Основы высшей алгебры

Алгебраич. система – это мн-во, на кот. определены операции и/или отношения.

Нас сейчас интересуют бинарные оп-ии. Оп-ю условно обозначаем @.

$\langle M, @\rangle$. M замкнуто отн. @ $\overset{def}{\Longleftrightarrow}$ $\forall a, b \in M,\ a@b \in M$. $@ : M\times M \to M$, т.е. оп-я – это, по сути, ф-я.

$\langle \mathbb{N}, +\rangle$ замкн. # $\langle \mathbb{N}, -\rangle$ не замкн. # $\langle \mathbb{Z}, -\rangle$ замкн. # $\langle \underset{\text{чётные}}{2\mathbb{Z}}, +\rangle$ замкн. # $\langle \underset{\text{нечётные}}{2\mathbb{Z}+1}, +\rangle$ не з.

Коммутативность: $a@b = b@a$. Ассоциативность: $(a@b)@c = a@(b@c)$.

комм. & асс. : $+$ на $\mathbb{Z}$, $*$ на $\mathbb{Z}$. # некомм. & неасс. : $-$ на $\mathbb{Z}$, $/$ на $\mathbb{R}^+$ $(a/b)/c \neq a/(b/c)$

некомм. & асс. : $\times$ матриц, $\circ$ подст-к # комм. & неасс. : $|a-b|$ на $\mathbb{Z}$, a^2b^2 на $\mathbb{Z}$, $a|b$ на $\{0,1\}$.

NB: $a|b = \overline{a\wedge b}$ – штрих Шеффера, И-НЕ, NAND. Почему ф-ии в русском и в английском имеют разный порядок?

У нас – в порядке применения: $\to\boxed{И}\to\boxed{НЕ}\to$, у них – NOT(AND(a, b)) = NAND(a, b).

$\langle M, @\rangle$, @ – бин. оп-я.

0. M замкнуто отн. @.
1. @ ассоциативна.

$\Big\}$ полугруппа $\Big\}$ моноид $\Big\}$ группа

2. $\exists e \in M : e@a = a@e = a \quad \forall a \in M$.
   e – нейтр. эл-т.
3. $\forall a \in M,\ \exists b \in M : a@b = b@a = e$.
   b – обратный к a.
   Обозначение: $b = a^{-1}$, если оп-я похожа на умножение (# $\circ$ подстановок), или
   $b = -a$, если оп-я похожа на сложение.

Если вып. 0–3 и оп-я @ коммутативна, то "абелева группа" (или "коммутативная группа").

$\langle \mathbb{N}, +\rangle$ – полугруппа # $\langle \mathbb{N}_0, +\rangle$ – моноид ($e=0$) # $\langle \mathbb{N}, -\rangle$ не замкн. # $\langle \mathbb{Z}, +\rangle$ – группа ($e=0,\ -(-7)=7$)

$\langle \mathbb{Z}, -\rangle$ не ассоц. # $\langle 2\mathbb{Z}, +\rangle$ – группа # $\langle \mathbb{Z}, *\rangle$ – моноид ($e=1$) # $\langle 2\mathbb{Z}, *\rangle$ – полугруппа

$\langle S_n, \circ\rangle$ – "симметрическая группа" (т.е. группа всех подст-к на n-элементном мн-ве)

$\langle \mathbb{R}, *\rangle$ – моноид, но не группа, т.к. $\nexists\, 0^{-1}$. # $\langle \mathbb{R}^+, *\rangle$ – группа. # $\langle \mathbb{R}\setminus\{0\}, *\rangle$ – группа.

$\langle \mathbb{R}\setminus\{0\}, +\rangle$ – не замкн.

Множество вычетов по модулю n: $\mathbb{Z}_n = \{0, .., n-1\}$ (все возможные остатки от деления на n).

NB: "вычет" – не синоним "остатку"! Это $\forall$ число, дающее такой остаток при делении на n.

Мн-во всех чисел, сравнимых с a по модулю m, называется классом вычетов a по модулю m.

$\mathbb{Z} = \{.., -2, -1, 0, 1, 2, ...\}$

$3\mathbb{Z} = \{.., -6, -3, 0, 3, 6, ..\}$

$1+3\mathbb{Z} = \{.., -5, -2, 1, 4, 7, ..\}$ мн-во $\mathbb{Z}$ разбилось на три (непересекающихся) класса вычетов.

$2+3\mathbb{Z} = \{.., -4, -1, 2, 5, 8, ..\}$

т.н. фактормножество: $\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\} \underset{\text{изоморфно}}{\simeq} \mathbb{Z}_3$.

(от каждого класса оставляем по одному представителю)

NB: не путать фактормножество $\mathbb{Z}/3\mathbb{Z}$ с разностью множеств $\mathbb{Z}\setminus 3\mathbb{Z}$!

$\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\}$ – разбиение $\mathbb{Z}$ на три подмножества: элементы одного при делении на 3 дают в остатке 0, другого – 1, третьего – 2.

$\mathbb{Z}\setminus 3\mathbb{Z} = (3\mathbb{Z}+1) \cup (3\mathbb{Z}+2)$ – все числа, не делящиеся на 3.

Дальше работаем с $\mathbb{Z}_n$.

$\langle \mathbb{Z}_5, \underset{\text{арифм.}}{+} \rangle$ не замкн., $2+3=5 \notin \mathbb{Z}_5$.

$\langle \mathbb{Z}_5, \underset{\text{mod } 5}{+} \rangle$ – группа. $e=0$, $-(2)=3$, $-(1)=4$, $-(0)=0$.

$\langle \mathbb{Z}_5, \underset{\text{mod } 6}{+} \rangle$ не замкн.

$\langle \mathbb{Z}_5, \underset{\text{mod } 4}{+} \rangle$ – полугруппа, не моноид, т.к. $\nexists e$. $4+0 \text{ mod } 4 = 0$, а должно сохраняться число 4.

$\langle \mathbb{Z}_5, \underset{\text{mod } 5}{*} \rangle$ – моноид, не группа, т.к. $\nexists\, 0^{-1}$, $0 * x \text{ mod } 5 = 1$ не имеет решений.

$\langle \mathbb{Z}_5\setminus\{0\}, \underset{\text{mod } 5}{*} \rangle$ – группа. $2^{-1}=3$, т.к. $2*3 \text{ mod } 5 = 1$. $3^{-1}=2$. $1^{-1}=1$. $4^{-1}=4$, т.к. $4*4 \text{ mod } 5 = 1$.

$\langle \mathbb{Z}_6, \underset{\text{mod } 6}{+} \rangle$ – группа.

$\langle \mathbb{Z}_6\setminus\{0\}, \underset{\text{mod } 6}{*} \rangle$ – не замкн., $2*3 \text{ mod } 6 = 0$. 2 и 3 – т.н. "делители нуля". 4 тоже: $4*3 \text{ mod } 6 = 0$.

$\langle \{1,5\}, \underset{\text{mod } 6}{*} \rangle$ – группа. $1^{-1}=1$, $5^{-1}=5$.

*	1	5
1	1	5
5	5	1

$\langle \mathbb{Z}_4\setminus\{0\}, \underset{\text{mod } 4}{*} \rangle$ – не замкн., $2*2 \text{ mod } 4 = 0$.

$\langle \{1,3\}, \underset{\text{mod } 4}{*} \rangle$ – группа.

*	1	3
1	1	3
3	3	1

$\boxed{\exists\, a^{-1} \text{ mod } n \iff \text{НОД}(a,n)=1.}$

$9^{-1} \text{ mod } 15$ $\nexists$, т.к. $9x \text{ mod } 15 = 1 \iff \underbrace{9x - 15q}_{\vdots 3} = 1$ не решается в целых числах.

$9^{-1} \text{ mod } 14$ $\exists$, $9x - 14q = 1$ – соотн-е Безу, кот. можно получить Расш. Алг-мом Евклида. Или подбором.
$9\cdot(-3)+14\cdot 2 = 1$, $9^{-1} = -3 \text{ mod } 14 = 11$. Действительно, $9\cdot 11 \text{ mod } 14 = 1$.

$\mathbb{Z}_n = \{0, \dots, n-1\}$ – аддитивная группа (по $+ \text{ mod } n$). $|\mathbb{Z}_n| = n$.

$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : \text{НОД}(x,n)=1\}$ – мультипликативная группа (по $* \text{ mod } n$). $|\mathbb{Z}_n^*| = \varphi(n)$.

$\mathbb{Z}_6^* = \{1,5\}$. $\mathbb{Z}_9^* = \{1,2,4,5,7,8\}$. $\mathbb{Z}_5^* = \{1,2,3,4\} = \mathbb{Z}_5\setminus\{0\}$.

$\mathbb{Z}_n^* = \mathbb{Z}_n\setminus\{0\} \iff n$ простое.

$\langle \mathbb{Z}_2, \underset{mod 2}{+} \rangle$ – группа.

+	0	1
0	0	1
1	1	0

$\langle \{1\}, \underset{mod 2}{*} \rangle$ – группа $(\mathbb{Z}_2^*)$

*	1
1	1

Особый случай – $\mathbb{Z}_1 = \{0\}$.

+	0
0	0

*	0
0	0

Тот случай, когда 0 – нейтральный эл-т не только по +, но и по *.

С группами разобрались, переходим к кольцам и полям.
Это мн-ва с двумя оп-ями, условно говоря, + и *. Можно обозначить @ и ∘ или как-то ещё.

Кольцо $\langle K, +, * \rangle$:

1. $\langle K, + \rangle$ – абелева группа
2. $\langle K, * \rangle$ – полугруппа
3. $\forall a, b, c \in K$:
   $a*(b+c) = a*b + a*c$
   $(b+c)*a = b*a + c*a$

Поле $\langle F, +, * \rangle$:

1. $\langle F, + \rangle$ – абелева группа
2. $\langle F \setminus \{0\}, * \rangle$ – абелева группа
3. $\forall a, b, c \in F$:
   $a*(b+c) = a*b + a*c$
   * коммутативно ⇒ второе условие дистриб-ти не нужно.

Примечание: 0 – условное обознач-е для нейтр. эл-та по + (число 0, нулевой многочлен, нулевая матрица и т.п.)
1 – нейтр. эл-т по *.

"Коммутативное кольцо" – кольцо, где * коммутативно.
"Кольцо с единицей" – кольцо, где есть нейтр. эл-т по *.
Можно сказать, что поле – это коммутативное кольцо с единицей, где все ненулевые эл-ты обратимы по *.

$\langle \mathbb{Z}_6, \underset{mod 6}{+}, \underset{mod 6}{*} \rangle$ – кольцо, но не поле, т.к., например, $\nexists \bar{2}^{-1}$.

$\langle \mathbb{Z}_5, \underset{mod 5}{+}, \underset{mod 5}{*} \rangle$ – кольцо и поле.

$\mathbb{Z}_n$ – кольцо для $\forall n \in \mathbb{N}$ (даже для $n=1$).
$\mathbb{Z}_n$ – поле $\Leftrightarrow$ n простое. # $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \dots$
NB: 1 – не простое число, и $\mathbb{Z}_1$ – не поле, потому что $\mathbb{Z}_1 \setminus \{0\} = \varnothing$, а $\varnothing$ не может быть группой
(в группе по определению есть минимум один эл-т – нейтральный).

$\mathbb{R}$ – поле вещественных чисел. $\mathbb{Q}$ – поле рациональных чисел. $\mathbb{Z}$ – кольцо целых чисел (не поле).