Основные алгебраические структуры

Опр: 1. Бинарная операция на множестве M - это отображение из множества пар $M \times M$ в само множество M:

$$M \times M \to M \colon (a, b) \mapsto a \circ b$$

называемая обычно умножением, где $a \circ b$ называется произведением элементов.

Rm: 1. По определению любой паре $(a, b) \in M \times M$ должен сопоставляться элемент множества M и причем ровно один.

Если $|M| = m$, то $|M \times M| = m^2 \Rightarrow$ всего m^{m^2} бинарных операций существует.

Опр: 2. Полугруппой $(S, \circ)$ называется множество S с бинарной операцией $\circ$, удовлетворяющей требованию ассоциативности:

$$\forall a, b, c \in S,\ a \circ (b \circ c) = (a \circ b) \circ c$$

Примеры полугрупп:

1) $(\mathbb{N}, +)$;
2) $(\mathbb{N}, \times)$;
3) Пусть S - множество всех отображений $M \to M$, пусть $\psi, \varphi \in S$, композиция $\varphi \circ \psi$ ассоциативна, тогда $(S, \circ)$ - полугруппа;
4) Пусть $S = M$, где M - любое множество, определим композицию: $\forall a, b \in S$, $a \circ b = a$, тогда такая операция ассоциативна. Действительно $\forall a, b, c \in S$:

$$a \circ (b \circ c) = a \circ b = a$$

$$(a \circ b) \circ c = a \circ c = a$$

5) Пусть $S = M$, где M - любое множество, определим композицию: $\forall a, b \in S$, $a \circ b = U \in M$, тогда такая операция ассоциативна. Действительно $\forall a, b, c \in S$:

$$a \circ (b \circ c) = a \circ U = U$$

$$(a \circ b) \circ c = U \circ c = U$$

6) Пусть $S = \mathbb{N}$, $\forall a, b \in S$, $a \circ b = a^b$, тогда такая операция не ассоциативна. Действительно:

$$2 \circ (1 \circ 3) = 2 \circ 1^3 = 2 \circ 1 = 2^1 = 2$$

$$(2 \circ 1) \circ 3 = 2^1 \circ 3 = 2^3 = 8$$

Опр: 3. Полугруппа $(S, \circ)$ называется моноидом, если в S существует единица или нейтральный элемент, то есть такой элемент $e \in S$:

$$\forall a \in S,\ a \circ e = e \circ a = a$$

Примеры моноидов:

1) $(\mathbb{N} \cup \{0\}, +)$, $e = 0$;
2) $(\mathbb{N}, \times)$, $e = 1$;

Группы

Опр: 4. Группа - это множество G, на котором задана бинарная операция $\circ\colon G \times G \to G$, которая должна удовлетворять свойствам, называемыми аксиомами группы:

1) **Ассоциативность**:
$$\forall a, b, c \in G,\ (a \circ b) \circ c = a \circ (b \circ c)$$

2) **Существование нейтрального элемента**:
$$\exists\, e \in G \colon \forall g \in G,\ g \circ e = e \circ g = g$$
где e - нейтральный элемент или ещё его называют единицей в группе G;

3) **Существование обратного элемента**:
$$\forall g \in G,\ \exists\, h \in G \colon g \circ h = h \circ g = e$$
где h - обратный элемент к элементу g;

Простейшие следствия аксиом группы

Утв. 1. Нейтральный элемент единственен:
$$\exists!\, e \in G \colon \forall g \in G,\ g \circ e = e \circ g = g$$

□ Пусть существует две единицы $e, e' \in S$, тогда:
$$e \circ e' = e' \wedge e \circ e' = e \Rightarrow e' = e$$
■

Утв. 2. Обратный элемент единственен:
$$\forall g \in G,\ \exists!\, h \in G \colon g \circ h = h \circ g = e$$

□ Пусть существуют два обратных элемента для $g \in S\colon h, h' \in S$, тогда:
$$h = e \circ h = (h' \circ g) \circ h = h' \circ (g \circ h) = h' \circ e = h'$$
■

Обозначение: обратный элемент для элемента $g \in G$ обозначается как g^{-1}.

Опр: 5. Группа $(G, \circ)$ называется коммутативной или Абелевой, если выполнена ещё одна аксиома:

4) **Аксиома коммутативности**:
$$\forall a, b \in G,\ a \circ b = b \circ a$$

Отметим, что операция $\circ$ может быть аддитивной или мультипликативной. В аддитивном случае $\circ \equiv +$, в мультипликативном $\circ \equiv \cdot$. В аддитивном случае $e = 0$, в мультипликативном $e = 1$. Обратный элемент в аддитивном случае обозначается как $-a$, в мультипликативном как a^{-1}.

Примеры групп:

1) $(\mathbb{N}, \times)$, $e = 1$ - не будет группой, поскольку нарушается 3-ья аксиома;

2) $(S_n, \circ)$ - множество подстановок S_n степени n с операцией композиции $\Rightarrow$ группа. Мы доказывали это, когда разбирали подстановки. Но эта группа - неабелева, нет коммутативности композиции;

3) $(\mathbb{R}^n, +)$ - множество строк или столбцов в $\mathbb{R}^n$ с операцией сложения строк или столбцов:
$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$
является абелевой группой, потому что оперция сложения строк - коммутативна;

4) $(\mathbb{Z}, +)$ - абелева группа: сложение целых чисел коммутативно и ассоциативно, $\forall a \in \mathbb{N}$, $-a$ это обратный элемент;

5) $(\mathbb{Q}_+, \times)$ - абелева группа: умножение коммутативно, ассоциативно, еденица - число 1, обратный элемент к $a \in \mathbb{Q}_+$ это $\frac{1}{a} \in \mathbb{Q}_+$;

6) $(\mathbb{Q} \setminus \{0\}), \times)$ - абелева группа. Для 0 не существует обратного элемента;

7) $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \times)$ - абелевы группы;

8) $(\mathbb{Z}_n, +)$ - группа вчетов по модулю n (будут обсуждаться далее) также абелева. Нейтральный элемент - $\overline{0}$. Обратный элемент к вычету $\overline{k}$ это вычет $\overline{n-k}$. Сложение вычетов ассоциативно и коммутативно. Заметим, что эта группа - конечна;

9) $(\mathrm{Mat}_{n,n}, \times)$ - является моноидом, но не группой. Единица - единичная матрица. Но у матриц с нулевым определителем не существует обратного элемента;

10) $(\mathrm{GL}_n(\mathbb{R}), \times)$, $\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}_{n,n} \colon |A| \neq 0\}$ - общая линейная группа это квадратные невырожденные матрицы $n \times n$ с операцией умножения $\Rightarrow$ группа. Единица - единичная матрица. Обратная матрица определена для всех элементов. Умножение матриц ассоциативно, но не коммутативно, следовательно группа неабелева;

11) $(\mathrm{SL}_n(\mathbb{R}), \times)$, $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}_{n,n} \colon |A| = 1\}$ - также будет группой с анологичными свойствами, как у $(\mathrm{GL}_n(\mathbb{R}), \times)$;

Опр: 6. Множество подстановок S_n степени n с операцией композиции называется симметрической группой.

Опр: 7. Множество квадратных матриц размера $n \times n$ у которых определитель не равен нулю называется общей линейной группой относительно операции умножения и обозначается:
$$\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}_{n,n} \colon |A| \neq 0\}$$
также она называется полной матричной группой.

Опр: 8. Множество квадратных матриц размера $n \times n$ у которых определитель равен единице называется специальной линейной группой относительно операции умножения и обозначается:
$$\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}_{n,n} \colon |A| = 1\}$$

Rm: 2. В абелевых группах операция часто называется сложением и обозначается соответственно.

Множество с бинарными операциями $\supseteq$ полугруппы $\supseteq$ моноиды $\supseteq$ группы $\supseteq$ абелевы группы.

Упр. 1. Пусть G - группа и $\forall g \in G$, $gg = e$. Доказать, что G - абелева.

□
$$\forall a, b \in G,\ abab = e = baba \Rightarrow aba = babab = b(abab) = b \Rightarrow (aa)ba = ba = ab$$

■

Терминология	**Мультипликативная**	**Аддитивная**
Операция в группе	Умножение: $a \circ b$ или $a{\cdot}b$	Сложение: $a + b$
Нейтральный элемент	Единица: e или 1	Нуль: 0
	Обратный элемент: g^{-1}	Противоположный элемент: $-g$
	Степень: g^n, $n \in \mathbb{Z}$ $n > 0$: $g^n = \underbrace{g{\cdot}\ldots{\cdot}g}_{n}$, $n \in \mathbb{N}$ $n < 0$: $g^n = \underbrace{g^{-1}{\cdot}\ldots{\cdot}g^{-1}}_{\lvert n\rvert}$, $n \in \mathbb{Z}$ $n = 0$: $g^0 = e$	Целое кратное: $n{\cdot}g$, $n \in \mathbb{Z}$ $n > 0$: $n{\cdot}g = \underbrace{g + \ldots + g}_{n}$, $n \in \mathbb{Z}$ $n < 0$: $n{\cdot}g = \underbrace{(-g) + \ldots + (-g)}_{\lvert n\rvert}$, $n \in \mathbb{Z}$ $n = 0$: $0{\cdot}g = 0$

Подгруппы

Опр: 9. Пусть G - группа. Подмножество $H \subseteq G$ называется подгруппой, если:

1) $H \neq \varnothing$;
2) $\forall a, b \in H$, $a{\cdot}b \in H$;
3) $\forall a \in H$, $a^{-1} \in H$;

то есть это непустое подмножество, которое замкнуто относительно операций перемножения элементов и взятия обратного.

Утв. 3. Единица всегда принадлежит подгруппе: $e \in H \subseteq G$.

□ Так как $H \neq \varnothing$, то
$$\exists\, h \in H \Rightarrow \exists\, h^{-1} \in H \Rightarrow h \cdot h^{-1} = e \in H$$

■

Утв. 4. Подгруппа сама является группой относительно той же операции $\circ$ в G, ограниченной на H.

□ Ограничивая $\circ$ на подмножество H, по свойству 2) мы не будем выходить за пределы H:
$$\forall a, b \in H \Rightarrow a \circ_H b \in H$$
Ассоциативность вытекает из ассоциативности на большем множестве, единичный элемент содержится по утверждению выше, по свойству 3) каждый обратный элемент также существует в $H \Rightarrow$ все три аксиомы группы выполнены. ■

Примеры подгрупп:

1) Множество четных подстановок $A_n \subset S_n$ это подгруппа, так как по свойствам знака подстановок, при перемножении четных подстановок снова получим четную подстановк, обратная к четной подстановке - четная, тождественная подстановка - четная $\Rightarrow$ непустое множество;

2) Множество нечетных подстановок $S_n \setminus A_n$ не является подгруппой, поскольку произведение любых двух нечетных подстановок будет четной подстановкой $\Rightarrow$ нарушается второе условие;

3) $(\mathbb{Z},+)$, $H = \{-1,1\}$ - не является подгруппой, поскольку не содержит 0, но является группо относительно умножения;

Опр: 10. Множество четных подстановок $A_n \subset S_n$ называется знакопеременной группой степени n.

Утв. 5. Верно следующее:

$$\forall a,b \in H,\ a\cdot b^{-1} \in H \Leftrightarrow \begin{cases} \forall a,b \in H,\ a\cdot b \in H \\ \forall a \in H,\ a^{-1} \in H \end{cases}$$

$\square$

$(\Rightarrow)$ $\forall a,b \in H,\ a\cdot b^{-1} \in H \Rightarrow a\cdot a^{-1} = e \in H$, тогда: $e\cdot b^{-1} = b^{-1} \in H$, $a\cdot (b^{-1})^{-1} = a\cdot b \in H$.

$(\Leftarrow)$ $\forall a,b \in H,\ a\cdot b \in H,\ b^{-1} \in H \Rightarrow a\cdot b^{-1} \in H$. $\blacksquare$

Rm: 3. В любой группе G всегда есть подгруппы $H = \{e\}$, $H = G$ - несобственные подгруппы. Остальные подгруппы - собственные.

Кольцо

Опр: 11. Кольцо $(K,+,\times)$ - это множество K с двумя бинарными операциями - сложением и умножением, которые удовлетворяют свойствам, называемыми аксиомами кольца:

1) **Коммутативность сложения**:
$$\forall a,b \in K,\ a+b = b+a$$

2) **Ассоциативность сложения**:
$$\forall a,b,c \in K,\ a+(b+c) = (a+b)+c$$

3) **Существование нулевого элемента**:
$$\exists\, 0 \in K : \forall a \in K,\ 0+a = a$$

4) **Существование противоположного элемента**:
$$\forall a \in K,\ \exists\, b \in K : a+b = 0$$

   Обозначение: $b = -a$

5) **Дистрибутивность умножения относительно сложения** (левая):
$$\forall a,b,c \in K,\ a\cdot(b+c) = a\cdot b + a\cdot c$$

6) **Дистрибутивность умножения относительно сложения** (правая):
$$\forall a,b,c \in K,\ (b+c)\cdot a = b\cdot a + c\cdot a$$

Свойства $1)-4)$ для множества K относительно операции сложения дают структуру абелевой группы, то есть: $(K,+)$ - абелева группа. Такая группа называется аддитивной группой кольца K.

Rm: 4. Правая дистрибутивность не следует из левой и наобоорот, потому что про умножение нет предположения о коммутативности.

Классы колец

Опр: 12. Кольцо $(K, +, \times)$ называется коммутативным, если $\forall a, b \in K,\ a{\cdot}b = b{\cdot}a$.

Опр: 13. Кольцо $(K, +, \times)$ называется ассоциативным, если $\forall a, b, c \in K,\ a{\cdot}(b{\cdot}c) = (a{\cdot}b){\cdot}a$.

Опр: 14. Кольцо $(K, +, \times)$ называется кольцом с единицей, если $\exists\, 1 \in K\colon \forall a \in K,\ 1{\cdot}a = a{\cdot}1 = a$.

Существуют и другие классы колец, которые мы пока затрагивать не будем.

Примеры колец:

1) $(\mathbb{Z}, +, \times)$ - коммутативное, ассоциативное кольцо с единицей;
2) $(\mathrm{Mat}_{n,n}, +, \times)$ - некоммутативное, ассоциативное кольцо с единицей;
3) $K = \{$**геом. векторы в пространстве**$\}$ с операциями сложения векторов и векторного произведения, где $\forall a, b \in K$ векторное произведение $a{\cdot}b$ это вектор, перпендикулярный плоскости натянутой на a, b, длина которого равна площади параллелограмма построенного на этих векторах.

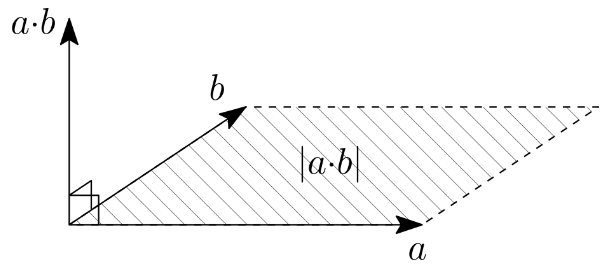

Рис. 1: Векторное произведение

Это будет некоммутативное, неассоциативное кольцо без единцы (поскольку любой вектор, умноженный сам на себя даст 0);

4) $(\mathbb{Z}, +, \times)$ - коммутативное, ассоциативное кольцо;
5) $(\mathbb{Q}, +, \times)$ - коммутативное, ассоциативное кольцо;
6) $(\mathbb{R}, +, \times)$ - коммутативное, ассоциативное кольцо;
7) $(\mathbb{Z}_n, +, \times)$ - конечное, коммутативное кольцо вычетов;
8) $(\mathcal{F}(M, \mathbb{R}), +, \times)$ - кольцо функций, где M - произвольное множество, $f\colon M \to \mathbb{R}$. Рассмотрим все такие функции $\mathcal{F}(M, \mathbb{R}) = \{f\colon M \to \mathbb{R}\}$ и введем на этом множестве бинарные операции:

$$(f_1 + f_2)(m) = f_1(m) + f_2(m),\ \forall m \in M$$

$$(f_1{\cdot}f_2)(m) = f_1(m){\cdot}f_2(m),\ \forall m \in M$$

Множество функций с операцией + - абелева группа, умножение функций ассоциативно и обладает единицей ($f \equiv 1$), умножение коммутативно поскольку коммутативно умножение действительных чисел. Следовательно, это коммутативное, ассоциативное кольцо;

Простейшие следствия аксиом кольца

Утв. 6. Нулевой элемент единственен:

$$\exists!\, 0 \in K \colon \forall a \in K,\, 0 + a = a$$

□ Следует напрямую из такого же свойства для группы. В качестве упражнения, пусть $0, 0' \in K$ - два нулевых элемента, тогда:

$$0 = 0 + 0' = 0' + 0 = 0'$$

■

Утв. 7. Противоположный элемент единственен для каждого $a \in K$:

$$\forall a \in K,\, \exists!\, b \in K \colon a + b = 0$$

□ Аналогично следует напрямую из свойства для группы. Пусть $b, b' \in K$ - два противоположных элемента $\forall a \in K$, тогда:

$$b = b + 0 = b + (a + b') = (b + a) + b' = 0 + b' = b'$$

■

Rm: 5. Всякое кольцо является абелевой группой по сложению и там мы уже доказывали свойства выше $\Rightarrow$ доказано.

Утв. 8. Единичный элемент для кольца с единицей - единственен:

$$\exists!\, 1 \in K \colon \forall a \in K,\, a{\cdot}1 = 1{\cdot}a = a$$

□ Пусть существует две единицы $1, 1' \in K$, тогда:

$$1 = 1{\cdot}1' = 1'{\cdot}1 = 1'$$

■

Утв. 9. $\forall a \in K,\, 0{\cdot}a = a{\cdot}0 = 0$.

□

$$\forall a \in K,\, 0{\cdot}a = (0 + 0){\cdot}a = 0{\cdot}a + 0{\cdot}a \Rightarrow 0{\cdot}a + (-(0{\cdot}a)) = 0{\cdot}a + 0{\cdot}a + (-(0{\cdot}a)) \Rightarrow 0 = 0{\cdot}a$$
$$\forall a \in K,\, a{\cdot}0 = a{\cdot}(0 + 0) = a{\cdot}0 + a{\cdot}0 \Rightarrow a{\cdot}0 + (-(a{\cdot}0)) = a{\cdot}0 + a{\cdot}0 + (-(a{\cdot}0)) \Rightarrow 0 = a{\cdot}0$$

■

Утв. 10. В кольце с единицей будет верно: $\forall a \in K,\, (-1){\cdot}a = a{\cdot}(-1) = -a$.

□

$$\forall a \in K,\, a + (-1){\cdot}a = 1{\cdot}a + (-1){\cdot}a = (1 + (-1)){\cdot}a = 0{\cdot}a = 0 \Rightarrow (-1){\cdot}a = -a$$
$$\forall a \in K,\, a + a{\cdot}(-1) = a{\cdot}1 + a{\cdot}(-1) = a{\cdot}(1 + (-1)) = a{\cdot}0 = 0 \Rightarrow a{\cdot}(-1) = -a$$

■

Будем рассматривать далее только **ассоциативные кольца с единицей**.

Обратимость элементов

Опр: 15. Пусть K - кольцо (ассоциативное с единицей). Элемент $a \in K$ назовем обратимым, если:

$$\exists\, b \in K\colon a{\cdot}b = b{\cdot}a = 1$$

элемент b называется обратным элементом к элементу a и обозначается $b = a^{-1}$.

Утв. 11. Обратный элемент для обратимого элемента a - единственен:

$$\exists!\, b \in K\colon a{\cdot}b = b{\cdot}a = 1$$

$\square$ Пусть $b, b' \in K$ - обратные элементы для $a \in K$, тогда:

$$b = b{\cdot}1 = b{\cdot}(a{\cdot}b') = (b{\cdot}a){\cdot}b' = 1{\cdot}b' = b'$$

$\blacksquare$

Rm: 6. Заметим, что не у каждого элемента есть обратный, тогда как в группе у каждого.

Утв. 12. Если $|K| > 1$, то 0 - необратим.

$\square$ Покажем сначала, что $1 \neq 0$, иначе:

$$\forall a \in K,\ a = a{\cdot}1 = a{\cdot}0 = 0 \Rightarrow |K| = 1$$

получили противоречие $\Rightarrow 1 \neq 0$, тогда:

$$\forall b \in K,\ 0{\cdot}b = b{\cdot}0 = 0 \neq 1 \Rightarrow \nexists\, 0^{-1}$$

$\blacksquare$

Rm: 7. Если $|K| = 1$, то ноль будет обратимым, поскольку умножением самого на себя даст сам себя.

Утв. 13. Положим $K^\times = \{a \in K\colon \exists\, b \in K\colon a{\cdot}b = b{\cdot}a = 1\}$. Докажем следующее:

1) $\forall a, b \in K^\times,\ a{\cdot}b \in K^\times$;
2) $(K^\times, \times)$ - группа, называемая мультипликативной группой кольца K;

Опр: 16. Мультипликативная группа кольца K это множество его обратимых элементов с операцией умножения.

$\square$

1) Докажем, что $(a{\cdot}b)^{-1} = b^{-1}{\cdot}a^{-1} \Rightarrow (a{\cdot}b)^{-1} \in K^\times$:

$$(a{\cdot}b){\cdot}(b^{-1}{\cdot}a^{-1}) = a{\cdot}(b{\cdot}b^{-1}){\cdot}a^{-1} = a{\cdot}1{\cdot}a^{-1} = a{\cdot}a^{-1} = 1$$

$$(b^{-1}{\cdot}a^{-1}){\cdot}(a{\cdot}b) = b^{-1}{\cdot}(a^{-1}{\cdot}a){\cdot}b = b^{-1}{\cdot}1{\cdot}b = b^{-1}{\cdot}b = 1$$

   Перестановку скобок во всех таких доказательствах мы делаем по ассоциативности операций;

2) $1 \in K^\times \Rightarrow K^\times \neq \varnothing$, множество обратимых элементов замкнуто относительно умножения $a{\cdot}b \in K^\times$. Если $a \in K^\times$ - обратим, то $a^{-1} \in K^\times$ и $(a^{-1})^{-1} = a$. Следовательно, это группа;

$\blacksquare$

Примеры мультипликативных группы кольца:

1) $\mathbb{Z}^{\times} = \{-1, 1\}$ - так как для всех остальных элементов обратные будут дробями;
2) $\mathrm{Mat}_{n,n}^{\times} = \mathrm{GL}_n(\mathbb{R}) = \{A\colon \operatorname{rk} A = n\} = \{A\colon \det A \neq 0\}$;
3) $\mathbb{Q}^{\times} = \mathbb{Q} \setminus \{0\}$;
4) $\mathbb{R}^{\times} = \mathbb{R} \setminus \{0\}$;
5) $\mathcal{F}(M, \mathbb{R})^{\times} = \{f\colon f(m) \neq 0, \forall m \in M\}$;
6) $\mathbb{Z}_n^{\times} = \{\overline{k} \in \mathbb{Z}_n \colon (k, n) = 1\}$ по теореме из курса теории чисел;

Опр: 17. Элемент $a \in K$, $a \neq 0$ называется левым делителем нуля, если:

$$\exists\, b \in K,\, b \neq 0\colon a{\cdot}b = 0$$

Опр: 18. Элемент $a \in K$, $a \neq 0$ называется правым делителем нуля, если:

$$\exists\, b \in K,\, b \neq 0\colon b{\cdot}a = 0$$

Rm: 8. Левые и правые делители бывают потому что умножение, вообще говоря, некоммутативно. Заметим, что к левому делителю нуля по определению прилагается правый делитель нуля и наоборот. При этом они могут быть не единственными.

Примеры делителей нуля:

1) В $\mathbb{Z}$ нет делителей нуля, в $\mathbb{Q}$ и в $\mathbb{R}$ также нет делителей нуля, так как произведение любых двух ненулевых элементов - ненулевое;
2) В $\mathcal{F}(M, \mathbb{R})$ рассмотрим функции $\mathcal{F}_0 = \{f\colon f \not\equiv 0 \wedge \exists\, m_0 \colon f(m_0) = 0\}$. Тогда, умножая на функцию:

$$g(m) = \begin{cases} 0, & m \neq m_0 \\ c \neq 0, & m = m_0 \end{cases} \Rightarrow f \in \mathcal{F}_0,\ f{\cdot}g \equiv 0$$

   получим, что делители нуля существуют;
3) В $\mathbb{Z}_n$ найдутся $\{\overline{k}\colon \overline{k} \neq 0 \wedge (n, k) \neq 1\} \Rightarrow$ будут делители нуля;
4) В $\mathrm{Mat}_{n,n}$ есть делители нуля, например:

$$A = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix},\ B = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \Rightarrow A, B \neq 0\colon A{\cdot}B = 0 = B{\cdot}A$$

   Таким образом, матрицы A, B - левые и правые делители нуля. Более того, в кольце квадратных матриц оказывается левые делители нуля совпадают с правыми;

Упр. 2. Доказать, что $A \in \mathrm{Mat}_{n,n}$ - делитель нуля (левый или правый) $\Leftrightarrow \operatorname{rk} A < n \Leftrightarrow \det A = 0$.

Утв. 14. Верны следующие утверждения относительно делителей нуля:

1) Делители нуля всегда необратимы;
2) Если $a, b, c \in K$, причем $a \neq 0$ и a является неделителем нуля слева (то есть не является делителем нуля слева), то тогда:
$$a \cdot b = a \cdot c \Rightarrow b = c$$
Если a является неделителем нуля справа (то есть не является делителем нуля справа), то тогда:
$$b \cdot a = c \cdot a \Rightarrow b = c$$

□

1) Пусть a - обратим и является делителем нуля слева, тогда:
$$a \cdot b = 0 \Rightarrow a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 \Rightarrow 1 \cdot b = b = a^{-1} \cdot 0 = 0 \Rightarrow b = 0$$
Аналогично, если a - делитель нуля справа, то:
$$b \cdot a = 0 \Rightarrow b \cdot a \cdot a^{-1} = 0 \cdot a^{-1} \Rightarrow b \cdot 1 = b = 0 \cdot a^{-1} = 0 \Rightarrow b = 0$$
Следовательно, элемент a не является левым и правым делителем нуля (неделитель нуля);
2) Пусть $a \cdot b = a \cdot c$, $a, b, c \in K$, тогда:
$$a \cdot b = a \cdot c \Rightarrow a \cdot b - a \cdot c = a \cdot (b - c) = 0$$
Но a это неделитель нуля слева, поэтому $b - c = 0 \Rightarrow b = c$. Пусть $b \cdot a = c \cdot a$, $a, b, c \in K$, тогда:
$$b \cdot a = c \cdot a \Rightarrow b \cdot a - c \cdot a = (b - c) \cdot a = 0 \Rightarrow b - c = 0 \Rightarrow b = c$$
где последнее верно в силу того, что a не является делителем нуля справа;

■

Нильпотент

Опр: 19. Элемент $a \in K$, $a \neq 0$ назвыается нильпотентом, если:
$$\exists\, n \colon a^n = 0$$

Примеры нильпотентов:

1) В $\mathrm{Mat}_{2,2}$ рассмотрим матрицы:
$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \Rightarrow A^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\ B = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \Rightarrow B^2 = \begin{pmatrix} 1-1 & 1-1 \\ -1+1 & -1+1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$
2) В $\mathbb{Z}_4$ есть $\overline{2}^2 = \overline{0}$;

Упр. 3. При каких n в $\mathbb{Z}_n$ существуют нильпотенты? Как они устроены?

Поле

Опр: 20. Поле - это ассоциативное, коммутативное кольцо K с единицей, в котором больше одного элемента (то есть $1 \neq 0$) и все ненулевые элементы - обратимы, то есть $K^{\times} = K \setminus \{0\}$.

Примеры полей:

1) $\mathbb{Z}$ - не является полем, так как мало обратимых элементов;
2) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ - являются полем;
3) Из матриц нельзя построить поле, так как даже для обратимых матриц возникает проблема со сложением: $A + (-A) = 0$ - необратимая матрица. Или:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$$

   Каждая из суммируемых матриц - обратима, а вот их сумма уже не обратима;

Опр: 21. Пусть K - кольцо/поле. Подмножество $L \subseteq K$ называется подкольцом/подполем, если выполнены следующие свойства:

1) Это непустое подмножество: $L \neq \varnothing$;
2) $\forall a, b, \in L,\ a + b, a{\cdot}b \in L$;
3) $\forall a \in L,\ -a \in L$, в частности $0 \in L$, так как $0 = a + (-a) \in L$;

Тогда L является подкольцом. Если выполнены ещё свойства:

4) $|L| > 1$;
5) $\forall a \in L,\ a \neq 0,\ a^{-1} \in L$, в частности $1 \in L$, так как $1 = a{\cdot}a^{-1} \in L$;

то тогда L является подполем.

По аналогии с группами, подкольцо/подполе L само является кольцом/полем относительно операций сложения и умножения в K, ограниченных на это подкольцо/подполе.

Пример подколец/подполей:

1) $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, $\mathbb{R}$ - поле $\Rightarrow \mathbb{Q}$ - это подполе в $\mathbb{R}$, а $\mathbb{Z}$ - это подкольцо в $\mathbb{Q}$, но не подполе;

Rm: 9. В теории СЛУ, векторных пространств, матриц и определители мы всюду использовали $\mathbb{R}$. Всё что мы использовали от $\mathbb{R}$ это свойства их арифметических операций. Все эти свойства имеют место для любого поля, следовательно множество $\mathbb{R}$ можно заменить на любое поле $\mathbb{K}$. И все определения, результаты и доказательства переносятся на случай произвольного поля без всяких изменений.