МИНОБРНАУКИ РОССИИ

Санкт-Петербургский государственный
электротехнический университет «ЛЭТИ»

Алгебраические структуры

Примеры и задачи

Санкт-Петербург
Издательство СПбГЭТУ «ЛЭТИ»
2010

УДК 512

Алгебраические структуры: Примеры и задачи / Сост.: Н. А. Жарковская, И. Г. Зельвенский, Ю. В. Крашенинникова, В. А. Смирнова. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2010. 32 с.

Содержат определения, формулировки основных теорем и примеры решения задач по теме «Алгебраические структуры».

Предназначены для поддержки алгебраических дисциплин на ФКТИ.

Утверждено
редакционно-издательским советом университета
в качестве методических указаний

Быстрое развитие компьютерных технологий сопровождается заметным расширением сферы применения алгебраических понятий и методов. Такие области как шифрование и кодирование, обработка звуковых сигналов и изображений, распознавание образов широко используют базовые алгебраические структуры: группы, кольца и поля. В связи с этим все более широкому кругу специалистов становится необходимым знакомство с основными алгебраическими конструкциями.

Настоящие методические указания разработаны в помощь студентам, изучающим курс алгебры, и ориентированы в первую очередь на решение задач. В настоящем издании содержатся подробные решения типовых задач по основным темам курса, посвященным алгебраическим структурам.

Каждый раздел методических указаний содержит необходимые определения, формулировки наиболее важных теорем и ряд примеров, иллюстрирующих эти сведения. Набор рассмотренных задач ориентирован на выработку базовых навыков оперирования с наиболее употребительными структурами.

1. Группы

1.1. Примеры групп

Определение 1.1. Множество G с бинарной операцией $\bullet$ называется группой, если:

1) операция $\bullet$ ассоциативна, т. е. $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ для $\forall\ a, b, c \in G$;

2) в G существует нейтральный элемент, т. е. такой элемент $e \in G$, что $a \bullet e = e \bullet a = a$ для $\forall\ a \in G$;

3) для $\forall\ a \in G$ существует обратный элемент, т. е. такой элемент $a' \in G$, что $a' \bullet a = a \bullet a' = e$.

Если, кроме того, операция $\bullet$ коммутативна, то группа G называется коммутативной или абелевой. Символы $\operatorname{card} G$, $|G|$ используются для обозначения мощности группы (числа элементов конечной группы). Группы с операцией умножения принято называть мультипликативными, а группы с операцией сложения − аддитивными.

Пример 1.1. Проверить, являются ли группами следующие множества:

1) $(G,\ +)$, где G — одно из множеств ***N***, ***Z***, ***Q***, ***R***, ***C***;

2) $\left(G^*,\ \cdot\right)$, где $G^* = G \setminus \{0\}$ и G − одно из множеств ***N***, ***Z***, ***Q***, ***R***, ***C***;

3) G − множество верхних треугольных матриц порядка n относительно операции умножения матриц;

4) множество комплексных чисел с фиксированным модулем r относительно умножения;

5) множество $[0, 1)$ с операцией $x \bullet y = \{x + y\}$ (через $\{x\}$ обозначается дробная часть вещественного числа);

6) множество корней степени n из единицы с операцией умножения.

Решение.

1. Множество ($\boldsymbol{N}$, +) не является группой, поскольку среди натуральных чисел отсутствуют нейтральный и противоположные элементы относительно операции сложения. Все остальные множества − группы, причем группы абелевы. Действительно, в любом из этих множеств число 0 является нейтральным элементом относительно сложения, а противоположное для числа a число $-a$ является обратным: $e = 0,\ a' = -a \quad \forall a \in G$.

2. Обратной по отношению к операции умножения в числовых множествах является операция деления. Множества натуральных и целых чисел не замкнуты относительно операции деления, а значит, не каждое такое число имеет обратный элемент. Поэтому эти множества не являются группами. Множества ($\boldsymbol{Q}^*$,·), ($\boldsymbol{R}^*$,·), ($\boldsymbol{C}^*$,·) — абелевы группы, в которых $e = 1$ и $a' = a^{-1} \quad \forall a \in G^*$.

3. Напомним, что множество верхних треугольных матриц замкнуто относительно операций умножения и обращения. То же самое верно для нижних треугольных матриц.

Проверим выполнение требований 1−3 определения группы. Из курса линейной алгебры известно [2, с. 157], что операция умножения матриц обладает свойством ассоциативности, а нейтральным элементом по умножению во множестве квадратных матриц одного и того же порядка является единичная матрица. В роли обратного элемента к матрице A выступает обратная матрица A^{-1}, которая существует тогда и только тогда, когда $|A| \neq 0$. Но для треугольной матрицы определитель равен произведению диагональных элементов, и если хотя бы один элемент на главной диагонали матрицы равен нулю, то она необратима. Вывод: G − не группа.

Если мы будем рассматривать только невырожденные матрицы, то у каждой матрицы будет обратный по умножению элемент (поскольку определитель

произведения матриц равен произведению их определителей, новое множество замкнуто относительно операции умножения матриц).

Итак, множество невырожденных верхних треугольных матриц является группой.

4. Рассмотрим модуль произведения двух комплексных чисел: $|z_1 \cdot z_2| = |z_1| \cdot |z_2| = r^2 = r$. Из этого равенства следует, что множество чисел с одинаковым модулем r замкнуто относительно операции умножения только в двух случаях: $r = 1$ или $r = 0$. Легко проверить, что все остальные аксиомы группы выполняются, следовательно, оба множества являются группами.

Заметим, что во втором случае множество состоит только из одного элемента $z = 0$. Операция умножения, определенная равенством $0 \cdot 0 = 0$, удовлетворяет всем требованиям определения группы, причем ноль играет роль нейтрального элемента по умножению и обратного по отношению к себе.

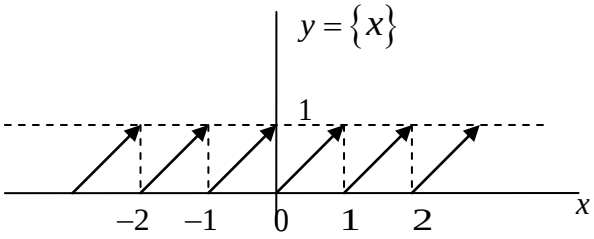

Рис. 1.1

Замечание 1.1. Всякое множество, состоящее из одного элемента x, имеет структуру группы относительно операции $x \bullet x = x$.

5. Функция $y = \{x\}$ является периодической с периодом 1, а множество ее значений есть промежуток $[0, 1)$ (рис. 1.1). Значит, множество $[0, 1)$ замкнуто относительно бинарной операции $x \bullet y = \{x + y\}$. Покажем, что данная операция ассоциативна. Выразим дробную часть числа через его целую часть: $\{x\} = x - [x]$, $[x] \in \boldsymbol{Z}$, и воспользуемся периодичностью функции $y = \{x\}$:

$$(x \bullet y) \bullet z = \{\{x + y\} + z\} = \{x + y - [x + y] + z\} = \{x + y + z\} =$$

$$= \{x + y + z - [y + z]\} = \{x + \{y + z\}\} = x \bullet (y \bullet z).$$

Ясно, что нейтральным элементом относительно данной операции является число 0, так как $0 \bullet x = x \bullet 0 = \{x + 0\} = \{x\} = x$ для любого $x \in [0, 1)$. Если для элемента x существует обратный элемент $x^{-1} \in [0, 1)$, то $x + x^{-1} \in [0, 2)$, но тогда $0 = x \bullet x^{-1} = \{x + x^{-1}\} = x + x^{-1} - [x + x^{-1}] = \begin{bmatrix} x + x^{-1} \\ x + x^{-1} - 1 \end{bmatrix} \Rightarrow \begin{bmatrix} x^{-1} = -x \\ x^{-1} = 1 - x \end{bmatrix}$.

Первое равенство возможно только для элемента $x=0$, а второе – для всех $x\in(0,\ 1)$. Итак, промежуток $[0,\ 1)$ с операцией $x\bullet y=\{x+y\}$ – группа.

6. Множество G корней степени n из единицы содержит n элементов: $\xi_k=\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}=e^{i\frac{2\pi k}{n}}$, $k=0,\ 1,\ \ldots,\ n-1$. Проверим, замкнуто ли множество G относительно операции умножения. Так как $\xi_k^n=1$ и $\xi_l^n=1$ $\forall\xi_k,\ \xi_l\in G$, то $(\xi_k\cdot\xi_l)^n=\xi_k^n\cdot\xi_l^n=1$. Таким образом, $\xi_k\cdot\xi_l\in G$, причем $\xi_k\cdot\xi_l=\xi_{k+l}$ (если $k+l>n$, то заменим его остатком от деления на n). Операция умножения на множестве комплексных чисел ассоциативна, а значит, она ассоциативна и на множестве G. Нейтральный относительно умножения чисел элемент 1 содержится в G, так как $1^n=1$ (заметим, что в наших обозначениях $1=\xi_0$). Каждый элемент ξ_k обратим в G: $\left(\xi_k^{'}\right)^n=\left(\frac{1}{\xi_k}\right)^n==\frac{1}{\xi_k{}^n}=1$, где $\xi_k^{'}=\xi_{n-k}$, $k=1,\ 2,\ \ldots,\ n-1$. Итак, множество G с операцией умножения является группой. Далее будем обозначать ее как C_n.

Определение 1.2. Группа, порожденная одним элементом, называется циклической группой и обозначается $\langle a\rangle$.

Мультипликативно записанная группа $\langle a\rangle=\{a^n\mid n\in N\}$ состоит из степеней одного элемента a. В циклической группе $\langle a\rangle=\{a^n\mid n\in N\}$ нейтральным элементом является a^0, а $a^{-n}=\left(a^n\right)^{-1}$. Если все степени элемента a различны, то $\langle a\rangle$ – бесконечная циклическая группа. Если же имеются совпадения $a^n=a^m$ $(n\neq m)$, то есть положительные степени элемента a, равные нейтральному элементу. Тогда $\langle a\rangle=\left\{e,\ a,\ a^2,\ \ldots,\ a^{q-1}\right\}$ – группа порядка q, где q – наименьший положительный показатель степени, для которого $a^q=e$.

Мультипликативная группа C_n, рассмотренная в примере 1.1, является циклической группой порядка n, порожденной элементом $e^{2\pi i/n}$.

Действительно, $\xi_k=\left(e^{2\pi i/n}\right)^k$, причем $\left(e^{2\pi i/n}\right)^n=1$.

В аддитивной записи циклическая группа имеет вид $\langle a\rangle = \{na \mid n \in N\}$. Примером бесконечной аддитивной циклической группы служит $Z = \langle 1\rangle$.

Симметрическая группа. Пусть $M = \{1,\ 2,\ \ldots,\ n\}$ конечное множество из n элементов. Группа $S_n = S(M)$ всех взаимно однозначных отображений множества M на себя с операцией умножения (композиции) называется симметрической группой степени n. Элементы симметрической группы называют подстановками. Число элементов группы S_n совпадает с числом перестановок n элементов $P_n = n!$. Действие подстановки π на множестве удобно описывать, указывая образы всех элементов множества M:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}, \text{ где } i_k = \sigma(i),\ k = 1,\ 2,\ \ldots,\ n.$$

Поскольку подстановки представляют собой взаимно однозначные отображения, то в строке образов все элементы i_k различны и исчерпывают все множество M. Подстановки $\sigma,\ \tau \in S_n$ умножаются в соответствии с общим правилом композиции отображений: $\sigma \cdot \tau(i) = \sigma(\tau(i))$. Нейтральным элементом в группе является тождественная подстановка $e(i) = i,\ i = 1,\ 2,\ \ldots,\ n$. Обратным элементом по отношению к подстановке σ служит обратное отображение σ^{-1}, для которого $i = \sigma^{-1}(i_k),\ k = 1,\ 2,\ \ldots,\ n$. Заметим, что операция умножения подстановок некоммутативна.

Пример 1.2. Найти в группе S_5 элемент $\sigma^{-1} \cdot \tau$, если $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}$.

Решение. Сначала построим элемент, обратный к σ. Для этого в подстановке σ поменяем местами ряд прообразов и ряд образов, попутно упорядочивая столбцы по возрастанию аргумента: $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix}$. Теперь найдем произведение подстановок, подействовав на элементы M сначала подстановкой τ, а затем подстановкой σ^{-1}:

$$\sigma^{-1}\cdot\tau=\begin{bmatrix}1&2&3&4&5\\ \downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\ 4&1&5&3&2\\ \downarrow&\downarrow&\downarrow&\downarrow&\downarrow\\ 2&3&5&4&1\end{bmatrix}=\begin{pmatrix}1&2&3&4&5\\ 2&3&5&4&1\end{pmatrix}.$$

Подстановка называется циклом длины k, если на некотором подмножестве $\{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\}$ множества M она действует следующим образом: $\begin{pmatrix} a_{i_1} & a_{i_2} & \ldots & a_{i_{k-1}} & a_{i_k} \\ a_{i_2} & a_{i_3} & \ldots & a_{i_k} & a_{i_1} \end{pmatrix}$, а остальные элементы множества M не изменяет. Цикл принято обозначать $(a_{i_1}, a_{i_2}, \ldots, a_{i_k})$. Два цикла называются независимыми, если они действуют на непересекающихся подмножествах M. Ясно, что независимые циклы коммутируют. Пусть σ – цикл длины k. Тогда он порождает в S_n циклическую подгруппу (см. 1.2) $\langle\sigma\rangle = \{e, \sigma, \sigma^2, \ldots, \sigma^{k-1}\}$ порядка k, в которой роль нейтрального элемента исполняет, как обычно, нейтральная подстановка, и $(\sigma^s)^{-1}=\sigma^{k-s}$, $s=1, 2, \ldots, k-1$.

Пример 1.3. Найти произведение подстановок $\sigma_1=(1375)(264)$ и $\sigma_2=(168)(25)(37)$ (ответ привести в циклической форме).

Решение. Запишем сначала подстановки в стандартном виде (как отображение):

$$(1375)(264)=\begin{pmatrix}1&2&3&4&5&6&7&8\\ 3&6&7&2&1&4&5&8\end{pmatrix},$$

$$(168)(25)(37)=\begin{pmatrix}1&2&3&4&5&6&7&8\\ 6&5&7&4&2&8&3&1\end{pmatrix}.$$

Далее, рассуждая как в примере 1.2, вычислим произведение подстановок, подействовав на элементы M сначала подстановкой σ_2, а затем подстановкой σ_1: $\sigma_1\square\sigma_2=\begin{pmatrix}1&2&3&4&5&6&7&8\\ 4&1&5&2&6&8&7&3\end{pmatrix}$. Легко видеть, что произведение подстановок оставляет на своем месте 7, а на непересекающихся подмножествах

{1, 2, 4} и {3, 5, 6, 8} действует как циклы $\begin{pmatrix}1 & 4 & 2\\ 4 & 2 & 1\end{pmatrix}$, $\begin{pmatrix}3 & 5 & 6 & 8\\ 5 & 6 & 8 & 3\end{pmatrix}$, следовательно, $\sigma_1\sigma_2 = (142)(3568)$ (цикл единичной длины в записи принято опускать, так как он однозначно восстанавливается по остальным циклам).

Теорема 1.1 [3, с. 150]. Каждая подстановка $\sigma \neq e$ в S_n является произведением независимых циклов. Это разложение в произведение определено однозначно с точностью до порядка следования циклов.

Следствие. Порядок подстановки σ равен НОК (наименьшему общему кратному) длин независимых циклов, входящих в разложение σ. Порядок подстановки является порядоком циклической подгруппы $\langle\sigma\rangle$.

Пример 1.4. Разложить подстановку σ в произведение непересекающихся циклов, определить порядок подстановки и вычислить σ^2 и σ^3, где $\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 4 & 1 & 2 & 3 & 6 & 7 & 9 & 8 & 5\end{pmatrix}$.

Решение. Подстановка раскладывается в произведение непересекающихся циклов $\sigma = \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 9\\ 6 & 7 & 9 & 5\end{pmatrix} = (1432)(5679)$. Порядок подстановки равен НОК $(4,\ 4) = 4$, т. е. циклическая подгруппа, порожденная подстановкой, состоит из 4 элементов $\langle\sigma\rangle = \{e,\ \sigma,\ \sigma^2,\ \sigma^3\}$. Наконец,

$$\sigma^2 = (1234)^2(5976)^2 = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 3 & 4 & 1 & 2 & 7 & 9 & 5 & 8 & 6\end{pmatrix} = (13)(24)(57)(69),$$

$$\sigma^3 = (1432)^3(5679)^3 = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 2 & 3 & 4 & 1 & 9 & 5 & 6 & 8 & 7\end{pmatrix} = (1234)(5976).$$

В последнем случае результат можно получить по-другому: $\sigma^3 = \sigma^{-1}$.

Пример 1.5. Каков максимальный порядок элемента в группе S_7?

Решение. Прежде всего, группа S_7 содержит циклы с длинами от 1 до 7. Выпишем возможные представления числа 7 в виде суммы положительных слагаемых: 6 + 1; 5 + 2; 5 + 1 + 1; 4 + 3; 4 + 2 + 1; 4 + 1 + 1 + 1; 3 + 3 + 1; 3 + + 2 + 2; 3 + 2 + 1 + 1; 3 + 1 + 1 + 1 + 1; 2 + 2 + 2 + 1; 2 + 2 + 1 + 1 + 1; 2 + 1 + + 1 + 1 + 1+ 1 (плюс еще два случая, когда подстановка уже есть цикл длины 7 или тождественна). Каждое такое представление отвечает какому-то разложению

подстановки в произведение непересекающихся циклов, и слагаемые равны длинам этих циклов. Считая НОК слагаемых в каждой сумме, получим все возможные порядки подстановок в S_7: 1, 2, 3, 4, 5, 6, 7, 10, 12. Максимальный порядок элемента в группе S_7 равен 12.

1.2. Подгруппы. Смежные классы по подгруппе

Определение 1.3. Подгруппой группы $(G, \bullet)$ называется такое подмножество H группы G, которое само является группой относительно бинарной операции $\bullet$, заданной в G.

Лемма 1.1. Для того чтобы подмножество H группы G являлось подгруппой, необходимо и достаточно, чтобы H было замкнуто относительно операции, введенной в G, и любой элемент из H был обратим.

Замечание 1.2. Любая подгруппа циклической группы $\langle a \rangle$ – циклическая группа. Она состоит или из единичного элемента, или из степеней элемента a^m (m – наименьший среди положительных показателей степени для элементов этой подгруппы).

Для бесконечной циклической группы число m может быть любым, а для циклической группы порядка n число m должно быть некоторым делителем n. В последнем случае подгруппа $\left\langle a^m \right\rangle$ имеет порядок $\frac{n}{m}$.

Определение 1.4. Пусть H − подгруппа группы $(G, \bullet)$. Левым смежным классом группы G по подгруппе H называется множество $aH = = \{ah : h \in H\}$, где a − фиксированный элемент группы G.

Аналогично определяются правые смежные классы Ha. Отметим следующие факты:

1) одним из смежных классов является сама подгруппа $H = eH = He$. Никакой другой смежный класс подгруппой не является (например, там нет нейтрального элемента);

2) число элементов во всех смежных классах одинаково и равно $|H|$;

3) в коммутативных группах соответствующие левые и правые смежные классы совпадают: $aH = Ha \quad \forall a \in H$;

4) разбиение G на левые (правые) классы индуцирует на G отношение эквивалентности $a \square b \Leftrightarrow a^{-1} \bullet b \in H$ ($a \square b \Leftrightarrow b \bullet a^{-1} \in H$), следовательно, смежные классы не пересекаются, а их объединение дает всю группу G.

Определение 1.5. Индексом $(G:H)$ подгруппы H в группе G называют число различных левых (правых) смежных классов по подгруппе H, если это число конечно.

Теорема Лагранжа. Порядок конечной группы равен произведению порядка подгруппы на индекс этой подгруппы, т. е. $|G|=|H|(G:H)$.

Определение 1.6. Подгруппа называется нормальной, если для любого $a \in G$ соответствующие левые и правые классы совпадают: $aH = Ha$.

Определение 1.7. Факторгруппой группы $(G,\ \bullet)$ по нормальной подгруппе H называется множество смежных классов $G \setminus H$ с операцией $aH \bullet bH = (a \bullet b)H$. Факторгруппа обозначается G/H.

Пример 1.6. Построить факторгруппу Z/mZ.

Решение. Согласно замечанию 1.2 бесконечная циклическая группа (***Z***, +) имеет циклические подгруппы вида $\langle m\rangle = \{mk, k \in Z\}$, состоящие из целых чисел, кратных m. Такие подгруппы обозначают $m\boldsymbol{Z}$. Так как любая подгруппа абелевой группы нормальна, то достаточно построить только левые смежные классы. Два целых числа x и y попадают в один смежный класс, если $-x + y = mk, k \in Z$, т. е. эти числа сравнимы по модулю m (имеют один и тот же остаток при делении на m). Принято это записывать так: $x \equiv y \pmod m$. Отношение сравнения по модулю на множестве Z является отношением эквивалентности [1, с. 4, 5] и порождает разбиение множества целых чисел на непересекающиеся классы эквивалентности, называемые классами вычетов по модулю m: $Z_m = \{0\}_m \cup \{1\}_m \cup \ldots \cup \{m-1\}_m$, где $\{r\}_m = \{ml + r: l \in Z\},\ r = 0,\ 1,\ \ldots,\ m-1$. Обозначим $\{r\}_m = \bar{r}$ и составим из полученных классов вычетов множество $\boldsymbol{Z}_m = \left\{\bar{0},\ \bar{1},\ \ldots,\ \overline{m-1}\right\}$, т. е. фактормножество множества ***Z*** по отношению сравнения по модулю m.

Итак, смежные классы группы ***Z*** по подгруппе $m\boldsymbol{Z}$ есть классы вычетов по модулю m, а факторгруппа $Z/mZ = \boldsymbol{Z}_m = \left\{\bar{0},\ \bar{1},\ \ldots,\ \overline{m-1}\right\}$. Операция сложения классов вычетов $\bar{r} + \bar{k} = \overline{r+k}$ сводится к соответствующей операции над представителями этих классов. Например, $\bar{2} + \bar{9} = \bar{1}$ в группе $\boldsymbol{Z}_{10}$, так как для представителей этих классов имеем: $2 + 9 = 11 = 10 \cdot 1 + 1$. В факторгруппе $\boldsymbol{Z}_m$ нейтральный элемент $e = \bar{0}$ и $-\bar{r} = \overline{m-r},\ r = 1,\ 2,\ \ldots,\ m-1$.

Пример 1.7. Построить факторгруппу $Z_{20}/5Z_{20}$.

Решение. Рассмотрим группу $Z_{20} = \{\bar{0},\ \bar{1}, \ldots, \overline{19}\}$. Группа Z_{20} − циклическая порядка 20, порожденная классом вычетов $\bar{1}$. Подгруппы Z_{20} порождаются классами вычетов вида $\overline{m}$, где m − делители числа 20 и имеют порядок, равный $\frac{20}{m}$ (см. замечание 1.2). Подгруппа $5Z_{20} = \langle\bar{5}\rangle = \{\bar{0},\ \bar{5}, \overline{10}, \overline{15}\}$ состоит из классов вычетов, элементы которых при делении на 20 дают остаток, кратный 5. Построим левые смежные классы по этой подгруппе. По теореме Лагранжа индекс подгруппы $5Z_{20}$ равен 20/4=5. Рассуждая, как в примере 1.6, получим, что два класса вычетов $\bar{k}$ и $\bar{l}$ попадают в один и тот же смежный класс по подгруппе $5Z_{20}$, если $k \equiv l \pmod 5$. Выпишем все получающиеся смежные классы: $5Z_{20} = \bar{0} + 5Z_{20} = \{\bar{0},\ \bar{5}, \overline{10}, \overline{15}\}$, $\bar{1} + 5Z_{20} = \{\bar{1},\ \bar{6}, \overline{11}, \overline{16}\}$, $\bar{2} + 5Z_{20} = \{\bar{2},\ \bar{7}, \overline{12}, \overline{17}\}$, $\bar{3} + 5Z_{20} = \{\bar{3}, \bar{8}, \overline{13}, \overline{18}\}$, $\bar{4} + 5Z_{20} = \{\bar{4}, \bar{9}, \overline{14}, \overline{19}\}$. Итак, $Z_{20}/5Z_{20} = \{5Z_{20}, \bar{1} + 5Z_{20},\ \bar{2} + 5Z_{20}, \bar{3} + 5Z_{20}, \bar{4} + 5Z_{20}\}$. Заметим, что в данном случае построить смежные классы можно было, пользуясь непосредственно определением 1.4.

Пример 1.8. Построить факторгруппу R/Z.

Решение. Два вещественных числа x и y попадают в один смежный класс по подгруппе $\boldsymbol{Z}$, если $– x + y = k$, $k \in \boldsymbol{Z}$, т. е. они имеют одну и ту же дробную часть (см. пример 1.1).

Обозначим смежный класс $x + Z = \bar{x} = \{y \in R | \{y\} = \{x\}\}$**.** Бинарная операция над смежными классами осуществляется по правилу $\bar{x} + \bar{y} = \overline{x + y}$. Итак, $R/Z = \{\bar{x},\ x \in [0,\ 1)\}$**.**

Пример 1.9. Разложить на левые (правые) смежные классы группу матриц $\mathrm{GL}_n(\boldsymbol{R})$ по подгруппе матриц $\mathrm{SL}_n(\boldsymbol{R})$.

Решение. $\mathrm{GL}_n(\boldsymbol{R})$ − мультипликативная группа невырожденных матриц порядка n с вещественными элементами, $\mathrm{SL}_n(\boldsymbol{R})$ − подгруппа матриц, определитель которых равен 1. Выясним условия, при которых матрицы попадают в один и тот же левый смежный класс. Пусть $A^{-1}\mathrm{B} \in SL_n(R)$, т. е. $\left|A^{-1}B\right| = 1$. Но, $\left|A^{-1}B\right| = \left|A^{-1}\right||B| = \frac{|B|}{|A|}$, откуда получаем $|A| = |B|$. Итак, левый смежный класс со-

стоит из всех матриц с равными определителями $A \cdot SL_n(R) = \bar{A} = \{X \in SL_n(R): |X| = |A|\}$. Построим правые смежные классы. Если $BA^{-1} \in \mathrm{SL}_n(\boldsymbol{R})$, то $\left|BA^{-1}\right| = |B| \cdot \left|A^{-1}\right| = \frac{|B|}{|A|} = 1 \Rightarrow |A| = |B|$. Значит, соответствующие правые и левые смежные классы совпадают и подгруппа $\mathrm{SL}_n(\boldsymbol{R})$ является нормальной. Разбиение на смежные классы порождает факторгруппу $\mathrm{GL}_n/\mathrm{SL}_n = \left\{\overline{A},\ A \in \mathrm{GL}_n\right\}$ с операцией $\overline{A} \cdot \overline{B} = \overline{AB}$.

1.3. Гомоморфизмы групп

Определение 1.8. Пусть $(G_1,\ \bullet)$ и $(G_2,\ *)$ − две группы, а f − отображение множества G_1 в множество G_2. Отображение f называется гомоморфизмом группы G_1 в группу G_2, если для любых $a,\ b \in G_1$ имеет место равенство $f(a \bullet b) = f(a) * f(b)$. Если, кроме того, f − биективное отображение, то f называется изоморфизмом G_1 на G_2. Записывается это так: $G_1 \cong G_2$.

Нейтральный элемент группы G_1 любым гомоморфизмом переводится в нейтральный элемент группы G_2. Кроме того, $f\left(a^{-1}\right) = f(a)^{-1},\ \forall a \in G_1$.

Определение 1.9. Пусть f − гомоморфизм группы G_1 в группу G_2. Ядром гомоморфизма $\mathrm{Ker}\, f$ называется множество прообразов нейтрального элемента группы G_2. Образом гомоморфизма $\mathrm{Im}\, f$ называется множество образов всех элементов группы G_1.

Лемма 1.2. Гомоморфный образ $f(H)$ любой подгруппы H группы G_1 является подгруппой в G_2 и, наоборот, полный прообраз $f^{-1}(S)$ любой подгруппы S группы G_2 является подгруппой в G_1.

Значит, ядро и образ гомоморфизма являются подгруппами групп G_1 и G_2 соответственно. В дальнейшем будем использовать следующую терминологию: эпиморфизм − сюръективный гомоморфизм ($\mathrm{Im}\, f$ есть G_2); мономорфизм − инъективный гомоморфизм ($\mathrm{Ker}\, f$ состоит только из нейтрального элемента); автоморфизм − изоморфное отображение группы на себя.

Пример 1.10. Пусть отображение f: $GL_5(\boldsymbol{R})\to GL_5(\boldsymbol{R})$ задано формулой $f(A)=\dfrac{A}{\sqrt[5]{|\det A|}}$. Доказать, что f − гомоморфизм групп. Найти его ядро и образ. Является ли f мономорфизмом, эпиморфизмом, изоморфизмом?

Решение. Прежде всего, заметим, что функция $f(A)=\dfrac{A}{\sqrt[5]{|\det A|}}$ имеет смысл на множестве невырожденных матриц и $f(A) \in GL_5(\boldsymbol{R})$. Покажем, что отображение f является гомоморфизмом групп: $f(A\cdot B)=\dfrac{A\cdot B}{\sqrt[5]{|\det A\cdot B|}}=$

$=\dfrac{A\cdot B}{\sqrt[5]{|\det A\cdot \det B|}}=\dfrac{A}{\sqrt[5]{|\det A|}}\cdot\dfrac{B}{\sqrt[5]{|\det B|}}=f(A)\cdot f(B)$. Равенство $\dfrac{A}{\sqrt[5]{|\det A|}}=E$, где E − единичная матрица пятого порядка, определяет $\operatorname{Ker} f$. Ясно, что этому равенству удовлетворяют все скалярные матрицы, то есть, матрицы вида λE.

Кроме того, отображение f накладывает ограничения на определитель образа произвольной матрицы из данной группы $GL_5(\boldsymbol{R})$:

$$\det f(A)=\det\frac{A}{\sqrt[5]{|\det A|}}=\left(\frac{1}{\sqrt[5]{|\det A|}}\right)^5\det A=\frac{\det A}{|\det A|}=\pm 1.$$

Итак, f − гомоморфизм, $\operatorname{Ker} f = \{\lambda E \mid \lambda \in \boldsymbol{R}^+\}$, $\operatorname{Im} f = \pm SL_5(R)$, отображение f не является ни эпиморфизмом, ни мономорфизмом.

Лемма 1.3. Пусть f − гомоморфизм группы G_1 в группу G_2. Ядро гомоморфизма f является нормальной подгруппой; смежные классы по ядру − это полные прообразы элементов из $\operatorname{Im} f$.

Определение 1.10. Подгруппа группы G, состоящая из тех элементов группы G, которые коммутируют (перестановочны) со всеми элементами группы, называется центром группы.

Ясно, что центр любой группы есть нормальная подгруппа.

Пример 1.11. Пусть H − центр группы $GL_3(\boldsymbol{R})$. Построить нетривиальный гомоморфизм f: $GL_3(\boldsymbol{R}) \to GL_3(\boldsymbol{R})$ с ядром H.

Решение. По определению центра группы $X \in H$, если $XA = AX$, $\forall A \in \mathrm{GL}_3(\boldsymbol{R})$. Таким свойством обладают только скалярные матрицы, т. е. необходимо, чтобы $\mathrm{Ker}\, f = \{\lambda E: \lambda \in \boldsymbol{R}\}$. Заметим, что для скалярных матриц третьего порядка верно равенство $\det(\lambda E) = \lambda^3 \det E = \lambda^3$, поэтому если положим $f(A) = \dfrac{A}{\sqrt[3]{\det A}}$, $\forall\, A \in \mathrm{GL}_3(\boldsymbol{R})$, то это отображение будет переводить скалярные матрицы (и только их) в единичную матрицу. Проверим, что f – гомоморфизм:

$$f(AB) = \frac{AB}{\sqrt[3]{\det AB}} = \frac{AB}{\sqrt[3]{\det A \cdot \det B}} = \frac{A}{\sqrt[3]{\det A}} \cdot \frac{B}{\sqrt[3]{\det B}} = f(A)\, f(B).$$

Остается заметить, что $\det f(A) = 1$ для всех матриц из $\mathrm{GL}_3(\boldsymbol{R})$, следовательно, $\mathrm{Im}\, f = \mathrm{SL}_3(R)$.

Пример 1.12. Построить эпиморфизм f: $\boldsymbol{Z} \to C_5$.

Решение. В примере 1.8 показано, что смежными классами группы $\boldsymbol{Z}$ по подгруппе $m\boldsymbol{Z}$ являются классы вычетов $\bar{0}$, $\bar{1}$, …, $\overline{m-1}$. Группа корней пятой степени из 1 содержит всего пять элементов: $e^{2\pi ki/5}$, $k = 0, 1, 2, 3, 4$. Значит, согласно лемме 1.3, смежных классов группы $\boldsymbol{Z}$ по ядру гомоморфизма $\mathrm{Ker}\, f$ должно быть ровно 5 классов: $\bar{0}$, $\bar{1}$, $\bar{2}$, $\bar{3}$, $\bar{4}$. Итак, $\mathrm{Ker}\, f = 5\boldsymbol{Z}$. Функция $f(n) = e^{2\pi ni/5}, \forall\, \mathrm{n} \in \boldsymbol{N}$ отображает числа из этой подгруппы в единицу: $f(5k) = e^{2\pi 5ki/5} = 1$. Из свойств показательной функции вытекает, что следующее отображение является гомоморфизмом:

$$f(k_1 + k_2) = e^{2\pi(k_1+k_2)i/5} = e^{2\pi k_1 i/5} \cdot e^{2\pi k_2 i/5} = f(k_1) \cdot f(k_2).$$

Таким образом, $f(n) = e^{2\pi ni/5}$ – эпиморфизм групп. Ясно, что $\mathrm{Z}_5 \cong \mathrm{C}_5$.

Замечание 1.3. Все циклические группы одного и того же порядка (в том числе и бесконечные) изоморфны. Функция $f(ka) = b^k$ устанавливает изоморфизм между циклическими группами одного и того же порядка, записанными аддитивно $(\langle a \rangle,\ +)$ и мультипликативно $(\langle b \rangle,\ \cdot)$. Например, $f(\bar{k}) = \left(e^{2\pi i/n}\right)^k$ есть изоморфизм групп Z_n и C_n.

Пример 1.13. Указать какой-нибудь нетривиальный гомоморфизм группы Z_6 в группу Z_8.

Решение. Группы $Z_6 = \langle \bar{1} \mid 6 \cdot \bar{1} = \bar{0} \rangle$ и $Z_8 = \langle \bar{1} \mid 8 \cdot \bar{1} = \bar{0} \rangle$ – аддитивные циклические группы шестого и восьмого порядков соответственно. Ненулевыми подгруппами Z_n являются подгруппы вида mZ_n. Пользуясь замечанием 1.2 и теоремой Лагранжа, выпишем для каждой группы возможные порядки подгрупп и соответствующие индексы этих подгрупп для Z_6. Полные прообразы всех элементов из $\mathrm{Im}\, f$ представляют собой смежные классы по ядру гомоморфизма, а $\mathrm{Im}\, f$ есть подгруппа Z_8. Значит, индекс ядра гомоморфизма должен совпадать с порядком образа гомоморфизма. В таблице только два совпадения: 1 и 2. В первом случае получаем тривиальный гомоморфизм: все элементы Z_6 отображаются в нейтральный элемент Z_8. Во втором случае $\mathrm{Im}\, f = 4Z_8 = \{\bar{0},\ \bar{4}\}$, а $\mathrm{Ker}\, f = 4Z_6 = \{\bar{0}, \bar{2}, \bar{4}\}$. Смежные классы по ядру гомоморфизма $Z_6/2Z_6 = \{2Z_6,\ 2Z_6 + \bar{1}\}$. Все элементы ядра гомоморфизма по определению отображаются в нейтральный элемент $\bar{0}$, а все элементы смежного класса $2Z_6 + \bar{1} = \{\bar{1}, \bar{3}, \bar{5}\}$ в $\bar{4}$. Легко проверить, что такое гомоморфное отображение осуществляется по правилу $f(k \cdot \bar{1}) = 4k \cdot \bar{1},\ k \in Z$.

Z_6	mZ_6	1	2	3	6
	(G: mZ_6)	6	3	**2**	**1**
Z_8	mZ_8	**1**	**2**	4	8

Теорема 1.2. Гомоморфный образ группы G изоморфен факторгруппе этой группы по ядру гомоморфизма, т. е. $\mathrm{Im}\, f \cong G/\mathrm{Ker}\, f$.

Пример 1.14. Пусть G – промежуток $[0, 1)$ с операцией $x * y = \{x + y\}$, а H – циклическая подгруппа в G, порожденная элементом $\frac{1}{5}$. Доказать, что $G/H \cong G$.

Решение. В примере 1.1 (п. 5) было доказано, что G – абелева группа. Элемент $\frac{1}{5}$ порождает в G циклическую подгруппу порядка 5: $\frac{1}{5} * \frac{1}{5} = \frac{2}{5}$; $\frac{1}{5} * \frac{2}{5} = \frac{3}{5}$; $\frac{1}{5} * \frac{3}{5} = \frac{4}{5}$; $\frac{1}{5} * \frac{4}{5} = \{1\} = 0$. Итак, $H = \left\{0,\ \frac{1}{5},\ \frac{2}{5},\ \frac{3}{5},\ \frac{4}{5}\right\}$. Для доказательства $G/H \cong G$ не обязательно строить факторгруппу G/H, достаточно установить эпиморфизм $f : G \to G$ с ядром H и сослаться на теорему 1.2.

Таким отображением служит функция $f(x)=\{5x\}$. Действительно, она переводит все элементы подгруппы H в 0: $f\left(\frac{k}{5}\right)=\{k\}=0$, $k=0,\ 1,\ 2,\ 3,\ 4$. Далее необходимо показать, что при отображении сохраняется действие, $f(x*y)=f(\{x+y\})=\{5\{x+y\}\}=\{5(x+y-[x+y])\}=\{5x+5y-$ $-5[x+y]\}=\{5x+5y\}$ и $f(x)*f(y)=\{\{5x\}+\{5y\}\}=\{5x-[5x]+5y-[5y]\}=$ $=\{5x+5y\}$. Видим, что $f(x*y)=f(x)*f(y)$, значит f – гомоморфизм. Осталось убедиться, что $\operatorname{Im} f$ есть вся группа G. Действительно, если $y=\{5x\}$, то $5x=[5x]+y$, где $[5x]=k$, $k=0,\ 1,\ 2,\ 3,\ 4$. Значит, полным прообразом любого элемента $y\in G$ будет являться смежный класс $\frac{y}{5}*H=$ $=\left\{\frac{y}{5}*\frac{k}{5}=\left\{\frac{y}{5}+\frac{k}{5}\right\}=\frac{y}{5}+\frac{k}{5},\ k=0,\ 1,\ 2,\ 3,\ 4\right\}$. Утверждение доказано.

Пример 1.15. Пусть H – циклическая подгруппа в $Z\oplus Z\oplus Z$, порожденная элементами $(1,\ 1,\ -3)$ и $(-2,\ 1,\ 1)$. Доказать, что $Z\oplus Z\oplus Z/H\cong Z$.

Решение. Элементами прямой суммы $Z\oplus Z\oplus Z$ являются всевозможные упорядоченные тройки целых чисел с бинарной операцией $(n_1,\ m_1,\ p_1)+(n_2,\ m_2,\ p_2)=(n_1+n_2,\ m_1+m_2,\ p_1+p_2)$, а элементами группы H – линейные комбинации троек $(1,\ 1,\ -3)$ и $(-2,\ 1,\ 1)$ с целыми коэффициентами. Построим эпиморфизм f: $Z\oplus Z\oplus Z\to Z$ с ядром H. Прежде всего заметим, что если $f(1,\ 0,\ 0)=\alpha$, $f(0,\ 1,\ 0)=\beta$, $f(0,\ 0,\ 1)=\gamma$, то для любого элемента $(x,\ y,\ z)$ группы $Z\oplus Z\oplus Z$ верно равенство $f(x,\ y,\ z)==\alpha x+\beta y+\gamma z$. Поскольку элементы группы H должны переводиться в нейтральный элемент образа, т. е. в 0, искомый гомоморфизм доложен удовлетворять условиям $f(1,\ 1,\ -3)=\alpha+\beta-3\gamma=0$ и $f(-2,\ 1,\ 1)=-2\alpha+\beta+\gamma=0$.

Проверьте самостоятельно, что числа $\alpha=4$, $\beta=5$, $\gamma=3$ этим условиям удовлетворяют и что функция $f(x,\ y,\ z)=4x+5y+3z$ является гомоморфизмом групп. Кроме того, надо проверить, что этот гомоморфизм переводит в 0 только элементы группы H и никакие другие. Но это следует из того, что система из двух линейных уравнений, определяющая коэффициенты α, β, γ, име-

ет решение с одним свободным параметром, следовательно, все ее решения получаются из найденного умножением на какой-то коэффициент.

Поскольку НОД $(4,\ 5,\ 3)=1$, то, согласно теореме о линейном представлении наибольшего общего делителя, найдутся такие целые числа $p,\ q,\ r$, что $4p+5q+3r=1$ и, следовательно, образ построенного гомоморфизма содержит единицу. Но тогда он совпадает с группой всех целых чисел. Итак, f – эпиморфизм. Ссылаясь на теорему 1.2, делаем вывод, что $Z\oplus Z\oplus Z/H\cong Z$.

1.4. Лемма Бернсайда. Задачи о раскрасках

Определение 1.11 [3, с. 301]. Пусть X – некоторое множество, а $S(X)$ – группа взаимно однозначных отображений множества X на себя с операцией композиции. Под действием группы G на множестве X понимается гомоморфизм $\varphi: G\to S(X)$. Образ $\varphi(g)(x)$ точки $x\in X$ относительно преобразования $\varphi(g)\in S(X),\ g\in G$ принято обозначать gx.

Поскольку φ – гомоморфизм, то для любого $x\in X$ и $g,\ h\in G$ действие группы на множестве обладает свойствами: 1) $ex=x$; 2) $gh(x)=g(h(x))$.

Две точки $x,\ x'\in X$ называются эквивалентными относительно группы G, действующей на X, если $x'=gx$ для некоторого элемента $g\in G$. В силу вышеупомянутых свойств это отношение является отношением эквивалентности, разбивающим множество X на непересекающиеся классы эквивалентности. Эти классы эквивалентности называют G-орбитами. Итак, орбитой элемента $x\in X$ под действием группы G является множество $Gx=\{gx: g\in G\}$. Количество элементов в данной орбите называется длиной орбиты [3, с. 303].

Определение 1.12. Неподвижными точками элемента $g\in G$ называются точки $x\in X$, для которых $gx=x$. Множество неподвижных точек элемента g обозначается X^g.

Теорема 1.3 (лемма Бернсайда). Количество орбит действия группы G на множестве X равно $\dfrac{1}{|G|}\sum\limits_{g\in G}\left|X^g\right|$.

Лемма Бернсайда позволяет решать комбинаторные задачи, в которых требуется найти количество объектов, не совмещаемых друг с другом определенными преобразованиями.

Пример 1.16. Сколькими способами можно раскрасить грани тетраэдра, используя краски трех цветов (с точностью до поворотов тетраэдра).

Решение. Занумеруем грани тетраэдра числами от 1 до 4. Тогда раскраска граней тетраэдра − это сопоставление каждому из этих чисел некоторого цвета: $x=(x_1,\ x_2,\ x_3,\ x_4)$, где x_k − это любой из трех цветов. Множество всех раскрасок $X=\{x\}$ содержит 3^4 элементов. Ясно, что некоторые раскраски могут переходить друг в друга в результате вращений тетраэдра.

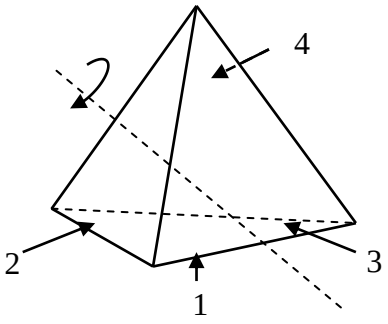

Рис. 1.3

Группа G вращений тетраэдра с операцией композиции состоит из вращений вокруг четырех осей, соединяющих вершины с центрами противоположных граней (8 вращений), вращений на угол π вокруг каждой из трех осей, соединяющих середины противоположных ребер (3 вращения) и тождественного преобразования. Поскольку, при каждом вращении тетраэдра, вершины переходят друг в друга, группа G изоморфна некоторой подгруппе симметрической группы S_4.

Опишем вращения тетраэдра с помощью подстановок, представленных в циклической форме. Обозначим через τ_1 вращение тетраэдра вокруг оси, проходящей через центр первой грани и противоположную вершину на угол $\frac{2\pi}{3}$. Тогда (рис. 1.2) $\tau_1=(243)$. Вращение вокруг этой же оси на угол $\frac{4\pi}{3}$ есть, очевидно $\tau_1^2=(234)$.

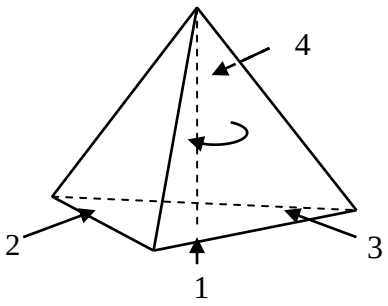

Рис. 1.2

Выпишем все остальные вращения относительно осей, проходящих через центры оставшихся граней: $\tau_2=(134)$, $\tau_2^2=(143)$, $\tau_3=(142)$, $\tau_3^2=(124)$, $\tau_4=(123)$, $\tau_4^2=(132)$. Подстановки $\sigma_1=(13)(24)$, $\sigma_2=(12)(34)$, $\sigma_3=(14)(23)$ (рис. 1.3) задают вращения на угол π вокруг каждой из трех осей, соединяющих середины противоположных ребер.

Итак, группа G действует на множестве раскрасок X. Раскраски граней тетраэдра, совмещаемые друг с другом каким-нибудь преобразованием группы G, лежат в одной орбите под действием группы G. Определить количество

различных раскрасок, означает найти число орбит действия группы G на множестве X. Для этого воспользуемся леммой Бернсайда. Выясним, сколько раскрасок из X оставляет на месте каждый элемент группы G.

Нейтральный элемент e оставляет на своем месте все раскраски, и поскольку их всего 3^4, то и $\left|X^e\right|=3^4$. Вращение $\tau_1=(243)=(1)(243)$ сохраняет раскраску, если грани с номерами 2, 3, 4 окрашены в один и тот же цвет, цвет же первой грани при этом может быть любым. Значит, первая грань может быть окрашена тремя способами, и в то же время оставшиеся грани вместе красятся в один из трех цветов, поэтому $\left|X^{\tau_1}\right|=3\cdot 3=3^2$. Поскольку остальные вращения τ_k^i имеют подобную циклическую структуру, то $\left|X^{\tau_1^2}\right|=$

$=\left|X^{\tau_2}\right|=\left|X^{\tau_2^2}\right|=\left|X^{\tau_3}\right|=\left|X^{\tau_3^2}\right|=\left|X^{\tau_4}\right|=\left|X^{\tau_4^2}\right|=3^2$. Подстановка $\sigma_1=(13)(24)$ сохранит раскраску граней при условии, что грани 1 и 3 выкрашены в один цвет (три возможности) и в то же время грани 2 и 4 выкрашены в один цвет (также три возможности). Значит, $\left|X^{\sigma_1}\right|=3^2$. Аналогичным образом имеем $\left|X^{\sigma_2}\right|=\left|X^{\sigma_3}\right|=3^2$. Учитывая, что порядок группы G равен 12, по лемме Бернсайда находим $N=\frac{1}{12}\left(3^4+11\cdot 3^2\right)=15$.

Пример 1.17. Две вершины правильного пятиугольника красят в зеленый цвет, а оставшиеся три − в синий цвет. С помощью леммы Бернсайда найти число существенно различных раскрасок вершин пятиугольника и перечислить их.

Решение. Занумеруем вершины пятиугольника числами от 1 до 5. Тогда раскраска $x=(x_1, x_2, x_3, x_4, x_5)$ − это сопоставление двум любым числам зеленого цвета, а оставшимся трем − синего. Количество подобных раскрасок равно числу способов, которыми можно выбрать два места под зеленый цвет, т. е. $|X|=C_5^2=10$. Найдем число орбит действия группы G самосовмещений правильного пятиугольника на множестве X.

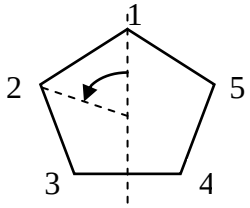

Рис. 1.4

Группа G состоит из вращений пятиугольника вокруг своего центра, отражений относительно пяти осей, соединя-

ющих вершины пятиугольника с серединами противолежащих сторон и тождественного преобразования. Группа G изоморфна некоторой подгруппе симметрической группы S_5.

Выпишем все подстановки в циклической форме. Вращениям вокруг центра пятиугольника отвечают подстановки: $\tau=(12345)$, $\tau^2=(13524)$, $\tau^3=(14253)$, $\tau^4=(15432)$. Подстановки $\sigma_1=(25)(34)$, $\sigma_2=(13)(45)$, $\sigma_3=(15)(24)$, $\sigma_4=(12)(35)$ и $\sigma_5=(13)(24)$ задают осевые симметрии (рис. 1.4). Порядок группы G равен 10. Выясним, сколько раскрасок из X оставляет на месте каждый элемент группы G. Нейтральный элемент e оставляет на своем месте все раскраски: $\left|X^e\right|=|X|=10$. Повороты τ и $\tau^4=\tau^{-1}$ переводят друг в друга соседние вершины пятиугольника. Для того чтобы раскраска сохранялась при повороте, нужно, чтобы любые две соседние вершины были окрашены в один цвет, т. е. все вершины имели бы одинаковый цвет, но таких раскрасок в множестве X нет, следовательно, $\left|X^\tau\right|=\left|X^{\tau^4}\right|=0$. Поворот $\tau^2=(13524)$ сохранит раскраску, если одинаковый цвет будут иметь одновременно вершины 1 и 3, 3 и 5, 5 и 2, 2 и 4, 4 и 1. Таким образом, мы опять приходим к требованию одноцветной раскраски всех вершин пятиугольника. Такие же рассуждения применимы и к повороту $\tau^3=\left(\tau^2\right)^{-1}$. Получаем $\left|X^{\tau^2}\right|=\left|X^{\tau^3}\right|=0$. Осевая симметрия $\sigma_1=(1)(25)(34)$ сохраняет только две раскраски: (с, з, с, с, з), (с, с, з, з, с).

Аналогично действуют и остальные осевые симметрии, поэтому $\left|X^{\sigma_1}\right|=\left|X^{\sigma_2}\right|=\left|X^{\sigma_3}\right|=\left|X^{\sigma_4}\right|=\left|X^{\sigma_5}\right|=2$. По лемме Бернсайда количество различных раскрасок вершин пятиугольника равно $\frac{1}{10}(10+4\cdot 0+5\cdot 2)=2$. Укажем их: (з, з, с, с, с) и (з, с, з, с, с).

2. Кольца и поля

2.1. Поля

Наиболее привычной и известной алгебраической структурой является поле.

Определение 2.1. Множество K называется полем, если на нем определены две бинарные операции: сложение и умножение, удовлетворяющие следующим условиям:

1) K является абелевой группой относительно сложения (с нейтральным элементом 0);

2) все элементы K, за исключением 0, образуют абелеву группу относительно умножения (с нейтральным элементом 1);

3) сложение и умножение связаны законом дистрибутивности:

$(a+b)c = ac + bc \quad \forall a,\ b,\ c \in K$.

Полями являются множества ***Q***, ***R***, ***C***. Полем также является множество классов вычетов по простому модулю.

По определению, поле содержит не менее двух элементов. Множество из двух элементов 0 и 1 с операциями 1 + 1 = 0 и 1·1 = 1 является полем.

Определение 2.2. Подполем данного поля K называется его подмножество, которое является полем относительно операций, определенных в поле *K*.

Например, в поле вещественных чисел подполем является множество всех чисел вида $a\sqrt{3}+b$, где a и b – рациональные числа.

Для того чтобы проверить, является ли данное подмножество некоторого поля подполем, достаточно проверить замкнутость этого множества относительно операций (т. е. следует убедиться, что вместе с каждым своим элементом a это подмножество содержит элементы $-a$ и $\grave{a}^{-1}$, а вместе с каждой парой элементов a и b содержит их сумму $a+b$ и произведение ab).

Элемент любого поля, полученный сложением n экземпляров единицы поля, обозначают $n\cdot 1$ или просто n. Существенно различаются следующие две ситуации:

1) среди элементов вида $n\cdot 1$ нет совпадающих;

2) при каких-то натуральных m и n верно равенство $n\cdot 1 = m\cdot 1$.

В первом случае говорят, что поле имеет характеристику 0, а во втором случае характеристикой поля называют наименьшее натуральное число p, для

которого $p \cdot 1 = 0$. Ненулевая характеристика поля всегда является простым числом.

Каждое поле ненулевой характеристики *p* содержит подполе, изоморфное Z_p, т. е. полю вычетов по модулю *p*. Каждое поле нулевой характеристики содержит подполе, изоморфное полю рациональных чисел Q.

Теорема 2.1. Мультипликативная группа конечного поля – циклическая.

Пример 2.1. Найти элемент поля Z_{19}, обратный к $\overline{11}$.

Решение. Найдем линейное представление НОД $(11, 19)$: $1 = 11 \cdot 7 - 19 \cdot 4$ (это можно сделать, например, с помощью алгоритма Евклида). Перейдя в этом равенстве к классам вычетов, получаем $\bar{1} = \overline{11} \cdot \bar{7}$, т. е. класс $\bar{7}$ является обратным к классу $\overline{11}$.

Пример 2.2. Найти все образующие мультипликативной группы поля Z_{13}.

Решение. Мультипликативная группа данного поля состоит из 12 элементов. Рассмотрим, например, серию степеней элемента $\bar{2}$: $\bar{2}^2 = \bar{4}$; $\bar{2}^3 = \bar{8}$; $\bar{2}^4 = \overline{16} = \bar{3}$; $\bar{2}^5 = \bar{2} \cdot \bar{3} = \bar{6}$; $\bar{2}^6 = \bar{6} \cdot \bar{2} = \overline{12}$.

Теперь достаточно вспомнить, что порядок любого элемента группы является делителем порядка этой группы. Мы перебрали в качестве показателей степени все делители числа 12 и ни разу не получили нейтральный элемент группы, следовательно, $\bar{2}$ – образующий элемент мультипликативной группы поля Z_{13}. Чтобы найти остальные образующие, достаточно вычислить степени элемента $\bar{2}$, показатели которых взаимно просты с 12, т. е. $\bar{2}^5 = \bar{6}$; $\bar{2}^7 = \overline{11}$ и $\bar{2}^{11} = \bar{7}$.

Определение 2.3. Если поле K является подполем поля *L*, то *L* называется расширением поля K. Поле *L* можно рассматривать как линейное пространство над K, размерность этого пространства называется степенью расширения.

Пример 2.3. Поле K получено присоединением к полю Q рациональных чисел элемента $\sqrt{2-\sqrt{3}}$. Найти степень этого расширения.

Решение. Введем обозначение: $\sqrt{2-\sqrt{3}} = \alpha$, тогда $\alpha^2 = 2 - \sqrt{3}$, $\sqrt{3} = 2 - \alpha^2$, следовательно, α является корнем многочлена с рациональными коэффициентами $f(\alpha) = \alpha^4 - 4\alpha^2 + 1$. Прежде всего заметим, что этот многочлен неприво-

дим над Q, т. е. не раскладывается на множители с рациональными коэффициентами. В частности, это значит, что любой многочлен над полем Q либо делится на $f(\alpha)=\alpha^4-4\alpha^2+1$, либо взаимно прост с ним.

Покажем теперь, что каждый элемент расширения можно представить как линейную комбинацию чисел 1, α, α^2, α^3 с рациональными коэффициентами. Очевидно, что для этого достаточно рассмотреть числа вида $g(\alpha)$ и $g(\alpha)^{-1}$, где $g(t)$ – некоторый многочлен от t с рациональными коэффициентами.

Если $g(t)$ делится на $f(t)$, то $g(\alpha)=0$, поэтому достаточно рассмотреть многочлены $g(t)$, взаимно простые с $f(t)$. Но для каждого такого многочлена найдутся многочлены $M(t)$ и $N(t)$, для которых верно равенство $g(t)M(t)+f(t)N(t)=1$. Подставив в это равенство вместо переменной t число α, получим $g(\alpha)M(\alpha)=1$. Таким образом, элемент, обратный к $g(\alpha)$ по умножению, так же как и $g(\alpha)$, является линейной комбинацией натуральных степеней числа α.

Разделим $g(t)$ на $f(t)$ с остатком: $g(t)=f(t)h(t)+r(t)$ (степень $r(t)$ не превосходит 3, т. е. $r(t)=a+bt+ct^2+dt^3$). Если в это равенство вместо переменной t подставить число α, то первое слагаемое обратится в 0, и получится представление числа $g(\alpha)$ в виде линейной комбинации чисел 1, α, α^2, α^3 с рациональными коэффициентами: $g(\alpha)=a+b\alpha+c\alpha^2+d\alpha^3$.

Итак, числа 1, α, α^2, α^3 образуют базис расширения как линейного пространства на полем Q, следовательно, степень этого расширения равна 4.

2.2. Кольца

Важным классом алгебраических структур являются кольца.

Определение 2.4. Множество A называется *кольцом,* если на нем определены две бинарные операции: сложение и умножение, обладающие следующими свойствами:

1) относительно сложения это множество является абелевой группой;
2) умножение ассоциативно;
3) операции сложения и умножения связаны законом дистрибутивности:

$$(a+b)\cdot c=a\cdot c+b\cdot c;\quad c\cdot(a+b)=c\cdot a+c\cdot b \qquad \forall\, a,\, b,\, c\in A.$$

Если операция умножения в кольце обладает нейтральным элементом, то говорят, что A – кольцо с единицей. Если операция умножения в кольце коммутативна, то кольцо называется коммутативным.

Замечание 2.1. Элементы кольца могут не иметь обратных по умножению. Если для элемента a кольца существует элемент b, такой что $ab = ba = 1$, то говорят, что элемент a обратим (элемент b при этом тоже, естественно, обратим).

Пример 2.4. Определить, какие из следующих множеств являются кольцами: 1) множество комплексных чисел с положительной мнимой частью; 2) множество нижних треугольных матриц третьего порядка.

Решение.

1. Пример $(5+3i)(-7+2i) = -41-11i$ показывает, что множество комплексных чисел с положительной мнимой частью не замкнуто относительно умножения и поэтому не является кольцом.

2. Прежде всего заметим, что сложение матриц ассоциативно и коммутативно, нулевая матрица является нейтральным элементом относительно сложения, а матрица $-A$ является противоположной по сложению для матрицы A. Кроме того, умножение матриц ассоциативно и связано со сложением законом дистрибутивности. Таким образом, для ответа на вопрос достаточно проверить замкнутость множества треугольных матриц относительно этих операций.

Замкнутость этого множества относительно сложения и вычисления элемента, противоположного по сложению, очевидна. Что касается замкнутости относительно умножения, то этот факт менее очевиден, но должен быть хорошо известен из начального курса алгебры.

Проверьте самостоятельно, что кольцами являются множество целых чисел, множество многочленов от конечного набора переменных с коэффициентами из произвольного поля, множество классов вычетов по произвольному целому модулю, а также множество функций, заданных на некотором фиксированном множестве (операции во всех этих случаях определяются стандартным образом).

Определение 2.5. Элементы a и b кольца, для которых $ab = 0$ и при этом $a \neq 0$, $b \neq 0$, называются делителями нуля.

Замечание 2.2. Если элемент кольца является делителем нуля, то он не может быть обратимым по умножению.

Пример 2.5. Содержит ли кольцо из примера 2.4 единицу и делители нуля?

Решение. Единицей данного кольца является единичная матрица. Делителями нуля являются, например, следующие матрицы:

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

2.3. Идеалы

Определение 2.6. Подмножество B кольца A называется подкольцом, если оно само является кольцом относительно тех же операций сложения и умножения, которые определены в кольце A.

Определение 2.7. Подкольцо H коммутативного кольца A называется идеалом, если произведение $ha = ah \in H$ при любых $a \in A$ и $h \in H$.

Замечание 2.3. Можно определить идеал и для некоммутативных колец. Так, подкольцо H некоммутативного кольца A называется левым идеалом, если произведение $ah \in H$ при любых $a \in A$ и $h \in H$. Аналогично определяются правые идеалы.

Если подкольцо некоммутативного кольца одновременно является и левым, и правым идеалом, оно называется двусторонним идеалом. В любом кольце A все кольцо A и подмножество $\{0\}$ (нулевое кольцо) являются идеалами. Если в кольце с единицей идеал содержит 1, то он совпадает со всем кольцом, поскольку каждый элемент a этого кольца можно представить в виде $a = a \cdot 1 = 1 \cdot a$, следовательно, он должен принадлежать идеалу.

Примеры идеалов: множество $n\boldsymbol{Z}$ – идеал кольца $\boldsymbol{Z}$; в кольце функций, определенных на отрезке $[a, b]$, идеалом является множество всех функций таких, что $f(c) = 0$ для некоторого $c \in [a, b]$.

Теорема 2.2. В коммутативном кольце A множество $\{xa : x \in A\}$ всех кратных любого фиксированного элемента $a \in A$ является идеалом.

Такие идеалы называют главными идеалами, порожденными элементом a, и обозначают (a). Если все идеалы кольца являются главными, его называют кольцом главных идеалов. Кольцом главных идеалов является, например, кольцо целых чисел.

Пример 2.6. Проверить, являются ли идеалами в кольце многочленов с целыми коэффициентами следующие множества: 1) подкольцо многочленов с четными коэффициентами; 2) подкольцо констант (состоящее из нуля и многочленов нулевой степени – ненулевых целых чисел).

Решение.

1. Каждый многочлен с четными коэффициентами можно представить в виде $2f(x)$, где $f(x)$ – некоторый многочлен с целыми коэффициентами. Следовательно, при умножении его на произвольный многочлен $g(x)$ с целыми коэффициентами получается многочлен $2f(x)g(x)$ с четными коэффициентами. Итак, это множество является идеалом.

2. Заметим, что любое число, отличное от нуля, умноженное на многочлен положительной степени, является многочленом положительной степени. Следовательно, подкольцо констант не является идеалом в кольце многочленов.

Пример 2.7. Проверить, являются ли левыми идеалами в кольце квадратных матриц второго порядка с целыми элементами следующие множества: 1) матрицы, у которых левый нижний элемент делится на 3; 2) матрицы, у которых все элементы кратны 6.

Решение.

1. Данное множество является подкольцом, но не является идеалом, так как, например, произведение $\begin{pmatrix} 2 & 5 \\ 5 & 7 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 6 & 1 \end{pmatrix}=\begin{pmatrix} 32 & 9 \\ 47 & 17 \end{pmatrix}$ не принадлежит этому множеству.

2. Элементы этого множества имеют вид $6B$, где B – некоторая матрица с целыми элементами, следовательно, произведение любой целочисленной матрицы A второго порядка на матрицу из этого множества имеет вид $6AB$, т. е. принадлежит этому же множеству.

Итак, множество матриц, все элементы которых кратны 6, является идеалом (двусторонним) в кольце всех целочисленных матриц порядка 2.

2.4. Факторкольца

Определение 2.8. Пусть H – двусторонний идеал кольца A, тогда факторкольцом кольца A по идеалу H называется факторгруппа аддитивной группы кольца по аддитивной группе идеала, на которой определена операция умножения классов смежности по следующему правилу: $(x+H)(y+H)=xy+H$.

Замечание 2.4. Элементами факторкольца являются классы смежности аддитивной группы кольца по аддитивной группе идеала. В частном случае, если основное кольцо – это кольцо целых чисел $\boldsymbol{Z}$, все идеалы – главные, т. е. имеют вид $m\boldsymbol{Z}$. Следовательно, в этом случае элементы факторкольца – это просто классы вычетов по модулю m.

По аналогии с этим случаем элементы факторкольца произвольного коммутативного кольца нередко называют классами вычетов и обозначают $\bar{x}=x+H$.

Теорема 2.3. В кольце $\boldsymbol{Z}_n$ обратимы в точности те элементы $\bar{k}$, для которых k взаимно просто с n.

Следствие. Если p – простое число, то $\boldsymbol{Z}_p$ – поле.

Пример 2.8. Проверить, являются ли идеалами в кольце $\boldsymbol{Z}_{18}$ следующие множества: 1) множество необратимых элементов; 2) множество элементов, кратных 3.

Решение.

1. Выпишем множество необратимых элементов кольца $\boldsymbol{Z}_{18}$. Это те элементы, которые имеют общие делители с числом 18, т. е. $\bar{2}$, $\bar{3}$, $\bar{4}$, …, $\overline{16}$. Поскольку, например, $\bar{2}+\bar{3}=\bar{5}$, то это множество не замкнуто относительно сложения. Значит, оно не является кольцом и тем более идеалом.

2. Ясно, что это множество замкнуто относительно сложения и умножения. Кроме того, при умножении его элементов на произвольные классы получаются классы, кратные 3, т. е. это множество является идеалом.

Пример 2.9. В кольце $\boldsymbol{Z}_{12}$ указать все обратимые элементы. Решить уравнения $\bar{5}\cdot x=\bar{4}$, $\bar{3}\cdot x=\bar{4}$ и $\overline{10}\cdot x=\bar{8}$.

Решение. Обратимые элементы – это классы $\bar{k}$, где k не имеет общих делителей с числом $\overline{12}$, т. е. $\bar{1}$, $\bar{5}$, $\bar{7}$, $\overline{11}$.

Чтобы решить уравнение $\bar{5}\cdot x=\bar{4}$, заметим, что класс $\bar{5}$ обратим, следовательно, обратный к нему находится среди выписанных классов. Легко проверить, что $\bar{5}\cdot\bar{5}=\bar{1}$, умножив обе части заданного уравнения на $\bar{5}$, получим $x=\bar{4}\cdot\bar{5}=\overline{40}=\overline{12\cdot 3+4}=\bar{4}$.

Во втором уравнении коэффициент $\bar{3}$ необратим, следовательно, рассмотренный метод применить невозможно. Более того, легко заметить, что левая часть при всех значениях x кратна $\bar{3}$, а правая – нет. Следовательно, это уравнение решений не имеет.

Наконец, можно проверить, что последнее уравнение имеет два решения: $\bar{2}$ и $\bar{8}$.

Заметим, что при рассмотрении этого примера мы просто подбирали подходящие классы вычетов, при больших значениях модуля для решения такого рода уравнений приходится решать диофантово уравнение.

Пример 2.10. В кольце $\boldsymbol{Z}_{25}$ решить уравнение $\bar{9}\cdot x=\overline{14}$.

Решение. Данное уравнение равносильно сравнению $9x-14\equiv 0\ (\mathrm{mod}\,25)$, или диофантовому уравнению $9x-25t=14$. Поскольку числа 9 и 25 взаимно просты, это уравнение имеет решение. Найдем линейное представление НОД (9, 25) = 1: $25=9\cdot 2+7$, $9=7\cdot 1+2$, $7=2\cdot 3+1$. Следовательно, $1=7-2\cdot 3=7-3(9-7)=4\cdot 7-3\cdot 9=4(25-9\cdot 2)-3\cdot 9=$ $=4\cdot 25-11\cdot 9$. Итак, $4\cdot 25-11\cdot 9=1$. Умножив последнее равенство на 14 и перейдя к сравнению по модулю 25, получим $\overline{-11\cdot 14}\cdot\bar{9}=\overline{14}$, или $\overline{25\cdot 6-154}\cdot\bar{9}=\overline{14}$, т. е. $\overline{-4}\cdot\bar{9}=\overline{14}$. Следовательно, решением данного уравнения является класс $\overline{-4}=\overline{21}$.

Поскольку кольцо многочленов с коэффициентами из некоторого поля, так же как и кольцо целых чисел, является кольцом главных идеалов, строение факторкольца кольца многочленов во многом схоже со строением кольца вычетов. При этом роль, аналогичную роли простых чисел, исполняют неприводимые многочлены (т. е. многочлены, которые нельзя разложить на множители с коэффициентами из данного поля).

Замечание 2.5. Для многочленов степени не выше 3 неприводимость эквивалентна отсутствию корней в данном поле.

Теорема 2.4. Элемент $g(x)+f(x)K[x]$ факторкольца кольца многочленов $K[x]$ с коэффициентами из поля K по главному идеалу, порожденному многочленом $f(x)$, обратим тогда и только тогда, когда многочлены $f(x)$ и $g(x)$ взаимно просты.

Следствие. Факторкольцо кольца многочленов $K[x]$ с коэффициентами из поля K по главному идеалу, порожденному многочленом $f(x)$, является полем тогда и только тогда, когда многочлен $f(x)$ неприводим над полем K.

Пример 2.11. Описать строение факторкольца кольца многочленов $\boldsymbol{Z}_2[x]$ по идеалу, порожденному многочленом $f(x)=x^3+x$.

1. Есть ли в этом факторкольце делители нуля?

2. Вычислить произведение классов, содержащих x^3 и $x+1$.

3. Обратим ли в этом факторкольце класс, содержащий многочлен x^2+x+1?

Решение. Поле $\boldsymbol{Z}_2$ состоит из двух элементов $\bar{0}$ и $\bar{1}$. Элемент $\bar{0}$ является корнем многочлена $f(x)=x^3+x$, следовательно, этот многочлен приводим над $\boldsymbol{Z}_2$.

Заметим, что два многочлена принадлежат одному классу вычетов по идеалу $(f(x))$ тогда и только тогда, когда их разность делится на $f(x)$. Следовательно, все многочлены из одного класса дают одинаковые остатки при делении на $f(x)$, а многочлены из разных классов дают разные остатки. При делении произвольного многочлена на $f(x)=x^3+x$ в качестве остатков могут появляться любые многочлены степени не более 2. Итак, в каждом классе есть ровно один многочлен вида ax^2+bx+c, где коэффициенты a, b, c – элементы поля $\boldsymbol{Z}_2$.

1. Так как многочлен $f(x)$ приводим, то делители нуля есть, например, если $g(x)=x$ и $h(x)=x^2+1$, то $\overline{g(x)}\neq\bar{0}$ и $\overline{h(x)}\neq\bar{0}$, но $\overline{g(x)}\cdot\overline{h(x)}=$ $=\overline{g(x)\cdot h(x)}=\overline{f(x)}=\bar{0}$.

2. Произведение классов $\overline{x^3}$ и $\overline{x+1}$ – это класс, содержащий многочлен $x^3(x+1)$. Если нужно найти стандартный представитель класса, надо этот многочлен разделить на x^3+x. Поскольку $x^4+x^3==\left(x^3+x\right)(x+1)+x^2+x$, то $\overline{x^3}\cdot\overline{x+1}=x^2+x$ (напомним, что в поле $\boldsymbol{Z}_2$ верно равенство $1=-1$).

3. Применим к многочленам x^2+x+1 и x^3+x алгоритм Евклида: $x^3+x=\left(x^2+x+1\right)(x+1)+x+1;\ \ x^2+x+1=(x+1)x+1$. Следовательно, эти многочлены взаимно просты, и класс $\overline{x^2+x+1}$ обратим. Из равенств $1=x^2+x+1+(x+1)x=x^2+x+1+\left(x^3+x\right)x+\left(x^2+x+1\right)\left(x^2+x\right)=$ $=\left(x^2+x+1\right)\left(x^2+x+1\right)+\left(x^3+x\right)x$ следует, что $\bar{1}=\overline{x^2+x+1}\cdot\overline{x^2+x+1}$, т. е. класс, содержащий многочлен x^2+x+1, обратен сам себе.

Список литературы

1. Группы, кольца, поля: Методические указания по дисциплине «Геометрия и алгебра» / Сост. И. Г. Зельвенский; ГЭТУ «ЛЭТИ». СПб., 1997.

2. Беклемишев Д. В. Курс аналитической геометрии и линейной алгебры: Учебник для вузов. М.: Физматлит, 2008.

3. Кострикин А. И. Введение в алгебру: Учебник для ун-тов. М.: Наука, 1977.

Содержание

Публикуется в авторской редакции

Подписано в печать 29.12.10. Формат 60×84 1/16. Бумага офсетная.
Печать офсетная. Гарнитура «Times». Печ. л. 2.0.
Тираж 290 экз. Заказ

Издательство СПбГЭТУ «ЛЭТИ»
197376, С.-Петербург, ул. Проф. Попова, 5