§ 13. ТЕЛА, ВЕКТОРНЫЕ ПРОСТРАНСТВА НАД ТЕЛАМИ

В этом параграфе будет расширено понятие числа для того, чтобы в дальнейшем для дезарговых плоскостей использовать основной метод аналитической геометрии – метод координат. Из школьного курса математики известно, что если на евклидовой плоскости, изучаемой в школе, задать прямоугольную систему координат, то для определения положения точки достаточно знать два вещественных числа – абсциссу и ординату точки. Для точки пространства к двум числам добавляется третье – аппликата. Эти наборы чисел называются *координатами* точки. Оказывается, что для введения "координат" в любой дезарговой плоскости вещественных чисел уже недостаточно. В качестве "координат" точек в таких плоскостях нужно брать обобщенные числа, которые мы определим, используя принцип намеренно неполного знания.

Мы знаем, что множество вещественных чисел **R**, также как множество рациональных чисел **Q** и множество комплексных чисел **C**, являются *полями* (определение 2.2). Это означает, что в каждом из этих множеств определены две алгебраические операции, называемые сложением и умножением. Относительно сложения каждое из множеств является коммутативной группой и удаление нейтрального элемента (нуля) приводит к тому, что множества, вновь получившиеся, оказываются коммутативными группами относительно умножения. Кроме того, обе операции связаны дистрибутивным (распределительным) законом. Предлагаемое обобщение заключается в том, что для вновь вводимых числовых множеств, которые называются *телами*, сохраняются все перечисленные выше свойства полей, кроме одного – не требуется коммутативности умножения.

Определение 13.1. *Множество* **D** *называется* ***телом****, если в* **D** *заданы две бинарные алгебраические операции: сложение* "+" *и умножение* "×" *такие, что выполняются следующие аксиомы.*

T₁. *Множество* **D** *– коммутативная группа относительно сложения* (*с нейтральным элементом* 0_D).

T₂. *Множество* $\mathbf{D}\setminus\{0_D\}$ *– группа относительно умножения* (*с нейтральным элементом* 1_D).

T₃. *Сложение и умножение связаны законами дистрибутивности, т.е. для любых* $a,b,c\in\mathbf{D}$ *верны следующие равенства:*

$$a\times(b+c)=a\times b+a\times c,$$

$$(b+c)\times a=b\times c+c\times a\,.$$

Итак, тело является более широким понятием по сравнению с полем, поскольку аксиомы поля включают аксиомы **T₁ – T₃** и накладывают одно дополнительное условие: в поле умножение коммутативно, чего не требуется для тела. Поэтому любое поле является телом, в частности, телами являются известные нам поля **Q**, **R**, **C**, а также поле $\mathbf{Z}/(p)$ классов вычетов целых чисел по модулю простого числа p (§. 2). Далее будут приведены примеры некоммутативных тел. Такие некоммутативные числовые системы играют важную роль в математике (в частности, в геометрии). С другой стороны, многие математические конструкции связаны с телами, в которых умножение коммутативно, т.е. с полями, и существует богатая и глубокая теория полей.

Замечание 13.1. Традиционно знак «×» для обозначения умножения в теле или заменяется точкой, или вообще опускается (если это не приводит к недоразумению). Точно так же для упрощения записи нейтральные элементы тела 0_D и 1_D будем обозначать просто 0 и 1.

Предварим примеры тел рассмотрением одного простого, но важного свойства.

Лемма 13.1. *Пусть* $\mathbf{D}$ *– тело. Тогда для любого элемента* $k \in \mathbf{D}$ $0k = k0 = 0$.

Доказательство. Согласно $\mathbf{T_3}$ имеем: $0k + k = (0+1)k = 1k = k$, откуда следует, что $0k = 0$. Аналогичным образом устанавливается, что $k0 = 0$.◄

Пример 13.1. Подмножество $\mathbf{Q}(\sqrt{p})$ множества вещественных чисел $\mathbf{R}$ вида $a + b\sqrt{p}$, где p – фиксированное простое число; a,b – произвольные рациональные числа, относительно операций, индуцируемых сложением и умножением в $\mathbf{R}$, является полем. (Проверьте это!).

Пример 13.2. Подобно тому, как комплексные числа можно рассматривать как упорядоченные пары вещественных чисел с операциями:

$$(a,b) + (c,d) = (a+c, b+d),$$
$$(a,b)(c,d) = (ac - bd, ad + bc),$$

можно рассмотреть множество $\mathbf{H} = \mathbf{C} \times \mathbf{C}$ упорядоченных пар комплексных чисел, введя операции сложения и умножения следующим образом:

$$(a,b) + (c,d) = (a+c, b+d),$$
$$(a,b)(c,d) = (ac - b\overline{d}, ad + b\overline{c}).$$

Здесь $\overline{d}, \overline{c}$ – числа, комплексно сопряженные соответственно к d,c.

Упражнение 13.1. *Проверьте, что* $\mathbf{H}$ *– тело (но не поле!). Указание: если* a,b *– одновременно не равны нулю, то элемент* $(a,b)(\overline{a},-b)$ *совпа-*

дает с элементом $(a\bar{a}+b\bar{b},0)$ *и что* $(a\bar{a}+b\bar{b},0)^{-1}=(\frac{1}{a\bar{a}+b\bar{b}},0)$. *Выведите отсюда, что всякий ненулевой элемент* $\mathbf{H}$ *обратим, т.е. имеет обратный. Тело* $\mathbf{H}$ *называется телом* ***гамильтоновых кватернионов***[1].

Приведем некоторые определения, относящиеся к телам, и докажем ряд утверждений, которые понадобятся в дальнейшем.

Определение 13.2. *Пусть* $\mathbf{D}_1$ *и* $\mathbf{D}_2$ *– тела. Отображение* $f:\mathbf{D}_1\to\mathbf{D}_2$ *называется* ***морфизмом*** (*или* ***гомоморфизмом***) *тела* $\mathbf{D}_1$ *в тело* $\mathbf{D}_2$, *если* f *не является постоянным отображением и* f *согласовано с операциями сложения и умножения в* $\mathbf{D}_1$ *и* $\mathbf{D}_2$, *т.е. для любых* $a,b\in\mathbf{D}_1$ *верны равенства:*

$$f(a+_1 b)=f(a)+_2 f(b);$$
$$f(a\times_1 b)=f(a)\times_2 f(b).$$

Здесь символами $+_i$ *и* $\times_i$ *обозначены операции в теле* $\mathbf{D}_i, i\in\{1,2\}$.

Замечание 13.2. Отметим, что любой морфизм тел $f:\mathbf{D}_1\to\mathbf{D}_2$ нуль и единицу тела $\mathbf{D}_1$ переводит соответственно в нуль и единицу тела $\mathbf{D}_2$, т.е. выполняются равенства:

$$f(0_1)=0_2,\ f(1_1)=1_2.$$

Действительно, для любого $a\in\mathbf{D}_1$ имеем: $f(a+_1 0_1)=f(a)+_2 f(0_1)$, откуда следует, что $f(0_1)=0_2$. Поскольку отображение f не постоянно, существует элемент $a\in\mathbf{D}_1$ такой, что $f(a)\neq 0_2$. Тогда $f(a)=f(a\times_1 1_1)=f(a)\times_2 f(1_1)$, откуда следует, что $f(1_1)=1_2$. Это наблюдение позволяет заключить, что

отображение $f:\mathbf{D}_1\to\mathbf{D}_2$ *является морфизмом тел тогда и только тогда, когда* $f:(\mathbf{D}_1,+_1)\to(\mathbf{D}_2,+_2)$ *является морфизмом аддитивных групп и* $f|_{D_1\setminus\{0_1\}}:(\mathbf{D}_1\setminus\{0_1\},\times_1)\to(\mathbf{D}_2\setminus\{0_2\},\times_2)$ *является морфизмом мультипликативных групп.*

Далее для упрощения записи возможное различие операций в различных телах будет подразумеваться, но не фиксироваться в записи; сумму и произведение элементов a и b в произвольном теле будем обозначать $a+b$ и ab.

[1] Иногда **H** называется просто ***телом кватернионов***.

Определение 13.3. ***Изоморфизмом*** *тела* $\mathbf{D}_1$ *на тело* $\mathbf{D}_2$ *называется биективный морфизм* $f:\mathbf{D}_1\to\mathbf{D}_2$. *Изоморфизм* $f:\mathbf{D}\to\mathbf{D}$ *тела* $\mathbf{D}$ *на себя называется* ***автоморфизмом*** *тела* $\mathbf{D}$.

Упражнение 13.2. (i) *Убедитесь, что сопряжение комплексных чисел, т.е. отображение*

$$\sigma:\mathbf{C}\to\mathbf{C},\ c=a+bi\ \mapsto\ a-bi=\overline{c},\ a,b\in\mathbf{R},$$

является автоморфизмом поля $\mathbf{C}$.

(ii) *Докажите, что отображение*

$$f:\mathbf{C}\to\mathbf{H},\ a\mapsto(a,0)$$

является инъективным морфизмом (*вложением*) *поля комплексных чисел* $\mathbf{C}$ *в тело кватернионов* $\mathbf{H}$.

Пример 13.3. Пусть $\mathbf{D}$ – тело, не являющееся полем. Для всякого фиксированного $d\in\mathbf{D}, d\neq 0,$ рассмотрим отображение

$$i_d:\mathbf{D}\to\mathbf{D},\ x\mapsto\ dxd^{-1}.$$

Нетрудно проверить, что i_d – автоморфизм $\mathbf{D}$ (не для всякого d тождественный), обычно называемый ***внутренним автоморфизмом***.

Лемма 13.2. *Всякий морфизм тел* $f:\mathbf{D}_1\to\mathbf{D}_2$ *инъективен.*

Доказательство. Пусть $Ker\,f$ – множество элементов $a\in\mathbf{D}_1$ таких, что $f(a)=0$. Покажем, что $Ker\,f=\{0\}$. Допустим, что $a\in Ker\,f$ и $a\neq 0$. Тогда для произвольного элемента $b\in\mathbf{D}_1$ верно:

$$f(b)=f(1b)=f(1)f(b)=f(aa^{-1})f(b)=(f(a)(f(a^{-1}))f(b)=$$
$$f(a)(f(a^{-1})f(b))=0(f(a^{-1})f(b))=0.$$

Получили, что $\mathrm{Im}\,f=\{0\}$, т.е. противоречие с условием непостоянства отображения f. Следовательно, $Ker\,f=\{0\}$. Далее, если $f(a)=f(b)$, то $f(a-b)=0$, откуда $a-b\in Ker\,f$ и потому $a=b$, т.е. отображение f инъективно.◄

Определение 13.4. *Подмножество* H *тела* $\mathbf{D}$ *называется* ***подтелом*** *тела* $\mathbf{D}$, *если* H *относительно ограничения операций сложения и умножения на* H *само является телом.*

Учитывая замечание 13.2 и тот факт, что при любом морфизме групп $f:G_1\to G_2$ образ отображения $\mathrm{Im}\,f$ является подгруппой группы G_2, получаем, что справедливо следующее утверждение.

Лемма 13.3. *Пусть* $f:\mathbf{D}_1 \to \mathbf{D}_2$ *– морфизм тел. Тогда образ отображения* f, *т.е. множество* $\operatorname{Im} f = \{ f(a) \mid a \in \mathbf{D}_1 \}$ *является подтелом тела* $\mathbf{D}_2$.

Появление в наших рассмотрениях тел значительно расширяет набор примеров плоскостей аффинного типа. Новые плоскости строятся аналогично тому, как для произвольного поля $\mathbf{F}$ строилась арифметическая модель плоскости аффинного типа $\mathrm{A}^2(\mathbf{F})$ (§ 2).

Пример 13.4. Пусть $\mathbf{D}-$ тело и $\mathrm{A}^2(\mathbf{D}) = \{(x,y) \mid x,y \in \mathbf{D}\}$ – множество упорядоченных пар, составленных из элементов $\mathbf{D}$. Элементы множества $\mathrm{A}^2(\mathbf{D})$, т.е. пары (x,y) будем называть *точками*. Пусть $(a,b,c)-$ упорядоченная тройка элементов тела $\mathbf{D}$ такая, что a и b не равны одновременно нулю. *Прямой* будем называть подмножество $l(a,b,c)$ множества $\mathbf{Б}^2(\mathbf{D})$, определяемое следующим образом:

$$l(a,b,c) = \{(\alpha_1,\alpha_2) \in \mathrm{A}^2(\mathbf{D}) \mid \alpha_1 a + \alpha_2 b + c = 0\}.$$

Легко проверить, что $\mathrm{A}^2(\mathbf{D})$ является плоскостью аффинного типа. Доказательство проводится точно так же, как это сделано в случае поля для $\mathrm{A}^2(\mathbf{F})$ в § 2.

Плоскость $\mathrm{A}^2(\mathbf{D})$ является плоскостью параллельных переносов. И здесь проявляется полная аналогия с плоскостью $\mathrm{A}^2(\mathbf{F})$. А именно (см. § 6), каждый параллельный перенос в плоскости $\mathrm{A}^2(\mathbf{D})$ определяется парой (a,b) элементов тела $\mathbf{D}$ и имеет вид:

$$\tau_{a,b}: \mathrm{A}^2(\mathbf{D}) \to \mathrm{A}^2(\mathbf{D}),\ (m,n) \mapsto (m+a, n+b).$$

Для любых точек (m,n), $(m',n') \in \mathrm{A}^2(\mathbf{D})$ параллельный перенос $\tau_{m'-m,\,n'-n}$, очевидно, переводит первую из точек во вторую.

Покажем, что плоскость $\mathrm{A}^2(\mathbf{D})$ является дезарговой плоскостью. Пусть $P,Q,R-$ три коллинеарные точки. Нужно указать гомотетию плоскости $\mathrm{A}^2(\mathbf{D})$ с центром в точке P, переводящую Q в R. Пусть вначале $P = O = (0,0), Q = (\alpha,\beta), R = (\gamma,\delta)$. Если $\alpha \neq 0$, то $l(P,Q) = l(-\alpha^{-1}\beta,1,0)$. Поскольку $R \in l(P,Q)$, то $\delta = \gamma\alpha^{-1}\beta$. Отметим, что, так как $R \neq P$, то $\gamma \neq 0$. Теперь рассмотрим отображение

$$h: \mathrm{A}^2(\mathbf{D}) \to \mathrm{A}^2(\mathbf{D}),\ (m,n) \mapsto (km,kn),\ \text{где } k = \gamma\alpha^{-1}.$$

Легко видеть, что h есть искомая гомотетия плоскости $\mathrm{A}^2(\mathbf{D})$. В случае, когда $\alpha = 0$, имеем: $\beta \neq 0$ и рассуждение проводится аналогично. Если точка P отлична от $O = (0,0)$, то рассмотрим параллельный перенос τ, переводящий P в O. Пусть $\tau(Q) = Q', \tau(R) = R'$. По доказанному, существует гомотетия h с центром O, переводящая Q' в R'. Тогда, очевидно, отображение $\tau^{-1}h\tau$ есть гомотетия с центром P, переводящая Q в R.

Оказывается, что конструкции тел естественным образом возникают в геометрии на основе плоскостей параллельных переносов. Для каждой такой плоскости $\mathcal{A}$ определим некоторое множество $D_{\mathcal{A}}$, в котором введем две операции, чтобы получить тело, связанное с геометрией плоскости $\mathcal{A}$.

Рассмотрим множество $\overrightarrow{H}(\mathcal{A})$ векторных частей гомотетий (§ 9) плоскости $\mathcal{A}$ и положим $D_{\mathcal{A}} = \overrightarrow{H}(\mathcal{A}) \cup \{\theta\}$, где

$$\theta : \mathbf{V}(\mathcal{A}) \to \mathbf{V}(\mathcal{A}),\ \vec{a} \mapsto \vec{0}$$

– постоянное отображение множества $\mathbf{V}(\mathcal{A})$ векторов плоскости $\mathcal{A}$ в нулевой вектор. Зададим операцию умножения в $D_{\mathcal{A}}$ как композицию отображений. Ясно тогда, что $\lambda\theta = \theta\lambda = \theta,\ \forall\lambda \in D_{\mathcal{A}}$. Такое определение влечет ассоциативность операции умножения в $D_{\mathcal{A}}$. Сложение в $D_{\mathcal{A}}$ определим, исходя из следующего наблюдения.

Лемма 13.4. *Пусть* $\mu, \nu \in D_{\mathcal{A}}$. *Тогда отображение*

$$\delta : \mathbf{V}(\mathcal{A}) \to \mathbf{V}(\mathcal{A}),\ \vec{a} \mapsto \mu(\vec{a}) - \nu(\vec{a})$$

также принадлежит множеству $D_{\mathcal{A}}$.

Доказательство. (i) Отметим сначала несколько случаев, когда утверждение леммы очевидно:

1) если $\mu = \nu$, то $\delta = \theta \in D_{\mathcal{A}}$;

2) если $\nu = \theta$, то $\delta = \mu \in D_{\mathcal{A}}$;

3) если $\mu = \theta$, то $\delta = \psi\nu \in D_{\mathcal{A}}$. Здесь ψ обозначает векторную часть центральной симметрии (см. замечание 12.1).

(ii) Осталось рассмотреть случай, когда $\mu, \nu \in \overrightarrow{H}(\mathcal{A})$ и $\mu \neq \nu$. Зафиксируем точку $O \in \mathcal{A}$ и рассмотрим отображение $h : \mathcal{A} \to \mathcal{A}$, переводящее произвольную точку $A \in \mathcal{A}$ в точку $h(A)$ такую, что

$$\overrightarrow{Oh(A)} = \mu(\overrightarrow{OA}) - \nu(\overrightarrow{OA}). \tag{1}$$

Покажем, что $h-$ гомотетия плоскости $\mathcal{A}$. Из (1), пользуясь соотношением Шаля, получаем, что для любых точек $A, B \in \mathcal{A}$ верно равенство

$$\overrightarrow{h(A)h(B)} = \mu(\overrightarrow{AB}) - \nu(\overrightarrow{AB}). \tag{2}$$

Убедимся, что отображение h инъективно. Рассуждаем от противного. Допустим, что $A \neq B$, но $h(A) = h(B)$. Тогда из (2) имеем: $\vec{0} = \overrightarrow{h(A)h(B)} = \mu(\overrightarrow{AB}) - \nu(\overrightarrow{AB})$, т. е. $\mu(\overrightarrow{AB}) = \nu(\overrightarrow{AB})$. По следствию 9.1 получаем, что $\mu = \nu$ – противоречие условию (ii). Итак, отображение h инъективно, в частности, не является постоянным отображением. Поскольку гомотетия каждую прямую переводит в параллельную прямую, векторы $\overrightarrow{AB}$, $\mu(\overrightarrow{AB})$ и $\nu(\overrightarrow{AB})$ коллинеарны, поэтому из (2) вытекает, что вектор $\overrightarrow{AB}$ коллинеарен вектору $\overrightarrow{h(A)h(B)}$. Отсюда следует, что при отображении h каждая прямая переходит в параллельную прямую, т.е. $h-$ дилатация плоскости $\mathcal{A}$. Из формулы (1) вытекает, что $O-$ неподвижная точка дилатации h, следовательно, $h-$ гомотетия, $\delta-$ векторная часть гомотетии h, т.е. $\delta \in D_{\mathcal{A}}$. ◄

Отображение δ в дальнейшем обозначается символом $\mu - \nu$. Теперь в множестве $D_{\mathcal{A}}$ можно ввести операцию сложения по формуле:

$$\forall\, \alpha, \beta \in D_{\mathcal{A}} \quad \alpha + \beta = \alpha - (\theta - \beta).$$

Упражнение 13.3. *Докажите, что* $(D_{\mathcal{A}}, +)-$ *коммутативная группа с нейтральным элементом* θ.

Следующий шаг в установлении того, что $(D_{\mathcal{A}}, +, \circ)-$ тело, состоит в доказательстве законов дистрибутивности.

Лемма 13.5. *Пусть* $\alpha, \beta, \gamma \in D_{\mathcal{A}}$. *Тогда*

$$(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma, \ \gamma(\alpha + \beta) = \gamma\alpha + \gamma\beta.$$

Доказательство. Заметим, прежде всего, что для любых $\vec{a} \in \mathbf{V}(\mathcal{A})$ и $\mu, \nu \in D_{\mathcal{A}}$

$$(\mu + \nu)(\vec{a}) = \mu(\vec{a}) + \nu(\vec{a}).$$

Далее, ввиду предыдущего, для любого $\vec{a} \in \mathbf{V}(\mathcal{A})$

$$\begin{aligned}((\alpha + \beta)\gamma)(\vec{a}) &= (\alpha + \beta)(\gamma(\vec{a})) = \alpha(\gamma(\vec{a})) + \beta(\gamma(\vec{a})) = \\ &= (\alpha\gamma)(\vec{a}) + (\beta\gamma)(\vec{a}) = (\alpha\gamma + \beta\gamma)(\vec{a}).\end{aligned}$$

Следовательно, правый дистрибутивный закон имеет место. Для доказательства левого дистрибутивного закона пользуемся тем, что γ – аддитивное отображение:

$$(\gamma(\alpha+\beta))(\vec{a})=\gamma(\alpha(\vec{a})+\beta(\vec{a}))=\gamma(\alpha(\vec{a}))+\gamma(\beta(\vec{a}))=$$
$$=(\gamma\alpha)(\vec{a})+(\gamma\beta)(\vec{a})=(\gamma\alpha+\gamma\beta)(\vec{a}).\blacktriangleleft$$

Таким образом, мы доказали следующее утверждение.

Теорема 13.1. *Пусть* $\mathcal{A}$ *– плоскость параллельных переносов. Тогда* $(D_{\mathcal{A}},+,\circ)$ *– тело.*

Обратимся теперь вновь к группе векторов $\mathbf{V}(\mathcal{A})$. В § 11 для $n\in\mathbf{N}\bigcup\{0\}$ были введены понятия n-кратного $n\vec{a}$ произвольного вектора $\vec{a}\in\mathbf{V}(\mathcal{A})$ и характеристики $p=\mathrm{char}\mathcal{A}$ плоскости $\mathcal{A}$. Нам известно, что характеристика любой плоскости параллельных переносов либо равна нулю, либо является простым числом. В плоскости положительной характеристики p для любого вектора $\vec{0}\neq\vec{a}\in\mathbf{V}(\mathcal{A})$ все различные кратные исчерпываются векторами $\vec{0},\vec{a},\ldots,(p-1)\vec{a}.$ Напротив, для плоскости нулевой характеристики все кратные $n\vec{a}$ каждого ненулевого вектора $\vec{a}$ попарно различны. В этом последнем случае, допуская вольность речи, можно сказать, что вектор $n\vec{a}$ в «n раз больше» вектора $\vec{a}$.

Зададимся вопросом, что следует понимать под вектором в «n раз меньшим»? Естественным кажется следующий ответ: вектор $\vec{b}$ в «n раз меньше» вектора $\vec{a},$ если $n\vec{b}=\vec{a}.$ Ясно, что для нулевого вектора $\vec{a}=\vec{0}$ в качестве $\vec{b}$ можно взять также нулевой вектор. В случае ненулевого $\vec{a}$ кратные вектора всегда существуют, а вопрос о существовании $\vec{b}$ требует своего решения. Ответ следующим образом зависит от характеристики плоскости $\mathcal{A}$.

Лемма 13.6. *Пусть* $\vec{a}\in\mathbf{V}(\mathcal{A}),\ \vec{a}\neq\vec{0},\ n\in\mathbf{N}$. *Тогда*

(i) *если* $\mathrm{char}\mathcal{A}=0,$ *то в плоскости* $\mathcal{A}$ *существует единственный вектор* $\vec{b}\in\mathbf{V}(\mathcal{A})$ *такой, что* $n\vec{b}=\vec{a}$;

(ii) *если* $p=\mathrm{char}\mathcal{A}>0,$ *то в плоскости* $\mathcal{A}$ *существует единственный вектор* $\vec{b}\in\mathbf{V}(\mathcal{A})$ *такой, что* $n\vec{b}=\vec{a},$ *тогда и только тогда, когда числа* n *и* p *взаимно просты.*

Доказательство. Если $p=\mathrm{char}\mathcal{A}>0,$ то (утверждение 11.1) число p – простое. Разделим n на p с остатком:

$$n=kp+r,\ k,r\in\mathbf{N}\bigcup\{0\},\ r<p.$$

Для любого вектора $\vec{b}\in\mathbf{V}(\mathcal{A})$ имеем:

$$n\vec{b} = k(p\vec{b}) + r\vec{b} = k\vec{0} + r\vec{b} = r\vec{b}. \quad (3)$$

Если числа n и p не взаимно просты, то n делится на p, т.е. $r = 0$. В таком случае из (3) для любого вектора $\vec{b} \in \mathbf{V}(\mathcal{A})$ $n\vec{b} = 0\vec{b} = \vec{0}$, т.е. вектора $\vec{b}$ с требуемым свойством не существует.

Пусть теперь $\mathrm{char}\mathcal{A} = 0$, или $p = \mathrm{char}\mathcal{A} > 0$ и числа n и p взаимно просты. Во втором случае, вновь используя (3), число n можно считать одним из ненулевых остатков от деления на p, т.е. $n \in \{1, ..., p-1\}$. Зафиксируем точку $O \in \mathcal{A}$ и пусть $\vec{a} = \overrightarrow{OA}$, $A \neq O$, $l = l(O, A)$. Пусть точка B лежит вне прямой l. На прямой $l_1 = l(O, B)$ существуют точки $O, B_1 = B, B_2, ..., B_n$ со свойством: $\overrightarrow{OB_1} = \overrightarrow{B_1B_2} = ... = \overrightarrow{B_{n-1}B_n}$. В рассматриваемой ситуации вектор $\overrightarrow{OB_n} = n\overrightarrow{OB} \neq \vec{0}$, поэтому $B_n \neq O$, т.е. точка B_n также лежит вне прямой l, следовательно, направление π прямой $l(B_n, A)$ отлично от направления прямой l. Пусть $A_1 = P_{l,\pi}(B)$ и $\vec{b} = \overrightarrow{OA_1}$. Применяя малую теорему Фалеса (теорема 11.1), получаем, что $n\vec{b} = \vec{a}$ (рис. 1).

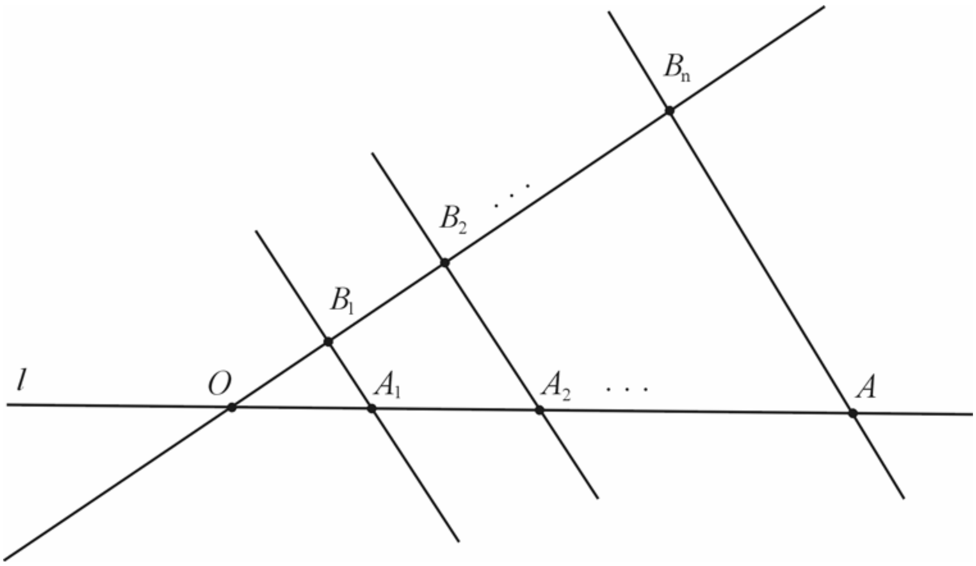

Рис. 1

Вектор $\vec{b}$ с таким свойством определяется однозначно: если $n\vec{b}_1 = n\vec{b}_2 = \vec{a}$, то $n(\vec{b}_2 - \vec{b}_1) = \vec{0}$, следовательно $\vec{b}_2 - \vec{b}_1 = \vec{0}$ или $\vec{b}_2 = \vec{b}_1$. ◄

В дальнейшем вектор $\vec{b}$ такой, что $n\vec{b}=\vec{a}$, будет обозначаться $\frac{1}{n}\vec{a}$. Теперь уже можно рассматривать и $\frac{m}{n}$-кратные векторы вида $\frac{m}{n}\vec{a}$, $m\in\mathbf{N}\bigcup\{0\}$, как m-кратные вектора $\frac{1}{n}\vec{a}$ и векторы $-\frac{m}{n}\vec{a}$ как $\frac{m}{n}$-кратные вектора $(-\vec{a})$.

Упражнение 13.4. *Докажите, что если* $mv=nu$, *где* n,v – *числа, взаимно простые с* $\operatorname{char}\mathcal{A}$, *то* $\frac{m}{n}\vec{a}=\frac{u}{v}\vec{a}$.

Из сказанного выше вытекает, что для всякого $n\in\mathbf{Z}$ и произвольного вектора $\vec{a}\in\mathbf{V}(\mathcal{A})$ определено n-кратное вектора $n\vec{a}\in\mathbf{V}(\mathcal{A})$, а в случае $\operatorname{char}\mathcal{A}=0$ даже «рациональное» кратное. Когда же $p=\operatorname{char}\mathcal{A}>0$, то для всякого $n\in\mathbf{Z}/(p)$ ($\mathbf{Z}/(p)$ – поле классов вычетов целых чисел по модулю простого числа p (см. § 2)) определено n-кратное вектора $\vec{a}$. Отметим некоторые свойства операции образования кратных. Для произвольных $\vec{a},\vec{b}\in\mathbf{V}(\mathcal{A})$ и $m,n\in\mathbf{Q}$ в случае $\operatorname{char}\mathcal{A}=0$ или $m,n\in\mathbf{Z}/(p)$ в случае $p=\operatorname{char}\mathcal{A}>0$ верны равенства:

(i) $(m+n)\vec{a}=m\vec{a}+n\vec{a}$;

(ii) $(mn)\vec{a}=m(n\vec{a})$;

(iii) $m(\vec{a}+\vec{b})=m\vec{a}+m\vec{b}$;

(iv) $1\vec{a}=\vec{a}$.

Упражнение 13.5. *Докажите свойства* (i) – (iv), *а также следующее свойство "умножения" векторов на нуль поля* $\mathbf{Q}$ (*или поля* $\mathbf{Z}/(p)$):

$$\forall\vec{a}\in\mathbf{V}(\mathcal{A})\quad 0\vec{a}=\vec{0}.$$

Посмотрим теперь на понятие такого обобщенного кратного с другой стороны. Тот факт, что n-кратное вектора $\vec{a}$, т.е. вектор $n\vec{a}$ определяется для *любого* $n\in\mathbf{Q}$ (или $n\in\mathbf{Z}/(p)$ в случае плоскости положительной характеристики) и *любого* $\vec{a}\in\mathbf{V}(\mathcal{A})$ означает, что задано отображение

$$\mathbf{Q}\times\mathbf{V}(\mathcal{A})\to\mathbf{V}(\mathcal{A}),(n,\vec{a})\mapsto n\vec{a}\quad(\text{или } \mathbf{Z}/(p)\times\mathbf{V}(\mathcal{A})\to\mathbf{V}(\mathcal{A}),(n,\vec{a})\mapsto n\vec{a}),$$

для которого выполняются условия (i) – (iv). Следующее утверждение проясняет роль равенств (i) – (iv). Значение этих условий состоит в том, что они являются характеристическими, т.е. однозначно определяющими операцию взятия кратного вектора.

Лемма 13.7. *Пусть* $\mathcal{A}$ *– плоскость параллельных переносов нулевой характеристики и пусть* $\varphi:\mathbf{Q}\times\mathbf{V}(\mathcal{A})\to\mathbf{V}(\mathcal{A})$ *– отображение такое, что для любых* $q,r\in\mathbf{Q}$ *и любых* $\vec{a},\vec{b}\in\mathbf{V}(\mathcal{A})$ *выполняются равенства:*

(i) $\varphi((q+r),\vec{a})=\varphi(q,\vec{a})+\varphi(r,\vec{a})$;

(ii) $\varphi((qr),\vec{a})=\varphi(q,\varphi(r\vec{a}))$;

(iii) $\varphi(q,(\vec{a}+\vec{b}))=\varphi(q,(\vec{a}))+\varphi(q,(\vec{b}))$;

(iv) $\varphi(1,\vec{a})=\vec{a}$.

Тогда $\varphi(q,\vec{a})=q\vec{a}$.

Доказательство. Если $q\in\mathbf{N}$, то из (i) следует, что

$$\varphi(q,\vec{a})=\varphi(\underbrace{1+...+1}_{q\text{ раз}},\vec{a})=\underbrace{\varphi(1,\vec{a})+...+\varphi(1,\vec{a})}_{q\text{ раз}}.$$

Ввиду (iv) $\varphi(1,\vec{a})=\vec{a}$, поэтому $\varphi(q,\vec{a})=q\vec{a}$.

Если $q=0$, то из (i) следует, что

$$\varphi(q,\vec{a})=\varphi(q+0,\vec{a})=\varphi(q,\vec{a})+\varphi(0,\vec{a}),$$

откуда $\varphi(0,\vec{a})=\vec{0}$, т.е. $\varphi(0,\vec{a})=0\vec{a}$.

Далее, для $q\in\mathbf{N}$ имеем:

$$\vec{0}=\varphi((q+(-q)),\vec{a})=\varphi(q,\vec{a})+\varphi(-q,\vec{a}),$$

откуда следует, что $\varphi(-q,\vec{a})=-\varphi(q,\vec{a})=-(q\vec{a})=(-q)\vec{a}$. Таким образом, в случае, когда $q\in\mathbf{Z}$, утверждение леммы справедливо.

Если $n\in\mathbf{N}$, то, используя равенство (iii), получаем:

$$\vec{a}=\varphi(1,\vec{a})=\varphi(n\frac{1}{n},\vec{a})=\varphi(n,\varphi(\frac{1}{n},\vec{a}))=n\varphi(\frac{1}{n},\vec{a}),$$

т.е. $\varphi(\frac{1}{n},\vec{a})=\frac{1}{n}\vec{a}$.

Доказательство завершается очевидным образом, если записать произвольное рациональное число в виде $q=\frac{m}{n}$, $m\in\mathbf{Z}, n\in\mathbf{N}$ и воспользоваться уже доказанным.◀

Упражнение 13.6. *Докажите аналогичное утверждение для случая, когда* $\mathrm{char}\mathcal{A}>0$.

Основываясь на таком подходе к описанию кратных, определим новый, более общий объект, играющий важную роль не только в наших рассмотрениях, но и в других разделах математики. Обобщение будет состоять в следующем:

1) вместо $\mathbf{V}(\mathcal{A})$ будем рассматривать произвольную абелеву группу $\mathbf{V}$;

2) вместо $\mathbf{Q}$ (или $\mathbf{Z}/(p)$) – произвольное тело $\mathbf{D}$;

3) вместо существование кратных векторов будем предполагать существование отображения $\varphi : \mathbf{D} \times \mathbf{V} \to \mathbf{V}$, удовлетворяющее условиям, аналогичным условиям (i) – (iv) из формулировки леммы 13.7.

Определение 13.5. *Пусть* $\mathbf{D}$ – *тело*, $\mathbf{V}$ – *абелева группа и*

$$\psi : \mathbf{D} \times \mathbf{V} \to \mathbf{V}, \ (\lambda, a) \mapsto \lambda a,$$

– *некоторое отображение, удовлетворяющее следующим условиям для любых* $\lambda, \mu \in \mathbf{D}$ *и* $a, b \in \mathbf{V}$:

$\mathbf{V}_1$. $(\lambda + \mu)a = \lambda a + \mu a$;

$\mathbf{V}_2$. $(\lambda\mu)a = \lambda(\mu a)$;

$\mathbf{V}_3$. $\lambda(a + b) = \lambda a + \lambda b$;

$\mathbf{V}_4$. $1a = a$.

Тогда тройка $(\mathbf{D}, \mathbf{V}, \psi)$ *называется* ***векторным*** (*или* ***линейным***) ***пространством над телом*** $\mathbf{D}$, *элементы группы* $\mathbf{V}$ – ***векторами***, *элементы тела* $\mathbf{D}$ – *скалярами, отображение* ψ – ***умножением*** *векторов на скаляры*[2].

Замечание 13.3. Хотя одна и та же группа $\mathbf{V}$ может быть основой различных векторных пространств, обычно векторное пространство $(\mathbf{D}, \mathbf{V}, \psi)$ обозначают одной буквой $\mathbf{V}$. Это происходит потому, что для конкретного векторного пространства в начале рассмотрения фиксируется область скаляров $\mathbf{D}$ и умножение ψ векторов на скаляры, которые не меняются в дальнейшем. $\mathbf{V}$ может обозначать также произвольное векторное пространство из некоторого класса пространств, если речь идет об общих свойствах, присущих любому векторному пространству этого класса (например, определяемому в следующем параграфе классу *конечномерных* векторных пространств). Элементы множества $\mathbf{V}$, т.е. векторы, будем далее обозначать, как обычно: $\vec{0}, \vec{a}, \vec{b}, \ldots$.

Простейшим примером векторного пространства над произвольным телом $\mathbf{D}$ является одноэлементная группа, содержащая только нулевой элемент: $\mathbf{V} = \{\vec{0}\}$. Умножение на скаляры в этом случае задается единст-

---

[2] Более точно, определенное векторное пространство называется *левым* векторным пространством над телом $\mathbf{D}$. Существует также понятие *правого* векторного пространства над телом $\mathbf{D}$ (см. [ ]). В случае, когда $\mathbf{D}$ – поле, эти понятия совпадают. В наших рассмотрениях правые векторные пространства не встречаются.

венно возможным способом: $\forall\,\lambda \in \mathbf{D}\ \ \lambda\vec{0} = \vec{0}$. Такое векторное пространство называется ***нулевым***.

Пример 12.5. Мы уже знаем, что для плоскости параллельных переносов $\mathcal{A}$ в случае $\operatorname{char}\mathcal{A} = 0$ группа $\mathbf{V}(\mathcal{A})$ – векторное пространство над полем $\mathbf{Q}$, а в случае $p = \operatorname{char}\mathcal{A} > 0$ – над полем $\mathbf{Z}/(p)$.

Кроме того, группу $\mathbf{V}(\mathcal{A})$ можно рассматривать также как векторное пространство над телом $D_{\mathcal{A}}$.

Утверждение 12.1. *Пусть $\mathcal{A}$ – плоскость параллельных переносов. Группа $\mathbf{V}(\mathcal{A})$ является векторным пространством над телом $D_{\mathcal{A}}$, если положить для $\lambda \in D_{\mathcal{A}}$ и $\vec{a} \in \mathbf{V}(\mathcal{A})$ $\ \lambda\vec{a} = \lambda(\vec{a})$.*

Упражнение 12.6. *Докажите сформулированное утверждение.*

Теперь мы применим принцип намеренно неполного знания для введения одного из основных объектов в математике. Для этого из всех свойств множества $\mathbf{V}(\mathcal{A})$ выделим только свойства $\mathbf{V}_1 - \mathbf{V}_4$ и не будем требовать, чтобы коэффициент кратности n принадлежал именно полю $\mathbf{Q}$ или $\mathbf{Z}/(p)$, а уже произвольному полю и даже телу.

Определение 12.5. *Пусть* $\mathbf{V}$ *– коммутативная группа, записываемая аддитивно* (*элементы* $\mathbf{V}$ *в рассматриваемом случае будем называть* ***векторами*** *и обозначать, как обычно,* $\vec{a}, \vec{b}, \ldots$), *а* $\mathbf{D}$ *– некоторое тело* (*возможно поле*), *элементы которого будем называть* ***скалярами***. *Предположим, что задано понятие «кратных» любого вектора* $\vec{a} \in \mathbf{V}$ *с коэффициентами кратности в* $\mathbf{D}$. *Иначе говоря, пусть для любой пары* $m \in \mathbf{D}$ *и* $\vec{a} \in \mathbf{V}$ *определен вектор, который будем обозначать* $m\vec{a}$ (*еще более формально, это означает существование отображения* $\mathbf{D} \times \mathbf{V} \to \mathbf{V}$, $(m, \vec{a}) \mapsto m\vec{a}$). *Группа* $\mathbf{V}$ *называется* ***левым векторным пространством*** *над телом* $\mathbf{D}$, *если для любых* $m, n \in \mathbf{D}$ *и* $\vec{a}, \vec{b} \in \mathbf{V}$ *выполнены свойства* $\mathbf{V}_1$ *–* $\mathbf{V}_4$.

Замечание 12.3. Коммутативная группа $\mathbf{V}$ называется *правым* векторным пространством над телом $\mathbf{D}$, если для отображения $\mathbf{D} \times \mathbf{V} \to \mathbf{V}$, $(m, \vec{a}) \mapsto m\vec{a}$) выполняются аксиомы $\mathbf{V}_1, \mathbf{V}_3, \mathbf{V}_4$ и аксиома

$\mathbf{V}_2'$: $(mn)\vec{a} = n(m\vec{a})$.

В таком случае отображение $\mathbf{D} \times \mathbf{V} \to \mathbf{V}$ обычно записывают в виде $(m, \vec{a}) \mapsto \vec{a}m$ и тогда аксиома $\mathbf{V}_2'$ выглядит более естественно: $\vec{a}(mn) = (\vec{a}m)n.$ Ясно, что если $\mathbf{D}$ – поле, то понятия левого и правого векторных пространств над $\mathbf{D}$ совпадают и говорят просто о *векторном пространстве над полем* $\mathbf{D}$.