



# АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

## ГРУППЫ, КОЛЬЦА И ПОЛЯ

2-е издание



**УМО ВО РЕКОМЕНДУЕТ**

УМО рекомендує

**ЮРАЙТ**  
поддержка  
biblio-online.ru

**С. В. Ларин**

# **АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ ГРУППЫ, КОЛЬЦА И ПОЛЯ**

**УЧЕБНОЕ ПОСОБИЕ ДЛЯ ВУЗОВ**

**2-е издание, исправленное и дополненное**

*Рекомендовано Учебно-методическим отделом высшего образования  
в качестве учебного пособия для студентов высших учебных заведений,  
обучающихся по естественнонаучным направлениям*

**Книга доступна на образовательной платформе «Юрайт» [urait.ru](https://urait.ru),  
а также в мобильном приложении «Юрайт.Библиотека»**

**Москва • Юрайт • 2022**



УДК 511.2(075.8)

ББК 22.132я73

Л25

**Автор:**

**Ларин Сергей Васильевич** — кандидат физико-математических наук, профессор кафедры алгебры, геометрии и методики их преподавания Института математики, физики и информатики Красноярского государственного педагогического университета имени В. П. Астафьева.

**Ларин, С. В.**

Л25

Алгебра и теория чисел. Группы, кольца и поля : учебное пособие для вузов / С. В. Ларин. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 160 с. — (Высшее образование). — Текст : непосредственный.

ISBN 978-5-534-05567-2

Учебное пособие адресовано в первую очередь студентам и аспирантам педагогических вузов математических специальностей и содержит материал по теории групп, колец и полей, излагаемый в рамках дисциплины «Алгебра» («Алгебра и теория чисел»). Вместе с тем изложение имеет целостный, замкнутый характер и может быть использовано всеми желающими для первичного знакомства с основами теории групп, колец и полей. В каждой главе материал расположен в порядке возрастания степени сложности, что способствует вариативному использованию пособия. Большое внимание уделяется примерам, которые предваряют введение новых понятий, на них отрабатывается и закрепляется изученный материал. Вопросы в конце параграфов, как правило, просты и способствуют усвоению основного содержания, а задачи помогают закрепить приложения теории.

УДК 511.2(075.8)

ББК 22.132я73

*Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав.*

ISBN 978-5-534-05567-2

© Ларин С. В., 2010

© Ларин С. В., 2018, с изменениями

© ООО «Издательство Юрайт», 2022

*Посвящаю светлой памяти  
моих учителей —  
Самсона Львовича Эдельмана  
и Николая Васильевича Лойко*

# Оглавление

|                                                                  |           |
|------------------------------------------------------------------|-----------|
| <b>Предисловие .....</b>                                         | <b>9</b>  |
| <b>Глава 1. Группы .....</b>                                     | <b>11</b> |
| 1.1. Определение группы, примеры и основные свойства групп ..... | 11        |
| 1.1.1. Определение группы, терминология .....                    | 11        |
| 1.1.2. Примеры групп.....                                        | 14        |
| 1.1.3. Основные свойства групп .....                             | 19        |
| 1.1.4. Подгруппы .....                                           | 21        |
| <i>Контрольные вопросы.....</i>                                  | <i>22</i> |
| <i>Задачи .....</i>                                              | <i>22</i> |
| 1.2. Порядок элемента группы .....                               | 23        |
| 1.2.1. Определение и примеры .....                               | 23        |
| 1.2.2. Основные свойства порядков элементов группы .....         | 25        |
| <i>Контрольные вопросы.....</i>                                  | <i>25</i> |
| <i>Задачи .....</i>                                              | <i>26</i> |
| 1.3. Циклические группы.....                                     | 26        |
| 1.3.1. Определение и примеры .....                               | 26        |
| 1.3.2. Подгруппы циклических групп .....                         | 28        |
| 1.3.3. Порождающие элементы циклической группы .....             | 29        |
| <i>Контрольные вопросы.....</i>                                  | <i>30</i> |
| <i>Задачи .....</i>                                              | <i>31</i> |
| 1.4. Смежные классы.....                                         | 31        |
| 1.4.1. Определение и примеры .....                               | 31        |
| 1.4.2. Основные свойства смежных классов .....                   | 33        |
| 1.4.3. Теорема Лагранжа и следствия из нее .....                 | 34        |
| <i>Контрольные вопросы.....</i>                                  | <i>36</i> |
| <i>Задачи .....</i>                                              | <i>36</i> |
| 1.5. Нормальная подгруппа и факторгруппа .....                   | 37        |
| 1.5.1. Определение нормальной подгруппы, примеры .....           | 37        |
| 1.5.2. Факторгруппа.....                                         | 39        |
| 1.5.3. Аддитивная группа классов вычетов .....                   | 40        |

|                                                                                                |           |
|------------------------------------------------------------------------------------------------|-----------|
| 1.5.4. Мультипликативная группа классов вычетов .....                                          | 41        |
| 1.5.5. Классы сопряженных элементов .....                                                      | 42        |
| <i>Контрольные вопросы</i> .....                                                               | 44        |
| <i>Задачи</i> .....                                                                            | 44        |
| 1.6. Изоморфизмы групп .....                                                                   | 45        |
| 1.6.1. Определение и примеры .....                                                             | 45        |
| 1.6.2. Основные свойства изоморфизмов групп .....                                              | 47        |
| 1.6.3. Изоморфизмы циклических групп .....                                                     | 48        |
| 1.6.4. Связь конечных групп с группами подстановок .....                                       | 49        |
| <i>Контрольные вопросы</i> .....                                                               | 51        |
| <i>Задачи</i> .....                                                                            | 51        |
| 1.7. Гомоморфизмы групп .....                                                                  | 52        |
| 1.7.1. Определение и свойства гомоморфизмов групп.<br>Ядро гомоморфизма .....                  | 52        |
| 1.7.2. Теорема о гомоморфизмах .....                                                           | 53        |
| <i>Контрольные вопросы</i> .....                                                               | 55        |
| <i>Задачи</i> .....                                                                            | 55        |
| 1.8*. Конечные абелевы группы .....                                                            | 55        |
| 1.8.1. Прямое произведение подгрупп .....                                                      | 55        |
| 1.8.2. Разложение циклических групп в прямое<br>произведение своих подгрупп .....              | 57        |
| 1.8.3. Разложение конечной абелевой группы в прямое<br>произведение циклических подгрупп ..... | 58        |
| <i>Контрольные вопросы</i> .....                                                               | 60        |
| <i>Задачи</i> .....                                                                            | 60        |
| <b>Глава 2. Кольца и поля</b> .....                                                            | <b>62</b> |
| 2.1. Определение и основные свойства колец .....                                               | 62        |
| 2.1.1. Определение и примеры колец .....                                                       | 62        |
| 2.1.2. Основные свойства колец .....                                                           | 64        |
| <i>Контрольные вопросы</i> .....                                                               | 64        |
| <i>Задачи</i> .....                                                                            | 65        |
| 2.2. Определение и основные свойства полей .....                                               | 65        |
| 2.2.1. Определение поля, примеры .....                                                         | 65        |
| 2.2.2. Основные свойства полей .....                                                           | 67        |
| <i>Контрольные вопросы</i> .....                                                               | 69        |
| <i>Задачи</i> .....                                                                            | 69        |
| 2.3. Подполя, подкольца, идеалы .....                                                          | 69        |
| <i>Контрольные вопросы</i> .....                                                               | 71        |
| <i>Задачи</i> .....                                                                            | 71        |

|                                                                                          |           |
|------------------------------------------------------------------------------------------|-----------|
| 2.4. Изоморфизмы и гомоморфизмы колец и полей .....                                      | 72        |
| <i>Контрольные вопросы</i> .....                                                         | 73        |
| <i>Задачи</i> .....                                                                      | 74        |
| 2.5. Характеристика кольца и поля .....                                                  | 74        |
| <i>Контрольные вопросы</i> .....                                                         | 77        |
| <i>Задачи</i> .....                                                                      | 77        |
| <b>Глава 3. Делимость в кольцах .....</b>                                                | <b>78</b> |
| 3.1. Основные понятия теории делимости в области целостности .....                       | 78        |
| 3.1.1. Область целостности .....                                                         | 78        |
| 3.1.2. Определение и основные свойства делимости .....                                   | 79        |
| 3.1.3. Наибольший общий делитель .....                                                   | 82        |
| <i>Контрольные вопросы</i> .....                                                         | 83        |
| <i>Задачи</i> .....                                                                      | 83        |
| 3.2. Факториальные кольца .....                                                          | 84        |
| 3.2.1. Простые элементы области целостности .....                                        | 84        |
| 3.2.2. Определение факториального кольца и примеры разложений на простые множители ..... | 86        |
| 3.2.3. Нахождение НОД и НОК в факториальном кольце .....                                 | 88        |
| <i>Контрольные вопросы</i> .....                                                         | 89        |
| <i>Задачи</i> .....                                                                      | 89        |
| 3.3. Евклидовы кольца .....                                                              | 90        |
| 3.3.1. Евклидово кольцо и алгоритм Евклида .....                                         | 90        |
| 3.3.2. Взаимно простые элементы евклидова кольца .....                                   | 92        |
| 3.3.3. Факториальность евклидова кольца .....                                            | 93        |
| <i>Контрольные вопросы</i> .....                                                         | 94        |
| <i>Задачи</i> .....                                                                      | 95        |
| 3.4. Примеры евклидовых колец .....                                                      | 95        |
| 3.4.1. Евклидовость кольца целых чисел .....                                             | 95        |
| 3.4.2. Евклидовость кольца целых комплексных чисел .....                                 | 98        |
| 3.4.3. Евклидовость кольца многочленов над полем .....                                   | 100       |
| 3.4.4. Примеры неевклидовых колец .....                                                  | 103       |
| <i>Контрольные вопросы</i> .....                                                         | 104       |
| <i>Задачи</i> .....                                                                      | 104       |
| 3.5. Кольца главных идеалов .....                                                        | 105       |
| 3.5.1. Определение и примеры колец главных идеалов .....                                 | 105       |
| 3.5.2. Существование разложения на простые множители в кольце главных идеалов .....      | 106       |
| 3.5.3. Факториальность кольца главных идеалов .....                                      | 106       |
| <i>Контрольные вопросы</i> .....                                                         | 107       |
| <i>Задачи</i> .....                                                                      | 108       |



## Глава 4. Расширения полей..... 109

|                                                                                                            |     |
|------------------------------------------------------------------------------------------------------------|-----|
| 4.1. Алгебраический над данным полем элемент<br>и его минимальный многочлен .....                          | 109 |
| 4.1.1. Алгебраические и трансцендентные элементы<br>над полем .....                                        | 109 |
| 4.1.2. Минимальный многочлен алгебраического элемента ...                                                  | 110 |
| 4.1.3. Освобождение от алгебраической иррацио-<br>нальности в знаменателе дроби.....                       | 111 |
| <i>Контрольные вопросы</i> .....                                                                           | 114 |
| <i>Задачи</i> .....                                                                                        | 114 |
| 4.2. Степень расширения .....                                                                              | 115 |
| 4.2.1. Базис и степень расширения .....                                                                    | 115 |
| 4.2.2. Повторное расширение поля.....                                                                      | 116 |
| <i>Контрольные вопросы</i> .....                                                                           | 117 |
| <i>Задачи</i> .....                                                                                        | 117 |
| 4.3. Простое расширение поля .....                                                                         | 118 |
| 4.3.1. Простое алгебраическое расширение поля.....                                                         | 118 |
| 4.3.2. Простое трансцендентное расширение поля.....                                                        | 121 |
| 4.3.3*. Существование простого алгебраического<br>расширения поля и поля разложения данного многочлена ... | 121 |
| <i>Контрольные вопросы</i> .....                                                                           | 122 |
| <i>Задачи</i> .....                                                                                        | 122 |
| 4.4. Составное расширение поля .....                                                                       | 123 |
| 4.4.1. Повторное алгебраическое расширение поля .....                                                      | 123 |
| 4.4.2. Составное расширение поля .....                                                                     | 123 |
| <i>Контрольные вопросы</i> .....                                                                           | 125 |
| <i>Задачи</i> .....                                                                                        | 126 |
| 4.5. Поле алгебраических чисел .....                                                                       | 126 |
| <i>Контрольные вопросы</i> .....                                                                           | 127 |
| <i>Задачи</i> .....                                                                                        | 128 |
| 4.6. Квадратичные расширения полей.....                                                                    | 128 |
| 4.6.1. От геометрии к алгебре .....                                                                        | 128 |
| 4.6.2. Неразрешимость некоторых задач на построение<br>циркулем и линейкой .....                           | 132 |
| 4.6.3*. Разрешимость уравнений в радикалах.....                                                            | 136 |
| <i>Контрольные вопросы</i> .....                                                                           | 137 |
| <i>Задачи</i> .....                                                                                        | 138 |
| 4.7. Конечные поля.....                                                                                    | 138 |
| 4.7.1. Число элементов конечного поля .....                                                                | 138 |
| 4.7.2*. Мультипликативная группа конечного поля.....                                                       | 139 |
| <i>Контрольные вопросы</i> .....                                                                           | 140 |
| <i>Задачи</i> .....                                                                                        | 141 |

|                                                                                        |            |
|----------------------------------------------------------------------------------------|------------|
| 4.8*. Конечные тела .....                                                              | 141        |
| 4.8.1. Предварительные сведения .....                                                  | 141        |
| 4.8.2. Основная теорема о конечном теле .....                                          | 143        |
| 4.9*. Алгебры над полями.....                                                          | 145        |
| 4.9.1. Тело кватернионов.....                                                          | 145        |
| 4.9.2. Алгебры с делением конечного ранга над полем<br>действительных чисел .....      | 147        |
| <i>Контрольные вопросы</i> .....                                                       | 151        |
| <i>Задачи</i> .....                                                                    | 151        |
| <b>Литература .....</b>                                                                | <b>153</b> |
| <b>Новые издания по дисциплине «Высшая математика»<br/>и смежным дисциплинам .....</b> | <b>155</b> |
| <b>Предметный указатель .....</b>                                                      | <b>158</b> |

## Предисловие

Учебное пособие адресовано в первую очередь студентам и аспирантам педагогических вузов математических специальностей и содержит материал по теории групп, колец и полей, излагаемый в рамках дисциплины «Алгебра» («Алгебра и теория чисел»). Вместе с тем изложение имеет целостный, замкнутый характер и может быть использовано всеми желающими для первичного знакомства с основами теории групп, колец и полей.

В первой главе, посвященной группам, кроме традиционно излагаемого материала рассматривается теория конечных абелевых групп, которая в четвертой главе используется при доказательстве того, что мультипликативная группа конечного поля циклическая.

Во второй главе рассматриваются основные понятия теории колец и полей. Первый параграф первой главы и основное содержание второй главы могут быть использованы для первичного знакомства с группами, кольцами и полями уже на первом курсе перед изучением векторных пространств над произвольными полями.

Третья глава посвящена теории делимости в кольцах. «Путеводной звездой» являются основная теорема арифметики и два способа нахождения наибольшего общего делителя двух целых чисел: с помощью разложения чисел на простые множители и с помощью алгоритма Евклида. Первый способ приводит к факториальным кольцам, а второй — к евклидовым кольцам. Рассмотрены кольца главных идеалов и доказана их факториальность.

Четвертая глава знакомит с расширениями полей. Рассматриваются тела как содержательные обобщения полей. Приведено доказательство теоремы о том, что конечное тело является полем. Рассмотрено тело кватернионов. В заключение описываются алгебры с делением конечного ранга над полем действительных чисел, доказана теорема Фробениуса, которая носит завершающий характер.

В каждой главе материал расположен в порядке возрастания степени сложности, что способствует вариативному использованию пособия. Текст, содержащий дополнительные сведения, помечен звездочкой. Вопросы в конце параграфов, как правило, просты и способствуют усвоению основного содержания, а задачи помогают закрепить приложения теории.

В результате усвоения изложенного материала студент должен приобрести следующие компетенции:

**знать**

- формулировки определений основных понятий;
- формулировки основных теорем;

**уметь**

- доказывать свойства основных понятий;
- решать задачи по теории групп, колец и полей;

**владеть**

• приложением материала для работы с многочленами, векторными пространствами и числовыми системами.

В тексте используются значки:  $\Leftrightarrow$  (тогда и только тогда, когда),  $\Rightarrow$  (отсюда следует). Знак  $(\Rightarrow)$  обозначает начало доказательства необходимости, а знак  $(\Leftarrow)$  — начало доказательства достаточности. Знак  $:$  означает «делится».

Автор благодарит профессора Н. Н. Осипова, замечания которого способствовали улучшению изложения.

# Глава 1

## ГРУППЫ

### 1.1. Определение группы, примеры и основные свойства групп

#### 1.1.1. Определение группы, терминология

Рассмотрим сложение натуральных чисел. Имеем:  $2 + 3 = 5$ . Упорядоченной паре слагаемых  $(2, 3)$  ставится в соответствие число 5. На базе этих представлений о сложении дадим общее определение.

**Определение 1.1.** *Бинарной алгебраической операцией* (или просто *бинарной операцией*) на непустом множестве  $G$  называется отображение множества всех упорядоченных пар  $\{(x, y) \mid x, y \in G\}$  в множество  $G$ . При этом если упорядоченной паре  $(a, b)$ , где  $a, b \in G$ , ставится в соответствие элемент  $c \in G$ , то пишут  $a * b = c$  и  $*$  называют бинарной операцией на множестве  $G$ , а совокупность двух объектов  $\langle G, * \rangle$  называют *алгебраической системой* с основным множеством  $G$  и бинарной операцией  $*$ .

Например, бинарная операция умножения натуральных чисел есть отображение, при котором, в частности, упорядоченной паре  $(2, 3)$  ставится в соответствие число 6. А вот вычитание не является бинарной операцией на множестве  $\mathbb{N}$ , так как при вычитании паре  $(2, 3)$  ставится в соответствие число  $-1 \notin \mathbb{N}$ . Вычитание есть бинарная операция на множестве целых чисел  $\mathbb{Z}$ . В дальнейшем мы будем рассматривать также алгебраические системы с двумя бинарными алгебраическими операциями типа  $\langle \mathbb{Z}, +, \cdot \rangle$ .

**Определение 1.2.** *Группой* называется алгебраическая система  $\langle G, * \rangle$  с основным множеством  $G$  и бинарной операцией  $*$ , если выполняются следующие условия:

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

2) существует элемент  $e \in G$ , называемый *нейтральным*, такой что  $a * e = e * a = a$  для любого  $a \in G$ ;

3) Для всякого элемента  $a \in G$  существует элемент  $a' \in G$ , называемый *симметричным* элементу  $a$ , такой что  $a * a' = a' * a = e$ .

Если групповая операция  $*$  коммутативна (т.е. для любых  $a, b \in G$   $a * b = b * a$ ), то группа называется *коммутативной*, или *абелевой*. Групповая операция обычно обозначается либо знаком «+» (плюс), либо знаком « $\cdot$ » (точка), а сама группа записывается либо в виде системы  $\langle G, + \rangle$ , либо  $\langle G, \cdot \rangle$ , причем в каждом случае используется своя терминология. Группа по сложению называется *аддитивной*, а по умножению — *мультипликативной*. При построении общей теории групп обычно пользуются мультипликативной терминологией, а при построении теории коммутативных групп — аддитивной. Приведем словарь терминов каждой из этих терминологий (табл. 1.1).

Таблица 1.1

Термины теории групп

| Общая терминология            | Аддитивная терминология                  | Мультипликативная терминология                      |
|-------------------------------|------------------------------------------|-----------------------------------------------------|
| Группа $\langle G, * \rangle$ | Аддитивная группа $\langle G, + \rangle$ | Мультипликативная группа $\langle G, \cdot \rangle$ |
| Бинарная операция $*$         | Сложение $+$                             | Умножение $\cdot$                                   |
| Результат $a * b$             | Сумма $a + b$                            | Произведение $a \cdot b$                            |
| Нейтральный элемент $e$       | Ноль $0$                                 | Единица $1$ или $e$                                 |
| Симметричный элемент $a'$     | Противоположный элемент $-a$             | Обратный элемент $a^{-1}$                           |

Если ясно, о какой операции идет речь, то группу обозначают одной буквой, соответствующей основному множеству системы, например аддитивная группа  $\mathbb{Z}$  (вместо  $\langle \mathbb{Z}, + \rangle$ ). Рассматривая теорию групп, мы будем использовать мультипликативную терминологию.

**Определение 1.3.** *Порядком группы  $G$  называется количество ее элементов (мощность множества  $G$ ). Обозначается  $|G|$ . Группа называется *конечной*, если ее порядок конечен, и называется *бесконечной*, если ее порядок бесконечен. Если группа  $G$  содержит  $n$  элементов, то пишут  $|G| = n$ , а если группа  $G$  бесконечна, то пишут  $|G| = \infty$ .*

Исторический экскурс

Впервые группы появились в работах Лагранжа при исследовании вопроса о том, можно ли выразить корни многочлена через

его коэффициенты с помощью операций сложения, вычитания, умножения, деления и извлечения корня (проблема решения уравнений в радикалах). Для многочленов второй степени такие формулы известны с глубокой древности. Труды итальянских математиков Дель Ферро, Тартальи и Кардано подобные формулы были найдены для многочленов третьей степени (в справочниках можно найти формулу Кардано для корней уравнения третьей степени). Методом Феррари решение уравнения четвертой степени сводится к решению уравнений третьей и второй степеней. Лагранж установил общую идею сведения решения уравнения данной степени  $n = 2, 3, 4$  к решению так называемого разрешающего уравнения меньшей степени (резольвенты). Однако в случае  $n = 5$  резольвента оказывается уравнением шестой степени. В исследовании этого вопроса в трудах Лагранжа впервые возникают группы подстановок. Например, за возможность сведения решения уравнения четвертой степени к решению уравнения третьей степени отвечает наличие в группе подстановок четвертой степени  $S_4$  инвариантной (нормальной) подгруппы  $H = \{e, i = (12)(34), j = (13)(24), ij = (14)(23)\}$  (четверная группа Клейна).

В 1824 г. Н. Абель доказал, что корни уравнения степени  $n \geq 5$ , вообще говоря, нельзя выразить через коэффициенты, используя указанные выше операции. В этом случае говорят, что уравнение не разрешимо в радикалах.

Выдающийся французский математик Э. Галуа в 1832 г. нашел связь между разрешимостью уравнения в радикалах и группой подстановок корней уравнения. Он ввел термины «группа» и ее «инвариантная подгруппа» (теперь такую подгруппу называют «нормальной»). Как пишет Ф. Клейн<sup>1</sup>, «особым достижением Галуа является то, что он в общем виде отчетливо осознал понятие инвариантной подгруппы и исследования, выполненные Лагранжем для уравнений 3-й и 4-й степени, расширил до фундаментальной общей концепции относительно решения уравнений произвольной степени». Тем самым «под задачу решения алгебраических уравнений, ставшую традиционной с XVI в., подведен некий новый фундамент», коим явилась абстрактная теория групп.

Идеи Галуа получили широкое распространение благодаря выходу в 1870 г. «Трактата по теории подстановок и алгебраических уравнений» К. Жордана.

В трудах Е. С. Федорова группы были использованы в кристаллографии в качестве естественного инструмента классификации.

Классификация геометрий с помощью понятия группы впервые прозвучала в докладе Ф. Клейна в его «Эрлангенской программе»,

---

<sup>1</sup> Лекции о развитии математики в XIX столетии. М. : Наука, 1989. С. 374.



с которой он выступил при вступлении в должность профессора Эрлангенского университета. В этой программе различные геометрии характеризовались группами преобразований и целью каждой геометрии объявлялось изучение инвариантов этих групп преобразований. Так, евклидова геометрия выделяется группой движений, а ее цель — изучение свойств фигур, не изменяющихся при движениях.

Впервые вне связи с приложениями теория групп была изложена как абстрактная аксиоматическая теория в книге О. Ю. Шмидта «Абстрактная теория групп». В нашей стране автор книги широко известен как полярный исследователь. В этой связи отметим, что предисловие ко второму изданию упомянутой книги подписано автором так: «Август 1933 г. Ледокольный пароход “Челюскин”». Этот ледокол во время полярной экспедиции, возглавляемой О. Ю. Шмидтом, был раздавлен льдами, и спасение членов экспедиции стало одной из ярких страниц истории освоения Арктики.

Основополагающие результаты по теории конечных групп принадлежат Л. Силову. Значительный вклад в развитие теории групп внесли известные отечественные математики А. Г. Курош и А. И. Мальцев.

В настоящее время теория групп превратилась в самостоятельную бурно развивающуюся ветвь алгебры с многочисленными приложениями. Глубже познакомиться с теорией групп можно по монографиям [8, 13, 18].

---

## 1.1.2. Примеры групп

### 1. Числовые группы.

Числа можно складывать и перемножать, но, говоря о группе, мы каждый раз будем фиксировать свое внимание лишь на одной операции.

1.1. Аддитивные числовые группы:  $\langle \mathbb{Z}, + \rangle$ ,  $\langle \mathbb{Q}, + \rangle$ ,  $\langle \mathbb{R}, + \rangle$ ,  $\langle \mathbb{C}, + \rangle$ ; кратко: аддитивные группы целых чисел  $\mathbb{Z}$ , рациональных чисел  $\mathbb{Q}$ , действительных чисел  $\mathbb{R}$  и комплексных чисел  $\mathbb{C}$ .  $\langle 2\mathbb{Z}, + \rangle$  — аддитивная группа четных целых чисел; аналогично  $\langle m\mathbb{Z}, + \rangle$  — аддитивная группа целых чисел, кратных фиксированному целому неотрицательному числу  $m$ . Аддитивная группа целых комплексных (гауссовых) чисел  $\mathbb{Z} + \mathbb{Z}i$  состоит из комплексных чисел вида  $a + bi$ , где  $a$  и  $b$  — целые числа;  $i$  — мнимая единица ( $i^2 = -1$ ).

1.2. Мультипликативные числовые группы:  $\langle \mathbb{Z}^*, \cdot \rangle$ ,  $\langle \mathbb{Q}^*, \cdot \rangle$ ,  $\langle \mathbb{R}^*, \cdot \rangle$ ,  $\langle \mathbb{C}^*, \cdot \rangle$ , где  $*$  обозначает взятие множества обратимых соответствующих чисел (когда обратное число принадлежит



тому же множеству). Например,  $\mathbb{Z}^* = \{1, -1\}$ ,  $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$  — множество всех рациональных чисел, отличных от нуля. Аналогично  $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ ,  $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ . Мультипликативная группа положительных действительных чисел  $\mathbb{R}^+$ . Мультипликативная группа целых степеней двойки:  $2^{\mathbb{Z}} = \{2^n \mid n \in \mathbb{Z}\}$ . Мультипликативная группа комплексных единиц  $\langle \{1, -1, i, -i\}, \cdot \rangle$ , она может быть охарактеризована как группа корней четвертой степени из единицы. Мультипликативная группа комплексных корней  $n$ -й степени из единицы обозначается  $\mathbb{C}_n$ . Мультипликативная группа всех корней из единицы степени  $p^n$  для фиксированного простого числа  $p$  и всех  $n = 1, 2, \dots$  называется *группой типа  $p^\infty$*  и обозначается  $\mathbb{C}_{p^\infty}$ .

## 2. Группы подстановок.

Напомним, что подстановкой на множестве символов  $M = \{1, 2, \dots, n\}$  называется всякое взаимно однозначное отображение множества  $M$  на себя. Записывается подстановка в виде двухстрочной матрицы, где в первой строке стоят символы множества  $M$ , а под ними во второй строке стоят образы символов первой строки. Умножением подстановок называется последовательное выполнение отображений. Например:

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

2.1. Группа всех подстановок  $n$  символов обозначается  $S_n$  и называется *симметрической группой  $n$ -й степени*. Всякую подстановку можно записать в виде произведения *независимых циклов*. При этом одноэлементные циклы можно не записывать. Например:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1324), \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23),$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (12)(3)(4) = (12).$$

Найдем произведение тех же подстановок в новой форме:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1324) \cdot (14) \cdot (23) = (12)(3)(4) = (12).$$

|| **Упражнение 1.1.** Заполните таблицу умножения элементов группы  $S_3$  ( $e$  обозначает тождественную подстановку):

|         | $e$    | $((123))$ | $(132)$ | $(12)$  | $(13)$ | $(23)$  |
|---------|--------|-----------|---------|---------|--------|---------|
| $e$     |        |           |         |         |        |         |
| $(123)$ |        |           |         |         |        |         |
| $(132)$ |        |           |         |         |        |         |
| $(12)$  |        |           |         |         |        |         |
| $(13)$  | $(13)$ | $(23)$    | $(12)$  | $(132)$ | $e$    | $(123)$ |
| $(23)$  |        |           |         |         |        |         |

Такого рода таблица умножения элементов группы называется *таблицей Кэли*.

2.2. Напомним, что всякий цикл можно записать в виде произведения транспозиций, т.е. двухэлементных циклов. Например:  $(1234) = (12)(13)(14)$  (найдите произведение  $(12) \cdot (13) \cdot (14)$  и убедитесь, что равенство верно). Подстановка называется *четной (нечетной)*, если она представима в виде четного (соответственно, нечетного) числа транспозиций. Легко видеть, что множество всех четных подстановок группы  $S_n$  само образует группу (подгруппу), она обозначается  $A_n$  и называется *знакопеременной (альтернативной)* группой подстановок  $n$  символов.

### 3. Группы в геометрии.

3.1. Группа всех преобразований плоскости (пространства) относительно умножения (суперпозиции) преобразований. Под умножением преобразований понимаем их последовательное выполнение. Единицей группы является тождественное преобразование.

3.2. Группа всех движений плоскости.

3.3. Группа всех параллельных переносов плоскости, она коммутативна.

3.4. Группа всех вращений плоскости вокруг данной точки — также коммутативная группа.

3.5. Группа самосовмещений правильного многоугольника.

Рассмотрим, например, группу  $G$  самосовмещений правильного треугольника. Она состоит из тождественного преобразования  $e$ , вращения  $a$  вокруг центра против часовой стрелки на  $120^\circ$ , квадрата этого вращения  $a^2$ , который получается в результате повторного вращения  $a$  и представляет собой поворот вокруг центра против часовой стрелки на  $240^\circ$ , и трех отражений  $b$ ,  $c$  и  $d$  относительно осей, содержащих соответствующие биссектрисы (рис. 1.1).

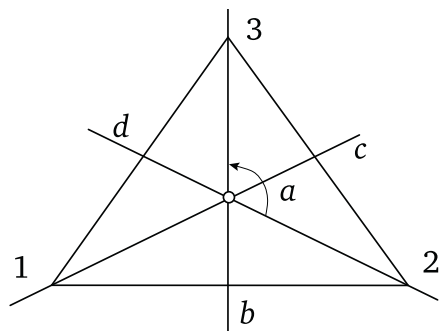


Рис. 1.1

Обозначим вершины треугольника через 1, 2 и 3. Тогда появляется возможность все преобразования треугольника представить в виде подстановок его вершин:  $e$  — тождественная подстановка, вращение  $a = (123)$ , его квадрат  $a^2 = (132)$ , отражения от биссектрис  $b, c$  и  $d$  соответственно подстановки  $b = (12)$ ,  $c = (23)$  и  $d = (13)$ .

Замечаем, что  $G = \{e, a, a^2, b, ab, a^2b\}$ , причем  $a^3 = b^2 = e$ ,  $ba = a^2b$ . Здесь элементы  $a$  и  $b$  называются *порождающими элементами группы*, а равенства, связывающие эти элементы, называются *определяющими соотношениями*. Последние позволяют укорачивать произведения, составленные из элементов  $a$  и  $b$ . Например, произведение  $b \cdot a^2b$  преобразуется следующим образом:

$$b \cdot a^2b = ba \cdot ab = a^2b \cdot ab = a^2 \cdot ba \cdot b = a^2 \cdot a^2b \cdot b = a^3 \cdot a \cdot b^2 = a.$$

**Определение 1.4.** Подмножество  $M$  группы  $G$  называется *порождающим*, если всякий элемент группы можно представить в виде произведения элементов множества  $M$  и их обратных. При этом пишут  $G = \langle M \rangle$ , читается:  $G$  есть группа, порожденная множеством  $M$ .

**Упражнение 1.2.** Пользуясь определяющими соотношениями, заполните таблицу умножения элементов группы (таблицу Кэли).

|        | $e$  | $a$ | $a^2$  | $b$ | $ab$ | $a^2b$ |
|--------|------|-----|--------|-----|------|--------|
| $e$    |      |     |        |     |      |        |
| $a$    |      |     |        |     |      |        |
| $a^2$  |      |     |        |     |      |        |
| $b$    |      |     |        |     |      |        |
| $ab$   | $ab$ | $b$ | $a^2b$ | $a$ | $e$  | $a^2$  |
| $a^2b$ |      |     |        |     |      |        |

Рассматривая группы вращений правильных многогранников, Ф. Клейн обратил внимание на существование многогранника, названного им  $n$ -угольным диэдром. Он представляет собой правильную  $n$ -угольную пластину с двумя совпавшими гранями. Его группа вращений (в пространстве) называется *группой вращений  $n$ -угольного диэдра*. Приведенную выше группу  $G$  можно рассматривать как группу вращений треугольного диэдра.

Группа вращений квадратной пластины в пространстве (четырёхугольного диэдра) состоит из тождественного преобразования, вращений вокруг оси, проходящей через центр квадрата перпендикулярно его плоскости, и вращений вокруг осей симметрий квадрата (рис. 1.2). Итого получаем восемь вращений. Если вершины занумеровать символами 1, 2, 3, 4, то самосовмещения квадрата можно записать в виде подстановок:  $e, a = (1234), a^2, a^3, b = (12)(34), ab, a^2b, a^3b$ . При этом  $ba = a^3b$  (проверьте).

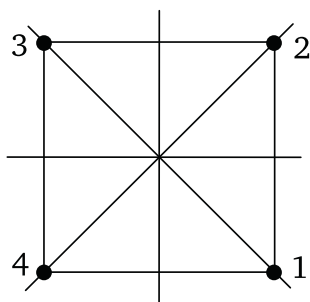


Рис. 1.2

**Упражнение 1.3.** Составьте таблицу умножения полученной группы четырёхугольного диэдра (таблицу Кэли).

#### 4. Группы в линейной алгебре.

Приводя примеры групп в линейной алгебре, мы будем использовать соответствующую терминологию, известную из предшествующего алгебраического материала. В частности, будем использовать понятия кольца и поля, хотя теория колец и полей у нас впереди. Напомним, что слова «над полем» означают, что элементы матриц, координаты векторов, коэффициенты многочленов берутся из данного поля.

4.1. Аддитивная группа арифметических векторов арифметического  $n$ -мерного векторного пространства над данным полем  $P$ .

4.2. Аддитивная группа матриц размерности  $m \times n$  над полем  $\mathbb{R}$ .

3.  $GL_n(\mathbb{R})$  — мультипликативная группа обратимых (невырожденных) квадратных матриц порядка  $n$  над полем  $\mathbb{R}$  (полная линейная группа матриц порядка  $n$ ). Напомним, что матрица  $A$  обратима (т.е. существует обратная матрица  $A^{-1}$ ) тогда и только тогда, когда ее определитель отличен от нуля ( $|A| \neq 0$ ).

4.4. Мультипликативная группа матриц над полем  $\mathbb{R}$  с ненулевыми элементами по главной диагонали, у которых ниже (или выше) главной диагонали стоят нули (верхнетреугольная и, соответственно, нижнетреугольная группы матриц).

4.5. Мультипликативная группа диагональных матриц над полем  $\mathbb{R}$  (с ненулевыми элементами по главной диагонали, вне которой все элементы равны нулю).

4.6. Мультипликативная группа скалярных матриц (скалярной называется диагональная матрица, у которой все диагональные элементы равны между собой).

### 1.1.3. Основные свойства групп

Докажем основные свойства групп, используя мультипликативную терминологию. Пусть дана группа  $\langle G, \cdot \rangle$ .

1. *Единица группы единственна.*

*Доказательство.* Пусть  $e$  и  $e_1$  — единицы группы  $G$ . Поскольку  $e$  — единица группы, то  $e \cdot e_1 = e_1$ , а так как  $e_1$  — единица группы, то  $e \cdot e_1 = e$ . Следовательно,  $e_1 = e$ .

2. *Для каждого элемента группы обратный элемент единственен.*

*Доказательство.* Пусть  $a \in G$  и элементы  $b, c \in G$  являются обратными для  $a$ . Это означает, что  $ab = ba = e$  и  $ac = ca = e$ . Используя это и ассоциативность умножения, получаем  $b = b \cdot e = b(a \cdot c) = (b \cdot a) \cdot c = e \cdot c = c$ .

3. *Для любых  $a, b \in G$  уравнения  $a \cdot x = b$  и  $y \cdot a = b$  однозначно разрешимы.*

*Доказательство.* Рассмотрим уравнение  $a \cdot x = b$ .

*Существование решения.* Легко проверить, что  $x_0 = a^{-1} \cdot b$  является решением данного уравнения.

*Единственность решения.* Пусть  $x_1$  и  $x_2$  — решения уравнения  $a \cdot x = b$ . Тогда  $a \cdot x_1 = b$  и  $a \cdot x_2 = b$ , откуда  $a \cdot x_1 = a \cdot x_2$ . Умножим равенство слева на  $a^{-1}$  и, воспользовавшись свойством ассоциативности, получим  $x_1 = x_2$ .

Уравнение  $y \cdot a = b$  рассматривается аналогично.

4. *Обратный элемент для произведения двух элементов находится по формуле  $(ab)^{-1} = b^{-1}a^{-1}$ .*

*Доказательство.*  $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$ .

5. Обратный элемент к обратному равен самому элементу:  
 $(a^{-1})^{-1} = a$  для любого  $a \in G$ .

*Доказательство.* Это свойство вытекает из равенства

$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

**Определение 1.5.** Для любого элемента  $a \in G$  положим  $a^0 = e$ . Для любого натурального числа  $n$  будем считать, что  $a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_n$  и  $a^{-n} = (a^{-1})^n$ . Выражение  $a^n$ , где  $n \in \mathbb{Z}$ , называется

степенью (элемента  $a$  с целым показателем).

6. Свойства степеней.

6.1.  $(a^n)^{-1} = a^{-n}$  для любого  $a \in G$  и любого  $n \in \mathbb{Z}$ .

*Доказательство.* Для любого натурального  $n$  имеем

$$(a^n)^{-1} = (\underbrace{a \cdot a \cdot \dots \cdot a}_n)^{-1} = \underbrace{a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1}}_n = (a^{-1})^n = a^{-n}.$$

Отсюда  $(a^{-n})^{-1} = a^n = a^{-(-n)}$ .

6.2.  $a^m \cdot a^n = a^{m+n}$  для любого  $a \in G$  и любых  $m, n \in \mathbb{Z}$ .

*Доказательство.* Рассмотрим все возможные случаи относительно целых  $m$  и  $n$ :

а)  $m, n \in \mathbb{N}$ , тогда

$$a^m \cdot a^n = (\underbrace{a \cdot a \cdot \dots \cdot a}_m)(\underbrace{a \cdot a \cdot \dots \cdot a}_n) = \underbrace{a \cdot a \cdot \dots \cdot a}_{m+n} = a^{m+n}.$$

б) Если хотя бы один из показателей  $m, n$  равен нулю, то доказываемое равенство очевидно.

в) Пусть  $m \in \mathbb{N}, n = -n_1$ , где  $n_1 \in \mathbb{N}$ . Тогда

$$a^m \cdot a^n = a^m \cdot a^{-n_1} = \underbrace{a \cdot a \cdot \dots \cdot a}_m \cdot \underbrace{a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1}}_{n_1}.$$

Если  $m < n_1$ , то ответом будет  $(a^{-1})^{n_1-m} = a^{-(n_1-m)} = a^{-n_1+m} = a^{m+n}$ .  
 Если  $m = n_1$ , то получим  $a^0 = a^{m-n_1} = a^{m+n}$ . Если же  $n_1 < m$ , то будем иметь  $a^{m-n_1} = a^{m+n}$ .

Случай  $n \in \mathbb{N}, m = -m_1$ , где  $m_1 \in \mathbb{N}$ , сводится к рассмотренному.

г) Пусть  $m = -m_1, n = -n_1$ , где  $m_1, n_1 \in \mathbb{N}$ . Тогда

$$\begin{aligned} a^m \cdot a^n &= a^{-m_1} \cdot a^{-n_1} = (a^{-1})^{m_1} \cdot (a^{-1})^{n_1} = \\ &= (a^{-1})^{m_1+n_1} = a^{-(m_1+n_1)} = a^{(-m_1)+(-n_1)} = a^{m+n}. \end{aligned}$$

6.3. Для любых  $m, n \in \mathbb{Z}$   $(a^m)^n = a^{mn}$ .

**Упражнение 1.4.** Докажите свойство 6.3 самостоятельно, рассмотрев все возможные случаи относительно целых показателей  $m$  и  $n$ .

#### 1.1.4. Подгруппы

**Определение 1.6.** Пусть дана группа  $\langle G, \cdot \rangle$ . Подмножество  $H \subseteq G$  называется *подгруппой* группы  $G$ , если  $\langle H, \cdot \rangle$  является группой относительно сужения операции  $\cdot$  на  $H$ . Обозначается:  $H \leq G$ . Читается:  $H$  есть подгруппа группы  $G$ . Если  $H \neq G$ , то подгруппа  $H$  называется *собственной*. При этом пишут:  $H < G$ . Читается:  $H$  есть собственная подгруппа группы  $G$ .

Очевидно, «самой маленькой» подгруппой группы  $\langle G, \cdot \rangle$  с единицей  $e$  будет единичная подгруппа  $\{e\}$ , а «самой большой» подгруппой — сама группа  $G$ . Полезно еще раз рассмотреть приведенные выше примеры групп и найти в них подгруппы.

**Теорема 1.1 (критерий подгруппы).** Подмножество  $H$  группы  $\langle G, \cdot \rangle$  является подгруппой тогда и только тогда, когда выполнены следующие условия:

- 1) подмножество  $H$  замкнуто относительно умножения, т.е. если  $a, b \in H$ , то  $a \cdot b \in H$ ;
- 2) единица группы  $e \in H$ ;
- 3) подмножество  $H$  замкнуто относительно взятия обратного элемента, т.е. если  $a \in H$ , то  $a^{-1} \in H$ .

**Доказательство.** ( $\Rightarrow$ ) 1. Пусть  $H$  — подгруппа группы  $\langle G, \cdot \rangle$ . По определению, это означает, что  $\langle H, \cdot \rangle$  является группой, а значит, сужение групповой операции на множество  $H$  является бинарной операцией на  $H$ , т.е. для любых элементов  $a, b \in H$  существует элемент  $c \in H$ , такой что  $a \cdot b = c$ . Следовательно,  $a \cdot b \in H$ . Но это и означает замкнутость множества  $H$  относительно группового умножения.

2. Пусть  $e$  — единица группы  $G$ . Поскольку  $\langle H, \cdot \rangle$  есть группа, то в  $H$  существует единица, которую обозначим  $e_1$ . Тогда  $e = e_1 \cdot e_1^{-1} \in H$ .

3. Так как  $\langle H, \cdot \rangle$  есть группа, то для любого  $a \in H$  в  $H$  существует обратный элемент, а поскольку обратный элемент  $a^{-1}$  в группе  $G$  единственный, то  $a^{-1} \in H$ .

( $\Leftarrow$ ). Если подмножество  $H \subseteq G$  удовлетворяет условиям 1) — 3), то, очевидно,  $\langle H, \cdot \rangle$  является группой, а значит, подгруппой в  $G$ .

**Теорема 1.2.** Пересечение двух подгрупп есть подгруппа.

**Доказательство.** Пусть  $A$  и  $B$  — подгруппы группы  $\langle G, \cdot \rangle$ . Следуя критерию подгруппы, докажем, что пересечение  $H = A \cap B$  есть подгруппа.

1. Подмножество  $H$  замкнуто относительно умножения. Действительно, для любых  $a, b \in H$  имеем:

$$a, b \in H = A \cap B \Rightarrow \begin{cases} a, b \in A \Rightarrow a \cdot b \in A, \\ a, b \in B \Rightarrow a \cdot b \in B \end{cases} \Rightarrow a \cdot b \in A \cap B = H.$$



2. Единица группы  $e \in H$ . В самом деле, поскольку  $A$  и  $B$  подгруппы, то  $e \in A$  и  $e \in B$ , откуда  $e \in A \cap B = H$ .

3. Подмножество  $H$  замкнуто относительно взятия обратного элемента. Действительно, имеем:

$$a \in H = A \cap B \Rightarrow \begin{cases} a \in A \Rightarrow a^{-1} \in A, \\ a \in B \Rightarrow a^{-1} \in B \end{cases} \Rightarrow a^{-1} \in A \cap B = H.$$

Вместе с тем теорема доказана.

## Контрольные вопросы

1. Существуют ли подгруппы в группе, не имеющие общих элементов?
2. Может ли в группе неединичный элемент совпадать со своим обратным?
3. Если  $A$  — подгруппа группы  $B$ , а  $B$  — подгруппа группы  $C$ , то будет ли  $A$  подгруппой группы  $C$ ?
4. Если  $H_1$  и  $H_2$  — подгруппы некоторой группы, то будет ли подгруппой объединение множеств  $H_1 \cup H_2$ ?
5. Может ли порядок собственной подгруппы группы равняться порядку самой группы? Если нет — докажите, если да — приведите пример.
6. Чему равны порядки групп  $S_n$  и  $A_n$ ?
7. В какой группе существует единственный обратный элемент для всех элементов группы?
8. Чему равно пересечение всех подгрупп группы?
9. Будет ли группа конечной, если число ее подгрупп конечно?
10. Будет ли группа коммутативной, если всякая ее собственная подгруппа коммутативна?

## Задачи

1. В каждой группе из приведенных в подпараграфе 1.1.2 примеров групп выберите элементы  $a, b$  и решите уравнения  $ax = b$  и  $ya = b$  в мультипликативной группе и уравнение  $a + x = b$  в аддитивной группе.
2. Докажите, что решения уравнений  $a \cdot x = b$  и  $y \cdot a = b$  совпадают тогда и только тогда, когда  $a \cdot b = b \cdot a$ .
3. В каждой группе из приведенных в подпараграфе 1.1.2 примеров групп приведите примеры подгрупп. В частности, выпишите все подгруппы групп  $S_3$  и  $S_4$ . Найдите в них подгруппы четных подстановок — соответственно  $A_3$  и  $A_4$ .
4. Докажите, что подмножество  $H$  группы  $G$  является подгруппой данной группы тогда и только тогда, когда  $H \neq \emptyset$  и для любых  $a, b \in H$



$a^{-1}b \in H$ . Сформулируйте этот критерий подгруппы в аддитивной терминологии.

5. Пусть  $p_1, p_2, \dots, p_n$  — различные простые натуральные числа,  $n \geq 2$ , и  $\bar{p}_i$  — произведение всех этих чисел, кроме числа  $p_i$ ,  $i = 1, \dots, n$ . Докажите, что  $Z = \langle \bar{p}_1, \dots, \bar{p}_n \rangle$  (т.е. аддитивная группа целых чисел порождается указанными произведениями) и ни одно из порождающих чисел нельзя удалить.

6. Пусть  $H$  — подгруппа группы  $G$  и  $g \in G$ .

1) Докажите, что подгруппами являются множества  $g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$  и  $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ .

2) Докажите, что  $g^{-1}Hg = H$  тогда и только тогда, когда  $gH = Hg$ , где  $gH = \{gh \mid h \in H\}$ ,  $Hg = \{hg \mid h \in H\}$ .

3) В каком случае  $g^{-1}Hg = gHg^{-1}$ ?

7. Существует ли в аддитивной группе комплексных чисел  $\mathbb{C}$  такая подгруппа  $H$ , что  $\mathbb{R} < H < \mathbb{C}$ ?

## 1.2. Порядок элемента группы

### 1.2.1. Определение и примеры

В мультипликативной группе  $\mathbb{Q}^*$  любая натуральная степень двойки отлична от единицы, т.е.  $2^n \neq 1$  при любом натуральном показателе  $n$ . В этом случае говорят, что элемент 2 имеет бесконечный порядок. В этой же группе  $(-1)^2 = 1$ . В этом случае говорят, что элемент  $-1$  имеет порядок 2. Дадим общее определение.

**Определение 1.7.** Пусть дана мультипликативная группа  $G$  с единицей  $e$  и  $a \in G$ . Если  $a^n \neq e$  для любого натурального показателя  $n$ , то будем говорить, что элемент  $a$  имеет бесконечный порядок, и писать  $|a| = \infty$  (читается: порядок элемента  $a$  бесконечен). Если же существует натуральное число  $m$ , такое что  $a^m = e$ , то наименьшее натуральное число  $n$ , такое что  $a^n = e$ , будем называть *порядком элемента  $a$*  и писать  $|a| = n$  (читается: порядок элемента  $a$  равен  $n$ ).

В аддитивной группе считаем  $|a| = \infty \Leftrightarrow \forall n \in \mathbb{N} \, na \neq 0$  и  $|a| = n \Leftrightarrow n$  — наименьшее натуральное число, такое что  $na = 0$ .

Если в группе  $G$  всякий неединичный элемент имеет бесконечный порядок, то говорят, что  $G$  — *группа без кручения*. Если же в группе  $G$  всякий элемент имеет конечный порядок, то группу  $G$  называют *периодической*. Если в группе  $G$  имеются элементы конечного и бесконечного порядков, то ее называют *смешанной группой*.

Если  $|a| = \infty$ , то все степени элемента  $a$  можно изобразить целочисленными точками числовой прямой, здесь «кручения» нет (рис. 1.3).

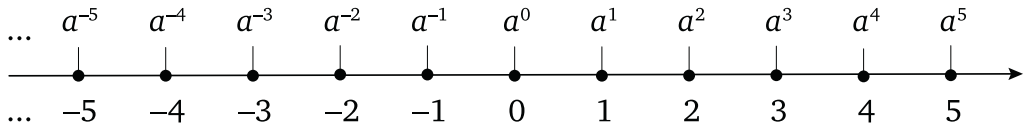


Рис. 1.3

Если же, например,  $|a| = 6$ , то степени элемента  $a$  повторяются с периодом 6, наблюдаем «кручение» (рис. 1.4).

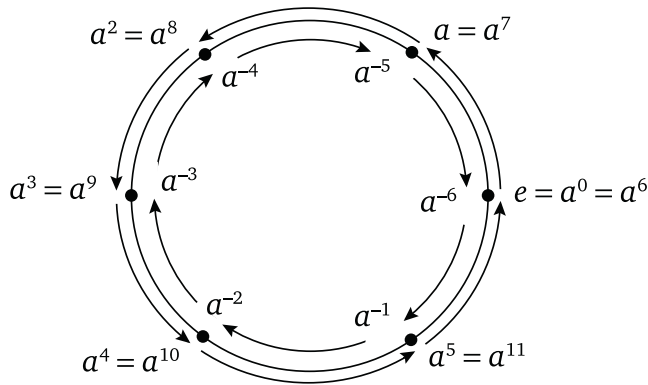


Рис. 1.4

Рассмотрим примеры.

1. Аддитивная группа целых чисел  $\mathbb{Z}$  является группой без кручения.

2. Ясно, что в конечной группе порядок всякого элемента конечен.

3. Мультипликативная группа комплексных корней всех степеней из единицы бесконечна, а всякий ее элемент имеет конечный порядок, т.е. это пример бесконечной периодической группы.

4. Найдём порядок подстановки  $a = (135)(24)$  в симметрической группе подстановок  $S_5$ . Терпеливо находим степени элемента  $a$ , пока не получим единицу группы (тождественную подстановку):

$$a^2 = (135)(24) \cdot (135)(24) = (153)(2)(4) = (153);$$

$$a^3 = a^2 \cdot a = (153) \cdot (135)(24) = (1)(24)(3)(5) = (24);$$

$$a^4 = a^3 \cdot a = (24) \cdot (135)(24) = (135)(2)(4) = (135);$$

$$a^5 = a^4 \cdot a = (135) \cdot (135)(24) = (153)(24);$$

$$a^6 = a^5 \cdot a = (153)(24) \cdot (135)(24) = (1)(2)(3)(4)(5) = e.$$

Следовательно,  $|a| = 6$ .

### 1.2.2. Основные свойства порядков элементов группы

Будем рассматривать мультипликативную группу  $G$  с единицей  $e$ . Пусть  $a$  — произвольный элемент группы  $G$ .

1.  $|a| = |a^{-1}|$ .

*Доказательство.* А. Пусть  $|a| = \infty$ . Предположим, что  $|a^{-1}|$  конечен и равен  $m$ . Тогда  $(a^{-1})^m = e$ , откуда  $(a^m)^{-1} = e$  и  $a^m = e$  — пришли к противоречию. Следовательно,  $|a^{-1}| = \infty = |a|$ .

Б. Пусть  $|a| = n$ . Тогда  $a^n = e$ , откуда  $a^{-n} = e$  и  $(a^{-1})^n = e$ . Таким образом,  $|a^{-1}|$  конечен, и если предположить, что  $|a^{-1}| = m$ , то по определению порядка элемента получаем  $m \leq n$ . С другой стороны, из равенства  $(a^{-1})^m = e$  следует, что  $a^m = e$ , откуда  $n \leq m$ . Следовательно,  $m = n$ .

2. Если  $|a| = n$ , то  $a^k = e$  тогда и только тогда, когда  $k : n$  (напомним, что знак  $:$  означает «делится»).

*Доказательство.* ( $\Rightarrow$ ) Пусть  $|a| = n$  и  $a^k = e$ . Разделим  $k$  на  $n$  с остатком:  $k = nq + r$ , где  $0 \leq r < n$ . Следовательно,  $e = a^k = a^{nq+r} = a^{nq} \cdot a^r = a^r$ . Если предположить, что  $r \neq 0$ , то приходим к противоречию с минимальностью показателя  $n$ . Следовательно,  $r = 0$  и  $k : n$ .

( $\Leftarrow$ ) Пусть  $|a| = n$  и  $k : n$ . Тогда  $k = nq$  при некотором целом  $q$  и  $a^k = a^{nq} = (a^n)^q = e^q = e$ . Свойство доказано.

3. Если  $|a| = n$ , то  $a^k = a^m$  тогда и только тогда, когда  $(k - m) : n$ .

*Доказательство.* Имеем:  $a^k = a^m \Leftrightarrow a^{k-m} = e$ , а по свойству 2, последнее равенство эквивалентно условию  $(k - m) : n$ .

## Контрольные вопросы

1. Могут ли элементы  $a \neq e$  и  $a^2$  иметь одинаковые порядки?
2. Может ли произведение двух элементов бесконечного порядка иметь конечный порядок?
3. Может ли произведение элементов порядка два иметь порядок больше двух?
4. Как можно охарактеризовать порядки элементов аддитивной группы целых чисел?

5. Может ли порядок элемента группы равняться порядку самой группы?
6. Чему равен порядок куба элемента бесконечного порядка?
7. Порядок элемента равен шести. Чему равен порядок куба этого элемента?

## Задачи

1. Найдите порядки всех элементов групп подстановок  $S_3$  и  $S_4$ .
2. Докажите равенство порядков элементов  $ab$  и  $ba$ .
3. Докажите равенство порядков элементов  $abc$ ,  $bca$  и  $cab$ .
4. В группе подстановок  $S_3$  сравните порядки элементов  $x$ ,  $y$ ,  $xу$ ,  $yx$ ,  $x^{-1}yx$ ,  $y^{-1}xy$  для различных элементов  $x, y \in S_3$ .
5. Найдите порядки элементов мультипликативной группы единиц  $G = \{1, -1, i, -i\}$ .
6. В мультипликативной матричной группе найдите порядки элементов:
  - а)  $\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ ; б)  $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ;
  - в)  $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ; г)  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ;
  - д)  $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ , где  $a = -\frac{1}{2}$ ,  $b = \frac{\sqrt{3}}{2}$ .
7. Для всех  $m \leq 10$  найдите порядки степеней элемента  $a$ , где  $|a| = m$ .
8. Докажите, что если элементы  $a$  и  $b$  группы  $G$  перестановочны и их порядки взаимно просты, то  $|ab| = |a| \cdot |b|$ .
9. Докажите, что если в группе порядок всякого неединичного элемента равен двум, то группа абелева.
10. Докажите равенство порядков элементов  $a$  и  $b^{-1}ab$ .

## 1.3. Циклические группы

### 1.3.1. Определение и примеры

Рассмотрим мультипликативную группу всех целых степеней двойки  $\langle 2\mathbb{Z}, \cdot \rangle$ , где  $2\mathbb{Z} = \{2^n \mid n \in \mathbb{Z}\}$ . Аналогом этой группы на аддитивном языке является аддитивная группа четных целых чисел  $\langle 2\mathbb{Z}, + \rangle$ ,  $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ . Дадим общее определение групп, частными примерами которых являются данные группы.

**Определение 1.8.** Мультипликативная группа  $\langle G, \cdot \rangle$  (аддитивная группа  $\langle G, + \rangle$ ) называется *циклической*, если она состоит из всех целых степеней (соответственно, всех целых кратных)

одного элемента  $a \in G$ , т.е.  $G = \{a^n \mid n \in \mathbb{Z}\}$  (соответственно,  $G = \{na \mid n \in \mathbb{Z}\}$ ). Обозначение:  $\langle a \rangle$ , читается: *циклическая группа, порожденная элементом  $a$* .

Рассмотрим примеры.

1. Примером мультипликативной бесконечной циклической группы может служить группа всех целых степеней некоторого фиксированного целого числа  $a \neq \pm 1$ , она обозначается  $a^{\mathbb{Z}}$ . Таким образом,  $a^{\mathbb{Z}} = \langle a \rangle$ .

2. Примером мультипликативной конечной циклической группы является группа  $\mathbb{C}_n$  корней  $n$ -й степени из единицы. Напомним, что корни  $n$ -й степени из единицы находятся по формуле  $\varepsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}$ , где  $k = 0, 1, \dots, n-1$ . Следовательно,  $\mathbb{C}_n = \langle \varepsilon_1 \rangle = \{\varepsilon_1^0 = 1, \varepsilon_1, \varepsilon_1^2 = \varepsilon_2, \dots, \varepsilon_1^{n-1} = \varepsilon_{n-1}\}$ . Вспомним, что комплексные числа  $\varepsilon_k$ ,  $k = 1, \dots, n-1$ , изображаются точками единичной окружности, которые делят ее на  $n$  равных частей.

3. Характерным примером аддитивной бесконечной циклической группы является аддитивная группа целых чисел  $\mathbb{Z}$ , она порождается числом 1, т.е.  $\mathbb{Z} = \langle 1 \rangle$ . Геометрически она изображается в виде целых точек числовой прямой. По существу так же изображается мультипликативная группа  $2^{\mathbb{Z}} = \langle 2 \rangle$ , в общем случае  $a^{\mathbb{Z}} = \langle a \rangle$ , где целое число  $a \neq \pm 1$  (см. рис. 1.3). Это сходство изображений мы обсудим в параграфе 1.6.

4. Выберем в произвольной мультипликативной группе  $G$  некоторый элемент  $a$ . Тогда все целые степени этого элемента образуют циклическую подгруппу  $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} \leq G$ .

5. Докажем, что аддитивная группа рациональных чисел  $\mathbb{Q}$  сама не циклическая, а любые два ее элемента лежат в циклической подгруппе.

А. Докажем, что аддитивная группа  $\mathbb{Q}$  не циклическая. Предположим противное: пусть  $\mathbb{Q} = \left\langle \frac{k}{m} \right\rangle$ . Существует целое число  $b$ , не делящее  $m$ . Поскольку  $\frac{1}{b} \in \mathbb{Q} = \left\langle \frac{k}{m} \right\rangle = \left\{ n \frac{k}{m} \mid n \in \mathbb{Z} \right\}$ , то существует целое число  $n_0$ , такое что  $\frac{1}{b} = n_0 \frac{k}{m}$ . Но тогда  $m = n_0 kb$ , откуда  $m : b$  — пришли к противоречию.

Б. Докажем, что два произвольных рациональных числа  $\frac{a}{b}$  и  $\frac{c}{d}$  принадлежат циклической подгруппе  $\left\langle \frac{1}{m} \right\rangle$ , где  $m$  есть наи-

меньшее общее кратное чисел  $b$  и  $d$ . В самом деле, пусть  $m = bu$  и  $m = dv$ ,  $u, v \in \mathbb{Z}$ , тогда  $\frac{a}{b} = \frac{au}{bu} = au \frac{1}{m} \in \left\langle \frac{1}{m} \right\rangle$  и  $\frac{c}{d} = \frac{cv}{dv} = cv \frac{1}{m} \in \left\langle \frac{1}{m} \right\rangle$ .

**Теорема 1.3.** *Порядок циклической группы равен порядку порождающего элемента этой группы, т.е.  $|\langle a \rangle| = |a|$ .*

*Доказательство.* 1. Пусть  $|a| = \infty$ . Докажем, что все натуральные степени элемента  $a$  различны. Предположим противное: пусть  $a^k = a^m$  и  $0 < k < m$ . Тогда  $m - k$  — натуральное число и  $a^{m-k} = e$ . Но это противоречит тому, что  $|a| = \infty$ . Таким образом, все натуральные степени элемента  $a$  различны, откуда следует бесконечность группы  $\langle a \rangle$ . Следовательно,  $|\langle a \rangle| = \infty = |a|$ .

2. Пусть  $|a| = n$ . Докажем, что  $\langle a \rangle = \{e = a^0, a, a^2, \dots, a^{n-1}\}$ . Из определения циклической группы вытекает включение  $\{a^0, a, a^2, \dots, a^{n-1}\} \subseteq \langle a \rangle$ . Докажем обратное включение. Произвольный элемент циклической группы  $\langle a \rangle$  имеет вид  $a^m$ , где  $m \in \mathbb{Z}$ . Разделим  $m$  на  $n$  с остатком:  $m = nq + r$ , где  $0 \leq r < n$ . Поскольку  $a^n = e$ , то  $a^m = a^{nq+r} = a^{nq} \cdot a^r = a^r \in \{a^0, a, a^2, \dots, a^{n-1}\}$ . Отсюда  $\langle a \rangle \subseteq \{a^0, a, a^2, \dots, a^{n-1}\}$ . Таким образом,  $\langle a \rangle = \{a^0, a, a^2, \dots, a^{n-1}\}$ .

Остается доказать, что все элементы множества  $\{a^0, a, a^2, \dots, a^{n-1}\}$  различны. Предположим противное: пусть  $0 \leq i < j \leq n$ , но  $a^i = a^j$ . Тогда  $a^{j-i} = e$  и  $0 < j - i < n$  — пришли к противоречию с условием  $|a| = n$ . Теорема доказана.

### 1.3.2. Подгруппы циклических групп

Следующая теорема описывает строение подгрупп циклических групп.

**Теорема 1.4.** *Подгруппа циклической группы циклическая. Если  $G = \langle a \rangle$  и  $H$  — неединичная подгруппа группы  $G$ , то  $H = \langle a^n \rangle$ , где  $n$  — наименьшее натуральное число, такое что  $a^n \in H$ .*

*Доказательство.* Пусть  $G = \langle a \rangle$  и  $H$  — подгруппа группы  $G$ . Если подгруппа  $H$  единичная, то  $H = \langle e \rangle$  — циклическая группа. Пусть  $H$  — неединичная подгруппа. Обозначим через  $n$  наименьшее натуральное число, такое что  $a^n \in H$ , и докажем, что  $H = \langle a^n \rangle$ . Включение  $\langle a^n \rangle \subseteq H$  очевидно. Докажем обратное включение. Пусть  $h \in H$ . Поскольку  $G = \langle a \rangle$ , то существует целый показатель  $k$ , такой что  $h = a^k$ . Разделим  $k$  на  $n$  с остатком:  $k = nq + r$ , где  $0 \leq r < n$ . Если предположить, что  $r \neq 0$ , то получим  $h = a^k = a^{nq+r} = a^{nq} \cdot a^r$ , откуда  $a^r = a^{-nq}h \in H$ . Пришли к противоречию с минимальностью показателя  $n$ . Следовательно,  $r = 0$  и  $k = nq$ . Отсюда  $h = a^k = a^{nq} \in \langle a^n \rangle$ . Таким образом,  $H \subseteq \langle a^n \rangle$ , а значит,  $H = \langle a^n \rangle$ . Теорема доказана.

### 1.3.3. Порождающие элементы циклической группы

Какими элементами может порождаться циклическая группа? Отвечают на этот вопрос следующие две теоремы.

**Теорема 1.5.** Пусть дана циклическая группа  $G = \langle a \rangle$  бесконечного порядка. Тогда  $\langle a \rangle = \langle a^k \rangle$  тогда и только тогда, когда  $k = \pm 1$ .

*Доказательство.* Пусть  $G = \langle a \rangle$ ,  $|a| = \infty$  и  $\langle a \rangle = \langle a^k \rangle$ . Тогда существует целое число  $n$ , такое что  $a = a^{kn}$ . Отсюда  $a^{kn-1} = e$ , а так как  $|a| = \infty$ , то  $kn - 1 = 0$ . Но тогда  $kn = 1$  и  $k = \pm 1$ . Обратное утверждение очевидно.

**Теорема 1.6.** Пусть дана циклическая группа  $G = \langle a \rangle$  порядка  $m$ . Тогда  $\langle a \rangle = \langle a^k \rangle$  тогда и только тогда, когда  $\text{НОД}(k, m) = 1$ .

*Доказательство.* ( $\Rightarrow$ ) Пусть  $\langle a \rangle = \langle a^k \rangle$ , докажем, что  $\text{НОД}(k, m) = 1$ . Обозначим  $\text{НОД}(k, m) = d$ . Поскольку  $a \in \langle a \rangle = \langle a^k \rangle$ , то  $a = a^{kn}$  при некотором целом  $n$ . По свойству порядков элементов отсюда следует, что  $(1 - kn) : m$ , т.е.  $1 - kn = mt$  при некотором целом  $t$ . Но тогда  $1 = (kn + mt) : d$ , откуда  $d = 1$  и  $\text{НОД}(k, m) = 1$ .

( $\Leftarrow$ ) Пусть  $\text{НОД}(k, m) = 1$ . Докажем, что  $\langle a \rangle = \langle a^k \rangle$ . Включение  $\langle a^k \rangle \subseteq \langle a \rangle$  очевидно. Обратное, из условия  $\text{НОД}(k, m) = 1$  следует существование целых чисел  $u$  и  $v$ , таких что  $ku + mv = 1$ . Пользуясь тем, что  $|a| = m$ , получаем  $a = a^{ku+mv} = a^{ku}a^{mv} = a^{ku} \in \langle a^k \rangle$ . Следовательно,  $\langle a \rangle = \langle a^k \rangle$ . Теорема доказана.

Напомним, что функция Эйлера  $\varphi(m)$  определяется как количество натуральных чисел, не превосходящих натурального числа  $m$  и взаимно простых с  $m$ . Отсюда получаем следствие.

**Следствие.** Циклическая группа  $\langle a \rangle$  порядка  $m$  имеет  $\varphi(m)$  различных порождающих элементов.

Для придания геометрической наглядности теореме 1.5 изобразим циклическую группу  $G = \langle a \rangle$  порядка  $m$  точками окружности  $A_0, A_1, \dots, A_{m-1}$ , делящими ее на  $m$  равных частей. Элемент  $a^k$  данной группы, соответствующий точке  $A_k$ , будет порождающим тогда и только тогда, когда, соединяя последовательно точки  $A_0, A_k, A_{2k}$  и т.д., мы придем в точку  $A_1$ . Найдём все такие  $k$  при  $m = 10$  простым перебором случаев (рис. 1.5). В результате получим  $k = 1, 3, 7, 9$ . Для циклической группы  $\langle a \rangle$  это означает, что  $\langle a \rangle = \langle a^3 \rangle = \langle a^7 \rangle = \langle a^9 \rangle$ . Обратное: найдя  $k$ , взаимно простое с данным числом  $m$ , можно смело вычерчивать соответствующую «звездочку», твердо зная, что рано или поздно попадешь в каждую точку, ибо  $\langle a \rangle = \langle a^k \rangle$ .



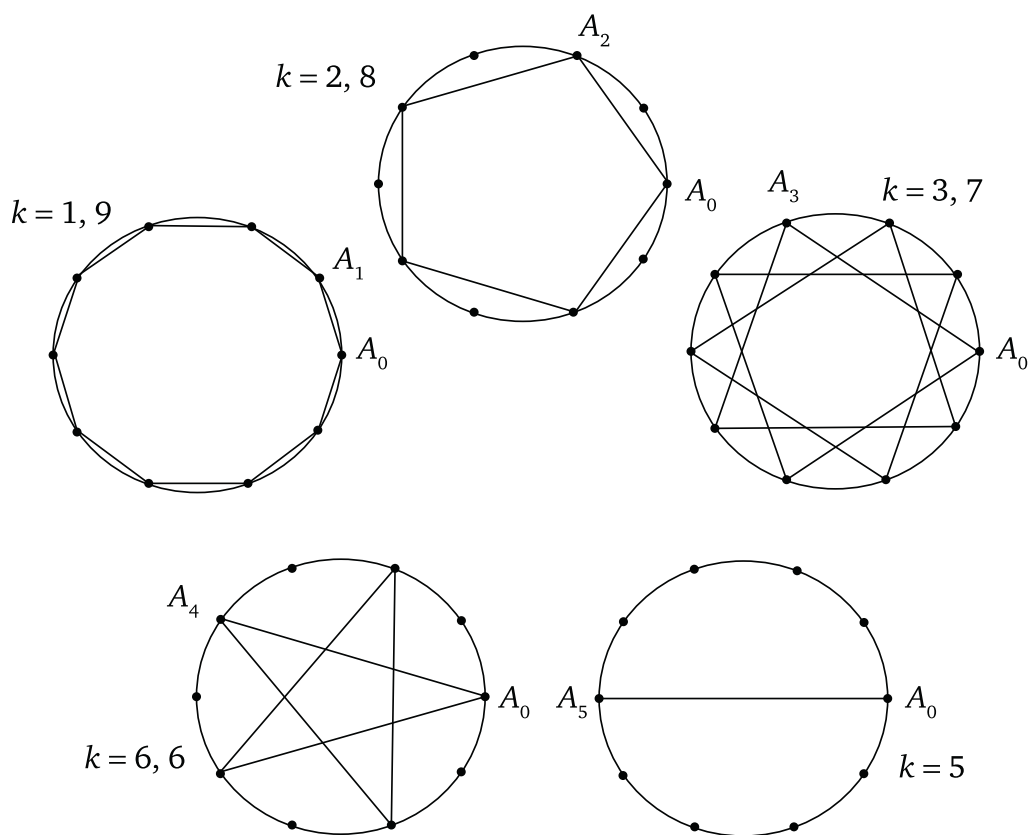


Рис. 1.5

## Контрольные вопросы

1. Может ли пересечение двух циклических подгрупп быть не циклической подгруппой?
2. Есть ли в бесконечной циклической группе неединичный элемент конечного порядка?
3. Имеет ли бесконечная циклическая группа конечную подгруппу?
4. Существует ли в бесконечной циклической группе минимальная неединичная подгруппа (т.е. не содержащая собственных неединичных подгрупп)? Максимальная подгруппа (т.е. собственная подгруппа, которая не содержится в большей собственной подгруппе)?
5. Если порядок циклической группы равен произведению  $m \cdot n$ , то существуют ли в ней подгруппы порядков  $m$  и  $n$ ?
6. Может ли пересечение двух бесконечных циклических подгрупп быть конечной подгруппой?
7. Содержит ли мультипликативная группа  $G = \langle a \rangle$  порядка  $n$  элемент  $a^{n+1}$ ?
8. Сколько порождающих элементов имеет группа  $G = \langle a \rangle$ , если  $|a| = 7$ ,  $|a| = 8$ ,  $|a| = 9$ ,  $|a| = 10$ ?



## Задачи

1. Найдите все подгруппы циклической группы порядка  $n$  для всех  $n \leq 7$ .
2. Убедитесь, что группа подстановок  $S_3$  сама не циклическая, а всякая ее собственная подгруппа — циклическая.
3. Выберите в бесконечной циклической группе две неединичные подгруппы и найдите их пересечение.
4. Выпишите все комплексные корни 6-й степени из единицы, убедитесь, что они образуют мультипликативную группу, и найдите в ней все порождающие элементы.
5. Докажите, что группа  $\mathbb{C}_{p^\infty}$  (группа всех корней всех степеней  $p^n$  для всевозможных натуральных  $n$  и фиксированного простого числа  $p$ ) сама не циклическая, а всякая ее собственная подгруппа циклическая.
6. Пусть  $A$  и  $B$  — подгруппы циклической группы порядка 9. Будет ли объединение множеств  $A \cup B$  подгруппой?
7. Найдите все порождающие элементы циклической группы порядка 12 и постройте рисунки, подобные рис. 1.5.
8. Найдите пересечение аддитивных циклических подгрупп  $\langle 1/3 \rangle \cap \langle 1/5 \rangle$ .
9. Найдите пересечение мультипликативных подгрупп  $\langle 1/3 \rangle \cap \langle 1/5 \rangle$ .
10. Найдите число порождающих группы  $\langle ab \rangle$ , если  $|a| = 3$ ,  $|b| = 5$ .

## 1.4. Смежные классы

### 1.4.1. Определение и примеры

**Определение 1.9.** Пусть  $G$  — группа,  $H$  — ее подгруппа,  $g \in G$ . Умножим каждый элемент  $h \in H$  слева на  $g$ . Получим множество  $gH = \{gh \mid h \in H\}$ , которое называется *левым смежным классом по подгруппе  $H$* . Аналогично определяется *правый смежный класс*:  $Hg = \{hg \mid h \in H\}$ .

Рассмотрим примеры.

1. Рассмотрим симметрическую группу подстановок трех символов  $S_3 = \{e, (12), (13), (23), (123), (132)\}$  и в ней подгруппу четных подстановок  $A_3 = \{e, (123), (132)\}$ . Умножим каждую четную подстановку *слева* на одну и ту же транспозицию  $(12)$ . Получим класс всех нечетных подстановок:

$$\begin{aligned}(12) \cdot A_3 &= \{(12) \cdot e, (12) \cdot (123), (12) \cdot (132)\} = \\ &= \{(12), (13), (23)\}\end{aligned}$$

Видим, что  $S_3 = A_3 \cup (12) \cdot A_3$  (рис. 1.6). Такое представление группы всех подстановок  $S_3$  называется *разложением группы на левые смежные классы по подгруппе  $A_3$* .

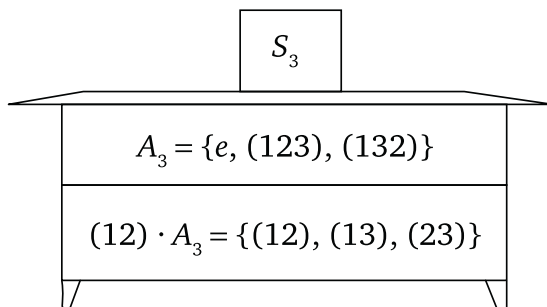


Рис. 1.6

Аналогично можно получить разложение группы  $S_3$  на правые смежные классы по подгруппе  $A_3$ :  $S_3 = A_3 \cup A_3 \cdot (12)$ . Понятно, что это те же самые два подмножества подстановок.

2. Теперь возьмем подгруппу  $H = \{e, (12)\}$  и подобным образом найдем левые смежные классы по подгруппе  $H$ . Перебираем подстановки  $g$ , не входящие в  $H$ , и образуем левые смежные классы  $gH$ , умножая каждую подстановку из  $H$  слева на выбранную подстановку  $g$ :

$$(13) \cdot H = \{(13) \cdot e, (13) \cdot (12)\} = \{(13), (132)\};$$

$$(23) \cdot H = \{(23) \cdot e, (23) \cdot (12)\} = \{(23), (123)\};$$

$$(123) \cdot H = \{(123) \cdot e, (123) \cdot (12)\} = \{(123), (23)\} = (23) \cdot H;$$

$$(132) \cdot H = \{(132) \cdot e, (132) \cdot (12)\} = \{(132), (13)\} = (13) \cdot H.$$

В итоге получаем разложение группы  $S_3$  на левые смежные классы по подгруппе  $H$  (рис. 1.7):

$$\begin{aligned} S_3 &= H \cup (13) \cdot H \cup (23) \cdot H = \\ &= H \cup (123) \cdot H \cup (132) \cdot H. \end{aligned}$$

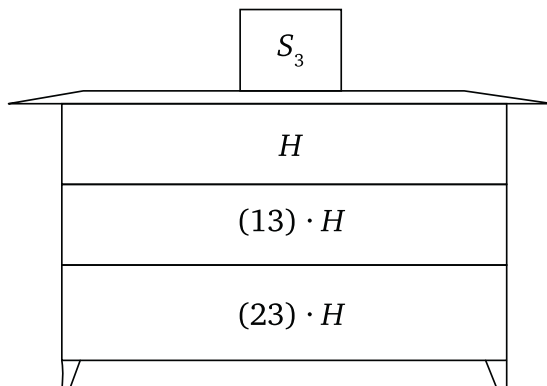


Рис. 1.7

Аналогично можно получить разложение группы  $S_3$  на правые смежные классы по подгруппе  $H$ :

$$S_3 = H \cup H \cdot (13) \cup H \cdot (23) = H \cup H \cdot (123) \cup H \cdot (132).$$

Замечаем, что хотя сами левые и правые смежные классы различны, количество левых смежных классов по подгруппе  $H$  равно количеству правых смежных классов по этой подгруппе. Это, как мы покажем ниже, не случайно.

#### 1.4.2. Основные свойства смежных классов

Доказываемые ниже свойства смежных классов можно наблюдать на приведенных выше примерах.

**Лемма 1.1 (условия совпадения смежных классов).** Пусть  $H$  — подгруппа группы  $G$  и  $a, b \in G$ . Тогда:

$$aH = bH \Leftrightarrow a^{-1}b \in H; Ha = Hb \Leftrightarrow ba^{-1} \in H.$$

*Доказательство.* Докажем условие совпадения левых смежных классов.

( $\Rightarrow$ ) Пусть  $aH = bH$ . Докажем, что  $a^{-1}b \in H$ . Имеем:  $b = b \cdot e \in bH = aH$ . Следовательно, существует элемент  $h \in H$ , такой что  $b = ah$ , откуда  $a^{-1}b = h \in H$ .

( $\Leftarrow$ ) Пусть  $a^{-1}b = h \in H$ . Докажем, что левые смежные классы  $aH$  и  $bH$  совпадают. Из условия  $a^{-1}b = h$  следует  $b = ah$ ,  $a = bh^{-1}$ . Для произвольного элемента  $x \in aH$  имеем  $x = ah_1$  при некотором  $h_1 \in H$ . Отсюда  $x = ah_1 = bh^{-1}h_1 \in bH$ . Следовательно,  $aH \subseteq bH$ . С другой стороны, для произвольного элемента  $y \in bH$  имеем  $y = bh_2$  при некотором  $h_2 \in H$ . Отсюда  $y = bh_2 = ahh_2 \in aH$ . Следовательно,  $bH \subseteq aH$ . Таким образом,  $aH = bH$ .

Аналогично доказывается условие совпадения правых смежных классов.

**Лемма 1.2.** Любые два левых (правых) смежных класса по одной и той же подгруппе либо не пересекаются, либо совпадают.

*Доказательство.* Предположим, что  $aH \cap bH \neq \emptyset$ , и докажем, что  $aH = bH$ . По условию, существует элемент  $c \in aH \cap bH$ . Отсюда следует существование элементов  $h_1, h_2 \in H$ , таких что  $c = ah_1$  и  $c = bh_2$ . Из первого равенства получаем  $a^{-1}c = h_1 \in H$ , а из второго  $b^{-1}c = h_2 \in H$ . По лемме 1.1 из первого соотношения следует, что  $aH = cH$ , а из второго получаем  $bH = cH$ . Следовательно,  $aH = bH$ .

**Лемма 1.3.** Любые два левых (правых) смежных класса по одной и той же подгруппе содержат одинаковое количество элементов.

*Доказательство.* Докажем, что произвольный смежный класс  $aH$  содержит столько же элементов, сколько их в подгруппе  $H$ . Для этого установим отображение  $\varphi: aH \rightarrow H$ , положив  $\varphi(ah) = h$  для любого  $h \in H$ , и докажем, что  $\varphi$  является взаимно однозначным отображением  $aH$  на  $H$ .

1.  $\varphi$  — отображение, т.е. из равенства  $ah_1 = ah_2$ ,  $h_1, h_2 \in H$ , следует  $\varphi(ah_1) = \varphi(ah_2)$ . Действительно,  $ah_1 = ah_2 \Rightarrow h_1 = h_2 \Rightarrow \varphi(ah_1) = \varphi(ah_2)$ .

2. Отображение  $\varphi$  взаимно однозначно, что доказывает проведение предыдущих рассуждений в обратном порядке.

3.  $\varphi$  — отображение на  $H$ . В самом деле, прообразом произвольного элемента  $h \in H$  является элемент  $ah \in aH$ .

Итак,  $\varphi$  — взаимно однозначное отображение  $aH$  на  $H$ , откуда следует, что  $aH$  и  $H$  содержат одинаковое количество элементов. Таким образом, любые два левых смежных класса по подгруппе  $H$  содержат одинаковое количество элементов.

**Определение 1.10.** Представление группы  $G$  в виде объединения различных левых (правых) смежных классов по подгруппе  $H$  называется *разложением группы на левые (правые) смежные классы по данной подгруппе*:

$$G = g_1H \cup g_2H \cup \dots, \quad G = Hg_1 \cup Hg_2 \cup \dots$$

Заметим, что среди всех смежных классов только один является подгруппой — это смежный класс  $eH = H$ , где  $e$  — единица группы  $G$ .

### 1.4.3. Теорема Лагранжа и следствия из нее

Рассмотрим разложение конечной группы  $G$  на левые смежные классы по подгруппе  $H$  (рис. 1.8):  $G = H \cup g_1H \cup g_2H \cup \dots \cup g_{k-1}H$ .

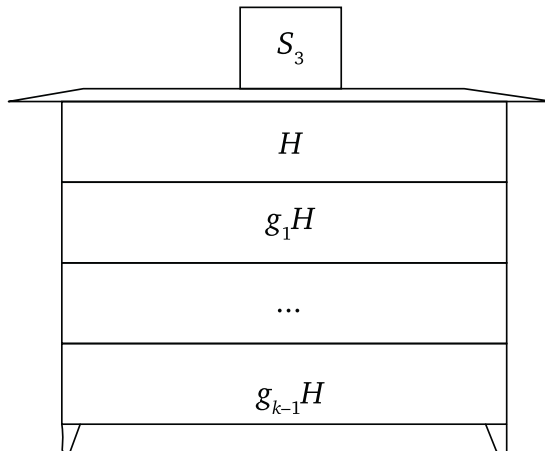


Рис. 1.8

Поскольку, как мы доказали, в каждом смежном классе столько же элементов, сколько их в подгруппе  $H$ , то  $|G| = |H| \cdot k$ . Этот же результат мы получим, рассматривая разложение данной группы на правые смежные классы по той же подгруппе. Таким образом, доказана следующая теорема.

**Теорема 1.7 (Лагранжа).** *Порядок конечной группы равен произведению порядка подгруппы на число левых (правых) смежных классов по этой подгруппе.*

Из теоремы Лагранжа вытекает, что число левых смежных классов конечной группы  $G$  по подгруппе  $H$  равно числу правых смежных классов по этой подгруппе. Докажем, что это верно в любой группе.

**Теорема 1.8.** *В любой группе  $G$  число (мощность множества) левых смежных классов по подгруппе  $H$  равно числу (мощности множества) правых смежных классов по этой подгруппе.*

*Доказательство.* Сопоставляя всякому левому смежному классу  $gH$  правый смежный класс  $Hg^{-1}$ , мы получаем взаимно однозначное отображение множества всех левых смежных классов по подгруппе  $H$  на множество всех правых смежных классов по этой подгруппе, что и доказывает теорему.

Доказанное свойство приводит к следующему определению.

**Определение 1.11.** *Индексом в группе  $G$  подгруппы  $H$  называется количество (мощность множества) левых или правых смежных классов по этой подгруппе.*

Индекс обозначается  $|G : H|$ .

С помощью введенного понятия теорему Лагранжа можно записать так:  $|G| = |H| \cdot |G : H|$ . Читается: *порядок конечной группы  $G$  равен произведению порядка подгруппы  $H$  на ее индекс.*

**Следствие 1.** *Порядок подгруппы конечной группы является делителем порядка группы.*

Заметим, что если  $|G| : m$ , то отсюда совсем не следует, что группа  $G$  содержит подгруппу порядка  $m$ . Например, группа четных подстановок четырех символов  $A_4$  имеет порядок 12, но, как легко видеть, она не содержит подгрупп порядка 6.

**Следствие 2.** *Порядок элемента конечной группы является делителем порядка группы.*

*Доказательство.* Пусть группа  $G$  конечна и  $a \in G$ . По теореме 1.3  $|\langle a \rangle| = |a|$ , а по следствию 1  $|G| : |\langle a \rangle| = |a|$ .

**Следствие 3.** *Группа простого порядка циклическая.*

*Доказательство.* Пусть  $|G| = p$ , где  $p$  — простое число, и  $e \neq a \in G$ . По следствию 2 порядок элемента  $a$  является делителем числа  $p$ , отличным от единицы. Следовательно,  $|a| = p$

и группа  $G$  исчерпывается всеми степенями элемента  $a$ . Другими словами,  $G = \langle a \rangle$ .

**Следствие 4.** Если  $|G| = n$ , то  $a^n = e$  для любого  $a \in G$ .

**Доказательство.** Пусть  $|a| = m$ . По следствию 2  $n \div m$ . Пусть  $n = mq$ ,  $q \in \mathbb{Z}$ , тогда  $a^n = a^{mq} = e^q = e$ .

## Контрольные вопросы

1. Какие смежные классы по подгруппе  $H$  содержат единицу группы?
2. Если порядок подгруппы конечной группы равен 5, то какова формула порядка группы?
3. Сколько подгрупп имеет группа порядка 7?
4. Каково пересечение подгрупп порядков 8 и 9?
5. Если группа  $G$  конечна,  $|G| = n$ ,  $H_1 < H_2 < G$  и  $|G : H_2| = k$ ,  $|H_2 : H_1| = m$ , то чему равен порядок подгруппы  $H_1$ ?
6. Чему равен индекс подгруппы  $\langle 5 \rangle$  в аддитивной группе  $\mathbb{Z}$ ?
7. Может ли индекс подгруппы в группе быть бесконечным?

## Задачи

1. Выпишите разложения аддитивной группы  $\mathbb{Z} = \langle 1 \rangle$  на смежные классы по подгруппам  $\langle m \rangle$  последовательно для  $m = 2, \dots, 6$ .
2. Выпишите разложения мультипликативной бесконечной циклической группы  $G = \langle a \rangle$  по подгруппам  $\langle a^m \rangle$  последовательно для  $m = 2, \dots, 6$ .
3. Выпишите разложения мультипликативной группы  $\mathbb{C}_m$  корней  $m$ -й степени из единицы по всем подгруппам для  $m = 2, \dots, 7$ .
4. Выпишите разложения на левые и правые смежные классы группы подстановок  $S_3$  по всем подгруппам.
5. Пусть  $H$  — подгруппа группы  $G$ . Определим на множестве элементов группы  $G$  отношение  $\sim$ , положив  $x \sim y \Leftrightarrow x^{-1}y \in H$  ( $yx^{-1} \in H$ ). Докажите, что отношение  $\sim$  является отношением эквивалентности и классы эквивалентных элементов совпадают с левыми (соответственно, правыми) смежными классами по подгруппе  $H$ .
6. Выпишите разложения на смежные классы:
  - а) аддитивной группы  $\mathbb{Q}_3 = \left\{ \frac{m}{3^n} \mid m \in \mathbb{Z}, n = 0, 1, \dots \right\}$  по подгруппе  $\mathbb{Z}$ ;
  - б) мультипликативной группы  $\mathbb{R}^*$  по подгруппе положительных действительных чисел  $\mathbb{R}^+$ ;
  - в) аддитивной группы целых комплексных чисел  $\mathbb{Z} + \mathbb{Z}i = \{a + bi \mid a, b \in \mathbb{Z}\}$  по подгруппе  $\mathbb{Z}$ ;
  - г) группы самосовмещений квадрата по всем ее подгруппам.
7. Найдите все подгруппы и их индексы циклической группы порядка 30.

8. Пусть  $G$  — аддитивная группа геометрических векторов плоскости, выходящих из начала координат (в прямоугольной системе координат), и  $\vec{a} \in G$ . Изобразите смежный класс  $\vec{b} + \langle \vec{a} \rangle$ . Что представляют собой концы векторов этого смежного класса?

## 1.5. Нормальная подгруппа и факторгруппа

### 1.5.1. Определение нормальной подгруппы, примеры

Элемент группы далеко не всегда перестановочен с другими элементами этой группы. Легко видеть, что множество всех элементов группы, перестановочных с каждым элементом группы, является подгруппой. Введем название для этой подгруппы.

**Определение 1.12.** Множество всех элементов группы  $G$ , перестановочных с каждым ее элементом, называется *центром* группы и обозначается  $C(G)$ .

Таким образом,  $C(G) = \{c \in G \mid \forall g \in G \, cg = gc\}$ . Понятно, что абелева группа совпадает со своим центром. В группе  $S_3$  центр является единичной подгруппой.

Если  $H = C(G)$ , то для любого элемента  $g \in G$  имеет место равенство  $gH = Hg$ . Введем обобщающее понятие.

**Определение 1.13.** Подгруппа  $H$  группы  $G$  называется *нормальной*, если она перестановочна с любым элементом группы, т.е.  $gH = Hg$  для любого  $g \in G$ .

Обозначение:  $H \triangleleft G$ . Читается:  $H$  — нормальная подгруппа группы  $G$ .

Равенство  $gH = Hg$  совсем не означает, что  $gh = hg$  для любого  $h \in H$ . Оно означает лишь, что для любого элемента  $gh \in gH$  существует элемент  $h_1 \in H$ , такой что  $gh = h_1g$ . Например, в равенстве  $(12)A_3 = A_3(12)$  левая часть есть множество

$$\begin{aligned} (12) \cdot \{e, (123), (132)\} = \\ = \{(12) \cdot e, (12) \cdot (123), (12) \cdot (132)\} = \{(12), (13), (23)\}, \end{aligned}$$

а правая часть есть множество

$$\begin{aligned} \{e, (123), (132)\} \cdot (12) = \{e \cdot (12), (123) \cdot (12), (132) \cdot (12)\} = \\ = \{(12), (23), (13)\}. \end{aligned}$$

Видим, что  $(12) \cdot (123) = (13) = (132) \cdot (12)$ , и это демонстрирует равенство  $gh = h_1g$  при  $g = (12)$ ,  $h = (123)$ ,  $h_1 = (132)$ .

Примеры.

1. В коммутативной группе всякая подгруппа нормальна.
2. В любой группе единичная подгруппа и сама группа нормальны.



3. Центр группы  $C(G)$  является нормальной подгруппой.

4. В группе  $S_3$  возьмем подгруппу  $H_1$  всех подстановок, оставляющих символ 1 на месте. Тогда  $H_1$  не является нормальной подгруппой, так как  $(12) \cdot H_1 \neq H_1 \cdot (12)$ .

5. Докажем, что  $A_n \trianglelefteq S_n$  для любого  $n$ . Пусть  $g \in S_n$ . Если  $g$  — четная подстановка, то  $gA_n = A_n = A_ng$ . Пусть  $g$  — нечетная подстановка. Тогда смежный класс  $gA_n$  состоит из нечетных подстановок и всякая нечетная подстановка содержится в  $gA_n$  (докажите). Следовательно, разложение группы  $S_n$  на левые смежные классы по подгруппе  $A_n$  имеет вид  $S_n = A_n \cup gA_n$ . Аналогично получаем разложение группы  $S_n$  на правые смежные классы:  $S_n = A_n \cup A_ng$ . Отсюда делаем вывод, что  $gA_n = A_ng$ . Следовательно,  $A_n \trianglelefteq S_n$ .

Замечаем, что в этом доказательстве решающую роль сыграло то обстоятельство, что  $|S_n : A_n| = 2$ . Докажем, что в произвольной группе подгруппа  $H$  индекса 2 является нормальной. В самом деле, по условию, для любого  $g \in G$  имеем  $G = H \cup gH = H \cup Hg$ . Отсюда  $gH = Hg$ . Следовательно,  $H \trianglelefteq G$ .

Чтобы сформулировать критерий нормальной подгруппы, введем одно новое понятие, играющее в теории групп важную роль.

**Определение 1.14.** В группе  $G$  элемент  $a \in G$  называется сопряженным с элементом  $b \in G$ , если существует элемент  $g \in G$ , такой что  $a = g^{-1}bg$ .

**Теорема 1.9 (критерий нормальной подгруппы).** Подгруппа  $H$  группы  $G$  является нормальной тогда и только тогда, когда она вместе с каждым своим элементом содержит и всякий сопряженный с ним элемент:

$$H \trianglelefteq G \Leftrightarrow \forall h \in H, \forall g \in G \ g^{-1}hg \in H.$$

**Доказательство.** ( $\Rightarrow$ ) Пусть  $H \trianglelefteq G$  и  $h \in H, g \in G$ . Докажем, что  $g^{-1}hg \in H$ . Используя определение нормальной подгруппы, получаем  $hg \in Hg = gH$ . Следовательно, существует элемент  $h_1 \in H$ , такой что  $hg = gh_1$ . Отсюда  $g^{-1}hg = h_1 \in H$ .

( $\Leftarrow$ ) Пусть из того, что  $h \in H, g \in G$ , следует, что  $g^{-1}hg \in H$ . Докажем, что  $gH = Hg$ . Произвольный элемент из  $Hg$  имеет вид  $hg$ , где  $h \in H$ . Имеем:  $hg = g \cdot g^{-1}hg = gh_1 \in gH$ , где  $g^{-1}hg = h_1 \in H$ . Следовательно,  $Hg \subseteq gH$ . Аналогично доказывается обратное включение. Таким образом,  $gH = Hg$  для любого  $g \in G$ , т.е.  $H \trianglelefteq G$ .

Рассмотрим примеры.

1. С использованием критерия нормальной подгруппы совсем просто доказывается нормальность подгруппы чет-

ных подстановок  $A_n$  в группе всех подстановок  $n$  символов  $S_n$ . В самом деле, если  $a \in A_n$ , то для любой подстановки  $s \in S_n$  подстановка  $s^{-1}as$  является четной, а значит, принадлежит  $A_n$ . Следовательно,  $A_n \triangleleft S_n$ .

2. Докажем, что в группе  $G = GL_n(\mathbb{R})$  обратимых квадратных матриц порядка  $n$  над полем  $\mathbb{R}$  подгруппа  $H$ , состоящая из матриц с определителем, равным единице, является нормальной. Пусть матрица  $A \in H$ , это значит, что ее определитель  $|A| = 1$ . Для любой матрицы  $B \in G$  имеем

$$|B^{-1}AB| = |B^{-1}| \cdot |A| \cdot |B| = |B^{-1}| \cdot 1 \cdot |B| = |B^{-1} \cdot B| = |E| = 1.$$

Следовательно,  $B^{-1}AB \in H$  и  $H \triangleleft G$ .

**Теорема 1.10.** *Пересечение двух нормальных подгрупп есть нормальная подгруппа.*

*Доказательство.* Пусть  $H_1$  и  $H_2$  — нормальные подгруппы группы  $G$  и  $H = H_1 \cap H_2$ . По теореме 1.2  $H$  есть подгруппа группы  $G$ . Для любых  $h \in H$  и  $g \in G$  имеем  $g^{-1}hg \in H_1$  и  $g^{-1}hg \in H_2$ . Следовательно,  $g^{-1}hg \in H_1 \cap H_2 = H$ . Теорема доказана.

### 1.5.2. Факторгруппа

Рассмотрим множество всех левых смежных классов группы  $G$  по подгруппе  $H$ . Естественно попытаться определить умножение левых смежных классов формулой  $aH \cdot bH = abH$  для любых  $a, b \in G$ . Но для этого нужно, чтобы элемент  $b$  всегда можно было переставить через  $H$ . Это возможно лишь в случае, когда  $H$  является нормальной подгруппой.

Пусть теперь подгруппа  $H$  нормальна в группе  $G$ . Тогда всякий левый смежный класс  $gH$  равен правому смежному классу  $Hg$  и можно говорить просто о смежных классах по нормальной подгруппе  $H$ . Докажем, что в этом случае результат  $aH \cdot bH = abH$  не зависит от выбора представителей смежных классов. Пусть  $aH = a_1H$ ,  $bH = b_1H$ . Докажем, что  $aH \cdot bH = a_1H \cdot b_1H$ . Для этого нужно доказать, что  $abH = a_1b_1H$ , а это равносильно условию  $(ab)^{-1}a_1b_1 \in H$ . Поскольку  $aH = a_1H$ ,  $bH = b_1H$ , то  $a^{-1}a_1 \in H$ ,  $b^{-1}b_1 \in H$ . Используя нормальность подгруппы  $H$ , получаем

$$(ab)^{-1}a_1b_1 = b^{-1}a^{-1}a_1b_1 = b^{-1}b_1 \cdot b_1^{-1}a^{-1}a_1b_1 = b^{-1}b_1 \cdot b_1^{-1}(a^{-1}a_1)b_1 \in H.$$

Таким образом, умножение смежных классов является бинарной операцией, и, как легко видеть, множество всех смежных классов относительно этой операции образует группу (с единицей  $H$ ). Она обозначается  $G/H$  (читается:  $G$  по  $H$ ). Введем название для этой группы.

**Определение 1.15.** Если  $H$  — нормальная подгруппа группы  $G$ , то группа смежных классов  $G/H$  называется *факторгруппой* группы  $G$  по подгруппе  $H$ .

**Теорема 1.11.** Факторгруппа циклической группы циклическая.

*Доказательство.* Пусть  $H$  — подгруппа группы  $G = \langle a \rangle$ . По теореме 1.4  $H = \langle a^n \rangle$  при некотором натуральном  $n$ . Тогда  $G/H = \{H, aH, a^2H, \dots, a^{n-1}H\} = \langle aH \rangle$  — циклическая группа. Теорема доказана.

Вместе с тем если нормальная подгруппа  $H$  и факторгруппа по ней  $G/H$  циклические, то группа  $G$  не обязана быть циклической. Например, группа подстановок  $S_3$  не является циклической, хотя она имеет циклическую подгруппу  $H = A_3 = \langle a \rangle$ , где  $a = (123)$ , и факторгруппа  $G/H = S_3/A_3 = \langle bA_3 \rangle$ , где  $b = (12)$ , является циклической.

### 1.5.3. Аддитивная группа классов вычетов

Зафиксируем натуральное число  $m$  и рассмотрим факторгруппу

$$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \{m\mathbb{Z}, 1 + m\mathbb{Z}, 2 + m\mathbb{Z}, \dots, (m-1) + m\mathbb{Z}\}.$$

Смежные классы этой факторгруппы называются *классами вычетов по модулю  $m$* , а число каждого класса называется *вычетом* этого класса. Используя условия равенства смежных классов, для целых чисел  $a$  и  $b$  получаем:  $a + m\mathbb{Z} = b + m\mathbb{Z} \Leftrightarrow a - b \in m\mathbb{Z}$ . В этом случае говорят, что  $a$  сравнимо с  $b$  по модулю  $m$  и пишут:  $a \equiv b \pmod{m}$ , а последняя запись называется *сравнением по модулю  $m$* . Сравнения изучаются в теории чисел, и наша задача — «навести мосты» между теорией групп и теорией чисел.

Введем обозначение:  $\bar{a} = a + m\mathbb{Z}$  для любого  $a \in \mathbb{Z}$ . Таким образом,  $\bar{a} = \{a + mt \mid t \in \mathbb{Z}\}$  и  $\bar{a} = \bar{b} \Leftrightarrow a - b \in m\mathbb{Z} \Leftrightarrow a \equiv b \pmod{m}$ . Факторгруппа  $Z_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$  называется *аддитивной группой классов вычетов по модулю  $m$* . Используя правило сложения смежных классов, получаем

$$\bar{a} + \bar{b} = (a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z} = \overline{a + b}.$$

Например, при  $m = 6$  получаем аддитивную группу классов вычетов  $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ .

**Упражнение 1.5.** Заполните таблицу сложения (таблицу Кэли) для этой группы. Вычисления для заполненной строки:  $\bar{3} + \bar{0} = \bar{3}$ ,  $\bar{3} + \bar{1} = \bar{4}$ ,  $\bar{3} + \bar{2} = \bar{5}$ ,  $\bar{3} + \bar{3} = \bar{6} = \bar{0}$ ,  $\bar{3} + \bar{4} = \bar{7} = \bar{1}$ ,  $\bar{3} + \bar{5} = \bar{8} = \bar{2}$ .

|           | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| $\bar{0}$ |           |           |           |           |           |           |
| $\bar{1}$ |           |           |           |           |           |           |
| $\bar{2}$ |           |           |           |           |           |           |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ |           |           |           |           |           |           |
| $\bar{5}$ |           |           |           |           |           |           |

Для наглядного восприятия множества  $Z_6$  построим числовую прямую и окружность длины  $m = 6$ , касающуюся числовой прямой в точке 0. Разделим окружность на шесть равных частей, начиная с точки касания. Легко видеть, что при наматывании числовой прямой на окружность справа и слева (рис. 1.9) в точках деления на окружности соберутся соответствующие классы вычетов.

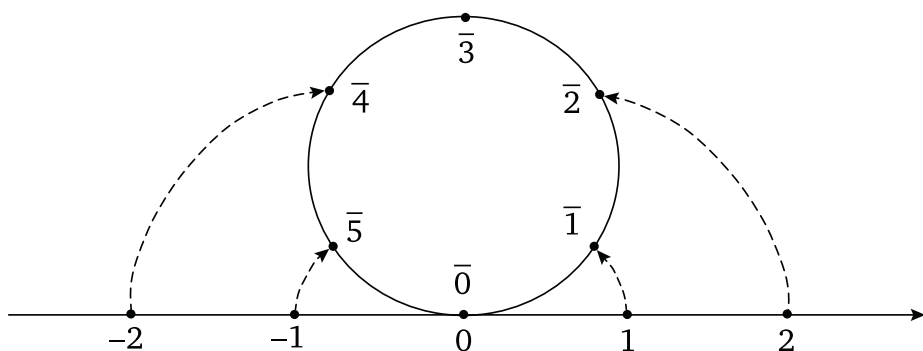


Рис. 1.9

#### 1.5.4. Мультипликативная группа классов вычетов

По аналогии со сложением определим на множестве классов вычетов  $\mathbb{Z}_m$  операцию умножения по формуле  $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$  для любых  $a, b \in \mathbb{Z}$ . Докажем независимость результата от выбора представителей классов. Пусть  $\bar{a} = \bar{a}_1$ ,  $\bar{b} = \bar{b}_1$ , докажем, что  $\bar{a} \cdot \bar{b} = \bar{a}_1 \cdot \bar{b}_1$ . Имеем:

$$\begin{aligned}
 \bar{a} = \bar{a}_1, \bar{b} = \bar{b}_1 &\Rightarrow (a - a_1) : m, (b - b_1) : m \Rightarrow (a - a_1)(b - b_1) : m \Rightarrow \\
 &\Rightarrow (a - a_1)(b - b_1) = ab - a_1b - ab_1 + a_1b_1 = \\
 &= (ab - a_1b_1) + a_1(b_1 - b) + b_1(a_1 - a) : m \Rightarrow \\
 &\Rightarrow (ab - a_1b_1) : m \Rightarrow \overline{ab} = \overline{a_1b_1} \Rightarrow \bar{a} \cdot \bar{b} = \bar{a}_1 \cdot \bar{b}_1.
 \end{aligned}$$

Легко видеть, что умножение классов вычетов ассоциативно, а класс  $\bar{1}$  играет роль единицы при умножении классов. Однако не всякий класс вычетов по модулю  $m$  обратим, т.е. не для всякого класса вычетов существует обратный класс. Например, при  $m = 6$  обратимыми будут лишь классы  $\bar{1}$  и  $\bar{5}$  ( $\bar{1}^{-1} = \bar{1}$ ,  $\bar{5}^{-1} = \bar{5}$ ). Вместе с тем если  $\mathbb{Z}_m^*$  обозначает множество всех обратимых классов вычетов по модулю  $m$ , то система  $\langle \mathbb{Z}_m^*, \cdot \rangle$  — мультипликативная группа, которая называется мультипликативной группой классов вычетов по модулю  $m$  и кратко обозначается  $\mathbb{Z}_m^*$ . Например,  $\mathbb{Z}_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ ,  $\mathbb{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ . Рассмотрим общий случай.

**Теорема 1.12.** *Класс вычетов  $\bar{a}$  принадлежит  $\mathbb{Z}_m^*$  тогда и только тогда, когда  $\text{НОД}(a, m) = 1$ .*

*Доказательство.* Если класс вычетов  $\bar{a}$  обратим, то существует класс вычетов  $\bar{b}$ , такой что  $\bar{a} \cdot \bar{b} = \bar{1} \Rightarrow \overline{ab} = \bar{1} \Rightarrow ab - 1 : m \Rightarrow \text{НОД}(a, m) = 1$ . Обратно, если  $\text{НОД}(a, m) = 1$ , то существуют  $u, v \in \mathbb{Z}$ , такие что  $au + mv = 1$ . Отсюда

$$\bar{1} = \overline{au + mv} = \bar{a}\bar{u} + \bar{m}\bar{v} = \bar{a}\bar{u} + \bar{0}\bar{v} = \bar{a}\bar{u}.$$

Следовательно,  $\bar{a}^{-1} = \bar{u}$ , т.е. класс  $\bar{a}$  обратим и  $\bar{a} \in \mathbb{Z}_m^*$ .

**Следствие.**  $|\mathbb{Z}_m^*| = \varphi(m)$ .

Например,  $|\mathbb{Z}_5^*| = \varphi(5) = 4$ ,  $|\mathbb{Z}_6^*| = \varphi(6) = 2$ ,  $|\mathbb{Z}_7^*| = \varphi(7) = 6$ .

**Теорема 1.13 (Эйлера).** *Если целое число  $a > 1$  взаимно просто с натуральным числом  $m$ , то  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .*

*Доказательство.* Рассмотрим мультипликативную группу классов вычетов  $\mathbb{Z}_m^*$ . По следствию, ее порядок равен  $\varphi(m)$ . По условию,  $\text{НОД}(a, m) = 1$ , откуда по теореме 1.12 класс вычетов  $\bar{a} \in \mathbb{Z}_m^*$ . Но тогда по следствию 4 из теоремы Лагранжа  $\bar{a}^{\varphi(m)} = \bar{1}$ , откуда  $a^{\varphi(m)} \equiv 1 \pmod{m}$ . Теорема доказана. (Другое доказательство теоремы см. в работе [3].)

### 1.5.5. Классы сопряженных элементов

Рассмотрим подробнее отношение сопряженности элементов группы. Легко видеть, что оно является отношением эквивалентности (оно рефлексивно: всякий элемент сопряжен сам с собой; симметрично: если первый элемент сопряжен со вторым, то второй сопряжен с первым; и транзитивно: если первый элемент сопряжен со вторым, а второй — с третьим, то первый элемент сопряжен с третьим). Вследствие этого группа  $G$  распадается на непересекающиеся классы сопряженных элементов. Класс элементов, сопряженных с элементом  $a$ , будем обозначать  $K_a$ .

Например, группа подстановок  $S_3$  распадается на следующие классы сопряженных элементов:  $\{e\}$ ,  $\{(12), (13), (23)\}$ ,  $\{(123), (132)\}$ .

Вообще, две подстановки сопряжены тогда и только тогда, когда их разложения в произведение независимых циклов состоят из циклов одинаковой длины. Например, подстановки  $a = (12)(345)$  и  $b = (54)(321)$  сопряжены. Чтобы найти сопрягающую подстановку, выписываем символы первой подстановки и подписываем под ними символы второй подстановки так, чтобы циклы одинаковой длины стояли друг под другом:

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix} = (15)(24).$$

Легко проверить, что  $s^{-1}as = b$ .

Множество всех элементов группы, перестановочных с данным элементом группы, очевидно, является подгруппой. Введем название для этой подгруппы.

**Определение 1.16.** Подгруппа всех элементов группы, перестановочных с данным элементом группы, называется *централизатором* данного элемента и обозначается  $C_G(a)$  (читается: централизатор элемента  $a$  в группе  $G$ ). Таким образом,  $C_G(a) = \{c \in G \mid ca = ac\}$ .

**Теорема 1.14.** Пусть  $K_a$  — класс всех элементов группы  $G$ , сопряженных с элементом  $a \in G$ . Тогда количество элементов класса  $K_a$  равно индексу централизатора элемента  $a$  в группе  $G$ , т.е.  $|K_a| = |G : C_G(a)|$ .

*Доказательство.* Обозначим  $H = C_G(a)$ . Элементу  $g^{-1}ag \in K_a$  поставим в соответствие правый смежный класс  $Hg$ , т.е. определим  $\varphi(g^{-1}ag) = Hg$  для любого  $g \in G$ . Докажем, что  $\varphi$  является взаимно однозначным отображением множества элементов класса  $K_a$  на множество всех правых смежных классов по подгруппе  $H$ . Отсюда и будет следовать равенство  $|K_a| = |G : H|$ .

1.  $\varphi$  является отображением. Действительно, пусть  $g^{-1}ag = g_1^{-1}ag_1$ , докажем, что  $\varphi(g^{-1}ag) = \varphi(g_1^{-1}ag_1)$ . Имеем:

$$\begin{aligned} g^{-1}ag = g_1^{-1}ag_1 &\Rightarrow g_1g^{-1}agg_1^{-1} = a \Rightarrow (gg_1^{-1})^{-1}a(gg_1^{-1}) = a \Rightarrow \\ &\Rightarrow gg_1^{-1} \in H \Rightarrow Hg = Hg_1 \Rightarrow \varphi(g^{-1}ag) = \varphi(g_1^{-1}ag_1). \end{aligned}$$

2. Отображение  $\varphi$  взаимно однозначно, т.е. если  $\varphi(g^{-1}ag) = \varphi(g_1^{-1}ag_1)$ , то  $g^{-1}ag = g_1^{-1}ag_1$ , что доказывается проведением предыдущих рассуждений в обратном порядке.



3. Очевидно,  $\varphi$  является отображением  $K_a$  на все множество правых смежных классов по подгруппе  $H$ .

Этим заканчивается доказательство теоремы.

Из доказанной теоремы и теоремы Лагранжа вытекает следствие.

**Следствие.** В конечной группе  $G$  число элементов, сопряженных с фиксированным элементом  $a \in G$ , является делителем порядка группы, т.е.  $|G| : |K_a|$ .

**Теорема 1.15.** Если порядок группы  $G$  равен  $p^n$ , где  $p$  — простое;  $n$  — натуральное число, то группа  $G$  имеет неединичный центр.

**Доказательство.** Рассмотрим разложение данной группы на непересекающиеся классы сопряженных элементов:

$$G = K_e \cup K_{g_1} \cup K_{g_2} \cup \dots \cup K_{g_m}.$$

Отсюда следует, что  $|G| = |K_e| + |K_{g_1}| + |K_{g_2}| + \dots + |K_{g_m}|$ . Очевидно,  $K_e = \{e\}$ , так что  $|K_e| = 1$ , а по следствию  $p^n = |G| : |K_{g_i}|$  для любого  $i = 1, 2, \dots, m$ . Следовательно, число  $|K_{g_i}|$  есть либо 1, либо кратно  $p$ . Поскольку  $|G| = p^n$ ,  $|K_e| = 1$ , то все числа  $|K_{g_1}|$ ,  $|K_{g_2}|$ , ...,  $|K_{g_m}|$  не могут быть кратными числу  $p$ . Таким образом, существует элемент  $g_j \in G$ ,  $g_j \neq e$ , такой что  $|K_{g_j}| = 1$ . Отсюда следует, что  $g_j \in C(G)$ . Теорема доказана.

## Контрольные вопросы

1. Во всякой ли группе есть собственная нормальная подгруппа?
2. Чему равно пересечение всех нормальных подгрупп группы?
3. Если  $A$  и  $B$  — нормальные подгруппы группы  $G$ , то будет ли нормальной подгруппой множество  $AB = \{ab \mid a \in A, b \in B\}$ ?
4. Если  $H \triangleleft G$ ,  $g \in G$ , то чему равна подгруппа  $g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$ ?
5. Может ли группа содержать один класс (два класса) сопряженных элементов?
6. Будет ли группа конечной, если она имеет конечную нормальную подгруппу, факторгруппа по которой конечна?
7. Будет ли группа циклической, если она имеет циклическую нормальную подгруппу, факторгруппа по которой циклическая?

## Задачи

1. Докажите, что пересечение любого количества нормальных подгрупп есть нормальная подгруппа.



2. Составьте таблицу сложения элементов факторгруппы  $\mathbb{Z}_m = \mathbb{Z}/\langle m \rangle$  для каждого  $m$ ,  $2 \leq m \leq 6$ .

3. Дана мультипликативная бесконечная циклическая группа  $G = \langle a \rangle$ . Составьте таблицу умножения элементов факторгруппы  $G/H$  для всех подгрупп  $\langle e \rangle < H \leq \langle a^7 \rangle$ .

4. Найдите все факторгруппы циклических групп порядков 7—10.

5. Найдите все факторгруппы групп подстановок  $S_3$  и  $S_4$ .

6. Выясните, что геометрически представляют собой смежные классы аддитивной группы комплексных чисел  $\mathbb{C}$  по подгруппе  $\mathbb{R}$  действительных чисел. Изобразите в прямоугольной системе координат смежные классы  $\mathbb{R}$ ,  $i + \mathbb{R}$  и  $2i + \mathbb{R}$ . Найдите и изобразите суммы этих смежных классов.

7. Убедитесь, что в аддитивной группе  $\mathbb{C}$  комплексных чисел множество  $H = \{x + kxi \mid x \in \mathbb{R}\}$  при фиксированном  $k \in \mathbb{R}$  является подгруппой. Какими точками в прямоугольной системе координат изображается эта подгруппа? Как изображаются смежные классы по этой подгруппе? Сформулируйте на геометрическом языке правило сложения смежных классов.

8. Докажите, что факторгруппа по центру не может быть циклической.

9. Представьте группу  $S_4$  в виде объединения классов сопряженных элементов.

10. Докажите, что порядки сопряженных элементов равны.

11. Выясните, какие из следующих матриц сопряжены в соответствующей группе обратимых матриц:  $M_1 = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ ,  $M_2 = \begin{pmatrix} 3 & 1 \\ -1 & 1 \end{pmatrix}$ ,  $M_3 = \begin{pmatrix} 2 & 1 \\ -2 & 0 \end{pmatrix}$ ,  $M_4 = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$ .

12. Рассмотрим множество  $K = \{1, -1, i, -i, j, -j, k, -k\}$ . Его элементы 1 и  $-1$  будем называть действительными единицами, а остальные элементы — мнимыми единицами и считать, что  $i^2 = j^2 = k^2 = ijk = -1$ , всякая действительная единица перестановочна с каждой мнимой единицей. Составьте таблицу умножения элементов множества  $K$  и убедитесь, что получили группу (она называется группой кватернионов). Найдите порядок каждого элемента группы кватернионов, все ее подгруппы и нормальные подгруппы, все факторгруппы, представьте группу кватернионов в виде объединения классов сопряженных элементов.

## 1.6. Изоморфизмы групп

### 1.6.1. Определение и примеры

Две группы  $\langle G, \cdot \rangle$  и  $\langle G_1, \circ \rangle$  с групповыми операциями  $\cdot$  и  $\circ$  будем считать одинаковыми и называть изоморфными, если

их можно совместить так, что результаты операций над соответствующими элементами совпадут. Под совмещением групп  $\langle G, \cdot \rangle$  и  $\langle G_1, \circ \rangle$  мы понимаем установление взаимно однозначного отображения  $f$  множества  $G$  на множество  $G_1$ , при котором  $f(x \cdot y) = f(x) \circ f(y)$  для любых элементов  $x, y \in G$  (рис. 1.10).

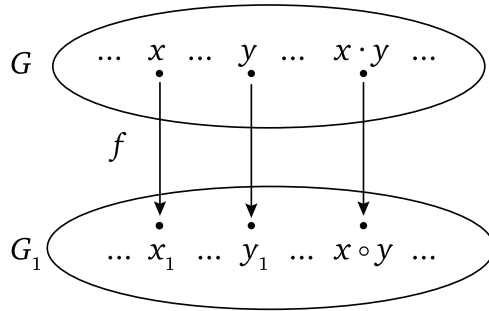


Рис. 1.10

**Определение 1.17.** Группа  $\langle G, \cdot \rangle$  называется *изоморфной* группе  $\langle G_1, \circ \rangle$ , если существует взаимно однозначное отображение  $f$  множества  $G$  на множество  $G_1$ , такое что для любых элементов  $x, y \in G$  выполняется равенство  $f(x \cdot y) = f(x) \circ f(y)$ . Имея в виду это равенство, говорят, что отображение  $f$  *сохраняет групповую операцию*. При этом отображение  $f$  называется *изоморфизмом* группы  $\langle G, \cdot \rangle$  на группу  $\langle G_1, \circ \rangle$ .

Примеры.

1. Рассмотрим аддитивную группу действительных чисел  $\mathbb{R}$  и аддитивную группу  $S$  скалярных матриц вида

$$M_a = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a \end{pmatrix},$$

где  $a \in \mathbb{R}$ , и сопоставим всякому действительному числу  $a \in \mathbb{R}$  матрицу  $M_a$ . Отображение  $f(a) = M_a$  для любого  $a \in \mathbb{R}$  является, как легко видеть, изоморфизмом группы  $\mathbb{R}$  на группу  $S$ .

2. Отображение мультипликативной группы положительных действительных чисел  $\mathbb{R}^+$  на аддитивную группу всех действительных чисел  $\mathbb{R}$ , при котором всякому числу  $a \in \mathbb{R}^+$  ставится в соответствие десятичный логарифм этого числа  $\lg(a) \in \mathbb{R}$ , обладает свойством  $\lg(a \cdot b) = \lg(a) + \lg(b)$ , т.е. является изоморфизмом группы  $\langle \mathbb{R}^+, \cdot \rangle$  на группу  $\langle \mathbb{R}, + \rangle$ . Этот изоморфизм можно увидеть, рассматривая график логарифмической функции. Практически этот изоморфизм использовался

при вычислениях на логарифмической линейке, когда умножение чисел сводится к сложению отрезков.

3. Рассмотрим отображение  $\varphi$  мультипликативной группы невырожденных матриц  $GL_n(\mathbb{R})$  на группу  $\langle \mathbb{R}^*, \cdot \rangle$ , при котором всякой матрице  $A$  ставится в соответствие ее определитель  $|A|$ . Это отображение обладает свойством  $\varphi(A \cdot B) = |A \cdot B| = |A| \cdot |B| = \varphi(A) \cdot \varphi(B)$ . Однако отображение  $\varphi$  не является изоморфизмом, так как оно не взаимно однозначно.

### 1.6.2. Основные свойства изоморфизмов групп

Пусть  $f$  — изоморфизм группы  $\langle G, \cdot \rangle$  на группу  $\langle G_1, \circ \rangle$ .

1. При изоморфизме единица  $e$  группы  $\langle G, \cdot \rangle$  переходит в единицу  $e_1$  группы  $\langle G_1, \circ \rangle$ .

*Доказательство.* Докажем, что образ единицы  $f(e)$  является единицей в  $G_1$ . Возьмем произвольный элемент  $a_1 \in G_1$ . Так как, по определению изоморфизма,  $f$  является отображением на  $G_1$ , то  $a_1$  имеет прообраз в  $G$ , т.е. существует  $a \in G$ , такой что  $f(a) = a_1$ . Но тогда  $a_1 \circ f(e) = f(a) \circ f(e) = f(a \cdot e) = f(a) = a_1$ . Аналогично устанавливаем, что  $f(e) \circ a_1 = a_1$ . Следовательно,  $f(e)$  — единица в  $G_1$ , а так как в группе  $\langle G_1, \circ \rangle$  единица  $e_1$  единственна, то  $f(e) = e_1$ .

2. Для любого  $a \in G$   $f(a^{-1}) = (f(a))^{-1}$ , т.е. образ обратного элемента равен обратному для образа этого элемента.

*Доказательство.* Обозначим  $f(a) = a_1$  и докажем, что  $f(a^{-1}) = a_1^{-1}$ . Имеем:  $f(a^{-1}) \circ f(a) = f(a^{-1} \cdot a) = f(e) = e_1$ . Аналогично доказывается, что  $f(a) \circ f(a^{-1}) = e_1$ . Следовательно,  $f(a^{-1})$  является обратным для элемента  $f(a) = a_1$ . Но в группе  $\langle G_1, \circ \rangle$  для элемента  $a_1$  обратный элемент  $a_1^{-1}$  единственный. Следовательно,  $f(a^{-1}) = a_1^{-1} = (f(a))^{-1}$ .

3. Обратное отображение  $f^{-1}$  является изоморфизмом группы  $\langle G_1, \circ \rangle$  на группу  $\langle G, \cdot \rangle$ .

*Доказательство.* Поскольку  $f$  является взаимно однозначным отображением  $G$  на  $G_1$ , то  $f^{-1}$  является взаимно однозначным отображением множества  $G_1$  на множество  $G$ . Возьмем произвольные элементы  $a_1, b_1 \in G_1$ . Существуют  $a, b \in G$ , такие что  $f(a) = a_1, f(b) = b_1$ . Из равенства  $f(a \cdot b) = f(a) \circ f(b)$  выводим, что  $a \cdot b = f^{-1}(f(a) \circ f(b))$ . Поскольку  $a = f^{-1}(a_1), b = f^{-1}(b_1)$ , то, производя замену, получаем  $f^{-1}(a_1) \cdot f^{-1}(b_1) = f^{-1}(a_1 \circ b_1)$ . Следовательно,  $f^{-1}$  является изоморфизмом группы  $\langle G_1, \circ \rangle$  на группу  $\langle G, \cdot \rangle$ .

Благодаря свойству 3 можно говорить об изоморфных группах. Если группы  $G$  и  $G_1$  изоморфны, то пишут:  $G \cong G_1$  (читается:

группа  $G$  изоморфна группе  $G_1$ ). Группы изучаются с точностью до изоморфизма, т.е. с точностью до обозначений элементов и групповых операций.

### 1.6.3. Изоморфизмы циклических групп

Циклические группы с точностью до изоморфизма описываются следующей теоремой.

**Теорема 1.16.** *Всякая бесконечная циклическая группа изоморфна аддитивной группе целых чисел  $\mathbb{Z} = \langle 1 \rangle$ , а всякая циклическая группа порядка  $t$  изоморфна мультипликативной группе  $C_m$  корней  $t$ -й степени из единицы.*

**Доказательство.** 1. Пусть дана мультипликативная бесконечная циклическая группа  $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ . Рисунок 1.11 подсказывает отображение  $f: \langle a \rangle \rightarrow \mathbb{Z}$  по формуле  $f(a^n) = n$  для любого  $n \in \mathbb{Z}$ .

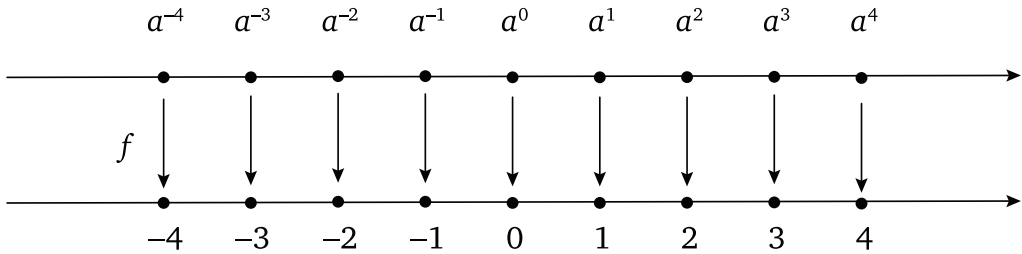


Рис. 1.11

Поскольку  $|a| = \infty$ , то для любых целых чисел  $m$  и  $n$  равенство  $a^m = a^n$  имеет место тогда и только тогда, когда  $m = n$ . Следовательно,  $f$  является взаимно однозначным соответствием и, очевидно, на все множество  $\mathbb{Z}$ . Кроме того,

$$f(a^m \cdot a^n) = f(a^{m+n}) = m + n = f(a^m) + f(a^n).$$

Следовательно, отображение  $f$  является изоморфизмом циклической группы  $\langle a \rangle$  на аддитивную циклическую группу  $\mathbb{Z} = \langle 1 \rangle$ .

2. Пусть дана мультипликативная циклическая группа  $G = \langle a \rangle$  порядка  $t$ . На рис. 1.12 ее элементы изображены точками на первой окружности, а точки на второй окружности изображают комплексные корни  $t$ -й степени из единицы, составляющие циклическую группу корней  $C_m = \langle \epsilon \rangle = \{1, \epsilon, \epsilon^2, \dots, \epsilon^{m-1}\}$ , где  $\epsilon = \cos \frac{2\pi}{m} + i \sin \frac{2\pi}{m}$ . Видим, что группы  $C = \langle a \rangle$  и  $C_m = \langle \epsilon \rangle$  изображаются одинаково и могут быть совмещены

с сохранением операции. Следовательно, они изоморфны. Докажем этот зримый факт формально логически.

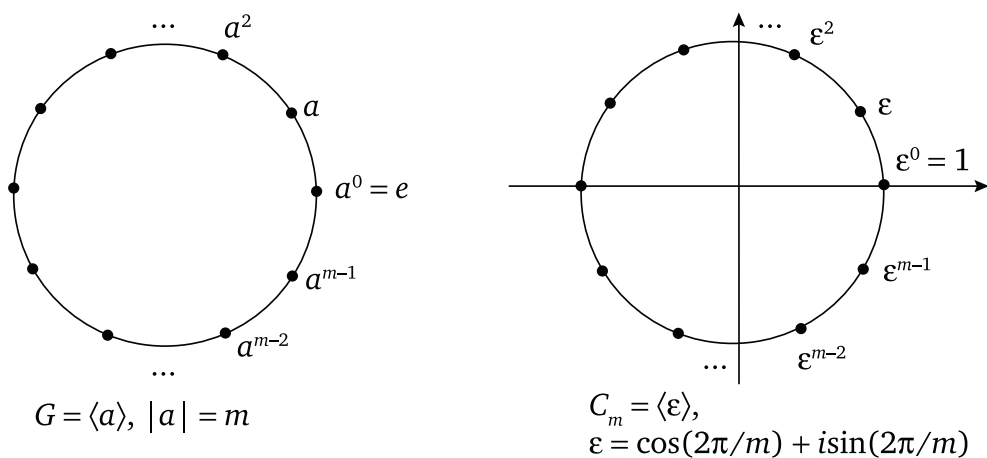


Рис. 1.12

Определим  $f(a^n) = \epsilon^n$  для любого целого  $n$ . Имеем:  $a^{n_1} = a^{n_2} \Leftrightarrow a^{n_1 - n_2} = e \Leftrightarrow n_1 - n_2 : m \Leftrightarrow \epsilon^{n_1} = \epsilon^{n_2}$ . Следовательно,  $f$  является взаимно однозначным отображением циклической группы  $\langle a \rangle$  на циклическую группу  $C_m = \langle \epsilon \rangle$ . В то же время

$$f(a^k \cdot a^n) = f(a^{k+n}) = \epsilon^{k+n} = \epsilon^k \cdot \epsilon^n = f(a^k) \cdot f(a^n).$$

Следовательно, отображение  $f$  является изоморфизмом циклической группы  $\langle a \rangle$  порядка  $m$  на циклическую группу  $C_m = \langle \epsilon \rangle$ . Теорема доказана.

**Следствие.** Две циклические группы изоморфны тогда и только тогда, когда их порядки равны.

**Доказательство.** ( $\Rightarrow$ ) Поскольку изоморфизм является взаимно однозначным отображением одной группы на другую, то изоморфные группы имеют равные порядки.

( $\Leftarrow$ ) Пусть  $|\langle a \rangle| = |\langle b \rangle|$ . Докажем, что  $\langle a \rangle \cong \langle b \rangle$ . Предположим сначала, что обе циклические группы бесконечны:  $|\langle a \rangle| = |\langle b \rangle| = \infty$ . По теореме 1.16 группы  $\langle a \rangle$  и  $\langle b \rangle$  изоморфны одной и той же аддитивной группе целых чисел, а значит, изоморфны между собой. Аналогично если  $|\langle a \rangle| = |\langle b \rangle| = m$ , то каждая из групп  $\langle a \rangle$  и  $\langle b \rangle$  изоморфна одной и той же циклической группе  $C_m = \langle \epsilon \rangle$ , а значит, снова группы  $\langle a \rangle$  и  $\langle b \rangle$  изоморфны. Следствие доказано.

#### 1.6.4. Связь конечных групп с группами подстановок

Оказывается, изучение конечных групп может быть сведено к изучению групп подстановок. Убеждает нас в этом следующая теорема.

**Теорема 1.17 (Кэли).** *Всякая конечная группа изоморфна подгруппе некоторой группы подстановок.*

*Доказательство.* Пусть даны конечная группа  $G = \{x_1, x_2, \dots, x_n\}$  и  $g$  — фиксированный элемент данной группы. Определим отображение  $f_g: G \rightarrow G$  по формуле  $f_g(x_i) = gx_i$ ,  $i = 1, \dots, n$ . Поскольку  $x_i = x_j \Leftrightarrow gx_i = gx_j$ , то  $f_g$  является взаимно однозначным отображением. Кроме того, для всякого элемента  $x_k \in G$  уравнение  $gx = x_k$  однозначно разрешимо, и если  $x_i$  является его решением, то  $f_g(x_i) = gx_i = x_k$ . Следовательно,  $f_g$  является взаимно однозначным отображением множества  $G$  на себя, т.е. является подстановкой на множестве  $G$ . Для наглядности подстановку  $f_g$  можно записать в привычном виде:

$$f_g = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ gx_1 & gx_2 & \dots & gx_n \end{pmatrix}.$$

Образ элемента  $x_i$  при отображении  $f_g$  будем записывать в виде  $x_i^{f_g}$  (а не в виде  $f_g(x_i)$ , что, быть может, более привычно, но в данном случае менее удобно). Для любых  $g_1, g_2 \in G$  и любого  $x_i \in G$  имеем:

$$x_i^{f_{(g_1 g_2)^{-1}}} = (g_1 g_2)^{-1} x_i = g_2^{-1} g_1^{-1} x_i = g_2^{-1} \cdot x_i^{f_{g_1^{-1}}} = x_i^{f_{g_1^{-1}} f_{g_2^{-1}}}.$$

Следовательно,  $f_{(g_1 g_2)^{-1}} = f_{g_1^{-1}} \cdot f_{g_2^{-1}}$ . Определим теперь отображение  $\phi$  группы  $G$  в группу подстановок  $S_G$  формулой  $\phi(g) = f_g \in S_G$  для любого  $g \in G$ . Рассмотрим подстановки

$$f_{g_1^{-1}} = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ g_1^{-1} x_1 & g_1^{-1} x_2 & \dots & g_1^{-1} x_n \end{pmatrix},$$

$$f_{g_2^{-1}} = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ g_2^{-1} x_1 & g_2^{-1} x_2 & \dots & g_2^{-1} x_n \end{pmatrix}.$$

Понятно, что из равенства элементов  $g_1 = g_2$  следует равенство подстановок  $f_{g_1^{-1}} = f_{g_2^{-1}}$ . Обратно, если  $f_{g_1^{-1}} = f_{g_2^{-1}}$ , то для любого  $x_i \in G$  имеем

$$x_i^{f_{g_1^{-1}}} = x_i^{f_{g_2^{-1}}} \Rightarrow g_1^{-1} x_i = g_2^{-1} x_i \Rightarrow g_1^{-1} = g_2^{-1} \Rightarrow g_1 = g_2.$$

Следовательно,  $\phi$  является взаимно однозначным отображением группы  $G$  в группу подстановок  $S_G$ . В то же время  $\phi(g_1 \cdot g_2) = f_{(g_1 g_2)^{-1}} = f_{g_1^{-1}} \cdot f_{g_2^{-1}} = \phi(g_1) \cdot \phi(g_2)$ . Таким образом,  $\phi$  является изоморфизмом данной группы  $G$  в группу подстановок  $S_G$ . Теорема доказана.

## Контрольные вопросы

1. Сколько неизоморфных подгрупп содержит группа целых чисел?
2. Может ли нециклическая группа быть изоморфной циклической группе?
3. Существует ли изоморфизм группы  $\mathbb{Z}$  на группу  $\mathbb{Q}$ ? Докажите.
4. Существует ли изоморфизм группы  $\mathbb{Q}$  на группу  $\mathbb{R}$ ? Докажите.
5. Сколько существует групп, изоморфных данной группе?
6. Сколько неизоморфных подгрупп содержит группа  $S_3$ ?
7. Сколько неизоморфных подгрупп содержит группа простого порядка?
8. Сколько существует изоморфных отображений бесконечной циклической группы на себя?
9. Сколько существует изоморфных отображений на себя циклической группы простого порядка?
10. Могут ли в изоморфных группах существовать неизоморфные подгруппы?

## Задачи

1. Используя изоморфизм  $\lg$  мультипликативной группы действительных чисел  $\mathbb{R}^+$  на аддитивную группу действительных чисел  $\mathbb{R}$ , найдите прообразы чисел  $2, 4, \frac{1}{3}, \frac{2}{3}, \pi, 2\pi$ .
2. Рассмотрите аддитивную группу двумерных арифметических векторов  $V_2$  над полем  $\mathbb{R}$  и найдите в ней подгруппу, изоморфную аддитивной группе  $\mathbb{R}$ .
3. В аддитивной группе квадратных матриц порядка 2 над полем  $\mathbb{R}$  найдите несколько подгрупп, изоморфных аддитивным группам  $\mathbb{Q}$  и  $\mathbb{R}$ .
4. В аддитивной группе комплексных чисел установите изоморфизм подгрупп  $\mathbb{R}$  и  $\mathbb{R}i$ . Укажите другие изоморфные подгруппы в  $\mathbb{C}$ .
5. Перечислите по экземпляру все неизоморфные (циклические) группы, порядок которых не превосходит 6.
6. Докажите, что всякая группа подстановок  $S_n$  изоморфна подгруппе группы подстановок  $S_{n+1}$ .
7. Докажите, что аддитивная группа  $n$ -мерного векторного пространства  $V_n$  над полем  $\mathbb{R}$  изоморфна аддитивной группе арифметических  $n$ -мерных векторов  $\mathbb{R}^n = \{(\alpha_1, \alpha_2, \dots, \alpha_n) \mid \alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{R}\}$ .
8. Докажите, что аддитивная группа комплексных чисел изоморфна аддитивной группе двумерных арифметических векторов с действительными компонентами.
9. Докажите, что группа всех параллельных переносов плоскости изоморфна аддитивной группе векторов плоскости, выходящих из одной точки.



## 1.7. Гомоморфизмы групп

### 1.7.1. Определение и свойства гомоморфизмов групп.

#### Ядро гомоморфизма

**Определение 1.18.** Отображение  $\varphi$  группы  $\langle G, \cdot \rangle$  на группу  $\langle G_1, \circ \rangle$  называется *гомоморфизмом*, если для любых элементов  $x, y \in G$   $\varphi(x \cdot y) = \varphi(x) \circ \varphi(y)$ . При этом группу  $\langle G_1, \circ \rangle$  называют *гомоморфным образом* группы  $\langle G, \cdot \rangle$ .

Таким образом, изоморфизм есть взаимно однозначный гомоморфизм. Как и для изоморфизма, легко доказать, что если  $e$  и  $e_1$  являются единицами соответственно групп  $G$  и  $G_1$ , то  $\varphi(e) = e_1$  и для любого  $a \in G$   $\varphi(a^{-1}) = (\varphi(a))^{-1}$ .

Введем понятие, характеризующее гомоморфизм одной группы на другую.

**Определение 1.19.** Ядром гомоморфизма  $\varphi$  группы  $\langle G, \cdot \rangle$  на группу  $\langle G_1, \circ \rangle$  называется множество всех элементов из  $G$ , отображающихся в единицу  $e_1$  из  $G_1$ .

Обозначение:  $\ker \varphi$  (от слова *kernel* — ядро). Таким образом,  $\ker \varphi = \{x \in G \mid \varphi(x) = e_1\}$ .

**Теорема 1.18.** Ядро гомоморфизма  $\varphi$  группы  $\langle G, \cdot \rangle$  на группу  $\langle G_1, \circ \rangle$  является нормальной подгруппой группы  $\langle G, \cdot \rangle$ .

*Доказательство.* Обозначим  $H = \ker \varphi$ .

1.  $H$  замкнуто относительно умножения. В самом деле, если  $h_1, h_2 \in H$ , то, по определению ядра гомоморфизма,  $\varphi(h_1) = e_1$ ,  $\varphi(h_2) = e_1$ . Но тогда  $\varphi(h_1 \cdot h_2) = \varphi(h_1) \circ \varphi(h_2) = e_1 \circ e_1 = e_1$ . Следовательно,  $h_1 \cdot h_2 \in H$ .

2. Поскольку  $\varphi(e) = e_1$ , то  $e \in H$ .

3. Если  $h \in H$ , то  $\varphi(h) = e_1$ , откуда  $\varphi(h^{-1}) = (\varphi(h))^{-1} = e_1$ , следовательно,  $h^{-1} \in H$ .

Таким образом,  $H$  является подгруппой.

4. Докажем, что подгруппа  $H$  нормальна, воспользовавшись критерием нормальной подгруппы. Для любых  $h \in H$  и  $g \in G$  имеем:

$$\begin{aligned}\varphi(g^{-1} \cdot h \cdot g) &= \varphi(g^{-1}) \circ \varphi(h) \circ \varphi(g) = \varphi(g^{-1}) \circ e_1 \circ \varphi(g) = \\ &= \varphi(g^{-1}) \circ \varphi(g) = \varphi(g^{-1} \cdot g) = \varphi(e) = e_1.\end{aligned}$$

Следовательно,  $g^{-1}hg \in H$ . Таким образом,  $H \triangleleft G$ . Теорема доказана.

*Примеры.*

1. Отображение  $\varphi: GL_n(R) \rightarrow \langle R^*, \cdot \rangle$ , при котором  $\varphi(A) = |A|$  для любой матрицы  $A \in GL_n(R)$ , является гомоморфизмом с ядром, состоящим из всех матриц с определителем, равным единице, т.е.  $\ker \varphi = \{A \in GL_n(R) \mid |A| = 1\}$ .

2. Гомоморфизмом аддитивной группы целых чисел  $\mathbb{Z} = \langle 1 \rangle$  на мультипликативную группу корней  $m$ -й степени из единицы  $\mathbb{C}_m = \langle \varepsilon \rangle$  является отображение  $\varphi(n) = \varepsilon^n$  для любого  $n \in \mathbb{Z}$ . Ядром этого гомоморфизма является подгруппа  $m\mathbb{Z}$  целых чисел, кратных  $m$ .

3. Отображение  $\varphi: S_n \rightarrow \mathbb{Z}^* = \{1, -1\}$ , которое всякой подстановке сопоставляет ее знак, т.е.  $\varphi(s) = \text{sign}(s)$  для любой подстановки  $s \in S$ , является гомоморфизмом симметрической группы подстановок  $S_n$  на мультипликативную группу  $\mathbb{Z}^*$ , и ядром этого гомоморфизма является нормальная подгруппа четных подстановок  $A_n$ .

4. Рассмотрим отображение  $\varphi$  мультипликативной группы действительных чисел  $\mathbb{R}^*$  на мультипликативную группу положительных действительных чисел  $\mathbb{R}^+$ , при котором  $\varphi(a) = |a|$  для любого  $a \in \mathbb{R}^*$ . Легко видеть, что  $\varphi$  является гомоморфизмом с ядром  $\ker \varphi = \{1, -1\}$ .

5. Пусть  $H$  — нормальная подгруппа группы  $G$ . Определим отображение  $\varphi$  группы  $G$  на факторгруппу  $G/H$ , положив  $\varphi(g) = gH$ . Нетрудно доказать, что  $\varphi$  является гомоморфизмом и  $\ker \varphi = H$ . Таким образом, *всякая нормальная подгруппа группы является ядром некоторого гомоморфизма*. Вместе с тем, сопоставляя всякому гомоморфизму данной группы  $G$  ядро этого гомоморфизма, мы получаем взаимно однозначное отображение множества всех гомоморфизмов данной группы на множество всех ее нормальных подгрупп.

### 1.7.2. Теорема о гомоморфизмах

Начнем с примера. Выше было доказано, что аддитивная группа классов вычетов  $\mathbb{Z}_m$  изоморфна мультипликативной группе корней  $m$ -й степени из единицы  $\mathbb{C}_m$ . С другой стороны, группу  $\mathbb{Z}_m$  можно рассматривать как факторгруппу  $\mathbb{Z}/m\mathbb{Z}$ . В то же время  $m\mathbb{Z}$  является ядром гомоморфизма аддитивной группы  $\mathbb{Z}$  на мультипликативную группу корней  $\mathbb{C}_m$  при отображении  $\varphi(n) = \varepsilon^n$  для любого  $n \in \mathbb{Z}$  (см. предыдущий параграф). Другими словами,  $m\mathbb{Z} = \ker \varphi$ . Таким образом,  $\mathbb{C}_m$  является гомоморфным образом группы  $\mathbb{Z}$  при гомоморфизме  $\varphi$  и факторгруппа  $\mathbb{Z}/\ker \varphi$  изоморфна группе  $\mathbb{C}_m$ . Отсюда получаем, что *гомоморфный образ группы  $\mathbb{Z}$ , т.е.  $\mathbb{C}_m$ , изоморфен факторгруппе  $\mathbb{Z}/\ker \varphi$  — факторгруппе группы  $\mathbb{Z}$  по ядру гомоморфизма  $\varphi$* . Докажем общую теорему.

**Теорема 1.19 (о гомоморфизмах).** *Гомоморфный образ группы изоморфен факторгруппе по ядру гомоморфизма.*

*Доказательство.* Пусть  $\varphi$  является гомоморфизмом группы  $G$  на группу  $G_1$  и  $H = \ker \varphi$  (рис. 1.13).

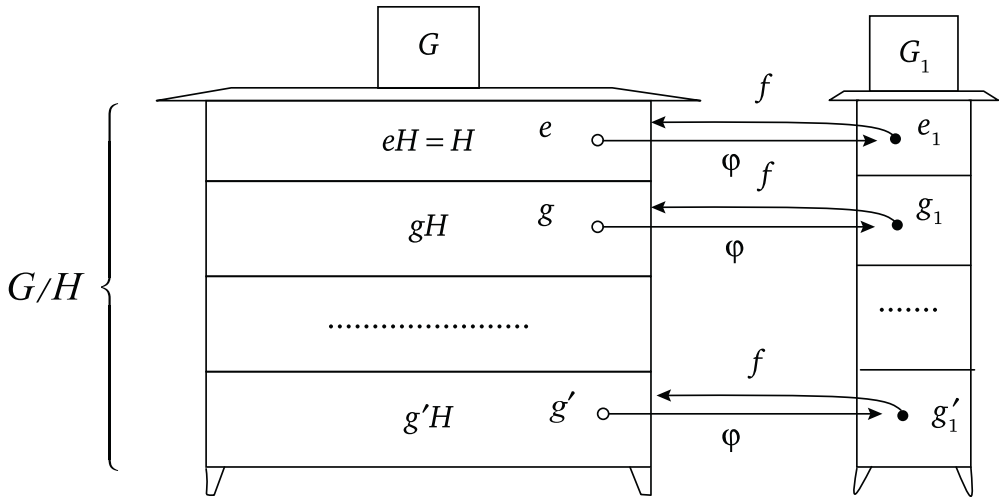


Рис. 1.13

Докажем, что группа  $G_1$  (гомоморфный образ группы  $G$ ) изоморфна факторгруппе  $G/H = G/\ker \varphi$  (факторгруппе группы  $G$  по ядру гомоморфизма  $\ker \varphi$ ). Пусть  $g_1 \in G_1$ . Поскольку  $\varphi$  является отображением на множество  $G_1$ , то у элемента  $g_1$  есть прообраз при  $\varphi$ . Другими словами, существует элемент  $g \in G$ , такой что  $\varphi(g) = g_1$ . Определим  $f(g_1) = f(\varphi(g)) = gH$  для любого  $g \in G$  и докажем, что  $f$  является искомым изоморфизмом группы  $G_1$  на факторгруппу  $G/H$ .

1.  $f$  является взаимно однозначным отображением  $G_1$  на  $G/H$ , т.е. для любых элементов  $g_1, g'_1 \in G_1$  имеет место равенство  $g_1 = g'_1$  тогда и только тогда, когда  $f(g_1) = f(g'_1)$ . Пусть  $g_1 = \varphi(g)$ ,  $g'_1 = \varphi(g')$ . Имеем:  $g_1 = g'_1 \Leftrightarrow \varphi(g) = \varphi(g') \Leftrightarrow \varphi(g)^{-1}\varphi(g') = e_1 \Leftrightarrow \varphi(g^{-1}g') = e_1 \Leftrightarrow g^{-1}g' \in \ker \varphi = H \Leftrightarrow gH = g'H \Leftrightarrow f(g_1) = f(g'_1)$ .

2.  $f$  является отображением  $G_1$  на  $G/H$ . Возьмем произвольный смежный класс  $gH \in G/H$  и найдем его прообраз при отображении  $f$ . Но, по определению,  $f(\varphi(g)) = gH$ . Следовательно, прообразом смежного класса  $gH$  при  $f$  является элемент  $g_1 = \varphi(g)$ .

3. Наконец,  $f$  сохраняет операцию. В самом деле, если  $g_1 = \varphi(g)$ ,  $g'_1 = \varphi(g')$ , то

$$\begin{aligned} f(g_1 g'_1) &= f(\varphi(g) \cdot \varphi(g')) = f(\varphi(g \cdot g')) = \\ &= gg'H = gH \cdot g'H = f(g_1) \cdot f(g'_1). \end{aligned}$$

Теорема доказана.

## Контрольные вопросы

1. Если группы изоморфны, то будет ли существовать гомоморфизм одной группы на другую?
2. Может ли гомоморфный образ коммутативной группы быть некоммутативной группой?
3. Может ли при гомоморфизме циклическая группа отображаться на нециклическую? Нециклическая — на циклическую?
4. Пусть  $\varphi$  — гомоморфизм конечной группы  $G$  на группу  $G_1$ . Будут ли эти группы изоморфны, если их порядки равны?
5. Если конечная группа  $G$  гомоморфно отображается на группу  $G_1$ , то каково соотношение между порядками этих групп?
6. Каковы гомоморфные образы группы простого порядка?
7. Всегда ли пересечение двух ядер гомоморфизмов является ядром некоторого гомоморфизма?

## Задачи

1. Опишите гомоморфные образы бесконечной циклической группы.
2. Опишите гомоморфные образы циклических групп порядков 7—9.
3. Установите гомоморфизм аддитивной группы целых чисел на мультипликативную циклическую группу порядка 10 и найдите его ядро.
4. Найдите все гомоморфные образы группы  $S_3$  и укажите ядра соответствующих гомоморфизмов.
5. Определим отображение мультипликативной группы  $\mathbb{C}^*$  на мультипликативную группу  $\mathbb{R}^+$ , при котором всякому комплексному числу, отличному от нуля, ставится в соответствие модуль этого числа. Докажите, что это отображение является гомоморфизмом, и найдите его ядро. Как геометрически изобразятся смежные классы по ядру гомоморфизма?
6. В группе  $S_4$  подгруппа  $H = \{e, (12)(34), (13)(24), (14)(23)\}$  называется *четверной группой Клейна*. Докажите, что она нормальна в  $S_4$ , и выпишите все смежные классы по этой подгруппе. Убедитесь, что в каждом из них содержится по одной подстановке, оставляющей на месте символ 4. Используя это, определите гомоморфизм группы  $S_4$  на группу  $S_3$ .
7. Опишите все гомоморфизмы периодической группы в группу без кручения.

## 1.8\*. Конечные абелевы группы

### 1.8.1. Прямое произведение подгрупп

Введем важную конструкцию, позволяющую группу «раскладывать на множители», подобно тому как всякое натуральное число можно разложить на простые множители.

**Определение 1.20.** Говорят, что группа  $G$  равна прямому произведению своих подгрупп  $A$  и  $B$ , если выполнены следующие условия:

1)  $A \leq G, B \leq G$ ;

2)  $A \cap B = \{e\}$  — единичная подгруппа;

3) Группа  $G$  порождается подгруппами  $A$  и  $B$ , т.е. всякий элемент группы  $G$  представим в виде произведения элементов, взятых из  $A$  и  $B$ .

Обозначение:  $G = A \times B$ . В случае аддитивной терминологии говорят о прямой сумме подгрупп и записывают  $G = A \oplus B$ .

**Теорема 1.20 (критерий прямого произведения).** Группа  $G$  равна прямому произведению своих подгрупп  $A$  и  $B$  тогда и только тогда, когда всякий элемент из  $A$  перестановочен со всяким элементом из  $B$  и всякий элемент  $g \in G$  однозначно представим в виде произведения  $g = ab$ , где  $a \in A, b \in B$ , т.е. если также  $g = a_1b_1, a_1 \in A, b_1 \in B$ , то  $a = a_1, b = b_1$ .

*Доказательство.* ( $\Rightarrow$ ) Пусть  $G = A \times B$ . Для произвольных элементов  $a \in A, b \in B$  рассмотрим элемент  $a^{-1}b^{-1}ab$ . С одной стороны, поскольку  $A \leq G$ , то  $a^{-1}b^{-1}ab = a^{-1} \cdot b^{-1}ab \in A$  (так как  $b^{-1}ab \in A$ ), с другой стороны, так как  $B \leq G$ , то  $a^{-1}b^{-1}ab = a^{-1}b^{-1}a \cdot b \in B$  (поскольку  $a^{-1}b^{-1}a \in B$ ). Следовательно,  $a^{-1}b^{-1}ab \in A \cap B$ . Но по условию 2) из определения 1.20  $A \cap B = \{e\}$ . Следовательно,  $a^{-1}b^{-1}ab = e$ , откуда  $ab = ba$ .

Из доказанного и пункта 3) определения 1.20 следует, что всякий элемент  $g \in G$  представим в виде  $g = ab$ , где  $a \in A, b \in B$ . Пусть  $g = a_1b_1$ . Тогда  $ab = a_1b_1$ , откуда  $a_1^{-1}a = b_1b^{-1}$ . Но по пункту 2) определения 1.20  $A \cap B = \{e\}$ . Следовательно,  $a_1^{-1}a = b_1b^{-1} = e$ , откуда  $a = a_1, b = b_1$ .

( $\Leftarrow$ ) Пусть всякий элемент из подгруппы  $A$  перестановочен со всяким элементом из подгруппы  $B$  и всякий элемент  $g \in G$  однозначно представим в виде произведения  $g = ab$ , где  $a \in A, b \in B$ . Тогда  $A \leq G, B \leq G$  и  $G = \langle A, B \rangle$ . Остается доказать, что  $A \cap B = \{e\}$ . Но предположив, что  $e \neq g \in A \cap B$ , получаем  $g = a \in A$  и  $g = b \in B$ , откуда  $g = a \cdot e = e \cdot b$ , что противоречит единственности представления. Теорема доказана.

Распространим определение прямого произведения на случай произвольного конечного числа подгрупп.

**Определение 1.21.** Группа  $G$  называется *прямым произведением* подгрупп  $H_1, H_2, \dots, H_k$ , если выполнены следующие условия:

1) подгруппа  $H_i \leq G$  для любого  $i = 1, 2, \dots, k$ ;

2) каждая из подгрупп  $H_i$  пересекается с подгруппой, порожденной остальными подгруппами, по единичной подгруппе;

3) группа  $G$  порождается данными подгруппами.

**Упражнение 1.6.** Подобно теореме 1.20 сформулируйте и докажите аналогичный критерий прямого произведения нескольких подгрупп.

Приведем примеры.

1. Мультипликативная группа действительных чисел  $\mathbb{R}^* = A \times B$ , где  $A = \{1, -1\}$ ,  $B = \mathbb{R}^+$  — мультипликативная группа положительных действительных чисел.

2. Напомним, что мультипликативная группа корней  $m$ -й степени из единицы определяется как  $\mathbb{C}_m = \langle \varepsilon \rangle$ , где  $\varepsilon = \cos(2\pi/n) + i \sin(2\pi/n)$ . Имеем:  $\mathbb{C}_6 = \langle \varepsilon^2 \rangle \times \langle \varepsilon^3 \rangle$ .

3. Аддитивная группа целых комплексных чисел  $\mathbb{Z} + \mathbb{Z}i = \mathbb{Z} \oplus \mathbb{Z}i$ .

4. Аддитивная группа рациональных чисел  $\mathbb{Q}$  не разложима в прямую сумму ненулевых подгрупп, так как любые две ее ненулевые подгруппы имеют ненулевое пересечение (докажите!).

### 1.8.2. Разложение циклических групп в прямое произведение своих подгрупп

**Теорема 1.21.** *Бесконечная циклическая группа не представима в виде прямого произведения неединичных подгрупп.*

*Доказательство.* Пусть дана бесконечная циклическая группа  $G = \langle a \rangle$ . Предположим, что  $G = A \times B$ , где  $A = \langle a^n \rangle$ ,  $B = \langle a^k \rangle$  при некоторых натуральных  $n \neq 1$  и  $k \neq 1$ . Пусть  $m$  — наименьшее общее кратное чисел  $n$  и  $k$ . Тогда  $e \neq a^m \in \langle a^n \rangle \cap \langle a^k \rangle$ , что противоречит определению прямого произведения. Теорема доказана.

Обратимся к конечным циклическим группам.

**Теорема 1.22.** *Если группа  $G = \langle g \rangle$  и  $|g| = p^\alpha$ , где  $p$  — простое, то  $G$  не представима в виде прямого произведения неединичных подгрупп.*

*Доказательство.* Предположим противное: пусть  $G = A \times B$ , где  $A = \langle a^n \rangle$ ,  $B = \langle a^k \rangle$  при некоторых  $0 < n < p^\alpha$  и  $0 < k < p^\alpha$ . Представим  $n$  в виде  $n = p^\beta n_1$ , где  $\text{НОД}(n_1, p) = 1$ ,  $0 < \beta < \alpha$ . Тогда  $a^n = a^{p^\beta n_1} \in \langle a^{p^\beta} \rangle$ , следовательно,  $A = \langle a^n \rangle \subseteq \langle a^{p^\beta} \rangle$ . С другой стороны, поскольку  $\text{НОД}(n_1, p^\alpha) = 1$ , то существуют целые числа  $u$  и  $v$ , такие что  $n_1 u + p^\alpha v = 1$ . Отсюда  $a = a^{n_1 u + p^\alpha v} = a^{n_1 u} a^{p^\alpha v} = a^{n_1 u}$ . Но тогда  $a^{n u} = a^{p^\beta n_1 u} = (a^{n_1 u})^{p^\beta} = a^{p^\beta}$ , откуда  $\langle a^{p^\beta} \rangle \subseteq \langle a^n \rangle = A$ . Таким образом,  $A = \langle a^{p^\beta} \rangle$ . Аналогично устанавливаем, что  $B = \langle a^{p^\gamma} \rangle$  при некотором натуральном  $\gamma$ ,  $0 < \gamma < \alpha$ . Но тогда  $A$  и  $B$  являются неединичными подгруппами, из которых одна содержится в другой, что противоречит условию  $A \cap B = \{e\}$ . Теорема доказана.



Наконец, рассмотрим случай, когда порядок конечной циклической группы можно разложить на два взаимно простых числа.

**Теорема 1.23.** Если  $G = \langle g \rangle$  и  $|g| = km$ , где  $k > 1$ ,  $m > 1$ ,  $\text{НОД}(k, m) = 1$ , то  $G = \langle a \rangle \times \langle b \rangle$ , где  $a = g^m$ ,  $b = g^k$  и  $|a| = k$ ,  $|b| = m$ .

*Доказательство.* Обозначим  $a = g^m$ ,  $b = g^k$ . Тогда  $|a| = k$ ,  $|b| = m$ . Легко доказать, что  $\langle a, b \rangle = \langle a \rangle \times \langle b \rangle$ , а так как порядок этой подгруппы равен  $km$ , то  $G = \langle a \rangle \times \langle b \rangle$ . Теорема доказана.

**Следствие.** Если порядок элемента  $g$  группы  $G$  равен  $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , где  $p_1, p_2, \dots, p_k$  — различные простые числа, то существуют элементы  $g_1, g_2, \dots, g_k \in G$ , такие что  $\langle g \rangle = \langle g_1 \rangle \times \langle g_2 \rangle \times \dots \times \langle g_k \rangle$  и  $|g_i| = p_i^{\alpha_i}$  для  $i = 1, 2, \dots, k$ .

*Доказательство.* Обозначим  $k = p_1^{\alpha_1}$ ,  $m = p_2^{\alpha_2} \dots p_k^{\alpha_k}$ . Тогда  $\text{НОД}(k, m) = 1$  и по теореме 1.23  $G = \langle a \rangle \times \langle b \rangle$ , где  $|a| = k$ ,  $|b| = m$ . Теперь повторяем рассуждения для циклической группы  $\langle b \rangle$ . Через конечное число шагов получим искомое разложение.

**Теорема 1.24.** Если группа  $G = \langle a \rangle \times \langle b \rangle$ ,  $|a| = k$ ,  $|b| = m$  и  $\text{НОД}(k, m) = 1$ , то  $G = \langle ab \rangle$ .

*Доказательство.* Включение  $G \supseteq \langle ab \rangle$  очевидно. Покажем обратное включение. Поскольку  $\text{НОД}(k, m) = 1$ , то существуют целые  $u$  и  $v$ , такие что  $ku + mv = 1$ . Отсюда  $a = a^{ku+mv} = a^{ku} a^{mv} = a^{mv} = (ab)^{mv} \in \langle ab \rangle$ . Аналогично  $b = b^{ku+mv} = b^{ku} b^{mv} = b^{ku} = (ab)^{ku} \in \langle ab \rangle$ . Следовательно,  $\langle a \rangle \times \langle b \rangle \subseteq \langle ab \rangle$ , откуда  $G = \langle ab \rangle$ . Теорема доказана.

### 1.8.3. Разложение конечной абелевой группы в прямое произведение циклических подгрупп

**Определение 1.22.** Пусть  $p$  — простое число. Группа  $G$  называется  $p$ -группой, если порядок всякого элемента группы равен некоторой степени простого числа  $p$ .

**Определение 1.23.** Силовской  $p$ -подгруппой конечной группы  $G$  называется такая ее  $p$ -подгруппа, которая не содержится в большей  $p$ -подгруппе данной группы.

**Теорема 1.25.** Конечная абелева группа равна прямому произведению своих силовских  $p$ -подгрупп.

*Доказательство.* Рассмотрим конечную абелеву группу  $G$  порядка  $n$  и пусть  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  — разложение числа  $n$  в произведение степеней различных простых чисел. Для  $i = 1, 2, \dots, k$  обозначим через  $H_i$  силовскую  $p_i$ -подгруппу и через  $\bar{H}_i$  — подгруппу, порожденную всеми  $H_j$  для  $j \neq i$ . Легко доказать, что  $H_i \cap \bar{H}_i = \{e\}$ . Следовательно,  $H = \langle H_1, H_2, \dots, H_k \rangle = H_1 \times H_2 \times \dots \times H_k$ . Предположим, что существует элемент  $g \in G$ , такой что  $g \notin H$ . По следствию 2 из теоремы Лагранжа  $|G| \vdots |g|$ . Отсюда следует, что



$|g| = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ , где  $\beta_i \leq \alpha_i$  для любого  $i = 1, 2, \dots, k$ . По следствию из теоремы 1.23 существуют элементы  $g_1, g_2, \dots, g_k \in G$ , такие что  $\langle g \rangle = \langle g_1 \rangle \times \langle g_2 \rangle \times \dots \times \langle g_k \rangle$  и  $|g_i| = p_i^{\beta_i}$  для  $i = 1, 2, \dots, k$ . Если предположить, что  $g_i \notin H_i$  для некоторого  $i$ , то получаем  $p_i$ -подгруппу  $\langle g_i, H_i \rangle \neq H_i$ , что противоречит определению силовой  $p_i$ -подгруппы. Таким образом, для любого  $i = 1, 2, \dots, k$   $g_i \in H_i$ , откуда  $g \in H$ . Следовательно,  $H = G$  и теорема доказана.

**Теорема 1.26.** Конечная абелева  $p$ -группа равна прямому произведению циклических подгрупп.

*Доказательство.* Пусть дана конечная абелева  $p$ -группа  $G$ . Выберем в ней элемент  $a$  максимального порядка  $p^\alpha$ , и пусть  $H$  — максимальная подгруппа, такая что  $\langle a \rangle \cap H = \langle e \rangle$ . Тогда  $\langle a, H \rangle = \langle a \rangle \times H$ . Обозначим  $G_1 = \langle a \rangle \times H$ .

Предположим, что  $G \neq G_1$ . Из всех элементов, не принадлежащих  $G_1$ , выберем элемент  $g$  минимального порядка  $p^\beta$ . Если предположить, что  $g^p \notin G_1$ , то поскольку  $|g^p| = p^{\beta-1}$ , мы приходим к противоречию с выбором элемента  $g$ . Следовательно,  $g^p \in G_1 = \langle a \rangle \times H$  и существуют целое число  $k$  и элемент  $h \in H$ , такие что  $g^p = a^k h$ . Отсюда  $a^k = g^p h^{-1}$ . Если  $\text{НОД}(k, p) = 1$ , то  $\text{НОД}(k, p^\alpha) = 1$  и существуют целые  $u, v$ , такие что  $ku + p^\alpha v = 1$ . Тогда

$$a = a^{ku+p^\alpha v} = a^{ku} a^{p^\alpha v} = a^{ku} = (g^p h^{-1})^u = g^{pu} h^{-u}.$$

В силу максимальной  $|a| = p^\alpha$  имеем  $g^{p^\alpha} = e$  и  $e \neq a^{p^{\alpha-1}} = (g^{pu} h^{-u})^{p^{\alpha-1}} = g^{p^\alpha u} h^{-up^{\alpha-1}} = h^{-up^{\alpha-1}} \in H$ , что противоречит условию  $\langle a \rangle \cap H = \{e\}$ . Следовательно,  $k : p$ .

Пусть  $k = pk_1$ . Тогда  $a^{pk_1} = a^k = g^p h^{-1}$ , откуда  $h = a^{-pk_1} g^p = (a^{-k_1} g)^p$ . Обозначим  $g_1 = a^{-k_1} g$ . Тогда  $g_1^p = h \in H$ . Если предположить, что  $g_1 = a^{-k_1} g \in G_1 = \langle a \rangle \times H$ , то  $g \in G_1$ , что противоречит выбору элемента  $g$ . Следовательно,  $g_1 \notin G_1$ , а значит,  $g_1 \notin H$ . Поскольку  $H$  — максимальная подгруппа с условием  $\langle a \rangle \cap H = \langle e \rangle$ , то  $\langle a \rangle \cap \langle g_1, H \rangle \neq \{e\}$ . Следовательно, существуют  $m, n \in \mathbb{Z}$  и элемент  $h_1 \in H$ , такие что  $e \neq a^m = g_1^n h_1$ .

Если предположить, что  $n : p$ , то  $n = pn_1$  при некотором  $n_1 \in \mathbb{Z}$  и  $e \neq a^m = g_1^n h_1 = g_1^{pn_1} h_1 \in H$ , что противоречит условию  $\langle a \rangle \cap H = \{e\}$ . Следовательно,  $\text{НОД}(n, p) = 1$  и  $g_1^n = a^m h_1^{-1}$ . Если  $|g_1| = p^\gamma$ , то  $\text{НОД}(n, p^\gamma) = 1$  и существуют  $u_1, v_1 \in \mathbb{Z}$ , такие что  $nu_1 + p^\gamma v_1 = 1$ . Отсюда  $g_1 = g_1^{nu_1+p^\gamma v_1} = g_1^{nu_1} g_1^{p^\gamma v_1} = g_1^{nu_1} = (a^m h_1^{-1})^{u_1} \in \langle a \rangle \times H = G_1$ . Снова пришли к противоречию. Таким образом, остается принять, что  $G = \langle a \rangle \times H$ . Теперь в подгруппе  $H$  аналогично выделяем прямым множителем циклическую подгруппу максималь-

ного в  $H$  порядка и т.д., пока не получим разложение группы  $G$  в прямое произведение циклических подгрупп. Теорема доказана.

**Теорема 1.27.** *Конечная абелева группа равна прямому произведению циклических  $p$ -подгрупп.*

Доказательство вытекает из теорем 1.25 и 1.26.

В заключение главы о группах отметим, что группу можно рассматривать как множество с одной бинарной операцией, которая ассоциативна, и для любых элементов  $a$  и  $b$  однозначно разрешимы уравнения  $ax = b$  и  $ya = b$ . Этот взгляд на группу приводит к двум обобщениям. С одной стороны, можно сосредоточиться на изучении значения ассоциативности операции, и это приводит к понятию полугруппы как множества с одной ассоциативной операцией (см. работу [14]). С другой стороны, можно игнорировать требование ассоциативности, и это приводит к понятию квазигруппы как множества с одной бинарной операцией, относительно которой однозначно разрешимы названные уравнения. Квазигруппа с единицей называется лупой (см. работу [2]). Теория полугрупп и теория квазигрупп превратились в две самостоятельно развивающиеся содержательные теории. Мы о них не упоминаем в основном тексте из соображений «максимально возможной минимальности» объема.

## Контрольные вопросы

1. Представимы ли в виде прямого произведения (прямой суммы) своих неединичных (ненулевых) подгрупп следующие группы:  $S_3$ ,  $\mathbb{Z}$ ,  $\mathbb{Z}_6$ ,  $\mathbb{C}$ , группа простого порядка, группа параллельных переносов плоскости?
2. Известно, что  $G = \langle a \rangle$  и  $|a| = p^n$ . Как изображаются на диаграмме Эйлера группа  $G$  и две ее собственные подгруппы?
3. Сохраняется ли представимость группы в виде прямого произведения двух подгрупп при изоморфизме групп? А при гомоморфизме?
4. Верно ли, что если группа представима в виде прямого произведения трех подгрупп, то она представима в виде прямого произведения двух подгрупп?
5. В каком случае прямое произведение двух циклических подгрупп является циклической группой?

## Задачи

1. Найдите разложения в произведение циклических подгрупп абелевых групп порядков 3, 4, 6, 8, 9, 12, 15, 16, 30.

2. Докажите, что если в абелевой группе  $G$  порядок всякого неединичного элемента равен  $n$ , то  $n$  — простое число и  $G$  представима в виде прямого произведения циклических групп одного и того же простого порядка.

3. Найдите разложение в прямую сумму циклических подгрупп для групп  $\mathbb{Z} + \mathbb{Z}\sqrt{3}$  и  $\mathbb{Z} + \mathbb{Z}i$ .

4. Докажите, что аддитивная группа  $\mathbb{Q}$  не представима в виде прямой суммы двух ненулевых подгрупп.

5. Представьте мультипликативную группу  $\mathbb{Q}^*$  в виде прямого произведения двух неединичных подгрупп.

# Глава 2

## КОЛЬЦА И ПОЛЯ

### 2.1. Определение и основные свойства колец

#### 2.1.1. Определение и примеры колец

Перейдем к рассмотрению множеств с двумя бинарными операциями. В качестве «образца для подражания» выберем множество целых чисел  $\mathbb{Z}$  с операциями сложения и умножения и множество всех квадратных матриц  $M_n(\mathbb{Z})$  порядка  $n$  с целочисленными элементами относительно сложения и умножения матриц. Введем общее понятие, частными случаями которого будут упомянутые примеры.

**Определение 2.1.** *Кольцом* называется алгебраическая система  $\langle K, +, \cdot \rangle$  с основным множеством  $K$  и бинарными операциями сложения и умножения, которая удовлетворяет следующим условиям.

1. Свойства сложения.

1.1. Сложение коммутативно и ассоциативно:  $a + b = b + a$ ,  $(a + b) + c = a + (b + c)$  для любых  $a, b, c \in K$ .

1.2. Существует элемент  $0 \in K$ , называемый нулем, такой что  $0 + a = a$  для любого  $a \in K$ .

1.3. Для любого  $a \in K$  существует элемент  $-a \in K$ , называемый противоположным для  $a$ , такой что  $a + (-a) = 0$ .

2. Умножение ассоциативно:  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  для любых  $a, b, c \in K$ .

3. Умножение дистрибутивно относительно сложения:  $a \cdot (b + c) = a \cdot b + a \cdot c$  и  $(b + c) \cdot a = b \cdot a + c \cdot a$  для любых  $a, b, c \in K$ .

Если умножение в кольце коммутативно, то кольцо называется коммутативным.

Обычно кольцо называют кратко, по имени основного множества  $K$ .

Термин «кольцо» был введен Д. Гильбертом (1862—1943).

Определение кольца можно сделать более кратким, если использовать понятие группы.

**Определение 2.2.** *Кольцом* называется множество  $K$  с двумя бинарными операциями — сложением и умножением, если  $K$  относительно сложения образует коммутативную группу, которая называется *аддитивной группой кольца*, умножение ассоциативно и дистрибутивно относительно сложения.

**Определение 2.3.** *Единицей* кольца  $K$  называется такой элемент  $e \in K$ , что для любого элемента  $a \in K$   $ae = ea = a$ . Элемент  $a \neq 0$  кольца  $K$  с единицей  $e$  называется *обратимым*, если существует элемент  $b \in K$ , такой что  $ab = ba = e$ . Элемент  $b$  называется *обратным* к  $a$  и обозначается  $b = a^{-1}$ . Элементы  $c$  и  $d$  кольца  $K$  называются *делителями нуля*, если  $c \neq 0$ ,  $d \neq 0$ , но  $cd = 0$ .

Легко видеть, что множество всех обратимых элементов кольца  $K$  с единицей относительно умножения образует группу, которая называется *мультипликативной группой кольца* и обозначается  $K^*$ .

Приведем примеры колец.

1. Числовые кольца: кольцо целых чисел  $\mathbb{Z}$ ; кольцо четных целых чисел  $2\mathbb{Z}$ ;  $m\mathbb{Z}$  — кольцо целых чисел, кратных  $m$ ; нулевое кольцо  $\{0\}$ , состоящее из одного нуля. Кольцо целых комплексных (гауссовых) чисел  $\mathbb{Z} + \mathbb{Z}i = \{a + bi \mid a, b \in \mathbb{Z}\}$ .

2.  $\mathbb{Z}_m$  — кольцо классов вычетов по модулю  $m$ . Его аддитивная и мультипликативная группы рассмотрены в подпараграфах 1.5.3 и 1.5.4.

3. Матричные кольца:  $M_n(K)$  — кольцо квадратных матриц порядка  $n$  над кольцом  $K$  (элементы матриц принадлежат кольцу  $K$ );  $T_n(K)$  — кольцо *треугольных* квадратных матриц порядка  $n$  над кольцом  $K$  (множество всех матриц, у которых ниже главной диагонали стоят нули);  $D_n(K)$  — кольцо *диагональных* квадратных матриц порядка  $n$  над кольцом  $K$  (в таких матрицах вне главной диагонали стоят нули);  $C_n(K)$  — кольцо *скалярных* квадратных матриц порядка  $n$  над кольцом  $K$  (диагональная матрица называется *скалярной*, если у нее все диагональные элементы равны).

4.  $K[x]$  — кольцо многочленов над кольцом  $K$  (т.е. с коэффициентами из  $K$ ); при  $K = \mathbb{Z}$  получаем кольцо многочленов с целыми коэффициентами  $\mathbb{Z}[x]$ , а при  $K = \mathbb{Q}$  получаем кольцо многочленов с рациональными коэффициентами  $\mathbb{Q}[x]$ .  $K[x_1, \dots, x_n]$  — кольцо многочленов от переменных  $x_1, \dots, x_n$  над кольцом  $K$ .

5. Любую аддитивную группу  $K$  можно превратить в кольцо, если задать на ней нулевое умножение:  $a \cdot b = 0$  для любых  $a, b \in K$ .

**Упражнение 2.1.** Среди приведенных примеров колец найдите: 1) кольца без единицы; 2) некоммутативные кольца; 3) кольца, содержащие делители нуля.

### 2.1.2. Основные свойства колец

Прежде всего отметим, что для аддитивной группы кольца  $K$  справедливы все свойства аддитивных групп. Рассмотрим свойства колец, связанные с умножением.

1. (Свойство нуля). Для любого элемента  $a$  кольца  $K$   $a \cdot 0 = 0 \cdot a = 0$ .

*Доказательство.*  $a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0 \Rightarrow a \cdot 0 = a \cdot 0 + a \cdot 0$ . Прибавив к обеим частям этого равенства по  $-(a \cdot 0)$ , получим  $0 = a \cdot 0$ . Подобным же образом доказывается, что  $0 \cdot a = 0$ .

2. (Правила знаков). Для любых элементов  $a$  и  $b$  кольца  $K$  имеют место равенства  $(-a)b = a(-b) = -(ab)$ ,  $(-a)(-b) = ab$ .

*Доказательство.* Имеем:  $ab + (-a)b = (a + (-a))b = 0 \cdot b = 0 \Rightarrow (-a)b = -(ab)$ ; аналогично доказывается, что  $a(-b) = -(ab)$ . Используя доказанное, получаем  $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$ .

**Определение 2.4.** Вычитанием в кольце  $K$  называется бинарная операция « $-$ », которая задается формулой  $a - b = a + (-b)$  для любых  $a, b \in K$ .

3. Умножение в кольце дистрибутивно относительно вычитания:  $(a - b)c = ac - bc$  и  $c(a - b) = ca - cb$  для любых  $a, b \in K$ .

*Доказательство.* Пользуясь определением вычитания, дистрибутивностью умножения относительно сложения и правилами знаков, получаем  $(a - b)c = (a + (-b))c = ac + (-b)c = ac + (-(bc)) = ac - bc$ . Аналогично доказывается второе равенство.

## Контрольные вопросы

1. Обязано ли быть коммутативным кольцо  $K$ , если в нем выполняется равенство  $a^2 - b^2 = (a + b)(a - b)$  для любых  $a, b \in K$ ?

2. Существуют ли кольца, в которых равенство  $a^2 - b^2 = (a + b) \times (a - b)$  не является тождеством?

3. Существуют ли кольца, в которых  $ac = bc$  и  $c \neq 0$ , но  $a \neq b$ ?

4. Существуют ли кольца, в которых  $a \neq 0$ ,  $b \neq 0$ , но  $ab = 0$ ?

5. Если кольцо содержит натуральные числа, то будет ли оно содержать все целые числа? Обязано ли оно содержать все рациональные числа?

## Задачи

Среди данных множеств, рассматриваемых относительно сложения и умножения, укажите кольца. Отметьте коммутативность или некоммутативность кольца, наличие или отсутствие делителей нуля, делителей единицы.

1.  $5\mathbb{Z}, 6\mathbb{Z}, 7\mathbb{Z}$ .
2.  $\mathbb{Z}_5, \mathbb{Z}_6, \mathbb{Z}_7$ .
3.  $A_1 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ .
4.  $A_2 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ .
5.  $A_3 = \{a + b\sqrt{2} \mid a, b \in \mathbb{R}\}$ .
6.  $A_4 = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}$ .
7.  $A_5 = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ .
8.  $A_6 = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{R}\}$ .
9.  $A_7 = \mathbb{Z} + \mathbb{Z}i = \{a + bi \mid a, b \in \mathbb{Z}\}$  (множество целых комплексных чисел).
10.  $A_8 = \mathbb{Q} + \mathbb{Q}i = \{a + bi \mid a, b \in \mathbb{Q}\}$ .
11. Множества многочленов  $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$  относительно их сложения и умножения.
12. Множества многочленов  $\mathbb{Z}[x_1, x_2], \mathbb{Q}[x_1, x_2], \mathbb{R}[x_1, x_2], \mathbb{C}[x_1, x_2]$ .
13.  $A_9$  — множество всех многочленов кольца  $K[x]$  с нулевым свободным членом.
14.  $A_{10} = \left\{ a + b \frac{-1 + i\sqrt{19}}{2} \mid a, b \in \mathbb{Z} \right\}$ .
15.  $A_{11} = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ .
16. Множество матриц вида  $\begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}$ , где  $a \in \mathbb{Q}$ .
17. Множество матриц вида  $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ , где  $a, b \in \mathbb{R}$ .
18. Множество матриц вида  $\begin{pmatrix} a & 3b \\ b & a \end{pmatrix}$ , где  $a, b \in \mathbb{Q}$ .
19.  $F_1 = \{a + b\sqrt{2} + c\sqrt{3} \mid a, b, c \in \mathbb{Q}\}$ .
20.  $F_2 = \{a + b\sqrt[3]{2} + b\sqrt[3]{4} \mid a, b, c \in \mathbb{N}\}$ .

## 2.2. Определение и основные свойства полей

### 2.2.1. Определение поля, примеры

Начнем с определения поля как «хорошего» в некотором смысле кольца.



**Определение 2.5.** *Поле* называется коммутативное кольцо с единицей, отличной от нуля, в котором для каждого ненулевого элемента существует обратный элемент.

Теперь определим поле без использования понятия кольца.

**Определение 2.6.** *Поле* называется алгебраическая система  $\langle P, +, \cdot \rangle$  с основным множеством  $P$ , на котором определены бинарные операции сложения и умножения, причем выполняются следующие условия.

1. Свойства сложения.

1.1. Сложение ассоциативно и коммутативно:  $(a + b) + c = a + (b + c)$  и  $a + b = b + a$  для любых  $a, b, c \in P$ .

1.2. Существует элемент  $0 \in P$ , называемый нулем, такой что  $0 + a = a$  для любого  $a \in P$ .

1.3. Для любого  $a \in P$  существует элемент  $-a \in P$ , называемый противоположным для  $a$ , такой что  $a + (-a) = 0$ .

2. Свойства умножения.

2.1. Умножение ассоциативно и коммутативно:  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  и  $a \cdot b = b \cdot a$  для любых  $a, b, c \in P$ .

2.2. Существует элемент  $1 \in P$ , называемый единицей, такой что  $1 \neq 0$  и  $1 \cdot a = a$  для любого  $a \in P$ .

2.3. Для любого элемента  $a \in P$ , отличного от нуля, существует элемент  $a^{-1} \in P$ , называемый обратным для  $a$ , такой что  $a \cdot a^{-1} = 1$ .

3. Умножение дистрибутивно относительно сложения:  $a \cdot (b + c) = a \cdot b + a \cdot c$  для любых  $a, b, c \in P$ .

Наконец, сформулируем более краткое определение, использующее понятие группы.

**Определение 2.7.** *Поле* называется алгебраическая система  $\langle P, +, \cdot \rangle$  с основным множеством  $P$ , на котором определены бинарные операции сложения и умножения, причем система  $\langle P, + \rangle$  является коммутативной группой, которая называется аддитивной группой поля, система  $\langle P^*, \cdot \rangle$ , где  $P^* = P \setminus \{0\}$  (множество элементов, отличных от нуля) также является коммутативной группой, которая называется мультипликативной группой поля, и умножение дистрибутивно относительно сложения.

Приведем примеры полей.

1. Числовые поля.

1.1. Множество всех рациональных чисел  $\mathbb{Q}$  относительно сложения и умножения (поле рациональных чисел).

1.2. Множество всех действительных чисел  $\mathbb{R}$  относительно сложения и умножения (поле действительных чисел).

1.3. Множество  $P = \mathbb{Q} + \mathbb{Q}\sqrt{p} = \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\}$ , где  $p$  — простое число.

1.4. Отрицательный пример: кольцо целых чисел не является полем, поскольку в нем, например, для числа 2 нет обратного, так как не существует такого целого числа  $b$ , для которого  $2b = 1$ .

**Упражнение 2.2.** Докажите, что числовые множества, перечисленные в примерах 1.1., 1.2, 1.3, относительно операций сложения и умножения являются полями.

2. Примером конечного поля является поле классов вычетов  $\mathbb{Z}_p$  по простому модулю  $p$ . Например,  $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ .

**Упражнение 2.3.** Составьте таблицы сложения и умножения элементов поля  $\mathbb{Z}_3$ , найдите аддитивные порядки всех элементов и мультипликативные порядки элементов, отличных от нуля. Рассмотрите по этой же схеме поля  $\mathbb{Z}_2$  и  $\mathbb{Z}_5$ .

3. Кольцо  $M_n(\mathbb{R})$  всех квадратных матриц порядка  $n \geq 2$  над полем  $\mathbb{R}$  относительно сложения и умножения матриц не является полем, хотя бы потому что оно не коммутативно.

**Упражнение 2.4.** Докажите, что полями являются следующие кольца матриц:

а) матрицы вида  $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ , где  $a, b \in \mathbb{R}$ ; б) матрицы вида  $\begin{pmatrix} a & b \\ 3b & a \end{pmatrix}$ , где  $a, b \in \mathbb{Q}$ .

### Исторический экскурс

Термин «поле» впервые появился в книге П. Дирихле (1805—1859) «Теория чисел», в примечаниях и дополнениях, написанных Р. Дедекиндом (1831—1916). Первоначально Дедекинд пользовался термином «рациональная область», что отражает замкнутость поля относительно «рациональных операций»: сложения, вычитания, умножения и деления.

### 2.2.2. Основные свойства полей

Прежде всего отметим, что для аддитивной и мультипликативной групп поля  $P$  выполняются доказанные ранее свойства групп. Отсюда следуют единственность в поле нуля 0 и единицы 1, для любого  $a \in P$  единственность противоположного элемента  $-a$  и если  $a \neq 0$ , то единственность обратного элемента  $a^{-1}$ . Далее, поскольку всякое поле является кольцом, то все свойства колец имеют место и для полей. В частности, в поле можно рассматривать операцию вычитания.

Перейдем к рассмотрению специфических свойств полей, выделяющих их среди колец.

1. Для элементов  $a$  и  $b$  поля  $P$  если  $ab = 0$ , то  $a = 0$  или  $b = 0$ . Другими словами, в поле нет делителей нуля.

*Доказательство.* Если  $a = 0$ , то доказывать нечего. Предположим, что  $a \neq 0$ . Тогда существует  $a^{-1} \in P$ . Умножив равенство  $ab = 0$  на  $a^{-1}$ , получим  $b = 0$ .

2 (свойство сократимости). В поле если  $ac = bc$  и  $c \neq 0$ , то  $a = b$ .

*Доказательство.* Поскольку  $c \neq 0$ , то существует  $c^{-1}$ . Умножив равенство  $ac = bc$  на  $c^{-1}$ , получим  $a = b$ .

**Определение 2.8.** Для любых элементов  $a$  и  $b \neq 0$  поля  $P$  произведение  $ab^{-1}$  называется *отношением* этих элементов, или *дробью*, и записывается в виде  $\frac{a}{b}$ . При этом  $a$  называется

числителем, а  $b$  — знаменателем дроби. Сопоставление всякой упорядоченной паре элементов  $(a, b)$  элемента  $ab^{-1}$  называется *делением*. При этом пишут:  $a : b = ab^{-1}$ . Легко видеть, что на множестве  $P^*$  всех элементов поля, отличных от нуля, деление является бинарной операцией.

Подчеркнем, что знаменатель дроби не равен нулю.

3. Свойства дробей.

3.1 (условие равенства дробей).  $\frac{a}{b} = \frac{c}{d}$  тогда и только тогда, когда  $ad = bc$ .

*Доказательство.* Пользуясь определением дроби, получаем

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ab^{-1} = cd^{-1} \Leftrightarrow ab^{-1} \cdot bd = cd^{-1} \cdot bd \Leftrightarrow ad = bc.$$

3.2 (основное свойство дроби).  $\frac{ac}{bc} = \frac{a}{b}$ .

3.3 (правило сложения дробей).  $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$ .

*Доказательство.*

$$\begin{aligned} \frac{a}{b} \pm \frac{c}{d} &= ab^{-1} \pm cd^{-1} = (ad \pm bc) \cdot b^{-1}d^{-1} = \\ &= (ad \pm bc) \cdot (b \cdot d)^{-1} = \frac{ad \pm bc}{bd}. \end{aligned}$$

3.4 (правило умножения дробей).  $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ .

|| **Упражнение 2.5.** Докажите самостоятельно свойства 3.2 и 3.4.

## Контрольные вопросы

1. Кольца находятся среди полей или поля среди колец?
2. Если поле содержит натуральные числа, то обязано ли оно содержать все рациональные числа?
3. Может ли поле содержать только один элемент?
4. Может ли поле содержать некоммутативное кольцо?
5. Может ли мультипликативная группа бесконечного поля содержать конечную подгруппу?
6. Во всяком ли поле имеет место тождество  $a^2 - b^2 = (a + b)(a - b)$ ?

## Задачи

1. Среди множеств, указанных в задачах к параграфу 2.1, укажите примеры полей.
2. В поле  $\mathbb{Z}_7$  решите уравнения  $\bar{2} \cdot x = \bar{3}$ ,  $\bar{3} \cdot x = \bar{3}$ ,  $\bar{3} \cdot x = \bar{2}$ ,  $\bar{5} \cdot x^2 - \bar{2} = \bar{0}$ . Решите эти же уравнения в полях  $\mathbb{Z}_5$  и  $\mathbb{Z}_{17}$ .
3. Докажите, что конечное коммутативное кольцо с единицей, отличной от нуля, и без делителей нуля является полем.
4. Выясните, может ли мультипликативная группа числового поля быть циклической.
5. Опишите порядки элементов аддитивной и мультипликативной групп поля рациональных чисел.
6. Найдите порядки элементов аддитивной и мультипликативной групп поля  $\mathbb{Z}_7$ .

## 2.3. Подполя, подкольца, идеалы

Аналогами подгрупп в группах являются подкольца и подполя в кольцах и полях.

**Определение 2.9.** Подмножество  $H$  кольца  $K$  (поля  $P$ ) называется *подкольцом* (соответственно *подполем*), если оно само является кольцом (полем) относительно сужения на  $H$  операций сложения и умножения, определенных в  $K$  (соответственно в  $P$ ).

Подкольцо (подполе) называется *собственным*, если оно не совпадает с самим кольцом (полем).

Используя критерий подгруппы, получаем критерии подкольца и подполя.

**Теорема 2.1 (критерий подкольца).** Подмножество  $H$  кольца  $K$  является подкольцом тогда и только тогда, когда выполнены следующие условия:

- 1) подмножество  $H$  замкнуто относительно операций сложения и умножения, т.е. если  $a, b \in H$ , то  $a + b \in H$  и  $a \cdot b \in H$ ;

2)  $H$  содержит нуль данного кольца  $K$ ;

3) если  $a \in H$ , то противоположный элемент  $-a \in H$ .

**Теорема 2.2 (критерий подполя).** Подмножество  $P$  поля  $F$  является подполем тогда и только тогда, когда выполнены следующие условия:

1) подмножество  $P$  замкнуто относительно операций сложения и умножения: если  $a, b \in P$ , то  $a + b \in P$  и  $a \cdot b \in P$ ;

2)  $P$  содержит нуль и единицу данного поля  $F$ ;

3) если  $a \in P$ , то противоположный элемент  $-a \in P$ , и если  $a \neq 0$ , то  $a^{-1} \in P$ .

Примеры.

1. Кольцо целых чисел  $\mathbb{Z}$  является подкольцом кольца (поля) рациональных чисел  $\mathbb{Q}$ . Поле  $\mathbb{Q}$  является подполем поля действительных чисел  $\mathbb{R}$ , а оно в свою очередь является подполем поля комплексных чисел  $\mathbb{C}$ .

2. Кольцо  $K = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$  содержит подкольцо  $\mathbb{Z}$ , а поле  $P = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$  содержит подполе  $\mathbb{Q}$ .

**Упражнение 2.6.** Есть ли в поле  $P = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$  другие подполя, кроме  $\mathbb{Q}$ ?

Легко доказать, что пересечение двух и более подколец (подполей) является подкольцом (соответственно подполем). «Самым большим» подкольцом (подполем) является само кольцо (поле). «Самым маленьким» подкольцом является нулевое подкольцо, состоящее из одного нулевого элемента данного кольца. Вид «самого маленького» подполя будет выяснен позже. Числовым кольцом (полем) называется всякое подкольцо (подполе) поля комплексных чисел.

В кольце целых чисел подкольцо четных целых чисел  $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$  замкнуто не только относительно сложения, но и относительно умножения на любое целое число. Рассмотрим в произвольном кольце подмножества с такими же свойствами.

**Определение 2.10.** Подкольцо  $H$  кольца  $K$  называется идеалом, если оно замкнуто относительно умножения на любой элемент из  $K$ , т.е. для любого  $x \in H$  и любого  $k \in K$  произведения  $kx, xk \in H$ .

**Определение 2.11.** Пусть дано коммутативное кольцо  $K$  и  $a_1, a_2, \dots, a_n \in K$ . Подмножество  $\{k_1a_1 + k_2a_2 + \dots + k_na_n \mid k_1, k_2, \dots, k_n \in K\}$  является, очевидно, идеалом в  $K$ , который называется идеалом, порожденным элементами  $a_1, a_2, \dots, a_n$ , и обозначается  $\langle a_1, a_2, \dots, a_n \rangle$ . В частности, идеал  $\langle a \rangle = \{ka \mid k \in K\}$  называется главным.

Рассмотрим примеры.

1. В произвольном кольце нулевое подкольцо есть нулевой идеал:  $\langle 0 \rangle = \{0\}$ . Само кольцо  $K$  также является идеалом. Если кольцо  $K$  содержит единицу 1, то  $K = \langle 1 \rangle$ , поскольку из единицы «можно сделать» любой элемент кольца:  $a = a \cdot 1$ . Этот идеал называется единичным.

2. Докажем, что всякий идеал поля либо нулевой, либо единичный.

Пусть  $H$  — идеал поля  $P$  и  $0 \neq a \in H$ . Тогда существует элемент  $a^{-1}$  и ввиду замкнутости  $H$  относительно умножения на любой элемент поля  $P$  имеем  $e = a \cdot a^{-1} \in H$ . Но тогда для любого  $x \in P$  получаем  $x = x \cdot e \in H$ . Следовательно,  $H = P$ .

Заметим, что всякий идеал в кольце является подкольцом. Обратное неверно. Например, кольцо целых чисел в поле рациональных чисел является подкольцом, но не идеалом.

Легко доказать, что пересечение двух идеалов есть идеал.

Идеал кольца — это в некотором смысле «идеальное подкольцо», т.е. такое подкольцо, которое замкнуто относительно умножения на любой элемент кольца. Ниже мы покажем, что идеалы в кольцах играют ту же роль, что и нормальные подгруппы в группах.

## Контрольные вопросы

1. Может ли поле содержать подмножество, являющееся кольцом, но не полем?
2. Может ли кольцо содержать подмножество, которое является полем?
3. Содержит ли поле комплексных чисел конечные подполя?
4. Содержится ли поле  $\mathbb{Z}_3$  в поле  $\mathbb{Z}_5$ ?
5. Содержится ли кольцо  $\mathbb{Z}_9$  в кольце  $\mathbb{Z}_{10}$ ?

## Задачи

1. Для множеств, указанных в задачах к параграфу 2.1, являющихся кольцами и полями, найдите в них примеры подколец, подполей и идеалов.
2. Перечислите все идеалы в кольцах  $\mathbb{Z}_5$  и  $\mathbb{Z}_6$ .
3. Докажите, что пересечение двух подколец есть подкольцо, пересечение двух подполей есть подполе и пересечение двух идеалов есть идеал.
4. В кольцах многочленов  $\mathbb{Z}[x]$  и  $\mathbb{Q}[x]$  найдите подкольца, которые не являются идеалами.



5. В поле комплексных чисел найдите все подполя, содержащие поле действительных чисел.
6. В поле  $P = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$  найдите все подполя, содержащие  $\mathbb{Q}$ .

## 2.4. Изоморфизмы и гомоморфизмы колец и полей

Введем для колец понятия, аналогичные изоморфизмам и гомоморфизмам групп.

**Определение 2.12.** Гомоморфизмом кольца  $\langle K, +, \cdot \rangle$  на кольцо  $\langle K_1, \oplus, \circ \rangle$  называется отображение  $f$  множества  $K$  на множество  $K_1$ , сохраняющее операции сложения и умножения, т.е. для любых  $a, b \in K$  имеют место равенства  $f(a + b) = f(a) \oplus f(b)$  и  $f(a \cdot b) = f(a) \circ f(b)$ . При этом кольцо  $\langle K_1, \oplus, \circ \rangle$  называется гомоморфным образом кольца  $\langle K, +, \cdot \rangle$ . Если гомоморфизм  $f$  является взаимно однозначным отображением, то он называется изоморфизмом кольца  $\langle K, +, \cdot \rangle$  на кольцо  $\langle K_1, \oplus, \circ \rangle$ .

Легко доказываются следующие свойства гомоморфизмов.

1. Гомоморфным образом кольца с единицей является кольцо с единицей.

2. Гомоморфный образ поля есть поле.

Кольца и поля изучаются с точностью до изоморфизма. Изоморфные кольца (поля) считаются «одинаковыми».

**Определение 2.13.** Ядром гомоморфизма  $\varphi$  кольца  $\langle K, +, \cdot \rangle$  на кольцо  $\langle K_1, \oplus, \circ \rangle$  называется множество всех прообразов нуля  $0_1 \in K_1$ .

Обозначение ядра  $\ker \varphi$ . Таким образом,  $\ker \varphi = \{x \in K \mid \varphi(x) = 0_1\}$ .

Легко доказать, что  $H = \ker \varphi$  есть идеал. Понятно, что  $H$  является подгруппой аддитивной группы кольца. Рассмотрим факторгруппу  $K/H$  и определим умножение смежных классов по формуле  $(a + H) \cdot (b + H) = ab + H$ . Получим кольцо, которое называется факторкольцом кольца  $K$  по идеалу  $H$ . Как и в случае групп, имеет место следующая теорема о гомоморфизмах для колец.

**Теорема 2.3.** Гомоморфный образ кольца изоморфен факторкольцу по ядру гомоморфизма.

Доказательство этой теоремы аналогично доказательству соответствующей теоремы для групп.

Рассмотрим два важных приложения этой теоремы: в теории чисел и в теории многочленов. Легко проверяется, что отображение  $\varphi$  кольца целых чисел  $\mathbb{Z}$  на кольцо классов вычетов  $\mathbb{Z}_m$  по модулю  $m$ , при котором для любого  $a \in \mathbb{Z}$   $\varphi(a) = \bar{a} \in \mathbb{Z}_m$



является гомоморфизмом с ядром  $\ker \varphi = \langle m \rangle = m\mathbb{Z}$ . По теореме о гомоморфизмах кольцо классов вычетов  $\mathbb{Z}_m$  изоморфно факторкольцу:  $\mathbb{Z}_m \cong \mathbb{Z}/\langle m \rangle$ .

В качестве второго приложения теоремы о гомоморфизмах докажем, что поле комплексных чисел  $\mathbb{C}$  изоморфно факторкольцу  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ . Для всякого многочлена  $f(x) \in \mathbb{R}[x]$  определим  $\varphi(f(x)) = f(i)$ . Легко видеть, что  $\varphi$  является отображением кольца многочленов  $\mathbb{R}[x]$  на поле комплексных чисел  $\mathbb{C}$ . Обозначим  $H = \langle x^2 + 1 \rangle$  и докажем, что этот идеал является ядром гомоморфизма  $\varphi$ . Для любого многочлена  $(x^2 + 1) \cdot q(x) \in H$  имеем  $\varphi((x^2 + 1) \cdot q(x)) = (i^2 + 1)q(i) = 0$ . Следовательно,  $H \subseteq \ker \varphi$ .

Обратно, пусть  $f(x) \in \ker \varphi$ , тогда  $\varphi(f(x)) = 0$ . Разделим  $f(x)$  на многочлен  $x^2 + 1$  с остатком. Пусть  $f(x) = (x^2 + 1) \cdot q(x) + r(x)$ , где остаток  $r(x)$  есть либо нулевой многочлен, либо его степень меньше степени делителя  $x^2 + 1$ . Пусть  $r(x) = ax + b$  при некоторых  $a, b \in \mathbb{R}$ . Тогда  $\varphi(f(x)) = (i^2 + 1) \cdot q(i) + (a + bi) = a + bi = 0$ . Следовательно,  $a = 0$  и  $b = 0$ , откуда  $r(x) = 0$  и  $f(x) = (x^2 + 1) \cdot q(x) \in \langle x^2 + 1 \rangle = H$ . Таким образом,  $\ker \varphi = H$ . По теореме о гомоморфизмах гомоморфный образ кольца  $\mathbb{R}[x]$ , т.е.  $\varphi(\mathbb{R}[x]) = \mathbb{C}$ , изоморфен факторкольцу кольца  $\mathbb{R}[x]$  по ядру гомоморфизма  $H = \langle x^2 + 1 \rangle$ , т.е.  $\mathbb{C}$  изоморфно факторкольцу  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ . Утверждение доказано.

Поскольку всякое поле является кольцом, то можно рассмотреть гомоморфизм  $\varphi$  поля  $P$  на поле  $P_1$ . Пусть  $H = \ker \varphi$ . Тогда  $H$  является идеалом, а значит, либо нулевым, либо единичным. Если  $H = \{0\}$  — нулевой идеал, то  $\varphi$  является изоморфизмом. Если же  $H$  — единичный идеал, то  $H = \langle 1 \rangle = P$ . Следовательно, всякий элемент поля  $P$  отображается в нуль поля  $P_1$ . Таким образом,  $\varphi$  является либо изоморфизмом, либо нулевым гомоморфизмом. Так что гомоморфизмы полей не представляют особого интереса.

## Контрольные вопросы

1. Изоморфны ли кольцо целых чисел и кольцо четных целых чисел?
2. Изоморфны ли кольца  $3\mathbb{Z}$  и  $5\mathbb{Z}$ ?
3. Может ли кольцо быть изоморфно полю?
4. Если кольцо  $K$  изоморфно (гомоморфно) кольцу  $K_1$ , то каково соотношение между количествами элементов  $|K|$  и  $|K_1|$ ?
5. Как связаны количества прообразов различных элементов при гомоморфизме одного кольца на другое?

## Задачи

- Докажите, что изоморфны следующие алгебраические системы:
  - поле рациональных чисел  $\langle \mathbb{Q}, +, \cdot \rangle$  (кольцо  $\langle \mathbb{Z}, +, \cdot \rangle$ ) и поле (кольцо) матриц вида  $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ , где  $a \in \mathbb{Q}$  (соответственно  $a \in \mathbb{Z}$ );
  - поле комплексных чисел и поле матриц вида  $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ , где  $a, b \in \mathbb{R}$ ;
  - поле (кольцо) чисел вида  $a + b\sqrt{3}$ , где  $a, b \in \mathbb{Q}$  (соответственно,  $a, b \in \mathbb{Z}$ ) и поле (кольцо) матриц вида  $\begin{pmatrix} a & b \\ 3b & a \end{pmatrix}$ .
- Докажите, что поле рациональных чисел не изоморфно полю чисел вида  $a + b\sqrt{3}$ , где  $a, b \in \mathbb{Q}$ .
- Докажите, что изоморфное отображение поля рациональных чисел на себя является тождественным отображением (всякий элемент отображается в себя).
- Выясните, может ли поле быть гомоморфным кольцу, которое не является полем.

## 2.5. Характеристика кольца и поля

Если в кольце единицы может и не быть, то в поле ее наличие гарантировано определением поля. Что можно извлечь из существования единицы? Вспомним, что в кольце целых чисел сумма любого количества единиц отлична от нуля, а в кольце классов вычетов  $\mathbb{Z}_4$  сумма четырех единиц равна нулю:  $\bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{4} = \bar{0}$ . Введем понятия, характеризующие эти ситуации.

**Определение 2.14.** Пусть кольцо  $K$  содержит единицу  $e$ . Если для любого натурального числа  $n$  сумма  $n$  единиц  $ne \neq 0$ , то будем говорить, что кольцо  $K$  имеет *характеристику 0*. Если же некоторая сумма единиц равна нулю, то *характеристикой* кольца  $K$  назовем наименьшее натуральное число  $n$ , такое, что  $ne = 0$ .

Поскольку поле — это «хорошее» кольцо, то данное определение относится и к полям: существуют поля характеристики 0 и характеристики, отличной от нуля.

**Лемма 2.1.** Ненулевая характеристика поля является простым числом.

*Доказательство.* Пусть  $n$  — ненулевая характеристика поля  $P$  с единицей  $e$ . Если предположить, что  $n = km$ , где  $0 < k < n$ , то  $0 < m < n$  и  $kme = ne = 0$ , откуда  $ke \cdot me = 0$ . Так как в поле нет

делителей нуля, то  $ke = 0$  или  $te = 0$ . Но то и другое противоречит минимальности числа  $n$  — пришли к противоречию. Следовательно,  $n$  — простое число. Лемма доказана.

Подобным образом можно доказать более общее утверждение: *ненулевая характеристика кольца с единицей без делителей нуля является простым числом.*

На языке теории групп характеристика кольца с единицей — это порядок единицы  $e$  в аддитивной группе кольца.

**Теорема 2.4.** *Если поле  $P$  имеет ненулевую характеристику  $p$  (нулевую характеристику), то порядок всякого ненулевого элемента аддитивной группы поля  $P$  равен  $p$  (соответственно бесконечен).*

*Доказательство.* Пусть  $0 \neq a \in P$  и  $e$  — единица поля  $P$ . Если характеристика поля  $P$  равна простому числу  $p$ , то

$$pa = \underbrace{a + a + \dots + a}_p = \underbrace{ea + ea + \dots + ea}_p = \underbrace{(e + e + \dots + e)}_p a = pe \cdot a = 0 \cdot a = 0.$$

Следовательно, аддитивный порядок элемента  $a$  равен  $p$ .

Пусть данное поле имеет характеристику 0. Предположим, что  $na = 0$  при некотором натуральном  $n$ . Тогда  $ne \cdot a = 0$ , а так как  $a \neq 0$ , то  $ne = 0$ , что противоречит условию. Теорема доказана.

Из свойств аддитивных порядков элементов поля вытекает следующее следствие.

**Следствие 1.** Если  $P$  — поле характеристики  $p$ , то для любого  $a \in P$  и натурального числа  $n$  имеем  $na = 0$  тогда и только тогда, когда  $n \vdots p$ .

**Следствие 2.** В поле  $P$  характеристики  $p$  для любых  $a, b \in P$  имеют место равенства  $(a + b)^p = a^p + b^p$  и  $(a - b)^p = a^p - b^p$ .

*Доказательство.* Пусть поле  $P$  имеет характеристику  $p$ . Пользуясь формулой бинома Ньютона, для любых элементов  $a, b \in P$  получаем

$$\begin{aligned} (a + b)^p &= a^p + pa^{p-1}b + \frac{p(p-1)}{2!}a^{p-2}b^2 + \dots + \\ &+ \frac{p(p-1)}{2!}a^2b^{p-2} + pab^{p-1} + b^p. \end{aligned}$$

В числитель каждого коэффициента, кроме первого и последнего, входит несократимое  $p$ . Поэтому каждый из этих коэффициентов является целым числом, кратным  $p$ . По теореме 2.4 в поле  $P$  характеристики  $p$  для любого  $a \in P$  имеем  $pa = 0$ . Следовательно, правая часть равенства равна  $a^p + b^p$ .

Второе равенство доказывается аналогично. Следствие доказано.

**Теорема 2.5.** *Всякое поле характеристики 0 содержит подполе, изоморфное полю рациональных чисел, а всякое поле характеристики  $p$  содержит подполе, изоморфное полю классов вычетов по простому модулю  $p$ .*

*Доказательство.* 1. Пусть поле  $P$  имеет характеристику 0 и пусть  $e$  — единица поля. Рассмотрим подмножество  $H = \left\{ \frac{me}{ne} \mid m, n \in \mathbb{Z}, n \neq 0 \right\}$ . Легко видеть, что  $H$  является подполем данного поля. Вспомним, что поле рациональных чисел  $\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \right\}$ . Нетрудно доказать, что отображение  $f: H \rightarrow \mathbb{Q}$  по правилу  $f\left(\frac{me}{ne}\right) = \frac{m}{n}$  является искомым изоморфизмом подполя  $H$  на поле рациональных чисел  $\mathbb{Q}$ .

2. Пусть теперь поле  $P$  имеет характеристику  $p$  и по-прежнему  $e$  обозначает единицу поля. Рассмотрим подмножество  $H = \{me \mid m \in \mathbb{Z}\}$ . Очевидно,  $H$  замкнуто относительно сложения, вычитания и умножения. Докажем замкнутость  $H$  относительно деления. Для этого достаточно доказать, что если  $ne \neq 0$ , то обратный элемент  $(ne)^{-1} \in H$ , т.е. имеет вид  $ke$  при некотором целом  $k$ . Поскольку характеристика поля равна простому числу  $p$ , то  $ne \neq 0$  тогда и только тогда, когда  $\text{НОД}(n, p) = 1$ . Последнее равносильно существованию целых чисел  $u$  и  $v$ , таких что  $pu + nv = 1$ . Отсюда  $(nu - 1) : p$ , откуда последовательно получаем  $(nu - 1)e = 0$ ,  $nue - e = 0$ ,  $ne \cdot ue = e$ ,  $(ne)^{-1} = ue \in H$ . Таким образом,  $H$  является подполем данного поля  $P$ . В то же время легко доказать, что отображение  $f: H \rightarrow \mathbb{Z}_p$  по правилу  $f(ne) = \bar{n}$  является искомым изоморфизмом подполя  $H$  на поле классов вычетов  $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \bar{p-1}\}$ . Теорема доказана.

Таким образом, в поле характеристики 0 «самым маленьким» подполем является подполе, изоморфное полю рациональных чисел, а в поле характеристики  $p$  «самым маленьким» подполем является подполе, изоморфное полю классов вычетов по простому модулю  $p$ .

**Определение 2.15.** Поле называется *простым*, если оно не содержит подполей, отличных от него самого.

**Следствие 3.** *Простое поле характеристики 0 изоморфно полю рациональных чисел, а простое поле характеристики  $p$  — полю классов вычетов по простому модулю  $p$ .*

|| **Упражнение 2.7.** Докажите утверждение следствия 3.

## Контрольные вопросы

1. Может ли подполе иметь характеристику, отличную от характеристики поля?
2. Существует ли поле характеристики 6?
3. Может ли поле характеристики 0 содержать элемент, аддитивный порядок которого конечен?
4. Чему равен порядок всякого ненулевого элемента аддитивной группы поля характеристики 3?
5. Может ли аддитивная группа поля содержать элемент порядка 15?
6. Чему равна характеристика числового поля?
7. Могут ли быть изоморфными поля разной характеристики?

## Задачи

1. Найдите характеристики всех полей, рассмотренных ранее в данной главе.
2. Укажите характеристики всех полей, содержащих не более 20 элементов.
3. Найдите аддитивный порядок каждого элемента простого поля характеристики  $p = 2, 3, 5$ .
4. При каком натуральном  $n$  в поле  $P$  характеристики  $p$  для элемента  $a \in P$  имеет место равенство  $na = 0$ ?
5. При каких натуральных  $n$  в поле  $P$  характеристики  $p$  для любых элементов  $a, b \in P$  имеет место равенство  $(a + b)^n = a^n + b^n$ ?
6. В кольце многочленов над простым полем характеристики 2 выпишите все квадратные уравнения и решите их.
7. В кольце многочленов над простым полем характеристики 3 приведите пример двух многочленов и найдите их НОД и НОК.

# Глава 3

## ДЕЛИМОСТЬ В КОЛЬЦАХ

### 3.1. Основные понятия теории делимости в области целостности

#### 3.1.1. Область целостности

Вспомним, что в поле  $P$ , если  $a \neq 0$  и  $b \neq 0$ , то  $ab \neq 0$ . А вот в кольце классов вычетов  $K = \mathbb{Z}_6$  имеем  $\bar{2} \neq \bar{0}$ ,  $\bar{3} \neq \bar{0}$ , но  $\bar{2} \cdot \bar{3} = \bar{0}$ .

Таким образом, в любом поле нет делителей нуля, а в кольце  $K = \mathbb{Z}_6$  классы вычетов  $\bar{2}$  и  $\bar{3}$  являются делителями нуля.

**Определение 3.1.** Областью целостности называется коммутативное кольцо с единицей, отличной от нуля, и без делителей нуля.

Кольцо целых чисел  $\mathbb{Z}$  является областью целостности. Кольцо  $\mathbb{Z} + \mathbb{Z}i = \{a + bi \mid a, b \in \mathbb{Z}\}$  целых комплексных (гауссовых) чисел также является областью целостности. Всякое поле есть область целостности. Если  $K$  — область целостности, то кольцо многочленов  $K[x]$  также является областью целостности. Не является областью целостности, например, кольцо четных целых чисел, поскольку оно не содержит единицы. Не является областью целостности кольцо квадратных матриц порядка  $n > 1$ , поскольку оно не коммутативно. Заметим, что нулевое кольцо — это единственное кольцо, в котором нуль равен единице. Оно не является областью целостности.

Кольцо  $\mathbb{Z}_m$  классов вычетов по модулю  $m$  является областью целостности тогда и только тогда, когда  $m = p$  — простое число. В этом случае кольцо  $\mathbb{Z}_p$  является полем.

Докажем основное свойство области целостности, выделяющее ее среди колец.

**Свойство сократимости.** Для любых элементов  $a, b$  и  $c \neq 0$  области целостности  $K$  если  $ac = bc$  или  $ca = cb$ , то  $a = b$ .

**Доказательство.** Пусть  $ac = bc$ . Тогда  $ac - bc = 0$ , откуда  $(a - b)c = 0$ , а так как  $c \neq 0$  и в области целостности нет дели-

телей нуля, то  $a - b = 0$ , откуда  $a = b$ . Аналогично доказывается, что из равенства  $ca = cb$  следует  $a = b$ . Свойство доказано.

Подобно тому как, пополняя целые числа дробями, мы получаем поле рациональных чисел, можно произвольную область целостности вложить в поле отношений. Докажем это.

**Теорема 3.1 (о вложении области целостности в поле).**  
*Всякая область целостности изоморфна подкольцу некоторого поля.*

*Доказательство.* Пусть дана область целостности  $K$ . Для любых элементов  $a, b \in K$ , где  $b \neq 0$ , рассмотрим упорядоченную пару  $(a, b)$ . Для двух таких пар определим  $(a, b) \sim (a_1, b_1) \Leftrightarrow ab_1 = ba_1$ . Легко видеть, что это отношение рефлексивно, симметрично и транзитивно, а значит, является отношением эквивалентности. По этому отношению множество всех упорядоченных пар  $\{(a, b) \mid a, b \in K, b \neq 0\}$  распадается на классы эквивалентных пар. Обозначим через  $\frac{a}{b}$  и назовем дробью класс пар, эквивалентных паре  $(a, b)$ . Множество всех дробей (классов эквивалентных пар) обозначим через  $P$ . Две дроби  $\frac{a}{b}$  и  $\frac{a_1}{b_1}$  будем называть равными и писать  $\frac{a}{b} = \frac{a_1}{b_1}$ , если  $(a, b) \sim (a_1, b_1)$ . Таким образом,  $\frac{a}{b} = \frac{a_1}{b_1} \Leftrightarrow ab_1 = ba_1$ .

Определим на  $P$  операции сложения и умножения, положив  $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$ ,  $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ . Легко доказать, что если  $\frac{a}{b} = \frac{a_1}{b_1}$ ,  $\frac{c}{d} = \frac{c_1}{d_1}$ , то  $\frac{a}{b} + \frac{c}{d} = \frac{a_1}{b_1} + \frac{c_1}{d_1}$  и  $\frac{a}{b} \cdot \frac{c}{d} = \frac{a_1}{b_1} \cdot \frac{c_1}{d_1}$ . Проверкой устанавливаем, что система  $\langle P, +, \cdot \rangle$  является полем, а отображение  $f: a \rightarrow \frac{a}{1}$  для всех  $a \in K$  является изоморфизмом области целостности  $K$  на подкольцо  $K_1 = \left\{ \frac{a}{1} \mid a \in K \right\}$ . Теорема доказана.

Построенное в доказательстве теоремы поле  $\langle P, +, \cdot \rangle$  называется *полем отношений* области целостности  $K$ .

### 3.1.2. Определение и основные свойства делимости

Единицу области целостности  $K$  будем обозначать 1. Целое число 6 делится на целое число 2 потому, что существует целое число 3, такое что  $6 = 2 \cdot 3$ . Отталкиваясь от этого примера,



дадим общее определение понятию делимости в произвольной области целостности.

**Определение 3.2.** Пусть  $K$  — область целостности и  $a, b \in K$ . Будем говорить, что элемент  $a$  *делится* на элемент  $b$ , и писать  $a : b$ , если существует элемент  $q \in K$ , такой что  $a = bq$ . При этом  $b$  называется *делителем* элемента  $a$  и  $a$  называется *кратным*  $b$ .

Легко доказать, что отношение «делится» на области целостности  $K$  рефлексивно ( $a : a$ ) и транзитивно (если  $a : b$  и  $b : c$ , то  $a : c$ ). Из делимости слагаемых на элемент  $d$  вытекает делимость суммы на  $d$ .

Обратим внимание на то, что  $0 : 0$ , и если  $a : 0$ , то  $a = 0$ . Вместе с тем в соответствии с определением 3.1 элемент 0 не является делителем нуля.

Рассмотрим *примеры*.

1. В кольце целых чисел делителями числа 2 являются 1,  $-1$ , 2 и  $-2$ .

2. В кольце  $\mathbb{Z} + \mathbb{Z}i$  имеем  $2 = (1 + i)(1 - i)$ . Очевидно,  $2 : \pm 1, \pm i, \pm(1 + i), \pm(1 - i), \pm 2, \pm 2i$ .

Докажем, что других делителей нет. Пусть  $\alpha = a + bi$  при целых  $a$  и  $b$  является делителем числа 2. Тогда  $2 = \alpha \cdot \beta$  при некотором  $\beta \in \mathbb{Z} + \mathbb{Z}i$ . Но тогда  $2^2 = |\alpha|^2 \cdot |\beta|^2$ . Таким образом, целое число  $|\alpha|^2 = a^2 + b^2$  является делителем числа 4, т.е. совпадает с одним из чисел 1, 2, 4. Если  $a^2 + b^2 = 1$ , то либо  $a = \pm 1, b = 0$ , либо  $a = 0, b = \pm 1$ , откуда либо  $\alpha = \pm 1$ , либо  $\alpha = \pm i$ . Если  $a^2 + b^2 = 4$ , то либо  $a = \pm 2, b = 0$ , либо  $a = 0, b = \pm 2$ , откуда либо  $\alpha = \pm 2$ , либо  $\alpha = \pm 2i$ . Если же  $a^2 + b^2 = 2$ , то либо  $\alpha = \pm(1 + i)$ , либо  $\alpha = \pm(1 - i)$ .

**Упражнение 3.1.** Докажите, что  $3 : \pm 1, \pm i, \pm 3, \pm 3i$  и других делителей нет.

Множество всех делителей единицы (обратимых элементов) области целостности  $K$  относительно умножения образует группу, которая называется *мультипликативной группой* области целостности и обозначается  $K^*$ .

Рассмотрим *примеры*.

1. Группа делителей единицы в кольце целых чисел есть  $\mathbb{Z}^* = \{1, -1\}$ .

2. Докажем, что группа делителей единицы в кольце целых комплексных чисел есть  $(\mathbb{Z} + \mathbb{Z}i)^* = \{1, -1, i, -i\}$ . Поскольку  $1 = 1 \cdot 1 = (-1) \cdot (-1) = i \cdot (-i)$ , то числа  $\pm 1$  и  $\pm i$  являются делителями единицы. Докажем, что других нет. Пусть  $\varepsilon$  — делитель единицы. Тогда существует  $\alpha \in \mathbb{Z} + \mathbb{Z}i$ , такое что  $1 = \varepsilon\alpha$ . Отсюда получаем  $1 = |\varepsilon\alpha|^2 = |\varepsilon|^2 \cdot |\alpha|^2$  и  $|\varepsilon|^2 = 1$ . Пусть  $\varepsilon = x + yi$ ,  $x, y$

$\in \mathbb{Z}$ . Тогда  $x^2 + y^2 = 1$ , откуда либо  $x^2 = 1, y = 0$ , либо  $x = 0, y^2 = 1$ . Следовательно, либо  $\varepsilon = \pm 1$ , либо  $\varepsilon = \pm i$ .

3. Группа делителей единицы в произвольном поле  $P$  состоит из всех элементов поля, отличных от нуля, и совпадает с мультипликативной группой поля  $P^* = P \setminus \{0\}$ . В частности,  $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ .

4. Группа делителей единицы в кольце многочленов  $(\mathbb{Z}[x])^* = \mathbb{Z}^* = \{1, -1\}$ . В кольце многочленов  $\mathbb{Q}[x]$  группа делителей единицы  $(\mathbb{Q}[x])^* = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ . В кольце многочленов  $K[x]$  над областью целостности  $K$  группа делителей единицы совпадает с группой делителей единицы  $K^*$ . В частности, в кольце многочленов  $P[x]$  над полем  $P$  группа делителей единицы (обратимых элементов) есть  $(P[x])^* = P^* = P \setminus \{0\}$ .

**Определение 3.3.** Пусть  $K$  — область целостности и  $a, b \in K$ . Элемент  $a$  называется ассоциированным с элементом  $b$ , если существует делитель единицы  $\varepsilon \in K$ , такой что  $a = \varepsilon b$ .

Легко доказать, что отношение ассоциированности элементов является отношением эквивалентности на области целостности  $K$ , т.е. оно рефлексивно, симметрично и транзитивно. В силу этого если элементы  $a$  и  $b$  ассоциированы, то будем писать  $a \sim b$ . По этому отношению множество  $K$  распадается на непересекающиеся классы ассоциированных элементов. Класс элементов, ассоциированных с элементом  $a$ , будем обозначать  $K_a$ .

**Лемма 3.1 (критерий ассоциированности элементов).** В области целостности  $K$  элементы  $a$  и  $b$  ассоциированы тогда и только тогда, когда  $a : b$  и  $b : a$ .

*Доказательство.* ( $\Rightarrow$ ) Пусть  $a \sim b$ . По определению, это означает существование делителя единицы  $\varepsilon \in K^*$ , такого что  $a = \varepsilon b$ . Отсюда следует, что  $a : b$ . Но  $b = \varepsilon^{-1}a$ , откуда  $b : a$ .

( $\Leftarrow$ ) Пусть  $a : b$  и  $b : a$ . Если предположить, что  $a = 0$ , то из условия  $b : a$  следует, что  $b = 0$ . Следовательно,  $a \sim b$ . При  $a \neq 0$  имеем

$$\left. \begin{array}{l} a : b \Rightarrow a = bq, q \in K \\ b : a \Rightarrow b = aq_1, q_1 \in K \end{array} \right| \Rightarrow a = aq_1q \Rightarrow 1 = q_1q.$$

Следовательно,  $q$  является делителем единицы и из равенства  $a = bq$  заключаем, что  $a \sim b$ . Лемма доказана.

**Примеры.**

1. В кольце целых чисел  $\mathbb{Z}$  класс элементов, ассоциированных с числом 2, состоит из чисел  $K_2 = \{2, -2\}$ . Аналогично  $K_3 = \{3, -3\}$ ,  $K_{-5} = \{5, -5\}$ ,  $K_1 = \{1, -1\}$ ,  $K_0 = \{0\}$ .

2. В кольце целых комплексных чисел  $K_2 = \{2, -2, 2i, -2i\}$ ,  $K_1 = \{1, -1, i, -i\}$ ,  $K_{1+i} = \{1+i, -1-i, -1+i, 1-i\}$ .

3. В поле  $P$  лишь два класса ассоциированных элементов:  $K_0 = \{0\}$  и  $K_1 = P^*$ .

4. В кольце многочленов  $\mathbb{Z}[x]$  имеем классы ассоциированных элементов  $K_2 = \{2, -2\}$ ,  $K_{2x^2+3} = \{2x^2 + 3, -2x^2 - 3\}$ . В кольце многочленов  $P[x]$  над полем  $P$  классы ассоциированных элементов  $K_0 = \{0\}$ ,  $K_1 = P^*$ ,  $K_x = \{ax \mid a \in P^*\}$ ,  $K_{f(x)} = \{a \cdot f(x) \mid a \in P^*\}$ ,  $f(x) \in P[x]$ .

### 3.1.3. Наибольший общий делитель

Обобщим известное понятие НОД двух целых чисел для элементов произвольной области целостности.

**Определение 3.4.** Пусть дана область целостности  $K$  и  $a, b \in K$ . Элемент  $d \in K$  называется *общим делителем* элементов  $a$  и  $b$ , если оба элемента делятся на  $d$ . *Наибольшим общим делителем* элементов  $a$  и  $b$  называется такой их общий делитель, который делится на любой другой их общий делитель. Обозначение:  $\text{НОД}(a, b)$ .

**Лемма 3.2.** Если  $\text{НОД}(a, b) = d$ , то  $\text{НОД}(a, b) = d_1$  тогда и только тогда, когда  $d$  и  $d_1$  ассоциированы.

*Доказательство.* ( $\Rightarrow$ ) Пусть  $\text{НОД}(a, b) = d$  и  $\text{НОД}(a, b) = d_1$ . Поскольку  $d_1$  — общий делитель, а  $d$  — наибольший общий делитель элементов  $a$  и  $b$ , то  $d : d_1$ . Аналогично рассуждая, получаем  $d_1 : d$ . Следовательно, по лемме 3.1  $d$  и  $d_1$  ассоциированы.

( $\Leftarrow$ ) Пусть  $\text{НОД}(a, b) = d$  и  $d_1 \sim d$ . По определению ассоциированности  $d_1 = \varepsilon d$ , где  $\varepsilon$  — делитель единицы. Легко доказать, что  $d_1$  является общим делителем элементов  $a$  и  $b$ , который делится на любой другой их общий делитель. Следовательно,  $\text{НОД}(a, b) = d_1$ . Лемма доказана.

Таким образом,  $\text{НОД}(a, b)$  представляет собой класс ассоциированных элементов и запись  $\text{НОД}(a, b) = d$  обозначает, что  $d$  есть один из наибольших общих делителей, а все остальные с ним ассоциированы.

Рассмотрим *примеры*.

1. В кольце целых чисел  $\text{НОД}(2, 3) = \pm 1$ ,  $\text{НОД}(6, 15) = \pm 3$ ,  $\text{НОД}(0, 3) = \pm 3$ ,  $\text{НОД}(0, 0) = 0$ .

2. В поле рациональных чисел  $\text{НОД}(2, 3) = \mathbb{Q}^*$ .

3. В кольце целых комплексных чисел  $\mathbb{Z} + \mathbb{Z}i$  найдем  $\text{НОД}(2, 3)$ . Выше найдены все делители числа 2. Выбирая из них делители числа 3, заключаем, что  $\text{НОД}(2, 3) = \{1, -1, i, -i\}$ .

4. В кольце многочленов  $\mathbb{Z}[x]$  имеем:  $\text{НОД}(2, 3) = \pm 1$ ,  $\text{НОД}(2x, 3) = \pm 1$ ,  $\text{НОД}(x^4 - 1, x^6 + 1) = \pm(x^2 + 1)$ .

5. В кольце многочленов  $P[x]$  над полем  $P$  наибольший общий делитель находится с точностью до ненулевого эле-

мента поля  $P$ . Точнее, если  $d(x)$  является одним из наибольших общих делителей многочленов  $f(x), g(x) \in P[x]$ , то  $\text{НОД}(f(x), g(x)) = \{k \cdot d(x) \mid k \in P^*\}$ . Например, в кольце многочленов  $\mathbb{Q}[x]$  имеем  $\text{НОД}(x^4 - 1, x^6 + 1) = k(x^2 + 1)$  для любого  $k \in \mathbb{Q}^*$ .

## Контрольные вопросы

1. Какие подкольца кольца целых чисел являются областями целостности?
2. Верно ли, что всякая числовая область целостности содержит кольцо целых чисел?
3. Если в кольце умножение обладает свойством сократимости, то будет ли оно областью целостности?
4. Если кольцо содержится в поле, то будет ли оно областью целостности?
5. Существует ли поле, содержащее область целостности, которая не является полем?
6. Всегда ли группа обратимых элементов кольца вместе с нулем образует поле?
7. Какие элементы ассоциированы с числом 3 в областях целостности  $\mathbb{Z}, \mathbb{Z} + \mathbb{Z}i, \mathbb{Z}[x], \mathbb{Q}[x]$ ?
8. Сколько делителей имеет единица во множестве  $\mathbb{N}$ , в областях целостности  $\mathbb{Z}, \mathbb{Z} + \mathbb{Z}i, \mathbb{Z}[x]$ ?

## Задачи

1. Среди множеств, являющихся кольцами, из задач параграфа 2.1 найдите примеры областей целостности. Найдите в них делители единицы. Укажите классы ассоциированных элементов.
2. В кольце многочленов  $\mathbb{Q}[x]$  найдите два многочлена, имеющих данный наибольший общий делитель  $d(x)$ : а)  $d(x) = x - 5$ ; б)  $d(x) = x^2 + x - 5$ .
3. Совпадает ли кольцо целых комплексных чисел с объединением классов ассоциированных элементов  $K_n$  по всем  $n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ ?
4. В кольцах  $\mathbb{Z}[x]$  и  $\mathbb{Q}[x]$  найдите многочлены, ассоциированные с многочленом  $x^2 + x + 1$ .
5. Пусть натуральное число  $d$  свободно от квадратов (т.е. не делится на квадрат простого числа) и пусть

$$\omega = \begin{cases} i\sqrt{d}, & \text{если } d = 4n+1 \text{ или } 4n+2, \\ \frac{1+i\sqrt{d}}{2}, & \text{если } d = 4n+3. \end{cases}$$

Докажите, что множество  $\mathbb{Z} + \mathbb{Z}\omega = \{a + b\omega \mid a, b \in \mathbb{Z}\}$  является областью целостности. Каковы в ней делители единицы?

## 3.2. Факториальные кольца

### 3.2.1. Простые элементы области целостности

Известны два способа нахождения наибольшего общего делителя (НОД) двух натуральных чисел: с помощью разложения чисел на простые множители и с помощью алгоритма Евклида. Анализ этих двух способов, попытка переноса их на более общие ситуации приводят к понятиям факториальных и евклидовых колец.

Первый способ нахождения НОД основан на следующей теореме.

**Теорема 3.2 (основная теорема арифметики).** *Всякое натуральное число, отличное от единицы, либо является простым, либо представимо в виде произведения простых натуральных чисел, причем однозначно, если не обращать внимания на порядок следования сомножителей.*

Например,  $6 = 2 \cdot 3$  — разложение составного числа 6 на простые натуральные числа 2 и 3. В натуральных числах есть еще одна возможность:  $6 = 3 \cdot 2$ . В кольце целых чисел к этим разложениям присоединяются  $6 = (-3) \cdot (-2)$  и  $6 = (-2) \cdot (-3)$ , где сомножители  $-2$  и  $-3$  являются простыми целыми числами. Все эти разложения считаются «одинаковыми». Сомножители любых двух разложений можно так сопоставить друг другу, что соответствующие простые множители окажутся ассоциированными. Для обобщения этой ситуации введем необходимые понятия. Начнем с определения понятия простого элемента области целостности.

**Определение 3.5.** Элемент  $p$  области целостности  $K$  называется *простым*, если он отличен от нуля, не является делителем единицы и не представим в виде произведения элементов, отличных от делителей единицы. Элемент  $a \neq 0$  из  $K$  называется *составным*, если он представим в виде произведения элементов, отличных от делителей единицы.

Таким образом, область целостности состоит из нуля, делителей единицы, а остальные элементы подразделяются на простые и составные.

Рассмотрим *примеры*.

1. В кольце целых чисел простыми будут  $\pm 2, \pm 3, \pm 5, \pm 7, \dots$ .
2. В кольце целых комплексных чисел число 2 уже не является простым:  $2 = (1 + i)(1 - i)$ . Докажем, что число  $1 + i$  является простым. Пусть  $1 + i = d \cdot q$ . Тогда  $2 = |1 + i|^2 = |d|^2 |q|^2$ . Поскольку  $|d|^2$  и  $|q|^2$  — натуральные числа, то либо  $|d|^2 = 1$ ,

либо  $|q|^2 = 1$ . Пусть  $|d|^2 = 1$  и  $d = a + bi$ . Тогда  $a^2 + b^2 = 1$ , откуда  $a = \pm 1$ ,  $b = 0$  или  $a = 0$ ,  $b = \pm 1$ . Значит,  $d = \pm 1$  или  $d = \pm i$ , т.е.  $d$  является делителем единицы. Если же  $|q|^2 = 1$ , то  $q$  является делителем единицы. Таким образом, хотя бы одно из чисел  $d$  или  $q$  является делителем единицы, и это доказывает простоту числа  $1 + i$ . Аналогично можно доказать простоту числа  $1 - i$ .

Подобным образом доказывается простота числа 3. А вот  $5 = (2 + i)(2 - i)$ , следовательно, 5 является составным числом.

Известно, что простое натуральное число  $p$  является простым в кольце целых комплексных чисел тогда и только тогда, когда оно имеет вид  $4n + 3$ , где  $n$  — целое неотрицательное число. Целое комплексное число  $\alpha = a + bi$  при  $a \neq 0$  и  $b \neq 0$  является простым в  $\mathbb{Z} + \mathbb{Z}i$  тогда и только тогда, когда  $a^2 + b^2$  — простое натуральное число вида  $4n + 1$  или 2. Доказательства этих фактов нетривиальны, используют теорию чисел, поэтому мы их не приводим.

3. В кольце многочленов  $P[x]$  над полем  $P$  простыми элементами являются в точности неприводимые над полем  $P$  многочлены. Напомним, что многочлен  $f(x)$  называется неприводимым над полем  $P$ , если его степень  $\geq 1$  и он не представим в виде произведения многочленов степени  $\geq 1$ .

4. Простые элементы кольца многочленов  $\mathbb{Z}[x]$  исчерпываются простыми целыми числами и неприводимыми над полем  $\mathbb{Q}$  примитивными многочленами. Напомним, что примитивным называется многочлен с целыми коэффициентами, у которого наибольший общий делитель всех коэффициентов равен единице.

5. В поле нет ни простых, ни составных элементов.

Отметим два свойства простых элементов области целостности.

1. *Делители простого элемента  $p$  исчерпываются делителями единицы  $\varepsilon$  и элементами  $\varepsilon p$ .*

*Доказательство.* Очевидно, делитель единицы  $\varepsilon$  и элемент  $\varepsilon p$  являются делителями  $p$ . Пусть  $p$  — простой элемент области целостности  $K$  и  $d$  — его делитель в  $K$ . Тогда  $p = d \cdot q$ , где  $q \in K$ . По определению простого элемента, либо  $d$ , либо  $q$  должны являться делителями единицы. Но если  $q$  — делитель единицы, то элемент  $\varepsilon = q^{-1}$  является делителем единицы и  $d = \varepsilon p$ .

2. *Если  $p$  и  $q$  — простые элементы области целостности  $K$  и  $p \mid q$ , то  $q = \varepsilon p$ , где  $\varepsilon$  — делитель единицы.*

*Доказательство.* По определению простого элемента,  $q$  не может быть делителем единицы. Поскольку  $q$  является дели-



телем простого элемента  $p$ , то по предыдущему свойству  $q = \varepsilon p$ , где  $\varepsilon$  — делитель единицы.

### 3.2.2. Определение факториального кольца и примеры разложений на простые множители

**Определение 3.6.** Будем говорить, что в области целостности  $K$  элемент  $a$  однозначно разложим на простые множители, если существуют простые элементы  $p_1, p_2, \dots, p_k \in K$ , такие что  $a = p_1 p_2 \cdot \dots \cdot p_k$ , и если имеем еще одно разложение данного элемента на простые множители  $a = q_1 q_2 \cdot \dots \cdot q_m$ , то  $k = m$  и при подходящей нумерации  $q_i = \varepsilon_i p_i$ , где  $\varepsilon_i$  — делители единицы,  $i = 1, \dots, k$ . Другими словами, соответствующие простые множители ассоциированы.

**Определение 3.7.** Факториальным кольцом называется область целостности  $K$ , в которой всякий ненулевой элемент, не являющийся делителем единицы, однозначно разложим на простые множители.

Образно говоря, кольцо факториально, если в нем имеет место аналог основной теоремы арифметики.

Рассмотрим *примеры разложений* на простые множители в кольце целых комплексных чисел  $\mathbb{Z} + \mathbb{Z}i$ .

$$1. -360i = -i \cdot 2^3 \cdot 3^2 \cdot 5 = -i \cdot (1+i)^3(1-i)^3 \cdot 3^2 \cdot (1+2i)(1-2i).$$

2.  $\alpha = 5 - 8i$ . Находим  $|\alpha|^2 = |5 - 8i|^2 = 5^2 + 8^2 = 89$  — простое число, и если предположить, что  $\alpha = \beta\gamma$ , где  $\beta, \gamma \in \mathbb{Z} + \mathbb{Z}i$ , то  $89 = |\alpha|^2 = |\beta|^2 \cdot |\gamma|^2$ , откуда либо  $|\beta|^2 = 1$ , либо  $|\gamma|^2 = 1$ , а значит, одно из чисел  $\beta$  или  $\gamma$  является делителем единицы. Это доказывает простоту числа  $\alpha$  (впрочем, как отмечалось выше, простота числа  $\alpha$  вытекает из того, что  $|\alpha|^2$  есть простое число вида  $4n + 1$ ).

$$3. \alpha = 7 + 9i. \text{ Находим}$$

$$\begin{aligned} |7 + 9i|^2 &= (7 + 9i)(7 - 9i) = 7^2 + 9^2 = 130 = 2 \cdot 5 \cdot 13 = \\ &= (1 + i)(1 - i)(1 + 2i)(1 - 2i)(2 + 3i)(2 - 3i). \end{aligned}$$

Теперь путем испытаний выбираем из этого разложения простые множители данного числа  $7 + 9i$ :

$$\begin{aligned} \frac{7+9i}{1+i} &= \frac{(7+9i)(1-i)}{1^2+1^2} = \frac{16+2i}{2} = 8+i; \\ \frac{8+i}{1+2i} &= \frac{(8+i)(1-2i)}{1^2+2^2} = \frac{10-15i}{5} = 2-3i. \end{aligned}$$

$$\text{Следовательно, } 7 + 9i = (1 + i)(1 + 2i)(2 - 3i).$$



Рассмотрим другую последовательность испытаний:

$$\frac{7+9i}{1-i} = \frac{(7+9i)(1+i)}{1^2+1^2} = \frac{-2+16i}{2} = -1+8i;$$

$$\frac{-1+8i}{1+2i} = \frac{(-1+8i)(1-2i)}{1^2+2^2} = \frac{15+10i}{5} = 3+2i.$$

Следовательно,  $7+9i = (1-i)(1+2i)(3+2i)$ . Сравнивая это разложение с первоначальным, видим, что  $1+i = i(1-i)$ ,  $2-3i = (-i)(3+2i)$ , т.е. соответствующие множители отличаются лишь на делители единицы, а значит, ассоциированы.

Заметим, что попытка выбрать множитель  $1-2i$  заканчивается неудачей:  $\frac{7+9i}{1-2i} = \frac{(7+9i)(1+2i)}{1^2+2^2} = \frac{-11+23i}{5}$  — нецелое комплексное число.

Рассмотренные примеры подсказывают следующую *стратегию разложения* целого комплексного числа  $\alpha = a+bi$  на простые множители.

1. Находим  $\text{НОД}(a, b) = d$  и представляем  $\alpha$  в виде  $\alpha = d(a_1 + b_1i)$ , где  $\text{НОД}(a_1, b_1) = 1$ .

2. Находим разложение числа  $d$  на простые множители в  $\mathbb{Z}$ . Простые множители этого разложения вида  $4n+3$  являются простыми в  $\mathbb{Z} + \mathbb{Z}i$ . Если в разложении есть простое число  $p=2$  или  $p=4n+1$ , то представляем его в виде суммы двух квадратов:  $p=x^2+y^2$ , а затем раскладываем на простые в  $\mathbb{Z} + \mathbb{Z}i$  множители:  $p=(x+yi)(x-yi)$ .

3. Если  $a_1 \neq 0$  и  $b_1 \neq 0$ , то находим разложение числа  $a_1 + b_1i$  на простые множители в  $\mathbb{Z} + \mathbb{Z}i$ . Для этого вычисляем  $a_1^2 + b_1^2$  и полученное число раскладываем на простые множители в  $\mathbb{Z} + \mathbb{Z}i$  (как в примере 2). Затем из полученного разложения выбираем путем испытаний простые множители числа  $a_1 + b_1i$ .

4. Соединяя результаты п. 2 и 3, записываем ответ.

**Пример.** Разложим число  $\alpha = 1309 + 357i$  на простые множители в  $\mathbb{Z} + \mathbb{Z}i$ .

*Решение.* 1. Находим  $\text{НОД}(1309, 357) = 119$ . Таким образом,  $\alpha = 119(11 + 3i)$ .

2. Находим разложение числа 119 на простые множители сначала в  $\mathbb{Z}$ , а потом и в  $\mathbb{Z} + \mathbb{Z}i$ :  $119 = 7 \cdot 17 = 7 \cdot (1+4i)(1-4i)$ .

3. Находим разложение на простые множители числа  $\beta = 11 + 3i$ . Имеем  $|\beta|^2 = |11 + 3i|^2 = 11^2 + 3^2 = 130$ . Выше было установлено, что  $130 = (1+i)(1-i)(1+2i)(1-2i)(2+3i)(2-3i)$ .

Выполним последовательное деление:

$$\frac{11+3i}{1+i} = \frac{(11+3i)(1-i)}{1^2+1^2} = \frac{14-8i}{2} = 7-4i;$$

$$\frac{7-4i}{1+2i} = \frac{(7-4i)(1-2i)}{1^2+2^2} = \frac{-1-18i}{5} \text{ — нецелое комплексное число;}$$

$$\frac{7-4i}{1-2i} = \frac{(7-4i)(1+2i)}{1^2+2^2} = \frac{15+10i}{5} = 3+2i.$$

Следовательно,  $11+3i = (1+i)(1-2i)(3+2i)$ .

Ответ:  $1309+357i = 7 \cdot (1+4i)(1-4i)(1+i)(1-2i)(3+2i)$ .

В заключение приведем примеры разложений на простые множители в кольцах многочленов. В кольце  $\mathbb{Q}[x]$  имеем:

$$x^4-1 = (x-1)(x+1)(x^2+1) = \left(\frac{1}{2}x - \frac{1}{2}\right)(6x+6)\left(\frac{1}{3}x^2 + \frac{1}{3}\right).$$

**Упражнение 3.2.** Разложите этот многочлен на простые множители в кольце  $\mathbb{C}[x]$ .

В кольце многочленов  $\mathbb{Z}[x]$  имеем разложение на простые множители  $45x^3 - 15x^2 - 30 = 3 \cdot 5 \cdot (3x^2 + 2x + 2)(x-1)$ .

Ниже мы докажем общую теорему, из которой будет следовать факториальность колец  $\mathbb{Z}$ ,  $\mathbb{Z} + \mathbb{Z}i$  и кольца многочленов  $P[x]$  над полем  $P$ . В дополнение отметим, что кольцо многочленов  $K[x]$  над факториальным кольцом  $K$  факториально. Отсюда, в частности, следует факториальность колец многочленов  $\mathbb{Z}[x_1, \dots, x_n]$  и  $(\mathbb{Z} + \mathbb{Z}i)[x_1, \dots, x_n]$ .

### 3.2.3. Нахождение НОД и НОК в факториальном кольце

**Определение 3.8.** Общим кратным элементов  $a$  и  $b$  факториального кольца  $K$  называется элемент  $m \in K$ , который делится на  $a$  и  $b$ . Наименьшим общим кратным элементов  $a$  и  $b$  называется такое их общее кратное, которое делит любое общее кратное данных элементов. Обозначение:  $\text{НОК}(a, b)$  или  $[a, b]$ .

Непосредственно из определения вытекает следующий способ нахождения НОД и НОК в факториальном кольце.

**Теорема 3.3.** Если даны разложения элементов  $a$  и  $b$  факториального кольца  $K$  в произведение степеней простых элементов:  $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  и  $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ , где простые элементы  $p_i$  и  $p_j$  не ассоциированы при  $i \neq j$ , то  $\text{НОД}(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_k^{\gamma_k}$ , где  $\gamma_i = \min\{\alpha_i, \beta_i\}$ , и  $\text{НОК}(a, b) = p_1^{\delta_1} p_2^{\delta_2} \dots p_k^{\delta_k}$ , где  $\delta_i = \max\{\alpha_i, \beta_i\}$ ,  $i = 1, 2, \dots, k$ .

**Определение 3.9.** Каноническим разложением элемента  $a$  факториального кольца  $K$  называется представление его в виде  $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , где простые элементы  $p_i$  и  $p_j$  не ассоциированы при  $i \neq j$ .

Отметим связь между наибольшим общим делителем и наименьшим общим кратным.

**Теорема 3.4.** Для любых элементов  $a$  и  $b$  факториального кольца  $\text{НОК}(a, b) \cdot \text{НОД}(a, b) = a \cdot b$ .

*Доказательство.* Если хотя бы один из элементов  $a, b$  равен нулю, то утверждение очевидно.

Пусть даны разложения ненулевых элементов  $a$  и  $b$  в произведение простых множителей:  $a = p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot q_1 \cdot q_2 \cdot \dots \cdot q_m$ ,  $b = q_1 \cdot q_2 \cdot \dots \cdot q_m \cdot r_1 \cdot r_2 \cdot \dots \cdot r_n$ , где разными буквами обозначены различные простые элементы, а среди элементов, обозначенных одной и той же буквой, но с разными индексами, могут быть и одинаковые. Тогда

$$\text{НОК}(a, b) = p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot q_1 \cdot q_2 \cdot \dots \cdot q_m \cdot r_1 \cdot r_2 \cdot \dots \cdot r_n;$$

$$\text{НОД}(a, b) = q_1 \cdot q_2 \cdot \dots \cdot q_m.$$

Перемножив эти равенства, получаем

$$\begin{aligned} & \text{НОК}(a, b) \cdot \text{НОД}(a, b) = \\ & = p_1 \cdot p_2 \cdot \dots \cdot p_k \cdot q_1 \cdot q_2 \cdot \dots \cdot q_m \cdot r_1 \cdot r_2 \cdot \dots \cdot r_n \cdot q_1 \cdot q_2 \cdot \dots \cdot q_m = a \cdot b. \end{aligned}$$

Теорема доказана.

## Контрольные вопросы

1. Как понимается единственность разложения на простые множители в факториальном кольце?
2. Как находятся НОД и НОК двух элементов в факториальном кольце?
3. Будет ли 5 простым элементом в кольцах  $\mathbb{Z}$ ,  $\mathbb{Z} + \mathbb{Z}i$ ,  $\mathbb{Q}$ ,  $\mathbb{Z}[x]$ ? Тот же вопрос относительно числа 3.
4. Каковы простые элементы в кольце многочленов над полем?
5. Существует ли область целостности, в которой нет ни простых, ни составных элементов?

## Задачи

1. Разложите в кольце  $\mathbb{Z}$  на простые множители числа 12 656 014, 770 769, 2 115 825.

2. В кольце  $\mathbb{Z}$  найдите НОД и НОК чисел  $a$  и  $b$  с помощью разложения на простые множители: а)  $a = 900$ ,  $b = 887$ ; б)  $a = 301\,889$ ,  $b = 60\,137$ .
3. Докажите, что если натуральное число  $n$  не делится ни на одно простое  $p \leq \sqrt{n}$ , то  $n$  — простое.
4. Докажите, что для любого натурального числа  $n > 1$  числа  $n^4 + 4$  и  $n^4 + n^2 + 1$  составные.
5. Будут ли простыми в  $\mathbb{Z} + \mathbb{Z}i$  числа  $383$ ,  $797$ ,  $929$ ,  $5 + 6i$ ,  $3 + 8i$ ,  $6 + 31i$ ?
6. Разложите на простые множители в  $\mathbb{Z} + \mathbb{Z}i$  числа  $3548$ ,  $49 - 73i$ ,  $78 + 87i$ .
7. С помощью разложения на простые множители в  $\mathbb{Z} + \mathbb{Z}i$  найдите НОД чисел  $56 + 56i$  и  $10 + 10i$ ;  $51 + 68i$  и  $7 + i$ ;  $11 + 23i$  и  $-1 + 23i$ .
8. Если  $a + bi$  — простое в  $\mathbb{Z} + \mathbb{Z}i$ , то будут ли простыми числа  $b + ai$ ,  $a - bi$ ,  $b - ai$ ?
9. Как найти все простые целые комплексные числа, модули которых не превосходят данного натурального числа  $n$ ? Найдите такие числа для  $n = 100$ .
10. Разложите на простые в  $\mathbb{Z} + \mathbb{Z}i$  множители число  $2^{18} + 3^{18}$ .
11. Найдите все разложения на простые множители числа  $10$  в  $\mathbb{Z} + \mathbb{Z}i$ .

### 3.3. Евклидовы кольца

#### 3.3.1. Евклидово кольцо и алгоритм Евклида

Вспомним, что для натуральных чисел  $a$  и  $b$  можно найти НОД( $a$ ,  $b$ ) не только с помощью разложения данных чисел на простые множители, но и с помощью алгоритма Евклида. Составной частью алгоритма Евклида является деление с остатком. Разделить с остатком целое число  $a$  на целое число  $b \neq 0$  — значит найти неполное частное  $q$  и остаток  $r$ , такие что  $a = bq + r$ , причем остаток  $r$  должен удовлетворять условию  $0 \leq r < |b|$ .

Например,  $-273 = 23 \cdot (-12) + 3$ , следовательно, при делении числа  $a = -273$  на  $b = 23$  получаем неполное частное  $q = -12$  и остаток  $r = 3$ .

В произвольной области целостности нет отношения «меньше». Поэтому, обобщая деление с остатком на область целостности, мы применим маленькую хитрость: свяжем с каждым элементом  $a \neq 0$  целое неотрицательное число  $h(a)$ . Дадим соответствующее определение.

**Определение 3.10.** *Евклидовым кольцом* называется область целостности  $K$ , в которой для всякого элемента  $a \neq 0$  однозначно определено целое неотрицательное число  $h(a)$ , называемое *нормой элемента  $a$* , такое что:

$$1) h(ab) \geq h(a), h(b);$$

2) для любых элементов  $a$  и  $b \neq 0$  из  $K$  существуют элементы  $q, r \in K$ , такие что  $a = bq + r$ , причем либо  $r = 0$ , либо  $h(r) < h(b)$  (возможность деления с остатком).

Перенесем известный для целых чисел алгоритм Евклида на произвольное евклидово кольцо.

**Определение 3.11.** Алгоритм Евклида, примененный к элементам  $a \neq 0$  и  $b \neq 0$  евклидова кольца  $K$ , состоит в следующем:

1)  $a$  делим на  $b$  с остатком (начало алгоритма);

2) если остаток отличен от нуля, то делитель делим на остаток (шаг алгоритма).

Следуя этому предписанию, выпишем шаги алгоритма:

$$\begin{array}{ll} a = bq_1 + r_1, & h(r_1) < h(b); \\ b = r_1q_2 + r_2, & h(r_2) < h(r_1); \\ r_1 = r_2q_3 + r_3, & h(r_3) < h(r_2); \\ \dots\dots\dots & \dots\dots\dots \\ r_{n-2} = r_{n-1}q_n + r_n, & h(r_n) < h(r_{n-1}); \\ r_{n-1} = r_nq_{n+1} + r_{n+1}, & r_{n+1} = 0. \end{array}$$

Поскольку нормы остатков строго убывают, являясь целыми неотрицательными числами, то алгоритм Евклида конечен и закончится, когда мы получим остаток, равный нулю. Пусть  $r_{n+1} = 0$ . Докажем, что тогда  $r_n = \text{НОД}(a, b)$ .

Рассмотрим равенства алгоритма Евклида снизу вверх. Из последнего равенства  $r_{n-1} = r_nq_{n+1}$  видим, что  $r_{n-1} \vdots r_n$ . Но тогда из предпоследнего равенства заключаем, что  $r_{n-2} \vdots r_n$ . Поднимаясь по равенствам снизу вверх, получаем, что  $r_n$  является общим делителем элементов  $a$  и  $b$ .

Пусть  $d$  является общим делителем элементов  $a$  и  $b$ . Рассматривая равенства алгоритма Евклида сверху вниз, последовательно заключаем, что все остатки делятся на  $d$ . Следовательно,  $r_n \vdots d$ . Таким образом,  $r_n$  является наибольшим общим делителем элементов  $a$  и  $b$ . В итоге получаем следующее утверждение.

**Теорема 3.5.** Пусть даны элементы  $a$  и  $b$  евклидова кольца  $K$ . Если  $a \vdots b$ , то  $\text{НОД}(a, b) = b$ . Если ни один из данных элементов не делится на другой, то применим к ним алгоритм Евклида и последний не равный нулю остаток в этом алгоритме равен  $\text{НОД}(a, b)$ .

Докажем следующее утверждение.

**Теорема 3.6 (о линейной форме НОД).** Для любых элементов  $a$  и  $b$  евклидова кольца  $K$  существуют элементы  $u, v \in K$ , такие что  $\text{НОД}(a, b) = a \cdot u + b \cdot v$ .

*Доказательство.* Если один из элементов  $a, b$  делится на другой, то утверждение очевидно. Пусть ни один из элементов  $a, b$  не делится на другой. Применим к ним алгоритм Евклида. Рассматривая равенства алгоритма сверху вниз, последовательно остатки выражаем через  $a$  и  $b$ . Из первого равенства находим  $r_1 = a - bq_1 = a \cdot 1 + b(-q_1)$ . Из второго равенства находим  $r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = a(-q_2) + b(1 + q_1q_2)$ . И т.д., на последнем шаге получим искомую линейную форму НОД.

### 3.3.2. Взаимно простые элементы евклидова кольца

Обобщим на евклидовы кольца понятие взаимно простых чисел.

**Определение 3.12.** Элементы  $a$  и  $b$  евклидова кольца  $K$  называются *взаимно простыми*, если  $\text{НОД}(a, b) = 1$ .

**Теорема 3.7 (критерий взаимно простых элементов).** Элементы  $a$  и  $b$  евклидова кольца  $K$  взаимно просты тогда и только тогда, когда существуют элементы  $u, v \in K$ , такие что  $a \cdot u + b \cdot v = 1$ .

*Доказательство.* ( $\Rightarrow$ ) Если элементы  $a$  и  $b$  взаимно просты, то, по определению, один из их наибольших общих делителей равен 1. Его линейная форма (найденная из алгоритма Евклида) имеет указанный в теореме вид.

( $\Leftarrow$ ) Пусть  $a \cdot u + b \cdot v = 1$ . Обозначим  $\text{НОД}(a, b) = d$ . Поскольку  $a : d$  и  $b : d$ , то  $1 : d$ , т.е.  $d$  является делителем единицы. Но тогда одним из наибольших общих делителей  $a$  и  $b$  является 1. Это и означает, что  $a$  и  $b$  взаимно просты.

Рассмотрим основные свойства взаимно простых элементов евклидова кольца.

1. Если  $(a \cdot b) : c$ ,  $a$  и  $c$  взаимно просты, то  $b : c$ .

*Доказательство.* Из условия взаимной простоты элементов  $a$  и  $c$  по критерию взаимной простоты (теорема 3.7) существуют элементы  $u$  и  $v$ , такие что  $a \cdot u + c \cdot v = 1$ . Умножив обе части равенства на  $b$ , получим  $ab \cdot u + bc \cdot v = b$ . По условию,  $ab : c$ . Поскольку оба слагаемых делятся на  $c$ , то и их сумма, равная  $b$ , делится на  $c$ .

2. Для элементов  $a$  и  $b$  евклидова кольца  $K$ , если  $\text{НОД}(a, b) = d$ , то существуют элементы  $a_1, b_1 \in K$ , такие что  $a = a_1 d$ ,  $b = b_1 d$  и  $\text{НОД}(a_1, b_1) = 1$ .

*Доказательство.* Из того, что  $\text{НОД}(a, b) = d$ , следует существование элементов  $a_1, b_1 \in K$ , таких что  $a = a_1 d$ ,  $b = b_1 d$ . С другой стороны, существуют элементы  $u, v \in K$ , такие что  $a \cdot u + b \cdot v = d$ . Тогда  $a_1 du + b_1 dv = d$ , откуда  $a_1 u + b_1 v = 1$ . Следовательно,  $\text{НОД}(a_1, b_1) = 1$ .



3. Если элементы  $a_1$  и  $a_2$  евклидова кольца  $K$  взаимно просты с элементом  $b \in K$ , то и произведение  $a_1 \cdot a_2$  взаимно просто с элементом  $b$ .

*Доказательство.* По условию,  $\text{НОД}(a_1, b) = 1$  и  $\text{НОД}(a_2, b) = 1$ . Следовательно, существуют элементы  $u_1, v_1, u_2, v_2 \in K$ , такие что  $a_1 u_1 + b v_1 = 1$  и  $a_2 u_2 + b v_2 = 1$ . Перемножив эти равенства, получим  $a_1 a_2 u_1 u_2 + b(a_1 u_1 v_2 + a_2 u_2 v_1 + b v_1 v_2) = 1$ . Следовательно,  $\text{НОД}(a_1 a_2, b) = 1$ .

Многократным применением этого свойства можно доказать, что если каждый из элементов  $a_1, \dots, a_k$  взаимно прост с каждым из элементов  $b_1, \dots, b_m$ , то произведения  $a_1 \cdot \dots \cdot a_k$  и  $b_1 \cdot \dots \cdot b_m$  взаимно просты. Отсюда следует, что из взаимной простоты элементов  $a$  и  $b$  следует взаимная простота их степеней.

### 3.3.3. Факториальность евклидова кольца

Сначала установим конечность процесса разложения на множители в евклидовом кольце. Поможет нам в этом следующая лемма.

**Лемма 3.3.** Если в евклидовом кольце  $K$  для элементов  $a, b, c \in K$  имеем  $0 \neq a = b \cdot c$ , где  $b$  и  $c$  отличны от делителей единицы, то  $h(a) > h(b)$ .

*Доказательство.* Если предположить, что  $b : a$ , то  $b = ad$  при некотором  $d \in K$ , откуда  $a = b \cdot c = adc$  и, сокращая на  $a \neq 0$ , получаем  $1 = dc$ . Следовательно,  $c$  оказывается делителем единицы, что противоречит условию. Таким образом,  $b$  не делится на  $a$ . Тогда  $b = aq + r$ , где  $h(r) < h(a)$ . Используя условие, получаем  $b = bcq + r$ , откуда  $r = b(1 - cq)$ , и по свойству нормы  $h(r) \geq h(b)$ . Таким образом,  $h(b) \leq h(r) < h(a)$ . Лемма доказана.

**Теорема 3.8.** Всякий элемент евклидова кольца, отличный от нуля и делителей единицы, либо является простым, либо представим в виде произведения простых множителей.

*Доказательство.* Пусть  $K$  — евклидово кольцо и элемент  $a \in K$  отличен от нуля и делителей единицы. Если элемент  $a$  простой, то доказывать нечего. Если  $a$  составной, то он представим в виде произведения  $a = b \cdot c$ , где  $b$  и  $c$  не являются делителями единицы. Тогда по лемме 3.3  $h(b) < h(a)$ ,  $h(c) < h(a)$ , и это обеспечивает конечность процесса разложения элемента  $a$  на множители. Следовательно, через конечное число шагов мы получим разложение элемента  $a$  на простые множители. Теорема доказана.



Теперь перейдем к доказательству единственности разложения на простые множители в евклидовом кольце. Поможет нам в этом следующая лемма.

**Лемма 3.4 (ключевая).** Если  $p$  — простой элемент евклидова кольца  $K$ ,  $a, b \in K$  и  $ab \vdots p$ , то  $a \vdots p$  или  $b \vdots p$ .

*Доказательство.* Пусть  $\text{НОД}(a, p) = d$ , тогда  $p \vdots d$ . Делителями простого элемента  $p$  являются лишь  $\varepsilon$  и  $\varepsilon p$ , где  $\varepsilon$  — делитель единицы. Если  $d = \varepsilon p$ , то  $a \vdots d \vdots p$ . Если же  $d = \varepsilon$ , то  $\text{НОД}(a, p) = 1$ . В этом случае, по теореме 3.6, существуют элементы  $u, v \in K$ , такие что  $a \cdot u + p \cdot v = 1$ . Умножив это равенство на  $b$ , получим  $ab \cdot u + pb \cdot v = b$ . Так как  $p bv \vdots p$  и, по условию,  $ab \vdots p$ , то  $b \vdots p$ . Лемма доказана.

Теперь у нас все готово для доказательства основной теоремы.

**Теорема 3.9.** Евклидово кольцо факториально.

*Доказательство.* Пусть  $a$  — ненулевой, отличный от делителя единицы элемент евклидова кольца  $K$ . Возможность его разложения на простые множители доказана в теореме 3.8. Пусть имеем два разложения элемента  $a$  в произведение простых множителей:  $a = p_1 p_2 \cdots p_k$  и  $a = q_1 q_2 \cdots q_m$ . Тогда  $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$ . Отсюда следует, что произведение  $(p_1 p_2 \cdots p_k) \vdots q_1$ . По ключевой лемме отсюда следует, что хотя бы один из сомножителей делится на  $p_1$ . Пусть  $p_1 \vdots q_1$ . По свойству простых элементов (см. подпараграф 3.2.1) отсюда следует, что  $q_1 = \varepsilon_1 p_1$ , где  $\varepsilon_1$  — делитель единицы. Следовательно,  $p_1 p_2 \cdots p_k = \varepsilon_1 p_1 q_2 \cdots q_m$  и после сокращения получаем  $p_2 \cdots p_k = \varepsilon_1 q_2 \cdots q_m$ . Теперь повторим рассуждения относительно простого элемента  $q_2$  и придем к равенству  $p_3 \cdots p_k = \varepsilon_1 \varepsilon_2 q_3 \cdots q_m$ . Если предположить, что  $k \neq m$ , то, не нарушая общности, можно считать, что  $k < m$ . Но тогда на  $k$ -м шаге получим равенство  $1 = \varepsilon_1 \varepsilon_2 \cdots \varepsilon_k q_{k+1} \cdots q_m$ . Отсюда следует, что элемент  $q_m$  обратим, что противоречит определению простого элемента. Следовательно,  $k = m$  и  $q_i = \varepsilon_i p_i$ ,  $i = 1, 2, \dots, k$ , при подходящей нумерации сомножителей. Теорема доказана.

## Контрольные вопросы

1. Будет ли евклидовым подкольцо евклидова кольца?
2. Могут ли в евклидовом кольце при делении  $a$  на  $b$  двумя способами остатки быть одинаковыми, а неполные частные — различными?
3. Может ли не факториальное кольцо быть евклидовым?
4. Существует ли область целостности, в которой процесс разложения на нетривиальные множители (представление в виде  $a = a_1 b_1 = a_1 a_2 b_2 = \dots$ ) бесконечен?
5. Какими способами можно найти НОД в евклидовом кольце?

## Задачи

1. Докажите, что для нахождения НОД( $a, b$ ) целых неотрицательных чисел  $a$  и  $b$  можно использовать следующий алгоритм: если  $a \geq b > 0$ , то  $a$  заменяем на разность  $a_1 = a - b$  и переходим к рассмотрению пары  $(a_1, b)$ , пока одно из чисел пары не окажется равным нулю. Тогда второе число является НОД данных чисел.

2. Докажите, что в определении евклидова кольца требование наличия единицы в кольце можно убрать, поскольку существование единицы вытекает из остальных условий.

3. Докажите, что для любых элементов  $a, b, c$  евклидова кольца  $K$  имеет место равенство  $\text{НОД}(\text{НОД}(a, b), c) = \text{НОД}(a, \text{НОД}(b, c))$ .

4. Докажите, что в евклидовом кольце  $\text{НОД}(a, b) = 1 \Leftrightarrow \text{НОД}(a^m, b^n) = 1$  для  $m, n \in \mathbb{N}$ .

5. Известно, что в алгоритме Евклида, примененном к элементам  $a, b$  евклидова кольца  $K$ , на пятом шаге делений с остатком получили остаток, равный нулю. Найдите линейную форму  $\text{НОД}(a, b)$ .

## 3.4. Примеры евклидовых колец

### 3.4.1. Евклидовость кольца целых чисел

Определим норму целого числа  $a \neq 0$ , положив  $h(a) = |a|$ . Поскольку  $h(ab) = |ab| \geq |a|, |b|$ , то свойство 1) из определения евклидова кольца выполнено (см. определение 3.10). Докажем возможность деления с остатком. Она вытекает из следующего более сильного утверждения.

**Теорема 3.10.** Для любых целых чисел  $a$  и  $b \neq 0$  существуют и притом единственные целые числа  $q$  и  $r$ , такие что  $a = bq + r$  и  $0 \leq r < |b|$ .

*Доказательство. Существование.* Рассмотрим случай  $b > 0$ . Разобьем числовую прямую на отрезки длиной  $b$  точками  $0, \pm b, \pm 2b, \dots$  (рис. 3.1).

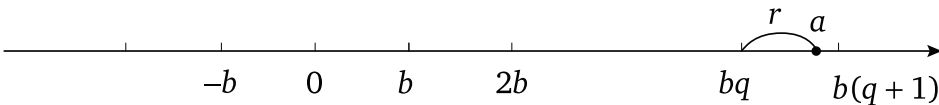


Рис. 3.1

Где бы ни было расположено число  $a$ , оно обязательно попадет в один из данных отрезков. Причем можно считать, что  $a$  не совпадает с правым концом отрезка, так как если бы это произошло, то мы рассмотрели бы следующий отрезок, для которого  $a$  было бы левым концом. Пусть  $a$  попало в отре-

зок  $[bq, b(q+1)]$ . Тогда  $bq \leq a < bq + b$ , откуда  $0 \leq a - bq < b$ . Обозначив  $r = a - bq$ , получим  $a = bq + r$ , где  $0 \leq r < b = |b|$ .

Теперь рассмотрим случай  $b < 0$ . Тогда  $-b > 0$  и по доказанному существуют целые числа  $q$  и  $r$ , такие что  $a = (-b) \cdot q + r$ , где  $0 \leq r < |-b| = |b|$ . Но тогда  $a = b \cdot (-q) + r$ , и существование доказано.

**Единственность.** Пусть  $a = bq + r$ , где  $0 \leq r < |b|$ , и  $a = bq_1 + r_1$ , где  $0 \leq r_1 < |b|$ . Тогда  $bq + r = bq_1 + r_1$ , и если  $r = r_1$ , то получаем  $q = q_1$ , что доказывает единственность. Предположим, что  $r \neq r_1$ , пусть  $r_1 < r$ . Тогда  $0 < r - r_1 = bq_1 - bq : b$  — противоречие, ибо натуральное число  $r - r_1 < |b|$  и не может делиться на  $b$ . Теорема доказана.

Вместе с тем доказана евклидовость кольца целых чисел, из которой следует факториальность этого кольца. В частности, доказана основная теорема арифметики.

Отметим, что стремление иметь единственный наибольший общий делитель двух целых чисел приводит к требованию, чтобы НОД был натуральным числом. В этой связи докажем эквивалентность трех возможных определений НОД как натуральных чисел.

**Теорема 3.11.** *Для произвольных целых чисел  $a$  и  $b$ , не равных нулю одновременно, следующие утверждения эквивалентны:*

- 1)  $d$  является наибольшим из общих делителей чисел  $a$  и  $b$ ;
- 2)  $d$  есть наименьшее натуральное число вида  $au + bv$ , где  $u, v \in \mathbb{Z}$ ;
- 3)  $d$  есть натуральный общий делитель чисел  $a$  и  $b$ , который делится на любой общий делитель этих чисел.

**Доказательство.**  $(1 \Rightarrow 2)$  Пусть  $d$  является наибольшим из общих делителей чисел  $a$  и  $b$ . Тогда  $d = \text{НОД}(a, b)$  и существуют целые числа  $u, v \in \mathbb{Z}$ , такие что  $d = au + bv$  (линейная форма НОД). Следовательно,  $d \in M = \{ax + by \mid x, y \in \mathbb{Z}\}$ , и если  $d_1$  есть наименьшее натуральное число множества  $M$ , то  $d_1 \leq d$ . Пусть  $d_1 = au_1 + bv_1$ . Легко видеть, что  $d_1 : d$ , откуда  $d \leq d_1$ . Следовательно,  $d = d_1$ .

$(2 \Rightarrow 3)$  Пусть  $d_1 = au_1 + bv_1$  — наименьшее натуральное число множества  $M = \{ax + by \mid x, y \in \mathbb{Z}\}$ . Докажем, что  $d_1$  есть общий делитель целых чисел  $a$  и  $b$ . Разделим  $a$  на  $d_1$  с остатком:  $a = d_1q + r$ , где  $0 \leq r < d_1$ . Если предположить, что  $r \neq 0$ , то получаем  $r = a - d_1q = a - (au_1 + bv_1)q = a(1 - u_1q) + b(1 - v_1q) \in M$ , что противоречит минимальности числа  $d_1$  в  $M$ . Следовательно,  $r = 0$  и  $a : d_1$ . Аналогично  $b : d_1$ . Поскольку  $d_1 = au_1 + bv_1$ , то  $d_1$  делится на любой общий делитель  $d$  чисел  $a$  и  $b$ .

(3  $\Rightarrow$  1) Пусть  $d_2$  — натуральный общий делитель чисел  $a$  и  $b$ , который делится на любой общий делитель этих чисел, а  $d$  — наибольший из общих делителей данных чисел. Тогда  $d_2 \leq d$ . С другой стороны, по условию,  $d_2 : d$ , откуда  $d \leq d_2$ . Следовательно,  $d_2 = d$ . Теорема доказана.

Покажем на примере, как реализуется алгоритм Евклида в кольце целых чисел.

### Пример 3.1

Найдем НОД( $a, b$ ) при  $a = 21\,125$ ,  $b = 9061$ .

*Решение.* Выполняем деление.

$$\begin{array}{r}
 a = 21\,125 \Big| 9061 = b \\
 \underline{18\,122} \quad 2 = q_1 \\
 - \quad 9061 \Big| 3003 = r_1 \\
 \underline{9009} \quad 3 = q_2 \\
 - \quad 3003 \Big| 52 = r_2 \\
 \underline{260} \quad 57 = q_3 \\
 - \quad 403 \\
 \underline{364} \\
 - \quad 52 \Big| 39 = r_3 \\
 \underline{39} \quad 1 = q_4 \\
 - \quad 39 \Big| 13 = r_4 \\
 \underline{39} \quad 3 \\
 \hline
 0
 \end{array}$$

Получаем НОД( $21\,125, 9061$ ) = 13.

Продолжим рассмотрение примера и найдем линейную форму НОД. Выпишем шаги алгоритма Евклида:

$$a = bq_1 + r_1,$$

$$b = r_1q_2 + r_2,$$

$$r_1 = r_2q_3 + r_3,$$

$$r_2 = r_3q_4 + r_4,$$

$$r_4 = \text{НОД}(a, b)$$

Выразим последовательно  $r_1, r_2, r_3$  и  $r_4$  через  $a$  и  $b$ :

$$r_1 = a - bq_1 = a - 2b,$$

$$r_2 = b - r_1q_2 = b - (a - 2b) \cdot 3 = -3a + 7b,$$

$$r_3 = r_1 - r_2 q_3 = (a - 2b) - (-3a + 7b) \cdot 57 = 172a - 401b,$$

$$r_4 = r_2 - r_3 q_4 = (-3a + 7b) - (172a - 401b) \cdot 1 = -175a + 408b.$$

Таким образом,  $\text{НОД}(21\,125, 9061) = -175a + 408b$ .

### 3.4.2. Евклидовость кольца целых комплексных чисел

**Определение 3.13.** Для целого комплексного числа  $0 \neq \alpha = a + bi$  определим норму:  $h(\alpha) = |\alpha|^2 = a^2 + b^2$ .

**Теорема 3.12.** Кольцо целых комплексных чисел евклидово.

*Доказательство.* Следуя определению евклидова кольца, нужно установить два свойства нормы  $h(\alpha)$ . Первое свойство  $h(\alpha\beta) \geq h(\alpha)$ ,  $h(\beta)$  вытекает из свойства модуля комплексного числа. Докажем второе свойство — возможность деления с остатком. Пусть даны целые комплексные числа  $\alpha$  и  $\beta \neq 0$ . Геометрически целые комплексные числа расположены в узлах целочисленной решетки, и где бы ни было расположено комплексное число  $\frac{\alpha}{\beta}$ , оно попадет в некоторый квадрат этой решетки (рис. 3.2).

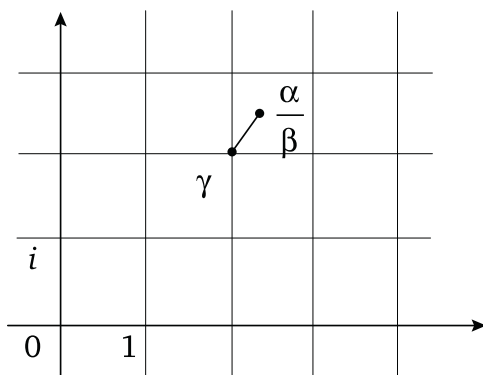


Рис. 3.2

Обозначим через  $\gamma$  ближайшее к  $\frac{\alpha}{\beta}$  целое комплексное число и положим  $\delta = \alpha - \beta\gamma$ , тогда  $\alpha = \beta\gamma + \delta$ . Поскольку расстояние от центра единичного квадрата до любой его вершины равно  $\frac{\sqrt{2}}{2} < 1$ , то  $\left| \frac{\alpha}{\beta} - \gamma \right| < 1$ . Следовательно,  $|\delta|^2 = |\alpha - \beta\gamma|^2 = |\beta|^2 \cdot \left| \frac{\alpha}{\beta} - \gamma \right|^2 < |\beta|^2$ . Таким образом,  $h(\delta) < h(\beta)$ , и евклидовость кольца  $\mathbb{Z} + \mathbb{Z}i$  доказана.

### Пример 3.2

Разделим с остатком  $\alpha = 5 - 8i$  на  $\beta = 2 + 3i$ .

Решение. Имеем

$$\begin{aligned}\frac{\alpha}{\beta} &= \frac{5-8i}{2+3i} = \frac{(5-8i)(2-3i)}{(2+3i)(2-3i)} = \\ &= \frac{(10-24)+(-15-16)i}{4+9} = -\frac{14}{13} - \frac{31}{13}i.\end{aligned}$$

Ближайшим к  $\frac{\alpha}{\beta}$  будет целое комплексное число  $\gamma = -1 - 2i$  (рис. 3.3).

Обозначим

$$\delta = \alpha - \beta\gamma = 5 - 8i - (2 + 3i)(-1 - 2i) = 1 - i.$$

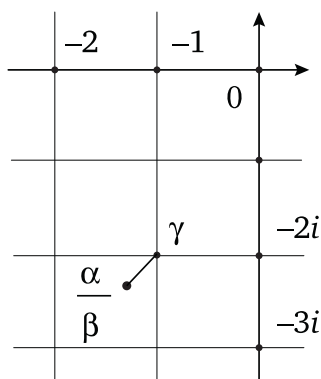


Рис. 3.3

Тогда

$$\alpha = \beta\gamma + \delta = (2 + 3i)(-1 - 2i) + 1 - i$$

и

$$|\delta|^2 = |1 - i|^2 = 1 + 1 < |\beta|^2 = 13.$$

Заметим, что если выбрать вершину квадрата  $\gamma_1 = -1 - 3i$ , и найти  $\delta_1 = \alpha - \beta\gamma_1 = 5 - 8i - (2 + 3i)(-1 - 3i) = -2 + i$ , то получим  $\alpha = \beta\gamma_1 + \delta_1$ , причем  $|\delta_1|^2 = |-2 + i|^2 = 4 + 1 < |\beta|^2 = 13$ . Значит,  $\gamma_1$  также можно взять в качестве неполного частного. Остальные две вершины квадрата, содержащего  $\frac{\alpha}{\beta}$ , не подходят (проверьте!).

Рисунок 3.4 показывает, что если  $\frac{\alpha}{\beta}$  попадет в закрашенную область, то в качестве  $\gamma$  можно взять любую из вершин квадрата, содержащего  $\frac{\alpha}{\beta}$ . Таким образом, деление с остатком в  $\mathbb{Z} + \mathbb{Z}i$  неоднозначно.

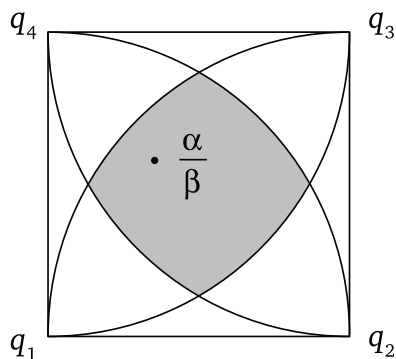


Рис. 3.4

### 3.4.3. Евклидовость кольца многочленов над полем

Евклидовость кольца многочленов  $P[x]$  над полем  $P$  вытекает из следующей теоремы.

**Теорема 3.13.** Для любых многочленов  $f(x)$  и  $h(x) \neq 0$  кольца многочленов  $P[x]$  над полем  $P$  существуют и единственные многочлены  $q(x), r(x) \in P[x]$ , такие что  $f(x) = h(x) \cdot q(x) + r(x)$ , причем  $r(x)$  либо нулевой многочлен, либо его степень меньше степени делителя  $h(x)$ .

*Доказательство. Существование.* Если  $f(x)$  — нулевой многочлен или его степень меньше степени делителя  $h(x)$ , то  $f(x) = h(x) \cdot 0 + f(x)$  и, положив  $q(x) = 0, r(x) = f(x)$ , получим требуемое.

Предположим теперь, что степень  $f(x)$  больше степени  $h(x)$ . Будем делить «уголком» многочлен  $f(x)$  на  $h(x)$ . Пусть  $f(x) = a_n x^n + a_{n-1} x_{n-1} + \dots + a_1 x + a_0$ ,  $h(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$  и  $n \geq m$ . Уравняем старшие члены этих многочленов, для чего  $h(x)$  умножим на  $\frac{a_n}{b_m} x^{n-m}$ , а затем найдем разность

$$f_1(x) = f(x) - h(x) \cdot \frac{a_n}{b_m} x^{n-m}.$$

$$\begin{array}{r|l} f(x) & h(x) \\ h(x) \cdot \frac{a_n}{b_m} x^{n-m} & \frac{a_n}{b_m} x^{n-m} \\ \hline f_1(x). & \end{array}$$

Получаем  $f(x) = h(x) \cdot \frac{a_n}{b_m} x^{n-m} + f_1(x)$ . Если  $f_1(x)$  — нулевой многочлен или его степень меньше степени делителя, то, обо-



значив  $q(x) = \frac{a_n}{b_m} x^{n-m}$ ,  $r(x) = f_1(x)$ , получим требуемое. Если же степень  $f_1(x)$  не меньше степени  $h(x)$ , то продолжим деление «уголком». Пусть  $f_1(x) = c_k x^k + c_{k-1} x^{k-1} + \dots + c_1 x + c_0$ . На втором шаге деления получаем

$$\begin{array}{r|l} - f(x) & h(x) \\ \hline h(x) \cdot \frac{a_n}{b_m} x^{n-m} & \frac{a_n}{b_m} x^{n-m} + \frac{c_k}{b_m} x^{k-m} \\ \hline - f_1(x) & \\ h(x) \cdot \frac{c_k}{b_m} x^{k-m} & \\ \hline & f_2(x). \end{array}$$

Таким образом,

$$f_2(x) = f_1(x) - h(x) \cdot \frac{c_k}{b_m} x^{k-m},$$

откуда

$$f_1(x) = h(x) \cdot \frac{c_k}{b_m} x^{k-m} + f_2(x).$$

Следовательно,

$$\begin{aligned} f(x) &= h(x) \cdot \frac{a_n}{b_m} x^{n-m} + f_1(x) = h(x) \cdot \frac{a_n}{b_m} x^{n-m} + h(x) \cdot \frac{c_k}{b_m} x^{k-m} + f_2(x) = \\ &= h(x) \left( \frac{a_n}{b_m} x^{n-m} + \frac{c_k}{b_m} x^{k-m} \right) + f_2(x). \end{aligned}$$

Если  $f_2(x)$  — нулевой многочлен или его степень меньше степени делителя  $h(x)$ , то, положив  $q(x) = \frac{a_n}{b_m} x^{n-m} + \frac{c_k}{b_m} x^{k-m}$ ,  $r(x) = f_2(x)$ , получим  $f(x) = h(x) \cdot q(x) + r(x)$ , что и требовалось доказать. Если же степень  $f_2(x)$  не меньше степени  $h(x)$ , то продолжим деление «уголком». Поскольку степени многочленов  $f(x), f_1(x), f_2(x), \dots$  убывают, то процесс деления «уголком» конечен, и на конечном шаге мы получим требуемое равенство.

*Единственность.* Предположим, что  $f(x) = h(x) \cdot q(x) + r(x)$  и  $f(x) = h(x) \cdot q_1(x) + r_1(x)$ , где многочлены  $r(x)$  и  $r_1(x)$  либо нулевые, либо их степени меньше степени многочлена  $h(x)$ .

Тогда  $h(x) \cdot q(x) + r(x) = h(x) \cdot q_1(x) + r_1(x)$ , откуда  $r(x) - r_1(x) = h(x)(q_1(x) - q(x))$ . Если предположить, что многочлен  $r(x) - r_1(x)$  ненулевой, то его степень меньше степени многочлена  $h(x)$ , в то время как в правой части равенства стоит многочлен, степень которого не меньше степени многочлена  $h(x)$ . Из полученного противоречия делаем вывод, что  $r(x) - r_1(x) = 0$ , откуда  $r(x) = r_1(x)$ . Но тогда  $h(x)(q_1(x) - q(x)) = 0$ , а так как  $h(x) \neq 0$ , то  $q_1(x) - q(x) = 0$  и  $q_1(x) = q(x)$ . Теорема доказана.

Заметим, что если в определение НОД двух многочленов включить требование, чтобы этот многочлен имел старший коэффициент, равный единице, то это обеспечит единственность НОД.

Покажем на примере, как реализуется алгоритм Евклида в  $\mathbb{Q}[x]$ .

### Пример 3.3

Упростим выражение

$$\frac{2x^3 + x^2 - x + 3}{3x^5 - 5x^4 + 5x^3 - 5x^2 + 3x - 3}.$$

*Решение.* С помощью алгоритма Евклида найдем наибольший общий делитель числителя  $f(x)$  и знаменателя  $g(x)$ , а затем произведем сокращение. Чтобы избежать дробей, многочлены  $f(x)$  и  $g(x)$  заменим на соответственно  $3f(x)$  и  $2g(x)$ . Подобные преобразования в дальнейшем будем отмечать двумя чертами:

$$\begin{array}{r|l} \underline{\underline{6x^5 - 10x^4 + 10x^3 - 10x^2 + 6x - 6}} & \underline{\underline{6x^3 + 3x^2 - 3x + 9}} \\ \underline{\underline{6x^5 + 3x^4 - 3x^3 + 9x^2}} & \underline{\underline{x^2 \parallel -13x \parallel + 39}} \\ \hline \underline{\underline{-13x^4 + 13x^3 - 19x^2 + 6x - 6}} & \\ \underline{\underline{-78x^4 + 78x^3 - 114x^2 + 36x - 36}} & \\ \underline{\underline{-78x^4 - 39x^3 + 39x^2 - 117x}} & \\ \hline \underline{\underline{117x^3 - 153x^2 + 153x - 36}} & \\ \underline{\underline{234x^3 - 306x^2 + 306x - 72}} & \\ \underline{\underline{234x^3 + 117x^2 - 117x + 351}} & \\ \hline \underline{\underline{-423x^2 + 423x - 423}} & \\ \hline \underline{\underline{2x^3 + x^2 - x + 3}} & \underline{\underline{x^2 - x + 1}} \\ \underline{\underline{2x^3 - 2x^2 + 2}} & \underline{\underline{2x + 3}} \\ \hline \underline{\underline{-3x^2 - 3x + 3}} & \\ \underline{\underline{3x^2 - 3x + 3}} & \\ \hline & 0. \end{array}$$

Следовательно,  $\text{НОД}(f(x), g(x)) = x^2 - x + 1$ . Произведя сокращение, получим

$$\frac{2x^3 + x^2 - x + 3}{3x^5 - 5x^4 + 5x^3 - 5x^2 + 3x - 3} = \frac{2x + 3}{3x^3 - 2x^2 - 3}.$$

### 3.4.4. Примеры неевклидовых колец

Существуют числовые факториальные кольца, которые не являются евклидовыми. Например, таковым является кольцо  $K = \left\{ a + b \frac{-1 + i\sqrt{19}}{2} \mid a, b \in \mathbb{Z} \right\}$ , но доказываются это не совсем просто.

Существуют нефакториальные кольца. Например, кольцо  $\mathbb{Z} + \mathbb{Z}i\sqrt{5}$  нефакториальное, в нем число 6 неоднозначно раскладывается на простые множители:  $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ .

Подобная ситуация и в кольце  $\mathbb{Z} + \mathbb{Z}i\sqrt{19}$ . Мы же докажем, что это кольцо нефакториальное, рассуждениями, которым можно придать общий характер. Обозначим  $\omega = \frac{-1 + i\sqrt{19}}{2}$ . Если

бы кольцо  $\mathbb{Z} + \mathbb{Z}i\sqrt{19}$  было факториальным, то нашлось бы в нем простое число  $p$ , входящее в разложение числителя  $\alpha = -1 + i\sqrt{19}$  в меньшей степени, чем в разложение знаменателя  $\beta = 2$ , иначе число  $\omega$  принадлежало бы кольцу  $\mathbb{Z} + \mathbb{Z}i\sqrt{19}$ , что не так. Легко проверить равенство  $\omega^2 + \omega + 5 = 0$ . Отсюда следует, что  $\alpha^2 = -\alpha\beta - 5\beta^2$ . Но это равенство невозможно, так как простое число  $p$  входит в разложение левой части в меньшей степени, чем в разложение правой. Полученное противоречие доказывает, что рассматриваемое кольцо нефакториальное.

В заключение рассмотрим два примера «странных» ситуаций с разложением на простые множители.

1. Пусть  $M$  есть множество всех чисел вида  $2^n$ , где  $n$  — неотрицательное рациональное число. Это множество замкнуто относительно умножения. Единственным делителем единицы в  $M$  является 1, а всякое другое число бесконечно раскладывается на убывающие сомножители, например  $2 = \frac{1}{2^2} \cdot 2^2 = \frac{1}{2^4} \cdot 2^4 \cdot \frac{1}{2^4} \cdot 2^4 = \dots$ .

2 (пример Д. Гильберта). Пусть  $M$  есть множество всех чисел вида  $4n + 1$ , где  $n$  — целое неотрицательное число. Тогда единственным делителем единицы в  $M$  является 1. Рассмотрим в этом множестве числа  $9 = 4 \cdot 2 + 1$ ,  $21 = 4 \cdot 5 + 1$ ,  $49 = 4 \cdot 12 + 1$

и  $441 = 4 \cdot 110 + 1$ . Легко видеть, что первые три числа являются простыми в  $M$ , а четвертое — составное число, которое неоднозначно раскладывается на простые множители:  $441 = 9 \cdot 49 = 21 \cdot 21$ .

## Контрольные вопросы

1. Однозначно ли деление с остатком в кольцах  $\mathbb{Z}$ ,  $\mathbb{Z} + \mathbb{Z}i$ ,  $\mathbb{Q}[x]$ ?
2. Сколько существует наибольших общих делителей двух данных чисел в кольцах  $\mathbb{Z}$  и  $\mathbb{Z} + \mathbb{Z}i$ ?
3. Если в кольце целых чисел  $\text{НОД}(a, b) = d$ , то чему может быть равен  $\text{НОД}(a, b)$  в кольце целых комплексных чисел?
4. Пусть поле  $P$  является подполем поля  $F$  и  $f(x), g(x) \in P[x]$ . Если  $\text{НОД}(f(x), g(x)) = d(x)$ , то чему равен  $\text{НОД}(f(x), g(x))$  в кольце  $F[x]$ ?

## Задачи

1. В кольце  $\mathbb{Z}$  разделите с остатком  $\pm 28$  на  $\pm 23$  и  $\pm 23$  на  $\pm 28$ .
2. В кольце  $\mathbb{Z} + \mathbb{Z}i$  разделите с остатком  $a$  на  $b$ , где: а)  $a = 10 + 15i$ ,  $b = 3 - i$ ; б)  $a = 13 + 2i$ ,  $b = 2 + 3i$ .
3. В кольце  $\mathbb{Z} + \mathbb{Z}i$  разделите с остатком  $a$  на  $b$  всеми возможными способами: а)  $a = -6 + 10i$ ,  $b = 1 + 3i$ ; б)  $a = -4 + 2i$ ,  $b = 2 + 2i$ ; в)  $a = -1 - 4i$ ,  $b = 1 - i$ .
4. Найдите  $\text{НОД}(a, b)$ , где: а)  $a = 9 + 3i$ ,  $b = 4 - 2i$ ; б)  $a = 6 - 3i$ ,  $b = 6 + 2i$ .
5. Найдите линейную форму  $\text{НОД}(a, b)$ , где  $a = 35 - 5i$ ,  $b = 8 - 6i$ .
6. В кольце  $\mathbb{Z}[x]$  опишите все делители многочлена  $x^4 - 1$ . Опишите все делители этого многочлена в кольце  $\mathbb{R}[x]$ .
7. Даны два многочлена  $f(x), g(x) \in \mathbb{Q}[x]$ . Как изменится  $\text{НОД}(f(x), g(x))$ , если каждый многочлен умножить: 1) на 5; 2) на  $\frac{3}{5}$ ; 3) на  $x - 3$ ? Тот же вопрос, если умножить один из многочленов на соответствующий множитель.
8. Найдите  $\text{НОД}(f(x), h(x))$ , если:
  - а)  $f(x) = x^6 + 8x^5 + 22x^4 + 43x^3 + 70x^2 + 57x + 39$ ,  $h(x) = x^4 + 7x^3 + 14x^2 + 21x + 33$ ;
  - б)  $f(x) = 2x^7 + x^6 - x^5 + 9x^4 - 3x^3 - 8x - 7$ ,  $h(x) = 2x^6 - x^5 + 11x^3 - 10x^2 + x - 9$ ;
  - в)  $f(x) = 6x^5 + x^4 + 12x^3 - 42x^2 + 30x + 25$ ,  $h(x) = 2x^4 - x^3 + 4x^2 - 17x + 20$ .
9. Найдите линейную форму  $\text{НОД}(f(x), g(x))$ , если:
  - а)  $f(x) = x^6 - x^5 - 10x^2 + 9x - 3$ ,  $h(x) = x^4 + x^3 + 2x^2 + 3x - 3$ ;
  - б)  $f(x) = 3x^7 + 2x^6 - 142x^5 - 79x^4 - 104x^3 + 50x^2 - 48x - 42$ ,  $h(x) = x^4 + x^3 - 47x^2 - 42x - 49$ ;
  - в)  $f(x) = x^7 - x^5 + 4x^3 - x - 1$ ,  $h(x) = x^6 + x^5 - x^4 - x^3 + x^2 + 2x + 1$ .

10. Упростите выражения:

$$\begin{aligned} \text{а) } & \frac{2x^5 + 11x^4 + 5x^3 - 2x^2 - 11x - 5}{x^3 + 4x^2 + 4x + 3}; \text{ б) } \frac{6x^4 + x^3 - 8x^2 + 4x - 3}{9x^7 + 21x^6 + 5x^5 - x^4 + 2x^3}; \\ \text{в) } & \frac{x^8 + 4x^7 + 8x^5 + 32x^4}{x^5 - 5x^4 - 3x^3 + 27x^2 - 72x + 60}; \text{ г) } \frac{2x^5 + x^4 - 19x^3 + 29x^2 - 26x + 8}{x^3 + x^2 - x + 2}. \end{aligned}$$

11. Покажите, что в кольце  $\mathbb{Z} + \mathbb{Z}i\sqrt{5}$  числа 2, 3,  $1 \pm i\sqrt{5}$  являются простыми, а числа 6 и 41 – составными. Представьте 41 в виде произведения простых в  $\mathbb{Z} + \mathbb{Z}i\sqrt{5}$  чисел двумя способами и тем самым докажете, что это кольцо не факториально.

12. В кольце  $K = \mathbb{Z} + \mathbb{Z}i\sqrt{5} = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$  найдите два числа, для которых среди общих делителей нет НОД.

13. Как определить норму в кольце  $K = \mathbb{Z} + \mathbb{Z}\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ , чтобы оно стало евклидовым кольцом?

14. Пусть  $\omega$  обозначает одно из чисел:  $i\sqrt{2}, \frac{1+i\sqrt{3}}{2}, \frac{1+i\sqrt{7}}{2}, \frac{1+i\sqrt{11}}{2}$ .

Докажите, что множество  $\mathbb{Z} + \mathbb{Z}\omega = \{a + b\omega \mid a, b \in \mathbb{Z}\}$  является евклидовым кольцом относительно нормы  $h(a + b\omega) = |a + b\omega|^2$  (отсюда следует факториальность всех этих колец).

## 3.5. Кольца главных идеалов

### 3.5.1. Определение и примеры колец главных идеалов

Оказывается, факториальность кольца можно доказать при более слабых условиях, чем евклидовость этого кольца. Дадим соответствующие определения. Предварительно напомним, что в произвольном коммутативном кольце  $K$  идеал  $\langle a \rangle = \{ka \mid k \in K\}$  называется главным.

**Определение 3.14.** Область целостности  $K$ , в которой всякий идеал главный, называется *кольцом главных идеалов*.

Например, в кольце целых чисел  $\mathbb{Z}$  всякий идеал имеет вид  $m\mathbb{Z} = \langle m \rangle$ . Следовательно,  $\mathbb{Z}$  — кольцо главных идеалов.

**Теорема 3.14.** Всякое евклидово кольцо является кольцом главных идеалов.

*Доказательство.* Пусть  $H$  — идеал евклидова кольца  $K$ . Если идеал  $H$  нулевой, то, очевидно, он главный. Пусть идеал  $H$  ненулевой и  $a$  — элемент идеала  $H$  с наименьшей нормой  $h(a)$ . Очевидно,  $\langle a \rangle \subseteq H$ . Докажем обратное включение. Пусть  $b \in H$ . Разделим  $b$  на  $a$  с остатком:  $b = aq + r$ , где либо  $r = 0$ , либо  $h(r) < h(a)$ . Поскольку  $r = b - aq \in H$  и элемент  $a$  с наименьшей нормой в  $H$ , то  $r = 0$ . Следовательно,  $b = aq \in \langle a \rangle$ . Таким образом,  $H = \langle a \rangle$ . Теорема доказана.

Из доказанной теоремы вытекает, что кольцами главных идеалов являются кольцо целых чисел, кольцо целых комплексных чисел, кольцо многочленов  $P[x]$  над полем  $P$ .

### 3.5.2. Существование разложения на простые множители в кольце главных идеалов

Чтобы доказать факториальность кольца главных идеалов, нужно, во-первых, доказать существование разложения на простые множители в этом кольце и, во-вторых, доказать единственность этого разложения.

**Теорема 3.15.** *В кольце главных идеалов всякий ненулевой элемент, отличный от делителей единицы, либо является простым, либо представим в виде произведения простых множителей.*

**Доказательство.** Пусть  $K$  — кольцо главных идеалов и  $a$  — ненулевой элемент кольца, отличный от делителей единицы. Если элемент  $a$  простой, то доказывать нечего. Пусть элемент  $a$  составной и  $a = a_1 \cdot b$ , где элементы  $a_1$  и  $b$  отличны от делителей единицы. Если оба сомножителя простые, то теорема доказана. Пусть элемент  $a_1$  составной. Из равенства  $a = a_1 \cdot b$  следует  $\langle a \rangle \subseteq \langle a_1 \rangle$ . Если предположить, что  $\langle a \rangle = \langle a_1 \rangle$ , то  $a_1 = ka$  при некотором  $k \in K$ . Но тогда  $a = kab$ , откуда  $1 = kb$ . Следовательно,  $b$  является делителем единицы, что противоречит условию. Итак, имеем строгое включение  $\langle a \rangle \subset \langle a_1 \rangle$ . Повторяя рассуждения, мы либо на конечном шаге получим разложение элемента  $a$  на простые множители, либо получим бесконечную, строго возрастающую цепочку идеалов  $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \dots$ . Покажем, что второе предположение ведет к противоречию. Обозначим через  $H$  объединение всех полученных идеалов:

$$H = \bigcup_{i=1}^{\infty} \langle a_i \rangle.$$
 Покажем, что  $H$  есть идеал. Если  $x, y \in H$ , то

существует номер  $n$ , такой что  $x, y \in \langle a_n \rangle$ . Но тогда  $x \pm y, kx \in \langle a_n \rangle \subseteq H$  для любого  $k \in K$ . Следовательно,  $H$  является идеалом, а значит, по условию, главным идеалом. Пусть  $H = \langle c \rangle$ . Существует номер  $m$ , такой что  $c \in \langle a_m \rangle$ . Но тогда  $H = \langle a_m \rangle$ , что противоречит бесконечности строго возрастающей цепочки идеалов. Теорема доказана.

### 3.5.3. Факториальность кольца главных идеалов

**Лемма 3.5.** *В кольце главных идеалов если произведение двух элементов делится на простой элемент, то по крайней мере один из сомножителей делится на этот элемент.*

**Доказательство.** Пусть  $K$  — кольцо главных идеалов,  $a, b \in K$  и  $(a \cdot b) : p$ , где  $p$  — простой элемент в  $K$ . Если  $a : p$ , то дока-

зывать нечего. Пусть  $a$  не делится на  $p$ . По условию, идеал  $\langle a, p \rangle$  главный, пусть  $\langle a, p \rangle = \langle d \rangle$ . Тогда  $p \vdots d$ , откуда либо  $d = \varepsilon$ , либо  $d = \varepsilon p$ , где  $\varepsilon$  — делитель единицы. Но во втором случае  $a \vdots d = \varepsilon p \vdots p$ , что противоречит нашему предположению. Следовательно,  $d = \varepsilon$  и  $\langle a, p \rangle = \langle \varepsilon \rangle = \langle 1 \rangle$ . Но тогда существуют элементы  $u, v \in K$ , такие что  $au + pv = 1$ . Умножив это равенство на  $b$ , получим  $abu + pbv = b$ . По условию  $a \cdot b \vdots p$ , и, очевидно,  $p bv \vdots p$ . Следовательно,  $b \vdots p$ . Лемма доказана.

Из теоремы 3.15 и леммы 3.5 вытекает следующая теорема.

**Теорема 3.16.** *Кольцо главных идеалов факториально.*

Итак, пытаясь доказать аналог основной теоремы арифметики в наиболее общей ситуации, мы выделили три класса колец: евклидовы кольца, кольца главных идеалов и факториальные кольца.

Мы доказали, что первый класс колец содержится во втором, а второй — в третьем:

$$\{\text{евклидовы кольца}\} \subset \{\text{кольца главных идеалов}\} \subset \{\text{факториальные кольца}\}.$$

Существуют кольца главных идеалов, которые не являются евклидовыми, например уже упоминавшееся выше кольцо

$$K = \left\{ a + b \frac{-1 + i\sqrt{19}}{2} \mid a, b \in \mathbb{Z} \right\}.$$

Примером факториального кольца,

не являющегося кольцом главных идеалов, является кольцо многочленов с целыми коэффициентами  $\mathbb{Z}[x_1, x_2]$ . В этом кольце идеал  $\langle x_1, x_2 \rangle$ , состоящий из многочленов без свободных членов, не является главным. В силу того что это кольцо не является кольцом главных идеалов, оно не является евклидовым.

В то время как в евклидовом кольце линейную форму НОД мы получаем из алгоритма Евклида, в кольце главных идеалов можно установить существование линейной формы НОД, минуя алгоритм Евклида. В самом деле, если  $a$  и  $b$  — элементы кольца главных идеалов  $K$ , то идеал  $\langle a, b \rangle = \langle d \rangle$  при некотором  $d \in K$ . Следовательно,  $a \vdots d, b \vdots d$  и существуют  $u, v \in K$ , такие что  $au + bv = d$ . Из этого равенства следует, что  $d$  делится на любой общий делитель элементов  $a$  и  $b$ . Таким образом,  $d = \text{НОД}(a, b)$ .

## Контрольные вопросы

1. Является ли поле кольцом главных идеалов?
2. Каким элементом порождается кольцо главных идеалов?



3. В каком случае два элемента порождают кольцо главных идеалов?
4. В каком случае два элемента кольца главных идеалов порождают собственное подкольцо?
5. Является ли кольцо  $\mathbb{Z}[x]$  кольцом главных идеалов?
6. Будет ли в произвольной области целостности пересечение главных идеалов снова главным идеалом?
7. Будет ли кольцо четных целых чисел кольцом главных идеалов?

## Задачи

1. В кольце  $\mathbb{Z}$  найдите число, порождающее идеал  $\langle a, b, c \rangle$ , если:
  - а)  $a = 243, b = 135, c = 811$ ;
  - б)  $a = 936, b = 1848, c = 360$ .
2. В кольце  $\mathbb{Z} + \mathbb{Z}i$  найдите число, порождающее идеал  $\langle a, b, c \rangle$ , если:
  - а)  $a = 1 + 2i, b = 3 + 7i, c = 4i$ ;
  - б)  $a = 7 + 4i, b = 1 + 7i, c = -1 + 3i$ .
3. Между какими идеалами из  $\langle 2 \rangle, \langle 6 \rangle, \langle 3 \rangle, \langle 8 \rangle, \langle 12 \rangle$  кольца  $\mathbb{Z}$  можно поставить знак  $\subseteq$ ? Найдите пересечения данных идеалов.
4. Определите, каким элементом в кольце  $\mathbb{Q}[x]$  порождается идеал  $\langle 2, x \rangle$ .
5. Определите, каким многочленом в кольце  $\mathbb{Q}[x]$  порождается идеал, состоящий из многочленов, не содержащих одночленов нулевой и первой степеней.

# Глава 4

## РАСШИРЕНИЯ ПОЛЕЙ

### 4.1. Алгебраический над данным полем элемент и его минимальный многочлен

#### 4.1.1. Алгебраические и трансцендентные элементы над полем

Введем основные понятия.

**Определение 4.1.** Если поле  $P$  является подполем поля  $F$ , то  $F$  называется *расширением* поля  $P$ . При этом элементы из  $F \setminus P$  называются *иррациональными* над полем  $P$ .

**Определение 4.2.** Пусть поле  $F$  является расширением поля  $P$ . Элемент  $\alpha \in F$  называется *алгебраическим над полем  $P$* , если существует ненулевой многочлен  $f(x) \in P[x]$ , имеющий  $\alpha$  своим корнем. В противном случае элемент  $\alpha$  называется *трансцендентным над полем  $P$* . Числа алгебраические (трансцендентные) над полем  $\mathbb{Q}$  называются просто *алгебраическими* (соответственно *трансцендентными*).

**Определение 4.3.** Пусть поле  $F$  является расширением поля  $P$ . Элемент  $\alpha \in F \setminus P$ , являющийся алгебраическим над полем  $P$ , называется *алгебраической иррациональностью* над полем  $P$ .

Рассмотрим *примеры*.

1. Числа  $\sqrt{2}$ ,  $\sqrt[3]{5}$ ,  $\pi$ ,  $e$ ,  $2\pi + 1$  являются иррациональными над полем  $\mathbb{Q}$ , или просто иррациональными. Из них только первые два являются алгебраическими иррациональностями над полем  $\mathbb{Q}$ , а остальные трансцендентны над  $\mathbb{Q}$ . Всякое трансцендентное число является иррациональным.

2. Докажем, что число  $\sqrt{2} + 3i$  является алгебраическим. Обозначим  $\alpha = \sqrt{2} + 3i$  и возведем равенство в квадрат:  $\alpha^2 = 2 + 6i\sqrt{2} - 9$ . Отсюда  $\alpha^2 + 7 = 6i\sqrt{2}$ . Снова возведем в квадрат:  $(\alpha^2 + 7)^2 = -72$ ,  $\alpha^4 + 14\alpha^2 + 49 = -72$ ,  $\alpha^4 + 14\alpha^2 + 121 = 0$ . Следовательно, число  $\alpha$  является корнем многочлена  $x^4 + 14x^2 + 121$ , а значит, является алгебраическим числом.

3. Всякое мнимое число (с ненулевой мнимой частью) является алгебраической иррациональностью над полем  $\mathbb{R}$ .

4. Заметим, что всякий элемент  $\alpha$  поля  $P$  является алгебраическим над  $P$ , так как он является корнем многочлена  $x - \alpha$  с коэффициентами из  $P$ .

#### 4.1.2. Минимальный многочлен алгебраического элемента

По определению, алгебраический над полем  $P$  элемент является корнем некоторого многочлена с коэффициентами из  $P$ . Выделим из этих многочленов один.

**Определение 4.4.** Минимальным многочленом алгебраического над полем  $P$  элемента  $\alpha$  называется приведенный многочлен с коэффициентами из  $P$  наименьшей степени, имеющий корень  $\alpha$ .

Напомним, что многочлен называется приведенным, если его старший коэффициент равен единице.

**Теорема 4.1.** Имеют место следующие утверждения.

1. Для любого алгебраического над полем  $P$  элемента  $\alpha$  существует и притом только один минимальный многочлен  $\varphi(x)$ .

2. Минимальный многочлен  $\varphi(x)$  неприводим над полем  $P$ .

3. Для любого многочлена  $f(x) \in P[x]$  имеем:

3.1) либо  $f(x)$  делится на  $\varphi(x)$ , либо  $\text{НОД}(f(x), \varphi(x)) = 1$ ;

3.2) многочлен  $f(x)$  делится на  $\varphi(x)$  тогда и только тогда, когда  $f(\alpha) = 0$ ;

3.3)  $\text{НОД}(f(x), \varphi(x)) = 1$  тогда и только тогда, когда  $f(\alpha) \neq 0$ .

*Доказательство.* 1. Пусть  $\alpha$  — алгебраический элемент над полем  $P$ . Это означает, что  $\alpha$  является корнем некоторого многочлена с коэффициентами из поля  $P$ . Из всех таких многочленов выберем многочлен наименьшей степени и разделим его на старший коэффициент. В результате получим минимальный многочлен  $\varphi(x)$ .

Пусть  $\varphi_1(x)$  — также минимальный многочлен элемента  $\alpha$ . Тогда степени многочленов  $\varphi(x)$  и  $\varphi_1(x)$  равны. Напомним, что их старшие коэффициенты равны единице. Если предположить, что  $\varphi_1(x) \neq \varphi(x)$ , то  $\varphi_1(x) - \varphi(x)$  — ненулевой многочлен, имеющий корень  $\alpha$ , и его степень меньше степени многочлена  $\varphi(x)$ , что противоречит определению минимального многочлена. Следовательно,  $\varphi_1(x) = \varphi(x)$ , что доказывает единственность минимального многочлена.

2. Предположим, что минимальный многочлен  $\varphi(x)$  приводим, пусть  $\varphi(x) = f(x) \cdot h(x)$ , где степени сомножителей меньше степени многочлена  $\varphi(x)$ . Но тогда  $f(\alpha) \cdot h(\alpha) = \varphi(\alpha) = 0$ , а так как в поле нет делителей нуля, то  $f(\alpha) = 0$  или  $h(\alpha) = 0$ . Но то и дру-

гое противоречит минимальности степени многочлена  $\varphi(x)$ . Следовательно, минимальный многочлен  $\varphi(x)$  неприводим.

3.1. Обозначим  $(f(x), \varphi(x)) = d(x)$ . Тогда  $\varphi(x) \vdots d(x)$ . Значит, существует многочлен  $q(x) \in P[x]$ , такой что  $\varphi(x) = d(x) \cdot q(x)$ . Очевидно,  $0 \leq \deg(d(x)) \leq \deg(\varphi(x))$ . Рассмотрим все возможные случаи относительно степени многочлена  $d(x)$ :

1)  $\deg(d(x)) = 0$ . Тогда  $d(x) = d \in P$ , откуда  $(f(x), \varphi(x)) = 1$ , что и требовалось доказать;

2)  $\deg(d(x)) = \deg(\varphi(x))$ . Тогда  $\deg(q(x)) = 0$ , а значит,  $q(x) = q \in P, q \neq 0$ . Но тогда  $\varphi(x) = d(x) \cdot q$ , откуда  $d(x) = \varphi(x) \cdot q^{-1}$  и  $f(x) \vdots d(x) \vdots \varphi(x)$ , что и требовалось доказать;

3) наконец, предположим, что  $0 < \deg(d(x)) < \deg(\varphi(x))$ . Имеем:  $0 = f(\alpha) = d(\alpha) \cdot q(\alpha)$ , откуда  $d(\alpha) = 0$  или  $q(\alpha) = 0$ . Но то и другое противоречит минимальности степени минимального многочлена  $\varphi(x)$ . Свойство доказано.

3.2. ( $\Rightarrow$ ) Пусть  $f(x) \vdots \varphi(x)$ , тогда  $f(x) = \varphi(x) \cdot h(x)$  при некотором  $h(x) \in P[x]$ . Но тогда  $f(\alpha) = \varphi(\alpha) \cdot h(\alpha) = 0$ .

( $\Leftarrow$ ) Пусть  $f(\alpha) = 0$ . Разделим  $f(x)$  на  $\varphi(x)$  с остатком:  $f(x) = \varphi(x) \cdot q(x) + r(x)$ . Если предположить, что  $r(x) \neq 0$ , то  $\deg(r(x)) < \deg(\varphi(x))$  и  $0 = f(\alpha) = \varphi(\alpha) \cdot q(\alpha) + r(\alpha)$ . Поскольку  $\varphi(\alpha) = 0$ , то  $r(\alpha) = 0$ . Пришли к противоречию с минимальностью степени многочлена  $\varphi(x)$ . Свойство доказано.

3.3. Это свойство доказывается от противного с использованием свойства 3.2. Вместе с тем теорема доказана.

Легко доказать, что приведенный неприводимый на поле  $P$  многочлен, имеющий корень  $\alpha$ , является минимальным многочленом элемента  $\alpha$ .

**Определение 4.5.** Степенью алгебраического над полем  $P$  элемента  $\alpha$  называется степень его минимального многочлена.

Примеры:

- степени алгебраических чисел  $-1, \sqrt{3}, \sqrt[4]{5}$  над полем  $\mathbb{Q}$  равны, соответственно, 1, 2, 4;
- степень алгебраического над полем  $\mathbb{Q}$  числа  $\sqrt{2} + 3i$  равна четырем, поскольку его минимальный многочлен  $x^4 + 14x^2 + 121$  имеет степень 4.

#### 4.1.3. Освобождение от алгебраической иррациональности в знаменателе дроби

Рассмотрим задачу из алгебры многочленов.

##### Задача 4.1

Пусть  $\alpha$  является корнем многочлена  $x^3 + 6x - 3$ . Нужно освободиться от алгебраической иррациональности в знаменателе дроби

$\frac{\alpha}{\alpha^2 + 5}$ , т.е. представить дробь в виде многочлена от  $\alpha$  с рациональными коэффициентами.

*Решение.* Знаменатель дроби есть значение от  $\alpha$  многочлена  $f(x) = x^2 + 5$ , а минимальным многочленом алгебраического элемента  $\alpha$  является  $\varphi(x) = x^3 + 6x - 3$ , поскольку этот многочлен неприводим над полем  $\mathbb{Q}$  (по критерию Эйзенштейна при простом  $p = 3$ ). Найдем НОД( $x^3 + 6x - 3, x^2 + 5$ ) с помощью алгоритма Евклида:

$$\begin{array}{r} \varphi(x) = x^3 + 6x - 3 \quad \Big| \quad x^2 + 5 = f(x) \\ \underline{- x^3 + 5x} \phantom{- 3} \quad \quad x = q_1(x) \\ f(x) = x^2 + 5 \quad \Big| \quad x - 3 = r_1(x) \\ \underline{- x^2 - 3x} \phantom{+ 5} \quad \quad x + 3 = q_2(x) \\ 3x + 5 \\ \underline{- 3x - 9} \\ 14 = r_2(x). \end{array}$$

Следовательно,

$$\varphi(x) = f(x) \cdot q_1(x) + r_1(x), f(x) = r_1(x) \cdot q_2(x) + r_2(x),$$

откуда

$$\begin{aligned} r_1(x) &= \varphi(x) - f(x) \cdot q_1(x), r_2(x) = f(x) - r_1(x) \cdot q_2(x) = \\ &= f(x) - (\varphi(x) - f(x)q_1(x))q_2(x) = f(x)(1 + q_1(x)q_2(x)) + (-q_2(x))\varphi(x). \end{aligned}$$

Итак,  $14 = f(x)[1 + x(x + 3)] + \varphi(x)(-x - 3) = f(x)(x^2 + 3x + 1) + \varphi(x)(-x - 3)$ .

Отсюда  $14 = f(\alpha)(\alpha^2 + 3\alpha + 1) + \varphi(\alpha)(-\alpha - 3) = f(\alpha)(\alpha^2 + 3\alpha + 1)$ .

Таким образом, чтобы избавиться от алгебраической иррациональности в знаменателе данной дроби, нужно числитель и знаменатель умножить на  $\alpha^2 + 3\alpha + 1$ . В результате получим

$$\frac{\alpha}{\alpha^2 + 5} = \frac{\alpha(\alpha^2 + 3\alpha + 1)}{14} = \frac{1}{14}(\alpha^3 + 3\alpha^2 + \alpha).$$

Обобщим ситуацию и рассмотрим общую задачу.

#### Задача 4.2

##### Задача об освобождении от алгебраической иррациональности в знаменателе дроби

Пусть  $\alpha$  — алгебраическая иррациональность над полем  $P$  с минимальным многочленом  $\varphi(x)$  и  $\beta = \frac{a_k \alpha^k + a_{k-1} \alpha^{k-1} + \dots + a_1 \alpha + a_0}{b_m \alpha^m + b_{m-1} \alpha^{m-1} + \dots + b_1 \alpha + b_0}$ , где коэффициенты многочленов в числителе и знаменателе дроби

принадлежат полю  $P$ . Освободиться от алгебраической иррациональности в знаменателе дроби, т.е. представить  $\beta$  в виде

$$\beta = c_n \alpha^n + c_{n-1} \alpha^{n-1} + \dots + c_1 \alpha + c_0,$$

где коэффициенты принадлежат полю  $P$ .

*Решение.* Обозначим  $f(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$  и  $\gamma = f(\alpha)$ . Поскольку  $\gamma \neq 0$ , то по свойству минимального многочлена  $\text{НОД}(f(x), \varphi(x)) = 1$ . Используя алгоритм Евклида, находим многочлены  $u(x)$  и  $v(x)$ , такие что  $f(x)u(x) + \varphi(x)v(x) = 1$ . Отсюда  $f(\alpha)u(\alpha) + \varphi(\alpha)v(\alpha) = 1$ , а так как  $\varphi(\alpha) = 0$ , то  $f(\alpha)u(\alpha) = 1$ . Следовательно, умножая числитель и знаменатель данной дроби на  $u(\alpha)$ , в знаменателе получим единицу, и задача решена.

Заметим, что общий прием освобождения от алгебраической иррациональности в знаменателе дроби в случае комплексных чисел  $\frac{a+bi}{c+di}$  приводит к известной процедуре умножения числителя и знаменателя на число, сопряженное знаменателю.

### Исторический экскурс

Впервые существование чисел, трансцендентных над полем  $\mathbb{Q}$ , обнаружил Ж. Лиувилль (1809—1882) в работах 1844 и 1851 гг. Одним из трансцендентных чисел Лиувилля является число  $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ . В десятичной записи  $\alpha = 0,1100010\dots$ . Ш. Эрмит (1822—1901) доказал трансцендентность числа  $e$  в 1873 г., а К. Ф. Линдман (1852—1939) доказал в 1882 г. трансцендентность числа  $\pi$ . Эти результаты были получены очень не просто. В то же время совсем просто Г. Кантор (1845—1918) доказал, что трансцендентных чисел «значительно больше», чем алгебраических: трансцендентных чисел «столько же», сколько всех действительных чисел, в то время как алгебраических чисел «столько же», сколько всех натуральных чисел. Точнее, множество алгебраических чисел счетно, а множество трансцендентных чисел несчетно. Доказательство этого факта, устанавливая существование трансцендентных чисел, не дает рецепта получения ни одного из них. Такого рода теоремы существования чрезвычайно важны в математике уже тем, что вселяют веру в успех поиска объекта, существование которого доказано. Вместе с тем существует направление в математике, представители которого не признают чистых теорем существования, называя их неконструктивными. Наиболее яркими из этих представителей являются Л. Кронекер и Я. Брауэр.

В 1900 г. на Всемирном конгрессе математиков в Париже немецкий математик Д. Гильберт (1862—1943) сформулировал следую-

щую проблему 22: Какова природа числа  $\alpha^\beta$ , где  $\alpha$  и  $\beta$  — алгебраические числа,  $\alpha \neq 0$ ,  $\alpha \neq 1$  и степень алгебраического числа  $\beta$  не меньше 2? А. О. Гельфонд (1906—1968) доказал, что такие числа трансцендентны. Отсюда следует, в частности, что числа  $2^{\sqrt{2}}$ ,  $3^i$  являются трансцендентными.

## Контрольные вопросы

1. Если  $\alpha$  является корнем многочлена  $f(x) = x^3 - 3x^2 + x - 3$ , то чему равна степень элемента  $\alpha$  над полем  $\mathbb{Q}$ ?
2. Пусть  $P$  есть подполе поля  $F$  и элемент  $\alpha \in F$  является алгебраическим над  $P$ . Будет ли  $\alpha$  алгебраическим над  $F$ ?
3. Пусть  $\varphi(x)$  является минимальным многочленом алгебраического над полем  $P$  элемента  $\alpha$  и  $k \in P$ . Будет ли минимальным для элемента  $\alpha$  многочлен  $f(x) = k\varphi(x)$ ?
4. Может ли многочлен быть минимальным для двух различных алгебраических элементов?
5. Может ли элемент быть алгебраическим и не иррациональным? Иррациональным, но не алгебраическим?
6. Пусть поле  $F$  является расширением поля  $P$  и  $A, B, C$  являются подмножествами поля  $F$ , соответственно, алгебраических, иррациональных и трансцендентных элементов над полем  $P$ . Изобразите на диаграмме и охарактеризуйте множества  $A \cap B, A \cap C, B \cap C, A \cup B, A \cup C, B \cup C$ .
7. Может ли минимальный многочлен алгебраической иррациональности над полем  $P$  иметь корень в этом поле?

## Задачи

1. Найдите минимальный многочлен и степень алгебраического над полем  $P$  элемента  $\alpha$ , если:
  - а)  $\alpha = 2, P = \mathbb{Q}$ ; б)  $\alpha = \sqrt{2}, P = \mathbb{Q}$ ; в)  $\alpha = \sqrt{2}, P = \mathbb{R}$ ; г)  $\alpha = \sqrt{2}, P = \mathbb{C}$ ;
  - д)  $\alpha = \sqrt[3]{2}, P = \mathbb{Q}$ ; е)  $\alpha = \sqrt[3]{2}, P = \mathbb{R}$ ; ж)  $\alpha = \sqrt{2} + \sqrt{3}, P = \mathbb{Q}$ ;
  - з)  $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{6}, P = \mathbb{Q}$ ; и)  $\alpha = \sqrt[3]{2} + \sqrt[3]{3}, P = \mathbb{Q}$ ;
  - к)  $\alpha = \sqrt[3]{4} - \sqrt[3]{2} + 1, P = \mathbb{Q}$ ; л)  $\alpha = i\sqrt[3]{3\sqrt{2}}, P = \mathbb{R}$ ; м)  $\alpha = \sqrt{1 + \sqrt{2}}, P = \mathbb{Q}$ .
2. Освободитесь от алгебраической иррациональности в знаменателе дроби:
  - а)  $\frac{14}{2 + 3\sqrt{2}}$ ; б)  $\frac{13}{2 + 3i}$ ; в)  $\frac{1}{\sqrt{2} - \sqrt{3}}$ ; г)  $\frac{1}{\sqrt{2} + \sqrt{3} + \sqrt{5}}$ ; д)  $\frac{1}{\sqrt[3]{2} - \sqrt[3]{3}}$ ;
  - е)  $\frac{\alpha - 1}{\alpha + 2}, \alpha^3 + 3\alpha^2 - 1 = 0$ ; ж)  $\frac{\alpha^2 - \alpha - 3}{\alpha^4 + 4\alpha + 4}, \alpha^3 + 4\alpha^2 + 8\alpha + 8 = 0$ ;
  - з)  $\frac{1}{3\alpha^3 - 6\alpha^2 + \alpha - 2}, \alpha^4 - 5\alpha^3 + 9\alpha^2 - 5\alpha - 2 = 0$ .



## 4.2. Степень расширения

### 4.2.1. Базис и степень расширения

Напомним, что векторным пространством над полем  $P$  называется множество элементов  $V$ , называемых векторами, на котором определена операция сложения векторов, определено умножение произвольного вектора  $\alpha \in V$  на произвольный элемент  $a \in P$  со значением  $a\alpha \in V$ , причем выполнены следующие условия:

- 1) система  $\langle V, + \rangle$  является коммутативной группой;
- 2) выполняется равенство ассоциативности:  $(ab)\alpha = a(b\alpha)$  для любых  $a, b \in P$  и  $\alpha \in V$ ;
- 3) выполняются равенства дистрибутивности:  $(a + b)\alpha = a\alpha + b\alpha$  и  $a(\alpha + \beta) = a\alpha + a\beta$  для любых  $a, b \in P$  и  $\alpha, \beta \in V$ ;
- 4) для единицы  $1$  поля  $P$  и любого вектора  $\alpha \in V$  имеет место равенство  $1\alpha = \alpha$ .

Базисом векторного пространства  $V$  над полем  $P$  называется максимальная линейно независимая система векторов.

Любые два базиса векторного пространства содержат одинаковое количество векторов. Векторное пространство называется конечномерным, если оно имеет конечный базис. Конечномерное векторное пространство называется  $n$ -мерным, если его базис состоит из  $n$  векторов. Примером бесконечномерного векторного пространства является пространство многочленов от переменной  $x$  над полем  $P$ , оно имеет бесконечный базис  $\{1, x, x^2, \dots\}$ .

Легко видеть, что расширение  $F$  поля  $P$  является векторным пространством над полем  $P$ . В этом случае элементы поля  $F$  называются векторами, а элементы поля  $P$  — скалярами.

**Определение 4.6.** Пусть поле  $F$  является расширением поля  $P$ . Если система векторов  $S \subseteq F$  является базисом векторного пространства  $F$  над полем  $P$ , то  $S$  будем называть *базисом расширения  $F$* , а количество векторов базиса  $S$  — *степенью расширения  $F$  поля  $P$* . Степень расширения  $F$  поля  $P$  обозначается  $|F : P|$  (читается: степень поля  $F$  относительно поля  $P$ ). Если степень расширения бесконечна, то пишут  $|F : P| = \infty$ , а если степень расширения конечна, то расширение  $F$  называется *конечным* и пишут  $|F : P| < \infty$ , или более точно  $|F : P| = n$ .

Рассмотрим *примеры*.

1. Пусть  $F = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ . Тогда поле  $F$  является расширением поля  $\mathbb{Q}$  с базисом расширения  $S = \{1, \sqrt{3}\}$ , а степень расширения  $|F : \mathbb{Q}| = 2$ .

2. Пусть  $G = \left\{ \frac{f(\pi)}{g(\pi)} \mid f(x), g(x) \in \mathbb{Q}[x], g(x) \neq 0 \right\}$ . Тогда поле  $G$

является расширением поля  $P$  с бесконечным базисом  $S = \{1, \pi, \pi^2, \dots\}$  и  $|G : \mathbb{Q}| = \infty$ .

3.  $|\mathbb{R} : \mathbb{Q}| = \infty$ .

4.  $|\mathbb{C} : \mathbb{R}| = 2$  и базис расширения  $S = \{1, i\}$ .

5.  $F = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$ ,  $|F : \mathbb{Q}| = 4$  и одним из базисов расширения является  $S = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ .

**Определение 4.7.** Расширение  $F$  поля  $P$  называется алгебраическим, если всякий элемент поля  $F$  является алгебраическим над полем  $P$ .

**Теорема 4.2.** Всякое конечное расширение поля является алгебраическим.

*Доказательство.* Пусть поле  $F$  является конечным расширением поля  $P$  и базис пространства  $F$  над полем  $P$  состоит из  $n$  векторов. Известно, что в этом случае всякая система  $n + 1$  векторов линейно зависима. Возьмем произвольный элемент  $\alpha \in F$ . Система  $\{\alpha^0 = 1, \alpha, \alpha^2, \dots, \alpha^n\}$  содержит  $n + 1$  векторов, а значит, линейно зависима. Следовательно, существуют элементы  $a_0, a_1, \dots, a_n \in P$ , среди которых есть отличные от нуля, такие что  $a_0 \cdot 1 + a_1 \alpha + \dots + a_n \alpha^n = 0$ . Но это означает, что элемент  $\alpha$  является корнем ненулевого многочлена  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ , т.е.  $\alpha$  — алгебраический элемент над полем  $P$ . Теорема доказана.

#### 4.2.2. Повторное расширение поля

**Определение 4.8.** Если поле  $F$  является расширением поля  $P$ , а поле  $G$  является расширением поля  $F$ , то  $G$  называется повторным расширением поля  $P$ .

**Теорема 4.3.** Если  $P \subseteq F \subseteq G$ , где поле  $F$  является расширением поля  $P$  с базисом  $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$ , а поле  $G$  является расширением поля  $F$  с базисом  $\{\beta_1, \beta_2, \dots, \beta_m\}$ , то система  $S = \{\alpha_i \beta_j \mid i = 1, 2, \dots, k; j = 1, 2, \dots, m\}$  является базисом расширения  $G$  поля  $P$ . Таким образом,  $|G : P| = |F : P| \cdot |G : F|$ .

*Доказательство.* Докажем сначала линейную независимость системы векторов  $S$  над полем  $P$ . Для этого предположим, что  $\sum_{\substack{1 \leq i \leq k \\ 1 \leq j \leq m}} a_{ij} \alpha_i \beta_j = 0$ , где  $a_{ij} \in P$ , и докажем, что каждый

коэффициент  $a_{ij} = 0$ . Запишем данную линейную комбинацию по-другому:  $\sum_{j=1}^m \left( \sum_{i=1}^k a_{ij} \alpha_i \right) \beta_j = 0$ . Поскольку  $\sum_{i=1}^k a_{ij} \alpha_i \in F$  для любого  $j = 1, 2, \dots, m$ , то имеем линейную комбинацию системы векто-

ров  $\{\beta_1, \beta_2, \dots, \beta_m\}$  над полем  $F$ , а так как эта система векторов является базисом векторного пространства  $G$  над полем  $F$ , то  $\sum_{i=1}^k a_{ij} \alpha_i = 0$ . Но система векторов  $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$  является базисом векторного пространства  $F$  над полем  $P$ . Следовательно,  $a_{ij} = 0$  для всех индексов  $i$  и  $j$ . Это доказывает линейную независимость системы  $S$  над полем  $P$ .

Теперь докажем, что всякий вектор  $\gamma \in G$  линейно выражается через систему векторов  $S$  с коэффициентами из поля  $P$ . Поскольку система векторов  $\{\beta_1, \beta_2, \dots, \beta_m\}$  является базисом векторного пространства  $G$  над полем  $F$ , то существуют элементы  $b_j \in F, j = 1, 2, \dots, m$ , такие что  $\gamma = \sum_{j=1}^m b_j \beta_j$ , а так как система

векторов  $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$  является базисом векторного пространства  $F$  над полем  $P$ , то для каждого  $b_j$  существуют элементы  $b_{ij} \in P, i = 1, 2, \dots, k$ , такие что  $b_j = \sum_{i=1}^k b_{ij} \alpha_i$ . Окончательно получаем  $\gamma = \sum_{j=1}^m \left( \sum_{i=1}^k b_{ij} \alpha_i \right) \beta_j$ , что и требовалось доказать.

Таким образом, система векторов  $S$  является базисом векторного пространства  $G$  над полем  $P$ . Отсюда следует, что  $|G : P| = k \cdot m = |F : P| \cdot |G : F|$ . Теорема доказана.

## Контрольные вопросы

1. Будет ли конечным полем конечное расширение конечного поля?
2. Пусть поле  $F$  является конечным расширением поля  $P$  и  $|F : P| = n$ . Чему может равняться степень алгебраического над полем  $P$  элемента поля  $F$ ?
3. Пусть дана цепочка расширений  $P \subset F \subset G$ . Верно ли, что если  $G$  — алгебраическое расширение поля  $P$ , то и  $F$  является алгебраическим расширением этого поля? Верно ли, что если  $|F : P| < \infty, |G : F| < \infty$ , то  $G$  — алгебраическое расширение поля  $P$ ? Какой может быть степень расширения  $|F : P|$ , если  $|G : P| = 6$ ?
4. Чему равны степени расширений  $|\mathbb{C} : \mathbb{R}|, |\mathbb{R} : \mathbb{R}|, |\mathbb{R} : \mathbb{Q}|$ ?
5. Какую степень может иметь конечное расширение: поля  $\mathbb{R}$ ; поля  $\mathbb{C}$ ; поля  $\mathbb{Q}$ ?

## Задачи

1. Пусть степень расширения  $F$  поля  $P$  равна 5. Опишите все подполя поля  $F$ , содержащие  $P$ .

2. Найдите степени расширений поля  $\mathbb{Q}$ :

а)  $F_1 = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ ; б)  $F_2 = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ ;

в)  $F_3 = \left\{ \frac{f(\pi)}{h(\pi)} \mid f(x), h(x) \in \mathbb{Q}[x], h(x) \neq 0 \right\}$ ; г)  $F_4 = \{a + bi \mid a, b \in \mathbb{Q}\}$ .

3. В расширении  $\mathbb{R}$  поля  $\mathbb{Q}$  для каждой системы векторов либо докажите ее линейную независимость над полем  $\mathbb{Q}$ , либо установите линейную зависимость: а)  $\{1, 2, 3\}$ ; б)  $\{1, \sqrt{2}, 3\}$ ; в)  $\{1, \sqrt{2}, \sqrt{3}\}$ ; г)  $\{2, \sqrt[3]{2}, \sqrt[3]{4}\}$ ; д)  $\{2, 2\pi, 2\pi^2\}$ . Рассмотрите линейную зависимость этих систем векторов над полем  $\mathbb{R}$ .

## 4.3. Простое расширение поля

### 4.3.1. Простое алгебраическое расширение поля

**Определение 4.9.** Пусть поле  $F$  является расширением поля  $P$  и  $\alpha \in F$ . Образует множество всех элементов, которые получаются из элементов поля  $P$  и элемента  $\alpha$  с помощью операций сложения, вычитания, умножения и деления. Очевидно, это множество является полем, которое называется *простым расширением поля  $P$  с помощью присоединения элемента  $\alpha$*  и обозначается  $P(\alpha)$ . Если элемент  $\alpha$  — алгебраический над полем  $P$ , то  $P(\alpha)$  называется *простым алгебраическим расширением*, а если  $\alpha$  — трансцендентный над  $P$ , то  $P(\alpha)$  называется *простым трансцендентным расширением* поля  $P$ .

Легко видеть, что  $P(\alpha) = \left\{ \frac{g(\alpha)}{h(\alpha)} \mid g(x), h(x) \in P[x], h(\alpha) \neq 0 \right\}$

и  $P(\alpha)$  есть минимальное поле, содержащее поле  $P$  и элемент  $\alpha$ .

**Теорема 4.4 (о строении простого алгебраического расширения поля).** Если  $\alpha$  — алгебраический элемент над полем  $P$  степени  $n$ , то:

1)  $P(\alpha) = \{f(\alpha) \mid f(x) \in P[x]\}$ ;

2)  $P(\alpha)$  является векторным пространством над полем  $P$  с базисом  $\{1 = \alpha^0, \alpha, \dots, \alpha^{n-1}\}$ , так что  $|P(\alpha) : P| = n$ ;

3) всякий элемент  $\beta \in P(\alpha)$  однозначно представим в виде значения  $f(\alpha)$  некоторого многочлена  $f(x)$  с коэффициентами из поля  $P$  степени, не превосходящей  $n - 1$ .

**Доказательство.** 1. Из определения простого алгебраического расширения поля  $P$  вытекает, что

$$P(\alpha) = \left\{ \frac{g(\alpha)}{h(\alpha)} \mid g(x), h(x) \in P[x], h(\alpha) \neq 0 \right\}.$$

В то же время из решения задачи об освобождении от алгебраической иррациональности в знаменателе дроби вытекает

возможность представить отношение  $\frac{g(\alpha)}{h(\alpha)}$  в виде  $\frac{g(\alpha)}{h(\alpha)} = f(\alpha)$ , где  $f(x) \in P[x]$ . Следовательно,  $P(\alpha) = \{f(\alpha) \mid f(x) \in P[x]\}$ .

2. Докажем, что система  $\{1 = \alpha^0, \alpha, \dots, \alpha^{n-1}\}$  является базисом векторного пространства  $P(\alpha)$  над полем  $P$ .

2.1. Докажем, что система векторов  $\{1 = \alpha^0, \alpha, \dots, \alpha^{n-1}\}$  линейно независима. Предположим, что существуют элементы  $a_0, a_1, \dots, a_{n-1} \in P$ , такие что  $a_0 \cdot 1 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1} = 0$ . Тогда  $\alpha$  оказывается корнем многочлена  $g(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \in P[x]$ . Если предположить, что этот многочлен ненулевой, то его степень меньше степени минимального многочлена элемента  $\alpha$ , что противоречит определению минимального многочлена. Следовательно, многочлен  $g(x)$  нулевой, т.е. все его коэффициенты равны нулю. Но это и означает линейную независимость системы векторов  $\{1 = \alpha^0, \alpha, \dots, \alpha^{n-1}\}$ .

2.2. Докажем, что всякий элемент  $\beta \in P(\alpha)$  является линейной комбинацией векторов системы  $\{1 = \alpha^0, \alpha, \dots, \alpha^{n-1}\}$ . В п. 1) доказано, что  $\beta = f(\alpha)$  при некотором  $f(x) \in P[x]$ . Разделим  $f(x)$  на минимальный многочлен  $\varphi(x)$  алгебраического элемента  $\alpha$ :  $f(x) = \varphi(x) \cdot q(x) + r(x)$ , где либо  $r(x) = 0$ , либо степень остатка  $r(x)$  строго меньше степени многочлена  $\varphi(x)$ , равной  $n$ . В первом случае  $f(x) = \varphi(x) \cdot q(x)$ ,  $\beta = f(\alpha) = \varphi(\alpha) \cdot q(\alpha) = 0$  и  $\beta = 0$  тривиально выражается через элементы данной системы. Во втором случае остаток имеет вид  $r(x) = b_0 + b_1 x + \dots + b_{n-1} x^{n-1}$ . Но тогда  $\beta = f(\alpha) = \varphi(\alpha) \cdot q(\alpha) + r(\alpha) = r(\alpha) = b_0 + b_1 \alpha + \dots + b_{n-1} \alpha^{n-1}$ , что и требовалось доказать. Итак, система векторов  $\{1 = \alpha^0, \alpha, \dots, \alpha^{n-1}\}$  является базисом.

3. Из определения базиса вытекает однозначность представления всякого элемента  $\beta \in P(\alpha)$  в виде линейной комбинации базисных элементов  $\{1 = \alpha^0, \alpha, \dots, \alpha^{n-1}\}$ . Теорема доказана.

**Следствие.** Степень простого алгебраического расширения  $P(\alpha)$  совпадает со степенью минимального многочлена элемента  $\alpha$ .

Рассмотрим *примеры*.

1. Простые алгебраические расширения поля  $\mathbb{Q}$ :  $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ ,  $\mathbb{Q}(\sqrt[3]{3}) = \{a + b\sqrt[3]{3} + c\sqrt[3]{9} \mid a, b, c \in \mathbb{Q}\}$ .

2. Рассмотрим поле классов вычетов по модулю 2:  $Z_2 = \{\bar{0}, \bar{1}\}$ , и многочлен над этим полем  $x^2 + x + \bar{1}$ . Проверкой устанавливаем, что он не имеет корней в  $Z_2$ , а значит, неприводим над  $Z_2$ . Будем считать, что в некотором расширении поля  $Z_2$  этот многочлен имеет корень  $\alpha$ . Тогда получаем простое алгебраическое расширение  $Z_2(\alpha) = \{\bar{0}, \bar{1}, \alpha, \alpha + \bar{1}\}$ .

**Упражнение 4.1.** Составьте таблицы сложения и умножения элементов расширения из предыдущего примера 2.

Как отмечалось выше, простое алгебраическое расширение  $F = P(\alpha)$  поля  $P$  является конечным, а значит, алгебраическим, т.е. всякий элемент  $\beta \in F$  является корнем некоторого многочлена с коэффициентами из  $P$ . Покажем на примере, как найти этот многочлен.

#### Пример 4.1

Пусть  $F = \mathbb{Q}(\alpha)$  и  $\alpha$  является корнем многочлена  $f(x) = x^3 + x - 1$ . Найдите минимальный многочлен элемента  $\beta = \alpha^2 + \alpha + 2$ .

*Решение.* По условию,  $\alpha^3 + \alpha - 1 = 0$ , отсюда  $\alpha^3 = 1 - \alpha$ . Из данного по условию равенства  $\beta = \alpha^2 + \alpha + 2$  находим  $\alpha^2 + \alpha + 2 - \beta = 0$ . Умножив данное равенство на  $\alpha$ , получаем  $\alpha\beta = \alpha^3 + \alpha^2 + 2\alpha = (1 - \alpha) + \alpha^2 + 2\alpha = \alpha^2 + \alpha + 1$ , откуда  $\alpha^2 + (1 - \beta)\alpha + 1 = 0$ . Наконец,  $\alpha^2\beta = \alpha^4 + \alpha^3 + 2\alpha^2 = \alpha(1 - \alpha) + (1 - \alpha) + 2\alpha^2 = \alpha^2 + 1$ , откуда  $(1 - \beta)\alpha^2 + 1 = 0$ . Таким образом, приходим к системе равенств

$$\begin{cases} \alpha^2 + \alpha + 2 - \beta = 0, \\ \alpha^2 + (1 - \beta)\alpha + 1 = 0, \\ (1 - \beta)\alpha^2 + 1 = 0. \end{cases}$$

Исключая  $\alpha^2$  и  $\alpha$ , приходим к равенству  $\beta^3 - 4\beta^2 + 3\beta - 1 = 0$ , которое говорит о том, что  $\beta$  является корнем многочлена  $\varphi(x) = x^3 - 4x^2 + 3x - 1$ . Этот многочлен, как легко видеть, не имеет рациональных корней, а значит, неприводим над полем  $\mathbb{Q}$ . Следовательно,  $\varphi(x)$  является искомым минимальным многочленом алгебраического над полем  $\mathbb{Q}$  элемента  $\beta$ .

Заметим, что при исключении  $\alpha$  из системы равенств можно привлечь знания по решению систем линейных уравнений. Равенства системы говорят о том, что вектор  $(\alpha^2, \alpha, 1)$  является ненулевым решением однородной системы линейных уравнений

$$\begin{cases} x_1 + x_2 + (2 - \beta)x_3 = 0, \\ x_1 + (1 - \beta)x_2 + 1 = 0, \\ (1 - \beta)x_1 + 1 = 0. \end{cases}$$

Следовательно, определитель матрицы системы равен нулю:

$$\begin{vmatrix} 1 & 1 & 2 - \beta \\ 1 & 1 - \beta & 1 \\ 1 - \beta & 0 & 1 \end{vmatrix} = 0.$$

Отсюда получаем равенство  $\beta^3 - 4\beta^2 + 3\beta - 1 = 0$ .

Наконец, отметим, что это упражнение можно превратить в школьную задачу: известно, что  $\alpha^3 + \alpha - 1 = 0$ ,  $\beta = \alpha^2 + \alpha + 2$ ; най-



дите уравнение с целыми коэффициентами, корнем которого является  $\beta$ .

---

### 4.3.2. Простое трансцендентное расширение поля

Пример простого трансцендентного расширения получаем, расширяя поле рациональных чисел с помощью трансцендентного числа  $\pi$ :

$$Q(\pi) = \left\{ \frac{f(\pi)}{g(\pi)} \mid f(x), g(x) \in \mathbb{Q}[x], g(x) \neq 0 \right\}.$$

**Теорема 4.5 (о строении простого трансцендентного расширения поля).** *Если  $\alpha$  — трансцендентный над полем  $P$  элемент, то простое трансцендентное расширение  $P(\alpha)$  изоморфно полю отношений кольца многочленов  $P[x]$ , т.е. полю*

$$\left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in P[x], g(x) \neq 0 \right\}.$$

*Доказательство.* Искомым изоморфизмом является, как легко проверить, отображение  $\varphi\left(\frac{f(x)}{g(x)}\right) = \frac{f(\alpha)}{g(\alpha)}$  для любого элемента  $\frac{f(x)}{g(x)} \in P(\alpha)$ .

### 4.3.3\*. Существование простого алгебраического расширения поля и поля разложения данного многочлена

Определяя простое алгебраическое расширение  $P(\alpha)$ , мы элемент  $\alpha$  брали в некотором расширении  $F$  поля  $P$ . Покажем, как можно построить расширение  $P(\alpha)$  без предположения о существовании поля  $F$ .

Пусть  $\varphi(x)$  — минимальный многочлен алгебраического элемента  $\alpha$ . Докажем, что факторкольцо  $P[x]/\langle\varphi(x)\rangle$  (факторкольцо кольца многочленов с коэффициентами из поля  $P$  по идеалу, порожденному многочленом  $\varphi(x)$ ) изоморфно полю  $P(\alpha)$ . Для любого смежного класса  $h(x) + \langle\varphi(x)\rangle$  определим  $f(h(x) + \langle\varphi(x)\rangle) = h(\alpha)$ . Легко проверить, что отображение  $f$  является искомым изоморфизмом  $P[x]/\langle\varphi(x)\rangle$  на  $P(\alpha)$ . При этом  $f(x + \langle\varphi(x)\rangle) = \alpha$  и для любого элемента  $a \in P$   $f(a + \langle\varphi(x)\rangle) = a$ . В силу этого изоморфизма можно считать, что факторкольцо  $P[x]/\langle\varphi(x)\rangle$  является простым алгебраическим расширением поля  $P$ . При этом роль элементов поля  $P$  выполняет множество



$\{a + \langle \varphi(x) \rangle \mid a \in P\}$ , а роль присоединяемого элемента  $\alpha$  — смежный класс  $x + \langle \varphi(x) \rangle$ .

Докажем существование *поля разложения* приведенного многочлена  $f(x) \in P[x]$ , т.е. такого расширения  $F$  поля  $P$ , которое содержит все корни  $\alpha_1, \alpha_2, \dots, \alpha_n$  данного многочлена. Благодаря этому многочлен  $f(x)$  над полем  $F$  можно разложить на линейные множители:  $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ . Известно, что над полем  $P$  данный многочлен можно разложить в произведение неприводимых множителей:  $f(x) = \varphi_1(x) \cdot \varphi_2(x) \cdot \dots \cdot \varphi_k(x)$ . Факторкольцо  $P[x]/\langle \varphi_1(x) \rangle$ , как показано выше, является простым алгебраическим расширением  $P(\alpha_1)$ , где  $\alpha_1 = x + \langle \varphi_1(x) \rangle$  является корнем данного многочлена  $f(x) \in P[x]$ . При этом мы считаем, что  $P$  есть множество  $\{a + \varphi_1(x) \mid a \in P\}$ . Над полем  $F_1$  имеем разложение  $f(x) = (x - \alpha_1) \cdot f_1(x)$ . Теперь рассмотрим многочлен  $f_1(x)$  над полем  $F_1$  и повторим для него те же рассуждения. В результате получим простое алгебраическое расширение  $F_2 = F_1(\alpha_2)$ , где  $\alpha_2$  является корнем многочлена  $f_1(x)$ . Но тогда над полем  $F_2$  имеем разложение  $f_1(x) = (x - \alpha_2) \cdot f_2(x)$ , а значит,  $f(x) = (x - \alpha_1)(x - \alpha_2) \cdot f_2(x)$ . И т.д., на последнем шаге получим искомое поле  $F = F_n$ , которое содержит все корни данного многочлена.

## Контрольные вопросы

1. В каком случае  $P(\alpha) = P$ ?
2. Если  $\alpha$  — алгебраический над полем  $P$  элемент, то будет ли простое расширение  $P(\alpha)$  алгебраическим? Конечным?
3. Если  $\alpha$  — корень многочлена  $x^3 - 3x^2 + 2x - 6$ , то чему равна степень расширения  $|P(\alpha) : P|$ ?
4. Пусть  $\varphi(x)$  — минимальный многочлен алгебраического над полем  $P$  элемента  $\alpha$  и  $\beta$  — корень многочлена  $\varphi(x)$  в некотором поле, содержащем поле  $P$ . Будет ли  $\varphi(x)$  минимальным многочленом для  $\beta$ ? Верно ли, что  $P(\alpha) = P(\beta)$ ?
5. Верно ли, что расширение  $P(\alpha)$  поля  $P$  является алгебраическим тогда и только тогда, когда элемент  $\alpha$  — алгебраический над полем  $P$ ?
6. Пусть поле  $F$  является расширением поля  $P$  степени 15. Какой может быть степень алгебраического над полем  $P$  элемента  $\alpha \in F$ ?
7. Содержит ли поле  $\mathbb{Q}(\sqrt{3})$  элементы: а)  $2 + 5\sqrt{3}$ ; б)  $3 + \sqrt{7}$ ; в)  $3 + \sqrt[3]{3}$ ?

## Задачи

1. Пусть  $F = \mathbb{Q}(\alpha)$  и  $\alpha$  является корнем многочлена  $f(x) \in \mathbb{Q}[x]$ . Найдите минимальный многочлен элемента  $\beta \in F$ , если: а)  $f(x) = x^3 - x + 1$ ,

$\beta = \alpha^2 - \alpha + 2$ ; б)  $f(x) = x^3 + 2x^2 - x - 1$ ,  $\beta = \alpha^2 - 1$ ; в)  $f(x) = x^3 - x^2 + x - 1$ ,  $\beta = \alpha^2 + 2$ ; г)  $f(x) = x^3 + x - 1$ ,  $\beta = \alpha^2 + \alpha + 2$ .

2. Найдите базис и степень расширения  $F$  поля  $P$ : а)  $F = \mathbb{Q}(\sqrt{3} + \sqrt{5})$ ,  $P = \mathbb{Q}$ ; б)  $F = \mathbb{Q}(\sqrt{3} + i)$ ,  $P = \mathbb{Q}$ ; в)  $F = \mathbb{Q}(\pi + i)$ ,  $P = \mathbb{Q}$ ; г)  $F = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ ,  $P = \mathbb{Q}(\sqrt{3})$ ; д)  $F = \mathbb{R}(i)$ ,  $P = \mathbb{R}$ .

3. Верно ли, что:

а)  $\mathbb{Q}\left(3 + \frac{5}{2 - \sqrt{3}}\right) = \mathbb{Q}(\sqrt{3})$ ; б)  $\mathbb{Q}\left(7 + \frac{2 - \sqrt{2} - \sqrt{3}}{\sqrt{6}}\right) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ ;

в)  $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{6})$ ?

4. Докажите линейную независимость системы векторов  $\{1, 1 + \sqrt[3]{2}, 3 - \sqrt[3]{4}\}$  расширения  $\mathbb{Q}(\sqrt[3]{2})$  над полем  $\mathbb{Q}$ . Будет ли линейно независимой над  $\mathbb{Q}$  система векторов  $\{1, 1 + \sqrt[3]{2}, 3 - \sqrt[3]{4}, 23\sqrt[3]{2}\}$ ?

## 4.4. Составное расширение поля

### 4.4.1. Повторное алгебраическое расширение поля

В этом и последующих параграфах будем рассматривать только алгебраические расширения полей.

Пусть поля  $P, F, G$  таковы, что  $P \subset F \subset G$ , причем  $F = P(\alpha)$  — простое алгебраическое расширение поля  $P$ , а  $G = F(\beta)$  — простое алгебраическое расширение поля  $F$ . Тогда поле  $G$  является повторным алгебраическим расширением поля  $P$  и обозначается  $G = P(\alpha)(\beta)$ .

**Теорема 4.6.** Пусть дано повторное алгебраическое расширение  $G = P(\alpha)(\beta)$  поля  $P$  и степень алгебраического над полем  $P$  элемента  $\alpha$  равна  $k$ , а степень алгебраического над полем  $F = P(\alpha)$  элемента  $\beta$  равна  $t$ . Тогда  $|G : P| = kt$  и система векторов  $S = \{\alpha^i \beta^j \mid i = 0, 1, \dots, k; j = 1, 2, \dots, t\}$  является базисом расширения  $G$  поля  $P$ .

**Доказательство.** По теореме о строении простого алгебраического расширения поля система векторов  $\{\alpha^0 = 1, \alpha, \dots, \alpha^{k-1}\}$  является базисом векторного пространства  $F$  над полем  $P$ , а система векторов  $\{\beta^0 = 1, \beta, \dots, \beta^{t-1}\}$  — базисом векторного пространства  $G$  над полем  $F$ . Но тогда по теореме 4.3 система векторов  $S$  является базисом векторного пространства  $G$  над полем  $P$  и  $|G : P| = kt$ . Теорема доказана.

### 4.4.2. Составное расширение поля

До сих пор мы присоединяли лишь по одному элементу. Перейдем к естественному обобщению простого расширения поля.

**Определение 4.10.** Пусть поле  $F$  является расширением поля  $P$  и  $\alpha_1, \alpha_2, \dots, \alpha_n \in F$ . Составным расширением поля  $P$  с помощью присоединения элементов  $M = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$  называется поле, которое получается из элементов поля  $P$  и элементов множества  $M$  с помощью операций сложения, вычитания, умножения и деления.

Обозначение:  $P(\alpha_1, \alpha_2, \dots, \alpha_n)$ . Если присоединяемые элементы алгебраические, то говорят о составном алгебраическом расширении поля.

**Теорема 4.7.** Составное алгебраическое расширение поля можно получить с помощью ряда повторных расширений.

*Доказательство.* Пусть  $\alpha_1, \alpha_2, \dots, \alpha_n$  — алгебраические элементы над полем  $P$ . Докажем, что  $P(\alpha_1, \alpha_2, \dots, \alpha_n) = P(\alpha_1)(\alpha_2)\dots(\alpha_n)$ . Поскольку  $P \subseteq P(\alpha_1)(\alpha_2)\dots(\alpha_n)$ ,  $\alpha_1, \alpha_2, \dots, \alpha_n \in P(\alpha_1)(\alpha_2)\dots(\alpha_n)$ , то  $P(\alpha_1, \alpha_2, \dots, \alpha_n) \subseteq P(\alpha_1)(\alpha_2)\dots(\alpha_n)$ .

Обратное включение докажем индукцией по  $n$ . При  $n = 1$  утверждение очевидно. Пусть уже доказано, что  $F_1 = P(\alpha_1)(\alpha_2)\dots(\alpha_{n-1}) \subseteq P(\alpha_1, \alpha_2, \dots, \alpha_{n-1})$ , докажем, что  $F_2 = P(\alpha_1)(\alpha_2)\dots(\alpha_n) \subseteq P(\alpha_1, \alpha_2, \dots, \alpha_n)$ . По теореме о строении простого алгебраического расширения, всякий элемент  $\beta \in F_2 = F_1(\alpha_n)$  является линейной комбинацией степеней элемента  $\alpha_n$  с коэффициентами из поля  $F_1$ . По индуктивному предположению,  $F_1 \subseteq P(\alpha_1, \alpha_2, \dots, \alpha_{n-1}) \subseteq P(\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \alpha_n)$ . Следовательно,  $F_2 = F_1(\alpha_n) \subseteq P(\alpha_1, \alpha_2, \dots, \alpha_n)$ . Таким образом,  $P(\alpha_1, \alpha_2, \dots, \alpha_n) = P(\alpha_1)(\alpha_2)\dots(\alpha_n)$ . Теорема доказана.

Рассмотрим составные расширения числовых полей. Начнем с примера.

#### Пример 4.2

Докажем, что составное алгебраическое расширение  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  можно получить присоединением к  $\mathbb{Q}$  одного элемента  $\alpha = \sqrt{2} + \sqrt{3}$ . В самом деле, числа  $\sqrt{2}$  и  $\sqrt{3}$  можно получить в виде линейных комбинаций степеней  $1 = \alpha^0, \alpha, \alpha^2, \alpha^3$ . (Докажите!)

Следовательно,  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$ . Обратное включение очевидно. Элемент  $\alpha$  в этом случае называется *примитивным*.

Докажем существование такого элемента в значительно более общей ситуации.

**Теорема 4.8 (о примитивном элементе).** Составное алгебраическое расширение числового поля является простым.

*Доказательство.* Пусть  $P$  — числовое поле. Докажем, что составное алгебраическое расширение  $F = P(\alpha, \beta)$  является про-

стым, т.е. существует примитивный элемент  $\theta \in F$ , такой что  $P(\alpha, \beta) = P(\theta)$ . Пусть  $f(x)$  и  $g(x)$  — минимальные многочлены элементов соответственно  $\alpha$  и  $\beta$  над полем  $P$ . Пусть  $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_k$  — все различные корни многочлена  $f(x)$  и  $\beta_1 = \beta, \beta_2, \dots, \beta_m$  — все различные корни многочлена  $g(x)$ . Рассмотрим уравнения  $\alpha_i + x\beta_j = \alpha + x\beta$  для всех  $1 < i \leq k$  и  $1 < j \leq m$ . Предположим, что одно из этих уравнений имеет два различных корня  $c_1$  и  $c_2$ . Тогда  $\alpha_i + c_1\beta_j = \alpha + c_1\beta$  и  $\alpha_i + c_2\beta_j = \alpha + c_2\beta$ . Вычитая из первого равенства второе, получим  $(c_1 - c_2)\beta_j = (c_1 - c_2)\beta$ , откуда  $\beta_j = \beta = \beta_1$ , что противоречит условию. Следовательно, каждое из рассматриваемых уравнений имеет в  $P$  не более одного решения. Поскольку поле  $P$  бесконечно, то существует элемент  $c \in P$ , который не является корнем ни одного из данных уравнений. Обозначим  $\theta = \alpha + c\beta$  и докажем, что  $P(\alpha, \beta) = P(\theta)$ . Очевидно,  $P(\alpha, \beta) \supseteq P(\theta)$ .

Докажем обратное включение. Для элемента  $\beta$  имеем:  $g(\beta) = 0$  и  $f(\theta - c\beta) = f(\alpha) = 0$ . Следовательно,  $\beta$  является общим корнем многочленов  $g(x)$  и  $f(\theta - cx)$ , а значит,  $x - \beta$  является общим множителем этих многочленов. Но тогда  $\text{НОД}(g(x), f(\theta - cx)) = d(x) : (x - \beta)$ . Предположим, что кроме  $x - \beta$  в разложении многочлена  $d(x)$  на линейные множители существует множитель  $x - \beta_j$  при некотором  $j = 1, \dots, m$ . Тогда  $f(\theta - c\beta_j) = 0$ .

Следовательно, существует номер  $i$ , такой что  $\alpha_i = \theta - c\beta_j$ , откуда  $\alpha + c\beta = \theta = \alpha_i + c\beta_j$ . Если предположить, что  $\beta_j \neq \beta$ , то приходим к противоречию с выбором элемента  $c$ . Следовательно,  $\beta_j = \beta$  и  $\beta$  оказывается кратным корнем многочлена  $F$ . Но этот многочлен неприводим над полем  $P$ , а значит, взаимно прост со своей производной и не может иметь кратных корней. Таким образом,  $\text{НОД}(g(x), f(\theta - c\beta)) = x - \beta$ . Алгоритм Евклида для нахождения НОД двух многочленов показывает, что коэффициенты многочлена, являющегося НОД, принадлежат тому же полю, что и коэффициенты многочленов  $g(x)$  и  $f(\theta - cx)$ , т.е. полю  $P(\theta)$ . Следовательно,  $\beta \in P(\theta)$ . Но тогда  $\alpha \in P(\theta)$ . Таким образом, доказано включение  $P(\alpha, \beta) \subseteq P(\theta)$ , а вместе с тем и равенство  $P(\alpha, \beta) = P(\theta)$ .

Пусть теперь дано составное алгебраическое расширение  $F$  числового поля  $P$ . Тогда  $F = P(\alpha, \beta, \gamma, \dots, \delta)$  и, по доказанному,  $P(\alpha, \beta, \gamma, \dots, \delta) = P(\alpha, \beta)(\gamma, \dots, \delta) = P(\theta_1)(\gamma, \dots, \delta) = \dots = P(\theta_n)$ .

## Контрольные вопросы

1. Пусть  $\alpha$  и  $\beta$  — алгебраические над полем  $P$  элементы степени соответственно  $k$  и  $m$ . Верно ли, что  $|P(\alpha, \beta) : P| = km$ ?

2. Всякое ли конечное расширение поля является составным?
3. Всякое ли алгебраическое расширение поля является составным?
4. Пусть  $P = \mathbb{Q}(\alpha)$ ,  $F = P(\beta)$ .
  - а) Если расширения  $P$  и  $F$  конечны, то будет ли  $F$  конечным расширением поля  $\mathbb{Q}$ ? Простым?
  - б) Если  $\alpha$  и  $\beta$  — алгебраические числа, то будет ли  $F$  алгебраическим расширением поля  $\mathbb{Q}$ ?
5. Если  $\alpha$  и  $\beta$  — алгебраические элементы над полем  $P$ , то будет ли алгебраическим расширением  $P(\alpha, \beta)$ ? Будет ли оно конечным? Если при этом поле  $P$  конечно, то будет ли конечным поле  $P(\alpha, \beta)$ ?

## Задачи

1. Найдите  $|F : \mathbb{Q}|$ , если:
  - а)  $F = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ ; б)  $F = \mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$ ; в)  $F = \mathbb{Q}(i, \sqrt{5})$ ; г)  $F = \mathbb{Q}(\alpha, \beta)$ ,  $\alpha^3 - 3\alpha + 1 = 0$ ,  $\beta^2 + \beta + 1 = 0$ .
2. Пусть  $P = \mathbb{Q}(\alpha)$ ,  $F = P(\beta)$ ,  $|P : \mathbb{Q}| = 4$ ,  $|F : P| = 6$ . Найдите  $|F : \mathbb{Q}|$ ,  $|F : F|$ .
3. Пусть  $P = \mathbb{Q}(\sqrt[3]{2})$ ,  $F = P(\sqrt{3})$ . Выясните, принадлежит ли число  $\beta$  полю  $F$ , и если «да», то выразите его через базис расширения  $F$  поля  $\mathbb{Q}$ :
  - а)  $\beta = \frac{\sqrt[3]{2}}{\sqrt{3}+1}$ ; б)  $\beta = \frac{\sqrt{3}}{\sqrt[3]{4}+1}$ ; в)  $\beta = \frac{\sqrt[3]{4}+\sqrt{3}}{\sqrt[3]{4}-\sqrt[3]{2}+1}$ ; г)  $\beta = \frac{\sqrt[3]{6}-5}{\sqrt{3}+7}$ .
4. Найдите примитивный элемент расширения  $F$  поля  $\mathbb{Q}$ , если:
  - а)  $F = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ ; б)  $F = \mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$ ; в)  $F = \mathbb{Q}(i, \sqrt{5})$ .

## 4.5. Поле алгебраических чисел

Напомним, что алгебраическим числом называется число  $\alpha \in \mathbb{C}$ , которое является алгебраическим над полем  $\mathbb{Q}$ , т.е. является корнем некоторого многочлена с рациональными (а значит, и некоторого многочлена с целыми) коэффициентами. Обозначим через  $P_A$  множество всех алгебраических чисел и докажем его основные свойства.

**Теорема 4.9.** *Множество  $P_A$  всех алгебраических чисел относительно сложения и умножения образует поле.*

**Доказательство.** Пусть  $\alpha, \beta \in P_A$ . Поскольку  $\alpha$  и  $\beta$  являются алгебраическими над полем  $\mathbb{Q}$ , то расширения  $\mathbb{Q}(\alpha)$  и  $\mathbb{Q}(\beta)$  конечны. Но тогда составное расширение  $\mathbb{Q}(\alpha, \beta)$  является конечным, а значит, алгебраическим. Отсюда следует, что элементы  $\alpha \pm \beta$  и  $\alpha\beta^{-1}$  при  $\beta \neq 0$  являются алгебраическими, а значит, принадлежат множеству  $P_A$ . Тем самым доказано, что  $P_A$  является полем.

Напомним, что поле  $P$  называется алгебраически замкнутым, если всякий многочлен степени  $\geq 1$  с коэффициентами из этого поля имеет в нем по крайней мере один корень. Известно, что поле комплексных чисел алгебраически замкнуто (основная теорема алгебры).

**Теорема 4.10.** *Поле алгебраических чисел  $P_A$  алгебраически замкнуто.*

*Доказательство.* Рассмотрим многочлен  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in P_A[x]$  степени  $n \geq 1$ . По основной теореме алгебры этот многочлен имеет корень  $\alpha$ . Поскольку коэффициенты многочлена — алгебраические числа, то составное алгебраическое расширение  $P = \mathbb{Q}(a_n, a_{n-1}, \dots, a_1, a_0)$  конечно, а так как элемент  $\alpha$  алгебраический над  $P$ , то и расширение  $P(\alpha)$  конечно. Но тогда конечным является расширение  $\mathbb{Q}(a_n, a_{n-1}, \dots, a_1, a_0, \alpha)$ , а значит, оно является алгебраическим расширением поля  $\mathbb{Q}$ . Отсюда следует, что  $\alpha$  является алгебраическим числом, т.е.  $\alpha \in P_A$ . Следовательно, поле  $P_A$  алгебраически замкнуто. Теорема доказана.

**Теорема 4.11.** *Степень поля алгебраических чисел относительно поля рациональных чисел бесконечна:  $|P_A : \mathbb{Q}| = \infty$ .*

*Доказательство.* Предположим противное, пусть  $|P_A : \mathbb{Q}| = n$ . Рассмотрим многочлен  $x^m - 2$ , где  $m > n$ . Он неприводим над полем  $\mathbb{Q}$  (по критерию Эйзенштейна). Его корень  $\alpha$  является алгебраическим числом степени  $m$ . Следовательно, степени этого числа  $1, \alpha, \alpha^2, \dots, \alpha^{m-1}$  линейно независимы над полем  $\mathbb{Q}$  — пришли к противоречию, ибо по предположению размерность векторного пространства  $P_A$  над полем  $\mathbb{Q}$  равна  $n$ .

## Контрольные вопросы

1. Каковы степени неприводимых над полем алгебраических чисел многочленов?
2. Какими могут быть степени минимальных многочленов алгебраических чисел?
3. Пусть  $P_A$  — поле алгебраических чисел и многочлен  $f(x) \in P_A[x]$  имеет степень  $n$ . Сколько сомножителей в разложении данного многочлена на неприводимые над полем  $P_A$  множители?
4. Число  $\alpha$  является корнем многочлена  $x^3\sqrt{3} - x^2 + ix + 7$ . Чему может равняться степень расширения  $P_A(\alpha)$  поля алгебраических чисел  $P_A$ ?
5. Содержит ли мультипликативная группа поля алгебраических чисел элементы порядков 2, 3, 4, 5, бесконечного порядка, произвольного порядка?



6. Для всякого ли конечного расширения  $F$  поля  $\mathbb{Q}$  существует алгебраическое число, не принадлежащее  $F$ ?

7. Всякое ли конечное расширение поля  $\mathbb{Q}$  содержится в поле алгебраических чисел?

8. Верно ли, что сумма (произведение) двух корней двух многочленов с целыми коэффициентами сама является корнем некоторого многочлена с целыми коэффициентами?

9. Будут ли алгебраическими числа  $2 + i\sqrt{5}$ ,  $\frac{1-i}{2+\sqrt[3]{2}}$ ,  $2 - \pi i$ ,  $\sqrt[3]{2-\sqrt{3}}$ ,  $\sin 30^\circ$ ,  $\sin 60^\circ + \cos 30^\circ$ ?

10. Если число  $\alpha$  алгебраическое,  $f(x), g(x) \in \mathbb{Q}[x]$ ,  $g(\alpha) \neq 0$ , то будет ли алгебраическим число  $\frac{f(\alpha)}{g(\alpha)}$ ?

## Задачи

1. Пусть  $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$ . Найдите алгебраическое число, не принадлежащее  $\mathbb{Q}(\alpha)$ .

2. Известно, что число  $\alpha$  является корнем многочлена  $\varphi(x) \in \mathbb{Z}[x]$  и  $\beta \in \mathbb{Q}(\alpha)$ . Найдите минимальный многочлен алгебраического числа  $\beta$ , если: а)  $\varphi(x) = x^3 - 2x + 2$  и  $\beta = \alpha^2 + \alpha + 1$ ; б)  $\varphi(x) = x^3 - 2x + 2$  и  $\beta = \alpha^2 + \alpha + 1$ ; в)  $\varphi(x) = x^3 - 2x + 2$  и  $\beta = \alpha^2 + \alpha + 1$ .

3. Числа  $\alpha$  и  $\beta$  являются корнями многочленов, соответственно  $f(x) \in \mathbb{Z}[x]$  и  $g(x) \in \mathbb{Z}[x]$ . Найдите многочлен с целыми коэффициентами, имеющий корень  $\alpha + \beta$ , если: а)  $f(x) = x^2 - 2$ ,  $g(x) = x^2 - 3$ ; б)  $f(x) = x^3 - 2$ ,  $g(x) = x^2 - 3x + 1$ ; в)  $f(x) = x^3 - 3x - 1$ ,  $g(x) = x^2 + x + 1$ .

## 4.6. Квадратичные расширения полей

### 4.6.1. От геометрии к алгебре

Для перевода на алгебраический язык задач на построение циркулем и линейкой введем необходимые понятия.

**Определение 4.11.** Пусть поле  $F$  является расширением поля  $P$ ,  $\alpha \in P$  и поле  $F$  содержит корень многочлена  $x^2 - \alpha$ , который обозначим через  $\sqrt{\alpha}$ . Если  $\sqrt{\alpha} \notin P$ , то простое алгебраическое расширение  $P(\sqrt{\alpha})$  называется *простым квадратичным расширением* поля  $P$ .

**Определение 4.12.** Поле  $F$  называется *квадратичным расширением* поля  $P$ , если существует цепочка полей  $P = F_0 \subset F_1 \subset \dots \subset F_n = F$ , где каждое следующее поле является простым квадратичным расширением предыдущего, т.е. для любого  $i = 0, 1, \dots, n-1$  имеем  $\alpha_i \in F_i$ ,  $\sqrt{\alpha_i} \notin F_i$  и  $F_{i+1} = F_i(\sqrt{\alpha_i})$ .



Числовой прямой будем называть прямую с выбранной на ней точкой (начало координат), положительным направлением и единичным отрезком. Следующая лемма дает алгебраическое осмысление геометрической задачи на построение циркулем и линейкой.

**Лемма 4.1.** *На числовой прямой можно построить циркулем и линейкой точку, соответствующую действительному числу  $\alpha$ , тогда и только тогда, когда это число принадлежит некоторому квадратичному расширению поля рациональных чисел.*

*Доказательство.* ( $\Rightarrow$ ) Пусть число  $\alpha$  можно построить на числовой прямой циркулем и линейкой. Использование этих инструментов приводит к построению прямых и окружностей и нахождению их точек пересечения. Пользуясь аналитической геометрией, получаем уравнения первой и второй степеней и их системы. Решение систем таких уравнений приводит к числу  $\alpha$ , которое выражается через единицу с помощью операций  $+$ ,  $-$ ,  $\cdot$ ,  $:$  и  $\sqrt{\phantom{x}}$ . Но это и означает, что  $\alpha$  принадлежит некоторому квадратичному расширению  $F$  поля  $\mathbb{Q}$ .

( $\Leftarrow$ ) Пусть  $\alpha$  принадлежит квадратичному расширению  $F$  поля рациональных чисел. Это означает, что существует цепочка полей  $\mathbb{Q} = F_0 \subset F_1 \subset \dots \subset F_n = F$ , где каждое следующее поле является простым квадратичным расширением предыдущего, т.е. для любого  $i = 0, 1, \dots, n - 1$  имеем  $\alpha_i \in F_i$ ,  $\sqrt{\alpha_i} \notin F_i$  и  $F_{i+1} = F_i(\sqrt{\alpha_i})$ . Если дан единичный отрезок, то всякое рациональное число можно построить циркулем и линейкой. Пусть уже доказано, что всякий элемент поля  $F_i$  можно построить циркулем и линейкой. Поскольку  $F_{i+1} = F_i(\sqrt{\alpha_i})$ , то произвольный элемент  $\alpha_{i+1} \in F_{i+1}$  имеет вид  $\alpha_{i+1} = a + b\sqrt{\alpha_i}$  при некоторых  $a, b \in F_i$ . По предположению, элементы  $a, b$  и  $\alpha_i$  поля  $F_i$  можно построить циркулем и линейкой. Построение же элемента  $\alpha_{i+1}$  сводится к построению суммы, разности, произведения уже построенных элементов и извлечению квадратного корня — все это возможно циркулем и линейкой. Следовательно, элемент  $\alpha$ , принадлежащий  $F_n = F$ , можно построить циркулем и линейкой. Лемма доказана.

Аналогично можно доказать следующее более общее утверждение.

**Лемма 4.1'.** *На числовой прямой можно построить циркулем и линейкой точку, соответствующую действительному числу  $\alpha$ , имея отрезки длин  $p, q, \dots, r$ , тогда и только тогда, когда  $\alpha$  принадлежит некоторому квадратичному расширению поля  $P = \mathbb{Q}(p, q, \dots, r)$ .*

Следующие лемма и теоремы ведут к решению классических геометрических задач древности: об удвоении куба и о трисекции угла, о которых речь пойдет ниже.

**Лемма 4.2.** Пусть дан многочлен  $f(x) = x^3 + a_2x^2 + a_1x + a_0$  с рациональными коэффициентами. Если один из корней данного многочлена принадлежит квадратичному расширению поля  $\mathbb{Q}$ , то и все его корни принадлежат некоторому квадратичному расширению поля  $\mathbb{Q}$ .

*Доказательство.* Пусть корень  $x_1$  данного многочлена  $f(x)$  принадлежит некоторому квадратичному расширению поля  $\mathbb{Q}$ . Разделим  $f(x)$  на  $x - x_1$  по схеме Горнера:

|       | 1 | $a_2$       | $a_1$                  | $a_0$        |
|-------|---|-------------|------------------------|--------------|
| $x_1$ | 1 | $x_1 + a_2$ | $x_1^2 + a_2x_1 + a_1$ | $f(x_1) = 0$ |

Таким образом,  $f(x) = (x - x_1)(x^2 + (x_1 + a_2)x + x_1^2 + a_2x_1 + a_1)$ . Отсюда находим два других корня данного многочлена:

$$x_{2,3} = -\frac{x_1 + a_2}{2} \pm \sqrt{\frac{(x_1 + a_2)^2}{4} - (x_1^2 + a_2x_1 + a_1)}.$$

Поскольку  $x_1$  и рациональные числа  $a_1, a_2$  принадлежат квадратичному расширению поля  $\mathbb{Q}$ , то и корни  $x_2, x_3$  принадлежат некоторому квадратичному расширению поля  $\mathbb{Q}$ . Лемма доказана.

**Теорема 4.12.** Корни многочлена  $f(x) = x^3 + a_2x^2 + a_1x + a_0$  с рациональными коэффициентами принадлежат некоторому квадратичному расширению поля рациональных чисел тогда и только тогда, когда этот многочлен имеет рациональный корень.

*Доказательство.* ( $\Rightarrow$ ) Пусть корни данного многочлена  $f(x)$  принадлежат некоторому квадратичному расширению  $F$  поля  $\mathbb{Q}$ . Докажем, что  $f(x)$  имеет рациональный корень. Предположим противное: пусть данный многочлен  $f(x)$  не имеет рациональных корней. По определению 4.12, существует цепочка полей  $\mathbb{Q} = F_0 \subset F_1 \subset \dots \subset F_n = F$ , где каждое следующее поле является простым квадратичным расширением предыдущего. Пусть  $x_1, x_2, x_3$  — корни данного многочлена, которые, по условию, принадлежат полю  $F$ . Поскольку, по предположению, поле  $\mathbb{Q} = F_0$  не содержит ни одного корня многочлена  $f(x)$ , а поле  $F$  содержит все корни этого многочлена, то существует номер  $k$ , такой что поле  $F_k$  еще не содержит ни одного корня многочлена  $f(x)$ , а  $F_{k+1}$  уже содержит хотя бы один корень,

пусть это будет  $x_1$ . Напомним, что  $F_{k+1} = F_k(\sqrt{\alpha_k})$ , где  $\alpha_k \in F_k$ , но  $\sqrt{\alpha_k} \notin F_k$ . Поскольку  $x_1 \in F_{k+1}$ , то  $x_1 = a + b\sqrt{\alpha_k}$  при некоторых  $a, b \in F_k$ . Так как  $x_1$  является корнем многочлена  $f(x)$ , то  $f(x_1) = 0$ . Отсюда  $(a + b\sqrt{\alpha_k})^3 + a_2(a + b\sqrt{\alpha_k})^2 + a_1(a + b\sqrt{\alpha_k}) + a_0 = 0$ . Раскрывая скобки и группируя, получаем

$$(a^3 + a_2a^2 + a_1a + a_0 + 3ab^2\alpha_k + a_2b^2\alpha_k) + \\ + (3a^2b + b^3\alpha_k + 2a_2ab + a_1b)\sqrt{\alpha_k} = A + B\sqrt{\alpha_k} = 0.$$

Легко видеть, что при замене  $b$  на  $-b$  слагаемое  $A$  не изменяется, а коэффициент  $B$  преобразуется в  $-B$ . Следовательно,  $f(a - b\sqrt{\alpha_k}) = A - B\sqrt{\alpha_k} = 0$ . Таким образом,  $a - b\sqrt{\alpha_k}$  является корнем данного многочлена  $f(x)$ . Пусть  $x_2 = a - b\sqrt{\alpha_k}$ . По формулам Виета,  $x_1 + x_2 + x_3 = -a_2 \in \mathbb{Q} \subset F_k$ . Но

$$x_1 + x_2 = (a + b\sqrt{\alpha_k}) + (a - b\sqrt{\alpha_k}) = 2a \in F_k.$$

Следовательно,  $x_3 \in F_k$  вопреки нашему предположению. Полученное противоречие заставляет нас принять, что данный многочлен  $f(x)$  имеет по крайней мере один рациональный корень.

( $\Leftarrow$ ) Предположим теперь, что данный многочлен  $f(x) = x^3 + a_2x^2 + a_1x + a_0$  имеет рациональный корень  $x_1$ . Тогда по лемме 4.2 все корни многочлена  $f(x)$  принадлежат некоторому квадратичному расширению поля  $\mathbb{Q}$ . Теорема доказана.

**Теорема 4.13.** *Корень  $\alpha$  многочлена  $f(x) = x^3 + a_2x^2 + a_1x + a_0$  нельзя построить циркулем и линейкой на числовой прямой тогда и только тогда, когда многочлен  $f(x)$  не имеет рациональных корней.*

**Доказательство.** ( $\Rightarrow$ ) Пусть корень  $\alpha$  многочлена  $f(x) = x^3 + a_2x^2 + a_1x + a_0$  нельзя построить циркулем и линейкой, исходя из единичного отрезка. Если предположить, что многочлен  $f(x)$  имеет рациональный корень, то по теореме 4.12 все его корни принадлежат некоторому квадратичному расширению поля рациональных чисел, а значит, по лемме 4.1 могут быть построены циркулем и линейкой на числовой прямой, что противоречит условию.

( $\Leftarrow$ ) Пусть многочлен  $f(x)$  не имеет рациональных корней. Если предположить, что корень  $\alpha$  многочлена  $f(x)$  можно построить циркулем и линейкой, исходя из единичного отрезка, то по лемме 4.1  $\alpha$  принадлежит квадратичному расширению поля  $\mathbb{Q}$ . Но тогда по лемме 4.2 все корни данного многочлена принадлежат некоторому квадратичному расширению поля  $\mathbb{Q}$ . По теореме 4.12 отсюда следует, что  $f(x)$  должен иметь рациональный корень, что противоречит условию. Теорема доказана.

## 4.6.2. Неразрешимость некоторых задач на построение циркулем и линейкой

В данном подпараграфе рассмотрим решение классических геометрических задач древности.

### Задача об удвоении куба

Дан куб. Циркулем и линейкой построить ребро нового куба, объем которого вдвое больше объема данного куба.

*Решение.* Возьмем ребро данного куба за единицу, а ребро нового куба обозначим через  $a$ . Тогда  $a^3 = 2$ , откуда  $a^3 - 2 = 0$ . Следовательно,  $a$  является корнем многочлена  $x^3 - 2$ . Поскольку рациональные корни этого многочлена должны быть целыми и находиться среди делителей свободного члена, то заключаем, что данный многочлен не имеет рациональных корней. По теореме 4.13 отсюда следует, что отрезок длины  $a$  нельзя построить циркулем и линейкой.

### Исторический экскурс

Эта задача появилась в школе пифагорейцев около 540 г. до н.э. Легенда гласит, что, когда в Афинах разразилась чума, жители отправили делегацию на древнегреческий остров Делос и оракул местного храма известил волю богов: нужно удвоить жертвенник храма, имеющий форму куба. Эта задача не поддавалась решению классическими инструментами — циркулем и линейкой, и чума долго свирепствовала, унеся множество жизней. Благодаря легенде задачу стали называть «делосской».

### Задача о трисекции угла

Данный угол циркулем и линейкой разделить на три равные части.

*Решение.* Обозначим величину данного угла через  $\varphi$ . На рис. 4.1 данный угол  $\angle AOC = \varphi$ , а искомый угол  $\angle BOC = \varphi/3$ . Обозначим  $a = \cos \varphi$ ,  $b = \cos \varphi/3$ .

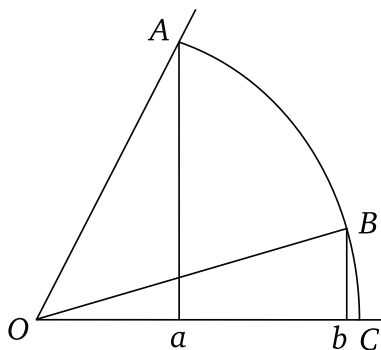


Рис. 4.1

Задача сводится к построению циркулем и линейкой по данному отрезку  $a$  искомого отрезка  $b$ . Найдем связь между ними. По формуле Муавра  $\left(\cos \frac{\varphi}{3} + i \sin \frac{\varphi}{3}\right)^3 = \cos \varphi + i \sin \varphi$ . С другой стороны,

$$\begin{aligned} \left(\cos \frac{\varphi}{3} + i \sin \frac{\varphi}{3}\right)^3 &= \left(\cos^3 \frac{\varphi}{3} - 3\cos \frac{\varphi}{3} \sin^2 \frac{\varphi}{3}\right) + \\ &+ i \left(-\sin^3 \frac{\varphi}{3} + 3\cos^2 \frac{\varphi}{3} \sin \frac{\varphi}{3}\right). \end{aligned}$$

Приравняем действительные части:

$$\begin{aligned} \cos \varphi &= \cos^3 \frac{\varphi}{3} - 3\cos \frac{\varphi}{3} \sin^2 \frac{\varphi}{3} = \\ &= \cos^3 \frac{\varphi}{3} - 3\cos \frac{\varphi}{3} \left(1 - \cos^2 \frac{\varphi}{3}\right) = 4\cos^3 \frac{\varphi}{3} - 3\cos \frac{\varphi}{3}, \end{aligned}$$

откуда  $4b^3 - 3b - a = 0$ . Следовательно, искомая величина  $b$  является корнем уравнения  $4x^3 - 3x - a = 0$ .

Возьмем конкретное значение  $\varphi = \frac{\pi}{3}$ . Тогда  $a = \cos \varphi = \cos \frac{\pi}{3} = \frac{1}{2}$  и уравнение принимает вид  $4x^3 - 3x - \frac{1}{2} = 0$ , откуда  $8x^3 - 6x - 1 = 0$ .

Таким образом,  $b$  является корнем многочлена  $8x^3 - 6x - 1$ . Вместе с тем этот многочлен, как легко видеть, не имеет рациональных корней. Это в соответствии с теоремой 4.13 говорит о том, что отрезок  $b$  в этом случае нельзя построить циркулем и линейкой, т.е. угол в  $60^\circ$  циркулем и линейкой нельзя разделить на три равные части. Отсюда делаем вывод о неразрешимости циркулем и линейкой задачи о трисекции угла.

## Задача о квадратуре круга

Циркулем и линейкой построить квадрат, площадь которого равна площади данного круга.

*Решение.* Пусть дан круг радиуса  $a$  и  $x$  — сторона искомого квадрата. По условию,  $x^2 = \pi a^2$ . При  $a = 1$  получаем уравнение  $x^2 = \pi$ . Но в 1882 г. К. Ф. Линдеман (1852—1901) доказал, что число  $\pi$  не является алгебраическим, а значит,  $x$  не может быть выражено через единицу с помощью арифметических операций и извлечения квадратного корня. Следовательно,  $\pi$ , а вместе с ним и  $x$ , не могут быть построены циркулем и линейкой. Это подвело черту под многочисленными попытками решить задачу.

В Мюнхенском университете перед математической аудиторией установлен бюст Карла Фердинанда Линдемана, и на постаменте изображен круг, пересеченный квадратом той же площади, внутри которого написана буква  $\pi$ .

## Задача о построении правильного семиугольника

Циркулем и линейкой построить правильный семиугольник.

*Решение.* Эта задача сводится к делению окружности на семь равных частей, т.е. к построению комплексных корней уравнения  $z^7 = 1$ , или  $z^7 - 1 = 0$ . Исключим корень  $\mathbb{Z}^7 = 1$ , или  $\mathbb{Z}^7 - 1 = 0$ . Исключим корень  $\mathbb{Z} = 1$ , который не надо строить. Разделив уравнение на  $\mathbb{Z} - 1$ , получим  $\mathbb{Z}^6 + \mathbb{Z}^5 + \mathbb{Z}^4 + \mathbb{Z}^3 + \mathbb{Z}^2 + \mathbb{Z} + 1 = 0$ . Разделим это уравнение на  $\mathbb{Z}^3$  и сгруппируем:

$$\left(z^3 + \frac{1}{z^3}\right) + \left(z^2 + \frac{1}{z^2}\right) + \left(z + \frac{1}{z}\right) = 0.$$

Введем новую переменную  $t = z + \frac{1}{z}$ . Тогда

$$t^2 = \left(z + \frac{1}{z}\right)^2 = z^2 + 2 + \frac{1}{z^2},$$

откуда  $z^2 + \frac{1}{z^2} = t^2 - 2$ . Аналогично

$$t^3 = \left(z + \frac{1}{z}\right)^3 = z^3 + 3z + 3\frac{1}{z} + \frac{1}{z^3} = \left(z^3 + \frac{1}{z^3}\right) + 3\left(z + \frac{1}{z}\right),$$

откуда  $z^3 + \frac{1}{z^3} = t^3 - 3t$ . Выполняя замену переменной, получаем уравнение  $t^3 + t^2 - 3t - 2 = 0$ . Многочлен  $t^3 + t^2 - 3t - 2$  не имеет рациональных корней. Отсюда по теореме 4.13 делаем вывод, что  $t$ , а вместе с ним и  $\mathbb{Z}$ , нельзя построить циркулем и линейкой.

Приведем без доказательства теорему, описывающую правильные многоугольники, которые можно построить циркулем и линейкой.

**Теорема 4.14 (Гаусса).** *Циркулем и линейкой можно построить правильный  $n$ -угольник тогда и только тогда, когда  $n = 2^m p_1 p_2 \cdots p_k$ , где  $m$  — целое неотрицательное число, а  $p_i$  — различные простые числа вида  $p_i = 2^{2^{\alpha_i}} + 1$ ,  $\alpha_i \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ ,  $i = 1, 2, \dots, k$ .*

В частности, циркулем и линейкой можно построить правильный 17-угольник — этому была посвящена первая публикация 19-летнего Гаусса, после чего он твердо решил посвятить себя не филологии, а исключительно математике.

## Задача о построении треугольника по биссектрисам

Циркулем и линейкой построить треугольник по данным его биссектрисам.

*Решение.* Рассмотрим частный случай общей задачи: циркулем и линейкой построить равнобедренный треугольник, описанный около единичной окружности, по данному отношению его биссектрис.

На рис. 4.2  $AF$  — одна из равных биссектрис и пусть длина биссектрисы  $BD = a$ . Обозначим  $\frac{BD}{AF} = k$ , тогда  $AF = \frac{a}{k}$ . Длину основания  $AC$  примем равной  $2b$ . Радиус вписанной окружности, по условию, равен единице. Из подобия треугольников  $ABD$  и  $OBE$  получаем  $\frac{BD}{AD} = \frac{BE}{OE}$ , откуда  $\frac{a}{b} = \frac{AB - AE}{1} = \sqrt{a^2 + b^2} - b$ . Следовательно,  $a = b(\sqrt{a^2 + b^2} - b)$ ,  $a + b^2 = b\sqrt{a^2 + b^2}$ ,  $a^2 + 2ab^2 + b^4 = b^2(a^2 + b^2) = a^2b^2 + b^4$ ,  $a^2 = a^2b^2 - 2ab^2 = ab^2(a - 2)$ , откуда  $b^2 = \frac{a}{a - 2}$ .

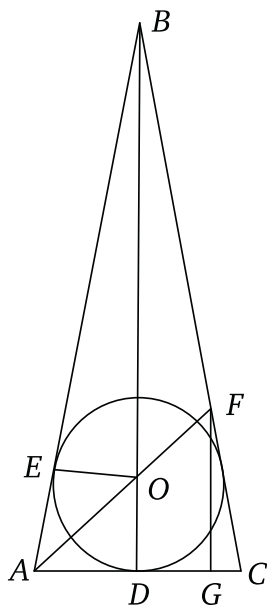


Рис. 4.2

Из прямоугольного треугольника  $AOD$  находим:  $AO = \sqrt{AD^2 + OD^2} = \sqrt{b^2 + 1}$ . Далее, из подобия треугольников  $AFG$  и  $AOD$  имеем  $\frac{AF}{FG} = \frac{AO}{OD}$ , откуда  $FG = \frac{AF \cdot OD}{AO} = \frac{a}{k\sqrt{b^2 + 1}}$ . Из прямоугольного треугольника  $AFG$  находим

$$\begin{aligned} AG &= \sqrt{AF^2 - FG^2} = \sqrt{\frac{a^2}{k^2} - \frac{a^2}{k^2(b^2 + 1)}} = \\ &= \frac{a}{k} \sqrt{1 - \frac{1}{b^2 + 1}} = \frac{ab}{k\sqrt{b^2 + 1}}. \end{aligned}$$



Из подобия треугольников  $CBD$  и  $CFG$  имеем  $\frac{CD}{BD} = \frac{CG}{FG}$ , откуда

$$CG = \frac{CD \cdot FG}{BD} = \frac{ab}{ak\sqrt{b^2+1}} = \frac{b}{k\sqrt{b^2+1}}.$$

Поскольку  $AG + GC = AC$ , то  $\frac{ab}{k\sqrt{b^2+1}} + \frac{b}{k\sqrt{b^2+1}} = 2b$ , откуда  $a+1 = 2k\sqrt{b^2+1}$ ,  $a^2 + 2a + 1 = 4k^2(b^2 + 1)$ . Подставляя сюда выражение  $b^2$  через  $a$ , получим

$$a^2 + 2a + 1 = 4k^2 \left( \frac{a}{a-2} + 1 \right) = 4k^2 \frac{2a-2}{a-2}.$$

После упрощения получаем  $a^3 - (8k^2 + 3)a + 8k^2 - 2 = 0$ . Следовательно,  $a$  является корнем уравнения  $x^3 - (8k^2 + 3)x + 8k^2 - 2 = 0$ . При  $k = 2$  получаем уравнение  $x^3 - 35x + 30 = 0$ . Оно не имеет рациональных корней, а значит, поставленная частная задача и вместе с ней общая задача не разрешимы циркулем и линейкой.

#### 4.6.3\*. Разрешимость уравнений в радикалах

Понятие квадратичного расширения поля появилось у нас как инструмент для установления неразрешимости некоторых задач на построение циркулем и линейкой. Вместе с тем это понятие можно связать с решением уравнений в квадратных радикалах в смысле следующего определения.

**Определение 4.13.** Пусть дан многочлен  $f(x)$  с коэффициентами из некоторого поля  $P$ . Говорят, что уравнение  $f(x) = 0$  разрешимо в квадратных радикалах, если его корни выражаются через коэффициенты с помощью конечного числа операций  $+$ ,  $-$ ,  $\cdot$ ,  $:$  и  $\sqrt{\phantom{x}}$ .

Например, всякое квадратное уравнение разрешимо в квадратных радикалах.

Ясно, что уравнение  $f(x) = 0$  разрешимо в квадратных радикалах тогда и только тогда, когда его корни принадлежат некоторому квадратичному расширению поля коэффициентов  $P$ . Это позволяет теорему 4.12 переформулировать следующим образом.

**Теорема 4.12'.** Уравнение  $x^3 + a_2x^2 + a_1x + a_0 = 0$  с рациональными коэффициентами разрешимо в квадратных радикалах тогда и только тогда, когда многочлен  $f(x) = x^3 + a_2x^2 + a_1x + a_0$  имеет рациональный корень.

Дадим естественное обобщение понятия разрешимости уравнения в квадратных радикалах.

**Определение 4.14.** Пусть дан многочлен  $f(x)$  с коэффициентами из некоторого поля  $P$ . Говорят, что уравнение  $f(x) = 0$  разрешимо в радикалах, если его корни выражаются через коэффициенты с помощью операций  $+$ ,  $-$ ,  $\cdot$ ,  $:$  и операций извлечения корней любой степени.

### Исторический экскурс

Проблема разрешимости уравнений в радикалах являлась предметом исследований с давних времен, пожалуй, с момента появления известных ныне каждому школьнику формул корней квадратного уравнения. Труды итальянских математиков дель Ферро, Тарталья и Кардано были найдены формулы для решения уравнений третьей степени (известная ныне формула Кардано). Ученик Кардано Феррари показал, как решение уравнения четвертой степени сводится к решению уравнения третьей степени. На уравнении пятой степени проблема застопорилась. Заметим, что основная теорема алгебры устанавливает существование комплексного корня любого многочлена с комплексными коэффициентами. Но выражается ли этот корень через коэффициенты с помощью арифметических операций и операций извлечения корней? Проблема о разрешимости уравнений в радикалах оставалась открытой вплоть до 1824 г. когда 22-летний норвежский математик Н. Х. Абель установил, что уравнения пятой степени и выше не разрешимы в радикалах. Замечательный французский математик Э. Галуа установил критерий разрешимости уравнения в радикалах, о чем поведал миру накануне роковой дуэли, унесшей жизнь молодого гения, когда ему исполнился 21 год. Его идеи легли в основу целого направления в алгебре, известного ныне как теория Галуа.

### Контрольные вопросы

1. Пусть  $F$  — квадратичное расширение поля  $P$ , а  $G$  — квадратичное расширение поля  $F$ . Будет ли  $G$  квадратичным расширением поля  $P$ ?
2. Может ли квадратичное расширение поля  $P$  содержать трансцендентный над полем  $P$  элемент?
3. Существует ли квадратичное расширение поля действительных чисел? Поля комплексных чисел?
4. Пусть  $F = P(\sqrt{\alpha})$  — простое квадратичное расширение поля  $P$ . Каков общий вид элементов поля  $F$ ? Существует ли элемент  $\beta \neq \sqrt{\alpha}$ , такой что  $F = P(\beta)$ ? Существует ли «промежуточное» поле  $P_1$ , такое что  $P \subset P_1 \subset F$ ?
5. Пусть  $F = \mathbb{Q}(\sqrt{3})$ . Как построить циркулем и линейкой произвольный элемент поля  $F$ ?

6. Пусть  $F = \mathbb{Q}(\sqrt{3})$ . Изобразим элемент  $\alpha = a + b\sqrt{3} \in F$  точкой плоскости с координатами  $(a, b)$ . Принадлежит ли полю  $F$  элемент, симметричный  $\alpha$  относительно оси  $Ox$ ? Оси  $Oy$ ? Начала координат? Биссектрис координатных углов?

7. Будет ли квадратичным расширением  $\mathbb{Q}(\alpha)$ , если: а)  $\alpha = 2 + 3i\sqrt{5}$ ; б)  $\alpha = 2 + 3i - \frac{7+2i}{1+\sqrt{3}}$ ; в)  $\alpha = 3 + 2i\sqrt[3]{2}$ ?

8. Является ли квадратичным расширением составное алгебраическое расширение  $F = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ ?

9. Разрешимы ли в квадратных радикалах уравнения  $x^2 - 1$ ,  $x^3 - 1$ ,  $x^4 - 1$ ?

## Задачи

1. Циркулем и линейкой постройте корни многочленов  $x^2 - 1$ ,  $x^3 - 1$ ,  $x^4 - 1$ ,  $x^6 - 1$ .

2. Определите, можно ли построить циркулем и линейкой корни данных уравнений: а)  $x^6 - 1 = 0$ ; б)  $x^7 - 1$ ; в)  $x^8 - 1$ ; г)  $x^{10} - 1$ ; д)  $x^3 - 113x - 113$ ; е)  $x^3 - 3x^2 + 5$ .

3. Докажите невозможность построения циркулем и линейкой правильного девятиугольника.

4. Докажите, что уравнение  $x^5 - 1 = 0$  разрешимо в квадратных радикалах.

5. Определите, разрешимо ли в квадратных радикалах уравнение  $x^7 - 1 = 0$ .

6. Докажите, что корни уравнения  $x^6 + x^3 + 1 = 0$  нельзя построить циркулем и линейкой.

7. Докажите, что если алгебраическое число  $\alpha$  можно построить циркулем и линейкой, имея единичный отрезок, то степень его минимального многочлена равна  $2^n$  при некотором целом неотрицательном  $n$ .

8. По единичному отрезку циркулем и линейкой постройте числа: а)  $2 + \sqrt{2 + \sqrt{2}}$ ; б)  $\frac{2 + \sqrt{3}}{1 - \sqrt{2}}$ ; в)  $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$ .

9. Определите, можно ли циркулем и линейкой построить ребро квадратной пластины, если ее площадь, будучи сложенной с утроенной длиной стороны квадрата, равна площади данного квадрата.

10. Определите, можно ли циркулем и линейкой разделить на три равные части углы  $45^\circ$ ,  $30^\circ$ ,  $120^\circ$ ,  $90^\circ$ .

## 4.7. Конечные поля

### 4.7.1. Число элементов конечного поля

Конечные поля по имени своего первооткрывателя Э. Галуа называются *полями Галуа*.

**Теорема 4.15.** Конечное поле  $F$  характеристики  $p$  содержит  $q = p^n$  элементов, где  $n$  есть степень расширения  $F$  относительно простого подполя  $P$ .

*Доказательство.* Пусть  $|F : P| = n$ . Это значит, что векторное пространство  $F$  над полем  $P$  имеет базис из  $n$  элементов:  $\{b_1, b_2, \dots, b_n\}$ . Но тогда всякий элемент  $a \in F$  однозначно представим в виде линейной комбинации базисных элементов:  $a = \alpha_1 b_1 + \alpha_2 b_2 + \dots + \alpha_n b_n$ , причем каждый коэффициент  $\alpha_i$ ,  $i = 1, 2, \dots, n$ , может принимать  $p$  различных значений. Отсюда следует, что число таких линейных комбинаций равно  $q = p^n$ . Теорема доказана.

В силу доказанной теоремы поле Галуа обозначается  $GF(p^n)$  или  $GF(q)$ . Корректность этого определения вытекает из того, что, как будет показано ниже, конечное поле однозначно с точностью до изоморфизма определяется числом его элементов  $q = p^n$ .

#### 4.7.2\*. Мультипликативная группа конечного поля

Рассматривая поля классов вычетов по простому модулю, убеждаемся, что в них мультипликативная группа поля циклическая. Докажем, что это верно для любого конечного поля.

**Теорема 4.16.** Мультипликативная группа конечного поля циклическая.

*Доказательство.* Пусть  $P$  — конечное поле и  $G = P^* — его мультипликативная группа. По теореме 1.25 она равна прямому произведению своих максимальных  $p$ -подгрупп по различным простым. Пусть  $S$  — одна из максимальных  $p$ -подгрупп группы  $G$ . Выберем в ней элемент максимального порядка. Пусть  $|a| = p^\alpha$ . Тогда для любого элемента  $s \in S$  имеем  $s^{p^\alpha} = 1$ , откуда  $s^{p^\alpha} - 1 = 0$ . Следовательно, всякий элемент из  $S$  является корнем многочлена  $x^{p^\alpha} - 1$ . Очевидно,  $a^0, a, a^2, \dots, a^{p^\alpha-1}$  — различные корни этого многочлена. Но многочлен степени  $p^\alpha$  имеет не более чем  $p^\alpha$  различных корней. Следовательно, перечисленными степенями элемента исчерпываются все корни многочлена  $x^{p^\alpha} - 1$ . Отсюда следует, что группа циклическая:  $S = \langle a \rangle$ . Итак, группа  $G$  является прямым произведением максимальных  $p$ -подгрупп, каждая из которых циклическая. Следовательно,  $G$  является прямым произведением циклических подгрупп взаимно простых порядков. По теореме 1.24 группа циклическая. Теорема доказана.$

Установим ряд интересных и важных свойств элементов конечного поля, которые приведут нас к одному утверждению в теории чисел.

**Теорема 4.17.** Элементы конечного поля  $P = GF(q)$  являются корнями многочлена  $x^q - x$ .

*Доказательство.* Порядок мультипликативной группы  $P^*$  данного поля  $P$  равен  $q - 1$ , следовательно, для любого ее элемента  $g$  имеем  $g^{q-1} = e$ , где  $e$  — единичный элемент поля. Отсюда следует, что всякий элемент поля является корнем многочлена  $x^q - x$ . Теорема доказана.

**Теорема 4.18.** Произведение всех ненулевых элементов конечного поля равно  $-e$ , где  $e$  — единичный элемент поля.

*Доказательство.* Пусть дано конечное поле  $P = GF(q)$ . Тогда порядок мультипликативной группы поля равен  $|P^*| = q - 1$ .

Пусть  $P^* = \{a_1, a_2, \dots, a_{q-1}\}$ . Многочлен  $(x^{q-1} - e) - \prod_{i=1}^{q-1} (x - a_i)$  имеет

$q - 1$  различных корней, а его степень меньше  $q - 1$ . Следовательно, это нулевой многочлен. В частности, его свободный

член равен нулю:  $-e - (-1)^{q-1} \prod_{i=1}^{q-1} a_i = 0$ . Если характеристика  $p$

данного поля нечетна, то число  $q - 1 = p^n - 1$  четно и  $(-1)^{q-1} = 1$ .

Но тогда  $-e - \prod_{i=1}^{q-1} a_i = 0$ , откуда  $\prod_{i=1}^{q-1} a_i = -e$ . Если же характеристика

поля  $p = 2$ , то имеем  $e = -e$ , откуда снова получаем  $\prod_{i=1}^{q-1} a_i = -e$ .

Теорема доказана.

**Следствие (теорема Вильсона).** Если натуральное число  $p$  является простым, то  $(p - 1)! \equiv -1 \pmod{p}$ .

*Доказательство.* Множество всех ненулевых элементов поля  $P = \mathbb{Z}_p$  исчерпывается классами вычетов  $\{\overline{1}, \overline{2}, \dots, \overline{p-1}\}$ , и по теореме 4,  $\overline{1} \cdot \overline{2} \cdot \dots \cdot \overline{p-1} = \overline{-1}$ , откуда  $(p-1)! = \overline{-1}$ , что равносильно сравнению  $(p - 1)! \equiv -1 \pmod{p}$ . (Другое доказательство см. в работе [3].)

## Контрольные вопросы

1. Существуют ли простые поля, состоящие из 4, 5, 6 элементов?
2. Может ли поле содержать 18 элементов?
3. Существует ли в конечном поле подмножество, образующее относительно умножения нециклическую подгруппу?
4. Чему равно произведение квадратов всех ненулевых элементов конечного поля?
5. Каковы корни многочлена  $x^{q-1} - \overline{1}$  в поле из  $q$  элементов?

## Задачи

1. Выпишите все элементы каждого из простых полей характеристики  $p < 10$ . Найдите аддитивный и мультипликативный порядок каждого элемента, убедитесь, что мультипликативные группы этих полей циклические.

2. Рассмотрите кольцо многочленов  $\mathbb{Z}_2[x]$  и в нем многочлен  $x^2 + x + \bar{1}$ . Установите его неприводимость. Обозначив корень многочлена через  $\alpha$ , выпишите элементы поля  $F = \mathbb{Z}_2(\alpha)$ . Убедитесь, что  $|(\mathbb{Z}_2(\alpha))^*| = 3$ .

3. Докажите неприводимость над полем  $\mathbb{Z}_2$  многочлена  $x^3 + x + \bar{1}$ . Обозначив его корень через  $\alpha$ , выпишите все элементы поля  $\mathbb{Z}_2(\alpha)$ . Выясните строение мультипликативной группы этого поля. По аналогии постройте расширение  $\mathbb{Z}_3[\beta]$ , где  $\beta$  — корень многочлена  $x^2 + \bar{1} \in \mathbb{Z}_3[x]$ . Опишите строение мультипликативной группы этого поля.

4. Рассмотрим поле  $F = \mathbb{Z}_2(\alpha)$  из задачи 2, кольцо многочленов  $F[\mathbb{Z}]$  и в нем многочлен  $z^2 + \alpha z + \bar{1}$ . Докажите, что он неприводим над полем  $F$ . Обозначив корень этого многочлена через  $\beta$ , рассмотрите поле  $F_1 = F(\beta) = \mathbb{Z}_2(\alpha)(\beta)$ . Выпишите все его элементы и опишите мультипликативную группу этого поля. Докажите, что элемент  $\gamma = \alpha\beta$  имеет порядок 15 и порождает мультипликативную группу поля  $F_1$ . Найдите минимальный многочлен этого элемента над полем  $\mathbb{Z}_2$ , базис расширения  $F_1 = \mathbb{Z}_2(\gamma)$  и представление всякого элемента поля в этом базисе. Для каждого элемента поля  $F_1$  найдите его минимальный многочлен относительно поля  $\mathbb{Z}_2$ .

## 4.8\*. Конечные тела

### 4.8.1. Предварительные сведения

Отказ от требования коммутативности умножения в определении поля порождает понятие, которое можно охарактеризовать как кольцо с делением. Однако прижился другой термин — тело.

**Определение 4.15.** *Телом* называется ненулевое кольцо с единицей, в котором всякий ненулевой элемент имеет обратный элемент.

Таким образом, тело есть алгебраическая система  $\langle T, +, \cdot \rangle$ , где система  $\langle T, + \rangle$  является коммутативной группой, система  $\langle T^*, \cdot \rangle$ , где  $T^* = T \setminus \{0\}$ , является группой (быть может, не коммутативной) и умножение дистрибутивно относительно сложения. Понятно, что коммутативное тело есть поле.

Существуют ли конечные некоммутативные тела? Оказывается, нет! Мы докажем этот удивительный результат, извест-



ный как теорема Веддербарна [3], следуя Витту [1]. Предварительно рассмотрим необходимый вспомогательный материал.

1. Напомним сведения из теории групп.

Пусть даны группа  $G$  и элемент  $a \in G$ . Тогда класс элементов, сопряженных с элементом  $a$ , есть  $K_a = \{g^{-1}ag \mid g \in G\}$ . Группа  $G$  распадается на непересекающиеся классы сопряженных элементов:  $G = \bigcup_{a \in G} K_a$ ,  $K_a \cap K_b = \emptyset$  при  $K_a \neq K_b$ .

Центром группы  $G$  называется множество всех элементов, перестановочных с каждым элементом данной группы. Обозначается  $C(G)$ .

Централизатором элемента  $a$  группы  $G$  называется множество всех элементов  $c \in G$ , которые перестановочны с элементом  $a$ . Обозначается  $C_G(a)$ . Таким образом,  $C_G(a) = \{c \in G \mid ac = ca\}$ . В соответствии с теоремой 1.14 количество элементов, сопряженных с элементом  $a$  группы  $G$ , равно индексу централизатора этого элемента (числу смежных классов группы  $G$  по централизатору  $C_G(a)$ ), т.е.  $|K_a| = |G : C_G(a)|$ .

2. Сведения из линейной алгебры.

**Лемма 4.3.** Если базис векторного пространства  $V$  над полем  $P$  содержит  $n$  векторов, а поле  $P$  содержит  $q$  элементов, то пространство  $V$  содержит  $q^n$  векторов.

*Доказательство.* Пусть система векторов  $\{a_1, a_2, \dots, a_n\}$  векторного пространства  $V$  над полем  $P$  является базисом. Тогда для любого вектора  $b \in V$  существует и единственный арифметический вектор  $(\alpha_1, \alpha_2, \dots, \alpha_n)$  с компонентами из поля  $P$ , такой что  $b = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n$ . Поскольку каждая компонента арифметического вектора  $(\alpha_1, \alpha_2, \dots, \alpha_n)$  может принимать  $q$  значений, то  $V$  содержит  $q^n$  векторов.

3. Одно свойство делимости натуральных чисел.

**Лемма 4.4.** Пусть даны натуральные числа  $n, m$  и  $q > 1$ . Если  $q^n - 1$  делится на  $q^m - 1$ , то  $n$  делится на  $m$ .

*Доказательство.* Разделим  $n$  на  $m$  с остатком:  $n = ms + r$ , где  $s \geq 0$ ,  $0 \leq r < m$ . По условию,

$$\left. \begin{array}{l} q^n - 1 : q^m - 1 \\ q^m - 1 : q^m - 1 \end{array} \right] \Rightarrow q^n - q^m = q^{ms+r} - q^m = \\ = q^m (q^{m(s-1)+r} - 1) : q^m - 1.$$

Так как  $\text{НОД}(q^m, q^m - 1) = 1$ , то  $(q^{m(s-1)+r} - 1) : (q^m - 1)$ . Повторяя эти рассуждения, приходим к выводу, что  $(q^r - 1) : (q^m - 1)$ , что возможно лишь в случае  $r = 0$ . Следовательно,  $n : m$ . Лемма доказана.



#### 4. Сведения о многочлене $x^n - 1$ .

Все корни многочлена  $x^n - 1$  образуют мультипликативную группу корней  $n$ -й степени из единицы. Из всех двучленов  $x - \lambda$ , где  $\lambda$  — корень  $n$ -й степени из единицы, имеющий порядок  $n$  в группе всех корней  $n$ -й степени из единицы, составим многочлен  $\varphi_n(x) = \prod_{\substack{\text{порядок } \lambda \\ \text{равен } n}} (x - \lambda)$ .

**Лемма 4.5.** *Многочлен  $\varphi_n(x)$  имеет целые коэффициенты, причем его свободный член равен либо 1, либо  $-1$ .*

*Доказательство.* Проведем доказательство индукцией по  $n$ . При  $n = 1$  имеем  $\varphi_1(x) = x - 1$ , и утверждение верно. Пусть оно верно для всех натуральных чисел, меньших  $n$ . В разложении многочлена  $x^n - 1$  на множители вида  $x - \lambda$ , где  $\lambda$  — корень  $n$ -й степени из единицы, выделим множители, составляющие многочлен  $\varphi_n(x)$ , и обозначим через  $p(x)$  произведение остальных линейных множителей указанного вида, где порядок корня  $\lambda$  меньше  $n$ . Тогда  $x^n - 1 = \varphi_n(x) \cdot p(x)$ . Из индуктивного предположения вытекает, что коэффициенты многочлена  $p(x)$  являются целыми и его свободный член равен 1 или  $-1$ . Пусть  $\varphi_n(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0$ ,  $p(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$ . Поскольку  $b_0 = \pm 1$  и  $a_0 b_0 = -1$ , то  $a_0 = \pm 1$ . Далее, так как  $a_1 b_0 + a_0 b_1 = 0$  и числа  $a_0, b_0, b_1$  целые, то  $a_1$  целое. Пусть уже доказано, что коэффициенты  $a_0, a_1, \dots, a_{t-1}$  целые для  $t < k$ . Поскольку  $a_t b_0 + a_{t-1} b_1 + \dots + a_0 b_t = 0$  и числа  $b_0, b_1, \dots, b_t$  целые, то и число  $a_t$  целое. Лемма доказана.

**Лемма 4.6.** *Если  $n > 1$ , то для любого натурального числа  $q > 1$  число  $q - 1$  не делится на  $\varphi_n(q)$ .*

*Доказательство.* Пусть  $\lambda = a + bi$ . Тогда  $a^2 + b^2 = 1$ , а так как  $\lambda \neq 1$ , то  $|a| < 1$ . Далее имеем:

$$\begin{aligned} |q - \lambda|^2 &= |q - a - bi|^2 = (q - a)^2 + b^2 = q^2 - 2aq + a^2 + b^2 = \\ &= q^2 - 2aq + 1 > q^2 - 2q + 1 = (q - 1)^2, \end{aligned}$$

откуда  $|q - \lambda| > q - 1 \geq 1$  для каждого сомножителя в произведении  $\varphi_n(q) = \prod_{\substack{\text{порядок } \lambda \\ \text{равен } n}} (q - \lambda)$ . Следовательно,  $q - 1$  не может

делиться на  $\varphi_n(q)$ . Лемма доказана.

#### 4.8.2. Основная теорема о конечном теле

Теперь мы можем приступить к доказательству основной теоремы, не отвлекаясь «по мелочам».

**Теорема 4.19 (Веддербарна).** Конечное тело является полем.

*Доказательство.* Пусть дано конечное тело  $T$ . Рассмотрим в нем множество  $C(T)$  всех элементов, перестановочных с каждым элементом из  $T$ :

$$C(T) = \{c \in T \mid ct = tc \ \forall t \in T\}.$$

Очевидно,  $C(T)$  является конечным полем. Пусть оно содержит  $q$  элементов. Рассмотрим  $T$  как векторное пространство над полем  $C(T)$ . Если его базис содержит  $n$  векторов, то  $T$  содержит  $q^n$  элементов (см. лемму 4.3).

Для каждого элемента  $a \in T$  обозначим через  $C_a(T)$  множество тех и только тех элементов, которые перестановочны с элементом  $a$  (централизатор элемента  $a$  в  $T$ ). Рассматривая  $C_a(T)$  как векторное пространство над полем  $C(T)$ , заключаем, что количество элементов  $C_a(T)$  равно  $q^{n_a}$  при некотором натуральном  $n_a$  (снова см. лемму 4.3).

Предположим, что тело  $T$  не коммутативно. Тогда  $C_a(T) \neq T$  для некоторого  $a \in T$  и, следовательно,  $q^{n_a} < q^n$ , откуда  $n_a < n$ .

Напомним, что  $T^*$  обозначает группу обратимых элементов тела  $T$ . Поскольку  $T^* = T \setminus \{0\}$ , то порядок группы  $T^*$  равен  $q^n - 1$ . Аналогично группа обратимых элементов  $(C_a(T))^*$  содержит  $q^{n_a} - 1$  элементов.

Для каждого элемента  $a$  группы  $T^*$  рассмотрим класс сопряженных элементов  $K_a = \{t^{-1}at \mid t \in T^*\}$ . Так как по предположению группа  $T^*$  не коммутативна, то существуют классы сопряженных элементов, содержащие более одного элемента, обозначим их  $K_{a_1}, K_{a_2}, \dots, K_{a_m}$ . По теореме 1.14 для любого  $i = 1, 2, \dots, m$  имеем  $|K_{a_i}| = |T^* : C_{a_i}|$ . По теореме Лагранжа (теорема 1.7)  $|T^*| = |C_{a_i}(T^*)| \cdot |T^* : C_{a_i}(T^*)| = |C_{a_i}(T^*)| \cdot |K_{a_i}|$ . Следовательно,  $|K_{a_i}| = \frac{|T^*|}{|C_{a_i}(T^*)|} = \frac{q^n - 1}{q^{n_{a_i}} - 1}$ . Поскольку  $q^n - 1 \div q^{n_{a_i}} - 1$ , то по лемме 4.4.  $n \div n_{a_i}$  для любого  $i = 1, 2, \dots, m$ .

Группа  $T^*$  состоит из элементов центра (их  $q - 1$  штук) и элементов, содержащихся в классах сопряженных элементов  $K_{a_1}, K_{a_2}, \dots, K_{a_m}$ , их количество равно  $|K_{a_1}| + |K_{a_2}| + \dots + |K_{a_m}| = \sum_{i=1}^m \frac{q^n - 1}{q^{n_{a_i}} - 1}$ . Таким образом,

$$q^n - 1 = q - 1 + \sum_{i=1}^m \frac{q^n - 1}{q^{n_{a_i}} - 1}. \quad (1)$$

Рассмотрим представление многочлена  $x^n - 1 = \prod (x - \lambda)$ , где  $\lambda$  пробегает все корни  $n$ -й степени из единицы. Сгруппируем линейные множители следующим образом:  $x^n - 1 = \prod_{n:d} \varphi_d(x)$ .

Напомним, что  $\varphi_d(x)$  есть произведение всех множителей вида  $x - \lambda$ , где  $\lambda$  есть корень  $d$ -й степени из единицы, имеющий порядок  $d$  в группе всех корней  $d$ -й степени из единицы. Зафиксируем номер  $i \in \{1, 2, \dots, m\}$  и, пользуясь тем, что  $n : n_{a_i}$ , выделим множитель  $x^{n_{a_i}} - 1$ :

$$x^n - 1 = \prod_{n:d} \varphi_d(x) = (x^{n_{a_i}} - 1) \cdot \varphi_n(x) \cdot \prod_{n:d, n_{a_i} \nmid d, d \neq n} \varphi_d(x).$$

При  $x = q$  получаем

$$q^n - 1 = (q^{n_{a_i}} - 1) \cdot \varphi_n(q) \cdot \prod_{n:d, n_{a_i} \nmid d, d \neq n} \varphi_d(q).$$

Поскольку по лемме 4.5 коэффициенты многочленов  $\varphi_k(x)$  целые при любом натуральном  $k$ , то получаем  $q^n - 1 : \varphi_n(q)$  и  $\frac{q^n - 1}{q^{n_{a_i}} - 1} : \varphi_n(q)$  для любого  $i$ . Из равенства (1) вытекает, что  $q - 1 : \varphi_n(q)$ . Но это противоречит лемме 4.6. Теорема доказана.

*Примечание.* Так как материал данного параграфа далеко выходит за рамки программы и адресован интересующимся магистрам и аспирантам, контрольные вопросы и задачи к нему не приводятся.

## 4.9\*. Алгебры над полями

### 4.9.1. Тело кватернионов

**Определение 4.16.** *Телом кватернионов* называется тело  $\langle H, +, \cdot \rangle$ , которое содержит поле действительных чисел  $\langle \mathbb{R}, +, \cdot \rangle$ , а также содержит так называемые мнимые единицы  $i, j, k$ , которые перестановочны с любым действительным числом и  $i^2 = j^2 = k^2 = ijk = -1$ , причем всякий элемент  $h \in H$  представим в виде  $h = a + bi + cj + dk$ , где  $a, b, c, d \in \mathbb{R}$ . Всякий элемент  $h \in H$  называется *кватернионом*, а его запись в указанной форме называется *алгебраической формой* кватерниона. При этом  $a$  называется *скалярной частью* кватерниона, а  $bi + cj + dk$  — его *векторной частью*. Если скалярная часть отсутствует ( $a = 0$ ), то кватернион называется *чисто векторным*.

Кватернионы ввел в 1848 г. В. Гамильтон, и в его честь тело кватернионов обозначается буквой  $H$ .

Пользуясь свойствами мнимых единиц из определения 4.16, легко вывести следующие правила умножения мнимых единиц:

$$ij = k, jk = i, ki = j, ji = -k, kj = -i, ik = -j.$$

Эти правила схематично изображены на рис. 4.3: произведение любых соседних мнимых единиц по стрелкам дает третью мнимую единицу, а против стрелок — третью мнимую единицу со знаком «минус». Легко видеть, что множество  $G = \{\pm 1, \pm i, \pm j, \pm k\}$  образует мультипликативную группу, она называется *группой кватернионов*.

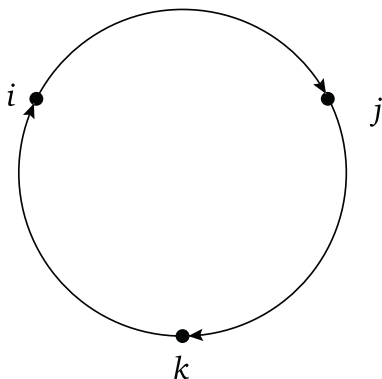


Рис. 4.3

Используя свойства кватернионов, зафиксированные в определении, легко вывести формулы сложения и умножения кватернионов:

$$\begin{aligned} & (a + bi + cj + dk) + (a_1 + b_1i + c_1j + d_1k) = \\ & = (a + a_1) + (b + b_1)i + (c + c_1)j + (d + d_1)k, \\ & (a + bi + cj + dk) \cdot (a_1 + b_1i + c_1j + d_1k) = \\ & = (aa_1 - bb_1 - cc_1 - dd_1) + (ab_1 + ba_1 + cd_1 - dc_1)i + \\ & + (ac_1 + ca_1 + db_1 - bd_1)j + (ad_1 + da_1 + bc_1 - cb_1)k. \end{aligned}$$

Заметим, что чисто векторный кватернион  $bi + cj + dk$  можно изобразить в виде вектора трехмерного векторного пространства с координатами  $(b, c, d)$ . При этом произведение чисто векторных кватернионов равно кватерниону, у которого скалярная часть противоположна скалярному произведению перемножаемых чисто векторных кватернионов, а векторная часть — их векторному произведению. Исторически из теории кватернионов появились термины «скалярное произведение» и «векторное произведение» векторов.

#### 4.9.2. Алгебры с делением конечного ранга над полем действительных чисел

Поле действительных чисел  $\langle \mathbb{R}, +, \cdot \rangle$ , поле комплексных чисел  $\langle \mathbb{C}, +, \cdot \rangle$  и тело кватернионов  $\langle H, +, \cdot \rangle$  являются векторными пространствами над полем действительных чисел. Общий взгляд на системы действительных, комплексных чисел и кватернионов порождает следующее определение.

**Определение 4.17.** Алгеброй с делением над полем  $P$  (в частности, над полем действительных чисел  $\mathbb{R}$ ) называется тело  $\langle A, +, \cdot \rangle$ , которое одновременно является векторным пространством над полем  $P$ , причем для любого скаляра  $a \in P$  и любых векторов  $\alpha, \beta \in A$   $(a\alpha) \cdot \beta = a(\alpha \cdot \beta) = \alpha \cdot (a\beta)$ . Размерность векторного пространства  $A$  над полем  $P$  (количество векторов базиса) называется рангом алгебры. Если ранг алгебры конечен, то она называется конечномерной.

Очевидно, поле действительных чисел, поле комплексных чисел и тело кватернионов являются конечномерными алгебрами с делением над полем действительных чисел соответственно рангов 1, 2 и 4 (их базисы, соответственно,  $\{1\}$ ,  $\{1, i\}$  и  $\{1, i, j, k\}$ ). Есть ли другие примеры? Отвечает на этот вопрос следующая теорема.

**Теорема 4.20 (Фробениуса).** Система  $\langle A, +, \cdot \rangle$  является алгеброй с делением конечного ранга над полем действительных чисел тогда и только тогда, когда она является либо полем действительных чисел, либо полем комплексных чисел, либо телом кватернионов.

*Доказательство.* Ввиду сказанного выше остается доказать, что если система  $\langle A, +, \cdot \rangle$  является алгеброй с делением конечного ранга над полем действительных чисел, то она является либо полем действительных чисел, либо полем комплексных чисел, либо телом кватернионов. Доказательство этого разобьем на ряд лемм.

**Лемма 4.7.** Алгебра с делением  $\langle A, +, \cdot \rangle$  над полем  $P$  содержит подполе, изоморфное полю  $P$ . С точностью до изоморфизма можно считать, что поле  $P$  содержится в  $A$ .

*Доказательство.* Пусть  $e$  — единица алгебры  $\langle A, +, \cdot \rangle$ . Очевидно, множество  $F = \{ae \mid a \in P\}$  является подполем в  $A$ . Для любого  $a \in P$  определим  $f(ae) = a$ . Легко доказать, что  $f$  является изоморфизмом подполя  $F$  на поле  $P$ . отождествляя элемент  $ae \in F$  с элементом  $a \in P$ , можно считать, что  $P \subseteq A$ . Лемма доказана.

**Следствие.** Если алгебра с делением  $\langle A, +, \cdot \rangle$  над полем  $\mathbb{R}$  имеет ранг 1, то она является полем действительных чисел.

*Доказательство.* По лемме 4.7  $\mathbb{R} \subseteq A$ , а так как ранг алгебры  $A$  равен 1, то линейно независимая над  $\mathbb{R}$  система  $\{1\}$  является базисом в  $A$ . Это значит, что для любого  $\alpha \in A$  существует число  $a \in \mathbb{R}$ , такое что  $\alpha = a1 = a \in \mathbb{R}$ . Следовательно,  $A = \mathbb{R}$ .

**Лемма 4.8.** *Всякий ненулевой элемент  $\alpha$  алгебры с делением  $\langle A, +, \cdot \rangle$  конечного ранга над полем  $P$  является корнем некоторого многочлена  $\varphi(x) \in P[x]$ , неприводимого над этим полем.*

*Доказательство.* Пусть ранг алгебры  $\langle A, +, \cdot \rangle$  равен  $n$ . Известно, что в  $n$ -мерном векторном пространстве всякие  $n + 1$  векторов линейно зависимы. Следовательно, для любого  $0 \neq \alpha \in A$  система векторов  $\{1 = \alpha^0, \alpha, \alpha^2, \dots, \alpha^n\}$  линейно зависима. Это значит, что существуют элементы поля  $a_0, a_1, a_2, \dots, a_n$ , среди которых есть элементы, отличные от нуля, такие что  $a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n = 0$ . Но это и означает, что  $\alpha$  является корнем многочлена  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in P[x]$ . Из всех многочленов с коэффициентами из  $P$ , имеющих корень  $\alpha$ , выберем тот, который имеет наименьшую степень, пусть это будет  $\varphi(x)$ . Тогда степень  $\varphi(x)$  не меньше 1. Предположим, что этот многочлен приводим над полем  $P$ , пусть  $\varphi(x) = \varphi_1(x) \cdot \varphi_2(x)$ , где  $\varphi_1(x), \varphi_2(x) \in P[x]$ , и степени сомножителей меньше степени многочлена  $\varphi(x)$ . Тогда  $\varphi_1(\alpha) \cdot \varphi_2(\alpha) = \varphi(\alpha) = 0$ , а так как тело не имеет делителей нуля, то  $\varphi_1(\alpha) = 0$  или  $\varphi_2(\alpha) = 0$ . Таким образом,  $\alpha$  является корнем одного из многочленов  $\varphi_1(x)$  или  $\varphi_2(x)$ , что противоречит минимальности степени многочлена  $\varphi(x)$ . Следовательно, многочлен  $\varphi(x)$  неприводим над полем  $P$ . Лемма доказана.

**Лемма 4.9.** *Алгебра с делением  $\langle A, +, \cdot \rangle$  над полем комплексных чисел  $\mathbb{C}$  изоморфна этому полю и с точностью до изоморфизма можно считать, что  $A = \mathbb{C}$ .*

*Доказательство.* По лемме 4.7 алгебра с делением  $\langle A, +, \cdot \rangle$  над полем  $\mathbb{C}$  содержит поле  $\mathbb{C}$ . По лемме 4.8 всякий ненулевой элемент  $\alpha \in A$  является корнем некоторого многочлена  $\varphi(x) \in \mathbb{C}[x]$ , неприводимого над полем  $\mathbb{C}$ . Известно, что неприводимыми над полем комплексных чисел являются лишь многочлены первой степени. Следовательно,  $\varphi(x) = ax + b$  при некоторых  $a, b \in \mathbb{C}$  и  $a \neq 0$ . Таким образом,  $a\alpha + b = \varphi(\alpha) = 0$ , откуда  $\alpha = -b/a \in \mathbb{C}$ . Следовательно,  $A = \mathbb{C}$ . Лемма доказана.

**Лемма 4.10.** *Если алгебра с делением  $\langle A, +, \cdot \rangle$  над полем  $\mathbb{R}$  имеет ранг  $n > 1$ , то она содержит подполе, изоморфное полю комплексных чисел  $\mathbb{C}$ , и с точностью до изоморфизма можно считать, что  $\mathbb{C} \subseteq A$ .*

*Доказательство.* По лемме 4.7 алгебра  $A$  содержит поле  $\mathbb{R}$ . Так как поле  $\mathbb{R}$  является одномерным векторным пространством



над полем  $\mathbb{R}$ , т.е. над самим собой (с базисом  $\{1\}$ ), а ранг  $A$  над полем  $\mathbb{R}$  равен  $n > 1$ , то  $A \neq \mathbb{R}$ . Пусть  $\alpha \in A \setminus \mathbb{R}$ . По лемме 4.8  $\alpha$  является корнем некоторого многочлена  $\varphi(x) \in \mathbb{R}[x]$ , неприводимого над полем  $\mathbb{R}$ . Известно, что неприводимыми над полем действительных чисел являются лишь многочлены первой степени и многочлены второй степени с отрицательными дискриминантами. Если предположить, что степень  $\varphi(x)$  равна единице и  $\varphi(x) = ax + b$ , где  $a, b \in \mathbb{R}$  и  $a \neq 0$ , то получаем  $a\alpha + b = \varphi(\alpha) = 0$ , откуда  $\alpha = b/a \in \mathbb{R}$ , что противоречит выбору элемента  $\alpha$ . Следовательно, степень  $\varphi(x)$  равна двум и  $\varphi(x) = ax^2 + bx + c$  при некоторых  $a, b, c \in \mathbb{R}$  и  $a \neq 0$ , причем дискриминант  $b^2 - 4ac < 0$ . Но тогда  $4ac - b^2 > 0$  и существует  $d \in \mathbb{R}$ , такое что  $d^2 = 4ac - b^2$ . Поскольку  $a\alpha^2 + b\alpha + c = \varphi(\alpha) = 0$ , то

$$\begin{aligned} 0 &= 4a^2\alpha^2 + 4ab\alpha + 4ac = \\ &= (2a\alpha + b)^2 + 4ac - b^2 = (2a\alpha + b)^2 + d^2 \end{aligned}$$

$$\text{и } \frac{(2a\alpha + b)^2}{d^2} = -1.$$

Обозначим  $i = \frac{2a\alpha + b}{d}$ , тогда  $i^2 = -1$ . Вместе с тем  $\mathbb{C} = \mathbb{R} + \mathbb{R}i = \{a + bi \mid a, b \in \mathbb{R}\}$  является полем комплексных чисел, содержащимся в  $A$ . Лемма доказана.

**Следствие.** Если алгебра с делением  $\langle A, +, \cdot \rangle$  над полем  $\mathbb{R}$  имеет ранг 2, то она является полем комплексных чисел.

**Доказательство.** По лемме 4.10  $\mathbb{C} \subseteq A$ . Система векторов  $\{1, i\}$  линейно независима над  $\mathbb{R}$ , а так как ранг  $A$  над полем  $\mathbb{R}$  по условию равен 2, то эта система является базисом в  $A$ . Следовательно, всякий элемент  $\alpha \in A$  является линейной комбинацией этих базисных векторов:  $\alpha = a \cdot 1 + b \cdot i$  для некоторых  $a, b \in \mathbb{R}$ . Таким образом,  $A = \mathbb{C}$ .

**Лемма 4.11.** Если алгебра с делением  $\langle A, +, \cdot \rangle$  над полем  $\mathbb{R}$  имеет ранг  $n > 2$ , то она является телом кватернионов.

**Доказательство.** По лемме 4.10  $\mathbb{C} \subseteq A$ , где  $\mathbb{C} = \mathbb{R} + \mathbb{R}i$ . Рассмотрим множества  $U = \{\alpha \in A \mid \alpha i = i\alpha\}$  и  $V = \{\beta \in A \mid \beta i = -i\beta\}$ . Легко видеть, что для любого  $\gamma \in A$  имеем  $\gamma - i\gamma i \in U$ , а  $\gamma + i\gamma i \in V$  и  $\gamma = \frac{1}{2}(\gamma - i\gamma i) + \frac{1}{2}(\gamma + i\gamma i) \in U + V$ . Следовательно,  $A = U + V$ .

Если предположить, что  $\delta \in U \cap V$ , то  $\delta \in U$ , откуда  $\delta i = i\delta$ , и  $\delta \in V$ , откуда  $\delta i = -i\delta$ . Следовательно,  $i\delta = -i\delta$ , откуда  $2i\delta = 0$ , а так как тело не содержит делителей нуля, то  $\delta = 0$ . Таким образом,  $U \cap V = \{0\}$ .



Выясним строение подмножеств  $U$  и  $V$ . Легко видеть, что  $U$  и  $V$  являются векторными пространствами над полем  $\mathbb{R}$ , причем  $U$  является алгеброй с делением над полем  $\mathbb{C}$  и по лемме 4.9  $U = \mathbb{C}$ .

По условию, ранг  $A$  равен  $n > 2$ , а так как ранг  $\mathbb{C}$  над полем  $\mathbb{R}$  равен двум, то  $V$  — ненулевое векторное пространство над полем  $\mathbb{R}$  и существует  $0 \neq \beta \in V$ . По лемме 4.8  $\beta$  является корнем некоторого многочлена  $\varphi(x) \in \mathbb{R}[x]$ , неприводимого над полем  $\mathbb{R}$ . Поскольку неприводимыми над полем  $\mathbb{R}$  являются лишь многочлены первой степени и второй степени с отрицательными дискриминантами, то степень  $\varphi(x)$  равна либо единице, либо двум. Рассмотрим оба случая.

В первом случае  $\varphi(x) = ax + b$ , где  $a, b \in \mathbb{R}$  и  $a \neq 0$ . Поскольку  $a\beta + b = \varphi(\beta) = 0$ , то  $\beta = -\frac{b}{a} \in \mathbb{R} \subseteq \mathbb{C} = U$ . Следовательно,  $\beta \in U \cap V = \{0\}$ , откуда  $\beta = 0$ , что противоречит предположению. Во втором случае  $\varphi(x) = ax^2 + bx + c$ , где  $a, b, c \in \mathbb{R}$ ,  $a \neq 0$  и дискриминант  $b^2 - 4ac < 0$ . Поскольку  $\beta$  — корень многочлена  $\varphi(x)$ , то  $0 = \varphi(\beta) = a\beta^2 + b\beta + c$ . Заметим, что  $\beta^2 \in U$ , и если предположить, что  $b \neq 0$ , то  $\beta = -\frac{a\beta^2 + c}{b} \in U$ .

С другой стороны,  $\beta^2 \in V$ . Следовательно,  $\beta \in U \cap V = \{0\}$ , откуда  $\beta = 0$ , что снова противоречит нашему предположению. Таким образом,  $b = 0$  и мы получаем  $a\beta^2 + c = 0$ , откуда  $\beta^2 = -\frac{c}{a}$ .

Так как дискриминант  $b^2 - 4ac < 0$ , то  $4ac > b^2 = 0$ , откуда  $\frac{c}{a} > 0$ .

Следовательно, существует  $d \in \mathbb{R}$ , такое что  $\frac{c}{a} = d^2$ . Таким образом,  $\beta^2 = -d^2$ , откуда  $\frac{\beta^2}{d^2} = -1$ . Обозначив  $j = \frac{\beta}{d}$ , получим  $j^2 = -1$ .

Докажем, что  $V = \mathbb{C}j$ . Так как  $j \in V$ , то  $(ij)i = i(ji) = i(-ij) = -i^2j = j$ ,  $i(ij) = i^2j = -j$ , откуда  $(ij)i = -i(ij)$ , значит,  $ij \in V$ . Но тогда для любого комплексного числа  $a + bi$  получаем  $(a + bi)j = aj + bij \in V$ . Таким образом,  $\mathbb{C}j \subset V$ . Обратно, для любого  $\beta \in V$  получаем  $(\beta j)i = \beta(ji) = \beta(-ij) = -(\beta i)j = -(-i\beta)j = i(\beta j)$ , откуда  $\beta j \in U = \mathbb{C}$  и, следовательно,  $\beta \in \mathbb{C}j$ . Таким образом,  $A = \mathbb{C} + \mathbb{C}j$ .

Обозначим  $k = ij$ . Легко проверить, что  $k^2 = ijk = -1$ . Всякий элемент  $h \in A$  представим в виде  $h = \mathbb{Z}_1 + \mathbb{Z}_2j$  при некоторых  $\mathbb{Z}_1, \mathbb{Z}_2 \in \mathbb{C}$ . Запишем эти комплексные числа в алгебраической форме:  $\mathbb{Z}_1 = a + bi$ ,  $\mathbb{Z}_2 = c + di$ . Тогда  $h = (a + bi) + (c + di)j = a + b + + cj + dij = a + bi + cj + dk$ . В этой записи мы узнаем кватернион. Следовательно, система  $\langle A, +, \cdot \rangle$  является телом кватернионов.

Вместе с тем теорема Фробениуса доказана.

Таким образом, можно сделать следующие выводы.

1. Поле действительных чисел — это единственная алгебра с делением над полем  $\mathbb{R}$  ранга 1.

2. Поле комплексных чисел — это единственная коммутативная и ассоциативная алгебра с делением над полем  $\mathbb{R}$  ранга  $n > 1$ .

3. Тело кватернионов — это единственная ассоциативная некоммутативная алгебра с делением над полем  $\mathbb{R}$  конечного ранга.

По поводу дальнейших расширений числовых множеств см. работу [6].

Заметим, что в соответствии с «Математической энциклопедией»<sup>1</sup> кольцом называется множество  $K$  с двумя бинарными операциями, которые называются сложением и умножением, причем  $K$  относительно сложения является абелевой группой, называемой аддитивной группой кольца, и умножение дистрибутивно относительно сложения:  $a(b + c) = ab + ac$  и  $(b + c)a = ba + ca$  для любых  $a, b, c \in K$ . В этом случае кольцо, определенное ранее, называется ассоциативным кольцом. Кольцом с делением называется кольцо  $K$  (необязательно ассоциативное), в котором для любых  $a, b \in K$ , где  $a \neq 0$ , разрешимы уравнения  $ax = b$  и  $ya = b$ . Если решения этих уравнений определены однозначно, то такое кольцо с делением называется квазителом.

## Контрольные вопросы

1. Существует ли алгебра с делением над полем  $\mathbb{R}$  ранга 3; ранга 5?
2. Каковы ранги алгебр  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $H$  над полем  $\mathbb{R}$ ?
3. Каковы размерности векторных пространств  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $H$  над полем  $\mathbb{Q}$ ?
4. Каковы размерности векторных пространств  $\mathbb{C}$ ,  $H$  над полем  $\mathbb{C}$ ?
5. Является ли кольцом тело кватернионов?

## Задачи

1. Составьте таблицу Кэли (таблицу умножения) для группы кватернионов  $G = \{\pm 1, \pm i, \pm j, \pm k\}$ .
2. Найдите порядок группы кватернионов и порядки всех ее элементов.

---

<sup>1</sup> Математическая энциклопедия. М. : Советская энциклопедия, 1979. С. 959.

3. Найдите все подгруппы группы кватернионов и выберите из них нормальные подгруппы.
4. Докажите, что свойства мнимых единиц, сформулированные в определении 4.16, эквивалентны правилам умножения мнимых единиц, представленным на рис. 4.3.
5. Выведите формулу нахождения обратного кватерниона.
6. Рассмотрите произведение чистых кватернионов и найдите скалярную и векторную части произведения. Объясните геометрический смысл полученного результата.
7. Выпишите несколько базисов векторного пространства кватернионов над полем действительных чисел.

# Литература

## Учебники, учебные пособия и монографии

1. Айгнер, М. Доказательства из Книги / М. Айгнер, Г. Циглер. — М. : Мир, 2006.
2. Белоусов, В. Д. Основы теории квазигрупп и луп / В. Д. Белоусов. — М. : Наука, 1967.
3. Бухштаб, А. А. Теория чисел : учеб. пособие / А. А. Бухштаб. — 2-е изд., испр. — М. : Просвещение, 1966.
4. Ван дер Варден, Б. Л. Алгебра / Б. Л. Ван дер Варден. — М. : Наука, 1976.
5. Винберг, Э. Б. Курс алгебры / Э. Б. Винберг. — М. : Факториал Пресс, 2002.
6. Глухов, М. М. Алгебра. Т. I, II / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. — М. : Гелиос АРВ, 2003.
7. Кантор, И. Л. Гиперкомплексные числа / И. Л. Кантор, А. С. Солодовников. — М. : Наука, 1973.
8. Каргаполов, М. И. Основы теории групп / М. И. Каргаполов, Ю. И. Мерзляков. — М. : Наука, 1982.
9. Кострикин, А. И. Основные структуры алгебры / А. И. Кострикин. — М. : Физматлит, 2001.
10. Кострикин, А. И. Основы алгебры / А. И. Кострикин. — М. : Физматлит, 2000.
11. Куликов, Л. Я. Алгебра и теория чисел / Л. Я. Куликов. — М. : Высшая школа, 1979.
12. Курош, А. Г. Курс высшей алгебры / А. Г. Курош. — М. : Высшая школа, 1979.
13. Курош, А. Г. Теория групп / А. Г. Курош. — М. : Наука, 1967.
14. Ляпин, Е. С. Полугруппы / Е. С. Ляпин. — М. : Физматлит, 1960.
15. Математическая энциклопедия. — М. : Советская энциклопедия, 1979.
16. Окунев, Л. Я. Высшая алгебра / Л. Я. Окунев. — М. : Просвещение, 1966.
17. Сушкевич, А. К. Основы высшей алгебры. — М. : Вузovская книга, 2017.

18. Холл, М. Теория групп / М. Холл. — М. : Иностранная литература, 1962.

19. Фаддеев, Д. К. Лекции по алгебре / Д. К. Фаддеев. — М. : Наука, 1984.

### Задачники

20. Куликов, Л. Я. Сборник задач по алгебре и теории чисел / Л. Я. Куликов, А. И. Москаленко, А. А. Фомин. — М. : Просвещение, 1993.

21. Ляпин, Е. С. Упражнения по теории групп / Е. С. Ляпин, А. Я. Айзенштат, М. М. Лесохин. — М. : Наука, 1967.

22. Солодовников, А. С. Задачник-практикум по алгебре / А. С. Солодовников, М. А. Родина. — М. : Просвещение, 1985.

23. Сборник задач по алгебре / под ред. А. И. Кострикина. — М. : Наука, 1987.

24. Фаддеев, Д. К. Сборник задач по высшей алгебре / Д. К. Фаддеев, И. С. Соминский. — М. : Наука, 1977.

## Новые издания по дисциплине «Высшая математика» и смежным дисциплинам

1. *Баврин, И. И.* Высшая математика для химиков, биологов и медиков : учебник и практикум для прикладного бакалавриата / И. И. Баврин. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017.

2. *Бекман, И. Н.* Высшая математика: математический аппарат диффузии : учебник для бакалавриата и магистратуры / И. Н. Бекман. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017.

3. *Богомолов, Н. В.* Математика. Задачи с решениями. В 2 ч : учеб. пособие для прикладного бакалавриата / Н. В. Богомолов. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2016.

4. *Бугров, Я. С.* Высшая математика. В 3 т. Т. 1. Дифференциальное и интегральное исчисление. В 2 кн. : учебник для академического бакалавриата / Я. С. Бугров, С. М. Никольский. — 7-е изд., стер. — М. : Издательство Юрайт, 2017.

5. *Бугров, Я. С.* Высшая математика. В 3 т. Т. 2. Элементы линейной алгебры и аналитической геометрии : учебник для академического бакалавриата / Я. С. Бугров, С. М. Никольский. — 7-е изд., стер. — М. : Издательство Юрайт, 2017.

6. *Бугров, Я. С.* Высшая математика. В 3 т. Т. 3. В 2 кн. Книга 1. Дифференциальные уравнения. Кратные интегралы : учебник для академического бакалавриата / Я. С. Бугров, С. М. Никольский. — 7-е изд., стер. — М. : Издательство Юрайт, 2016.

7. *Бугров, Я. С.* Высшая математика. В 3 т. Т. 3. В 2 кн. Книга 2. Ряды. Функции комплексного переменного : учебник для академического бакалавриата / Я. С. Бугров, С. М. Никольский. — 7-е изд., стер. — М. : Издательство Юрайт, 2016.

8. *Бугров, Я. С.* Высшая математика. Задачник : учеб. пособие для академического бакалавриата / Я. С. Бугров, С. М. Никольский. — М. : Издательство Юрайт, 2017.

9. Высшая математика : учебник и практикум для академического бакалавриата / М. Б. Хрипунова [и др.] ; под общ. ред. М. Б. Хрипуновой, И. И. Цыганок. — М. : Издательство Юрайт, 2017.

10. Высшая математика для экономического бакалавриата. В 3 ч. : учебник и практикум для академического бакалавриата / под ред. Н. Ш. Кремера. — 5-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017.

11. Гисин, В. Б. Математика. Практикум : учеб. пособие для бакалавриата и магистратуры / В. Б. Гисин, Н. Ш. Кремер. — М. : Издательство Юрайт, 2017.

12. Далингер, В. А. Информатика и математика. Решение уравнений и оптимизация в mathcad и maple : учебник и практикум для прикладного бакалавриата / В. А. Далингер, С. Д. Симонженков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017.

13. Дорофеева, А. В. Высшая математика : учебник для академического бакалавриата / А. В. Дорофеева. — 3-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017.

14. Дорофеева, А. В. Высшая математика. Сборник задач : учеб.-практ. пособие для академического бакалавриата / А. В. Дорофеева. — 2-е изд. — М. : Издательство Юрайт, 2017.

15. Кремер, Н. Ш. Высшая математика для экономического бакалавриата : учебник и практикум / Н. Ш. Кремер ; отв. ред. Н. Ш. Кремер. — 4-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017.

16. Ларин, С. В. Алгебра: многочлены : учеб. пособие для академического бакалавриата / С. В. Ларин. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017.

17. Ларин, С. В. Числовые системы : учеб. пособие для академического бакалавриата / С. В. Ларин. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017.

18. Мачулис, В. В. Высшая математика : учеб. пособие для вузов / В. В. Мачулис. — 5-е изд., перераб. и доп. — М. : Издательство Юрайт, 2016.

19. Павлюченко, Ю. В. Высшая математика для гуманитарных направлений : учебник и практикум для прикладного бакалавриата / Ю. В. Павлюченко, Н. Ш. Хассан ; под общ. ред. Ю. В. Павлюченко. — 4-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017.

20. Попов, А. М. Высшая математика для экономистов : учебник для бакалавров / А. М. Попов, В. Н. Сотников. — М. : Издательство Юрайт, 2017.



21. *Поспелов, А. С.* Сборник задач по высшей математике. В 4 ч. : учеб. пособие для прикладного бакалавриата / А. С. Поспелов ; под ред. А. С. Поспелова. — М. : Издательство Юрайт, 2017.

22. Сборник задач по высшей математике. Ч. 1 : учеб. пособие для прикладного бакалавриата / А. С. Поспелов [и др.] ; под ред. А. С. Поспелова. — М. : Издательство Юрайт, 2017.

23. *Сухотин, А. М.* Высшая математика. Альтернативная методология преподавания : учеб. пособие для прикладного бакалавриата / А. М. Сухотин, Т. В. Тарбокова. — М. : Издательство Юрайт, 2016.

24. *Фоменко, Т. Н.* Высшая математика. Общая алгебра. Элементы тензорной алгебры : учебник и практикум для академического бакалавриата / Т. Н. Фоменко. — М. : Издательство Юрайт, 2017.

25. *Шипачев, В. С.* Высшая математика : учебник и практикум / В. С. Шипачев. — 8-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017.

26. *Шипачев, В. С.* Высшая математика. Полный курс. В 2 т. : учебник для академического бакалавриата / В. С. Шипачев ; под ред. А. Н. Тихонова. — 4-е изд., испр. и доп. — М. : Издательство Юрайт, 2016.

## Предметный указатель

- Алгебраическая иррациональность 109
- Алгебраическая система 11
- Алгебра с делением 147
- Алгоритм Евклида 91
- Базис расширения 115
- Бинарная операция 11
- Вычитание (в кольце) 64
- Гомоморфизм 52, 72
- Группа 11
- $p$ -группа 58
  - абелева (коммутативная) 12
  - аддитивная 12
    - классов вычетов 40
    - кольца 63
    - целых комплексных (гауссовых) чисел 14
    - целых чисел, кратных целому неотрицательному числу 14
  - без кручения 23
  - бесконечная 12
  - вращений  $n$ -угольного диэдра 18
  - Клейна 55
  - конечная 12
  - мультипликативная 12
    - классов вычетов 42
    - кольца 63
    - корней  $n$ -й степени из единицы 15
    - обратимых квадратных матриц над полем  $\mathbb{R}$  19
    - типа  $p^\infty$  15
    - целых степеней двойки 15
    - периодическая 23
    - подстановок
      - знакопеременная 16
      - симметрическая 15
    - порожденная множеством  $M$  17
    - смешанная 23
    - циклическая 26
- Делитель
- единицы 80
  - наибольший общий 82
  - нуля 63
  - общий 82
  - элемента 80
- Дробь (отношение) 68
- Идеал 70
- главный 70
  - единичный 71
  - нулевой 71
  - порожденный элементами  $a_1, a_2, \dots, a_n$  70
- Изоморфизм 46, 72
- Индекс подгруппы в группе 35
- Класс вычетов 40
- Кольцо 62, 63
- главных идеалов 105
  - евклидово 90
  - квадратных матриц 63
  - классов вычетов 63
  - многочленов 63, 100
  - факториальное 86
  - целых комплексных чисел 63
- Кратное 80
- наименьшее общее 88
  - общее 88

Критерий  
   ассоциированности элемен-  
   тов 81  
   взаимно простых элементов  
   92  
   нормальной подгруппы 38  
   подгруппы 21  
   подкольца 69  
   подполя 70  
   прямого произведения 56  
 Многочлен минимальный  
 110  
 Норма элемента в евклидо-  
 вом кольце 90  
 Область целостности 78  
 Подгруппа  
   силовская  $p$ -подгруппа 58  
   собственная 21  
 Подгруппа группы 21  
   нормальная 37  
 Подкольцо 69  
 Подполе 69  
 Поле 66  
   алгебраических чисел 126  
   Галуа 138  
   классов вычетов по про-  
   стому модулю 67  
   отношений 79  
   простое 76  
 Порождающее подмножество  
 17  
 Порядок элемента группы 23  
 Прямое произведение под-  
 групп 56  
 Разложение  
   группы на смежные классы  
   по данной подгруппе 34  
   каноническое 89  
   на простые множители 86  
 Разрешимость  
   в квадратных радикалах 136  
   в радикалах 137  
 Расширение поля 109  
   алгебраическое 116  
   квадратичное 128  
   повторное 116  
     алгебраическое 123  
   простое 118  
     алгебраическое 118  
     квадратичное 128  
   трансцендентное 118  
   составное 124  
 Смежный класс по подгруппе  
 31  
 Степень  
   алгебраического над полем  
   элемента 111  
   расширения 115  
   элемента группы 20  
 Таблица Кэли 16  
 Теорема  
   Вильсона 140  
   Кэли 50  
   Лагранжа 35  
   о вложении области целост-  
   ности в поле 79  
   о гомоморфизмах для групп  
   53  
   о гомоморфизмах для колец  
   72  
   о линейной форме НОД 91  
   о примитивном элементе  
   124  
   основная теорема арифме-  
   тики 84  
   о строении простого алге-  
   браического расширения  
   поля 118  
   о строении простого транс-  
   цендентного расширения  
   поля 121  
   Фробениуса 147  
   Эйлера 42  
 Факторгруппа 40

Характеристика кольца  
(поля) 74  
Централизатор 43  
Центр группы 37  
Число  
    алгебраическое 109, 126  
    трансцендентное 109  
Элемент  
    алгебраический над полем  
    109  
    ассоциированный 81  
    единичный 19, 63  
    иррациональный 109

    нейтральный 11  
    обратимый 63  
    обратный 19, 63  
    примитивный 124  
    простой 84  
    симметричный 12  
    сопряженный 38  
    составной 84  
    трансцендентный над полем  
    109  
Элементы взаимно простые  
92  
Ядро гомоморфизма 52, 72