Линейные пространства

Определение. Множество L называется ***вещественным линейным пространством***, если для любых элементов $a,b,c \in L$ и для любых чисел $\alpha, \beta \in \mathbf{R}$ выполняются условия:

1. $a + b = b + a$;
2. $(a+b)+c = a+(b+c)$;
3. Существует нулевой элемент o, что $a + o = a$;
4. Для любого $a \in L$ существует противоположный элемент $-a \in L$ такой, что $a + (-a) = o$;
5. $\alpha(\beta a) = (\alpha\beta)a$;
6. $(\alpha + \beta)a = \alpha a + \beta a$;
7. $\alpha(a+b) = \alpha a + \alpha b$;
8. $1a = a$.

Лемма 1.1. Пусть L – вещественное линейное пространство. Тогда для любых элементов $a, b \in L$ и любых действительных чисел α, β справедливы следующие утверждения:

1 $0 \cdot a = o, \quad \alpha \cdot o = o;$

2 $(-\alpha) \cdot a = \alpha \cdot (-a) = -\alpha\, a, \quad (-\alpha) \cdot (-a) = \alpha\, a;$

3 $\alpha \cdot (a - b) = \alpha \cdot a - \alpha \cdot b, \; (\alpha - \beta) \cdot a = \alpha \cdot a - \beta \cdot a.$

1. $a+b=b+a$;

2 $(a+b)+c=a+(b+c)$;

3 Существует нулевой элемент o, что $a+o=a$;

4 Для любого $a \in L$ существует противоположный элемент $-a \in L$ такой, что $a+(-a)=o$;

5 $\alpha(\beta a)=(\alpha\beta)a$;

6 $(\alpha+\beta)a=\alpha a+\beta a$;

7 $\alpha(a+b)=\alpha a+\alpha b$;

8 $1a=a$.

Пусть M – некоторое множество, элементы которого можно складывать и умножать на числа, $m_1, m_2, \ldots, m_k \in M$, $\alpha_1, \alpha_2, \ldots, \alpha_k$ – числа.

Тогда $\alpha_1 \cdot m_1 + \alpha_2 \cdot m_2 + \ldots + \alpha_k \cdot m_k$ – ***линейная комбинация*** элементов $m_1, m_2, \ldots, m_k$.

Если $m = \alpha_1 \cdot m_1 + \alpha_2 \cdot m_2 + \ldots + \alpha_k \cdot m_k$, то говорят, что m ***линейно выражается*** через элементы m_1, $m_2, \ldots, m_k$.

L – линейное пространство, $a_1, a_2, \ldots, a_k \in L$.

Определение. Говорят, что векторы $a_1, a_2, \ldots, a_k$ ***линейно зависимы***, если существуют числа $\alpha_1, \alpha_2, \ldots, \alpha_k$, не все равные нулю одновременно, такие, что $\alpha_1 \cdot a_1 + \alpha_2 \cdot a_2 + \ldots + \alpha_k \cdot a_k = o$ (нулевому элементу линейного пространства L).

Если же равенство $\alpha_1 \cdot a_1 + \alpha_2 \cdot a_2 + \ldots + \alpha_k \cdot a_k = o$ возможно только при условии $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 0$, то векторы $a_1, a_2, \ldots, a_k$ называют ***линейно независимыми***.

Лемма 2.1. Векторы $a_1, a_2, \ldots, a_k$ линейно зависимы тогда и только тогда, когда хотя бы один из них линейно выражается через оставшиеся.

Доказательство.
Смотри лемму о линейной зависимости строк (столбцов) матрицы (§4, глава 1) или лемму 3.1 о линейной зависимости свободных векторов (§3, глава 2).

Примеры.

1. $\mathbf{E}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\mathbf{E}_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\mathbf{E}_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $\mathbf{E}_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

2. $g_1(x) = 1$, $g_2(x) = x$, $g_3(x) = x^2$, $g_4(x) = (1 + x)^2$.

3. $\mathbf{a}_1 = (2;\, -3;\, 1)$, $\mathbf{a}_2 = (3;\, -1;\, 5)$, $\mathbf{a}_3 = (1;\, -4;\, 3)$.

Определение. Максимальная линейно независимая система векторов линейного пространства называется ***базисом*** этого линейного пространства.

$e_1, e_2, \ldots, e_n \in L$ – базис, если

1) $e_1, e_2, \ldots, e_n$ – линейно независимы;

2) $e_1, e_2, \ldots, e_n, a$ – линейно зависимы для любого a из L.

Теорема 2.2. Любые два базиса линейного пространства состоят из одного и того же числа векторов.

Если в линейном пространстве L существует базис из n векторов, то пространство называют ***конечномерным***, а n называют **размерностью** линейного пространства.

$$\dim L = n$$

Если в линейном пространстве L для любого натурального n можно найти линейно независимую систему векторов, то пространство называют ***бесконечномерным***.

$$\dim L = \infty$$

Теорема 2.3 (о базисе). Каждый вектор линейного пространства линейно выражается через любой его базис, причем единственным образом.

Доказательство.
Доказательство этой теоремы полностью совпадает с доказательством теоремы 3.6 (глава 2, §3).

Определение. Коэффициенты в разложении вектора по базису называются ***координатами*** этого вектора в данном базисе.

Теорема 2.4. 1) Если вектор a имеет в базисе e_1, e_2, $\ldots$, e_n координаты $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, а вектор b имеет в том же базисе координаты $\{\beta_1, \beta_2, \ldots, \beta_n\}$, то вектор $a+b$ будет иметь в базисе e_1, e_2, $\ldots$, e_n координаты $\{\alpha_1+\beta_1, \alpha_2+\beta_2, \ldots, \alpha_n+\beta_n\}$.

2) Если вектор a имеет в базисе e_1, e_2, $\ldots$, e_n координаты $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, то для любого числа $\lambda \in \mathbb{R}$ вектор λa будет иметь в том же базисе координаты $\{\lambda\alpha_1, \lambda\alpha_2, \ldots, \lambda\alpha_n\}$.

Доказательство.

По условию $a = \alpha_1 e_1 + \alpha_2 e_2 + \dots + \alpha_n e_n,$

$b = \beta_1 e_1 + \beta_2 e_2 + \dots + \beta_n e_n.$

Тогда $a + b = (\alpha_1 e_1 + \alpha_2 e_2 + \dots + \alpha_n e_n) +$

$+ (\beta_1 e_1 + \beta_2 e_2 + \dots + \beta_n e_n) =$

$= (\alpha_1 + \beta_1) e_1 + (\alpha_2 + \beta_2) e_2 + \dots + (\alpha_n + \beta_n) e_n$

и $\lambda a = \lambda(\alpha_1 e_1 + \alpha_2 e_2 + \dots + \alpha_n e_n) =$

$= \lambda\alpha_1 e_1 + \lambda\alpha_2 e_2 + \dots + \lambda\alpha_n e_n$

Теорема 2.5. Пусть $e_1, e_2, \ldots, e_n$ и $e'_1, e'_2, \ldots, e'_n$ – два базиса линейного пространства L. Причем

$$\begin{array}{ccccccccc}
e'_1 & = & t_{11}e_1 & + & t_{21}e_2 & + & \ldots & + & t_{n1}e_n, \\
e'_2 & = & t_{12}e_1 & + & t_{22}e_2 & + & \ldots & + & t_{n2}e_n, \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
e'_n & = & t_{1n}e_1 & + & t_{2n}e_2 & + & \ldots & + & t_{nn}e_n.
\end{array}$$

Если вектор a имеет в базисе $e_1, e_2, \ldots, e_n$ координаты $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, а в базисе $e'_1, e'_2, \ldots, e'_n$ – координаты $\{\beta_1, \beta_2, \ldots, \beta_n\}$, то справедливо $\mathbf{A} = \mathbf{TB}$,

где $\mathbf{A} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}$, $\mathbf{T} = \begin{pmatrix} t_{11} & t_{12} & \ldots & t_{1n} \\ t_{21} & t_{22} & \ldots & t_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ t_{n1} & t_{n2} & \ldots & t_{nn} \end{pmatrix}$ –

так называемая матрица перехода от базиса $e_1, e_2, \ldots, e_n$ к базису $e'_1, e'_2, \ldots, e'_n$.

Пусть L – вещественное линейное пространство, L_1 – непустое подмножество в L.

Определение. L_1 называется ***подпространством*** линейного пространства L, если оно само образует линейное пространство относительно операций, определенных на L.

Теорема 3.1 (критерий подпространства). Пусть L – вещественное линейное пространство, L_1 – непустое подмножество в L. L_1 является подпространством линейного пространства L тогда и только тогда, когда для любых элементов $a, b \in L_1$ и любого действительного α выполняются условия:

1) $a - b \in L_1$; 2) $\alpha \cdot a \in L_1$.

Пример. M – множество решений системы линейных однородных уравнений с n неизвестными.

Покажем, что M – линейное пространство.
Для этого покажем, что M – подпространство $\mathbf{R}^n$.

По свойству решений СЛОУ (параграф 6, глава 2) линейная комбинация решений – также решение $\Rightarrow$
для любых $a, b \in M$ и любого действительного α:

$a - b$ и $\alpha \cdot a$ являются решениями $\Rightarrow$

$a - b \in M$ и $\alpha \cdot a \in M$.

По критерию подпространства M – подпространство $\mathbf{R}^n$, то есть само линейное пространство.

Базисом пространства M является ФСР.

$L^{(n)}$ – линейное пространство размерности n.

Определение. Отображение $f : L^{(n)} \to L^{(n)}$ называется ***линейным оператором*** линейного пространства $L^{(n)}$, если для $\forall x, y \in L^{(n)}$

1) $f(x+y) = f(x) + f(y)$,

2) $f(\alpha \cdot x) = \alpha \cdot f(x)$.

Замечание. $f(o) = f(0 \cdot x) = 0 \cdot f(x) = 0$

Пусть f – линейный оператор пространства $L^{(n)}$, $e_1, e_2, \ldots, e_n$ – некоторый базис $L^{(n)}$.

Любой вектор линейно выражается через базис $\Rightarrow$

$$
\begin{aligned}
f(e_1) &= a_{11}e_1 + a_{21}e_2 + \cdots + a_{n1}e_n \\
f(e_2) &= a_{12}e_1 + a_{22}e_2 + \cdots + a_{n2}e_n \\
&\vdots \\
f(e_n) &= a_{1n}e_1 + a_{2n}e_2 + \cdots + a_{nn}e_n
\end{aligned}
\qquad \textbf{(1)}
$$

$$
A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}
$$

– ***матрица линейного оператора*** в базисе $e_1, e_2, \ldots, e_n$

Из (1) $\Rightarrow$ $\boxed{(f(e_1)\, f(e_2)\, \ldots\, f(e_n)) = (e_1\, e_2\, \ldots\, e_n)\cdot A}$ **(2)**

$\mathbb{R}^n[x]$, f – оператор дифференцирования

Базис $1, x, x^2, x^3, \ldots, x^{n-1}$, $\quad \dim \mathbb{R}^n[x] = n$

$$f(1) = 0 = 0 \cdot 1 + 0 \cdot x + 0 \cdot x^2 + \cdots + 0 \cdot x^{n-2} + 0 \cdot x^{n-1}$$

$$f(x) = 1 = 1 \cdot 1 + 0 \cdot x + 0 \cdot x^2 + \cdots + 0 \cdot x^{n-2} + 0 \cdot x^{n-1}$$

$$f(x^2) = 2x = 0 \cdot 1 + 2 \cdot x + 0 \cdot x^2 + \cdots + 0 \cdot x^{n-2} + 0 \cdot x^{n-1}$$

$$f(x^3) = 3x^2 = 0 \cdot 1 + 0 \cdot x + 3 \cdot x^2 + \cdots + 0 \cdot x^{n-2} + 0 \cdot x^{n-1}$$

…

$$f(x^{n-1}) = (n-1)x^{n-2} = 0 \cdot 1 + 0 \cdot x + \cdots + (n-1) \cdot x^{n-2} + 0 \cdot x^{n-1}$$

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 2 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & n-1 \\ 0 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Теорема 4.1. Существует взаимно однозначное соответствие между множеством линейных операторов n-мерного линейного пространства и множеством квадратных матриц порядка n.

Определение. Если f – линейный оператор линейного пространства $L^{(n)}$, то $f(x)$ называют ***образом*** вектора $x \in L^{(n)}$.

Пусть f – линейный оператор пространства $L^{(n)}$,
A – матрица линейного оператора f,
$e_1, e_2, \ldots, e_n$ – некоторый базис $L^{(n)}$.

Теорема 4.2. Если A – матрица линейного оператора f в базисе $e_1, e_2, \ldots, e_n$ и вектор x имеет координаты $x_1, x_2, \ldots, x_n$ в этом же базисе, то координаты $y_1, y_2, \ldots, y_n$ вектора $f(x)$ находятся следующим образом:

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = A \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \quad \text{или} \quad \boxed{Y = A \cdot X} \qquad \textbf{(5)}.$$

$$
\begin{aligned}
f(e_1) &= a_{11}e_1 + a_{21}e_2 + \cdots + a_{n1}e_n \\
f(e_2) &= a_{12}e_1 + a_{22}e_2 + \cdots + a_{n2}e_n \\
&\vdots \\
f(e_n) &= a_{1n}e_1 + a_{2n}e_2 + \cdots + a_{nn}e_n
\end{aligned}
$$

$$
A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}
$$

Лемма 4.3. Если для любого столбца $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ имеет равенство $AX = BX$, где A и B – квадратные матрицы порядка n, то $A = B$.

Теорема 4.4. Если A – матрица линейного оператора f в базисе $e_1, e_2, \ldots, e_n$, то матрица B этого линейного оператора в базисе $e'_1, e'_2, \ldots, e'_n$ имеет вид:

$$\boxed{B = T^{-1} \cdot A \cdot T,}$$

где T – матрица перехода от базиса $e_1, e_2, \ldots, e_n$ к базису $e'_1, e'_2, \ldots, e'_n$.

Определение. Ненулевой вектор $x \in L^{(n)}$ называется ***собственным вектором*** линейного оператора f, если существует такое $\lambda_0 \in$ ▯ , что

$$f(x) = \lambda_0 x,$$

при этом λ_0 называют ***собственным значением*** линейного оператора и говорят, что собственный вектор x ***относится*** к собственному значению λ_0.

Теорема 5.1. Собственный вектор линейного оператора относится к единственному собственному значению.

Теорема 5.2 (свойство собственных векторов). Если $x_1, x_2, \ldots x_n$ – линейно независимые собственные векторы линейного оператора, относящиеся к одному и тому же собственному значению, то любая нетривиальная линейная комбинация этих векторов является собственным вектором, относящимся к этому же собственному значению.

Теорема 5.3. Собственные векторы x_1 и x_2 линейного оператора, относящиеся к различным собственным значениям, линейно независимы.

Теорема 5.4. Собственные векторы линейного оператора, относящиеся к его попарно различным собственным значениям, линейно независимы.

Пусть f – линейный оператор пространства $L^{(n)}$,
A – его матрица в некотором базисе $e_1, e_2, \ldots, e_n$.

Определение. Матрица $\lambda E - A$ называется ***характеристической матрицей*** оператора f.

$$|\lambda E - A| = \begin{vmatrix} \lambda - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \lambda - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & \lambda - a_{nn} \end{vmatrix}$$

– многочлен от λ степени n.

Определение. Определитель $|\lambda E - A|$ называется ***характеристическим многочленом*** оператора f.

Теорема 5.5. Характеристический многочлен линейного оператора не зависит от выбора базиса, то есть является инвариантом линейного оператора.

Определение. Корни характеристического многочлена, то есть корни уравнения $|\lambda E - A| = 0$, называются ***характеристическими корнями*** линейного оператора.

Теорема 5.6. 1) Любое собственное значение линейного оператора является его характеристическим корнем.
2) Любой вещественный характеристический корень линейного оператора является его собственным значением.

Определение. Оператор называется ***диагонализируемым***, если существует базис, относительно которого его матрица диагональная.

Теорема 5.7 (критерий диагонализируемости линейного оператора). Оператор является диагонализируемым тогда и только тогда, когда в пространстве существует базис, каждый вектор которого является собственным вектором этого оператора.

Определение. Пусть $L^{(n)}$ – вещественное линейное пространство. Отображение, ставящее в соответствие каждой паре векторов $x, y \in L^{(n)}$ некоторое вещественное число, обозначаемое (x, y), называется ***скалярным произведением*** векторов, если для $\forall x, y \in L^{(n)}$ и $\forall \alpha \in \mathbb{R}$ выполняется:

1) $(x, y) = (y, x)$;
2) $(\alpha x, y) = \alpha (x, y)$;
3) $(x_1 + x_2, y) = (x_1, y) + (x_2, y)$;
4) $(x, x) \geq 0$, причём $(x, x) = 0 \Leftrightarrow x = 0$.

Замечания. 1) $(x, \alpha y) = (\alpha y, x) = \alpha (y, x) = \alpha (x, y)$

2) $(x, y_1 + y_2) = (y_1 + y_2, x) = (y_1, x) + (y_2, x) = (x, y_1) + (x, y_2)$

3) $(x, o) = (x, 0 \cdot y) = 0 \cdot (x, y) = 0$

Определение. Вещественное линейное пространство, в котором определено скалярное произведение векторов, называется ***евклидовым.***

$$E^{(n)}$$

Определение. Векторы $x, y \in E^{(n)}$ называются ***ортогональными***, если $(x,\ y) = 0$.

Система векторов $x_1, x_2, \ldots, x_n \in E^{(n)}$ называется ***ортогональной***, если эти векторы попарно ортогональны.

Теорема 6.1. Любая ортогональная система ненулевых векторов является линейно независимой.

Процесс ортогонализации векторов Грама – Шмидта

Пусть $a_1, a_2, \ldots, a_n$ – линейно независимая система векторов пространства $E^{(n)}$.

Построим с помощью этой системы векторов ортогональную систему ненулевых векторов $b_1, b_2, \ldots, b_n$

Замечание. $b_1, b_2, \ldots, b_n$ – ортогональная система ненулевых векторов $\Rightarrow$ по теореме 6.1 является линейно независимой.

Определение. ***Длиной*** вектора $x \in E^{(n)}$ называется

$$|x| = \sqrt{(x, x)}$$

Также говорят ***модуль*** вектора или ***норма*** вектора.

Определение. Базис $e_1, e_2, \ldots, e_n$ евклидова пространства называется ***ортогональным***, если $\boxed{(e_i, e_k) = 0}$ при $i \neq k$.

Базис $e_1, e_2, \ldots, e_n$ евклидова пространства называется ***ортонормированным***, если

$$(e_i, e_k) = \begin{cases} 0, & i \neq k \\ 1, & i = k \end{cases}$$

Замечание. Если $e_1, e_2, \ldots, e_n$ – ортонормированный базис, то векторы $e_1, e_2, \ldots, e_n$ – попарно ортогональны и $|e_1| = |e_2| = \ldots = |e_n| = 1$.

Теорема 6.2. В любом евклидовом пространстве существуют ортонормированные базисы.

Теорема 6.3 (неравенство Коши–Буняковского). Для $\forall x, y \in E^{(n)}$ $(x,y)^2 \le (x,x)\cdot(y,y)$.

Определение. ***Углом*** между векторами $x, y \in E^{(n)}$ называется угол, косинус которого равен

$$\cos\varphi = \frac{(x,y)}{|x|\cdot|y|}$$

Определение. Говорят, что на множестве M задана ***бинарная алгебраическая операция***, если любой паре элементов из этого множества ставится в соответствие однозначно определённый элемент из этого же множества.

$$< M, * >$$

Определение. Множество M с введённой на нём бинарной алгебраической операцией называется ***полугруппой***, если для любых элементов $a, b, c \in M$ выполняется

$$a*(b*c) = (a*b)*c\ ,$$

то есть выполняется закон ассоциативности.

Определение. Пусть на множестве M задана бинарная алгебраическая операция $*$.

Элемент $e \in M$ называется ***нейтральным***, если для любого элемента $a \in M$ выполняется

$$a * e = e * a = a .$$

Элемент $a' \in M$ называется ***симметричным*** к элементу $a \in M$, если

$$a * a' = a' * a = e .$$

Лемма 7.1. Если нейтральный элемент существует, то он – единственный.

Лемма 7.2. Пусть $< M, * >$ – полугруппа. Если элемент $a \in M$ имеет симметричный элемент, то этот симметричный элемент – единственный.

Определение. Множество M с введённой на нём бинарной алгебраической операцией называется ***группой***, если

1) M – полугруппа;

2) в M существует нейтральный элемент;

3) для любого элемента $a \in M$ существует симметричный элемент.

Определение. Группа $< M, * >$ называется ***абелевой (коммутативной)***, если для любых элементов $a, b \in M$ выполняется

$$a * b = b * a.$$

Определение. Пусть M – множество, на котором заданы две алгебраические операции, которые будем называть сложение и умножение. Множество M называется ***кольцом***, если

1) $< M, + >$ – абелева группа;
2) $< M, \cdot >$ – полугруппа;
3) сложение и умножение в M связаны законами дистрибутивности, то есть для любых элементов $a, b, c \in M$ выполняется $a \cdot (b + c) = a \cdot b + a \cdot c$,

$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

Лемма 7.3. Пусть M – кольцо. Тогда для любого элемента $a \in M$ выполняется

$$a \cdot 0 = 0 \cdot a = 0.$$

Определение. Пусть M – произвольное кольцо, $a, b \in M$, $a \neq 0$, $b \neq 0$, но $ab = 0$. В этом случае элементы a и b называют ***делителями*** нуля, элемент a – ***левым***, элемент b – ***правым***.

Определение. Кольцо M называется ***коммутативным***, если для умножения выполняется коммутативный закон, то есть для любых элементов $a, b \in M$ выполняется

$$a \cdot b = b \cdot a .$$

Определение. Коммутативное кольцо называется ***полем***, если оно состоит не только из одного нулевого элемента и все элементы, отличные от нуля, образуют группу относительно операции умножения.

$< M, +, \cdot >$ – поле, если

1) $M \neq \{0\}$;

2) $< M, + >$ – абелева группа;

3) $< M \setminus \{0\}, \cdot >$ – абелева группа;

4) сложение и умножение в M связаны законами дистрибутивности.

Характерные отличия поля от кольца:

1. Любое поле содержит единичный элемент, так как относительно умножения все элементы, отличные от нулевого, образуют группу.

Кольцо не обязательно содержит единичный элемент.

2. Поле не содержит делителей нуля.

3. В поле справедлив закон сокращения для умножения, в кольце он необязательно имеет место.