1. *Множества, подмножества. Способы определения множеств. Равенство множеств. Операции над множествами (объединение, пересечение, разность, симметрическая разность, дополнение). Методы доказательства теоретико-множественных тождеств.*

~~~ ~~~

• Множество – совокупность объектов, заданных перечислением ($A = \{4,8,15,16,23,42\}$), или указанием какого-либо их общего свойства, называемым коллективизирующим ($B = \{x \in \mathbb{R}, x \geq 0\}$). Множество называется пустым, если оно не содержит элементов

• Пусть A и B множества. Тогда A является подмножеством B, если любой элемент из A является элементом B. A равно B, если любой элемент из A является элементом B и наоборот.

• Пусть $A, B \subseteq U$ (универсум). По определению,

- пересечение $A \cap B = \{x \in U\colon\ x \in A, x \in B\}$;
- объединение $A \cup B = \{x \in U\colon\ x \in A\ \vee\ x \in B\}$; *//логическое или, дизъюнкция*
- разность $A \backslash B = \{x \in U\colon\ x \in A, x \notin B\}$
- симметрическая разность $A \Delta B = \{(A \backslash B) \cup (B \backslash A)\}$
- дополнение $\bar{A} = U \backslash A$

• Теоретико-множественными тождествами называют равенства $A \cup B = B \cup A,\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ и т.п., верные для любых входящих в них множеств. Доказать эти равенства можно

- методом двух включений (доказать что если x принадлежит левой части, то он принадлежит и правой, и наоборот)
- методом характеристических функций (основывается на свойствах характеристических функций вида $\Phi_A(x) = \begin{cases} 1, x \in A \\ 0, \text{иначе} \end{cases}$)
- методом эквивалентных преобразований (основывается на использовании ранее доказанных тождеств).

//наставление автора: там 22 свойства для двух включений и 7 для харфункций, всё было на первом семинаре, учите и обрящете)

2. *Неупорядоченная пара, упорядоченная пара, кортеж. Декартово произведение множеств.*

~~~ ~~~

• Пусть A и B – произвольные множества.

Неупорядоченной парой на множествах A и B называется любое множество $\{a, b\}$, где $a \in A,\ b \in B$ или $a \in B, b \in A$. Если A=B, то говорят о неупорядоченной паре на множестве A.

Упорядоченная пара (a,b) на множествах A и B определяется не только самимим элементами $a \in A,\ b \in B,$ но и порядком, в котором они записаны.

Кортеж (упорядоченный n-набор) $(a_1, \dots, a_n)$ на множествах $A_1, \dots, A_n$ характеризуется не только входящими в него элементами $a_1 \in A_1, \dots a_n \in A_n$, но и порядком, в котором они перечисляются; кортеж является обобщением понятия упорядоченной пары.

• Множество всех кортежей длины n на множествах $(A_1, \dots, A_n)$ называют декартовым произведением этих множеств и обозначают как $A_1 \times \dots \times A_n$. Если все множества $A_i,\ i = \overline{1,n}$ равны между собой, то декартово произведение называют n-й декартовой степенью множества A.

3. *Отображения: область определения, область значений. Инъективное, сюръективное и биективное отображения. Частичное отображение.*

~~~ ~~~

• Отображение f из множества A в множество B считается заданным, если каждому элементу $x \in A$ сопоставлен единственный элемент $y \in B;\ \ f\colon A \to B$. Элемент y называют образом элемента x при отображении f, элемент x – прообразом.

Множество всех $y \in B$ таких, что найдётся $x \in A$, для которого $y = f(x)$ называют областью значений отображения f, R(f).

• Отображение $f\colon A \to B$ называют:

- инъективным, если каждый элемент из области его значений имеет единственный прообраз, т.е. из равенства $f(x1) = f(x2)$ следует равенство x1=x2.
- сюръективным, если его область значений совпадает со всем множеством B (сюръективное отображением ИЗ A в B называют также отображением A НА B).
- биективным, если оно одновременно инъективно и сюръективно – т.е. каждому элементу множества A отвечает единственный элемент множества B и наоборот.

• Отображение называется частичным, если образ определен не для каждого элемента множества A, а для некоторых элементов этого множества.

4. *Соответствия. График и граф соответствия, область определения, область значения. Сечение соответствия. Сечение соответствия по множеству. Функциональность соответствия по компоненте. Бинарные и n-арные отношения. Связь между отношениями, соответствиями и отображениями.*

~~~ ~~~

• Если каждому элементу $x \in A$ сопоставлен не один, а несколько образов $y \in B$, то говорят, что задано соответствие из множества A в множество B.

• График соответствия p из множества A в множество B можно определить как множество C_p упорядоченных пар (x,y) таких, что $x \in A, y \in B$ и элементы x,y связаны соответствием p, т.е. $y \in p(x)$.

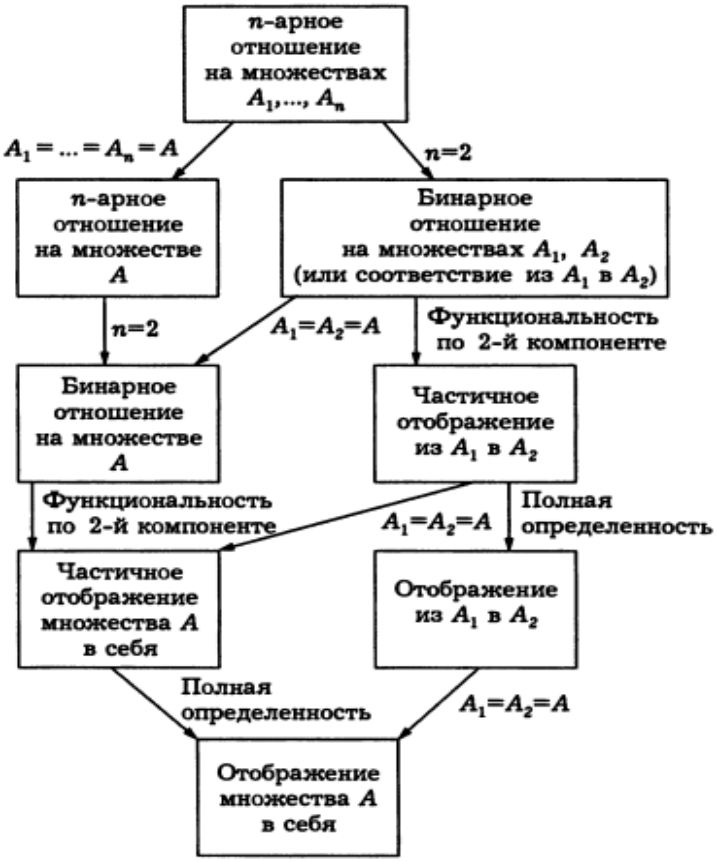
Область определения соответствия $\rho \subseteq A \times B$ из множества A в B – это множество всех первых компонент упорядоченных пар из ρ, $D(\rho) = \{x\colon (\exists y \in B)(x, y) \in \rho\}$. Область значения соответствия – множество всех вторых компонент упорядоченных пар, $R(\rho) = \{y\colon (\exists x \in A)(x, y) \in \rho\}$.

• Сечением соответствия p для фиксированного элемента $x \in A$ называется множество $\rho(x) = \{y\colon (x, y) \in \rho\}$; сечение соответствия p(x) есть множество всех образов элемента x при данном соответствии. Сечением соответствия по множеству $C \subseteq A$ называется множество $\rho(C) = \{y\colon (x, y) \in \rho, x \in C\}$.

• Соответствие $\rho \subseteq A \times B$ называется функциональным по первой компоненте, если для любых двух упорядоченных пар $(x, y) \in \rho,\ (x', y') \in \rho$ из равенства y=y' следует равенство x=x'; функциональным по второй компоненте, если из x=x' следует

y=y'. *(//1 – два x не могут вести в один y, 2 – один x не может вести в два y).*

• n-арным отношением на множествах $A_1, \dots, A_n$ называют произвольное подмножество ρ декартова произведения $A_1 \times \dots \times A_n$; в случае n=2 говорят о бинарном отношении на множествах A1 и A2 – соответствии из A1 в A2, где эти множества в общем случае различны.



5. *Композиция соответствий, обратное соответствие и их свойства (с доказательством).*

~~~ ~~~

Композицией соответствий $\rho \subseteq A \times B$ и $\sigma \subseteq B \times C$ называют соответствие $\rho \circ \sigma = \{ (\exists z \in B)\ (x,z) \in \rho) \wedge ((z,y) \in \sigma) \}$. Соответствие, обратное соответствию $\rho \subseteq A \times B$, есть соответствие из B в A, обозначаемое $\rho^{-1} = \{(y,x) : (x,y) \in \rho\}$.

Основные свойства:

1) $\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau$ — *ассоциативность*
2) $\forall \rho:\ \rho \circ \emptyset = \emptyset \circ \rho = \emptyset$ — *аннулирующее свойство*
3) $\rho \circ (\sigma \cup \tau) = (\rho \circ \sigma) \cup (\rho \circ \tau)$ — *дистрибутивность по объединению*
4) $\forall \rho \in A^2:\ \rho \circ id_A = id_A \circ \rho = \rho$ — *нейтральный элемент*
5) $(\rho^{-1})^{-1} = \rho$
6) $(\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \rho^{-1}$.

Все доказательства проводятся методом двух включений. На примере свойства 3: пусть $(x,y) \in \rho \circ (\sigma \cup \tau)$. Тогда $\exists z:\ (x,z) \in \rho,\ (z,y) \in (\sigma \cup \tau)$. Последнее означает, что $(z,y) \in \sigma$ или $(z,y) \in \tau$; следовательно для элемента z: $[(x,z) \in \rho,\ (z,y) \in \sigma]$ или $[(x,z) \in \rho,\ (z,y) \in \tau]$. Первое возможно при $(x,y) \in (\rho \circ \tau)$, второе при $(x,y) \in (\rho \circ \tau)$, $\Longrightarrow$ $(x,y) \in (\rho \circ \sigma) \cup (\rho \circ \tau)$ - включение доказано. *//в обратную сторону аналогично, и аналогично же для всего остального, ну вы пони*

6. *Специальные свойства бинарных отношений на множестве (рефлексивность, иррефлексивность, симметричность, антисимметричность, транзитивность).*

~~~ ~~~

Бинарное отношение ρ на множестве A называют:

1) Рефлексивным, если $\forall x \in A\ (x,x) \in \rho$	$id_A \subseteq \rho$
2) Иррефлексивным, если $\forall x \in A\ (x,x) \notin \rho$	$id_A \cap \rho = \emptyset$
3) Симметричным, если для любых $x, y \in A$ из $x\ \rho\ y$ следует $y\ \rho\ x$	$\rho^{-1} = \rho$
4) Антисимметричным, если для любых $x, y \in A$ из $x\ \rho\ y$ и $y\ \rho\ x$ следует, что $x = y$	$\rho^{-1} \cap \rho \subseteq id_A$
5) Транзитивным, если для любых $x, y, z \in A$ из $x\ \rho\ y$ и $y\ \rho\ z$, следует $x\ \rho\ z$	$\rho \circ \rho \subseteq \rho$

7. *Классификация бинарных отношений на множестве: эквивалентность, толерантность, порядок, предпорядок, строгий порядок.*

~~~ ~~~

Бинарное отношение на *некотором* множестве называют:

1) Эквивалентностью, если оно рефлексивно, симметрично и транзитивно;	(Р _ С _ Т)
2) Толерантностью, если оно рефлексивно и симметрично;	(Р _ С _ _)
3) Порядком, если оно рефлексивно, антисимметрично и транзитивно;	(Р _ _ А Т)
4) Предпорядком, если оно рефлексивно и транзитивно;	(Р _ _ _ Т)
5) Строгим порядком, если оно иррефлексивно, антисимметрично и транзитивно.	(_ И _ А Т)
~~~

8. *Отношение эквивалентности. Класс эквивалентности. Фактор-множество.*

~~~ ~~~

• Бинарное отношение на некотором множестве называют эквивалентностью, если оно рефлексивно, симметрично и транзитивно.

• Пусть $\rho -$ эквивалентность на множестве A, и $x \in A$. Классом эквивалентности по отношению ρ называется множество элементов $\{y: y \in A,\ \ y\ \rho\ x\}$ (эквивалентных x); класс эквивалентности обозначается $[x]_\rho$.

• Фактор-множеством множества A по отношению ρ (обозначается A/ρ) называют множество всех классов эквивалентности по данному отношению на данном множестве.

9. *Отношения предпорядка и порядка. Наибольший, максимальные, наименьший и минимальные элементы. Точная нижняя и верхняя грани множества.*

~~~ ~~~

• Бинарное отношение на некотором множестве называют порядком, если оно рефлексивно, антисимметрично и транзитивно; предпорядком, если оно только рефлексивно и транзитивно.

• Упорядоченным множеством называют множество M вместе с заданным на нем отношением порядка $\leq$; элементы x и y упорядоченного множества $(M, \leq)$ называют сравнимыми, если $x \leq y$ или $y \leq x$, и несравнимыми в противном случае.

Пусть $(A, \leq) -$ упорядоченное множество. Элемент $a \in A$ называют:

1) наибольшим элементом множества A, если $\forall x \in A \ \ x \leq a$;
2) максимальным элементом множества A, если $\forall x \in A \ \ x \leq a$ или x и a не сравнимы
3) наименьшим, если $\forall x \in A \ \ a \leq x$;
4) минимальным, если $\forall x \in A \ \ a \leq x$ или a и x не сравнимы.

• Пусть также $B \subseteq A$. Элемент $a \in A$ называется верхней (нижней) гранью множества B, если для всех элементов $x \in B$ $x \leq a$ $\left(\text{или соответственно } (a \leq x)\right)$. Точной верхней (точной нижней) гранью B называют наименьший элемент множества всех верхних граней (соответственно наибольший элемент множества всех нижних граней); обозначается sup B (inf B) *//sup, /b/*

10. *Точная верхняя грань последовательности. Индуктивное упорядоченное множество. Теорема о неподвижной точке (с доказательством). Пример вычисления неподвижной точки.*

~~~ ~~~

• Последовательность $\{x_i\}_{i \in N}$ элементов упорядоченного множества $\mathcal{A} = (A, \leq)$ называют неубывающей, если $\forall i \in \mathbb{N} \ \ x_i \leq x_{i+1}$. Элемент a упорядоченного множества $\mathcal{A}$ называют точной верхней гранью последовательности $\{x_i\}_{i \in N}$, если он есть точная верхняя грань множества всех членов этой последовательности.

• Упорядоченное множество $\mathcal{A}$ называется индуктивно упорядоченным, если в нем есть наименьший элемент, а любая неубывающая последовательность элементов $\{a_n\}_{n \geq 0}$ имеет точную верхнюю грань.

• Пусть $(A, \leq), (B, \preccurlyeq) -$ индуктивные упорядоченные множества. Отображение $f: A \to B$ называется непрерывным, если справедливо равенство $f(\sup a_n) = \sup f(a_n)$. Элемент $a \in A$ называют неподвижной точкой отображения $f: A \to A$, если $f(a) = a$. Элемент a называют наименьшей неподвижной точкой отображения, если он является наименьшим элементом множества всех неподвижных точек отображения.

Теорема: любое непрерывное отображение f индуктивно упорядоченного множества $(M, \leq)$ $f: M \to M$ имеет наименьшую неподвижную точку.

Доказательство: Пусть $\mathbb{0}$ – наименьший элемент ИндуктивноУпорядоченногоМножества M. Построим последовательность $\{\mathbb{0}, f(\mathbb{0}), f(f(\mathbb{0})), \dots f^n(\mathbb{0}), \dots\}$, где $f^n(x) = f(f^{n-1}(x))$. Т.к. $\mathbb{0}$ – наименьший элемент, то $\mathbb{0} \leq f(\mathbb{0})$, т.е. при n=0 $f^n(\mathbb{0}) \leq f^{n+1}(\mathbb{0})$. Пусть $f^n(\mathbb{0}) \leq f^{n+1}(\mathbb{0})\ \ \forall n \leq k.\ \ f^{k+1}(\mathbb{0}) = f(f^k(\mathbb{0})) \leq f(f^{k+1}(\mathbb{0}))$, следовательно, $f^{k+1} \leq f^{k+2}(\mathbb{0})$, т.е. последовательность не убывает. Обозначим $a = \sup f^n(\mathbb{0}),\ n \geq 0$. Тогда $f(a) = f(\sup f^n(\mathbb{0})) = \sup\limits_{n \geq 0}\left(f^{n+1}(\mathbb{0})\right) = \sup\limits_{n \geq 1} f^n(\mathbb{0}) = a$. Таким образом, f(a)=a, т.е. a – неподвижная точка.

Пусть теперь f(b)=b. $\mathbb{0} \leq b, \implies f(\mathbb{0}) \leq f(b) = b,\ f(f(\mathbb{0})) \leq f(f(b)) = b, \dots .\ (\forall n \geq 0)\ (f^n(\mathbb{0}) \leq b)$ – значит b является верхней гранью последовательности $\{f^n(\mathbb{0})\}_{n \geq 0}$. Однако a – ТОЧНАЯ верхняя грань этой последовательности, поэтому $a \leq b$.

• Пример: рассмотрим уравнение $f(x) = \frac{1}{2}x + \frac{1}{4}$ на ИУМ $A = [0; 1]$ с естественным числовым порядком. Для данного множества наименьшим элементом является 0. Последовательно вычисляя $f^0(0) = 0, f(0) = \frac{1}{4}, f(f(0) = \frac{1}{2} * \frac{1}{4} + \frac{1}{4} = \frac{3}{8}, f^3(0) = \frac{7}{16}, \dots$, получаем последовательность приближений к наименьшей неподвижной точке. $f^n(0) = \frac{2^n - 1}{2^{n+1}}$, и предел $\lim_{n \to +\infty} f^n(0) = \frac{1}{2}$. Следовательно, наименьшая неподвижная точка отображения f, определяемого правой частью уравнения, равна ½.

11. *Операции на множестве. Понятие алгебраической структуры. Свойства операций (ассоциативность, коммутативность, идемпотентность). Нуль и нейтральный элемент (единица) относительно операции. Примеры. Универсальная алгебра, носитель, сигнатура. Примеры. Однотипные алгебры.*

~~~ ~~~

• n-арной операцией на множестве A называется любое отображение $\omega: A^n \to A$; n-арная операция ω каждому кортежу $(a_1, \dots, a_n) \in A^n$ однозначно сопоставляет элемент $b \in A$. Рассмотрим бинарную операцию (n=2) на множестве A, обозначив её *. Эту операцию называют:

1) ассоциативной, если $(x * y) * z = x * (y * z)$;
2) коммутативной, если $x * y = y * x$;
3) идемпотентной, если $x * x = x$,

$\forall x, y, z \in A$.

• Элемент 0 множества A называют левым (правым) нулем относительно операции •, если 0 • x=0 (x • 0=0) $\forall x \in A$. Если левый и правый нуль существуют, то они совпадают; в этом случае говорят просто о нуле относительно операции.

Элемент 1 множества A называют левым (правым) нейтральным элементом относительно •, если 1 • x=x (x • 1=x). Если существуют левый и правый нейтральный элемент, то они также совпадают; элемент 1 называют просто нейтральным элементом.

Примеры: На множестве целых чисел нулем является число 0, а нейтральным элементом – число 1; на множестве квадратных матриц – нулевая и единичная матрица соответственно.

• Универсальная алгебра считается заданной, если задано некоторое множество A (носитель алгебры) и некоторое множество операций Ω на A (сигнатура алгебры). Если носитель алгебры – конечное множество, то алгебру называют конечной. Две алгебры (A_1, Ω_1) и (A_2, Ω_2) называются однотипными, если существует такая биекция Ω_1 на Ω_2, при которой n-арная операция из Ω_1 для любого n переходит в n-арную из Ω_2.

• Примеры: $\left(2^M, \{\cup, \cap, \setminus, \Delta, \bar{}, \emptyset, M\}\right)$: носитель – множество всех подмножеств произвольно фиксированного множествм M, сигнатура состоит из объединения, пересечения, разности, симметрической разности и дополнения; пустое множество и множество M определяют нульарные операции.

Алгебры $\mathcal{A}_1 = (2^M, \cup, \cap, \emptyset, M)$ и $\mathcal{A}_2 = (\mathbb{R}, +, \bullet, 0, 1)$ являются однотипными; биекцию между их сигнатурами, сохраняющую арность операций, можно определить как $\cup \to +,\ \cap \to *,\ \emptyset \to 0,\ M \to 1$.

12. *Группоиды, полугруппы, моноиды. Единственность нейтрального элемента. Обратный элемент. Группа. Единственность обратного элемента в группе.*

~~~ ~~~

• *Группоидом* называют произвольную алгебру $\mathcal{G} = (G, \bullet)$ сигнатура которой состоит из одной бинарной операции (ограничений на операцию нет). Группоид $\mathcal{G}$ называют *полугруппой*, если его операция ассоциативна $(\forall a, b, c \in G\ \ a \bullet (b \bullet c) = (a \bullet b) \bullet c)$. Группоид называют *моноидом*, если его операция ассоциативна и относительно неё существует нейтральный элемент (единица моноида). Группоид называют *группой*, если его операция ассоциативна, относительно нее существует нейтральный элемент, и $(\forall x \in G)$ существует обратный элемент по данной операции.

• Для левого и правого нейтральных элементов 1' и 1", если они существуют, выполннены равенства $1' = 1' * 1'' = 1''$ - т.е. они совпадают; единица моноида определена однозначно. Элемент $x' \in G$ называют обратным к элементу $x \in G$ по операции •, если $x \bullet x' = x' \bullet x = 1$.

• Пусть в группе $(G, *)$ с единицей 1 для некоторого a существуют элементы a', a", обратные ему. Тогда $a' = a' * 1$, и т.к. $1 = a * a'',$ то $a' = a' * (a * a'') = (a' * a) * a'' = a''$. Обратный элемент определен однозначно.

13. *Циклическая полугруппа (группа). Образующий элемент. Примеры конечных и бесконечных циклических полугрупп и групп. Порядок конечной группы. Порядок элемента. Теорема о равенстве порядка образующего элемента конечной циклической группы порядку группы.*

~~~ ~~~

• Полугруппу (в частности – группу) $(A, *)$ называют циклической, если существует такой элемент a, что любой элемент x полугруппы является некоторой целой степенью элемента a, который называют образующим элементом полугруппы (группы).

• Пример: полугруппа $(\mathbb{N}, +)$ является циклической, образующий элемент: 1 (также бесконечная - $\forall n\ \ 1^n$ попарно различны). Возведение элемента a в положительную степень n есть сумма n этих элементов, что можно записать как n*a. Группа вычетов по модулю 3 $(\mathbb{Z}_3, +, 0)$ также циклическая; любой ее ненулевой элемент является образующим.

• Группа называется конечной, если ее носитель – конечное множество; порядком конечной группы называют количество элементов в ней. Порядок элемента a циклической группы – наименьшее положительное число n такое, что $a^n = 1$.

• **Теорема:** Порядок образующего элемента конечной циклической группы равен порядку самой этой группы

14. *Кольца. Аддитивная группа и мультипликативный моноид кольца. Коммутативное кольцо. Кольца вычетов. Теорема о тождествах кольца (аннулирующем свойстве нуля, свойстве обратного по сложению при умножении, дистрибутивности вычитания относительно умножения).*

~~~ ~~~

• Кольцом называют алгебру вида $(R, +, *, 0, 1)$, сигнатура которой состоит из двух бинарных (сложение кольца и умножение кольца) и двух нульарных операций, причем для любых $a, b, c \in R$ выполняются равенства, называемые аксиомами кольца:

1) $a + (b + c) = (a + b) + c$
2) $a + b = b + a$
3) $a + 0 = a$
4) $\forall a \in R\ \exists(-a)\colon\ a + (-a) = 0$
5) $a * (b * c) = (a * b) * c$
6) $a * 1 = 1 * a = 1$
7) $a * (b + c) = a * b + a * c;\ \ (b + c) * a = b * a + c * a$

• Аксиомы 1-4 означают, что алгебра (R,+,0) является абелевой (коммутативной) группой, называемой аддитивной группой кольца. Аксиомы 5 и 6 показывают, что алгебра (R,*,1) является моноидом, называемым мультипликативным моноидом кольца.

• Кольцо называется коммутативным, если его операция умножения коммутативна.

• Кольцо (коммутативное) вычетов по модулю k – алгебра вида $Z_k = (\{0, 1, \ldots, k-1\}, \oplus_k, \odot_k, 0, 1)$ с операциями сложения по модулю к и умножения по модулю к.

• **Теорема:** в любом кольце выполняются следующие тождества:

1) $0 * a = a * 0 = 0$
2) $(-a) * b = -(a * b) = a * (-b)$
3) $(a - b) * c = a * c - b * c;\ \ c * (a - b) = c * a - c * b$
~~~

15. *Тела и поля. Примеры полей. Область целостности. Теорема о конечной области целостности (с доказательством). Поля вычетов. Решение систем линейных уравнений в поле вычетов.*

~~~ ~~~

• Кольцо, в котором множество всех ненулевых элементов по умножению образует группу, называют *телом*; коммутативное тело – *полем*. В поле, помимо аксиом кольца, выполняются еще два тождества: $\forall a \neq 0 \in R,\ \exists a^{-1}\colon\ a * a^{-1} = 1;\quad a * b = b * a.$

Примеры: поля рациональных чисел $(\mathbb{Q}, +, *, 0, 1)$, действительных чисел $(\mathbb{R}, +, *, 0, 1)$.

• Ненулевые элементы a,b кольца R называют делителями нуля, если $a * b = 0$ или $b * a = 0$. Областью целостности называется коммутативное кольцо без делителей нуля (к примеру, кольцо целых чисел).

Теорема: Конечная область целостности является полем.

Доказательство: Поле – кольцо, умножение которого коммутативно, а каждый ненулевой элемент имеет обратный элемент относительно умножения. Так как по определению область целости является коммутативным кольцом, то достаточно доказать, что для конечной области целостности любой ненулевой элемент обратим.

Фиксируем произвольный $a \neq 0$ и определим отображение f_a множества всех ненулевых элементов в себя: $f_a(x) = a * x$. Это отображение будет инъекцией – из равенства $a * x = a * y$ следует $a * (x - y) = 0$; ввиду отсутствия делителей нуля получаем что $x - y = 0;\quad x = y$. Так как носитель по условию теоремы конечен, то f_a будет также и биекцией. Поэтому для любого y существует единственный элемент x, такой, что $y = a * x$. При $y = 1$ равенство $a * x = 1$ выполняется для некоторого однозначно определенного $x = a^{-1}$.

• Кольцо вычетов по модулю p $\mathbb{Z}_p$ является полем тогда и только тогда, когда p – простое число.

• Рассмотрим пример решения СЛАУ в поле $\mathbb{Z}_5$; при записи уравнений будем опускать знак $\odot_5$ умножения, если это не приводит к путанице. *//а я так вообще не буду писать кружки и индексы – думай сам, тут всё просто!*

$$\begin{cases} x_1 \oplus_5 2x_2 \oplus_5 3x_3 = 1 \\ 2x_1 \oplus_5 2x_2 \oplus_5 4x_3 = 3 \\ 4x_1 \oplus_5 3x_2 \oplus_5 x_3 = 0 \end{cases}$$ Домножим первую строку на 3, прибавим ее к 2 строке:

$(3+2)x_1 + (3*2+2)x_2 + (3*3+4)x_3 = 3+3$. В итоге имеем $0 * x_1 + 3x_2 + 3x_3 = 1$. Прибавив к третьей строке первую, получим $(1+4)x_1 + (2+3)x_2 + (3+1)x_3 = 1$, откуда $4x_3 = 1$. Система привелась к виду $\begin{cases} x_1 + 2x_2 + 3x_3 = 1 \\ 3x_2 + 3x_3 = 1 \\ 4x_3 = 1. \end{cases}$. Из последнего уравнения находим $x_3 = 4^{-1} * 1 = 4 * 1 = 4$. Подставив $x_3 = 4$ во второе уравнение будем иметь $3x_2 + 3 * 4 = 1$, т.е. $3x_2 = 1 + (-2) = -1 = 4$. Отсюда $x_2 = 3^{-1} * 4 = 2 * 4 = 3$. Из первого и второго уравнения после подстановки найденных значений переменных получим $x_1 + 2 * 3 + 3 * 4 = 1,\ \ x_1 + 1 + 2 = 1,\ \ x_1 = -2 = 3$.

//шок автора: лягать мой круп, определение $^{-1}$ степени для избавления от коэффициента это гениально! алсо мы на семинарах делали все это в матричном виде, а не в системном

16. *Подполугруппа, подмоноид, подгруппа. Примеры. Циклические подгруппы. Подкольца и подполя.*

~~~ ~~~

• Пусть $\mathcal{G} = (G, *)$ - произвольный группоид, $H \subseteq G$ – некоторое подмножество G. Множество H замкнуто относительно относительно операции *, если $\forall x, y \in H\ \ (x * y \in H)$.

Подмножество H с операцией * будет группоидом $\mathcal{H} = (H, *)$, называемым *подгруппоидом* группоида $\mathcal{G}$. Если группоид $\mathcal{G}$ является полугруппой, то всякий его подгруппоид также является полугруппой, называемой *подполугруппой* полугруппы $\mathcal{G}$.

Пусть $\mathcal{M} = (M, *, 1)$ – моноид. Если подмножество $P \subseteq M$ замкнуто относительно операции * и содержит единицу этого моноида, то $\mathcal{P} = (P, *, 1)$ также является моноидом – *подмоноидом* моноида $\mathcal{M}$.

Пусть $\mathcal{G} = (G, *, ^{-1}, 1)$ – группа, $H \subseteq G$ подмножество замкнуто относительно операции *, содержит единицу этой группы и вмете с каждым элементом $x \in H$ содержит x^{-1} обратный к x. Тогда $\mathcal{H} = (H, *, ^{-1}, 1)$ также есть группа – *подгруппа* группы $\mathcal{G}$.

//масло масляное, ну(у кого-нибудь это вообще было в вопросах?

Пример: Рассмотрим аддитивную полугруппу натуральных чисел вместе с нулем $(\mathbb{N}_0, +)$. Подмножество всех положительных четных чисел замкнуто относительно сложения, поэтому на нем может быть определена подполугруппа *полугруппы* $(\mathbb{N}_0, +)$. В то же время аддитивная полугруппа натуральных чисел с нулем также является моноидом с нейтральным элементов 0. Тогда построенная выше подполугруппа всех положительных не будет подмножеством *моноида* $(\mathbb{N}_0, +, 0)$, поскольку ее носитель не содержит нуля, являющегося единицей моноида.

• Подгруппу группы $\mathcal{G}$, заданную на множестве всех степеней фиксированного элемента a, называют циклической подгруппой, порождённой элементом a.

• Рассмотрим кольцо $\mathcal{R} = (R, +, *, 0, 1)$. Если множество $Q \subseteq R$ замкнуто относительно сложения и умножения кольца, содержит нуль и единицу кольца и вместе с каждым $x \in Q$ содержит противоположный к нему (по сложению) элемент –x, то $Q = (Q, +, *, 0, 1)$ также является кольцом – подкольцом кольца $\mathcal{R}$. Аналогично дается определение подполя какого-либо поля (добавляется условие содержания в Q обратного элемента по умножению)

17. *Смежные классы подгруппы по элементу. Теорема Лагранжа.*

~~~ ~~~

Пусть $\mathcal{G} = (G, *, 1)$ – группа, $\mathcal{H} = (H, *, 1)$ – ее подгруппа. Левым смежным классом подгруппы $\mathcal{H}$ по элементу $a \in G$ называют множество $aH = \{y\colon\ y = a * h, h \in H\}$.; правым смежным классом – множество $Ha = \{y\colon\ y = h * a, h \in H\}$.

Теорема Лагранжа: порядок конечной группы делится на порядок любой ее подгруппы.

18. *Полукольцо. Идемпотентное полукольцо. Естественный порядок идемпотентного полукольца.*

~~~ ~~~

• Полукольцом называется алгебра с двумя бинарными и двумя нульарными операциями, $(S, +, *, 0, 1)$, два призвольные элементы a,b,c которой обладают следующими свойствами:

1) $a + (b + c) = (a + b) + c$
2) $a + b = b + a$;
3) $a + 0 = a$

4) $(a*b)*c = a*(b*c)$
5) $a*1 = 1*a = a$
6) $a(b+c) = ab + ac$ и $(b+c)a = ba + ca$
7) $a*0 = 0*a = 0$.

Данные равенства называют аксиомами или основными тождествами полукольца. *//в отличие от кольца: нет свойства про –a по сложению, есть 0 по умножению*

• Полукольцо называется идемпотентным, если его операция сложения идемпотентна, т.е. a+a=a.

• На носителе *идемпотентного* полукольца может быть введено отношение порядка; для произвольных $x, y \in S$ положим $x \le y$ тогда и только тогда, когда $x + y = y$. Отношение $\le$ есть отношение порядка (рефлексивно, антисимметрично, транзитивно), называемое естественным порядком полукольца.

19. *Замкнутое полукольцо. Итерация элемента. Примеры вычисления итерации в различных замкнутых полукольцах.*

~~~ ~~~

• Полукольцо$(S, +, *, 0, 1)$ называется замкнутым, если:

1) оно идемпотентно
2) любая последовательность X элементов множества S имеет точную верхнюю грань относительно естественного порядка этого полукольца
3) операция умножения полукольца сохраняет точные верхние грани последовательностей;
   $\forall a \in S, \forall X = \{x_n \in S\}_{n\in\mathbb{N}}\quad a \sup X = \sup aX,\quad (\sup X)a = \sup(Xa)$.

• Итерация x^* элемента x определяется как точная верхняя грань последовательности всех степеней элемента, т.е. $x^* = \sum_{n=0}^{\infty} x^n$, где $x^0 = 1,\quad x^n = x^{n-1}x,\ n = 1,2,\dots$.

Пример: $\mathcal{B} = (\{0,1\}, +, *, 0, 1)$ – идемпотентное полукольцо. $\sup \mathcal{B} = 1$, если хотя бы один ее член равен 1, и =0 в противном случае. Итерация любого элемента полукольца $\mathcal{B}$ равна 1. Для 1* это очевидно, для 0* имеем $0^* = 0^0 + 0^1 + \cdots + 0^K + \cdots = 1 + 0 + \cdots + 0 + \cdots = 1$.

20. *Непрерывность операции сложения в замкнутом полукольце. Теорема о наименьшем решении линейного уравнения в замкнутом полукольце.*

~~~ ~~~

Для любой последовательности $\{x_n\}_{n\in\mathbb{N}}$ элементов замкнутого полукольца и любого элемента a этого полукольца выполняется равенство $a + \sum x_n = \sum(a + x_n)$ – операция сложения в замкнутом полукольце непрерывна.

Теорема: Наименьшими решениями уравнений $x = ax + b$ и $x = xa + b$ в замкнутых полукольцах являются соответственно $x = a^*b$ и $x = ba^*$; a* - итерация элемента a.

21. *Квадратные матрицы порядка n над идемпотентным полукольцом. Теорема о полукольце квадратных матриц. Замкнутость полукольца квадратных матриц над замкнутым полукольцом. Решение систем линейных уравнений в замкнутых полукольцах.*

~~~ ~~~

• Рассмотрим систему линейных уравнений вида $(*)$ $\begin{cases} x_1 = a_{11}x_1 + \cdots + a_{1n}x_n + b_1 \\ \dots \\ x_n = a_{n1}x_1 + \cdots + a_{nn}x_n + b_n \end{cases}$, где все элементы a_{ij} и b_i – элементы некоторого замкнутого полукольца. Введем в рассмотрение множество $M_{m\times n}(\mathcal{S})$ прямоугольных матриц с элементами из произвольного идемпотентного полукольца $\mathcal{S} = (S, +, \bullet, 0, 1)$. Обозначим как $\mathbb{M}_n(\mathcal{S})$ множество всех квадратных матриц порядка n, элементы которых принадлежат этому полукольцу.

• **Теорема:** Алгебра $M_n(S) = (\mathbb{M}_n(\mathcal{S}), +, \bullet, O, E)$ есть идемпотентное полукольцо. Если замкнуто полукольцо $\mathcal{S}$, то полукольцо $M_n(S)$ также замкнуто.

• Пусть $\mathcal{S}$ – замкнутое полукольцо, $\{A_m\}_{m\in\mathbb{N}}$ - произвольная последовательность квадратных матриц $A_m = \left(a_{ij}^m\right)$ порядка n. Рассмотрим матрицу $B = \left(\sum_{m\in N} a_{ij}^m\right)$. Каждый элемент $b_{ij} = \sum_{m\in N} a_{ij}^m$ является точной верхней гранью последовательности элементов a_{ij}^m (эти точные верхние грани существуют, поскольку a_{ij}^m – элементы замкнутого полукольца $\mathcal{S}$). Так как сложение матриц и отношение порядка в полукольце матриц определяется поэлементно, то матрица B и будет точной верхней гранью последовательности матриц A_m. Следовательно полукольцо $M_n(\mathcal{S})$ – замкнуто над полукольцом $\mathcal{S}$.

• Рассмотрим процедуру решения системы уравнений (*). Запишем первое уравнение системы так:
$x_1 = a_{11}x_1 + (a_{12}x_2 + \cdots + a_{1n}x_n + b_1)$. Из первого уравнения системы выразим x_1 через остальные неизвестные:
$x_1 = a_{11}^*(a_{12}x_2 + \cdots + a_{1n}x_n + b_1)$. Подставляя это выражение вместо x1 в остальные уравнения, получаем систему из n-1 уравнений, не содержащую x1: $\begin{cases} x_2 = a_{21}a_{11}^*(a_{12}x_2 + \cdots + a_{1n}x_n + b_1) + a_{22}x_2 + \cdots + a_{2n}x_n + b_2 \\ x_3 = a_{31}a_{11}^*(a_{12}x_2 + \cdots + a_{1n}x_n + b_1) + a_{32}x_2 + \cdots + a_{3n}x_n + b_3 \\ \dots \\ x_n = a_{n1}a_{11}^*(a_{12}x_2 + \cdots + a_{1n}x_n + b_1) + a_{n2}x_2 + \cdots + a_{nn}x_n + b_n \end{cases}$.

Приводя подобные члены и повторяя процедуру, получаем $(**)$ $x_i = a_i^*\gamma_i$, где выражение a_i^* не содержит неизвестных, а γ_i может содержать только неизвестные, начиная с (i+1)-го. При i=n имеем $x_n = a_n^*\gamma_n$, где оба выражения не содержат неизвестных.

Таким образом, исходная система преобразована к «треугольному» виду: правая часть уравнения не содержит неизвестных, уравнение (**) при i=n-1 в правой части содержит только неизвестное. Каждое следующее уравнение при просмотре «снизу вверх» содержит на одно неизвестное больше чем предыдущее. После этого мы последовательно вычисляем значения всех неизвестных $x_1, \dots, x_{n-1}$, начиная с последнего.
~~~