

## Программа экзамена, первый семестр

1. Определение коммутативной группы. Единственность нейтрального и обратного элементов. Подгруппа. Циклическая группа. Порядок элемента. Порядки элементов в циклической группе. Подгруппы циклической группы.
2. Коммутативное кольцо. Единственность единицы.  $0 * a = 0, (-1) * a = -a$ . Делители нуля. Целостные кольца. Обратимые элементы. Поля. Примеры.
3. Идеалы в коммутативных кольцах. Сумма и пересечение идеалов. Конечны порожденные идеалы. Главные идеалы.
4. Гомоморфизм колец.  $\ker f$  — идеал,  $\operatorname{im} f$  — подкольцо.  $f(0) = 0$ . Для целостных колец  $K_1, K_2$  и гомоморфизма  $f : K_1 \rightarrow K_2$  верно, что либо  $\ker f = K_1$ , либо  $f(1) = 1$ .
5. Фактор кольцо. Теорема о гомоморфизме колец.
6. Евклидово кольцо. Деление с остатком. Алгоритм Евклида. Существование НОД. Евклидово кольцо — кольцо главных идеалов. Линейное представление НОД. Взаимная простота.
7. Неприводимые элементы кольца. В кольце главных идеалов  $K$  для неприводимого  $p \in K$  идеал  $(p)$  максимальный, простой и  $K/(p)$  поле.
8. Кольцо главных идеалов факториально.
9. Деление с остатком в целых числах  $\mathbb{Z}$ , в любом поле  $\mathbb{k}$ , в кольце многочленов над полем  $\mathbb{k}[x]$ , в кольце формальных степенных рядов  $\mathbb{k}[[x]]$ , в кольце целых гауссовых чисел  $\mathbb{Z}[i]$ , в кольце целых чисел Эйзенштейна  $\mathbb{Z}[w]$ , где  $w^2 + w + 1 = 0$ ,  $\mathbb{Z}[\sqrt{2}]$ .
10. Целые гауссовы числа  $\mathbb{Z}[i]$ . Евклидово кольцо, идеалы, факториальность, простые целые гауссовы числа. Разложение натурального числа в сумму двух квадратов целых чисел. Поля  $\mathbb{Z}[i]/(p)$ .
11. Все идеалы в  $\mathbb{k}[[x]]$ . Обратимые и неприводимые в  $\mathbb{k}[[x]]$ .
12. Примеры нефакториальных целостных колец в которых существует разложение на неприводимые  $\mathbb{Z}[\sqrt{-5}]$ ,  $\mathbb{Z}[\sqrt{5}]$ .
13. Прямое произведение колец. Китайская теорема об остатках.
14. Поле. Характеристика поля. Конечная характеристика поля — простое число.
15. Поля  $\mathbb{Z}/(p)$ . Малая теорема Ферма  $x^p - x = 0 \pmod{p}$ . Теорема Вильсона  $(p-1)! = -1 \pmod{p}$ .
16. Группа обратимых элементов кольца  $(\mathbb{Z}/(m))^*$  и функция Эйлера  $\varphi(m) = \#(\mathbb{Z}/(m))^*$ ,  $\varphi(p^n)$ , мультипликативность функции Эйлера для взаимно простых чисел.
17. Многочлены. Теорема Безу для многочленов над полем. Сколько может быть корней у многочлена степени  $n$  в поле.
18. Интерполяционный многочлен Лагранжа.
19. Расширения полей. Алгебраическое расширение поля. Присоединение корня неприводимого многочлена.
20. Поле разложения для многочлена.
21. Число элементов в конечном поле  $p^n$ . Построение поля  $\mathbb{F}_{p^n}$ . Изоморфизм полей с одинаковым количеством элементов.
22. Эндоморфизм Фробениуса для поля с конечной характеристикой.
23. Циклическая мультипликативная группа конечного поля.
24. Поле частных целостного кольца.

25. Факториальное кольцо. Неприводимые и простые элементы факториального кольца.
- 26 (Лемма Гаусса). Многочлен  $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  с коэффициентами в факториальном кольце  $R$  с содержанием  $\text{cont}(f) = \text{НОД}(a_0, a_1, \dots, a_n) = 1$  неприводим в кольце многочленов над полем частных  $Q_R[x]$  факториального кольца  $R$ , если и только если он неприводим в кольце многочленов над самим кольцом  $R[x]$ .
27. Факториальность кольца многочленов  $\mathbb{Z}[x]$ .
28. Критерий Эйзенштейна неприводимости многочлена.

$$\Phi_p = x^{p-1} + x^{p-2} + \dots + x + 1$$

неприводимый над  $\mathbb{Q}$  многочлен, если  $p$  - простое.

29. Разложение рациональной функции в сумму простейших дробей.
30. Линейная рекуррентная последовательность. Рациональные производящие функции. Характеристический многочлен оператора сдвига  $\varphi(t) \mapsto \frac{\varphi(t) - \varphi(0)}{t}$ .
31. Формула Бине для чисел Фибоначчи.
32. Общий вид  $k$ -го элемента линейной рекуррентной последовательности.
33. Рациональная производящая функция и линейное рекуррентное соотношение для последовательности  $z_k = P_n(k)$ , где  $P_n$  - многочлен степени  $n$ .
34. Симметрические многочлены. Элементарные симметрические многочлены. Теорема Виета.
35. Лексикографический порядок на мономах. Старший моном произведения многочленов. Вид старшего монома симметрического многочлена. Основная теорема о симметрических многочленах.
36.  $s_k = \sum_{i=1}^n x_i^k$ . Производящая функция для элементарных симметрических многочленов и ее логарифмическая производная. Тождества Ньютона для  $s_k$  и  $\sigma_i$ .

## Список литературы

- [1] В.СЕНДЕРОВ, А.СПИВАК, Суммы квадратов и целые гауссовы числа
- [2] А. И. Кострикин Введение в алгебру. Часть 1
- [3] А.Л.Городенцев. Алгебра–1
- [4] А.Л.Городенцев. Алгебра–2
- [5] Э.Б. Винберг, Курс Алгебры