



М. М. Глухов, И. А. Круглов

ЭЛЕМЕНТЫ ТЕОРИИ ОБЫКНОВЕННЫХ ПРЕДСТАВЛЕНИЙ И ХАРАКТЕРОВ КОНЕЧНЫХ ГРУПП С ПРИЛОЖЕНИЯМИ В КРИПТОГРАФИИ

	ε	(12)(34)	(13)(24)	(14)(23)
$(\chi_1)_H$	1	1	1	1
$(\chi_2)_H$	1	1	1	1
$(\chi_3)_H$	1	1	1	1
$(\chi_4)_H$	3	-1	1	1

$$\varphi_1(g_1) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$$\varphi_1(g_2) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\begin{aligned}
 B_{k,l} &= \sum_{g \in G} \left(\sum_{\nu=1}^{m_l} \varphi_l(g)_{k,\nu} (A \varphi_l(g^{-1}))_{\nu,j} \right) = \sum_{g \in G} \left(\sum_{\nu=1}^{m_l} \varphi_l(g)_{k,\nu} \left(\sum_{\mu=1}^{m_l} A_{\nu,\mu} \varphi_l(g^{-1})_{\mu,j} \right) \right) \\
 &= \sum_{g \in G} \left(\sum_{\nu=1}^{m_l} \varphi_l(g)_{k,\nu} \left(\sum_{\mu=1}^{m_l} \delta_{\nu,\mu} \delta_{\mu,j} \varphi_l(g^{-1})_{\mu,j} \right) \right) = \sum_{g \in G} \left(\sum_{\nu=1}^{m_l} \varphi_l(g)_{k,\nu} \delta_{\nu,j} \left(\sum_{\mu=1}^{m_l} \varphi_l(g^{-1})_{\mu,j} \right) \right) \\
 &= \sum_{g \in G} \left(\sum_{\nu=1}^{m_l} \varphi_l(g)_{k,\nu} \delta_{\nu,j} \varphi_l(g^{-1})_{\nu,j} \right) = \sum_{g \in G} \varphi_l(g)_{k,j} \left(\sum_{\nu=1}^{m_l} \varphi_l(g^{-1})_{\nu,j} \varphi_l(g)_{\nu,j} \right) \\
 &= \sum_{g \in G} \varphi_l(g^{-1})_{j,j} \varphi_l(g)_{k,j} = \sum_{g \in G} \varphi_l(g)_{j,j} \varphi_l(g^{-1})_{k,j}
 \end{aligned}$$

М. М. ГЛУХОВ, И. А. КРУГЛОВ

ЭЛЕМЕНТЫ ТЕОРИИ ОБЫКНОВЕННЫХ ПРЕДСТАВЛЕНИЙ И ХАРАКТЕРОВ КОНЕЧНЫХ ГРУПП С ПРИЛОЖЕНИЯМИ В КРИПТОГРАФИИ

РЕКОМЕНДОВАНО

*УМО по образованию в области информационной безопасности
в качестве учебного пособия для аспирантов научных организаций
и образовательных организаций высшего образования,
обучающихся по направлению подготовки
«Информационная безопасность»*



• САНКТ-ПЕТЕРБУРГ •
• МОСКВА • КРАСНОДАР •
2022

ББК 21.131я73

Г 55

Глухов М. М., Круглов И. А.

Г 55 Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии: Учебное пособие. — СПб.: Издательство «Лань», 2022. — 176 с.: ил. — (Учебники для вузов. Специальная литература).

ISBN 978-5-8114-1855-8

Учебное пособие содержит минимально необходимые сведения по общей теории обыкновенных представлений и характеров групп, по теории представлений и характеров симметрических групп подстановок, а также о некоторых подходах в применениях теории представлений групп к решению криптографических задач.

Учебное пособие предназначено для студентов, обучающихся по направлению «Информационная безопасность», специалистов в области криптографии и защиты информации, может использоваться при чтении спецкурсов и при подготовке аспирантов к кандидатскому экзамену.

ББК 21.131я73

Рецензенты:

А. В. КОРОЛЬКОВ — кандидат технических наук, доцент, заведующий кафедрой БК-252 факультета кибернетики Московского государственного института радиотехники, электроники и автоматики (технического университета), член-корреспондент Академии криптографии Российской Федерации;

А. В. МИХАЛЕВ — доктор физико-математических наук, профессор кафедры высшей алгебры механико-математического факультета МГУ им. М. В. Ломоносова, заведующий кафедрой теоретической информатики, заслуженный деятель науки Российской Федерации.

Обложка
Е. А. ВЛАСОВА

© Издательство «Лань», 2022
© М. М. Глухов, И. А. Круглов,
2022
© Издательство «Лань»,
художественное оформление,
2022

ОГЛАВЛЕНИЕ

Предисловие	5
Основные обозначения	7
<i>Глава 1</i>	
Линейные и матричные представления групп	
§ 1. Понятие линейного и матричного представления группы. Примеры	9
§ 2. Эквивалентные и неэквивалентные представления	17
§ 3. Ортогональные и унитарные представления групп	21
§ 4. Приводимые и неприводимые представления	24
§ 5. Неприводимые представления конечных абелевых групп над полем комплексных чисел	29
<i>Глава 2</i>	
Представления групп и групповые кольца	
§ 1. Определения модуля, группового кольца и групповой алгебры	36
§ 2. Соответствие между линейными представлениями конечной группы и левыми модулями над групповым кольцом	39
§ 3. Разложение группового кольца в прямую сумму простых колец	45
§ 4. Разложение группового кольца в прямую сумму минимальных левых идеалов	51
§ 5. Строение минимальных двусторонних идеалов группового кольца над полем комплексных чисел	53
§ 6. Соответствие между неприводимыми комплексными представлениями конечной группы и ее классами сопряженных элементов	58
§ 7. Неприводимые комплексные составляющие регулярного представления конечной группы	60

*Глава 3***Характеры представлений групп**

- § 1. Понятие и простейшие свойства характеров группы.
Приводимые и неприводимые характеры 63
- § 2. Соотношения ортогональности для неприводимых
характеров и их обобщения 66
- § 3. Комплексные характеры как центральные функции
на группе 71
- § 4. Степени неприводимых комплексных представлений
конечной группы 74
- § 5. Тензорные произведения представлений
и их характеры 78
- § 6. Подстановочные представления групп
и их характеры 82
- § 7. Вычисление комплексных характеров некоторых групп 88

*Глава 4***Индукцированные представления и их характеры**

- § 1. Понятие о представлении группы, индуцированном
представлением ее подгруппы 92
- § 2. Теорема взаимности (Фробениуса)
для характеров индуцированных представлений 96
- § 3. Использование индуцированных представлений
для изучения групп Фробениуса 99

*Глава 5***Представления и характеры симметрических групп
над полем комплексных чисел**

- § 1. Диаграммы Юнга и соответствующие им
группы подстановок 107
- § 2. Описание минимальных левых идеалов
групповой алгебры симметрической группы 111
- § 3. О матричных представлениях
и характерах симметрических групп 119

*Глава 6***О приложениях теории представлений
и характеров групп в криптографии**

- § 1. Использование теории характеров
для изучения дискретных функций 129
- 1.1. Характеризация близости дискретных функций
к линейным функциям 132
- § 2. Использование теории характеров для вероятностной
оценки числа подстановок в произведениях групп 143
- § 3. Применение теории представлений к исследованию
матриц переходных вероятностей поточных шифров 151

- Литература** 171