

## Программа учебной дисциплины «Алгебра» (основной поток)

Утверждена

Академическим советом ООП  
Протокол № от «\_\_»\_\_\_\_20\_\_ г.

Автор	Р.С.Авдеев, кандидат физико-математических наук ( <a href="mailto:suselr@yandex.ru">suselr@yandex.ru</a> , <a href="mailto:ravdeev@hse.ru">ravdeev@hse.ru</a> )
Число кредитов	3
Контактная работа (час.)	40
Самостоятельная работа (час.)	74
Курс	1
Формат изучения дисциплины	без использования онлайн курса

### I. ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ

Цель освоения дисциплины «Алгебра» — познакомить слушателей с основными структурами современной алгебры. Первые пять лекций посвящены теории групп, последние пять — кольцам и полям. Мы докажем базовые факты об этих структурах и продемонстрируем их возможные приложения.

В результате освоения дисциплины «Алгебра» студент должен:

- Знать основные факты о таких алгебраических структурах, как группы, кольца и поля; освоить алгоритмические аспекты современной алгебры.
- Уметь производить базовые вычисления с алгебраическими структурами, применять изученные факты и методы в прикладных задачах.
- Иметь навыки работы с конечными группами и конечными полями, овладеть основными техническими приёмами алгебры многочленов и теории абелевых групп.

Для освоения учебной дисциплины студенты должны владеть знаниями и навыками в объёме программы средней школы по математике и освоить учебные курсы:

- Дискретная математика,
- Математический анализ-1,
- первые три модуля курса «Линейная алгебра и геометрия».

Основные положения дисциплины могут быть использованы в дальнейшем при изучении следующих дисциплин:

- Математический анализ,
- Дифференциальные уравнения,
- Математические модели в экономике,
- Безопасность и криптография,
- Базы данных,
- Оптимизация,
- Теория вычислений,
- Алгоритмы и сложность,
- выполнение курсовых работ, предусмотренных РУП по направлению 01.03.02.

### II. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

## 1. Группы

Бинарные операции. Полугруппы, моноиды, группы, коммутативные (абелевы) группы. Порядок группы. Примеры групп. Подгруппы. Описание всех подгрупп в группе целых чисел по сложению. Циклические подгруппы. Порядок элемента группы. Связь между порядком элемента и порядком порождаемой им циклической подгруппы. Циклические группы. Левые и правые смежные классы группы по подгруппе. Индекс подгруппы, теорема Лагранжа и пять следствий из неё. Нормальные подгруппы. Факторгруппа группы по нормальной подгруппе. Гомоморфизмы групп, простейшие свойства. Изоморфизм групп, изоморфные группы. Классификация циклических групп с точностью до изоморфизма. Ядро и образ гомоморфизма групп. Теорема о гомоморфизме для групп. Прямое произведение групп и разложение группы в прямое произведение подгрупп. Разложение конечной циклической группы. Примарные абелевы группы. Теорема о разложении конечной абелевой группы в прямое произведение примарных циклических групп, доказательство единственности числа и порядков примарных циклических множителей. Экспонента конечной абелевой группы, критерий цикличности. Криптография с открытым ключом. Задача дискретного логарифмирования. Система Диффи-Хеллмана обмена ключами. Криптосистема Эль-Гамала.

## 2. Кольца

Понятие кольца, примеры. Коммутативные кольца. Обратимые элементы, делители нуля, нильпотенты. Поля. Критерий того, что кольцо вычетов является полем. Алгебры над полем, размерность алгебры. Подкольца, подполя, подалгебры, гомоморфизмы, изоморфизмы. Идеалы в кольце. Главные идеалы и идеалы, порождённые подмножеством коммутативного кольца. Факторкольцо кольца по идеалу. Ядро и образ гомоморфизма колец. Теорема о гомоморфизме для колец. Делимость в коммутативных кольцах без делителей нуля. Ассоциированные элементы. Кольца главных идеалов. Теорема о том, что всякое евклидово кольцо является кольцом главных идеалов. Наибольший общий делитель двух элементов. Существование наибольшего общего делителя для двух элементов  $a$  и  $b$  евклидова кольца и его линейная выразимость через  $a$  и  $b$ . Простые элементы. Факториальные кольца. Факториальность колец главных идеалов. Лексикографический порядок на множестве одночленов от нескольких переменных. Лемма о конечности убывающих цепочек одночленов. Старший член многочлена от нескольких переменных. Элементарная редукция многочлена относительно другого многочлена. Лемма о конечности цепочек элементарных редукций относительно системы многочленов. Остаток многочлена относительно заданной системы многочленов. Системы Грёбнера. Характеризация систем Грёбнера в терминах цепочек элементарных редукций.  $S$ -многочлены. Критерий Бухбергера. Базис Грёбнера идеала в кольце многочленов от нескольких переменных, теорема о трёх эквивалентных условиях. Решение задачи вхождения многочлена в идеал. Лемма о конечности цепочек одночленов, в которых каждый следующий одночлен не делится ни на один из предыдущих. Алгоритм Бухбергера построения базиса Грёбнера идеала.

## 3. Поля

Поля. Примеры. Характеристика поля. Простое подполе. Расширение полей, его степень. Степень композиции двух расширений. Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента и его свойства. Поле, порождённое алгебраическим элементом. Существование конечного расширения исходного поля, в котором заданный многочлен имеет корень. Поле разложения многочлена. Конечные поля. Порядок конечного поля. Автоморфизм Фробениуса. Существование и

единственность конечного поля, порядок которого — степень простого числа. Поле из четырёх элементов. Цикличность мультипликативной группы конечного поля. Неприводимые многочлены над полем вычетов. Описание подполей конечного поля. Коды над конечным алфавитом. Расстояние Хэмминга. Минимальное расстояние кода. Коды, исправляющие  $t$  ошибок: определение и эквивалентные переформулировки. Код с повторением. Линейные коды. Проверочная матрица. Связь минимального расстояния линейного кода с его проверочной матрицей. Бинарный код Хэмминга, его минимальное расстояние и число ошибок, которое он может исправлять. Коды БЧХ. Теорема о количестве ошибок, исправляемых кодом БЧХ. Оценка на размерность кода БЧХ.

### III. ОЦЕНИВАНИЕ

Текущий контроль знаний осуществляется в следующих формах:

- письменная контрольная работа (на последней учебной неделе);
- выполнение письменных домашних заданий (задания выдаются еженедельно, каждое задание содержит 4 задачи);

Аудиторная и самостоятельная внеаудиторная работы оцениваться не будут.

Итоговый контроль проводится в форме устного экзамена.

Накопленная оценка за текущий контроль формируется из оценок за домашние задания и контрольную работу следующим образом:

$$O_{\text{накопл}} = 0,6 * O_{\text{д/з}} + 0,4 * O_{\text{к/р}}.$$

Итоговая оценка за дисциплину рассчитывается следующим образом:

$$O_{\text{итог}} = 0,5 * O_{\text{накопл}} + 0,5 * O_{\text{экс}}.$$

Все оценки выставляются по 10-балльной системе. Округление производится только для итоговой оценки. Способ округления – арифметический.

### IV. ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ

Оценочные средства для текущего контроля и промежуточной аттестации

Для текущего контроля знаний, а также промежуточной аттестации можно использовать задачи из Сборника задач по алгебре под редакцией А.И. Кострикина.

Примерные темы задач на контрольной работе (в скобках даны номера типовых задач по Сборнику задач по алгебре под редакцией А.И.Кострикина):

- Порядки элементов и подгруппы в конечных абелевых группах [60.39, 60.40, 60.42, 60.43, 60.45]
- Алгоритм Евклида и линейное представление НОД в кольце многочленов [25.2, 25.3, 25.7]
- Разложение многочленов на неприводимые множители над полями  $R$ ,  $C$  и  $Z_p$  [27.1, 27.2]
- Базисы Грёбнера и задача вхождения
- Минимальные многочлены и вычисления в конечных расширениях полей [67.3, 67.13]
- Системы линейных уравнений с коэффициентами в конечном поле

Примерный список вопросов для подготовки к экзамену:

1. Бинарные операции. Полугруппы, моноиды и группы. Коммутативные группы. Примеры групп. Порядок группы. Подгруппы. Описание всех подгрупп в группе  $(Z,+)$ .

2. Подгруппы. Циклические подгруппы. Циклические группы. Порядок элемента. Связь между порядком элемента и порядком порождаемой им циклической подгруппы.
3. Смежные классы. Индекс подгруппы. Теорема Лагранжа.
4. Пять следствий из теоремы Лагранжа.
5. Нормальные подгруппы и факторгруппы.
6. Гомоморфизмы групп. Простейшие свойства гомоморфизмов. Изоморфизмы групп. Ядро и образ гомоморфизма групп, их свойства.
7. Теорема о гомоморфизме для групп.
8. Классификация циклических групп.
9. Прямое произведение групп. Разложение конечной циклической группы.
10. Примарные абелевы группы. Теорема о строении конечных абелевых групп, доказательство единственности.
11. Экспонента конечной абелевой группы и критерий цикличности.
12. Криптография с открытым ключом. Задача дискретного логарифмирования. Система Диффи-Хеллмана обмена ключами. Криптосистема Эль-Гамала.
13. Кольца. Коммутативные кольца. Обратимые элементы, делители нуля и нильпотенты. Примеры колец. Поля. Критерий того, что кольцо вычетов является полем.
14. Идеалы колец. Факторкольцо кольца по идеалу. Гомоморфизмы и изоморфизмы колец. Ядро и образ гомоморфизма колец. Теорема о гомоморфизме для колец.
15. Делимость и ассоциированные элементы в коммутативных кольцах без делителей нуля. Наибольший общий делитель. Кольца главных идеалов. Существование наибольшего общего делителя и его линейного выражения в кольце главных идеалов.
16. Простые элементы. Факториальные кольца. Факториальность колец главных идеалов: доказательство существования разложения на простые множители.
17. Простые элементы. Факториальные кольца. Факториальность колец главных идеалов: доказательство единственности разложения на простые множители.
18. Теорема о том, что кольцо многочленов над полем является кольцом главных идеалов.
19. Лексикографический порядок на множестве одночленов от нескольких переменных. Лемма о конечности убывающих цепочек одночленов.
20. Старший член многочлена от нескольких переменных. Элементарная редукция многочлена относительно другого многочлена. Лемма о конечности цепочек элементарных редукций относительно системы многочленов.
21. Остаток многочлена относительно заданной системы многочленов. Системы Грёбнера. Характеризация систем Грёбнера в терминах цепочек элементарных редукций.
22. S-многочлены. Критерий Бухбергера.
23. Базис Грёбнера идеала в кольце многочленов от нескольких переменных, теорема о трёх эквивалентных условиях. Решение задачи вхождения многочлена в идеал.
24. Лемма о конечности цепочек одночленов, в которых каждый следующий одночлен не делится ни на один из предыдущих. Алгоритм Бухбергера построения базиса Грёбнера идеала.
25. Лемма Диксона. Теорема о существовании конечного базиса Грёбнера в идеале кольца многочленов от нескольких переменных. Теорема Гильберта о базисе идеала.
26. Характеристика поля и простое подполе.
27. Расширение полей. Конечное расширение и его степень. Степень композиции двух расширений.
28. Критерий того, что факторкольцо кольца многочленов над полем является полем. Степень расширения этого поля.
29. Существование конечного расширения исходного поля, в котором заданный многочлен (а) имеет корень; (б) разлагается на линейные множители. Поле разложения многочлена.
30. Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента и его свойства.
31. Подполе в расширении полей, порождённое алгебраическим элементом.

32. Порядок конечного поля. Автоморфизм Фробениуса.
33. Теорема существования и единственности для конечных полей.
34. Цикличность мультипликативной группы конечного поля и неприводимые многочлены над  $Z_p$ .
35. Подполя конечного поля.
36. Коды над конечным алфавитом. Расстояние Хэмминга. Минимальное расстояние кода. Коды, исправляющие  $t$  ошибок: определение и эквивалентные переформулировки. Код с повторением.
37. Линейные коды. Проверочная матрица. Связь минимального расстояния линейного кода с его проверочной матрицей. Бинарный код Хэмминга, его минимальное расстояние и число ошибок, которое он может исправлять.
38. Коды БЧХ. Теорема о количестве ошибок, исправляемых кодом БЧХ. Оценка на размерность кода БЧХ.

## V. РЕСУРСЫ

### V.1 Основная литература

1. Винберг Э. Б. Курс алгебры. М.: Факториал, 1999 (или любое последующее издание)
2. Сборник задач по алгебре под редакцией А.И.Кострикина. И.В.Аржанцев, В.А.Артамонов и другие. М.: МЦНМО, 2009 (или любое последующее издание)

### V.2 Дополнительная литература

1. Кострикин А.И. Введение в алгебру. Основы алгебры. М.: Физматлит, 1994 (или любое последующее издание)
2. Кострикин А.И. Введение в алгебру. Часть III. Основные алгебраические структуры. М.: Физматлит, 2000 (или любое последующее издание)
3. Лидл Р., Нидеррайтер Г. Конечные поля (2 тома). М.: Мир, 1988
4. Аржанцев И.В. Базисы Грёбнера и системы алгебраических уравнений. М.: МЦНМО, 2003

### V.3 Программное обеспечение

№ п/п	Наименование	Условия доступа
1	Microsoft Windows 7 Professional RUS Microsoft Windows 10 Microsoft Windows 8.1 Professional RUS	<i>Из внутренней сети университета (договор)</i>
2.	Microsoft Office Professional Plus 2010	<i>Из внутренней сети университета (договор)</i>

### V.4 Профессиональные базы данных, информационные справочные системы, интернет-ресурсы (электронные образовательные ресурсы)

№ п/ п	Наименование	Условия доступа
<i>Профессиональные базы данных, информационно-справочные системы</i>		
1.	Консультант Плюс	<i>Из внутренней сети университета (договор)</i>
2.	Электронно-библиотечная система Юрайт	URL: <a href="https://biblio-online.ru/">https://biblio-online.ru/</a>
<i>Интернет-ресурсы (электронные образовательные ресурсы)</i>		
1.	Открытое образование	URL: <a href="https://openedu.ru/">https://openedu.ru/</a>

#### **V.5 Материально-техническое обеспечение дисциплины**

Учебные аудитории для лекционных, семинарских и самостоятельных занятий по дисциплине не требуют специального технического оснащения.

## Программа учебной дисциплины «Алгебра» (пилотный поток)

Утверждена

Академическим советом ООП

Протокол № от «\_\_» \_\_\_\_ 20\_\_ г.

Автор	И.В.Аржанцев, доктор физико-математических наук, профессор ( <a href="mailto:arjantsev@hse.ru">arjantsev@hse.ru</a> )
Число кредитов	3
Контактная работа (час.)	40
Самостоятельная работа (час.)	74
Курс	1
Формат изучения дисциплины	без использования онлайн курса

### III. ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ

Цель освоения дисциплины «Алгебра» — познакомить слушателей с основными структурами современной алгебры: группами, кольцами и полями. Мы докажем базовые факты об этих структурах и продемонстрируем их возможные приложения. Сдавшие этот курс смогут, среди прочего, перечислить с точностью до изоморфизма все коммутативные группы из 100 элементов, найти сумму кубов корней данного многочлена, доказать, что многочлен от многих переменных однозначно раскладывается на простые множители, и объяснить, почему не существует поля из 6 элементов.

В результате освоения дисциплины «Алгебра» студент должен:

- Знать основные факты о таких алгебраических структурах, как группы, кольца и поля; освоить алгоритмические аспекты современной алгебры.
- Уметь производить базовые вычисления с алгебраическими структурами, применять изученные факты и методы в прикладных задачах.
- Иметь навыки работы с конечными группами и конечными полями, овладеть основными техническими приёмами алгебры многочленов и теории абелевых групп.

Для освоения учебной дисциплины студенты должны владеть знаниями и навыками в объёме программы средней школы по математике и освоить учебные курсы:

- Дискретная математика,
- Математический анализ-1,
- первые три модуля курса «Линейная алгебра и геометрия».

Основные положения дисциплины могут быть использованы в дальнейшем при изучении следующих дисциплин:

- Математический анализ,
- Дифференциальные уравнения,
- Математические модели в экономике,
- Безопасность и криптография,
- Базы данных,

- Оптимизация,
- Теория вычислений,
- Алгоритмы и сложность,
- выполнение курсовых работ, предусмотренных РУП по направлению 01.03.02.

#### IV. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

**Лекция 1.** Полугруппы и группы: основные определения и примеры. Группы подстановок и группы матриц. Подгруппы. Порядок элемента и циклические подгруппы. Смежные классы и индекс подгруппы. Теорема Лагранжа и её следствия.

**Лекция 2.** Нормальные подгруппы. Факторгруппы и теорема о гомоморфизме. Центр группы. Прямое произведение групп. Факторизация по сомножителям. Разложение конечной циклической группы.

**Лекция 3.** Конечно порождённые и свободные абелевы группы. Подгруппы свободных абелевых групп. Теорема о согласованных базисах. Алгоритм приведения целочисленной матрицы к диагональному виду.

**Лекция 4.** Строение конечно порождённых абелевых групп. Конечные абелевы группы. Экспонента конечной абелевой группы. Криптография с открытым ключом. Задача дискретного логарифмирования. Система Диффи–Хеллмана обмена ключами. Криптосистема Эль–Гамала.

**Лекция 5.** Действие группы на множестве. Орбиты и стабилизаторы. Транзитивные и свободные действия. Три действия группы на себе. Классы сопряжённости. Теорема Кэли.

**Лекция 6.** Кольца. Делители нуля, обратимые элементы, нильпотенты и идемпотенты. Поля и алгебры. Идеалы и факторкольца. Теорема о гомоморфизме. Центр алгебры матриц над полем. Простота алгебры матриц над полем.

**Лекция 7.** Элементарные симметрические многочлены. Основная теорема о симметрических многочленах. Лексикографический порядок. Теорема Виета. Дискриминант многочлена.

**Лекция 8.** Примеры полей. Характеристика поля. Расширения полей, алгебраические и трансцендентные элементы. Минимальный многочлен. Конечное расширение и его степень. Присоединение корня многочлена. Поле разложения многочлена: существование и единственность.

**Лекция 9.** Конечные поля. Простое подполе и порядок конечного поля. Автоморфизм Фробениуса. Теорема существования и единственности для конечных полей. Поле из четырёх элементов. Циклическость мультипликативной группы конечного поля. Неприводимые многочлены над конечным полем. Подполя конечного поля.

**Лекция 10.** Основная задача теории кодирования. Расстояние Хэмминга. Коды, исправляющие ошибки. Характеристики кода. Неравенство Синглтона. Совершенные коды. Линейные коды. Вес Хэмминга. Код Хэмминга  $[7,4,3]_2$ . Коды Рида–Соломона. Циклические коды и главные идеалы. Алгоритм декодирования по лидеру смежного класса.

#### IV. ОЦЕНИВАНИЕ

Текущий контроль знаний осуществляется в следующих формах:

- письменная контрольная работа (на последней учебной неделе);
- выполнение письменных домашних заданий (задания выдаются еженедельно, каждое задание содержит 4-5 задач);

Аудиторная и самостоятельная внеаудиторная работы оцениваться не будут.

Итоговый контроль проводится в форме устного экзамена.

Все оценки выставляются по 10-балльной системе.



Накопленная оценка за текущий контроль формируется из оценок за домашние задания и контрольную работу следующим образом:

$$O_{\text{накопл}} = 0,6 * O_{\text{д/з}} + 0,4 * O_{\text{к/р}}$$

Итоговая оценка за дисциплину рассчитывается следующим образом:

$$O_{\text{итог}} = 0,5 * O_{\text{накопл}} + 0,5 * O_{\text{экз}}$$

Способ округления накопленной и итоговой оценок – арифметический.

## V. ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ

Оценочные средства для текущего контроля и промежуточной аттестации

Для текущего контроля знаний, а также промежуточной аттестации можно использовать задачи из Сборника задач по алгебре под редакцией А.И. Кострикина.

Типовые задачи для подготовки к контрольной работе (номера даны по Сборнику задач по алгебре под редакцией А.И.Кострикина):

- Порядки элементов и подгруппы в конечных абелевых группах [60.39, 60.40, 60.42, 60.43, 60.45]
- Факторгруппы свободных абелевых групп [60.52, 60.53, 60.54]
- Орбиты и стабилизаторы для действий групп на множествах [57.1, 57.2, 57.3, 57.9]
- Симметрические многочлены и теорема Виета [31.2, 31.3, 31.4, 31.9, 31.10, 31.25, 31.26]
- Минимальные многочлены и вычисления в конечных расширениях полей [67.3, 67.13]

Примерный список вопросов для подготовки к экзамену:

- 1) Множества с бинарной операцией, полугруппы, моноиды и группы. Коммутативные группы. Порядок группы. Примеры групп.
- 2) Подгруппы. Циклические подгруппы. Порядок элемента. Циклические группы.
- 3) Смежные классы. Индекс подгруппы. Теорема Лагранжа.
- 4) Пять следствий из теоремы Лагранжа.
- 5) Нормальные подгруппы и факторгруппы.
- 6) Гомоморфизмы и изоморфизмы групп. Классификация циклических групп.
- 7) Ядро и образ гомоморфизма групп. Теорема о гомоморфизме.
- 8) Центр группы.
- 9) Прямое произведение групп. Теорема о факторизации по сомножителям.
- 10) Разложение конечной циклической группы.
- 11) Конечно порожденная абелева группа. Свободная абелева группа и ее ранг. Классификация свободных абелевых групп. Характеризация базисов.
- 12) Подгруппа свободной абелевой группы свободна.
- 13) Целочисленные элементарные преобразования и алгоритм приведения целочисленной матрицы к диагональному виду.
- 14) Теорема о согласованных базисах.
- 15) Примарные абелевы группы. Классификация конечно порожденных абелевых групп. Разложение конечной абелевой группы в сумму примарных циклических.
- 16) Экспонента конечной абелевой группы и критерий циклическости.
- 17) Криптография с открытым ключом. Задача дискретного логарифмирования. Система Диффи-Хеллмана обмена ключами.
- 18) Криптосистема Эль-Гамала.
- 19) Действие группы на множестве. Орбиты и стабилизаторы. Число элементов в орбите.
- 20) Транзитивные, свободные и эффективные действия групп. Ядро неэффективности.

- 21) Три действия группы на себе. Изоморфизм действий. Описание свободных транзитивных действий.
- 22) Теорема Кэли.
- 23) Кольца. Коммутативные кольца. Обратимые элементы, делители нуля, нильпотенты и идемпотенты. Примеры колец. Поля. Кольца вычетов. Алгебры над полями.
- 24) Идеалы колец. Главные идеалы и идеалы, порожденные подмножеством, в коммутативных кольцах.
- 25) Факторкольца. Теорема о гомоморфизме для колец.
- 26) Простое кольцо. Простота алгебры матриц. Центр алгебры матриц.
- 27) Симметрические многочлены. Степенные суммы и элементарные симметрические многочлены. Формулировка основной теоремы о симметрических многочленах. Примеры.
- 28) Лексикографический порядок и старший член. Лемма о старшем члене.
- 29) Доказательство основной теоремы о симметрических многочленах.
- 30) Теорема Виета. Дискриминант многочлена.
- 31) Примеры полей. Характеристика поля и простое подполе.
- 32) Расширение полей. Конечное расширение и его степень. Степень композиции расширений.
- 33) Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента и его свойства.
- 34) Минимальное подполе, порожденное алгебраическим элементом.
- 35) Присоединение корня неприводимого многочлена. Поле разложения многочлена.
- 36) Порядок конечного поля. Автоморфизм Фробениуса.
- 37) Теорема существования и единственности для конечных полей.
- 38) Цикличность мультипликативной группы конечного поля.
- 39) Существование неприводимого многочлена произвольной степени над полем вычетов.
- 40) Постановка задачи теории кодирования. Расстояние Хэмминга. Коды, исправляющие ошибки. Характеристики кода. Неравенство Синглтона. Совершенные коды.
- 41) Линейные коды. Вес Хэмминга.  $[7,4,3]$ -код Хэмминга.
- 42) Коды Рида-Соломона. Циклические коды и главные идеалы. Алгоритм декодирования по лидеру смежного класса.

## **VI. РЕСУРСЫ**

### **VI.1 Основная литература**

3. Винберг Э. Б. Курс алгебры. М.: Факториал, 1999 (или любое последующее издание).
4. Сборник задач по алгебре под редакцией А.И.Кострикина. И.В.Аржанцев, В.А.Артамонов и другие. М.: МЦНМО, 2009 (или любое последующее издание)

### **VI.2 Дополнительная литература**

5. Кострикин А.И. Введение в алгебру. Основы алгебры. М.: Физматлит, 1994 (или любое последующее издание).
6. Кострикин А.И. Введение в алгебру. Часть III. Основные алгебраические структуры. М.: Физматлит, 2000 (или любое последующее издание).
7. Лидл Р., Нидеррайтер Г. Конечные поля (2 тома). М.: Мир, 1988

### **VI.3 Программное обеспечение**

<b>№ п/п</b>	<b>Наименование</b>	<b>Условия доступа</b>
1	Microsoft Windows 7 Professional RUS Microsoft Windows 10 Microsoft Windows 8.1 Professional RUS	<i>Из внутренней сети университета (договор)</i>
2.	Microsoft Office Professional Plus 2010	<i>Из внутренней сети университета (договор)</i>

**VI.4 Профессиональные базы данных, информационные справочные системы, интернет-ресурсы (электронные образовательные ресурсы)**

<b>№ п/п</b>	<b>Наименование</b>	<b>Условия доступа</b>
<i><b>Профессиональные базы данных, информационно-справочные системы</b></i>		
1.	Консультант Плюс	<i>Из внутренней сети университета (договор)</i>
2.	Электронно-библиотечная система Юрайт	URL: <a href="https://biblio-online.ru/">https://biblio-online.ru/</a>
<i><b>Интернет-ресурсы (электронные образовательные ресурсы)</b></i>		
1.	Открытое образование	URL: <a href="https://openedu.ru/">https://openedu.ru/</a>

**VI.5 Материально-техническое обеспечение дисциплины**

Учебные аудитории для лекционных, семинарских и самостоятельных занятий по дисциплине не требуют специального технического оснащения.