

Теоретический минимум к экзамену по курсу «Прикладная алгебра»

(5 семестр, III поток)

Незнание ответа на *любой* из нижеследующих вопросов автоматически влечет неудовлетворительную оценку за экзамен. Данные вопросы являются лишь необходимым требованием, т.е. знание ответов только на них не обеспечивает положительной оценки за экзамен.

1. Понятие группы, подгруппы, факторгруппы, индекса группы по подгруппе. Примеры. Теорема Лагранжа.
2. Понятие циклической группы. Структура подгрупп циклической группы. Количество порождающих элементов.
3. Понятие кольца, подкольца, факторкольца, евклидова кольца, идеала в кольце. Примеры.
4. Расширенный алгоритм Евклида и его применение.
5. Понятие поля. Построение конечных полей с помощью неприводимых многочленов (привести пример). Полиномиальное и степенное представление элементов поля.
6. Алгоритм нахождения всех корней многочлена $f(x)$ над полем \mathbb{F}_p .
7. Минимальные многочлены для элементов конечного поля. Алгоритм нахождения минимального многочлена.
8. Теорема Хэмминга. Пример построения кода Хэмминга.
9. Коды БЧХ: определение, примеры кодов с исправлением одной, двух и трех ошибок.
10. Коды БЧХ: общая схема декодирования.
11. Понятие действия группы на множестве, фиксатор и стабилизатор. Примеры.
12. Лемма Бернсайда и её применение.
13. Цикловой индекс действия группы.
14. Группы симметрий правильных многоугольников (диэдральные группы) и группы вращений правильных многогранников. Примеры. Их цикловые индексы.
15. Теорема Редфилда-Пойа и её применение.