

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ ИМ. В.Г. БЕЛИНСКОГО

Факультет физико-математических и
естественных наук

Кафедра
«Математическое образование»

Направление подготовки 44.03.01 Педагогическое образование

Профиль «Математика»

Форма обучения: очная

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

бакалаврская работа на тему:

«Построение кольца $Z[\sqrt{3}]$ и его евклидовость»

Студент

Коротнёва - 04.06.21
(подпись, дата)

Коротнёва Кристина Алексеевна
(ФИО полностью)

Руководитель

Сулатнов - 04.06.21
(подпись, дата)

Сулатнов А.Я.
(фамилия, инициалы)

Нормоконтролёр

Журавлева - 29.06.2021
(подпись, дата)

Журавлева Е.Г.
(фамилия, инициалы)

Работа допущена к защите (протокол заседания кафедры от 07.06.21 № 8)

Заведующий кафедрой

Паньженский - 07.06.21
(подпись, дата)

Паньженский В.И.
(фамилия, инициалы)

Работа защищена с оценкой хорошо (протокол заседания ГЭК от 07.07.21 № 4)

Секретарь ГЭК

Журавлева - 07.07.21
(подпись, дата)

Журавлева Е.Г.
(фамилия, инициалы)

Пенза 2021

Оглавление

ВВЕДЕНИЕ	4
ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОБЛАСТЕЙ ЦЕЛОСТНОСТИ..	6
1.1. Определение кольца и области целостности	6
1.2. Определение подкольца и идеалов. Примеры	8
1.3. Отношение делимости в области целостности и свойства. Обратимые элементы	9
1.4. Простые и составные элементы области целостности	11
1.5. Факториальные кольца. Кольца главных идеалов	12
1.6. Евклидовы кольца	12
1.7. Наибольший общий делитель и наименьшее общее кратное в кольце целостности	13
ГЛАВА 2. ОСНОВНЫЕ ФАКТЫ ТЕОРИИ КВАДРАТИЧНЫХ КОЛЕЦ $\mathbb{Z}[\sqrt{3}]$	16
2.1. Определение квадратичного поля $\mathbb{Q}(\sqrt{k})$	16
2.2. Квадратичное кольцо $\mathbb{Z}[\sqrt{3}]$	18
2.3. Операция сопряжения в поле $\mathbb{Q}(\sqrt{3})$	20
2.4. Норма в поле $\mathbb{Q}(\sqrt{3})$	21
2.5. Свойства операции сопряжения в кольце $\mathbb{Z}[\sqrt{3}]$	21
2.6. Норма в кольце $\mathbb{Z}[\sqrt{3}]$	23
2.7. Обратимые элементы кольца $\mathbb{Z}[\sqrt{3}]$	24
2.8. Ассоциированные числа в кольце $\mathbb{Z}[\sqrt{3}]$	25
2.9. Простые и составные числа кольца $\mathbb{Z}[\sqrt{3}]$	27
2.10. Евклидовость кольца $\mathbb{Z}[\sqrt{3}]$	28
2.11. Алгоритм деления с остатком в $\mathbb{Z}[\sqrt{3}]$	31
ГЛАВА 3. ВНЕКЛАСНЫЕ ЗАНЯТИЯ ПО ТЕМЕ «КВАДРАТИЧНЫЕ КОЛЬЦА»	36
4.1. Об истории внеклассных занятий по математике в школах СССР и	

современной России.....	36
4.2. Рабочая программа факультативного курса «Основные элементы квадратичного кольца $\mathbb{Z}[\sqrt{3}]$ ».....	37
4.3. Примеры факультативных занятий по теме «Квадратичное кольцо $\mathbb{Z}[\sqrt{3}]$ ».....	39
ЗАКЛЮЧЕНИЕ	50
СПИСОК ЛИТЕРАТУРЫ	51

ВВЕДЕНИЕ

Современный человек в повседневной жизни постоянно сталкивается с числами и цифрами - они повсюду. Все системы счисления используются всегда, когда требуется что-то рассчитать, начиная с вычислений учениками младших классов, выполняемых карандашом на бумаге, заканчивая вычислениями, выполняемыми на электронных устройствах. С открытием цифр на них появились операции, затем возникла необходимость расширения операций над нулевыми, отрицательными числами и новыми числами. В результате появилась потребность в системе целых чисел, с которыми можно выполнять математические действия: сложение и умножение. Дальнейшее развитие математики связано с рациональными, иррациональными и вещественными числами. В более позднее время открываются и другие числа, полученные путем присоединения к кольцу целых чисел квадратичных иррациональностей. Эти кольца называются квадратичными. Новые числа по своим свойствам в некотором смысле напоминали обычные целые числа, но имели ряд необычных свойств, теорем и результатов.

В данной выпускной квалификационной работе проводится исследование свойства чисел действительных квадратичных колец.

Объект исследования: теория колец и областей целостности.

Предметом исследования настоящей работы являются квадратичные кольца.

Цель исследования – изучение свойств квадратичных колец $\mathbb{Z}[\sqrt{3}]$ и применения полученных результатов в курсе алгебры и теории чисел.

Задачи исследования:

- Определить понятие «квадратичное кольцо»;
- Изучить свойства данных колец;
- Разработать алгоритм деления с остатком в рассматриваемом кольце;
- Подобрать задачи, упражнения и образцы решения этих задач;

- Разработать рабочую программу факультативного курса на данную тему и привести примеры факультативных занятий.

В школьном курсе математики квадратичные кольца не рассматриваются, поэтому практическая значимость результатов работы может быть применена на факультативных занятиях в школе.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОБЛАСТЕЙ ЦЕЛОСТНОСТИ

1.1. Определение кольца и области целостности

Примером для определения области целостности является кольцо целых чисел.

Определение. Непустое множество S называется областью целостности, если в нем заданы две операции: умножения ($*$), сложения ($+$) так, что выполняются некоторые условия.

Условия будем называться аксиомами.

Рассмотрим основные аксиомы, которым соответствуют данные операции.

№	Операция сложения (+)
1	Для любых элементов $x, y \in S$: $x + y = y + x$
2	Для любых трёх элементов $x, y, z \in S$: $x + (y + z) = (x + y) + z$
3	Существует элемент $0 \in S$ такой, что для любого элемента $x \in S$: $x + 0 = x$
4	Для любого элемента $x \in S$ существует элемент $(-x)$: $x + (-x) = 0$

Нетрудно заметить, что $(S, +)$ является абелевой группой.

Определение. Элемент 0 называется нулем или нейтральным элементом относительно операции сложения, а элемент $(-x)$ для элемента x называется противоположным в группе $(S, +)$.

Далее имеем:

№	Операция умножения (*)
5	Для любых элементов $x, y \in S$: $xy = yx$
6	Для любых трёх элементов $x, y, z \in S$: $x(yz) = (xy)z$
7	Для любых трёх элементов $x, y, z \in S$: $x(y + z) = xy + xz$ и $(y + z)x = yx + zx$
8	Существует элемент $1 \in S$ такой, что для любого элемента $x \in S$: $1 * x = x * 1$
9	Для любых $x, y \in S$ ($x \neq 0, y \neq 0$): $xy \neq 0$

Следствие. Если $xy = 0$, то либо $x = 0$, либо $y = 0$. Данная аксиома исключает наличие делителей нуля в S .

Простейшими примерами областей целостности являются совокупности чисел (целых $\mathbb{Z}$, рациональных $\mathbb{Q}$, вещественных $\mathbb{R}$, комплексных $\mathbb{C}$).

Определение. Непустое множество S , с заданными алгебраическими

операциями, сложения (+) и умножения (*), удовлетворяющие требованиям аксиом 1 – 4 и аксиомы 7 в определении 1 области целостности, называется определением кольца в общем виде.

Примеры. Совокупности числовых функций, определённых на заданном множестве. Во всех случаях имеется множество, похожее на совокупности чисел в том смысле, что его элементы можно складывать и умножать, причём эти операции ведут себя естественным образом.

Выделим основные свойства колец:

1⁰. В любом кольце нулевой элемент относительно сложения является единственным.

Доказательство. Действительно, пусть 0_1 и 0_2 – два нулевых элемента кольца S . Получим $0_1 + 0_2 = 0_1$, так как 0_2 – нуль кольца S , и $0_1 + 0_2 = 0_2$, так как 0_1 – нуль кольца S . Отсюда получается равенство, $0_1 = 0_2$.

2⁰. В любом кольце имеют место равенства: $x*0 = 0$ и $0*x = 0$.

Доказательство. Заметим, что $0 + 0 = 0 \Rightarrow x*0 + 0 = x*0$. С другой стороны, в силу аксиомы 7, получим $x*0 + x*0 = x*0$. Прибавив к обеим частям этого равенства элемент $((-x)*0)$, противоположный к $(x*0)$, получим $x*0 = 0$.

Аналогично доказывается и $0*x = 0$.

3⁰. В каждом кольце S для каждого элемента x имеют место равенства:

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

Доказательство. Рассмотрим сумму $(-x)y + xy$. В силу аксиомы 7, эту сумму преобразуем следующим образом: $(-x)y + xy = ((-x) + x)y = 0y = 0$.

Отсюда, по определению противоположного элемента, получим:

$$(-x)y = -(xy).$$

Аналогично доказываем и $x(-y) = -(xy)$.

4⁰. Если в кольце S имеется элемент 1 такой, что $1*x = x*1 = x$, то $(-1)x = -x$ и $x(-1) = -x$.

Доказательство. Рассмотрим сумму $(-1)x + x$ и преобразуем её.

Тогда $(-1)x + x = (-1)x + 1*x = ((-1) + 1)x = 0x = 0$. Отсюда следует, что $(-1)x = -x$. Аналогично доказываем $x*(-1) = -x$.

В кольце C можно определить операцию вычитания по формуле:

$$x - y = x + (-y).$$

1.2. Определение подкольца и идеалов. Примеры

Определение. Подмножество $U \neq \emptyset$ кольца C , которое само является кольцом относительно операций, введенных в кольце C , называется подкольцом кольца C .

Теорема (критерий подкольца): Непустое подмножество $U \subset C$ является подкольцом кольца C тогда и только тогда, когда для любых $x, y \in U$ выполняются условия:

1) $x + y \in U$

2) $(-x) \in U$

Доказательство. Если $U \neq \emptyset$ является подкольцом, то операции $(+)$ и $(*)$ кольца C являются алгебраическими операциями в U , поэтому $x + y \in U$, $xu \in U$. Из того, что выполняется аксиома 4 кольца, следует $(-x) \in U$. Обратно, если выполняются условия (1) – (3), то выполняются аксиомы 1 – 4 и 7 кольца, так как операции $(+)$ и $(*)$, определенные на U , являются ограничениями этих операций, заданных на C .

Дадим определение идеала кольца.

Определение. Непустое подмножество U кольца C называется правым (левым) идеалом, если для любых элементов $x, y \in U$ их разность $(x - y)$ принадлежит U и $ax \in U$ ($xa \in U$) для каждого элемента $a \in C$.

Определение. Непустое подмножество U кольца C называют идеалом (двусторонним), если оно является одновременно и левым и правым идеалом кольца C .

Для коммутативного кольца все три определения совпадают, поэтому говорят просто об идеалах.

Рассмотрим примеры важных идеалов областей целостности:

1) В кольце целых чисел $\mathbb{Z}$ множества $U = \{n * k \mid n - \text{фиксированное целое число, } k \in \mathbb{Z}\}$ является идеалом. Этот идеал состоит из всевозможных целых чисел, кратных числу n . Этот идеал называется главным идеалом кольца $\mathbb{Z}$. Обозначает идеал U символом $\langle n \rangle$.

2) Пусть $a_1, a_2, \dots, a_t$ – фиксированные элементы области целостности C . Совокупность выражений $a_1x_1 + a_2x_2 + \dots + a_kx_k$, где $x_1, x_2, \dots, x_k$ – всевозможные элементы кольца C , является идеалом кольца C .

3) В приведённом примере 2 выделим важный частый случай, соответствующий $k = 1$: $\langle a_1 \rangle = \{a_1x \mid x \in K\}$. Этот идеал называется главным идеалом кольца C .

1.3. Отношение делимости в области целостности и свойства.

Обратимые элементы

Пусть C – область целостности и a, b – произвольные элементы этого кольца.

Определение. Элемент b называется делителем элемента a , если существует элемент c кольца C , удовлетворяющий условию $a = bc$.

Если b – делитель элемента a , то говорят также, что a делится на b и записывают $a : b$. Запись $b|a$ означает, что b делит элемент a .

Может оказаться, что a делится на b , а также b делится на a , тогда элементы a и b называется ассоциированными.

Обозначают отношение ассоциированности символом $\sim$.

Пример. В кольце $\mathbb{Z}$ числа 5 и -5 – ассоциированы. Действительно, так как $5 = (-1)(-5)$, то $5 : (-5)$. Из того, что $-5 = (-1)5$ следует, что $-5 : 5$. Отсюда получаем, что $5 \sim (-5)$.

Определение. Элемент a области целости C называется обратимым элементом в K , если существует элемент $b \in K$ такой, что $ab = 1$.

Обратный элемент иначе называется делителем единицы. Многие авторы обратимый элемент называют единицей. Если $ab = 1$, то элемент b называют обратным к элементу a и обозначают $b = a^{-1}$.

Целесообразно ввести определение поля.

Определение. Область целостности C , в которой каждый элемент, отличный от нуля, является обратимым, называется полем.

С каждой областью целостности можно связать поле. Опишем, как это поле получается. Для каждой пары $a, b \in C$ составим выражение $\frac{a}{b}$, при условии $b \neq 0$. Это выражение называется рациональной дробью, отношением, частным и т.д. Две дроби $\frac{a}{b}$ и $\frac{c}{d}$ называются равными тогда и только тогда, когда $ad = bc$. Множество всех дробей обозначим через C' . Ясно, что $C \subset C'$, так как $a = \frac{a}{1}$. Введем в C' операции сложения и умножения дробей по следующим правилам:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd};$$
$$\frac{a}{b} * \frac{c}{d} = \frac{ac}{bd}.$$

Тогда $(C'; +; *)$ является полем. Это поле называется полем отношений (полем частных области целостности C).

Рассмотрим свойства отношения делимости в области целостности:

- 1) Если $a : b$ и $b : c$, то $a : c$.
- 2) $a : a$.
- 3) Если $a : b$, то $ax : b$ для любого элемента $x \in C$.
- 4) a ассоциирован с элементом b области целостности C тогда и только

тогда, когда существует обратимый элемент ε в C такой, что $a = \varepsilon b$.

Доказательство. Пусть $a \sim b$ тогда $a : b$, то есть $a = \varepsilon b$ и $b : a$. Отсюда $b = \varepsilon' a$. Значит, $a = \varepsilon \varepsilon' a$. Отсюда $(1 - \varepsilon \varepsilon') a = 0$. Если $a = 0$, то и $b = 0$. Пусть утверждение $a = \varepsilon b$, где ε – обратимый элемент кольца C , является верным. Если $a \neq 0$, то $1 - \varepsilon \varepsilon' = 0$, так как C – область целостности. Следовательно, $1 = \varepsilon \varepsilon'$, поэтому ε – обратимый элемент. Утверждение доказано.

Предположим, что $a = \varepsilon b$, ε – обратимый элемент кольца C . Тогда $a : b$.

Поскольку существует элемент ε' такой, что $\varepsilon \varepsilon' = 1$, то, умножив равенство $a = \varepsilon b$ на ε' , получим $\varepsilon' a = b$. Отсюда b делится на a . Итак, $a : b$ и

$b : a$, то есть a и b – ассоциированы.

5) Множество G всех обратимых элементов области целостности C образует группу по операции умножения кольца C .

Доказательство. Пусть a и b – произвольные обратимые элементы из множества G . Покажем, что произведение элементов a и b принадлежит G . Так как $a \in G$, то существует элемент $a_1 \in C$, удовлетворяющий условиям $aa_1 = 1$. Аналогично существует элемент $b_1 \in C$ такой, что $bb_1 = 1$. Умножим равенства $aa_1 = 1$ и $bb_1 = 1$ по частям: $(aa_1)(bb_1) = 1$. В силу ассоциативности и коммутативности операции умножения в кольце C , последнее равенство перепишем: $(ab)(a_1b_1) = 1$. Отсюда следует, что ab – обратимый элемент кольца целостности C , то есть $ab \in G$. Тогда в G условие ассоциативности умножения выполняются автоматически. Далее, так как $1 \cdot 1 = 1$, то $1 \in G$. Из равенства $aa_1 = 1$ следует, что a_1 – обратимый элемент кольца C . Таким образом, G – множество всех обратимых элементов области целостности C является группой.

1.4. Простые и составные элементы области целостности

Пусть C – область целостности.

Определение. Элемент $a \in C$ называется простым элементом этого кольца, если выполняются следующие условия:

- 1) $a \neq 0$;
- 2) a – необратим в C ;
- 3) Если $a = bc$, то b или c является обратимым элементом.

Примеры.

1. В кольце целых чисел $\mathbb{Z}$ простыми элементами является $\pm 2, \pm 3, \pm 5, \dots$
2. Если C – поле, то в нем нет простых элементов, так как любой элемент $a \neq 0$ кольца C обратим в C .

Определение. Элемент $a \in C$ называется составным или приводимым, если:

- 1) $a \neq 0$
- 2) a можно представить в виде произведения двух необратимых элементов кольца C .

Примеры.

1. В кольце целых чисел $\mathbb{Z}$ число 15 является составным: $15 = 3 \cdot 5$.
2. Если C – поле, то в нем нет составных элементов.

1.5. Факториальные кольца. Кольца главных идеалов

Пусть C – область целостности, $a \in C$.

Определение. Говорят, элемент a разложим единственным образом в области целостности, если выполняются следующие условия:

- 1) Существует в C простые элементы $p_1, p_2, \dots, p_m$, что $a = p_1 p_2 \dots p_m$;
- 2) Если $a = q_1 q_2 \dots q_k$ – другое разложение элемента a на простые множители $q_1, q_2, \dots, q_k$, то $m = k$ и при подходящей нумерации p_1 ассоциирован с q_1 , p_2 ассоциирован с q_2 , $\dots$, p_m ассоциирован с q_m .

Среди колец выделяются кольца, обладающие однозначным разложением на простые множители. К числу таких колец относится кольцо целых чисел.

Определение. Кольцо C называется факториальным, если:

- 1) C – область целостности;
- 2) Каждый отличный от нуля необратимый элемент обладает однозначным разложением на простые множители.

Широкий класс факториальных колец выделяется по признаку: является ли кольцо кольцом главных идеалов.

Определение. Область целостности C называется кольцом главных идеалов, если каждый идеал в нем является главным.

Примеры. Кольцо целых чисел является кольцом главных идеалов. Другим примером кольца главных идеалов является кольцо многочленов $P[x]$ от одной переменной над произвольным полем.

1.6. Евклидовы кольца

Рассмотрим класс колец, близкий по своим свойствам к кольцу целых

чисел.

Пусть C - область целостности и $\mathbb{N}$ – множество натуральных чисел, включающее 0.

Определение. Область целостности C называется евклидовым кольцом, если существует отображение $h: C \setminus \{0\} \rightarrow \mathbb{N}$, причем выполняются условия:

- 1) Для любых a и $b \neq 0$ кольца C существует также элементы q и $r \in C$, что $a = bq + r$;
- 2) $h(r) < h(b)$ или $r = 0$.

Отображение h называется евклидовой нормой. Представлением элемента a в виде $a = bq + r$ с требованиями 2) называется делением с остатком элемента a на $b \neq 0$. Элемент q при этом называется неполным частным, а элемент r называется остатком.

Пример. Кольцо целых чисел $\mathbb{Z}$ является евклидовым кольцом с евклидовой нормой $h(x) = |x|$.

Отметит замечательное свойство евклидова кольца.

Теорема. Евклидово кольцо является кольцом главных идеалов.

Следствие. Любое евклидово кольцо является факториальным кольцом.

1.7. Наибольший общий делитель и наименьшее общее кратное в кольце целостности

Пусть C – область целостности, $a_1, a_2, \dots, a_m$ и c - элементы кольца C .

Элемент c называется общим делителем элементов $a_1, a_2, \dots, a_m$, если каждый элемент $a_1, a_2, \dots, a_m$ делится на c .

Определение. Наибольшим общим делителем элементов $a_1, a_2, \dots, a_m$ называется такой элемент $d \in C$, если выполняются следующие условия:

- 1) d - общий делитель этих элементов;
- 2) d делится на любой общий делитель элементов $a_1, a_2, \dots, a_m$.

Наибольший общий делитель элементов $a_1, a_2, \dots, a_m$ обозначен через $\text{НОД}(a_1, a_2, \dots, a_m)$.

Из определения НОД следует, что если d и d' - два наибольших общих делителей элементов $a_1, a_2, \dots, a_m$, то они ассоциированы, то есть d делится на d' и наоборот.

Теорема. Пусть $a_1, a_2, \dots, a_m$ – произвольные отличные от нуля элементы области целости S .

Положим, $d_1 = \text{НОД}(a_1, a_2)$, $d_2 = \text{НОД}(d_1, a_3)$, $\dots$, $d_{m-1} = \text{НОД}(d_{m-2}, a_m)$.

Тогда $d_{m-1} = \text{НОД}(a_1, a_2, \dots, a_m)$.

На основании этой теоремы заключаем, что нахождение наибольшего общего делителя сводится к нахождению наибольших общих делителей двух элементов.

Предположим, что кольцо S является евклидовым кольцом. Тогда наибольший общий делитель двух элементов a и b можно найти с помощью последовательности делений с остатком (с помощью алгоритма Евклида):

$$\begin{array}{ll} a = bq_1 + r_1, & h(r_1) < h(b), \\ b = r_1q_2 + r_2, & h(r_2) < h(r_1), \\ r_1 = r_2q_3 + r_3, & h(r_3) < h(r_2), \\ & \dots \\ r_{s-2} = r_{s-1}q_s + r_s, & h(r_s) < h(r_{s-1}), \\ & r_{s-1} = r_sq_{s+1}. \end{array}$$

Теорема. Наибольший общий делитель элементов a и b равен последнему отличному от нуля остатку: $\text{НОД}(a, b) = r_s$ в алгоритме Евклида.

Следствие. Существуют элементы $x, y \in S$, такие что $\text{НОД}(a, b) = ax + by$.

Доказательство. Из предпоследнего равенства находим $r_s = r_{s-2} - r_{s-1}q_s$.

Далее, переписав равенства алгоритма Евклида в обратном порядке будем выражать остатки и, последовательно исключая их, мы подойдем к равенству $r_s = ax + by$, где $r_s = \text{НОД}(a, b)$. Тем самым получим линейное представление

НОД (a, b) через элементы a и b кольца C .

Используя теорему о нахождении НОД $(a_1, a_2, \dots, a_m)$ можно доказать, что существуют элементы $x_1, x_2, \dots, x_m$ евклидова кольца C , что имеет место равенство $\text{НОД}(a_1, a_2, \dots, a_m) = a_1x_1 + a_2x_2 + \dots + a_mx_m$.

Определение. Элементы $a_1, a_2, \dots, a_m$, наибольший общий делитель которых ассоциирован с единицей, называется взаимно простым.

Теорема. Если элементы a, b - взаимно просты, то существуют элементы x, y евклидова кольца C , что выполняется равенство $ax + by = 1$.

Введем понятие наименьшего общего кратного элементов евклидова кольца. Пусть $a_1, a_2, \dots, a_k$ - произвольные отличные от нуля элементы евклидова кольца C .

Определение. Элемент $m \in C$ называется наименьшим общим кратным элементов $a_1, a_2, \dots, a_k$, если выполняются условия:

1) Элемент m делится на каждый из элементов $a_1, a_2, \dots, a_k$ (m - общее кратное этих элементов);

2) Если M - общее кратное элементов $a_1, a_2, \dots, a_k$, то M делится на m .
Можно доказать следующее свойство наименьшего общего кратного - $\text{НОК}(a_1, a_2, \dots, a_k)$. Если m_1 и m_2 - наименьшие общие кратные элементов $a_1, a_2, \dots, a_k$, то они ассоциированы, то есть $m_1 = \varepsilon m_2$, для некоторого обратимого элемента ε кольца C .

Теорема. Пусть $a_1, a_2, \dots, a_m$ - произвольные отличные от нуля элементы области целостности C . Пусть $m_1 = \text{НОК}(a_1, a_2)$, $m_2 = \text{НОК}(m_1, a_3)$, $\dots$, $m_{k-1} = \text{НОК}(m_{k-2}, a_k)$, тогда $m_{k-1} = \text{НОК}(a_1, a_2, \dots, a_k)$.

Можно доказать, что наименьшее общее кратное можно получить, вычисляя последовательно наименьшее общее кратное двух элементов, а $\text{НОК}(a, b) = \frac{ab}{\text{НОД}(a, b)}$. Если a и b - взаимно простые элементы евклидова кольца, то $\text{НОК}(a, b) = \varepsilon ab$, где ε - обратимый элемент кольца C .

ГЛАВА 2. ОСНОВНЫЕ ФАКТЫ ТЕОРИИ КВАДРАТИЧНЫХ КОЛЕЦ $\mathbb{Z}[\sqrt{3}]$

2.1. Определение квадратичного поля $\mathbb{Q}(\sqrt{k})$

Большое внимание в школьном курсе математики уделяется уравнениям, системам уравнений. Мы ограничимся рассмотрением квадратных уравнений вида $x^2 - k = 0$, где k – фиксированное целое число, не делящееся на квадрат никакого простого натурального числа. В таком случае говорят, что число k свободно от квадратов. Например, числа 2, 3, 5, 6, 17 свободны от квадратов, а числа 4, 8, 9, 12, 16, -4 , -12 не свободны от квадратов, так как 4 делится на $4 = 2^2$, 12 делится на 2^2 , 8 делится на 2^2 , 9 делится на 3^2 , 16 делится на 2^2 (а также на 4^2), -4 делится на 2^2 , -12 делится на 2^2 .

Рассматриваемые уравнения не всегда имеют корни в поле действительных чисел $\mathbb{R}$. Так, уравнения $x^2 - 1 = 0$ имеют корни 1, -1 . Вообще при $k > 0$ уравнение $x^2 - k = 0$ имеет два решения. При $k < 0$ это уравнение не имеет решения в $\mathbb{R}$. Если решения этих уравнений будем искать в поле рациональных чисел $\mathbb{Q}$, включающегося в поле действительных чисел $\mathbb{R}$, то мы обнаружим, что при некоторых положительных целых числах уравнения типа $x^2 - k = 0$ в поле рациональных чисел $\mathbb{Q}$ не будет иметь решений.

Докажем, например, что уравнение $x^2 - 3 = 0$ не имеет решений в поле $\mathbb{Q}$. Доказательство проведем методом от противного. Предположим, что рациональное число $\frac{m}{n}$, где $m \in \mathbb{Z}$, $n \in \mathbb{N}$, является решением этого уравнения. Будем считать, что дробь $\frac{m}{n}$ несократима, то есть числа m и n могут иметь лишь делители 1 или -1 . Из определения понятия «решения» следует, что равенство $\frac{m^2}{n^2} - 3 = 0$ является верным числовым равенством, то есть истинным высказыванием. Умножив обе части этого равенства на n^2 , мы получим также истинные равенства $m^2 - 3n^2 = 0$. Правая часть этого равенства делится на 3, значит и левая часть делится на 3. Так как $-3n^2$ делится на 3, то число m^2 должно делиться на 3. Тогда m является четным числом, то есть $m = 3p$.

Поэтому $(3p)^2 - 3n^2 = 0$ – истинные высказывания. Сократив обе части полученного равенства на 3, получим $3p^2 - n^2 = 0$. Это равенство является истинным равенством. Отсюда n^2 делится на 3, то есть $n = 3q$. Тогда дробь $\frac{m}{n}$ окажется сократимой, так как $\frac{m}{n} = \frac{3p}{3q}$; это означает, что m и n имеют общий делитель 3 – отличный от ± 1 . Значит, уравнение $x^2 - 3 = 0$ не имеет решений в $\mathbb{Q}$. При $k < 0$ уравнение $x^2 - k = 0$ не имеет решений в поле $\mathbb{R}$, а значит и в $\mathbb{Q}$. Пусть $k > 0$ и k – свободно от квадратов и отлично от 1. Тогда уравнение $x^2 - k = 0$ не имеет решений в $\mathbb{Q}$. Это утверждение можно доказать аналогично случаю $k = 3$.

Во множестве $\mathbb{R}$ выделим подмножество $\mathbb{Q}(\sqrt{k}) = \{\alpha + \beta\sqrt{k} | \alpha, \beta \in \mathbb{Q}\}$. Для любых чисел $\alpha + \beta\sqrt{k}, \gamma + \delta\sqrt{k}$ равенство $\alpha + \beta\sqrt{k} = \gamma + \delta\sqrt{k}$ возможно тогда и только тогда, когда $\alpha = \gamma$ и $\beta = \delta$.

Докажем это утверждение. Пусть имеет место это равенство. Тогда $\alpha - \gamma = (\delta - \beta)\sqrt{k}$. Предположим, что $\delta - \beta \neq 0$, то $\frac{\alpha - \gamma}{\delta - \beta} = \sqrt{k}$. Возводя обе части этого равенства в квадрат, получим $\left(\frac{\alpha - \gamma}{\delta - \beta}\right)^2 = k$. Отсюда следует, что рациональное число $\frac{\alpha - \gamma}{\delta - \beta}$ является корнем квадратного уравнения $x^2 - k = 0$. Получим противоречие. Значит, предположение $\delta - \beta \neq 0$ неверно, поэтому $\beta = \gamma$. Тогда и $\alpha = \gamma$. Обратно, при $\alpha = \gamma$ и $\beta = \delta$ имеем $\alpha + \beta\sqrt{k} = \gamma + \delta\sqrt{k}$.

Во множестве $\mathbb{Q}(\sqrt{k})$ операции сложения и умножения определим, как и в поле $\mathbb{R}$:

$$\begin{aligned}(\alpha + \beta\sqrt{k}) + (\gamma + \delta\sqrt{k}) &= (\alpha + \gamma) + (\beta + \delta)\sqrt{k}, \\(\alpha + \beta\sqrt{k})(\gamma + \delta\sqrt{k}) &= (\alpha\gamma + k\beta\delta) + (\alpha\delta + \beta\gamma)\sqrt{k}.\end{aligned}$$

Тогда введенные операции будут обладать всеми свойствами сложения и умножения поля $\mathbb{R}$.

Теорема. $\mathbb{Q}(\sqrt{k})$ с введенными операциями сложения (+) и умножения (*) является областью целостности, то есть коммутативным, ассоциированным

кольцом с единицей без делителей нуля.

В области целостности $\mathbb{Q}(\sqrt{k})$ каждое отличное от нуля число обратимо. Действительно, пусть число $x = \alpha + \beta\sqrt{k}$ отлично от нуля. Рассмотрим число $y = \frac{\alpha}{\alpha^2 - k\beta^2} - \frac{\beta}{\alpha^2 - k\beta^2}\sqrt{k}$, которое существует, так как $\alpha^2 - k\beta^2 \neq 0$, поскольку $\alpha + \beta\sqrt{k} \neq 0$. В самом деле, если предположить $\alpha^2 - k\beta^2 = 0$, получим что $\left(\frac{\alpha}{\beta}\right)^2 - k = 0$, $\beta \neq 0$. Значит рациональное число $\frac{\alpha}{\beta}$ является корнем уравнения $x^2 - k = 0$. Противоречие. Тогда $\beta = 0$ и $\alpha = 0$. Но $\alpha + \beta\sqrt{k} \neq 0$. Получим противоречие. Вычислим произведение xy :

$$xy = (\alpha + \beta\sqrt{k})(\alpha - \beta\sqrt{k}) \frac{1}{\alpha^2 - k\beta^2} = (\alpha^2 - k\beta^2) \frac{1}{\alpha^2 - k\beta^2} = 1.$$

Таким образом, число x – обратимое число, причем $x^{-1} = y$.

2.2. Квадратичное кольцо $\mathbb{Z}[\sqrt{3}]$

Рассмотрим квадратичное поле $\mathbb{Q}(\sqrt{3})$ и выделим в нем множество $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} | a, b \in \mathbb{Z}\}$. Из рассмотренного в 1.1. следует, что $a + b\sqrt{3} = c + d\sqrt{3}$ тогда и только тогда, когда $a = c$, $b = d$. Сумму и произведение в множестве операции также, как и в поле $\mathbb{Q}(\sqrt{3})$. Тогда множество $\mathbb{Z}[\sqrt{3}]$ будет областью целостности.

Определение. Область целостности $\mathbb{Z}[\sqrt{3}]$ называется квадратичным расширением кольца $\mathbb{Z}$, иначе квадратичным кольцом, полученным присоединением к кольцу числа $\sqrt{3}$.

Упражнения на арифметические действия в кольце $\mathbb{Z}[\sqrt{3}]$.

$$1) \quad (\sqrt{3})^0 = 1 \text{ (по определению степени с нулевым показателем);}$$

$$2) \quad (\sqrt{3})^1 = \sqrt{3} \text{ (по определению степени с показателем 1);}$$

$$3) \quad (\sqrt{3})^2 = 3 \text{ (по определению корня второй степени из положительного вещественного числа);}$$

$$4) \quad (\sqrt{3})^{-1} = \frac{1}{\sqrt{3}} \text{ (по определению степени с отрицательным}$$

показателем), значит $(\sqrt{3})^{-1} = \frac{\sqrt{3}}{3}$ в поле $\mathbb{Q}(\sqrt{3})$.

Вычислить:

5) $(1 + 2\sqrt{3})(3 - \sqrt{3})$

6) $(1 + 2\sqrt{3})(1 - 2\sqrt{3})$

7) $(1 + 2\sqrt{3})(1 - \sqrt{3})$

8) $(1 + \sqrt{3})^2$

9) $(1 + \sqrt{3})^{-1}$

10) $(1 + \sqrt{3})^{-2}$

11) $(1 + \sqrt{3})(1 + \sqrt{3})^{-2}$

12) $(3 - 2\sqrt{3})(1 + \sqrt{3})^{-1}$

13) $\frac{5+2\sqrt{3}}{1-\sqrt{3}}$

14) $\frac{5-2\sqrt{3}}{(1-\sqrt{3})^2}$

Решим пример 14. Преобразуем дробь в поле $\mathbb{Q}(\sqrt{3})$. Это можно сделать разными способами. Вот один из способов, который начинается с возведения в квадрат числа $1 - \sqrt{3}$:

$$\frac{5-2\sqrt{3}}{(1-\sqrt{3})^2} = \frac{5-2\sqrt{3}}{1-2\sqrt{3}+3} = \frac{5-2\sqrt{3}}{4-2\sqrt{3}}$$

Чтобы получить стандартную запись полученного числа в поле $\mathbb{Q}(\sqrt{3})$, умножим числитель и знаменатель дроби на выражение, сопряженное знаменателю. Тогда

$$\begin{aligned} \frac{5-2\sqrt{3}}{(1-\sqrt{3})^2} &= \frac{5-2\sqrt{3}}{4-2\sqrt{3}} = \frac{(5-2\sqrt{3})(4+2\sqrt{3})}{(4-2\sqrt{3})(4+2\sqrt{3})} = \\ &= \frac{5 \cdot 4 + 5 \cdot 2\sqrt{3} - 8\sqrt{3} - (2\sqrt{3})(2\sqrt{3})}{16 - (2\sqrt{3})^2} = \frac{20 + 10\sqrt{3} - 8\sqrt{3} - 12}{16 - 12} = \frac{8 + 2\sqrt{3}}{4} = \frac{4 + \sqrt{3}}{2}. \end{aligned}$$

Получим число, принадлежащее кольцу $\mathbb{Z}[\sqrt{3}]$. Значит, имеет место равенство $5 - 2\sqrt{3} = (1 - \sqrt{3})^2 \frac{4 + \sqrt{3}}{2}$. Отсюда следует, что число $5 - 2\sqrt{3}$ делится

на $(1 - \sqrt{3})^2$ и на число $\frac{4+\sqrt{3}}{2}$ в кольце $\mathbb{Z}[\sqrt{3}]$.

16) Найдите значения выражения в $\mathbb{Z}[\sqrt{3}]$ и в поле $\mathbb{Q}(\sqrt{3})$:

а) $1 * \sqrt{3}$; б) $\sqrt{3} * \sqrt{3}$; в) $(\sqrt{3})^3$; г) $(\sqrt{3})^{2k}$, $k \in \mathbb{Z}$; д) $(\sqrt{3})^{2k+1}$.

17) Докажите, что число $5 - 7\sqrt{3}$ делится на числа $7 + 5\sqrt{3}$, $7 - 5\sqrt{3}$.

18) Найдите значение выражения $\frac{10+3\sqrt{3}}{(1+\sqrt{3})^3}$.

19) Выясните, являются ли числа $31 - \sqrt{3}$ и $97 - 65\sqrt{3}$, 25 и $75 - 50\sqrt{3}$ ассоциированными?

20) Выясните, чему равно значение выражения в поле $\mathbb{Q}(\sqrt{3})$:

а) $\frac{5-2\sqrt{3}}{3+4\sqrt{3}}$ б) $\frac{21-2\sqrt{3}}{1+3\sqrt{3}}$ в) $\frac{(1-\sqrt{3})^3}{2+\sqrt{3}}$ г) $\frac{(1+\sqrt{3})^2}{(1-\sqrt{3})}$ д) $\frac{23+2\sqrt{3}}{(1+\sqrt{3})^3}$

Какие из них принадлежат кольцу $\mathbb{Z}[\sqrt{3}]$?

2.3. Операция сопряжения в поле $\mathbb{Q}(\sqrt{3})$

Пусть $\alpha = a + b\sqrt{3}$ и $c + d\sqrt{3}$ – любые два числа из поля $\mathbb{Q}(\sqrt{3})$.

Определение. Отображение $\varphi: \mathbb{Q}(\sqrt{3}) \rightarrow \mathbb{Z}$, определенное условием $\varphi(a + b\sqrt{3}) = a - b\sqrt{3}$ называется сопряжением в поле $\mathbb{Q}(\sqrt{3})$.

Обычно $\varphi(a + b\sqrt{3})$ обозначается через $a - b\sqrt{3}$.

Свойства отображения сопряжений:

1. φ является линейным отображением. Это значит, что выполняются условия:

а) $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$;

б) $\varphi(\alpha\beta) = \varphi(\alpha) * \varphi(\beta)$.

Это свойство проверяется на основании определения отображения φ .

2. $\varphi(\varphi(\alpha)) = \alpha$

3. $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$

Действительно, пусть $\alpha = a + b\sqrt{3}$, $\beta = c + d\sqrt{3}$, тогда

$$\varphi(\alpha\beta) = \varphi(ac + 3bd + (bc + ad\sqrt{3})) = ac + 3bd - (bc + ad)\sqrt{3}.$$

С другой стороны:

$$\varphi(\alpha)\varphi(\beta) = (a - b\sqrt{3})(c - d\sqrt{3}) = (ac + 3bd) - (bc - ad)\sqrt{3}.$$

Отсюда следует, что $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.

$$4. \varphi\left(\frac{\alpha}{\beta}\right) = \frac{\varphi(\alpha)}{\varphi(\beta)}.$$

Доказательство. Дробь $\frac{\alpha}{\beta}$ представим как произведение $\frac{\alpha}{\beta} = \alpha * \frac{1}{\beta}$. Тогда

$$\varphi\left(\frac{\alpha}{\beta}\right) = \varphi(\alpha)\varphi\left(\frac{1}{\beta}\right). \text{ Чтобы найти } \varphi\left(\frac{1}{\beta}\right) \text{ воспользуемся равенством } \beta * \frac{1}{\beta} = 1,$$

$$\text{тогда } \varphi\left(\beta * \frac{1}{\beta}\right) = \varphi(1). \text{ Отсюда } \varphi(\beta)\varphi\left(\frac{1}{\beta}\right) = 1. \text{ Тогда } \varphi\left(\frac{1}{\beta}\right) = \frac{1}{\varphi(\beta)}.$$

$$\text{Следовательно, } \varphi\left(\frac{\alpha}{\beta}\right) = \varphi(\alpha) * \frac{1}{\varphi(\beta)} = \frac{\varphi(\alpha)}{\varphi(\beta)}.$$

$$5. \varphi(\alpha)\alpha \in \mathbb{Q}.$$

2.4. Норма в поле $\mathbb{Q}(\sqrt{3})$

Определение. Нормой в $\mathbb{Q}(\sqrt{3})$ называется отображение $n: \mathbb{Q}(\sqrt{3}) \rightarrow \mathbb{Z}$, определенное условием $n(\alpha) = \alpha\bar{\alpha}$.

Из определения нормы в $\mathbb{Q}(\sqrt{3})$ следует формула вычисления нормы:

$$n(a + b\sqrt{3}) = a^2 - 3b^2.$$

$$\text{Доказательство. } n(a + b\sqrt{3}) = (a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - (b\sqrt{3})^2 = a^2 - 3b^2.$$

Свойства нормы:

$$1. n(\alpha) = 0 \text{ тогда и только тогда, когда } \alpha = 0;$$

$$2. n(a) = a^2 \text{ для любых } a \in \mathbb{Q}.$$

$$3. n(\alpha\beta) = n(\alpha) * n(\beta).$$

Доказательство. Пусть $\alpha = a + b\sqrt{3}$, $\beta = c + d\sqrt{3}$. Тогда $n(\alpha) = a^2 - 3b^2$, $n(\beta) = c^2 - 3d^2$. Поэтому, $n(\alpha)n(\beta) = (\alpha\bar{\alpha})(\beta\bar{\beta}) = (\alpha\beta)(\alpha\beta) = n(\alpha\beta)$. При этом $n(\alpha\beta) = (a^2c^2 + 9b^2d^2) - 3(a^2d^2 - c^2b^2)$.

2.5. Свойства операции сопряжения в кольце $\mathbb{Z}[\sqrt{3}]$

$\alpha = a + b\sqrt{3}$, $a, b \in \mathbb{Q}$ $\bar{\alpha} = a - b\sqrt{3}$ — число, сопряжённое α .

$$1. \bar{\bar{\alpha}} = \alpha.$$

$$2. \overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}.$$

Действительно, пусть $\beta = c + d\sqrt{3}$.

Тогда $\alpha + \beta = (a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3}$.

$$\overline{\alpha + \beta} = (a + c) - (b + d)\sqrt{3} = a + c - b\sqrt{3} - d\sqrt{3} = (a - b\sqrt{3}) + (c - d\sqrt{3}) = \bar{\alpha} + \bar{\beta}.$$

3. Для любого целого числа $c \in \mathbb{Q}$ выполняется равенство:

$$\overline{c\alpha} = c\bar{\alpha}$$

Действительно, $c\alpha = c(a + b\sqrt{3}) = ca + (cb)\sqrt{3}$. Тогда $\overline{c\alpha} = ca - (cb)\sqrt{3} = c(a - b\sqrt{3}) = c\bar{\alpha}$.

$$4. \overline{\alpha\beta} = \bar{\alpha}\bar{\beta}.$$

Доказательство. $\alpha\beta = (a + b\sqrt{3})(c + d\sqrt{3}) = ac + (ad)\sqrt{3} + (bc)\sqrt{3} + bd\sqrt{3}\sqrt{3} = (ac + 3bd) + (ad + bc)\sqrt{3}$. Отсюда, $\overline{\alpha\beta} = (ac + 3bd) - (ad + bc)\sqrt{3}$. Далее $\bar{\alpha} = a - b\sqrt{3}$, $\bar{\beta} = c - d\sqrt{3}$. Поэтому $\bar{\alpha}\bar{\beta} = ac - (ad)\sqrt{3} - (bc)\sqrt{3} + bd\sqrt{3}\sqrt{3} = (ac + 3bd) - (ad + bc)\sqrt{3}$. Следовательно, $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$.

5. $\overline{\alpha_1 + \alpha_2 + \dots + \alpha_k} = \bar{\alpha}_1 + \bar{\alpha}_2 + \dots + \bar{\alpha}_k$ (доказательство методом математической индукции)

6. $\overline{\alpha_1\alpha_2 \dots \alpha_k} = \bar{\alpha}_1 \cdot \bar{\alpha}_2 \dots \bar{\alpha}_k$ (доказательство методом математической индукции)

7. $\overline{\alpha^n} = (\bar{\alpha})^n$, n – произвольное натуральное число, то есть $n = 1, 2, \dots$

8. Для любых чисел $c \in \mathbb{Q}$, $\bar{\bar{c}} = c$.

Действительно, $c = c + 0\sqrt{3}$, $a\bar{c} = c - 0\sqrt{3}$.

9. $\overline{\alpha^{-n}} = (\bar{\alpha})^{-n}$, n – произвольное натуральное число.

Операцию сопряжения в кольце $\mathbb{Z}[\sqrt{3}]$ определим как операцию сопряжения в $(\mathbb{Q}(\sqrt{3}))$ применительно к элементам кольца $\mathbb{Z}[\sqrt{3}]$. В таком случае говорят, что операция сопряжения в кольце $\mathbb{Z}[\sqrt{3}]$ является ограничением операции сопряжения, определенного в поле $\mathbb{Q}(\sqrt{3})$ на $\mathbb{Z}[\sqrt{3}]$. Все перечисленные свойства операции сопряжения в $\mathbb{Q}(\sqrt{3})$ остаются в силе и в

кольце $\mathbb{Z}[\sqrt{3}]$.

2.6. Норма в кольце $\mathbb{Z}[\sqrt{3}]$

Возьмем произвольное число $a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$.

Произведение $(a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2$ является целым числом.

Определение. Число $a^2 - 3b^2$ называется алгебраической нормой числа $a + b\sqrt{3}$ и обозначается $n(a + b\sqrt{3})$.

Таким образом, норма в кольце $\mathbb{Z}[\sqrt{3}]$ представляет собой ограничение нормы поля $\mathbb{Q}(\sqrt{3})$.

Упражнения.

1. $n(0) = n(0 + 0\sqrt{3}) = 0^2 - 3 \cdot 0^2 = 0$

2. Пусть $n(a + b\sqrt{3}) = 0$, тогда $a^2 - 3b^2 = 0$. Отсюда, если $b \neq 0$, то $\frac{a^2}{b^2} = 3$, то есть $\left(\frac{a}{b}\right)^2$. Но, этого не может быть, так как $\frac{a}{b}$ – число рациональное, а число 3 не может быть квадратом рационального числа. Поэтому, предположение $b \neq 0$ приведет к противоречию. Значит, равенство $a^2 - 3b^2 = 0$ влечет равенство $b = 0$. Тогда $a^2 = 0$, следовательно, $a = 0$. Таким образом, если $n(a + b\sqrt{3}) = 0$, то $a = 0$ и $b = 0$, то есть $a + b\sqrt{3} = 0$.

3. $n(1) = 1$, так как $1 = 1 + 0\sqrt{3}$, а $n(1 + 0\sqrt{3}) = 1^2 - 3 \cdot 0^2 = 1$.

4. Покажите, что $n(\alpha) = n(\alpha)$, где $\alpha = a + b\sqrt{3}$, а $\alpha = a - b\sqrt{3}$.

5. Найдите норму чисел: $1 + \sqrt{3}$, $1 - \sqrt{3}$, $2 + 3\sqrt{3}$, $2 - 3\sqrt{3}$, $1 + 2\sqrt{3}$

6. Найдите нормы $(1 + \sqrt{3})(1 - \sqrt{3})$, $(1 + \sqrt{3})(1 + 2\sqrt{3})$ и сравните с нормами чисел $1 - \sqrt{3}$ и $1 + 2\sqrt{3}$ соответственно.

7. Докажите, что $n(2 + \sqrt{3}) = 1$ и $n(2 - \sqrt{3}) = 1$.

8. Докажите, что $n(\alpha) = n(\varepsilon\alpha)$, где $\alpha = a + b\sqrt{3}$; $\varepsilon = 2 + \sqrt{3}$ или $\varepsilon = 2 - \sqrt{3}$.

Решение. Из определения нормы следует, что $n(\alpha) = a^2 - 3b^2$. Найдем произведения $\varepsilon\alpha$. Возможны два случая: а) $\varepsilon\alpha = (2 + \sqrt{3})(a + b\sqrt{3})$ или б) $\varepsilon\alpha = (2 - \sqrt{3})(a + b\sqrt{3})$. В случае а) $\varepsilon\alpha = 2a + 2b\sqrt{3} + a\sqrt{3} + b\sqrt{3}\sqrt{3} =$

$(2a + 3b) + (a + 2b)\sqrt{3}$. Поэтому, $n(\varepsilon\alpha) = (2a + 3b)^2 - 3(a + 2b)^2 = 4a^2 + 12ab + 9b^2 - 3a^2 - 12ab - 12b^2 = a^2 - 3b^2 = n(\alpha)$. Таким образом, $n(\varepsilon\alpha) = n(\alpha)$ или $n(\alpha) = n(\varepsilon\alpha)$.

б) $\varepsilon\alpha = (2 - \sqrt{3})(a + b\sqrt{3}) = 2a + 2b\sqrt{3} - a\sqrt{3} - b\sqrt{3}\sqrt{3} = (2a - 3b) + (2b - a)\sqrt{3}$. $n(\varepsilon\alpha) = (2a - 3b)^2 - 3(2b - a)^2 = 4a^2 - 12ab + 9b^2 - 12b^2 + 12ab - 3a^2 = a^2 - 3b^2 = n(\alpha)$.

Отсюда $n(\alpha) = n(\varepsilon\alpha)$.

9. Найдите нормы чисел: $(1 + \sqrt{3})^2$, $(1 - \sqrt{3})^2$, $(1 \pm \sqrt{3})^3$.

Теорема (мультипликативность нормы). Для любых чисел α и β из кольца $\mathbb{Z}[\sqrt{3}]$ выполняется равенство: $n(\alpha\beta) = n(\alpha)n(\beta)$.

Доказательство. Пусть $\alpha = a + b\sqrt{3}$ и $\beta = c + d\sqrt{3}$.

Тогда $\bar{\alpha} = a - b\sqrt{3}$, $\bar{\beta} = c - d\sqrt{3}$, поэтому $n(\alpha\beta) = (\alpha\beta)(\overline{\alpha\beta}) = (\alpha\beta)(\bar{\alpha} \cdot \bar{\beta}) = (\alpha\bar{\alpha})(\beta\bar{\beta}) = n(\alpha)n(\beta)$.

Замечание. При преобразовании произведения $(\alpha\beta)(\bar{\alpha}\bar{\beta})$ мы использовали ассоциативность и коммутативность операции умножения в кольце $\mathbb{Z}[\sqrt{3}]$.

Упражнения.

1. Найдите нормы чисел 2 ; -1 ; $2 + \sqrt{3}$; $2 - \sqrt{3}$; $3 + \sqrt{3}$; $11 - 3\sqrt{3}$
2. Могут ли числа $0, 1, -1, 2, 3, 4, -3, -4, 5, -5, 6, -6, 7, -7$ быть нормами некоторых чисел кольца $\mathbb{Z}[\sqrt{3}]$?
3. Как связаны нормы $n(\alpha)$ и $n(2\alpha)$; $n(\alpha)$ и $n(3\sqrt{\alpha})$?

2.7. Обратимые элементы кольца $\mathbb{Z}[\sqrt{3}]$

Определение. Элемент $a + b\sqrt{3}$ называется обратимым, если существует элемент $x + y\sqrt{3}$ из $\mathbb{Z}[\sqrt{3}]$, удовлетворяющий условию:

$$(a + b\sqrt{3})(x + y\sqrt{3}) = 1.$$

Примеры. Число $7 + 4\sqrt{3}$ обратимо в кольце $\mathbb{Z}[\sqrt{3}]$, так как $(7 + 4\sqrt{3})(7 - 4\sqrt{3}) = 49 - 16(\sqrt{3})^2 = 1$.

Упражнения.

1. Покажите, что числа $26 - 15\sqrt{3}$ и $26 + 15\sqrt{3}$ обратимы в кольце $\mathbb{Z}[\sqrt{3}]$.

2. Покажите, что число $\frac{(2-\sqrt{3})^{20}}{(2+\sqrt{3})^7}$ является обратимым в кольце $\mathbb{Z}[\sqrt{3}]$.

3. Представьте число из упражнения 2 в виде степени $(2 + \sqrt{3})^k$ и найдите показатель k .

Известно, что в кольце $\mathbb{Z}[\sqrt{3}]$ каждое обратимое число ε имеет вид: $\varepsilon = \pm(2 + \sqrt{3})^n$, где n – произвольное целое число. Обратимый элемент $2 + \sqrt{3}$ называется главным обратимым элементом.

2.8. Ассоциированные числа в кольце $\mathbb{Z}[\sqrt{3}]$

Напомним, элементы a и b , отличные от нуля области целостности называются ассоциированными, если каждый из них делится на второй элемент.

Теорема (критерий ассоциированности элементов). Элементы a и b кольца $\mathbb{Z}[\sqrt{3}]$ ассоциированы тогда и только тогда, когда существует делитель ε единицы этого кольца, что выполняется равенство $a = \varepsilon b$.

Как мы уже отмечали, всякий делитель единицы кольца $\mathbb{Z}[\sqrt{3}]$ и вид $(2 + \sqrt{3})^n$ или $-(2 + \sqrt{3})^n$, где n – произвольное целое число.

Теорема (условие ассоциированности). Числа a и b ассоциированы, тогда и только тогда, когда $n\left(\frac{a}{b}\right) = \pm 1$, то есть нормы этих чисел либо равны, либо противоположны.

Примеры.

1. Числа 2 и 3 не ассоциированы в кольце $\mathbb{Z}[\sqrt{3}]$.

Действительно, $n(2) = 4$, $n(3) = 9$. То есть $n(2) \neq n(3)$ и $n(2) \neq -n(3)$.

2. Число 2 ассоциировано с числом $4 - 2\sqrt{3}$, так как $4 - 2\sqrt{3} = (2 - \sqrt{3})2$, а $2 - \sqrt{3}$ – делитель 1.

3. Число 1 ассоциировано с числом $2 - \sqrt{3}$ так как $1 = (2 + \sqrt{3})(2 - \sqrt{3})$, а $2 - \sqrt{3}$ – делитель 1.

4. Покажем, что числа $4 - 3\sqrt{3}$ и $1 + 2\sqrt{3}$ ассоциированы в $\mathbb{Z}[\sqrt{3}]$. Для этого, сначала проверим выполняется ли необходимое условие ассоциированности – равенство абсолютных значений норм этих чисел.

Находим:

$$n(4 - 3\sqrt{3}) = 4^2 - 3 \cdot 9 = 16 - 27 = -11.$$

$$n(1 + 2\sqrt{3}) = 1 - 3 \cdot 4 = -11.$$

Отсюда заключаем, что $n(4 - 3\sqrt{3}) = n(1 + 2\sqrt{3})$, то есть, абсолютное значение этих чисел равны 11. Поэтому необходимое условие ассоциированности выполняется. А это значит, что рассматриваемые числа возможно ассоциированы. Далее, в поле $\mathbb{Q}(\sqrt{3})$ найдем значение отношения этих чисел:

$$\frac{4-3\sqrt{3}}{1+2\sqrt{3}} = \frac{(4-3\sqrt{3})(1-2\sqrt{3})}{(1+2\sqrt{3})(1-2\sqrt{3})} = \frac{(4+6\cdot 3)-(8+3)\sqrt{3}}{-11} = \frac{22-11\sqrt{3}}{-11} = -2 + \sqrt{3} \in \mathbb{Z}[\sqrt{3}].$$

Найдем норму этой дроби:

$$n\left(\frac{4 - 3\sqrt{3}}{1 + 2\sqrt{3}}\right) = \frac{n(4 - 3\sqrt{3})}{n(1 + 2\sqrt{3})} = \frac{-11}{-11} = 1$$

Из этих двух условий следует, что $n(-2 + \sqrt{3}) = 1$ и $4 - 3\sqrt{3} = (-2 + \sqrt{3})(1 + 2\sqrt{3})$, где $-2 + \sqrt{3}$ – делитель единицы в кольце $\mathbb{Z}[\sqrt{3}]$.

Упражнения.

1. Будут ли ассоциированы числа:

а) 2 и 4;

б) $41 + 29\sqrt{3}$ и $1 + \sqrt{3}$;

в) $10 + 7\sqrt{3}$ и $4 - 3\sqrt{3}$;

г) $1 + 2\sqrt{3}$ и $-3 + \sqrt{3}$;

д) $3 - 5\sqrt{3}$ и $2 + 3\sqrt{3}$;

е) $7 + 17\sqrt{3}$ и $3 + 4\sqrt{3}$ – ?

2.9. Простые и составные числа кольца $\mathbb{Z}[\sqrt{3}]$

Как было отмечено элемент x кольца целостности S называется простым, если x удовлетворяет следующим условиям:

- 1) $x \neq 0$;
- 2) x не является делителем единицы (то есть x – необратимый элемент);
- 3) Если $x = \alpha\beta$, то либо α – обратимый элемент, либо β – обратимый элемент.

Отметим следующий достаточный признак необратимости.

Теорема. Если норма числа $\alpha \in \mathbb{Z}[\sqrt{3}]$ не равна $+1$ или -1 , и $\alpha \neq 0$, то α – необратимый элемент.

Доказательство. Пусть α удовлетворяет условиям теоремы и α является обратимым. Тогда существует элемент $\beta \in \mathbb{Z}[\sqrt{3}]$ такой, что $\alpha\beta = 1$. Тогда $n(\alpha\beta) = n(1)$, значит $n(\alpha)n(\beta) = 1$. Отсюда число $n(\alpha)$ делит 1. Но этого быть не может, так, как $n(\alpha) \neq \pm 1$.

Теорема. Если число α – является простым в кольце $\mathbb{Z}[\sqrt{3}]$, то для каждого обратимого элемента ε число $\varepsilon\alpha$ является простым числом.

Доказательство. Проверим, что число $\varepsilon\alpha$, где α – простое число, удовлетворяет условиям 1) – 3) простоты:

- 1) $\varepsilon\alpha \neq 0$;
- 2) $\varepsilon\alpha$ – необратим, так как равенство $(\varepsilon\alpha)\beta = 1$ не может выполняться.

Действительно, $n(\varepsilon\alpha) = n(1)$ или иначе $n(\varepsilon)n(\alpha) = 1$. Поскольку $n(\varepsilon) = \pm 1$, то $n(\alpha) = \pm 1$, чего быть не может.

- 3) Пусть $\varepsilon\alpha = \beta\gamma$, то $\alpha = (\eta\beta)\gamma$, где $\eta\varepsilon = 1$. Так как α – простой элемент, то $\varepsilon\beta$ или γ – обратимы.

Значит, $\varepsilon\beta$ – простой элемент.

Определение. Число $\alpha \in \mathbb{Z}[\sqrt{3}]$ называется составным, если $\alpha \neq 0$ и его можно представить в виде произведения двух необратимых чисел.

Пример. Число 3 является в $\mathbb{Z}[\sqrt{3}]$ составным, так как $3 = \sqrt{3} * \sqrt{3}$ и

$\sqrt{3}$ простое число.

Упражнения.

1. Какие из чисел $3, 3 + 3\sqrt{3}, 1 - 3\sqrt{3}, 3 + 2\sqrt{3}$ являются простыми?
2. Докажите, что числа $-9 + \sqrt{3}, 9, 5 - 5\sqrt{3}$ – составные числа в $\mathbb{Z}[\sqrt{3}]$
3. Докажите, что в каждом поле нет простых элементов.
4. Докажите, что в каждом поле нет составных элементов.

2.10. Евклидовость кольца $\mathbb{Z}[\sqrt{3}]$

Для доказательства евклидовости кольца $\mathbb{Z}[\sqrt{3}]$ рассмотрим отображение $h: \mathbb{Z}[\sqrt{3}] \setminus \{0\} \rightarrow \mathbb{N}$ положив $h = |n|$, где n – алгебраическая норма кольца $\mathbb{Z}[\sqrt{3}]$. Таким образом, $h(\alpha) = |n(\alpha)|$. Из свойств алгебраической нормы вытекает, что $h(\alpha)$ обладает следующим свойством:

1. $h(\alpha) = 0$ тогда и только тогда, когда $\alpha = 0$;

Доказательство. Пусть $\alpha = 0$, тогда $h(0) = |n(0)| = |0| = 0$. Обратно, пусть $h(\alpha) = 0$. Тогда $|n(\alpha)| = 0$. Из определения модуля числа, получим, что $n(\alpha) = 0$. Отсюда, на основании свойства алгебраической нормы n , заключаем, что $\alpha = 0$.

2. $h(\alpha) = 1$ тогда и только тогда, когда α является делителем единицы.

Доказательство. Пусть $h(\alpha) = 1$. Тогда $|n(\alpha)| = 1$. Отсюда $n(\alpha) = 1$ или $n(\alpha) = -1$. Если $\alpha = a + b\sqrt{3}$, то на основании тождества $(a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2$ имеем $a(a - b\sqrt{3}) = n(\alpha)$, то есть $\alpha(-a - b\sqrt{3}) = 1$ (*). Следовательно, α – делитель единицы. Если $n(\alpha) = -1$, то умножив обе части равенства (*) на (-1) , получим $\alpha(-a + b\sqrt{3}) = -1$. Значит, число $\alpha \in \mathbb{Z}[\sqrt{3}]$ является обратимым. Предположим, что α – делитель единицы. Тогда $n(\alpha) = \pm 1$. Значит $h(\alpha) = |n(\alpha)| = |\pm 1| = 1$.

3. $h(\alpha\beta) = h(\alpha)h(\beta)$.

Доказательство. Из определения отображения h и свойства модуля числа, имеем:

$$h(\alpha\beta) = |n(\alpha\beta)| = |n(\alpha)n(\beta)| = |n(\alpha)||n(\beta)| = h(\alpha)h(\beta).$$

Таким образом, отображение h обладает свойством мультипликативности

Теорема. Для любых двух чисел $\alpha = a + b\sqrt{3}$ и $\beta = c + d\sqrt{3} \neq 0$ существуют такие числа $\gamma = a_1 + b_1\sqrt{3}$ и $r \in \mathbb{Z}[\sqrt{3}]$, что выполняются следующие условия:

- 1) $\alpha = \beta\gamma + r$;
- 2) $h(r) < h(\beta)$ или $r = 0$.

Доказательство. Пусть $\alpha = a + b\sqrt{3}$, $\beta = c + d\sqrt{3}$ и $\beta \neq 0$. Найдем отношение $\frac{\alpha}{\beta}$ в $\mathbb{Q}(\sqrt{3})$ и приведем его к алгебраическому виду:

$$\frac{a+b\sqrt{3}}{c+d\sqrt{3}} = \frac{(a+b\sqrt{3})(c-d\sqrt{3})}{(c+d\sqrt{3})(c-d\sqrt{3})} = \frac{(ac-3bd)(bc-ad)\sqrt{3}}{c^2-3d^2} = \frac{ac-3bd}{m} + \frac{bc-ad}{m}\sqrt{3} (*),$$

где $m = c^2 - 3d^2 = n(\beta)$ – норма числа $\beta = c + d\sqrt{3}$.

Найдем целые и дробные части чисел $\frac{ac-3bd}{m}$ и $\frac{bc-ad}{m}$. Введем следующие обозначения: $a_1 = [\frac{ac-3bd}{m}]$ и $b_1 = [\frac{bc-ad}{m}]$ для целых частей указанных дробей.

Дробные части этих чисел обозначим как $a_2 = \{\frac{ac-3bd}{m}\}$ и $b_2 = \{\frac{bc-ad}{m}\}$.

Дробные части a_2 и b_2 определяются как разности $a_2 = \frac{ac-3bd}{m} - a_1$ и $b_2 = \frac{bc-ad}{m} - b_1$. Отсюда следует, что $0 \leq a_2 < 1$, $0 \leq b_2 < 1$. Для a_2 (также и для b_2)

возможны следующие случаи:

1-ый случай.

$$0 \leq a_2 < \frac{1}{2}; (0 \leq b_2 < \frac{1}{2});$$

2-ой случай.

$$a_2 = \frac{1}{2}; (b_2 = \frac{1}{2})$$

3-ий случай.

$$a_2 > \frac{1}{2}; (b_2 > \frac{1}{2})$$

В первом случае, в силу равенства $a_2 + a_1 = \frac{ac-3bd}{m}$, целое число a_1 будет ближайшим числом к дроби $\frac{ac-3bd}{m} = x$.

Если имеет место второй случай, то $\frac{ac-3bd}{m} = a_1 + \frac{1}{2}$. Эти равенства можно представить иначе: $\frac{ac-3bd}{m} = (a_1 + 1) - \frac{1}{2}$. Найдем расстояния от чисел $\frac{ac-3bd}{m}$ до a_1 и $a_1 + 1$. На основании геометрической интерпретации модуля числа, имеем: $\left| \frac{ac-3bd}{m} - a_1 \right| = \left| \frac{1}{2} \right|$, $\left| \frac{ac-3bd}{m} - (a_1 + 1) \right| = \left| -\frac{1}{2} \right| = \frac{1}{2}$.

Следовательно, целые числа a_1 и $a_1 + 1$ находятся на одном и том же расстоянии от числа $\frac{ac-3bd}{m} = x$ на числовой прямой. Поэтому, любое из чисел a_1 или $a_1 + 1$ можно взять в качестве ближайшей к дроби x . Чтобы выбрать однозначно ближайшее число, условились выбрать наибольшее из чисел a_1 и $a_1 + 1$.

В третьем случае дробь x можно представить так: $x = (a_1 + 1) + (a_2 - 1)$.

Тогда $|a_2 - 1| = 1 - a_2 < 1 - \frac{1}{2} = \frac{1}{2}$ и ближайшим целым числом к числу x будет целое число $a_1 + 1$. Ближайшее целое число к числу x в литературе обозначается x' . Исходя из рассмотренного, получаем, что каждое целое число x можно представить в виде суммы $x = x' + \tilde{x}$, где x' – ближайшее целое число к x , а $\tilde{x}$ удовлетворяет условию $|\tilde{x}| \leq \frac{1}{2}$. Ясно, что $\tilde{x} = x - x'$.

Теперь равенство (*) можно представить следующим образом:

$$\frac{a + b\sqrt{3}}{c + d\sqrt{3}} = \left(\frac{a + b\sqrt{3}}{m} \right)' + \left(\frac{bc - ad}{m} \right)' + \left(\frac{a + b\sqrt{3}}{m} \right)^* + \left(\frac{bc - ad}{m} \right)^* \sqrt{3}$$

Умножим обе части полученного равенства на $c + d\sqrt{3}$, получим:

$$a + b\sqrt{3} = (c + d\sqrt{3}) \left(\left(\frac{a+b\sqrt{3}}{m} \right)' + \left(\frac{bc-ad}{m} \right)' \right) + (c + d\sqrt{3}) \left(\left(\frac{a+b\sqrt{3}}{m} \right)^* + \left(\frac{bc-ad}{m} \right)^* \sqrt{3} \right).$$

$$\text{Введем обозначения } r, r = (c + d\sqrt{3}) \left(\left(\frac{a+b\sqrt{3}}{m} \right)^* + \left(\frac{bc-ad}{m} \right)^* \sqrt{3} \right).$$

Число r представляет собой разность $\alpha - \beta\gamma$ чисел из $\mathbb{Z}[\sqrt{3}]$, поэтому $r \in$

$\mathbb{Z}[\sqrt{3}]$.

Полученное равенство примет вид: $\alpha = \beta\gamma + r$.

Возможен случай: $r = 0$ или $r \neq 0$. Во втором случае найдем модуль нормы числа r :

$$|n(r)| = |n(c + d\sqrt{3})| \left| n\left(\frac{a+b\sqrt{3}}{m}\right)^* + \left(\frac{bc-ad}{m}\right)^* \sqrt{3} \right| = |n(c + d\sqrt{3})| \left| \left(\left(\frac{a+b\sqrt{3}}{m}\right)^*\right)^2 - 3\left(\left(\frac{bc-ad}{m}\right)^*\right)^2 \right|.$$

На основании свойства $|x + y| \leq |x| + |y|$ модуля и неравенства $|\tilde{x}| \leq \frac{1}{2}$,

получим:
$$\left| \left(\left(\frac{a+b\sqrt{3}}{m}\right)^*\right)^2 - 3\left(\left(\frac{bc-ad}{m}\right)^*\right)^2 \right| \leq \left| \left(\left(\frac{a+b\sqrt{3}}{m}\right)^*\right)^2 - 3\left(\left(\frac{bc-ad}{m}\right)^*\right)^2 \right| \leq \frac{3}{4}.$$

Следовательно, $|n(r)| \leq |n(c + d\sqrt{3})| * \frac{3}{4} < |n(c + d\sqrt{3})|$, ч. т. д.

Эту теорему можно сформулировать еще следующим образом.

Теорема. Квадратичное кольцо $\mathbb{Z}[\sqrt{3}]$ является евклидовым кольцом с евклидовой нормой h , определенной условием $h(\alpha) = |n(\alpha)|$.

Теорема. В кольце $\mathbb{Z}[\sqrt{3}]$ каждый отличный от 0 необратимый элемент можно, с точностью до ассоциированности, разложить на простые множители.

Способ доказательства первой теоремы позволяет сформулировать основные шаги алгоритма деления с остатком в квадратичном кольце $\mathbb{Z}[\sqrt{3}]$.

2.11. Алгоритм деления с остатком в $\mathbb{Z}[\sqrt{3}]$

Задача. Разделить число $a + b\sqrt{3}$ на число $c + d\sqrt{3}$ в кольце $\mathbb{Z}[\sqrt{3}]$.

Шаг 1. Составим дробь $\frac{a+b\sqrt{3}}{c+d\sqrt{3}} = x$

Шаг 2. В поле $\mathbb{Q}(\sqrt{3})$ число x представим в алгебраической форме

$$\begin{aligned} x &= \frac{(a + b\sqrt{3})(c - d\sqrt{3})}{(c + d\sqrt{3})(c - d\sqrt{3})} = \frac{(ac - 3bd) + (bc - ad)\sqrt{3}}{c^2 - 3d^2} = \\ &= \frac{ac - 3bd}{c^2 - 3d^2} - \frac{bc - ad}{c^2 - 3d^2} \sqrt{3}. \end{aligned}$$

Шаг 3. Находим ближайшее число $a_1 = \left(\frac{ac-3bd}{c^2-3d^2}\right)'$, $c_l = \left(\frac{bc-ad}{c^2-3d^2}\right)'$.

Шаг 4. Находим $a_1^* = \frac{ac-3bd}{c^2-3d^2} - a_1$, $c_1^* = \frac{bc-ad}{c^2-3d^2} - c_1$.

Шаг 5. Представим x в виде суммы найденных в шаге 4 чисел:

$$x = a_1 + a_1^* - c_1\sqrt{3} - c_1^*\sqrt{3} = (a_1 - c_1\sqrt{3}) + (a_1^* - c_1^*\sqrt{3})$$

Шаг 6. Обе части равенства, полученного в шаге 5, умножим на $c + d\sqrt{3}$:

$$a + b\sqrt{3} = (c + d\sqrt{3})(a_1 - c_1\sqrt{3}) + (c + d\sqrt{3})(a_1^* - c_1^*\sqrt{3})$$

Полученное равенство и есть результат деления с остатком числа $a + b\sqrt{3}$ на $c + d\sqrt{3}$.

Пример.

1. Разделить число -11 на 3 с остатком в кольце $\mathbb{Z}[\sqrt{3}]$.

Решение. Воспользуемся алгоритмом деления с остатком в $\mathbb{Z}[\sqrt{3}]$

Шаг 1. Составим дробь $-\frac{11}{3}$.

Шаг 2. $-\frac{11}{3} = -\frac{11}{3} + 0 * \sqrt{3}$

Шаг 3. Находим целую и дробную части числа $-\frac{11}{3}$: $-\frac{11}{3} = \frac{-12+1}{3} = -4 + \frac{1}{3}$. Отсюда $\left[\frac{11}{3}\right] = -4$, а дробная часть $\left\{-\frac{11}{3}\right\} = \frac{1}{3}$. $\left(-\frac{11}{3}\right)' = -4$ – ближайшее число.

Шаг 4. Отклонение числа $-\frac{11}{3}$ от ближайшего числа к нему -4 равно $\left(-\frac{11}{3}\right)^* = -\frac{11}{3} - (-4) = \frac{1}{3}$.

Шаг 5. Запишем число $-\frac{11}{3}$, используя ближайшее число и отклонение:

$$-\frac{11}{3} = -4 + \frac{1}{3}.$$

Шаг 6. Умножим обе части полученного в шаге 5 равенства на 3 :

$$-11 = 3(-4) + 1.$$

Так как $h(3) = |n(3)| = |9| = 9$, $h(1) = |n(1)| = |1| = 1$, то $h(1) < h(3)$. Таким образом, полученное в шаге 6 равенство выражает результат деления с остатком в кольце $\mathbb{Z}[\sqrt{3}]$.

Заметим, что равенство $-11 = 3(-3) + (-2)$ также выражает результат

деления числа -11 на 3 в $\mathbb{Z}[\sqrt{3}]$, так как $h(-2) = |n(-2)| = |4| = 4$, $h(3) = 9$. Причем $h(-2) < h(3)$. Этот пример показывает, что деление с остатком в $\mathbb{Z}[\sqrt{3}]$ не выполняется единственным образом. Таким образом, описанный алгоритм деления с остатком в $\mathbb{Z}[\sqrt{3}]$ всегда дает результат, но возможны и другие результаты.

В процессе деления с остатком приходится решать задачу **отыскания ближайшего числа к действительному числу x** . Отметим короткий алгоритм решения этой задачи. Пусть x – данное действительное число. Необходимо найти число x' , ближайшее к x , а также его отклонения $x^* = x - x'$ от ближайшего к нему целому числу x' .

Шаг 1. Находим целую часть $[x]$ данного числа x .

Шаг 2. Находим дробную часть этого числа $\{x\} = x - [x]$.

Шаг 3. Сравним $\{x\}$ с $\frac{1}{2}$. Если:

- 1) $\{x\} < \frac{1}{2}$, то $x' = [x]$.
- 2) $\{x\} = \frac{1}{2}$, то $x' = \max\{[x], [x] + 1\}$
- 3) $\{x\} > \frac{1}{2}$, то $x' = [x] + 1$.

Шаг 4. Найдем отклонение x^* от x до x' по формуле $x^* = x - x'$.

Примеры.

1) Найдите x' и x^* следующих чисел:

а) $-9,2$; б) $-9,5$; в) $-9,7$.

Решение.

а) Воспользуемся описанным алгоритмом нахождения ближайшего целого числа.

Шаг 1. Находим целую часть $[-9,2] = -10$.

Шаг 2. Находим дробную часть $\{-9,2\} = -9,2 - (-10) = 0,8$

Шаг 3. Сравним $\{-9,2\}$ с $\frac{1}{2}$: $\{-9,2\} = 0,8 > 0,5$. Имеем $(-9,2)' = [-9,2] + 1 = -9$.

Шаг 4. Находим отклонение $(-9,2)^* = (-9,2) - (-9,2)' = -9,2 + 9 = -0,2$.

Ответ: $(-9,2)' = -9$, а $(-9,2)^* = -0,2$.

б) 1. $[-9,5] = -10$;

2. $\{-9,5\} = -9,5 - 10 = 0,5$.

3. $\{-9,5\} = 0,5$, поэтому $(-9,5)' = \max\{-10; -10 + 1\} = -9$.

4. $(-9,5)^* = -9,5 - (-9) = -0,5$

в) 1. $[-9,7] = -10$;

2. $\{-9,7\} = -9,7 - (-10) = 0,3$

3. $\{-9,7\} < \frac{1}{2}$. Значит, $x' = -10$

4. $(-9,7)^* = 0,3$

Задачу отыскания ближайшего числа можно решать графически, используя изображения действительных чисел на числовой оси.

Предположим, что надо найти ближайшее число к числу $-9,2$. На числовой оси изобразим это число в виде точки и ближайшую пару целых чисел, между которыми находим это число, и выберем то число, которое ближе к числу $-9,2$:



Из рисунка видно, что $(-9,2)' = -9$. Отклонения числа $(-9,2)$ от ближайшего целого числа -9 находим как расстояния между ними со знаком $(-)$, так как числа находятся в отрицательной полуоси $(-9,2)^* = -|-9,2 - 9| = -0,2$.

Упражнения:

1. Найдите:

а) $(-1,7)'$ и $(-1,7)^*$;

б) $(-1,5)'$ и $(-1,5)^*$;

в) $(-1,8)'$ и $(-1,8)^*$;

г) $(0,5)'$ и $(0,5)^*$;

д) $(-0,5)'$ и $(-0,5)^*$;

е) $(-7)'$ и $(-7)^*$;

ж) $(0)'$ и 0^* .

2. Решите предыдущие задачи графически.

3. Выполните деления с остатком в $\mathbb{Z}[\sqrt{3}]$:

а) $8 - 3\sqrt{3}$ на $5 + 2\sqrt{3}$;

б) $118 - 71\sqrt{3}$ на $23 + \sqrt{3}$;

в) $5 + 3\sqrt{3}$ на $3 - 2\sqrt{3}$;

г) $13 + 5\sqrt{3}$ на $7 + 3\sqrt{3}$;

д) $3 + \sqrt{3}$ на $\sqrt{3}$;

ГЛАВА 3. ВНЕКЛАССНЫЕ ЗАНЯТИЯ ПО ТЕМЕ «КВАДРАТИЧНЫЕ КОЛЬЦА»

4.1. Об истории внеклассных занятий по математике в школах СССР и современной России

История возникновения и развития школьного образования в России и в странах ближнего зарубежья начинается в первые годы Советской власти. Большое внимание в советской школе обращалось на внеклассные занятия учащихся, в частности и по математике. Эти занятия оказались мощным средством получения углубленных знаний по математике. Форма работы была разнообразной. В школах создавались кружки по математике, проводились и проводятся конкурсы и математические олимпиады, математические вечера, викторины и другие виды работ. В 60-е годы XX века возникла новая форма проведения внеклассных занятий по математике, как факультативные занятия. При крупных научных центрах возникли математические школы. Многие выпускники этих школ впоследствии стали известными математиками.

В связи с развитием внеклассной работы по математике было обращено внимание на подготовку и издание популярных книг и брошюр по математике, начиная с 1925 года. Отметим здесь такие книги Я.И. Перельмана, как «Занимательная геометрия на вольном воздухе и дома» (1925 г.), «Занимательная математика» (1927 г.), «Занимательные задачи» (1928 г.), «Занимательная арифметика» (1932 г.), «Занимательная алгебра» (1938 г.), «Живая математика» (1934 г.). Эти книги были переизданы в СССР несколько раз.

В те же годы была создана серия книг, которые составили библиотеку для учащихся по математике. Эти книги имели целью повышение интереса учеников к математике. При написании этих книг принимали участие математики и методисты: П.С. Александров, В.А. Ефремович, В.М. Бредис и другие. Создана «Библиотека для математического кружка» усилиями Г.М.

Фихтенгольца, О.К. Житомирского и других математиков.

С 1951 г. начали выходить из печати известные «Лекции по математике», которые пользовались и пользуются до сих пор во многих вузах, школах не только у нас в России, но и во многих зарубежных странах.

Школы юных математиков, которые были организованы при вузах, впервые созданы замечательным ученым академиком А.И. Мальцевым в г. Иваново при Ивановском педагогическом институте, где в то время работал А.И.Мальцев профессором. Идею школы юных математиков подхватили многие университеты, пединституты, а так же технические вузы. Для этих школ была создана ценная математическая литература.

В связи с возникновением математических олимпиад в СССР (первая олимпиада была проведена в 1934 г.) и в других странах, появились книги: Р.Н. Бончковский «Московские олимпиады 1935 и 1936 годов» (1936 г.), «Сборник задач в помощь участникам школьных математических олимпиад» (1950 г.) и т.д. Появились сборники зарубежных математических, а так же сборники международных математических олимпиад. Следует сказать, почти во всех международных олимпиадах советские школьники занимали первые и вторые места по очкам, присужденным за решение задач.

4.2. Рабочая программа факультативного курса «Основные элементы квадратичного кольца $\mathbb{Z}[\sqrt{3}]$ »

Пояснительная записка

Данный курс предназначен для учащихся 10-11 классов, проявляющих повышенный интерес к математике и собирающихся продолжить образование в учебных заведениях математического профиля.

Цель курса – расширить и углубить знания, умения и навыки учащихся по теме «Основные элементы квадратичного кольца $\mathbb{Z}[\sqrt{3}]$ », развивая при этом математическое мышление учащихся.

Задачи курса:

- сформировать систему знаний и умений по теме «Основные

элементы квадратичного кольца $\mathbb{Z}[\sqrt{3}]$ »;

- подготовить учащихся к дальнейшему обучению в других учебных заведениях;
- способствовать развитию познавательных интересов и способности самостоятельно добывать знания;
- способствовать развитию логического мышления учащихся.

Рабочая программа по факультативному курсу на тему «Основные элементы квадратичного кольца $\mathbb{Z}[\sqrt{3}]$ » разработана на один учебный год. Занятия проводятся один раз в неделю. Основная форма проведения занятий – лекции и практики. Итоговые контрольные мероприятия представлены в формах коллоквиума и контрольной работы.

Таблица 1.

**Календарно-тематическое планирование по теме: «Основные
элементы квадратичного кольца $\mathbb{Z}[\sqrt{3}]$ »**

№	Тема	Количество часов		
		Общее	Лекции	Практики
1	Квадратичное расширение $\mathbb{Z}[\sqrt{3}]$ кольца целых чисел (элементы множества $\mathbb{Z}[\sqrt{3}]$, операции, кольцо $\mathbb{Z}[\sqrt{3}]$)	3	1	2
2	Квадратичное кольцо $\mathbb{Z}[\sqrt{3}]$ и его норма (отсутствие делителей нуля, алгебраическая норма, обратимые элементы)	3	1	2
3	Совокупность дробей вида $\frac{a+b\sqrt{3}}{c+d\sqrt{3}}$ и их свойства	2	1	1
4	Задача об определении обратной дроби для дроби вида $\frac{a+b\sqrt{3}}{c+d\sqrt{3}}$. Теорема об обратных элементах	2	1	1
5	Отношение делимости и его свойства в кольце $\mathbb{Z}[\sqrt{3}]$	3	1	2
6	Деление с остатком в кольце $\mathbb{Z}[\sqrt{3}]$. Евклидова норма	3	1	2
7	Деление с остатком в кольце $\mathbb{Z}[\sqrt{3}]$. Алгоритм деления с остатком	3	1	2

Продолжение таблицы 1.

8	Алгоритм Евклида в квадратичном кольце $\mathbb{Z}[\sqrt{3}]$	3	1	2
9	Наибольший общий делитель в кольце $\mathbb{Z}[\sqrt{3}]$. Алгоритм отыскания НОД двух чисел из этого кольца	3	1	2
10	Решение задач на пройденные темы	2		2
11	Коллоквиум на тему «Основные элементы квадратичного кольца $\mathbb{Z}[\sqrt{3}]$ »	1		
12	Контрольная работа на тему «Основные элементы квадратичного кольца $\mathbb{Z}[\sqrt{3}]$ »	1		
13	Итоговое занятие (рефлексия)	1		
	Итого:	30	9	18

4.3. Примеры факультативных занятий по теме

«Квадратичное кольцо $\mathbb{Z}[\sqrt{3}]$ »

Тема факультативного занятия №1: Квадратичное расширение $\mathbb{Z}[\sqrt{3}]$ кольца целых чисел.

Цель: создать условия учащимся для успешного изучения темы расширения кольца целых чисел $\mathbb{Z}$ с помощью иррационального числа $\sqrt{3}$.

Классы: 10–11 класс

Форма проведения: лекция (приобретение новых знаний)

Продолжительность: 45 минут.

План урока.

1. Определение множества $\mathbb{Z}[\sqrt{3}]$.
2. Сложение и умножение чисел из $\mathbb{Z}[\sqrt{3}]$. Свойство этих операций.
3. Кольцо $(\mathbb{Z}[\sqrt{3}], +, *)$. Нуль и единица этого кольца.

Ход урока.

- Добрый день, ребята! Сегодня мы познакомимся с крайне увлекательной темой. Но для этого давайте вернёмся к тому, что мы ранее проходили. Ребята, вы знаете, что $\sqrt{3}$ – число иррациональное. Ранее, мы уже доказывали это утверждение на уроках алгебры, давайте сделаем это и сейчас.

Какой метод мы для этого использовали? (*Метод от противного*).

- Предположим, что число $\sqrt{3}$ – рациональное, какой вид имеет рациональное число? (*Рациональное число – это число, которое представимо в виде $\frac{a}{b}$, где a, b – целые, взаимно простые числа*).

То есть $\sqrt{3} = \frac{a}{b}$, где a, b – целые числа. Выразим a и возведём обе части данного равенства в квадрат. ($a = b\sqrt{3}$. Возводя обе части этого равенства в квадрат, получим $a^2 = 3b^2$)

- Отсюда заключаем, что по свойствам делимости a^2 делится на 3. Если делится на 3 квадрат числа, то будет ли само число делиться на 3? (*Да, ведь в противном случае квадрат числа будет не делиться на 3*)

- Значит, $a = 3p$. Подставим в исходное равенство, что мы получим? ($9p^2 = 3b^2$; значит $b^2 = 3p^2$)

- Отсюда аналогично с выводом о числе a , можем сказать, что $b = 3q$. Что же у нас получилось? (*Мы пришли к противоречию, т.к. ранее предполагали, что a и b – взаимно простые числа, т.е. наше предположение было не верно. Таким образом, $\sqrt{3}$ – число иррациональное*).

- Этот вывод поможет нам прийти к новому множеству чисел – множество всех чисел вида $a + b\sqrt{3}$, где a, b – целые числа. Это множество обозначим через $\mathbb{Z}[\sqrt{3}]$. Таким образом, $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} | a, b \in \mathbb{Z}\}$. Запишем это в тетрадь. Рассмотрим несколько **примеров**: $a + b\sqrt{3}$. Это множество в некоторых смыслах похоже на все известные нам множества. Позднее мы в этом не раз убедимся. А пока ответьте на следующий вопрос: как вы думаете, когда два элемента из данного множества равны: $a + b\sqrt{3} = c + d\sqrt{3}$? (*Выдвигают предположения, одно из них, если $a = c$ и $b = d$*).

- Молодцы, действительно, существует следующая **теорема**. Равенство $a + b\sqrt{3} = c + d\sqrt{3}$ имеет место тогда и только тогда, когда $a = c$ и $b = d$.

- Как мы знаем, каждая теорема требует доказательства. Давайте докажем и её:

1. Рассмотрим равенство $a + b\sqrt{3} = c + d\sqrt{3}$, тогда в поле действительных чисел будем иметь $(a - c) + (b - d)\sqrt{3} = 0$.

Предположим, что $b - d \neq 0$. Тогда $\sqrt{3} = -\frac{a-c}{b-d}$, где $a - c$, $b - d$ это целые числа. Следовательно, число $-\frac{a-c}{b-d}$ – рациональное число. По доказанному, $\sqrt{3}$ – рациональное. Получим противоречие. Значит $b - d = 0$, тогда $a - c = 0$. Значит, $a = c$ и $b = d$.

1. Пусть $a = c$ и $b = d$. Тогда $b - d = 0$, $a - c = 0$.

Тогда $(a - c) + (b - d)\sqrt{3} = 0 + 0\sqrt{3} = 0$. Отсюда $a + b\sqrt{3} = c + d\sqrt{3}$.

- Теперь давайте перейдем к операциям. Какие основные операции у нас есть на множестве действительных чисел? (*сложение, вычитание, умножение, деление*).

- Приступим к первой из них. Довольно легко понять, как определяется операции сложения в $\mathbb{Z}[\sqrt{3}]$. Если взять два произвольных элемента $a + b\sqrt{3}$ и $c + d\sqrt{3}$ из этого кольца, то как будет выглядеть сумма? $((a + b) + (c + d)\sqrt{3})$.

- Верно! Запишем определение. Суммой $(a + b\sqrt{3}) + (c + d\sqrt{3})$ называется элемент $(a + b) + (c + d)\sqrt{3}$. Приведем пример: $(-1 + 2\sqrt{3}) + (4 - \sqrt{3}) = 3 + \sqrt{3}$.

- Как и для любой операции, для операции сложения в $\mathbb{Z}[\sqrt{3}]$. Существуют свои свойства. Для начала вспомним, какие свойства сложения есть на множестве действительных чисел? (*Переместительный, сочетательный*).

- Существуют еще два свойства, связанные со сложением нуля с элементами, а также с противоположными элементами. Давайте попытаемся описать эти свойства для элементов данного множества (*Учащиеся выдвигают предположения*).

Верно! Запишем в тетрадь:

Для любых $\alpha, \beta, \gamma \in \mathbb{Z}[\sqrt{3}]$ выполняются равенства:

1. $\alpha + \beta = \beta + \alpha$ (коммутативность сложения или переместительный

закон сложения).

2. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ (ассоциативность сложения или сочетательный закон).

3. Элемент $0 = 0 + 0\sqrt{3}$ обладает свойством: $\alpha + 0 = 0 + \alpha = \alpha$.

4. Для любого элемента $\alpha = a + b\sqrt{3}$ элемент $\alpha' = -a - b\sqrt{3}$ при сложении с α дает 0: $\alpha + \alpha' = 0$.

Элемент α' называется противоположным к элементу α и обозначает $-\alpha$.

- Теперь необходимо определить операции разности, однако мы уже это сделали, ведь разность можно определить через сложение. А теперь выполним следующие упражнения:

1. Решить уравнения $(3 + \sqrt{3}) + x = \sqrt{3}$.

2. Найдите сумму $1 + (3 + 4\sqrt{3}) + (-4 + 5\sqrt{3})$.

3. Вычислите $(9 - \sqrt{3}) - 3\sqrt{3} - 5$.

- Как же определяется операция умножения для двух любых элементов $\alpha = a + b\sqrt{3}$ и $\beta = c + d\sqrt{3}$? (Раскрыв скобки и приведя слагаемые $\alpha\beta = (ac + 3bd) + (ad + bc)\sqrt{3}$).

- Теперь определим свойства операции умножения. Какие свойства сложения есть на множестве действительных чисел? (*Переместительный, сочетательный, распределительный, связанный с умножением на единицу*)

- Давайте попытаемся описать эти свойства для элементов данного множества. (*Выдвигают свои предположения*)

- Верно! Обоснуем их и запишем в тетрадь:

Свойства операции умножения.

5. $\alpha\beta = \beta\alpha$, для любых $\alpha, \beta \in \mathbb{Z}[\sqrt{3}]$ (коммутативность).

Действительно, вычислим произведение $\beta\alpha$:

$$\beta\alpha = (c + d\sqrt{3})(a + b\sqrt{3}) = (ca + 3db) + (da + cb)\sqrt{3}.$$

Поскольку операция сложения и умножения целых чисел обладает свойством коммутативности, то:

$$ca + 3db = ac + 3bd \text{ и } (da + cb) \sqrt{3} = (ad + bc) \sqrt{3}.$$

Поэтому $\alpha\beta = \beta\alpha$.

6. Для любых элементов $\alpha, \beta, \gamma \in \mathbb{Z}[\sqrt{3}]$ имеет место равенство:

$$\alpha(\beta\gamma) = (\alpha\beta)\gamma$$

Это свойство доказывается аналогично.

7. Для каждого элемента $\alpha \in \mathbb{Z}[\sqrt{3}]$ и элемента $1 + 0\sqrt{3}$ выполняется равенство $\alpha(1 + 0\sqrt{3}) = (1 + 0\sqrt{3})\alpha = \alpha$.

Действительно, пусть $\alpha = a + b\sqrt{3}$, $a, b \in \mathbb{Z}[\sqrt{3}]$.

$$\text{Тогда } \alpha(1 + 0\sqrt{3}) = (a + b\sqrt{3})(1 + 0\sqrt{3}) = (a * 1 + 3b * 0) + (a * 0 + b * 1)\sqrt{3} = a + b\sqrt{3}.$$

В силу этого элемент $1 + 0\sqrt{3}$ называется единицей относительно операции умножения, заданного в $\mathbb{Z}[\sqrt{3}]$. Эту единицу кратко также обозначают 1.

8. Для любых элементов $\alpha, \beta, \gamma \in \mathbb{Z}[\sqrt{3}]$ выполняется равенство:

$$(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma.$$

Действительно, пусть $\alpha = a + b\sqrt{3}$, $\beta = c + d\sqrt{3}$, $\gamma = m + n\sqrt{3}$.

$$\begin{aligned} \text{Тогда } (\alpha + \beta)\gamma &= ((a + c) + (b + d)\sqrt{3})(m + n\sqrt{3}) = ((a + c)m + 3(b + d)n) + ((a + c)n + (b + d)m)\sqrt{3} \\ &= (am + cm + 3bn + 3dn) + (an + cm + 3bn + 3dn) + (an + cm + 3bn + 3dn) + (an + cm + 3bn + 3dn)\sqrt{3} \\ &= (am + 3bn) + (cm + 3dn) + ((an + bm) + (cn + dm))\sqrt{3} = ((am + 3bn) + (an + bm)\sqrt{3}) + ((cm + 3dn) + (cn + dm)\sqrt{3}) \\ &= \alpha\gamma + \beta\gamma. \end{aligned}$$

- Из последнего свойства можно получить следующее следствие. Для любых элементов $\alpha, \beta, \gamma \in \mathbb{Z}[\sqrt{3}]$ имеет место равенство

$$\gamma(\alpha + \beta) = \gamma\alpha + \gamma\beta.$$

Действительно, в силу коммутативности операции умножения в $\mathbb{Z}[\sqrt{3}]$, имеем $\gamma(\alpha + \beta) = (\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma = \gamma\alpha + \gamma\beta$, ч.т.д.

- Теперь выполним следующие упражнения:

1. Докажите свойство β^0 умножения в $\mathbb{Z}[\sqrt{3}]$.

2. Выполните указанные действия:

а) $(2 + \sqrt{3})(2 - \sqrt{3})$

б) $(2 + \sqrt{3})(\sqrt{3} - 2)$

в) $(3 + \sqrt{3})(3 - 2\sqrt{3}) + (5 - 7\sqrt{3})$

Итак, мы изучили операции на данном множестве и их свойства, теперь исходя из доказанных свойств операций, определенных в $\mathbb{Z}[\sqrt{3}]$ можно сформулировать теорему: Множество $\mathbb{Z}[\sqrt{3}]$ с введенными операциями сложения и умножения, обладающие свойствами 1 – 8, является **коммутативным ассоциативным кольцом с единицей**. Нулем этого кольца является число $0 + 0\sqrt{3}$, единицей кольца $\mathbb{Z}[\sqrt{3}]$ является число $1 + 0\sqrt{3}$. Запишем это в тетрадь.

- Подведём итог. Что мы узнали нового на данном занятии?
(Высказывают своё мнение)

- Верно, сегодня мы узнали много нового. На следующих занятиях мы с вами ещё глубже изучим свойства кольца $\mathbb{Z}[\sqrt{3}]$. А пока, до новых встреч, ребята!

Тема факультативного занятия №2: Квадратичное кольцо $\mathbb{Z}[\sqrt{3}]$ и его норма.

Цель: Создать условия учащимся для успешного изучения темы квадратичного кольца $\mathbb{Z}[\sqrt{3}]$ и его нормы.

Классы: 10-11 класс.

Форма проведения: лекция (приобретение новых знаний)

Продолжительность: 45 минут.

Ход урока.

- Здравствуйте, ребята! Мы продолжаем изучение кольца $\mathbb{Z}[\sqrt{3}]$, сегодня мы узнаем ещё больше нового о данном кольце. Для начала давайте вспомним, что мы проходили на прошлом факультативном занятии. Ответьте на следующие вопросы:

1. Что называется кольцом $\mathbb{Z}[\sqrt{3}]$?
2. Какие операции есть на данном множестве?
3. Назовите свойства операций.

А также решите следующие упражнения:

- 1) $(4 + 2\sqrt{3})(3 - 4\sqrt{3})$;
- 2) $(5 + \sqrt{3})(3 - 5\sqrt{3})$;
- 3) $(3 + 3\sqrt{3})(2 - \sqrt{3}) + (6 - 2\sqrt{3})$;

А теперь рассмотрим следующее определение: число $a + b\sqrt{3} \neq 0$ называется **делителем нуля**, если существует число $x + y\sqrt{3} \neq 0$ из $\mathbb{Z}[\sqrt{3}]$ такое, что $(a + b\sqrt{3})(x + y\sqrt{3}) = 0$.

Давайте покажем, что делителей нуля в $\mathbb{Z}[\sqrt{3}]$ нет. А именно, докажем, что имеет место теорема: Если $(a + b\sqrt{3})(x + y\sqrt{3}) = 0$ и $a + b\sqrt{3} \neq 0$, то $x + y\sqrt{3} = 0$.

- Итак, что нам дано? $((a + b\sqrt{3})(x + y\sqrt{3}) = 0$ и $a + b\sqrt{3} \neq 0$)

Что необходимо доказать? $(x + y\sqrt{3} = 0)$

Преобразуем первое равенство, используя определение произведения

элементов в кольце $\mathbb{Z}[\sqrt{3}]$. Что получим? $((ax + 3by) + (ay + ba)\sqrt{3} = 0)$.

Теперь воспользуемся определением равенства элементов в $\mathbb{Z}[\sqrt{3}]$, какая система получится? (Получим следующую систему линейных уравнений в кольце $\mathbb{Z}$:

$$\begin{cases} ax + 3by = 0 \\ bx + ay = 0. \end{cases}$$

Умножим обе части первого уравнения на (a) , а обе части второго уравнения на $(-3b)$, после чего полученные равенства сложим. В результате получим следующую систему:

$$\begin{cases} ax + 3by = 0, \\ (a^2 - 3b^2)x = 0. \end{cases}$$

Будет ли эта система равносильна исходной? *(Да)*

По условию $a + b\sqrt{3} \neq 0$, тогда $a^2 - 3b^2 \neq 0$. Действительно, покажем это методом от противного. Если $a^2 - 3b^2 = 0$ и $b \neq 0$, то $\frac{a^2}{b^2} = 3$, отсюда $\left|\frac{a}{b}\right| = \sqrt{3}$ – рациональное число. Получим противоречие. Значит $a^2 - 3b^2 \neq 0$ и $b = 0$, следовательно, $a^2 = 0$, то есть $a = 0$. Из полученных равенств получим $a + b\sqrt{3} = 0$. Противоречие. Значит, $a - b\sqrt{3} \neq 0$. Что тогда следует из последнего равенства системы? *(Тогда $x = 0$)*

- Мы получили первый вывод. Вернёмся к исходной системе, теперь умножим обе части первого уравнения на $(-b)$, второго на (a) . Затем полученные уравнения сложим:

$$\begin{cases} ax + 2by = 0 \\ (a^2 - 3b^2)y = 0 \end{cases}$$

- Проведите аналогичные рассуждения для второго уравнения. Какой вывод мы получим? *(Поскольку $a - b\sqrt{3} \neq 0$, то из второго уравнения находим $y = 0$)*

- Сделайте вывод о сумме $x + y\sqrt{3}$ ($x + y\sqrt{3} = 0$, что и требовалось доказать)

- Мы доказали данную теорему, т.е. делителей нуля в $\mathbb{Z}[\sqrt{3}]$ нет. Из данной теоремы следует:

Следствие 1. Если $(a + b\sqrt{3})(c + d\sqrt{3}) = 0$, то хотя бы один из сомножителей равен нулю.

Следствие 2. В кольце $\mathbb{Z}[\sqrt{3}]$ нет делителей нуля.

- При решении системы линейных уравнений мы получали выражение $a^2 - 3b^2$, которое связано с числом $a + b\sqrt{3}$. Это выражение часто возникает при решении задач. В связи с этим мы введем следующее определение: функция $n(a + b\sqrt{3}) = a^2 - 3b^2$ называется **алгебраической нормой** элемента $a + b\sqrt{3}$.

- Рассмотрим следующие примеры.

1. $n(1) = 1^2 = 1$;

2. $n(1 + \sqrt{3}) = 1^2 - 3 * 1^2 = -2$;

3. $n(4 + 2\sqrt{3}) = 4^2 - 3 * 2^2 = 4$;

4. $n(6 + 3\sqrt{3}) = 6^2 - 3 * 3^2 = 36 - 27 = 9$;

- Итак, мы ввели новое определение. Отметим свойства алгебраической нормы.

1. $n(1) = 1$;

2. Для любых элементов $\alpha, \beta \in \mathbb{Z}[\sqrt{3}]$ выполняется равенство $n(\alpha\beta) = n(\alpha)n(\beta)$.

- Докажем это равенство. Пусть $\alpha = a + b\sqrt{3}, \beta = c + d\sqrt{3}$. Тогда $\alpha\beta = (ac + 3bd) + (ad + bc)\sqrt{3}$, поэтому $n(\alpha\beta) = (ac + 3bd)^2 - 3(ad + bc)^2 = a^2c^2 + 9b^2d^2 - 3a^2d^2 - 3b^2c^2 = (a^2 - 3b^2)c^2 - 3(a^2 - 3b^2)d^2 = (a^2 - 3b^2)(c^2 - 3d^2) = n(\alpha)n(\beta)$.

3. Если α является делителем 1, то алгебраической нормой этого элемента α равна ± 1 .

- Докажем и это свойство. Пусть α – делитель единицы. Тогда $1 = \alpha * x$, где $x \in \mathbb{Z}[\sqrt{3}]$. Отсюда на основании свойства 1, получим $n(1) = n(\alpha)n(x)$,

значит $1 = n(\alpha)n(x)$. Поскольку $x \neq 0$, то $n(\alpha) \neq 0$. Следовательно, $n(\alpha)$ является делителем единицы в кольце $\mathbb{Z}$, поэтому $n(\alpha) = \pm 1$.

- Решим следующие задания. Найдите нормы чисел: 2 ; -1 ; $3 + \sqrt{3}$; $3 - \sqrt{3}$; $2 + \sqrt{3}$; $11 - 3\sqrt{3}$.

- В последнем свойстве мы рассмотрели особый элемент α . Что это за элемент? (α – делитель единицы)

- Введём определение. Элемент α кольца $\mathbb{Z}[\sqrt{3}]$ называется **обратимым**, если существует такой элемент β из $\mathbb{Z}[\sqrt{3}]$, что $\alpha\beta = 1$.

- Выясним, при каких условиях элементы кольца $\mathbb{Z}[\sqrt{3}]$ обратимы. Для этого рассмотрим следующую **теорему**. Элемент α кольца $\mathbb{Z}[\sqrt{3}]$ обратим тогда и только тогда, когда $n(\alpha) = \pm 1$.

- Если элемент $\alpha \in \mathbb{Z}[\sqrt{3}]$ обратим, то элемент $\beta \in \mathbb{Z}[\sqrt{3}]$ удовлетворяющий условию $\alpha\beta = 1$, обозначается: $\beta = \alpha^{-1}$.

- Рассмотрим примеры:

1. Число $\alpha = 2 + \sqrt{3}$ обратимо, так как $n(\alpha) = 2^2 - 3 \cdot 1^2 = 1$.

2. $\alpha^{-1} = -2 + \sqrt{3}$. Действительно, $\alpha\alpha^{-1} = (2 + \sqrt{3})(-2 + \sqrt{3}) = -4 + 3 = -1$

- Далее решим следующие упражнения:

1. Докажите, что числа $7 + 4\sqrt{3}$, $26 - 15\sqrt{3}$, $-7 + 4\sqrt{3}$, $-7 - 4\sqrt{3}$ обратимы в $\mathbb{Z}[\sqrt{3}]$.

2. Покажите, что если α – обратимое число в $\mathbb{Z}[\sqrt{3}]$, то число α^{-1} также обратимое число.

2. Покажите, что если α – обратимое число в $\mathbb{Z}[\sqrt{3}]$, то число α^{-1} также обратимое число.

- А наше сегодняшнее занятие хочу закончить цитатой А.Г. Конфоровича: «Математика уступает свои крепости лишь сильным и смелым». Подведем итог. Что мы узнали сегодня нового и интересного?

- Сегодня мы с вами изучили огромный теоретический материал. На

следующих занятиях мы уделим внимание упражнениям по нему. До новых встреч!

ЗАКЛЮЧЕНИЕ

В ходе исследования выпускной квалификационной работы мы получили следующие результаты: определили понятие «квадратичное кольцо», разработали алгоритм деления с остатком в кольце $\mathbb{Z}[\sqrt{3}]$, подобрали задачи и упражнения для решения в этом кольце, разработали рабочую программу факультативного «Основные элементы квадратичного кольца $\mathbb{Z}[\sqrt{3}]$ » и привели примеры занятий, изучили свойства квадратичного кольца.

Отметим эти свойства.

1. Кольцо, рассматриваемое в данной выпускной квалификационной работе, а именно квадратичное кольцо $\mathbb{Z}[\sqrt{3}]$ является областью целостности.
2. В этом кольце можно ввести отношение делимости, свойства которого такие же, как и свойства отношения делимости в кольце $\mathbb{Z}$ целых чисел.
3. В кольце $\mathbb{Z}[\sqrt{3}]$ можно выделить группу обратимых элементов.

Отметим основные свойства этого кольца:

- а) Группа обратимых элементов кольца $\mathbb{Z}[\sqrt{3}]$ бесконечна.
- б) Всякий обратимый элемент ε в кольце $\mathbb{Z}[\sqrt{3}]$ имеет вид: $\varepsilon = \pm\sqrt{3}$, где n – произвольное целое число. Обратимый элемент $2 + \sqrt{3}$ называется главным обратимым элементом.
- в) Кольцо $\mathbb{Z}[\sqrt{3}]$ является евклидовым.

В целом, данную работу можно рассматривать как дополнение к курсу алгебры и теории чисел. Изучение данного материала не входит в учебную программу по алгебре, поэтому актуальность изучения квадратичных колец обуславливается преемственностью при изучении этой темы в высших учебных заведениях. Многие вопросы, рассмотренные в работе доступны учащимся 10-11 классов, соответственно данный материал вполне можно использовать на факультативных занятиях.

СПИСОК ЛИТЕРАТУРЫ

1. Александров П.С., Маркушевич А.И., Хинчин А.Я. Энциклопедия элементарной математики. Книга 1. Арифметика. М.-Л. : ГТТИ, 1961. 448 с.
2. Алфутова Н.Б., Устинов А. В. Алгебра и теория чисел: сборник задач для матем. школ. 3-е изд., испр. и доп. М. : МЦНМО, 2009. 336 с.
3. Айерлэнд К., Роузен М. Классическое введение современную теорию чисел. М. : Мир, 1987. 428 с.
4. Беньш-Кривец В.В., Мельников О.В. Лекции по алгебре : группы, кольца, поля: учеб. пособие для математических специальностей. Минск : БГУ, 2008. 116 с.
5. Борович З.И., Шафаревич И.Р. Теория чисел. 3-е изд., доп. М. : Наука, 1985. 504 с.
6. Васильев А.В., Мазуров В.Д. Высшая алгебра : конспект лекций, в 2-х частях. Новосибирск : Новосибирский гос. ун-т, 2010. 143 с.
7. Винберг Э.Б. Курс алгебры. 2-е изд., испр. и доп. М. : изд-во «Факториал Пресс», 2001. 544 с.
8. Кострикин А.И. Введение в алгебру. Часть 1. Основы алгебры. 3-е изд. М. : физико-математическая литература, 2000. 272 с.
9. Куликов Л.Я. Алгебра и теория чисел : учеб. пособия для педагогических институтов. М. : изд-во «Высшая школа», 1979. 559 с.
10. Матысик О.В., Трофимук А.А. Теория чисел : курс лекций. М. : Брест, 2013. 105 с.
11. Родосский К.А. Алгоритм Евклида. М. : изд-во «Наука, 1988. – 240 с.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное
учреждение высшего образования

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ ИМ. В.Г. БЕЛИНСКОГО

Факультет физико-математических
и естественных наук

Кафедра
«Математическое образование»

Направление подготовки
44.03.01 Педагогическое образование
Профиль подготовки «Математика»
Форма обучения: очная

Утверждаю: зав. кафедрой
«25» сентября 2020 г.

 Паньженский В.И.

Задание

по ВКР студента Коротнёвой Кристины Алексеевны
(ФИО полностью)

Тема работы «Построение кольца $Z[\sqrt{3}]$ и его евклидовость».

Утверждена приказом по Университету от «25» ноября 2020 г. № 0883/о.

Срок сдачи студентом законченной работы «4» июня 2021 г.

КАЛЕНДАРНЫЙ ПЛАН ВЫПОЛНЕНИЯ ВКР

№ п/п	Перечень подлежащих разработке вопросов	Сроки выполнения	Примечания
1	Побор литературы по теме исследования	Октябрь	Выполнено
2	Изучение теоретического материала по теории колец, колец целостности.	Ноябрь	Выполнено
3	Составление и решение примеров, задач по теории колец целостности.	Декабрь, январь	Выполнено
4	Изучение квадратичного поля $Q(\sqrt{3})$ и квадратичного кольца $Z[\sqrt{3}]$.	Февраль, март	Выполнено
5	Составление задач и упражнений на отношение делимости в кольце $Z[\sqrt{3}]$.	Март, апрель	Выполнено
6	Евклидовость кольца $Z[\sqrt{3}]$.	Апрель	Выполнено
7	Деление с остатком в кольце $Z[\sqrt{3}]$. Составление и подбор упражнений на деление с остатком в кольце $Z[\sqrt{3}]$.	Апрель	Выполнено
8	Разработка рабочей программы факультативного курса «Основные элементы квадратичного кольца $Z[\sqrt{3}]$ » и конспектов двух занятий.	Май	Выполнено
9	Оформление работы и сдача на кафедру. Подготовка выступления.	Июнь	Выполнено

Дата выдачи задания «15» сентября 2020 г.

Руководитель С.И. Суматов А.И.
(подпись) (Ф.И.О.)

Задание принял к исполнению
Королев И.И. Королев И.И.
(подпись) (Ф.И.О.)

Ректору Пензенского
государственного университета
А.Д. Гулякову
студента (ки) 4 курса ФФМЕН
очной формы обучения

Коротковой Кристины
Алексеевны

ЗАЯВЛЕНИЕ

Я, Короткова Кристина Алексеевна,
Ф.И.О. студента

студент(ка) 4 курса очной формы обучения направления подготовки 44.03.01
Педагогическое образование профиля подготовки «Математика» прошу
провести проверку с использованием системы «Антиплагиат. ВУЗ»
бакалаврской работы на тему « Понятие кода Z[3] и его
единственность »,
выполненной мной самостоятельно, на содержание элементов плагиата.

Все прямые заимствования из печатных и электронных источников, а
также из защищенных ранее выпускных квалификационных работ,
кандидатских и докторских диссертаций имеют соответствующие ссылки.

Я ознакомлен с действующим Стандартом университета «Выпускная
квалификационная работа обучающихся по образовательным программам
высшего образования – программам бакалавриата, программам специалитета
и программам магистратуры», согласно которому обнаружение плагиата
является основанием для недопуска ВКР к защите и отчисления из
университета.

Короткова
подпись
04.06.21
дд.мм.гггг

ВКР представлена на проверку 04.06.21
дд.мм.гггг

Руководитель ВКР Сн Агзам Яхиевич Султанов
подпись И.О.Ф.

Протокол

проверки на оригинальность в системе «Антиплагиат. ВУЗ» выпускной квалификационной работы на тему «Построение кольца $Z[\sqrt{3}]$ и его евклидовость» студентки 4 курса Коротнёвой Кристины Алексеевны направления подготовки 44.03.01 Педагогическое образование профиля «Математика»
Руководитель ВКР Султанов А.Я.



Отчет о проверке на заимствования №1



Автор: Султанов Адгам Яхиевич sultanovaya@rambler.ru / ID: 163
Проверяющий: Султанов Адгам Яхиевич (sultanovaya@rambler.ru / ID: 163)
Организация: Пензенский государственный университет
Отчет предоставлен сервисом «Антиплагиат» - <http://pnzgu.antiplagiat.ru>

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 226
Начало загрузки: 11.06.2021 10:01:30
Длительность загрузки: 00:00:22
Имя исходного файла: DIPLOM.docx
Название документа: DIPLOM
Размер текста: 1 кБ
Тип документа: Выпускная квалификационная работа
Символов в тексте: 63683
Слов в тексте: 8224
Число предложений: 588

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Последний готовый отчет (ред.)
Начало проверки: 11.06.2021 10:01:53
Длительность проверки: 00:04:26
Комментарии: не указано
Поиск с учетом редактирования: да
Модули поиска: ИПС Адилет, Библиография, Сводная коллекция ЭБС, Интернет Плюс, Сводная коллекция РГБ, Цитирование, Переводные заимствования (RuEn), Переводные заимствования по eLIBRARY.RU (EnRu), Переводные заимствования по Интернету (EnRu), Переводные заимствования издательства Wiley (RuEn), eLIBRARY.RU, СПС ГАРАНТ, Медицина, Диссертации НББ, Перефразирования по eLIBRARY.RU, Перефразирования по Интернету, Патенты СССР, РФ, СНГ, Модуль поиска "ПГУ", СМИ России и СНГ, Шаблонные фразы, Кольцо вузов, Издательство Wiley, Переводные заимствования

ЗАИМСТВОВАНИЯ
12.48%

САМОЦИТИРОВАНИЯ
0%

ЦИТИРОВАНИЯ
2.62%

ОРИГИНАЛЬНОСТЬ
84.9%

11.06.2021

дд.мм.гггг.

подпись

Султанов А.Я.

И.О.Ф. руководителя ВКР

Отзыв
РУКОВОДИТЕЛЯ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ
на тему: «Построение кольца $\mathbb{Z}[\sqrt{3}]$ и его евклидовость»
студентки Коротнёвой Кристины Алексеевны
факультета физико-математических и естественных наук направления
подготовки 44.03.01 «Педагогическое образование», профиль подготовки
«математика», гр 17ФПМ1

Выпускная работа Коротнёвой К.А. посвящена элементам арифметики квадратичного кольца $\mathbb{Z}[\sqrt{3}]$ и возможности внедрения ее в качестве факультативного курса в среднюю школу.

Иррациональные числа занимают достаточно большое место в школьном курсе алгебры. Числа, изученные в ВКР Коротнёвой К.А. интересны тем, что они позволяют школьникам прийти к понятиям кольца, области целостности и к теории делимости в этих кольцах. Сказанное позволяет заключить об актуальности темы исследования.

Работа состоит из введения, трех глав, заключения и списка литературы. Во введении дано обоснование актуальности темы, выделены объект и предмет, цель исследования.

В первой главе приведены теоретические основы отношения делимости в евклидовых кольцах.

Во второй главе изучаются свойства квадратичного кольца $\mathbb{Z}[\sqrt{3}]$. Сначала дается определение квадратичного поля $\mathbb{Q}(\sqrt{3})$ и квадратичного кольца $\mathbb{Z}[\sqrt{3}]$. Затем понятие нормы элементов указанных алгебр. На основании нормы изучаются обратимые элементы в кольце $\mathbb{Z}[\sqrt{3}]$, ассоциированные элементы. Выделены простые и составные элементы этого кольца. Доказана евклидовость квадратичного кольца $\mathbb{Z}[\sqrt{3}]$.

Третья глава посвящена внеклассным занятиям по теме «квадратичные кольца». Разработана рабочая программа, приведены примеры факультативных занятий по этому курсу.

Работа автором самостоятельно, изложение материала построено правильно. Работа удовлетворяет требованиям, предоставленным к выпускным работам. Доклад правильно отображает содержание ВКР.

Считаю, что работа Коротнёвой К.А. заслужила оценку «отлично».

Руководитель, к.ф.-м.н., доцент,
доцент кафедры «Математическое образование»



Султанов А.Я.