

Алгебра и теория чисел :: занятие 04 (09.03.2010)

День 1 (09.03.2010)

Задачи 1. Дискретное логарифмирование, перестановки и неабелевы группы

- A. disclog Дискретное логарифмирование
- B. permorder Порядок перестановки
- C. nonabelian Неабелева группа

Лекция 1. (Теория) Основы теории групп

1. Определение полугруппы, моноида, группы
2. Единственность единицы и обратного элемента в группе
3. Абелева группа, конечная группа, изоморфизм групп
4. Примеры групп
 - a. Группа целых чисел \mathbb{Z}
 - b. Группа остатков по модулю $n - \mathbb{Z}/n\mathbb{Z}$
 - c. Группа движений плоскости
 - d. Группа симметрий фигуры F
 - e. Группа перестановок S_n (симметрическая группа степени n)
 - f. Группа четных перестановок A_n (знакопеременная группа степени n)
 - g. Группа невырожденных матриц $n \times n$ (общая линейная группа, GL_n)
 - h. Группа матриц $n \times n$ с единичным определителем (специальная линейная группа, SL_n)
5. Порядок элемента группы, циклические группы, конечно порожденные группы, p -группы
6. Подгруппа, примеры
7. Теорема о подгруппах циклической группы
8. Представление конечных групп перестановками (регулярное представление группы)
9. Смежные классы, теорема Лагранжа, нормальные подгруппы, факторгруппы
10. * Гомоморфизмы и изоморфизмы, образ и ядро, теорема о нормальности ядра
11. * Теорема о изоморфности образа и фактор группы по ядру при гомоморфизме

Лекция 2. (Практика) Основы теории групп

1. Вычисление порядка элемента в группе
2. Вычисление порядка перестановки в группе S_n
3. Дискретное логарифмирование в группе
4. Действие группы на множестве
 - a. Орбита элемента множества
 - b. Стабилизатор элемента множества
 - c. Множество неподвижных точек элемента группы
5. Лемма Бернсайда, задача о числе ожерелий