

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный университет имени М.В.Ломоносова»

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

УТВЕРЖДАЮ

Декан механико-математического
факультета, д.ф.-м.н.,
член-корр. РАН, профессор

/А.И. Шафаревич/

30 сентября 2022 г.

ПРОГРАММА-МИНИМУМ

кандидатского экзамена по специальности

1.1.5. Математическая логика, алгебра, теория чисел и дискретная математика

Область науки: **1. Естественные науки**

Группа научных специальностей: **1.1. Математика и механика**

Наименование отраслей науки, по которым присуждаются ученые степени:
физико-математические науки

Рабочая программа рассмотрена и одобрена
Учебно-методической комиссией факультета
(протокол № 6 от 30 сентября 2022 г.)
(При наличии учебно-методической комиссии на факультете)

Москва 2022

1. Описание программы:

Настоящая программа охватывает основополагающие разделы и области знания, в основе данной программы лежат следующие дисциплины:

алгебра, дискретная математика, математическая логика и теория чисел.

2. Основные разделы и вопросы к экзамену:

1. Математическая логика

1. Понятие алгоритма и вычислимой функции, перечислимого и разрешимого множества.
2. Универсальная вычислимая функция. Существование перечислимого неразрешимого множества. Алгоритмические проблемы.
3. Определение вычислимости в теоретико-множественных терминах (например, вычислимость по Тьюрингу). Тезис Чёрча.
4. Построение полугруппы с неразрешимой проблемой распознавания равенства. Неразрешимость проблемы существования целочисленного решения у системы полиномиальных уравнений (без доказательства.)
5. Сложность вычисления. Классы P и NP. Полиномиальная сводимость и NP-полные задачи. Теорема об NP-полноте задачи выполнимости булевых формул.
6. Логика высказываний. Представимость булевых функций формулами логики высказываний. Конъюнктивные и дизъюнктивные нормальные формы.
7. Булевы алгебры. Теорема Стоуна о представлении конечных булевых алгебр.
8. Логика предикатов (отношений). Определимость отношений в структуре (алгебраической системе). Приведение формул логики предикатов к предварённой нормальной форме.
9. Исчисление предикатов, его корректность. Теорема о дедукции.
10. Полнота исчисления предикатов. Теорема Мальцева о компактности.
11. Полнота непротиворечивой теории, не имеющей конечных моделей и категоричной в некоторой бесконечной мощности.
12. Разрешимые теории. Теория плотного линейного порядка без первого и последнего элемента, её разрешимость и полнота.
13. Формальная арифметика (система PA). Теорема о представимости вычислимых функций в формальной арифметике (без доказательства).
14. Теорема Гёделя о неполноте формальной арифметики. Теорема Тарского о невыразимости арифметической истинности в арифметике. Неразрешимость алгоритмической проблемы выводимости для арифметики и логики предикатов.

15. Фильтры, ультрафильтры, ультрапроизведения. Теорема об элементарной эквивалентности структуры и её ультрастепени.
16. Критерии аксиоматизируемости и конечной аксиоматизируемости класса структур.
17. Теорема о полноте минимальной нормальной модальной логики К относительно семантики Крипке.
18. Теорема о полноте интуиционистской логики высказываний относительно семантики Крипке.
19. Аксиоматическая теория множеств, система аксиом Цермело – Френкеля, аксиома выбора. Ординалы, принцип трансфинитной индукции. Построение ординальных функций с помощью трансфинитной рекурсии. Континуум-гипотеза. Неразрешимость аксиомы выбора и континуум-гипотезы (без доказательства).

2. Теория чисел

1. Квадратичный закон взаимности.
2. Первообразные корни и индексы.
3. Неравенства Чебышева для функции $\pi(x)$.
4. Дзета-функция Римана. Асимптотический закон распределения простых чисел.
5. Характеры и L-функции. Теорема Дирихле о простых числах в арифметической прогрессии.
6. Тригонометрические суммы. Модуль гауссовой суммы. Полные тригонометрические суммы и число решений сравнений.
7. Критерий Вейля равномерного распределения. Теорема Вейля о последовательности значений многочлена.
8. Модулярная группа и модулярные функции. Теорема о строении алгебры модулярных форм.
9. Представление целых чисел в виде суммы двух и четырех квадратов.
10. Представление целых чисел унимодулярными квадратичными формами.
11. Приближение вещественных чисел рациональными дробями. Теорема Лиувилля о приближении алгебраических чисел рациональными дробями. Примеры трансцендентных чисел.
12. Трансцендентность чисел e и π .

3. Дискретная математика

1. Многозначные логики. Проблема полноты. Теорема о полноте систем функций алгебры логики. Алгоритм распознавания полноты систем функций k -значной логики. Теоремы Слупецкого и Яблонского. Особенности k -значных логик.
2. Автоматы. Регулярные события и их представление в автоматах.

Эксперименты с автоматами. Алгоритмическая неразрешимость проблемы полноты для автоматов.

3. Вычислимые функции. Эквивалентность класса рекурсивных функций и класса функций, вычислимых на машинах Тьюринга.
Алгоритмическая неразрешимость проблемы эквивалентности слов в ассоциативных исчислениях.
4. Элементы комбинаторного анализа. Основные комбинаторные числа. Оценки и асимптотики для комбинаторных чисел.
5. Графы и сети. Оценки числа графов и сетей различных типов. Плоские и планарные графы. Формула Эйлера для плоских графов. Необходимые условия планарности в теореме Понтрягина-Куратовского (без доказательства достаточности). Экстремальная теория графов. Теорема Турана. Теорема Рамсея.
6. Алфавитное кодирование. Критерии однозначности декодирования. Неравенство Крафта-Макмиллана. Полные коды. Оптимальное кодирование. Построение кодов с минимальной избыточностью.
7. Самокорректирующиеся коды. Граница упаковки. Коды Хемминга, исправляющие единичную ошибку. Конечные поля и их основные свойства. Коды Боуза-Чоудхури-Хоквингема. Коды Рида-Маллера.
8. Понятие управляющей системы. Основные модельные классы управляющих систем: дизъюнктивные нормальные формы, формулы, контактные схемы, схемы из функциональных элементов, автоматы, машины Тьюринга, операторные алгоритмы. Основные проблемы теории управляющих систем.
9. Дизъюнктивные нормальные формы. Проблема минимизации булевых функций. Дизъюнктивные нормальные формы (ДНФ). Постановка задачи в геометрической форме. Тупиковые и минимальные ДНФ. Локальные алгоритмы построения ДНФ. Построение ДНФ СУММА ТУПИКОВЫХ с помощью локального алгоритма. Невозможность построения ДНФ СУММА МИНИМАЛЬНЫХ в классе локальных алгоритмов.
10. Синтез и сложность управляющих систем. Асимптотически оптимальный метод Лупанова синтеза схем из функциональных элементов. Асимптотически оптимальный метод Лупанова построения формул. Инвариантные классы Яблонского и их свойства. Синтез схем для функций из инвариантных классов.
11. Нижние оценки сложности реализации булевых функций схемами и формулами.
12. Эквивалентные преобразования управляющих систем. Эквивалентные преобразования формул алгебры логики. Теорема Линдона. Пример Линдона.
13. Надежность и контроль функционирования управляющих систем. Логический подход к контролю исправности и диагностике неисправностей управляющих систем. Тесты.
14. Потoki в сетях. Теорема Форда-Фалкерсона. Алгоритм нахождения

максимального потока. Теорема о целочисленности. Теорема Кенига-Эгервари. Теорема Холла. Теорема Дилуорса.

15. Задачи целочисленного линейного программирования и алгоритмы их решения. Метод Гомори. Метод ветвей и границ. Задача коммивояжера. Сводимость комбинаторных проблем. Классы сложности P и NP. Приближенные методы решения NP-трудных задач.

4. Алгебра

1. Свободные группы. Теорема Нильсена – Шрайера. Копредставления групп (задание образующими и определяющими соотношениями), примеры.
2. Расширения полей. Базис трансцендентности. Конечные расширения. Алгебраическое замыкание подполя. Алгебраические числа. Сепарабельные расширения. Теорема о примитивном элементе.
3. Поле разложения многочлена. Расширения Галуа. Основная теорема теории Галуа. Разрешимость алгебраических уравнений в радикалах. Группа Галуа кубического многочлена и формула Кардано. Конечные поля.
4. Кольца главных идеалов, их факториальность. Теорема о строении конечно порождённых модулей над кольцами главных идеалов, её применение к абелевым группам и линейным операторам.
5. Нётеровы кольца и модули. Нётеровость кольца многочленов (теорема Гильберта о базисе идеала). Конечные расширения нётеровых колец. Целое замыкание подкольца. Целозамкнутые кольца. Целые алгебраические числа.
6. Конечно порождённые коммутативные алгебры и аффинные алгебраические многообразия. Теорема Гильберта о нулях. Топология Зарисского и неприводимые компоненты алгебраического многообразия. Поле рациональных функций и размерность неприводимого алгебраического многообразия.
7. Мономиальные упорядочения. Базис Грёбнера полиномиального идеала. S-полиномы и алгоритм Бухбергера. Критерии совместности и конечности числа решений системы алгебраических уравнений над алгебраически замкнутым полем.
8. Линейные представления групп и ассоциативных алгебр. Неприводимые и вполне приводимые представления. Полная приводимость линейных представлений компактных (в частности, конечных) групп. Морфизмы представлений. Лемма Шура. Изотипные компоненты вполне приводимого представления. Теорема Бернсайда. Неприводимые представления прямого произведения групп.
9. Радикал ассоциативного кольца. Нильпотентность радикала артинова кольца. Радикал коммутативного кольца. Теорема плотности для

- полупростых модулей. Строение полупростых артиновых колец и полупростых ассоциативных алгебр.
10. Конечномерные ассоциативные алгебры с делением. Обобщённые алгебры кватернионов. Теоремы Фробениуса и Веддербёрна.
 11. Групповая алгебра конечной группы, её полупростота (в нулевой характеристике). Центр групповой алгебры и характеры неприводимых представлений конечной группы. Соотношения ортогональности.
 12. Группы Ли и их касательные алгебры Ли. Классические линейные группы Ли. Присоединённое представление группы Ли. Экспоненциальное отображение. Полная приводимость линейных представлений групп Ли $GL_n(\mathbb{C})$ и $SL_n(\mathbb{C})$ (унитарный трюк). Неприводимые линейные представления группы Ли $SL_2(\mathbb{C})$ и алгебры Ли $\mathfrak{sl}_2(\mathbb{C})$.
 13. Простые и разрешимые алгебры Ли, примеры. Теорема Ли о разрешимых алгебрах. Универсальная обёртывающая алгебра. Теорема Пуанкаре – Биркгофа – Витта.

III. Критерии оценивания

Критерии и показатели оценивания ответа на экзамене			
1	2	3	4
Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Фрагментарные знания в области алгебры, дискретной математики, математической логики и теории чисел	Неполные знания в области алгебры, дискретной математики, математической логики и теории чисел	Сформированные, но содержащие отдельные пробелы знания в области алгебры, дискретной математики, математической логики и теории чисел	Сформированные и систематические знания в области алгебры, дискретной математики, математической логики и теории чисел

IV. Рекомендуемая основная литература:

К разделу 1

1. М. Н. Бежанишвили. *Логика модальностей знания и мнения*. М.: УРСС, 2007.
2. Н. К. Верещагин, А. Шень. *Математическая логика и теория алгоритмов. Часть 1. Начала теории множеств*, изд. 4-е. М.: МЦНМО, 2012.
3. Н. К. Верещагин, А. Шень. *Математическая логика и теория алгоритмов. Часть 2. Языки и исчисления*, изд. 4-е. М.: МЦНМО, 2012.
4. Н. К. Верещагин, А. Шень. *Математическая логика и теория алгоритмов. Часть 3. Вычислимые функции*, изд. 4-е. М.: МЦНМО, 2012.

5. М. Гэри, Д. Джонсон. *Вычислительные машины и труднорешаемые задачи*. М.: Мир, 1982.
6. Ю. Л. Ершов. *Проблемы разрешимости и конструктивные модели*. М.: Наука, 1980.
7. Ю. Л. Ершов, Е.А.Палютин. *Математическая логика*. Изд. 2. М.: Наука, 1987.
8. С. Клини. *Математическая логика*. М.: Мир, 1973.
9. П. Дж. Коэн. *Теория множеств и континуум-гипотеза*. М.: Мир, 1969.
10. В. Н. Крупский, В. Е. Плиско. *Математическая логика и теория алгоритмов*. М.: Академия, 2013.
11. А. И. Мальцев. *Алгоритмы и рекурсивные функции*. Изд. 2-е. М.: Наука, 1986.
12. Э. Мендельсон. *Введение в математическую логику*. Изд. 3-е. М.: Наука, 1984.
13. П. С. Новиков. *Элементы математической логики*. Изд. 2-е. М.: Наука, 1973.
14. В. Е. Плиско, В. Х. Хаханян. *Интуиционистская логика*. М.: Изд-во при мех.-мат. ф-те МГУ, 2009.
15. Е. Расёва, Р. Сикорский. *Математика метаматематики*. М.: Наука, 1972.
16. Р. Сикорский. *Булевы алгебры*. М.: Мир, 1969.
17. Л. А. Скорняков. *Элементы общей алгебры*. М.: Наука, 1983.
18. Дж. Шенфилд. *Математическая логика*. М.: Наука, 1975.

К разделу 2

- 1) Борович З.И., Шафаревич И.Р., Теория чисел, М., Наука, 1985.
- 2) Бухштаб А.А., Теория чисел, М., Просвещение, 1960.
- 3) Виноградов И.М., Основы теории чисел, М., Наука, 1981.
- 4) Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б., Введение в теорию чисел, М., МГУ, 1995
- 5) Карацуба А.А., Основы аналитической теории чисел, М., Наука, 1983.
- 6) Кейперс Л., Нидеррейтер Г., Равномерное распределение последовательностей, М., Наука, 1985.
- 7) Коробов Н.М., Тригонометрические суммы и их приложения, М., Наука, 1989.
- 8) Серр Ж.П., Курс арифметики, М., Мир, 1972.
- 9) Чандрасекхаран К., Введение в аналитическую теорию чисел, М., Мир, 1974.

К разделу 3

- 1) Яблонский С. В. Введение в дискретную математику. М.: Высшая школа, 2001.
- 2) Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. М.: Наука, 1985.

- 3) Мальцев А. И. Алгоритмы и вычислимые функции. М.: Наука, 1986.
- 4) Оре О. Теория графов. М.: Наука, 1980
- 5) Кибернетический сборник. Вып. 1-9; вып. 1-28 (новая серия). М.: Мир, 1960-1990.
- 6) Дискретная математика и математические вопросы кибернетики. Том I. / Под общ. ред. С. В. Яблонского и О. Б. Лупанова. М.: Наука, 1974.
- 7) Нигматуллин Р. Г. Сложность булевых функций. М.: Наука, 1991.
- 8) Проблемы кибернетики. Вып. 1-41. М.: Наука, 1959-1984.
- 9) Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И. Лекции по теории графов. М.: Наука, 1990.
- 10) Труды Математического института им. В. А. Стеклова. Том 51 М.: Изд-во АН СССР, 1958.
- 11) Математические вопросы кибернетики. Вып. 1-19. М.: Наука, 1988-2019.
- 12) МакВильмс Ф. Дж., Слоэн Н. Дж. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
- 13) Форд Л., Фалкерсон Р. Потoki в сетях. М.: Мир, 1966.
- 14) Пападимитриу Х., Стайглиц К. Комбинаторная оптимизация. М.: Наука, 1985.
- 15) Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

К разделу 4

- 1) М. Атья, И. Макдональд. Введение в коммутативную алгебру. Москва, Факториал Пресс, 2003.
- 2) Ю. А. Бахтурин. Основные структуры современной алгебры. Москва, Наука, 1990.
- 3) Н. Бурбаки. Коммутативная алгебра. Москва, Мир, 1971.
- 4) Э. Б. Винберг. Курс алгебры. Москва, МЦНМО, 2013.
- 5) А. И. Кострикин. Введение в алгебру. Часть III: Основные структуры алгебры. Москва, МЦНМО, 2009.
- 6) М. И. Каргаполов, Ю. И. Мерзляков. Основы теории групп. Москва, Наука, 1982.
- 7) Д. Кокс, Дж. Литтл, Д. О'Ши. Идеалы, многообразия и алгоритмы. Москва, Мир, 2000.
- 8) К. Кэртис, И. Райнер. Теория представлений конечных групп и ассоциативных алгебр. Москва, Наука, 1969.
- 9) И. Ламбек. Кольца и модули. Москва, Факториал, 2005.
- 10) С. Ленг. Алгебра. Москва, Мир, 1968.
- 11) Р. Пирс. Ассоциативные алгебры. Москва, Мир, 1986.
- 12) В. В. Прасолов. Многочлены. Москва, МЦНМО, 2003.
- 13) Ж.-П. Серр. Линейные представления конечных групп. Москва, Мир, 1970.
- 14) Дж. Хамфрис. Введение в теорию алгебр Ли и их представлений. Москва, МЦНМО, 2003.

- 15) И. Херстейн. Некоммутативные кольца. Москва, Мир, 1972.
- 16) И. Р. Шафаревич. Основы алгебраической геометрии. Том 1. Москва, Наука, 1988.

v. Дополнительная литература:

К разделу 3:

- 1) Лупанов О. Б. Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984.
- 2) Сэвидж Дж. Э. Сложность вычислений. М.: Факториал, 1998.
- 3) Марков А. А. Введение в теорию кодирования. М.: Наука, 1982.
- 4) Орлов В. А. Простое доказательство алгоритмической неразрешимости некоторых задач о полноте автоматных базисов. // Кибернетика. 1973 № 4 С. 109-113.
- 5) Редькин Н. П. Надежность и диагностика схем. М.: Изд-во МГУ, 1992.
- 6) Соловьев Н. А. Тесты (теория, построение, применения). Новосибирск: Наука, 1978.
- 7) Дистель Р. Теория графов. Новосибирск: Изд-во Института математики, 2002.
- 8) Угольников А. Б. Эквивалентные преобразования формул в P_2 // Вестник Моск. ун-та. Серия 1 Матем. Механ. 2009 № 5 С.25-32.

vi. Авторы временной программы:

- 1) Академик РАН, проф. Семёнов Алексей Львович
- 2) Академик РАН, проф. Орлов Дмитрий Олегович
- 3) Член-корр. РАН, проф. Нестеренко Юрий Валентинович
- 4) Проф. Кочергин Вадим Васильевич
- 5) Проф. Гасанов Эльяр Эльдарович
- 6) Доц. Тимашев Дмитрий Андреевич