quad \text{и} \quad R_b = \{(a, b) \mid \; (a, b) \in R\}.$$

Понятно, что $|R_a| = |(a)|$ и $|R_b| = |(b)|$, причём каждое из двух семейств

$$\{R_a \mid \ a \in A\} \quad \text{и} \quad \{R_b \mid \ b \in B\}$$

образует разбиение R. Следовательно,

$$|R| = \sum_{a \in A} |R_a| = \sum_{b \in B} |R_b|,$$

откуда и следуют требуемые равенства. □

Задачи

15.5. Доказать, что число нечётных граней у любого многогранника чётно.

15.6. Сколько вершин у многогранника, в каждой вершине которого сходятся две восьмиугольные и одна треугольная грани?

Определение 15.3 (Отношения «на»). Пусть M — произвольное множество. Любое подмножество $R \subset M \times M$ называется *отношением на* множестве M. В отличие от отношений *между* в случае отношений *на* реже используется термин инцидентность. Чаще используется интерпретация в виде ориентированных графов (орграфов). Элементы из M называются вершинами орграфа, упорядоченные пары $(a, b) \in R$ — рёбрами орграфа, a — началом и b — концом этого ребра.

Аналогом теоремы о двойном подсчёте инцидентностей в случае орграфов служит теорема о двойном подсчёте рёбер орграфа. Для формулировки этой теоремы нам потребуется понятие степени входа вершины и степени выхода.

Для любой вершины a в орграфе $\Gamma = \Gamma(M, R)$ через $\operatorname{indeg}(a)$ будем обозначать число рёбер графа Γ с концом в вершине a, а через $\operatorname{outdeg}(a)$ будем обозначать число рёбер графа Γ с началом в вершине a. Число $\operatorname{indeg}(a)$ будем называть степенью входа вершины a, число $\operatorname{outdeg}(a)$ — степенью выхода.

Теорема (о двойном подсчёте рёбер).

$$|R| = \sum_{a \in M} \operatorname{indeg}(a) = \sum_{a \in M} \operatorname{outdeg}(a).$$

Хотя язык орграфов и является очень наглядным, в некоторых случаях используется другое наглядное представление бинарного отношения R. Это касается случаев, когда рёбер в орграфе очень много. В дальнейшем часто будут возникать два таких отношения: отношение эквивалентности и отношение порядка на множестве. Для определения этих двух отношений нам потребуется ряд дополнительных терминов.

Определение 15.4 (Свойства отношений). Пусть $R \subset \subset M \times M$. Тогда отношение R называется

1) *рефлексивным*, если $\forall\, a \in M \quad (a, a) \in R$,
2) *симметричным*, если $\forall\, a, b \in M \quad (a, b) \in R \Rightarrow (b, a) \in R$,
3) *антисимметричным*, если $\forall\, a, b \in M \quad (a, b) \in R \quad \& \quad \& \quad (b, a) \in R \Rightarrow a = b$,
4) *транзитивным*, если $\forall\, a, b, c \in M \quad (a, b) \in R \quad \& \quad (b, c) \in \in R \Rightarrow (a, c) \in R$.

Определение 15.5 (Эквивалентность). Рефлексивное симметричное транзитивное отношение называется *отношением эквивалентности*. Если R — отношение эквивалентности на множестве M, то обычно вместо $(a, b) \in R$ используется другое обозначение $a \equiv b$ или $a \approx b$ и говорят, что элементы a и b *эквивалентны*.

Множество всех элементов из M, эквивалентных элементу a, называется *классом эквивалентности*, содержащим элемент a. Обозначение:

$$(a) = \{b \in M \mid \ (a, b) \in R\}.$$

Из свойств отношений эквивалентности следует

1) $a \in (a)$.

   В частности, все классы эквивалентности образуют покрытие множества M;
2) $(a) \cap (b) \neq \varnothing \Rightarrow (a) = (b)$.

Таким образом, семейство всех классов — разбиение M. Обратно, если $\mathcal{L}$ — некоторое разбиение множества M, то, полагая $(a, b) \in R \ \Leftrightarrow \ \exists\, L \in \mathcal{L}\colon \ a \in L \quad \& \quad b \in L$, мы получаем отношение эквивалентности R на M. Следовательно, понятие эквивалентности можно рассматривать как некоторую формализацию понятия разбиения.

Множество всех классов эквивалентности R называют *фактормножеством* по эквивалентности R и обозначают через M/R.

Определение 15.6 (Порядок). Рефлексивное антисимметричное транзитивное отношение называется *отношением* (нестрогого) *порядка.* Отношение порядка R называется *линейным порядком*, если выполнено условие *сравнимости*:

$$\forall\, a, b \in M \quad (a, b) \in R \vee (b, a) \in R.$$

Обычно отношение порядка обозначается через $a \leqslant b$ для $(a, b) \in R$ и наглядно представляется в виде более правого или более высокого расположения одного элемента относительно другого.

Задачи

15.7. Для произвольного натурального числа n определим отношение R на множестве целых чисел $\mathbb{Z}$ следующим образом:

$$(a, b) \in R \ \Leftrightarrow \ a - b \text{ делится на } n.$$

а) Доказать, что R — отношение эквивалентности;

б) Найти число классов этой эквивалентности.

Замечание. Для R существует стандартное обозначение. Вместо $(a, b) \in R$ пишут $a \equiv b \pmod n$ и говорят: число a сравнимо по модулю n с числом b.

15.8. Сколькими способами можно линейно упорядочить множество из n элементов?

§ 16. Отображения

Определение 16.1. Пусть A и B — произвольные множества. С формальной точки зрения, отображение f из A в B есть такое подмножество $f \subset A \times B$, для которого справедливы условия

(Fun 1) $\quad (a, b) \in f \quad \& \quad (a, c) \in f \Rightarrow b = c \qquad$ (однозначность)

(Fun 2) $\quad \forall\, a \in A \quad \exists\, b \in B \quad (a, b) \in f \qquad$ (тотальность)

Мы в дальнейшем чаще будем использовать другие, более привычные обозначения

$$f:\ a \to B \ \Leftrightarrow\ f \subset A \times B \quad \text{и выполнены условия Fun1–2;}$$
$$f(a) = b \ \Leftrightarrow\ (a, b) \in f.$$

При этом, если $f(a) = b$, то элемент b будем называть *образом* элемента a, элемент a будем называть *прообразом* элемента b. Множество $\{a \in A \mid\ f(a) = b\}$ будем называть *полным прообразом* элемента b. Часто полный прообраз элемента b обозначают $f^{-1}(b)$.

Для любого $M \subset A$ множество $\{f(a) \mid\ a \in M\}$ называют образом M при отображении f и обозначают $f(M)$. Часто используется другое обозначение $\operatorname{Im} f$ для $f(A)$, которое читается как *образ* f.

Отображение f: $A \to B$ называется
сюръекцией, если $f(A) = B$,
инъекцией, если $f(x) = f(y) \Rightarrow x = y$,
биекцией, если f — сюръекция и инъекция.

Задачи

16.1. Найти число биективных отображений n-элементного множества на себя.

Замечание. Биективное отображение множества на себя обычно называется *подстановкой* множества.

16.2. Пусть отображение f: $\mathbb{R}^2 \to \mathbb{R}^2$ определено следующим образом:

$$f(x, y) = (ax + by, cx + dy),$$

где $a, b, c, d \in \mathbb{R}$. Доказать равносильность следующих условий:

1) f — биекция; 2) f — сюръекция;
3) f — инъекция; 4) $ad \neq bc$.

Понятие «биекция», в частности, используется для формализации выражения «одинаковое строение, с точностью до обозначений», т.е. под биекцией понимается просто переобозначение элементов некоторой структуры. Например, два пространства прямых $(M_1, \mathcal{L}_1)$ и $(M_2, \mathcal{L}_2)$ называют изоморфными, если существует биекция $f\colon\ M_1 \to M_2$, для которой выполнено условие

$$\forall\, A \subset M_1 \quad f(A) \in L_2 \;\Leftrightarrow\; A \in L_1.$$

Таким образом, более точно задачу 14.5 можно переформулировать следующим образом: описать, с точностью до изоморфизма, все пространства прямых, содержащие не более 10 точек.

Пусть $f\colon\ A \to B$ и $g\colon\ B \to C$. С помощью этих двух отображений f и g можно определить новое отображение $h\colon$ $A \to C$, которое называется *произведением* (или композицией) отображений. Это новое отображение h определяется следующим образом:

$$h(x) = g(f(x))$$

для произвольного $x \in A$.

§ 17. Алгебраические структуры

Определение 17.1 (Операция). Пусть M — произвольное множество. Отображение $f\colon\ M \times M \to M$ называется операцией на M, если вместо $f(a, b)$ использовать обозначение $a \circ b$, где $\circ$ — знак операции. Заметим, что переход от языка отображений к языку операций на практике означает подключение навыков работы со стандартными операциями сложения и умножения чисел. Конечно, эти навыки можно применять, если операция обладает свойствами, близкими к знакомым нам свойствам числовых операций. Например, операция $\circ$ называется

- *ассоциативной*, если $(a \circ b) \circ c = a \circ (b \circ c)$ для любых $a, b, c \in M$. Отсюда следует, что результат операции не зависит от расстановки скобок и, следовательно, скобки можно опустить;

- *коммутативной*, если $a \circ b = b \circ a$ для любых $a, b \in M$.

Определение 17.2 (Алгебраический зоопарк). В зависимости от того, какими свойствами обладает операция $\circ$, множество M с определённой на нём операцией $\circ$ имеет своё название. Например, M называется *магмой*, если на операцию не наложено никаких ограничений; M называется *полугруппой*, если операция ассоциативна.

Далее нам потребуются понятия нейтрального и обратного элементов.

Пусть M — произвольная магма. Элемент $e \in M$ называется нейтральным элементом магмы, если для любого $x \in M$ $x \circ e = e \circ x = x$.

Задачи

17.1. Доказать, что любая магма содержит не более одного нейтрального элемента.

В магме $(\mathbb{R}, +)$ нейтральным элементом является 0, а в магме $(\mathbb{R}, \cdot)$ нейтральным элементом является 1. В дальнейшем в любой магме, операция которой обозначена $+$, мы будем нейтральный элемент, если он, конечно, существует, обозначать через 0 и называть *нулевым*, а в магме с операцией умножения $\cdot$ — нейтральный элемент обозначать 1 и называть *единичным*.

Полугруппа, содержащая нейтральный элемент, называется *моноидом*.

17.2. Описать, с точностью до изоморфизма, все 2-элементные магмы, полугруппы и моноиды.

Пусть $(M, \circ)$ — произвольный моноид с нейтральным элементом e. Элемент $y \in M$ называется *обратным* к элементу $x \in M$, если

$$x \circ y = y \circ x = e.$$

Элемент x, для которого существует обратный элемент, называется *обратимым*. Нетрудно показать, что обратный элемент, если он, конечно, существует, единственен. Действительно, пусть y_1 и y_2 — обратные элементы к элементу x. Тогда

$$y_1 = y_1 \circ e = y_1 \circ (x \circ y_2) = (y_1 \circ x) \circ y_1 = e \circ y_2 = y_2.$$

Для обратного к x элемента, в силу его единственности, существует стандартное обозначение x^{-1}. Правда, в моноидах с операцией сложения $+$ для обратных элементов применяется другое обозначение и название. Обратный к x элемент называют *противоположным* и обозначают $-x$.

Определение 17.3 (Морфизмы). С помощью понятия биекции нетрудно уточнить выражение «магмы имеют одинаковое строение, с точностью до обозначения элементов магмы». Действительно, пусть A и B — две магмы, в которых операция обозначена одним и тем же знаком $\circ$. Будем говорить, что магмы A и B *изоморфны* (и писать $A \simeq B$), если существует такая биекция $f\colon A \to B$, что

$$f(x \circ y) = f(x) \circ f(y) \tag{$*$}$$

для любых $x, y \in A$. Само отображение f в этом случае называется *изоморфизмом*.

Конечно, операции в магмах могут иметь и различные обозначения. Например, в магме B операция может быть обозначена через $+$. Тогда условие $(*)$ перепишется в виде $f(x \circ y) = f(x) + f(y)$.

Кроме понятия изоморфизма, в алгебре часто используются ещё три вида отображений. Если роль изоморфизма ясна, то потребности в других отображениях пока не возникает. Несмотря на это обстоятельство, мы сразу дадим определения остальных трёх морфизмов, чтобы далее не возникало путаницы.

1. Гомоморфизм. Пусть A и B — произвольные магмы с операцией $\circ$. Отображение $f\colon A \to B$ называется *гомоморфизмом*, если $f(x \circ y) = f(x) \circ f(y)$. Таким образом, понятие гомоморфизма есть обобщение понятия изоморфизма.

2. Эндоморфизм. Гомоморфизм $f\colon A \to A$ магмы A в себя называется *эндоморфизмом* A.

3. Автоморфизм. Изоморфизм $f\colon A \to A$ магмы A на A называется *автоморфизмом* A.

Определение 17.4 (Группы). Нетрудно привести примеры моноидов, в которых не каждый элемент обратим. Моноид, в котором обратим каждый элемент, называется группой.

Задачи

17.3. Пусть $(G, \cdot)$ — произвольная группа. Доказать, что для любых x, $x_1, \ \ldots, x_n \in G$ справедливы равенства
1) $(x^{-1})^{-1} = x$;
2) $(x_1 \cdot \ \ldots \cdot x_n)^{-1} = x_n^{-1} \cdot \ \ldots \cdot x_1^{-1}$.

17.4. Пусть $(G, \cdot)$ — произвольная группа и $a \in G$. Доказать, что отображения $l\colon\ G \to G$ и $r\colon\ G \to G$, определённые следующим образом:

$$l(x) = ax \quad \text{и} \quad r(x) = xa,$$

являются биекциями.

17.5. Найти все, с точностью до изоморфизма, группы, содержащие не более 4-х элементов.

17.6. Доказать, что множество всех подстановок множества M относительно операции их произведения образует группу.

Замечание. Эта группа обозначается $\mathrm{Sym}(M)$ и называется симметрической группой подстановок множества M.

ЧАСТЬ III. **ПРИЛОЖЕНИЕ**

§ 18. Программа по курсу «Теория групп»

1. Рождение теории групп.
   От гармонии и порядка к понятиям симметрии и группы симметрий. Формализация понятий однородности и правильности. Группы в геометрии. Понятия группы подстановок, группового действия и группового пространства. От геометрии к группам и от групп к геометрии. Два языка, алгебраический и геометрический, и две системы образов в теории групп.
2. Базисные понятия.
   Подстановки и их циклическая структура. Транспозиции. Симметрическая группа и группы подстановок. Подгруппы. Порождающие множества и конечнопорожденные группы. Циклические группы. Граф Кэли группы. Функция роста групп и гипотеза Милнора. Сортировка на неориентированных связных графах и диаметр графа Кэли симметрической группы, порожденной данным множеством транспозиций. (Распределение тем зачетных исследовательских работ студентов.)
3. Теорема Лагранжа.
   Понятие смежного класса и индекса подгруппы. Группы простого порядка. Малая теорема Ферма. Теорема Лагранжа в групповых пространствах. Понятие групповой орбиты и стабилизатора точки. Связь между мощностью орбиты точки и мощностью ее стабилизатора. Применение в комбинаторике орбитно-стабилизаторного свойства.
4. Гомоморфизмы групп.
   Понятие гомоморфизма алгебраических структур. Гомоморфизмы, конгруэнции и факторалгебры. Понятие нормальной подгруппы. Нормальные подгруппы и факторгруппы. Основная теорема о гомоморфизмах. Простые группы. Композиционные ряды и расширения групп.

Классификация конечных простых групп. Классические простые группы.

5. Знакопеременные группы.

   Четные и нечетные подстановки. Разрезание и склеивание циклов. Теория декремента подстановок. Теория инверсий и пузырьковый метод сортировки. Понятие знакопеременной группы и ее простота.

6. Уравнение классов.

   Понятие автоморфизма группы. Внутренние и внешние автоморфизмы группы. Действие группы сопряжением. Классы сопряженных элементов как орбиты действия. Понятие централизатора и нормализатора подмножества элементов в группе. Мощность класса сопряженных элементов. Уравнение классов и его решения. Группы с конечным числом классов сопряженных элементов. Центр группы. Нетривиальность центра конечной p-группы.

7. Лемма Бернсайда.

   Орбиты и неподвижные точки в групповых пространствах. Двойной подсчет инцидентностей в бинарных отношениях. Формула для подсчета числа групповых орбит и ее применение в комбинаторике.

8. Примитивные групповые пространства.

   Блоки и системы импримитивности в групповых пространствах. Импримитивные и примитивные групповые действия. Критерий примитивности в терминах стабилизатора точки. Орбиты стабилизатора и орбиталы. Примитивность группы и связность орбитала. Замыкания в топологии поточечной сходимости и группы автоморфизмов орбиталов.

9. Базисные идеи теории Галуа.

   Расширения полей и расширения Галуа. Связь между решеткой подполей и решеткой подгрупп группы Галуа. Понятие разрешимой группы. Связь между разрешимостью в радикалах алгебраического уравнения и разрешимостью группы Галуа этого уравнения.

§ 19. Экзаменационные вопросы по курсу лекций «ТЕОРИЯ ГРУПП», 3 семестр, 2011–12 учебный год

1. Теория инверсий. Понятие ориентации множества пар. Независимость числа инверсий подстановки от выбора ориентации. Правило нечетности. Четные и нечетные подстановки и их свойства. Инверсии линейного порядка. Связь между числом линейных инверсий и ее длиной.
2. Разрезание и склеивание циклов. Циклическое строение подстановки. Изменение циклической структуры подстановки при умножении ее на транспозицию. Декремент подстановки. Связь между декрементом подстановки и ее длиной.
3. Понятия группы и подгруппы. Симметрическая и знакопеременная группы. Порождающие множества. Циклические группы. Смежные классы подгрупп и теорема Лагранжа.
4. Классы сопряженных элементов. Центр группы. Понятие централизатора элемента. Теорема о мощности класса сопряженных элементов. Уравнение классов.
5. Сопряженные подгруппы. Понятие нормальной подгруппы. Конструкция факторгруппы. Понятия изоморфизма и гомоморфизма. Ядро и образ гомоморфизма, их свойства. Естественный гомоморфизм на факторгруппу. Первая теорема об изоморфизме.
6. Конструкция прямого произведения, его ассоциативность. Координатные подгруппы и их свойства. Теорема о разложении группы в прямое произведение двух подгрупп.
7. Понятие действия группы. Связь между действием группы и ее подстановочным представлением. Понятие точного действия. Примеры: действие сопряжением на элементах и подгруппах, действие на парах точек и на функциях. Понятия орбиты точки и тран-

зитивного действия. Стабилизаторы точек и орбитно-стабилизаторное свойство группы.

8. Действие группы правыми и левыми сдвигами на элементах группы и смежных классах подгрупп. Теорема Кэли о регулярном подстановочном представлении группы. Обобщение теоремы Кэли для действия на смежных классах подгрупп и его следствия для подгрупп небольшого индекса в простых и симметрических группах.
9. Подсчет числа орбит группового пространства. Теорема Коши–Фробениуса (лемма Бернсайда) и ее следствия. Применение к подсчету числа различных раскрасок.
10. Теорема Коши о существовании в группе элемента простого порядка. Понятие силовской p-подгруппы и теорема о существовании силовской p-подгруппы.
11. Понятие p-группы и характеризация конечных p-групп с помощью теоремы Коши. Свойства конечных p-групп: нетривиальность центра, нормализаторное условие, индексы максимальных подгрупп, теоремы о порядках ее подгрупп и строении p-групп небольшого порядка.
12. Теоремы о сопряженности силовских p-подгрупп и об их числе.
13. Абелевы группы и примарное разложение конечных абелевых групп. Строение мультипликативной группы конечного поля.
14. Теорема о разложении абелевой примарной группы в прямую сумму циклических подгрупп. Основная теорема о строении конечных абелевых групп.
15. Группа диэдра. Правило нечетности для двух инволюций. Вращения и отражения в группе диэдра. Свойства группы диэдра. Критерий сопряженности всех отражений.
16. Группы Кокстера. Достаточные условия конечности группы, порожденной тремя инволюциями. Теорема о существовании бесконечных групп, порожденных тремя инволюциями, на порядки произведений которых наложены некоторые ограничения.

17. Метрика и функция длины на группе. Связь между инвариантными метриками и функциями длины. Диаметр метрического пространства и группы относительно функции длины. Длина элемента и функция роста группы. Связь между функциями длины, функциями роста и диаметром группы относительно различных порождающих множеств. Понятия экспоненциального и полиномиального роста группы.
18. Действие группы на метрическом пространстве и понятие девиации подстановки. Верхняя оценка диаметра группы относительно интегральной девиации. Понятие графа Кэли группы и его свойства. Пример графа Кэли симметрической группы 4-й степени.

Литература

1. *Кострикин А.И.* Введение в алгебру. Ч. 1, 2. – М.: Физматлит, 2000.
2. *Винберг Э.Б.* Курс алгебры. – М.: Факториал-пресс, 2001.
3. Сборник задач по алгебре /под ред. А.И. Кострикина. – М.: Физматлит, 2001.

Дополнительная литература

4. *Dixon J., Mortimer B.* Permutation Groups // Graduate Texts in Mathematics. – V. 163. – Berlin: Springer, 1996.
5. *Rotman J.* An Introduction to the Theory of Groups // Graduate Texts in Mathematics. – V. 148. – Berlin: Springer, 1995.

Беляев Виссарион Викторович

ЗАДАЧИ

ПО ТЕОРИИ ГРУПП

Тираж 200 экз.