С.Н. Тронин

ВВЕДЕНИЕ В ТЕОРИЮ ГРУПП
ЗАДАЧИ И ТЕОРЕМЫ
ЧАСТЬ 1

Казань — 2006

Казанский государственный университет
им. В.И. Ульянова-Ленина

С.Н. Тронин

ВВЕДЕНИЕ В ТЕОРИЮ ГРУПП
ЗАДАЧИ И ТЕОРЕМЫ
ЧАСТЬ 1

УЧЕБНОЕ ПОСОБИЕ

Казань
2006

УДК 512

Печатается по решению
Учебно-методической комиссии
механико-математического факультета КГУ

Научный редактор
доктор физико-математических наук, профессор И.И. Сахаев

Тронин С.Н.

Введение в теорию групп. Задачи и теоремы. Часть 1.: Учебное пособие — Казань: Казанский государственный университет, 2006. 80 с.

Данное учебное пособие предназначено для студентов-математиков младших курсов. Оно может быть использовано для работы на практических занятиях по курсу алгебры как дополнение к уже имеющейся литературе, а также для самостоятельной работы. Материал пособия в целом охватывает все разделы теории групп, содержащиеся в действующей на данный момент программе курса алгебры.

СОДЕРЖАНИЕ

Введение

Данное учебное пособие предназначено для студентов-математиков, изучающих курс алгебры. В этот курс входят в качестве составной части некоторые начальные сведения из теории групп. Основам теории групп и посвящается данная книга. Собственный опыт автора свидетельствует о том, что иногда возникает разрыв между материалом, излагаемым на лекциях, и тем, что приходится делать на практических занятиях. Цель данной книжки — если не ликвидировать, то, по крайней мере, уменьшить этот разрыв. Автор попытался соединить в ней небольшой задачник и некоторое количество теоретических сведений, необходимых для решения задач и для понимания основ теории в целом.

Опишем вкратце содержание. Первая часть содержит четыре раздела. В первом разделе приводится некоторое количество определений и примеров, с которых можно начинать изучение теории групп. Второй раздел посвящен группам подстановок. В нем содержится тот минимум сведений, которые каждый студент-математик должен знать о подстановках. Большая часть материала представлена в виде взаимосвязанных задач. При решении последующих очень часто необходимо использовать результаты предыдущих. Третий раздел содержит задачи о смежных классах группы по подгруппе, о порядках элементов и о классах сопряженных элементов. Задачи в этом разделе преобладают. Четвертый раздел посвящен гомоморфизмам групп, факторгруппам и прямым произведениям групп. Он также состоит в основном из задач, хотя сформулированы и все необходимые для их понимания и решения теоретические результаты.

Остальные пять разделов составляют содержание второй части пособия. Задачи и теоремы пятого раздела связаны с действием групп на множествах. Это фундаментальная конструкция, работающая во многих

областях математики, а не в одной только алгебре. Техника действий используется при доказательстве многих важных теорем. В данный параграф включены задачи, основанные на теоремах Силова, проясняющими строение конечных групп. В шестом разделе рассматриваются линейные действия и самые простейшие понятия теории линейных представлений групп. То обстоятельство, что мы сознательно ограничились именно простейшими понятиями, существенно повлияло на тематику задач этого раздела. Седьмой раздел содержит некоторые теоремы и задачи о группах вращений в двумерном и трехмерном евклидовом пространствах, и совсем немного — о конечных подгруппах групп вращений. В конечном счете речь идет об математических основах понятия симметрии. Восьмой раздел посвящен кватернионам — четырехмерному обобщению поля комплексных чисел. На первый взгляд, эта тема не относится прямо к теории групп. Но, во-первых, она интерсна сама по себе, и студенту-математику будет полезен тот минимум сведений, который приведен в данном разделе. Во-вторых, кватернионы существеннейшим образом используются при доказательстве основных теорем следующего, девятого раздела, где выясняется строение специальной унитарной группы $SU(2)$ и специальной ортогональной группы $SO(3)$ — группы вращений в трехмерном евклидовом пространстве. В отличие от некоторых других учебников (например, [3]), где эти же результаты доказываются с использованием ссылок на общие теоремы линейной алгебры, мы приводим прямое доказательство, где ссылки на линейную алгебру сведены к минимуму, а известный факт о представлении каждого поворота в виде суперпозиции трех последовательных вращений вокруг осей OX, OZ и OX (“углы Эйлера”) выводится как следствие.

Данное пособие охватывает весь материал теории групп, включенный в ныне действующую университетскую программу. Оно, разумеется, не может заменить подробных учебников, и не является альтернативой задачнику [4], не говоря уже о специализированном задачнике [5]. Автор надеется только, что его книга хотя бы в некоторых отношениях может служить им дополнением.

1. Определения, обозначения, примеры

Полугруппа P есть множество вместе с заданной на нем *бинарной операцией*, то есть отображением

$$P \times P \longrightarrow P \quad , \quad (x, y) \mapsto xy,$$

(результат применения которого часто называется “умножением"), причем должно быть выполнено следующее тождество *ассоциативности*: для любых $x, y, z \in P$ имеет место равенство $(xy)z = x(yz)$. Полугруппа называется *коммутативной*, если для всех $x, y \in P$ имеет место равенство $xy = yx$. Элемент $e \in P$ называется *нейтральным элементом* полугруппы, если для любого $x \in P$ имеют место равенства $xe = ex = x$. Нейтральный элемент часто называют *единицей полугруппы* и используют для него соответствующее обозначение: $e = 1$. Полугруппа с единицей называется также *моноидом*.

Убедимся, что в полугруппе может быть не более одного нейтрального элемента. Допустим, что их два. Например, e_1 и e_2. Тогда элемент e_1e_2 должен быть равным e_2, так как e_1 нейтральный элемент. Но тот же e_1e_2 должен быть равным и e_1, так как e_2 тоже нейтральный элемент. Следовательно, $e_1 = e_2$.

Результат бинарной операции $P \times P \longrightarrow P$, вообще говоря, можно обозначать самым произвольным образом. Запись в виде $(x, y) \mapsto xy$ называют *мультипликативной*. Кроме нее, часто используется так называемая *аддитивная запись* $(x, y) \mapsto x + y$ (операция “сложения"), для которой тождество ассоциативности выглядит так:

$$(x + y) + z = x + (y + z),$$

а нейтральный элемент называется *нулем*, и обозначается соответственно как 0. Чаще всего аддитивные обозначения используются для коммутативных полугрупп, то есть когда $x + y = y + x$. Далее в тексте многие определения и факты формулируются только в мультипликативной записи. Подразумевается, что в случае необходимости читатель сможет сам перейти к другой форме обозначений.

Вот некотороые примеры полугрупп.

Пример 1.1. $\mathbf{N}$ — множество всех неотрицательных целых чисел с бинарной операцией сложения. Это коммутативная полугруппа. Нейтральный элемент — нуль.

Пример 1.2. $\mathbf{N}_+$ — множество положительных целых чисел с операцией умножения. Это также коммутативная полугруппа, но нейтральный элемент в ней — единица.

Пример 1.3. Рассмотрим любое множество X, и пусть P_X есть множество всех отображений из X в X. Определим на P_X бинарную операцию как взятие суперпозиции отображений. Точнее, если $f_1, f_2 \in P_X$, то результат умножения $f_1 f_2$ есть суперпозиция отображений $X \xrightarrow{f_2} X \xrightarrow{f_1} X$. Так как суперпозиция отображений ассоциативна, то P_X превращается в полугруппу, единицей которой является тождественное отображение 1_X. Заметим, что при $|X| \geq 2$ полугруппа P_X не является коммутативной.

Пример 1.4. Свободная ассоциативная полугруппа FP_X с базисом X определяется как множество всевозможных конечных последовательностей вида $(x_1, x_2, \ldots, x_n)$, $x_i \in X$, $1 \leq i \leq n$, $n \geq 0$. "Умножение"двух таких последовательностей $a = (x_1, x_2, \ldots, x_n)$ и $b = (y_1, y_2, \ldots, y_m)$ есть приписывание их друг к другу:

$$ab = (x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m).$$

Ясно, что эта операция ассоциативна. Роль нейтрального элемента (единицы) играет вводимая формально последовательность нулевой длины, приписывание которой слева или справа к любой другой ничего не меняет. Более традиционная форма записи: $(x_1, x_2, \ldots, x_n) = x_1 x_2 \ldots x_n$. Это можно назвать строкой, или словом в алфавите X. Полугруппы вида FP_X играют большую роль в теории кодирования. Как и в примере 3, при $|X| \geq 2$ полугруппа FP_X не является коммутативной.

Пример 1.5. Пусть P — произвольная полугруппа. Рассмотрим множество $\mathbf{P}$, состоящее из всех непустых подмножеств множества P, и определим на нем бинарную операцию умножения следующим образом. Пусть A и B — элементы множества $\mathbf{P}$. Это означает, что $A \subseteq P$ и $B \subseteq P$. Положим по определению

$$AB = \{\ ab \mid a \in A, b \in B\ \} \tag{1}$$

Покажем, что эта операция ассоциативна, т.е. если $C \subseteq P$, то $(AB)C = A(BC)$. Так как речь идет о множествах, необходимо установить включения $(AB)C \subseteq A(BC)$, $A(BC) \subseteq (AB)C$. Пусть $x \in (AB)C$. Это значит, что $x = yc$, где $y \in AB$, $c \in C$. $y \in AB$ означает, что $y = ab$, где $a \in A$, $b \in B$. Тогда $x = (ab)c = a(bc)$ по свойству ассоциативности. Иными словами, $x = az$, где $z = bc \in BC$. Следовательно, по определению, $x \in A(BC)$. Обратное включение устанавливается аналогичным рассуждением. Итак, $\mathbf{P}$ вместе с операцией (1) является полугруппой. Условимся о следующем. Будем отождествлять элементы из P и соответствующие одноэлементные множества. Если, например, $a \in P$, то вместо $\{a\}$, будем писать просто a, и вместо, например, $\{a\}B$ будем писать $aB = \{ab|b \in B\}$, и точно так же в других подобных случаях. Таким образом, умножение в P становится частным случаем умножения (1) в $\mathbf{P}$. Если в полугруппе P есть нейтральный элемент e, то этот же элемент (или одноэлементное множество $\{e\}$) будет нейтральным элементом в $\mathbf{P}$. В самом деле, для каждого $A \subseteq P$ множества $eA = \{ea|a \in A\} = \{a|a \in A\}$ и $Ae = \{ae|a \in A\} = \{a|a \in A\}$ совпадают с A. Если полугруппа P коммутативна, то коммутативна и $\mathbf{P}$. В самом деле, если $ab = ba$ для любых a и b, то $AB = \{ab|a \in A, b \in B\} = \{ba|a \in A, b \in B\} = BA$.

Этому примеру уделено так много места потому, что умножение подмножеств и свойство его ассоциатиности (а иногда и коммутативности) будет использоваться в дальнйшем очень часто. Заметим еще, что если операция в P записывается аддитивно, то вместо (1) надо использовать следующее определение:

$$A + B = \{\ a + b \mid a \in A, b \in B\ \} \tag{2}$$

Нейтральным элементом в $\mathbf{P}$ в этом случае является нуль полугруппы P (если он есть).

Группой называется полугруппа G с нейтральным элементом e (который чаще всего будет называться *единицей группы*), в которой для каждого $x \in G$ существует такой элемент $y \in G$, что $xy = yx = e$. Элемент y называется *обратным* к элементу x, и обозначается x^{-1}.

Каждая группа является полугруппой с нейтральным элементом. Обратное неверно. Так, ни одна из полугрупп в примерах 1 – 4 группой заведомо не является. В примере 5 ситуация более сложная, но и в нем

все множество $\mathbf{P}$ группой, вообще говоря, не будет. Однако некоторые подмножества $\mathbf{P}$ могут быть группами, если сама полугруппа P является группой. Эти случаи разобраны далее в разделе 4.

Соберем все свойства из определения группы вместе. Итак, должна быть определена бинарная операция (умножение):

$$G \times G \longrightarrow G, \quad (g_1, g_2) \mapsto g_1 g_2,$$

такая, что выполняются следующие свойства:

1) (асоциативность) $(g_1 g_2) g_3 = g_1 (g_2 g_3)$ для любых $g_1, g_2, g_3 \in G$;

2) существует $e \in G$, такой, что для всех $g \in G$ имеют место равенства: $ge = eg = e$;

3) для каждого $x \in G$ найдется $y \in G$ такой, что $xy = yx = e$.

Покажем, что элемент y из свойства 3) определяется однозначно. Допустим, что для данного x нашлось два обратных элемента y_1 и y_2. Тогда $(y_1 x) y_2 = e y_2 = y_2$. Но, с другой стороны, $(y_1 x) y_2 = y_1 (x y_2) = y_1 e = y_1$. Итак, $y_1 = y_2$. Так как обратный к $g \in G$ элемент определяется однозначно, его обозначают как g^{-1}. Свойство единственности g^{-1} используется при доказательстве некоторых важных соотношений. Покажем, например, что в любой группе G для всех $x, y \in G$ имеет место равенство:

$$(xy)^{-1} = y^{-1} x^{-1}$$

Для этого достаточно проверить, что $(xy)(y^{-1}x^{-1}) = (y^{-1}x^{-1})(xy) = e$, что не должно вызывать затруднений. Отсюда следует, что элемент $y^{-1}x^{-1}$ обладает в точности теми же самыми свойствами, которые характеризуют $(xy)^{-1}$. Ввиду единственности обратного элемента заключаем, что $(xy)^{-1} = y^{-1}x^{-1}$. Индукцией нетрудно показать, что

$$(x_1 x_2 \dots x_n)^{-1} = x_n^{-1} \dots x_2^{-1} x_1^{-1}$$

для всех n.

1.1. Докажите, что если G — любая группа, $x \in G$, и $x^n = e$, то $x^{-1} = x^{n-1}$. Верно и обратное: из $x^{-1} = x^{n-1}$ следует $x^n = e$. Докажите также более общий факт: если $1 \leq k \leq n-1$ и $x^n = 1$, то $x^{-k} = x^{n-k}$.

В частности, свойство $x = x^{-1}$ равносильно тому, что $x^2 = e$.

Наименьшее целое положительное n, для которого $x^n = e$, называется *порядком* элемента x. Свойства порядков элементов будут подробно изучаться в разделе 3.

Отметим еще, что $(x^{-1})^{-1} = x$. Это также можно установить, используя свойство единственности обратного элемента. Положим $y = x^{-1}$, и найдем y^{-1}. Для этого достаточно заметить, что равенства $xy = yx = e$ могут служить не только определением обратного элемента для x, но и обратного элемента для y, а этим элементом оказывается именно x, и только он, ввиду единственности обратного для y.

И еще одно (возможно, тривиальное) замечание. Элемент $\overbrace{xx\dots x}^{n}$ (n-кратное произведение x на x) принято обозначать через x^n. Будем считать очевидным, что, ввиду ассоциативности умножения, $x^n x^m = x^{n+m}$ (в некоторых книгах это равенство доказывается!). Будем также полагать по определению, что $x^{-n} = \overbrace{x^{-1}x^{-1}\dots x^{-1}}^{n}$. Проверьте, что $(x^n)^{-1} = x^{-n}$. Для групп, в которых вместо умножения пишется сложение, вместо x^{-1} надо писать $-x$, вместо x^n должно стоять $x+\dots+x = nx$, и соответственно вместо x^{-n} используется запись $-nx$.

Следующий пример является одним из центральных во всей теории групп.

Пример 1.6. Пусть F — поле. Например, это может быть любое из полей $\mathbb{Q}$ (рациональные числа), $\mathbb{R}$ (действительные числа), $\mathbb{C}$ (комплексные числа). Обозначим через $GL_n(F)$ множество всех невырожденных $n \times n$-матриц с компонентами из поля F. Напомним, что матрица A называется невырожденной, если ее определитель $det(A)$ не равен нулю. Это эквивалентно существованию обратной к A матрицы, то есть такой матрицы A^{-1}, что

$$AA^{-1} = A^{-1}A = E_n.$$

Здесь E_n — единичная $n \times n$-матрица. Хорошо известно, что произведение невырожденных матриц является невырожденной матрицей. Следо-

вательно, произведение матриц определяет бинарную операцию

$$GL_n(F) \times GL_n(F) \longrightarrow GL_n(F), \quad (A, B) \mapsto AB.$$

Известно, что произведение матриц ассоциативно, а матрица E_n обладает свойством нейтрального элемента: $AE_n = E_nA = A$. Все это показывает, что $GL_n(F)$ является группой. Группа $GL_n(F)$ называется *общей линейной группой* степени n над полем F. В группе $GL_n(F)$ определена операция транспонирования: $A \mapsto {}^tA$, где i, j-й элемент матрицы ${}^tA$ равен j, i-му элементу A для всех $1 \leq i, j \leq n$. Одно из свойств операции транспонирования таково: ${}^t(AB) = ({}^tB)({}^tA)$. Кроме того ${}^t({}^tA) = A$. Это показывает, что операция транспонирования походит на операцию взятия обратного элемента. В дальнейшем (разделы 7 и 9) будут подробно изучены множества невырожденных матриц, у которых транспонированные матрицы совпадают с обратными. А пока докажем, что

$$({}^tA)^{-1} = {}^t(A^{-1}).$$

Пусть $X = {}^tA$. Любая матрица Y, такая, что $XY = YX = E_n$, будет обратной к X. Покажем, что в качестве Y можно взять ${}^t(A^{-1})$. В самом деле, используя свойства транспонирования, получим:

$$XY = ({}^tA)({}^t(A^{-1})) = {}^t(A^{-1}A) = {}^tE_n = E_n,$$

и точно так же проверяется, что $YX = E_n$. Ввиду единственности обратного элемента в группе требуемое равенство доказано.

Отметим, что при $n = 1$ группа $GL_n(F)$ является множеством всех ненулевых элементов поля F, а операция умножения 1×1-матриц сводится к операции умножения элементов поля. Таким образом, множество ненулевых элементов поля F, обозначаемое часто как F^*, является группой относительно операции умножения поля. Группы $\mathbb{R}^*$ и $\mathbb{C}^*$ в дальнейшем будут часто использоваться.

Гомоморфизм h из группы G_1 в группу G_2 — это отображение $h : G_1 \longrightarrow G_2$, удовлетворяющее следующим двум свойствам. Во-первых, для любых $x, y \in G_1$ имеет место равенство $h(xy) = h(x)h(y)$. Во-вторых, нейтральный элемент группы G_1 должен отображаться в нейтральный элемент группы G_2, то есть $h(e) = e$, или $h(1) = 1$, если нейтральные элементы обозначены символом 1.

Если из контекста не будет ясно, к какой группе принадлежит тот или иной нейтральный элемент,то надо использовать обозначения вида e_{G_1} или e_1 для нейтрального элемента G_1, и т.п.

Гомоморфизмы групп будут подробно изучены далее в разделе 4, а пока докажем, что для каждого $g \in G_1$ имеет место равенство:

$$h(g^{-1}) = h(g)^{-1}.$$

Положим $x = h(g)$, и пусть $y = h(g^{-1})$. Тогда

$$xy = h(g)h(g^{-1}) = h(gg^{-1}) = h(e) = e,$$
$$yx = h(g^{-1})h(g) = h(g^{-1}g) = h(e) = e.$$

Таким образом, $y = x^{-1}$, что и утверждалось.

Гомоморфизм h называется *изоморфизмом*, если существует гомоморфизм $f : G_2 \longrightarrow G_1$, такой, что $hf = 1_{G_2}$ и $fh = 1_{G_1}$. Здесь через 1_{G_1} и 1_{G_2} обозначаются тождественные отображения G_1 и G_2.

Иными словами, для каждого $x \in G_1$ имеетместо равенство $f(h(x)) = x$, а для каждого $y \in G_2$ — равенство $h(f(y)) = y$.

1.2. Докажите, что в определении изоморфизма достаточно потребовать, чтобы гомоморфизм h был биективным отображением. Тогда обратное отображение f будет гомоморфизмом автоматически.

Если существует какой-нибудь изоморфизм из G_1 в G_2, то говорят, что *группы* G_1 *и* G_2 *изоморфны*. Это обозначается следующим образом: $G_1 \cong G_2$.

1.3. Пусть G — группа. Зафиксируем какой-нибудь $g \in G$, и рассмотрим отображение $\alpha_g : G \to G$, действующее по правилу: $\alpha_g(x) = gxg^{-1}$. Доказать, что α_g — гомоморфизм групп. Более того, α_g — изоморфизм: $\alpha_g^{-1} = \alpha_{g^{-1}}$. Проверьте это.

Изоморфизмы из G в G называются *автоморфизмами* группы G. Автоморфизмы вида α_g называются *внутренними автоморфизмами*. Элементы x и gxg^{-1} называются *сопряженными* (иногда говорят — сопряженными посредством элемента g). Заметим, что если $y = gxg^{-1}$, то $x = (g^{-1})y(g^{-1})^{-1}$.

Пусть G — группа. Мощность множества G, обозначаемая через $|G|$, называется *порядком группы* G. Если $G_1 \cong G_2$, то $|G_1| = |G_2|$, обратное неверно.

Некоторые свойства гомоморфизмов собраны в следующей простой лемме.

Лемма 1.1. *Если даны два гомоморфизма групп* $h_1 : G_1 \to G_2$, $h_2 : G_2 \to G_3$, *то их суперпозиция* $h_2h_1 : G_1 \to G_3$, *определяемая как* $(h_2h_1)(x) = h_2(h_1(x))$, *также является гомоморфизмом групп. Тождественное отображение из группы* G *в* G *есть гомоморфизм групп (очевидно, что это изоморфизм). Суперпозиция изоморфизмов является изоморфизмом. Если* α_g *и* α_w *— внутренние автоморфизмы, то* $\alpha_g\alpha_w = \alpha_{gw}$.

1.4. Докажите эту лемму.

Подгруппой G' группы G называется подмножество $G' \subseteq G$, обладающее следующими свойствами:

1) нейтральный элемент (единица) группы G принадлежит G';

2) из $x, y \in G'$ следует $xy \in G'$;

3) если $x \in G'$, то $x^{-1} \in G'$.

Это определение означает, что, если взять ограничение бинарной операции для G на $G' \times G' \subseteq G \times G$, то его можно рассматривать как отображение в G', и относительно этой бинарной операции множество G' само становится группой, причем отображение включения $G' \subseteq G$ оказывается гомоморфизмом групп. Сама группа G и множество $\{e\}$ являются подгруппами G. Эти подгруппы принято называть тривиальными.

Очевидно, что если G' — подгруппа группы G, а G'' — подгруппа группы G', то G'' является и подгруппой группы G.

Рассмотрим несколько примеров подгрупп.

1.5. Пусть $SL_n(F) = \{A \in GL_n(F) | det(A) = 1\}$. Доказать, что это подгруппа группы $GL_n(F)$.

$SL_n(F)$ называется *специальной линейной группой* n-й степени над полем F.

1.6. Пусть $D_n(F)$ есть множество диагональных матриц из $GL_n(F)$, то есть матриц вида:

$$diag(\lambda_1, \lambda_2, \ldots, \lambda_n) = \begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \lambda_n \end{pmatrix},$$

где $\lambda_1, \lambda_2, \ldots, \lambda_n$ — ненулевые элементы поля F. Доказать, что это подгруппа группы $GL_n(F)$.

$D_n(F)$ обычно называют группой диагональных матриц.

1.7. Пусть $T_n(F)$ есть множество верхнетреугольных матриц из $GL_n(F)$, то есть матриц вида:

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ 0 & a_{2,2} & \ldots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_{n,n} \end{pmatrix},$$

где $a_{1,1}, a_{2,2}, \ldots, a_{n,n}$ — ненулевые элементы поля F. Доказать, что $T_n(F)$ — подгруппа группы $GL_n(F)$, а $D_n(F)$ — подгруппа группы $T_n(F)$.

Группу $T_n(F)$ принято называть треугольной группой.

1.8. Пусть $UT_n(F)$ есть множество верхнетреугольных матриц из $GL_n(F)$, на главной диагонали которых стоят единицы, то есть матриц вида:

$$\begin{pmatrix} 1 & a_{1,2} & \ldots & a_{1,n} \\ 0 & 1 & \ldots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}.$$

Доказать, что $UT_n(F)$ — подгруппа и группы $T_n(F)$, и группы $GL_n(F)$.

Группа $UT_n(F)$ называется унитреугольной.

1.9. Доказать, что имеет место изоморфизм аддитивной группы поля F и группы $UT_2(F)$.

Указание. Отображение $h : F \to UT_2(F)$ строится так. Пусть $a \in F$. Тогда

$$h(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

Докажите, что h — биекция и гомоморфизм. Групповая операция в F — сложение, а в $UT_2(F)$ — умножение. Поэтому h будет гомоморфизмлм, если $h(a+b) = h(a)h(b)$ и $h(0) = E_2$.

1.10. Пусть $1 \le m \le n-2$ и $UT_n^m(F)$ есть множество матриц из $T_n(F)$, у которых $m-1$ диагоналей выше главной диагонали состоят из одних нулей, то есть матриц вида:

$$\begin{pmatrix}
1 & 0 & & \dots & 0 & a_{1,m+1} & a_{2,m+1} & \dots & a_{1,n} \\
0 & 1 & 0 & & \dots & 0 & a_{2,m+2} & \dots & a_{2,n} \\
0 & 0 & 1 & 0 & & \dots & 0 & \ddots & \vdots \\
 & & & \ddots & \ddots & & & \ddots & a_{n-m,n} \\
 & & & & \ddots & & & \dots & 0 \\
 & & & & & & \ddots & & \\
 & & & & & & & \ddots & \vdots \\
 & & & & & & & \ddots & 0 \\
0 & & & & & & & & 1
\end{pmatrix}.$$

Здесь предполагается, что “пустые"места в матрице ниже главной диагонали заполнены нулями. Доказать, что $T_n^m(F)$ — подгруппа группы $T_n(F)$. При этом $T_n^1(F) = T_n(F)$.

1.11. Доказать, что имеет место изоморфизм аддитивной группы поля F и группы $UT_n^{n-2}(F)$.

Указание. Отображение $h : F \to UT_n^{n-2}(F)$ строится так. Пусть $a \in F$. Тогда

$$h(a) = \begin{pmatrix}
1 & 0 & \dots & 0 & a \\
0 & 1 & \dots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \dots & 1 & 0 \\
0 & 0 & \dots & 0 & 1
\end{pmatrix}.$$

Докажите, что h — биекция и гомоморфизм.

1.12. Доказать, что если H — подгруппа группы G, и $g \in G$, то множество $gHg^{-1} = \{gxg^{-1} | x \in H\}$ также будет подгруппой группы G.

Доказать, что $|H| = |gHg^{-1}|$.

Указание. Рассмотреть автоморфизм $\alpha_g : x \mapsto gxg^{-1}$.

Подгруппу gHg^{-1} называют подгруппой, сопряженной к H.

1.13. Пусть K и H — подгруппы группы G. Доказать, что множество $KH = \{xy | x \in K, y \in H\}$ будет подгруппой группы G тогда и только тогда, если $KH = HK$.

Лемма 1.2. *Пусть $h : G_1 \longrightarrow G_2$ — гомоморфизм групп, и G' — подгруппа G. Тогда множество $h(G') = \{\ h(x) \mid x \in G'\ \} \subseteq G_2$ является подгруппой группы G_2. Гомоморфизм h можно представить в виде суперпозиции сюръективного гомоморфизма $G_1 \to h(G_1)$ и инъективного гомоморфизма (включения) $h(G_1) \subseteq G_2$.*

1.14. Докажите эту лемму.

Если $f : X \longrightarrow Y$ — любое отображение, и $Z \subseteq Y$, то через $f^{-1}(Z)$ обозначается множество $\{\ x \in X \mid f(x) \in Z\ \}$. Оно называется (полным) прообразом Z относительно f. Отображение f инъективно тогда и только тогда, если прообраз любого элемента $y \in Y$ есть либо пустое множество, либо множество из одного элемента.

Лемма 1.3. *Пусть $h : G_1 \longrightarrow G_2$ — гомоморфизм групп, и G_2' — подгруппа группы G_2. Тогда $G_1' = h^{-1}(G_2')$ является подгруппой группы G_1'.*

1.15. Докажите эту лемму.

Лемма 1.4. *Пересечение любого семейства подгрупп снова является подгруппой.*

1.16. Докажите эту лемму.

Сформулируем в явном виде аксиомы группы для случая, когда групповая операция записывается как $x + y$ (сложение). Операция сложения должна удовлетворять следующим свойствам:

1) (ассоциативность) $(g_1 + g_2) + g_3 = g_1 + (g_2 + g_3)$ для любых $g_1, g_2, g_3 \in G$;

2) существует элемент $0 \in G$, такой, что для всех $g \in G$ имеют место равенства: $g + 0 = 0 + g = e$;

3) для каждого $x \in G$ найдется $y \in G$ такой, что $x + y = y + x = 0$. В аддитивной записи обратный элемент y обозначается как $-x$, при этом используется также обозначение $a - b = a + (-b)$.

Аддитивная запись групповой операции чаще всего используется для коммутативных групп, то есть групп, в которых

4) $x + y = y + x$ для всех $x, y \in G$.

Такие группы часто называются *абелевыми*. Простейший пример такой группы — группа $\mathbb{Z}$ всех целых чисел.

Гомоморфизм абелевых групп $h : G_1 \longrightarrow G_2$ должен удовлетворять свойствам:

1) $h(x + y) = h(x) + h(y)$ для всех $x, y \in G_1$;

2) $h(0) = 0$.

Отсюда следует, что $h(-x) = -h(x)$.

Пример 1.7. Каждое линейное (или векторное) пространство является абелевой группой по сложению. Каждое линейное отображение векторных пространств является гомоморфизмом абелевых групп.

Таким образом, теорию групп можно считать и обобщением теории векторных пространств и линейных отображений.

Напомним, что в дальнейшем, как правило, операция в произвольной группе будет обозначаться как умножение. Подразумевается, что читетель сумеет в случае необходимости дать переформулировку для случая аддитивных обозначений.

Пусть G — некоторая группа, и $X \subseteq G$ — подмножество G. Рассмотрим множество $\langle X \rangle = \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_m^{\varepsilon_m} | x_i \in X, \varepsilon_i = \pm 1, 1 \leq i \leq m, m \geq 0\}$. Элементы этого множества будем называть *словами* в алфавите X. Число m естественно назвать длиной слова $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_m^{\varepsilon_m}$ Подразумевается, что при $m = 0$ соответствующее слово есть нейтральный элемент (единица) группы G. В множество $\langle X \rangle$ входят все возможные слова в алфавите X всех возможных длин. В частности, слова длины 1 — это элементы $x \in X$ и $x^{-1}, x \in X$. Таким образом, $X \subseteq \langle X \rangle$.

Лемма 1.5. *Множество $\langle X \rangle$ является подгруппой группы G, содержащей множество X. Если G' — какая-то другая подгруппа группы G, содержащая множество X, то $\langle X \rangle \subseteq G'$.*

Доказательство. Единица (нейтральный элемент) группы G по определению принадлежит $\langle X \rangle$. Если $x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m} \in \langle X \rangle$, то $(x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m})^{-1} = x_m^{-\varepsilon_m} \dots x_1^{-\varepsilon_1}$. Показатели $-\varepsilon_i$ равны плюс или минус единицам, откуда следует, что произведение $x_m^{-\varepsilon_m} \dots x_1^{-\varepsilon_1}$ удовлетворяет определению элементов $\langle X \rangle$. Если $x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m} \in \langle X \rangle$, и $x_{m+1}^{\varepsilon_{m+1}} \dots x_{m+k}^{\varepsilon_{m+k}} \in \langle X \rangle$, то произведение этих элементов есть слово

$$x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m} x_{m+1}^{\varepsilon_{m+1}} \dots x_{m+k}^{\varepsilon_{m+k}},$$

которое также согласно определению должно содержаться в $\langle X \rangle$. Таким образом, все свойства из определения подгруппы выполнены. □

1.17. Доказать, что $\langle X \rangle$ совпадает с пересечением всех подгрупп группы G, содержащих подмножество X.

Говорят, что подгруппа $\langle X \rangle$ *порождена* множеством X, и что X есть множество *порождающих* (или *образующих*) элементов этой подгруппы. Особый интерес представляет нахождение множеств образующих элементов для всей группы G. Этот класс задач немного походит на задачи о нахождении базисов векторнорных пространств.

Пример 1.8. Пусть групповая операция в G обозначается как плюс, и группа G коммутативна (абелева). Возьмем $X \subseteq G$, и посмотрим, что такое $\langle X \rangle$. Применение общего определения показывает, что после “приведения подобных членов"это будет множество $\{n_1 x_1 + n_2 x_2 +$

$\cdots + n_m x_m | x_1, \ldots, x_m \in X, n_1, \ldots, n_m \in \mathbb{Z}, m \geq 0\}$. Напомним, что $\mathbb{Z}$ есть множество всех целых чисел. Отсюда видно, что конструкция абелевой подгруппы, порожденной множеством X, очень походит на линейную оболочку множества в векторном пространстве. В общем (неабелевом и неаддитивном) случае аналогия между $\langle X \rangle$ и линейной оболочкой также может оказаться полезной.

1.18. Докажите, что $\langle X \rangle = X$ тогда и только тогда, если X — подгруппа G. Выведите отсюда, что $\langle\langle X \rangle\rangle = \langle X \rangle$.

Возможно, простейшими группами являются *циклические группы* — группы, порожденные одним элементом, т.е. группы, которые состоят из степеней (положительных и отрицательных) одного элемента. Иными словами, если G — циклическая группа, то существует $x \in G$, такой, что $G = \{1, x, x^{-1}, x^2, x^{-1}, \ldots\}$ (или, для аддитивных обозначений $G = \{0, \pm x, \pm 2x, \pm 3x, \ldots\}$).

Пример 1.9. Группа (с операцией сложения) всех целых чисел $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ является циклической с образующим элементом 1, так как любой ее ненулевой элемент равен либо $1 + \cdots + 1$, либо $(-1) + \ldots + (-1)$.

Рассмотрим множество $\mathbf{U}_n$, состоящее из всех комплексных корней n-й степени из единицы. Хорошо известно, что множество $\mathbf{U}_n$ состоит из элементов $u_0, u_1, \ldots, u_{n-1}$, где $u_k = \cos\dfrac{2\pi k}{n} + i \sin\dfrac{2\pi k}{n} = e^{i\frac{2\pi k}{n}}$, при $k = 0, 1, \ldots, n-1$. Из свойств комплексных чисед следует, что $u_k u_l = u_{k+l \pmod n}$, где $k + l \pmod n$ означает остаток от деления на n. В часности, произведение двух корней n-й степени из единицы — снова корень n-й степени из единицы. Отсюда же следует, что $u_k = u_1^k$. Очевидно, что $u_1^n = 1$, откуда следует, что $u_k^{-1} = u_{n-k}$. Таким образом, $\mathbf{U}_n$ оказывается подгруппой группы $\mathbb{C}^* = GL_1(\mathbb{C})$, и ясно, что эта группа циклическая с образующим u_1.

Основные свойства циклических групп собраны в следующей теореме.

Теорема 1.1. *Каждая циклическая группа изоморфна либо $\mathbb{Z}$ (бесконечная циклическая группа), либо $\mathbf{U}_n$ — конечная циклическая группа. Любая подгруппа циклической группы является циклической.*

Доказательство. Пусть $G = \langle x \rangle = \{\ldots x^{-2}, x^{-1}, 1, x^1, x^2, \ldots\}$. Сначала выясним, когда возможна такая ситуация: $x^k = x^m$ при $k \neq m$ например при $k < m$. Умножая обе части этого равенства на x^{-k}, приходим к равенству $x^{m-k} = 1$, причем $m - k > 0$. Рассмотрим множество всех целых положительных чисел l таких, что $x^l = 1$. Как только что выяснилось, это множество непусто. Пусть n — наименьшее число из этого множества. Рассмотрим элементы $1, x, \ldots, x^{n-1}$, и покажем, что среди них нет одинаковых. Если бы $x^k = x^m$ при $0 \leq k < m < n$, то снова получилось бы $x^{m-k} = 1$, но $0 < m - k < n$, и это противоречит выбору n. С другой стороны, пусть x^m — произвольный элемент из G. Разделим m на n с остатком: $m = nq + r$, где $0 \leq r < n$. Тогда

$$x^m = x^{nq+r} = x^{nq}x^r = (x^n)^q x^r = x^r,$$

так как $x^n = 1$. Отсюда следует, что $x^m \in \{1, x, \ldots, x^{n-1}\}$, и это означает, что вся группа G состоит из попарно различных элементов $1, x, \ldots, x^{n-1}$, и, в частности, является конечной.

Определим отображение $h : G \to \mathbf{U}_n$, полагая при $0 \leq k \leq n-1$ его значение равным $h(x^k) = e^{\frac{2\pi k}{n} i} = u^k$, где $u = \cos\dfrac{2\pi}{n} + i \sin\dfrac{2\pi}{n}$. Ясно, что это биекция, и что $h(1) = 1$. Остается проверить, что $h(x^k x^l) = h(x^{k+l}) = h(x^k)h(x^l)$ для любых $0 \leq k, l < n$. Если $k + l < n$, то это очевидно. Если же $m = k + l > n$, то пусть, как и выше, $m = nq + r$, $0 \leq r < n$. Тогда $x^m = x^r$, и $h(x^m) = h(x^r) = u^r$ (надо помнить, что значение $h(x^k)$ определено только при $0 \leq k < n$). С другой стороны,

$$h(x^k)h(x^l) = u^k u^l = u^{k+l} = u^{nq}u^r = (u^n)^q u^r = u^r,$$

так как u есть корень n-й степени из единицы. Следовательно, h является гомоморфизмом, а значит, и изоморфизмом.

Если же группа G бесконечна, то соотношение вида $x^k = x^m$ при $k \neq m$ невозможно. Это значит, что все степени x^k при $k \in \mathbb{Z}$ различны, и отображение $h : \mathbb{Z} \to G$, $h(k) = x^k$ является биекцией. Так как $x^0 = 1$, $x^{k+l} = x^k x^l$, то это к тому же гомоморфизм групп. Итак, построен биективный гомоморфизм, то есть изоморфизм $\mathbb{Z} \cong G$.

Пусть теперь $G = \langle x \rangle$ — некоторая циклическая группа, и допустим, что $G' \subseteq G$ — нетривиальная подгруппа G. Множество G' состоит из степеней элемента x, положительных и (возможно) отрицательных.

Выберем элемент $y = x^n \in G'$ с наименьшим возможным $n > 0$, и покажем, что G' состоит из всевозможных степеней y, и только из них. С одной стороны понятно, что $y^k = x^{nk} \in G'$ для любого целого m. Пусть $x^m \in G'$. Представим m в виде $m = nq + r$, с $0 \leq r < n$. Тогда $x^m = (x^n)^q x^r$. Отсюда $x^r = (x^n)^{-q} x^m$. Так как $x^m \in G'$ и $x^n \in G'$, отсюда следует, что $x^r \in G'$. Если $r > 0$, то получим противоречие с минимальностью n. Значит, $r = 0$, $m = nq$, и $x^m = (x^n)^q = y^q$. Итак, G' состоит из всех возможных степеней y. $\square$

Будем в дальнейшем обозначать конечные циклические группы порядка n через Z_n (в некоторых книгах встречается также обозначение C_n). Итак, $Z_n = \{1, x, x^2, \ldots, x^{n-1}\}$ и $x^n = 1$.

Пример 1.10. Опишем некоторое множество образующих для группы $GL_n(F)$. Для этого предварительно введем один базис в линейном пространстве $M_n(F)$ квадратных $n \times n$-матриц над полем F. Пусть $E_{i,j}$ есть матрица, в которой все компоненты равны нулю, кроме i,j-й, равной единице. Если $A \in M_n(F)$ — матрица с компонентами $a_{k,l}$ в k-й строке и l-м столбце $(1 \leq k, l \leq n)$, то

$$A = \sum_{k=1}^{n} \sum_{l=1}^{n} a_{k,l} E_{k,l}.$$

Например, для $n = 2$ это выглядит так:

$$\begin{pmatrix} a_{1,1} & a_{2,1} \\ a_{1,2} & a_{2,2} \end{pmatrix} = a_{1,1} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + a_{1,2} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + a_{2,1} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + a_{2,2} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$
$$= a_{1,1}E_{1,1} + a_{1,2}E_{1,2} + a_{2,1}E_{2,1} + a_{2,2}E_{2,2}$$

Очевидно, что матрицы $E_{i,j}$ линейно независимы над F. Основные свойства матричных единиц таковы:

$$E_{i,j}E_{j,k} = E_{i,k}, \;\; E_{i,j}E_{l,k} = 0 \;\; \text{при} \;\;\; j \neq l,$$
$$\sum_{k=1}^{n} E_{k,k} = E_n.$$

Эти тождества легко проверяются прямым вычислением. Также легко проверяется, что $E_{i,j}A$ есть матрица, в которой i-я строка есть j-я строка A, а все остальные элементы равны нулю. Аналогично, $AE_{i,j}$ есть

матрица, в которой j-й столбец есть i-й столбец A, а все остальные компоненты нулевые. Определим следующие матрицы $(1 \leq i, j \leq n)$:

$$\begin{array}{l} t_{i,j}(\lambda) = E + \lambda E_{i,j} \ (i \neq j, \lambda \in F), \\ d_i(\gamma) = E + (\gamma - 1)E_{i,i} = diag(1, \ldots, \gamma, \ldots, 1) \\ (\gamma \in F, \gamma \neq 0, \text{ этот элемент расположен на } i\text{-месте}) \end{array} \quad (3)$$

Умножение $t_{i,j}(\lambda)$ на A слева равносильно прибавлению к i-й строке A ее j-й строки, умноженной на скаляр λ, а умножение $t_{i,j}(\lambda)$ на A справа равносильно прибавлению к j-му столбцу i-го столбца, умноженного на λ. Иными словами, это известные с 1-го курса элементарные преобразования. Заметим, что $t_{i,j}(\lambda) \in GL_n(F)$, так как $t_{i,j}(\lambda)^{-1} = t_{i,j}(-\lambda)$ (проверьте это!). Матрица $d_i(\gamma)$ также обратима: $d_i(\gamma)^{-1} = d_i(\gamma^{-1})$. Умножение $d_i(\gamma)$ на A слева равносильно умножению всех элементов i-й строки A на ненулевой элемент γ, умножение справа равносильно умножению на g всего i-го столбца A. Таким образом, это снова известное с первого курса элементарное преобразование. Теперь надо вспомнить алгоритм нахождения обратной к $A \in GL_n(F)$ матрицы с помощью элементарных преобразований. В его основе — последовательность элементарных преобразований, переводящих A в единичную матрицу. Поскольку в каждой строке и каждом столбце A на каждом этапе преобразований заведомо есть ненулевые элементы, то необходимости в перестановке строк и столбцов нет: достаточно к строке (или столбцу), i-й диагональный элемент которой (которого) нулевой, прибавлять ту строку (или столбец), где элемент i-го столбца (или строки) не равен нулю. Так как элементарное преобразование означает умножение слева или справа на матрицы вида $t_{i,j}(\lambda)$ или $d_i(\gamma)$, то в результате должно получиться равенство вида:

$$B_1 B_2 \ldots B_m A C_1 C_2 \ldots C_k = E_n,$$

где матрицы B_s, C_r — это некоторые матрицы $t_{i,j}(\lambda)$ или $d_i(\gamma)$. Отсюда получаем для A равенство:

$$A = B_m^{-1} \ldots B_1^{-1} C_k^{-1} \ldots C_1^{-1}.$$

Поскольку матрицы, обратные к $t_{i,j}(\lambda)$ и $d_i(\gamma)$ — это снова матрицы элементарных преобразований таких же типов, приходим к следующему выводу: группа $GL_n(F)$ порождается множеством всех матриц вида (3).

1.19. Доказать, что в качестве множества образующих для $GL_n(F)$ можно взять элементы $t_{i,j}(\lambda)$ и $d_n(\gamma)$.

1.20. Доказать, что элементы $t_{i,j}(\lambda)$ порождают группу $SL_n(F)$.

1.21. Доказать, что элементы $d_i(\gamma)$, $1 \leq i \leq n$ порождают группу $D_n(F)$.

1.22. Доказать, что в качестве множества образующих для $T_n(F)$ можно взять элементы $t_{i,j}(\lambda)$ при i, j и $diag(\gamma_1, \ldots, \gamma_n)$, $\gamma_1, \ldots, \gamma_n \neq 0$.

1.23. Доказать, что элементы $t_{i,j}(\lambda)$ при $i < j$ порождают группу $UT_n(F)$.

1.24. Зафиксируем m, $1 \leq m \leq n-2$. Доказать, что элементы $t_{i,j}(\lambda)$ при $j - i \geq m$ порождают группу $UT_n^m(F)$.

Обозначим через $[x, y]$ элемент $xyx^{-1}y^{-1}$. Этот элемент называется *коммутатором* элементов x и y. Легко заметить, что $[x, y] = 1$ тогда и только тогда, если $xy = yx$. Кроме того, $[x, y]^{-1} = [y, x]$.

1.25. Докажите, что если G — любая группа, $x, y, z \in G$, то

$$[x, yz] = [x, y][x, z][[x, z], y]$$

1.26. Докажите, что

$$[xy, z] = [y, z][[z, y], x][x, z]$$

1.27. Проверьте тождество:

$$[xy, z] = (x[y, z]x^{-1})[x, z]$$

1.28. Будем обозначать через ${}^a b$ элемент aba^{-1}. Докажите, что если G — любая группа, $x, y, z \in G$, то

$$[[x, y], {}^y z][[y, z], {}^z x][[z, x], {}^x y] = 1.$$

2. Группы подстановок

Пусть X — некоторое множество. Обозначим через S_X множество всех биективных отображений из X в X. Через 1_X обозначим тождественное (единичное) отображение из X в X, то есть такое отображение, что $1_X(x) = x$ для каждого элемента $x \in X$. Если даны $\sigma, \tau \in S_X$, то суперпозиция функций σ и τ обозначается через $\sigma\tau$ и является отображением, действующим по правилу $\sigma\tau(x) = \sigma(\tau(x))$. Суперпозиция биективных отображений является биективным отображением, т.е. $\sigma\tau \in S_X$. Известно, что суперпозиция любых отображений ассоциативна: если даны три отображения $f : Z \longrightarrow W$, $g : Y \longrightarrow Z$, $h : X \longrightarrow Y$, то $(fg)h = f(gh)$. Тем более ассоциативна суперпозиция элементов S_X. Ввиду биективности $\sigma \in S_X$ существует обратное к нему отображение $\sigma^{-1} \in S_X$, характеризующееся свойствами: $\sigma\sigma^{-1} = 1_X$, $\sigma^{-1}\sigma = 1_X$. Суперпозицию функций из S_X можно рассматривать как бинарную операцию на S_X:

$$S_X \times S_X \longrightarrow S_X, \qquad (\sigma, \tau) \mapsto \sigma\tau.$$

Суперпозиция функций в данном случае обычно называется умножением элементов S_X. Перечисленные выше свойства этого умножения означают, что оно превращает S_X в *группу* с единицей 1_X.

Положим $X = \{1, 2, \ldots, n\}$. Вместо S_X в этом случае используется обозначение S_n. Эта группа называется *группой подстановок n-й степени*, или *симметрической группой*. Элементы этой группы называются подстановками n-й степени, или просто подстановками. Как известно, некоторые функции определяются таблицами, в которых каждому значениюю аргумента сопоставлено значение функции от этого аргумента. Для функций из S_n используется следующая разновидность табличного задания: таблица походит на матрицу из двух строк, в верхней строке записаны элементы из множества аргументов функции, а в нижней — из множеством значений функции, причем значение функции $\sigma(i)$ записывается под значением аргумента i. В случае произвольного $\sigma \in S_n$ это выглядит так:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(i) & \ldots & \sigma(n) \end{pmatrix}$$

Например, единичная (или тождественная) подстановка, которая в дальнейшем будет обозначаться как 1_n или просто как 1, записывается в виде:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Следует отметить, что порядок следования аргументов в верхней строке не является существенным. Существенным для задания функции является только вертикальное соответствие между значением аргумента i и значением функции $\sigma(i)$. Например, таблицы

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 3 & 5 & 1 & 4 & 2 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$$

являются просто разными формами записи одной и той же функции, т.е. подстановки, и получаются одна из другой перестановками столбцов. Из того, что знак функции записывается слева от аргумента, и из определения суперпозиции $\sigma\tau(i) = \sigma(\tau(i))$ следует, что при вычислении умножения (суперпозиции) двух подстановок надо начинать с аргумента, находящегося в верхней строке самой правой подстановки, и двигаться справа налево. Это можно представить так:

$$\begin{pmatrix} \dots & \tau(i) & \dots \\ \dots & \sigma(\tau(i)) & \dots \end{pmatrix} \begin{pmatrix} \dots & i & \dots \\ \dots & \tau(i) & \dots \end{pmatrix} = \begin{pmatrix} \dots & i & \dots \\ \dots & \sigma(\tau(i)) & \dots \end{pmatrix}$$

Например,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$$

Подстановку, обратную к заданной подстановке σ, можно вычислить, просто поменяв местами верхнюю и нижнюю строки в таблице, задающей подстановку. Например, если

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix} \quad \text{то} \quad \sigma^{-1} = \begin{pmatrix} 3 & 4 & 2 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}.$$

2.1. Доказать, что мощность множества S_n равна $n!$.

Напомним, что мощность множества элементов группы G называется *порядком* группы и обозначается через $|G|$.

Пусть дана подстановка $\sigma \in S_n$. Множество $\{\, i \mid i \in \{1, 2, \dots, n\}, \sigma(i) \neq i \,\}$ будем называть множеством *перемещаемых символов* подстановки σ, а множество $\{\, i \mid i \in \{1, 2, \dots, n\}, \sigma(i) = i \,\}$ — множеством *неподвижных символов* подстановки σ.

2.2. Доказать, что если $\sigma, \tau \in S_n$, и множества перемещаемых символов у σ и τ не пересекаются, то $\sigma\tau = \tau\sigma$.

Определим подстановки специального вида, называемые *циклами*. Пусть дано подмножество $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$. Рассмотрим отображение σ, такое, что $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, $\ldots$, $\sigma(i_{k-1}) = i_k$, $\sigma(i_k) = i_1$, а для $j \notin \{i_1, i_2, \ldots, i_k\}$ положим $\sigma(j) = j$. Легко убедиться, что это отображение биективно, то есть $\sigma \in S_n$. Подстановка σ называется *циклом длины* k и обозначается через $(i_1, i_2, \ldots, i_k)$. Порядок следования элементов $i_1, i_2, \ldots, i_k$ в записи цикла является существенным. Циклы длины 2 принято также называть *транспозициями*. Легко убедиться, что $(i, j) = (j, i) = (i, j)^{-1}$. Перемещаемые символы цикла $(i_1, i_2, \ldots, i_k)$ — это множество $\{i_1, \ldots, i_k\}$.

2.3. Пусть $\sigma = (i_1, i_2, \ldots, i_k)$, $\tau = (j_1, j_2, \ldots, j_m)$. Доказать, что $\sigma\tau = \tau\sigma$ тогда и только тогда, если $\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_m\} = \emptyset$.

Циклы с описанными в этой задаче свойствами называются *независимыми*. Запись цикла в виде $(i_1, i_2, \ldots, i_k)$ не является однозначной. Исходя из определения цикла как отображения, нетрудно убедиться, что $(i_1, i_2, \ldots, i_k) = (i_2, i_3, \ldots, i_k, i_1) = (i_3, i_4, \ldots, i_k, i_1, i_2) = \ldots = (i_k, i_1, i_2, \ldots, i_{k-1})$.

2.4. Доказать, что количество циклов длины k в группе S_n равно $\dfrac{n(n-1)\ldots(n-k+1)}{k}$.

Теорема 2.1. *Каждую подстановку $\sigma \in S_n$ можно представить в виде произведения попарно независимых циклов $\sigma = \sigma_1\sigma_2\ldots\sigma_r$. Множество циклов $\{\sigma_1, \ldots, \sigma_r\}$ определяется по подстановке σ однозначно. Это значит, что если имеется второй способ записи σ в виде произведения независимых циклов $\sigma = \sigma'_1\sigma'_2\ldots\sigma'_d$, то $r = d$ и $\{\sigma_1, \ldots, \sigma_r\} = \{\sigma'_1, \ldots, \sigma'_r\}$*

Краткое доказательство. Пусть дано разложение подстановки σ в произведение независимых циклов: $\sigma = \sigma_1\sigma_2\ldots\sigma_r$. Пусть X_j — множество перемещаемых символов цикла σ_j, $j = 1,\ldots,r$. По определению независимых циклов, при $j \neq t$ множества X_j и X_t не пересекаются. Множество перемещаемых символов σ — это $X_1 \cup X_2 \cup \ldots \cup X_r$. Если $i \in X_j$, то $\sigma(i) = \sigma_j(i)$. Иными словами, отображение σ_j на подмножестве X_j совпадает с σ, а вне этого множества действует тождественно. Если $X_j = \{i_1, i_2, \ldots, i_k\}$ и $\sigma_j = (i_1, i_2, \ldots, i_k)$, то $i_2 = \sigma(i_1)$, $i_2 = \sigma(i_2) = \sigma(\sigma(i_1)) = \sigma^2(i_1)$, $i_3 = \sigma(\sigma(\sigma(i_1))) = \sigma^3(i_1), \ldots, i_k = \sigma^{k-1}(i_1)$, $i_1 = \sigma^k(i_1)$. При этом выбор $i_1 \in X_j$ по сути, произволен, так как $(i_1, i_2, \ldots, i_k) = (i_2, i_3, \ldots, i_k, i_1) = (i_3, i_4, \ldots, i_k, i_1, i_2) = \ldots$. Из всего этого можно сделать вывод, что множества X_1, $\ldots$, X_r, и сами циклы σ_1, $\ldots$, σ_r определяются по подстановке σ однозначно.

Исходя из этого наблюдения, можно построить множества X_1, $\ldots$, X_r и циклы $\sigma_1, \ldots, s_r$ для произвольной подстановки следующим образом. Пусть X — множество перемещаемых символов σ. Выберем какой-нибудь аргумент $i \in X$, и рассмотрим последовательность i, $\sigma(i)$, $\sigma^2(i)$, $\sigma^3(i)$, $\ldots$. Так как множество аргументов $\{1, 2, \ldots, n\}$ конечно, то для некоторых $m < q$ получим $\sigma^m(i) = \sigma^q(i)$. Так как отображение σ биективно, то это означает, что $\sigma^{q-m}(i) = i$. Пусть $k > 1$ — наименьшее число со свойством $\sigma^k(i) = i$. Положим $X_1 = \{i, \sigma(i), \ldots, \sigma^{k-1}(i)\}$ (так как выбрано k со свойством минимальности, то все эти элементы различны), и $\sigma_1 = (i, \sigma(i), \ldots, \sigma^{k-1}(i))$. Очевидно, что $\sigma(t) = \sigma_1(t)$ для каждого $t \in X_1$. Выберем далее произвольным образом $d \in X \setminus X_1$, и рассмотрим последовательность $d, \sigma(d), \sigma^2(d), \sigma^3(d), \ldots$. Аналогично тому, как это было сделано выше, убеждаемся, что она конечна, и что можно выбрать p так, что $\sigma^p(d) = d$ и p — минимальное число, обладающее этим свойством. Положим $X_2 = \{d, \sigma(d), \ldots, \sigma^{p-1}(d)\}$, $\sigma_2 = (d, \sigma(d), \ldots, \sigma^{p-1}(d))$. Снова легко убедиться в том, что $\sigma(t) = \sigma_2(t)$ для $t \in X_2$. Проверим, что $X_1 \cap X_2 = \emptyset$. В самом деле, если бы, например, $\sigma^m(d) = \sigma^q(i)$ при $m \leq q$, то $d = \sigma^{q-m}(i) \in X_1$, что противоречит выбору d. Если же $m > q$, то $i = \sigma^{m-q}(d)$. Вспоминая, что $\sigma^p(d) = d$, выберем число v так, что $v + m - q = pl$, и применим к левой и правой частям равенства $i = \sigma^{m-q}(d)$ подстановку σ^v. В результате получим $d = \sigma^v(i)$ — снова противоречие. Итак, σ_1 и σ_2 — независимые циклы. Пусть уже построены

независимые циклы $\sigma_1, \ldots, \sigma_{j-1}$ с множествами перемещаемых символов $X_1, \ldots, X_{j-1}$ соответственно, причем $X_1, \ldots, X_{j-1} \subseteq X$, и $\sigma(t) = \sigma_l(t)$ для любого $1 \leq l \leq j-1$ и всех $t \in X_l$. Пусть $\sigma' = \sigma_1 \ldots \sigma_{j-1}$. Тогда $\sigma(t) = \sigma'(t)$ при $t \in X' = X_1 \cup \ldots \cup X_{j-1}$. Если $X = X'$, то разложение σ в произведение независимых циклов получено. Если же существует $w \in X \setminus X'$, то можно повторить описанное выше построение, и получить цикл $\sigma_j = (w, \sigma(w), \sigma^2(w), \ldots)$ с множеством перемещаемых символов $X_j = \{w, \sigma(w), \ldots\}$. Рассуждения, аналогичные уже проведенным, показывают, что $\sigma(t) = \sigma_j(t)$ при $t \in X_j$, и $X_j \cap X' = \emptyset$. Таким образом, цикл σ_j независим от циклов $\sigma_1, \ldots, \sigma_{j-1}$. Продолжая этот процесс до полного исчерпания множества X, получим независимые циклы $\sigma_1, \ldots, \sigma_r$, такие, что σ и $\sigma_1 \ldots \sigma_r$ принимают одинаковые значения на каждом аргументе. $\square$

В доказательстве этой теоремы содержится и алгоритм разложения подстановок в произведение независимых циклов. Рассмотрим пример.

Пример 2.1. Пусть дана подстановка

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 4 & 5 & 2 & 10 & 8 & 12 & 11 & 9 & 1 & 6 & 7 \end{pmatrix}.$$

Следуя ходу рассуждений теоремы, выберем какой-то перемещаемый символ σ, скажем, 1. Тогда $\sigma(1) = 3$, $\sigma(3) = 5$, $\sigma(5) = 10$, $\sigma(10) = 1$. На этом построение первого цикла закончено. Этот цикл — $(1, 3, 5, 10)$. Его перемещаемые символы — множество $\{1, 3, 5, 10\}$. Далее выбираем любой перемещаемый символ σ, не принадлежащий этому множеству, например 6. Получим $\sigma(6) = 8$, $\sigma(8) = 11$, $\sigma(11) = 6$. Итак, второй цикл в нашем разложении — $(6, 8, 11)$. Следующий перемещаемый символ σ надо выбирать вне множества $\{1, 3, 5, 10\} \cup \{6, 8, 11\}$. Пусть это элемент 2. Тогда $\sigma(2) = 4$, $\sigma(4) = 2$. Получаем цикл $(2, 4)$. Наконец, возьмем элемент 7, не являющийся перемещаемым символом ни в одном из уже построенных циклов. Тогда $\sigma(7) = 12$, $\sigma(12) = 7$. Итак, следующий цикл — $(7, 12)$. Но больше перемещаемых символов у σ нет (так как $\sigma(9) = 9$, то это не перемещаемый символ), поэтому найденный цикл $(7, 12)$ является последним. Окончательно получаем:

$$\sigma = (1, 3, 5, 10)(6, 8, 11)(2, 4)(7, 12).$$

Напомним следующее определение. Пусть G — некоторая группа, $X \subseteq G$. Говорят, что множество X *порождает* группу G (или что G порождается множеством X, или что X есть *множество образующих* группы G), если каждый элемент из G можно представить в виде $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_m^{\varepsilon_m}$, где $x_i \in X$, $\varepsilon_i = \pm 1$ для всех i, $1 \le i \le m$, и $m \ge 0$. Случай $m = 0$ соответствует единице группы G. Группа, порожденная множеством X, обозначается через $\langle X \rangle$. Знание множества образующих элементов группы G часто дает весьма существенную информацию о всей группе, при этом чем меньше множество образующих, тем (как правило) оно удобнее для использования. Приведенная выше теорема утверждает, что группа S_n порождается множеством всех содержащихся в этой группе циклов. В следующих задачах описываются некоторые гораздо меньшие множества, порождающие группы подстановок.

2.5. $(i_1, i_2, \dots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \dots (i_1, i_3)(i_1, i_2) =$
$= (i_{k-1}, i_k)(i_{k-2}, i_k) \dots (i_2, i_k)(i_1, i_k)$

2.6. Доказать, что S_n порождается всеми транспозициями.

2.7. $(i, j) = (k, i)(k, j)(k, i)$

Здесь i, j, k попарно различны. Аналогичное предположение действует и в других задачах этого раздела: различные буквы обозначают различные элементы множества $\{1, 2, \dots, n\}$.

2.8. $(i, j)(i, k) = (i, k, j)$, $(i, j)(k, m) = (j, k, m)(i, m, j)$

2.9. $(i, j, k)^2 = (i, k, j)$

2.10. $(i, j, k, m)^2 = (i, k)(j, m)$

2.11. Проверить, что
$(i_1, i_2, \dots, i_k)^k = 1$;
$(i_1, i_2, \dots, i_k)^{-1} = (i_1, i_2, \dots, i_k)^{k-1} =$
$= (i_1, i_k, i_{k-1} \dots, i_2) = (i_k, i_{k-1}, \dots, i_2, i_1)$.

В следующих двух задачах через $[x, y]$ обозначается элемент $xyx^{-1}y^{-1}$.

2.12. $[(i,j),(i,k)] = (i,j,k)$

2.13. $[(i,j,d),(i,k,m)] = (i,j,k)$

Пусть даны две подстановки $\sigma, \sigma' \in S_n$. Говорят, что они имеют *одинаковое циклическое строение*, если и в и разложении σ, и в разложении σ' в произведение независимых циклов содержится по одному и тому же количеству циклов одной и той же длины. Таковы, например, подстановки

$$\sigma = (1,2,3,4)(5,6,7)(8,9,10)(11,12)(13,14)(15,16), \quad \text{и}$$
$$\sigma' = (16,15,14,13)(12,11,10)(9,8,7)(6,5)(4,3)(2,1).$$

2.14. Пусть даны две подстановки σ и σ', имеющие одинаковое циклическое строение. Рассмотрим их разложения в произведения независимых циклов

$$\sigma = (\alpha_1, \alpha_2, \ldots)(\beta_1, \beta_2, \ldots)(\ldots), \quad \sigma' = (\alpha'_1, \alpha'_2, \ldots)(\beta'_1, \beta'_2, \ldots)(\ldots),$$

где сомножители упорядочены так, что циклы одинаковой длины соответствуют друг другу. Например, одинаковую длину имеют циклы $(\alpha_1, \alpha_2, \ldots)$ и $(\alpha'_1, \alpha'_2, \ldots)$, $(\beta_1, \beta_2, \ldots)$ и $(\beta'_1, \beta'_2, \ldots)$, и т.д. Рассмотрим подстановку

$$x = \begin{pmatrix} \alpha_1 \, \alpha_2 \, \ldots \, \beta_1 \, \beta_2 \, \ldots \\ \alpha'_1 \, \alpha_2 \, \ldots \, \beta_1 \, \beta_2 \, \ldots \end{pmatrix}.$$

Доказать, что $\sigma' = x\sigma x^{-1}$.

2.15. Пусть $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$, $x \in S_n$. Тогда $\alpha' = x\alpha x^{-1}$ — снова цикл длины k. При этом, если

$$x = \begin{pmatrix} \ldots \alpha_1 \; \alpha_2 \ldots \alpha_k \ldots \\ \ldots \alpha'_1 \; \alpha'_2 \ldots \alpha'_k \ldots \end{pmatrix}, \quad \text{то} \qquad \alpha' = (\alpha'_1, \alpha'_2, \ldots, \alpha'_k).$$

2.16. Доказать, что две подстановки σ и σ' связаны соотношением $\sigma' = x\sigma x^{-1}$ тогда и только тогда, если они имеют одинаковое циклическое строение.

2.17. Пусть $1 \le i < j \le n$, и $\sigma = (i, i+1)(i+1, i+2)\dots(j-2, j-1)$. Показать, что $(i, j) = \sigma(j-1, j)\sigma^{-1}$. Учесть при этом, что в любой группе $(xy)^{-1} = y^{-1}x^{-1}$, и что для любой транспозиции $(a, b) = (b, a) = (a, b)^{-1}$.

2.18. Доказать, что группа S_n порождается транспозициями вида $(i, i+1)$.

2.19. Рассмотрим группу S_3, и пусть $A = (1, 2) \in S_3$, $B = (1, 2, 3) \in S_3$. Прямым вычислением показать, что $S_3 = \{1, A, B, B^2, AB, AB^2\}$, причем $A^2 = 1$, $B^3 = 1$, $BA = AB^2$. (В частности, A и B порождают группу S_3.)

2.20. В группе S_4 рассмотрим циклы $R = (3, 4)$, $S = (1, 2, 3)$, $T = (1, 2, 3, 4)$. Доказать, что R, S и T порождают группу S_4. Проверить соотношения $R^2 = S^3 = T^4 = 1$, $RST = 1$.

2.21. Доказать, что S_4 порождается циклами $C = (1, 2)$, $D = (1, 2, 3, 4)$. Проверить соотношения $C^2 = D^4 = 1$, $(CD)^3 = 1$.

2.22. Доказать, что группа S_n порождается двумя циклами $X = (1, 2)$, $Y = (1, 2, \dots, n)$.

Определим для произвольной подстановки $\sigma \in S_n$ число (называемое *знаком подстановки* σ):

$$sgn(\sigma) = \prod_{n \ge i > j \ge 1} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

2.23. Доказать, что $sgn(\sigma) = \pm 1$, и что если

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix},$$

то $sgn(\sigma) = (-1)^r$, где r есть количество транспозиций в упорядоченной последовательности (перестановке) $(i_1, i_2, \dots, i_n)$, то есть количеству тех пар (i_s, i_t), для которых $s < t$, но $i_s > i_t$. В частности, $sgn(1) = +1$ (знак единичной подстановки равен единице).

2.24. Доказать, что для произвольных подстановок $\sigma\tau \in S_n$ имеет место равенство $sgn(\sigma\tau) = sgn(\sigma)sgn(t)$.

Указание. Можно начать с тождества

$$\prod_{n\geq i>j\geq 1} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{i-j} = \prod_{n\geq i>j\geq 1} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i)-\tau(j)} \prod_{n\geq i>j\geq 1} \frac{\tau(i)-\tau(j)}{i-j}.$$

Остается показать, что

$$\prod_{n\geq i>j\geq 1} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i)-\tau(j)} = \prod_{n\geq i>j\geq 1} \frac{\sigma(i)-\sigma(j)}{i-j}.$$

Для этого достаточно рассмотреть два случая: пусть $i > j$, тогда либо $\tau(i) > \tau(j)$, либо $\tau(i) < \tau(j)$.

Напомним, что соотношения $sgn(\sigma\tau) = sgn(\sigma)sgn(t)$ и $sgn(1) = 1$ означают, что отображение $sgn : S_n \longrightarrow \{+1, -1\}$ является *гомоморфизмом* из группы S_n в $\mathbf{U}_2 = \{\pm 1\}$.

2.25. Доказать, что $sgn((i,j)) = -1$ для любой транспозиции (i,j). (Указание: можно ограничиться случаем транспозиций вида $(i, i+1)$. Почему?)

2.26. Показать, что для любого цикла $\sigma = (i_1, i_2, \ldots, i_k)$ имеет место равенство $sgn(\sigma) = (-1)^{k-1}$. В частности, если k нечетно, то $sgn(\sigma) = +1$.

2.27. Пусть дано разложение произвольной подстановки $\sigma \in S_n$ в произведение независимых циклов: $\sigma = \sigma_1 \ldots \sigma_r$, и пусть t — количество неподвижных аргументов σ, то есть количество тех j, для которых $\sigma(j) = j$. Показать, что $sgn(\sigma) = (-1)^{n-(r+t)}$.

Пример 2.2. Вычислим знак подстановки σ из примера 1.1. В примере 1.1 было найдено разложение σ в произведение четырех независимых циклов, так что $r = 4$. Кроме того, один символ был неподвижным, то есть $t = 1$. Наконец, $n = 12$. Следовательно, $sgn(\sigma) = (-1)^{12-(4+1)} = (-1)^7 = -1$.

2.28. Положим $A_n = \{\sigma \in S_n | sgn(\sigma) = +1\}$. Доказать, что A_n — подгруппа группы S_n, и что $x\sigma x^{-1}$ для каждого $\sigma \in A_n$ и произвольного $x \in S_n$. Доказать, что A_n состоит в точности из тех подстановок, которые можно представить в виде произведения четного числа транспозиций.

Подстановка σ со свойством $sgn(\sigma) = +1$ называется *четной*, а если $sgn(\sigma) = -1$, то *нечетной*. Таким образом, циклы нечетной длины оказываются четными подстановками, а циклы четной длины — нечетными. Группа A_n называется группой четных подстановок n-й степени, или же *знакопеременной группой n-й степени*.

2.29. Зафиксируем транспозицию (i, j) (напомним, что это нечетная подстановка). Рассмотрим множество нечетных подстановок $S_n \setminus A_n$ и определим два отображения, $f : A_n \longrightarrow S_n \setminus A_n$ и $h : S_n \setminus A_n \longrightarrow A_n$, определяемых следующим образом: $f(\sigma) = (i, j)\sigma$, $h(\tau) = (i, j)\tau$. Доказать, что эти отображения определены корректно, т.е. если $\sigma \in S_n$, то $f(\sigma) \in S_n \setminus A_n$, а если $\tau \in S_n \setminus A_n$, то $h(\tau) \in A_n$. Далее, проверить, что f и h — взаимно обратные отображения. Вывести отсюда, что количество четных подстановок n-й степени равно $\frac{1}{2}n!$, и равно количеству нечетных подстановок n-й степени.

2.30. Найти в явном виде все элементы групп A_3 и A_4.

В следующей серии задач описываются множества образующих элементов групп четных подстановок.

2.31. Доказать, что группа A_n порождается циклами длины 3 ("тройными циклами").

Указание. Использовать задачи **2.8** и **2.28**.

2.32. Доказать, что при $n \geq 5$ любые два тройных цикла (j_1, j_2, j_3) и (i_1, i_2, i_3) связаны соотношением $(j_1, j_2, j_3) = x(i_1, i_2, i_3)x^{-1}$, где x — четная подстановка.

2.33. Доказать, что группа A_4 порождается элементами $S = (1, 2, 3)$ и $R = (1, 2)(3, 4)$. Проверить, что имеют место равенства $S^3 = R^2 = (SR)^3 = 1$.

2.34. Доказать, что группа A_5 порождается элементами $R = (1,2)(4,5)$ и $S = (1,3,4)$. Проверить , что имеют место равенства $S^3 = R^2 = (RS)^5 = 1$.

2.35. Доказать, что при четном $n > 3$ группа A_n порождается элементами $X = (1,2)(3,4,\ldots,n)$ и $Y = (1,2,3)$, а при нечетном $n > 3$ — элементами $Z = (3,4,\ldots,n)$ и $Y = (1,2,3)$.

Напомним, что матричной единицей называется матрица $E_{i,j}$, все элементы которой равны нулю, кроме $i\,j$-го, равного единице. Любая матрица A с элементами $a_{i\,j}$ однозначно представляется в виде $A = \sum\limits_{i,j=1}^{n} a_{i\,j}E_{i,j}$. Иными словами, матричные единицы являются базисом в пространстве всех $n \times n$-матриц. Основные свойства матричных единиц сформулированы в примере 1.10.

Пусть $\sigma \in S_n$. Сопоставим подстановке σ матрицу

$$M(\sigma) = \sum_{i=1}^{n} E_{\sigma(i),i}.$$

Иными словами, в i-м столбце матрицы $M(\sigma)$ единица находится в строке с номером $\sigma(i)$, все остальные элементы равны нулю. Например, если $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$, то

$$M(\sigma) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$M(\sigma)$ называется *матрицей подстановки* σ.

2.36. Доказать, что $M(1_n) = E_n$, $M(\sigma\tau) = M(\sigma)M(\tau)$, $M(\sigma^{-1}) = M(\sigma)^{-1} = {}^tM(\sigma)$, а отображение $\sigma \mapsto M(\sigma)$ инъективно.

Таким образом, отображение, сопоставляющее подстановке σ матрицу $M(\sigma)$, является гомоморфизмом из группы S_n в группу $GL_n(F)$, где в качестве F можно взять любое поле (или даже кольцо, так как требуется только наличие в F несовпадающих нуля и единицы). В следующей задаче можно предполагать, что $F = \mathbb{Q}$ — поле рациональных чисел.

2.37. Доказать, что для любой подстановки $sgn(\sigma) = det(M(\sigma))$.

3. Смежные классы, классы сопряженных элементов, порядки

Теоретической основой для задач этого раздела является следующая конструкция. Дана группа G, множество X, и отображение

$$G \times X \longrightarrow X,$$

которое переводит пару элементов (g, x) в элемент $gx \in X$. При этом должны выполняться два свойства:

1) $(g_1 g_2)x = g_1(g_2 x)$ для всех $g_1, g_2 \in G$, $x \in X$;

2) $1x = x$ для любого $x \in X$. Здесь $1 \in G$ — единица группы G.

Если эти свойства выполняются, то говорят, что задано *действие* группы G на множестве X, или что *группа G действует на множестве X*. Точнее, таким образом определяется *левое действие* (группа G действует слева на множестве X). *Правое действие* определяется аналогично: задается отображение вида $X \times G \to X$, $(x, g) \mapsto xg$, и должны выполняться два свойства: $x(g_1 g_2) = (xg_1)g_2$ и $x1 = x$. Свойства правого действия полностью аналогичны свойствам левого действия, и не нуждаются в отдельных доказательствах. Это вытекает, в частности, и из следующего утверждения:

3.1. Пусть задано левое действие G на X. Введем обозначение $xg = g^{-1}x$. Доказать, что отображение $X \times G \to X$, задаваемое формулой $(x, g) \mapsto xg = g^{-1}x$, является правым действием G на X. Аналогичным образом по правому действию можно построить левое действие: $gx = xg^{-1}$. Этим задается взаимно-однозначное соответствие между левыми и правыми действиями G на X.

Важно помнить, что операция "умножения" $(g, x) \mapsto gx$ может в конкретных частных случаях задаваться самыми разными способами и по-разному обозначаться. Рассмотрим несколько примеров.

3.2. Пусть Y — произвольное множество, $X = Y^n$, $G = S_n$. Для $g \in G$ и $x = (y_1, y_2, \ldots, y_n)$ положим $gx = (y_{g^{-1}(1)}, y_{g^{-1}(2)}, \ldots, y_{g^{-1}(n)})$. Доказать, что это — левое действие S_n на $X = Y^n$. Далее, положим $xg = (y_{g(1)}, y_{g(2)}, \ldots, y_{g(n)})$. Проверить, что эта формула определяет правое действие S_n на Y^n.

3.3. Допустим, что X — группа, а G — подгруппа группы X. Показать, что умножение (в группе X) элементов G слева на элементы X определяет левое действие G на X. (В этом случае принято говорить, что G действует на X *левыми сдвигами*.) Аналогично, умножение элементов G справа на элементы X задает правое действие G на X — действие *правыми сдвигами*.

Элементы x и gxg^{-1} принято называть *сопряженными*. Сопряженными будут также элементы x и $g^{-1}xg = yxy^{-1}, y = g^{-1}$.

3.4. Пусть опять G — подгруппа группы X. Для $g \in G$, $x \in X$ положим ${}^g x = gxg^{-1}$. Тем самым определено отображение $G \times X \to X$, $(g, x) \mapsto {}^g x$. Показать, что это — левое действие G на X (говорят, что G действует сопряжениями на X). Аналогично, можно определить правое действие $(x, g) \mapsto x^g = g^{-1}xg$.

Вернемся на некоторое время вновь к произвольному левому действию G на X. Пусть $x \in X$. Обозначим через Gx множество всех элементов вида gx, где g пробегает всю группу G. Это множество называется *орбитой* действия группы G на множестве X. Элемент x называется *представителем* орбиты Gx. Из определения следует, что орбита полностью задается своим представителем. В следующем упражнении сформулированы основные свойства орбит.

3.5. 1) $x \in Gx$;

2) если $y \in Gx$, то $Gy = Gx$ (представителем орбиты может быть любой ее элемент);

3) если Gx и Gy — две орбиты, то либо $Gx = Gy$, либо Gx и Gy не пересекаются;

4) множество X можно представить в виде объединения попарно непересекающихся орбит.

3.6. Рассмотрим произвольную подстановку $\sigma \in S_n$, и пусть $G = \langle\sigma\rangle$ — циклическая подгруппа группы S_n, порожденная элементом σ. Положим $X = \{1, 2, \ldots, n\}$, и определим отображение $G \times X \to X$, полагая $\sigma^k i$ равным $s^k(i)$, т.е. значению подстановки (отображения) σ^k на аргументе i. Докажите, что это действие группы G на множестве X.

Пусть $\sigma = \sigma_1 \ldots \sigma_r$ — разложение подстановки σ в произведение независимых циклов, и пусть X_j есть множество перемещаемых символов цикла σ_j для всех $j = 1, \ldots, r$. Пусть $\{x_{i_1}, \ldots, x_{i_t}\}$ — множество неподвижных символов σ (возможно, пустое). Положим $X_{r+1} = \{x_{i_1}\}$, $X_{r+2} = \{x_{i_2}\}$, $\ldots$, $X_{r+t} = \{x_{i_t}\}$. Докажите, что множества X_1, $\ldots$, X_r, X_{r+1}, $\ldots$, X_{r+t} являются орбитами построенного только что действия.

Рассмотрим подробно случай, когда подгруппа G действует сдвигами на группе X. Орбиты этого действия называются *смежными классами* группы X по подгруппе G. Если G действует левыми сдвигами, то соответствующие смежные классы называются *правыми смежными классами* X по G, а если правыми сдвигами — то *левыми смежными классами.* Итак, правые смежные классы имеют вид $Gx = \{gx | g \in G\}$, а левые — $xG = \{xg | g \in G\}$. Для смежных классов имеют место все свойства орбит, сформулированные в предыдущей задаче.

3.7. Пусть X — группа, а G — ее подгруппа, $x, y \in G$, $z, w \in X$.

1) $Gx = G$ $(xG = G)$ тогда и только тогда, если $x \in G$;

2) $Gx = Gy$ $(xG = yG)$ тогда и только тогда, если $xy^{-1} \in G$ (соответственно, если $x^{-1}y \in G$).

3) Отображения $z \mapsto zx$ и $w \mapsto wx^{-1}$ являются взаимно обратными биекциями между G и Gx. В частности, равны мощности множеств G и Gx для всех x. Сформулируйте и докажите аналогичные утверждения для левых смежных классов.

4) Пусть $Gx_1, Gx_2, \ldots$ — множество всех различных (именно различных) правых смежных классов X по G. Тогда $x_1^{-1}G, x_2^{-2}G, \ldots$ — множество всех различных левых смежных классов X по G. В частности, мощность множества всех различных правых смежных

классов X по G равна мощности множества всех различных левых смежных классов.

Напомним, что мощность $|G|$ группы G называется *порядком* группы, а смежных классов группы G по ее подгруппе H (оно одинаково и для левых, и для правых классов) называется *индексом группы G по подгруппе H*, и обозначается через $|G : H|$. Из результата предыдущей задачи легко выводится следующая теорема.

Теорема 3.1. (Лагранж) $|G| = |G : H| \cdot |H|$, *если группа G конечна.*

Таким образом, порядок группы делится нацело на порядок любой ее подгруппы.

3.8. Пусть K и H — конечные подгруппы группы G, причем НОД$(|K|, |H|) = 1$. Доказать, что тогда $K \cap H = \{1\}$.

Чтобы вычислить в явном виде множество всех различных смежных классов группы G по подгруппе H, часто бывает достаточно найти в каждом классе по одному представителю. Будем говорить об этом множестве как о *полной системе представителей смежных классов* (правых или левых) G по H, или (кратко) как о полной системе представителей G по H.

3.9. Доказать, что множество $K = \{g_i | i \in I\}$ элементов группы G является полной системой представителей правых смежных классов G по H тогда и только тогда, если выполняются два условия:

1) $g_i g_j^{-1} \notin H$ для любых двух различных $g_i, g_j \in Z$;

2) для каждого $g \in G$ существуют элементы $h \in H$ и $g_i \in Z$ такие, что $g = hg_i$ (это еще можно выразить в форме $G = HK$.

Доказать, что если условия 1) и 2) выполняются, то представление элемента $g \in G$ в виде произведения $g = hg_i$, где $h \in H$, $g_i \in K$, явлеется единственно возможным.

Сформулировать и доказать аналогичное утверждение для полной системы представителей левых смежных классов G по H.

Из этих фактов можно сделать следующий вывод. Если G — группа, H — ее подгруппа, и K — полная система представителей правых смежных классов G по H, то существует взаимно-однозначное соответствие между G и прямым произведением множеств $H \times K$. Оно устанавливается отображением $g \mapsto (h, g_i)$, где $h \in H$ и $g_i \in K$ — элементы, существование которых утверждается в пункте 2) предыдущей задачи. Обратное отображение выглядит так: $(h, g_j) \mapsto hg_j$. Таким образом, выбор полной системы представителей K приводит к появлению в группе G своего рода "системы координат": подгруппа H играет роль одной координатной оси, а другая координатная ось — это множество K.

Особый интерес представляют случаи, когда можно выбрать такую полную систему представителей, которая сама является подгруппой группы G.

3.10. Пусть дана группа G и две ее подгруппы H и K. Допустим, что выполнены два условия:

1) $H \cap K = \{1\}$;

2) $G = HK$.

Докажите, что множество K является полной системой представителей правых смежных классов G по H, а множество H — полной системой представителей левых смежных классов G по K.

Как надо изменить формулировку, чтобы получить аналогичное утверждение для случая правых смежных классов?

Докажите, что равенство $G = HK$ равносильно равенству $G = KH$.

3.11. Пусть дана конечная группа G и две ее подгруппы H и K. Допустим, что $H \cap K = \{1\}$. Доказать, что тогда из $|G| = |K| \cdot |H|$ следует $G = HK = HK$.

В некоторых дальнейших задачах рассматриваемые группы *коммутативны* (т.е. для любых элементов a, b выполнено равенство $ab = ba$). Для коммутативных групп правые смежные классы совпадают с левыми, т.е. $Hx = xH$ для всех $x \in G$ и любой подгруппы H.

Определим некоторые группы и их подгруппы, которые будут встречаться далее в задачах этого и следующего разделов. Все эти группы коммутативны.

Пусть $\mathbb{R}$ — множество всех действительных чисел, $\mathbb{C}$ — множество всех комплексных чисел. Это поля и, следовательно, группы по сложению, нейтральными элементами которых являются нули. Через $\mathbb{R}^2$, как обычно, обозначается множество пар упорядоченных пар (r_1, r_2), где r_1, r_2 — действительные числа. Это векторное (линейное) пространство над полем $\mathbb{R}$, которое изображается обычно как плоскость. Любое векторное пространство (а значит, и $\mathbb{R}^2$) является группой по сложению.

Обозначим через $\mathbb{R}^*$ и $\mathbb{C}^*$ множества ненулевых элементов в $\mathbb{R}$ и $\mathbb{C}$. Это группы по умножению, нейтральные элементы в них — единицы. В $\mathbb{R}^*$ содержится подгруппа $\mathbb{R}_+$ всех положительных действительных чисел.

Положим $\mathbf{U} = \{u \in \mathbb{C} \mid |u| = 1\}$ (множество комплексных чисел, модуль которых равен единице), $\mathbf{U}_n = \{u \in \mathbb{C} \mid u^n = 1\}$ (множество корней n-й степени из единицы), $\mathbf{K}_n = \{z \in \mathbb{C} \mid z^n \in \mathbb{R}_+\}$. (Заметим, что обозначение $\mathbf{K}_n$, в отличие от всех остальных, не является общеупотребительным.)

3.12. Доказать, что $\mathbf{U}$, $\mathbf{U}_n$, $\mathbf{K}_n$ — подгруппы группы $\mathbb{C}^*$. Изобразить на плоскости множества $\mathbf{U}$, $\mathbf{U}_2$, $\mathbf{U}_3$, $\mathbf{U}_4$.

В следующих задачах желательно дать и аналитическое, и графическое решение (в виде рисунка).

3.13. Найти смежные классы группы $G = \mathbb{R}^2$ по подгруппе $H = \{(r, 0) |\ r \in \mathbb{R}\}$, и по подгруппе $K = \{(0, r) |\ r \in \mathbb{R}\}$. (Найти полные системы представителей смежных классов и описать классы целиком как множества.)

3.14. Найти смежные классы группы $G = \mathbb{C}^*$ по подгруппе $H = \mathbf{U}$, и по подгруппе $K = \mathbb{R}_+$. (Найти полные системы представителей смежных классов и описать классы целиком как множества.)

Легко проверяется, что $\mathbf{U}_n \subset \mathbf{U}_{kn}$, $\mathbf{U}_2 = \{+1, -1\}$, $\mathbf{U}_4 = \{+1, -1, +i, -i\}$, $\mathbf{U}_n \subset \mathbf{K}_n$, $\mathbb{R}_+ \subset \mathbf{K}_n$.

3.15. Найти явный вид элементов $\mathbf{K}_n$. В частности, показать, что $\mathbf{K}_2 = \mathbb{R}^*$. Изобразить графически $\mathbf{K}_2$, $\mathbf{K}_3$, $\mathbf{K}_4$, $\mathbf{K}_6$.

3.16. Рассмотрим множество $\{z \in \mathbb{C}^* \mid z^n \in \mathbb{R}^* \}$. Доказать, что это группа, и что она совпадает с $\mathbf{K}_{2n}$.

3.17. Положим $G = \mathbf{K}_n$, $H = \mathbf{U}_n$, $K = \mathbb{R}_+$. Найти смежные классы G по H и G по K.

3.18. Пусть $G = \mathbf{U}_6$, $H = \mathbf{U}_3$, $K = \mathbf{U}_2$. Найти смежные классы G по H и G по K.

3.19. Пусть $G = \mathbf{U}_{15}$, $H = \mathbf{U}_3$. Найти смежные классы G по H. (Картинку можно не рисовать.) В этой задаче удобно отвлечься от конкретного вида элементов $\mathbf{U}_{15}$, а выбрать какой-то x — первообразный корень из единицы 15-й степени, и тогда все элементы $\mathbf{U}_{15}$ — это множество $\{1, x, x^2, x^3, \ldots, x^{14}\}$, а подгруппа $\mathbf{U}_3$ состоит из элементов $\{1, x^5, x^{10}\}$ (докажите это!). Теперь будет нетрудно выписать все смежные классы в явном виде, и полную систему представителей смежных классов. Нельзя ли выбрать полной системой представителей какую-нибудь подгруппу группы $\mathbf{U}_{15}$?

3.20. Решить аналогичную задачу для $G = \mathbf{U}_{16}$ и $H = \mathbf{U}_4$.

3.21. Аналогично предыдущим задачам, пусть x — первообразный корень из единицы n-й степени. Тогда $\mathbf{U}_n = \{1, x, x^2, \ldots, x^{n-1}\}$. Пусть $n = mk$. Какие степени элемента x составляют подгруппу $\mathbf{U}_m$ группы $\mathbf{U}_n$? Найти смежные классы $\mathbf{U}_{mk}$ по $\mathbf{U}_m$ явно, и какую-нибудь полную систему представителей для этих смежных классов. Когда можно выбрать в качестве системы представителей подгруппу группы $\mathbf{U}_{mk}$?

Напомним, что группа G, все элементы которой можно выразить в виде степеней одного элемента, называется *циклической*, и что все бесконечные циклические группы изоморфны группе (по сложению) всех целых чисел $\mathbb{Z}$, а любая конечная циклическая группа порядка n изоморфна группе $\mathbf{U}_n$. Таким образом, в предыдущих задачах фактически был разобран общий случай конечных циклических групп.

Рассмотрим теперь несколько задач с некоммутативными группами.

3.22. Рассмотрим в группе S_4 подмножество $V_4 = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ и подмножество K, состоящее из всех подстановок вида

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ * & * & * & 4 \end{pmatrix}.$$

Доказать, что V_4 и H — подгруппы, и что $H \cong S_3$. Чему равно множество $V_4 \cap H$? Используя предыдущую задачу, найти полную систему представителей смежных классов (правых или левых) S_4 по V_4. Найти в явном виде и правые, и левые смежные классы S_4 по V_4. Заметим, что в старых книгах подгруппу V_4 иногда называют “четверной группой Клейна".

Рассмотрим матрицы

$$a = \begin{pmatrix} \cos\dfrac{2\pi}{n} & -\sin\dfrac{2\pi}{n} \\ \sin\dfrac{2\pi}{n} & \cos\dfrac{2\pi}{n} \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Группа D_n, порожденная этими двумя матрицами, называется *группой диэдра* n-й степени, и состоит из $2n$ элементов:

$$1, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b.$$

Здесь единица означает единичную матрицу. При этом выполняются соотношения: $a^n = b^2 = 1$, $ba = a^{n-1}b$. Последнее соотношение, ввиду равенства $a^{-1} = a^{n-1}$, равносильно соотношению $(ab)^2 = 1$. Подробное обоснование того, что группа D_n устроена именно таким образом, можно найти в книге [24] на с. 319 – 320.

3.23. Рассмотрим в D_n подмножество $H = \{1, b\}$. Доказать, что это подгруппа, и найти в явном виде левые и правые смежные классы D_n по H. Существует ли подгруппа K со свойствами $H \cap K = \{1\}$ и $HK = D_n$?

Лемма 3.1. *Пусть H — подгруппа группы G. Тогда эквивалентны следующие три условия:*

1) $xH = Hx$ *для каждого* $x \in G$;

2) $xHx^{-1} = H$ *для любого* $x \in G$;

3) $xHx^{-1} \subseteq H$ *для любого* $x \in G$.

Доказательство. Здесь используются свойства умножения подмножеств группы, описанные в примере 1.5. В частности, используется ассоциативность этого умножения. Допустим, что $xH = Hx$ для каждого $x \in G$. Умножим обе части этого равенства справа на x^{-1}, и

получим равенство $xHx^{-1} = H$. Очевидно, что из условия 2) следует условие 3). Покажем, что из 3) следует 2). Здесь необходимо убедиться, что если $xHx^{-1} \subseteq H$ для всех x, то $H \subseteq xHx^{-1}$. Здесь ключевую роль играет условие "для всех x". "Для всех $x \in G$" означает, что в том числе и для x^{-1}. Заменяя x на x^{-1}, получаем, что из 3) следует $x^{-1}H(x^{-1})^{-1} = x^{-1}Hx \subseteq H$. Умножая слева на x, а справа на x^{-1}, получим требуемое включение $H \subseteq xHx^{-1}$. Осталось показать, что из условия 2) следует условие 1). И снова берем равенство $xHx^{-1} = H$, и умножаем его справа на x. Получим требуемое равенство $xH = Hx$. $\square$

Подгруппа H группы G называется *нормальной*, если выполняется любое из эквивалентных условий 1), 2), 3) этой леммы. Любая подгруппа коммутативной группы является нормальной подгруппой.

3.24. Доказать, что если подгруппа H группы G является нормальной, $x, y \in G$, и $xy \in H$, то и $yx \in H$.

3.25. Доказать, что подгруппа V_4 группы S_4 является нормальной, а подгруппа H (из той же задачи, где была введена V_4) нормальной не является.

3.26. Доказать, что каждая подгруппа H группы G такая, что $|G : H| = 2$, является нормальной. Доказать, что для всех n имеет место равенство $|S_n : A_n| = 2$, так что все знакопеременные подгруппы нормальны.

3.27. Доказать, что если H — нормальная подгруппа группы G, а K — произвольная подгруппа, то $HK = KH$, и это множество является подгруппой группы G.

3.28. Доказать, что если H и K — нормальные подгруппы группы G, и $K \cap H = \{1\}$, то $xy = yx$ для любых $x \in K$ и $y \in H$.

3.29. Доказать, что если H и K — нормальные подгруппы группы G, то нормальными подгруппами будут также $H \cap K$ и HK. Доказать, что пересечение произвольного семейства нормальных подгрупп также будет нормальной подгруппой.

3.30. Доказать, что унитреугольная группа $UT_n(F)$ является нормальной подгруппой треугольной группы $T_n(F)$ (определения этих групп см. в разделе 1).

3.31. Доказать, что группы $UT_n^m(F)$ являются нормальными подгруппами треугольной группы $T_n(F)$ (определения этих групп см. в разделе 1).

3.32. В произвольной группе G рассмотрим множество $C(G) = \{x \in G \mid xg = gx \text{ для всех } g \in G\}$. Доказать, что $C(G)$ — нормальная подгруппа группы G.

Подгруппа $C(G)$ называется *центром* группы G. Группа G коммутативна тогда и только тогда, если $C(G) = G$.

3.33. Доказать, что $C(S_n) = \{1\}$.

3.34. Рассмотрим группу $GL_n(F)$ всех квадратных невырожденных $n \times n$-матриц над полем F. Доказать, что центр $GL_n(F)$ состоит из всех скалярных невырожденных матриц, т.е. из матриц, все диагональные компоненты которых равны одному и тому же ненулевому элементу F, а недиагональные компоненты равны нулю.

3.35. Рассмотрим группу Q_8 (называемую *группой кватернионов*), состоящую из элементов $1, a, a^2, a^3, b, ab, a^2b, a^3b$. При этом должны быть выполнены соотношения: $a^4 = 1$, $a^2 = b^2$, $ba = a^2b$. Показать, что центр Q_8 состоит из элементов 1 и $a^2 = b^2$.

Рассмотрим произвольную группу G, и ее подмножество X. Положим $\bar{X} = \{gxg^{-1} | x \in X, g \in G\}$, и рассмотрим подгруппу $\langle \bar{X} \rangle$, порожденную множеством $\bar{X}$.

3.36. Доказать, что $\langle \bar{X} \rangle$ — нормальная подгруппа группы G.

3.37. Доказать, что если H — какая-нибудь подгруппа группы G, и $X \subseteq H$, то $\langle \bar{X} \rangle \subseteq H$. Вывести отсюда, что $\langle \bar{X} \rangle$ является пересечением всех нормальных подгрупп группы G, содержащих подмножество X.

Будем называть $\langle \bar{X} \rangle$ *нормальной подгруппой группы* G, *порожденной множеством* X. Рассмотрим подробнее нормальную подгруппу группы G, порожденную всеми коммутаторами, то есть элементами $[x, y] = xyx^{-1}y^{-1}$. Эта нормальная подгруппа обозначается через $[G, G]$, и называется *коммутантом* группы G. Так как $[x, y] = 1$ тогда и только тогда, если $xy = yx$, то в коммутативных группах коммутант тривиален: это подгруппа, состоящая из одного единичного (нейтрального) элемента.

3.38. Доказать, что подгруппа, порожденная всеми коммутаторами, совпадает с нормальной подгруппой, пороженной всеми коммутаторами, т.е. с коммутантом.

Указание. Проверить тождество $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$, и использовать его.

3.39. Проверить тождество $[x, y]^{-1} = [y, x]$. Доказать, используя его, что элементы коммутанта — это всевозможные произведения коммутаторов:

$$[x_1, y_1][x_2, y_2] \dots [x_n, y_n], \quad n \geq 0.$$

3.40. Проверить, что $[S_2, S_2] = 1$, $[A_3, A_3] = 1$.

3.41. Доказать, что $[S_n, S_n] = A_n$ для всех n.

3.42. Доказать, что $[A_4, A_4] = V_4$. Напомним, что

$$V_4 = \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

3.43. Доказать, что при $n \geq 5$ имеет место равенство $[A_n, A_n] = A_n$.

3.44. Пусть F есть одно из полей $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Доказать, что

$$[GL_n(F), GL_n(F)] = SL_n(F)$$

для всех $n \geq 1$.

3.45. Пусть F есть одно из полей $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Доказать, что

$$[SL_n(F), SL_n(F)] = SL_n(F)$$

для всех $n \geq 1$.

3.46. Пусть снова F есть одно из полей $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Доказать, что $[T_n(F), T_n(F)] = UT_n(F)$ для всех $n \geq 1$.

3.47. При тех же предположениях относительно поля F доказать, что $[UT_n^r(F), UT_n^s(F)] = UT_n^{r+s}(F)$ для всех n, m, r, s.

3.48. Найти коммутант группы кватернионов Q_8.

Рассмотрим далее подробно действие группы G на самой себе сопряжениями. Орбита элемента x в этом случае есть множество $\{gxg^{-1} \mid g \in G$. Эти орбиты называются *классами сопряженных элементов* группы G. Как следует из общих свойств орбит, любые два класс сопряженных элементов либо не пересекаются, либо совпадают. Если G конечна, то известно, что количество элементов в каждом классе сопряженных элементов делит порядок группы (это будет доказано в разделе 5). Если группа коммутативна, то каждый класс сопряженных элементов состоит из одного элемента. Как уже фактически известно (см. раздел 2), в группах S_n классами сопряженных элементов являются множества подстановок, имеющих одинаковое циклическое строение. На первом курсе доказывается, что в группе $GL_n(\mathbb{C})$ две матрицы A и B принадлежат одному классу сопряженных элементов (т.е. $B = XAX^{-1}$) тогда и только тогда, если A и B имеют одну и ту же жорданову нормальную форму (один и тот же набор жорданаовых клеток). Из этих примеров видно, что классы сопряженных элементов группы содержат элементы, обладающие некоторыми общими свойствами.

3.49. Доказать, что подгруппа H группы G нормальна тогда и только тогда, если является объединением нескольких классов сопряженных элементов. Если H состоит из более чем одного элемента, то в этом объединении не менее двух классов (почему?).

3.50. Доказать, что центр $C(G)$ группы G является объединением всех тех классов сопряженных элементов, которые состоят в точности из одного элемента.

3.51. Найти в явном виде классы сопряженных элементов группы кватернионов Q_8.

3.52. Установить следующие соотношения между элементами группы диэдра D_n:

$$(a^k b)a^r(a^k b)^{-1} = a^{-r} = a^{n-r},\ ba^r = a^{n-r}b,$$
$$(a^k b)b(a^k b)^{-1} = a^{2k}b,\ (a^k b)ab(a^k b)^{-1} = a^{2k-1}b.$$

3.53. Доказать, что при $n = 2m$ классами сопряженных элементов D_n являются множества:

$$\{1\},\ \{a^m\}, \{a^k, a^{2m-k}\}, 1 \le k \le m-1,$$
$$\{b, a^2b, a^4b, \ldots, a^{2m-2}b\}, \{ab, a^3b, a^5b, \ldots, a^{2m-1}b\}.$$

3.54. Доказать, что при $n = 2m+1$ классами сопряженных элементов D_n являются множества:

$$\{1\},\ \{a^k, a^{2m+1-k}\}, 1 \le k \le m,$$
$$\{b, ab, a^2b, a^3b, a^4b, \ldots, a^{2m-1}b, a^{2m}b\}.$$

Отсюда, в частности, следует, что центр D_{2m} — это подгруппа $\{1, a^m\}$, а центр D_{2m+1} состоит только из единицы.

3.55. Найти явно смежные классы группы D_{2m} по ее центру $H = \{1, a^m\}$.

3.56. Вычислить коммутант $[D_n, D_n]$ группы диэдра.

Напомним, что *порядок* элемента g группы G — это наименьшее целое положительное число n, такое, что $x^n = 1$. Если такого $n > 0$ найти нельзя, то говорят, что порядок g бесконечен. Порядок нейтрального элемента группы равен единице. В конечной группе порядки всех элементов конечны. В дальнейшем рассматриваются только элементы конечного порядка. Название “порядок"согласуется с тем, что число n равно порядку подгруппы $\langle g \rangle$, порожденной элементом g: $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$.

Лемма 3.2. 1) *Если n — порядок g, и $g^m = 1$, то m делится на n без остатка. Если $g^k = g^l$, то $k - l$ делится на n.*

2) *Если элемент g имеет бесконечный порядок, то из $g^k = g^l$ следует $k = l$.*

Из теоремы Лагранжа следует простое, но важное утверждение:

Теорема 3.2. *В конечной группе G порядок любого элемента делит порядок группы. В частности, для каждого $g \in G$ имеет место равенство $g^{|G|} = 1$.*

3.57. Доказать, что если порядок $g \in G$ равен mk, то порядок g^k равен m.

3.58. В общем случае, если порядок g равен n, то порядок g^k равен $\frac{n}{\text{НОД}(n,k)}$.

3.59. Пусть x, y — элементы группы G такие, что $xy = yx$, и пусть n — порядок x, а m — порядок y. Доказать, что если n и m взаимно просты (т.е. $\text{НОД}(n,m) = 1$), то порядок элемента xy равен nm.

3.60. Показать, что порядок элемента g равен порядку элемента xgx^{-1}.

3.61. Показать, что порядок xy равен порядку yx.

3.62. Показать, что один и тот же порядок имеют элементы xyz, zxy и yzx.

3.63. Доказать, что если порядок каждого неединичного элемента группы равен двум, то группа коммутативна.

3.64. Чему равны порядки элементов $a^k b$ в группе диэдра D_n?

3.65. Доказать, что группы Q_8 и D_4 не изоморфны. (На первый взгляд, эта задача никак не связана с темой порядков. Однако наиболее простое решение основано на том, что у изоморфных групп должно быть одинаковое количество элементов одних и тех же порядков. Остается подсчитать количество элементов порядка 2 в группах Q_8 и D_4, и сделать выводы.)

3.66. Если G — некоммутативная группа из 6 элементов, то $G \cong S_3$. (Указание: расмотреть в G элементы порядков 2 и 3. Почему обязательно должны существовать элементы таких порядков? Какие соотношения между ними обязательно должны выполняться?)

3.67. Пусть для $\sigma \in S_n$ известно разложение σ в произведение независимых циклов $\sigma = \sigma_1\sigma_2 \dots \sigma_m$, и пусть для всех i, $1 \leq m$ длина цикла σ_i равна k_i. Доказать, что порядок σ равен наименьшему общему кратному чисел $k_1, \dots, k_m$.

В следующей серии заданий даны группы из 16 элементов, указаны порождающие их элементы, и выписано явное задание всех остальных элементов в виде произведений порождающих элементов. Указаны также соотношения между порождающими элементами, с помощью которых можно вычислить произведения и обратные элементы для всех элементов группы.

3.68. Дана группа G с элементами

$$1, S, S^2, S^3, S^4, S^5, S^6, S^7, T, ST, S^2T, S^3T, S^4T, S^5T, S^6T, S^7T,$$

которые удовлетворяют следующим соотношениям:

$$S^8 = T^2 = 1,\ TS = S^3T.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $X = ST$.
4) Найти левые и правые смежные классы G по $H = \langle X \rangle$.
5) Найти коммутант $[G, G]$.

3.69. Дана группа G с элементами

$$1, S, S^2, S^3, S^4, S^5, S^6, S^7, T, ST, S^2T, S^3T, S^4T, S^5T, S^6T, S^7T,$$

которые удовлетворяют следующим соотношениям:

$$S^8 = T^2 = 1,\ TS = S^5T.$$

1) Найти в явном виде классы сопряженных элементов G.

2) Найти центр G.
3) Найти порядок элемента $X = S^2T$
4) Найти левые и правые смежные классы G по $H = \langle X \rangle$.
5) Найти коммутант $[G, G]$.

3.70. Дана группа G с элементами

$$1, S, S^2, S^3, T, T^2, T^3, TS, TS^2, TS^3, T^2S, T^2S^2, T^2S^3, T^3S, T^3S^2, T^3S^3,$$

которые удовлетворяют следующим соотношениям:

$$S^4 = T^4 = 1, ST = TS^3.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $X = TS$.
4) Найти левые и правые смежные классы G по $H = \langle X \rangle$.
5) Найти коммутант $[G, G]$.

3.71. Дана группа G с элементами

$$1, R, R^2, R^3, S, S^2, S^3, SR, SR^2, SR^3, S^2R, S^2R^2, S^2R^3, S^3R, S^3R^2, S^3R^3,$$

которые удовлетворяют следующим соотношениям:

$$R^4 = S^4 = 1, RS = S^3R^3, R^3S = S^3R.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $X = SR^2$.
4) Найти левые и правые смежные классы G по $H = \langle X \rangle$.
5) Найти коммутант $[G, G]$.

3.72. Дана группа G с элементами

$$1, R, S, T, RS, RT, TR, SR, ST, TS, A, A^2, A^3, B, C, D,$$

которые удовлетворяют следующим соотношениям:

$$R^2 = S^2 = T^2 = 1, RST = TRS = STR, (RST)^4 = 1,$$
$$TRT = SRS, RTR = STS, TST = RSR,$$
$$A = RST, B = TRT, C = RTR, D = TST.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $X = RS$.
4) Найти левые и правые смежные классы G по $H = \langle X \rangle$.
5) Найти коммутант $[G, G]$.

Указание: доказать предварительно, что $AR = RA$, $AS = SA$, $AT = TA$.

3.73. Дана группа G с элементами

$$1, S, S^2, S^3, S^4, S^5, S^6, S^7, T, ST, S^2T, S^3T, S^4T, S^5T, S^6T, S^7T,$$

которые удовлетворяют следующим соотношениям:

$$S^8 = T^4 = 1, S^4 = T^2, TS = S^7T, ST = TS^7.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $X = ST$.
4) Найти левые и правые смежные классы G по $H = \langle X \rangle$.
5) Найти коммутант $[G, G]$.

3.74. Дана группа G с элементами

$$1, S, S^2, S^3, S^4, S^5, S^6, S^7, X, SX, S^2X, S^3X, S^4X, S^5X, S^6X, S^7X,$$

которые удовлетворяют следующим соотношениям:

$$S^8 = X^4 = 1, S^4 = X^2, XS = S^3X.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $Y = S^2X$.
4) Найти левые и правые смежные классы G по $H = \langle Y \rangle$.
5) Найти коммутант $[G, G]$.

3.75. Дана группа G с элементами

$$1, S, S^2, S^3, S^4, S^5, S^6, S^7, X, SX, S^2X, S^3X, S^4X, S^5X, S^6X = X^3, S^7X,$$

которые удовлетворяют следующим соотношениям:

$$S^8 = X^8 = 1, X^2 = S^6, X^4 = S^4, X^6 = S^2, XS = S^5X.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $Y = SX$.
4) Найти левые и правые смежные классы G по $H = \langle Y \rangle$.
5) Найти коммутант $[G, G]$.

3.76. Дана группа G с элементами

$$1, X, Y, Z, XY, XZ, YZ, (YZ)^2, (YZ)^3,$$
$$YZY, ZYZ, XYZ, XZY, XYZY, XZYZ, X(YZ)^2,$$

которые удовлетворяют следующим соотношениям:

$$X^2 = Y^2 = Z^2 = 1, XY = YX, XZ = ZX, ZY = (YZ)^3.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $S = YZ$.
4) Найти левые и правые смежные классы G по $H = \langle S \rangle$.
5) Найти коммутант $[G, G]$.

3.77. Дана группа G с элементами

$$1, S, S^2, S^3, S^4, S^5, S^6, S^7, R, SR, S^2R, S^3R, S^4R, S^5R, S^6R, S^7R,$$

которые удовлетворяют следующим соотношениям:

$$S^8 = R^4 = 1, S^4 = R^2, RS^2 = S^2R^3, RS^3 = S^5R.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $X = RS^2$.
4) Найти левые и правые смежные классы G по $H = \langle X \rangle$.
5) Найти коммутант $[G, G]$.

3.78. Дана группа G с элементами

$$1, R, S, T, R^2, R^3, S^3, S^3, RS, SR, TR, TS, TR^2, TRS, TR^3, TS^3, TSR,$$

которые удовлетворяют следующим соотношениям:

$$R^4 = T^2 = 1, R^2 = S^2 = (RS)^2, RT = TR, TS = ST.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $X = TSR$.
4) Найти левые и правые смежные классы G по $H = \langle X \rangle$.
5) Найти коммутант $[G, G]$.

3.79. Дана группа G с элементами

$$1, A, B, A^2, A^3, A^4, A^5, A^6, A^7, B, AB, A^2B, A^3B, A^4B, A^5B, A^6B, A^7B,$$

которые удовлетворяют следующим соотношениям:

$$A^8 = B^2 = 1, BA^7 = A^5B.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $X = A^5B$.
4) Найти левые и правые смежные классы G по $H = \langle X \rangle$.
5) Найти коммутант $[G, G]$.

3.80. Дана группа G с элементами

$$1, P, Q, P^2, P^3, P^4, P^5, P^6, P^7, Q, PQ, P^2Q, P^3Q, P^4Q, P^5Q, P^6Q, P^7Q,$$

которые удовлетворяют следующим соотношениям:

$$P^8 = Q^2 = 1, QP^7 = P^3Q.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $X = P^6Q$.
4) Найти левые и правые смежные классы G по $H = \langle X \rangle$.
5) Найти коммутант $[G, G]$.

3.81. Дана группа G с элементами

$$1, U, U^2, U^3, V, V^2, V^3, VU, VU^2, VU^3, V^2U, V^3U, V^3U^2, V^2U^2, V^2U^3, V^3U^3,$$

которые удовлетворяют следующим соотношениям:

$$U^4 = V^4 = 1, U^3V^3 = V^3U.$$

1) Найти в явном виде классы сопряженных элементов G.

2) Найти центр G.

3) Найти порядок элемента $X = V^3U^3$.

4) Найти левые и правые смежные классы G по $H = \langle X \rangle$.

5) Найти коммутант $[G, G]$.

3.82. Дана группа G с элементами

$$1, X, X^2, X^3, Y, Y^2, Y^3, XY, XY^2, XY^3,$$
$$X^2Y, X^2Y^2, X^2Y^3, X^3Y, X^3Y^2, X^3Y^3,$$

которые удовлетворяют следующим соотношениям:

$$X^4 = Y^4 = 1, X^{-1} = YXY, Y = XY^{-1}X.$$

1) Найти в явном виде классы сопряженных элементов G.

2) Найти центр G.

3) Найти порядок элемента $Z = XY^2$.

4) Найти левые и правые смежные классы G по $H = \langle Z \rangle$.

5) Найти коммутант $[G, G]$.

3.83. Дана группа G с элементами

$$1, X, Y, Z, XY, XZ, ZX, YX, YZ, ZY,$$
$$XYZ, (XYZ)^2, (XYZ)^3, XYX, XZX, YXY,$$

которые удовлетворяют следующим соотношениям:

$$X^2 = Y^2 = Z^2 = 1, XY = Z(XY)Z, ZX = Y(ZX)Y, ZY = X(ZY)X,$$
$$XYX = ZYZ, XZX = YZY, YXY = ZXZ.$$

1) Найти в явном виде классы сопряженных элементов G.

2) Найти центр G.

3) Найти порядок элемента $R = XZ$.

4) Найти левые и правые смежные классы G по $H = \langle R \rangle$.

5) Найти коммутант $[G, G]$.

Указание. Пусть $W = XYZ$. Показать, что $W^4 = 1$, и что $XW = WX$, $YW = WY$, $ZW = WZ$.

3.84. Дана группа G с элементами

$$1, X, Y, X^2, X^3, X^4, X^5, X^6, X^7, Y, XY, X^2Y, X^3Y, X^4Y, X^5Y, X^6Y, X^7Y,$$

которые удовлетворяют следующим соотношениям:

$$X^8 = 1, X^4 = Y^2, YXY^{-1} = X^{-1}, XYX = Y.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $Z = XY$.
4) Найти левые и правые смежные классы G по $H = \langle Z \rangle$.
5) Найти коммутант $[G, G]$.

3.85. Дана группа G с элементами

$$1, U, U^2, U^3, U^4, U^5, U^6, U^7, V, V^3, UV, U^2V, UV^3, U^2V^3U^3V, U^3V^3,$$

которые удовлетворяют следующим соотношениям:

$$U^8 = 1, V^2 = U^4, VU^3V^{-1} = U.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $X = U^2V$.
4) Найти левые и правые смежные классы G по $H = \langle X \rangle$.
5) Найти коммутант $[G, G]$.

3.86. Дана группа G с элементами

$$1, C, C^2, C^3, C^4, C^5, C^6, C^7, Y, CY, C^2Y, C^3Y, C^4Y, C^5Y, C^6Y, C^7Y,$$

которые удовлетворяют следующим соотношениям:

$$C^8 = Y^8, Y^2 = C^6, Y^4 = C^4, Y^6 = C^2, YCY = C^3.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $X = CY$.
4) Найти левые и правые смежные классы G по $H = \langle X \rangle$.
5) Найти коммутант $[G, G]$.

3.87. Дана группа G с элементами

$$1, A, B, C, AB, AC, BC, (BC)^2, (BC)^3,$$
$$BCB, CBC, ABC, ACB, ABCB, ACBC, A(BC)^2,$$

которые удовлетворяют следующим соотношениям:

$$A^2 = B^2 = C^2 = (BC)^4 = 1, AB = BA, AC = CA.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $X = ABC$.
4) Найти левые и правые смежные классы G по $H = \langle X \rangle$.
5) Найти коммутант $[G, G]$.

3.88. Дана группа G с элементами

$$1, X, X^2, X^3, X^4, X^5, X^6, X^7, Y, XY, X^2Y, X^3Y, X^4Y, X^5Y, X^6Y, X^7Y,$$

которые удовлетворяют следующим соотношениям:

$$Y^4 = 1, Y^2 = X^4, YX^2 = X^6Y, YX = X^7Y.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $Z = X^2Y$.
4) Найти левые и правые смежные классы G по $H = \langle Z \rangle$.
5) Найти коммутант $[G, G]$.

3.89. Дана группа G с элементами

$$1, X, X^2, X^3, Y, Y^3, Z, XY, YX, ZX, ZY, ZX^2, ZXY, ZX^3, ZY^3, ZYX,$$

которые удовлетворяют следующим соотношениям:

$$X^2 = Y^2 = (XY)^2, Z^2 = (XY)^4 = 1, ZXZ^{-1} = X, ZYZ^{-1} = Y.$$

1) Найти в явном виде классы сопряженных элементов G.
2) Найти центр G.
3) Найти порядок элемента $W = ZYX$.
4) Найти левые и правые смежные классы G по $H = \langle W \rangle$.
5) Найти коммутант $[G, G]$.

4. Факторгруппы и прямые произведения

Пусть G и W — группы. Напомним, что отображение $h : G \longrightarrow W$ называется *гомоморфизмом* групп, если выполнены два условия:
а) $h(g_1g_2) = h(g_1)h(g_2)$ для любых $g_1, g_2 \in G$ и б) $h(1) = 1$ (нейтральный элемент группы G отображается в нейтральный элемент группы W). Из этих условий вытекает, что $h(g^{-1}) = (h(g))^{-1}$.

Если групповые операции в группах G и W записываются с помощью знака "+", а нейтральные элементы обозначаются как нули, то свойства гомоморфизма выглядят так: $h(g_1+g_2) = h(g_1)+h(g_2)$, $h(0) = 0$, $h(-g) = -h(g)$.

Но возможны ситуации, когда в одной из групп, например, в G, групповая операция записывается мультипликативно (как умножение), а в другой, т.е. в W — аддитивно (в виде сложения). Тогда h является гомоморфизмом, если $h(g_1 + g_2) = h(g_1)h(g_2)$, $h(0) = 1$, $h(-g) = (h(g))^{-1}$. Если, наоборот, аддитивно записывается операция в W, а мультипликативно — в G, то отображение h является гомоморфизмом групп при условиии, что $h(g_1g_2) = h(g_1) + h(g_2)$, $h(1) = 0$, $h(g^{-1}) = -h(g)$.

Примеры групп и отображений всех этих разновидностей обнаруживаются без труда. Вот некоторые из них.

Пример 4.1. $G = W = \mathbb{C}^*$, $h(z) = z^n$ для фиксированного целого ненулевого n. Свойство $(z_1z_2)^n = z_1^n z_2^n$ означает, что $h(z_1z_2) = h(z_1)h(z_2)$, а $1^n = 1$ означает, что $h(1) = 1$. Той же формулой можно задать гомоморфизмы между другими группами. Например, если $G = \mathbb{R}^*$, $W = \mathbb{R}_+$, а $n = 2k$, то получаем отображение $h : \mathbb{R}^* \longrightarrow \mathbb{R}_+$ такое, что $h(r) = r^{2k}$. Оно будет гомоморфизмом групп.

Пример 4.2. Пусть G, W — векторные (линейные) пространства. Это — группы относительно операции сложения. Любое линейное отображение $h : G \longrightarrow W$ является гомоморфизмом этих групп, так как по определению линейного отображения $h(g_1+g_2) = h(g_1)+h(g_2)$, $h(0) = 0$, $h(-g) = -h(g)$. Когда речь идет о группах, то умножения на скаляры (элементы поля) не рассматриваются.

Пример 4.3. Пусть F — любое поле (или коммутативное кольцо), $GL_n(F)$ — группа невырожденных $n \times n$-матриц над F, F^* — группа (по умножению) всех обратимых элементов F. Если F — поле, то это просто все ненулевые элементы F. Если же, например, $F = \mathbb{Z}$, то $F^* = \{+1, -1\}$. Для матрицы $A \in GL_n(F)$ обозначим через $det(A)$

ее определитель. Это — элемент множества F^* (почему?). Отображение $det : GL_n(F) \longrightarrow F^*$ является гомоморфизмом групп, так как, согласно известным свойствам определителя, $det(AB) = det(A)det(B)$ и $det(E_n) = 1$ (напомним, что E_n — это единичная $n \times n$-матрица).

Пример 4.4. Пусть $\mathbb{R}$ — группа (относительно операции сложения) всех действительных чисел, a — некоторое фиксированное положительное число. Определим отображение $h : \mathbb{R} \longrightarrow \mathbb{R}_+$ по формуле $h(x) = a^x$. Из свойств функции a^x следует, что $h(x_1 + x_2) = h(x_1)h(x_2)$ и $h(0) = 1$.

Пример 4.5. Рассмотрим отображение $h : \mathbb{R}_+ \longrightarrow \mathbb{R}$, определенное формулой $h(x) = \log_a x$, где a — фиксированное положительное число. Из свойств логарифмической функции следует, что $h(x_1x_2) = h(x_1) + h(x_2)$, $h(1) = 0$.

Пример 4.6. Рассмотрим запись комплексных чисел в форме $z = |z|e^{i\varphi}$, где $|z|$ — модуль комплексного числа, а $e^{i\varphi} = \cos\varphi + i\sin\varphi$. Из свойств модуля $|z_1z_2| = |z_1| \cdot |z_2|$ и $|1| = 1$ следует, что формула $h(z) = |z|$ определяет гомоморфизм из группы $\mathbb{C}^*$ в группу $\mathbb{R}_+$.

Пример 4.7. Вернемся к формуле $z = |z|e^{i\varphi}$, $\varphi = \arg z$. Заметим, что модуль $e^{i\varphi}$ равен единице. Формула $h(z) = e^{i\varphi} = \dfrac{z}{|z|}$ определяет гомоморфизм из $\mathbb{C}^*$ в $\mathbf{U} = \{z \in \mathbb{C} \mid |z| = 1\}$. Здесь $h(z_1z_2) = h(z_1)h(z_2)$ и $h(1) = 1$.

Отметим еще важное для решения многих задач этого раздела свойство: если даны два гомоморфизма групп $h : G_1 \longrightarrow G_2$ и $f : G_2 \longrightarrow G_3$, то их суперпозиция fh является гомоморфизмом из группы G_1 в группу G_3. Например, отображение $A \mapsto (det(A))^m$ (m фиксировано) есть суперпозиция гомоморфизма $det : GL_n(F) \longrightarrow F^*$ и гомоморфизма из F^* в F^*, переводящего x в x^m.

Ядро гомоморфизма групп $h : G \longrightarrow W$ определяется как подмножество $Ker(h) = \{\ g \in G \mid h(g) = 1\ \}$. Если групповая операция в W обозначается символом "+", а нейтральный элемент записывается в виде нуля, определение ядра должно иметь следующий вид: $Ker(h) = \{\ g \in G \mid h(g) = 0\ \}$. В случае иных обозначений следует вносить соответствующие коррекции, относящиеся, впрочем, не к сути дела, а только к способу записи.

Напомним, что *нормальной* называется подгруппа H группы G, об-

ладающая свойством: $gH = Hg$ для каждого $g \in G$. Это эквивалентно тому, что $gHg^{-1} \subseteq H$, или что $gHg^{-1} = H$ для всех $g \in G$. В коммутативной группе каждая подгруппа является нормальной.

Лемма 4.1. *Ядро любого гомоморфизма — это нормальная подгруппа.*

Доказательство. Рассмотрим гомоморфизм $h : G \to W$. Покажем, что $Ker(h)$ является подгруппой группы G. Так как $h(1) = 1$, то $1 \in Ker(h)$. Пусть $g_1, g_2 \in Ker(h)$, тогда $h(g_1g_2) = h(g_1)h(g_2) = 1 \cdot 1 = 1$, отсюда следует, что $g_1g_2 \in Ker(h)$. Если $h(g) = 1$, то $h(g^{-1}) = h(g)^{-1} = 1^{-1} = 1$. Отсюда $g^{-1} \in Ker(h)$. Таким образом, $Ker(h)$ является подгруппой.

Снова пусть $g \in Ker(h)$, то есть $h(1) = 1$. Если $x \in G$, то $h(xgx^{-1}) = h(x)h(1)h(x)^{-1} = h(x)h(x)^{-1} = 1$. Это означает, что $xgx^{-1} \in Ker(h)$, то есть $Ker(h)$ является нормальной подгруппой. □

Ядра некоторых гомоморфизмов имеют особое значение. Например, ядро гомоморфизма $det : GL_n(F) \longrightarrow F^*$ (т.е. множество всех $n \times n$-матриц A таких, что $det(A) = 1$) называется *специальной линейной группой* степени n над полем (или над кольцом) F, и обозначается $SL_n(F)$ (напомним, что группа $GL_n(F)$ называется *общей линейной группой* степени n). Знакопеременная группа A_n определяется как ядро гомоморфизма sgn.

Напомним, что если $f : X \longrightarrow Y$ — некоторое отображение, и $Y' \subseteq Y$, то *полным прообразом* Y' относительно f называется множество $f^{-1}(Y') = \{x \in X | f(x) \in Y'\} \subseteq X$. Из этого определения следует, что $f(f^{-1}(Y')) \subseteq Y'$.

Лемма 4.2. *Пусть $h : G \longrightarrow W$ — гомоморфизм групп, и $H = Ker(h)$. Тогда для каждого $w \in W$ полный прообраз $h^{-1}(\{w\})$ есть либо пустое множество, либо множество вида $gH = Hg$, где $h(g) = w$. Элемент $g \in h^{-1}(\{w\})$ можно здесь выбирать произвольным образом.*

Доказательство. Вместо $h^{-1}(\{w\})$ будем писать $h^{-1}(w)$. Это множество всех таких $g \in G$, что $h(g) = w$. Иначе говоря, $h^{-1}(w)$ есть множество решений уравнения $h(x) = w$. Заметим, что по самому определению $Ker(h) = h^{-1}(1)$.

Предположим, что $h^{-1}(w)$ непусто. Выберем какой-нибудь $g \in h^{-1}(w)$, и пусть $x \in H = Ker(h)$. Тогда $h(gx) = h(g)h(x) = w \cdot 1 = w$, и аналогично $h(xg) = w$. Это означает, что $gH \subseteq h^{-1}(w)$ и $Hg \subseteq h^{-1}(w)$. Пусть $y \in h^{-1}(w)$, т.е. $h(y) = w$. Рассмотрим $x = g^{-1}y$. Так как $h(x) = h(g)^{-1}h(y) = w^{-1}w = 1$, то $x \in H$. Отсюда $y = gx \in gH$. Следовательно, $h^{-1}(w) \subseteq gH$, а значит, $h^{-1}(w) = gH$. Если же взять $x = yg^{-1}$, то $h(x) = 1$, $x \in H$, $y = xg \in Hg$, а значит $h^{-1}(w) = Hg$. В частности, $Hg = gH$. $\square$

Следствие 4.1. *Гомоморфизм h инъективен тогда и только тогда, если его ядро $Ker(h)$ состоит только из одного элемента (т.е. это множество, содержащее лишь нейтральный элемент группы).*

Доказательство. Отображение h инъективно тогда и только тогда, если все непустые $h^{-1}(w)$, где $w \in W$, состоят лишь из одного элемента. Это просто другая формулировка определения инъективности: в каждый элемент $w \in W$ отображается не более одного элемента из G. Если h – инъективное отображение, то все $h^{-1}(w)$ состоят из одного элемента, в том числе и $h^{-1}(1) = Ker(h)$. Обратно, пусть $|H| = |Ker(h)| = 1$. Тогда, если $h^{-1}(w)$ не пусто, будем иметь $|h^{-1}(w)| = |gH| = |H| = 1$. $\square$

Задачи о нахождении ядра заданного гомоморфизма очень похожи на задачи о нахождении корней уравнения (или системы уравнений).

Пример 4.8. Пусть $G = \mathbb{R}^4$, $W = \mathbb{R}^3$, и линейное отображение $h : \mathbb{R}^4 \to \mathbb{R}^3$ задается матрицей:

$$A = \begin{pmatrix} 1 & -1 & 0 & 2 \\ 2 & 0 & 1 & -1 \\ 1 & -2 & -1 & 0 \end{pmatrix}$$

Иными словами, $h(x) = Ax$, где $x = (x_1, x_2, x_3, x_4)$. Ядро $Ker(h)$ — это множество решений системы $Ax = 0$:

$$\begin{cases} x_1 - x_2 + 2x_4 = 0 \\ 2x_1 + x_3 - x_4 = 0 \\ x_1 - 2x_2 - x_3 = 0 \end{cases}$$

Пример 4.9. Зафиксируем действительное число $a \neq 0$, и пусть $x \in \mathbb{R}$. Тогда модуль комплексного числа $e^{iax} = \cos ax + i \sin ax$ равен единице. Рассмотрим отображение $f_a : \mathbb{R} \to \mathbf{U}$, $f_a(x) = e^{iax}$. Легко

проверяется, что $h(x+y) = h(x)h(y)$ и $h(0) = 1$. Таким образом, h — гомоморфизм. Этот гомоморфизм сюръективен. В самом деле, каждое комплексное число, по модулю равное единице, имеет вид e^{iy}, где y — действительное число, $0 \leq y < 2\pi$. Пролагая $x = \dfrac{y}{a}$, получим $e^{iy} = e^{iax} = h(x)$. Вычислим $Ker(f_a)$. Это множество состоит из всех тех $x \in \mathbb{R}$, для которых $h(x) = 1$. Иными словами, это множество всех решений уравнения $e^{iax} = 1$. Известно (фактически это школьная тригонометрия), что $e^{iy} = 1$ тогда и только тогда, если $y = 2\pi k, k = 0, \pm 1, \pm 2, \ldots$. Следовательно, $Ker(f_a) = \{ \dfrac{2\pi}{a}k \mid k = 0, \pm 1 \pm 2, \ldots \} = \dfrac{2\pi}{a}\mathbb{Z}$. В частности, при $a = 2\pi$ ядро будет равно $\mathbb{Z}$ — группе (по сложению) всех целых чисел.

4.1. Будет ли гомоморфизм $det : GL_n(F) \longrightarrow F^*$ сюръективным?

4.2. Вычислить ядро гомоморфизма $h : \mathbb{C}^* \longrightarrow \mathbb{C}^*$, $h(z) = z^n$ для некоторого фиксированного $n > 0$. Выяснить, будет ли этот гомоморфизм сюръективным.

4.3. Вычислить ядро гомоморфизма $h : \mathbb{C}^* \longrightarrow \mathbb{R}_+$, $h(z) = |z|$. Выяснить, будет ли этот гомоморфизм сюръективным.

4.4. Вычислить ядро гомоморфизма $h : \mathbb{C}^* \longrightarrow \mathbf{U}$, $h(z) = \dfrac{z}{|z|}$. Выяснить, будет ли этот гомоморфизм сюръективным. Рассмотреть гомоморфизм $f : \mathbf{U} \longrightarrow \mathbf{U}$, определенный по той же формуле $f(u) = u^n$. Вычислить его ядро, и выяснить, будет ли он сюръективным.

4.5. Вычислить ядро гомоморфизма $h : \mathbb{C}^* \longrightarrow \mathbf{U}$, $h(z) = \left(\dfrac{z}{|z|}\right)^n$ для некоторого фиксированного $n > 0$. Найти эту подгруппу группы $\mathbb{C}^*$ среди групп, изучавшихся в предыдущем параграфе. Выяснить, будет ли этот гомоморфизм сюръективным.

4.6. Вычислить ядро гомоморфизма $h : GL_n(F) \longrightarrow F^*$, $h(A) = (det(A))^m$ для некоторого фиксированного $m > 0$. Рассмотреть отдельно случаи $F = \mathbb{R}$ и $F = \mathbb{C}$. Выяснить, будет ли этот гомоморфизм сюръективным.

4.7. Пусть $F = \mathbb{R}$ или $F = \mathbb{C}$. Вычислить ядро гомоморфизма $h : GL_n(F) \longrightarrow \mathbb{R}_+$, $h(A) = |det(A)|$. Рассмотреть отдельно случаи $F = \mathbb{R}$ и $F = \mathbb{C}$. Выяснить, будет ли этот гомоморфизм сюръективным.

4.8. Вычислить ядро гомоморфизма $h : GL_n(F) \longrightarrow F^*$, определяемого по формуле $h(A) = \dfrac{det(A)}{|det(A)|}$. Рассмотреть отдельно случаи $F = \mathbb{R}$ и $F = \mathbb{C}$. Выяснить, будет ли этот гомоморфизм сюръективным.

4.9. Пусть F — поле. Рассмотрим в $GL_{n+m}(F)$ подмножество G, состоящее из блочных матриц вида:

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix},$$

таких, что A есть невырожденная $n \times n$-матрица, C — невырожденная $m \times m$-матрица, а остальные блоки имеют соответствующие размеры. Доказать, что множество G является подгруппой группы $GL_{n+m}(F)$. Доказать, что отображения

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \mapsto A, \quad \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \mapsto C$$

будут гомоморфизмами из G в $GL_n(F)$ и $GL_m(F)$ соответственно. Вычислить ядра этих гомоморфизмов и выяснить, будут ли они сюръективными.

Пусть H есть нормальная подгруппа группы G. Обозначим через G/H множество различных смежных классов G по H. Так как для нормальной подгруппы $Hx = xH$ для каждого $x \in G$, то нет необходимости различать левые и правые смежные классы. Напомним (см. пример 1.5), что если $A, B \subseteq G$, то $AB = \{ab | a \in A, b \in B\}$, и это произведение ассоциативно: $(AB)C = A(BC)$ для любых непустых $A, B, C \subseteq G$.

Лемма 4.3. *Смежные классы по нормальной подгруппе H обладают следующими свойствами:*

1) $HH = H$.

2) *Произведение двух смежных классов снова является смежным классом. Точнее, если* $A = xH$, $B = yH$, *то* $AB = xyH$. *Таким образом,* G/H *является полугруппой относительно операции умножения смежных классов.*

3) *Класс* H *является нейтральным элементом (единицей) полугруппы* G/H.

4) *Пусть* A *— некоторый смежный класс. Определим* A^{-1} *как множество* $\{a^{-1}|a \in A\}$,. *Тогда* A^{-1} *снова является смежным классом. В часности, если* $A = xH$, *то* $A^{-1} = x^{-1}H$. *При этом* $AA^{-1} = A^{-1}A = H$.

Доказательство. Докажем 1). Необходимо установить включения: $HH \subseteq H$ и $H \subseteq HH$. По определению, $HH = \{x_1x_2|x_1, x_2 \in H\}$. Но так как H — подгруппа, то из $x_1, x_2 \in H$ следует $x_1x_2 \in H$. Отсюда $HH \subseteq H$. Так как $1 \in H$, то любой $x \in H$ представим в виде $x = x_1x_2$, где $x_1, x_2 \in H$: $x_1 = x, x_2 = 1$.

Теперь легко доказать 2). Представим класс A в виде $A = xH$, класс B в виде $B = yH$, и тогда

$$AB = (xH)(yH) = (x(Hy))H = (x(yH))H = (xy)(HH) = xyH.$$

Здесь использована ассоциативность умножения мподмножеств группы, свойство нормальности H $(Hy = yH)$ и свойство 1): $HH = H$. Итак классы умножаются по следующему правилу:

$$(xH)(yH) = xyH \tag{1}$$

Из доказательства видно, что результат произведения не зависит от способа представления классов в виде xH, yH.

Примерно так же доказывается свойство 3):

$$(xH)H = x(HH) = xH, \quad H(xH) = (Hx)H = (xH)H = x(HH) = xH.$$

Свойство 4) можно вывести из двух общих свойств произведений подмножеств подгруппы: $H^{-1} = H$ для любой подгруппы H, и $(AB)^{-1} = B^{-1}A^{-1}$ для любых $A, B \subseteq G$. В самом деле, если $x \in H$, то $x^{-1} \in H$. Это значит, что $H^{-1} \subseteq H$. С другой стороны, каждый $x \in H$ представми в виде $x = (x^{-1})^{-1}$, где $x^{-1} \in H$. Это значит, что $H \subseteq H^{-1}$. Далее,

$(AB)^{-1} = \{(ab)^{-1} = b^{-1}a^{-1} | a \in A, b \in B\}$, $B^{-1}A^{-1} = \{b^{-1}a^{-1} | b \in B, a \in A\}$. Очевидно, что это одно и то же множество.

Пусть теперь $A = xH = \{x\}H$. Тогда

$$A^{-1} = H^{-1}\{x\}^{-1} = H^{-1}x^{-1} = Hx^{-1} = x^{-1}H.$$

Итак,

$$(xH)^{-1} = x^{-1}H \tag{2}$$

Как и в (1), правая часть равенства (2) не зависит от выбора представителя x в классе xH.

Наконец, если $A = xH$, $A^{-1} = x^{-1}H$, то

$$AA^{-1} = (xH)(x^{-1}H) = (xx^{-1})H = H,$$
$$A^{-1}A = (x^{-1}H)(xH) = (x^{-1}x)H = H.$$

□

Все эти свойства смежных классов означают, что умножение классов превращает множество G/H в группу с нейтральным элементом H. Эта группа называется *факторгруппой* группы G по нормальной подгруппе H. Формулы (1) и (2) задают способ вычисления произведения элементов факторгруппы и обратных элементов.

Сопоставляя элементу $x \in G$ смежный класс xH, получим сюръективное отображение $\pi : G \longrightarrow G/H$, $\pi(x) = xH$. Ясно, что $\pi(x) = H$ тогда и только тогда, если $x \in H$. Формула (1) записывается как $\pi(xy) = \pi(x)\pi(y)$. Таким образом, π оказывается сюръективным гомоморфизмом групп, ядро которого есть H. Этот гомоморфизм называется (естественной) *проекцией* группы G на факторгруппу G/H.

Следующая теорема называется *теоремой о гомоморфизме.*

Теорема 4.1. *Пусть дана группа G, ее нормальная подгруппа H, и гомоморфизм групп $h : G \longrightarrow W$ такой, что $H \subseteq Ker(h)$. Тогда существует, притом только один, гомоморфизм $\psi : G/H \longrightarrow W$, такой, что $\psi\pi = h$ (иными словами, $\psi(xH) = h(x)$).*

Гомоморфизм ψ инъективен тогда и только тогда, если $H = Ker(h)$. Гомоморфизм ψ сюръективен тогда и только тогда, если сюръективен гомоморфизм h.

Доказательство. Допустим, что гомоморфизм ψ со свойством $\psi\pi = h$ существует. Покажем, что он определен однозначно. Допустим, что есть

два отображения, ψ_1 и ψ_2, такие, что $\psi_1\pi = \psi_2\pi = h$. Отображение π сюръективно: каждый элемент G/H имеет вид $xH = \pi(x)$ для некоторого $x \in G$. Тогда $\psi_1(xH) = \psi_1(\pi(x)) = h(x)$, и $\psi_2(xH) = \psi_2(\pi(x)) = h(x)$. Таким образом, значения отображений ψ_1 и ψ_2 совпадают для всех значений аргумента. Значит, $\psi_1 = \psi_2$. Из этих же рассуждений должно быть ясно, что если ψ существует, то его значение на аргументе $xH \in G/H$ должно быть равно $h(x)$.

Покажем, что условие $H \subseteq Ker(h)$ позволяет корректно определить такое отображение. Проблема здесь заключается в том, что один и тот же класс можно задать несколькими способами: $x_1H = x_2H = \ldots$, и не очевидно, что тогда значение ψ на этом аргументе определено однозначно, так как определение зависит от выбора представителя класса. Однозначность получится, если из $x_1H = x_2H$ будет следовать $h(x_1) = h(x_2)$. Итак, пусть $x_1H = x_2H$. Тогда $x_1^{-1}x_2 \in H \subseteq Ker(h)$. Это значит, что $h(x_1^{-1}x_2) = 1$. Применяя определение гомоморфизма, получаем, что $h(x_1^{-1}x_2) = h(x_1)^{-1}h(x_2) = 1$, откуда и следует, что $h(x_1) = h(x_2)$.

Итак, отображение $\psi : G/H \longrightarrow W$ со свойством $\psi(xH) = h(x)$ существует и определено однозначно. Покажем, что оно является гомоморфизмом групп. Единицей группы G/H является класс $H = 1H$ с представителем $1 \in G$. По определению ψ будем иметь $\psi(H) = h(1) = 1$. Далее,

$$\psi((xH)(yH)) = \psi(xyH) = h(xy) = h(x)h(y) = \psi(xH)\psi(yH).$$

Этим доказано, что ψ является гомоморфизмом.

Из самого определения ψ следует, что это отображение сюръективно тогда и только тогда, когда сюръективен гомоморфизм h. Вычислим ядро ψ. Класс xH принадлежит ядру тогда и только тогда, если $\psi(xH) = h(x) = 1$, то есть в том и только в том случае, если $x \in Ker(h)$. Если гомоморфизм ψ инъективен, то его ядро состоит из единственного класса H, а это значит, что из $x \in Ker(h)$ следует $xH = H$. Но отсюда следует $x \in H$, что означает $Ker(h) \subseteq H$. Так как обратное включение имеется по условию, то $H = Ker(h)$. Обратно, если $H = Ker(h)$, то ядро ψ состоит из тех классов xH, для которых $x \in Ker(h) = H$, то есть $xH = H$, и ядро состоит из одного элемента. Как уже было показано выше, это означает инъективность h. $\square$

Как следствие, получается теорема, называемая *теоремой об изоморфизме.*

Теорема 4.2. *Пусть дана группа G, ее нормальная подгруппа H, и сюръективный гомоморфизм групп $h : G \longrightarrow W$ такой, что $H = Ker(h)$. Тогда имеет место изоморфизм $G/H \cong W$.*

4.10. В задачах **4.1** — **4.9**, там, где гомоморфизмы сюръективны, фактически (с точностью до изоморфизма) вычислены факторгруппы. Сформулировать эти утверждения в явном виде и обосновать их.

4.11. Доказать, что $\mathbb{Z}/n\mathbb{Z} \cong \mathbf{U}_n$. Указание: рассмотреть гомоморфизм $h : \mathbb{Z} \to \mathbf{U}_n$, $h(m) = e^{\frac{2\pi m}{n}}$.

4.12. Доказать, что $\mathbf{U}_{nm}/\mathbf{U}_m \cong \mathbf{U}_n$. Указание: рассмотреть гомоморфизм $h : \mathbb{C}^* \to \mathbb{C}^*$, $h(z) = z^m$, и его ограничение на подгруппу $\mathbf{U}_{nm}$. Найти образ и ядро этого гомоморфизма.

4.13. Вычислить факторгруппу $\mathbb{C}^*/\mathbf{K}_n$. Напомним, что $\mathbf{K}_n = \{z \in \mathbb{C}^* | z^n \in \mathbb{R}_+\}$.

Указание: используя определение $\mathbf{K}_n$, найти гомоморфизм из $\mathbb{C}^*$, ядром которого будет подгруппа $\mathbf{K}_n$. Затем определить образ этого гомоморфизма.

4.14. Доказать, что факторгруппа $D_{2n}/C(D_{2n})$ группы диэдра D_{2n} по ее центру $C(D_{2n})$ изоморфна группе D_n.

4.15. Доказать, что факторгруппа $G/[G,G]$ группы G по ее коммутанту коммутативна.

4.16. Доказать, что если $h : G \longrightarrow W$ — гомоморфизм произвольной группы G в коммутативную группу W, то $[G,G] \subseteq Ker(h)$. Что можно вывести из этого факта с помощью теоремы о гомоморфизме?

Указание. Проверить, что в ядре h содержатся коммутаторы всех элементов группы G. Используя определение коммутанта, вывести отсюда требуемое утверждение.

Смысл очередной серии заданий проясняет следующая теорема:

Теорема 4.3. *Пусть дана группа G и две ее подгруппы H и K такие, что H — нормальная подгруппа, $G = KH$, и $K \cap H = \{1\}$. Тогда $G/H \cong K$.*

Набросок доказательства. Рассмотрим естественную проекцию $\pi : G \longrightarrow G/H$, и определим гомоморфизм $h : K \longrightarrow G/H$ как ограничение π на подгруппу K. Ввиду того, что π отображает в единицу только элементы H, а единственным элементом K, содержащимся в H, является единица группы G, ядро гомоморфизма h состоит из одного элемента — единицы. Следовательно, гомоморфизм h инъективен. С другой стороны, рассмотрим произвольный элемент gH группы G/H. Так как $G = KH$, то $g = xy$ для некоторых $x \in K$, $y \in H$. Тогда $gH = xyH = xH$, так как $yH = H$ при $y \in H$. Остается заметить, что $xH = h(x)$ при $x \in K$ по определению гомоморфизма h. Итак, h есть изоморфизм между K и G/H. $\square$

4.17. Доказать, что если H и K — подгруппы группы G, и $KH = G$, то $K \cap H$ является нормальной подгруппой в K, и
$G/H \cong K/(K \cap H)$.

Указание. Воспользоваться приведенным выше доказательством теоремы 4.3.

4.18. Доказать, что $T_n(F)/UT_n(F) \cong D_n(F)$. (Определения этих групп — в разделе 1.)

В следующей группе упражнений задано множество G, имеющее вид

$$G = \begin{pmatrix} G_1 & G_2 \\ 0 & G_2 \end{pmatrix} = \left\{ \begin{pmatrix} g_1 & g_2 \\ 0 & g_2 \end{pmatrix} | g_1 \in G_1, g_2 \in G_2, g_3 \in G_3 \right\},$$

и подмножество H, устроенное по тому же принципу (т.е. некоторое множество матриц второго порядка).

Требуется показать, что

а) G — группа;

б) H — нормальная подгруппа;

Далее требуется найти подгруппу K группы G, обладающую следующими свойствами: $G = KH$, пересечение K и H состоит только из единичной матрицы.

4.19.

$$G = \begin{pmatrix} \mathbb{R}^* & \mathbb{R} \\ 0 & \mathbb{R}^* \end{pmatrix}, \quad H = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R}^* \right\}$$

4.20.

$$G = \begin{pmatrix} \mathbb{R}^* & \mathbb{R} \\ 0 & \mathbb{R}^* \end{pmatrix}, \quad H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$$

4.21.

$$G = \begin{pmatrix} \mathbb{R}^* & \mathbb{R} \\ 0 & \mathbb{R}^* \end{pmatrix}, \quad H = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{R}^*, b \in \mathbb{R} \right\}$$

4.22.

$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}_+ & \mathbb{C} \\ 0 & \mathbb{R}_+ \end{pmatrix}$$

4.23.

$$G = \begin{pmatrix} \mathbb{C}^* & 0 \\ \mathbb{C} & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U} & 0 \\ \mathbb{C} & \mathbf{U} \end{pmatrix}$$

4.24.

$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}_+ & \mathbb{C} \\ 0 & \mathbf{U} \end{pmatrix}$$

4.25.

$$G = \begin{pmatrix} \mathbb{C}^* & 0 \\ \mathbb{C} & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U} & 0 \\ \mathbb{C} & \mathbb{R}_+ \end{pmatrix}$$

4.26.

$$G = \begin{pmatrix} \mathbb{R}^* & 0 \\ \mathbb{C} & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}_+ & 0 \\ \mathbb{C} & \mathbb{R}_+ \end{pmatrix}$$

4.27.

$$G = \begin{pmatrix} \mathbb{R}^* & 0 \\ \mathbb{C} & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}_+ & 0 \\ \mathbb{C} & \mathbf{U} \end{pmatrix}$$

4.28.

$$G = \begin{pmatrix} \mathbb{R}^* & 0 \\ \mathbb{C} & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_2 & 0 \\ \mathbb{C} & \mathbb{R}_+ \end{pmatrix}$$

4.29.

$$G = \begin{pmatrix} \mathbb{R}^* & 0 \\ \mathbb{C} & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_2 & 0 \\ \mathbb{C} & \mathbf{U} \end{pmatrix}$$

4.30.

$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbb{R}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}_+ & \mathbb{C} \\ 0 & \mathbb{R}_+ \end{pmatrix}$$

4.31.

$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbb{R}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U} & \mathbb{C} \\ 0 & \mathbb{R}_+ \end{pmatrix}$$

4.32.

$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbb{R}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}_+ & \mathbb{C} \\ 0 & \mathbf{U}_2 \end{pmatrix}$$

4.33.

$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbb{R}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U} & \mathbb{C} \\ 0 & \mathbf{U}_2 \end{pmatrix}$$

4.34.

$$G = \begin{pmatrix} \mathbb{R}^* & \mathbb{R} \\ 0 & \mathbb{R}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}_+ & \mathbb{R} \\ 0 & \mathbb{R}_+ \end{pmatrix}$$

4.35.

$$G = \begin{pmatrix} \mathbb{R}^* & 0 \\ \mathbb{R} & \mathbb{R}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_2 & 0 \\ \mathbb{R} & \mathbb{R}_+ \end{pmatrix}$$

4.36.

$$G = \begin{pmatrix} \mathbb{R}^* & \mathbb{R} \\ 0 & \mathbb{R}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}_+ & \mathbb{R} \\ 0 & \mathbf{U}_2 \end{pmatrix}$$

4.37.

$$G = \begin{pmatrix} \mathbf{K}_4 & \mathbb{C} \\ 0 & \mathbf{K}_4 \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}_+ & \mathbb{C} \\ 0 & \mathbb{R}_+ \end{pmatrix}$$

4.38.

$$G = \begin{pmatrix} \mathbf{K}_4 & \mathbb{C} \\ 0 & \mathbf{K}_4 \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_4 & \mathbb{C} \\ 0 & \mathbf{U}_4 \end{pmatrix}$$

4.39.

$$G = \begin{pmatrix} \mathbf{K}_4 & 0 \\ \mathbb{C} & \mathbf{K}_4 \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}_+ & 0 \\ \mathbb{C} & \mathbf{U}_4 \end{pmatrix}$$

4.40.

$$G = \begin{pmatrix} \mathbf{K}_4 & 0 \\ \mathbb{C} & \mathbf{K}_4 \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_4 & 0 \\ \mathbb{C} & \mathbb{R}_+ \end{pmatrix}$$

4.41.

$$G = \begin{pmatrix} \mathbf{K}_4 & \mathbb{C} \\ 0 & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}_+ & \mathbb{C} \\ 0 & \mathbb{R}_+ \end{pmatrix}$$

4.42.

$$G = \begin{pmatrix} \mathbb{C}^* & 0 \\ \mathbb{C} & \mathbf{K}_4 \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U} & 0 \\ \mathbb{C} & \mathbf{U}_4 \end{pmatrix}$$

4.43.

$$G = \begin{pmatrix} \mathbb{C}^* & 0 \\ \mathbb{C} & \mathbf{K}_4 \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U} & 0 \\ \mathbb{C} & \mathbb{R}_+ \end{pmatrix}$$

4.44.

$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbb{R}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}_+ & \mathbb{C} \\ 0 & \mathbf{U}_2 \end{pmatrix}$$

4.45.

$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbb{R}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U} & \mathbb{C} \\ 0 & \mathbf{U}_2 \end{pmatrix}$$

4.46.

$$G = \begin{pmatrix} \mathbb{R}^* & \mathbb{C} \\ 0 & \mathbb{R}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_2 & \mathbb{C} \\ 0 & \mathbf{U}_2 \end{pmatrix}$$

Пусть даны группы G_1 и G_2. Рассмотрим множество $G = G_1 \times G_2$, состоящее из всех упорядоченных пар вида (g_1, g_2), где $g_1 \in G_1$, $g_2 \in G_2$. Бинарная операция на этом множестве определяется следующим образом:

$$(g_1', g_2')(g_1'', g_2'') = (g_1' g_1'', g_2' g_2'').$$

Легко проверить, что эта операция ассоциативна. Она будет также коммутативной, если коммутативны обе группы G_1 и G_2. Если 1_{G_1} — единица группы G_1, а 1_{G_2} — единица группы G_2, то элемент $(1_{G_1}, 1_{G_2})$ является единицей $G_1 \times G_2$. Обратные элементы вычисляются по формуле $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$. В конечном счете получается группа, которая называется *прямым произведением* групп G_1 и G_2.

4.47. Доказать, что отображения $\pi_1 : G_1 \times G_2 \longrightarrow G_1$, $\pi_2 : G_1 \times G_2 \longrightarrow G_2$, такие, что $\pi_1(g_1, g_2) = g_1$, $\pi(g_1, g_2) = g_2$, являются сюръективными гомоморфизмами групп.

Гомоморфизмы π_1 и π_2 называются *естественными проекциями* прямого произведения групп на первый и второй множители соответственно.

4.48. Проверить, что ядро π_1 состоит из всех пар вида $(1_{G_1}, g_2)$, $g_2 \in G_2$. Доказать, что эта подгруппа группы $G_1 \times G_2$ изоморфна группе G_2. Изоморфизм устанавливается соответствием $g_2 \longleftrightarrow (1, g_2)$. Аналогичным образом ядро π_2, состоящее из всех пар вида $(g_1, 1)$, $g_1 \in G_1$, изоморфно группе G_1.

Если отождествить G_2 с изоморфной ей подгруппой $Ker(\pi_1)$, то по теореме об изоморфизме получим следующий изоморфизм:

$$(G_1 \times G_2)/G_2 \cong G_1.$$

Аналогично этому имеет место изоморфизм

$$(G_1 \times G_2)/G_1 \cong G_2.$$

Эти изоморфизмы дают некоторое обоснование термину “факторгруппа"и обозначению G/H.

Заметим еще, что имеют место соотношения:

$$(g_1, g_2) = (g_1, 1)(1, g_2) = (1, g_2)(g_1, 1).$$

Обратно, имеет место следующая теорема.

Теорема 4.4. *Пусть в группе G имеются две подгруппы K, H, обладающие следующими свойствами:*

1) $G = KH$;

2) $K \cap H = \{1\}$;

3) *для любых* $x \in K$ *и* $y \in H$ *имеет место равенство* $xy = yx$. *(Это свойство автоматически выполнено в случае коммутативной группы* G.*)*

Тогда существует изоморфизм $G \cong K \times H$.

Доказательство. Определим отображение $h : K \times H \longrightarrow G$, по правилу: $(x, y) \mapsto h(x, y) = xy$. Здесь $x \in K$, $y \in H$. Ввиду условия 1), это сюръекция. Проверим, что h является гомоморфизмом. Ясно, что единица группы $K \times H$, т.е. элемент $(1, 1)$, отображается в единицу группы G. Пусть $x', x'' \in K$, $y', y'' \in H$. Тогда

$$h((x', y')(x'', y'')) = h(x'x'', y'y'') = (x'x'')(y'y'') =$$
$$= x'(x''y')y'' = x'(y'x'')y'' = (x'y')(x''y'') = h(x'y')h(x''y'').$$

Здесь $x''y' = y'x''$ согласно условию 3). Наконец, вычислим ядро гомоморфизма h. Пусть $h(x, y) = xy = 1$. Тогда $y = x^{-1}$. Итак, элемент x, по выбору, принадлежит подгруппе K. И он же равен элементу y^{-1} из группы H. Значит, $x \in K \cap H$. Но по условию 2) это пересечение состоит только из единичного элемента. Отсюда $x = y = 1$. Заключаем, что ядро h тривиально, и следовательно, гомоморфизм h инъективен. $\square$

На этой теореме основаны решения следующих далее задач. Начнем с примера.

Пример 4.10. Пусть

$$G = \begin{pmatrix} \mathbf{U} & 0 \\ 0 & \mathbf{U}_4 \end{pmatrix}$$

Определим подгруппы

$$K = \begin{pmatrix} \mathbf{U} & 0 \\ 0 & 1 \end{pmatrix}, H = \begin{pmatrix} 1 & 0 \\ 0 & \mathbf{U}_4 \end{pmatrix}.$$

Легко проверить, что эти подгруппы удовлетворяют всем трем свойствам из теоремы 4.4. Более того, очевидно, что $K \cong \mathbf{U}$, $H \cong \mathbf{U}_4$. Таким образом, $G \cong \mathbf{U} \times \mathbf{U}_4$.

4.49. Убедиться, что множества решений уравнений $y = ax$ и $y = bx$ (обозначим их соответственно через K и H) являются подгруппами группы $G = \mathbb{R}^2$. Доказать, что при $a \neq b$ эти подгруппы удовлетворяют условиям теоремы 4.4. Каким известным группам изоморфны подгруппы H и K?

Напомним, что через Z_n обозначается конечная циклическая группа порядка n: $Z_n = \{1, x, \ldots, x^{n-1}\}$, $x^n = 1$.

4.50. Рассмотрим четверную группу Клейна

$$V_4 = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

Доказать, что эта группа изоморфна произведению двух циклических подгрупп порядка 2, т.е.

$$V_4 \cong Z_2 \times Z_2.$$

4.51. Доказать, что $\mathbb{C}^* \cong \mathbb{R}_+ \times \mathbf{U}$.

4.52. Доказать, что $\mathbf{K}_n \cong \mathbb{R}_+ \times \mathbf{U}_n$. В частности, $\mathbb{R}^* \cong \mathbb{R}_+ \times \{+1, -1\}$.

4.53. Доказать, что если n нечетно, то $D_{2n} \cong D_n \times Z_2$.

4.54. Доказать, что если n и m взаимно просты, то $Z_{nm} \cong Z_n \times Z_m$.

4.55. Пусть Z'_1, Z'_2, $\ldots$, Z'_n — классы сопряженных элементов группы G_1, Z''_1, Z''_2, $\ldots$, Z''_m — классы сопряженных элементов группы G_2. Доказать, что классами сопряженных элементов группы $G_1 \times G_2$ являются множества $Z'_i \times Z''_j = \{(g_1, g_2) | g_1 \in Z'_i, g_2 \in Z''_j\}$, $1 \leq i \leq n$, $1 \leq j \leq m$.

4.56. Доказать, что центр группы $G_1 \times G_2$ равен произведению центров сомножителей: $C(G_1 \times G_2) = C(G_1) \times C(G_2)$.

Точно так же, как было определено произведение двух групп, можно определить произведение произвольного количества групп. Пусть $G_1, \ldots, G_n$ — группы. Через $G = G_1 \times \cdots \times G_n$ (другое обозначение: $\prod_{i=1}^{n} G_i$) обозначим множество всех упорядоченных последовательностей:

$$(g_1, g_2, \ldots, g_n), \quad \text{где} \quad g_1 \in G_1, g_2 \in G_2, \ldots, g_n \in G_n.$$

Произведение двух элементов G определяется по формуле:

$$(g'_1, g'_2, \ldots, g'_n)(g''_1, g''_2, \ldots, g''_n) = (g'_1 g''_1, g'_2 g''_2, \ldots, g'_n g''_n).$$

Легко проверяется ассоциативность, и то, что элемент $(1, 1, \ldots, 1)$ является единицей G. Обратный элемент определяется так:

$$(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}).$$

В случае, если групповые операции во всех G_i обозначаются плюсами, все эти определения выглядят так:

$$(g'_1, g'_2, \ldots, g'_n) + (g''_1, g''_2, \ldots, g''_n) = (g'_1 + g''_1, g'_2 + g''_2, \ldots, g'_n + g''_n)$$
$$-(g_1, g_2, \ldots, g_n) = (-g_1, -g_2, \ldots, -g_n)$$

а нейтральным элементом будет $(0, 0, \ldots, 0)$. Легко заметить сходство этого определения с определением линейного пространства строк.

4.57. Доказать, что

$$D_n(F) \cong \overbrace{F^* \times \cdots \times F^*}^{n}.$$

(Напомним, что $D_n(F)$ — группа диагональных матриц над полем F, определенная в разделе 1.)

4.58. Доказать, что

$$UT_n^m(F)/UT_n^{m+1)} \cong \overbrace{F \times \cdots \times F}^{n-m}.$$

Здесь F есть аддитивная группа поля F.

Указание. Рассмотреть соответствие, сопоставляющее матрице

$$A = \begin{pmatrix}
1 & 0 & & \ldots & 0 & a_{1,m+1} & a_{2,m+1} & \ldots & a_{1,n} \\
0 & 1 & 0 & & \ldots & 0 & a_{2,m+2} & \ldots & a_{2,n} \\
0 & 0 & 1 & 0 & & \ldots & 0 & \ddots & \vdots \\
 & & & \ddots & \ddots & & & \ddots & a_{n-m,n} \\
 & & & & \ddots & & & \ldots & 0 \\
 & & & & & & \ddots & & \\
 & & & & & & & \ddots & \vdots \\
 & & & & & & & \ddots & 0 \\
0 & & & & & & & & 1
\end{pmatrix}.$$

элемент

$$h(A) = (a_{1,m+1}, a_{2,m+2}, \ldots, a_{n-m,n}),$$

и показать, что это гомоморфизм групп. В данном случае надо проверить, что $h(AB) = h(A) + h(B)$ и $h(E) = 0$ (строка из нулей). Затем надо доказать сюръективность h и вычислить его ядро.

4.59. Пусть дана группа

$$G = \begin{pmatrix} G_1 & F \\ 0 & G_2 \end{pmatrix},$$

состоящая из матриц вида

$$\begin{pmatrix} x & z \\ 0 & y \end{pmatrix},$$

где $x \in G_1$, $y \in F$, $z \in G_2$, множество F является кольцом (или полем), G_1 и G_2 — подгруппы мультипликативной группы обратимых элементов F. Допустим, что имеются два гомоморфизма групп $h_1 : G_1 \longrightarrow W_1$, $h_2 : G_2 \longrightarrow W_2$ и $H_1 = Ker(h_1)$, $H_2 = Ker(h_2)$. Рассмотрим группу $W = W_1 \times W_2$, и отображение $h : G \longrightarrow W$, соспоставляющее матрице

$$\begin{pmatrix} x & z \\ 0 & y \end{pmatrix} \in G$$

элемент $(h_1(x), h_2(y))$. Доказать, что

1) отображение h является гомоморфизмом групп;

2) гомоморфизм h является сюръективным, если сюръективны h_1 и h_2;

3) ядром гомоморфизма h является множество

$$H = \begin{pmatrix} H_1 & F \\ 0 & H_2 \end{pmatrix}.$$

Отсюда по теореме об изоморфизме будет следовать, что $G/H \cong W_1 \times W_2$.

В следующей группе упражнений для исходных данных того же типа, что и выше, требуется показать, что

а) G — группа;

б) H — нормальная подгруппа;

в) вычислить в явном виде факторгруппу G/H.

Предупреждение: подгруппы K, которые можно было найти в некоторых предыдущих задачах, здесь искать не стоит.

4.60.
$$G = \begin{pmatrix} \mathbb{R}^* & 0 \\ \mathbb{C} & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_2 & 0 \\ \mathbb{C} & \mathbb{R}^* \end{pmatrix}$$

4.61.
$$G = \begin{pmatrix} \mathbb{R}^* & 0 \\ \mathbb{C} & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}_+ & 0 \\ \mathbb{C} & \mathbf{U}_n \end{pmatrix}$$

4.62.
$$G = \begin{pmatrix} \mathbb{R}^* & 0 \\ \mathbb{C} & \mathbf{U} \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_2 & 0 \\ \mathbb{C} & \mathbf{U}_n \end{pmatrix}$$

4.63.
$$G = \begin{pmatrix} \mathbf{U} & \mathbb{C} \\ 0 & \mathbb{R}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_n & \mathbb{C} \\ 0 & \mathbb{R}_+ \end{pmatrix}$$

4.64.
$$G = \begin{pmatrix} \mathbb{C}^* & 0 \\ \mathbb{C} & \mathbf{K}_4 \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U} & 0 \\ \mathbb{C} & \mathbf{U}_4 \end{pmatrix}$$

4.65.
$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}^* & \mathbb{C} \\ 0 & \mathbb{R}_+ \end{pmatrix}$$

4.66.
$$G = \begin{pmatrix} \mathbf{K}_4 & \mathbb{C} \\ 0 & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_4 & \mathbb{C} \\ 0 & \mathbb{R}^* \end{pmatrix}$$

4.67.
$$G = \begin{pmatrix} \mathbf{K}_4 & \mathbb{C} \\ 0 & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}^* & \mathbb{C} \\ 0 & \mathbf{U}_n \end{pmatrix}$$

4.68.
$$G = \begin{pmatrix} \mathbf{K}_4 & \mathbb{C} \\ 0 & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}^* & \mathbb{C} \\ 0 & \mathbb{R}^* \end{pmatrix}$$

4.69.
$$G = \begin{pmatrix} \mathbf{K}_4 & \mathbb{C} \\ 0 & \mathbf{K}_4 \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_4 & \mathbb{C} \\ 0 & \mathbb{R}^* \end{pmatrix}$$

4.70.

$$G = \begin{pmatrix} \mathbf{K}_4 & \mathbb{C} \\ 0 & \mathbf{K}_4 \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}^* & \mathbb{C} \\ 0 & \mathbb{R}_+ \end{pmatrix}$$

4.71.

$$G = \begin{pmatrix} \mathbb{C}^* & 0 \\ \mathbb{C} & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}^* & 0 \\ \mathbb{C} & \mathbf{U} \end{pmatrix}$$

4.72.

$$G = \begin{pmatrix} \mathbb{R}^* & \mathbb{C} \\ 0 & \mathbf{U} \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_2 & \mathbb{C} \\ 0 & \mathbf{U}_n \end{pmatrix}$$

4.73.

$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}^* & \mathbb{C} \\ 0 & \mathbb{R}_+ \end{pmatrix}$$

4.74.

$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}^* & \mathbb{C} \\ 0 & \mathbb{R}^* \end{pmatrix}$$

4.75.

$$G = \begin{pmatrix} \mathbf{K}_4 & 0 \\ \mathbb{C} & \mathbf{K}_4 \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}^* & 0 \\ \mathbb{C} & \mathbb{R}^* \end{pmatrix}$$

4.76.

$$G = \begin{pmatrix} \mathbb{C}^* & 0 \\ \mathbb{C} & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_n & 0 \\ \mathbb{C} & \mathbb{R}_+ \end{pmatrix}$$

4.77.

$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}_+ & \mathbb{C} \\ 0 & \mathbf{U}_n \end{pmatrix}$$

4.78.

$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_n & \mathbb{C} \\ 0 & \mathbf{U} \end{pmatrix}$$

4.79.

$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_n & \mathbb{C} \\ 0 & \mathbf{U}_n \end{pmatrix}$$

4.80.

$$G = \begin{pmatrix} \mathbf{K}_4 & \mathbb{C} \\ 0 & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbb{R}^* & \mathbb{C} \\ 0 & \mathbb{R}_+ \end{pmatrix}$$

4.81.

$$G = \begin{pmatrix} \mathbb{C}^* & 0 \\ \mathbb{C} & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{K}_4 & 0 \\ \mathbb{C} & \mathbf{U}_n \end{pmatrix}$$

4.82.

$$G = \begin{pmatrix} \mathbb{C}^* & \mathbb{C} \\ 0 & \mathbf{K}_4 \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_n & \mathbb{C} \\ 0 & \mathbb{R}_+ \end{pmatrix}$$

4.83.

$$G = \begin{pmatrix} \mathbf{U} & 0 \\ \mathbb{C} & \mathbf{K}_4 \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_n & \mathbb{C} \\ \mathbb{C} & \mathbf{U}_2 \end{pmatrix}$$

4.84.

$$G = \begin{pmatrix} \mathbb{R}^* & \mathbb{C} \\ 0 & \mathbb{C}^* \end{pmatrix}, \quad H = \begin{pmatrix} \mathbf{U}_2 & \mathbb{C} \\ 0 & \mathbf{K}_4 \end{pmatrix}$$

Литература

[1] Кострикин А.И. Введение в алгебру. Часть I. Основы алгебры. — 2-е изд., исправл. — М.: Физ.-мат. лит., 2001. — 272 с.

[2] Кострикин А.И. Введение в алгебру. Часть II. Линейная алгебра. — 2-е изд., исправл. — М.: Физ.-мат. лит., 2001. — 368 с.

[3] Кострикин А.И. Введение в алгебру. Часть III. Основные структуры. — 2-е изд., исправл. — М.: Физ.-мат. лит., 2001. — 272 с.

[4] Сборник задач по алгебре / Под ред. А.И. Кострикина. — М.: Наука. Гл.ред. физ.-мат. лит. , 1987. — 352 с.

[5] Белоногов В.А. Задачник по теории групп. — М.: Наука, 2000. — 239 с.

[6] Курош А.Г. Теория групп. — 3-е изд. — М.: Наука. Гл. ред. физ.-мат. лит., 1967. — 648 с.

[7] Холл М. Теория групп. — М: ИЛ, 1962. — 468 с.

[8] Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. — 3-е изд., перераб. и доп. — М.: Наука, 1982. — 288 с.

[9] Богопольский О.В. Введение в теорию групп. — Москва-Ижевск: Институт компьютерных исследований, 2002. — 148 с.

[10] Ван-дер-Варден Б.Л. Алгебра. — М.:Наука, 1976. — 648 с.

[11] Ленг С. Алгебра. — М.: Мир, 1968 — 564 с.

[12] Скорняков Л.А. Элементы алгебры. — М.: Наука. Гл.ред. физ.-мат. лит. , 1980. — 240 с.

[13] Бахтурин Ю.А. Основные структуры современной алгебры. — М.: Наука, 1990. — 320 с.

[14] Фаддеев Д.К. Лекции по алгебре. — Изд. 3-е, стер. — СПб.: Лань, 2004. — 415 с.

[15] Винберг Э.Б. Курс алгебры. — 3-е изд., перераб. и доп. — М.: Факториал Пресс, 2002. — 544 с.

[16] Коксетер Г.С.М., Мозер У.О. Порождающие элементы и определяющие соотношения дискретных групп. — М.: Наука. Гл. ред. физ.-мат. лит., 1980. — 240 с.

[17] Кэртис Ч., Райнер И. Теория представлений конечных групп и ассоциативных алгебр. — М.: Наука. Гл. ред. физ.-мат. лит., 1980. — 668 с.

[18] Клейн Ф. Лекции об икосаэдре и решении уравнений пятой степени. — М.: Наука. Гл. ред. физ.-мат. лит., 1989. — 336 с.

[19] Дьедонне Ж. Линейная алгебра и элементарная геометрия. — М.: Наука. Гл.ред. физ.-мат. лит. , 1972. — 336 с.

[20] Бранец В.Н., Шмыглевский И.П. Применение кватернионов в задачах оринтации твердого тела. — М.: Наука. Гл.ред. физ.-мат. лит., 1973. — 320 с.

[21] Кантор И.Л., Солодовников А.С. Гиперкомплексные числа. — М.: Наука. Гл.ред. физ.-мат. лит., 1973. — 144 с.

[22] Гильберт Д., Кон-Фоссен С. Наглядная геометрия. — 3-е изд. — М.: Наука, 1981. — 344 с.

[23] Вейль Г. Симметрия. — М.: Наука. Гл. ред. физ.-мат. лит., 1968. — 192 с.

[24] Головина Л.И. Линейная алгебра и некоторые ее приложения. — Изд. 2-е, дополн. — М.: Наука. Гл. ред. физ.-мат. лит., 1975. — 408 с.

[25] Шубников А.В., Копцик В.А. Симметрия в науке и искусстве. — Изд. 3-е, дополн. — Москва-Ижевск: Ин-т компьютерн. исслед., 2004. — 560 с.

[26] Эллиот Дж., Добер П. Симметрия в физике. Том 1. Основные принципы и простые приложения. — М.: Мир, 1983. — 368 с.

[27] Эллиот Дж., Добер П. Симметрия в физике. Том 2. Дальнейшие приложения. — М.: Мир, 1983. — 416 с.

[28] Любарский Г.Я. Теория групп и физика. — М.: Наука. Гл. ред. физ.-мат. лит., 1986. — 224 с.

[29] Винберг Э.Б. Линейные представления групп. — М.: Наука. Гл. ред. физ.-мат. лит., 1985. — 144 с.

[30] Медведев Б.В. Начала теоретической физики. — М.: Наука. Гл. ред. физ.-мат. лит., 1977. — 496 с.