## Дискретная математика. 3 семестр.

Для сдачи экзамена необходимо знать:

**Определения:** транспортная сеть, поток в транспортной сети, мощность потока, двудольный граф, паросочетание, совершенное паросочетание, задача об оптимальном назначении кольцо, идеал, алгебра, поле, характеристика поля, кольцо многочленов, кольцо формальных степенных рядов, изоморфизм колец, мультипликативная группа кольца, неприводимый многочлен, минимальный многочлен элемента алгебры, отображение Фробениуса.

**Алгоритмы:** алгоритм Форда-Фалкерсона, венгерский алгоритм, алгоритм нахождения оптимального назначения.

**Для сдачи экзамена необходимо уметь проводить вычисления:** сложение, умножение и обращение формальных степенных рядов, проверка неприводимости многочлена над конечным полем, перечисление неприводимых многочленов малых степеней над малыми конечными полями, явное описание фактор-кольца кольца многочленов по идеалу, порожденному данным многочленом, построение конечного поля из $p^n$ элементов, нахождение порядка заданного элемента (по умножению), нахождение минимального многочлена заданного элемента алгебры.

**Теоремы.**

1) Корректность алгоритма Форда-Фалкерсона.
2) Корректность венгерского алгоритма.
3) Корректность алгоритма нахождения оптимального назначения.
4) Поток в транспортной сети. Определение мощности потока.
5) Сумма значений потока в транспортной сети на ребрах любого разреза равна мощности потока.
6) Теорема Форда-Фалкерсона.
7) Теорема Менгера (реберная).
8) Теорема Холла.
9) Определение характеристики поля. Любое конечное поле содержит простое подполе $\mathbb{F}_p$.
10) Теорема о делении многочленов с остатком. Теорема Безу.
11) Определение идеала. Любой идеал кольца многочленов порожден одним элементом.
12) Определение идеала. Перечисление идеалов кольца формальных степенных рядов.
13) Многочлен над полем степени $n$ имеет не более $n$ корней. Пример многочлена над кольцом, имеющего больше корней, чем его степень.
14) Теорема о разрешимости диофантова уравнения в кольце многочленов над полем: если многочлены $A(t)$ и $B(t)$ не имеют общих множителей, то существуют такие многочлены $X(t)$ и $Y(t)$, что $A(t)X(t) + B(t)Y(t) = 1$.

15) Теорема об однозначности разложения многочлена над полем на неприводимые множители. Пример многочлена над кольцом, для которого это не так.

16) Конечное кольцо без делителей нуля есть поле. Конечномерная алгебра без делителей нуля есть поле.

17) Пусть $\mathbb{K}$ — поле, дан многочлен ненулевой степени $P(t) \in \mathbb{K}[t]$. Конструкция фактор-кольца $\mathbb{L} = \mathbb{K}[t]/(P(t))$. Доказательство того, что $\mathbb{L}$ поле тогда и только тогда, когда многочлен $P(t)$ неприводим.

18) Пусть $\mathbb{K}$ — поле, дан неприводимый многочлен ненулевой степени $P(t) \in \mathbb{K}[t]$. Конструкция фактор-кольца $\mathbb{L} = \mathbb{K}[t]/(P(t))$. Доказательство того, что многочлен $P(t)$ имеет корень в $\mathbb{L}$.

19) Конечное поле характеристики $p$ содержит $p^n$ элементов.

20) Любой ненулевой элемент конечного поля из $p^n$ элементов удовлетворяет уравнению $x^{p^n-1} - 1 = 0$.

21) Отображение Фробениуса $\Phi(x) = x^p$. Его свойства.

22) Пусть неприводимый многочлен $P(t) \in \mathbb{F}_p[t]$ степени $n$ имеет в поле $\mathbb{F}_{p^n}$ корень $\alpha$. Тогда $P(t)$ имеет в $\mathbb{F}_{p^n}$ ровно $n$ различных корней, получающихся из одного из них применением автоморфизма Фробениуса.

23) Конечная подгруппа мультипликативной группы поля циклическая.

24) Многочлен 2 и 3 степени неприводим, если он не имеет корней. Пример приводимого многочлена более высокой степени, не имеющего корней.

25) Существование неприводимых многочленов любой степени над полем $\mathbb{F}_p$. Число неприводимых многочленов степени $n$ над $\mathbb{F}_p$, задающих последовательности максимального возможного периода $p^n - 1$.

26) Периодические последовательности, задаваемые многочленом над конечным полем; возможные значения периода в случае, когда многочлен неприводим. Оценка сверху на длину периода в случае приводимого многочлена (в простейшем случае произведения двух разных неприводимых многочленов).

27) Производящий ряд последовательности. Линейные рекуррентные последовательности. Производящий ряд линейной рекуррентной последовательности есть рациональная функция.

28) Периодическая последовательность, задаваемая неприводимым многочленом над конечным полем, является линейной рекуррентной последовательностью.