Дискретная математика. Основные тезисы.

(К экзамену)

1. Два множества A и B называются *равными* $(A = B)$, если они состоят из одних и тех же элементов.
2. Множество A называется *подмножеством* множества B если любой элемент множества A принадлежит множеству B.
3. Если $A \subset B$ и $A \neq B$, то A называется *собственным подмножеством* B. В этом случае B содержит хотя бы один элемент, не принадлежащий A.
4. *Объединением* множеств A и B (обозначение $A \cup B$) называется множество элементов x таких, что x принадлежит хотя бы одному из двух множеств A или B
5. *Пересечением* множеств A и B (обозначение $A \cap B$) называется множество, состоящее из элементов x, которые принадлежат и множеству A и множеству B
6. *Разностью* множеств A и B называется множество всех тех элементов множества A, которые не принадлежат множеству B
7. *Симметрической разностью* множеств A и B называется множество $A \Delta B = (A \setminus B) \cup (B \setminus A)$
8. *Абсолютным дополнением* множества A называется множество всех элементов, не принадлежащих A, т.е. множество $\overline{A} = U \setminus A$, где U – универсальное множество
9. Свойства операций *1. Коммутативность объединения и пересечения*

   2. Ассоциативность объединения и пересечения

   3.Дистрибутивность пересечения относительно объединения и объединения относительно пересечения

   4.Идемпотентность объединения и пересечения

   5.Свойства универсального и пустого множеств

   6.Закон двойного дополнения

   7.Законы де Моргана

10. Парадокс Рассела. Рассмотрим множество F, содержащее те и только те множества, которые не являются элементами самих себя: $F = \{ M \mid M -$ множество и $M \notin M \}$. Парадокс состоит в том, что после такого способа задания множества F мы не можем однозначно ответить на вопрос: само множество F *как элемент* принадлежит F или нет?
11. Множество всех подмножеств данного множества называют *булеаном* множества.
12. $A = \{1,2,3,4,...,n\}$, т.е. $|A| = n$. Доказать, что мощность множества $\mathcal{B}(A)$ = 2^n

13. *Упорядоченной парой* называют пару элементов (x, y) такую, что равенство двух пар $(x, y) = (a, b)$ возможно тогда и только тогда, когда $x = a$ и $y = b$.
14. *Прямым (декартовым) произведением* двух множеств A и B называется множество $A \times B = \{(x, y) \mid x \in A,\ y \in B\}$
15. Три свойства прямого произведения
16. *Соответствием* между множествами A и B называют любое подмножество G их прямого произведения.
17. *Областью определения соответствия* (или *первой проекцией*) называется множество $Dom\, G = np_1 G = \{\, x \mid (x, y) \in G \,\}$
18. *Областью значений соответствия* (или *второй проекцией*) называется множество $Im\ G = np_2 G = \{\, y \mid (x, y) \in G \,\}$
19. *Сечением соответствия* G *по элементу* x_0 называется множество $G|_{x_0} = \{y \mid (x_0, y) \in G\}$.
20. *Сечением соответствия* G *по элементу* y_0 называется множество $G|_{y_0} = \{y \mid (x, y_0) \in G\}$.
21. *Соответствием, обратным соответствию* G, называется множество $G^{-1} = \{(y, x) \mid (x, y) \in G\}$.
22. *Пустым* называется соответствие, которое не содержит ни одного элемента.
23. Соответствие называется *полным,* если $G = A \times B$.
24. Матрицы, каждый элемент которых равен нулю или единице, называются *булевыми*
25. *Дизъюнкция и конъюнкция* $\wedge$
26. Пусть заданы три множества X, Y и Z и два соответствия – $G_1 \subset X \times Y$ и $G_2 \subset Y \times Z$. Композицией соответствий G_1 и G_2 называется подмножество G_3 прямого произведения $X \times Z$: $G_3 = G_2 \circ G_1 = \{(x, z) \mid (x, y) \in G_1,\ (y, z) \in G_2\}$.
27. Композиция $G_2 \circ G_1 \neq \varnothing$, если пересечение $Dom\, G_2 \cap Im\, G_1 \neq \varnothing$.
28. Соответствие $G \subset X \times Y$ называется *отображением*, если область определения соответствия совпадает с множеством X (т.е. $Dom\, G = X$ или $np_1 G = X$).
29. Отображение называется ф*ункциональным* (или *однозначным*), если любое сечение $G|_x$ содержит только один элемент.
30. Шесть свойств отображений.
31. Отображение $f : X \to Y$ называется *сюръективным* или отображением *на* множество Y, если $\mathrm{Im} f = Y$. Другими словами, f сюръективно, если каждый элемент $y \in Y$ имеет хотя бы один прообраз, т.е. $\forall y \in Y\ \exists x \in X : y = f(x)$.
32. Отображение $f : X \to Y$ называется *инъективным*, если из условия $x_1 \neq x_2$ следует, что $f(x_1) \neq f(x_2)$, т.е. различные элементы множества X должны иметь различные образы.

33. Отображение называется *биективным* если оно одновременно сюръективно и инъективно.
34. Пусть заданы два отображения $f: X \to Y$ и $g: Y \to Z$. *Композицией отображений (сложным отображением, суперпозицией отображений)* называют отображение $\varphi: X \to Z$, определяемое условием $\varphi(x) = g \circ f(x) = g(f(x))$, $\forall x \in X$.
35. Композиция отображений ассоциативна, т.е. для заданных трех отображений $f: X \to Y$, $g: Y \to Z$, $h: X \to Z$, справедливо равенство $h \circ (g \circ f) = (h \circ g) \circ f$.
36. Отображение g называется *обратным* к отображению f если одновременно выполняются два условия $g \circ f = e_X$ и $f \circ g = e_Y$.
37. Когда справедливо только одно из двух условий, например, $g \circ f = e_X$, то g называют *левым обратным* отображением. Соответственно, если выполнено только второе равенство $f \circ g = e_Y$, то g называют *правым обратным* отображением.
38. Лемма. Если для композиции двух отображений выполняется равенство $g \circ f = e_X$, то g является сюръекцией, а f - инъекцией.
39. Теорема Отображение $f: X \to Y$ имеет обратное тогда и только тогда, когда f является биективным отображением.
40. Если $f: X \to Y$ биективно, то обратное отображение $f^{-1}: Y \to X$ также является биекцией, причем $\left(f^{-1}\right)^{-1} = f$.
41. Пусть $f: X \to Y$ и $g: Y \to Z$ биективные отображения. Тогда: композиция $g \circ f$ биективных отображений биективна. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
42. *Бинарной операцией* на множестве X называется любое фиксированное отображение $\varphi: X \times X \to X$.
43. Бинарная операция $*$ на множестве X называется *ассоциативной,* если $a*(b*c) = (a*b)*c$ для любых $a, b, c \in X$. Операция $*$ называется *коммутативной,* если $a*b = b*a$.
44. Элемент $e \in X$ называется *единичным* (или *нейтральным*) относительно бинарной операции $*$, если $e*x = x*e = x$ для любого элемента $x \in X$.
45. Единичный элемент является единственным.
46. Множество X с заданной на этом множестве ассоциативной операцией (т.е. алгебраическая структура $(X, *)$ с ассоциативной операцией) называется *полугруппой*.
47. Полугруппа с единичным элементом называется *полугруппой с единицей* или *моноидом*.
48. *Обратным* к элементу x моноида $(X, *, e)$ называется элемент $y \in X$ такой, что $xy = yx = e$.
49. Моноид $(X, *, e)$, у которого для каждого элемента $x \in X$ существует обратный элемент $x^{-1} \in X$, называется *группой*.
50. Четыре аксиомы, которым удовлетворяет группа.
51. *Мультипликативная и аддитивная группа.*

52. Группа с коммутативной бинарной операцией называется *коммутативной* или *абелевой.*
53. Непустое подмножество $H \subset G$ называется *подгруппой* группы G, если для любых $h_1, h_2 \in H$ элемент $h_1 * h_2 \in H$ и для любого $h \in H$ элемент $h^{-1} \in H$.
54. Подгруппа H, отличная от E и G, называется *собственной подгруппой* группы G.
55. Таблица *Кэли.*
56. Доказать, что каждый столбец (строка) таблицы *Кэли* содержит все элементы группы.
57. *Симметрической группой* S_n называется множество всех биективных отображений множества X на себя, снабженное бинарной операцией композиции отображений.
58. Циклическая группа содержит все возможные целые степени одного и того же элемента a.
59. Если циклическая группа содержит только элементы e, a, $a^2, \ldots, a^n$, то такую циклическую группу называют *конечной* (Card $G = n$). Если же для любого натурального n все степени a^n различны, то G называется *бесконечной* циклической группой.
60. Сравнение по модулю m является отношением эквивалентности.
61. Группы G и H называются *изоморфными* (обозначение $G \prec H$), если существует биективное отображение $f: G \to H$, «сохраняющее» групповую операцию, т.е. $f(x * y) = f(x) \circ f(y)$.
62. Три свойства изоморфизма.
63. **Теорема** Кэли. Любая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n (без доказательства).
64. **Теорема.** Любая циклическая группа порядка m изоморфна группе $\mathbf{Z}_m$ классов вычетов по модулю m (без доказательства).
65. Пусть K есть непустое множество, на котором заданы две бинарные операции: $+$ (сложение) и $\bullet$ (умножение), удовлетворяющие следующим условиям: структура (K, $+$) является абелевой (коммутативной) группой; структура (K, $\bullet$) есть полугруппа; операции сложения и умножения связаны законом дистрибутивности: $(a+b)\cdot c = a\cdot c + b\cdot c$ и $c\cdot(a+b) = c\cdot a + c\cdot b$ для любых $a, b, c \in K$. Алгебраическая структура (K, $+$, $\bullet$), подчиненная этим требованиям, называется *кольцом*. При этом структура (K, $+$) называется аддитивной группой кольца, а структура (K, $\bullet$) называется его мультипликативной полугруппой.
66. Кольцо (K, $+$, $\bullet$) называется *полем,* если выполняются следующие условия: структура (K, $+$, 0) – абелева группа; структура ($K \setminus \{0\}$, $\bullet$, 1) – коммутативная группа; выполняется закон дистрибутивности $a\cdot(b+c) = a\cdot b + a\cdot c$ для любых $a, b, c \in K$.
67. **Теорема.** Кольцо классов вычетов ($\mathbf{Z}_m$, $+$, $\bullet$) тогда и только тогда является полем, когда m есть простое число.