Оглавление

Предисловие ко второму изданию

В традиционных курсах алгебры, предназначенных для студентов первого курса математичеких факультетов, вводятся такие понятия как алгебраическая система, изоморфизм, подсистема. Далее, разбираются конкретные алгебраические системы: группы, кольца, векторные пространства, в которых эти понятия интерпретируются. Вместе с тем, для доказательства теоремы о существовании корня, приходится определять фактор–кольца, для построения жордановой формы линейного преобразования необходимо определить фактор–пространства. В настоящем учебном пособии, помимо традиционных понятий алгебраическая система, изоморфизм, подсистема, вводятся такие понятия как гомоморфизм, фактор–множество и фактор–система. Затем эти понятия рассматриваются для групп, колец и векторных пространств. Понимая, что вчерашнему школьнику придётся повозиться, чтобы разобраться с этими вещями, тем не менее, мы верим в наше подрастающее поколение и уверены в том, что им доступны и более высокие вершины.

Во втором издании добавлены задачи из задачников И. В. Проскурякова и Д. К. Фаддеева, И. С. Соминского, которые обычно разбираются на практических занятияха. Также добавлены некоторые из задач, предлагавшихся на студенческих олимпиадах в Московском, Казанском и других университетах. Кроме того, в конце каждого параграфа добавлен раздел Мозаика, в котором собраны интересные факты, красивые задачи, и просто красивые вещи из полэзии и литературы, а также нерешенные задачи из алгебры и теории чисел. При этом, как правило, мы не поясняем — является задача простой, сложной или вообще нерешённой.

Символом (П) с соответствующим номером отмечена задача из задачника:

(П) Проскуряков И. В. Сборник задач по линейной алгебре. М.: Наука, 1978.

Символом (Ф.С) отмечена задача из задачника:

(Ф.С.) Фаддеев Д. К., Соминский И. С. Сборник задач по высшей алгебре. М.: Наука, 1977.

Символом (ОК) отмечена задача из сборника:

(ОК) Задачи студенческих олимпиад по математике, посвященных

дню рождения Н. И. Лобачевского. Казанский университет (1999–2019 гг.): учеб.–метод. пособие/ сост. Д. Ф. Абзалилов, И. С. Григорьева, Э. Ю. Лернер. — Казань: Фэн, 2020.

Благодарю Э. Ю. Лернера, подарившего мне эту книгу, а также организовавшего экскурсии в музей Казанского университета.

Обозначения

Введём обозначения, которые будем использовать на протяжении нашего курса. Символом

$$A = \{a_1, a_2, \ldots\}$$

обозначается множество A, состоящее из элементов $a_1, a_2, \ldots$ Запись $a \in A$ означает, что элемент a принадлежит множеству A; запись $a \notin A$ означает, что a не принадлежит множеству A. Если B является подмножеством множества A, то символически это обозначается так: $B \subseteq A$. Пустое множество будем обозначать символом $\varnothing$. Если $A = \{a_1, a_2, \ldots, a_n\}$ — конечное множество, то символом $|A| = n$ обозначается число элементов множества A.

Для числовых множеств будем использовать следующие обозначения:

$$\mathbb{N} = \{1, 2, \ldots\}$$

— *множество натуральных чисел*;

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$$

— *множество целых чисел*;

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N} \right\}$$

— *множество рациональных чисел*; символом $\mathbb{R}$ будем обозначать множество вещественных (действительных) чисел, которое можно представлять как множество точек на вещественной оси;

$$\mathbb{R}_+ = \{r \in \mathbb{R} \mid r > 0\}$$

— множество положительных вещественных чисел;

$$\mathbb{R}_{\geq 0} = \{r \in \mathbb{R} \mid r \geq 0\}$$

— множество неотрицательных вещественных чисел;

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}, i^2 = -1\}$$

— *множество комплекснных чисел.*

Следующая конструкция позволяет строить новые множества. Если $A_1, A_2, \ldots, A_n$ — непустые множества, то их *декартовым произведением* $A_1 \times A_2 \times \ldots \times A_n$ называется множество упорядоченных n–ок:

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i\}.$$

В частности, если $A_1 = A_2 = \ldots = A_n = A$, то декартово произведение $A_1 \times A_2 \times \ldots \times A_n$ называется n–й *декартовой степенью* множества A и обозначается A^n.

Отображение множества A в множество B будем обозначать либо

$$\varphi\colon A \longrightarrow B, \text{ либо } A \xrightarrow{\varphi} B.$$

Если $a \in A$, то образ элемента a при отображении φ обозначается либо $\varphi(a)$, либо $a\varphi$. Если $D \subseteq A$, то символом $\varphi|_D$ обозначается *ограничение φ на подмножество* D, т. е. отображение $\varphi|_D\colon D \longrightarrow B$, определённое равенством $\varphi|_D(d) = \varphi(d)$ при $d \in D$.

Если имеется два отображения

$$\varphi\colon A \longrightarrow B, \quad \psi\colon B \longrightarrow C,$$

то их *композицией* называется отображение $\varphi \circ \psi\colon A \longrightarrow C$, определяемое равенством $a(\varphi \circ \psi) = (a\varphi)\psi$ при $a \in A$. Таким образом, отображение $\varphi\circ\psi$ есть результат последовательного выполнения сначала отображения φ, а затем — отображения ψ. Если использовать функциональную запись, то надо писать $(\varphi \circ \psi)(a) = \psi(\varphi(a))$, т. е. рассматривать действие справа налево, что менее привычно. Поэтому мы будем использовать первую форму записи.

Введение: Истоки алгебры

Истоки алгебры зародились в цивилизациях Вавилона, Древнего Египта и Древней Греции. Именно там стали изучать действия над целыми и рациональными положительными числами. В Древней Греции (III в. н. э) была написана книга “Арифметика” Диофанта, и серия книг под общим названием “Начала” Евклида, в которой, в частности, сформулированы знаменитые задачи на построение при помощи циркуля и линейки: задача о трисекции угла, задача об удвоении куба и др. Задача о трисекции угла состоит в том, чтобы разбить угол на три равных угла. Задача об удвоении куба — в том, чтобы по заданному кубу объема $V = a^3$ построить куб, объема $2V$, т. е. надо найти величину b такую, что $b^3 = 2V = 2a^3$. Следовательно, надо построить отрезок длины $\sqrt[3]{2}$. Отметим, что задачу о бисекции угла (разбиение угла на два равных угла) и задачу о построении величины $\sqrt{2}$ при помощи циркуля и линейки вы решали в школе.

Мы проследим развитие алгебры на примере решения уравнений. Рассмотрим следующее уравнение:

$$a\,x = b. \tag{1}$$

Здесь a и b — некоторые известные числа, а x — неизвестное. Это линейное (первой степени) алгебраическое уравнение от одной неизвестной. Что значит “решить уравнение”? Это значит, найти все его решения или доказать, что решений нет. При этом надо указывать множество, в котором ищется решение, так как может оказаться, что в одном множестве решений не существует, но если его вложить в некоторое большое множество, то в нём могут существовать решения. Под решением уравнения (1) мы понимаем такое число x^0, которое при подстановке в уравнение вместо неизвестной приводит к верному равенству.

При изучении любого уравнения (или системы уравнений) нас интересуют следующие два вопроса: имеет ли данное уравнение решение и, если ответ утвердительный, как найти все множество решений? Из школьного курса алгебры известно, что уравнение (1) разрешимо тогда и только тогда, когда либо a отлично от нуля, либо $a = b = 0$. В первом случае решение единственно и определяется равенством $x = a^{-1}\,b$, а во втором случае решением является любое число.

Более сложным, по сравнению с (1), является уравнение

$$a\,x^2 + b\,x + c = 0, \quad a \neq 0, \tag{2}$$

где опять a, b, c – заданные числа, а x — неизвестное. Это так называемое *квадратное уравнение* от одной неизвестной. Такие уравнения умели решать еще в IX в. на Востоке. В это же время возник и сам термин "алгебра". Решения уравнения (2) определяются по формуле

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4\,a\,c}}{2\,a}. \tag{3}$$

Теперь мы можем пойти дальше и определить алгебраическое уравнение степени n от одной неизвестной:

$$a_0\,x^n + a_1\,x^{n-1} + \ldots + a_{n-1}\,x + a_n = 0, \quad a_0 \neq 0. \tag{4}$$

Что известно про решения таких уравнений? При $n = 3$ известна *формула Кардано*, похожая на формулу (3), которая позволяет найти корни любого уравнения третьей степени. При $n = 4$ существует *метод Феррари*, сводящий решение уравнения 4–й степени к решению уравнения 3–й степени. Формулы для решения уравнений 3–й и 4–й степени были получены итальянскими математиками: С. Ферро (1465–1526), Н. Тарталья (1500–1557), И. Кардано (1501–1576), Л. Феррари (1522–1565) в XVI в. После этого многие математики пытались найти аналогичные формулы для решения общего уравнения 5–й степени. Эти попытки продолжались до тех пор, пока в 1813 г. А. Руффини (1765–1822) (в первом приближении) и в 1827 г. Н. Абель (1802–1829) (независимо и совершенно строго) доказали, что общее уравнение (4) при $n \geq 5$ неразрешимо в радикалах, т. е. не существует формул, выражающих решение через коэффициенты при помощи основных алгебраических операций: сложения, вычитания, умножения, деления, возведения в степень и извлечения корня. Подчеркнем, что речь идет именно об уравнении общего вида, так как легко указать конкретные уравнения сколь угодно высокой степени, разрешимые в радикалах. Например, уравнение

$$x^{100} - 3\,x^{50} + 2 = 0$$

сотой степени легко сводится к квадратному уравнению.

Французский математик Эварист Галуа (1811–1832), занимаясь условиями разрешимости уравнения в радикалах, создал теорию, которая

в настоящее время называется *теорией Галуа*. Эту теорию можно считать началом современной алгебры. Э. Галуа впервые ввел такие понятия, как *группа*, *поле*, *автоморфизм*. Помимо критерия разрешимости уравнения в радикалах, теория Галуа позволяет доказать неразрешимость задачи о трисекции угла, задачи об удвоении куба и ряда других задач, сформулированных еще в Древней Греции.

Интересна судьба Э. Галуа. По нашим меркам у него не было даже высшего образования. При поступлении в Политехническую школу Галуа провалился на экзамене по математике Он запустил тряпку для стирания с доски в голову экзаменатора, посчитав его вопросы слишком тривиальными. В 1829 г. Галуа поступил в Нормальную школу, из которой был отчислен за свои политические убеждения. Затем сидел в тюрьме и в 1832 г. убит на дуэли. За свою жизнь он написал несколько работ, которые представил во французскую Академию наук. К сожалению, некоторые из них были потеряны, другие же не получили признания современников. После этого имя Эвариста Галуа надолго было предано забвению. Все его математические работы попали к Огюсту Шевалье, но тот не смог найти никого, кто согласился бы их издать. Только в 1846 г. Ж. Лиувиль впервые опубликовал их в основанном им математическом журнале.

Математические работы Галуа, посвященные разрешимости уравнения в радикалх, составляют около сорока страниц. Никогда еще труды столь малого объема не доставляли автору такой широкой известности. Через несколько десятков лет после смерти Галуа, немецкий математик Давид Гильберт назвал теорию Галуа “установлением определенного остова понятий”. Сам Галуа так писал о цели своих исследований: “Подчинить вычисления своей воле, сгруппировать математические операции, научиться их классифицировать по степени трудности, а не по внешним признакам – вот задачи математиков будущего так, как я их понимаю, вот путь, по которому я хочу пойти”.

Мы разобрали одно из возможных обобщений уравнения (1), получив при этом уравнение n–й степени от одной неизвестной. Возможно и обобщение в другом направлении. Сохраним условие линейности, но будем рассматривать уравнения, зависящие от нескольких неизвестных. Придём к *системе линейных уравнений.* Систему m линей-

ных уравнений от n неизвестных можно записать в виде

$$\begin{cases} a_{11}\,x_1 + a_{12}\,x_2 + \ldots + a_{1n}\,x_n = b_1, \\ a_{21}\,x_1 + a_{22}\,x_2 + \ldots + a_{2n}\,x_n = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}\,x_1 + a_{m2}\,x_2 + \ldots + a_{mn}\,x_n = b_m, \end{cases}$$

где $a_{i,j}, b_i$ — заданные числа, а x_j — неизвестные. При исследовании системы нас будут интересовать следующие вопросы: разрешима ли система? как описать всё множество решений? *Решением* мы называем упорядоченную n–ку чисел $x^0 = (x_1^0, x_2^0, \ldots, x_n^0)$, которые при подстановке в систему дают верные равенства. Системы такого вида хорошо изучены, и мы научимся отвечать на оба поставленных вопроса.

Если ввести следующие таблицы:

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}, \quad X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix},$$

которые называются *матрицей системы*, *столбцом неизвестных* и *столбцом свободных членов*, то нашу систему можно записать в виде

$$A\,X = B.$$

Сравним эту запись с уравнением (1). Видим, что по форме они очень похожи. Более того, иногда решение системы можно находить по формуле $X = A^{-1}\,B$, где A^{-1} — матрица, обратная к матрице A.

Наконец, если, рассматривая уравнение (1), мы откажемся от условия линейности и допустим наличие нескольких неизвестных, то придем к полиномиальному уравнению или, более общо, к системе полиномиальных уравнений. Наиболее известным таким уравнением является уравнение

$$x^n + y^n = z^n.$$

где x, y, z — неизвестные целые числа. При $n = 2$ все целочисленные решения описаны. Они образуют пифагоровы тройки. В частности,

$$3^2 + 4^2 = 5^2.$$

Оказывается, что при $n > 2$ это уравнение уже не имеет нетривиальных целочисленных решений. Эта теорема называется Великой, или

Последней теоремой Ферма и была сформулирована Пьером Ферма в 1637 г. на полях книги "Арифметика" Диофанта. Ферма записал её с припиской, что найденное им остроумное доказательство этой теоремы слишком длинно, чтобы его можно было поместить на полях книги: "Наоборот, невозможно разложить куб на два куба, биквадрат на два биквадрата и вообще никакую степень, большую квадрата, на две степени с тем же показателем. Я нашёл этому поистине чудесное доказательство, но поля книги слишком узки для него". С тех пор было предпринято много попыток найти элементарное доказательство этой теоремы, которые не увенчались успехом. Полное доказательство (совсем неэлементарное) было найдено в 1995 г. английским математиком Эндрю Уайлсом.

Решения систем полиномиальных уравнений изучаются в курсе алгебраической геометрии, и мы лишь слегка коснемся этой темы, доказав знаменитую теорему Гильберта, которая утверждает, что всякая система полиномиальных уравнений от конечного числа неизвестных равносильна некоторой конечной подсистеме.

Большой вклад в развитие алгебры внесли отечественные математики. Одним из основателей Сибирской алгебраической школы является А. И. Мальцев (1909–1967), много лет работавший в НГУ. Его именем названа лекционная аудитория в старом корпусе университета. Также с Институтом математики и Новосибирским государственным университетом связаны имена А. И. Ширшова (1921–1981), М. И. Каргаполова (1928–1976), Ю. И. Мерзлякова (1940–1995) и многих других математиков, внёсших огромный вклад в развитие алгебры.

Глава 1

ОСНОВНЫЕ ПОНЯТИЯ АЛГЕБРЫ

§ 1. Алгебраические системы

1.1. Алгебраическая операция, алгебраическая система. Множества и отображения на них — вот два основных объекта, к изучению которых сводится любая математическая теория. Пусть задано некоторое непустое множество A.

О п р е д е л е н и е. Функция $f\colon A^n \longrightarrow A$, аргументы которой пробегают множество A, и значения которой также лежат в A называется n-арной *алгебраической операцией*. В частности, при $n = 1$ операция называется *унарной,* при $n = 2$ — *бинарной,* при $n = 3$ — *тернарной* и т. д.

В школьном курсе вы уже встречались с такими операциями, как сложение и умножение. Для их обозначения вы использовали не функциональную запись $f(x, y)$, а писали: $x+y$ и $x\cdot y$. В дальнейшем мы тоже будем использовать подобные обозначения для бинарных операций.

Как следует из определения, всякая алгебраическая операция определена на некотором множестве. Поэтому можно дать такое

О п р е д е л е н и е. *Алгебраической системой* называется непустое множество A с определенными на нем алгебраическими операциями:

$$\mathcal{A} = \langle A;\ f_i\,(i \in I)\rangle,$$

где I — некоторое множество индексов, конечное или бесконечное. Множество A называется *носителем алгебраической системы.*

Чтобы проиллюстрировать это понятие, приведем

П р и м е р ы алгебраических систем:

1) $\mathcal{A}_1 = \langle \mathbb{Z}; +, \cdot \rangle$;

2) $\mathcal{A}_2 = \langle \{\text{действительные числа}\}$; взятие среднего арифметического, умножение на $10\rangle = \langle \mathbb{R}; \frac{a+b}{2}, 10a\rangle$;

3) $\mathcal{A}_3 = \langle \{\text{положительные действительные числа}\}$; взятие среднего геометрического, возведение в 10-ю степень$\rangle = \langle \mathbb{R}_+; \sqrt{ab}, a^{10}\rangle$;

4) $\mathcal{A}_4 = \langle \{\text{точки на плоскости}\}$; взятие центра тяжести треугольника с заданными вершинами$\rangle$;

5) $\mathcal{A}_5 = \langle \{\text{выпуклые замкнутые множества}\}$; операция пересечения$\rangle$.

Как видно уже из этих примеров, алгебраических систем существует достаточно много и изучать все системы довольно проблематично. Определяемое ниже понятие изоморфизма позволяет сократить число изучаемых систем.

1.2. Гомоморфизм и изоморфизм алгебраических систем. Предположим, что заданы два непустых множества A и A'. Отображение $\varphi\colon A \longrightarrow A'$ называется

1) *однозначным*, если одному элементу из A соответствует только один элемент из A';

2) *унивалентным*, если два разных элемента из A переходят в два разных элемента из A';

3) отображением *на*, если для всякого $a' \in A'$ существует $a \in A$ такой, что $a\varphi = a'$.

Рисунок 1.1 иллюстрирует введенные понятия.

Далее, отображение φ удовлетворяющее условиям 1) и 2), называется *взаимнооднозначным*. Отображение, удовлетворяющее условиям 1) – 3) называется *биективным* или *биекцией*. Легко заметить, что для биективного отображения $\varphi\colon A \longrightarrow A'$ существует обратное отображение φ^{-1}, т. е. такое отображение $\varphi^{-1}\colon A' \longrightarrow A$, что композиция $\varphi^{-1}\varphi = 1_{A'}$ и $\varphi\varphi^{-1} = 1_A$, где $1_{A'}$ и 1_A — тождественные отображения на A' и A, соответственно. *Тождественным* мы называем отображение, переводящее каждый элемент в себя.

Отметим, что некоторые авторы называют унивалентное отображение *инъективным* или *инъекцией*, а отображение *на* называют *сюръективным* или *сюръекцией*. В этой терминологии биективное отображение — это отображение инъективное и сюръективное одновременно.

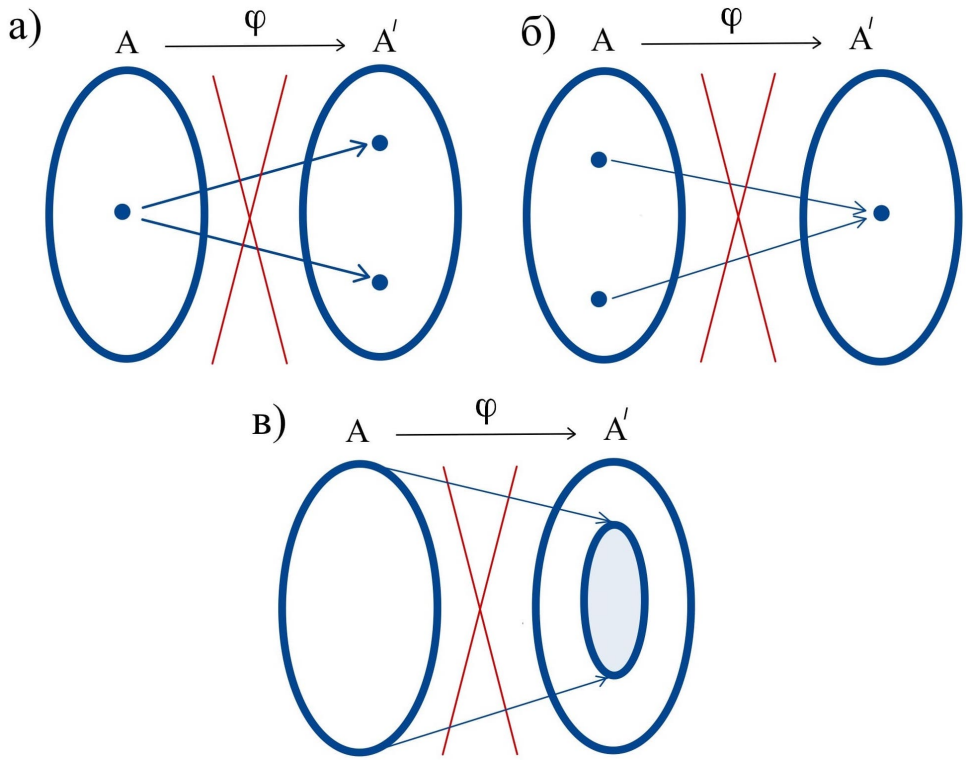

Рис. 1.1: Примеры неоднозначного отображения, неунивалентного отображения и отображения *в*

Пусть теперь заданы две алгебраические системы

$$\mathcal{A} = \langle A;\ f_i\,(i \in I)\rangle, \quad \mathcal{A}' = \langle A';\ f_i'\,(i \in I)\rangle$$

с одинаковыми наборами алгебраических операций (т. е. арность операции f_i равна арности операции f_i' для всех $i \in I$). Такие системы называются *однотипными*. Будем говорить, что отображение

$$\varphi\colon A \longrightarrow A',$$

сохраняет операции, если для всех индексов $i \in I$ и всех наборов $a_1, \ldots, a_{n_i}$ элементов из A справедливо равенство

$$\varphi\,(f_i(a_1, \ldots, a_{n_i})) = f_i'(\varphi(a_1), \ldots, \varphi(a_{n_i})),$$

где n_i — арность операции f_i.

О п р е д е л е н и е. Для однотипных алгебраических систем

$$\mathcal{A} = \langle A;\ f_i\,(i \in I)\rangle, \quad \mathcal{A}' = \langle A';\ f_i'\,(i \in I)\rangle$$

отображение $\varphi\colon A \longrightarrow A'$, сохраняющее операции, называется *гомоморфизмом* системы $\mathcal{A}$ в систему $\mathcal{A}'$. Гомоморфизм, для которого φ является биекцией называется *изоморфным отображением*, или *изоморфизмом* системы $\mathcal{A}$ на систему $\mathcal{A}'$. При этом системы $\mathcal{A}$ и $\mathcal{A}'$ называются *изоморфными*, что символически записывается так: $\mathcal{A} \simeq \mathcal{A}'$.

Отметим, что для гомоморфизмов часто используется следующая терминология. Инъективный гомоморфизм называется *мономорфизмом*, сюрьективный гомоморфизм — *эпиморфизмом*. Очевидно, что гомоморфизм, являющийся одновременно мономорфизмом и эпиморфизмом является изоморфизмом.

П р и м е р гомоморфизма. Пусть $\mathcal{A} = \mathcal{A}' = \langle \mathbb{Z}; + \rangle$. Определим отображение $\varphi\colon \mathbb{Z} \longrightarrow \mathbb{Z}$ правилом $\varphi(a) = 2a$, $a \in \mathbb{Z}$. Очевидно, это отображение однозначно. Чтобы проверить унивалентность, предположим, что для некоторых целых чисел a и b справедливо равенство $\varphi(a) = \varphi(b)$, которое равносильно равенству $2a = 2b$. Отсюда следует, что $a = b$. Следовательно, φ — взаимно однозначно. Также легко заметить, что φ не является отображением *на* (нечетные числа не имеют прообразов). Чтобы проверить, что φ является гомоморфизмом, надо проверить, что равенство $\varphi(a+b) = \varphi(a)+\varphi(b)$ справедливо для любых $a, b \in \mathbb{Z}$. Так как это равенство равносильно $2(a+b) = 2a+2b$, получим нужное утверждение. Таким образом, φ является взаимно однозначным гомоморфизмом, но не является изоморфизмом.

Если в качестве $\mathcal{A}'$ взять алгебраическую систему $\langle 2\mathbb{Z}; + \rangle$, где $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ — множество четных целых чисел, то отображение

$$\varphi\colon \mathbb{Z} \longrightarrow 2\mathbb{Z}, \quad \varphi(a) = 2a, \quad a \in \mathbb{Z},$$

будет изоморфизмом.

У п р а ж н е н и е. Докажите, что если множество A конечно и отображение $\varphi\colon A \longrightarrow A$ взаимно однозначно, то φ является отображением *на*, т. е. биекций.

Заметим, что если отображение $\varphi\colon A \longrightarrow A'$ задает изоморфизм алгебраической системы $\mathcal{A}$ на алгебраическую систему $\mathcal{A}'$, то существует обратное отображение $\varphi^{-1}\colon A' \longrightarrow A$, задающее изоморфизм

алгебраической системы $\mathcal{A}'$ на алгебраическую систему $\mathcal{A}$. Таким образом, отношение изоморфности симметрично, т. е. если $\mathcal{A}$ изоморфно $\mathcal{A}'$, то и $\mathcal{A}'$ изоморфно $\mathcal{A}$

Изоморфные системы с алгебраической точки зрения одинаковы, т. е. все алгебраические свойства системы $\mathcal{A}$ выполняются и в системе $\mathcal{A}'$. Поэтому в алгебре их не различают или рассматривают как точные копии друг друга — подобно тому, как мы не различаем экземпляры одного и того же романа, напечатанные разным шрифтом и на разной бумаге, если интересуемся только содержанием романа. Теперь мы можем дать определение нашего предмета. *Алгебра* — это наука, изучающая алгебраические системы с точностью до изоморфизма.

П р и м е р изоморфных систем. Покажем, что алгебраические системы $\mathcal{A}_2$ и $\mathcal{A}_3$ из приведенного выше примера изоморфны. Рассмотрим отображение

$$\varphi\colon \mathbb{R} \longrightarrow \mathbb{R}_+,$$

определенное правилом $\varphi(a) = 2^a$. Из школьного курса известно, что φ — взаимно однозначно и *на*. Чтобы проверить, что φ сохраняет операции, мы должны проверить следующие два равенства:

$$\varphi\left(\frac{a+b}{2}\right) = \sqrt{\varphi(a)\cdot\varphi(b)},$$

$$\varphi(10a) = (\varphi(a))^{10},$$

справедливость которых следует из свойств показательной функции.

1.3. Подсистема. Если $\mathcal{A} = \langle A;\, f_i\,(i \in I)\rangle$ — алгебраическая система, а B — непустое подмножество в A, то мы можем рассматривать ограничения операций f_i, $i \in I$, на подмножество B:

$$f_i|_B\colon B^{n_i} \longrightarrow A, \quad i \in I,$$

где n_i — арность операции f_i. Если при этом все операции $f_i|_B$, $i \in I$, являются алгебраическими на B, то получим алгебраическую систему $\mathcal{B} = \langle B;\, f_i|_B\,(i \in I)\rangle$, которая называется *подсистемой* алгебраической системы $\mathcal{A}$.

П р и м е р. Подсистемой алгебраической системы $\mathcal{A} = \langle \mathbb{Z}; + \rangle$ является система $\mathcal{B} = \langle 2\mathbb{Z}; + \rangle$, состоящая из четных чисел с операцией сложения. Множество нечетных чисел не образует алгебраическую подсистему.

1.4. Отношение эквивалентности и фактор–множество. Заметим, что знак равенства удовлетворяет следующим условиям:

1) $a = a$;

2) из $a = b$ следует $b = a$;

3) из $a = b$ и $b = c$ следует $a = c$.

Обобщая отношение равенства, будем говорить, что на множестве A задано *бинарное отношение* $\sim$, если для любой пары $(a, b) \in A^2$ мы можем сказать: находится ли элемент a в отношении $\sim$ к элементу b (пишем $a \sim b$), либо — нет (пишем $a \not\sim b$). Бинарное отношение $\sim$ на A определяет подмножество $R_\sim \subseteq A \times A$ следующим образом: пара (a, b) лежит в $R_\sim$ тогда и только тогда, когда $a \sim b$. Нетрудно, проверить, что и любое подмножество $R \subseteq A \times A$ задает некоторое бинарное отношение на A.

Отношения, для которых справедливы те же условия, что и для отношения равенства, имеют специальное название.

О п р е д е л е н и е. Бинарное отношение $\sim$, определенное на A называется *отношением эквивалентности*, если оно удовлетворяет следующим условиям:

1) $a \sim a$ — рефлексивность;

2) из $a \sim b$ следует $b \sim a$ — симметричность;

3) из $a \sim b$ и $b \sim c$ следует $a \sim c$ — транзитивность,

для любых $a, b, c \in A$.

Если на A задано отношение эквивалентности $\sim$, то для каждого $a \in A$ определим множество

$$K_a = \{x \in A \mid x \sim a\},$$

состоящее из элементов эквивалентных a. Заметим, что любые два элемента из K_a эквивалентны. Действительно, если x, y — два элемента из K_a, то $x \sim a$ и $y \sim a$. Из симметричности и транзитивности $\sim$ следует, что $x \sim y$. Поэтому множество K_a называется *классом эквивалентности*

П р и м е р. 1) Мы знаем, что отношение равенства на множестве вещественных чисел $\mathbb{R}$ является отношением эквивалентности. Отношение ‘меньше’: $<$ не является отношением эквивалентности на $\mathbb{R}$ так как $a \not< a$ и, из того, что $a < b$ не следует $b < a$, но из того, что $a < b$ и $b < c$ следует $a < c$. Таким образом, отношение $<$ не является ни рефлексивным, ни симметричным, но является транзитивным.

2) Отношение ‘меньше или равно‘: $\leq$ так же не является отношением эквивалентности на $\mathbb{R}$, но является рефлексивным, транзитивным

и *антисимметричным*. Последнее означает, что если $a \leq b$ и $b \leq a$, то $a = b$.

3) На $\mathbb{Z}$ введем отношение $\equiv$, полагая $a \equiv b$ тогда и только тогда, когда $a - b$ делится на 2 (символически это записывается $(a - b) \vdots 2$ или $2|(a - b)$). Покажем, что это отношение является отношением эквивалентности. Действительно, так как $a - a = 0$ — делится на 2, то $a \equiv a$; если $a - b = 2k$ — делится на 2, то $b - a = 2(-k)$ также делится на 2, т. е. отношение $\equiv$ симметрично. Пусть, наконец, $a \equiv b$ и $b \equiv c$, т. е. $a - b = 2k$ и $b - c = 2l$ для некоторых целых k и l. Тогда $(a - b) + (b - c) = 2(k + l)$ делится на 2, но это и означает, что $a \equiv c$. Следовательно, отношение $\equiv$ является отношением эквивалентности.

Введение отношения эквивалентности на множестве, позволяет разбить это множество в объединение непересекающихся подмножеств и работать уже с этим множеством подмножеств, считая каждое подмножество одним элементом. Приведенная конструкция вам хорошо знакома еще из детского сада. Помните, воспитательница просила вас выбрать среди набора шариков, кубиков, пирамидок фигуры, имеющие один цвет. Отношение “иметь один цвет” является отношением эквивалентности и, разложив фигуры по кучкам, вы разбили все множество фигур на подмножества, состоящие из фигур одного цвета. Думаю,что все вы легко справлялись с этой задачей, а потому легко докажете теорему, о связи отношения эквивалентности с разбиением множества в объединение непересекающихся подмножеств.

Прежде чем сформулировать эту теорему, введем необходимые определения. Пусть A — некоторое множество,

$$M = \{M_i \subseteq A \mid i \in I\}$$

— семейство его подмножеств таких, что $A = \cup_{i \in I} M_i$. Если при этом каждое M_i непусто и пересечение $M_i \cap M_j = \varnothing$ при $i \neq j$, то говорим, что семейство M является *разбиением множества A на классы*, а множество A — независимым объединением семейства M, что будем записывать так:

$$A = \coprod_{i \in I} M_i.$$

Т е о р е м а (о разбиении на классы). *Всякое отношение эквивалентности $\sim$ на множестве A определяет разбиение A на классы.*

Обратно, всякое разбиение множества A на классы, определяет отношение эквивалентности на A.

Доказательство. Рассмотрим множество классов эквивалентности

$$\{K_a \mid a \in A\}.$$

Так как $a \sim a$, то $K_a \neq \varnothing$, т. е. содержит, по крайней мере, элемент a, а потому $A = \cup_{a\in A} K_a$. Пусть теперь K_a и K_b — два класса эквивалентности. Предположим, $a \sim b$ и покажем, что в этом случае, $K_a = K_b$. Вначале докажем включение $K_a \subseteq K_b$. Пусть $x \in K_a$ т. е. $x \sim a$. Так как и $a \sim b$, то по транзитивности, $x \sim b$, а потому $x \in K_b$. Обратное включение $K_a \supseteq K_b$ проверяется аналогично.

Предположим, что для некоторых $a, b \in A$ таких, что $a \not\sim b$ пересечение $K_a \cap K_b \neq \varnothing$, т. е. найдется $x \in K_a \cap K_b$ такой, что $x \sim a$ и $x \sim b$, но из симметричности и транзитивности $\sim$ следует, что $a \sim b$ — противоречие. Таким образом, если два элемента из A эквивалентны, то они лежат в одном классе эквивалентности, если нет, то — в разных. В каждом классе эквивалентности выберем по одному представителю. Обозначая полученное множество представителей A_0, видим, что множество

$$\{K_a \mid a \in A_0\}$$

является искомым разбиением A на классы.

Обратно. Пусть $M = \{M_i \subseteq A \mid i \in I\}$ — некоторое разбиение A на классы. Введем на A отношение $\sim_M$ полагая $a \sim_M b$ тогда и только тогда, когда a и b оба лежат в M_i для некоторого $i \in I$. Проверим, что $\sim_M$ — отношение эквивалентности. Действительно, так как каждый элемент $a \in A$ лежит в некотором M_i, то $a \sim_M a$. Далее, если $a \sim_M b$, то и $b \sim_M a$. Пусть, наконец, $x \sim_M y$ и $y \sim_M z$, но это означает, что элементы x, y, z лежат в одном классе разбиения M, т. е. $x \sim_M z$, а потому отношение $\sim_M$ транзитивно. Теорема доказана.

Множество различных классов K_a разбиения $\{K_a \mid a \in A_0\}$ множества A, будем называть *фактор–множеством* множества A по эквивалентности $\sim$ и обозначать $A/_\sim$. Отображение $A \to A/_\sim$, сопоставляющее всякому элементу $a \in A$ класс K_{a_0} такой, что $a \sim a_0$ называется *естественным отображением.*

Выше мы разбирали пример отношения эквивалентности из детского садика. Учитывая, что вы уже взрослые разберём более сложный

П р и м е р. Пусть A — множество студентов НГУ. Введём несколько отношений на множестве студентов:

$\sim_1$ — учиться в одном вузе;

$\sim_f$ — учиться на одном факультете;

$\sim_c$ — учиться на одном курсе;

$\sim_g$ — учиться в одной группе;

$\sim_0$ — быть полностью одинаковыми.

Нетрудно проверить, что все эти отношения являются отношениями эквивалентности. При этом фактор–множество $A/_{\sim_1} = \{A\}$ состоит из одного класса эквивалентности — самого множества A и $R_{\sim_1} = A \times A$. Фактор–множество $A/_{\sim_f}$ — множество всех факультетов; фактор–множество $A/_{\sim_c}$ — множество шести курсов (считаем, что магистранты тоже относятся к студентам); фактор–множество $A/_{\sim_g}$ — множество всех учебных групп; наконец фактор–множество $A/_{\sim_0} = \{\{a\} \mid a \in A\}$, т. е. каждый студент является классом эквивалентности и $R_{\sim_0} = \{(a, a) \mid a \in A\}$ — диагональ множества $A \times A$. Можно заметить, что деление на факультеты и деление на курсы почти не связаны между собой. С другой стороны, каждый факультет, равно как и каждый курс состоит из набора групп.

На каждом множестве A есть самое слабое отношение эквивалентности $a \sim_1 b$, при котором любые два элемента из A эквивалентны. В этом случае $A = \{K_{a_0}\}$, для некоторого фиксированного $a_0 \in A$, т. е. имеется лишь один класс эквивалентности. С другой стороны, существует и самое сильное отношение эквивалентности $\sim_0$ при котором $a \sim_0 b$ только тогда, когда $a = b$. В этом случае каждый класс эквивалентности состоит из одного элемента: $K_a = \{a\}$, $a \in A$, и мы имеем разбиение $A = \{\{a\} \mid a \in A\}$.

1.5. Фактор–система. Учитывая то, с какой легкостью вы разобрались с понятием фактор–множество, рассмотрим более сложную ситуацию. Предположим, что A является носителем алгебраической системы $\mathcal{A} = \langle A;\ f_i\,(i \in I)\rangle$ и на A определено отношение эквивалентости $\sim$. Говорят, что отношение $\sim$ *стабильно на алгебраической системе* $\mathcal{A}$, если оно стабильно относительно каждой операции f_i, что означает, что для любых двух наборов $a_1, a_2, \ldots, a_{n_i}$ и $b_1, b_2, \ldots, b_{n_i}$ множества A, связанных соотношениями

$$a_1 \sim b_1, \quad a_2 \sim b_2, \ldots, a_{n_i} \sim b_{n_i},$$

где n_i — арность операции f_i, справедлива эквивалентность

$$f_i(a_1, a_2, \ldots, a_{n_i}) \sim f_i(b_1, b_2, \ldots, b_{n_i}).$$

О п р е д е л е н и е. Отношение эквивалентности $\sim$, опредёленное на A, называется *конгруэнцией* на алгебраической системе $\mathcal{A} = \langle A;\ f_i\,(i \in I)\rangle$, если $\sim$ стабильно на $\mathcal{A}$.

Покажем, что в этом случае, фактор–множество $A/_\sim$ можно превратить в алгебраическую систему, котороя является гомоморфным образом системы $\mathcal{A}$. Действительно, элементами фактор–множества $A/_\sim$ являются классы эквивалентности K_a, где a пробегает множество представителей A_0. Определим на них операцию $\bar{f}_i$, $i \in I$, имеющую ту же арность n_i, что и f_i, полагая для любого набора $a_1, a_2, \ldots, a_{n_i}$:

$$\bar{f}_i(K_{a_1}, K_{a_2}, \ldots, K_{a_{n_i}}) = K_{f_i(a_1, a_2, \ldots, a_{n_i})}, \quad i \in I.$$

Т е о р е м а (о фактор–системах). *Множество $A/_\sim$ с операциями $\bar{f}_i$, $i \in I$, является алгебраической системой*

$$\bar{\mathcal{A}} = \langle A/_\sim; \bar{f}_i(i \in I)\rangle.$$

Существует гомоморфизм $\varphi\colon \mathcal{A} \longrightarrow \bar{\mathcal{A}}$, определенный равенством $\varphi(a) = K_{a_0}$, где $a \in A_0$ такой, что $a \sim a_0$ для набора представителей A_0 классов эквивалентностей.

Д о к а з а т е л ь с т в о. Чтобы показать, что $\bar{\mathcal{A}}$ является алгебраической системой, надо показать, что операция $\bar{f}_i$ корректно определена, т. е. не зависит от случайного выбора представителей и является алгебраической операцией. Предположим, что $b_1, b_2, \ldots, b_{n_i}$ — множество элементов из A таких, что

$$b_j \in K_{a_j}, \quad j = 1, 2, \ldots, n_i.$$

Тогда

$$\bar{f}_i(K_{a_1}, K_{a_2}, \ldots, K_{a_{n_i}}) = K_{f_i(b_1, b_2, \ldots, b_{n_i})}.$$

Из того, что $\sim$ стабильно относительно f_i, заключаем, что

$$f_i(b_1, b_2, \ldots, b_{n_i}) \sim f_i(a_1, a_2, \ldots, a_{n_i}),$$

но это и означает, что

$$K_{f_i(b_1, b_2, \ldots, b_{n_i})} = K_{f_i(a_1, a_2, \ldots, a_{n_i})}.$$

Следовательно, $\bar{f}_i$ корректно определена.

Так как $\bar{f}_i\colon (A/_\sim)^{n_i} \longrightarrow A/_\sim$, операция $\bar{f}_i$ является алгебраической.

Покажем, что отображение φ является гомоморфизмом. Для этого рассмотрим операцию f_i и, действуя φ, получим

$$\varphi\left(f_i(a_1, a_2, \ldots, a_{n_i})\right) = K_{f_i(a_1,a_2,\ldots,a_{n_i})}.$$

С другой стороны,

$$\bar{f}_i(\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_{n_i})) = \bar{f}_i(K_{a_1}, K_{a_2}, \ldots, K_{a_{n_i}}).$$

Из определения $\bar{f}_i$ следует, что правые части этих равенств равны, но тогда равны и левые:

$$\varphi\left(f_i(a_1, a_2, \ldots, a_{n_i})\right) = \bar{f}_i(\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_{n_i})),$$

что означает, что φ сохраняет операции, а потому является гомоморфизмом. Теорема доказана.

Алгебраическая система $\bar{\mathcal{A}}$, построенная в теореме, называется *фактор–системой* системы $\mathcal{A}$ по конгруэнции $\sim$. Если надо указать какую конгруэнцию мы рассматриваем, то пишем $\mathcal{A}/_\sim = \bar{\mathcal{A}}$.

П р и м е р. Рассмотрим алгебраическую систему $\mathcal{A} = \langle \mathbb{Z}; + \rangle$ и определим на множестве $\mathbb{Z}$ отношение $\sim$, полагая $a \sim b$ тогда и только тогда, когда $a - b$ делится на 2. Легко убедиться, что $\sim$ является отношением эквивалентности и у нас есть классом эквивалентности K_1 числа 1, состоящее из всех нечётных чисел и класс эквивалентности K_2 числа 2, состоящий из всех чётных чисел. Семейство $\{K_1, K_2\}$ является разбиением множества $\mathbb{Z}$ и фактор–множество $\mathbb{Z}/_\sim$ состоит из двух элементов: K_1 и K_2. Чтобы построить фактор-систему $\mathcal{A}/_\sim$ определим операцию $\bar{+}$ полагая:

$$K_1 \bar{+} K_1 = K_{1+1} = K_2, \quad K_1 \bar{+} K_2 = K_{1+2} = K_3 = K_1,$$

$$K_2 \bar{+} K_1 = K_{2+1} = K_3 = K_1, \quad K_2 \bar{+} K_2 = K_{2+2} = K_4 = K_2.$$

Эти правила сложения хорошо известны. Они означают, что сумма двух нечётных чисел — число чётное, сумма нечётного и четного чисел — число нечётное, сумма двух чётных чисел — число чётное. Мы построили алгебраическую систему $\mathcal{A}/_\sim = \langle \{K_1, K_2\}; \bar{+} \rangle$ состоящую из двух элементов.

В этом параграфе мы ввели основные понятия: алгебраическая система, гомоморфизм, изоморфизм, подсистема, фактор–система. Далее будем изучать конкретные алгебраические систем: группы, кольца, поля, векторные пространства и в них рассматривать подгруппы, подкольца, подполя, подпространства, а также интерпретировать понятие изоморфизма, фактор–группы, фактор–кольца, фактор–пространства.

1.6. *Задачи по алгебраическим системам.*

1) Выяснить, образует ли алгебраическую систему каждое из следующих множеств при указанных операциях над элементами:

а) целые числа относительно операции $a * b = |a - b|$;

б) натуральные числа относительно операции $a * b = \{$множество всех общих кратных a и $b\}$?

2) Пусть A — непустое множество. Символом $\mathcal{P}(A)$ будем обозначать множество всех подмножеств A, символом $\cup$ — объединение подмножеств, символом $\cap$ — пересечение подмножеств.

а) Будет ли множество $\mathcal{P}(A)$ с операциями $\cup$ и $\cap$ алгебраической системой?

б) Каким аксиомам удовлетворяет каждая из операций $\cup$ и $\cap$?

в) Какие аксиомы связывают обе эти операции?

г) Есть ли в $\mathcal{P}(A)$ выделенные элементы?

д) Пусть $B = \{0, 1, 2, 3\}$. Содержит ли $\mathcal{P}(B)$ собственные подсистемы?

е) Какие эндоморфизмы (автоморфизмы) определены на $\mathcal{P}(B)$?

ж) Какие графы можно связать с $\mathcal{P}(B)$?

3) Пусть в алгебраической системе $\langle G; * \rangle$ с одной бинарной операцией $*$ существуют элементы e_l и e_r такие, что

$$e_l * x = x, \quad x * e_r = x \text{ для всех } x \text{ из } G.$$

Докажите, что $e_l = e_r$.

4) Какие из следующих отображений будут гомоморфизмами?

а) $\varphi\colon \langle \mathbb{R}^n; + \rangle \to \langle \mathbb{R}; + \rangle$, $\varphi((x_1, x_2, \ldots, x_n)) = x_1 + x_2$;

б) $\varphi\colon \langle \mathbb{R}; + \rangle \to \langle \mathbb{Z}; + \rangle$, $\varphi(x) = [x]$ — целая часть числа x;

в) $\varphi\colon \langle \mathbb{R}; \cdot \rangle \to \langle \mathbb{Z}; \cdot \rangle$, $\varphi(x) = [x]$ — целая часть числа x

5) Изоморфны ли алгебраические системы

а) $\langle \mathbb{N}; + \rangle$ и $\langle 2\mathbb{N}; + \rangle$?

б) $\langle \mathbb{Z}; + \rangle$ и $\langle \mathbb{R}; + \rangle$?

6) Докажите, что существует лишь два гомоморфизма алгебраической системы $\langle \mathbb{Z}; +, \cdot \rangle$ в себя φ_0 и φ_1, где $\varphi_0(n) = 0$ и $\varphi_1(n) = n$ для любого $n \in \mathbb{Z}$.

7) На множестве $A = \{a, b, c\}$ заданы три операции своими таблицами умножения:

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

,

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

,

$\cdot$	a	b	c
a	a	a	b
b	b	b	a
c	c	c	c

.

Выяснить, какие из алгебраических систем $\langle A; + \rangle$, $\langle A; * \rangle$, $\langle A; \cdot \rangle$ являются изоморфными. (*Отметим, что последняя алгебраическая система — это знаменитый квандл Джойса, который "очень далёк" от первых двух алгебраических систем.*)

1.7. *Задачи для любознательных.*

1) Множество с определенной на нем одной унарной операцией называется *унаром.* Это простейшая (в смысле определения) алгебраическая система. Для всякого натурального числа n на множестве целых чисел определим унарную операцию f_n правилом $f_n(x) = nx$.

а) Докажите, что унар $U_2 = \langle \mathbb{Z}; f_2 \rangle$ изоморфен унару $U_3 = \langle \mathbb{Z}; f_3 \rangle$.

б) Для каких натуральных n и m имеет место изоморфизм $U_n \simeq U_m$?

2) (ОК, 02-3) На множестве A задана бинарная алгебраическая операция $*$ такая, что для любых x, y из A выполняются соотношения

$$(x * y) * y = x \text{ и } y * (y * x) = x.$$

Доказать, что эта операция коммутативна, т. е. $x * y = y * x$ для любых x, y из A.

3) (ОК, 04-1) Решить систему

$$\begin{cases} x^2y^2 - 2x + y^2 = 0, \\ 2x^2 - 4x + 3 + y^3 = 0. \end{cases}$$

4) (ОК, 06-3) В каждой вершине треугольной пирамиды написано число. На каждом ребре написана сумма чисел, стоящих на его

концах. Известно, что сумма чисел на ребрах равна 3 и сумма их квадратов равна 3. Доказать, что сумма их кубов также равна 3.

5) (ОК, 12-2) Судоку–куб. Куб разбит на 9^3 одинаковых кубиков. Можно ли каждому из них приписать число от 1 до 9 так, чтобы в каждой "строке", "столбце" или "столбике" из 9 кубиков каждая цифра встречалась ровно по одному разу.

Можно начать исследования с куба разбитого на 3^3 одинаковых кубиков.

1.8. *Мозаика: детские задачи, сравнение множеств.*

Причем здесь математика? В формулировках некоторых задач трудно понять: причем здесь математика? Одной из таких задач является следующая задача, предложенная Э. Ю. Лернером и, являющаяся вариантом задачи Джона Конвея о двух волшебниках (см. (ОК, стр. 89)).

(ОК, 08-9) Встретились два математика, давно не видевших друг друга. Диалог при встрече:

– Как давно мы не виделись! Я слышал, у тебя большая семья?

– Да, трое детей. Младший — просто ангелочек! Кстати, произведение возрастов моих детей равно количеству лет, сколько мы не виделись.

– Этих сведений мне недостаточно, чтобы однозначно определить возраст твоих детей.

– Мой старший — огненно–рыжий.

– Теперь все ясно.

Сколько лет детям и сколько лет не виделись математики?

Задача о червяке из книги В. И. Арнольда «Задачи для детей от 5 до 15 лет». На книжной полке стоят два тома сочинителя Феди Пупкина, первый и второй (у Арнольда стояли два тома Пушкина, но сочинения Пушкина жалко отдавать на съедение червям). Толщина страниц каждого тома — 2 см, а каждой обложки – 2 мм. Книжный червь сидел на первой странице первого тома и прогрыз (по кратчайшему пути) до последней страницы второго. Какое расстояние он прогрыз?

Понятно, что Вы легко и быстро справитесь с этой задачей, но правильный ответ — 4 миллиметра, возможно, поколеблет веру в Вашу гениальность и заставит задуматься.

Если все же Вы не разуверились в своей гениальности, то вставьте пропущенную букву П В С ... П С В.

Сравнение конечных и бесконечных множеств. Как сравнить два множества, т. е. определить: какое множество "больше", а какое "меньше"? Для конечных множеств ответ очевиден. Надо посчитать число элементов в каждом из них и множество, содержащее больше элементов является большим. Если же число элементов в каждом множестве одинаково, то говорят, что множества равномощны. Как быть если же число элементов в каждом из множеств бесконечно, например, одно множество — множество натуральных чисел, а второе — множество целых чисел. Вы конечно можете сказать, что целых чисел гораздо больше так как это множество содержит все натуральные числа, ноль и все отрицательные числа. Давайте не будем спешить и разберем такой пример. Представьте, что ваша учебная группа пришла в аудиторию на практические занятия по алгебре. Как проверить: чего больше — стульев в аудитории или студентов. Разумеется можно посчитать тех и других, но можно поступить и по другому. Пусть студенты рассядутся и если останутся свободные стулья, то стульев больше, если кому–то не хватит стульев, то больше студентов. Рассадить студентов на стулья означает построить отображение между множеством студентов и множеством стульев. Если вам удалось построить биективное отображение (все студенты сидят и нет свободных стульев), то эти два множества равномощны.

Предположим теперь, что в вашей группе столько же студентов сколько натуральных чисел, т. е. каждому студенту соответствует натуральное число (номер в журнале). Вы опять приходите на занятия по алгебре в аудиторию, в которой стоят стулья, занумерованные натуральными числами. Каждый студент с номером n садится на стул с тем же номером. Все студенты сидят и не осталось свободных стульев. Следовательно, эти два множества равномощны. Предположим теперь, что в вашу группу зачислили еще двоих студентов. Сможете их посадить? Если бы вас было конечное число, то им бы пришлось стоять или сидеть на полу, но вы можете поступить следующим образом: студент с номером n садится на стул с номером $n+2$. Что произойдет? Все студенты будут сидеть, и два стула окажутся свободными. Построенное отображение $\mathbb{N} \longrightarrow \mathbb{N}$, $n \mapsto n+2$, является однозначным и унивалентным, но не является отображением *на*. Именно поэтому нам удалось освободить два стула, на которые и сядут новые студенты. Таким образом, мы построили биекцию между множеством $\mathbb{N} \cup \{a, b\}$, где символы a и b соответствуют новым сту-

дентам и множеством $\mathbb{N}$. Поэтому мы должны считать эти множества равномощными.

Представьте теперь, что преподаватель другой группы заболел и студенты, которых столько же сколько натуральных чисел пришли к вам на занятия. Сможете их посадить? Стульев свободных нет. Вы дружно поднимаетесь и студент с номером n садится на стул с номером $2n$ (сравните с отображением $\varphi\colon \mathbb{Z} \longrightarrow \mathbb{Z}$, $\varphi(a) = 2a$, $a \in \mathbb{Z}$, из первого примера в пункте 1.2), освободившиеся стулья занимают студенты другой группы, а точнее, студент с номером n садится на стул с номером $2n - 1$. В результате студенты обеих групп будут сидеть и все стулья будут заняты. Это означает, что множество ненулевых целых чисел равномощно множеству натуральных чисел, которое, как нетрудно доказать, равномощно множеству всех целых чисел. Более того, можно показать, что и множество рациональных чисел равномощно множеству натуральных чисел. Множество, равномощное множеству натуральных чисел называется *счётным*.

Существуют множества, для нумерации элементов которых натуральных чисел недостаточно. Их называют *несчётными*. К несчётным множествам принадлежат множество всех подмножеств счётного множества, а также множество вещественных чисел на отрезке $[0, 1]$. Для доказательства несчётности, можно использовать *диагональный метод Кантора*.

§ 2. Группы

2.1. Аксиоматика. Некоторые алгебраические системы столь часто встречаются в различных областях математики, что их изучение стало предметом самостоятельных теорий. Именно таково понятие группы — предмет изучения теории групп. Группа — это множество с одной бинарной операцией, подчиняющейся некоторым аксиомам. В теории групп бинарную операцию обычно называют умножением и обозначают точкой (которую почти всегда опускают), реже используют $+$, $\odot$, $*$ и другие символы. Запись операции точкой называют ещё *мультипликативной записью*, а запись плюсом — *аддитивной записью*.

О п р е д е л е н и е. *Группой* называется алгебраическая система $\langle G; \cdot \rangle$ с одной бинарной операцией $\cdot$, для которой выполнены следующие аксиомы.

1. Операция *ассоциативна*, т. е. $(ab)c = a(bc)$ для любых a, b, c из G.

2. Операция гарантирует единицу, т. е. в G существует такой элемент e — он называется *единицей*, что $ae = ea = a$ для любого a из G.

3. Операция гарантирует обратные элементы, т. е для любого a из G существует в G такой элемент x — он называется *обратным* к a, что $ax = xa = e$.

В дальнейшем, если понятно, о какой операции идёт речь, будем обозначать группу $\langle G; \cdot \rangle$ символом G.

Отметим также, что используется и такая терминология. Алгебраическая система с одной бинарной операцией называется *группоидом*. Ассоциативный группоид называется *полугруппой*. Полугруппа с единицей называется *моноидом*. Понятно, что моноид, в котором каждый элемент имеет обратный, будет группой.

Установим некоторые следствия из определения группы.

С л е д с т в и е 1. *В группе существует единственный единичный элемент.*

Действительно, пусть e' и e'' — единичные элементы группы G. Тогда $e'e'' = e''$, с другой стороны, $e'e'' = e'$. Следовательно, $e' = e''$.

С л е д с т в и е 2. *В каждой группе для каждого a существует единственный обратный элемент, который будем обозначать символом a^{-1}.*

Действительно, предположим, что x и y — два обратных элемента к элементу a. Рассмотрим равенство $(xa)y = x(ay)$, справедливое в силу аксиомы ассоциативности. По определению обратного элемента, левая часть этого равенства равна

$$(xa)y = ey = y,$$

аналогичным образом преобразуем правую часть:

$$x(ay) = xe = x.$$

Следовательно, $x = y$.

С л е д с т в и е 3. *Для любых элементов a, b группы G справедливо равенство $(ab)^{-1} = b^{-1}a^{-1}$.*

Действительно,

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e.$$

Благодаря ассоциативности, элемент $(ab)c = a(bc)$ можно записывать как abc. По той же причине однозначно определено произведение n элементов $a_1a_2\dots a_n$ — без указания скобок, но в указанном порядке. Произведение n элементов, равных a, называется n–й *степенью* элемента a и обозначается a^n. Полагаем далее $a^0 = e$ и для $n < 0$ $a^n = (a^{-n})^{-1}$ или $a^n = (a^{-1})^{-n}$, что, как легко видеть, одно и то же.

О п р е д е л е н и е. *Порядком* элемента a группы G называется наименьшее натуральное число n такое, что $a^n = e$ (обозначение: $|a| = n$). Если такого натурального n не существует, то говорим, что a имеет бесконечный порядок и пишем $|a| = \infty$. *Порядком группы* называется число элементов, входящих в неё (обозначение $|G|$). Группу, содержащую бесконечное число элементов называют *бесконечной*.

У п р а ж н е н и е. Если a — произвольный элемент группы, m, n — целые числа, то $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$.

О п р е д е л е н и е. Группа $\langle G; \cdot\rangle$ называется *коммутативной* или *абелевой*, если операция $\cdot$ удовлетворяет следующей аксиоме коммутативности: для любых a, b из G справедливо равенство

$$ab = ba.$$

Операцию в абелевой группе обычно обозначают символом $+$, единичный элемент называют *нулевым элементом* и обозначают символом 0, а обратный к элементу $a \in G$ называют *противоположным* и обозначают символом $-a$.

П р и м е р ы групп:

1) $\langle \mathbb{Z}; +\rangle$ — множество целых чисел относительно операции сложения;

2) $\langle 2\mathbb{Z}; +\rangle$ — множество четных чисел относительно операции сложения;

3) $\langle \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}; \cdot\rangle$ — множество ненулевых рациональных чисел относительно операции умножения;

4) предыдущий пример показывает, что достаточно удалить 0 из множества рациональных чисел, чтобы получить группу относительно умножения. Если мы захотим проделать то же самое с множеством целых чисел, то удалить 0 недостаточно. Надо удалить все элементы, не имеющие обратных. В результате, получим $\langle \mathbb{Z}^* = \{-1, 1\}; \cdot\rangle$ — группа;

5) $\langle \mathbb{R}_+; \cdot\rangle$ — множество положительных вещественных чисел относительно операции умножения;

6) $\langle$\{вращения квадрата\}; композиция вращений$\rangle$.

Нетрудно проверить, что все эти группы являются абелевыми. Примером неабелевой группы является группа симметрий квадрата, т. е. группа преобразований пространства, переводящих квадрат в себя, относительно композиции преобразований.

2.2. Гомоморфизм. Изоморфизм. Пусть $\langle G;\cdot\rangle$ и $\langle G';\odot\rangle$ — две группы. Отображение $\varphi\colon G\longrightarrow G'$ называется *гомоморфизмом* группы G в группу G', если φ сохраняет операцию умножения, т. е. для любых элементов $x,y\in G$ справедливо равенство

$$\varphi(x\cdot y)=\varphi(x)\odot\varphi(y).$$

Гомоморфизм группы в себя называется *эндоморфизмом*. Множество всех эндоморфизмов группы G обозначается $\mathrm{End}(G)$.

П р и м е р. Пусть m — некоторое целое число. Определим отображение $\varphi_m\colon\mathbb{Z}\longrightarrow\mathbb{Z}$ равенством $\varphi_m(a)=ma$, $a\in\mathbb{Z}$. Чтобы показать, что φ_m является гомоморфизмом, найдем

$$\varphi_m(a+b)=m(a+b)=ma+mb,\quad a,b\in\mathbb{Z}.$$

С другой стороны,

$$\varphi_m(a)+\varphi_m(b)=ma+mb,\quad a,b\in\mathbb{Z}.$$

Следовательно, для всех $a,b\in\mathbb{Z}$ справедливо равенство

$$\varphi_m(a+b)=\varphi_m(a)+\varphi_m(b),$$

т. е. φ_m является эндоморфизмом. При $m=0$ этот эндоморфизм переводит все элементы в ноль, при $m\neq 0$ эндоморфизм φ_m является унивалентным, а при $m\in\{-1,1\}$ — биективным. При этом φ_1 — тождественное отображение.

Из того, что гомоморфизм сохраняет операции, выводится

Л е м м а 1. *Всякий гомоморфизм переводит единичный элемент в единичный, а обратный — в обратный.*

Д о к а з а т е л ь с т в о. Рассмотрим гомоморфизм $\langle G;\cdot\rangle\to\langle G';\odot\rangle$. По определению единичного элемента,

$$a\cdot e=e\cdot a=a.$$

Действуя φ, найдём

$$\varphi(a\cdot e)=\varphi(e\cdot a)=\varphi(a).$$

Учитывая, что φ — гомоморфизм, заключаем:

$$\varphi(a) \odot \varphi(e) = \varphi(e) \odot \varphi(a) = \varphi(a),$$

но это и означает, что $\varphi(e)$ — единичный элемент группы G'.

По определению обратного элемента,

$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

Действуя φ, получим

$$\varphi(a \cdot a^{-1}) = \varphi(a^{-1} \cdot a) = \varphi(e).$$

Из того, что φ — гомоморфизм, заключаем

$$\varphi(a) \odot \varphi(a^{-1}) = \varphi(a^{-1}) \odot \varphi(a) = \varphi(e) = e.$$

Следовательно, $\varphi(a^{-1})$ — обратный к $\varphi(a)$. Лемма доказана.

Изоморфизмом группы $\langle G; \cdot \rangle$ на группу $\langle G'; \odot \rangle$ называется биективный гомоморфизм $\varphi\colon G \longrightarrow G'$.

Например, множество $\mathbb{R}$ всех действительных чисел есть группа относительно обычного сложения чисел, множество $\mathbb{R}_+$ положительных действительных чисел — группа относительно обычного умножения чисел, а отображение $\varphi\colon \mathbb{R} \longrightarrow \mathbb{R}_+$, определяемое формулой $\varphi(a) = 2^a$, — изоморфизм $\mathbb{R}$ на $\mathbb{R}_+$ (сравните с примером из пункта 1.2).

Изоморфизм группы на себя называется *автоморфизмом*. Множество всех автоморфизмов группы G обозначается $\mathrm{Aut}(G)$.

2.3. Подгруппа. Подмножество группы G называется её *подгруппой,* если оно замкнуто относительно операции, имеющейся в G, и само является группой относительно этой операции. Если H — подгруппа группы G, то пишем $H \leq G$.

П р и м е р ы подгрупп:

1) группа $\langle \mathbb{Z}; + \rangle$, ее подгруппа $\langle 2\mathbb{Z}; + \rangle$.

2) группа $\langle \mathbb{R}_+; \cdot \rangle$ не является подгруппой группы $\langle \mathbb{R}; + \rangle$, так как имеет другую операцию.

Сформулируем необходимые и достаточные условия того, что некоторое подмножество является подгруппой.

Л е м м а 2. *Подмножество $H \subseteq G$ является подгруппой группы G в том и только том случае, когда выполнены следующие два условия*:

а) *из того, что* $a, b \in H$, *следует, что и* $ab \in H$ (*замкнутость относительно умножения*);

б) *из того, что* $a \in H$, *следует, что и* $a^{-1} \in H$ (*замкнутость относительно взятия обратного*).

Доказательство. Если H является подгруппой, то очевидно, что условия а) и б) выполняются.

Покажем теперь, что если выполнены условия а) и б), то H является подгруппой. Для этого надо проверить аксиомы группы.

1. Аксиома ассоциативности $(ab)c = a(bc)$ выполнена в H, так как она выполняется в G.

3. Аксиома существования обратного элемента следует из условия б).

2. Пусть $a \in H$; по условию б) $a^{-1} \in H$, найдем $aa^{-1} = e$, и по условию а) $e \in H$.

Лемма доказана.

Условия леммы (замкнутость относительно умножения и взятия обратного) символически записывают так:

$$HH \subseteq H, \quad H^{-1} \subseteq H.$$

С каждым гомоморфизма

$$\varphi\colon G \longrightarrow G'$$

группы $\langle G; \cdot \rangle$ в группу $\langle G'; \odot \rangle$, можно связать два множества: *ядро гомоморфизма* φ:

$$\operatorname{Ker}(\varphi) = \{g \in G \mid \varphi(g) = e\} \subseteq G$$

и *образ гомоморфизма* φ:

$$\operatorname{Im}(\varphi) = \{\varphi(g) \mid g \in G\} \subseteq G'.$$

Покажем, что на самом деле, ядро $\operatorname{Ker}(\varphi)$ является подгруппой группы G, а образ $\operatorname{Im}(\varphi)$ — подгруппой группы G'. Более того, $\operatorname{Ker}(\varphi)$ является нормальной подгруппой.

Определение. Подгруппа H группы G называется *нормальной подгруппой* группы G, если для любых $h \in H$ и $g \in G$ справедливо включение $g^{-1}hg \in H$. Символически это можно записать так

$$g^{-1}Hg \subseteq H \quad \text{для любого } g \in G.$$

Элемент $g^{-1}hg$ называется *сопряженным* с элементом h.

Легко заметить, что обратным к отображению *сопряжения*:

$$\widehat{g}\colon H \to H, \quad h \mapsto g^{-1}hg$$

будет отображение

$$\widehat{g^{-1}}\colon H \to H, \quad h \mapsto ghg^{-1}.$$

Следовательно, сопряжение является биекцией, а потому справедливо равенство

$$g^{-1}Hg = H \quad \text{для любого } g \in G.$$

Чтобы подчеркнуть, что H — нормальная подгруппа, пишем $H \trianglelefteq G$.

Л е м м а 3. *Если* $\varphi\colon G \longrightarrow G'$ — *гомоморфизм, то*

1) $\mathrm{Ker}(\varphi)$ — *нормальная подгруппа группы* G;

2) $\mathrm{Im}(\varphi)$ — *подгруппа группы* G'.

Д о к а з а т е л ь с т в о. 1) Пусть $a, b \in \mathrm{Ker}(\varphi)$. Тогда

$$\varphi(ab) = \varphi(a) \odot \varphi(b) = e \odot e = e.$$

Следовательно, $ab \in \mathrm{Ker}(\varphi)$. Далее, ввиду леммы 1, $\varphi(a^{-1}) = \varphi(a)^{-1} = e^{-1} = e$. Следовательно, $a^{-1} \in \mathrm{Ker}(\varphi)$. Ввиду леммы 2, $\mathrm{Ker}(\varphi)$ является подгруппой. Пусть теперь $g \in G$. Найдем

$$\varphi(g^{-1}ag) = \varphi(g^{-1}) \odot \varphi(a) \odot \varphi(g) = \varphi(g)^{-1} \odot e \odot \varphi(g) = e,$$

т. е. $g^{-1}ag \in \mathrm{Ker}(\varphi)$, а потому $\mathrm{Ker}(\varphi)$ — нормальная подгруппа.

2) Выберем два элемента $\varphi(a)$ и $\varphi(b)$ из $\mathrm{Im}(\varphi)$. Тогда $\varphi(a) \odot \varphi(b) = \varphi(ab)$, т. е. их произведение лежит в $\mathrm{Im}(\varphi)$. Далее, $\varphi(a)^{-1} = \varphi(a^{-1})$, т. е. обратный элемент тоже лежит в образе гомоморфизма φ. Опять, ввиду леммы 2, $\mathrm{Im}(\varphi)$ является подгруппой.

Лемма доказана.

2.4. Фактор–группа. В первом параграфе мы ввели понятие фактор–системы. Используя эту конструкцию, определим понятие фактор–группы и установим некоторые её свойства.

Пусть H — подгруппа группы G. Определим отношение $\sim$, которое будем называть *левой смежностью* на множестве G, полагая по определению

$$a \sim b \Leftrightarrow a^{-1}b \in H$$

и, аналогично, отношение *правой смежности*:

$$a \sim b \Leftrightarrow ab^{-1} \in H.$$

У п р а ж н е н и е. Докажите, что отношение левой (правой) смежности является отношением эквивалентности на G для любой подгруппы H.

Как мы помним, каждому элементу $g \in G$ отвечает класс эквивалентности $K_g = \{x \in G \mid x \sim g\}$ — множество элементов, эквивалентных g. Покажем, что этот класс эквивалентности относительно левой смежности равен

$$gH = \{gh \mid h \in H\}.$$

Действительно, если $x \in K_g$, то $x \sim g \Leftrightarrow x^{-1}g = h \in H \Leftrightarrow g^{-1}x = h^{-1} \in H$, а потому $x = gh^{-1} \in gH$. Обратно, если $y = gh \in gH$, то $g^{-1}y = h \in H$ или $y^{-1}g = h^{-1} \in H$, что означает $y \sim g$, т. е. $y \in K_g$. Будем называть класс эквивалентности $K_g = gH$ *левым смежным классом* группы G по подгруппе H.

Аналогично, правое отношение смежности определяет классы эквивалентности, которые совпадают с *правыми смежными классами*:

$$Hg = \{hg \mid h \in H\}, \quad g \in G.$$

Так как соответствие $gH \leftrightarrow Hg^{-1}$, определяемое переходом к обратному элементу: $gh \leftrightarrow h^{-1}g^{-1}$, взаимно однозначно, то мощность множества смежных классов не зависит от того, левые или правые классы рассматриваются. Она называется *индексом* подгруппы H в группе G и обозначается $|G : H|$.

Таким образом, мы имеем два разложения группы G:

$$G = \bigcup_{g \in G} gH = \bigcup_{g \in G} Hg.$$

По теореме о разбиении, в каждом классе эквивалентности можно выбрать по одному представителю и мы представим G в виде независимого объединения смежных классов:

$$G = \coprod_{i \in I} g_i H = \coprod_{i \in I} Hg_i',$$

где мощность множества I равна индексу $|G : H|$.

Теперь мы готовы доказать простое, но важное утверждение теории конечных групп.

Т е о р е м а (Лагранж). *Если H — подгруппа конечной группы G, то*

$$|G| = |H| \cdot |G : H|.$$

Д о к а з а т е л ь с т в о. Каждый класс gH равномощен подгруппе H, что следует из взаимно однозначного соответствия

$$h \leftrightarrow gh, \quad h \in H.$$

Из построенного выше разложения группы G, получаем равенство

$$|G| = |H| \cdot I = |H| \cdot |G : H|.$$

Теорема доказана.

Из этой теоремы вытекает

С л е д с т в и е. *Порядок подгруппы делит порядок группы.*

Таким образом, мы научились по всякой подгруппе H группы G строить фактор–множества, состоящие из левых (правых) смежных классов. Возникает естественный вопрос: можно ли на этом фактор–множестве определить структуру группы? Для этого, как мы знаем из теории алгебраических систем, отношение эквивалентности, разбивающее множество G на классы, должно быть конгруэнцией на группе G, т. е. быть стабильным относительно операции умножения: если $a \sim a'$ и $b \sim b'$, то $ab \sim a'b'$. Для левой эквивалентности это означает, что если $a' = ah_1$ и $b' = bh_2$, то $a'b' = abh_3$ для некоторых $h_1, h_2, h_3 \in H$. Для доказательства преобразуем произведение:

$$a'b' = (ah_1) \cdot (bh_2) = ab(b^{-1}h_1b)h_2.$$

Положим $h_3 = (b^{-1}h_1b)h_2$. Видим, что этот элемент лежит в H, если для любого $b \in G$ справедливо включение

$$b^{-1}Hb \subseteq H,$$

которое, как мы знаем, выполняется для нормальной подгруппы H.

Заметим также, что нормальность означает,

$$g^{-1}Hg = H \Leftrightarrow Hg = gH,$$

т. е. множество левых смежных классов совпадает с множеством правых смежных классов. В дальнейшем множество смежных классов будем обозначать G/H. Как мы видели, отношение смежности для нормальной подгруппы является конгруэнцией и мы можем ввести групповую структуру на классах G/H.

Т е о р е м а. *Пусть H — нормальная подгруппа группы G. Определим произведение смежных классов равенством*

$$aH \cdot bH = abH, \quad a, b \in G.$$

Тогда алгебраическая система $\langle G/H;\cdot\rangle$ *является группой и существует групповой гомоморфизм* $G \to G/H$, *переводящий элемент* g *из* G *в смежный класс, которому принадлежит* g. *Этот гомоморфизм называется естественным гомоморфизмом.*

Доказательство. Корректность определенной операции умножения следует из того, что для нормальной подгруппы отношение смежности является конгруэнцией и утверждение следует из теоремы о фактор–системах (см. § 1). С другой стороны, можно дать и прямое доказательство.

В смежных классах aH и bH выберем другие представители: $a' = ah_1$ и $b' = bh_2$, соответственно, и рассмотрим произведение

$$a'H \cdot b'H = (a' \cdot b')H = (ah_1 \cdot bh_2)H = ab(b^{-1}h_1b)h_2H.$$

Ввиду нормальности H элемент $(b^{-1}h_1b)h_2$ лежит в H, а потому

$$a'H \cdot b'H = abH.$$

Следовательно, операция умножения корректно определена.

Покажем, что операция ассоциативна. Имеем

$$aH{\cdot}(bH{\cdot}cH) = aH{\cdot}(bc)H = a(bc)H = (ab){\cdot}cH = abH{\cdot}cH = (aH{\cdot}bH){\cdot}cH.$$

Далее, единичным элементом является класс $eH = H$, а обратным $(aH)^{-1} = a^{-1}H$. Мы установили, что $\langle G/H;\cdot\rangle$ — группа.

Рассмотрим отображение $\varphi\colon G \to G/H$, переводящее g в класс gH. Покажем, что это отображение является гомоморфизмом. Действительно, выберем $a, b \in G$ и, по определению, найдем $\varphi(ab) = (ab)H$. С другой стороны,

$$\varphi(a)\varphi(b) = aH \cdot bH = ab(b^{-1}Hb) \cdot H$$

и, ввиду нормальности H, получаем $ab(b^{-1}Hb) \cdot H = abH \cdot H = abH$. Следовательно,

$$\varphi(ab) = \varphi(a)\varphi(b),$$

т. е. φ является гомоморфизмом.

Теорема доказана.

2.5. Порождающие множества. Установим следующее утверждение.

Лемма 4. *Пересечение любого семейства подгрупп некоторой группы является подгруппой.*

Д о к а з а т е л ь с т в о. Пусть в группе G задано семейство подгрупп H_α, $\alpha \in J$. Рассмотрим их пересечение $H = \bigcap_{\alpha\in J} H_\alpha$. Покажем, что H — подгруппа группы G. По лемме 2 достаточно доказать, что для H выполнены условия а) и б). Выберем два элемента $a, b \in H$. Тогда $a, b \in H_\alpha$ для любого индекса $\alpha \in J$. Так как H_α — группа, то $ab \in H_\alpha$. Следовательно, $ab \in H$ и условие а) установлено. Рассмотрим элемент $a \in H$. Тогда обратный элемент $a^{-1} \in H_\alpha$ для любого индекса $\alpha \in J$. Так как H_α является группой, то существует обратный элемент $a^{-1} \in H_\alpha$ для всех $\alpha \in J$. Следовательно, $a^{-1} \in H$ и условие б) справедливо. Таким образом, пересечение H является подгруппой. Лемма доказана.

Если M — некоторое подмножество группы G, то пересечение (M) всех подгрупп, содержащих M, называется подгруппой, *порождённой множеством* M, а само M — *порождающим множеством* подгруппы (M):

$$(M) = \bigcap_{H\le G, M\subseteq H} H.$$

В этом случае говорят, что элементы множества M являются *порождающими элементами* подгруппы (M). Подгруппу (M) иногда обозначают также через гр(M).

Т е о р е м а. *Если M — подмножество группы G, то*

$$(M) = \{m_1^{\varepsilon_1} m_2^{\varepsilon_2} \dots m_n^{\varepsilon_n} \mid m_i \in M, \varepsilon_i = \pm 1, n = 1, 2, \dots\}.$$

Д о к а з а т е л ь с т в о. Обозначим правую часть через H. Так как подгруппа (M) содержит все m_i из M, то справедливо включение $(M) \supseteq H$. С другой стороны, очевидно, что $HH \subseteq H$, $H^{-1} \subseteq H$, поэтому ввиду леммы 2 множество H — подгруппа, содержащая M. Отсюда $H \supseteq (M)$ и окончательно $H = (M)$.

Ткорема доказана.

Укажем порождающие множества некоторых встречавшихся ранее групп.

П р и м е р ы.

1) $\mathbb{Z} = (1)$, т. е. группа целых чисел по сложению порождается единицей;

2) $\mathbb{Q} = \left(\frac{1}{n} \mid n = 1, 2, \dots\right)$;

3) $\mathbb{Q}^* = (-1, 2, 3, 5, 7, 11, \dots)$.

Группа, порожденная одним элементом, называется *циклической.* По теореме, циклическая группа, порожденная элементом a состоит

из всевозможных его степеней:

$$(a) = \{a^n \mid n = 0, \pm 1, \pm 2, \ldots\}.$$

Если порядок элемента a бесконечен, то эта группа изоморфна аддитивной группе целых чисел. Если порядок a конечен и равен m, то группа

$$(a) = \{a, a^2, \ldots, a^{m-1}, a^m = e\}$$

состоит из m элементов (имеет порядок m) и называется *циклической группой порядка* m. Циклические группы — простейшие группы. Мы знаем про них фактически всё. В следующем параграфе более подробно познакомимся с конечными циклическими группами. Важность циклических групп объясняется тем, что всякая группа как бы сшита из циклических групп, но связаны между собой они могут быть весьма причудливо. Если мы рассмотрим группы, порожденные двумя элементами, то таких групп существует очень много. Более того, знаменитая теорема Хигмана, Б. Нейман и Х. Нейман утверждает, что всякая счетная группа является подгруппой некоторой двупорождённой группы.

2.6. *Задачи по группам.*

1) (П, 1634) Выяснить, образует ли группу каждое из следующих множеств при указанной операции над элементами:

(1) целые числа относительно сложения;

(2) четные числа относительно сложения;

(3) целые числа, кратные данному натуральному числу n, относительно сложения;

(4) степени данного действительного числа a, $a \neq 0, \pm 1$, с целыми показателями относительно умножения;

(5) неотрицательные целые числа относительно сложения;

(6) нечетные целые числа относительно сложения;

(7) целые числа относительно вычитания;

(8) рациональные числа относительно сложения;

(9) рациональные числа относительно умножения;

(10) рациональные числа, отличные от нуля, относительно умножения;

(11) положительные рациональные числа относительно умножения;

(12) положительные рациональные числа относительно деления;

(13) двоично-рациональные числа, т. е. рациональные числа, знаменатели которых — степени числа 2 с целыми неотрицательными показателями, относительно сложения;

(14) все рациональные числа, знаменатели которых равны произведениям простых чисел из данного множества M (конечного или бесконечного) с целыми неотрицательными показателями (лишь конечное число которых может быть отлично от нуля), относительно сложения;

(15) взаимно однозначные отображения множества $\mathbb{N} = \{1, 2, 3, \ldots\}$ натуральных чисел на себя, каждое из которых перемещает лишь конечное число чисел, если за произведение отображений s и t принято отображение st, которое получается при последовательном выполнении отображений s и t;

(16) преобразования множества M, т. е. взаимно однозначные отображения этого множества на себя, если за произведение преобразований s и t принято преобразование st, которое получается при последовательном выполнении преобразований s и t;

(17) параллельные переносы трехмерного пространства $\mathbb{R}^3$, если за произведение переносов s и t принято их последовательное выполнение;

(18) повороты трехмерного пространства $\mathbb{R}^3$ вокруг данной точки O, если за произведение поворотов s и t принято их последовательное выполнение;

(19) все движения трехмерного пространства $\mathbb{R}^3$, если за произведение движений s и t принято движение st, получающееся при последовательном выполнении движений s и t;

(20) положительные действительные числа, если операция определяется так:

$$a * b = ab;$$

(21) положительные действительные числа, если операция определяется так:

$$a * b = a^2 b^2;$$

(22) действительные многочлены степени n (включая нуль) от неизвестного x относительно сложения;

(23) действительные многочлены степени n от неизвестного x относительно сложения;

(24) действительные многочлены любых степеней (включая нуль) от неизвестного x относительно сложения.

2) (П, 1635) Доказать, что конечное множество G, в котором определена ассоциативная алгебраическая операция и каждое из уравнений

$$ax = b, \quad ya = b$$

для любых a и b из G имеет в G не более одного решения, будет группой.

3) (П, 1636) Доказать, что если $a^2 = e$ для любого элемента a группы G, то эта группа абелева.

4) (П, 1640) Доказать, что группы 1)–4) задачи (П, 1634) изоморфны между собой.

5) (П, 1641) Доказать, что:

а) все бесконечные циклические группы изоморфны между собой;

б) все конечные циклические группы данного порядка n изоморфны между собой.

6) (П, 1642) Доказать, что:

а) группа положительных действительных чисел по умножению изоморфна группе всех действительных чисел по сложению;

б) группа положительных рациональных чисел по умножению не изоморфна группе всех рациональных чисел по сложению.

7) (П, 1645) Доказать, что если e — единица и a — элемент порядка n группы G, то $a^k = e$ тогда и только тогда, когда k делится на n.

8) (П, 1646) Найти все образующие элементы аддитивной группы целых чисел.

9) (П, 1647) Пусть $G = (a)$ — циклическая группа порядка n и $b = a^k$. Доказать, что:

а) элемент b тогда и только тогда будет образующим группы G, когда числа n и k взаимно просты;

б) порядок элемента b равен n/d, где d — наибольший общий делитель n и k;

в) если n и k взаимно просты, то в G существует корень $\sqrt[k]{a}$, т. е. a является k-й степенью некоторого элемента из G и обратно;

г) в группе нечетного порядка все элементы являются квадратами.

10) (П, 1649) Какие из групп задачи (П, 1634) являются подгруппами других из этих групп?

11) (П, 1650) Доказать, что:

а) если H — конечное множество элементов группы G и произведение двух любых элементов из H снова лежит в H, то H будет подгруппой группы G;

б) если все элементы множества H группы G имеют конечные порядки и произведение двух любых элементов из H снова лежит в H, то H будет подгруппой группы G.

12) Докажите, что всякий эндоморфизм группы $\langle \mathbb{Z}; + \rangle$ совпадает с одним из эндоморфизмом $\varphi_m \colon \mathbb{Z} \longrightarrow \mathbb{Z}$, $\varphi_m(a) = ma$, $a \in \mathbb{Z}$, для некоторого целого m.

13) Докажите, что всякий автоморфизм группы $\langle \mathbb{Z}; + \rangle$ либо является тождественным отображением φ_1, либо равен φ_{-1}.

14) Докажите, что если группа $\langle G; + \rangle$ — абелева, то отображение $\varphi_{-1} \colon G \to G$, $\varphi_{-1}(g) = -g$, $g \in G$, является автоморфизмом.

15) Докажите, что для каждого элемента g группы G отображение $\hat{g} \colon G \to G$, определенное правилом $\hat{g}(x) = g^{-1}xg$, $x \in G$, является автоморфизмом.

16) Докажите, что множество автоморфизмов $\mathrm{Aut}(G)$ произвольной группы G образует группу относительно композиции автоморфизмов.

17) Докажите, что группа автоморфизмов $\mathrm{Aut}(\mathbb{Z})$ бесконечной циклической группы $\mathbb{Z}$ изоморфна циклической группе порядка 2.

18) Какие алгебраические системы с одной бинарной операцией можно определить на множестве, состоящем из 3-х элементов? Сколько среди них будет неизоморфных групп?

19) Доказать, что $\mathbb{R} \setminus \{-1\}$ является группой относительно операции $x * y = x + y + xy$.

2.7. *Мозаика: Н. Н. Парфентьев, латинские и магические квадраты.*

Таблицы умножения. В музеи Казанского университета есть стенд, посвященный декану физико–математического факультета профессору Николаю Николаевичу Парфентьеву (1877–1943).

Среди экспонатов можем увидеть страницу рукописи с тремя таблицами (см. рисунок 2.2):

Рис. 2.1: Н. Н. Парфентьев и его диссертация

По-видимому, это рукописная страница статьи: Н. Н. Парфентьев, Несколько слов о магических квадратах: (По поводу ст. г. И. Износкова, появившейся в Изв. Физ.-мат. О–ва в Казани, Т. XX: 1), Изв. КФМО, Т. XX, № 3, 1915. Ниже изображены эти квадраты:

2	7	6
9	5	1
4	3	8

,

красн	желт	син
желт	син	красн
син	красн	желт

,

собака	кошка	волк
кошка	волк	собака
волк	собака	кошка

.

Самый левый квадрат — магический квадрат. Напомним, что *магический квадрат* — это квадрат, заполненный числами так, что сумма чисел по строкам, столбцам и двум диагоналям — одинакова. В нашем случае она равна 15.

Для нас более интересными являются следующие два квадрата. Это латинские квадраты. Под *латинским квадратом* понимается

квадратная $n \times n$–таблица, заполненная n символами так, что в каждой строке и в каждом столбце все символы различны. Для латинских квадратов, изображенных на рисунках, определим два множества:

$$G_1 = \{\text{красн, желт, син}\}, \quad G_2 = \{\text{собака, кошка, волк}\},$$

и на каждом из них бинарную алгебраическую операцию:

$$*_1 \colon G_1 \times G_1, \quad *_2 \colon G_2 \times G_2.$$

Что можно сказать про алгебраические системы $\langle G_1; *_1 \rangle$ и $\langle G_2; *_2 \rangle$?

Отметим, что если на множестве остатков $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ от деления целых чисел на 3 определить операцию сложения сдедующей таблицей

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

,

то полученная алгебраическая система $\langle \mathbb{Z}_3; + \rangle$ будет группой (циклическая группа порядка 3).

Говоря про Казанский университет нельзя не вспомнить про Николая Ивановича Лобачевского (1792–1856), который в течение 40 лет преподавал в Императорском Казанском университете, в том числе 19 лет руководил им в должности ректора. Про связь геометрии Лобачевского с геометрией Евклида читаем в стихотворении Иосифа Бродского “Келломяки”:

Можно кивнуть и признать, что простой урок
лобачевских полозьев ландшафту пошел не впрок,
что Финляндия спит, затаив в груди
нелюбовь к лыжным палкам — теперь, поди,
из аллюминия: лучше, видать, для рук.
Но по ним уже не узнать, как горит бамбук,
не представить пальму, муху цеце, фокстрот,
монолог попугая — вернее, тот
вид параллелей, где голым — поскольку край
света — гулял, как дикарь, Маклай.

М. Цветаева, И. Бродский и Р. М. Рильке. Марина Цветаева (1892–1941) начала сочинять стихи в шесть лет на русском, французском и немецком языках.

Иосиф Бродский (1940–1996) — лауреат Нобелевской премии по литературе 1987 года, поэт–лауреат США 1991–1992 годов. Писать стихи начал с 16 лет, однако впоследствии относил начало своего творчества лишь к 1960 году. Считал М. Цветаеву одним из четырех величайших русских поэтов XX века (Кто три другие поэта?).

Райнер Мария Рильке (1875–1926) — австрийский поэт и переводчик.

Какая связь существует между этими тремя поэтами?

Симметрии магического квадрата. Известно, что группа симметрий квадрата — группа диэдра D_8 порядка 8, порожденная поворотом на 90 градусов относительно центра квадрата и отражением относительно диагонали. Верно ли, что применяя любую симметрию к магическому квадрату, получим магический квадрат?

Латинские подквадраты. Пусть K_n — латинский квадрат порядка $n > 2$. Его латинским подквадратом порядка k, $1 < k < n$, назовем подквадрат, построенный на пересечении k строк и k столбцов матрицы K_n, который сам является латинским. Для каждого $n > 2$ построить латинский квадрат, содержащий латинские подквадраты порядков $1 < k_1 < k_2 < \ldots < k_s < n$ и s — максимальное с этим свойством.

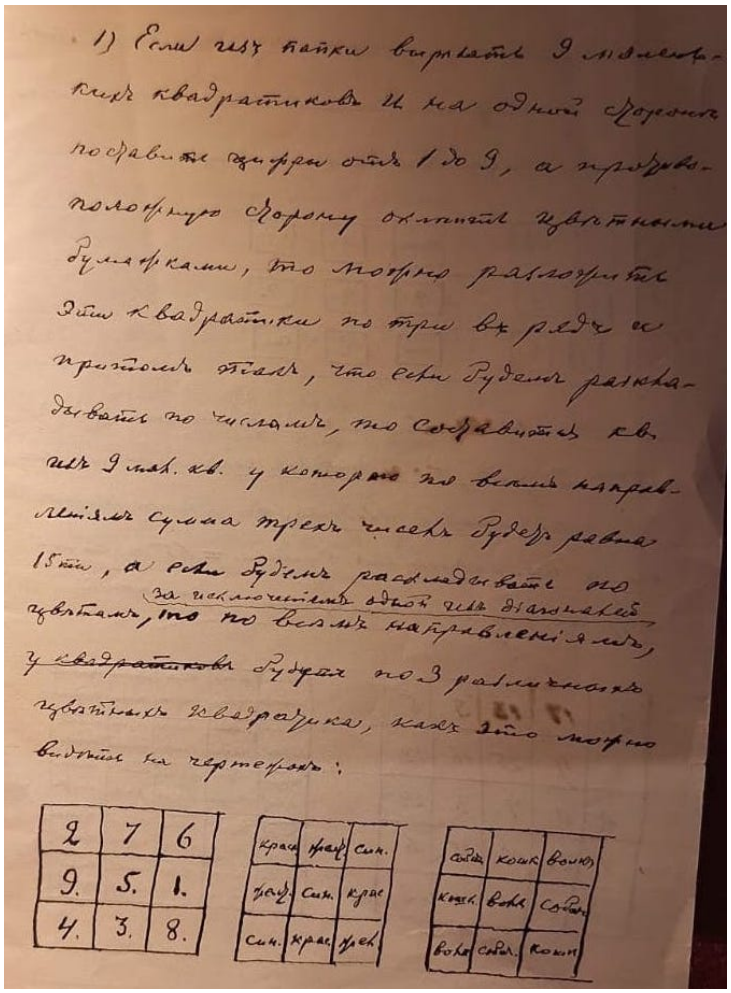

Рис. 2.2: Таблицы, составленные Н. Н. Парфентьевым