Компьютерная алгебра

(курс лекций)

Игорь Алексеевич Малышев

Computer.Algebra@yandex.ru

КСПТ

КОМПЬЮТЕРНЫЕ СИСТЕМЫ И ПРОГРАММНЫЕ ТЕХНОЛОГИИ

МАТЕМАТИЧЕСКИЕ ОБЪЕКТЫ И ИХ ПРЕДСТАВЛЕНИЯ

Лекция 6

Элементы общей алгебры и теории чисел

Содержание лекции

- Основные понятия теории множеств
- Алгебраические системы
- Числовые системы

План лекции: тема подраздела

- **Основные понятия теории множеств**
- Алгебраические системы
- Числовые системы

Основные понятия теории множеств

Интуитивная теория множеств (Георг Кантор)

Множество – это произвольная совокупность определённых предметов, отличимых друг от друга и представимых как единое целое W.

Любой предмет, входящий в состав множества – **элемент** множества ($w \in W$).

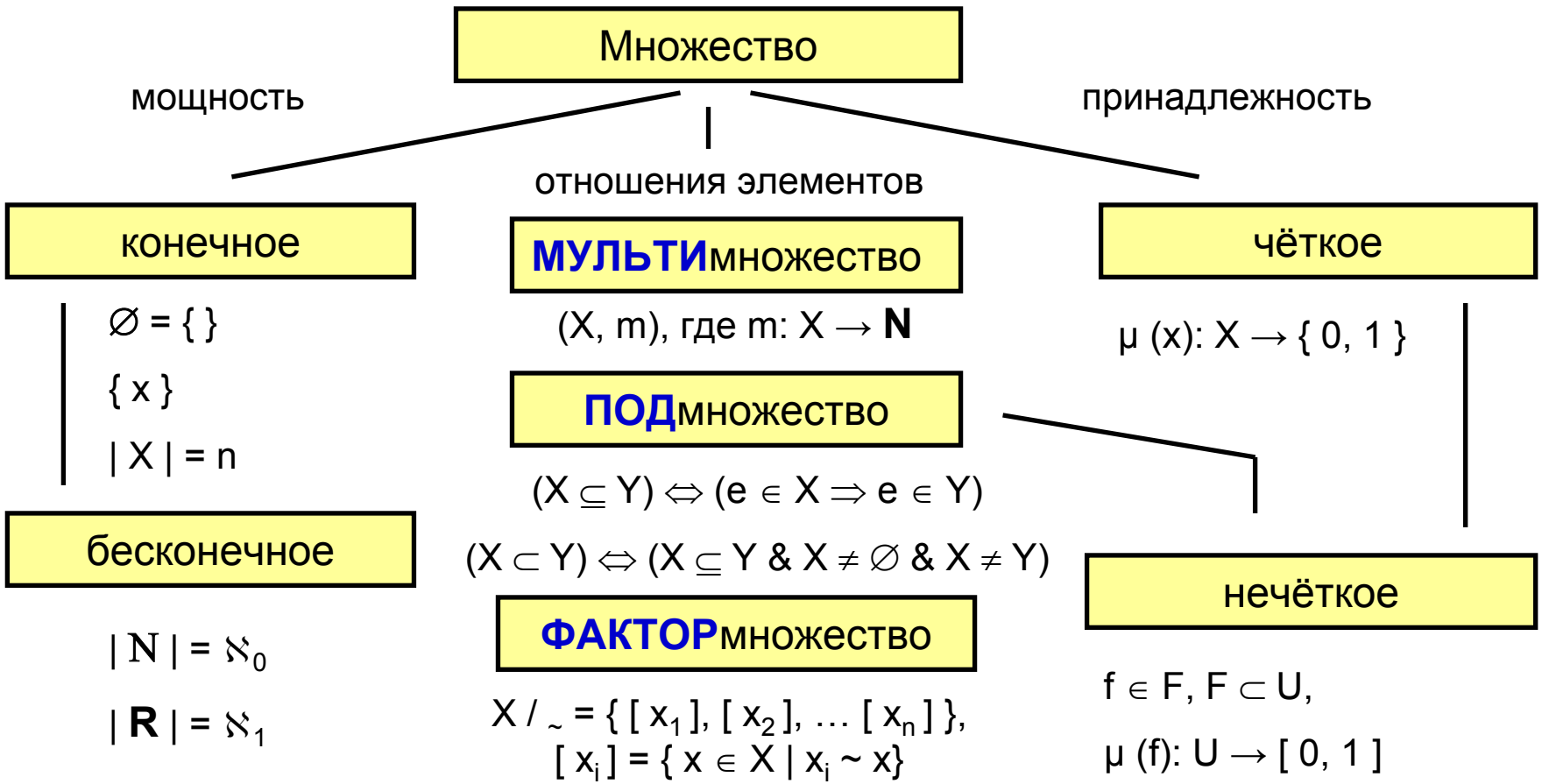
Пусть U – некоторое универсальное множество, тогда B (U) – множество всех подмножеств множества U (множество-степень, **булеан** множества U).

Если множество V – объединение подмножеств V_1, V_2, … V_n, …, то совокупность подмножеств $\{V_1, V_2, \ldots V_n, \ldots\}$ называется **покрытием** множества V.

Если совокупность подмножеств покрытия множества V такова, что $V_i \cap V_j = \varnothing$ при $i \neq j$, то совокупность $\{V_1, V_2, \ldots V_n, \ldots\}$ называется **разбиением** множества V, а подмножества V_i – **классами** этого разбиения, i = 1, 2, … n, …

Основные понятия теории множеств

Основные типы множеств



Основные понятия теории множеств

Отношения

Отношение, определённое (заданное) на множествах $X_1, X_2, \ldots X_n$ – это произвольное подмножество декартова произведения указанных множеств:

$R \subseteq X_1 \times X_2 \times \ldots \times X_n$

Элемент отношения R – это **кортеж** (последовательность) элементов множеств:

$(x_1, x_2, \ldots x_n)$, где $x_i \in X_i$, $1 \le i \le n$

Пусть $R_1 \subseteq X_1 \times X_2$, $R_2 \subseteq X_2 \times X_3$ – два отношения.

Отношение R_1^{-1}, заданное на множестве $X_2 \times X_1$, называется **обратным** к R, если: $R_1^{-1} = \{ (x_2, x_1) \mid x_1 R x_2 \}$.

Отношение $R_2 \circ R_1$, заданное на множестве $X_1 \times X_3$ называется **композицией** (произведением, суперпозицией) отношений R_1 и R_2, если:
$R_2 \circ R_1 = \{ (x_1, x_3) \mid x_1 \in X_1 \,\&\, x_3 \in X_3 \,\&\, (\exists\, x_2 \in X_2) (x_1 R_1 x_2 \,\&\, x_2 R_2 x_3) \}$

Основные понятия теории множеств

Бинарные отношения

Декартово произведение множеств X_1 , X_2 , … X_n , для которых выполнено равенство $X_1 = X_2 = \ldots = X_n = X$, называется декартовым произведением n-й степени множества X (X^n), а отношение R, заданное на X^n, т.е. $R \subseteq X^n$ n-арным отношением на множестве X.

Наиболее часто используемые отношения (n – **арность**):

- нульарные (n = 0)
- унарные (n = 1)
- бинарные (n = 2)
- тернарные (n = 3)

Отношение I_X, заданное на декартовом квадрате множества X, т.е. $I_X \subseteq X^2$, элементами которого являются бинарные кортежи (пары) вида (x, x), где $x \in X$, называется отношением **тождества** (диагональю, **идеалом**).

Для любого бинарного отношения $R \subseteq X2$ имеет место равенство:
$I_X \circ R = R \circ I_X = R$

Основные понятия теории множеств

Свойства бинарных отношений

Отношение / Свойство	reflex	¬ reflex	symm	¬ symm	trans	¬ trans	every
Эквивалентность	+		+		+		+
Толерантность	+		+				+
Доминирование		+		+			+
Частичный порядок	+			+	+		+
Строгий порядок		+		+	+		+
Предпорядок (квазипорядок)	+				+		+
Предикция		+		+		+	+

(¬) reflex – (анти) рефлексивность, (¬) symm – (анти) симметричность,

(¬) trans – (анти) транзитивность, every – всюду определённость

Основные понятия теории множеств

Отношение эквивалентности

Лемма 1. Всякое разбиение множества X на классы задаёт на этом множестве отношение эквивалентности.

Лемма 2. Всякое отношение эквивалентности R, определяемое на множестве X, задаёт разбиение этого множества на классы.

Теорема 1. Между разбиениями множества на классы и отношениями эквивалентности, заданными на этом множестве, существует взаимно однозначное соответствие.

Теорема 2. Если R_1 и R_2 – отношения эквивалентности, заданные на множестве X, то:

(1) R_1^{-1} – отношение эквивалентности на X

(2) $R_2 \circ R_1$ – отношение эквивалентности на X тогда и только тогда, когда $R_2 \circ R_1 = R_1 \circ R_2$

(3) $R_2 \cap R_1$ – отношение эквивалентности на X

(4) R_1` (дополнение множества R_1 в множестве X^2) не является отношением эквивалентности на X.

Теорема 3. Объединение $R_2 \cup R_1$ отношений эквивалентности R_1 и R_2 является эквивалентностью тогда и только тогда, когда пересечение любого класса эквивалентности по R_1 с любым классом эквивалентности по R_2 либо совпадает с одним из них, либо пусто. Если $R_2 \cup R_1$ – эквивалентность, то $R_2 \cup R_1 = R_2 \circ R_1$.

Основные понятия теории множеств

Замыкание отношений

Пусть R – некоторое бинарное отношение на множестве X. Тогда:

Рефлексивным замыканием R_i отношения R называется отношение $R \cup i$,
где i – отношение тождества (диагональ) на X.

Симметричным замыканием R_s отношения R называется отношение $R \cup R^{-1}$,
т.е. если $(x_1, x_2) \in R$, то $(x_1, x_2) \in R_s$ и $(x_2, x_1) \in R_s$.

Транзитивным замыканием R_t отношения R называется отношение
$R_t = R \cup R^2 \cup R^3 \cup \ldots \cup R^n \cup \ldots$,
т.е. если $(x_1, x_2) \in R_t$ тогда и только тогда, когда существуют элементы
$y_1, y_2, y_3, \ldots y_n \in R$, причём $y_1 = x_1$ и $y_n = x_2$, такие, что
$(y_1 R y_2 , y_2 R y_3 , y_3 R y_4 , \ldots y_{n-1} R y_n)$.

Если некоторое отношение содержит свои рефлексивное, симметричное и транзитивное замыкания, то оно является отношением эквивалентности и наоборот.

Основные понятия теории множеств

Отношение частичного порядка

С каждым отношением частичного порядка $\leq$
связано отношение строгого порядка $<$ и наоборот:
$(x_1 < x_2) \Leftrightarrow x_1 \leq x_2$ и $x_1 \neq x_2$
$(x_1 \leq x_2) \Leftrightarrow x_1 < x_2$ или $x_1 = x_2$

С каждым отношением квазипорядка $<<$
связаны отношения строгого порядка $<$ и эквивалентности $\sim$:
$(x_1 < x_2) \Leftrightarrow x_1 << x_2$ и $\neg (x_1 << x_2)$
$(x_1 \sim x_2) \Leftrightarrow x_1 << x_2$ и $x_1 << x_2$

Любое отношение квазипорядка $<<$, заданное на множестве X,
индуцирует отношение частичного порядка $\leq$ на фактор-множестве $X / \sim$:
$([x_1] \leq [x_2]) \Leftrightarrow x_1 << x_2$

Основные понятия теории множеств

Операции

Отношение F, заданное на множествах $X_1, X_2, \ldots X_n, Y$, называется функциональным, если для любого элемента $(x_1, x_2, \ldots x_n)$ из декартова произведения $X_1 \times X_2 \times \ldots \times X_n$ существует не более одного элемента y из Y такого, что $(x_1, x_2, \ldots x_n , y) \in F$.

Отношение F, заданное на множествах $X_1, X_2, \ldots X_n, Y$, называется (частичным) **отображением** или (частичной) функцией из $X_1 \times X_2 \times \ldots \times X_n$ в Y, если F – функциональное и (частично определённое, т.е. $Dom (F) \subset X_1 \times X_2 \times \ldots \times X_n$) полностью определённое, т.е. $Dom (F) = X_1 \times X_2 \times \ldots \times X_n$.

Dom (F) – область определения отображения F.
Im (F) – область значений отображения F.

Если $F: X^n \rightarrow Y$, то

- F – n-арная **функция** из X в Y;
- F – n-арный **предикат** на множестве X, если $Y = \{ 0, 1 \}$;
- F – n-арная **операция** на множестве X, если $Y = X$.

Операция F называется частичной (частично определённой), если F – частичная функция.

Основные понятия теории множеств

Свойства бинарных операций

Пусть на множестве X определена бинарная операция, обозначаемая $\Diamond$.

Бинарная операция $\Diamond$ называется :
ассоциативной, если для любых x, y, z $\in$ X верно:
$(x \Diamond y) \Diamond z = x \Diamond (y \Diamond z)$
коммутативной, если для любых x, y $\in$ X верно:
$x \Diamond y = y \Diamond x$
идемпотентной, если для любого x $\in$ X верно:
$x \Diamond x = x$

Элемент **0** множества X называется **левым (правым) нулём** относительно данной операции, если для любого x $\in$ X верно $\mathbf{0} \Diamond x = \mathbf{0}$ ($x \Diamond \mathbf{0} = \mathbf{0}$). Нуль, являющийся одновременно и левым и правым, называется просто нулём.

Элемент **1** множества X называется **левым (правым) нейтральным элементом** относительно данной операции, если для любого x $\in$ X верно $\mathbf{1} \Diamond x = x$ ($x \Diamond \mathbf{1} = x$). Нейтральный элемент, являющийся одновременно и левым и правым, называется просто нейтральным элементом.

Основные понятия теории множеств

Аксиоматика теории множеств

Георг Кантор:
Аксиомы объёмности и «математической свободы».

Эрнст Цермело, Абрахам Френкель (ZFC-система):
Аксиомы объёмности, свёртки, пары, объединения, бесконечности, булеана, выбора, подстановки.

Джон фон Нейман (Пауль Бернайс, Курт Гёдель):
Аксиома регулярности (основания, фундирования).

Основные понятия теории множеств

ZFC - система

Аксиома объёмности. Два множества равны тогда и только тогда, когда они состоят из одних и тех же элементов.
Аксиома свёртки. Любое свойство P (x) определяет некоторое множество A с помощью условия: элементами множества A являются те и только те предметы a, которые имеют свойство P.
Аксиома пары. Если a и b – различные предметы, то существует множество { a, b }, которое состоит в точности из предметов a и b.
Аксиома объединения. Для произвольного множества A существует множество B, которое состоит в точности из всех элементов, входящих в множество A.
Аксиома бесконечности. Существует хотя бы одно бесконечное множество – множество натуральных чисел **N**.
Аксиома булеана. Для любого множества A существует множество B (A) всех подмножеств множества A.
Аксиома выбора. Если дано множество A, то существует функция f, которая ставит в соответствие каждому непустому подмножеству B из множества A один определённый элемент f (B) из множества B.
Аксиома подстановки. Для любого множества A и однозначной функции f, определённой на множестве A, существует множество, которое состоит в точности из элементов f (x) для $x \in A$.

План лекции: тема подраздела

- Основные понятия теории множеств
- **Алгебраические системы**
- Числовые системы

Алгебраические системы

Универсальные алгебры

Универсальной Ω-алгеброй (или просто **алгеброй**) называется система $G = (A, \Omega)$, состоящая из некоторого непустого множества A (основное множество или **носитель алгебры**) и множества определённых на A операций $\Omega = \{ \omega_1^{k1}, \omega_2^{k2}, \ldots \omega_n^{kn}, \ldots \}$ (**сигнатура алгебры**), где k_i – арность операции ω_i, $k_i \in \mathbf{N}$, $ar(\omega_i) = k_i$ (функция арности), $i = 1, 2, \ldots, n, \ldots$
Операции из множества Ω называются **основными операциями алгебры**.

Подмножество $A' \subseteq A$ называется **замкнутым** относительно операции $\omega \in \Omega$, если для любых $a_1, a_2, \ldots a_n$ из A' истинно $\omega(a_1, a_2, \ldots a_n) \in A'$.

Система (A', Ω) называется **подалгеброй** алгебры (A, Ω), если $A' \subseteq A$ и A' замкнуто относительно любой основной операции алгебры (A, Ω).

Теорема. Пересечение произвольной совокупности подалгебр универсальной алгебры, если оно не пусто, будет подалгеброй этой алгебры.

Конечно-порождённые алгебры

Следствие из предыдущей теоремы:
Для произвольного подмножества $D \subseteq A$ алгебры G
существует однозначно определённая подалгебра { D } ,
минимальная среди подалгебр, включающих множество D.
Это будет пересечение всех подалгебр из G , включающих D.

Если { D } = G , то D называется **системой образующих** для G.

Алгебра G = { D } называется **конечно-порождённой**, если множество D конечно.

Примеры.
С помощью операции сложения можно породить следующие множества:

- множество натуральных чисел из множества D = { 0, 1 }
- множество целых чисел из множества D = { -1, 1 }

Алгебраические системы

Понятие алгебраической системы

А.И. Мальцев обобщил понятие «(универсальная) алгебра» до понятия «алгебраическая система».

Алгебраической системой $A = (A, \Omega_F, \Omega_P)$ называется система, состоящая из трёх множеств:
(1) непустого множества A (носитель алгебраической системы);
(2) множества алгебраических операций Ω_F , определённых на множестве A;
(3) множества отношений Ω_P , определённых на множестве A.

Если алгебраическая система не содержит операций, то она называется **моделью**.

Если алгебраическая система не содержит отношений, то она называется **алгеброй**.

Типом алгебраической системы называется кортеж арностей операций и отношений. Операции и отношения в типе алгебраической системы составляют пару отдельных наборов, а внутри каждого набора расположены в порядке убывания значений арностей.

Алгебраические системы

Морфизмы универсальных алгебр

Универсальные алгебры G (A, Ω) и Q (B, Ω') называются **однотипными** алгебрами, если между элементами сигнатур Ω и Ω' можно установить такое взаимно однозначное соответствие, при котором любая операция ω из Ω и соответствующая ей операция ω' из Ω' будут иметь одну и ту же арность.
Очевидно, что в однотипных алгебрах задана одна и та же сигнатура операций.

Для однотипных алгебр определены следующие морфизмы
(отображения носителей алгебр, сохраняющие свойства операций, входящих в их сигнатуры) :
Гомоморфизм – это отображение h : A → B такое, что для всех элементов a_1, a_2, … a_n из A и любой n-арной операции ω из Ω справедливо равенство :
$h (\omega (a_1 , a_2 , \dots a_n)) = \omega (h (a_1) , h (a_2) , \dots h (a_n))$
Изоморфизм – это взаимно однозначное отображение алгебры G на алгебру Q (G ~ Q).
Эпиморфизм (**мономорфизм**) – это гомоморфизм алгебры на (в) себя, т.е. h : G → G
Автоморфизм – это изоморфизм алгебры на себя.

Если алгебра G изоморфна некоторой подалгебре алгебры G' ,
то говорят, что алгебра G **изоморфно вкладывается** в алгебру G'.

Алгебраические системы

Пример изоморфизма универсальных алгебр

Пусть $G = (D^{+} , \Omega)$ – алгебра положительных вещественных чисел.
Носитель алгебры:
$D^{+} = \{ x \in D \mid x > 0 \}$
Сигнатура алгебры Ω состоит из следующих операций:
Бинарная операция умножения (*);
Унарная операция взятия обратного элемента ($^{-1}$);
Нульарная операция, фиксирующая единичный элемент (**1**).

Пусть $G' = (D , \Omega')$ – алгебра, носитель которой D –
множество всех вещественных чисел.
Сигнатура алгебры Ω' состоит из следующих операций:
Бинарная операция сложения (+);
Унарный минус (-);
Нульарная операция, фиксирующая нулевой элемент (**0**).

Отображение f = lg (десятичный логарифм) – изоморфизм алгебры G на G' :

$\lg (a * a') = \lg a + \lg a'$

$\lg (\mathbf{1} / a) = \lg (\mathbf{1}) - \lg (a) = \mathbf{0} - \lg (a) = - \lg (a)$

$\lg \mathbf{1} = \lg (a * (\mathbf{1} / a)) = \lg (a) - \lg (a) = \mathbf{0}$

Алгебраические системы

Группоиды (A, $f_{\otimes}^{2}$)

Структура / Свойство	ASSOC	COMMUT	e	b
Полугруппа	+			
Моноид	+		+	
Абелев моноид	+	+	+	
Группа	+		+	+
Лупа (квазигруппа)			+	+
Абелева группа	+	+	+	+

ASSOC – ассоциативность, COMMUT – коммутативность,

e – нейтральный элемент: 0 (для аддитивного группоида)

1 (для мультипликативного группоида)

b – обратный элемент : b = - x (для аддитивного группоида), $x \in X$

$b = x^{-1}$ (для мультипликативного группоида), $x \in X$

Алгебраические системы

Операционные структуры: определения

Полугруппой называется множество **S** с ассоциативной бинарной операцией $\otimes$:
$x \otimes (y \otimes z) = (x \otimes y) \otimes z$, для всех $x, y, z \in \mathbf{S}$

Моноидом называется множество **M**, на котором задана ассоциативная бинарная операция (обычно именуемая умножением) и в которой существует такой элемент e, называемый единицей, что
$e \otimes x = x \otimes e = x$, при любом $x \in \mathbf{M}$
Иными словами, моноид – это полугруппа с единицей.
В любом моноиде существует ровно одна единица.
Если в моноиде бинарная операция коммутативна,
то её обычно называют сложением, а единицу – нулём.

Группой G называется множество элементов с ассоциативной бинарной операцией, для которой существует единица (см. моноид) и каждому элементу $x \in \mathbf{G}$ соответствует обратный к нему (по отношению к $\otimes$) элемент $y \in \mathbf{G}$ такой, что
$x \otimes y = e = y \otimes x$ (если абелева группа, иначе правый и левый обратные элементы)

Алгебраические системы

Операционные структуры: примеры

Пример 1.
Пусть A = { a, b, c, d, … x, y, z } – латинский алфавит, т.е. элементы множества A – это символьные имена (символы) букв алфавита.
Определим A* как множество всех (не обязательно конечных) строк символов из алфавита A.
Определим на A* бинарную операцию конкатенации _ (символ подчёркивания) следующим образом: если $\alpha, \beta \in A^*$, то $\alpha \_ \beta = \alpha\beta$
Пусть символ Λ обозначает пустую строку. Очевидно, что $\Lambda \in A^*$.
Система (A^* , _ , Λ) является моноидом, т.к. Λ – единица: $\Lambda \_ \alpha = \alpha \_ \Lambda = \alpha$

Пример 2.
Множество всех отображений произвольного множества в себя является моноидом относительно операции суперпозиции отображений.

Пример 3.
Множество целых чисел является абелевой группой по сложению.

Алгебраические системы

Кольца и поля (A, $f_{\oplus}^{2}$, $f_{\otimes}^{2}$)

Структура / Свойство	ASSOC	COMMUT	u	q
Кольцо				
Ассоциативное кольцо	+			
Абелево кольцо	+	+		
Область целостности	+	+	+	
Унитарное кольцо	+		+	
Тело	+		+	+
Поле	+	+	+	+

ASSOC – ассоциативность, COMMUT – коммутативность,

u – мультипликативный нейтральный элемент,

q – мультипликативный обратный элемент

Алгебраические системы

Арифметические структуры : кольца

Кольцом называется множество **R**
с двумя определёнными на нём бинарным операциями –
сложением ($\oplus$) и умножением ($\otimes$), которые обладают следующими свойствами:
(1) относительно операции сложения множество **R** является абелевой группой;
(2) операции сложения и умножения связаны законами дистрибутивности:
$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$, $(x \oplus y) \otimes z = (x \otimes z) \oplus (y \otimes z)$,
для всех $x, y, z \in \mathbf{R}$

Замечание.
Умножение, определённое в кольце, не обязано быть ни ассоциативным, ни коммутативным.

Кольцо с ассоциативным умножением называется ассоциативным,
а если умножение к тому же ещё и коммутативно – коммутативным (абелевым).

Алгеброй Ли называется кольцо с антикоммутативным умножением
(обычно обозначаемым [a, b]), удовлетворяющим тождеству Карла Густава Якоби:
$[a, [b, c]] \oplus [b, [a, c]] \oplus [c, [a, b]] = 0$, для любых $a, b, c \in \mathbf{R}$
Причём, для любого $a \in \mathbf{R}$ выполнено условие : $[a, a] = 0$

Алгебраические системы

Кольца: примеры

Пример 1.
Все целые, рациональные, вещественные, комплексные числа являются коммутативными кольцами.

Пример 2.
Множество всех многочленов с вещественными коэффициентами и операциями сложения и умножения вещественных чисел (называемых далее для краткости – обычными) является коммутативным кольцом.

Пример 3.
Множество всех квадратных матриц n-го порядка, состоящих из вещественных чисел, по отношению к обычным операциям сложения и умножения является ассоциативным (но не коммутативным !) кольцом.

Пример 4.
Множество всех векторов трёхмерного пространства с обычным сложением и векторным умножением является кольцом Ли.

Алгебраические системы

Арифметические структуры : области целостности

Аддитивной группой кольца называется абелева группа,
которая получится, если в кольце рассмотреть только операцию сложения.
Нулевой элемент такой группы называется **нулём кольца**.

Если для элементов a, b кольца **R** верно равенство:
$a \otimes b = 0$, где $a \neq 0$, $b \neq 0$ то a и b называются **делителями нуля**.
Если **R** – не коммутативное кольцо, то a – левый, b – правый делители нуля.

Если в кольце **R** нет делителей нуля,
то **R** называется **кольцом без делителей нуля**.

Областью целостности D называется коммутативное кольцо с единицей,
не имеющее делителей нуля.

Замечание.
Каждая конечная область целостности является полем.
Однако существуют примеры бесконечных областей целостности, не являющихся полями.

Алгебраические системы

Области целостности: примеры

Пример 1.
Коммутативные кольца целых, рациональных, вещественных и комплексных чисел являются областями целостности.

Пример 2.
Все функции, определённые и непрерывные на отрезке [- 1, +1] относительно обычных операций сложения и умножения образуют коммутативное кольцо с делителями нуля.

Делителями нуля являются следующие функции :

$f_1(x) = \{ 0$, если $x \in [-1, 0]$; x , если $x \in [0, 1] \}$
$f_2(x) = \{ x$, если $x \in [-1, 0]$; 0 , если $x \in [0, 1] \}$

Указанные функции являются делителями нуля, т.к.
во-первых, ни одна из них не равна нулю рассматриваемого кольца,
во-вторых, их произведение равно этому нулю.

Алгебраические системы

Арифметические структуры : кольца с единицей

Элемент u кольца **R** называется **единицей кольца**,
если для любого элемента a $\in$ R верны равенства :
$a \otimes u = u \otimes a = a$

Замечание. Единицы в кольце может и не быть.

Если в кольце **R** есть единица, то **R** называется **кольцом с единицей**.

В кольце с единицей u для элемента $a \neq 0$ этого кольца может существовать элемент b такой, что верны равенства :
$a \otimes b = b \otimes a = u$
Тогда b называют (правым, левым) **обратным** к a элементом : $b = a^{-1}$

Замечание. Обратного элемента может и не быть.

Элементы кольца с единицей, для которых обратный элемент существует, называются (правым, левым) **делителями единицы**.

Алгебраические системы

Кольца с единицей: примеры

Пример 1.
Кольцо всех целых чисел является кольцом с единицей.

Пример 2.
Кольцо всех чётных чисел является кольцом без единицы.

Пример 3.
В кольце всех квадратных матриц n-го порядка единицей является единичная матрица, а её делителями являются все невырожденные матрицы.

Пример 4.
Система $(Z_m , *, +)$,
где множество Z_m порождено отображением $\rho : Z \rightarrow Z_m$
(ставящим в соответствие каждому целому числу $z \in Z$ его остаток от деления на натуральное число m),
является коммутативным кольцом с единицей для любого $m \in \mathbf{N}$.
Z_m не имеет делителей нуля тогда и только тогда, когда m – простое число.

Арифметические структуры : кольца с идеалами

Подкольцо **I** кольца **R** называется **левым идеалом кольца R**,
если оно вместе с каждым элементом a
содержит все элементы следующего вида :
$r \otimes a$, r – любой элемент кольца **R**.

Аналогично, подкольцо **J** кольца **R** называется **правым идеалом кольца R**,
если оно вместе с каждым элементом a
содержит все элементы следующего вида :
$a \otimes r$, r – любой элемент кольца **R**.

Элемент нуль в любом кольце является двухсторонним идеалом.

Если других идеалов в кольце нет, то оно называется **простым кольцом**.

Алгебраические системы

Арифметические структуры : поля

Полем F = (F , $\otimes$, $\oplus$) называется коммутативно-ассоциативное кольцо с единицей, множество ненулевых элементов которого образует группу относительно умножения.

Аксиоматика:

$\forall x, y \in F\ (x \oplus y = y \oplus x)$	коммутативность $\oplus$
$\forall x, y, z \in F\ (x \oplus (y \oplus z) = (x \oplus y) \oplus z)$	ассоциативность $\oplus$
$\forall x \in F\ \exists e \in F\ (x \oplus e = x)$	существование нуля $e \equiv 0$
$\forall x \in F\ \exists y \in F\ (x \oplus y = 0)$	существование аддитивного обратного элемента $y \equiv -x$
$\forall x, y \in F\ (x \otimes y = y \otimes x)$	коммутативность $\otimes$
$\forall x, y, z \in F\ (x \otimes (y \otimes z) = (x \otimes y) \otimes z)$	ассоциативность $\otimes$
$\forall x \in F\ \exists u \in F\ u \neq 0\ (x \otimes u = x)$	существование единицы $u \equiv 1$
$\forall x \in F\ \exists y \in F\ (x \otimes y = 1)$	существование мультипликативного обратного элемента $y \equiv x^{-1}$
$\forall x, y, z \in F\ (x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z))$	дистрибутивность $\otimes$ по отношению к $\oplus$

Алгебраические системы

Векторные пространства

Линейным (**векторным**) **пространством** V (F) над полем F
называется непустое множество V, на котором определены следующие операции:

(1) операция сложения, т.е. каждой паре элементов x , y $\in$ V
ставится в соответствие элемент того же множества, обозначаемый x + y $\in$ V

(2) операция умножения на скаляр (т.е. элемент поля F),
которая любому элементу $\lambda \in$ F и любому элементу x $\in$ V
ставит в соответствие единственный элемент из V (F), обозначаемый λ x $\in$ V (F)

Метрическим (векторным) **пространством** M
называется множество точек (векторов), с фиксированной функцией расстояния
(**метрикой**) d : M x M $\rightarrow$ **R** , удовлетворяющей следующим аксиомам :

d (x , y) = 0 $\Leftrightarrow$ x = y – аксиома тождества
d (x , y) = d (y , x) – аксиома симметрии
d (x , z) $\leq$ d (x , y) + d (y , z) – аксиома треугольника

для любых x , y , z $\in$ **R** , где **R** – множество вещественных чисел.

Алгебраические системы

Топологические пространства

Пусть X – некоторое множество.
Система T его подмножеств называется **топологией** на X,
если выполнены следующие аксиомы:

(1) объединение произвольного семейства множеств,
принадлежащих T, принадлежит T
(2) пересечение конечного семейства множеств,
принадлежащих T, принадлежит T
(3) $X , \varnothing \in T$

Пара (X , T) называется **топологическим пространством**.
Множества, принадлежащие T, называются **открытыми множествами**.

Множество E называется **топологическим векторным пространством**, если :
(1) E – векторное пространство над полем вещественных или комплексных чисел;
(2) E – топологическое пространство;
(3) операции сложения и умножения на скаляр непрерывны относительно заданной в E топологии.

Алгебраические системы

(Частично) - упорядоченные множества

Множество, на котором определено отношение (частичного) порядка, называется **(частично) - упорядоченным множеством**.

Элемент a частично-упорядоченного множества A называется **нижней (верхней) гранью** для подмножества $B \subseteq A$,
если между a и любым $x \in B$ определено отношение частичного порядка :
$a \leq x$ (для нижней грани), $x \leq a$ (для верхней грани).

Нижнюю (верхнюю) грань a называют **наибольшей нижней (наименьшей верхней) гранью – ННГ (НВГ)** ,
что обозначается $a = \inf B$ ($a = \sup B$),
если для любой другой нижней (верхней) грани a’ подмножества B
выполняется условие : $a' \leq a$ ($a \leq a'$).
Если у данного множества существует ННГ и/или НВГ, то они единственны.

Элемент a частично-упорядоченного множества A называют **наименьшим** – нулём 0 (**наибольшим** – единицей 1), если для любого $x \in A$ выполняется : $a \leq x$ ($x \leq a$).

Алгебраические системы

Решётки

Алгебра $G = (A , \Omega)$ называется **решёткой** (или **структурой**), если на множестве A определены две бинарные операции – верхняя грань ($\vee$) и нижняя грань ($\wedge$)
т.е. $\Omega = (\vee , \wedge)$.

Аксиомы решётки : для любых $a , b , c \in A$ выполняются соотношения :

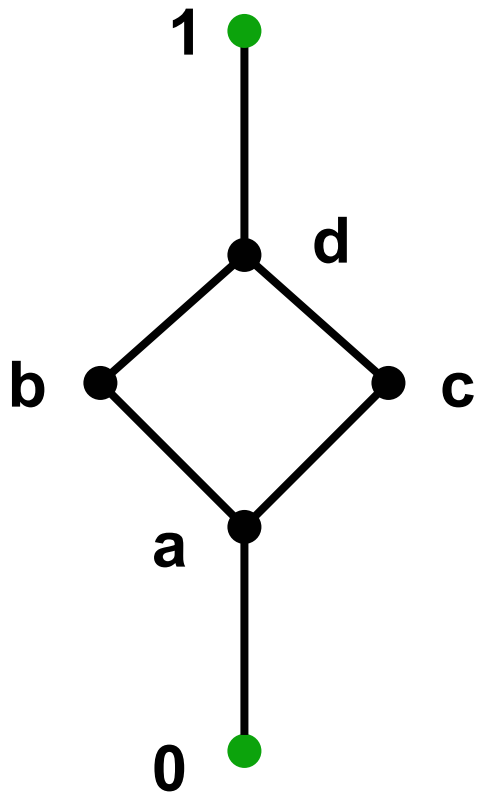
$a \vee a = a \wedge a = a$	– идемпотентность
$a \vee b = b \vee a , a \wedge b = b \wedge a$	– коммутативность
$a \vee (b \vee c) = (a \vee b) \vee c , a \wedge (b \wedge c) = (a \wedge b) \wedge c$	– ассоциативность
$a \vee (a \wedge b) = a , a \wedge (a \vee b) = a$	– поглощение

Если на множестве A задана только операция $\vee$ ($\wedge$) , то алгебра $G = (A , \Omega)$ называется **верхней** (**нижней**) **полурешёткой** (или **полуструктурой**).

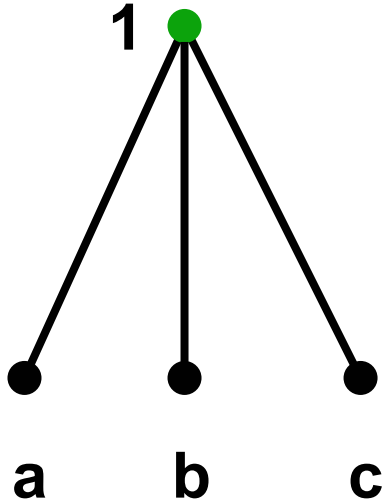
Решётка называется **дистрибутивной**, если для операций $\vee$ и $\wedge$ выполняются соотношения взаимной дистрибутивности :
$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) , a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

Алгебраические системы

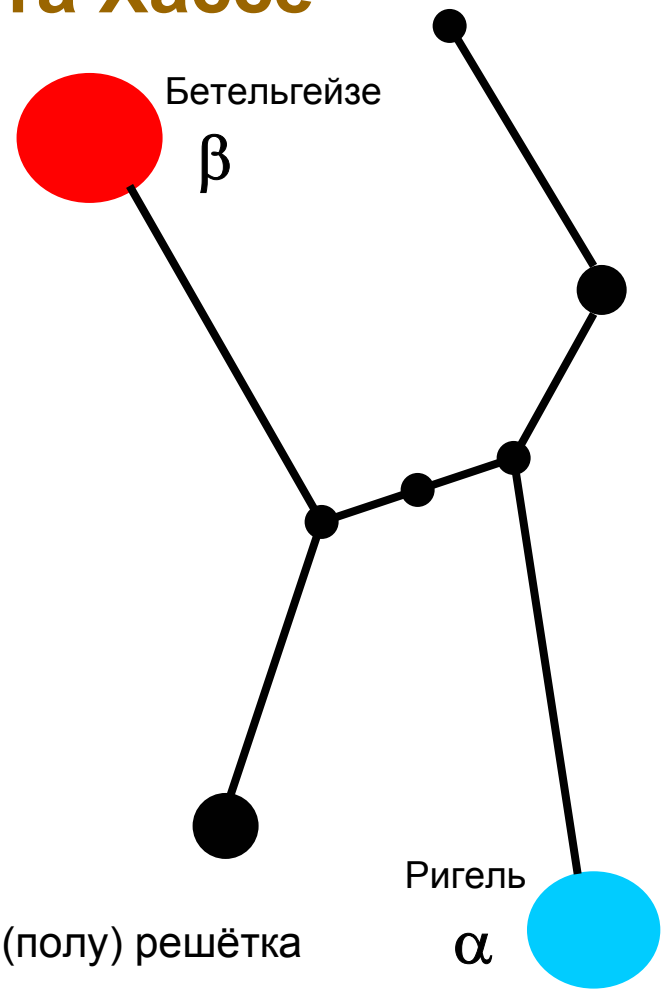
Диаграммы Гельмута Хассе



Не дистрибутивная решётка
(элементы b и c не сравнимы)



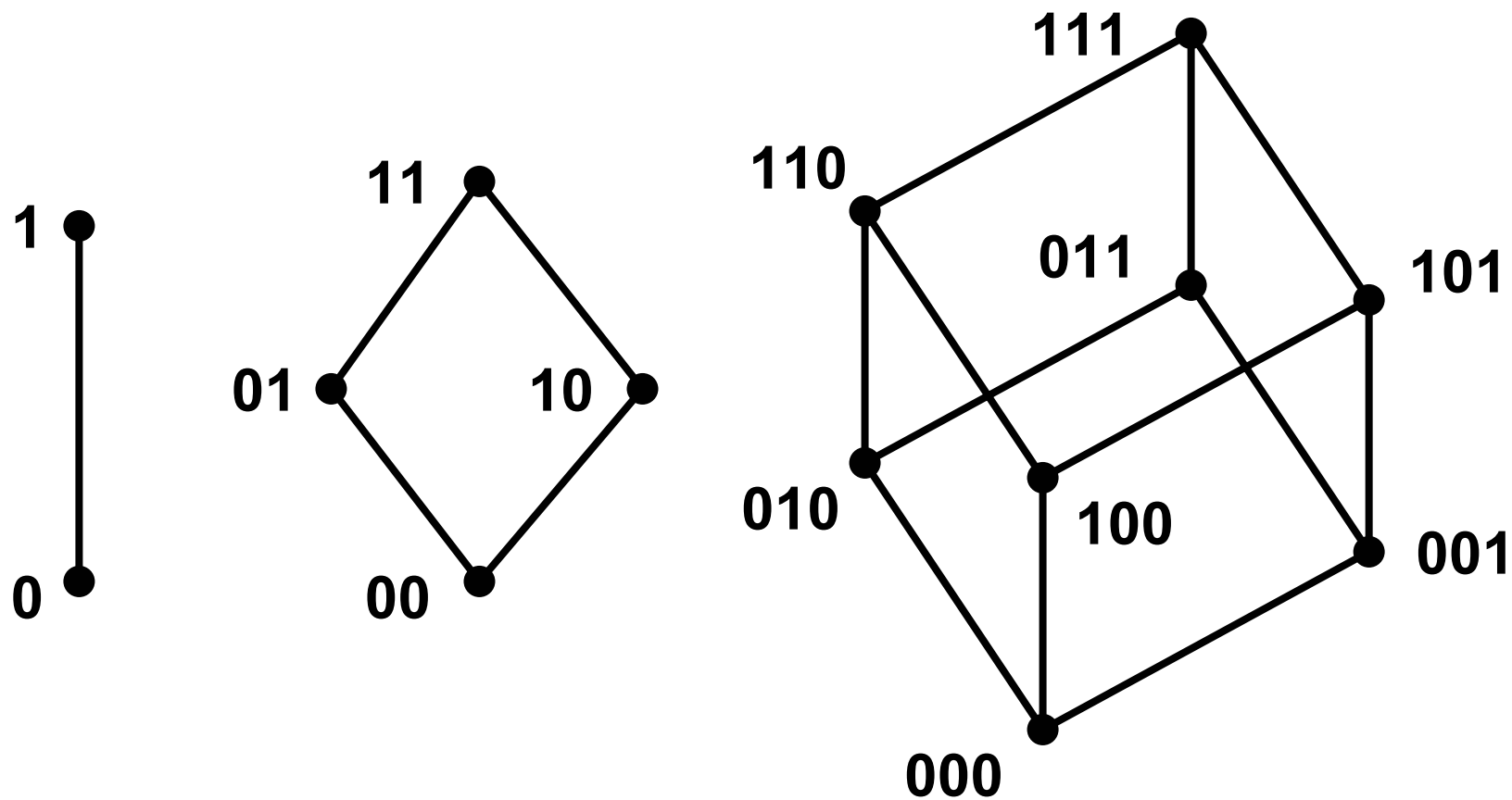
Верхняя полурешётка
(элементы a , b , c
попарно не сравнимы)



Не (полу) решётка

Алгебраические системы

Диаграммы Хассе для булевых решёток



Алгебраические системы

Булевы алгебры

В решётке с нулём 0 и единицей 1 **дополнением** элемента a называют элемент $\neg a$, удовлетворяющий следующим условиям :

$a \wedge \neg a = 0$

$a \vee \neg a = 1$

Очевидно, что $\neg 1 = 0$ и $\neg 0 = 1$.

Решётка с нулём и единицей называется **решёткой с дополнениями**, если каждый её элемент имеет хотя бы одно дополнение.

В дистрибутивной решётке выполняется свойство :
ни один элемент не может иметь двух различных дополнений.

Всякая дистрибутивная решётка с дополнениями называется **булевой решёткой**.

Булева решётка, рассматриваемая как алгебра вида (A , $\vee$, $\wedge$, $\neg$, 0 , 1), называется **булевой алгеброй**.

Алгебраические системы

Нечёткие алгебры

Алгебра вида (A , $\vee$, $\wedge$, $\neg$, 0 , 1), в которой выполняются аксиомы дистрибутивной решётки (идемпотентность, коммутативность, ассоциативность, поглощение и дистрибутивность), а также следующие аксиомы :

$x \wedge 1 = x$ – нейтральность единицы

$x \vee 0 = x$ – нейтральность нуля

$\neg (x \vee y) = \neg x \wedge \neg y$

$\neg (x \wedge y) = \neg x \vee \neg y$ – аксиомы Огастеса де Моргана

$\neg \neg x = x$ – аксиома двойного дополнения

$x \wedge \neg x \vee (y \vee \neg y) = y \vee \neg y$

$(x \wedge \neg x) \wedge (y \vee \neg y) = x \wedge \neg x$ – аксиомы Стивена Коула Клини

называется **нечёткой алгеброй** (**алгеброй Клини**).
Аксиома Клини является более слабым условием, чем аксиома дополнения.

Алгебраические системы

Обобщения алгебраических систем

- Частичные и многоосновные алгебры

  В частичных алгебрах используются операции,
  частично определённые на носителе алгебры.
  В многоосновных алгебрах используется
  несколько различных носителей, на которых определены операции
  над элементами одного или нескольких носителей.
  Например, многоосновными алгебрами являются алгебры алгоритмов
  В.М. Глушкова.
- Функциональные системы

  Это алгебры, носителями которых являются множества функций.
  Например, функциональной системой является булева алгебра
  характеристических функций подмножеств некоторого множества.
- Категории

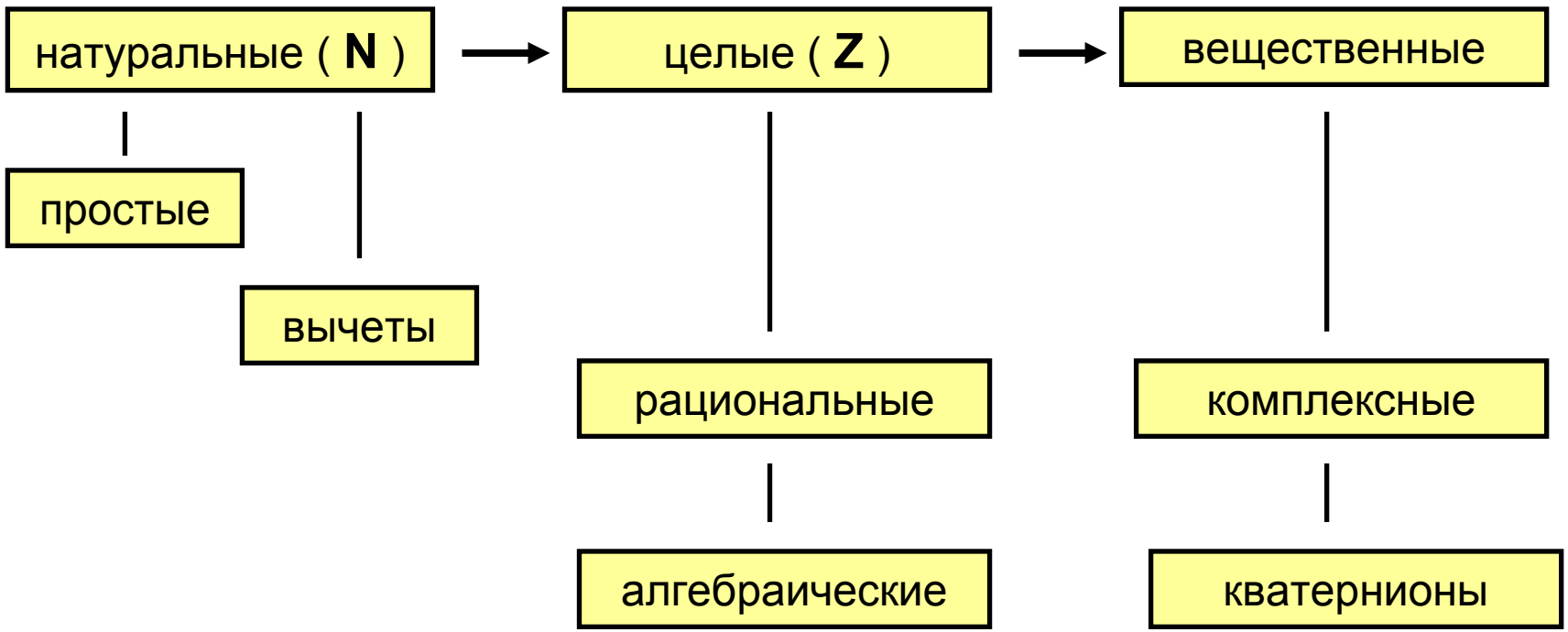
  Каждая категория состоит из (алгебраических) объектов и морфизмов,
  определённых над этими объектами. Например, категория множеств использует
  в качестве объектов всевозможные множества, а в качестве морфизмов –
  всевозможные отображения.

План лекции: тема подраздела

- Основные понятия теории множеств
- Алгебраические системы
- **Числовые системы**

Числовые системы

Основные типы чисел



Числовые системы

Делимость чисел

Пусть a , b $\in$ **Z**. Число a делится на число b (a кратно b), если найдётся такое число q $\in$ **Z**, что a = q * b.

Отношение делимости b | a (b делит a), заданное на **N**, является рефлексивным, антисимметричным и транзитивным, т.е. отношением частичного порядка.

Наибольшее (наименьшее) целое число,
на которое делятся (которое делится на)
заданные целые числа a , b , c , …, n $\in$ **Z** называется их
наибольшим общим делителем – НОД (наименьшим общим кратным – НОК)
и обозначается (a , b , c , …, n) для НОД, [a , b , c , …, n] для НОК.

Если (a , b , c , …, n) = 1 ,
то числа a , b , c , …, n называются **взаимно простыми**.

Количество чисел ряда 0 , 1 , 2 , … , a – 1 взаимно простых с числом a
называется функцией Леонарда Эйлера, которая обозначается φ (a).

Числовые системы

Основная теорема арифметики

Число $p \in \mathbf{N}$, $p \neq 1$ называется **простым**,
если p имеет в точности два положительных делителя: 1 и p.
Остальные натуральные числа принято называть **составными**.
Число 1 не является ни простым, ни составным.

Замечание 1. Наименьший делитель любого числа $a \in \mathbf{N}$, отличный от 1, является простым числом.
Замечание 2. Наименьший отличный от 1 делитель любого составного числа $a \in \mathbf{N}$ не превосходит числа $\sqrt{a}$.

Теорема (Евклид). Простых чисел бесконечно много.

Теорема (основная теорема арифметики). Всякое целое число, отличное от -1, 0, 1, единственным образом (с точностью до порядка сомножителей) разложимо в произведение простых чисел.
(Справедливость теоремы основана на аддитивной структуре кольца целых чисел).

Числовые системы

Цепные (непрерывные) дроби - 1

Цепной (или непрерывной) дробью называется выражение следующего вида:

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{\ddots + \cfrac{1}{q_n + \cfrac{1}{\ddots}}}}}}$$

Числовые системы

Цепные (непрерывные) дроби - 2

Числа q_1 , q_2, … q_n называются **неполными частными**,
причём $q_1 \in \mathbf{Z}$, q_2, … $q_n \in \mathbf{N}$

Числа $\delta_1 = q_1$, $\delta_2 = q_1 + 1/ q_2$ и т.д. называются **подходящими дробями** цепной дроби.

Конечная цепная дробь представляет некоторое рациональное число.

Теорема. Всякое вещественное число может быть разложено в цепную дробь единственным образом, и всякая конечная или бесконечная цепная дробь имеет своим значением некоторое вещественное число.

Всякое иррациональное число если и можно представить,
то только с помощью бесконечной цепной дроби.

Числовые системы

Сравнимость чисел - 1

Зафиксируем натуральное число m. Два целых числа a и b называются **сравнимыми по модулю m**, если остатки от их деления на m одинаковы, что обозначается : $a \equiv b \pmod m$
или в другой форме записи : $a \equiv_m b$

Если для чисел a и b вышеуказанное соотношение не выполняется, то эти числа называются **несравнимыми по модулю m**.

Сравнимые по модулю m числа образуют множество, называемое **классом вычетов по модулю m**.

Для данного числа m все целые числа распадаются на m классов вычетов. Любое число из данного класса называется **представителем** этого класса.

Если натуральное число d делит число m без остатка, то :
$a \equiv b \pmod m \Rightarrow a \equiv b \pmod d$

Сравнимость чисел - 2

Бинарное отношение сравнимости $\equiv_m$ (неважно, по какому модулю)
является отношением эквивалентности на множестве целых чисел.

Говоря алгебраически более строго, отношение сравнимости $\equiv_m$
является конгруэнцией кольца Z, фактор-кольцо по которой $Z / \equiv_m$
это кольцо вычетов Z_m. Кольцо вычетов является полем только если m – простое.

Очевидно, что число a сравнимо с числом b по модулю m тогда и только тогда,
когда (a – b) делится на m нацело.

Свойства сравнений похожи на свойства отношения равенства :
(1) сравнения по одинаковому модулю можно почленно складывать и умножать;
(2) обе части сравнения можно возвести в одну и ту же степень;
разделить на их общий делитель, взаимно простой с модулем и т.д.

Числовые системы

Обобщения базовых числовых систем

- **Обобщения целых чисел** ($n \in \mathbf{Z}$, $d \in \mathbf{N}$)

  рациональные числа:

  m / d

  алгебраические числа:

  Алгебраическое число над полем F является корнем многочлена
  (не равного тождественно нулю) с коэффициентами из F.
  По умолчанию, в качестве поля используется поле рациональных чисел.
  Целыми алгебраическими числами являются корни многочленов
  с целыми коэффициентами и со старшим коэффициентом равным единице.

- **Обобщения вещественных чисел** ($x , y , z \in \mathbf{R}$)

  комплексные числа:

  $C = x + \mathbf{i}\, y$, где $\mathbf{i} = \sqrt{(-1)}$

  гиперкомплексные числа (**кватернионы**):

  $H = a + \mathbf{i}\, x + \mathbf{j}\, y + \mathbf{k}\, z$, где $\mathbf{i} = \mathbf{j} = \mathbf{k} = \sqrt{(-1)}$

Спасибо за внимание !

Вопросы ?