МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
"МОГИЛЕВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. А. А. КУЛЕШОВА"

В.Н. БОРБАТ
Н.В. САКОВИЧ

КОЛЬЦА

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ
И ЗАДАЧИ
ДЛЯ САМОСТОЯТЕЛЬНОГО РЕШЕНИЯ**

Могилев
МГУ им. А.А.Кулешова
2002

Борбат В.Н., Сакович Н.В.

Б82 Кольца: Методические указания и задачи для самостоятельного решения — Могилев: МГУ им. А.А.Кулешова, 2002. — 32 с.

Методические указания "Кольца" предназначены для оказания помощи студентам физико-математического факультета при подготовке к практическим занятиям по алгебре и теории чисел. Все содержание методических указаний разбито на шесть занятий, каждое из которых содержит контрольные вопросы, рекомендуемую литературу, образцы решения задач, задачи для домашнего задания и дополнительные задачи.

УДК 511(075.8), 512(075.8)
ББК 22.14

Технический редактор *А. Н. Гладун*

т 7.0
печ

Занятие 1

КОЛЬЦО, ПОДКОЛЬЦО, ИДЕАЛ. ГОМОМОРФИЗМ КОЛЕЦ

Вопросы к занятию

1. Определение кольца и подкольца. Критерий подкольца.
2. Идеал. Критерий идеала.
3. Смежные классы по идеалу. Фактор-кольцо.
4. Гомоморфизм и изоморфизм колец.
5. Теоремы о гомоморфизме колец

Литература: [1], с. 104-111, 430-436.

Образцы решения задач

Задача 1. Доказать, что алгебраическая система $(\{a+b\sqrt{2} \mid a, b\in Z\},+,\ \cdot)$ является кольцом. Указать его подкольца, идеалы и соответствующие гомоморфизмы, фактор-кольца.

Решение. Проверим замкнутость обеих операций:

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

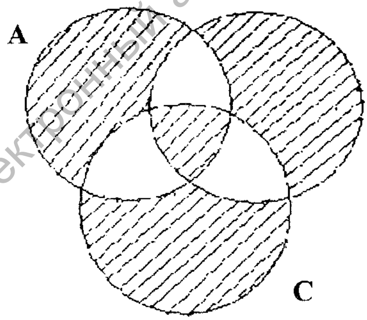
$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}.$$

Так как числа $a+c,\ b+d,\ ac+2bd,\ ad+bc$ целые, то операции сложения и умножения замкнуты. Сложение и умножение любых действительных чисел коммутативны и ассоциативны, умножение дистрибутивно относительно сложения. Нуль и единица содержатся среди этих чисел. Каждое число $a+b\sqrt{2},\ a,\ b\in Z$ обладает противоположным числом того же вида. Следовательно, указанная алгебра является кольцом. Обозначим это кольцо $Z[\sqrt{2}\,]$. При $b=0$ получаем, что кольцо целых чисел является подкольцом кольца $Z[\sqrt{2}\,]$. Но Z не является идеалом в $Z[\sqrt{2}\,]$, ибо произведение целого числа на число $a+b\sqrt{2},\ a,\ b\in Z$, не есть целое число. Любое подкольцо кольца Z является подкольцом в $Z[\sqrt{2}\,]$, но не является идеалом в $Z[\sqrt{2}\,]$, хотя является идеалом в Z. Очевидно, что $\{\,a+b\sqrt{2} \mid a,\ b\in 2Z\,\}$ замкнуто по сложению, умножению и взятию противоположного числа, то есть является подкольцом в $Z[\sqrt{2}\,]$. Более того, это подкольцо есть идеал, ибо если a и b четные числа, то при любых целых c и d числа $ac+2db,\ ad+bc$ являются четными. Аналогично, при любом натуральном m $I = \{ a+b\sqrt{2} \mid a, b \in mZ \}$ есть идеал в кольце $Z[\sqrt{2}]$. Рассмотрим смежные классы по идеалу I. Для того чтобы числа $a+b\sqrt{2}$ и $c+d\sqrt{2}$ принадлежали одному смежному классу, их разность должна принадлежать идеалу, то есть числа $a-c$, $b-d$ должны быть кратны m. В этом случае $a \equiv c \pmod{m}$, $b \equiv d \pmod{m}$. Если хотя бы одно из указанных сравнений ложно, то взятые числа принадлежат разным смежным классам. Отсюда следует, что, взяв два экземпляра полной системы вычетов по модулю m и комбинируя каждый вычет с каждым, получим, m^2 чисел $a+b\sqrt{2}$, являющихся представителями различных смежных классов по идеалу I. Очевидно, что этим будут исчерпаны все смежные классы, то есть фактор - кольцо по идеалу I состоит из m^2 элементов. Например, при $m = 2$ фактор - кольцо состоит из элементов I, $1+I$, $\sqrt{2}+I$, $1+\sqrt{2}+I$. Как обычно, отображение элемента кольца на содержащий его смежный класс задает гомоморфизм кольца $Z[\sqrt{2}]$ на фактор-кольцо.

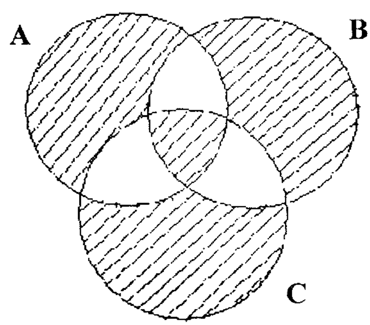
Задача 2. Обозначим операции над множествами следующим образом:

$A + B = (A \cup B) \setminus (A \cap B)$ (симметрическая разность), $A \cdot B = A \cap B$ (пересечение). Пусть M – некоторое множество, $P(M) = P$ – множество всех его подмножеств. Исследовать алгебру $(P, +, \cdot)$.

Решение. Операция сложения коммутативна, ибо объединение и пересечение множеств есть коммутативные операции. Ее ассоциативность можно строго доказать, однако это довольно громоздко, поэтому ограничимся построением диаграмм Эйлера-Венна.



(A+B)+C



A+(B+C)

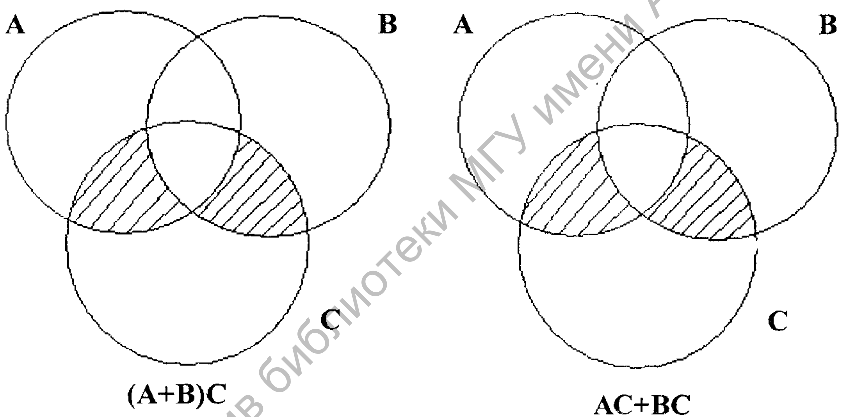
Пустое множество является нейтральным элементом по сложению: $A+\varnothing=(A\bigcup\varnothing)\setminus(A\bigcap\varnothing)=A\setminus\varnothing=A$.

Каждое множество противоположно само себе: $A+A=(A\bigcup A)\setminus(A\bigcap A)=A\setminus A=\varnothing$.

Итак *(P, +)* – коммутативная группа. Операция умножения коммутативна и ассоциативна. Нейтральным элементом является универсальное множество M:

$$A\cdot M=A\bigcap M=A$$

Умножение дистрибутивно относительно сложения, что опять рассмотрим лишь на диаграммах Эйлера-Венна.



Следовательно, $(P,\ +,\ \cdot\ )$ есть коммутативное кольцо с единицей. Пусть $S\subset M$. Тогда обе операции, очевидно, замкнуты в S и все приведенные выше рассуждения для *P(M)* применимы и к *P(S)*. То есть $(P(S),\ +,\ \cdot\ )$ подкольцо кольца $(P,\ +,\ \cdot\ )$. Более того указанное подкольцо является идеалом кольца $(P,\ +,\ \cdot\ )$. Действительно, пусть $T\subseteq S,\ A\subseteq M$, тогда $T\cdot A=T\cap A\subseteq T\subseteq S$

Задача 3. Пусть $(F,\ +,\ \cdot\ )$ кольцо действительных функций $f(x)$, определенных на всей числовой прямой с обычными операциями сложения и умножения и c – действительное число. Докажите, что отображение $\varphi\left(f(x)\right)=f(c)$ является гомоморфизмом кольца F на поле действительных чисел. Укажите ядро этого гомоморфизма *I*. Опишите смежные классы кольца F по идеалу *I*.

Решение. Пусть $f_1(x)$, $f_2(x)$ произвольные функции, принадлежащие F.

Тогда

$$\varphi(f_1(x)+f_2(x))=(f_1+f_2)(c)=f_1(c)+f_2(c)=\varphi(f_1(x))+\varphi(f_2(x)),$$
$$\varphi(f_1(x)\cdot f_2(x))=(f_1\cdot f_2)(c)=f_1(c)\cdot f_2(c)=\varphi(f_1(x))\cdot\varphi(f_2(x)).$$

Следовательно, φ – гомоморфизм кольца $(F,\ +,\ \cdot\ )$ на поле действительных чисел. Нейтральным элементом по сложению в поле действительных чисел является 0. Следовательно, ядром гомоморфизма в отображении φ будет множество $I=\{\,f(x)\in F \mid f(c)=0\,\}$. Пусть $f(x)$ произвольная функция из F. Смежный класс кольца F по идеалу I, порожденный элементом $f(x)$ содержит все функции из F, значения которых при $x=c$ равны $f(c)$.

Задача 4. Доказать, что фактор-кольцо $Z[\sqrt{2}]/3Z[\sqrt{2}]$ есть поле порядка девять.

Решение. Решение задачи 1 при $m=3$ дает фактор-кольцо порядка $3^2=9$.

В данном случае фактор-кольцо состоит из элементов

$I=3Z[\sqrt{2}]$, $1+I$, $2+I$, $1+\sqrt{2}+I$, $2+\sqrt{2}+I$, $\sqrt{2}+I$, $2\sqrt{2}+I$, $1+2\sqrt{2}+I$, $2+2\sqrt{2}+I$.

Докажем, что любой ненулевой элемент фактор-кольца имеет себе обратный. Для того чтобы найти элемент обратный к $a+b\sqrt{2}+I$ требуется решить уравнение $(a+b\sqrt{2}+I)(x+y\sqrt{2}+I)=1+I$. Это уравнение равносильно сравнению $(a+b\sqrt{2})(x+y\sqrt{2})\equiv 1 (\mathrm{mod}\, I)$, которое равносильно системе двух сравнений:

$$\begin{cases} ax+2by \equiv 1 \pmod 3 \\ bx+ay \equiv 0 \pmod 3 \end{cases} \tag{1}$$

Требуется показать, что если a или b не сравнимы с нулем по модулю 3, т.е. $a+b\sqrt{2}$ не принадлежит идеалу I, то система (1) имеет решение. Рассмотрим три возможных случая:

1) $a\equiv 0 \pmod 3$, $b\not\equiv 0 \pmod 3$
2) $a\not\equiv 0 \pmod 3$, $b\equiv 0 \pmod 3$
3) $a\not\equiv 0 \pmod 3$, $b\not\equiv 0 \pmod 3$

В первом случае второе сравнение системы принимает вид $bx\equiv 0 \pmod 3$, откуда $x\equiv 0 \pmod 3$. Тогда из первого сравнения получаем сравнение $2by \equiv 1 \pmod{3}$, которое имеет решение, так как НОД($2b$,3) = 1. Аналогично рассматривается второй случай. Из второго сравнения получаем $y \equiv 0 \pmod{3}$. Тогда из первого сравнения имеем $ax \equiv 1 \pmod{3}$. Последнее сравнение имеет решение, так как НОД(a, 3) = 1. В третьем случае умножим первое сравнение системы на b, второе сравнение – на a и почленно вычтем, исключая x. Получим:

$$(2b^2 - a^2)y \equiv b \pmod{3} \qquad (2),$$

где пара (a,b) может принимать следующие значения (1;1), (1;2), (2;1), (2;2). При всех указанных значениях по теореме Ферма $a^2 \equiv 1 \pmod{3}$, $b^2 \equiv 1 \pmod{3}$. Следовательно, сравнение (2) сводится к сравнению $y \equiv b \pmod{3}$. Подставляя найденное значение во второе сравнение системы (1) получаем сравнение $bx + ab \equiv 0 \pmod{3}$. Так как НОД($b$, 3) = 1, то $x \equiv -a \pmod{3}$.

Задача 5. Найти все идеалы кольца верхних треугольных матриц второго порядка с целыми элементами.

Решение. Так как все идеалы кольца целых чисел имеют вид mZ, где m – натуральное число, то рассмотрим множество $I = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \; a, b, c \in mZ \right\}$. Очевидно, что I замкнуто по сложению, умножению и взятию противоположного элемента, т.е. является подкольцом. При любых целых x, y, z и a, b, c кратных m, имеем:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \times \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay + bz \\ 0 & cz \end{pmatrix} \in I,$$

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \times \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} ax & bx + cy \\ 0 & cz \end{pmatrix} \in I$$

Получим, что множество I замкнуто относительно умножения слева и справа на элементы кольца. Следовательно, I есть идеал кольца верхних треугольных матриц второго порядка с целыми элементами. Рассмотрим далее множество

$$I_1 = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \; a \in mZ, \; b \in lZ, \; c \in nZ \right\},$$

где m, l, n – натуральные числа. Легко видеть, что множество I_1 также как и множество I, замкнуто по сложению, умножению и взятию противоположного элемента, то есть также является подкольцом. Пусть x, y, z – целые числа, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in I_1$, тогда $ax \in mZ$, $cz \in nZ$. Если НОД $(m, l) = d$ и $d = l$, то $ay + bz$ всегда принадлежит множеству lZ. Аналогично, если НОД$(n, l) = l$, то $bx + cy$ всегда принадлежит множеству lZ. Следовательно I_1 является идеалом кольца верхних треугольных матриц второго порядка с целыми элементами при условии, что $m \vdots l$, $n \vdots l$.

Домашнее задание

1. Исследовать алгебру $(M,+,\cdot)$ где $M = \{a + b\sqrt{3} \mid a, b \in Z\}$

2. Доказать, что фактор – кольцо $Z/7Z$ является полем.

3. Пусть $A = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| \ a, b \in Z \right\}$. Докажите, что отображение $\varphi : A \to Z$ такое, что $\varphi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix}\right) = a - b$ гомоморфизм колец. Укажите его ядро.

Дополнительные задачи

1. Доказать, если идеал кольца содержит обратимый элемент, то он совпадает со всем кольцом.

2. Пусть J идеал кольца K, I идеал кольца J. Верно ли, что I идеал кольца J?

3. Доказать, что фактор-кольцо кольца $R[x]$ многочленов с действительными коэффициентами по идеалу многочленов, делящихся на $x^2 + 1$, изоморфно полю комплексных чисел.

Занятие 2

ОТНОШЕНИЕ ДЕЛИМОСТИ В КОЛЬЦАХ. ОБЛАСТЬ ЦЕЛОСТНОСТИ

Вопросы к занятию

1. Отношение делимости в кольцах и его свойства.
2. Обратимые элементы кольца и классы ассоциированных элементов.
3. Делители нуля. Область целостности.
4. Поле частных области целостности.

Литература: [1], с. 439-446.

Образцы решения задач

Задача 1. Найти все обратимые элементы кольца целых гауссовых чисел $(\{ a+bi \mid a, b \in Z\}, +, \cdot)$.

Решение. ***I способ.*** Обозначим кольцо целых гауссовых чисел A. Пусть $a+bi \in A$. Элемент $x+iy$, принадлежащий кольцу A, будет обратным для $a+bi$ если $(a+bi)(x+iy)=1$. Приравнивая действительные и мнимые части комплексных чисел, стоящих в левой и правой частях последнего уравнения, получим систему уравнений

$$\begin{cases} ax-by=1 \\ ay+bx=0 \end{cases}$$

Решая ее, получим

$$\begin{cases} x=\dfrac{a}{a^2+b^2} \\ y=-\dfrac{b}{a^2+b^2} \end{cases}$$

Учитывая, что a и b целые числа заключаем, что x, y удовлетворяют неравенствам $-1 \le x \le 1$, $-1 \le y \le 1$. Так как x, y целые числа, то их возможные значения будут -1, 0, 1. Если $x = -1$, то $a = -1$, $b = 0$ и, следовательно, $y = 0$. Если $x = 0$. то $a = 0$ и $y = -\dfrac{1}{b}$. Откуда получаем, что $b= 1$ и $y = -1$ или $b = -1$, $y = 1$. Если $x = 1$, то $a = 1$, $b = 0$ и, следовательно, $y = 0$. Таким образом, обратимыми элементами кольца целых гауссовых чисел являются $1, -1, i, -i$.

II способ. Наиболее эффективным методом исследования свойств делимости в кольце является построение такого отображения кольца во множество натуральных чисел с нулем, при котором образ произведения равен произведению образов сомножителей. Такое отображение позволяет найти обратимые элементы кольца, а для факториальных колец и простые элементы кольца. Для любого элемента $a+bi$ кольца целых гауссовых чисел обозначим $N(a+bi)$ число a^2+b^2 и назовем нормой этого элемента. Проверим, что норма произведения равна произведению норм сомножителей. Действительно,

$$N((a+bi)(c+di)) = N(ac-bd+(ad+bc)i) = (ac-bd)^2+(ad+bc)^2 =$$

$$= a^2c^2-2abcd+b^2d^2+a^2d^2+2abcd+b^2c^2 = a^2(c^2+d^2)+b^2(c^2+d^2) =$$

$$= (a^2+b^2)(c^2+d^2) = N(a+bi)N(c+di)$$

Пусть элемент $c+di \in A$ является обратным для элемента $a+bi \in A$. Тогда $(a+bi)(c+di)=1$ и следовательно $N(a+bi)N(c+di)=1$. Так как $N(a+bi)$, $N(c+di)$ принадлежат множеству натуральных чисел с нулем, то $N(a+bi)=1$, $N(c+di)=1$. Можно показать и обратное. Если $a+bi \in A$ и $N(a+bi)=1$, то $a+bi$ обратим в кольце A. Действительно $N(a+bi)=(a+bi)(a-bi)=1$. Следовательно, элемент $a+bi$ имеет обратный $a-bi$, то есть, обратим в кольце A.

Таким образом, элемент $a+bi$ обратим в кольце целых гауссовых чисел тогда и только тогда когда $a^2+b^2=1$. Последнее равенство возможно лишь при $a = 1$, $b = 0$; $a = -1$, $b = 0$; $a = 0$, $b = 1$; $a = 0$, $b = -1$. Следовательно, обратимыми элементами кольца целых гауссовых чисел будут 1, -1, i, $-i$.

Задача 2. Доказать, что обратимый элемент коммутативного кольца с единицей не может быть делителем нуля.

Решение. Пусть $(K, +, \cdot)$ коммутативное кольцо с единицей e и a некоторый обратимый элемент кольца K. Следовательно существует элемент b, принадлежащий K, такой, что $a\cdot b = b\cdot a = e$. Предположим, что элемент a является делителем нуля в кольце K. Это означает, что $a \neq 0$ и существует элемент $c \neq 0$, принадлежащий кольцу K, такой, что

$$a\cdot c = 0 \qquad (1).$$

Домножим обе части равенства (1) слева на b. Получим $ba \cdot c = b \cdot 0$ или $e \cdot c = 0$, или $c = 0$. Но по предположению $c \neq 0$. Получили противоречие. Следовательно, наше предположение о том, что a является делителем нуля неверно, т.е. a не является делителем нуля.

Задача 3. Выясните, какие из ниже приведенных колец являются кольцами с делителями нуля:

а) Кольцо матриц вида

$$\begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & a_2 & 0 & \dots & 0 \\ 0 & 0 & a_3 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_n \end{pmatrix}$$

порядка $n \geq 2$ с действительными элементами относительно сложения и умножения матриц

б) Кольцо непрерывных функций на $[-1; 1]$ с обычными операциями сложения и умножения

в) Кольцо классов вычетов по модулю n, $n \in N$, $n \geq 2$.

г) Кольцо матриц вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ с рациональными a, b относительно операций сложения и умножения матриц.

д) Кольцо $(P, +, \cdot)$ из задачи 2 занятия 1.

е) Кольцо многочленов одной переменной с целыми коэффициентами, имеющих четные свободные члены относительно операций сложения и умножения многочленов.

ж) Кольцо матриц $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$ с действительными a, b, c, d где $i^2 = -1$, относительно операций сложения и умножения матриц.

Какие из указанных колец являются областями целостности ?

Решение. а) Рассмотрим матрицу A, у которой $a_1 = a_2 = \dots = a_k = 0$, $k < n$, а элементы a_{k+1}, a_{k+2}, ..., a_n отличны от нуля и матрицу B, у которой элементы a_1, a_2, ..., a_k отличны от нуля, а $a_{k+1} = a_{k+2} = \dots = a_n = 0$. Очевидно, что произведение $A \cdot B$ является нулевой матрицей n-го порядка, которая служит нулем данного кольца. Таким образом, матрицы A и B – делители нуля.

б) Нулем указанного кольца является непрерывная на $[-1;1]$ функция, принимающая значение 0 при любом значении аргумента. Рассмотрим функции $f_1(x)=\begin{cases}0, & x\le 0\\ x, & x>0\end{cases}$, $f_2(x)=\begin{cases}x, & x\le 0\\ 0, & x>0\end{cases}$. Произведение функций $f_1(x)\cdot f_2(x)$ принимает значение 0 при любом значении аргумента. Следовательно, функции $f_1(x)$, $f_2(x)$ являются делителями нуля.

в) Рассмотрим два возможных случая:

1. Число n является составным.

2. Число n является простым.

В первом случае $n=a\cdot b$, где $a,\ b\in N$, $1<a<n$, $1<b<n$. Следовательно $\overline{a}\cdot\overline{b}=\overline{0}$ и классы $\overline{a},\overline{b}$ отличны от класса $\overline{0}$. Таким образом классы $\overline{a},\overline{b}$ – делители нуля. Покажем, что во втором случае любой ненулевой элемент кольца является обратимым. Единицей кольца класса вычетов является класс $\overline{1}$. Пусть $\overline{a}$ произвольный не нулевой класс вычетов. Рассмотрим уравнение

$$\overline{a}\cdot\overline{x}=\overline{1}\quad, \tag{2}$$

которое равносильно сравнению

$$ax\equiv 1\ (\mathrm{mod}\ \ n) \tag{3}$$

Так как $НОД(a,n)=1$, то сравнение (3), а, следовательно, и уравнение (2) имеют решения. Учитывая, что кольцо классов вычетов коммутативно, и используя задачу 2 , заключаем, что при простом n указанное кольцо не содержит делителей нуля.

г) Рассмотрим произвольную не нулевую матрицу $\begin{pmatrix}a & b\\ 2b & a\end{pmatrix}$ с рациональными a и b. Ее определитель равен a^2-2b^2 и отличен от нуля. Нулем указанного кольца является нулевая матрица $\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$. Так как определитель произведения матриц равен произведению определителей сомножителей, то произведение двух ненулевых матриц вида $\begin{pmatrix}a & b\\ 2b & a\end{pmatrix}$ с рациональными a и b является невырожденной матрицей и следовательно не может быть нулевой матрицей. Таким образом, указанное кольцо не содержит делителей нуля.

д) Нулем кольца $(P, +, \cdot)$ является $\varnothing$. Пусть A непустое собственное подмножество множества M, тогда его дополнение $\overline{A}$ также не пусто и $A \cdot \overline{A} = A \cap \overline{A} = \varnothing$. Следовательно, кольцо $(P, +, \cdot)$ обладает делителями нуля.

е) Пусть $f_1(x)$, $f_2(x)$ ненулевые многочлены одной переменной с целыми коэффициентами, имеющие четные свободные члены. Если степень хотя бы одного из многочленов $f_1(x)$ или $f_2(x)$ положительна, то многочлен $f_3(x) = f_1(x) \cdot f_2(x)$ имеет положительную степень и, следовательно, не может быть нулевым многочленом. Если же многочлены $f_1(x)$ и $f_2(x)$ имеют нулевую степень, то, учитывая, что кольцо $(2Z, +, \cdot)$ не содержит делителей нуля, также заключаем, что их произведение не является нулевым многочленом. Таким образом, указанное кольцо не обладает делителями нуля.

ж) Так как произвольная ненулевая матрица $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$, где $a, b, c, d \in R$, $i^2 = -1$, является невырожденной, то, как и в пункте г) заключаем, что указанное кольцо матриц не содержит делителей нуля.

Поскольку кольца из пунктов а), б), д) и кольцо классов вычетов по составленному модулю содержат делители нуля, то они не являются областями целостности.

Кольцо классов вычетов по простому модулю коммутативно, поскольку коммутативно кольцо целых чисел. Единицей этого кольца является класс $\overline{1}$. Следовательно, кольцо классов вычетов по простому модулю является областью целостности.

Кольцо матриц вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ с рациональными a и b коммутативно. Действительно,

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

Единицей указанного кольца служит единичная матрица $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Следовательно, это кольцо является областью целостности.

Кольцо многочленов одной переменной с целыми коэффициентами, имеющих четные свободные члены с операциями сложения и умножения многочленов и кольцо матриц $\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$, где a, b, c, d действительные числа, $i^2=-1$ с операциями сложения и умножения матриц областями целостности не являются. Поскольку первое из них не содержит единицы, а второе – некоммутативно. Действительно

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \cdot \begin{pmatrix} a_1+b_1 i & c_1+d_1 i \\ -c_1+d_1 i & a_1-b_1 i \end{pmatrix} =$$

$$= \begin{pmatrix} aa_1-bb_1-cc_1-dd_1+i(ab_1+a_1b+cd_1-c_1d) & ac_1-bd_1+ca_1+db_1+i(ad_1+bc_1-cb_1+da_1) \\ -ca_1-db_1-ac_1+bd_1+i(-cb_1+da_1+ad_1+bc_1) & -cc_1-dd_1+aa_1-bb_1+i(-cd_1+dc_1-ab_1-a_1b) \end{pmatrix}$$

$$\begin{pmatrix} a_1+b_1 i & c_1+d_1 i \\ -c_1+d_1 i & a_1-b_1 i \end{pmatrix} \cdot \begin{pmatrix} a+b\,i & c+d\,i \\ -c+d\,i & a-b\,i \end{pmatrix} =$$

$$= \begin{pmatrix} aa_1-bb_1-cc_1-dd_1+i(a_1b+ab_1-cd_1+c_1d) & ac_1+bd_1+ca_1-db_1+i(ad_1-bc_1+cb_1+da_1) \\ -a_1c+db_1-ac_1-bd_1+i(cb_1+da_1+ad_1-bc_1) & -cc_1-dd_1+aa_1-bb_1+i(cd_1-dc_1-ab_1-a_1b) \end{pmatrix}$$

Домашнее задание

1. Докажите, что в кольце $(\{a+b\sqrt{2} \mid a,\ b\in Z\},\ +,\cdot\ )$ существует бесконечно много обратимых элементов.

2. Докажите, что в кольце квадратных матриц порядка n с элементами из некоторого поля с операциями сложения и умножения матриц вырожденные матрицы, и только они , являются делителями нуля.

3. Верно ли , что в коммутативном кольце с единицей всякий элемент, который не является делителем нуля, обратим?

Дополнительные задачи

1. Пусть R кольцо с единицей 1, S его подкольцо.

a) Верно ли, что $1\in S$?

b) Может ли подкольцо S иметь единицу e, отличную от 1?

2.Пусть R и S кольца с единицей, $\varphi : R \to S$ – гомоморфизм. Верно ли, что образ единицы кольца R является единицей кольца S?

3. Верно ли, что гомоморфный образ области целостности является областью целостности?

4.Решите задачу 3 из домашнего задания, если кольцо конечно.

5.Найдите все обратимые элементы кольца
$(\{ a+b\sqrt{2} \mid a,\ b \in Z\},\ +,\ \cdot\ )$.

Занятие 3

СРАВНЕНИЕ ПО ИДЕАЛУ. ОПЕРАЦИИ НАД ИДЕАЛАМИ

Вопросы к занятию:

1. Идеалы, порожденные подмножествами.
2. Сравнения по идеалу.
3. Пересечение идеалов.
4. Сумма идеалов.
5. Произведение идеалов.
6. Частное идеалов.

Литература: [1], с. 431-433.

Образцы решения задач

Задача 1. В кольце целых чисел найдите: 1) $\langle 3\rangle+\langle 4\rangle$; 2) $\langle 3\rangle\bigcap\langle 4\rangle$; 3) $\langle 3\rangle\cdot\langle 4\rangle$; 4) $\langle 4\rangle:\langle 6\rangle$.

Решение. 1) Идеал $\langle 3\rangle$ представляет собой множество целых чисел кратных 3, $\langle 3\rangle=\{\,3k \mid k\in Z\,\}$, аналогично $\langle 4\rangle=\{\,4t \mid t\in Z\,\}$. Тогда $\langle 3\rangle+\langle 4\rangle=\{\,3k+4t \mid k,t\in Z\,\}$.

Так как единица принадлежит множеству $\langle 3\rangle+\langle 4\rangle$, то $\langle 3\rangle+\langle 4\rangle=\langle 1\rangle=Z$.

2) Пересечением множеств $\{\,3k \mid k\in Z\,\}$ и $\{\,4t \mid t\in Z\,\}$ является множество $\{\,12n \mid n\in Z\,\}$. Следовательно, $\langle 3\rangle\bigcap\langle 4\rangle=\langle 12\rangle$.

3) $\langle 3\rangle\cdot\langle 4\rangle=\{\,3k\cdot 4t \mid k,t\in Z\,\}=\{\,12kt \mid k,t\in Z\,\}=\{\,12n \mid n\in Z\,\}$. Таким образом, $\langle 3\rangle\cdot\langle 4\rangle=\langle 12\rangle$.

4) $\langle 6\rangle=\{\,6l \mid l\in Z\,\}$. Тогда
$\langle 4\rangle:\langle 6\rangle=\{\,n\in Z \mid n\cdot\langle 6\rangle\subset\langle 4\rangle\,\}=\{\,n\in Z \mid n\cdot 6k=4t,\ k,\ t\in Z\,\}$.

Следовательно, n любое четное число. Таким образом, $\langle 4\rangle:\langle 6\rangle=\langle 2\rangle$.

Задача 2. Проверить, являются ли в кольце многочленов с целыми коэффициентами $Z[x]$ сравнимыми по идеалу $I = \langle x,2 \rangle$ элементы $f(x) = x^2 + 3x + 4$ и $g(x) = x + 2$.

Решение. Многочлены *f(x)* и *g(x)* сравнимы по идеалу I, если их разность принадлежит этому идеалу. Так как

$$I = \langle x, 2 \rangle = \left\{ x \cdot \varphi(x) + 2 \cdot h(x) \;\middle|\; \varphi(x), h(x) \in Z[x] \right\},$$

то

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

Следовательно, $x^2 + 3x + 4 \equiv x + 2 \pmod{I}$.

Задача 3. Пусть $K = \left\{ a + bi\sqrt{3} \;\middle|\; a, b \in Z \right\}$, $I_1 = \langle 2 \rangle$, $I_2 = \langle 1 + i\sqrt{3} \rangle$ – идеалы кольца $(K, +, \cdot)$. Верно ли, что $I_1 + I_2 = K$?

Решение. Обозначим сумму $I_1 + I_2$ через I. Тогда

$$I = \left\{ 2(a + bi\sqrt{3}) + (1 + i\sqrt{3})(c + di\sqrt{3}) \;\middle|\; a, b, c, d \in Z \right\} =$$

$$= \left\{ (2a + c - 3d) + (2b + c + d)i\sqrt{3} \;\middle|\; a, b, c, d \in Z \right\}$$

Поскольку кольцо K можно рассматривать как идеал, порожденный числом 1, то выясним, принадлежит ли 1 идеалу I. Для этого решим в целых числах систему уравнений:

$$\begin{cases} 2a + c - 3d = 1 \\ 2b + c + d = 0 \end{cases} \qquad (1)$$

Если система (1) имеет решение в целых числах, то $1 \in I$, если же не имеет, то $1 \notin I$.

От системы уравнений (1) перейдем к системе сравнений по модулю 2:

$$\begin{cases} c - 3d \equiv 1 \pmod 2 \\ c + d \equiv 0 \pmod 2 \end{cases} \qquad (2)$$

Почленно вычитая из второго сравнения первое, получим:

$$4d \equiv -1 \pmod 2 \qquad (3)$$

Сравнение (3) не имеет решений в целых числах и, следовательно, $1 \notin I$, т.е. равенство $I_1 + I_2 = K$ не верно.

Задача 4. Пусть I сумма идеалов I_1 и I_2. Причем любой элемент $x \in \mathrm{I}$ единственным образом представляется в виде $x = x_1 + x_2$, где $x_1 \in \mathrm{I}_1$, $x_2 \in \mathrm{I}_2$. В этом случае сумма называется прямой. Докажите, что $\mathrm{I}_1 \bigcap \mathrm{I}_2 = \{0\}$.

Решение. Пусть $\mathrm{I}_3 = \mathrm{I}_1 \bigcap \mathrm{I}_2$ и y – произвольный элемент из I_3. Так как I_3 является идеалом, то $-y \in \mathrm{I}_3$. Следовательно, $0 = -y + y$. Учитывая, что сумма идеалов I_1 и I_2 прямая, имеем $y = 0$. В силу произвольности выбора y заключаем, что $\mathrm{I}_1 \bigcap \mathrm{I}_2 = \{0\}$.

Домашнее задание

1. Пусть I_1, I_2 идеалы кольца K. Докажите, что если $\mathrm{I}_1 : \mathrm{I}_2 = \mathrm{K}$, то $\mathrm{I}_2 \subset \mathrm{I}_1$.

2. Пусть $\mathrm{I} = \mathrm{I}_1 + \mathrm{I}_2$ – сумма идеалов I_1 и I_2 и $\mathrm{I}_1 \bigcap \mathrm{I}_2 = \{0\}$. Верно ли, что сумма I_1 и I_2 является прямой?

Дополнительные задачи

1. Доказать, что если $\mathrm{I} = \mathrm{I}_1 + \mathrm{I}_2$ – прямая сумма идеалов I_1, I_2, то произведение любого элемента из I_1 на любой элемент из I_2 равно нулю.

2. Пусть $\mathrm{I} = \langle \mathrm{p} \rangle$, где p – простое число, идеал кольца целых гауссовых чисел A. Найдите условие, при котором фактор-кольцо A/I содержит делители нуля.

Занятие 4

ФАКТОРИАЛЬНЫЕ КОЛЬЦА

Вопросы к занятию:

1. Неразложимые элементы кольца.
2. Простые элементы кольца и их неразложимость.
3. Факториальные кольца.
4. Критерий факториального кольца.

Литература: [1], с. 446-447, 450, [3], с. 93-95.

Образцы решения задач

Задача 1. Доказать, что из равенства $2\cdot 3=(\sqrt{6}\cdot i)\cdot(-\sqrt{6}\cdot i)$ следует, что кольцо $\left(\left\{ a+bi\sqrt{6} \mid a,b\in Z\right\}, +, \cdot\right)$ не является факториальным.

Решение. Для доказательства данного утверждения требуется показать, что элементы $2, 3, \sqrt{6}i, -\sqrt{6}i$ неразложимы в кольце $\left(\left\{a+bi\sqrt{6}, a,b\in Z\right\}, +,\cdot\right)$, которое обозначим K, а также, что числа 2 и 3 неассоциированы ни с одним из чисел $\sqrt{6}i$ и $-\sqrt{6}i$ в указанном кольце. Предположим, что элемент 2 разложим в кольце K. Тогда

$$2=\alpha\cdot\beta \qquad (1)$$

где числа α, β принадлежат кольцу K, и ни одно из них не является в K обратимым элементом.

Аналогично, как и в задаче 1 из занятия 2 введем понятие нормы элемента кольца K. Пусть $x+iy\sqrt{6}\in K$, тогда

$$N\left(x+iy\sqrt{6}\right)=x^2+6y^2$$

Следовательно, из (1) имеем $N(2)=N(\alpha)\cdot N(\beta)$ или

$$4=N(\alpha)\cdot N(\beta) \qquad (2)$$

Пусть $\alpha=a+bi\sqrt{6}$, $\beta=c+di\sqrt{6}$, тогда $N(\alpha)=a^2+6b^2$, $N(\beta)=c^2+6d^2$.

Учитывая , что $N(\alpha)\geq 0$, $N(\beta)\geq 0$ и $N(\alpha)$и $N(\beta)$ целые числа из (2) получаем, что $N(\alpha)=1$, $N(\beta)=4$, или $N(\alpha)=4$, $N(\beta)=1$, или $N(\alpha)=2$, $N(\beta)=2$.

Если $N(\alpha)=1$, или $N(\beta)=1$, то α или β обратимые элементы кольца K, что противоречит выбору элементов α и β. Следовательно, $N(\alpha)=2$ и $N(\beta)=2$. Тогда $a^2+6b^2=2$, но последнее уравнение не имеет решений в целых числах. Таким образом, в кольце K нет элементов с нормой 2. Следовательно, элемент 2 неразложим в кольце K.

Аналогично показывается, что элементы $3, \sqrt{6}i, -\sqrt{6}i$ также неразложимы в кольце K.

Для того чтобы показать, что элементы 2 и 3 неассоциированы ни с одним из чисел $\sqrt{6}$ и $-\sqrt{6}i$ необходимо найти обратимые элементы кольца K. Пусть e обратимый элемент кольца K. Тогда существует элемент $e' \in K$, такой, что $e \cdot e' = 1$. Следовательно,

$$N(e) \cdot N(e') = N(1)$$

или

$$N(e) \cdot N(e') = 1 \tag{3}$$

Из (3) получаем, что $N(e)=1$.

Пусть $e = x + i\sqrt{6}y$, тогда

$$x^2 + 6y^2 = 1 \tag{4}$$

Решениями уравнения (4) в целых числах будут x = 1, y = 0 и x = -1, y = 0. В результате получим, что обратимыми элементами кольца K будут числа 1,-1. Следовательно, 2 и 3 неассоциированы ни с одним из чисел $\sqrt{6}i$ и $-\sqrt{6}i$.

Задача 2. Проверить, является ли в кольце $\left(\left\{ a+bi\sqrt{17} \mid a,b \in Z \right\},+,\cdot\right)$ элемент a^2+17b^2 а) неразложимым; б) простым. Выясните, является ли указанное кольцо факториальным.

Решение. Обозначим указанное кольцо K. а) определим норму элемента $a+bi\sqrt{17} \in K$, как a^2+17b^2. Предположим, что элемент $1+i\sqrt{17}$ разложим в кольце K, тогда в кольце K существуют необратимые элементы α и β, такие что $1+i\sqrt{17} = \alpha \cdot \beta$. Или, переходя к нормам получаем

$$18 = N(\alpha) \cdot N(\beta)$$

Следовательно, $N(\alpha)=2, N(\beta)=9$ или $N(\alpha)=3, N(\beta)=6$ или наоборот. Так уравнения $a^2+17b^2=2$ и $a^2+17b^2=3$ не имеют решений в целых числах, то в кольце К не существует элементов с нормой 2 или 3 и элемент $1+i\sqrt{17}$ неразложим в К.

б) $N\left(1+i\sqrt{17}\right)=18$, с другой стороны $18=\left(1+i\sqrt{17}\right)\cdot\left(1-i\sqrt{17}\right)$. То есть 18 делится на $1+i\sqrt{17}$ в кольце К. Так как $18=3\cdot 6$, то проверим, делит ли $1+i\sqrt{17}$ элементы 3 и 6 в кольце К.

$$3:\left(1+i\sqrt{17}\right)=\frac{3\left(1-i\sqrt{17}\right)}{18}=\frac{1}{6}-\frac{1}{6}i\sqrt{17},$$

$$6:\left(1+i\sqrt{17}\right)=\frac{6\left(1-i\sqrt{17}\right)}{18}=\frac{1}{3}-\frac{1}{3}i\sqrt{17}$$

Поскольку числа $\frac{1}{6}-\frac{1}{6}i\sqrt{17}$ и $\frac{1}{3}-\frac{1}{3}i\sqrt{17}$ не принадлежат кольцу К, то элемент $1+i\sqrt{17}$ не делит элементы 3 и 6 и, следовательно, не является простым.

Кольцо является факториальным тогда и только тогда, когда любой его неразложимый элемент является простым. Из пунктов а) и б) заключаем, что кольцо К не факториально.

Задача 3. Используя тот факт, что кольцо целых гауссовых чисел А факториально, найти все его простые элементы.

Решение. Так как кольцо целых гауссовых чисел А факториально, то нет необходимости различать неразложимые и простые элементы. Будем называть их гауссовыми простыми. Прежде чем перейти к нахождения гауссовых простых чисел докажем вначале два вспомогательных утверждения.

1) Если α – произвольное гауссово целое число и $N(\alpha)$ – рациональное простое число, то α – гауссово простое число.

Действительно, если $\alpha=\beta\cdot\gamma$ для некоторых гауссовых целых β, γ, то $N(\alpha)=N(\beta)\cdot N(\gamma)$. Тогда либо $N(\beta)$, либо $N(\gamma)$ равна 1. Следовательно, либо β, либо γ является обратимым элементом в кольце А. Тогда элемент α неразложим и является гауссовым простым числом.

2) Каждое гауссово простое число π делит в точности одно рациональное простое число р.

Действительно, так как π делит $N(\pi)$, то существует наименьшее положительное рациональное простое число р, что π делит р. При этом р является рациональным простым, так как если бы $p = m \cdot n$, где m, n-целые числа, то в силу того, что π – гауссово простое получили бы, что π делит m или π делит n. Поэтому из свойства минимальности р следует, что либо m, либо n равно 1.

Простое число р единственно, так как если p' – другое рациональное простое число, то существуют целые числа a и a', такие что $ap + a'p' = 1$. Тогда если π делит р и p', то π делит 1,что невозможно.

Перейдем теперь к нахождению гауссовых простых чисел. Пусть р-некоторое простое рациональное число, тогда по утверждению 2 р делится на некоторое гауссово простое число π, и, следовательно, $p = \pi \cdot \lambda$ для некоторого гауссова целого числа λ. Отсюда получаем

$$N(\pi) \cdot N(\lambda) = N(p) = p^2 .$$

Если $N(\lambda) = 1$, то λ – обратимый элемент кольца A и р- число, ассоциированное с π. Если $N(\lambda) = p$, то $N(\pi) = p$ и λ и π – гауссовы простые числа по утверждению 1.

Пусть $\pi = x + iy, \ x, \ y \in Z, \ N(\pi) = x^2 + y^2 = p$. Последнее уравнение равносильно сравнению

$$x^2 \equiv -y^2 (\text{mod } p) \tag{1}$$

Сравнение (1) имеет решение, если – 1 является квадратичным вычетом по модулю р. Так как $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$, то -1 является квадратичным вычетом для $p \equiv 1 \ (\text{mod } 4)$. Следовательно, случай $N(\lambda) = 1, \ N(\pi) = p^2$ реализуется для $p \equiv 3 \ (\text{mod } 4)$.

Осталось рассмотреть случай р = 2. Для р = 2 имеем $2 = (1+i) \cdot (1-i)$. Здесь $1+i, \ 1-i$ гауссовы простые и, кроме того, ассоциированные. Объединяя все рассуждения, находим, что все гауссовы простые числа задаются рациональными простыми р, для которых $p \equiv 3 \ (\text{mod } 4)$, множителями π и π' в представлении $p = \pi \cdot \pi'$, соответствующем простым p, для которых $p \equiv 1 \pmod 4$ и числом $1 + i$ вместе со всеми ассоциированными с ними, получающимися умножением на ± 1, $\pm i$.

Домашнее задание

1. Следует ли из равенства $(1+\sqrt{5})\cdot(-1+\sqrt{5}) = 2\cdot 2$, что кольцо $(\{a+b\sqrt{5} \mid a, b \in Z\}, +, \cdot)$ не является факториальным ?

2. Является ли элемент $4+\sqrt{10}$ в кольце $(\{a+b\sqrt{10} \mid a, b \in Z\}, +, \cdot)$

а) неразложимым,

б) простым ?

Дополнительные задачи

1. Доказать, что существует бесконечно много неразложимых элементов в кольце $(\{a+b\sqrt{d} \mid a, b \in Z\}, +, \cdot)$, где $d \equiv 2,3 \pmod 4$, d не делится на квадрат натурального числа большего 1.

2. Учитывая тот факт, что кольцо $(\{a+b\sqrt{2} \mid a, b \in Z\}, +, \cdot)$ факториально найдите все его простые элементы.

3. Показать, что если π – гауссово простое число, то ряд $1, 2, \ldots, N(\pi)$ образует полную систему вычетов по модулю π, то есть показать, что ни одна из разностей не делится на π.

Занятие 5

КОЛЬЦА ГЛАВНЫХ ИДЕАЛОВ

Вопросы к занятию:

1. Главный идеал и его свойства.
2. Кольцо главных идеалов.
3. Делимость в кольце главных идеалов.
4. Факториальность кольца главных идеалов.

Литература: [1], с. 431, 448 - 451, 453 - 458.

Образцы решения задач

Задача 1. Выяснить, какие из идеалов в указанных кольцах являются главными.

а) Идеал $\mathrm{I} = \left\{ a + bi \;\middle|\; a, b \in 3\mathrm{Z} \right\}$ в кольце целых гауссовых чисел A.

б) Идеал $\mathrm{I} = \langle x, 2 \rangle$ в кольце многочленов переменной x с целыми коэффициентами.

в) Идеал $\mathrm{I} = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \;\middle|\; a \in Z \right\}$ в кольце $(A, +, \cdot)$, где $A = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathrm{Z} \right\}$.

г) Идеал $\mathrm{P}(S)$ в кольце $(\mathrm{P}(M), +, \cdot)$, $S \subset M$, где алгебра $(\mathrm{P}(M), +, \cdot)$ определена в задаче 2 из занятия 1.

Решение. а) Любой элемент идеала I может быть представлен в виде $3 \cdot (a + bi)$, где $a, b \in \mathrm{Z}$. Следовательно, I – главный идеал, порожденный элементом 3.

б) Так как элементы x и 2 неразложимы в кольце целочисленных многочленов, то их общим делителем в указанном кольце может быть только обратимый элемент. Следовательно, идеал I может быть главным идеалом только в том случае, когда I совпадает со всем кольцом.

Пусть $f(x)$ – произвольный многочлен идеала I, тогда

$$f(x) = x \cdot \varphi(x) + 2 \cdot g(x) \qquad (1)$$

где $\varphi(x)$, $g(x)$ – целочисленные многочлены. Из (1) получаем, что многочлен $f(x)$ имеет четный свободный член. Следовательно, целочисленные многочлены, имеющие нечетные свободные члены, не принадлежат идеалу I, и идеал I не является главным.

в) Легко проверить, что кольцо **A** коммутативно. Тогда любой элемент $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$, где $a \in Z$, идеала I можно представить в виде

$\begin{pmatrix} a & a \\ a & a \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in \mathbf{A}$. Следовательно, I - главный идеал, порожденный элементом $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

г) Так как $S \subset M$, то любое подмножество S можно рассматривать как пересечение множества S и некоторого подмножества множества M. Следовательно, $\mathrm{P}(S) = S \cdot \mathrm{P}(M)$, любой идеал $\mathrm{P}(S)$ является главным идеалом, порожденным множеством S.

Задача 2. Доказать, что кольцо $\left(\{a+bi\sqrt{5} \mid a,b\in Z\}, +, \cdot\right)$ не является кольцом главных идеалов.

Решение. Обозначим данное кольцо K.

I способ

Нетрудно заметить, что

$$\left(1+i\sqrt{5}\right)\cdot\left(1-i\sqrt{5}\right) = 2\cdot 3 \qquad (2)$$

Вводя для любого элемента $a+bi\sqrt{5}$ кольца K понятие нормы $\mathrm{N}\left(a+bi\sqrt{5}\right) = a^2+5b^2$ можно доказать, как в задаче 1 из занятия 4, что элементы $1+i\sqrt{5}$, $1-i\sqrt{5}$, 2, 3 неразложимы в кольце K и ни один из элементов $1+i\sqrt{5}$, $1-i\sqrt{5}$ неассоциирован с элементами 2 или 3. Тогда из равенства (2) следует, что кольцо K не является факториальным и, следовательно, не является кольцом главных идеалов.

II способ

Доказав, что элементы $1+i\sqrt{5}$ и 2 неразложимы в кольце K, рассмотрим идеал, $\mathrm{I} = \left\langle 2,\ 1+i\sqrt{5}\right\rangle$. Так как элементы $1+i\sqrt{5}$ и 2 неразложимы в кольце K, то их общим делителем в K может быть только обратимый элемент этого кольца. Следовательно, I будет главным идеалом лишь в том случае, когда I совпадает со всем кольцом. Покажем, что I не содержит 1. По определению идеала, порожденного подмножеством, имеем:

$$\mathrm{I} = \left\{ 2\left(a + bi\sqrt{5}\right) + \left(1 + i\sqrt{5}\right)\cdot\left(c + di\sqrt{5}\right) \middle| \quad a, b, c, d \in \mathrm{Z} \right\} =$$
$$= \left\{ \left(2a + c - 5d\right) + \left(2b + c + d\right)i\sqrt{5} \;\middle|\; a, b, c, d \in \mathrm{Z} \right\}.$$

1 не принадлежит I, если система уравнений

$$\begin{cases} 2a + c - 5d = 1 \\ 2b + c + d = 0 \end{cases} \tag{3}$$

не имеет решений в целых числах.

Вычитая из первого уравнения системы второе, получим уравнение

$$2a - 2b - 6d = 1 \tag{4}$$

Уравнение (4) не имеет решений в целых числах и, следовательно, 1 не принадлежит I. Таким образом кольцо K не является кольцом главных идеалов.

Задача 3. Доказать, что кольцо A целых гауссовых чисел является кольцом главных идеалов.

Решение. Пусть I – некоторый ненулевой идеал кольца целых гауссовых чисел и β – ненулевой элемент из I, имеющий наименьшую норму. Покажем, что β – порождающий элемент идеала I. Пусть $\alpha \in \mathrm{I}$, тогда $\dfrac{\alpha}{\beta} = u + vi$, где u, v – рациональные числа. Обозначим через x, y ближайшие целые числа к u и v соответственно. Положим $r=u-x$, $s=v-y$. Тогда

$$|r| \le \frac{1}{2},\ |s| \le \frac{1}{2} \tag{5}$$

Пусть $\gamma = x + iy$. Тогда

$$\alpha = \beta(u + vi) = \beta\left(x + r + (y + s)i\right) = \beta\gamma + \delta \tag{6}$$

где $\delta = \beta(r + si)$.

Отсюда $N(\delta)=N(\beta)(r^2+s^2)$. Учитывая (5) получаем, что $N(\delta)<N(\beta)$. Далее $\delta=\alpha-\beta\gamma$ принадлежит I. Следовательно, исходя из выбора элемента β, имеем, что $\delta=0$. Тогда из (6) получаем $\alpha=\beta\cdot\gamma$, где $\gamma\in A$, т.е. идеал I - главный с порождающим элементом β.

Домашнее задание

1. Является ли идеал $I=\left\{\left.\begin{pmatrix}0&b&c\\0&0&b\\0&0&0\end{pmatrix}\right| b,c\in Z\right\}$ главным в кольце

$$\left(\left\{\left.\begin{pmatrix}a&b&c\\0&a&b\\0&0&a\end{pmatrix}\right| a,b,c\in Z\right\},+,\cdot\right)?$$

2. Докажите, что кольцо $\left(\left\{a+b\sqrt{2}\mid a,b\in Z\right\},+,\cdot\right)$ является кольцом главных идеалов.

Дополнительные задачи

1. Является ли в кольце функций непрерывных на отрезке [-1;1] главным идеалом множество таких функций g, что $g(\frac{1}{2})=0$?

2. Доказать, что любое кольцо, заключенное между кольцом главных идеалов K и его полем частных P, само является кольцом главных идеалов.

3. Докажите, что кольцо $\left(\left\{\frac{a}{2}+\frac{b}{2}\sqrt{5}\mid a,b\in Z,\ a\equiv b\,(\mathrm{mod}\,2)\right\},+,\cdot\right)$ является кольцом главных идеалов.

Занятие 6

ЕВКЛИДОВЫ КОЛЬЦА

Вопросы к занятию:

1. Определение евклидова кольца, примеры евклидовых колец.
2. Евклидово кольцо как кольцо главных идеалов.

Литература: [1], с. 451 - 453.

Образцы решения задач

Задача 1. Докажите, что кольцо $\left(\left\{a+b\sqrt{3} \mid a,b\in Z\right\},+,\cdot\right)$ является евклидовым кольцом.

Решение: При доказательстве, что кольца квадратичных полей $\left(\left\{a+b\sqrt{d} \mid a,b\in Q\right\},+,\cdot\right)$, где d – целое число, свободное от квадратов, являются евклидовыми, отображение f задается следующим образом. Для каждого элемента $a+b\sqrt{d}$ имеем

$$f\left(a+b\sqrt{d}\right)=\left|\,N\left(a+b\sqrt{d}\right)\right|=\left|\,a^2-db^2\,\right|.$$

Обозначим данное кольцо K и для любого $a+b\sqrt{3}\in K$ положим $f\left(a+b\sqrt{3}\right)=\left|\,N\left(a+b\sqrt{3}\right)\right|$, где $N\left(a+b\sqrt{3}\right)=a^2-3b^2$ – норма элемента $a+b\sqrt{3}$. Рассмотрим произвольные элементы α, β, где $\beta\neq 0$, кольца K. Тогда $\dfrac{\alpha}{\beta}=u+v\sqrt{3}$, для некоторых рациональных u, v. Пусть x, y ближайшие целые числа к u и v соответственно. Положим $r=u-x,\ s=v-y$. Тогда, $|r|\le\dfrac{1}{2},\ |s|\le\dfrac{1}{2}$. Пусть $\delta=x+y\sqrt{3}$. Тогда $\alpha=\beta\left(u+v\sqrt{3}\right)=\beta\left(x+r+(y+1)\sqrt{3}\right)=\beta\gamma+\delta$, где $\delta=\beta\left(r+s\sqrt{3}\right)$. Отсюда $N(\delta)=N(\beta)\cdot\left(r^2-3s^2\right)$. Следовательно, $|\,N(\delta)\,|<|\,N(\beta)\,|$ так как $\left|\,r^2-3s^2\,\right|\le\max\left(r^2,3s^2\right)\le\dfrac{3}{4}$. Этим евклидовость кольца K доказана.

Задача 2. Доказать, что кольцо $\left(\left\{\frac{a}{2}+\frac{b}{2}i\sqrt{3}\ \middle|\ a,b\in Z,\quad a\equiv b(\bmod 2)\right\},\ +,\ \cdot\ \right)$ является евклидовым кольцом.

Решение. Обозначим данное кольцо K и положим $f\left(\frac{a}{2}+\frac{bi\sqrt{3}}{2}\right)=\left|N\left(\frac{a}{2}+\frac{bi\sqrt{3}}{2}\right)\right|=\frac{a^2}{4}+\frac{3b^2}{4}$, где $N\left(\frac{a}{2}+\frac{bi\sqrt{3}}{2}\right)$ норма элемента $\frac{a}{2}+\frac{bi\sqrt{3}}{2}$. Пусть α и β – элементы кольца K и $\beta\neq 0$. Тогда $\frac{\alpha}{\beta}=u+vi\sqrt{3}$, где $u,\ v$ рациональные числа.

Пусть y – ближайшее целое число к числу $2v$, x – ближайшее целое число к числу $u-\frac{1}{2}y$. Положим $r=u-\frac{1}{2}y-x,\ s=v-\frac{1}{2}y$. Тогда

$$|r|\leq\frac{1}{2},\ |s|\leq\frac{1}{4}.$$

Пусть $\gamma=x+\frac{1}{2}y\left(1+i\sqrt{3}\right)$, тогда

$$\alpha=\beta\left(u+vi\sqrt{3}\right)=\beta\left(x+\frac{1}{2}y+r+\left(\frac{1}{2}y+s\right)i\sqrt{3}\right)=\beta\gamma+\delta,$$

где $\delta=\beta\left(r+si\sqrt{3}\right)$.

Отсюда имеем

$$|\,N(\delta)\,|=N(\delta)=N(\beta)\cdot\left(r^2+3s^2\right)\leq N(\beta)\cdot\frac{7}{16}<N(\beta)=|\,N(\beta)\,|$$

Следовательно, кольцо К евклидово.

Задача 3. Докажите, что кольцо $\left(\left\{a+bi\sqrt{13} \mid a,b\in Z\right\} +, \cdot\right)$ не является евклидовым.

Решение. Обозначим данное кольцо K и зададим отображение f как в задачах 1, 2. Пусть f отображает каждый элемент кольца K на модуль его нормы:

$$a+bi\sqrt{13} \xrightarrow{f} \left|\,N\left(a+bi\sqrt{13}\right)\right| = a^2+13b^2 .$$

Предположим, что кольцо K евклидово. Тогда для элементов $i\sqrt{13}, 2\in K$ имеем:

$$i\sqrt{13} = 2\gamma+\delta,\ \left|\,N(\delta)\right| < \left|\,N(2)\right| = 4 \text{ и } \gamma,\ \delta\in K .$$

Пусть $\gamma = x+yi\sqrt{13},\ \delta = x'+iy'\sqrt{13}$, тогда x, y, x', y' целые числа. Следовательно, получаем

$$i\sqrt{13} = 2\left(x+yi\sqrt{13}\right)+x'+y'i\sqrt{13} \qquad (1)$$

Из (1) имеем

$$2x+x'=0,\ 2y+y'=1 \qquad (2)$$

Так как $\left|\,N(\delta)\right| = x'^2+13y'^2$ и $\left|\,N(\delta)\right| < 4$, то $y'=0$.

Тогда из (2) получаем, что $y=\dfrac{1}{2}$, что противоречит тому, что y целое число. Следовательно, кольцо K не является евклидовым.

Домашнее задание

1. Докажите, что кольцо $\left(\left\{a+b\sqrt{2} \mid a,b\in Z\right\} +, \cdot\right)$ является евклидовым.

2. Докажите, что кольцо $\left(\left\{\dfrac{a}{2}+\dfrac{b}{2}i\sqrt{19} \mid a,b\in Z,\ a\equiv b \pmod 2\right\} +, \cdot\right)$ не является евклидовым.

Дополнительные задачи

1. Используя тот факт, что кольцо $\left(\left\{a+b\sqrt{3}\mid a, b\in Z\right\}+, \cdot\right)$ евклидово, найти $\alpha, \beta \in \left\{a+b\sqrt{3} \mid a, b\in Z\right\}$ такие, что $\left(1+2\sqrt{3}\right)\alpha+\left(5+\sqrt{3}\right)\beta=1$.

2. Пусть K – евклидово кольцо. Докажите, что:

а) если u – обратимый элемент в K и $a=bu$, то $f(a)=f(b)$;

б) если $a \vdots b$ и $f(a)=f(b)$, то $a=bu$, где u – обратимый элемент;

в) $f(a)=f(1)$ тогда и только тогда, когда а обратимый элемент в K.

Литература:

1. ***Куликов Л.Я.*** Алгебра и теория чисел. – М.: Высшая школа, 1979. – 559с.
2. ***Бухштаб А.А.*** Теория чисел. – М.: Просвещение, 1966. – 384с.
3. ***А. Бейкер.*** Введение в теорию чисел. – Мн.: Высшая школа, 1995. – 132с.
4. ***Шнеперман Л.Б.*** Сборник задач по алгебре и теории чисел. – Мн.: Высшая школа, 1982. – 223с.
5. Сборник задач по алгебре / Под ред. ***А.И. Кострикина.*** – М.: Наука, 1987. – 352с.
6. ***Проскуряков И.В.*** Сборник задач по линейной алгебре. – М.: Наука, 1984. – 336с.