МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. М.В.ЛОМОНОСОВА

Факультет Вычислительной математики и кибернетики

Вопросы к экзамену по курсу «Прикладная алгебра»

(5 семестр, III поток)

1. Конечное поле и его характеристика. Мультипликативная группа, примитивный элемент поля Галуа и его нахождение. Основная теорема алгебры.
2. Алгоритм Евклида и его применение.
3. Теорема Безу и расширенный алгоритм Евклида.
4. Неприводимые многочлены: существование и нахождение неприводимых многочленов в конечных полях.
5. Построение конечных полей с помощью неприводимых многочленов (привести пример). Изоморфизм конечных полей.
6. Векторное пространство многочленов. Базис в $\mathbb{F}_p^n$. Поля Галуа как векторные пространства. Подполя конечного поля.
7. Минимальные многочлены над конечным полем: примеры и свойства. Корнями какого многочлена являются все элементы конечного поля? Делителями какого многочлена являются все неприводимые многочлены *n*-й степени?
8. Теорема о степени любого неприводимого делителя многочлена $x^{p^n-1}-1$.
9. Теорема о корнях неприводимого многочлена. Многочлены над конечным полем: решение уравнений.
10. Алгоритм нахождения всех корней многочлена *f(x)* над полем $\mathbb{F}_p$.
11. Мультипликативная группа расширения поля. Существование неприводимого многочлена степени *n* над полем $\mathbb{F}_p$.
12. Лемма о числе неприводимых нормированных многочленов из $\mathbb{F}_p^n$. Среднее число неприводимых многочленов.
13. Изоморфизм полей Галуа с одинаковым числом элементов.
14. Теорема о неприводимом нормированном многочлене-делителе порождающего элемента идеала.
15. Циклическое пространство: определение и примеры.
16. Количество и степени неприводимых делителей x^n-1.
17. Задачи построения кодов, исправляющих ошибки. Основные понятия метрики на единичном кубе.

18. Групповые (линейные) коды: определения, свойства. Кодовое расстояние. Построение кода как задача плотной упаковки.
19. Линейные коды. Порождающая и проверочная матрица. Систематическое кодирование и синдромное декодирование. Примеры.
20. Теорема Хэмминга. Пример построения кода Хэмминга.
21. Коды Хэмминга как частный случай кодов БЧХ. Алгоритм декодирования. Примеры.
22. Циклические коды. Порождающий и проверочный полином. Систематическое кодирование и синдромное декодирование. Примеры.
23. Коды БЧХ как частный случай циклических кодов. Идея построения кода БЧХ и оценка его кодового расстояния.
24. Декодирование БЧХ кодов. Синдромный полином и полином локаторов ошибок. Ключевое уравнение. Декодеры PGZ и Евклида. Примеры.
25. Действие группы на множестве: два определения. g-циклы, тип перестановки. Орбиты.
26. Неподвижные точки группы преобразований: фиксатор и стабилизатор. Лемма Бёрнсайда.
27. Группы вращений платоновых тел. Примеры.
28. Применение леммы Бёрнсайда для решения комбинаторных задач. Примеры.
29. Действие группы вращений куба на его элементы.
30. Цикловой индекс: определение и свойства. Вычисление числа орбит через цикловой индекс. Примеры.
31. Решения комбинаторной задачи об ожерельях.
32. Решения комбинаторной задачи о раскраски элементов куба.
33. Теорема Редфилда-Пойа и её применение для решения комбинаторных задач. Примеры.
34. Частично упорядоченные множества: определение, примеры, основные понятия. Диаграммы Хассе и особые элементы частично упорядоченного множества.
35. Ранжированные частично упорядоченные множества. Цепное условие Жордана-Дедекинда. Порядковые гомоморфизмы.
36. Идеалы и фильтры частично упорядоченных множеств. Конусы. Точные грани.
37. Операции над частично упорядоченными множествами.
38. Теорема Шпильрайна. Линейное продолжение частично упорядоченного множества и топологическая сортировка.
39. Линеаризации частично упорядоченного множества и вероятностное пространство над ними. *XYZ*-теорема. Проблема сортировки и «*1/3 - 2/3 предположение*».
40. Спектр и размерность частично упорядоченного множества. Свойства размерности, d-несводимые множества и проблема Ногина.

41. Решёточно упорядоченное множество, алгебраические решётки и их эквивалентность. Примеры.
42. Гомоморфизмы решёток, связь порядкового и решёточного гомоморфизмов. Сечения Макнила.
43. Идеалы решёток. Модулярные и дистрибутивные решётки. Критерии модулярности и дистрибутивности решётки.
44. Неразложимые элементы решёток и представление произвольных элементов решётки через неразложимые. Изоморфизм частично упорядоченного множества и неразложимых элементов решётки его порядковых идеалов.
45. Фундаментальная теорема о конечных дистрибутивных решётках.
46. Задача классификации по прецедентам. Закон обратного отношения между содержанием и объёмом понятия. Соответствия Галуа.
47. Анализ формальных понятий. Формальные объём и содержание. Решётка формальных понятий.
48. Гипотезы при решении задачи классификации методом анализа формальных понятий. Простейшее решающее правило классификации.

Литература

1. *Воронин В.П.* Дополнительные главы дискретной математики. - М.: ф-т ВМК МГУ, 2002 [http://padabum.com/d.php?id=10281].
2. *Гуров С.И.* Булевы алгебры, упорядоченные множества, решетки: Определения, свойства, примеры. -М.: Либроком, 2013.
3. *Журавлёв Ю.И., Флёров Ю.А., Вялый М.Н.* Дискретный анализ. Основы высшей алгебры. - М.: МЗ Пресс, 2007.
4. *Лидл Р., Нидеррайтер Г.* Конечные поля: В 2-х т. - М.: Мир, 1988.
5. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. - М.: Связь, 1979.
6. *Нефёдов В.Н., Осипова В.А*. Курс дискретной математики. - М.: Изд-во МАИ, 1992.
7. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. - М.: Мир, 1976.