Оглавление

1 Матрицы, определители и линейные уравнения

В данной книге F обозначает некоторое поле, где лежат скалярные элементы рассматриваемых объектов: определителей, матриц, коэффициентов линейных уравнений. Определение поля приведено в 1.1.5.
Заметим, что почти повсюду в данной книге читатели вполне могут обойтись наиболее важным и простым случаем, когда поле F – это множество $\mathbb{R}$ всех действительных чисел с обычными арифметическими операциями. Такие читатели могут пропустить подразделы 1.1.2–1.1.5 при первом чтении.[1]

Элементы поля F называются скалярами; в случае $F = \mathbb{R}$ скаляры – это обычные числа. Мы пока только заметим, что любое поле F содержит нулевой элемент 0 и ненулевой единичный элемент 1 и для произвольных элементов $a, b \in F$ определены операции "суммы"$a + b$ и "произведения"ab, причем эти "сумма"и "произведение"удовлетворяют определенным аксиомам, которым удовлетворяют обычные операции сложения и умножения во множестве $\mathbb{R}$. Для любого ненулевого элемента $b \in F$ определен обратный элемент по умножению b^{-1}, и определено деление $\frac{a}{b}$ любого элемента $a \in F$ на ненулевой элемент b как произведение ab^{-1}. Во многих случаях различные алгебраические объекты из данной книги содержат скаляры из поля F, которые, как было отмечено, могут рассматриваться читателями просто как обычные числа.

1.1 Группы, поля, пространства F^n и $(F^n)^T$

1.1.1. Числовые множества.

Через $\mathbb{R}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ обозначаются множества всех действительных чисел, всех натуральных чисел $n = 1, 2, \ldots$, всех целых чисел $z = 0, \pm 1, \pm 2, \ldots$ и всех рациональных чисел m/n, где $m \in \mathbb{Z}$ и $n \in \mathbb{N}$.

1.1.2. Комплексные числа.

Комплексными числами называются пары действительных чисел $z = (a, b)$ с операциями сложения и умножения

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2), (a_1, b_1)(a_2, b_2 = (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1). \quad 1.1.2(1)$$

Множество всех комплексных чисел обозначается через $\mathbb{C}$. Отождествим число $a \in \mathbb{R}$ с парой $(a, 0)$. Из 1.1.2(1) видно, что при этом отождествлении сумма переходит в сумму, а произведение – в произведение.

[1] Автор благодарен И.В.Стаценко за многочисленные полезные замечания.

Поэтому $\mathbb{R} \subset \mathbb{C}$. В дальнейшем мы будем отождествлять комплексное число $(a, 0)$ с действительным числом a.

Положим $i = (0, 1)$. Из 1.1.2(1) следует, что $i^2 = (-1, 0) = -1$. Кроме того, $(a, b) = a+bi$. Такое представление комплексного числа называется алгебраической формой комплексного числа.

Комплексное число $\overline{z} = a - bi$ называется комплексно сопряженным к z.

Модулем комплексного числа $z = a + bi$ называется неотрицательное действительное число $|z| = \sqrt{a^2 + b^2}$.

Ниже через z, z_1, z_2 и z_3 обозначаются произвольные комплексные числа. С помощью 1.1.2(1) непосредственно проверяются приведенные ниже свойства 1.1.2(2)–1.1.2(6) комплексным чисел.

$$\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}, \quad \overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}\,. \tag{1.1.2(2)}$$

Умножение комплексных чисел коммутативно и ассоциативно, т.е.,

$$z_1 z_2 = z_2 z_1, \quad (z_1 z_2) z_3 = z_1 (z_2 z_3). \tag{1.1.2(3)}$$

Модуль произведения комплексных чисел – произведение их модулей:

$$|z_1 z_2| = |z_1||z_2|, \tag{1.1.2(4)}$$

Для любого комплексного числа z имеем

$$z\overline{z} = |z|^2, \quad \text{в частности} \quad z \neq 0 \;\Leftrightarrow\; |z| \neq 0. \tag{1.1.2(5)}$$

Для любого ненулевого комплексного числа z существует обратное число, т.е. если обозначим $z^{-1} = \dfrac{1}{|z|^2}\overline{z}$, то

$$z z^{-1} = z^{-1} z = 1. \tag{1.1.2(6)}$$

1.1.3. Аддитивные и мультипликативные моноиды.
Пусть A – некоторое непустое множество, в котором выделен некоторый элемент 0_A, называемый нулем или нулевым элементом,[2] и для любых элементов $a, b \in A$ определен некоторый элемент из A, обозначаемый через $a + b$ и называемый суммой элементов a и b. Множество A или, точнее, набор $\langle A, +, 0_A, \rangle$ называется (аддитивным) моноидом, если в A выполняются указанные ниже аксиомы M1 и M2.

M1. $(a + b) + c = a + (b + c)$ для любых элементов $a, b, c \in A$.
M2. $a = a + 0_A = 0_A + a$ для любого элемента $a \in A$.

[2] По приведенному ниже свойству 4 нулевой элемент аддитивного моноида является единственным.

Часто также используются не аддитивные, а мультипликативные моноиды A, в которых вместо нулевого элемента 0_A выделен единичный элемент 1_A,[3] для любых элементов $a, b \in A$ определен некоторый единственный элемент из A, обозначаемый через $a \cdot b$ (или просто ab) и называемый произведением элементов a и b, причем в A выполняются указанные ниже аксиомы M1' и M2', фактически являющиеся аксиомами M1 и M2, записанными в другой (мультипликативной) форме. Множество A или, точнее, набор $\langle A, \cdot, 1_A, \rangle$ называется (мультипликативным) моноидом, если в A выполняются указанные ниже аксиомы M1 и M2.

M1'. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для любых элементов $a, b, c \in A$.
M2'. $a = a \cdot 1_A = 1_A \cdot a$ для любого элемента $a \in A$.

Ясно, что любым свойствам аддитивных моноидов соответствуют аналогичные свойства мультипликативных моноидов и наоборот. Поэтому свойства моноидов достаточно доказывать только для аддитивного или мультипликативного случая.

Аддитивный (соотв., мультипликативный) моноид называется коммутативным, если вдобавок к аксиомам M1 и M2 (соотв., M1' и M2') выполнена аксиома M3 (соотв., M3').

M3. $a + b = b + a$ для любых элементов $a, b \in A$.
M3'. $a \cdot b = b \cdot a$ для любых элементов $a, b \in A$.

1. Из хорошо известных свойств чисел следует, что упомянутые в 1.1.1 числовые множества $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$ и множество $\mathbb{Z}_{\geq 0}$ всех неотрицательных целых чисел являются как аддитивными моноидами относительно обычного числового сложения, так и мультипликативными моноидами относительно обычного числового умножения.

2. Множество всех натуральных чисел $\mathbb{N}$ является мультипликативным моноидом относительно обычного умножения, но не является аддитивным моноидом относительно обычного сложения, поскольку не содержит нуля.

3. Множество $\mathbb{Z}_{<0}$ всех отрицательных целых чисел не является ни аддитивным моноидом относительно обычного числового сложения (поскольку не содержит нуля), ни мультипликативным моноидом относительно обычного числового умножения (поскольку, например, произведение $(-1)(-1)$) не содержится в $\mathbb{Z}_{<0}$).

4. Нулевой (соотв., единичный) элемент аддитивного (соотв., мультипликативного) моноида A является единственным, т.е., если, например, 0_A и $0'_A$ – два нулевых элемента аддитивного моноида A, то из аксиомы

[3] По приведенному ниже свойству 4 единичный элемент мультипликативного моноида является единственным.

М2 следует, что $0'_A = 0'_A + 0_A = 0_A + 0'_A = 0_A$.

1.1.4. Группы.
Аддитивный моноид A называется (аддитивной) группой, если для любого элемента $a \in A$ задан некоторый элемент из A, обозначаемый через $-a$ и называемый противоположным к a элементом, причем вдобавок к аксиомам М1 и М2 выполнена аксиома Г1.

Г1. $a + (-a) = (-a) + a = 0_A$ для любого элемента $a \in A$.

Аналогично, мультипликативный моноид A называется (мультипликативной) группой, если для любого элемента $a \in A$ задан некоторый элемент из A, обозначаемый через a^{-1} и называемый обратным к a элементом, причем вдобавок к аксиомам М1' и М2' выполнена аксиома Г1'.

Г1'. $a \cdot a^{-1} = a^{-1} \cdot a = 1_A$ для любого элемента $a \in A$.

Аддитивная (соотв., мультипликативная) группа A называется коммутативной или абелевой группой, если A – коммутативный аддитивный (соотв., мультипликативный) моноид.

Итак, аддитивная абелева группа – это непустое множество A, где в A выделен единственный нулевой элемент 0_A, для любого элемента $a \in A$ задан единственный противоположный элемент $-a$ из A, для любых элементов $a, b \in A$ определен единственный элемент $a+b \in A$, называемый суммой элементов a и b, причем выполняются указанные ниже аксиомы АГ1–АГ4.

АГ1. $a = a + 0_A = 0_A + a$ для любого элемента $a \in A$.
АГ2. $(a + b) + c = a + (b + c)$ для любых элементов $a, b, c \in A$.
АГ3. $a + (-a) = (-a) + a = 0_A$ для любого элемента $a \in A$.
АГ4. $a + b = b + a$ для любых элементов $a, b \in A$.

Аналогично, мультипликативная абелева группа – это непустое множество A, где в A выделен единственный единичный элемент 1_A, для любого элемента $a \in A$ задан единственный обратный элемент a^{-1} из A, для любых элементов $a, b \in A$ определен единственный элемент $a \cdot b \in A$ (или просто $ab \in A$), называемый произведением элементов a и b, причем выполняются указанные ниже аксиомы АГ1'–АГ4'.

АГ1'. $a = a \cdot 1_A = 1_A \cdot a$ для любого элемента $a \in A$.
АГ2'. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для любых элементов $a, b, c \in A$.
АГ3'. $a \cdot a^{-1} = a^{-1} \cdot a = 1_A$ для любого элемента $a \in A$.
АГ4'. $a \cdot b = b \cdot a$ для любых элементов $a, b \in A$.

1. Из хорошо известных свойств чисел вытекает, что числовые множества $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$ являются аддитивными абелевыми группами относительно обычного числового сложения, но не мультипликативными абелевы-

ми группами относительно обычного числового умножения, поскольку нуль не имеет обратного элемента по умножению.

2. Относительно обычного числового сложения множество $\mathbb{Z}_{\geq 0}$ всех неотрицательных целых чисел является аддитивным моноидом, но не является группой, так как, например,не содержит число -1.

3. Множество $\mathbb{R} \setminus 0$ (соотв., $\mathbb{Q} \setminus 0$) всех действительных (соотв., рациональных) ненулевых чисел является мультипликативной группой относительно обычного умножения, но не является аддитивным моноидом относительно обычного сложения, поскольку не содержит нуля.

1.1.5. Поля и кольца.

Пусть A – непустое множество, содержащее, как минимум, два разных элемента 0_A и 1_A, причем для любых элементов a и b единственным образом определены элементы $a+b \in A$ и $a \cdot b \in A$, называемые суммой и произведением элементов a и b.

Множество A называется кольцом со сложением $+$, умножением $\cdot$, нулем 0_A и единицей 1_A, если выполнены аксиомы К1–К7:

К1. $a = a + 0_A = 0_A + a$ для любого элемента $a \in A$.
К2. $(a+b)+c = a+(b+c)$ для любых элементов $a, b, c \in A$.
К3. $a + (-a) = (-a) + a = 0_A$ для любого элемента $a \in A$.
К4. $a + b = b + a$ для любых элементов $a, b \in A$.
К5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для любых элементов $a, b, c \in A$.
К6. $a = a \cdot 1_A = 1_A \cdot a$ для любого элемента $a \in A$.
К7. $(a+b)c = a+b$, $c(a+b) = ca+b$ для любых элементов $a, b, c \in A$.

Кольцо A называется коммутативным, если в A, в дополнение к приведенным выше аксиомам **К1–К7** выполняется следующая аксиома:
К8. $ab = ba$ для любых элементов $a, b \in A$.

Заметим, что выполнение аксиом К1–К4 означает, что A – аддитивная абелева группа относительно сложения $+$ с нулем 0_A, выполнение аксиом К5–К6 ознчает, что A – мультипликативный моноид относительно умножения $\cdot$ с единицей 1_A, а выполнение аксиомы К7 связывает между собой операции сложения и умножения. Аксиома К8 означает, что мультипликативный моноид A коммутативен.

Коммутативное кольцо A называется полем, если множество $F^* = F \setminus 0$ всех его ненулевых элементов является группой, т.е. для любого ненулевого элемента $a \in F$ существует такой элемент $a^{-1} \in A^*$ (называемый обратным к a), что $aa^{-1} = a^{-1}a = 1_A$.

1. Из известных свойств чисел вытекает, что числовые множества $\mathbb{R}$ и $\mathbb{Q}$ являются полями.

2. Из 1.1.2 вытекает, что множество $\mathbb{C}$ всех комплексных чисел является

полем относительно определенных в 1.1.2 сложения и умножения.

3. Кольцо целых чисел. Из известных свойств чисел вытекает, что целые числа $\mathbb{Z}$ образуют коммутативное кольцо, не являющееся полем. Например, ненулевой элемент 2 не имеет обратного элемента по умножению в $\mathbb{Z}$.

4. Четные целые числа. Множество $2\mathbb{Z}$ всех целых чисел является аддитивной абелевой группой, в которой все аксимы коммутативного кольца кроме одной – аксиомы **K6**. Поэтому $2\mathbb{Z}$ не является кольцом в смысле нашего определения кольца.[4]

5. Множество $\mathbb{R}[x]$ всех многочленов от одной переменной x с обычными операциями сложения и умножения многочленов является коммутативным кольцом, но не является полем.
Если n – натуральное число, то множество $(\mathbb{R}[x])_{\leq n}$ всех многочленов степени $\leq n$ из $\mathbb{R}[x]$ является аддитивной абелевой группой, но не является кольцом, поскольку произведение двух многочленов степени $n \geq 1$ имеет степень $2n > n$. Заметим, что в **5** вместо $\mathbb{R}$ можно подставить любое поле F.

6. Кольца и поля характеристики 0**.** Говорят, что кольцо A – кольцо характеристики 0 или кольцо нулевой характеристики (пишут $\operatorname{char} A = 0$), если для любого натурального числа n сумма n экземпляров единицы 1_A не равна нулю 0_A.

Если F – поле характеристики 0, то можно без ограничения общности считать, что поле F содержит поле $\mathbb{Q}$ всех рациональных чисел, единицы полей F и $\mathbb{Q}$ совпадают, причем операции поля F при действии в $\mathbb{Q}$ совпадают с обычными арифметическими операциями в $\mathbb{Q}$. При этом рациональные числа m/n, где $m \in \mathbb{Z}$ и $0 \neq n \in \mathbb{Z}$, отождествляются с элементами $(m \cdot 1_A)(n \cdot 1_F)^{-1}$ поля F.

Поля $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ рациональных, действительных и комплексных чисел соответственно являются примерами полей характеристики 0.

7. Кольца положительной характеристики $n \in \mathbb{N}$ **и кольца вычетов** $\mathbb{Z}/n\mathbb{Z}$ **по модулю** n**.** Пусть A – кольцо и n – натуральное число ≥ 2. Говорят, что кольцо A – кольцо характеристики n (пишут $\operatorname{char} A = n$), если сумма n экземпляров единицы 1_A равна нулю 0_A и сумма k экземпляров 1_A не равна 0_A при $k < n$.

Для любого целого числа $m \geq 0$ обозначим через $[m]$ остаток от деления m на n. Такие остатки еще называются вычетами по модулю n. Для отрицательных чисел $-m$ будем по определению считать, что $[-m] = -[m]$.

[4] В некоторых источниках в определении кольца не требуют наличия единицы по умножению. Поэтому в таких источниках $2\mathbb{Z}$ является кольцом.

Через $\mathbb{Z}/n\mathbb{Z}$ обозначается конечное множество всех таких остатков, состоящее из n чисел $0, 1, \ldots, n-1$. Заметим, что для любых целых чисел $x, y \in \mathbb{Z}$ равенство $[x] = [y]$ равносильно тому, что число $x - y$ нацело делится на n. В частности, равенство $[x] = [0]$ равносильно тому, что x нацело делится на n.

Зададим на множестве $\mathbb{Z}/n\mathbb{Z}$ операции "сложения"$\oplus$ и "умножения"$\odot$ по правилу $[x] \oplus [y] = [x + y]$ и $[x] \odot [y] = [x \cdot y]$, где $+$ и $\cdot$ – обычные сложение и умножение целых чисел. Достаточно рутинная проверка, основанная на том, что каждое натуральное число $m \geq 2$ единственным образом разложимо в произведение степеней разных простых чисел, показывает, что множество $\mathbb{Z}/n\mathbb{Z}$ является конечным коммутативным кольцом с операциями сложения $\oplus$ и умножения $\odot$, причем нулевым и единичным элементами этого кольца являются вычеты $[0]$ и $[1]$. Противоположным элементом для вычета $[m]$ является вычет $[n - m]$.

Кольцо вычетов $\mathbb{Z}/n\mathbb{Z}$ – кольцо характеристики $k > 0$, где k – делитель числа n, равный произведению всех разных простых[5] делителей числа n. Так как сумма n экземпляров единицы $[1]$ этого кольца равна $[n] = [0]$, то $\mathbb{Z}/n\mathbb{Z}$ – кольцо некоторой характеристики $k > 0$, $k \leq n$, $[k] = [0]$ и $[y] \neq [0]$ для любого ненулевого $y \in \mathbb{N}$ с условием $y < k$. Если $k = n$, то k – делитель числа n.

Допустим, что $k < n$ и k – неделитель n. Поделив n на k с остатком, получаем $n = kx + y$, где $x, y \in \mathbb{N}$ и $0 < y < k$. Тогда $[y] = [n - ky] = [n] - [ky] = [0]$. Так как $[y] \neq [0]$, получено противоречие.

Мы показали, что k – делитель числа n. Доказательство того, что k – произведение всех различных простых делителей числа n, оставляется читателю.

8. Если x и y – ненулевые элементы поля F, то $xy \neq 0$.
Допустим, что $xy = 0$. Так как F – поле, то его ненулевой элемент y имеет обратный элемент y^{-1}. Тогда

$$x = x1 = x(yy^{-1}) = (xy)y^{-1} = 0y^{-1} = 0$$

и получаем противоречие.

9. Поля положительной характеристики и поля вычетов по модулю простого числа $p \in \mathbb{N}$.
Если F – поле характеристики $p > 0$, то p – простое число.
Допустим противное. Тогда $p = xy$, где $2 \leq x, y < p$. Из определения характеристики следует, что $[x] \neq [0]$ и $[y] \neq [0]$. Но $[x][y] = [xy] = [p] = [0]$, что противоречит 7.

[5] Напомним, что натуральное число p называется простым, если p не делится ни на какое натуральное число q с условием $1 < q < p$.

Если p – простое число, то кольцо вычетов $\mathbb{Z}/p\mathbb{Z}$ является конечным полем характеристики $p > 0$.

Обозначим через F кольцо вычетов $\mathbb{Z}/p\mathbb{Z}$. Так как сумма p экземпляров единицы $[1]$ кольца F равна $[p] = [0]$, то по 6 F – коммутативное кольцо характеристики $k \geq 2$ и k – делитель простого числа p. Поэтоиу $k = p$.

Остается доказать, что любой ненулевой элемент $[q] \in \mathbb{Z}/p\mathbb{Z}$ имеет обратный элемент. Так как $[q] \neq [0]$, то $0 < q < p$. Поскольку p делится лишь на 1 и на p, то наибольший общий делитель целых чисел p и q равен 1. Поэтому найдутся такие целые числа y и x, что $xp + yq = 1$. Поэтому $[y][q] = [yq]+[0] = [yq]+[xp] = [yq+xp] = [1]$, т.е. произвольный ненулевой элемент $[y]$ из $\mathbb{Z}/p\mathbb{Z}$ обратим.

1.1.6. Линейные (векторные) пространства.
Пусть F – поле. Линейным или векторным пространством над F или линейным F-пространством называется множество L, в котором определена операция сложения $x+y$ элементов из L, называемых векторами, и операция αx умножения вектора x на скаляры $\alpha \in F$, причем выполнены указанные ниже 8 аксиом.

Л1. Сложение ассоциативно, т.е.
$(x + y) + z = x + (y + z)$ для всех $x, y, z \in L$.

Л2. Сложение коммутативно, т.е. $x + y = y + x$ для всех $x, y \in L$.

Л3. Существует такой элемент $0 \in L$, называемый нулем или нулевым вектором , что $x + 0 = x$ для всех $x \in L$.

Л4. Для любого $x \in L$ существует такой элемент $-x \in L$, называемый противоположным к x, что $x + (-x) = 0$.

Л5. Если $\alpha, \beta \in F$ и $x \in L$, то $(\alpha\beta)x = \alpha(\beta x)$.

Л6. Если $\alpha, \beta \in F$ и $x \in L$, то $(\alpha + \beta)x = \alpha x + \beta x$.

Л7. Если α – скаляр и $x, y \in L$, то $\alpha(x + y) = \alpha x + \alpha y$.

Л8. Если $x \in L$ и 1 – единица поля F, то $1x = x$.

Выполнение аксиом **Л1–Л4** означает, что L – абелева группа относительно сложения $+$ в смысле 1.1.4.

1. Любое поле F и рассмотренные ниже в 1.1.8 пространства F^n и $(F^n)^T$ являются примерами линейных F-пространств.

2. Примерами $\mathbb{R}$-пространств являются множество всех геометрических векторов на плоскости Oxy, множество всех геометрических векторов в пространстве $Oxyz$, множество всех функций (непрерывных функций) на интервале (a, b).

3. Пусть F – поле. Множество $F_{m\times n}$ всех матрицнад F размера $m \times n$

является примером линейного F-пространства.

1.1.7. Вектор-столбцы и вектор-строки.

Пусть F – поле (например, $F = \mathbb{R}$). Столбец $(a_k)_{k=1}^n = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$, состоящий из скаляров $a_k \in F$, называется n-мерным F-вектором (или вектор-столбцом, или F-столбцом высоты n) с координатами $a_1, \ldots, a_n$. Столбец $(a_k)_{k=1}^n$ также обозначается $\vec{a}$.

Столбцу $\vec{a}$ соответствует F-строка $\vec{a}^T = (a_1, \ldots, a_n)$ длины n, где a_k – k-я координата столбца $\vec{a}$ и строки $\vec{a}^T$. Вместо $\vec{a}$ будем также писать $(a_k)_{k=1}^n$ или просто (a_k). Переход от $\vec{a}$ к $\vec{a}^T$ (и обратно) называется транспонированием вектор-строки (вектор-столбца).

Вектор-столбцы высоты n (соотв., вектор-строки длины n) часто называют столбцами (соотв., строками) или F-векторами размерности n.

1.1.8. Пространства F^n и $(F^n)^T$.
Через F^n обозначается множество всех F-столбцов высоты n. Множество всех строк длины n обозначается через $(F^n)^T$.

Если $\vec{a} = (a_k)$ и $\vec{B} = (b_k)$ – векторы из F^n, то вектор $(a_k + b_k) \in F^n$ называется суммой векторов $\vec{a}$ и $\vec{B}$ и обозначается через $\vec{a} + \vec{B}$.

Если $\vec{a}$ – вектор из F^n и $\alpha \in F$, то вектор (αa_k) из F^n, у которого k-я координата равна αa_k, $k = 1, \ldots, n$, называется произведением вектора $\vec{a}$ на элемент α поля F и обозначается через $\alpha\vec{a}$.

Нулевой столбец из одних нулей обозначается через $\vec{0}$.

Столбец $-\vec{a} = (-1) \cdot \vec{a} = (-a_k)$ называется противоположным к $\vec{a}$.

Аналогично в $(F^n)^T$ определяются сложение вектор-строк, умножение вектор-строк на числа, нулевые и противоположные вектор-строки.

Множества F^n и F^T вместе с определенными выше операциями сложения векторов и умножения их на числа называются арифметическими n-мерными пространствами.

С помощью аксиом поля из 1.1.5 нетрудно проверить, что в пространствах F^n и $(F^n)^T$ выполнены аксиомы **Л1**–**Л8** из 1.1.6. Поэтому F^n и $(F^n)^T$ являются линейными F-пространствами и обладают указанными ниже свойствами **1**–**8**, в которых L обозначает F^n или $(F^n)^T$.

1. $\vec{a} + (\vec{B} + \vec{c}) = (\vec{a} + \vec{B}) + \vec{c}$ для любых $\vec{a}, \vec{B}, \vec{c} \in L$.

2. $\vec{0} + \vec{a} = \vec{a}$ для любого $\vec{a} \in L$.

3. $\vec{a} + (-\vec{a}) = \vec{0}$.

4. $\vec{a} + \vec{B} = \vec{B} + \vec{a}$ для любых $\vec{a}, \vec{B} \in L$.

5. $1 \cdot \vec{a} = \vec{a}$ для любого $\vec{a} \in L$.

6. $(\alpha\beta) \cdot \vec{a} = \alpha \cdot (\beta \cdot \vec{a})$ для любых $\alpha, \beta \in \mathbb{R}$ и каждого $\vec{a} \in L$.

7. $(\alpha + \beta) \cdot \vec{a} = \alpha \cdot \vec{a} + \beta \cdot \vec{a}$ для любых $\alpha, \beta \in \mathbb{R}$ и каждого $\vec{a} \in L$.

8. $\alpha \cdot (\vec{a} + \vec{B}) = \alpha \cdot \vec{a} + \alpha \cdot \vec{B}$ для любого $\alpha \in \mathbb{R}$ и любых $\vec{a}, \vec{B} \in L$.

1.2 Матрицы и операции над ними

Пусть F – поле (например, $F = \mathbb{R}$).

1.2.1. Определение и обозначения матриц.

Таблица $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$,

элементов a_{ij} поля F, состоящая из m строк длины n и n столбцов высоты m называется матрицей размера $m \times n$ (над F) и также обозначается $A_{m\times n}$, $(a_{ij})_{m\times n}$ или (a_{ij}), где a_{ij} – ij-й элемент матрицы A.

Множество всех матриц размера $m \times n$ с элементами из поля F обозначается через $F_{m\times n}$. Кроме того, скаляры могут рассматриваться как матрицы размера 1×1.

Заметим, что $F_{m\times 1}$ – это множество F^m всех вектор-столбцов и $F_{1\times n} = {F^n}^T$. Поэтому вектор-столбцы и вектор-строки являются частными случаями матриц.

Столбцы и строки матрицы $A = (a_{ij})$ обозначаются $\overline{A_1}, \dots, \vec{A}_n$ $\vec{A}_1^T, \dots, \overline{A_m}^T$ соответственно.

Матрица A также записывается в виде

$A = \left(\vec{A}_1 \dots \vec{A}_n\right)$ и $A = \left(\vec{A}_1^T, \dots, \overline{A_m}^T\right)$

1.2.2. Сложение матриц и умножение их на скаляры.
Пусть $A = (a_{ij})$ и $B = (b_{ij})$ – две $m \times n$ матрицы над полем F.
Матрица $(a_{ij} + b_{ij})$ того же размера $m \times n$ называется суммой матриц A и B и обозначается через $A + B$.
Если $\alpha \in F$ и – число, то матрица (αa_{ij}) из $F_{m\times n}$, у которой ij-й элемент равен αa_{ij}, называется произведением матрицы A на число α и обозначается через αA.

Например, $(-2) \cdot \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} -2 & -4 & -6 \\ -8 & -10 & -12 \end{pmatrix}$,

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} + \begin{pmatrix} -1 & 0 & 1 \\ 2 & -3 & -4 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 4 \\ 3 & 2 & 2 \end{pmatrix}.$$

1.2.3. Некоторые матрицы.

Пусть F – поле и $A = (a_{ij}) = \left(\vec{A}_1 \dots \vec{A}_n\right) = \left(\vec{A}_1^T, \dots, \overline{A_m}^T\right)$ – матрица размера $m \times n$ с элементами $a_{ij} \in F$.

Матрица $-A = (-a_{ij})$ называется противоположной к A.

Через $O_{m\times n}$ обозначается нулевая матрица размера $m \times n$, состоящая из одних нулей поля F.

Главной диагональю матрицы A называется та ее часть, где стоят все элементы a_{kk}, $k = 1, \dots, \min(m, n)$.

Матрица A называется диагональной, если все ее элементы, лежащие вне главной диагонали, равны нулю. Диагональная матрица A обозначается $\mathrm{diag}(a_{11}, \dots)$.

Транспонированной матрицей для матрицы A размера $m \times n$ называется матрица, в которой на месте (i, j) стоит элемент a_{ji} матрицы A. Ясно, что A^T – это матрица $(b_{ij})_{n\times m} = (a_{ji})$ размера $n \times m$, получающаяся из A операцией транспонирования, при которой первая, вторая, ... строки матрицы A становятся первым, вторым, ... столбцами матрицы A^T.

Например, $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$. Результат транспонирования столбца $\vec{a} = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ высоты n – это строка $\vec{a}^T = (a_1, \dots, a_n)$ длины n.

Матрица A называется квадратной (порядка n), если $m = n$ (т.е. число строк m матрицы A равно числу n ее столбцов).

Через δ_{ij} обозначается символ Кронекера, который равен $1 \in F$, если $i = j$ и равен $0 \in F$, если $i \neq j$. Квадратная матрица E_n порядка n называется единичной матрицей (порядка n), если у нее на главной диагонали стоят единицы, а на остальных местах – нули.[6] Отметим, что единичная матрица $E = E_n \in F_{n\times n}$ – это матрица, у которой на месте (i, j) стоит символ Кронекера δ_{ij}.

Скалярными матрицами называются все квадратные диагональные матрицы, у которых везде на главной диагонали стоит одно и то же число λ, а на остальных местах стоят нули. Скалярные матрицы – это матрицы вида λE_n, $\lambda \in \mathbb{R}$.

[6] Заметим, что матрица из одних единиц **НЕ** называется единичной матрицей.

Квадратная матрица $A = (a_{ij})$ называется симметрической, если она симметрична относительно главной диагонали, т.е. если $a_{ij} = a_{ji}$ для всех i и j. Например, $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ – симметрическая матрица.

Матричной единицей $E_{ij} \in F_{m\times n}$ называется матрица E_{ij}, у которой на месте (i, j) стоит 1, и все остальные элементы равны нулю.

Через $D_i(\alpha) = E_n + (\alpha - 1)E_{ii} \in F_{n\times n}$ обозначается диагональная матрица, у которой i-ый диагональный элемент равен $\alpha \in F$, а остальные диагональные элементы равны $1 \in F$.

Элементарными матрицами называются квадратные матрицы вида $E_n + \alpha E_{ij}$ при $i \neq j$ и вида $D_i(\beta)$ при $\beta \neq 0$.

1.2.4. Свойства сумм матриц и умножения их на числа. Обозначим через L множество $F_{m\times n}$ всех матриц размера $m \times n$ над полем F. Матрицы из L будем обозначать через $A, B, C \ldots$. В L операции сложения и умножения на число, обладают указанными ниже 8 свойствами, вытекающими из соответствующих свойств операций над столбцами; см. 1.1.8. Выполнение этих 8 свойств означает, $F_{m\times n}$ является линейным F-пространством; см. 1.1.6.

Пусть A, B, C – матрицы из L одного размера и $\lambda, \nu \in F$.

1. Сложение матриц коммутативно, т.е. $A + B = B + A$.

2. Сложение матриц ассоциативно, т.е.
$(A + B) + C = A + (B + C) = A + B + C$.

3. $O + A = A + O = A$ для произвольной матрицы $A \in L$ и нулевой матрицы O того же размера.

4. Для любой матрицы A имеется такая матрица $-A$, что $A+(-A) = O$.

5. $\lambda(A + B) = \lambda A + \lambda B$.

6. $(\lambda + \nu)A = \lambda A + \nu A$.

7. $(\lambda\nu)A = \lambda(\nu A)$.

8. Если 1 – единица поля F, то $1 \cdot A = A$.

◁ **1.** $A + B = (a_{ij} + b_{ij}) = (b_{ij} + a_{ij}) = B + A$.

2. $(A + B) + C = (a_{ij} + b_{ij}) + (c_{ij}) = (a_{ij} + b_{ij} + c_{ij}) = (a_{ij}) + (b_{ij} + c_{ij}) = A + (B + C)$.

3–8. Утверждения доказываются аналогично утверждениям 1 и 2. ▷

1.2.5. Умножение строки на матрицу.
По определению произведение $\vec{a}^T \cdot \vec{B}$ произвольной строки $\vec{a}^T = (a_1, \ldots, a_n)$ длины n на столбец $\vec{B} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$ высоты n – это число, задаваемое правилом $\vec{a}^T \cdot \vec{B} = a_1 b_1 + \cdots a_n b_n$.

Например, $(1;2;3) \cdot \begin{bmatrix} 4 \\ -5 \\ 0 \end{bmatrix} = 1 \cdot 4 + 2 \cdot (-5) + 3 \cdot 0 = -6.$

Заметим, что при $n > 1$ произведение $\vec{B} \cdot \vec{a}^T$ не определено.

Пусть теперь $\vec{a}^T = (a_1, \ldots, a_n)$ строка длины n и

$$B = \left(\vec{B}_1 \vec{B}_2 \ldots \vec{B}_p\right) = \begin{pmatrix} b_{11} & b_{12} & \ldots & b_{1p} \\ \vdots & \vdots & \vdots & \vdots \\ b_{n1} & b_{12} & \ldots & b_{np} \end{pmatrix}$$

– $n \times p$ матрица, состоящая из p столбцов $\vec{B}_1, \vec{B}_2, \ldots \vec{B}_p$ высоты n.

По определению произведение $\vec{a}^T \cdot B$ строки $\vec{a}^T$) на матрицу B – это строка $\vec{C}^T = (c_1, \ldots, c_p)$ длины p, у которой первый элемент c_1 равен произведению $\vec{a}^T \cdot \vec{B}_1 = a_1 b_{11} + \ldots + a_n b_{n1}$ строки $\vec{a}^T$ на первый столбец $\vec{B}_1$ матрицы B, второй элемент c_2 равен произведению $\vec{a}^T \cdot \vec{B}_2 = a_1 b_{12} + \ldots + a_n b_{n2}$ строки $\vec{a}^T$ на второй столбец $\vec{B}_2$ матрицы B, ..., элемент c_p равен произведению $\vec{a}^T \cdot \vec{B}_p = a_1 b_{1p} + \ldots + a_n b_{np}$ строки $\vec{a}^T$ на столбец $\vec{B}_p$ матрицы B.

Например, $(1;2;3) \cdot \begin{pmatrix} 4 & 0 \\ -5 & 1 \\ 0 & -1 \end{pmatrix} = (-6;-1).$

1.2.6. Умножение $m \times n$ матрицы на $n \times p$ матрицу.
Пусть $A = (a_{ij})$ и $B = (b_{jk})$ – матрицы размеров $m \times n$ и $n \times p$ соответственно, и все их элементы лежат в поле F.
Произведением $A \times B$ называется матрица $A \cdot B$ размера $m \times p$, у которой первая строка – это определенное в 1.2.5 произведение первой строки матрицы A на матрицу B, вторая строка – произведение второй строки