Алгебра

1 Введение

В древние времена люди решали уравнения вида:

$$ax + b = 0$$

Далее научились решать квадратные уравнения и системы следующего вида:

$$ax^2 + bx + c = 0 \qquad \begin{cases} a_{11}x + a_{12}y = 0 \\ a_{21}x + a_{22}y = 0 \end{cases}$$

Дальше в Европе развитии алгебры затихло. Следующим достижением было решение кубического уравнения:

$$ax^3 + bx^2 + cx + d = 0$$

При его решении понадобилось введение комплексных чисел.

2 Кольца и арифметика коммутативных колец

Пусть X - непустое множество.

Определение. *Внутренней бинарной алгебраической операцией называется*

$$f : X \times X \longrightarrow X$$

Определение. *Нульнарная операция:*

$$\{*\} \longrightarrow X$$

Определение. *Унарная операция:*

$$X \longrightarrow X$$

Чаще всего используются записи:

1. Аддитивная $+$
2. Мультипликативная $\cdot$

Определение. ***Нейтральным*** *элементом из* $(X, *)$ *называется* $e \in X$*, такой что* $\forall x \in X \; x * e = x$

Определение. ***Симметричным элементом*** *называется такой* $x' \in X$, *что* $x * x' = e = x' * x$

Определение. *Операция* $*$ *называется* ***ассоциативной***, *если* $\forall x, y, z \in X$

$$(x * y) * z = x * (y * z)$$

Определение. *Операция* $*$ *называется* ***коммутативной***, *если* $\forall x, y \in X$

$$x * y = y * x$$

Примеры неассоциативных операций:

1. Вычитание $(x - y) - z \neq x - (y - z)$
2. Деление
3. Возведение в степень: $\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \quad (m, n) \longrightarrow m^n$

Интересным примером является операция:

$$\mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}^3$$

и называется она векторным произведением. Для нёё справедливо **тождество Якоби**:

$$(u \times v) \times w + (u \times w) \times v + (v \times w) \times u = 0$$

3 Простейшие алгебраические структуры

3.1 Моноиды

Определение. *Тройка* $(X, *, e)$ *называется* ***моноидом***, *если:*

1. $*$ *- ассоциативна*
2. *Существует нейтральный элемент* $e \in X$

Примеры:

1. $(\mathbb{N}, \cdot\,, 1)$
2. $(\mathbb{N}_0, +, 0)$
3. $(\mathbb{R}^+, \cdot\,, 1)$
4. С операцией: $lcm : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$

Определение. *Элемент* $x \in X$ *называется* ***регулярным слева***, *если* $\forall y, z \in X$ *из соотношения* $x * y = x * z$ *следует* $y = z$ *и* ***регулярным справа***, *если* $y * x = z * z \implies y = z$

Лемма. *Элемент* $x \in X$ *обратимый слева/справа регулярен слева/справа*

3.2 Группы

Определение. $(G, mult, inv, 1)$, *где опредлена операция* $mult : G \times G \longrightarrow G$, *то есть* $(x, y) \longrightarrow x \cdot y$, *а также операция* $inv : G \longrightarrow G$, *которая* $x \longrightarrow x^{-1}$ *и задана единица* $1 \in G$. *А также выполняются свойства:*

1. *Ассоциативнось* $mult$
2. *Нейтральный элемент* $1 \cdot x = x = x \cdot 1$
3. *Обратный элемент* $\forall x \in G \; \exists \, x^{-1}$, *такой что* $x \cdot x^{-1} = 1 = x^{-1} \cdot x$

Элементарные свойства групп:

1. Сокращение $\forall x, y, z \in G$ из $xy = xz \implies y = z$, а также из $yx = zx \implies y = z$
2. Деление $\forall h, g \in G \; \exists! x \; hx = g \; (x = h^{-1}g), xh = g \; (x = hg^{-1})$

Примеры:

1. $(\mathbb{Z}, +)$ - бесконечная циклическая группа
2. C_n - циклическая группа порядка n
3. D_n - диэдральная группа порядка n
4. S_n - симметрическая группа порядка n $S_x = B_{ij} \, (X, X)$ - множество биекций X на себя относительно композиции

Определение. *Группа* G *называется* ***абелевой****, если умножение в ней коммутативно, т.е* $\forall x, y \in G \; xy = yx$

Определение. *Пусть* H, G *- группы, отображение* $\varphi : \; H \longrightarrow G$ *называется* ***гомоморфизмом****, если:*

$$\varphi(xy) = \varphi(x)\varphi(y)$$

Примеры гомоморфизмов:

1. Экспонента $\exp : \mathbb{R} \longrightarrow \mathbb{R}^+$, которая $x \longrightarrow e^x$

$$e^{x+y} = e^x \cdot e^y$$

2. Логарифм $\log : \mathbb{R}^+ \longrightarrow \mathbb{R}$, который $x \longrightarrow \log(x)$

$$\log(xy) = \log(x) + \log(y)$$

Лемма. *Биективные гомоморфизмы называются* ***изоморфизмами****. Две группы называются* ***изоморфными****, если между ними существует изоморфизм и обозначаются:*

$$H \cong G$$

Определение. *Гомоморфизм в себя называется* ***эндоморфизмом***

Определение. *Изоморфизм в себя называется* ***автоморфизмом***

4 Кольца. Первые примеры

Определение. *Непустое множество R называется кольцом, если на нём заданы операции сложения $R \times R \longrightarrow R, (x, y) \longrightarrow x + y$ и умножения $R \times R \longrightarrow R, (x, y) \longrightarrow x \cdot y$*

Свойства:

По + образует абелеву группу

1. Ассоциативна
2. Имеет нейтральный элемент
3. Имеет противоположный элемент

А также:

1. $x(y + z) = xy + xz$
2. $(x + y)z = xz + yz$
3. $(xy)z = x(yz)$
4. $\exists 1 \in R, \forall x \in R, 1 \cdot x = x = x \cdot 1$

Определение. *Ассоциативное кольцо с 1 называется* ***коммутативным****, если выполняется:*

$$\forall x, y \in R \; xy = yx$$

Определение. *Ассоциативное кольцо с 1 называется* ***телом****, если выполняется:*

$$\forall x \in R \; \exists x^{-1} \; x \cdot x^{-1} = 1$$

Определение. *Тело R называется* ***полем****, если оно коммутативно по умножению.*

Примеры:

1. Кольцо целых чисел $\mathbb{Z}$
2. Кольцо двоичных дробей $\mathbb{Z}\left[\frac{1}{2}\right]$
3. Кольцо десятичных дробей $\mathbb{Z}\left[\frac{1}{2}, \frac{1}{5}\right]$
4. Кольцо 60-ричных дробей $\mathbb{Z}\left[\frac{1}{2}, \frac{1}{5}, \frac{1}{3}\right]$

$$\mathbb{Z}\left[\frac{1}{2}\right], \mathbb{Z}\left[\frac{1}{2}, \frac{1}{5}\right] \subseteq \mathbb{Q}$$

5. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ - поля
6. Кольцо вычетов по модулю n $\mathbb{Z}/_n\mathbb{Z}$ - также простейший пример фактор-кольца

7. Кольцо с нулевым умножением A - абелева группа по сложению, определим умножение
$$\cdot : \ A \times A \longrightarrow A, \ \forall x, y \longrightarrow 0$$

8. Булево кольцо множеств X - множество, $R = 2^X$ - булеан (множество всех подмножеств X. Операция сложения:
$$Y, Z \subseteq X : \ Y + Z = Y \Delta Z = (Y \setminus Z) \cup (Z \setminus Y)$$

Вообще говоря,

$$\mathbb{Z}/_2\mathbb{Z} \cong \mathbb{F}_2$$
$$\mathbb{Z}/_3\mathbb{Z} \cong \mathbb{F}_3$$

Но $\mathbb{Z}/_4\mathbb{Z}$ не изоморфно F_4
Рассмотрим таблицы Кэли для $\mathbb{Z}/_4\mathbb{Z}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Определение. ***Нильпотентом*** *называется* $x \in R : \ \exists k \in \mathbb{N} : \ x^k = 0$

▷ В данном примере нильпотентом является 2. Так как $2^2 = 0$

Определение. ***Идемпотентом*** *называется* $x \in R : \ x^2 = x$

▷ Например в теории множеств пересечение является умножением, $X \cap X = X$. Любой элемент является идемпотентом.

▷ Ассоциативное, коммутативное кольцо с 1 - то место, где выполняются все основные правила школьной алгебры.

Посмотрим на формулу:

$$(x + y)(x - y) = x^2 - xy + yx - y^2$$

Определение. ***Коммутатором*** *над элементами ассоциативного кольца называется:*

$$[a, b] = ab - ba$$

Если коммутатор тождественно равен нулю в кольце, значит элементы коммутируют. Умножение в кольце, соответственно, коммутативно. Тогда:

$$(x + y)(x - y) = x^2 - y^2$$

4.1 Простейшие конструкции

1. R - коммутативное, ассоциативное кольцо с единицей. $R[t]$ - кольцо многочленов от одной переменной с коэффициентами из R.

$$f = \sum_{k=0}^{n} a_n t^n,\ a_k \in R$$

2. Кольцо матриц R - ассоциативное кольцо с единицей. $Mat_{[n\times n]}(R)$ - кольцо квадратных матриц степени n над R.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

Стандартные матричные единицы:

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$e_{ij}e_{hk} = \delta_{ij}e_{ik}$$

Где:

$$\delta_{ij} = \begin{cases} 1 & \text{для } i = j \\ 0 & \text{для } i \neq j \end{cases} - \textbf{символ Кронекера}$$

3. Непример кольца: $(R[t], +, \cdot)$, где $\cdot$ - композиция многочленов. Композиция ассоциативна. t - единичные элемент.

4. R, S - кольца. Прямая сумма:

$$R \oplus S = \{(x, y) |\ x \in R, y \in S\}$$

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$
$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2)$$

5. Противоположное кольцо R^o. R - кольцо. Как множество $R = R^o$, с тем же сложением, но умножение определяется как $x \cdot y = yx$.