МИНИСТЕРСТВО НАРОДНОГО ОБРАЗОВАНИЯ БССР

ГОМЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. Ф.СКОРИНЫ

Кафедра алгебры и геометрии

ЛАБОРАТОРНЫЕ РАБОТЫ

по курсу "Алгебра и теория чисел"
для студентов математического факультета

Гомель 1990

Составители: С.Ф.Каморников, А.П.Кармазин, В.С.Монахов

Рекомендовано к печати методическим советом математического факультета Гомельского государственного университета имени Ф.Скорины

ВВЕДЕНИЕ

Предлагаемые работы посвящены введению в один из разделов современной алгебры теории колец и адресованы в первую очередь студентам второго курса математического факультета в качестве учебного пособия по дисциплине "Алгебра и теория чисел". Кроме того, это издание можно использовать при изучении спецкурса "Теория колец" в рамках специализации "Алгебра и теория чисел".

Структура настоящего пособия сохранена прежней, как и в предыдущих трех частях лабораторных работ по алгебре и теории чисел. Каждой из шести лабораторных работ предшествует краткое, но достаточно полное изложение теоретического материала. Усвоение этого материала студент может проверить с помощью вопросов для самоконтроля. Большую помощь при выполнении индивидуальных заданий студентов призваны оказать решения тех типовых примеров, которыми насыщены все лабораторные работы.

Такое построение пособий по алгебре и теории чисел отражает технологию обучения студентов математике, сложившуюся в последнее время на кафедре алгебры и геометрии.

При составлении лабораторных работ использовалась следующая литература:

1. В а н д е р В а р д е н Б.Л. Алгебра. - М.: Наука, 1979.

2. К о с т р и к и н А.И. Введение в алгебру. - М.: Наука, 1977.

3. П р о с к у р я к о в И.В. Сборник задач по линейной алгебре. – М.: Наука, 1962.

4. Сборник задач по алгебре: Учебное пособие // Под редакцией А.И.Кострикина. – М.: Наука, 1987.

5. Сборник задач по алгебре и аналитической геометрии // Под редакцией А.С.Феденко. – Мн.: Университетское, 1989.

6. С к о р н я к о в Л.Я. Элементы алгебры. – М.: Наука, 1986.

7. Ф е й с К. Алгебра: Кольца, модули и категории. – М.: Мир, Т.I – 1977; Т.II – 1979.

Лабораторная работа № I
КОЛЬЦА И ИХ НАЧАЛЬНЫЕ СВОЙСТВА

Непустое множество K с двумя бинарными алгебраическими операциями (сложением и умножением) называется **к о л ь ц о м**, если выполняются следующие условия:

I) множество K с операцией сложения является абелевой группой; эта группа называется **а д д и т и в н о й   г р у п п о й   к о л ь ц а** и обозначается через $(K,+)$;

2) умножение определено на K и ассоциативно; т.е. $ab \in K$ и $(ab)c = a(bc)$ для всех $a, b, c \in K$;

3) операция сложения связана с операцией умножения законами дистрибутивности, т.е. $(a+b)c = ac + bc$, $a(b+c) = ab + ac$ для любых $a, b, c \in K$.

Если в кольце K умножение коммутативно, т.е. $ab = ba$ для любых $a, b \in K$, то кольцо K называется **к о м м у т а т и в н ы м**. Если в кольце K существует элемент e такой, что $xe = ex = x$ для всех $x \in K$, то e называется **е д и н и ц е й   кольца** K, а само кольцо K – **к о л ь ц о м   с   е д и н и ц е й**.

П р и м е р ы I. Относительно операций сложения и умножения чисел множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ являются коммутативными кольцами. Каждое из этих колец является кольцом с единицей.

2. Множество всех четных чисел (это множество будем обозначать через $2\mathbb{Z}$) относительно операций сложения и умножения является коммутативным кольцом, которое не обладает единицей.

3. Через $P[x]$ обозначим множество всех многочленов переменной x с коэффициентами из поля P. Множество $P[x]$ относительно сложения и умножения многочленов является коммутативным кольцом с единицей. Роль единицы в кольце $P[x]$ играет единичный элемент поля P, рассматриваемый как многочлен нулевой степени.

4. Относительно операций сложения и умножения матриц множество $M(n,P)$ всех $n \times n$ – матриц над полем P образует кольцо, которое называется **п о л н ы м   м а т р и ч н ы м   к о л ь ц о м** над полем P. Это кольцо не является коммутативным. Роль нуля и единицы в кольце $M(n,P)$ играют нулевая и единичная матрицы.

$$O_n = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}, \quad E_n = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ 0 & & \ddots 1 \end{pmatrix},$$

где 0 и I – нулевой и единичный элементы поля P.

5. Пусть $\mathbb{Z}$ – множество всех целых чисел, n – фиксированное натуральное число. Обозначим через $\mathbb{Z}_n$ множество всех классов вычетов по модулю n. На множестве $\mathbb{Z}_n$ определим операции сложения и умножения следующим образом:

$$\bar{a} + \bar{b} = \overline{a+b},$$
$$\bar{a}\,\bar{b} = \overline{ab}$$

для любых классов вычетов $\bar{a}, \bar{b} \in \mathbb{Z}_n$. Тогда множество с введенными операциями сложения и умножения является коммутативным кольцом с единицей. Роль единицы в $\mathbb{Z}_n$ играет класс $\bar{1} = \{1 + nt \mid t \in \mathbb{Z}\}$. Кольцо $\mathbb{Z}_n$ называется **кольцом классов вычетов** по модулю n. Это кольцо конечное, оно относит из n элементов.

Пусть K – произвольное кольцо. Из того, что $(K, +)$ – группа, следует существование нулевого элемента 0 и противоположных элементов $(-a)$ для всех $a \in K$. Поэтому в кольце K уравнение $a + x = b$ имеет единственное решение $x = (-a) + b$. Кроме того, из ассоциативности сложения вытекает обобщенный закон ассоциативности сложения:

$$(a_1 + \dots + a_s) + (a_{s+1} + \dots + a_n) = (a_1 + \dots + a_t) + (a_{t+1} + \dots + a_n),$$

который позволяет сумму $a_1 + \dots + a_n$ обозначать через $\sum\limits_{i=1}^{n} a_i$. В случае $a_1 = \dots = a_n = a$ получаем **кратное**

$$na = \underbrace{a + \dots + a}_{n \text{ раз}}$$

Положим $0a = 0$ и $(-n)a = -(na)$. Для любых целых n и m легко установить справедливость равенств

$$na + ma = (n+m)a,$$
$$n(ma) = (nm)a,$$
$$n(a+b) = na + nb,$$
$$n(ab) = (na)b = a(nb)$$

Из ассоциативности умножения вытекает обобщенный закон ассоциативности умножения:

$$(a_1 \dots a_s)(a_{s+1} \dots a_n) = (a_1 \dots a_t)(a_{t+1} \dots a_n),$$

который позволяет произведение $a_1 \dots a_n$ обозначить через $\prod\limits_{i=1}^{n} a_i$. В случае $a_1 = \dots = a_n = a$ получем **степень**

$$a^n = \underbrace{a \dots a}_{n \text{ раз}}$$

Для любых натуральных n и m легко установить справедливость равенств

$$a^n a^m = a^{n+m},$$
$$(a^n)^m = a^{(nm)} \qquad \text{(I.I)}$$

В кольцах справедлив и обобщенный закон дистрибутивности

$$(a_1 + \dots + a_n)(b_1 + \dots + b_m) = a_1 b_1 + \dots + a_1 b_m + \dots + a_n b_1 + \dots + a_n b_m = \sum_{j=1}^{m} \sum_{i=1}^{n} a_i b_j,$$

который дает привычное правило для перемножения сумм.

Если 0 – нулевой элемент кольца K, то

$$a0 = a(b - b) = ab + a(-b) = ab - ab = 0,$$

т.е. если один из сомножителей – нулевой элемент, то произведение равно нулю. Обратное утверждение нарушается в матричных кольцах. Например, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ и $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ – ненулевые элементы кольца $M(2, \mathbb{R})$, а их произведение

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

равно нулевому элементу.

Элементы a и b кольца K называются **делителями нуля**, если $a \neq 0 \neq b$ и $ab = 0$. Коммутативное кольцо с единицей $1 \neq 0$ без делителей нуля называется **целостным кольцом** или **областью целостности**. Числовые кольца $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ и кольцо многочленов $P[x]$ являются целостными. Полное матричное кольцо $M(n, \mathbb{R})$ не целостное.

Теорема I.I. Коммутативное кольцо K с единицей является целостным тогда и только тогда, когда в нем выполнен закон сокращения, т.е. из $ab = ac$ и $a \neq 0$ следует $b = c$ для всех a, b и $c \in K$.

В кольце K с единицей e естественно рассматривать множество обратимых элементов. Элемент a называется **обратимым** (или **делителем единицы**), если существует элемент $a^{-1} \in K$, для которого $aa^{-1} = a^{-1}a = e$. В этом случае элемент a^{-1} называется **обратным** к элементу a.

Теорема 1.2. В кольце с единицей все обратимые элементы образуют группу относительно умножения.

Кольцо с единицей, в котором все ненулевые элементы образуют группу относительно умножения, называется **телом**. Коммутативное тело называется **полем**.

Таким образом, тело объединяет в себе сразу две группы: мультипликативную и аддитивную. Обе они связаны дистрибутивными законами.

В теле T для ненулевых элементов можно положить $a^0 = e$, $a^{-n} = (a^{-1})^n$, $n \in N$. Легко проверить, что равенства (1.1) остаются справедливыми для всех целых n и m.

Пусть A – аддитивная абелева группа. Обозначим через $End\,A$ множество всех эндоморфизмов группы A. На этом множестве введем операции сложения и умножения эндоморфизмов по следующим правилам:

$$(f_1 + f_2)(x) = f_1(x) + f_2(x),$$
$$(f_1 f_2)(x) = f_1(f_2(x))$$

для всех $f_1, f_2 \in End\,A$.

Теорема 1.3. Совокупность $End\,A$ всех эндоморфизмов аддитивной абелевой группы A является кольцом относительно операций сложения и умножения эндоморфизмов.

Кольцо $End\,A$ является кольцом с единицей. Роль единицы здесь играет тождественный автоморфизм.

Подмножество L кольца K называется **подкольцом**, если L само является кольцом относительно операций сложения и умножения, определенных в K.

Теорема 1.4. (Критерий для подколец). Непустое подмножество L кольца K является его подкольцом тогда и только тогда, когда выполняются следующие условия:

1) $a + b \in L$ для любых $a, b \in L$;
2) $-a \in L$ для любого $a \in L$;
3) $ab \in L$ для любых $a, b \in L$.

Сразу же отметим, что условия 1) и 2) в теореме 1.4 могут быть

заменены одним условием: $a - b \in L$ для любых $a, b \in L$.

Всякое кольцо содержит **нулевое** подкольцо, т.е. подкольцо, состоящее из одного нулевого элемента 0. Само кольцо является своим подкольцом.

Кольца K_1 и K_2 называются **изоморфными**, если существует взаимно однозначное отображение f между элементами колец K_1 и K_2, при котором

$$f(a+b) = f(a) + f(b),$$
$$f(ab) = f(a)f(b).$$

Отображение f в этом случае называют **изоморфизмом** колец K_1 и K_2. Изоморфные кольца обозначают так: $K_1 \cong K_2$.

Теорема 1.5. Любое кольцо K изоморфно подкольцу кольца эндоморфизмов некоторой абелевой группы A. Если K – кольцо с единицей, то в качестве A можно взять аддитивную группу $(K, +)$ кольца K.

Эта теорема является кольцевым аналогом известной теоремы Кэли: всякая группа изоморфна группе взаимно однозначных отображений некоторого множества на себя.

Примеры решения и оформления задач

Пример 1. Пусть X – произвольное множество и $\mathcal{P}(X)$ – совокупность всех подмножеств из X. На $\mathcal{P}(X)$ введем операции сложения и умножения следующим образом:

$$A + B = (A \cup B) \setminus (A \cap B),$$
$$AB = A \cap B.$$

для любых $A, B \in \mathcal{P}(X)$. Доказать, что относительно этих операций $\mathcal{P}(X)$ – коммутативное кольцо с единицей, причем все элементы аддитивной группы $(\mathcal{P}(X), +)$ имеют порядок 2. Будет ли $\mathcal{P}(X)$ целостным кольцом?

Решение. Покажем сначала, что $\mathcal{P}(X)$ является абелевой группой относительно операции сложения.

На основании свойств операций над множествами убеждаемся, что $(A+B)+C = A+(B+C)$ для всех $A, B, C \in \mathcal{P}(X)$, т.е. операция сложения, определенная на $\mathcal{P}(X)$, ассоциативна. Роль нулевого элемента в $\mathcal{P}(X)$ играет пустое множество $\varnothing$, так как $A + \varnothing = (A \cup \varnothing) \setminus (A \cap \varnothing) = A \setminus \varnothing = A$ и

$$\varnothing + A = (\varnothing \cup A) \setminus (\varnothing \cap A) = A \setminus \varnothing = A.$$

Противоположным элементом к A будет само множество A, так как $A+A=(A\cup A)\setminus(A\cap A)=A\setminus A=\varnothing$

Таким образом, $\mathcal{P}(X)$ является группой относительно операции сложения. Из последнего равенства следует, что все элементы этой группы имеют порядок 2. Группа $(\mathcal{P}(X),+)$ абелева, так как $A+B=(A\cup B)\setminus(A\cap B)=(B\cup A)\setminus(B\cap A)=B+A$ для всех $A,B\in\mathcal{P}(X)$.

Проверим аксиому 2) из определения кольца:

$$(AB)C=(A\cap B)\cap C=A\cap(B\cap C)=A(BC)$$

далее $A(B+C)=A\cap((B\cup C)\setminus(B\cap C))=$

$$=(A\cap(B\cup C))\setminus(A\cap(B\cap C))=((A\cap B)\cup(A\cap C))\setminus$$

$$\setminus((A\cap B)\cap(A\cap C))=(AB\cup AC)\setminus(AB\cap AC)=$$

$$=AB+AC$$

Аналогично, $(A+B)C=AC+BC$

Итак, $\mathcal{P}(X)$ – кольцо. Это кольцо коммутативно, так как $AB=A\cap B=B\cap A=B\cap A=BA$ для любых $A,B\in\mathcal{P}(X)$. Роль единичного элемента в $\mathcal{P}(X)$ играет множество X, так как $AX=A\cap X=A$ и $XA=X\cap A=A$ для любого множества $A\in\mathcal{P}(X)$. Кольцо $\mathcal{P}(X)$ является целостным тогда и только тогда, когда множество X содержит только один элемент. Действительно, если X содержит более одного элемента, то, взяв в качестве A и B различные одноэлементные подмножества из X, получаем: $AB=A\cap B=\varnothing$, т.е. A и B являются в этом случае делителями нуля. Следовательно, при $\operatorname{card} X>1$ кольцо $\mathcal{P}(X)$ не является целостным.

Пример 2. В кольце $\mathbb{Z}_{231}$ решить уравнение

$$\overline{71}\,\overline{x}=\overline{25}$$

Решение. Так как $\overline{71}\,\overline{x}=\overline{71x}$, то имеем $\overline{71x}=\overline{25}$. Два класса вычетов равны тогда и только тогда, когда представители этих классов вычетов сравнимы. Значит,

$$71x\equiv 25\pmod{231}$$

Решим это сравнение. Для этого найдем числитель предпоследней подходящей дроби числа $\dfrac{231}{71}$. Применим алгоритм Евклида

$$\begin{array}{r|l} 231 & 71 \\ -213 & 3 \\ \hline 18 & \end{array}\qquad \begin{array}{r|l} 71 & 18 \\ -54 & 3 \\ \hline 17 & \end{array}\qquad \begin{array}{r|l} 18 & 17 \\ -17 & 1 \\ \hline 1 & \end{array}\qquad \begin{array}{r|l} 17 & 1 \\ -17 & 17 \\ \hline 0 & \end{array}$$

Составим таблицу

q_k		3	3	1	17
P_k	1	3	10	13	231

Применим формулу для решения сравнения:

$$x\equiv(-1)^{n-1}P_{n-1}b\pmod{m}$$

В нашем случае $n=4$, $P_{n-1}=P_3=13$, $b=25$. Значит,

$$x\equiv(-1)^3\,13\cdot 25\pmod{231}$$

или

$$x\equiv-325\pmod{231}\quad \text{Отсюда } x\equiv 137\pmod{231}$$

Значит, $\overline{x}=\overline{137}$

Пример 3. Составить таблицы сложения и умножения в кольце $\mathbb{Z}_4$. Найти в $\mathbb{Z}_4$ все делители нуля (если они есть). Показать, что множество всех обратимых элементов кольца $\mathbb{Z}_4$ относительно умножения образуют группу. Составить таблицу умножения в этой группе.

Решение. Кольцо $\mathbb{Z}_4$ состоит из четырех элементов $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$. Складываются и умножаются эти элементы по правилам: $\overline{a}+\overline{b}=\overline{a+b}$, $\overline{a}\cdot\overline{b}=\overline{ab}$. Отметим сразу, что два класса $\overline{a}$ и $\overline{b}$ равны тогда и только тогда, когда $a\equiv b\pmod 4$. Учитывая это, найдем, например:

$$\overline{2}+\overline{3}=\overline{5}=\overline{1}, \text{ так как } 5\equiv 1\pmod 4$$

$$\overline{2}\cdot\overline{3}=\overline{6}=\overline{2}, \text{ так как } 6\equiv 2\pmod 4$$

Окончательно все вычисления сведем в таблицы:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Из таблицы видим, что делителем нуля в кольце $\mathbb{Z}_4$ является элемент $\bar{2}$, так как $\bar{2}\cdot\bar{2}=\bar{0}$. Здесь же замечаем, что обратимыми в кольце $\mathbb{Z}_4$ являются элементы $\bar{1}$ и $\bar{3}$, так как $\bar{1}\cdot\bar{1}=\bar{1}$ и $\bar{3}\cdot\bar{3}=\bar{1}$. Таблица умножения обратимых элементов кольца имеет вид

$\cdot$	$\bar{1}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$

Из таблицы легко выводим, проверяя аксиомы группы, что множество $\{\bar{1},\bar{3}\}$ относительно умножения является группой.

Пример 4. Пусть X – произвольное множество, $E(X)$ – совокупность всех конечных подмножеств из X. Показать, что $E(X)$ – подкольцо кольца $\mathcal{P}(X)$ (см.пример I).

Решение. Применим критерий для подколец. Пусть $A,B\in E(X)$, т.е. $\operatorname{card} A<\infty$, $\operatorname{card} B<\infty$. Тогда $\operatorname{card}(A+B)=\operatorname{card}((A\cup B)\setminus(A\cap B))\leq \operatorname{card}(A\cup B)\leq \operatorname{card} A+\operatorname{card} B<\infty$. Значит, $A+B\in E(X)$.

Аналогично, $\operatorname{card}(AB)=\operatorname{card}(A\cap B)\leq \max\{\operatorname{card} A,\operatorname{card} B\}<\infty$. Значит, $AB\in E(X)$.

Противоположным к A в $\mathcal{P}(X)$ является само множество A. Значит, $\operatorname{card}(-A)=\operatorname{card} A<\infty$, т.е. $-A\in E(X)$. В силу теоремы I.3 $E(X)$ является подкольцом кольца $\mathcal{P}(X)$.

Вопросы для самоконтроля

I. Как определяется аддитивная абелева группа?
2. Как задать кольцо?
3. Приведите примеры колец без единицы.
4. Приведите примеры некоммутативных колец.

5. Какие элементы в кольцах $\mathbb{Z}$, $\mathbb{R}[x]$, $M(n,\mathbb{R})$ обратимы?
6. Докажите, что кольцо K не может иметь два различных нулевых элемента.
7. Сколько единиц может иметь кольцо?
8. Приведите примеры колец, которые не являются областями целостности.
9. В чем отличие тела от кольца и поля?
I0. Всегда ли в кольце K из $ab=ac$ следует, что $b=c$?
II. Пусть A – аддитивная абелева группа. Какой эндоморфизм группы A является нулем кольца $\operatorname{End} A$?
I2. Какой эндоморфизм группы A является единицей $\operatorname{End} A$?
I3. Опишите обратимые элементы кольца $\operatorname{End} A$.
I4. Покажите, что пересечение подколец кольца K является подкольцом.
I5. Является ли изоморфизм колец отношением эквивалентности?
I6. Сформулируйте определение изоморфизма колец K_1 и K_2 в предположении, что в K_1 операции обозначаются через $+$ и $\cdot$, а в K_2 – $\oplus$ и $\odot$.
I7. Пусть $\varphi: K_1\to K_2$ – изоморфизм колец K_1 и K_2. Доказать, что K_2 – коммутативное кольцо с единицей, если таковым является K_1.

Задания к лабораторной работе

I. Является ли множество $\mathbb{Z}$ целых чисел кольцом относительно операций $\oplus$ и $\odot$. Если $\mathbb{Z}$ является кольцом, то найти в нем все делители нуля и единицы (если они существуют):

а) $a\oplus b=a+b+1$, $a\odot b=a+b+ab$;
б) $a\oplus b=a+b-2$, $a\odot b=a+b+2ab$;
в) $a\oplus b=a+b-1$, $a\odot b=a+b-ab$;
г) $a\oplus b=2a+2b+4$, $a\odot b=ab+a+b$;
д) $a\oplus b=a+b+2$, $a\odot b=a+b-2ab$.

2. Являются ли кольцами множества K и M с определенными на них операциями сложения и умножения? Изоморфны ли они?

а) $K=\{a+b\sqrt{3}\mid a,b\in\mathbb{Z}\}$,
$M=\left\{\begin{pmatrix} a & 3b\\ b & a\end{pmatrix}\mid a,b\in\mathbb{Z}\right\}$;
б) $K=\{a+bi\mid a,b\in 3\mathbb{Z}\}$,
$M=\left\{\begin{pmatrix} a & -b\\ b & a\end{pmatrix}\mid a,b\in 3\mathbb{Z}\right\}$;

в) $K=\{a+b\sqrt{2} \mid a,b\in 2\mathbb{Z}\}$,

$M=\left\{\begin{pmatrix} a & 2b \\ b & a\end{pmatrix} \mid a,b\in 2\mathbb{Z}\right\}$;

г) $K=\{a+bi \mid a,b\in \mathbb{Q}\}$,

$M=\left\{\begin{pmatrix} a & b \\ b & a\end{pmatrix} \mid a,b\in \mathbb{Q}\right\}$;

д) $K=\left\{\frac{a+bi\sqrt{3}}{2} \mid a,b\in\mathbb{Z}; a,b\right.$ одинаковой четности$\left.\right\}$,

$M=\left\{\begin{pmatrix} \frac{1}{2}a & -\frac{3}{2}b \\ \frac{1}{2}b & \frac{1}{2}a\end{pmatrix} \mid a,b\in\mathbb{Z}; a,\right.$" одинаковой четности$\left.\right\}$.

3. В кольце $\mathbb{Z}_m$ решить уравнения:

а) $\overline{19}\,\overline{x}=\overline{25}$, $m=36$;
б) $\overline{14}\,\overline{x}=\overline{3}$, $m=17$;
в) $\overline{31}\,\overline{x}=\overline{23}$, $m=41$;
г) $\overline{41}\,\overline{x}=\overline{11}$, $m=51$;
д) $\overline{29}\,\overline{x}=\overline{19}$, $m=37$.

4. Составить таблицы сложения и умножения в кольце $\mathbb{Z}_m$. Найти в $\mathbb{Z}_m$ все делители нуля (если они существуют). Показать, что множество обратимых элементов кольца $\mathbb{Z}_m$ относительно умножения образует группу. Составить таблицу умножения в этой группе:

а) $m=6$; б) $m=7$; в) $m=8$; г) $m=9$; д) $m=10$;

5. Будет ли подмножество L кольца K подкольцом в K ?

а) $L=\{a+bi \mid a=b\in\mathbb{Z}\}$,
$K=\{a+bi \mid a,b\in\mathbb{Z}\}$;

б) $L=\{(a+bi)(1+i) \mid a,b\in\mathbb{Z}\}$,
$K=\{a+bi \mid a,b\in\mathbb{Z}\}$;

в) L – множество многочленов из $\mathbb{Z}[x]$, не содержащих членов с x^2,

г) L – множество многочленов из $\mathbb{Z}[x]$ с четными свободными членами;
$K=\mathbb{Z}[x]$;

д) $L=\{a+b\sqrt{3} \mid a,b\in\mathbb{Q}\}$,
$K=\mathbb{R}$.

6. В кольце $M(3,\mathbb{Q})$ найти элемент, обратный к A :

а) $A=\begin{pmatrix} 2&1&3\\5&3&2\\1&4&3\end{pmatrix}$; б) $A=\begin{pmatrix} 3&2&1\\2&5&3\\3&4&2\end{pmatrix}$; в) $A=\begin{pmatrix} 3&2&-4\\4&1&-2\\5&2&-3\end{pmatrix}$

г) $A=\begin{pmatrix} 1&1&1\\1&2&3\\1&3&6\end{pmatrix}$; д) $A=\begin{pmatrix} 5&6&3\\0&1&0\\7&4&5\end{pmatrix}$;

7. Показать, что матрица A является делителем нуля в $M(2,\mathbb{R})$. Найти все такие матрицы $B\in M(2,\mathbb{R})$, для которых $AB=O$:

а) $A=\begin{pmatrix} 1&0\\2&0\end{pmatrix}$; б) $A=\begin{pmatrix} 0&0\\2&3\end{pmatrix}$; в) $A=\begin{pmatrix} 1&2\\2&4\end{pmatrix}$;

г) $A=\begin{pmatrix} 1&1\\2&2\end{pmatrix}$; д) $A=\begin{pmatrix} 0&1\\0&3\end{pmatrix}$.

Распределение задач по вариантам

Вариант 1: №№ 1(а), 2(а), 3(а), 4(а), 5(а), 6(а), 7(а).
Вариант 2: №№ 1(б), 2(б), 3(б), 4(б), 5(б), 6(б), 7(б).
Вариант 3: №№ 1(в), 2(в), 3(в), 4(в), 5(в), 6(в), 7(в).
Вариант 4: №№ 1(г), 2(г), 3(г), 4(г), 5(г), 6(г), 7(г).
Вариант 5: №№ 1(д), 2(д), 3(д), 4(д), 5(д), 6(д), 7(д).

Лабораторная работа № 2
ПОЛЯ

Напомним, что непустое множество T с двумя бинарными алгебраическими операциями (сложением и умножением) называется **телом**, если выполняются следующие условия:

1) множество T с операцией сложения является абелевой группой; эта группа называется **аддитивной группой тела** и обозначается $(T,+)$;

2) множество $T^{\#}=T\setminus\{0\}$ с операцией умножения является группой; эта группа называется **мультипликативной группой** тела и обозначается через $(T^{\#},\cdot)$;

3) операция сложения связана с операцией умножения законами дистрибутивности, т.е. $(a+b)c=ac+bc$, $a(b+c)=ab+ac$ для любых $a,b,c\in T$.

Если в теле T умножение коммутативно, т.е. $ab=ba$ для любых $a,b\in T$, то тело T называется **полем**. Другими словами, поле – это коммутативное кольцо с единицей, отличной от нуля, в котором каждый ненулевой элемент обратим. Примерами полей служат множества $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ рациональных, действительных и комплексных чисел с обычными операциями сложения и умножения чисел. Кольцо $\mathbb{Z}$ целых чисел не является полем, но кольцо $\mathbb{Z}_p$ классов вычетов по простому модулю p является полем из p элементов:

$$\mathbb{Z}_p=\{\bar{0},\bar{1},\bar{2},\ldots,\overline{p-1}\}$$

Пример. Показать, что множество

$$T=\left\{\begin{pmatrix} u & v\\ -\bar{v} & \bar{u}\end{pmatrix} \;\middle|\; u,v\in\mathbb{C}\right\}$$

– некоммутативное тело.

Решение. Если $u=a+bi$ – комплексное число, то $\bar{u}=a-bi$ – сопряженное ему число, и $u\bar{u}=a^2+b^2\geqslant 0$. Кроме того, $\overline{u+v}=\bar{u}+\bar{v}$, $\overline{uv}=\bar{u}\,\bar{v}$ и $\bar{\bar{u}}=u$. Поэтому

$$\begin{pmatrix} u & v\\ -\bar{v} & \bar{u}\end{pmatrix}+\begin{pmatrix} w & z\\ -\bar{z} & \bar{w}\end{pmatrix}=\begin{pmatrix} u+w & v+z\\ -\overline{(v+z)} & \overline{u+w}\end{pmatrix}\in T,$$

$$\begin{pmatrix} u & v\\ -\bar{v} & \bar{u}\end{pmatrix}\begin{pmatrix} w & z\\ -\bar{z} & \bar{w}\end{pmatrix}=\begin{pmatrix} uw+v(-\bar{z}) & uz+v\bar{w}\\ -\bar{v}w-\bar{u}\bar{z} & -\bar{v}z+\bar{u}\bar{w}\end{pmatrix}=\begin{pmatrix} uw-v\bar{z} & uz+v\bar{w}\\ -\overline{(uz+v\bar{w})} & \overline{uw-v\bar{z}}\end{pmatrix}\in T$$

т.е. сложение и умножение матриц определено на множестве T. Ясно, что сложение коммутативно и ассоциативно. Нулевая матрица содержится в T, а противоположная

$$-\begin{pmatrix} u & v\\ -\bar{v} & \bar{u}\end{pmatrix}=\begin{pmatrix} -u & -v\\ \bar{v} & -\bar{u}\end{pmatrix}$$

для матрицы из T также находится в T. Итак, $(T,+)$ – абелева группа.

Умножение матриц из T ассоциативно, но некоммутативно. Действительно, так как $\bar{i}=-i$, то

$$\begin{pmatrix} i & 0\\ 0 & \bar{i}\end{pmatrix}=\begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix}\in T,\quad \begin{pmatrix} 0 & i\\ -\bar{i} & 0\end{pmatrix}=\begin{pmatrix} 0 & i\\ i & 0\end{pmatrix}\in T$$

Но эти матрицы не перестановочны:

$$\begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix}\begin{pmatrix} 0 & i\\ i & 0\end{pmatrix}=\begin{pmatrix} 0 & -1\\ 1 & 0\end{pmatrix}\neq\begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}=\begin{pmatrix} 0 & i\\ i & 0\end{pmatrix}\begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix}$$

Единичная матрица содержится в T, а если $\begin{pmatrix} u & v\\ -\bar{v} & \bar{u}\end{pmatrix}$ – ненулевая матрица, то $u\bar{u}+v\bar{v}>0$ и существует матрица

$$\frac{1}{u\bar{u}+v\bar{v}}\begin{pmatrix} \bar{u} & -v\\ \bar{v} & u\end{pmatrix},$$

которая принадлежит T и является обратной к матрице $\begin{pmatrix} u & v\\ -\bar{v} & \bar{u}\end{pmatrix}$. Таким образом, каждая ненулевая матрица из T обладает в T обратной матрицей.

Поскольку сложение и умножение матриц дистрибутивно, то T – тело, но не поле. Это тело называется **телом кватернионов**.

Два тела или два поля P_1 и P_2 называются **изоморфными**, если они изоморфны как кольца, т.е. если существует взаимно однозначное отображение $f: P_1\to P_2$, при котором

$$f(a+b)=f(a)+f(b),$$
$$f(ab)=f(a)f(b)$$

для любых $a,b\in P_1$.

Введем теперь понятие характеристики. Пусть K – произвольное целостное кольцо. Тогда вместе с единичным элементом 1 кольцо содержит все его кратные $n1=\underbrace{1+1+\ldots+1}_{n\ \text{раз}}$, $n\in\mathbb{N}$. Возможны два условия:

1) $n1\neq 0$ для любого натурального n. В этом случае говорят, что целостное кольцо K имеет **характеристику нуль** и пишут $\operatorname{char} K=0$;

2) $n1=0$ для некоторого $n\in\mathbb{N}$. В этом случае **характеристикой** целостного кольца K называют наименьшее натуральное число n такое, что $n1=0$.

Т е о р е м а 2.1. Для целостного кольца K справедливы следующие утверждения.

1) характеристикой K является либо нуль, либо простое число;

2) если $\mathrm{char}\, K = 0$, то $na \neq 0$ для любых $a \in K^{\#}$ и $n \in \mathbb{N}$;

3) если $\mathrm{char}\, K = p \neq 0$, то p - простое и $pa = 0$ для всех $a \in K$. Кроме того, $ma = 0$, $a \in K^{\#}$, тогда и только тогда, когда m кратно p.

Поскольку всякое поле есть целостное кольцо, то мы можем говорить о характеристике поля. Ясно, что $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ - поле характеристики нуль, а $\mathbb{Z}_p$ - поле характеристики p.

Подмножество L поля P называется п о д п о л е м, если L само является полем относительно операций сложения и умножения, определенных в K. Поле, не обладающее никаким собственным подполем, называется п р о с т ы м.

Т е о р е м а 2.2. I) Поля $\mathbb{Q}$ и $\mathbb{Z}_p$ - простые.

2) Каждое поле P содержит в точности одно простое подполе P_0.

3) Если $\mathrm{char}\, P = 0$, то P_0 изоморфно $\mathbb{Q}$.

4) Если $\mathrm{char}\, P = p \neq 0$, то P_0 изоморфно $\mathbb{Z}_p$.

Представляет определенный интерес вопрос о вложении целостного кольца в поле. Поле F называется п о л е м ч а с т н ы х ц е л о с т н о г о к о л ь ц а K, если выполнены условия:

1) K есть подкольцо поля F;

2) для любого $x \in F$ существуют в K также элементы a и b, что $x = ab^{-1}$.

Т е о р е м а 2.3. I) Для любой области целостности существует поле частных.

2) Если F_1 и F_2 - поля частных целостного кольца K, то существует изоморфизм поля F_1 на поле F_2, переводящий каждый элемент кольца K в себя.

П р и м е р ы р е ш е н и я и о ф о р м л е н и я з а д а ч

П р и м е р I. Являются ли изоморфными полями следующие множества:

$$P_1 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\};$$

$$P_2 = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{Q} \right\}.$$

Р е ш е н и е. В начале проверим, что P_1 - поле. Заметим, что любое число из P_1 единым образом представляется в виде двучлена $a + b\sqrt{2}$ с рациональными a и b. Действительно, если $a + b\sqrt{2} = c + d\sqrt{2}$, то $a - c = (d - b)\sqrt{2}$. В случае, $d \neq b$ получилось бы, что $\sqrt{2} = \frac{a-c}{d-b}$ - рациональное число, что невозможно. Поэтому $d = b$, но тогда и $a = c$.

Возьмем теперь два числа $a + b\sqrt{2}$, $c + d\sqrt{2}$ из множества P_1. Их сумма и произведение

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2},$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

принадлежит тому же множеству.

Сложение и умножение чисел ассоциативно, коммутативно и дистрибутивно. Числа $0 = 0 + 0\sqrt{2}$ и $1 = 1 + 0\sqrt{2}$ принадлежат P_1. Противоположные числа

$$-(a + b\sqrt{2}) = -a - b\sqrt{2}$$

также имеются в P_1. Поэтому P_1 - коммутативное кольцо с единицей.

Наконец, если $a + b\sqrt{2} \neq 0$, то a и b одновременно неравны нулю, а так как a и b - рациональные, то $a^2 - 2b^2 \neq 0$. Поэтому существует число $\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$,

и оно принадлежит P_1. Это число будет обратным к $a + b\sqrt{2}$, поскольку $(a + b\sqrt{2})\left(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}\right) =$

$$= \frac{1}{a^2 - 2b^2}(a + b\sqrt{2})(a - b\sqrt{2}) = \frac{1}{a^2 - 2b^2}(a^2 - 2b^2) = 1$$

Итак, мы проверили, что P_1 - поле.

Аналогично проверяется, что P_2 - поле. В частности, обратной к ненулевой матрице $\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$ будет матрица $\frac{1}{a^2 - 2b^2}\begin{pmatrix} a & -2b \\ -b & a \end{pmatrix}$,

которая существует и принадлежит P_2.

Зададим отображение

$$f : a + b\sqrt{2} \mapsto \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$$

из поля P_1 на поле P_2. Ясно, что f - взаимнооднозначное отображение. Так как

$$f((a + b\sqrt{2}) + (c + d\sqrt{2})) = f(a + c + (b + d)\sqrt{2}) =$$

$$= \begin{pmatrix} a+c & 2(b+d) \\ b+d & a+c \end{pmatrix} = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} + \begin{pmatrix} c & 2d \\ d & c \end{pmatrix} =$$

$$= f(a+b\sqrt{2}) + f(c+d\sqrt{2})$$

и $f((a+b\sqrt{2})(c+d\sqrt{2})) = f(ac+2bd+(ad+bc)\sqrt{2}) =$

$$= \begin{pmatrix} ac+2bd & 2(ad+bc) \\ ad+bc & ac+2bd \end{pmatrix} = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\begin{pmatrix} c & 2d \\ d & c \end{pmatrix} =$$

$$= f(a+b\sqrt{2})\, f(c+d\sqrt{2}),$$

то отображение f удовлетворяет всем требованиям изоморфизма полей. Поэтому поля P_1 и P_2 изоморфны.

П р и м е р 2. Показать, что множество чисел вида $a+b\alpha+c\alpha^2$ с рациональными a, b и c, где α - один из корней многочлена x^3-5, образует поле относительно сложения и умножения. Найти обратный элемент $(1+\alpha+\alpha^2)^{-1}$.

Р е ш е н и е. Обозначим через P рассматриваемое множество чисел вида $a+b\alpha+c\alpha^2$ с рациональными a, b, c, где α - один из корней многочлена x^3-5. Проверим, что каждый элемент из P единственным образом выражается в виде трехчлена $a+b\alpha+c\alpha^2$. В самом деле, пусть $a+b\alpha+c\alpha^2 = a_1+b_1\alpha+c_1\alpha^2$. Тогда $(a-a_1)+(b-b_1)\alpha+(c-c_1)\alpha^2=0$. Если $c-c_1=0$, то при $b-b_1\neq 0$ получается, что $\alpha = \frac{a_1-a}{b-b_1}$ - рациональное, что невозможно. Если же $c-c_1=0$ и $b-b_1=0$, то $a-a_1=0$, т.е. $a=a_1$, $b=b_1$, $c=c_1$. Таким образом, остается разобрать случай $c-c_1\neq 0$. В этом случае α является корнем квадратного уравнения

$$\alpha^2+p\alpha+q=0,$$

где $p=\frac{b-b_1}{c-c_1}$, $q=\frac{a-a_1}{c-c_1}$. Отсюда получается, что

$$\alpha^2=-p\alpha-q;\quad \alpha^3=-p\alpha^2-q\alpha=-p(-p\alpha-q)-q\alpha;$$
$$\alpha^3=(p^2-q)\alpha+pq.$$

Так как $\alpha^3=5$, то $(p^2-q)\alpha+pq-5=0$. В силу иррациональности α отсюда вытекает, что $p^2-q=0$, $pq-5=0$, и, значит, $p^3=5$. Это невозможно, так как $\sqrt[3]{5}$ - иррациональное число.

Итак, каждое число $a+b\alpha+c\alpha^2$ из P однозначно определяется тремя рациональными числами a, b и c. Поэтому операции сложения и умножения чисел P определяются так

$$(a_1+b_1\alpha+c_1\alpha^2)+(a_2+b_2\alpha+c_2\alpha^2)=(a_1+a_2)+(b_1+b_2)\alpha+(c_1+c_2)\alpha^2$$

$$(a_1+b_1\alpha+c_1\alpha^2)(a_2+b_2\alpha+c_2\alpha^2)=a_1a_2+(a_1b_2+b_1a_2)\alpha+(a_1c_2+$$
$$+b_1b_2+c_1a_2)\alpha^2+(b_1c_2+c_1b_2)\alpha^3+c_1c_2\alpha^4=a_1a_2+5(b_1c_2+$$
$$+c_1b_2)+(a_1b_2+b_1a_2+5c_1c_2)\alpha+(a_1c_2+b_1b_2+c_1a_2)\alpha^2$$

Здесь мы использовали равенства $\alpha^3=5$, $\alpha^4=5\alpha$. Из этих равенств следует, что операции сложения и вычитания определены на P. Так как $P\subseteq\mathbb{R}$, то эти операции ассоциативны, коммутативны и дистрибутивны. Нулевым элементом будет $0=0+0\alpha+0\alpha^2$, а единичным - $1=1+0\alpha+0\alpha^2$. Противоположным будет -

$$-(a+b\alpha+c\alpha^2)=-a-b\alpha-c\alpha^2$$

Перейдем к нахождению обратного элемента. Рассмотрим уравнение

$$(a+b\alpha+c\alpha^2)(x+y\alpha+z\alpha^2)=1$$

Если в его левой части перемножить многочлены, заменить α^3 и α^4 соответственно на 5 и 5α и сгруппировать члены по возрастающим степеням α, то получится

$$(a_{11}x+a_{12}y+a_{13}z)+(a_{21}x+a_{22}y+a_{23}z)\alpha+$$
$$(a_{31}x+a_{32}y+a_{33}z)\alpha^2=1,$$

где a_{ij} - некоторое рациональное число. Отсюда

$$\begin{cases} a_{11}x+a_{12}y+a_{13}z=1, \\ a_{21}x+a_{22}y+a_{23}z=0, \\ a_{31}x+a_{32}y+a_{33}z=0. \end{cases} \qquad \text{(I)}$$

Определитель d этой системы отличен от нуля. В самом деле, если бы $d=0$, то система однородных уравнений

$$\begin{cases} a_{11}x+a_{12}y+a_{13}z=0, \\ a_{21}x+a_{22}y+a_{23}z=0, \\ a_{31}x+a_{32}y+a_{33}z=0 \end{cases}$$

с теми же коэффициентами a_{ij}, что и предыдущая система, имела бы нулевое решение, например x_0, y_0, z_0. Поэтому произведение двух чисел $x_0+y_0\alpha+z_0\alpha^2$ и $a+b\alpha+c\alpha^2$, отличных от нуля, равнялось бы нулю, что невозможно.

Но если $d\neq 0$, то система (I) имеет единственное решение, т.е. существует единичное число $a_1+b_1\alpha+c_1\alpha^2$ с рациональными a_1, b_1, c_1, обратное для $a+b\alpha+c\alpha^2$ и лежащее в P

Таким образом, мы убедились, что P – поле.

Отсюда получается довольно простой способ нахождения обратного элемента в поле P. Например, для $\beta=1+\alpha+\alpha^2$ находим обратный элемент β^{-1} следующим образом. Полагая $\beta^{-1}=x+y\alpha+z\alpha^2$, получаем

$$x+(x+y)\alpha+(x+y+z)\alpha^2+(y+z)\alpha^3+z\alpha^4=1$$

Так как $\alpha^3=5$, $\alpha^4=\alpha^3\alpha=5\alpha$, то последнее равенство преобразуется к следующему.

$$(x+5y+5z)+(x+y+5z)\alpha+(x+y+z)\alpha^2=1$$

Отсюда получаем систему

$$\begin{cases} x+5y+5z=1 \\ x+y+5z=0 \\ x+y+z=0 \end{cases}$$

Решая эту систему, находим, что $x=-\frac{1}{4}$, $y=\frac{1}{4}$, $z=0$. Таким образом, $(1+\alpha+\alpha^2)^{-1}=-\frac{1}{4}+\frac{1}{4}\alpha$.

П р и м е р 3. Найти наибольший общий делитель многочленов

$$f(x)=x^3+x^2+2x+2\,,\quad g(x)=x^2+x+1$$

над полем $\mathbb{Z}_5$.

Р е ш е н и е. В поле $\mathbb{Z}_5$ пять элементов 0,I,2,3,4, которые складываются и умножаются по модулю 5. Противоположными будут элементы $-0=0$, $-1=4$, $-2=3$, $-4=1$, а обратными $1^{-1}=1$, $2^{-1}=3$, $3^{-1}=2$, $4^{-1}=1$. Используя эти равенства, разделим $f(x)$ на $g(x)$:

$$\begin{array}{r|l} -\;x^3+x^2+2x+2 & x^2+x+1 \\ \underline{x^3+x^2+x\qquad} & x \\ x+2 & \end{array}$$

Имеем: $f(x)=g(x)x+(x+2)$. Теперь разделим $g(x)$ на первый остаток $(x+2)$:

$$\begin{array}{r|l} -\;x^2+x+1 & x+2 \\ \underline{x^2+2x\quad} & x+4 \\ -\;4x+1 & \\ \underline{4x+3} & \\ 3 & \end{array}$$

Имеем: $g(x)=(x+2)(x+4)+3$. Теперь разделим $x+2$ на 3:

$$\begin{array}{r|l} -\;x+2 & 3 \\ \underline{x\quad} & 2x+4 \\ -\;2 & \\ \underline{2} & \\ 0 & \end{array}$$

Итак, алгоритм Евклида для многочленов $f(x)$ и $g(x)$ принимает вид:

$$f(x)=g(x)x+(x+2),$$
$$g(x)=(x+2)(x+4)+3,$$
$$x+2=3(2x+4)$$

Последний отличный от нуля остаток будет наибольшим общим делителем многочленов, т.е. $НОД(f(x),g(x))=3$.

П р и м е р 4. Разложить на неприводимые многочлены над полем $\mathbb{Z}_3$ все многочлены второй степени от x со старшим коэффициентом I.

Р е ш е н и е. Поле $\mathbb{Z}_3$ состоит из трех элементов 0,I,2, которые складываются и умножаются по модулю 3. Многочлены второй степени со старшим коэффициентом I исчерпываются следующими многочленами:

x^2, x^2+1, x^2+2; x^2+x, x^2+x+1, x^2+x+2, x^2+2x, x^2+2x+1, x^2+2x+2

Очевидно, $x^2=x\,x$, $x^2+x=x(x+1)$, $x^2+2x=x(x+2)$.

Для остальных многочленов будем искать корни. Поскольку уравнению x^2+1 не удовлетворяет ни один из элементов поля $\mathbb{Z}_3$, то x^2+1 не имеет в $\mathbb{Z}_3$ корней, и, по теореме Безу, этот многочлен неприводим. Аналогично проверяется, что x^2+x+2 и x^2+2x+2 неприводимы.

Многочлен x^2+2 имеет корнем элемент I и, по теореме Безу, x^2+2 делится на $x-1=x+2$:

$$\begin{array}{r|l} -\;x^2+2 & x+2 \\ \underline{x^2+2x} & x+1 \\ -\;x+2 & \\ \underline{x+2} & \\ 0 & \end{array}$$

Следовательно, $x^2+2=(x+2)(x+1)$

Многочлен x^2+x+1 имеет корнем элемент I и, по теореме Безу, x^2+x+1 делится на $x+2$.

$$
\begin{array}{r|l}
x^2+x+1 & x+2 \\
\underline{-\,x^2+2x} & \overline{x+2} \\
2x+1 & \\
\underline{-\,2x+1} & \\
0 &
\end{array}
$$

Следовательно, $x^2+x+1=(x+2)^2$. Ясно, что $x^2+2x+1=(x+1)^2$.

Ответ: $x^2=x\,x$, $x^2+2=(x+2)(x+1)$, $x^2+x=x(x+1)$, $x^2+x+1=(x+2)^2$, $x^2+2x=x(x+2)$, $x^2+2x+1=(x+1)^2$, а многочлены x^2+1 , x^2+x+2 и x^2+2x+2 неприводимы.

Вопросы для самопроверки

I. Почему в теле не менее двух элементов?
2. Может ли нулевой элемент тела совпадать с единичным?
3. Проверить, что множество скалярных матриц над телом (полем) T также является телом (полем), изоморфным T .
4. Покажите, что тело не содержит делителей нуля.
5. Будет ли тело (поле) целостным кольцом?
6. Является ли изоморфизм тел (полей) отношением эквивалентности.
7. Покажите, что если два тела изоморфны, и одно из них является полем, то и другое будет полем.
8. Будет ли отображение $\varphi: \mathbb{C} \to \mathbb{C}$, где $\varphi(z)=\overline{z}$, - изоморфизмом? Когда $\varphi(z)=z$?
9. Пусть F - конечное поле, содержащее m элементов. Почему $a^m=a$ для любого $a \in F$?
I0. Докажите, что конечное целостное кольцо является полем.
II. Сформулируйте опеределение характеристики поля.
I2. Установите связь между характеристикой целостного кольца K и порядком единичного элемента в группе $(K,+)$.
I3. Покажите, что изоморфные поля имеют равные характеристики.
I4. Может ли конечное поле иметь характеристику нуль?
I5. Приведите примеры бесконечного поля характеристики 5.
I6. Проверьте, что пересечение подполей вновь является подполем.

Задания к лабораторной работе

I. Над полем $\mathbb{C}$ комплексных чисел решить систему уравнений :

а) $\begin{cases} (2+i)x-(3+i)y=i \\ (3+i)x-(2-i)y=i \end{cases}$

б) $\begin{cases} (2-i)x+(5-3i)y=2+3i \\ (7+4i)x-(4+5i)y=4+i \end{cases}$;

в) $\begin{cases} ix+(1+i)y=3-i \\ (1-i)x-(6-i)y=4 \end{cases}$;

г) $\begin{cases} (1+i)x-2iy=-2 \\ (1-i)x+(2-i)y=3-3i \end{cases}$;

д) $\begin{cases} (1-i)x-(3+i)y=4 \\ 5x-(4+2i)y=9+2i \end{cases}$.

2. В поле $\mathbb{Z}_p$ укажите каждому элементу противоположный и обратный
а) $p=17$; б) $p=13$; в) $p=11$; г) $p=7$; д) $p=19$

3. Найти матрицу, обратную к матрице A над полем $\mathbb{Z}_p$:

а) $A=\begin{pmatrix} 2 & 1 & 3 \\ 5 & 3 & 2 \\ 1 & 4 & 3 \end{pmatrix}$ $p=13$;

б) $A=\begin{pmatrix} 3 & 2 & 1 \\ 2 & 5 & 3 \\ 3 & 4 & 2 \end{pmatrix}$ $p=5$,

в) $A=\begin{pmatrix} 3 & 2 & 1 \\ 2 & 5 & 3 \\ 3 & 1 & 4 \end{pmatrix}$ $p=3$,

г) $A=\begin{pmatrix} 1 & 4 & 3 \\ 2 & 1 & 3 \\ 5 & 3 & 2 \end{pmatrix}$ $p=11$;

д) $A=\begin{pmatrix} 5 & 3 & 2 \\ 1 & 4 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $p=7$.

4. Над полем $\mathbb{Z}_p$ решить систему уравнений

а) $\begin{cases} x+2z=1 \\ y+2z=2 \\ 2x+z=1 \end{cases}$ $p=7$;

б) $\begin{cases} 3x+y+2z=1 \\ x+2y+3z=1 \\ 4x+3y+2z=1 \end{cases}$ $p=11$;

в) $\begin{cases} 2x + z = 1 \\ y + 2z = 2 \\ x + 2z = 1 \end{cases}$ $p = 5$;

г) $\begin{cases} x + 2y + 3z = 1 \\ 4x + 3y + 2z = 1 \\ 3x + y + 2z = 1 \end{cases}$ $p = 7$;

д) $\begin{cases} 4x + 3y + 2z = 1 \\ 3x + y + 2z = 1 \\ x + 2y + 3z = 1 \end{cases}$ $p = 5$.

5. Найти наибольший общий делитель многочленов $f(x)$ и $g(x)$ над полем $\mathbb{Q}$ и $\mathbb{Z}_p$:
   а) $f(x) = x^3 + x^2 + 2x + 2$;
   $g(x) = x^2 + x + 1$
   $p = 3$
   б) $f(x) = 5x^3 + x^2 + 5x + 1$
   $g(x) = 5x^2 + 21x + 4$,
   $p = 7$
   в) $f(x) = x^4 + 1$
   $g(x) = x^3 + x + 1$;
   $p = 5$
   г) $f(x) = 5x^3 + x^2 + 5x + 1$
   $g(x) = 5x^2 + 21x + 4$;
   $p = 5$
   д) $f(x) = x^4 + 1$
   $g(x) = x^3 + x + 1$
   $p = 7$
6. Разложить на непри одимые множители над полем $\mathbb{Z}_p$:
   а) все многочлены третьей степени от x , $p = 2$,
   б) все многочлены второй степени от x , $p = 2$:
   в) многочлен $x^4 + x^3 + x + 2$, $p = 5$;
   г) многочлен $x^5 + x^3 + x^2 + 1$, $p = 2$;
   д) многочлен $x^3 + 2x^2 + 4x + 1$, $p = 5$.
7. Показать, что матрицы вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, a и $b \in \mathbb{R}$, образуют поле, изомо фное полю комплексных чисел.
8. Во множестве $P = \{-1, 0, 1\}$ сложение определено следующим образом: $1 + 1 = -1$, $(-1) + (-1) = 1$, остальные строки сложения - как обычно. Умножение в P тоже обычное. Доказать, что P - поле и найти его характеристику.

9. Пусть $*$ означает операцию $a * b = 2ab$. Доказать, что $\mathbb{R}$ с обычным сложением и умножением $*$ является полем, изоморфным полю действительных чисел.
10. Изоморфно ли полю действительных чисел множество матриц $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$ $a \in \mathbb{R}$ с обычными операциями сложения и умножения матриц?
11. Изоморфно ли полю рациональных чисел множество матриц $\begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix}$ $a \in \mathbb{Q}$ с обычными операциями сложения и умножения матриц?

Распределение задач по вариантам

Вариант 1: №№ 1(а), 2(а), 3(а), 4(а), 5(а), 6(а), 9.
Вариант 2: №№ 1(б), 2(б), 3(б), 4(б), 5(б), 6(б), 10.
Вариант 3: №№ 1(в), 2(в), 3(в), 4(в), 5(в), 6(в), 8.
Вариант 4: №№ 1(г), 2(г), 3(г), 4(г), 5(г), 6(г), 11.
Вариант 5: №№ 1(д), 2(д), 3(д), 4(д), 5(д), 6(д), 7.

Лабораторная работа № 3
ДЕЛИМОСТЬ В ЦЕЛОСТНЫХ КОЛЬЦАХ

Пусть K - целостное кольцо, т.е. коммутативное кольцо с единицей $1 \neq 0$ без делителей нуля. Говорят, что элемент $a \in K$ **делится** на $b \in K$ (или b **делит** a), если существует такой элемент $c \in K$, что $a = bc$. Элемент b называется **делителем** элемента a . Для обозначения делимости элемента a на элемент b применяются две записи: 1) $a \vdots b$ - читается: a делится на b ; 2) $b \mid a$ - читается: b делит a .

Из определения следует, что делители единицы - это в точности обратимые элементы целостного кольца K .

Два элемента $a, b \in K$ называются **ассоциированными элементами**, если $a = bu$, где u - обратимый элемент кольца K . Очевидно, что ассоциированные элементы делят друг друга.

Всякий элемент $a \in K$ делится на любой обратимый элемент и на каждый ассоциированный с a элемент. Такие делители называют **тривиальными делителями** элемента a . **Составным**, или **приводимым** в K элементом называется отличный от нуля элемент $a \in K$, представимый в виде произведения двух нетривиальных делителей. Другими словами, элемент a называется **составным**, если он отличен от нуля и его можно представить в виде произведения двух необратимых элементов.

Элемент $p \in K$ называется **простым**, или **неприводимым**, если он неприводим и его нельзя представить в виде $p = ab$, где a и b – необратимые элементы.

Таким образом, множество всех элементов целостного кольца распадается на четыре класса:

I) множество, содержащее один элемент – ноль;

2) множество всех обратимых элементов = множество всех делителей единицы;

3) множество всех простых элементов;

4) множество всех составных элементов.

Пример I. В кольце $\mathbb{Z}$ целых чисел делителями единицы являются числа I и -I. Ассоциированными элементами в $\mathbb{Z}$ будут противоположные числа a и $-a$, для каждого $a \in \mathbb{Z}$. Далее, только I и -I обратимы в $\mathbb{Z}$. Поэтому простыми элементами в $\mathbb{Z}$ будут числа $\pm p$, где p – простое число.

Пример 2. Кольцо $\mathbb{R}[x]$ многочленов над полем действительных чисел является целостным. Если $f(x)g(x) = 1$, то $\deg f(x) + \deg g(x) = 0$ и $\deg f(x) = \deg g(x) = 0$. Таким образом, многочлен $f(x)$ обратим (= является делителем единицы) тогда и только тогда, когда $\deg f(x) = 0$ и $f(x)$ – отличное от нуля число в $\mathbb{R}$. Поэтому ассоциированные многочлены отличаются друг от друга на ненулевой действительный множитель. Простыми элементами в $\mathbb{R}[x]$ будут неприводимые многочлены, т.е. все многочлены первой степени и многочлены второй степени с отрицательным дискриминантом.

Пример 3. В любом поле каждый ненулевой элемент обратим (= является делителем единицы). Поэтому в поле нет простых элементов и нет составных.

Отметим следующие основные свойства отношения делимости в целостном кольце K:

I) если $a = bc$, $b \neq 0$, то с однозначно определяется элементами a и b;

2) отношение делимости транзитивно, т.е. если $a \vdots b$ и $b \vdots c$, то $a \vdots c$;

3) если $a \vdots c$ и $b \vdots c$, то $(ua + vb) \vdots c$ при любых $u, v \in K$;

4) если $a \vdots b$, то $a \vdots ub$ при любом обратимом элементе $u \in K$;

5) если $a \vdots b$, то $ac \vdots b$ при любом $c \in K$;

6) если $a = bs + t$, то $a \vdots c$ и $b \vdots c$ тогда и только тогда, когда $b \vdots c$ и $t \vdots c$;

7) если каждый из элементов $a_1, a_2, \dots, a_n$ делится на c, то $\left(\sum_{i=1}^{n} u_i a_i\right) \vdots c$ при любых $u_1, u_2, \dots, u_n \in K$;

8) отношение ассоциированности на K является отношением эквивалентности.

Под **наибольшим общим делителем** двух элементов $a, b \in K$ понимается элемент $d \in K$, обозначаемый символом $НОД(a, b)$ и обладающий двумя свойствами:

а) $d | a$, $d | b$

б) если $c | a$ и $c | b$, то $c | d$.

Другими словами, наибольшим общим делителем элементов $a, b \in K$ называется такой их общий делитель d, который делится на любой общий делитель этих элементов.

Наибольший общий делитель элементов a и b определяется неоднозначно, так как вместе с d свойствми а) и б) обладает любой ассоциированный с ним элемент. Более того, если c и d – два наибольших общих делителя элементов a и b, то будем иметь $c | d$ и $d | c$, так что c и d ассоциированы. Поэтому в дальнейшем равенство $НОД(a, b) = d$ понимается с точностью до обратимого множителя.

Кроме того, не в каждом целостном кольце любые два элемента имеют наибольший общий делитель.

Пример 4. Множество $K = \{a + bi\sqrt{3} \mid a, b \in \mathbb{Z}\}$ с обычными операциями сложения и умножения является целостным кольцом. Ясно, что K – подкольцо поля $\mathbb{C}$ комплексных чисел. Рассмотрим два числа 4 и $2 + 2i\sqrt{3}$ из K. Можно проверить, что их общими делителями будут числа 2, -2, $1 + i\sqrt{3}$, $-(1 + i\sqrt{3})$ и только они. Но 2 не делится в кольце K на $1 + i\sqrt{3}$, и $1 + i\sqrt{3}$ не делится на 2. Поэтому в кольце K числа 4 и $2 + 2i\sqrt{3}$ не имеют наибольшего общего делителя.

Нетрудно доказать следующие свойства:

9) $HOD(a,b)=a$ тогда и только тогда, когда $a \mid b$;

10) если $a \neq 0$, то $HOD(a,0)=a$,

11. $HOD(HOD(a,b),c)=HOD(a,HOD(b,c))$;

12) если $HOD(a,b)$ существует, то при любом $c \in K$ существует $HOD(ac,bc)$, причем $HOD(ac,bc)=c\,HOD(a,b)$.

По аналогии с $HOD(a,b)$ вводится понятие наименьшего общего кратного $m=HOK(a,b)$ элементов $a,b \in K$, также определенного с точностью до ассоциированности двумя свойствами:

а) $a \mid m$, $b \mid m$;

б) если $a \mid c$, $b \mid c$, то $m \mid c$.

Следующая теорема устанавливает связь между наибольшим общим делителем и наименьшим общим кратным элементов a , b целостного кольца K .

Теорема 3.1. Если для элементов a и b целостного кольца K существуют $HOD(a,b)$ и $HOK(a,b)$, то

$$HOD(a,b)\,HOK(a,b)=ab$$

Теорема 3.1 не дает способа вычисления наибольшего общего делителя элементов целостного кольца. Однако следующее определение позволяет из всех целостных колец выделить кольца с весьма эффективным способом нахождения наибольшего общего делителя элементов.

Целостное кольцо E называется евклидовым, если существует отображение $\delta : E^{\#} \to N \cup \{0\}$, удовлетворяющее условиям:

(E1) $\delta(ab) \geqslant \delta(a)$ для всех $a,b \in E^{\#}$;

(E2) для любых $a,b \in E$, где $b \neq 0$, найдутся элементы q , $r \in E$ такие, что $a=bq+r$, причем $\delta(r) < \delta(b)$ или $r=0$.

Отображение δ называется евклидовой нормой.

Кольцо целых чисел с отображением δ , заданным формулой $\delta(x)=|x|$ для любого $x \in \mathbb{Z}$, евклидово. Кольцо многочленов $P[x]$ над полем P с $\delta(f(x))=\deg f(x)$, евклидово.

Евклидова норма определяется аксиомами E1 и E2 неоднозначно. Например, если δ – евклидова норма в некоторм евклидовом кольце, то при любом фиксированном $n \in N$ отображение $n\delta$ также является евклидовой нормой в том же кольце. Но это нам не мешает, так как, говоря о конкретном евклидовом кольце, мы будем иметь дело с одной, каким-то образом выбранной, евклидовой нормой.

Представление элемента a через элемент $b \neq 0$ в виде $a=bq+r$ называется делением с остатком a на b ; элемент q называется неполным частным и элемент

r – остатком, независимо от того, равен r нулю или не равен.

В евклидовых кольцах существует способ нахождения $HOD(a,b)$, называемый алгоритмом последовательного деления, или алгоритмом Евклида и заключающийся в следующем. Разделим a на b с остатком: $a=bs_1+r_1$, $\delta(r_1)<\delta(b)$. Если $r_1 \neq 0$, то разделим b на r_1 с остатком: $b=r_1 s_2+r_2$, $\delta(r_2)<\delta(r_1)$. Если $r_2 \neq 0$, то разделим r_1 на r_2 с остатком: $r_1=r_2 s_3+r_3$, $\delta(r_3)<\delta(r_2)$, и т.д.

Описанный процесс последовательного деления с остатком обрывается через конечное число шагов, т.е. $r_{n-1}=r_n s_{n+1}$ при некотором n

Система равенств

$$\begin{aligned}
&a=bs_1+r_1, \quad \delta(r_1)<\delta(b);\\
&b=r_1 s_2+r_2, \quad \delta(r_2)<\delta(r_1);\\
&r_1=r_2 s_3+r_3, \quad \delta(r_3)<\delta(r_2);\\
&\text{— — — — — — — — —}\\
&r_{n-2}=r_{n-1}s_n+r_n, \quad \delta(r_n)<\delta(r_{n-1})\\
&r_{n-1}=r_n s_{n+1}
\end{aligned}$$

называется последовательностью Евклида для элементов $a,b \in K$, $(b \neq 0)$.

Теорема 3.2. В евклидовом кольце K наибольший общий делитель любых двух элементов всегда существует. Если a делит b , то $HOD(a,b)=a$. Если a не делит b , $a \neq 0$, то $HOD(a,b)$ совпадает с последним отличным от нуля остатком в последовательности Евклида для элементов a и b .

Следствие. В евклидовом кольце K для любых элементов a , b существует наименьшее общее кратное.

Теорема 3.3. Пусть K – евклидово кольцо, $a,b \in K$, $b \neq 0$, $d=HOD(a,b)$. Тогда существует элементы $u,v \in K$, для которых $d=ua+vb$.

Элементы a , b евклидова кольца K называются взаимно простыми, если их наибольший общий делитель равен единице.

Из теоремы 3.3 следует, что элементы a и b евклидова кольца K взаимно просты тогда и только тогда, когда существуют такие $u,v \in K$, что $ua+vb=1$.

Разложением элемента a целостного кольца K на простые множители называется представление a в виде

$$\alpha = u p_1 p_2 \cdots p_s,$$

где $p_1, p_2, \dots, p_s$ – простые элементы кольца K.

Целостное кольцо K называется **факториальным**, если каждый ненулевой необратимый элемент $\alpha \in K$ имеет однозначное с точностью до порядка сомножителей и обратимых множителей разложение на простые множители, т.е. α можно представить в виде $\alpha = u p_1 p_2 \cdots p_s$, где u – обратимый элемент кольца K, а $p_1, p_2, \dots, p_s$ – простые элементы (не обязательно попарно различные), и если есть еще одно такое разложение $\alpha = v q_1 q_2 \cdots q_t$, то $s = t$, и при соответствующей нумерации простых множителей $q_1 = u_1 p_1$, $q_2 = u_2 p_2$ ... $q_s = u_s p_s$, где $u_1, u_2, \dots, u_s$ – обратимые элементы.

Основная теорема арифметики утверждает, что кольцо $\mathbb{Z}$ факториально. Факториальным является и кольцо $P[x]$ многочленов переменной x над полем P. В кольце $K = \{a + bi\sqrt{3} \mid a, b \in \mathbb{Z}\}$ имеются два существенно различных разложения числа 4 на простые множители: $4 = 2 \cdot 2$, $4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$. Последний пример показывает, что существуют целостные кольца, которые не являются факториальными.

Теорема 3.4. Пусть K – факториальное кольцо. Пусть $\mathcal{P}$ – такое множество простых элементов из K, что всякий простой элемент из K ассоциирован с одним и только одним элементом из $\mathcal{P}$. Тогда каждый ненулевой необратимый элемент $\alpha \in K$ можно представить в виде $\alpha = u p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, где u – обратимый элемент, $p_1, p_2, \dots, p_s$ – попарно неравные элементы из $\mathcal{P}$, $\alpha_i > 0$, $i = 1, 2, \dots, s$.

Такое разложение по аналогии с кольцом $\mathbb{Z}$ называется **каноническим**.

Теорема 3.4 позволяет получить легко запоминаемый признак делимости элементов в факториальных кольцах. Рассматривая канонические разложения двух элементов a, b – факториального кольца K, удобно считать, что в них входят одинаковые элементы из $\mathcal{P}$, но некоторые, возможно, с нулевыми показателями, т.е.

$$a = u p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}, \quad b = v p_1^{l_1} p_2^{l_2} \dots p_r^{l_r}, \quad (*)$$

u, v – обратимые элементы K, $k_i \geqslant 0$, $l_i \geqslant 0$, $i = 1, 2, \dots, r$.

Теорема 3.5 (Признак делимости). Пусть a, b – элементы факториального кольца K, записанные в виде $(*)$. Тогда и только тогда $a \mid b$, когда $k_i \leqslant l_i$, $i = 1, 2, \dots, r$.

Следствие. Пусть a, b – элементы факториального кольца

K, записанные в виде $(*)$. Справедливы утверждения:

1) $НОД(a, b) = p_1^{s_1} p_2^{s_2} \dots p_r^{s_r}$, где $s_i = \min\{k_i, l_i\}$, $i = 1, 2, \dots, r$

2) $НОК(a, b) = p_1^{t_1} p_2^{t_2} \dots p_r^{t_r}$, где $t_i = \max\{k_i, l_i\}$, $i = 1, 2, \dots, r$

Таким образом, при отыскании $НОД(a, b)$ в качестве s_i нужно брать наименьший из двух показателей k_i, l_i, а при отыскании $НОК(a, b)$ в качестве t_i – наибольший. В частности, элементы $a, b \in K$ взаимно просты в точности тогда, когда простые множители, входящие в разложение одного элемента, не входят в разложение другого.

Теорема 3.6 Всякое евклидово кольцо K факториально.

Существуют факториальные кольца, которые не являются евклидовыми. К таковым относится, например, кольцо $P[x, y]$ многочленов двух переменных x и y над полем P.

Примеры решения и оформления задач

Пример 1. Доказать, что в кольце $\mathbb{Z}[\sqrt{2}] = \{x + \sqrt{2}y \mid x, y \in \mathbb{Z}\}$ элемент $a = 6 - \sqrt{2}$ делится на $b = 5 + 2\sqrt{2}$.

Решение. По определению, элемент $a = 6 - \sqrt{2}$ делится на $b = 5 + 2\sqrt{2}$, если существует элемент $c = x + \sqrt{2}y$ кольца $\mathbb{Z}[\sqrt{2}]$ такой, что $a = bc$. Положим

$$6 - \sqrt{2} = (5 + 2\sqrt{2})(x + \sqrt{2}y).$$

Тогда $6 - \sqrt{2} = 5x + 4y + (2x + 5y)\sqrt{2}$

Отсюда получаем

$$\begin{cases} 5x + 4y = 6 \\ 2x + 5y = -1 \end{cases}$$

Решая эту систему, находим $x = 2$, $y = -1$. Значит, $c = 2 - \sqrt{2}$. Поэтому элемент a делится на элемент b.

Пример 2. Применяя алгоритм Евклида, найти наибольший общий делитель чисел 2346, 646. Вычислить наименьшее общее кратное чисел 2346, 646.

Решение. В данном случае имеем:

$$
\begin{array}{l}
-\begin{array}{r|l} 2346 & 646 \\ \hline 1938 & 3 \end{array} \\
\quad -\begin{array}{r|l} 646 & 408 \\ \hline 408 & 1 \end{array} \\
\quad\quad -\begin{array}{r|l} 408 & 238 \\ \hline 238 & 1 \end{array} \\
\quad\quad\quad -\begin{array}{r|l} 238 & 170 \\ \hline 170 & 1 \end{array} \\
\quad\quad\quad\quad -\begin{array}{r|l} 170 & 68 \\ \hline 136 & 2 \end{array} \\
\quad\quad\quad\quad\quad -\begin{array}{r|l} 68 & 34 \\ \hline 68 & 2 \end{array} \\
\quad\quad\quad\quad\quad\quad 0
\end{array}
$$

Последний отличный от нули остаток равен 34, следовательно,

$$HOD(2346, 646) = 34$$

Наименьшее общее кратное находим по формуле

$$HOK(a, b) = \frac{mn}{HOD(m, n)}.$$

В нашем случае имеем $HOK(2346, 646) = \frac{2346 \cdot 646}{34} = 44574$

П р и м е р 3. Доказать, что кольцо $\mathbb{Z}[i] = \{x+iy \mid x, y \in \mathbb{Z}\}$ ц е л ы х г а у с с о в ы х ч и с е л является евклидовым. Найти алгоритм деления в кольце $\mathbb{Z}[i]$.

Р е ш е н и е. Покажем, что отображение $\delta : \mathbb{Z}[i]^{\#} \to \mathbb{N} \cup \{0\}$, определяемое равенством $\delta(m+in) = m^2 + n^2$,

является евклидовой нормой на $\mathbb{Z}[i]$.

Пусть $z_1, z_2 \in \mathbb{Z}[i]$, $z_2 \neq 0$. Тогда

$$\delta(z_1 z_2) = \delta((x_1+iy_1)(x_2+iy_2)) = \delta((x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1)) =$$

$$= (x_1x_2 - y_1y_2)^2 + (x_1y_1 + x_2y_1)^2 = (x_1^2 + y_1)(x_2^2 + y_2^2) = \delta(z_1)\delta(z_2) \geqslant \delta(z_1)$$

Таким образом, свойство (E1) из определения евклидова кольца выполняется.

Убедимся в справедливости свойства (E2). Возьмем произвольно два числа $z_1 = a + ib$, $z_2 = c + id \neq 0$ из $\mathbb{Z}[i]$. В поле частных

преобразуем отношение взятых чисел следующим образом:

$$\frac{z_1}{z_2} = \frac{a+ib}{c+id} = \frac{(a+ib)(c-id)}{c^2+d^2} = \frac{ac+bd}{\delta(z_2)} + \frac{bc-ad}{\delta(z_2)} i = \alpha + i\beta,$$

где $\alpha, \beta \in \mathbb{Q}$. Возьмем ближайшие к α, β целые числа k, l такие, что $\alpha = k + \nu$, $\beta = l + \mu$, $|\nu| \leq \frac{1}{2}$, $|\mu| \leq \frac{1}{2}$. Тогда

$$z_1 = z_2[(k+\nu) + (l+\mu)i] = z_2(k+li) + z_2(\nu + \mu i) = z_2 q + r,$$

где $q = k + li$, $r = z_2(\nu + \mu i)$.

По построению, $q \in \mathbb{Z}[i]$. Так как $r = z_1 - z_2 q$, то и $r \in \mathbb{Z}[i]$.

При этом имеем:

$$\delta(r) = \delta(z_2(\nu + \mu i)) = \delta(z_2)\delta(\nu + \mu i) = \delta(z_2)(\nu^2 + \mu^2) \leq$$

$$\leq \delta(z_2)\left(\frac{1}{4} + \frac{1}{4}\right) = \frac{1}{2}\delta(z_2) < \delta(z_2), \text{ т.е. } \delta(r) < \delta(z_2)$$

Таким образом, свойство $(E2)$ из определения евклидова кольца выполняется. Значит, δ -евклидова норма на $\mathbb{Z}[i]$, а кольцо $\mathbb{Z}[i]$ - евклидово. Попутно найдем алгоритм деления чисел в кольце $\mathbb{Z}[i]$.

П р и м е р 4. В кольце $\mathbb{Z}[i]$ разделить с остатком $122 + 19i$ на $5 - 11i$

Р е ш е н и е. Вычисления начинаем в поле частных кольца $\mathbb{Z}[i]$:

$$\frac{122 + 19i}{5 - 11i} = \frac{(122 + 19i)(5 + 11i)}{146} = \frac{401}{146} + \frac{1437}{146} i$$

Выделяя из рациональных дробей ближайшие целые, получаем равенство

$$\frac{122 + 19i}{5 - 11i} = 3 + 10i - \left(\frac{37}{146} + \frac{23}{146} i\right)$$

После умножения этого равенства на $5 - 11i$ получаем окончательный результат:

$$122 + 19i = (5 - 11i)(3 + 10i) + (3 + 2i).$$

П р и м е р 5. Применяя алгоритм Евклида, найти наибольший общий делитель элементов $33 + 31i$ и $21 + 4i$ кольца $\mathbb{Z}[i]$. Найти линейное представление HOD этих чисел. Вычислить их наименьшее общее кратное.

Р е ш е н и е. Выполняя повторные деления с остатком так, как выполнено деление с остатком в примере 4, получим равенства:

$$33 + 31i = (21 + 4i)(2 + i) - 5 + 2i,$$

$$21 + 4i = (-5 + 2i)(-3 - 2i) + 2,$$

$$-5 + 2i = 2(-2 + i) - 1,$$

$$2 = (-1)(-2).$$

В данной последовательности Евклида последний отличный от нуля остаток равен -I. Значит,

$$HOD(33+31i,\ 21+4i)=-1$$

Так как все обратимые элементы кольца $\mathbb{Z}[i]$ исчерпываются числами: $-1, 1, i, -i$, то мы можем считать, что $HOD(33+31i,\ 21+4i)$ равен либо -I, либо I, либо $-i$, либо i.

Для нахождения линейного представления найденного HOD напишем составляющую алгоритм Евклида систему равенств, кроме последнего, в обратном порядке; кроме того, заданные числа $33+31i$ и $21+4i$ обозначим через a и b соответственно найденные же остатки через r_1, r_2, r_3. Таким образом, получим систему равенств:

$$r_3=(2-i)r_2+r_1,$$
$$r_2=(3+2i)r_1+b,$$
$$r_1=(-2-i)b+a$$

Исключая из выражения для r_3 сначала r_2, затем r_1, найдем искомое линейное представление для HOD:

$$-1=(9+i)a-(15+12i)b$$

Применяя теорему 3.I, находим с точностью до ассоциированности $HCK(a,b)$:

$$HOK(33+31i,\ 21+4i)=\frac{(33+31i)(21+4i)}{(-1)}=-569-793i$$

П р и м е р 6. Найти каноническое разложение целых чисел 7038 и 2584. Вычислить HOD и HOK этих чисел.

Р е ш е н и е. Разложим данные числа на простые множители:

$$7038=2\cdot 3\cdot 3\cdot 17\cdot 23,$$
$$2584=2\cdot 2\cdot 2\cdot 17\cdot 19$$

Каноническими разложениями их будут разложения:

$$7038=2\cdot 3^2\cdot 17\cdot 23,\quad 2584=2^3\cdot 17\cdot 19$$

На основании следствия из теоремы 3.5 имеем:

$$HOD(7038,2584)=2\cdot 17=34,$$
$$HOK(7038,2584)=2^3\cdot 3^2\cdot 17\cdot 19\cdot 23=534888$$

В о п р о с ы   д л я   с а м о к о н т р о л я

1. Найдите все обратимые элементы кольца $P[x]$ многочленов над полем P.
2. Докажите, что два ненулевых многочлена $f(x)$ и $g(x)\in P[x]$ ассоциированны тогда и только тогда, когда $f(x)=\lambda g(x)$, $\lambda\in P$
3. Сформулируйте и докажите основные свойства отношения делимости в целостном кольце.
4. Как определяется наибольший общий делитель элементов в кольцах $\mathbb{Z}$ и $P[x]$?
5. Сколько наибольших общих делителей имеется для элементов a и b целостного кольца?
6. Докажите, что элементы d_1 и d_2 являются наибольшим общим делителем элементов a и b целостного кольца K тогда и только тогда, когда d_1 и d_2 ассоциированы.
7. Сформулируйте и докажите основные свойства наибольшего общего делителя элементов целостного кольца.
8. Как связаны между собой HOD и HOK элементов целостного кольца?
9. Всегда ли существует HOD элементов в целостном кольце?
10. Приведите примеры евклидовых колец.
11. Докажите, что для любого $n\in\mathbb{N}$ и любой евклидовой нормы δ евклидова кольца E отображение $n\delta$ также является евклидовой нормой.
12. Изложите сущность алгоритма Евклида в кольцах $\mathbb{Z}$ и $\mathbb{R}[x]$.
13. Как найти линейное представление HOD элементов a и b евклидова кольца K?
14. Какие элементы являются простыми в кольце $\mathbb{C}[x]$?
15. Что означает факториальность колец $\mathbb{Z}$ и $\mathbb{C}[x]$?

З а д а н и я   к   л а б о р а т о р н о й   р а б о т е

1. Делится ли элемент a кольца K на элемент b?

а) $K=\mathbb{Z}_{23}$, $a=\overline{4}$, $b=\overline{14}$;

б) $K=\mathbb{Z}[\sqrt{3}]$, $a=-8-6\sqrt{3}$, $b=4+2\sqrt{3}$;

в) $K=\left\{\begin{pmatrix} x & -y \\ y & x\end{pmatrix} \middle| x,y\in\mathbb{Z}\right\}$, $a=\begin{pmatrix} 45 & 45 \\ -45 & 45\end{pmatrix}$, $b=\begin{pmatrix} 3 & -6 \\ 6 & 3\end{pmatrix}$;

г) $K=\{x+\sqrt{5}y \mid x,y\in\mathbb{Z}\}$, $a=4+\sqrt{5}6$, $b=-2+\sqrt{5}8$;

д) $K=\mathbb{Z}_2[x]$, $a=x^5+x^4+x^3+1$, $b=x^3+x+1$;

е) $K=\mathbb{Z}_3[x]$, $a=x^5-x^2+x-1$, $b=x^2+x+1$;

ж) $K=\{m5^n \mid n\in\mathbb{Z}, m\in\mathbb{Z}, HOD(m,5)=1\}\cup\{0\}$,
$a=925$, $b=\frac{111}{125}$;

з) $K=\mathbb{Q}[x]$, $a=x^4-2x^2+x+2$, $b=x^2+x-1$;

и) $K=\left\{\frac{x+yi\sqrt{3}}{2} \mid x,y\in\mathbb{Z},\ x,y\right.$ одинаковой четности$\left.\right\}$,
$a=\frac{2+4i\sqrt{3}}{2}$, $b=\frac{-1-i\sqrt{3}}{2}$;

к) $K=\mathbb{Z}[x]$, $a=x^4+x^3+x^2+2x-2$, $b=x^2+2$

2. Найти все обратимые элементы кольца K :

а) $K=\mathbb{Z}[\sqrt{3}]$;

б) $K=\mathbb{Z}_3[x]$;

в) $K=\mathbb{Z}[\sqrt{5}]$;

г) $K=\{m5^n \mid n\in\mathbb{Z}, HOD(m,5)=1\}\cup\{0\}$

д) $K=\left\{\frac{x+yi\sqrt{3}}{2} \mid x,y\in\mathbb{Z},\ x,y\right.$ одинаковой четности$\left.\right\}$

3. Применяя алгоритм Евклида, найти HOD элементов m , n кольца $\mathbb{Z}$. Вычислите $HOK(m,n)$:

а) $m=6188$, $n=4709$;
б) $m=3640$, $n=7650$;
в) $m=1403$, $n=1058$;
г) $m=12606$, $n=6494$;
д) $m=1232$, $n=1672$.

4. Применяя алгоритм Евклида, найдите наибольший общий делитель многочленов $m(x)$, $n(x)$ кольца $\mathbb{R}[x]$. Вычислите наименьшее общее кратное многочленов $m(x)$, $n(x)$

а) $m(x)=x^4+4x^3-7x+2$,
$n(x)=x^3+x^2-4$;

б) $m(x)=x^6-x^4+3x^3-2x+2$,
$n(x)=x^3+2$;

в) $m(x)=x^5-x^4+x^3-x^2+2x-2$,
$n(x)=x^5-1$;

г) $m(x)=3x^5+6x^4+3x^3-x^2-2x-1$,
$n(x)=x^4-2x^2+1$;

д) $m(x)=2x^6-3x^4-x^2-4x-2$,
$n(x)=-2x^6+3x^4-2x^3-3x^2-4x-4$.

5. В кольце $\mathbb{Z}[i]$ разделите с остатком a на b :

а) $a=40+3i$, $b=3-i$;
б) $a=15+16i$, $b=7+i$;
в) $a=17+11i$, $b=8-5i$;
г) $a=23+9i$, $b=7-5i$;
д) $a=100$, $b=17+5i$.

6. Применяя алгоритм Евклида, найти наибольший общий делитель элементов a и b кольца $\mathbb{Z}[i]$. Найти линейное представление наибольшего общего делителя этих чисел. Вычислить их наименьшее общее кратное.

а) $a=20+9i$, $b=11+2i$;
б) $a=15-4i$, $b=10+7i$,
в) $a=14-3i$, $b=8+5i$;
г) $a=9+i$, $b=7-6i$;
д) $a=21+4i$, $b=5+i$.

7. Найдите HOD и HOK многочленов $f(x)$ и $g(x)\in\mathbb{R}[x]$

а) $f(x)=(x^3-8)(x^2-4x+4)$, $g(x)=(x^2-4)^3$;
б) $f(x)=(x^2+x-6)^3$, $g(x)=(x-1)(x+2)^3(x-3)$;
в) $f(x)=(x^3+2x^2-3)^2$, $g(x)=(x-1)^2(x^3-19x-30)$;
г) $f(x)=x^4-3x^2+2$, $g(x)=x^4-x^3-x+1$;
д) $f(x)=2x^4+5x^3-60x^2+25x+28$, $g(x)=x^3+3x^2-28x$.

Распределение задач по вариантам

Вариант 1: №№ 1(а,д), 2(а), 3(а), 4(а), 5(а), 6(а), 7(а).
Вариант 2: №№ 1(б,е), 2(б), 3(б), 4(б), 5(б), 6(б), 7(б).
Вариант 3: №№ 1(в,з), 2(в), 3(в), 4(в), 5(в), 6(в), 7(в).

риант 4: №№ 1(г,ж), 2(г), 3(г), 4(г), 5(г), 6(г), 7(г).
риант 5: №№ 1(и,к), 2(д), 3(д), 4(д), 5(д), 6(д), 7(д).

Лабораторная работа № 4
ИДЕАЛЫ КОЛЕЦ

В теории колец фундаментальную роль играют подкольца, выдерживающие правые или левые умножения на элементы кольца. Подкольцо I кольца K называется **левым идеалом**, если $ra \in I$ для всех $r \in K$ и $a \in I$. Подкольцо I кольца K называется **правым идеалом**, если $ar \in I$ для всех $r \in K$, $a \in I$. Если I является одновременно левым и правым идеалом, то I называется **двусторонним идеалом** или просто **идеалом** кольца K. Другими словами, подкольцо I называется **идеалом** кольца K, если $ra \in I$, $ar \in I$ для всех $r \in K$, $a \in I$. Ясно, что в коммутативном кольце понятие левого, правого и двустороннего идеалов совпадают.

В произвольном кольце K иделами являются само кольцо и нулевое подкольцо. Эти идеалы называют **тривиальными**.

Следующие подкольца являются идеалами:

1) в кольце $\mathbb{Z}$ – подкольцо $n\mathbb{Z}$ чисел, кратных n, $n \geq 1$;

2) в кольце $C[a,b]$ функций, непрерывных на отрезке $[a,b]$, – подкольцо $I = \{f \in C[a,b] \mid f(c) = 0, c \in [a,b]\}$;

3) в кольце $R = \{\begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z}\}$ – подкольцо
$$I = \{\begin{pmatrix} a & a \\ a & a \end{pmatrix} \mid a \in \mathbb{Z}\}$$

В кольце $M(n, \mathbb{R})$ множество матриц, у которых все столбцы, кроме s-го, нулевые, образует идеал, который не является двусторонним.

Теорема 4.1 (Критерий для идеалов). Непустое подмножество I кольца K является левым (правым) идеалом тогда и только тогда, когда выполняются следующие условия:

1) $a - b \in I$ для всех $a, b \in I$;

2) $ra \in I$ (соответственно $ar \in I$) для всех $r \in K$, $a \in I$.

Следствие. Непустое подмножество I кольца K является идеалом тогда и только тогда, когда выполняются следующие условия;

1) $a - b \in I$ для всех $a, b \in I$;

2) $ra \in I$, $ar \in I$ для всех $a \in I$, $r \in K$.

Сразу же отметим, что условие 2) следствия в коммутативном кольце может быть заменено более слабым условием: $ra \in I$ для всех $r \in K$, $a \in I$.

Пусть A, B – подмножества кольца K. **Суммой** подмножеств A и B называется множество
$$A + B = \{a + b \mid a \in A, b \in B\}$$

Произведением множеств A и B называется множество AB, состоящее из всех конечных сумм вида $a_1 b_1 + \dots + a_k b_k$, где $a_i \in A$, $b_i \in B$.

Теорема 4.2. Сумма двух левых, правых или двусторонних идеалов кольца K является соответственно левым, правым или двусторонним идеалом кольца K.

Теорема 4.3. 1) Если I – левый идеал, T – непустое множество элементов кольца K, то IT – левый идеал K.

2) Если I – правый идеал кольца K, то TI – правый идеал K.

3) Если I, J – идеалы кольца K, то IJ – идеал K.

Теорема 4.4. Пересечение любого множества левых, правых или двусторонних идеалов кольца K является соответственно левым правым или двусторонним идеалом кольца K.

Теорема 4.4 позволяет ввести следующее определение. Пусть M – некоторое множество элементов кольца K. Пересечение всех левых идеалов кольца K, содержащих M, обозначается через $(M\rangle$ и называется **левым идеалом, порожденным множеством** M. Пересечение всех правых идеалов, содержащих M обозначается через $\langle M)$ и называется **правым идеалом, порожденным множеством** M. Пересечение всех идеалов, содержащих M, обозначается через (M) и называется **идеалом, порожденным множеством** M

Если множество M состоит из одного элемента a, то идеалы $(a\rangle$, $\langle a)$, (a) называются **главными**. Элемент a называется в этом случае **образующим элементом** главного идеала.

В коммутаивном кольце $(M) = \langle M) = (M\rangle$ и $(a) = (a\rangle = \langle a)$.

Структура главных идеалов проясняется следующими теоремами

Теорема 4.5. Пусть a – произвольный элемент кольца K. Тогда $(a\rangle = Ka + \mathbb{Z}a$, $\langle a) = aK + a\mathbb{Z}$,
$$(a) = KaK + \mathbb{Z}a + Ka + aK$$

Т е о р е м а 4.6 1) Если K – кольцо с единицей, то для любого $a \in K$ имеет место $(a\rangle = Ka$, $\langle a) = aK$, $(a) = KaK$.

2) Если K – коммутативное кольцо, то $(a) = (a\rangle = \langle a) = aK + a\mathbb{Z}$

3) Если K – коммутативное кольцо с единицей, то $(a) = aK$

Целостное кольцо с единицей, в котором все идеалы главные, называется **к о л ь ц о м г л а в н ы х и д е а л о в**.

Т е о р е м а 4.7. Кольцо целых чисел является кольцом главных идеалов. Если I – ненулевой идеал кольца $\mathbb{Z}$, то $I = m\mathbb{Z}$, где m – наименьшее натуральное число из I.

Т е о р е м а 4.8. Кольцо $P[x]$ многочленов переменной x над полем P является кольцом главных идеалов. Если I – ненулевой идеал кольца $P[x]$, то $I = (f(x))$, где $f(x)$ – ненулевой многочлен наименьшей степени, содержащийся в I.

Обобщением этих теорем служит следующая

Т е о р е м а 4.9. Всякое евклидово кольцо является кольцом главных идеалов. Если I – ненулевой идеал евклидова кольца K, то

1) существует такой ненулевой элемент $m \in I$, что $\delta(m) \le \delta(c)$ для любого ненулевого $c \in I$;

2) $I = (m) = mK$

Т е о р е м а 4.10. Всякое кольцо главных идеалов факториально.

Подводя итог, получаем

$$\left\{\begin{matrix}\text{евклидовы}\\ \text{кольца}\end{matrix}\right\} \subset \left\{\begin{matrix}\text{кольца}\\ \text{главных идеалов}\end{matrix}\right\} \subset \left\{\begin{matrix}\text{факториальные}\\ \text{кольца}\end{matrix}\right\}$$

П р и м е р ы р е ш е н и я и о ф о р м л е н и я з а д а ч

П р и м е р 1. Будет ли множество I чисел $a + bi$ с четными a и b подкольцом и идеалом в кольце $\mathbb{Z}[i]$?

Р е ш е н и е . Применим критерий для подколец. Пусть $z_1 = a_1 + b_1 i$, $z_2 = a_2 + b_2 i$ – произвольные элементы множества I. Тогда

$$z_1 - z_2 = (a_1 + b_1 i) - (a_2 + b_2 i) = (a_1 - a_2) + (b_1 - b_2)i$$

Так как разность четных чисел есть четное число, то $z_1 - z_2 \in I$.

Аналогично, $z_1 z_2 = (a_1 + b_1 i)(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i \in I$, так как $a_1 a_2 - b_1 b_2$ и $a_1 b_2 + a_2 b_1$ – четные числа. Итак, I – подкольцо кольца $\mathbb{Z}[i]$.

Пусть $z = a + bi$ – произвольный элемент кольца $\mathbb{Z}[i]$. Тогда $z z_1 = (a + bi)(a_1 + b_1 i) = (a a_1 - b b_1) + (a b_1 + b a_1)i \in I$, так как $a a_1 - b b_1$ и $a b_1 + a_1 b$ – четные числа. Ввиду критерия для идеалов в коммутативных кольцах получаем, что I – идеал

кольца $\mathbb{Z}[i]$.

П р и м е р 2. Образуют ли кольцо и идеал все необратимые элементы кольца $\mathbb{Z}_6$.

Р е ш е н и е . Кольцо $\mathbb{Z}_6$ состоит из элементов $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$. Элемент $\overline{a}$ кольца $\mathbb{Z}_6$ необратим тогда и только тогда, когда числа a и 6 не взаимно просты. Значит, необратимыми в кольце $\mathbb{Z}_6$ будут элементы $\overline{0}, \overline{2}, \overline{3}, \overline{4}$. Обозначим множество всех необратимых элементов кольца $\mathbb{Z}_6$ через I.

Так как $\overline{3} - \overline{2} = \overline{1} \notin I$, то I не является подкольцом кольца $\mathbb{Z}_6$. Но тогда I не может являтся и идеалом кольца $\mathbb{Z}_6$.

П р и м е р 3. Доказать, что множество $I = \{ f(x) = (x^2 + x + 1)m(x) + (x - 1)n(x) \mid m(x), n(x) \in \mathbb{R}[x] \}$ является идеалом кольца $\mathbb{R}[x]$. Найти образующий элемент идеала I.

Р е ш е н и е . Применим критерий для идеалов. Пусть $f_1(x)$, $f_2(x) \in I$. Это означает, что

$$f_1(x) = (x^2 + x + 1)m_1(x) + (x - 1)n_1(x),$$
$$f_2(x) = (x^2 + x + 1)m_2(x) + (x - 1)n_2(x),$$

где $m_1(x)$, $m_2(x)$, $n_1(x)$, $n_2(x) \in \mathbb{R}[x]$. Тогда

$$f_1(x) - f_2(x) = (x^2 + x + 1)(m_1(x) - m_2(x)) + (x - 1)(n_1(x) - n_2(x)) \in I.$$

Для любых $f(x) \in I$ и $g(x) \in \mathbb{R}[x]$ имеем

$$g(x)f(x) = (x^2 + x + 1)g(x)m(x) + (x - 1)g(x)n(x) \in I.$$

Так как кольцо $\mathbb{R}[x]$ коммутативно, то $f(x)g(x) \in I$. Значит, I – идеал кольца $\mathbb{R}[x]$.

Пусть $\tau(x)$ – наибольший общий делитель многочленов $x^2 + x + 1$ и $x - 1$. Покажем, что $I = \tau(x)\mathbb{R}[x]$. Пусть $f(x) \in I$. Так как $x^2 + x + 1 = \tau(x) f_1(x)$, $x - 1 = \tau(x) f_2(x)$, то $f(x) = (x^2 + x + 1)m(x) + (x - 1)n(x) = \tau(x)(f_1(x)m(x) + f_2(x)n(x)) \in \tau(x)\mathbb{R}[x]$. Значит, $I \subseteq \tau(x)\mathbb{R}[x]$. Пусть теперь $g(x) \in \tau(x)\mathbb{R}[x]$. Тогда $g(x) = \tau(x)S(x)$. По теореме о выражении наибольшего общего делителя через исходные многочлены имеем $\tau(x) = (x^2 + x + 1)U(x) + (x - 1)V(x)$. Отсюда $g(x) = (x^2 + x + 1)U(x)S(x) + (x - 1)V(x)S(x) \in I$ т.е. $\tau(x)\mathbb{R}[x] \subseteq I$

Итак, $I = \tau(x)\mathbb{R}[x]$. Ввиду теоремы 4.6 $I = (\tau(x))$, т.е. $\tau(x)$ – образующий элемент идела I.

Найдем $\tau(x)$ с помощью алгоритма Евклида

$$
\begin{array}{l|l}
x^2+x+1 & x-1 \\
\underline{-\;x^2-x} & \overline{x+2} \\
\quad 2x+1 & \\
\quad \underline{-\;2x-2} & \\
\end{array}
\qquad x^2+x+1=(x-1)(x+2)+3
$$

$$
\begin{array}{l|l}
x-1 & 3 \\
\underline{-\;x} & \overline{\frac{1}{3}x-\frac{1}{3}} \\
\quad -1 & \\
\quad \underline{-\;-1} & \\
\quad\; 0 & \\
\end{array}
\qquad x-1=3\left(\frac{1}{3}x-\frac{1}{3}\right)
$$

Значит, $r(x)=1$.

Поэтому $I=(1)=\mathbb{R}[x]$.

П р и м е р 4. В кольце $\mathbb{R}[x]$ найти идеалы $(x^2-1)+(x^3-1)$, $(x^2-1)\cap(x^3-1)$, $(x^2-1)(x^3-1)$. Указать их образующие.

Р е ш е н и е. Обозначим $I=(x^2-1)$, $J=(x^3-1)$. Ввиду теоремы 2.6 $I=(x^2-1)\mathbb{R}[x]=\{(x^2-1)f(x)\mid f(x)\in\mathbb{R}[x]\}$

$$J=(x^3-1)\mathbb{R}[x]=\{(x^3-1)g(x)\mid g(x)\in\mathbb{R}[x]\}.$$

По определению суммы множеств I и J имеем:

$$I+J=\{(x^2-1)f(x)+(x^3-1)g(x)\mid f(x),g(x)\in\mathbb{R}[x]\}.$$

Как и в примере 3 показывается, что $I+J=(r(x))$, где $r(x)$ – наибольший общий делитель x^2-1 и x^3-1. Так как

$$НОД(x^2-1,x^3-1)=(x-1),$$

то $I+J=(x-1)$, т.е. $x-1$ – образующий элемент $I+J$.

Идеал $I\cap J$ содержит те и только те многочлены $f(x)$, которые делятся на x^2-1 и x^3-1 одновременно. Но тогда

$$f(x)=НОК((x^2-1),(x^3-1))g(x),\ g(x)\in\mathbb{R}[x],$$

т.е.

$$I\cap J=(НОК(x^2-1,x^3-1))$$

Применим формулу $НОК(m(x),n(x))=\dfrac{m(x)\,n(x)}{НОД(m(x),n(x))}$.

В нашем случае $НОК(x^2-1,x^3-1)=\frac{(x^2-1)(x^3-1)}{x-1}=x^4+x^2-x-1$.

Значит, $I\cap J=(x^4+x^2-x-1)$, т.е. x^4+x^2-x-1 – образующий элемент идеала $I\cap J$.

По определению произведения множеств I и J множество IJ состоит из всевозможных многочленов $f(x)$ вида

$$f(x)=f_1(x)g_1(x)+\dots+f_n(x)g_n(x),$$

где $f_i(x)\in I$, $g_i(x)\in J$. Но тогда

$f(x)=(x^2-1)(x^3-1)m(x)$, где $m(x)\in\mathbb{R}[x]$. Поэтому $IJ=(x^2-1)(x^3-1)\mathbb{R}[x]=$
$=(x^5-x^3-x^2+1)\mathbb{R}[x]=(x^5-x^3-x^2+1)$,
т.е. $x^5-x^3-x^2+1$ – образующий элемент идеала IJ.

П р и м е р 5. Найти все идеалы кольца $\mathbb{Z}_{18}$.

Р е ш е н и е. Кольцо $\mathbb{Z}_{18}$ относительно операции сложения является циклической группой, порожденной классом вычетов $\bar{1}=\{1+18t\mid t\in\mathbb{Z}\}$, и, сладовательно, все ее подгруппы циклические. Таких подгрупп будет шесть:

$$I_1=\langle 0\rangle=\{\bar{0}\}$$
$$I_2=\langle\bar{2}\rangle=\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10},\overline{12},\overline{14},\overline{16}\}$$
$$I_3=\langle\bar{3}\rangle=\{\bar{0},\bar{3},\bar{6},\bar{9},\overline{12},\overline{15}\}$$
$$I_4=\langle\bar{6}\rangle=\{\bar{0},\bar{6},\overline{12}\}$$
$$I_5=\langle\bar{9}\rangle=\{\bar{0},\bar{9}\}$$
$$I_6=\langle\bar{1}\rangle=\mathbb{Z}_{18}$$

В любом кольце идеал обязательно является подгруппой аддитивной группы кольца. Поэтому идеалы кольца $\mathbb{Z}_{18}$ следует искать среди перечисленных подгрупп. Проверка показывает, что все эти подгруппы и являются идеалами кольца $\mathbb{Z}_{18}$.

В о п р о с ы д л я с а м о к о н т р о л я

1. Приведите примеры идеалов.
2. Приведите пример левого идеала, который не является правым.
3. Сформулируйте критерий для иделов.
4. Какие идеалы содержит тело?
5. Как определяются в кольце сумма и произведение двух подмножеств?
6. Всегда ли произведение двух левых идеалов является левым идеалом?
7. Будет ли идеалом произведение левого и правого идеалов?
8. Будет ли идеалом произведение правого и левого идеалов?
9. Пусть a – некоторый элемент кольца K. Что можно сказать о множествах Ka и aK?
10. Пусть a, b – элементы коммутативного кольца K. Что из себя представляют элементы идеала $(\{a,b\})$?
11. Опишите элементы идеала (5) кольца $\mathbb{Z}$.
12. Опишите элементы идеала (x^2-1) кольца $\mathbb{R}[x]$.
13. Каковы идеалы поля?

Задания к лабораторной работе

I. Будет ли множество I подкольцом или идеалом кольца K ?

а) $I = n\mathbb{Z}$, $n>1$, $K=\mathbb{Z}[x]$;

б) $I=\mathbb{Z}$, $K=\mathbb{Z}[x]$;

в) $I=n\mathbb{Z}[x]$, $n>1$, $K=\mathbb{Z}[x]$;

г) $I=\mathbb{N}$, $K=\mathbb{Z}$;

д) $I=\mathbb{Z}$, $K=\mathbb{Z}[i]$;

е) $I=\{a+bi \mid a,b\in\mathbb{Z},\ a=b\}$, $K=\mathbb{Z}[i]$;

ж) $I=\{x(1+i) \mid x\in\mathbb{Z}[i]\}$, $K=\mathbb{Z}[i]$;

з) I - множество многочленов из $\mathbb{Z}[x]$, не содержащих членов с x^k для всех $k<n$, $n>1$, $K=\mathbb{Z}[x]$;

и) I - множество многочленов из $\mathbb{Z}[x]$ с четными свободными членами, $K=\mathbb{Z}[x]$;

к) $I=\mathbb{Z}[\sqrt{3}]=\{m+n\sqrt{3} \mid m,n\in\mathbb{Z}\}$, $K=\mathbb{R}$

2. Образуют ли подкольцо или идеал все необратимые элементы кольца $\mathbb{Z}_n$:

а) $n=8$; б) $n=10$; в) $n=12$; г) $n=14$;

д) $n=15$; е) $n=24$; ж) $n=18$; з) $n=16$;

и) $n=9$; к) $n=25$;

3. Докажите, что множество I является идеалом кольца $\mathbb{Z}$. Найдите образующий элемент идеала I:

а) $I=\{x \mid x=26u+65v,\ u,v\in\mathbb{Z}\}$;

б) $I=\{x \mid x$ делится на 8, 14 и 35$\}$;

в) $I=\{x \mid x=35u+48v,\ u,v\in\mathbb{Z}\}$;

г) $I=\{x \mid x$ делится на 5 и $x=18u+42v,\ u,v\in\mathbb{Z}\}$;

д) $I=\{x \mid x=14v+25u+18t,\ u,v,t\in\mathbb{Z}\}$;

4. В кольце $\mathbb{Z}$ найдите идеалы $(n)+(k)$, $(n)\cap(k)$, $(n)(k)$. Укажите их образующие.

а) $n=3$, $k=4$;

б) $n=6$, $k=6$;

в) $n=4$, $k=6$;

г) $n=8$, $k=6$;

д) $n=5$, $k=4$.

5. Найдите образующий элемент идеала I кольца $\mathbb{Z}$:

а) $I=(6,9,15)+(10,25,30)$;

б) $I=(6,9,15)\cap(20,25,30)$;

в) $I=(6,9,15)(20,25,30)$;

г) $I=(4,6,10)+(10,14,15)$;

д) $I=(5,6,8)\cap(12,15,20)$.

6. Докажите, что множество I является идеалом кольца $\mathbb{R}[x]$. Найдите образующий элемент идела I:

а) $I=\{f(x) \mid f(x)=(x^2+1)m(x)+(x-1)n(x),\ m(x),n(x)\in\mathbb{R}[x]\}$;

б) $I=\{f(x) \mid f(x)$ делится на x^2+1 и $x-1\}$;

в) $I=\{f(x) \mid f(x)=(x^3+1)m(x)+(x^2-1)n(x),\ m(x),n(x)\in\mathbb{R}[x]\}$;

г) $I=\{f(x) \mid f(x)$ делится на x^3+1 и $x^2-1\}$;

д) $I=\{f(x) \mid f(x)$ делится на $(x+1)^2$, x^2-1 и $x^3+1\}$;

7. В кольце $\mathbb{R}[x]$ найдите идеалы $(f(x))+(g(x))$, $(f(x))\cap(g(x))$, $(f(x))(g(x))$. Укажите их образующие:

а) $f(x)=x^4-2x^3+x^2$, $g(x)=x^3-8$;

б) $f(x)=x^4-1$, $g(x)=x^3+2x^2-x-2$;

в) $f(x)=x^4+4x^3-7x+12$, $g(x)=x^3+3x^2-4$;

г) $f(x)=x^2+x-6$, $g(x)=x^3-2x^2-5x+6$;

д) $f(x)=x^3+8$, $g(x)=x^3-x^2-4x+4$.

Р а с п р е д е л е н и е з а д а ч п о в а р и а н т а м

В а р и а н т 1.: №№ 1(г,и), 2(а,ж), 3(а), 4(а), 5(а), 6(а), 7(а).
В а р и а н т 2.: №№ 1(д,з), 2(б,к), 3(б), 4(б), 5(б), 6(б), 7(б).
В а р и а н т 3.: №№ 1(а,е), 2(е,и), 3(в), 4(в), 5(в), 6(в). 7(в).
В а р и а н т 4.: №№ 1(б,к), 2(в.з), 3(г), 4(г), 5(г), 6(г), 7(г).
В а р и а н т 5.: №№ 1(в,ж), 2(г,д), 3(д), 4(д), 5(д), 6(д), 7(д).

Лабораторная работа № 5
ФАКТОРКОЛЬЦА

Важную роль в теории колец играет следующая конструкция, позволяющая по заданному кольцу и его идеалу строить новое кольцо. Пусть I - идеал кольца K. Обозначим через K/I множество всех смежных классов $k+I=\{k+x \mid x\in I\}$ аддитивной группы кольца K по нормальной подгруппе I. На элементах множества K/I определим операции сложения и умножения следующим образом:

$$(k_1+I)+(k_2+I)=(k_1+k_2)+I,$$

$$(k_1+I)(k_2+I)=k_1k_2+I.$$

Тогда множество $K/I=\{k+I \mid k\in K\}$, рассматриваемое с введенными операциями сложения и умножения, удовлетворяет всем аксиомам кольца. Это кольцо называется **ф а к т о р к о л ь ц о м** кольца K по идеалу I или **к о л ь ц о м к л а с с о в в ы ч е т о в п о м о д у л ю и д е а л а** I. Нулем факторкольца K/I является класс $o+I=I$, где o - нулевой элемент кольца K. Противоположным к классу $a+I$ является класс $(-a)+I$.

Если K - коммутативное кольцо, то K/I - коммутативное кольцо. Если K - кольцо с единицей e, то K/I - кольцо с единицей $e+I$.

Пусть (0) - нулевой идеал кольца K. Тогда факторкольцо $K/(0)$ изоморфно кольцу K. Факторкольцо K/K изоморфно нулевому кольцу.

Пусть I - идеал кольца $\mathbb{Z}$. Ввиду теоремы 4.7 $I=m\mathbb{Z}=(m)$, где m - некоторое натуральное число. Тогда

$$\mathbb{Z}/I=\mathbb{Z}/m\mathbb{Z}=\{\bar{0},\bar{1},\bar{2},\dots,\overline{m-1}\}.$$

Факторкольцо $\mathbb{Z}/m\mathbb{Z}$ называется **к о л ь ц о м к л а с с о в в ы ч е т о в п о м о д у л ю** m и обозначается через $\mathbb{Z}_m$. Таким образом, из бесконечного кольца $\mathbb{Z}$ можно построить конечное факторкольцо из m элементов для любого натурального m. Более того, все нетривиальные факторкольца кольца целых чисел исчерпываются кольцами классов вычетов по модулю m, когда m пробегает множество всех натуральных чисел.

Факторкольцо K/I целостного кольца не обязательно является целостным кольцом. Например, факторкольцо $\mathbb{Z}_{10}$ кольца $\mathbb{Z}$ по идеалу $10\mathbb{Z}$ содержит делители нуля 5 и 2. Напомним, что факторкольцо $\mathbb{Z}_n$ содержит делители нуля тогда и только тогда, когда n - составное число. Другими словами, $\mathbb{Z}_n$ является полем тогда и только тогда, когда n - простое число.

Приведем две следующие теоремы для того, чтобы подчеркнуть имеющийся определенный параллелизм теории колец с теорией групп.

Т е о р е м а 5.1. Пусть L - подкольцо, а I - идеал кольца K. Тогда $L+I$ - подкольцо в K, содержащее I в качестве идеала, $L\cap I$ - идеал L, причем

$$(L+I)/I\cong L/L\cap I$$

Т е о р е м а 5.2. Пусть K - кольцо, I, L - его подкольца, причем I - идеал в K и $I\subseteq L$. Тогда $\bar{L}=L/I$ - подкольцо в K/I и $\pi: L\to\bar{L}$ является биективным отображением множества $\Omega(K,I)$ подколец из K, содержащих I, на множество $\Omega(\bar{K})$ всех подколец кольца $\bar{K}=K/I$. Если $L\in\Omega(K,I)$, то L - идеал в K тогда и только тогда, когда $\bar{L}$ - идеал в $\bar{K}$, причем

$$K/L\cong(K/I)/(L/I)$$

Идеал I кольца K называется **м а к с и м а л ь н ы м**, если $I\neq K$ и идеал I не содержится ни в каком другом идеале, отличном от I и K.

Т е о р е м а 5.3. Пусть K - коммутативное кольцо с единицей. Факторкольцо K/I является полем тогда и только тогда, когда I - максимальный идеал кольца K.

Из теоремы 5.3. легко следует, что идеал I кольца $\mathbb{Z}$ является максимальным тогда и только тогда, когда $I=(p)=p\mathbb{Z}$, где p - некоторое простое число.

Примеры решения и оформления задач

Пример 1. Найти все идеалы кольца $\mathbb{Z}_{12}$ и определить, по каким из них факторкольца являются полями.

Решение. В примере 5 лабораторной работы № 4 показано, что все идеалы кольца $\mathbb{Z}_{12}$ исчерпываются следующими идеалами:

$$I_1 = (\bar{0}) = \{\bar{0}\}$$
$$I_2 = (\bar{2}) = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}\}$$
$$I_3 = (\bar{3}) = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15}\}$$
$$I_4 = (\bar{6}) = \{\bar{0}, \bar{6}, \overline{12}\}$$
$$I_5 = (\bar{9}) = \{\bar{0}, \bar{9}\}$$
$$I_6 = (\bar{1}) = \mathbb{Z}_{12}$$

Идеалы I_2, I_3 являются максимальными идеалами кольца $\mathbb{Z}_{12}$, так как они не содержатся ни в каком другом идеале, отличном от $\mathbb{Z}_{12}$. По теореме 5.3 среди факторколец $\mathbb{Z}_{12}/I_K$, где $K = 1,2,3,4,5,6$, только факторкольца $\mathbb{Z}_{12}/I_2$ и $\mathbb{Z}_{12}/I_3$ являются полями.

Пример 2. Составить таблицы сложения и умножения элементов факторкольца $K = {}_3\mathbb{Z}/{}_9\mathbb{Z}$. Указать нулевой и противоположные элементы. Найти в K все делители нуля и все обратимые элементы.

Решение. Так как

$$3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \dots\},$$
$$9\mathbb{Z} = \{0, \pm 9, \pm 18, \dots\}$$

– идеалы кольца $\mathbb{Z}$ и $9\mathbb{Z} \subseteq 3\mathbb{Z}$, то $9\mathbb{Z}$ – идеал кольца $3\mathbb{Z}$. Рассмотрим смежные классы кольца $3\mathbb{Z}$ по идеалу $9\mathbb{Z}$.

$$0 + 9\mathbb{Z} = 9\mathbb{Z} = \{0, 9, 18, \dots, -9, -18, \dots\}$$

$$3 + 9\mathbb{Z} = \{3, 12, 21, \dots, -6, -15, \dots\}$$

$$6 + 9\mathbb{Z} = \{6, 15, 24, \dots, -3, -12, \dots\}$$

Ясно, что $3\mathbb{Z} = 9\mathbb{Z} \cup (3 + 9\mathbb{Z}) \cup (6 + 9\mathbb{Z})$, поэтому $K = \{9\mathbb{Z}, 3 + 9\mathbb{Z}, 6 + 9\mathbb{Z}\}$. Составим таблицы сложения и умножения элементов факторкольца K.

$+$	$9\mathbb{Z}$	$3+9\mathbb{Z}$	$6+9\mathbb{Z}$
$9\mathbb{Z}$	$9\mathbb{Z}$	$3+9\mathbb{Z}$	$6+9\mathbb{Z}$
$3+9\mathbb{Z}$	$3+9\mathbb{Z}$	$6+9\mathbb{Z}$	$9\mathbb{Z}$
$6+9\mathbb{Z}$	$6+9\mathbb{Z}$	$9\mathbb{Z}$	$3+9\mathbb{Z}$

$\cdot$	$9\mathbb{Z}$	$3+9\mathbb{Z}$	$6+9\mathbb{Z}$
$9\mathbb{Z}$	$9\mathbb{Z}$	$9\mathbb{Z}$	$9\mathbb{Z}$
$3+9\mathbb{Z}$	$9\mathbb{Z}$	$9\mathbb{Z}$	$9\mathbb{Z}$
$6+9\mathbb{Z}$	$9\mathbb{Z}$	$9\mathbb{Z}$	$9\mathbb{Z}$

Из таблицы сложения элементов кольца K получаем, что $9\mathbb{Z}$ – нулевой элемент кольца K, а противоположными будут элементы $-(3+9\mathbb{Z}) = 6 + 9\mathbb{Z}$, $-(6+9\mathbb{Z}) = 3 + 9\mathbb{Z}$. Таблица умножения показывает, что K – кольцо с нулевым умножением (произведение любых элементов из K равно нулю). Поэтому $3 + 9\mathbb{Z}$ и $6 + 9\mathbb{Z}$ – делители нуля, а обратных элементов в K нет.

Пример 3. Доказать, что $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$.

Решение. Напомним, что $\mathbb{Z}[x]$ – это кольцо многочленов переменной x с целыми коэффициентами, а (x) – главный идеал кольца $\mathbb{Z}[x]$, порожденный многочленом $g(x) = x$. Ввиду теоремы 4.6 имеем, что

$$I = (x) = x\mathbb{Z}[x] = \{x\, m(x) \mid m(x) \in \mathbb{Z}[x]\}$$

Значит, идеал (x) состоит из тех и только из тех многочленов из $\mathbb{Z}[x]$, у которых свободный член равен нулю.

Пусть $m_1(x) + I$ и $m_2(x) + I$ – два смежных класса кольца $\mathbb{Z}[x]$ по идеалу I. Эти смежные классы равны тогда и только тогда, когда $m_1(x) - m_2(x) \in I$, т.е. когда $m_1(x)$ и $m_2(x)$ имеют равные свободные члены. С другой стороны, если

$$m(x) = K_n x^n + K_{n-1} x^{n-1} + \dots + K_1 x + K_0,$$

то $m(x) + I = K_0 + I$. Следовательно, произвольный смежный класс кольца $\mathbb{Z}[x]/(x)$ имеет вид $n + (x)$, где n – некоторое целое число. При этом классы $n + (x)$ и $\ell + (x)$ различны, если $n \neq \ell$.

Итак, $\mathbb{Z}[x]/(x) = \{n + (x) \mid n \in \mathbb{Z}\}$.

Рассмотрим отображение f кольца $\mathbb{Z}[x]/(x)$ в кольцо $\mathbb{Z}$, определяемое равенством $f(n + (x)) = n$. Тогда

$$f((n + (x)) + (\ell + (x))) = f((n + \ell) + (x)) = n + \ell = f(n + (x)) + f(\ell + (x)),$$

$$f((n + (x))(\ell + (x))) = f(n\ell + (x)) = n\ell = f(n + (x))\, f(\ell + (x))$$

Отображение f является, очевидно, взаимнооднозначным. Поэтому и является искомым изоморфизмом колец $\mathbb{Z}[x]/(x)$ и $\mathbb{Z}$.

Вопросы для самоконтроля

1. Почему в определении факторкольца K/I нельзя идеал I заменить подкольцом I?
2. Пусть K/I – кольцо с единицей, $a+I$ – обратимый элемент K/I. Какой смежный класс из K/I будет обратным к $a+I$?
3. Пусть I – идеал целостного кольца K. Всегда ли K/I – целостное кольцо?
4. Постройте все факторкольца тела T.
5. Сформулируйте аналоги теорем 5.I и 5.2 для групп.
6. Опишите все максимальные идеалы кольца $\mathbb{Z}$.
7. Пусть I – идеал кольца K, $a+I$, $b+I$ – два смежных класса по идеалу I. В каком случае $a+I=b+I$?
8. Пусть K – кольцо. Что представляют собой факторкольца $K/(0)$ и K/K?
9. Пусть K – кольцо с нулевым умножением. Опишите все факторкольца K.
10. Докажите, что факторкольцо K/I нулевое, если идеал I кольца K содержит обратимый элемент.
11. Проверьте, что K/I – коммутативное кольцо с единицей, если таковым является кольцо K.
12. Когда $\mathbb{Z}_m$ – целостное кольцо?
13. Приведите примеры немаксимальных идеалов кольца $\mathbb{Z}$.
14. Приведите пример кольца с нулевым умножением, у которого некоторое факторкольцо – кольцо с нулевым умножением.

Задания к лабораторной работе

1. Найдите все идеалы кольца $\mathbb{Z}_n$ и определите, по каким из них факторкольца являются полями?

   а) $n=14$; б) $n=12$; в) $n=6$;
   г) $n=8$; д) $n=10$.

2. Составьте таблицы сложения и умножения элементов факторкольца:

   а) $n=5, k=10$; б) $n=3, k=12$; в) $n=2, k=8$;
   г) $n=5, k=15$; д) $n=7, k=21$.

3. Пусть $K=n\mathbb{Z}/k\mathbb{Z}$. Укажите: нулевой элемент кольца K; все делители нуля кольца K; все обратимые элементы кольца K; для каждого элемента противоположный элемент

   а) $n=5, k=10$; б) $n=3, k=12$; в) $n=2, k=8$;
   г) $n=5, k=15$; д) $n=7, k=21$.

4. Покажите, что I – идеал кольца K, найдите классы вычетов кольца K по идеалу I и выясните, является ли факторкольцо K/I полем?

   а) $K=\{a+b\sqrt{3} \mid a,b\in\mathbb{Z}\}$, $I=\{a+b\sqrt{3} \mid a,b\in 2\mathbb{Z}\}$;
   б) $K=\{a+b\sqrt{2} \mid a,b\in\mathbb{Z}\}$, $I=\{a+b\sqrt{2} \mid a,b\in 3\mathbb{Z}\}$;
   в) $K=\{a+bi \mid a,b\in\mathbb{Z}\}$, $I=\{a+bi \mid a,b\in 3\mathbb{Z}\}$;
   г) $K=\{a+bi \mid a,b\in\mathbb{Z}\}$, $I=\{a+bi \mid a,b\in 2\mathbb{Z}\}$;
   д) $K=\{a+b\sqrt{2} \mid a,b\in\mathbb{Z}\}$, $I=\{a+bi \mid a,b\in 3\mathbb{Z}\}$;
   е) $K=\mathbb{R}[x]$, $I=(x^2+1)$;
   ж) $K=\mathbb{Z}[x]$, $I=(x^2+1)$;
   з) $K=\mathbb{Z}_2[x]$, $I=(x^2+x+1)$;
   и) $K=\mathbb{Z}_3[x]$, $I=(x^2+1)$;
   к) $K=\mathbb{Z}_2[x]$, $I=(x^2+x)$.

5. Доказать, что факторкольцо $\mathbb{Z}[i]/(5)$ не является полем.
6. Доказать, что факторкольцо $\mathbb{Z}[i]/(2)$ не является полем.
7. Доказать, что факторкольцо $\mathbb{Z}[i]/(7)$ является полем.
9. Доказать, что факторкольцо $\mathbb{Z}[i]/(3)$ является полем.
10. Доказать, что факторкольцо $\mathbb{Z}[i]/(11)$ является полем.
11. Доказать, что факторкольцо $\mathbb{Z}[i]/(n)$ является полем тогда и только тогда, когда n – простое число, не равное сумме двух квадратов целых чисел.
12. Доказать, что при любом натуральном $n>1$ факторкольцо $\mathbb{Z}[x]/(n)$ изоморфно $\mathbb{Z}_n[x]$.
13. Установите следующие изоморфизмы:

    а) $\mathbb{Q}[x]/(x)\cong\mathbb{Q}$;
    б) $\mathbb{R}[x]/(x-1)\cong\mathbb{R}$;
    в) $\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$.

г) $\mathbb{Z}[i]/(i) \cong (0)$;

д) $\mathbb{Z}[x]/(x^2) \cong \mathbb{Z}[i]$.

Распределение задач по вариантам

Вариант 1.: №№ 1(а), 2(а), 3(а), 4(а,к), 5, 11, 12(а).
Вариант 2.: №№ 1(б), 2(б), 3(б), 4(б,ж), 6, 10, 12(б).
Вариант 3.: №№ 1(в), 2(в), 3(в), 4(в,к), 7, 11, 12(в).
Вариант 4.: №№ 1(г), 2(г), 3(г), 4(г,з), 8, 10, 12(г).
Вариант 5.: №№ 1(д), 2(д), 3(д), 4(д,е), 9, 11, 12(д).

Лабараторная работа № 6
ГОМОМОРФИЗМЫ КОЛЕЦ

Отображение $f: K_1 \to K_2$ кольца K_1 в кольцо K_2 называется **гомоморфизмом**, если для всех $a, b \in K_1$ выполняются условия: 1) $f(a+b) = f(a) + f(b)$; 2) $f(ab) = f(a)f(b)$.

Первое условие в определении гомоморфизма колец определяет гомоморфизм аддитивной группы $(K_1, +)$ кольца K_1 в аддитивную группу $(K_2, +)$ кольца K_2. Поэтому при гомоморфизме колец нулевой элемент переходит в нулевой, а противоположный – в противоположный.

Если f – гомоморфизм кольца K_1 в кольцо K_2, то множество $Im f = \{f(k) \mid k \in K_1\}$ называется **образом** гомоморфизма f, а множество $Ker f = \{k \in K_1 \mid f(k) = 0\}$ – **ядром** гомоморфизма. Если $Ker f = \{0\}$ – то гомоморфизм f называется **мономорфизмом**, а если $Im f = K_2$, то – **эпиморфизмом**. Гомоморфизм, являющийся одновременно мономорфизмом и эпиморфизмом, называется **изоморфизмом**; в этом случае говорят, что кольца K_1 и K_2 **изоморфны** и пишут $K_1 \cong K_2$. Нетрудно проверить, что отношение изоморфизма колец является отношением эквивалентности.

Лемма 6.1. Пусть $f: K_1 \to K_2$ – гомоморфизм кольца K_1 в K_2. Тогда справедливы следующие утверждения:

1) $Ker f$ – идеал кольца K_1;
2) $Im f$ – подкольцо кольца K_2;
3) если K_1 – кольцо с единицей e, то $f(e)$ – единица кольца $Im f$;
4) если a – обратимый элемент кольца K_1, то $f(a)$ – обратимый элемент кольца K_2, причем $(f(a))^{-1} = f(a^{-1})$.

Из этой леммы следует, что не имеет смысла говорить о гомоморфизмах тел и полей, так как любой гомоморфизм f тела T_1 в T_2 является либо нулевым гомоморфизмом ($Ker f = T_1$, $Im f = \{0\}$), либо изоморфным вложением ($Ker f = \{0\}$, $Im f = T_1$).

Лемма 6.2. Пусть K – кольцо, I – идеал в K. Тогда отображение $\varphi: a \to a + I$ является эпиморфизмом кольца K на факторкольцо K/I, ядро которого совпадает с I.

Теорема 6.3. (Основная теорема о гомоморфизмах). Если $f: K \to H$ – произвольный гомоморфизм кольца K в кольцо H, то факторкольцо кольца K по ядру $Ker f$ гомоморфизма изоморфно образу гомоморфизма: $K/Ker f \cong Im f$.

Основную теорему о гомоморфизмах для колец дополняют теоремы 5.1 и 5.2 об изоморфизме.

В дальнейшем нам понадобятся следующие теоретико-кольцевые конструкции. Пусть $K_1, K_2, \ldots, K_n$ – некоторые кольца, $K = K_1 \times K_2 \times \ldots \times K_n$ – декартово произведение множеств $K_1, K_2, \ldots, K_n$, т.е. $K = \{(k_1, k_2, \ldots, k_n) \mid k_i \in K_i,\ i = 1, 2, \ldots, n\}$. Введем на K структуру кольца, определив операции сложения и умножения покомпонентно:

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n).$$
$$(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1 y_1, x_2 y_2, \ldots, x_n y_n)$$

Кольцо K называется **внешней прямой суммой** колец $K_1, K_2, \ldots, K_n$ и обозначается $K_1 \oplus K_2 \oplus \ldots \oplus K_n$. Нулевым элементом в кольце K будет элемент $(0, 0, \ldots, 0)$, противоположным элементом к $(x_1, x_2, \ldots, x_n)$ будет элемент $(-x_1, -x_2, \ldots, -x_n)$.

Кольцо K является **внутренней прямой суммой** своих идеалов $I_1, I_2, \ldots, I_n$, если выполняются следующие условия: 1) $K = I_1 + I_2 + \ldots + I_n$; 2) $I_i \cap (I_1 + \ldots + I_{i-1} + I_{i+1} + \ldots + I_n) = 0$ для всех $i = 1, 2, \ldots, n$.

Как и в теории групп, различие между внутренними и внешними прямыми суммами колец – чисто теоретико-множественное. Так, например, кольцо $K = K_1 \oplus K_2 \oplus \ldots \oplus K_n$ можно рассматривать как внутреннюю прямую сумму идеалов I_i, $i = 1, 2, \ldots, n$, где $I_i = \{(0, \ldots, 0, x_i, 0, \ldots, 0) \mid x_i \in K_i\}$. Обратно, если K – внутренняя прямая сумма идеалов $I_1, I_2, \ldots, I_n$, то любой элемент $x \in K$ однозначно представим в виде $x = x_1 + x_2 + \ldots + x_n$, где $x_1 \in K_1, x_2 \in K_2, \ldots, x_n \in K_n$. Отсюда легко выводится, что

$$K \cong I_1 \oplus I_2 \oplus \ldots \oplus I_n$$

Теорема 6.4 (Китайская теорема об остатках). Пусть $I_1, I_2, \ldots, I_n$ – идеалы кольца K. Если K – кольцо с единицей и $I_i + I_j = K$

для $1 \le i \ne j \le n$, то отображение

$$\varphi : x \rightarrow (x + I_1, \ldots, x + I_n)$$

является эпиморфизмом кольца K на кольцо $K/I_1 \oplus \ldots \oplus K/I_n$

Из теоремы 6.3 следует, что если выполняются условия теоремы 6.4, то

$$K/I_1 \cap I_2 \cap \ldots \cap I_n \cong K/I_1 \oplus K/I_2 \oplus \ldots \oplus K/I_n$$

Следствие. Пусть n – натуральное число с каноническим разложением $n = p_1^{m_1} p_2^{m_2} \ldots p_s^{m_s}$. Тогда

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{m_1}} \oplus \mathbb{Z}_{p_2^{m_2}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{m_s}}$$

Примеры решения и оформления задач

Пример 1. Пусть $p_1(x), p_2(x), \ldots, p_s(x)$ – взаимно простые неприводимые многочлены над полем $\mathbb{R}$, $f(x) = p_1^{k_1}(x) p_2^{k_2}(x) \ldots p_s^{k_s}(x)$. Доказать, что

$$\mathbb{R}[x]/f(x)\mathbb{R}[x] \cong \mathbb{R}[x]/p_1^{k_1}(x)\mathbb{R}[x] \oplus \ldots \oplus \mathbb{R}[x]/p_s^{k_s}(x)\mathbb{R}[x]$$

Решение. Обозначим $\mathbb{R}[x] = K$, $f(x)\mathbb{R}[x] = I$, $p_1^{k_1}(x)\mathbb{R}[x] = I_1, \ldots, p_s^{k_s}(x)\mathbb{R}[x] = I_s$. Покажем, что $I_i + I_j = K$ для всех $i \ne j$. Так как $НОД(p_i^{k_i}(x), p_j^{k_j}(x)) = 1$, то найдутся многочлены $U_i(x)$ и $V_j(x)$ такие, что

$$1 = U_i(x) p_i^{k_i}(x) + V_j(x) p_j^{k_j}(x).$$

Пусть $g(x)$ – произвольный многочлен кольца $\mathbb{R}[x]$. Тогда

$$g(x) = g(x) \cdot 1 = p_i^{k_i}(x)(g(x)U_i(x)) + p_j^{k_j}(x)(g(x)V_j(x)) \in$$
$$\in p_i^{k_i}(x)\mathbb{R}[x] + p_j^{k_j}(x)\mathbb{R}[x] = I_i + I_j$$

Значит, $I_i + I_j = K$ для всех $i \ne j$.

Рассмотрим гомоморфизм

$$\varphi : g(x) \longmapsto (g(x) + I_1, \ldots, g(x) + I_s)$$

Найдем ядро этого гомоморфизма. По определению $Ker\,\varphi =$

$$= \{ g(x) \in K \mid \varphi(g(x)) = 0 \in K/I_1 \oplus \ldots \oplus K/I_s \} =$$
$$= \{ g(x) \in K \mid (g(x) + I_1, \ldots, g(x) + I_s) = (I_1, \ldots, I_s) \} =$$
$$= \{ g(x) \in K \mid g(x) + I_1 = I_1, \ldots, g(x) + I_s = I_s \} =$$
$$= \{ g(x) \in K \mid g(x) \in I_1, \ldots, g(x) \in I_s \} = I_1 \cap \ldots \cap I_s$$

По теореме 6.4 $Im\,\varphi = K/I_1 \oplus \ldots \oplus K/I_s$

По основной теореме о гомоморфизмах колец имеем

$$K/Ker\,\varphi = K/I_1 \cap \ldots \cap I_s \cong Im\,\varphi = K/I_1 \oplus \ldots \oplus K/I_s$$

Остается заметить, что $I = I_1 \cap \ldots \cap I_s$. Действительно, пусть $g(x) \in I$. Так как $I = f(x)\mathbb{R}[x]$, то найдется многочлен $d(x)$, такой, что $g(x) = f(x)d(x)$. Поэтому

$$g(x) = p_1^{k_1}(x) \ldots p_s^{k_s}(x) d(x) \in p_i^{k_i}(x)\mathbb{R}[x] = I_i$$

для всех $i = 1, 2, \ldots, s$. Итак, $I \subseteq I_1 \cap \ldots \cap I_s$. Пусть теперь $m(x) \in I_1 \cap \ldots \cap I_s$. Тогда $m(x) = p_1^{k_1}(x) m_1(x), \ldots, m(x) = p_s^{k_s}(x) m_s(x)$

Так как многочлены $p_1(x), \ldots, p_s(x)$ попарно взаимно просты, то $m(x) = p_1^{k_1}(x) \ldots p_s^{k_s}(x) n(x) = f(x) n(x) \in f(x)\mathbb{R}[x] = I$

Итак, $K/I \cong K/I_1 \oplus \ldots \oplus K/I_s$

Пример 2. Пусть A, B – некоторые кольца. Доказать, что отображение $f : A \oplus B \rightarrow A$, $f : (a, b) \mapsto a$ является гомоморфизмом кольца $A \oplus B$ в кольцо A. Найти $Ker\,f$ и $Im\,f$.

Решение. Проверим, что отображение f является гомоморфизмом кольца $A \oplus B$ в кольцо A. Пусть $x = (a_1, b_1) \in A \oplus B$, $y = (a_2, b_2) \in A \oplus B$. Тогда $f(x + y) = f((a_1, b_1) + (a_2, b_2)) =$

$$= f((a_1 + a_2, b_1 + b_2)) = a_1 + a_2 = f(x) + f(y), \; f(xy) = f((a_1, b_1)(a_2, b_2))$$
$$= f((a_1 a_2, b_1 b_2)) = a_1 a_2 = f(x) f(y)$$

Найдем ядро гомоморфизма f. По определению $Ker\,f =$

$$= \{(a, b) \in A \oplus B \mid f(a, b) = 0 \in A\} = \{(a, b) \in A \oplus B \mid a = 0 \in A\} =$$
$$= \{(0, b) \in A \oplus B \mid b \in B\}$$

Очевидно, отображение $f : A \oplus B \rightarrow A$ сюръективно. Поэтому $Im\,f = A$

Пример 3. Доказать, что отображение $f : \mathbb{C} \rightarrow \mathbb{C}$, определяемое равенством $f(z) = \bar{z}$, является автоморфизмом поля $\mathbb{C}$.

Решение. Очевидно, отображение f является взаимнооднозначным. Кроме того, если $z_1 = x_1 + y_1 i$, $z_2 = x_2 + y_2 i$, то

$$f(z_1 + z_2) = f((x_1 + x_2) + (y_1 + y_2)i) = (x_1 + x_2) - (y_1 + y_2)i =$$
$$= (x_1 - y_1 i) + (x_2 - y_2 i) = \bar{z}_1 + \bar{z}_2 = f(z_1) + f(z_2) \text{ и } f(z_1 z_2) =$$
$$= f((x_1 + y_1 i)(x_2 + y_2 i)) = f((x_1 x_2 - y_1 y_2) + (x_1 y_2 + y_1 x_2)i) =$$
$$= (x_1 x_2 - y_1 y_2) - (x_1 y_2 + x_2 y_1)i = (x_1 - y_1 i)(x_2 - y_2 i) = \bar{z}_1 \bar{z}_2 =$$
$$= f(z_1) f(z_2)$$

Значит, f – автоморфизм поля $\mathbb{C}$.

Пример 4. Найти все гомоморфизмы кольца $\mathbb{Z}$ в кольцо $M(2, \mathbb{Z}_2)$.

Решение. Напомним, что $M(2, \mathbb{Z}_2) = \left\{ \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \middle| \right.$ x_1, x_2, x_3, x_4 – либо $\bar{0}$, либо $\bar{1}$ $\}$. Пусть f – произвольный гомоморфизм кольца $\mathbb{Z}$ в кольцо $M(2, \mathbb{Z}_2)$. Тогда $f(n) = f(n \cdot 1) = n f(1)$, причем $(f(1))^2 = f(1) f(1) = f(1 \cdot 1) = f(1)$. Значит, гомоморфизм имеет вид $f: n \mapsto n f(1)$, причем элемент $f(1) \in M(2, \mathbb{Z}_2)$ обладает свойством $(f(1))^2 = f(1)$. Таким свойством кольце $M(2, \mathbb{Z}_2)$ обладают только 8 элементов:

$$E_1 = \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}, \quad E_2 = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, \quad E_3 = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}, \quad E_4 = \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix},$$

$$E_5 = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{0} \end{pmatrix}, \quad E_6 = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{0} \end{pmatrix}, \quad E_7 = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{0} & \bar{1} \end{pmatrix}, \quad E_8 = \begin{pmatrix} \bar{0} & \bar{0} \\ \bar{1} & \bar{1} \end{pmatrix}$$

Итак, существует только 8 гомоморфизмов кольца $\mathbb{Z}$ в кольцо $M(2, \mathbb{Z}_2)$. Все они имеют вид $f_i: n \to n E_i$, $i = 1, 2, \ldots, 8$.

Вопросы для самоконтроля

1. Как задать гомоморфизм колец?
2. Пусть φ -гомоморфизм кольца K_1 в кольцо K_2. Докажите, что
   а) $\varphi(a-b) = \varphi(a) - \varphi(b)$ для всех $a, b \in K_1$;
   б) $\varphi(-a) = -\varphi(a)$ для любого $a \in K_1$;
   в) $\varphi(0_1) = 0_2$, где 0_1 и 0_2 - нулевые элементы колец K_1 и K_2 соответственно.
3. Докажите, что отношение изоморфизма колец является отношением эквивалентности.
4. Докажите, что гомоморфизм f кольца K_1 в кольцо K_2 является мономорфизмом тогда и только тогда, когда f - инъективное отображение.
5. Докажите, что гомоморфизм f кольца K_1 в кольцо K_2 является эпиморфизмом тогда и только тогда, когда f - сюръективное отображение.
6. Пусть K_1 и K_2 - кольца с единицей, $\varphi: K_1 \to K_2$ - гомоморфизм
   а) Верно ли, что образ единицы кольца K_1 является единицей кольца K_2.
   б) Верно ли утверждение а), если φ - эпиморфизм.
7. Пусть K - прямая сумма колец $K_1, K_2, \ldots, K_n$.
   а) При каких условиях K коммутативно; имеет единицу; не имеет делителей нуля?
   б) Найти в K все обратимые элементы; все делители нуля.
8. Доказать, что любой гомоморфизм поля в кольцо является или нулевым, или изоморфным отображением на некоторое подполе.
9. Доказать, что кольцо классов вычетов $\mathbb{Z}_{p_1 p_2 \ldots p_k}$, где $p_1, p_2, \ldots, p_k$ - различные простые числа, является прямой суммой полей.

10. Пусть $f: K_1 \to K_2$ - гомоморфизм кольца K_1 в кольцо K_2. Доказать, что $f(nx) = n f(x)$ для любого $x \in K_1$ и любого $n \in \mathbb{Z}$.

Задания к лабораторной работе

1. Показать, что следующее отображение удовлетворяет одному условию из определения гомоморфизма колец, но не удовлетворяет другому условию:
   а) $\varphi: \mathbb{Z} \to 2\mathbb{Z}$, $\varphi(n) = 2n$;
   б) $\varphi: \mathbb{C} \to \mathbb{R}$, $\varphi(a+bi) = a$;
   в) $\varphi: \mathbb{C} \to \mathbb{C}$, $\varphi(z) = z^2$;
   г) $\varphi: M(2, \mathbb{C}) \to \mathbb{C}$, $\varphi(A) = \det A$;
   д) $\varphi: \mathbb{C} \to \mathbb{R}$, $\varphi(a+bi) = b$.

2. Пусть f - отображение кольца K_1 в кольцо K_2. Доказать, что f - гомоморфизм. Найти $\operatorname{Ker} f$ и факторкольцо $K_1 / \operatorname{Ker} f$.
   а) $K_1 = \mathbb{Z}$, K_2 - произвольное кольцо с единицей e, $f: n \mapsto ne$
   б) K_1 - кольцо всех непрерывных функций на отрезке $[-1, 1]$, $K_2 = \mathbb{R}$, $f: \varphi \mapsto \varphi(0)$;
   в) $K_1 = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$, $K_2 = \mathbb{Z}$, $f: \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mapsto a+b$
   г) $K_1 = \mathbb{Z}$, $K_2 = \mathbb{Z}_2$
   $$f: n \mapsto \begin{cases} \bar{0}, & \text{если } n \text{ - четное число}, \\ \bar{1}, & \text{если } n \text{ - нечетное число}. \end{cases}$$
   д) $K_1 = K_2 = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}$, $f: a + b\sqrt{2} \mapsto a - b\sqrt{2}$.
   е) $K_1 = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| a, b \in \mathbb{Z} \right\}$, $K_2 = \mathbb{Z}$, $f: \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mapsto a-b$;
   ж) $K_1 = \left\{ \begin{pmatrix} a & b \\ a & b \end{pmatrix} \middle| a, b \in \mathbb{R} \right\}$, $K_2 = \mathbb{R}$, $f: \begin{pmatrix} a & b \\ a & b \end{pmatrix} \mapsto a+b$;

3. Найти все гомоморфизмы кольца $\mathbb{Z}_n$ в кольцо $\mathbb{Z}_m$:
   а) $n=6$, $m=5$; б) $n=8$, $m=3$; в) $n=9$, $m=5$;
   г) $n=10$, $m=3$; д) $n=12$, $m=7$.

4. Разложить кольцо $\mathbb{Z}_n$ в прямую сумму колец:
а) $n=1526$; б) $n=3752$; в) $n=2310$;
г) $n=1256$; д) $n=885$.

5. Разложить кольцо $\mathbb{R}[x]/(f(x))$ в прямую сумму колец:
а) $f(x)=x^3+3x^2-4$;
б) $f(x)=x^3-x^2-4x+4$;
в) $f(x)=x^3-6x^2+11x-6$;
г) $f(x)=2x^4-7x^3+9x^2-5x+1$;
д) $f(x)=5x^4+14x^3+12x^2+2x-1$.

6. Найти все гомоморфизмы кольца K_1 в кольцо K_2:
а) $K_1=\mathbb{Z}$, $K_2=2\mathbb{Z}$;
б) $K=2\mathbb{Z}$, $K_2=2\mathbb{Z}$;
в) $K_1=2\mathbb{Z}$, $K_2=3\mathbb{Z}$;
г) $K_1=\mathbb{Z}$, $K_2=\mathbb{Q}$;
д) $K_1=\mathbb{Q}$, $K_2=\mathbb{Z}$.

7. Докажите, что в кольце $K=\left\{\begin{pmatrix} a & b \\ a & b \end{pmatrix} \mid a,b\in\mathbb{R}\right\}$ множества $I_1=\left\{\begin{pmatrix} a & -a \\ a & -a \end{pmatrix} \mid a\in\mathbb{R}\right\}$, $I_2=\left\{\begin{pmatrix} c & 0 \\ c & 0 \end{pmatrix} \mid c\in\mathbb{R}\right\}$ являются идеалами и что $K=I_1\oplus I_2$. Имеются ли единицы в идеалах I_1 и I_2 ?

8. Докажите, что если $K=I_1\oplus I_2$, то произведение любого элемента из I_1 на любой элемент из I_2 равно нулю.

9. Кольцо K всех 2×2 - матриц над $\mathbb{R}$, коммутирующих с матрицей $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$, разложите в прямую сумму двух идеалов, каждый из которых изоморфен $\mathbb{R}$.

10. Докажите, что если $K=I_1\oplus I_2$, то $K/I_1\cong I_2$ и $K/I_2\cong I_1$.

11. Докажите, что если $K=I_1\oplus I_2$ и e_1, e_2 - единицы в I_1 и I_2, то e_1+e_2 - единица в K.

Распределение задач по вариантам

Вариант I.: №№ I(а), 2(а,е), 3(а), 4(а), 5(а), 6(а), II.

Вариант 2.: №№ I(б), 2(б,ж), 3(б), 4(б), 5(Б), 6)б), I0.
Вариант 3.: №№ I(в), 2(в,д), 3(в), 4(в), 5(в), 6(в), 9.
Вариант 4.: №№ I(г), 2(г,в), 3(г), 4(г), 5(г), 6(г), 8.
Вариант 5.: №№ I(д), 2(д,ж), 3(д), 4(д), 5(д), 6(д), 7.

Содержание

Лабораторные работы
по курсу "Алгебра и теория чисел"
для студентов математического факультета

Составители: Каморников Сергей Федорович
Карызин Александр Петрович
Монахов Виктор Степанович

Ответственный за выпуск А.П.Кармазин

Подписано к печати 27 .03.90. Формат 60х84 I/I6
Бумага писчая № I. Печать офсетная. Усл.п.л.3,5 Уч.-изд.л.3,2.
Тираж 200 экз. Заказ 70 . Бесплатно

Отпечатано на ротапринте ГГУ, г.Гомель, ул.Советская, I04.